

# Check Point InterSpect

## 業界初の内部セキュリティ・ゲートウェイ

### 製品の特徴

- ・インテリジェントなワーム防御機能
- ・ネットワーク・ゾーンのセグメント化
- ・疑わしいコンピュータの隔離
- ・LANプロトコルの防御
- ・事前の攻撃的防御

### 製品の利点

- ・ネットワーク内部でワームや攻撃の拡散をブロック
- ・ネットワークを組織別のセキュリティ・ゾーンにセグメント化
- ・攻撃および危険にさらされたデバイスを隔離
- ・Microsoftやその他のLANプロトコルを広範かつ包括的にサポート
- ・脆弱性を悪用される前の事前防御

### 課題

今日まで、ITセキュリティの担当者は、ネットワークの境界におけるセキュリティに焦点を絞ってきました。しかし、最近では攻撃がネットワーク内部から発生するケースが増加しているのが現状です。日々、ノートパソコン、PDAその他の装置がネットワークの内外を移動する環境では、正当な利用者が内部ネットワークへ感染させたり、無意識の中でトロイの木馬またはスパイウェアを通じて攻撃者にネットワーク・アクセスを許す可能性があります。

たとえば、多くのワームの場合、外部で感染したノートパソコンが内部に持ち込まれることで内部ネットワーク全体にワームが拡散し被害を発生させています。ネットワーク・デバイスが1台でもワームに感染すると、一瞬にして、ネットワーク全体に広がります。「フラッシュ・ワーム」あるいは「ブリッツ・ワーム」と呼ばれることが多い高速に被害が拡大するタイプのワームは、一旦発生すると数分以内に世界中に拡散します。

このような甚大な被害を及ぼす脅威がますます一般的になるにつれて、企業はネットワーク内部で発生するワーム、不正アクセスの脅威、その他の攻撃に対抗できる、より効果的な防御策の必要性を認識するようになりました。

### 解決策

Check Point InterSpect™は、ネットワーク内部におけるワームや攻撃の拡散をブロックし、ネットワーク・ゾーンをセグメント化する機能を備えたネットワーク内部セキュリティ専用のゲートウェイです。チェック・ポイントの実績あるセキュリティ技術であるINSPECT™、ステートフル・インスペクション、Application Intelligence™、SMART管理アーキテクチャをベースとするInterSpectは、内部ネットワーク・セキュリティに特化して開発されました。InterSpectには、以下の特長があります。

- ・インテリジェントなワーム防御機能 (Intelligent Worm Defender™)
  - ネットワーク内部におけるワームや攻撃の拡散を防止
- ・ネットワーク・ゾーンのセグメント化
  - 内部ネットワークを部門別のセキュリティ・ゾーンにセグメント化
- ・疑いのあるコンピュータの隔離
  - 攻撃を行っているデバイスやワームなどに感染したデバイスを隔離
- ・LANプロトコルの防御
  - Microsoftおよび、その他のLANプロトコルを広範かつ包括的にサポート
- ・攻撃を未然に防御
  - 脆弱な部分をあらかじめ防御し、攻撃を未然に防御



InterSpectは、柔軟かつシームレスに既存ネットワーク環境に導入できるように設計され、内部セキュリティ専用開発された管理インタフェースを備えています。



Intelligent Security

## 機能と特長

### インテリジェントなワーム防御機能 ( Intelligent Worm Defender )

Intelligent Worm Defenderは、チェック・ポイントのステートフル・インスペクションおよびApplication Intelligence技術を応用し、内部ネットワークをワームから非常に強力に保護します。これらの技術は、最も包括的で適応力のある保護を提供するチェック・ポイントのINSPECT技術をベースにしています。InterSpectは、保護すべきネットワーク・ゾーンの間にインストールし、接続デバイスからのトラフィックをチェックし、危険なトラフィックをブロックすることで、ネットワーク内部でワームが拡散することを防ぎます。

### ネットワーク・ゾーンのセグメント化

InterSpectは、管理者が定義した複数のセキュリティ・ゾーンにネットワークをセグメント化（分割）し、ゾーン間の不正アクセスを防止します。これにより、データを参照する権限のユーザやワームに汚染されたコンピュータがゾーンを越えて情報やシステムにアクセスすることを防止します。ネットワーク・ゾーンのセグメント化には、攻撃をネットワークのサブセグメント内に封じ込める働きもあります。

### 隔離

InterSpectは、ネットワーク上で疑いのあるコンピュータまたは感染したコンピュータを識別して隔離することにより、他のネットワークに攻撃が及ぶことや、ワームへの感染が拡散することを防止します。また、管理者がセキュリティ・パッチによる対策を行うまでの間、コンピュータを隔離することも可能です。疑わしきデバイスを隔離することで、ネットワーク管理者が必要なパッチを確認し、インストールしテストを行う間に感染が広がるリスクを低減します。

InterSpectは隔離されたことをユーザに通知する独自機能があります。ネットワーク利用者のコンピュータからウイルスやワームへの感染が検出されたなどの理由により隔離されると、このユーザに対しカスタマイズされた動的なWebページで通知します。この通知により、ヘルプ・デスクは、問題のトラブルシューティングにかかる時間を最小限におさえ、また、ネットワーク管理者も問題をいち早く認識することができるため、ネットワークのダウンタイムを大幅に短縮します。

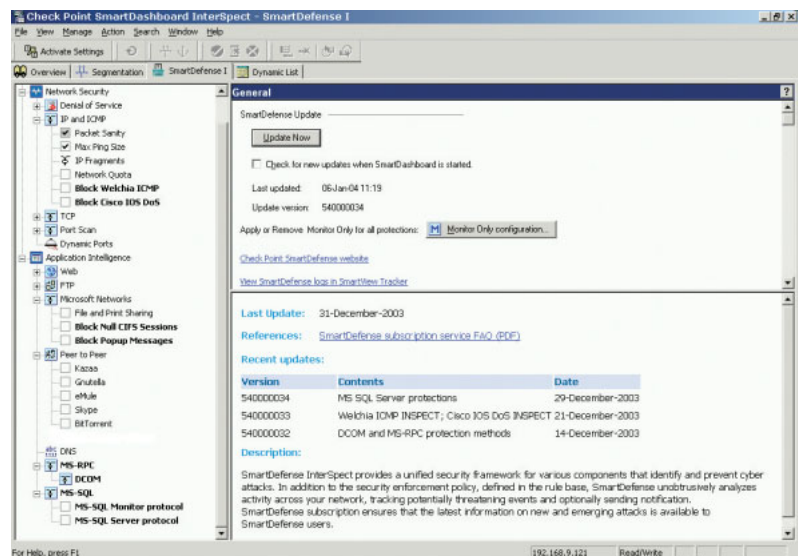
## LANプロトコルの防御

InterSpectは、Sun RPC、DCE RPC、HTTPなどを含むLANプロトコルに加え、MS RPC、CIFS、MS SQL、DCOMなどのMicrosoftプロトコルも広範かつ包括的にサポートします。InterSpectは、INSPECT技術を使用して、業界で最も適応性の高いセキュリティ検査機能を実現しています。チェック・ポイントのSmartDefense™サービスへの加入により定期的に提供されるINSPECTのアップデートを活用することにより、InterSpectのユーザは、新しい攻撃や脅威が出現しても、内部セキュリティ・インフラを常に最新の状態に維持することができます。

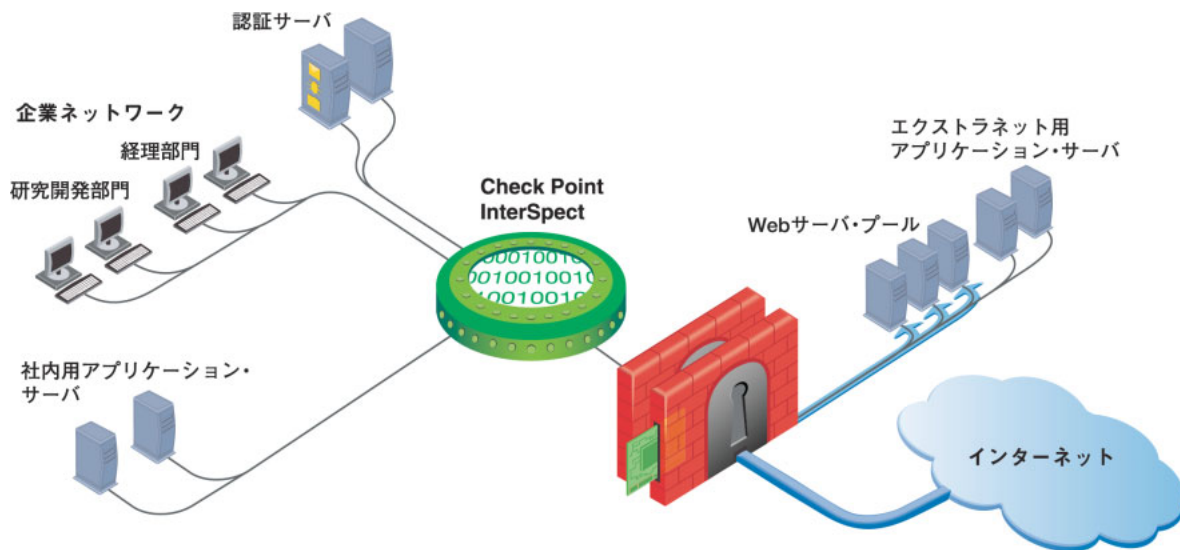
### 攻撃を未然に防御

InterSpectは、既知および未知の攻撃に対し能動的で動的な保護機能を提供しますので、脆弱性を突いた攻撃が行われる前に確実な防御を行うことができます。

InterSpectは、内部ネットワーク・セキュリティ専用にかスタマイズされたSmartDefenseが組み込まれているため、管理者は業界で最もインテリジェントで適応性の高いセキュリティ検査技術であるINSPECTを基礎にしたステートフル・インスペクションおよびApplication Intelligenceを用いて、ネットワークやアプリケーションへのあらゆる攻撃に対して防御機能を導入、実施し、アップデートすることが可能です。



InterSpectは、内部ネットワーク用のSmartDefenseを内蔵し、ネットワーク内部における既知および未知の攻撃からネットワークを能動的に保護します。



InterSpectは、内部セキュリティ専用設計された唯一のソリューションです。

### 内部セキュリティ管理機能

InterSpectの管理は、内部セキュリティ専用設計された管理インターフェースを使用することで容易に行えます。この管理インターフェースは、チェック・ポイントのSMART管理アーキテクチャをベースにしており、内部セキュリティ固有の設定やポリシー管理に対応した、高機能で使いやすいインターフェースです。

一般的に、ネットワーク・レベルのファイアウォールは、明示的に許可しないかぎり、すべてのトラフィックをドロップするように設定されますが、通常このような方法で設定を行

う製品を内部ネットワーク用として使用すると、設定が極端に複雑になる可能性があります。対照的に、チェック・ポイントのInterSpectでは、ネットワークにInterSpectを導入し、ネットワーク・セキュリティ・ゾーンを定義するだけで、セキュリティ・ゾーンのセグメント化が非常に簡単に行えます。ネットワーク内に導入されたInterSpectは、直ちにネットワーク・トラフィックに対する検査を開始し、通常のLANトラフィックの通過をすべて許可しながら、不正なコンテンツの通過をブロックします。管理者は、使いやすいインターフェースを使用して内部セキュリティ・ゾーンを構成すると共に、特定のトラフィック・パターンを明示的に指定して通過を禁止することができます。

ID	Name	Traffic type	IP Address/Net Mask	Action	Expiration	Log	Hit Count	Comments	Originator Name
1	Worm	To	123.34.4.4	Quarantine	By Date 01/14/2004 02:58	Alert	5	Worm detection ...	SmartDefense
2	Blocked IPs	From	192.168.0.44	Block	Never	Alert	19	Blocked Ip's wt...	Admin
3	Blocked IPs	To	194.68.0.44	Block	By Date 01/14/2004 11:58	Alert	55	Blocked Ip's wt...	Admin
4	Allowed Traffic	From	223.220.16.24	Bypass	By Date 01/14/2004 03:58	Log	0	Allowed Traffic (...)	Admin

InterSpectの管理インターフェースは、内部セキュリティ専用設計された強力なインターフェースで、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を簡単に行えます。

### パフォーマンス

InterSpectは、内部セキュリティに必要なパフォーマンス要求を満たすように設計されたアプライアンスで、チェック・ポイントがセキュリティを強化したオペレーティング・システムであるSecurePlatformをベースに開発されました。InterSpectには、チェック・ポイントが特許を持ち、最高レベルのパフォーマンスを実現するためのセキュリティ・アクセラレーション技術であるSecureXL™ も組み込まれています。

## InterSpectの動作モード

InterSpectは、様々な環境に対し柔軟な導入をサポートするために、3種類のインライン・オペレーティング・モード（ブリッジ・モード、スイッチ・モード、ルータ・モード）に対応しています。すべてのモードでモニター専用機能に対応しています。

機能説明	導入へのシナリオ
<b>ブリッジ・モード</b> InterSpectは、1つまたは複数のセグメントをバックボーンに対しブリッジします。InterSpectはIPネットワークからは透過的となります。	既存環境を大幅に変更することなく、ワーム防御と隔離を透過的に展開
<b>スイッチ・モード</b> InterSpectは、マルチポート・ブリッジとして動作します。すべてのポートをブリッジして、1つのゾーンを構成します。	完全なセグメンテーションが不要な場合に、ワーム防御と隔離を透過的に展開
<b>ルータ・モード</b> InterSpectは、ルータとして動作します。アクティブな各ポートはそれぞれ異なるIPセグメントとして設定します。	ネットワーク・ゾーンとしてセグメント化による、複数のセキュリティ・ゾーンに対応
<b>モニター専用機能</b> InterSpectは、トラフィックをチェックするのみで、防御や隔離などのアクションを行いません。（ブリッジ、スイッチ、ルータのいずれのモードでも使用できます）。	InterSpectの導入前に既存環境やアプリケーションに対する影響や効果を調査するための評価用機能として主に利用

## InterSpect の仕様

	InterSpect 210	InterSpect 410	InterSpect 610	InterSpect 610F
<b>導入ターゲット</b>	1つのワークグループを保護	複数のワークグループを保護	ギガビット・ネットワークを保護	ギガビット・ネットワークを保護
<b>プラットフォーム</b>	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform
<b>スループット</b>	200Mbps	500Mbps	1000Mbps	1000Mbps
<b>ファイバ・インターフェース</b>	なし	なし	追加可能	含む
<b>インターフェースの通信速度</b>	10/100Mbps	10/100/1000Mbps	10/100/1000Mbps	10/100/1000Mbps
<b>拡張スロット数</b>	なし	1	1	1
<b>検査ポート数</b>	2	3～10	3～10	3～10
<b>管理ポート数</b>	1	1	1	1
<b>最大ポート数</b>	3	10	10	10
<b>VLANサポート数</b>	8VLAN	128VLAN	VLAN数制限なし	VLAN数制限なし
<b>電源冗長化</b>	なし	オプション	含む	含む
<b>SmartDefenseのスク립ション</b>	1年分含む	1年分含む	1年分含む	1年分含む
<b>幅</b>	42.42cm	44.7cm	44.7cm	44.7cm
<b>高さ</b>	4.2cm(1U)	4.2cm(1U)	4.2cm(1U)	4.2cm(1U)
<b>奥行き</b>	55.5cm	27.0cm	27.0cm	27.0cm
<b>重量</b>	12.25 Kg	15.88 Kg	15.88 Kg	15.88 Kg
<b>電圧</b>	100～220V 50/60Hz	100～220V 50/60Hz	100～220V 50/60Hz	100～220V 50/60Hz

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

記載された製品仕様は予告なく変更される場合があります。

©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, InterSpect, 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。本書に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。