

InterSpect NGX™

全般的な質問：

InterSpect はどのような製品ですか？

InterSpect は内部セキュリティ・ゲートウェイ製品です。InterSpect は、ワーム、DoS 攻撃（サービス不能攻撃）、電子メールで感染するマルウェアなど、ネットワーク内部から拡散する脅威を検出してブロックします。InterSpect はネットワーク内部の保護を目的として設計されており、以下の機能を提供します。

- ネットワークへの侵入を検出してブロックする。
- ネットワークを複数のセキュリティ・ゾーンに分割する。
- 不審なコンピュータを隔離する。
- LAN プロトコルを保護する。
- Web アプリケーションを保護する。
- Check Point Integrity™ と統合してエンドポイント・セキュリティを提供する。

InterSpect は高度な柔軟性を備えているため、既存のネットワーク環境にも簡単に導入できます。

内部セキュリティ・ゲートウェイ (ISG) とは何ですか？

内部セキュリティ・ゲートウェイは、社内や組織内のネットワークを、トラフィックを阻害せずに保護できるように設計されたソリューションです。内部セキュリティ・ゲートウェイである InterSpect は、導入直後は許可ベースで動作します（明示的に禁止されたトラフィック以外を許可する）。これにより、ミッション・クリティカルなアプリケーションの通信を誤って妨げることなしに、ネットワークへの侵入をインテリジェントに検出・防御して、悪質なトラフィックがネットワーク全体に拡散するのを防ぎます。内部セキュリティ・ゲートウェイにとって最も重要なのは、セキュリティ上の脅威となるマルウェアや、セキュリティ要件を満たさないエンドポイントをセキュリティ・ゾーン内部に隔離して、他のゾーンへの脅威の拡大を未然に防ぐ機能です。InterSpect はセキュリティ・ゾーン間で送受信されるトラフィックを検査し、悪質なトラフィックを検出した場合は、そのトラフィックの発信元をゾーン内に隔離して、それ以外のゾーンへの被害拡大を防ぎます。

企業や組織のネットワーク上では、多種多様なプロトコルやアプリケーションが使用されています。それらを的確に保護するには、内部セキュリティ・ゲートウェイが、主要な LAN プロトコルを的確かつ包括的にサポートしている必要があります。ここで言う主要な LAN プロトコルには、Microsoft RPC、CIFS、Microsoft SQL、DCOM、DCE RPC、Citrix ICA、DNS、HTTP、FTP、インスタント・メッセージング (IM)、ピアツーピア・アプリケーションなどが含まれます。

InterSpect はどのプラットフォームをサポートしていますか？

InterSpect は、チェック・ポイントから専用アプライアンスの形で提供されます。現在、InterSpect シリーズの各アプライアンスは、デル社とのパートナーシップを通じて開発・製造されています。また、InterSpect はクロスビーム社の X40、X45、および X80 にも搭載されており、これらはクロスビーム社から「InterSpect On X」という商品名で提供されています。

InterSpect NGX はいつリリースされますか？

チェック・ポイントの EBS（エンタープライズ・サポート）をご契約のお客様には、2005 年末までに InterSpect NGX のソフトウェア・アップグレードが提供される予定です。

内部セキュリティと境界セキュリティは違うのですか？

内部セキュリティと境界セキュリティとは、セキュリティ上の課題や焦点が異なります。内部セキュリティは多種多様なプロトコルを対象としているため、セキュリティ規則を定義して構成する際に、境界セキュリティとは異なるアプローチが必要となります。同時に、内部セキュリティには境界セキュリティよりも高い処理速度が求められます。

通常、境界セキュリティは、LAN 内部でしか使用されない悪用されやすいプロトコルをブロックします。SQL や MS RPC はこうしたプロトコルの代表です。SQL は Microsoft SQL Server や Oracle Database などのデータベース・アプリケーションで使用され、MS RPC は Microsoft Exchange Server などの Microsoft 製アプリケーションで使用されます。これらのプロトコルとアプリケーションは、LAN 上で営まれる日常業務の生命線を握っています。そのため内部セキュリティには、これらのプロトコルを単にサポートしているだけでなく、攻撃や誤用を防ぐ高度なセキュリティ機能を提供する能力が求められます。内部セキュリティと境界セキュリティのもう一つの違いは、アクセス制御に対するアプローチです。通常、境界セキュリティには Deny モード（拒否モード）での動作が求められます（明示的に許可されたトラフィック以外を禁止する）。一方で内部セキュリティには、許可ベースでの動作が求められます（明示的に禁止されたトラフィック以外を許可する）。これは、内部ネットワークで使用されるプロトコルやアプリケーションの数が多く、構成も非常に複雑なためです。InterSpect は、このような内部セキュリティに求められる高度な要件を満たすべく設計されています。

InterSpect は SmartDefense™ とは違うのですか？

SmartDefense は InterSpect が搭載する機能の一つで、内部ネットワークへの侵入を阻止する機能において中心的な役割を果たします。

当社はレガシーなネットワーク・レベルのファイアウォール（または VPN コンセントレータ）を設置していますが、InterSpect を導入する意義はありますか？

はい、あります。InterSpect は、レガシーなネットワーク・レベルのデバイスを使用している環境でも、既存のインフラストラクチャを変更せずに導入できます。また、InterSpect を導入することで、アプリケーションを狙った攻撃からネットワークを保護できるようになります。

InterSpect は IDS や IPS とは違うのですか？

InterSpect は、アプリケーション層を保護したり、特定のパラメータに基づいてトラフィックの検査、ブロック、ログ取得を行ったりするなど、既存の IDS や IPS と同様のコンセプトを一部共有しています。しかし、InterSpect はより完全な内部セキュリティ・ソリューションを目指して開発されています。InterSpect は内部ネットワークを複数のセキュリティ・ゾーンに分割したうえで、ネットワーク・レベルおよびアプリケーション・レベルから保護することができます。InterSpect は内部ネットワークにインラインで（直列で）接続され、ネットワークをリアルタイムに保護します。通常、IDS や IPS は、アプリケーション層の攻撃をネットワーク境界でブロックするために、ネットワーク境界や DMZ に設置されます。そのため、IDS や IPS は、事実上は境界セキュリティを強化する製品に位置づけられます。また、IDS や IPS は InterSpect とは異なり、内部ネットワークを複数のセキュリティ・ゾーンに分割したり、脅威を隔離したりする機能を持たないため、ネットワーク内部から拡散する脅威を封じ込めることができません。加えて、IDS や IPS には導入、設定、管理が悪夢のように複雑であるという欠点があります。しかし InterSpect は、ほぼすべてのネットワーク環境に文字通り数分で導入できるというメリットがあります。

当社はアプリケーション・サーバにホスト・ベースの IDS/IPS を導入済みです。それでも InterSpect を導入する意義はありますか？

はい、あります。ホスト・ベースの IDS や IPS は、内部ネットワークを複数のセキュリティ・ゾーンに分割し、個別に隔離する機能を備えていないため、ワームや DoS 攻撃など、ネットワーク内部から拡散する脅威を封じ込めることができません。また、ホスト・ベースの IDS や IPS は、それらがインストールされている特定のデバイスしか保護できません。既存の IDS や IPS は、境界セキュリティを強化する形で導入されるため、内部ネットワークを包括的に保護することができません。

製品に関する質問：

InterSpect はどのオペレーティング・システムを使用していますか？

InterSpect は SecurePlatform™ を使用しています。SecurePlatform は、チェック・ポイントが提供するセキュリティ強化型のオペレーティング・システムで、多くのチェック・ポイント製品に採用されています。

チェック・ポイントの OPSEC パートナーは InterSpect を搭載した製品を提供していますか？

提供しています。InterSpect はクロスビーム社の X-Series 製品に搭載されています。「InterSpect On X」と呼ばれるこれらの製品は単一のハードウェア・デバイスであり、コア・ルータ、分散スイッチ、またはアクセス・ルータとシームレスに統合できます。InterSpect-On-X は高いポート密度を備えているため、数多くの独立したネットワーク・セグメントを保護できます。また、ブリッジ・モードまたはスイッチ・モードで動作するため、ネットワーク設定をほとんど変更せずに導入できます。InterSpect-On-X は、内部セキュリティ・ソリューションとして、最高レベルの可用性とスケーラビリティを備えています。詳細については、http://www.crossbeamsystems.com/products_js.asp を参照するか、チェック・ポイントの営業担当者またはクロスビーム社のパートナーにお問い合わせください。

InterSpect はソフトウェアの形で購入できますか？

できません。InterSpect は単一のアプライアンスとして提供されます。

InterSpect を導入することで、内部ネットワークのパフォーマンスに影響はありますか？

InterSpect は内部ネットワークのトラフィック保護に主眼を置いて開発されています。そのため、InterSpect はスループットや接続レートなど、内部ネットワークに求められる数多くのパフォーマンス要件を満たしています。InterSpect のパフォーマンスに関する詳細は、製品のデータシートを参照してください。

InterSpect はどのように管理するのですか？

InterSpect は中央の管理サーバから一元的に管理することも、ローカルで管理することもできます。

ローカルで管理する場合は、SmartConsole（管理用のクライアント・アプリケーション）を使用して InterSpect のアプライアンスに直接接続します。SmartDefense のアップデートや設定の有効化など、各種の管理作業はローカルの SmartDashboard（SmartConsole の管理用 GUI）で行います。一方、InterSpect を集中管理する場合は、中央の管理サーバの SmartDashboard を使用します。その場合は、InterSpect を VPN-1、Connectra、VPN-1 Edge など他のチェック・ポイント製品と共に一括で管理することもできます。中央から行うことができる管理作業には、以下のものがあります。

- 設置されている InterSpect のすべて、または一部に対して、SmartDefense のアップデートと設定の有効化を同時に行う。
- SmartView Monitor（SmartConsole の監視用 GUI）を使用して、InterSpect のパフォーマンスとセキュリティの状態を監視する。

上記に加えて、管理者は InterSpect をローカルで管理する場合と同様に、中央の SmartDashboard 上で InterSpect のオブジェクトを作成して管理できます。なお、InterSpect は SmartCenter Express では管理できません。

InterSpect は HA 環境（高可用性環境）に導入できますか？

はい、InterSpect は既存の HA インフラストラクチャに導入できます。また、既存の HA インフラストラクチャを活かして複数の InterSpect を設置することで、内部セキュリティに冗長性を確保できます。

InterSpect はどのように LAN プロトコルを保護しますか？

InterSpect は、Application Intelligence とステートフル・インスペクションを通じて LAN プロトコルを保護します。Application Intelligence は、設定の自由度が高い非常に強固なセキュリティ機能を備えています。Application Intelligence のセキュリティ機能は、以下の 4 種類に大別されます。

- セキュリティ基準への適合性を検証する。
- プロトコルが標準的な用途で使用されているかどうかを検証する。
- 悪質なデータをブロックする。
- アプリケーションによる危険な通信をブロックする。

InterSpect は、MS SQL、MS RPC、CIFS、DCOM など Microsoft のプロトコルや、Citrix ICA、Sun RPC、DCE RPC、HTTP などの各種 LAN プロトコルに対し、市場で最も強力かつ包括的な保護を提供します。

InterSpect はフェイルオープン NIC をサポートしていますか？

はい、サポートしています。ネットワークのセグメント間に設置されている InterSpect が、電源遮断など不測の事態で動作を停止した場合も、フェイルオープン NIC を使用していれば、セグメント間のネットワーク通信が維持されます。NIC を含むアドオン機能の詳細については、『Check Point InterSpect : Description of Port Options』および価格リストを参照してください。

InterSpect はメール・プロトコルをサポートしていますか？

はい、サポートしています。InterSpect が搭載する SmartDefense は、POP3 と IMAP4 で転送される電子メール・メッセージを解析し、悪質なデータをブロックします。たとえば、攻撃者は非常に長いユーザ名やパスワードを使用して、メール・サーバの異常終了を引き起こそうとする場合がありますが、SmartDefense を使用すると、ユーザ名とパスワードの最大文字数を制限できます。また、SmartDefense は SMTP もサポートしているため、セキュリティ上好ましくない場合は Web ベースのメール・サービスをブロックできます。

InterSpect はシスコ社の ISL (Inter-Switch Link) プロトコルをサポートしていますか？

はい、サポートしています。

InterSpect はノーテル社の SMLT (Split Multi-Link Trunking) プロトコルをサポートしていますか？

はい、サポートしています。InterSpect は SMLT プロトコルを使用するネットワークにも透過的に導入できます。この場合、InterSpect はコア・スイッチとエッジ・スイッチの間に設置する必要があります。

サポートに関する質問：

InterSpect にはどのようなサポートが提供されますか？

InterSpect の EBS (エンタープライズ・サポート) にご契約いただくと、以下のサービスが提供されます。

- ハードウェアに故障が発生した場合、翌営業日のオンサイト・サポート
- InterSpect のソフトウェアのバージョンアップ・サービス
- パッチやホット・フィックスなど、修正ファイルのダウンロード・サービス
- 製品ドキュメントのダウンロード・サービス

または、EBS の代わりに InterSpect オンサイト・サポート・サービスにご契約いただくと、上記のサービスに加えて、当日の 4 時間オンサイト・サポートや設定の復旧サービスなど、より総合的なサポートが提供されます。

InterSpect のサポート・サービスの詳細については、<http://www.checkpoint.co.jp/products/interspect/isonsite/index.html> を参照するか、チェック・ポイントまたはパートナー各社の営業担当者にお問い合わせください。