



# チェック・ポイントの オープン・パフォーマンス・アーキテクチャ

データセンター・レベルの高速アプリケーション層セキュリティを提供

# Contents

本書の内容

はじめに .....	3
パフォーマンスとセキュリティの微妙なバランス .....	3
帯域要件の増大 .....	3
アプリケーション層の脅威の増加 .....	4
チェック・ポイントのオープン・パフォーマンス・アーキテクチャ .....	5
オープンなアーキテクチャは、ソリューションのライフサイクルを通じて パフォーマンス価値を向上させる .....	6
オープンなアーキテクチャは、コストとパフォーマンスの両面で 顧客にメリットをもたらす .....	7
チェック・ポイントのアクセラレーション技術 .....	7
ClusterXL: スマート・ロード・バランシング .....	7
SecureXL: セキュリティ・アクセラレーション .....	8
CoreXL: マルチコア・アクセラレーション .....	10
まとめ .....	11

## はじめに

これまで多くの企業は、ネットワークを運用するに際して、セキュリティを重視してパフォーマンスの低下には目をつぶるか、パフォーマンスを優先して攻撃を受けるリスクを甘受するかを選択を余儀なくされてきましたが、今日、どちらを重視するかの判断はより困難になっています。その理由の1つに、ハッカーやマルウェアが攻撃経路としてアプリケーション層を使用するようになってきていることがあります。正当なトラフィックに偽装されたこれらの攻撃を検出するには、より深いレベルでの検査を実施する必要があり、そのためにより多くの処理能力が必要になります。もう1つの理由としては、多くのネットワーク環境が10G Ethernetへ移行が進んでいることが挙げられます。10G Ethernetは、2006年には約60パーセントもの成長率で普及しており、その投資を無駄にしないために、この速度に対応できるだけのパフォーマンスを提供することがセキュリティ・ソリューションに求められています。

チェック・ポイントのオープン・パフォーマンス・アーキテクチャは、この課題—高いスループットと高いセキュリティ・レベルの両立—を克服することを念頭に設計されています。チェック・ポイントが特許を保有する(または特許を出願中の)複数のアクセラレーション技術で構成されるオープン・パフォーマンス・アーキテクチャは、単一のプラットフォームで高いレベルのセキュリティとパフォーマンスを実現し、そのいずれも妥協せずにパフォーマンスとセキュリティを兼ね備えた環境の構築が可能になります。これらのアクセラレーション技術は、IntelのマルチコアCPUといった先進技術と連携して動作し、高速なアプリケーション層セキュリティを実現します。この技術白書では、オープン・パフォーマンス・アーキテクチャの基本概念を解説すると共に、各アクセラレーション技術について詳しく説明します。

## パフォーマンスとセキュリティの微妙なバランス

ネットワークをセキュリティで保護しようとすると、必ず何かを妥協しなければならないという問題が発生します。ネットワークは情報へのアクセスを可能にする技術であり、人々はいつでもデータに—VoIPの場合は人に—アクセスできることを期待し、それを要求します。一方、セキュリティは、人々がアクセスできる範囲を制限するための技術です。今日、多くのネットワーク環境では、各種法規制の施行とセキュリティ意識の高まりにより、セキュリティ・ポリシーの見直しとセキュリティ対策の強化を迫られています。ネットワーク環境のセキュリティが厳格化されるのに伴い、人々がアクセスできる範囲はより制限されていくことになります。

厄介なのは、セキュリティによるコントロールが強化されるにつれてセキュリティ・ツール自体の負荷が高まり、その結果パフォーマンスが低下してアクセス・レベルにも間接的な影響が及ぶことです。高度に洗練された攻撃と情報漏洩など、今対策が必要なリスク要因からネットワークを保護するためには、情報が境界ゲートウェイを通過する際に、深いレベルでの検査を実施しなければなりません。しかし、情報に対して行われるセキュリティ・チェックの項目が多くなると、そのセキュリティ・ポリシーを実施する際、セキュリティ・ツールに多大な処理負荷がかかることになります。これは、セキュリティ検査の速度を確実に低下させます。

情報アクセスとセキュリティのバランスというこの問題は、「帯域要件の増大」と「アプリケーション層の脅威の増加」という2つの主要因によって、より顕著になってきています。

### 帯域要件の増大

現在、企業ネットワークは、1G Ethernetから10G Ethernetに移行しつつあります。このことは、境界におけるスループット要件の増大に直接つながるわけではありませんが、全体としてのセキュリティ・パフォーマンス要件の増大をもたらします。統合型のファイアウォール/VPNは、ネットワークの境界部分でセキュリティ検査を実施するだけでなく、大規模オフィスやデータセンターではネットワーク・セグメントの切り分けや重要サーバの分離といった大きな役割を果たしているからです。したがって、ネットワークを10G Ethernetに移行する場合は、内部的にファイアウォールのパフォーマンス向上も求められることになります。

<sup>1</sup> Network World, February 15, 2007, "Increased 10g adoption pushes the market past \$1 billion," Phil Hochmuth

大規模環境においてバックボーンやFast Ethernetを保護する取り組みが進む一方、支社・支店などの小中規模環境においてもパフォーマンス要件に変化が生じてくと予想されます。今日、VoIPなどのマルチメディア・アプリケーションは、支社・支店環境を含むネットワーク全体に導入され、より多くの環境で利用されるようになってきています。IDCが2005年11月に実施した調査「Enterprise VoIP Spending in 2005」によると、35パーセントの組織がVoIP用のIP PBXを支社・支店環境に導入する計画があるとし、41パーセントがホスティング型VoIPサービスの導入を検討中であるとしています。低遅延/高スループットが要求されるマルチメディア・アプリケーションが支社・支店環境に導入されるのであれば、そこで求められるセキュリティ・パフォーマンス要件も増大することになります。

### アプリケーション層の脅威の増加

最近の『Information Security』誌に掲載された記事によると、Webサイトへの攻撃の75パーセントはアプリケーション層に対して行われています<sup>2</sup>。また『Network World』の2006年4月の記事によれば、インスタント・メッセージ、チャット、ピア・ツー・ピア・アプリケーションに対する攻撃は前年比で何と700パーセントも増加しています<sup>3</sup>。「今日の攻撃は、正当なアプリケーション層トラフィックを装って行われるようになってきている」ということは以前より指摘されていましたが、これらの数字は、まさにこのことを裏付けるものと言えます。攻撃がアプリケーション層に対して行われるようになって理由としては、従来型のファイアウォールをベースとするセキュリティ対策はネットワーク層でのアクセスに重点を置いたものであり、許可されていないユーザが特定のIPアドレスやネットワークにアクセスできないようにすることを目的としている、ということが挙げられます。これに対しアプリケーション層への攻撃では、ファイアウォールを通過できるように、信頼されたユーザとしてトラフィックの偽装を行います。セキュリティ検査でこれらの攻撃を検出するには、侵入防御と同様のより深いレベルでの検査をファイアウォールで実施しなければなりません。しかしながら、追加のセキュリティ検査を実施した場合、ファイアウォールのトラフィック処理速度はそれに伴って低下し、想定されるパフォーマンス・レベルも低下します。

従来、セキュリティ・パフォーマンス要件の増大に対応するには、ASIC (Application-Specific Integrated Circuits) などの専用ハードウェアをベースとするクローズドなアーキテクチャを使用するのが一般的でした。これらの特定用途向けデバイスは、特定のタスクを効率よく処理できるように設計されており、汎用プロセッサと比較して大幅に高いパフォーマンスが得られます。例えば、ネットワーク・アドレス変換 (NAT) や基本的なパケット・フィルタリングといったセキュリティ・タスクは、この種のデバイスを使用することで比較的容易にパフォーマンスを向上させることができます。

クローズドなシステムの問題は、動的に変化するという特徴を持つアプリケーション層の脅威に適宜対応できるように設計されていないことです。ASICベースのシステムは、開発元が初期設定を行った後、新手の攻撃に対処できるようロジックを書き換えることができません。システムによっては、新しい攻撃に対処できるよう、ロジックの書き換えが可能な汎用プロセッサを搭載している場合もありますが、このプロセッサはASICにあるようなアクセラレーション技術を備えていません。クローズドなシステムのこれらの特徴は、次の2つの大きな問題を生み出します。

1. 高速と低速という2つの検査パスがある：単純なタスクの場合、ASICはトラフィックを高速処理できます。しかし、Webトラフィックや電子メール、VoIPに関するものや機密情報にアクセスするものなど、より複雑なタスクの場合、トラフィックはセカンダリのプロセッサ、すなわち低速パスに送られます。この低速パスの場合、処理速度はパスの転送速度やプロセッサの性能に依存しますが、このような低速パスでの処理は、ASICベースのシステムにおいてはどちらかと言うと目的外の利用であり、実際にアプリケーション層の脅威に対処するにはパフォーマンスが不十分であることが少なくありません。このためASICベースのシステムは、オープンなシステムと比較して、新しい攻撃に対しては特にパフォーマンスが低下する傾向にあります。

<sup>2</sup> Information Security, August 2006, "Web Application Break-In," Michael Cobb

<sup>3</sup> Network World, April 10, 2006, "IM, P2P Attacks Up 700 percent," Gregg

2. クローズドなシステムは、時間の経過と共にパフォーマンス価値が低下する：ASICは、毎日のように出現する新たな脅威に対処できるよう後からロジックを書き換えることができません。そのためクローズドなシステムは、設計が完了した後、新しい攻撃が出現するたびに処理が低速になっていきます。クローズドなシステムを使用している間、その管理者は、パフォーマンスの低下を受け入れるか、新しい攻撃については防御を実施しないようにするかの選択を迫られることになります。

## チェック・ポイントのオープン・パフォーマンス・アーキテクチャ

チェック・ポイントのオープン・パフォーマンス・アーキテクチャは、セキュリティとパフォーマンスの二者択一をユーザに要求するのではなく、その両立を実現するフレームワークを提供することにより、このトレードオフ問題を解決します。100万円以下クラスの単一のオープン・サーバ上で最大12Gbpsのスループットを実現するVPN-1®は、侵入防御技術のSmartDefense™を併用し、高いパフォーマンスが求められる環境において深いレベルのセキュリティ検査を実施できるようにします。例えば、サーバ・ファームまたはDMZを保護する場合は、HTTPベースのワームや、特定サーバ（メール・サーバやFTPサーバなど）に対する攻撃をブロックする必要がありますが、この場合、SmartDefenseのデフォルト設定を使用し、5.3 Gbpsのスループットが得られます。さらに、外部の脅威から内部ネットワークを保護する場合には、VoIPやインスタント・メッセージング、ピア・ツー・ピアでのファイル交換といったアクティビティを制御することのできるより厳格なプロファイルを使用することになります。VPN-1ゲートウェイは、この厳格な保護プロファイルを有効にした場合でも、1.8 Gbpsのスループットを維持することができます。

これだけのパフォーマンスを実現するうえで鍵となるのは、オープンなシステムの技術革新とチェック・ポイントが特許を保有するアクセラレーション技術の組み合わせです。オープンなセキュリティ・ソリューションで利用可能なオープン・プロセッサの演算能力は、「ムーアの法則」（ゴードン・ムーア氏が経験則に基づいて提唱した「プロセッサの演算能力は18か月ごとに2倍になる」という法則）に基づき、速いペースで向上しています。特に、バスの転送速度の向上やマザーボード・アーキテクチャの改良といった他の技術革新と組み合わせた場合の性能向上には目を見張るものがあります。

こうしたハードウェアの技術革新をうまく活用するためには、ソフトウェアの方もそれに見合う技術革新を遂げる必要があります。オープン・パフォーマンス・アーキテクチャは、チェック・ポイントの3つの特許技術で構成されています。

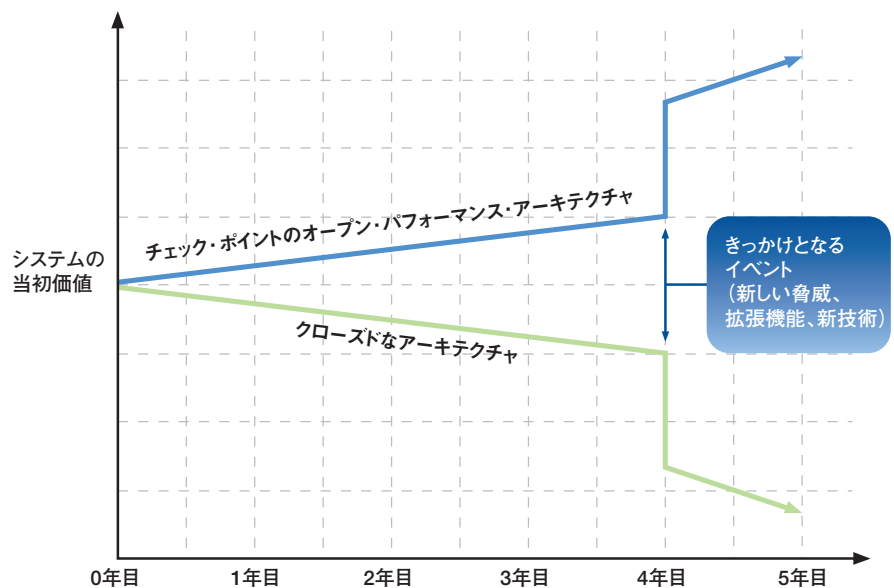
- **CoreXL™マルチコア・アクセラレーション**：CoreXLマルチコア・アクセラレーションは、マルチコア・プロセッサをフル活用できるように設計された初めてのセキュリティ技術です。CoreXLは、セキュリティ検査の負荷をすべてのコアに分散します。
- **SecureXL™セキュリティ・アクセラレーション**：SecureXLセキュリティ・アクセラレーションは、ネットワーク・トラフィックがセキュリティ・デバイスを通過する際に生じる遅延を排除してセキュリティ検査を高速化します。
- **ClusterXL™スマート・ロード・バランシング**：ClusterXLは、複数のVPN-1システムをクラスタリングしてパフォーマンスをほぼニアに向上させられるようにします。

オープン・パフォーマンス・アーキテクチャでは、これら3つの技術が連携して動作することによりセキュリティ検査を単一のパスで高速実行できるようにし、それによって高いパフォーマンスと高いセキュリティの両立を実現します。これらの技術は、次の2つの基本理念に基づいて開発されています。

### オープンなアーキテクチャは、ソリューションのライフサイクルを通じてパフォーマンス価値を向上させる

セキュリティ・システムの真の価値は、既知の脅威だけでなく未知の脅威にも確実に対処できるかどうかによって決まります。オープン・パフォーマンス・アーキテクチャの重要な特徴の1つは、パフォーマンスを一定のレベルに保ちながら新しい脅威に対処できるということです。これは、一般的に利用可能なハードウェア技術をベースに、検査パスを統一することによって実現されています。VPN-1では、新しい攻撃手法が登場した場合でも、ASICから汎用プロセッサへと検査パスを切り替えるに伴うパフォーマンスの低下が生じません。新種の攻撃に対する検査は、既存の攻撃に対する検査と同じパスで処理されます。このためネットワーク環境では、新しいセキュリティ・ポリシーを実施してもパフォーマンスは一定のレベルに保たれるという安心感を得ることができます。

これに対してASICベースのシステムは、新しい攻撃が出現してトラフィックが低速な検査パスに送られるようになるのと同時にその価値が低下し始めます。実際、深いレベルの検査設定を有効にした途端にパフォーマンスが急激に低下し、当初の1~5パーセント程度の性能しか発揮できなくなります。ここで理解しておく必要があるのは、このパフォーマンス価値の低下は、システムを購入したときに始まるのではなく、システム的设计が完了したときに始まるということです。システムのライフサイクルが終わりに近づくにつれて、その価値は大幅に低下します。



上のグラフは、新しいタイプの攻撃が出現したとき、2つのシステム—オープン・パフォーマンス・アーキテクチャに基づくシステムとクローズドなアーキテクチャに基づくシステム—の間にどのような違いが生じるかを示したものです。2つのシステムの最初のパフォーマンス価値は同じであるにもかかわらず、新しい攻撃が出現した途端に両者の間には大きな差が生じています。問題となるのは、Webのビジネス利用の一般化や、SlammerおよびBlasterワームの出現を契機とするアプリケーション層攻撃時代の幕開けといった、クローズドなシステムでは対応することのできないセキュリティ上のパラダイム・シフトが3~4年おきに起きていることです。オープンな技術を使用するチェック・ポイントのソリューションは、大規模なパラダイム・シフトが発生した場合でも、非常に素早く対応することが可能です。

## オープンなアーキテクチャは、コストとパフォーマンスの両面で顧客にメリットをもたらす

チェック・ポイントは、最良のセキュリティ・ソリューションを顧客に提供するべく尽力しており、その研究開発リソースは顧客環境のセキュリティ強化に寄与する技術にのみ向けられています。ハードウェア・プラットフォームについては、セキュリティ・アプライアンスやオープン・サーバなどを開発するプラットフォーム・メーカーおよびIntelなどのマイクロプロセッサ・メーカーの双方と緊密に協力しています。チェック・ポイントでは、こうしたパートナーシップを築くことによって、複合型ソリューション（セキュリティ・ソフトウェア+ハードウェア）の総コストを大幅に低減することに成功しています。例えば、クアッドコアIntel Xeonプロセッサ5300シリーズを2基搭載するリファレンス・システムにインストールされたVPN-1ソリューションは、12Gbpsのスループットを実現しながら、そのコストはリファレンス・システムを含めて200万円を下回ります。またこのシステムは、厳格なセキュリティ・プロファイルを適用した場合でも、1.8Gbpsの侵入防御スループットを発揮します。各パートナーがそれぞれの専門分野ごとに分業するこのパートナーシップは、セキュリティ・エコシステムと呼ぶべきものです。このセキュリティ・エコシステムにより、クローズドなシステムよりも質の高いネットワーク・セキュリティ・ソリューションを、コスト・パフォーマンスに優れた価格で提供することが可能になっています。

これに対しクローズドなシステムのベンダーの場合、専用ハードウェアの設計を自社内で行う必要があるため、個々のシステムの全体的なコストはどうしても割高になります。これは特に、大きな需要が見込めないハイエンド環境向けの製品で顕著です。市場規模の小さいクローズドなシステムの開発コストは、オープンなシステムよりも格段に小さい顧客ベースで負担せざるを得ないのです。

またクローズドなシステムには、新しい技術を採用するための時間がかかるという欠点もあります。ASICベースのシステムを新たに開発するには時間とコストがかかるため、ベンダーは、マルチコア・プロセッサや高速なバス・アーキテクチャといった新技術をそう簡単に採り入れることができません。そのため、クローズドなシステムのライフサイクルは3~4年単位となってしまいます。一方、オープンなアーキテクチャの場合、顧客は、Intelなどのマイクロプロセッサ・メーカーが公開しているロードマップを参照することで、今後どのような技術改良が行われる予定なのかを知ることができます。さらにチェック・ポイントの場合は、新たに投入される技術についてIntelと密接な協力関係を築いているため、ハードウェアにおける特定の技術革新に合わせてソフトウェア技術を開発できるという相乗効果も享受できます。その格好の例が、クアッドコア・プロセッサの登場とほぼ同時期にリリースされたマルチコア・アクセラレーション技術のCoreXLです。オープン・パフォーマンス・アーキテクチャは、短期間のうちに新技術を採り入れ、セキュリティ・パフォーマンスの向上を図れるようにする柔軟性をもたすのです。

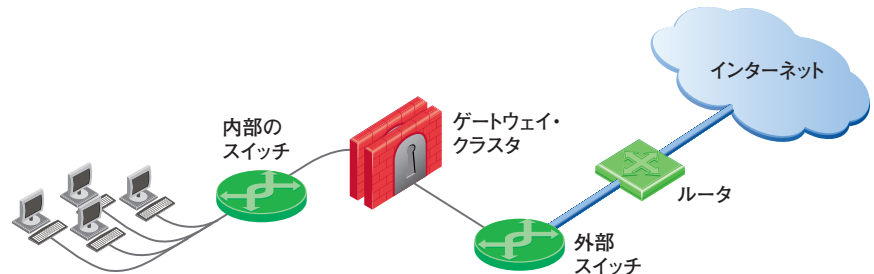
## チェック・ポイントのアクセラレーション技術

ハードウェアの改良やコードの最適化など、パフォーマンスの向上に寄与する要因は多々ありますが、チェック・ポイントのオープン・パフォーマンス・アーキテクチャは、あくまでもClusterXL、SecureXL、CoreXLという3つの技術によってパフォーマンスを向上させることを目指しています。これら3つの技術は、相互に連携することによって、広範なオープン・サーバおよびアプライアンス上でのパフォーマンスを最大化します。以降では、各技術の仕組みについて説明します。

### ClusterXL：スマート・ロード・バランシング

ClusterXLは、大量のトラフィックをインテリジェントな手法で複数のゲートウェイに分散させる手段を提供します。これにより、ほぼリニアな拡張性を実現すると共に、信頼性を大幅に向上させることが可能になります。ClusterXLによるゲートウェイ・クラスタは、物理的に同じ場所に配置することも、内部バックボーンを介して別々の拠点に分散配置することも可能です。後者の場合は、ビジネスの継続性を維持するために必要な冗長性がさらに向上します。

運用時には、クラスタを構成するVPN-1ゲートウェイは、それぞれ固有のIPアドレスと物理MACアドレスを保持することになります。ただし、クラスタに参加していないシステムからすると、いずれのクラスタ・メンバーも、クラスタを表す同一の仮想IPアドレスを持っているように見えます。また各ゲートウェイは、内部ネットワークでも外部ネットワークでも、ハブ型ネットワークかスイッチ型ネットワークで接続されます。このため、各クラスタ・メンバーは素早く情報を共有することができます。



このやり取りは、セキュリティに関する情報および判断を各VPN-1ゲートウェイ間で確実に同期するために行われます。この同期が必要なのは、ネットワークを行き来するトラフィックが、行きと帰りで同じクラスタ・メンバーを通過するとは限らないためです。例えばあるコンピュータが、クラスタの背後にあるサーバにアクセスするために、TCPのスリーウェイ・ハンドシェイクを開始したとします。このとき、最初のハンドシェイクがゲートウェイ1を通過してサーバに送られた後、そのサーバのレスポンスは、別のクラスタ・メンバーであるゲートウェイ2に送られる可能性があります。しかしサーバは、TCPハンドシェイクへのレスポンスで通信を開始するべきではないため、ゲートウェイ2は、ゲートウェイ1の判断を知らされていない場合、このトラフィックをブロックしてしまいます。ゲートウェイ1の判断を知らされていた場合、ゲートウェイ2はこのトラフィックを通過させます。このように情報を共有することを「ステート同期」と呼びます。このステート同期により、1つのゲートウェイに障害が発生した場合に、残りのゲートウェイが中断なしでトラフィックを引き継ぐことも可能になります。

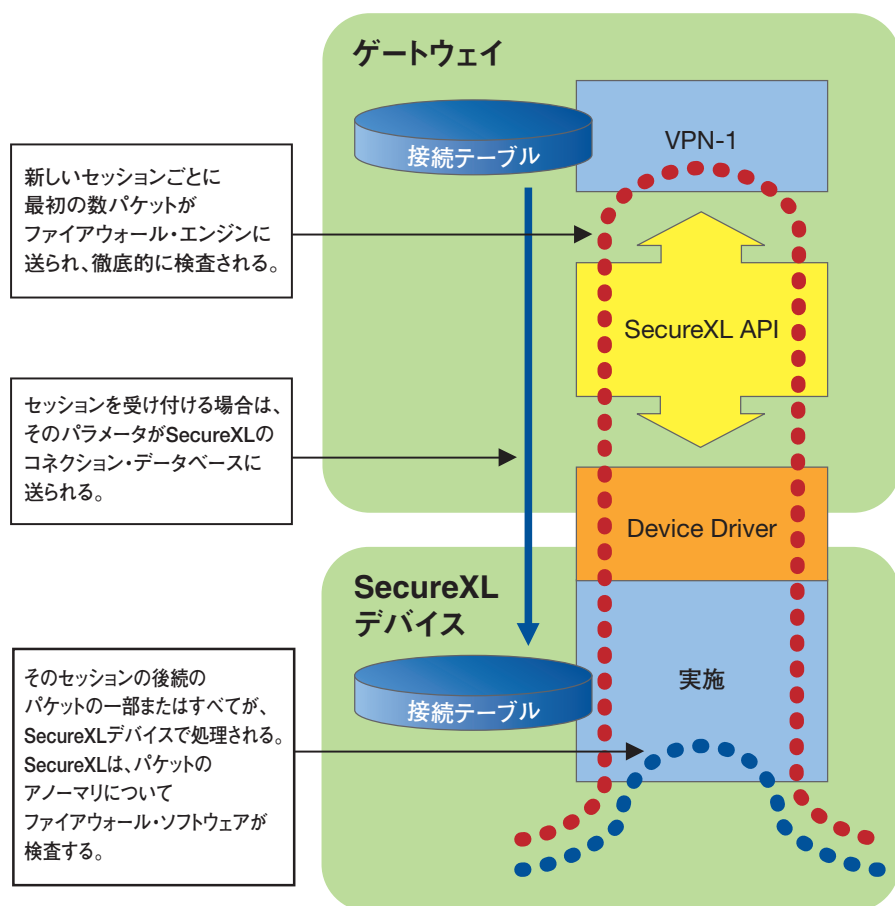
実際のロード・バランシングに関する判断は、ユニキャスト・モードとマルチキャスト・モードのいずれかの方法で行われます。ユニキャスト・モードでは、1台のVPN-1ゲートウェイが「ピボット」と呼ばれるクラスタ全体のコーディネータ役を担います。ピボットは、すべての内向きトラフィックを受信し、どのクラスタ・メンバーがその接続またはトラフィックを処理するかを決定します。一方のマルチキャスト・モードでは、複数の物理ネットワーク・インタフェース・カードをボンディング(1つに束ねること)して、単一の仮想MACアドレスを持つ単一の仮想インタフェースを作ることができます。これにより、複数のネットワーク・セグメントが存在する複雑な導入シナリオにおける柔軟性を向上させることができます。このシナリオでは、1つの仮想インタフェースを持つ各クラスタ・メンバーがすべてのパケットを受信します。パケットを処理するべきかどうかを各ゲートウェイが判断し、最終的に1つのゲートウェイがそのパケットを処理します。そして、その最初のパケットを処理したゲートウェイが、その接続の処理を担当することになります。

### SecureXL：セキュリティ・アクセラレーション

チェック・ポイントが特許を保有するアクセラレーション技術SecureXLは、負荷の高い複数のセキュリティ・オペレーション(チェック・ポイントのステートフル・インスペクション・ファイアウォールが実行するオペレーションなど)を高速化するための、APIを含むソフトウェア・パッケージです。ステートフル・インスペクション・ファイアウォールでは、SecureXL APIを使用することで、こうしたオペレーションの処理を「SecureXLデバイス」と呼ばれる専用モジュールにオフロードすることができます。SecureXLデバイスには、サードパーティが提供する専用ハードウェア・コンポーネントか、パフォーマンスが最適化されたソフトウェア・モジュールを使用できます。

SecureXL対応ゲートウェイのファイアウォールはまず、SecureXL APIを使用してSecureXLデバイスにクエリを発行し、どのような機能が備わっているのかを確認します。次に、その機能に応じて、どのセッションのどの部分をファイアウォールで処理する必要があり、どの部分をSecureXLデバイスにオフロードできるのかを判別するポリシーを実装します。実際にそのゲートウェイを介して新しいセッションの確立が試行されると、ファイアウォールは、各セッションの最初のパケットを検査して、そのセッションが許可されたものであるかどうか、悪意のないものであるかどうかをチェックします。ファイアウォールは、このパケットを検査する際、セッションに対して実行する必要のある処理を判断し、ポリシーに従ってそのうちの一部またはすべてをSecureXLデバイスに転送します。それ以降、そのセッションの該当するパケットは、直接SecureXLデバイスで検査されます。SecureXLデバイスは、対象トラフィックの詳細な分析および処理に必要なセキュリティ・ロジックを実装しています。パケットにアノマリ（異常な部分）を見つけた場合は、ファイアウォール・ソフトウェアでチェックします。またSecureXLには、接続の確立を完全にSecureXLデバイスで行うためのモードが用意されており、これを利用することで膨大な量のセッションを処理することが可能になります。

SecureXLは、セキュリティ・アクセラレーション用途としては最も先進的な技術です。SecureXLでは、どの処理を自ら行い、どの処理をファイアウォール・モジュールで扱うべきかの判断をきめ細かく調節することができます。このため、各ネットワーク環境が必要とするセキュリティ要件に合わせて、セキュリティとパフォーマンスの最適なバランスを得ることが可能です。



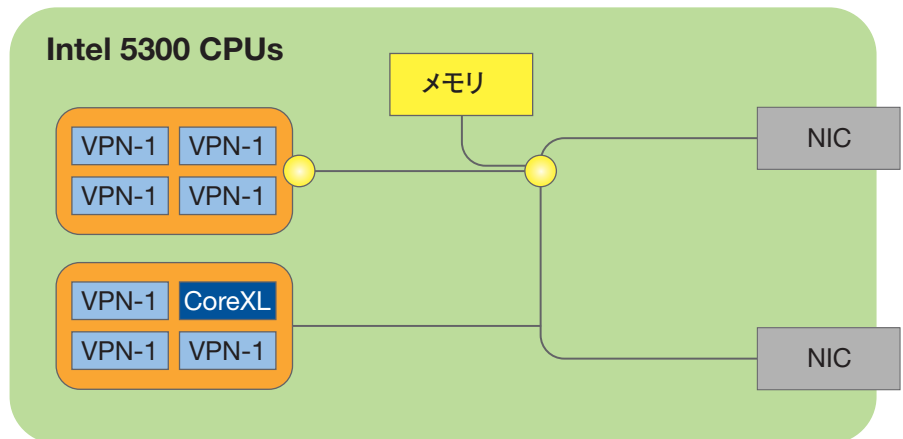
### CoreXL: マルチコア・アクセラレーション

クアッドコアIntel Xeonプロセッサ5300シリーズなどの汎用マルチコア・プロセッサをフル活用する初めてのセキュリティ技術であるCoreXLは、先進のロード・バランシング機能を提供することにより、ファイアウォールで侵入防御を実施するために必要な深いレベルの検査のスループットを向上させます。侵入防御など、これまで高速化が行われていなかったセキュリティ機能のパフォーマンスを向上させるCoreXLは、ネットワークにおいて高いパフォーマンスと高いセキュリティを両立できるように設計されています。

CoreXL技術が有効にされたVPN-1は、まずトラフィックのディレクターとなるコアを決定します。そして、ディレクター以外のコアがVPN-1のインスタンスを実行します。例えば、クアッドコア・プロセッサを2基搭載するシステムの場合、1つのコアがディレクターとして動作し、残りの7つのコアがVPN-1を実行することになります。ディレクターとして動作するコアには、大きく2つの役割があります。1つは、トラフィック受信時にそれをSecureXLで高速化できるかどうかを判断することで、もう1つは、トラフィックに対して深いレベルのセキュリティ検査を実施するコアを割り当てることです。

VPN-1は、セキュリティ検査の負荷を複数のコアに分散させることで、従来のマルチスレッド型のセキュリティ・アプリケーションよりも高い効率性を実現します。これらのセキュリティ・アプリケーションでも、アプリケーションの複数のインスタンスを各コアで実行することにより、マルチコアのメリットを引き出すことは可能ですが、負荷を各コアに均等に分散させることはできません。このため、100パーセントの使用率で動作しているコアがある一方、10パーセントの使用率で動作しているコアもあるといった状況が生まれてしまいます。CoreXLでは、ディレクター・コアにインテリジェンスを持たせることで、各コアへのより均等な負荷分散を可能にしています。

このような負荷分散の仕組みを採り入れた結果、CoreXLでは、スループットを600パーセント向上させることに成功しています。2.66GHzのクアッドコアIntel Xeonプロセッサ5300シリーズを2基搭載したリファレンス・システムでは、CoreXLを有効にすることで、スループットが300 Mbpsから1.8 Gbps超へと向上しています。使用されたテスト・パラメータは、SmartDefense1の7割の設定を有効にした厳格な保護プロファイルです。またリファレンス・システムを通過するトラフィックには、実際にインターネットを流れているものと同様のプロトコルおよびアプリケーションのトラフィックが使用されています。



CoreXLでは、複数のコアにわたリインテリジェントなロード・バランシングを行うことで、より効率的なセキュリティ負荷分散を実現しています。

## まとめ

今日、ネットワークを介して行われる攻撃が、ネットワーク層ではなくアプリケーション層に対して動的に行われるようになったことで、ゲートウェイのセキュリティ・パフォーマンスの向上が強く求められるようになってきました。この問題に対処するには、高いレベルのセキュリティを維持しつつ、パフォーマンス強化につながる新技術をすぐさま採り入れることのできるアーキテクチャが必要です。現状のクローズドなASICベースのアーキテクチャは、アプリケーション層の脅威に素早く対処することができていません。チェック・ポイントのオープン・パフォーマンス・アーキテクチャでは、大規模環境やデータセンターにおいて、高いレベルのセキュリティを維持しながら高いパフォーマンスを実現するために必要となる基盤を提供します。

ClusterXL、SecureXL、CoreXLというチェック・ポイントの3つの特許技術が統合されたオープン・パフォーマンス・アーキテクチャは、常に進化を遂げるアプリケーション層の脅威からネットワークを確実に保護すると同時に、パフォーマンスを一定のレベルに保ちます。またこのアーキテクチャは、マルチコア・プロセッサのさらなる進化といったハードウェアの分野における新たな技術革新を直ちに採り入れることのできる拡張性を備えているため、新技術が登場した場合には迅速にパフォーマンスの向上を図ることができます。このオープン・パフォーマンス・アーキテクチャにより、パフォーマンス低下を心配することなく侵入防御機能を統合できるセキュリティ環境が実現されます。

## Check Point Software Technologies Ltd.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・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、世界中の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、データ・セキュリティおよびVPN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、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。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“ベスト・オブ・ブリード”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・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076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。

The Check Point Open Performance Architecture

P/N:502661-J 2007.08

※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**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD.

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\_jp@checkpoint.com Tel: 03 (5367) 2500