



LIONIC
Security Chip Provider

セキュリティゲートウェイ

**アンチウイルス機能
および
アンチハッキング機能**

高速化手法と利点



Thank you for choosing Lionix

はじめに

このホワイトペーパーでは、図1に示されるようなゲートウェイにおけるセキュリティ機能の進歩とその理由について検討します。従来のゲートウェイの問題点も議論され、それを解決するためにアンチウイルス、侵入防御機能を具備した次世代のゲートウェイの利点を説明します。[1] まず、これまでのセキュリティ・ゲートウェイの進歩を概観すると、大きく3つの世代に分類されます。

第1世代（1990年代後半から2000年頃）はネットワーク機器、特にルータあるいはレイヤ3スイッチに実装されたセキュリティ機能です。これらの機能のある特定経路へのパケットの転送を許可・禁止するアクセス制御リスト（ACL）で代表される非常に初歩的なセキュリティと言えるでしょう。現在はルータおよびレイヤ3スイッチにはほとんどこの機能は実装されています。

第2世代（2000年から2004年頃）は、ルータあるいはレイヤ3スイッチから独立した機器としてのファイアウォールやVPNゲートウェイに代表されます。ファイアウォールは主に発信元のアドレス（IP、MAC）と宛先のアドレスをベース（付加情報としてTCP/UDPポートを利用する場合があります）に、パケットの転送・廃棄を判断するものです。VPNゲートウェイは、発信元から宛先までの仮想的なトンネルを作成することにより、第三者のパケット情報の盗聴、改ざんなどを防ぐ目的で開発されました。

そして、現在は第3世代のセキュリティアプライアンスが必要されていると言えるでしょう。大きな特徴は第1世代、第2世代がパケットの転送、廃棄の判断、あるいはパケットの盗聴防止、改ざん防止を目的としているのに対して、送受信されるデータの内容の正しさ、悪意のあるソフトウェア（Malware、マルウェアと呼ばれます）の添付などを防ぐ事に焦点を置いていることです。



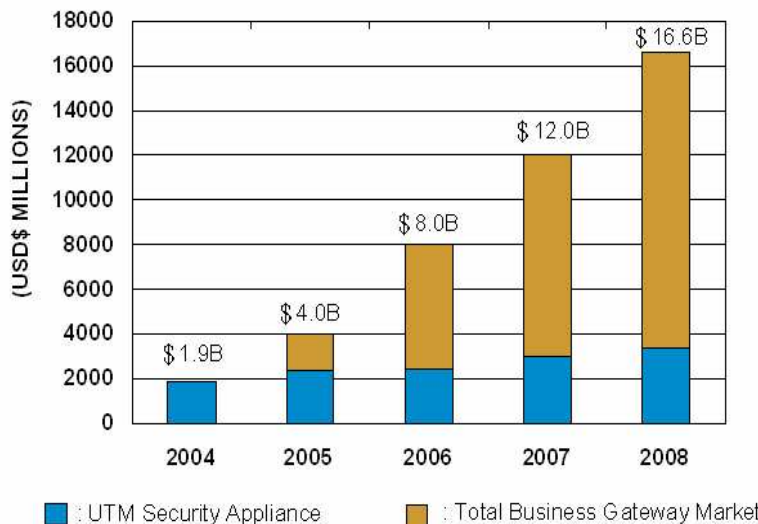
図1 セキュリティ・ゲートウェイ機器の進歩



米国における著名な市場調査会社のIDCは、第3世代のセキュリティアプライアンスの市場規模は2008年には34億米ドル（約4000億円）を超え、かつ年間成長率は16.8%を維持するであろうと予測しています。

またもうひとつの調査会社In-Statによれば、セキュリティアプライアンスに加えて、無線LAN、VoIP、そのほかのアプリケーションレベルの処理をひとつのボックスで扱ういわゆるビジネスゲートウェイの市場規模はさらに大きく、2008年までには166億米ドル（約1兆9000億円）を超えると推定しています。

Worldwide Business Gateway Market Forecast,2004-2008



"(We expect) UTM appliances to overtake conventional firewall/VPN devices in the near future. By 2007, 80 percent of security solutions will be delivered via a dedicated appliance."
-IDC,2004

"The Business Gateway could be responsible for turning the networking equipment industry upside down. Business Gateways will serve a small business entire data, security, and voice communications needs."
-In-Stat/MDR,2004

- IDC forecasts the global Threat Management Market will exceed \$3.4billion in 2008, representing a GAGR of 16.8%
- In-Stat/MDR forecasts broader Business Gateway market (including converged UTM, WLAN, VoIP appliances) will exceed \$16.6 billion in 2008

Lionic社はこのようなセキュリティ市場のトレンドを見据え、現在の問題を解決するとともに将来への展開に備えるべくユニークなアーキテクチャによるセキュリティチップを設計・開発する事をミッションとしています。



ルータによる処理の限界

図2では従来のルータ（あるいはレイヤ3スイッチ）によるセキュリティリスクが示されています。ルータの基本機能は異なるネットワーク間でのパケットの転送に焦点が置かれています。つまり、複数のネットワークシステム間の接続機器として、パケットのルーティングを行うのであって、セキュリティの提供は基本的には考慮されていません。

ルータはネットワーク間のトラフィック転送を効率よく扱うために設計されたのであり、その処理はルータに送られるパケットの論理（IP）アドレスに依存しています。このシンプルな概念により、それまでのX.25などの複雑な通信システムに比べて、ルータによるIP通信はその簡単明瞭な概念と実装によりパーソナルコンピュータ、ワークステーションなどを基礎として、市場に広く受け入れられて急速に成長しました。

しかしながら、そのようなIPの基本概念と処理はネットワークのホストを外部に無防備なままさらけだし、そこにはセキュリティ保護に関する考慮はほとんどされていません。つまり、IP通信ネットワークは基本的にネットワークに存在するホストが、データ通信機能を実装して相互接続されることを前提としています[2]

したがって、もしネットワーク内部に悪意のある中継者やホストが存在すれば、データの盗難や不正な盗聴などが簡単に行われてしまいます。これは例えばIPネットワークの初期に開発された代表的な通信プロトコルであるTELNET、FTPなどをみると即座に理解できます。ユーザIDやパスワードは平文で交換されるために第三者が盗み見ることはきわめて容易です。あるいは電子メールを考えてみてください。通常利用されるSMTP/POPプロトコルでは、全てのメッセージは可視的なテキストとしてルータ間で送受されています。

このためにルータやレイヤ3スイッチをベースとするゲートウェイには、これまでのパケット転送（ルーティング）、アクセス制御に加えて、ファイアウォールやVPN機能を統合する必要性が出てきました。これらの機能はルータ自体に実装されたり、あるいは必要に応じて外部の独立したアプライアンスとして実装されたりしています。

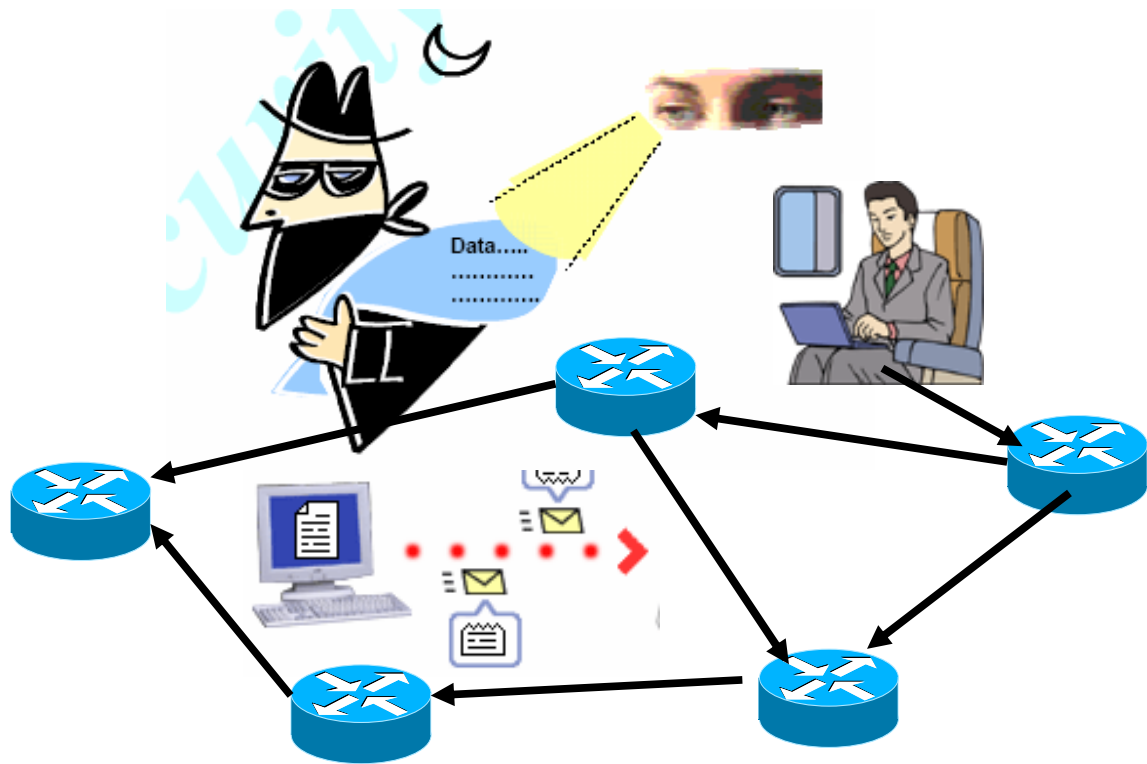


図2 ルータによるパケット転送と第三者による盗聴のリスク

ファイアウォールやVPNだけではもはや十分ではない

これまでのネットワーク環境では、ファイアウォールやVPNはユーザの必要とするネットワークセキュリティの要望を十分に満たしてきました。しかし、今日では、ネットワークの中にトロイの木馬やワームなどの新しい攻撃あるいは脅威が出現してきました。残念ながらファイアウォールやVPNはこれらの新しい攻撃を処理するのは困難であり、より強固な防御のシステムが求められています。 [3]

図3に見られるように、ファイアウォールはパケットのヘッダ部分のみを調査します。検査される情報は、宛先IPアドレス、発信元IPアドレス、宛先ポート番号、発信元ポート番号に加えて、簡単なフラグだけです。アナリストのレポートによれば、このような手法は特定ポートへのパケットの送信を拒絶したり、特定のIPアドレス、MACアドレス、フラグを持つパケットを破棄したりできます。このことから明らかなように、ファイアウォールは攻撃者がネットワークの外部に存在して、社内ネットワークへの侵入を試みるという前提で開発されたものです。 [4]

しかし、それらはウイルスやハッキングのように一見しただけでは正常なネットワークアクセス手法を利用しての攻撃を効率的に防ぐことはできません。たとえば正規の発信元からの電子メールに、発信者本人が知らないうちに悪意あるウイルスが添付される可能性は、現在では広く知られています。これらのウイルスは添付ファイルなどを詳細に吟味しない限り、検出ができません。つまり、発信元や宛先アドレスだけのような表面的な情報だけを検査するだけでは不十分なのです。

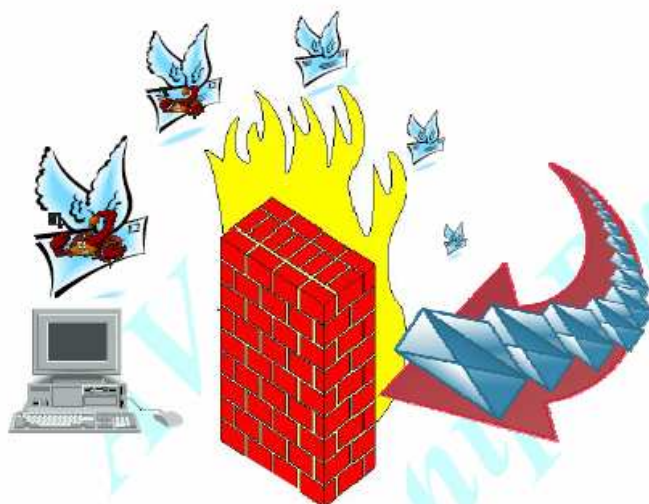


図3 ファイアウォールによる表面的セキュリティのリスク

また、図4ではトランスポート層においてデータを暗号化するVPN機能が示されています。しかし何らかの手段により、暗号化キーが漏洩あるいは解読されればデータは簡単に解読されてしまうでしょう。 [5].

さらにファイアウォールと同様に、この手法も送受信されるデータの内容を検査するものではありません。

結論としてはファイアウォールやVPNは一定のセキュリティソリューションを提供するものの、完全なソリューションではありません。

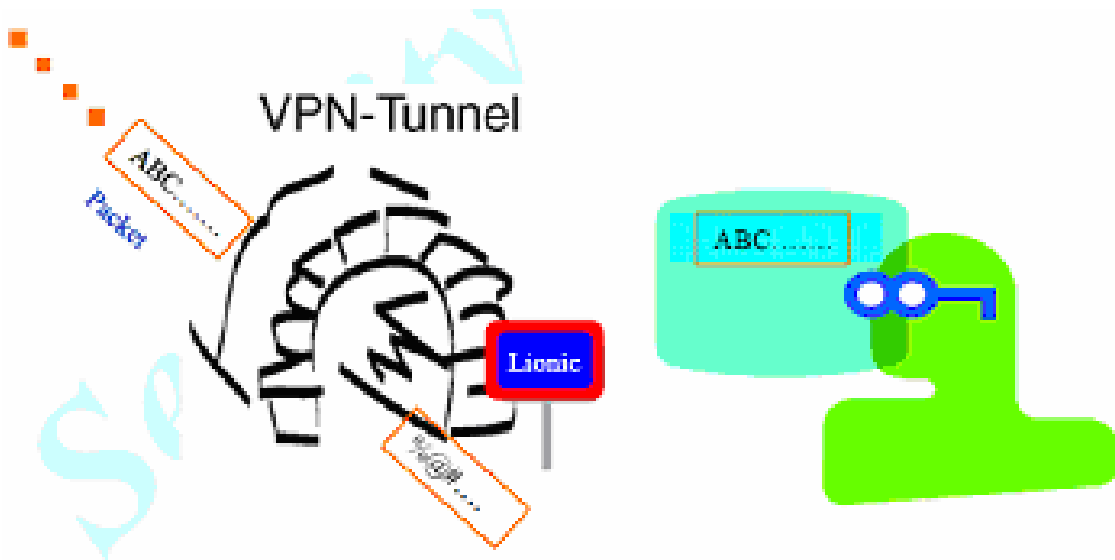


図4 VPNにおける暗号化鍵の漏洩と解読のリスク

ファイアウォールおよびVPNゲートウェイの限界

このセクションでは、ユーザが単純にファイアウォールやVPNゲートウェイ機能だけを利用している場合の損失について検討します。図5－（1）および（2）はこれらのセキュリティソリューションでは防ぐことのできないウイルスやスパイウェアなどの被害状況の統計データです。なお独立行政法人情報処理推進機構（IPA）ではこれらの調査結果と独自の算出モデルにより、2003年のウイルスによる国内被害総額（風評などによる二次被害は含まず）を3,025億円、1事業所あたり約28万円と見積もっています。

これらのレポートを一見してわかることは、アンチウイルスやアンチハッキングなどの新たなセキュリティメカニズムの導入は、それが無い場合の復旧作業による損失を十分に補って余りあるものです。さらにビジネス上の影響は計算することもできないでしょう。

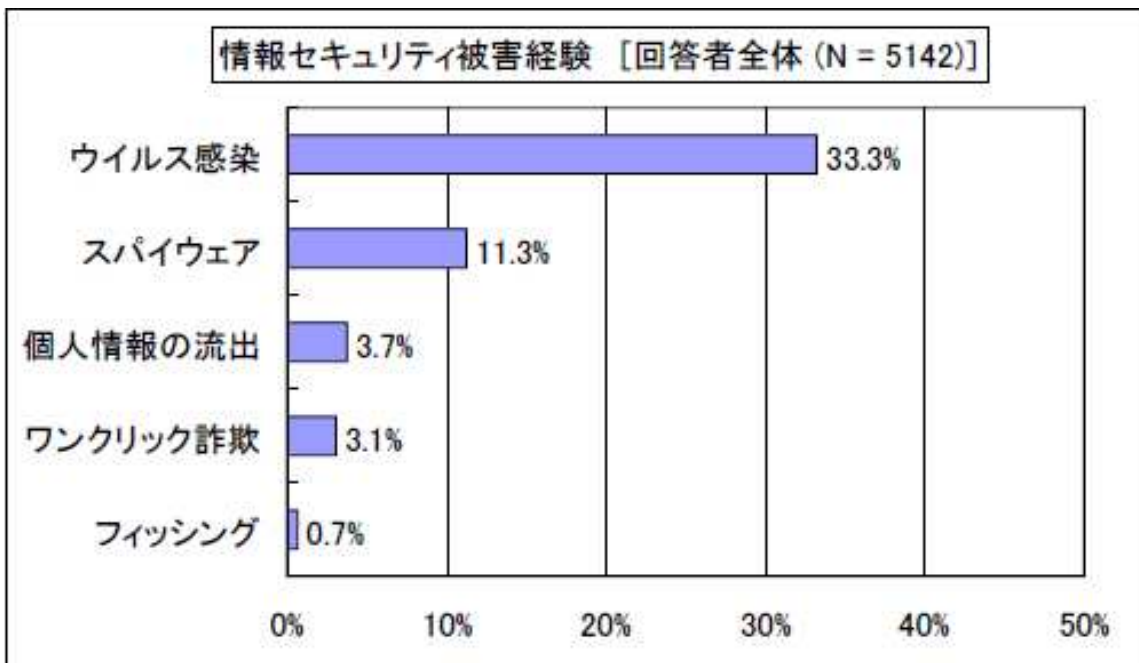


図5－（1） ファイアウォールとVPN利用のユーザのリスク
独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/fyl7/reports/ishiki/index.html>

情報セキュリティ被害経験 1.被害経験の有無 [職業別]

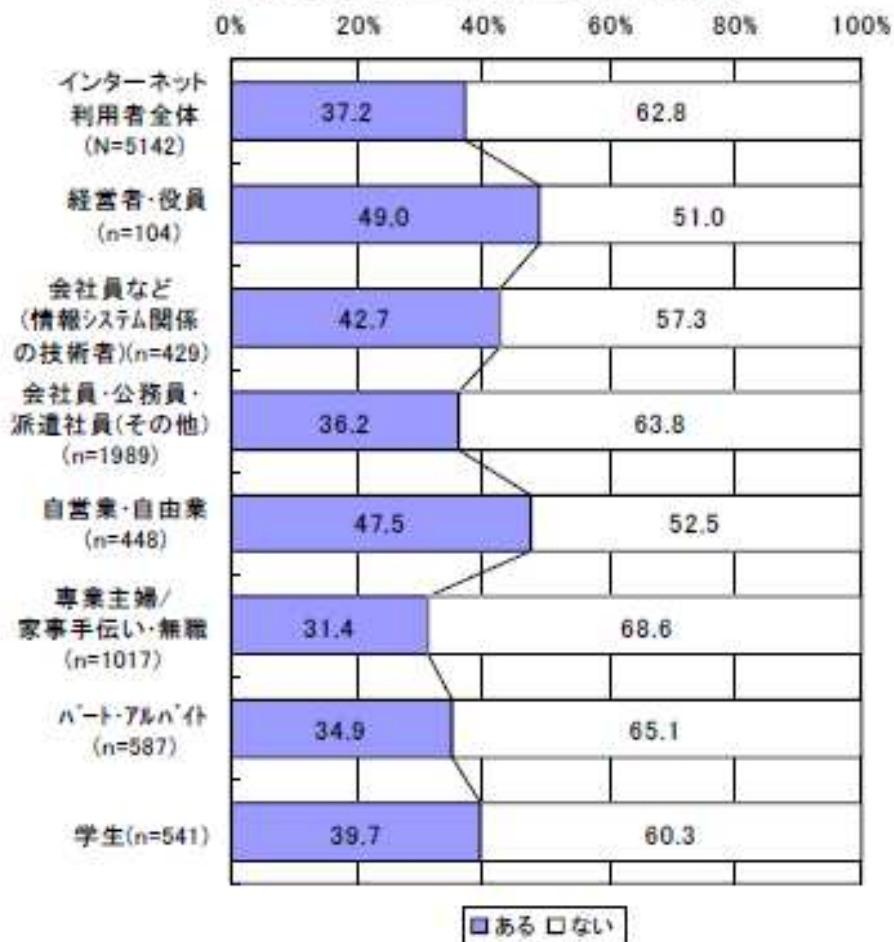


図5－(2) ファイアウォールとVPN利用のユーザのリスク
独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/fy17/reports/ishiki/index.html>



他方、Table1には2種類の新たなセキュリティイベントがその影響する損失とともにリストアップされています。ここには先年大きな社会的問題となったSQLスラマーやMSブラスターによる経済的被害が示されています。これらの数字は多くの人を驚かせるに十分な値でしょう。

Table 1; Two serious worm attack in 2003

	Occur Date	Attack	Damage	Sufferer
SQL slammer	2003/1/24	Port 1434/UDP	1 Infect 67,000 servers in ten minutes 2 Damage over 120,000 servers in 5 hours	The bank of American Microsoft Continental airline Seattle 911
W32/Blaster	2003/8/11	DDoS	1 To cause serious loss 2 Still distribute over the world 2 Polymorphic Viruses: W32/Blaster.A W32/Blaster.B W32/Blaster.C W32/Blaster.D	Japan USA Korea China Taiwan

SQL Slammer Loss: reference Trend micro website

W32/Blaster Loss: reference communication magazine, CA website

図6と7は深刻な結果となった全世界におけるウイルス感染状況の資料です。

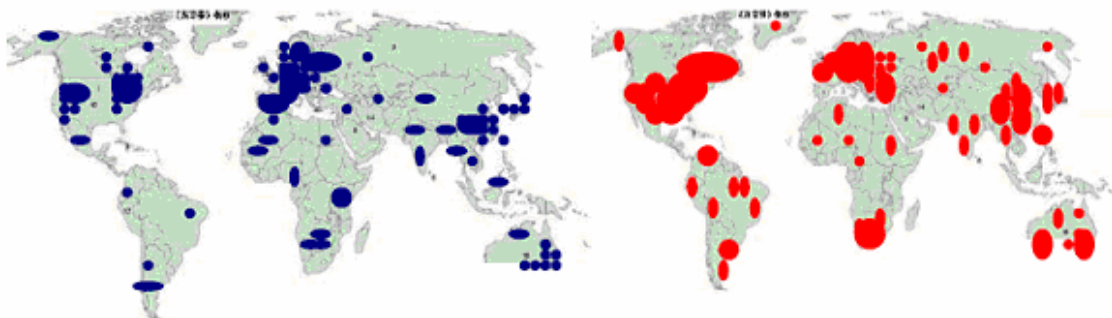


図6 SQLスラマーの感染被害

図7 W32/ブラスターの感染被害

完全なセキュリティのためのアンチウイルス、侵入防御機能

図7に示されているように、ウイルスやハッキングなどの悪意あるコードは、しばしばユーザペイロード（データ部分）に隠されています。したがって、リスクや損失を未然に防ぎ、LANからウイルスやハッキングコードを取り除きたければ、このユーザペイロードを検査する必要があります。

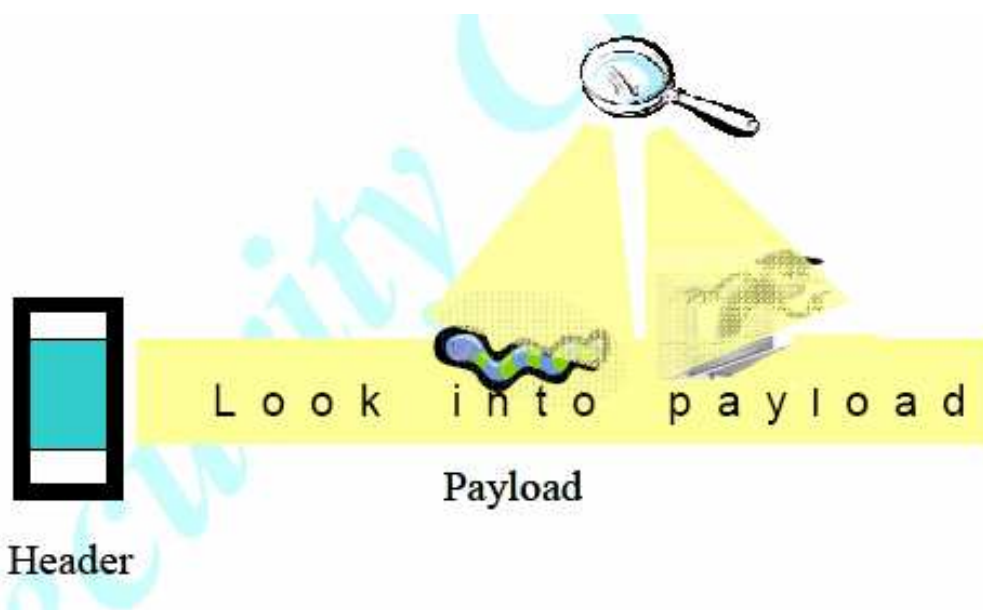


図7 ウイルスは通常ペイロード内に隠れている

そして、これこそがファイアウォールやVPNによるヘッダー検査では実現できない機能なのです。したがって将来の統合型ゲートウェイにアンチウイルス、侵入防御機能を追加することは、ウイルスやハッキング攻撃を効率よく防ぐ手法となります。

しかし、どうすれば効率よくペイロードの検査を実行できるのでしょうか？また、将来の新たな攻撃にすばやく対処するためにはどうすればいいのでしょうか？現在のネットワーク環境は、ウイルス、トロイの木馬、ワームなどの攻撃に加えて、フィッシング、ファームなどの被害が報告されています。しかもそれらの攻撃は多種多様であり、ほとんど毎日といいほど新種の攻撃が報告されています。このような多岐にわたる攻撃に、どのように対処すればいいのでしょうか？すべての攻撃に対する回答を、しかも遅滞なく提供するにはどうすればいいのでしょうか？



この質問に対するひとつの興味ある回答は、オープンソースをベースとしたセキュリティアプライアンスです。これはオペレーティングシステム、侵入検知、アンチウイルス、アンチハッキングなどにオープンソースのソフトウェアを採用して、統合型セキュリティ・ゲートウェイを提供するソリューションです。オープンソースの明確な利点は、それが全世界の知恵を結集した成果であるということです。幅広いコミュニティからの迅速な対応は何にもまして魅力的なソリューションです。実例を挙げればSNORTです。SNORTは全世界で30万件を超えるダウンロード数を持ち、最も多く利用されている侵入検知システムであり、日々新しい機能を取り入れて進化しています。しかしながらSNORTの大きな弱点はその処理性能です。参照されるルール数が多くなると指数級数的にスループットは低減します。

しかしながら、このような課題にもかかわらず、例えばドイツに本社を置くASTAROを筆頭とする多くのスタートアップベンチャー企業が、このようなアプローチを採用して、オペレーティングシステムにはLinux、ポート監視にはNMAP、侵入検知にはSNORTなどのソフトウェアを利用して、統合型セキュリティアプライアンスを構築しています。

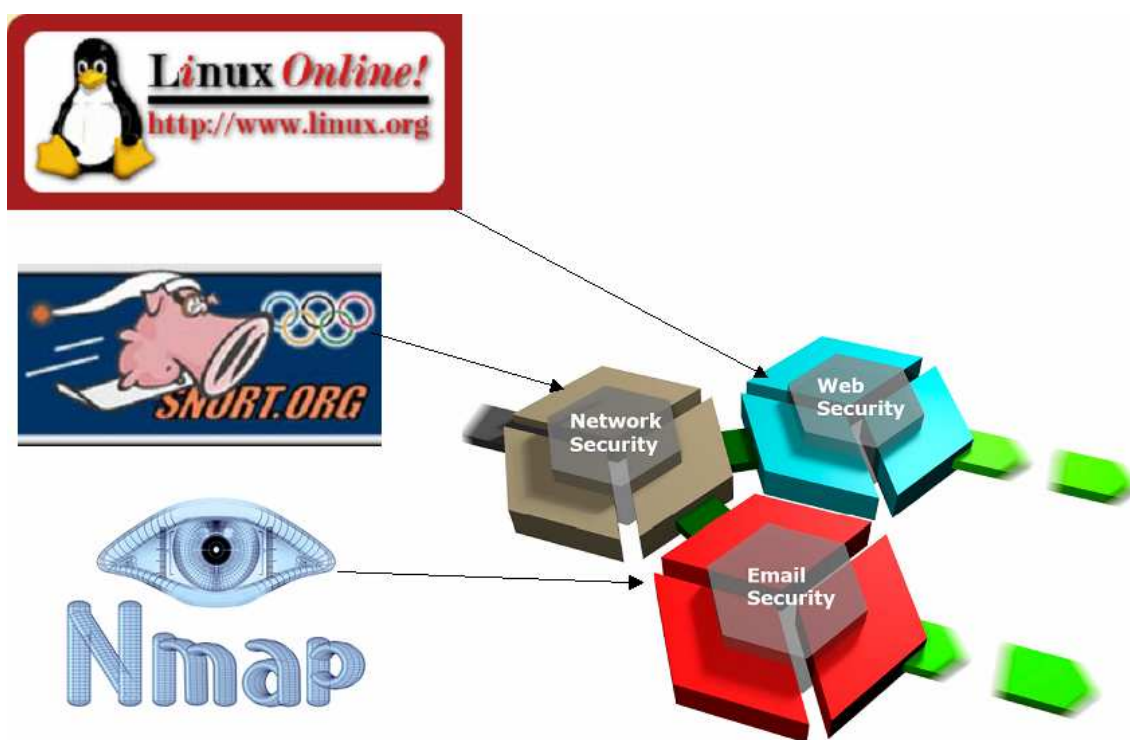


図8 オープンソース・セキュリティアプローチの一例

オフィス規模と用途を基準にした2つの「統合」

ファイアウォールやアンチウイルスなど様々なセキュリティ対策を施す企業が増えたにもかかわらず、ウイルスやワームによる被害は後を絶ちません。その最大の原因はセキュリティ上の脅威が複合化したことです。2001年夏に大流行したNimdaやCodeRedの頃からウイルスやワームが、トロイの木馬、バックドア、脆弱性攻撃など複合化し、大きな被害を与えていることは周知の事実です。

これに対抗するには、ファイアウォールやアンチウイルス、侵入検知など従来個別に導入されていたソリューションを組み合わせる必要があります。そこで、今脚光を浴びているのが「統合型セキュリティ・アプライアンス」製品です。ここで言う「統合」は、オフィス規模と用途を基準にして2つに分けることができます。ひとつは複数のセキュリティ・ソリューションを統合することで、大規模な拠点やオフィスでのセキュリティを徹底的に高めることで、もうひとつはセキュリティ・ソリューションとネットワーク機能を統合することで、中小規模の拠点やオフィスでのセキュリティをコストをかけずに高めることです（図）。従来、こうした統合をセキュリティ・アプライアンスで実現しようとする、技術的には可能であっても価格が高くなり過ぎて導入は難しかったのですが、近年は、安価で高いパフォーマンスを備えた製品が市場に登場するようになったので、かなり導入しやすくなっています。

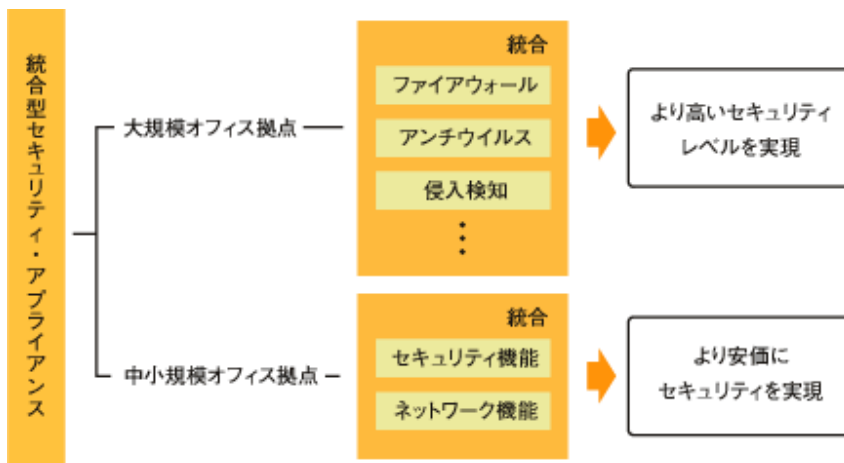


図9. オフィス規模と用途を基準にして最適なセキュリティ・アプライアンスを選択する



ゲートウェイでセキュリティ対策を実施、セキュリティレベルを高める

セキュリティ・アプライアンスで重要なのは、ネットワークの入り口にあるゲートウェイで共通インタフェースを使って包括的に対処し、抜けのないセキュリティ対策を実施することです。ゲートウェイでの対策は、アンチウイルス、侵入検知の両面で大きな効果があるでしょう。

まずアンチウイルスですが、アンチウイルスは、ハードディスク内のファイル・スキャンから、書き込み時スキャン、メモリ内スキャンという形で発展してきました。しかし、その後Webサイト閲覧時に感染するNimdaのような形で侵入するウイルスが登場したことから、現在は、クライアントやサーバーにファイルやトラフィックが到達する前にゲートウェイでブロックするのがベストソリューションとして認識されつつあります。

また、最近では定義ファイルが配布される以前に新種ウイルスを検出するヒューリスティック・スキャンも出てきたが、定義ファイルで徹底してウイルススキャンを行うことは相変わらず極めて重要です。にもかかわらず、定義ファイルを適用していても、大規模なネットワーク環境では取り残されるクライアントが出てくる可能性が排除しきれません。その場合にもゲートウェイでウイルス対策を施しておけば、感染リスクを抑えることができるでしょう。

一方、侵入検知はコンピュータへの不正な侵入対策というイメージが強いが、実際にはネットワークに無差別にパケットを送りつけるDoS攻撃なども検知する必要があります。ファイアウォールの役割は基本的には外部からの通信を通すか、通さないかであり、DoS攻撃には対応できません。そこで、ゲートウェイの侵入検知で不審なパケットをブロックすることができれば、社内のネットワークがオーバーフローを起こすことがないでしょう。その意味で、ゲートウェイで侵入検知を行うメリットは非常に大きいと考えられます。

図10には、このようなアンチウイルス、侵入防御機能を統合したゲートウェイを利用する利点が示されています。これらの製品は多くの利点をもたらす、ウイルスやハッキング攻撃を防ぐレイヤ7のセキュリティ機能を提供するので、多くのユーザにとって魅力的であるでしょう。これらの技術的、市場的動向は、結果的に近い将来において、ネットワークの各階層におけるセキュリティ機能の実装（マルチレイヤセキュリティ）を必要とするでしょう。



Function

Real-time update signature
 Real-time to defend attack
 Protect internal network
 Defend in the front of LAN

Cost

Reduce IT manpower
 Low appliance cost
 Low maintenance fee

Benefits

Multi-Layer Security Solutions

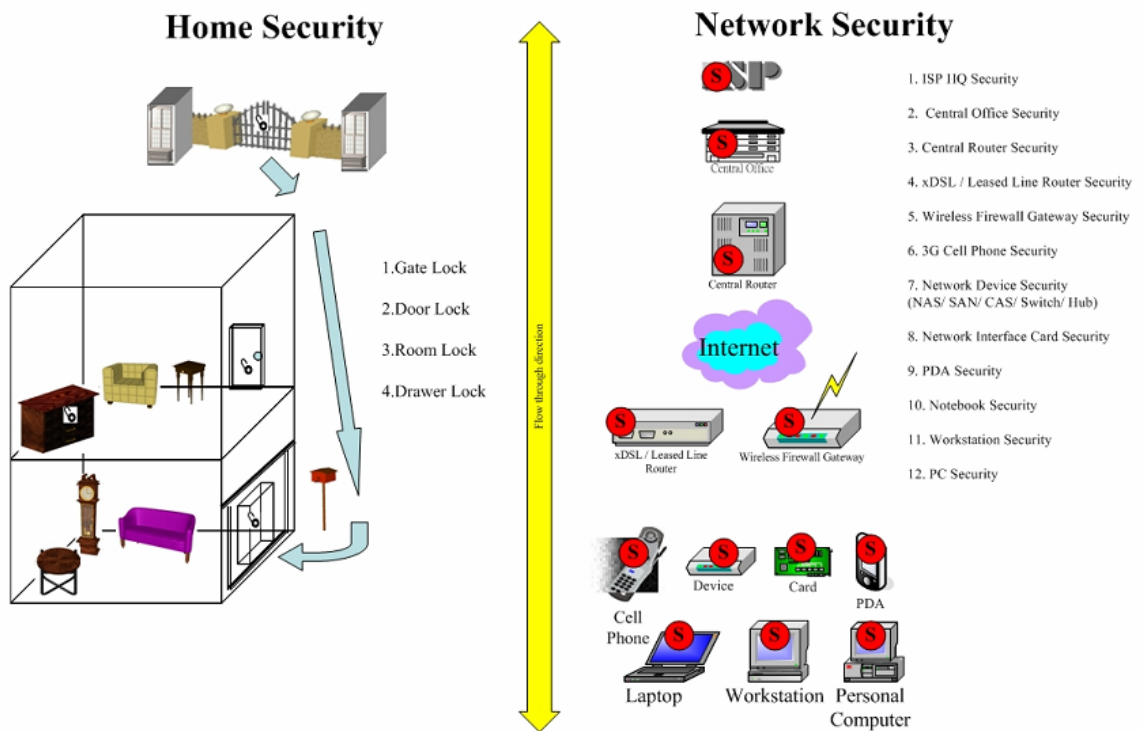


図10 統合型セキュリティ・ゲートウェイの利点



結論

ネットワークセキュリティ要求の観点から、このペーパーではネットワーク内部におけるアンチウイルス、侵入防御機能を統合したゲートウェイの重要性について記述しました。

セキュリティアプライアンス市場の需要傾向として、IDCは2008年まで年率16.8%の成長を予測しています。また、In-stat/MDRのレポートでは、マルチセキュリティ・ゲートウェイの市場は2008年度に1兆8千億円を超えると推定しています。つまり、アンチウイルス、侵入防御機能は次世代セキュリティ・ゲートウェイにとって必要不可欠なものです。

それではLionicはどのようにこの問題に取り組んでいるかをご説明しましょう。Lionicはまずセキュリティに対するアプローチは多岐にわたり、単独のソリューションでは困難であることから、オープンソースによるソリューションに全面的に同意します。しかし、オープンソースは前述のとおり、ソフトウェアに大きく依存するので処理性能に懸念があります。

これを解決するにはどうすべきか？そのヒントは他ならぬPCにおける心臓部とも言えるCPUのアーキテクチャにヒントがあります。代表的なマイクロプロセッサであるインテルのマイクロプロセッサを例にとりましょう。現在のXeon、Pentium-4などの高速プロセッサは、その本質的アーキテクチャは15年前の80386と同等です。80386は当時のコンピュータの処理性能に対する要望のうち、テキスト処理や分岐判断などの高速に実行するために設計されていました。ところがコンピュータでの仕事の範囲がひろがるにつれ、このような処理だけでは十分でないことが判明してきました。例えばCADなどの図形処理はその内部で多量の数値計算を実行しなければなりません。80386の数値演算処理は、きわめて簡単なものでしかも整数演算処理に限定されていました。浮動小数点演算はソフトウェアで実行されたために非常に性能の悪いものでした。

そこで、インテルはこの問題を解決すべく浮動小数点演算を専門に実行するハードウェアを開発しました。これが80387と呼ばれるチップです。ところが、ここでひとつの問題が発生しました。それはすでに市場にはあまたの浮動小数点演算を実行するアプリケーションが存在したことです。これらはインテルにとってはユーザが開発したものですから、新たにアプリケーションを開発するように依頼することはできませんでした。どうしても既存のアプリケーションを実行しなければならなかったのです。

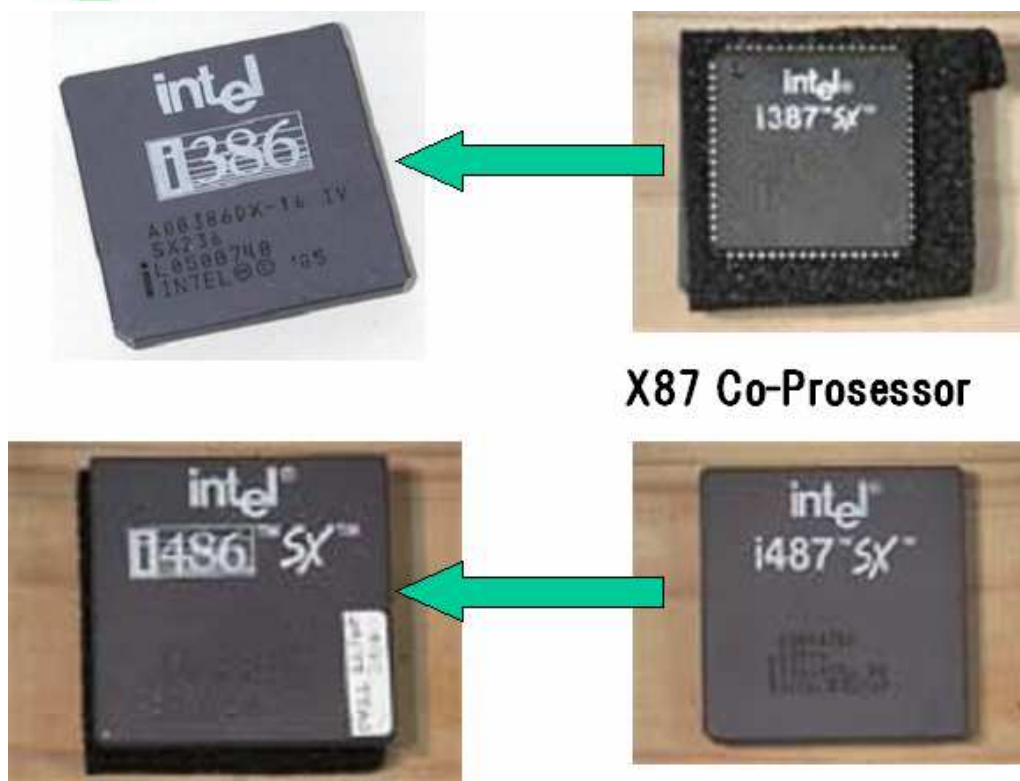


図11 インテルのマイクロプロセッサと浮動小数点演算プロセッサ

そこで、インテルがとったアプローチは現在ではよく知られています。浮動小数点演算命令を実行するときに、専用のハードウェアチップ(80387)が存在するかどうかをチェックして、もし存在すればこの処理をそのチップに任せることとして、もし、存在しなければソフトウェアによるシミュレーションを実行する事でアプリケーション・ソフトウェアからはその違いを隠蔽したのです。

この方法は、既存のアプリケーション・ソフトウェアの膨大な資産を有効利用しながら、リスクなく高速化するという意味で画期的なアイデアでした。しかも高速化とコストの選択肢をユーザは自由に選べます。例えば高速化よりもコストが重要な場合には全てをソフトウェアでシミュレーションすればよいのです。そしてこうして開発されたアプリケーションソフトウェアを高速化する必要に迫られた場合にこの浮動小数点演算プロセッサを追加することにより、アプリケーションの修正やテストを一切必要とせず直ちに目的を達成することが可能です。

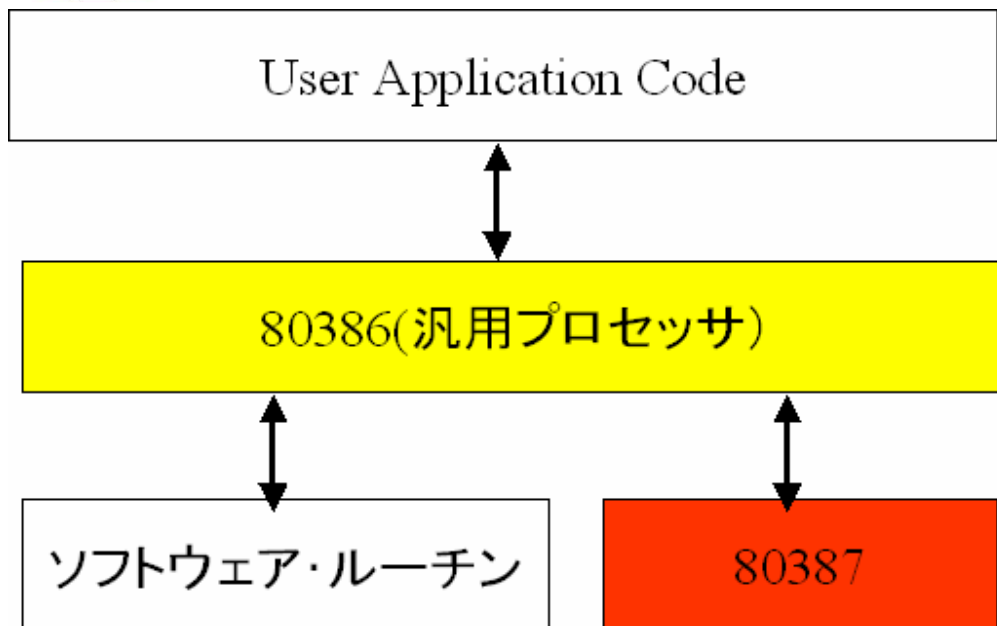


図12 浮動小数点演算プロセッサとユーザアプリケーション

Lionicはこのアプローチにヒントを得ました。Lionicの分析では現在のセキュリティ・アプライアンスの機能はパターンの検索機能に依存しています。ウイルスのシグネチャ、異常動作分析、さらには遺伝子解析などに利用される機能は、全文検索とあいまい検索の処理で代表される非常にCPU依存度の高いプロセスです。これはセキュリティのみならず、パターンの認識、比較を実行する処理に汎用的に適用できるものです。

とりわけ重要な機能は、Unixで多用される「正規表現」です。この正規表現処理は現在全てのセキュリティ・アプライアンスで重要な機能として利用されています。この代表的な例が前述のSNORTです。また全文検索システムとして有名なNAMAZUなどでも頻繁に利用されますが、そのホームページでは正規表現によるフィルタは非常に強力であることと同時に、最もCPUパワーを必要とし、従って最も処理時間がかかるという報告がされています。

さらにこのようなCPUハングリーなアプリケーションのセキュリティ分野における必要性を裏付ける資料は、世界最大のマイクロプロセッサベンダーであるインテルが、図13のような予想を公開しています。

このデータによれば、ルータなどの第1世代の頃に必要とされたプロセッサ能力は、ひとつの packets 処理において約50命令とされていました。ところが第3世代の代表である侵入検知あるいはアンチウイルスでは、これが約4万5000命令と



ほぼ900倍と推定されています。そして、この傾向は今後も続くであろうということは予測に難くありません。

- L7 (content) lookups ? 900 times of Layer-2/3/4 lookups
- Our solution overcomes this computing intensive task.

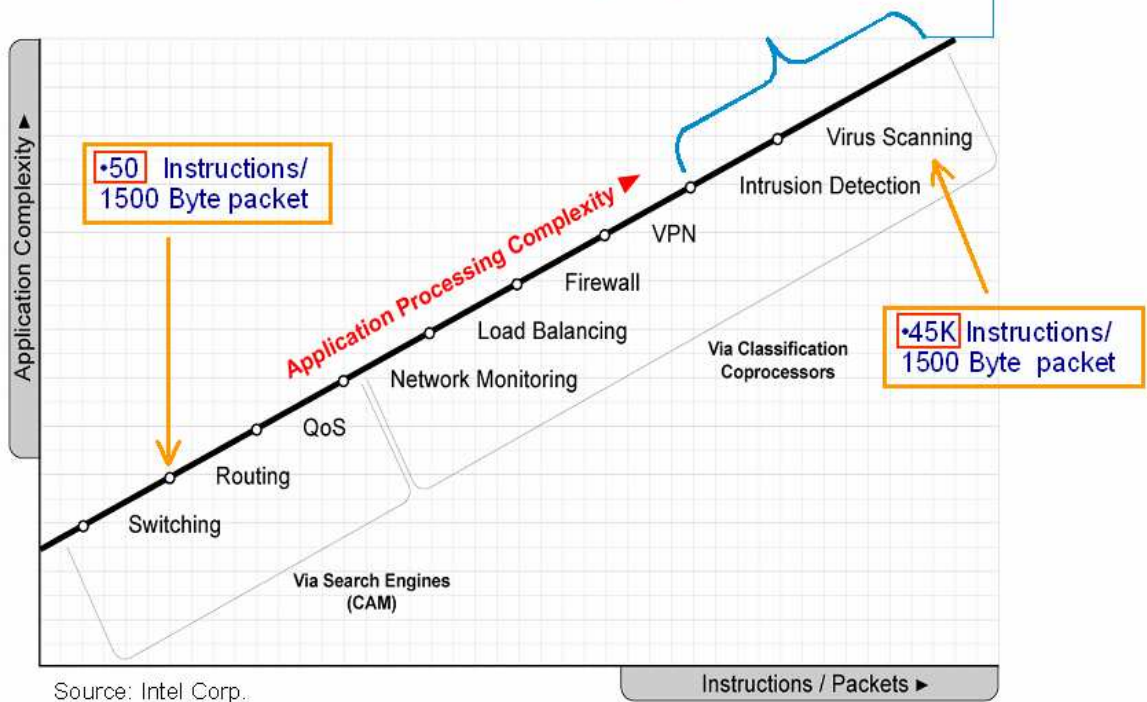


図13 CPUと付加プロセッサによるパターンマッチング高速化の比較

さらにアンチウイルス、アンチハッキング機能を実現するには、大容量のシグネチャ・データベース（ルール・データベース）との比較が発生します。これはプロセッサとメモリ間の頻繁なアクセスを引き起こすので、効率よくこのデータベースを格納、圧縮、伸展、精査する機能も重要な要素です。

例えば、一般にウイルスは大きな電子メールに添付されるでしょう。この場合、ネットワーク上でみれば電子メールは複数のパケットに分割されています。したがって、ネットワーク型の侵入検知システムでは通常このパケットの格納、再構成がウイルスの検査に先立って必要です。明らかにこのような処理は速度に大きな影響を及ぼすものです。

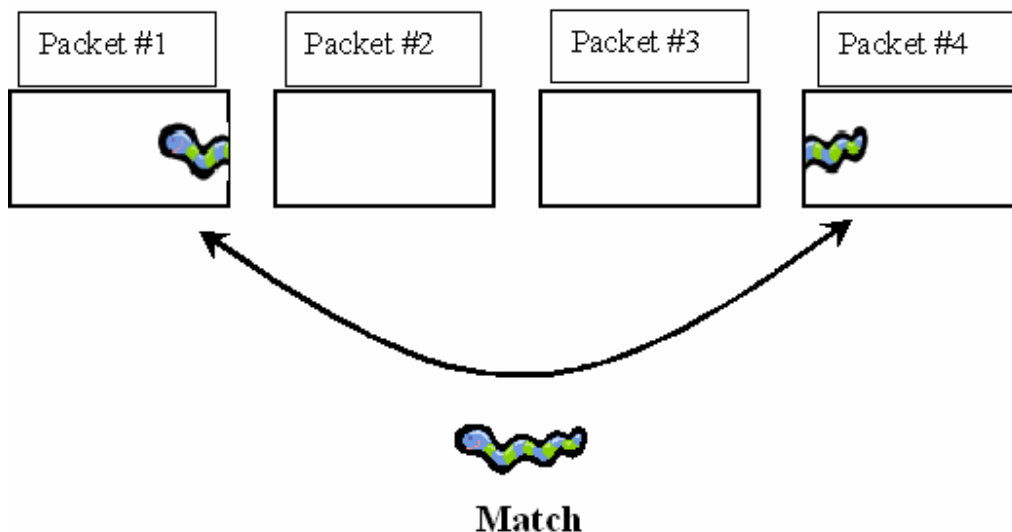


図14 複数パケットに分割されたウイルスの検出

あるいは、検査すべきデータに加えて、ウイルスのシグネチャあるいはルール定義のデータベースが最近では何万ルールとなるものも珍しくありません。これは直ちに検査プロセスとメモリアクセスシステムとの間でのボトルネックを引き起こすことが明確です。

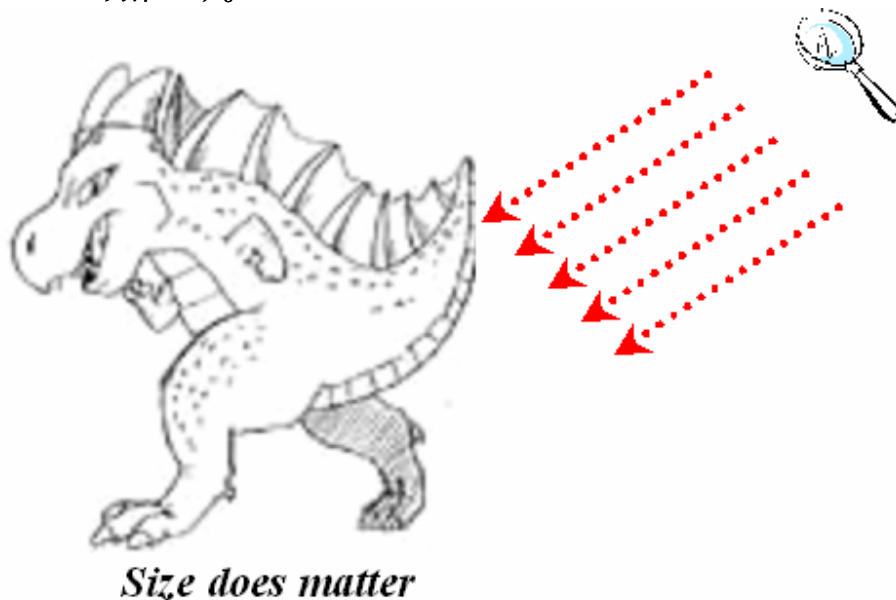


図15 巨大なデータとシグネチャルールの検索によるメモリアクセス

また、データの内容をスキャンするには任意の場所から、バイト単位に正確に比較を実行しなければなりません。シグネチャが長いものやあるいは複数の部分



に分割されるものなどに関しては、バイト単位での連続的なスキャンが非常に多く発生します。これはCPU処理とメモリアクセスの両方に大きな負担をかけるものです。

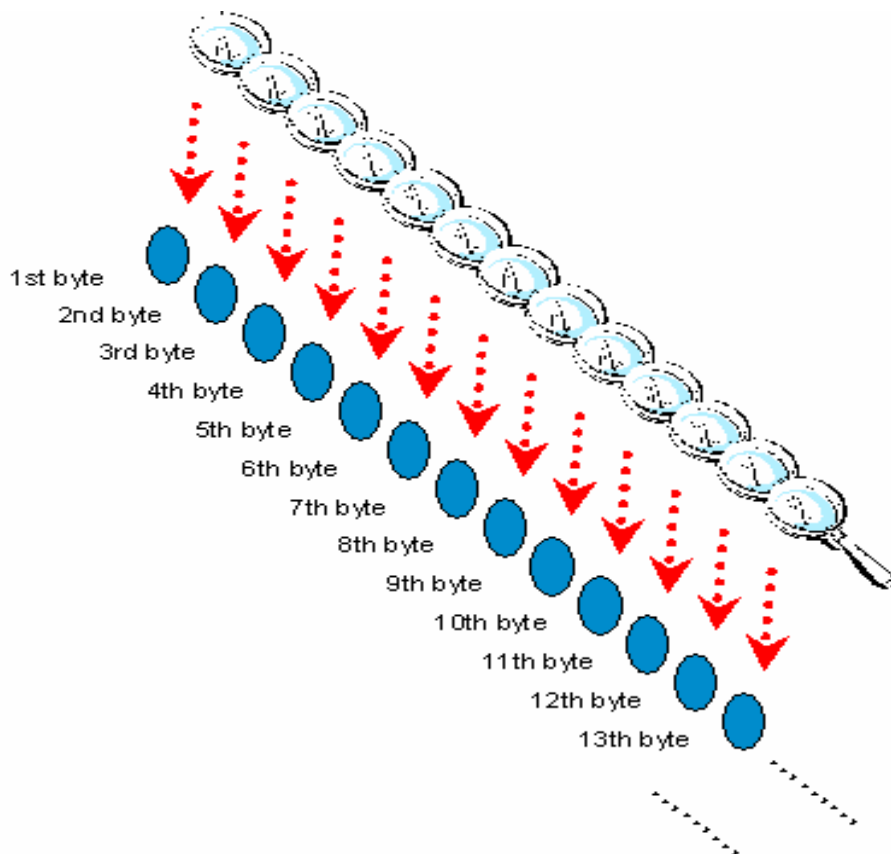


図16 メモリ内容の詳細なバイト単位の比較

Lionicは、上記のような考察に基づき、ユーザアプリケーションとしてのアンチウイルス、アンチスパム、侵入検知ソフトウェアなどに最適化されたパターンマッチング（正規表現）高速化チップ（商品名ePavis）とそのAPIライブラリを開発しました。

これらのチップはPCIやMini-PCIインターフェイスの基盤に実装されて、SNORTのアクセラレータとして評価されています。

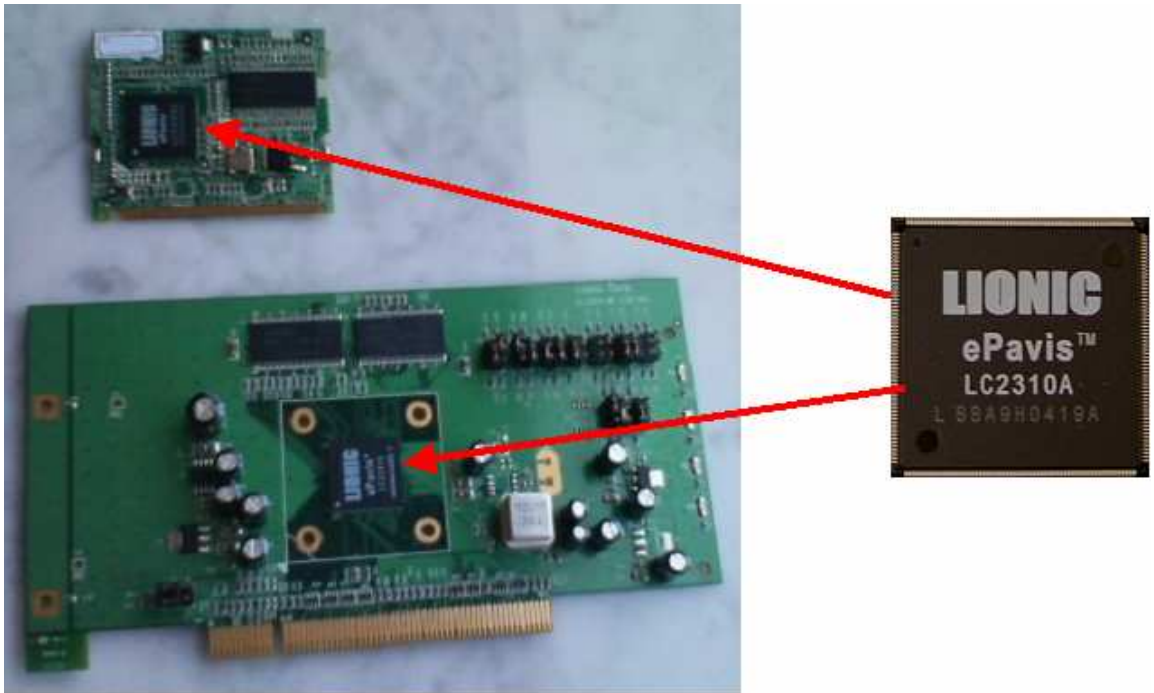


図17 LionicチップとPCIボード上の実装

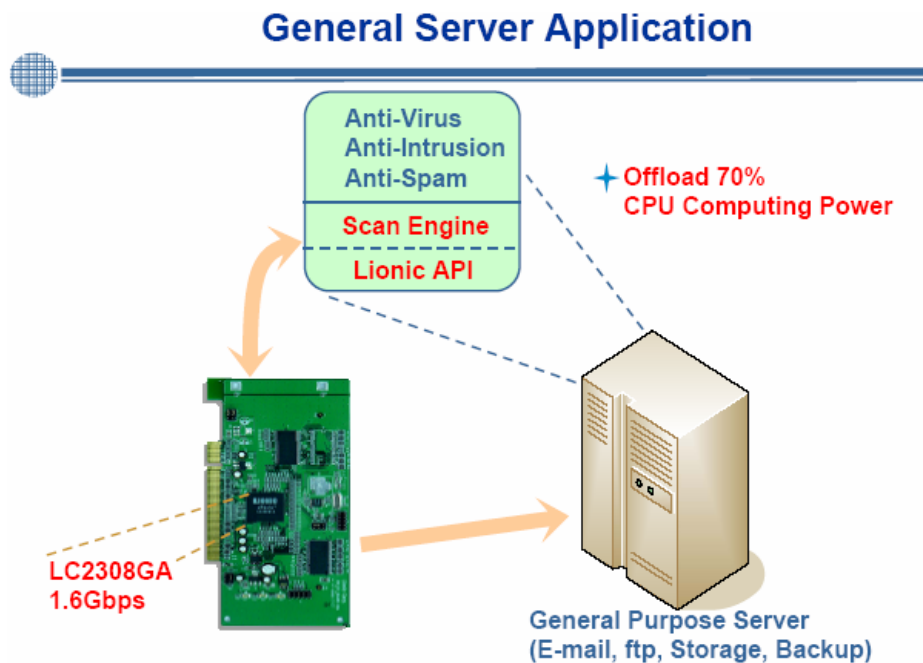


図18 LionicチップとAPI ライブラリ、スキャンエンジンによる高速化



実際にこのアプローチによるハードウェア高速のベンチマークレポートを次に示します。この例ではセキュリティソフトウェアとしてSNORTを採用し、LinuxベースのPC（1.2GHzモバイルCeleron、128MBメモリ、4ポート10/100イーサネット）にPCIインターフェイスで高速化ボードを付加した場合とソフトウェアだけの場合の性能を比較しています。

結果は非常に印象的なもので、特に負荷が高い場合においてはソフトウェアだけでは1.2Mbpsまで処理能力が低減したのに対し、高速化ボードを併用した場合には36Mbpsの処理能力を維持しました。その差は実に3000倍と開いています。

Scenario 1 (Normal case)	Scenario 2 (Extreme case)
<ul style="list-style-type: none"> ■ SW: uCLinux, Linux 2.6.12 ■ Chariot 5.0 <ul style="list-style-type: none"> ■ 10 TCP connections ■ Random port ■ Random Size ■ Duration time : 10 Minutes ■ Standard Snort with rule number:2951 	<ul style="list-style-type: none"> ■ SW: uCLinux, Linux 2.6.12 ■ Chariot 5.0 <ul style="list-style-type: none"> ■ 10 TCP connections ■ FTP file transfer used to increase CPU workload ■ Random Size ■ Duration time : 10 Minutes ■ Standard Snort with rule number:2951

	Scenario 1 (Normal case)		Scenario 2 (extreme case)	
	Snort only	Lannic-100B accelerated	Snort only	Lannic-100B accelerated
Throughput	79M	148M	1.2M	36M
CPU Utilization	99.29%	9.92%	99.60%	79.02%



また、前述のSNORTエンジンのAPIライブラリに加えて、アンチウイルスソフトウェアでは、ロシアの著名なAVソフトウェアベンダーであるKasperskyとの戦略的なパートナーシップを締結しており、定評あるウイルススキャンエンジンとの統合を図ったSDKを開発しました。このチップ、APIライブラリ、スキャンエンジンとの組み合わせにより、ユーザはすでに実証された信頼性の高いアンチウイルスソフトウェアの、ハードウェアによる高速化をローコストで実現できます。

Lionicではこのチップの利用範囲は非常に広く、セキュリティアプライアンスから、VoIP機器（VoIPで利用されるSIPプロトコルはHTML類似のテキストベースなので、テキスト処理が多いと予想されます）やあるいはネットワークアクセスストレージ（NAS）、さらにはモバイル通信における低コストで高速なアドオンプロセッサとしての需要が存在すると期待して、様々な市場の有力ベンダーとの戦略的パートナーシップを結んでいます。

図19には、現時点におけるLionicの戦略的パートナーのリストの一部が示されています。



図19 Lionic戦略的パートナー



さらに将来の有望なアプリケーションとしてはXMLベースのソフトウェアがあります。AJAXに代表される開発用のプラットフォームをはじめとして、XMLによる新規システムの開発、あるいはSIPなどのHTML準拠のアプリケーションプロセスは文字列処理の塊と言っていいでしょう。このようなアプリケーションはセキュリティという枠を超えて一般的にはビジネス・ゲートウェイと呼ばれています。

ビジネスゲートウェイは、複数のプライマリ機能の実行向けに特別に設計された次世代のネットワークデバイスで、従来型の単独の機能やアプリケーションに最適化された多くのマルチサービス機器とは対照的なものと期待されています。半導体および高度通信機器およびサービスに関する市場調査、分析及び予測を専門に行っている In-Stat（米国）では、次世代の新しいマルチサービス、ビジネスゲートウェイについて調査分析を行い、その報告によれば、マルチサービスビジネスゲートウェイの機器市場は2007年に上昇し始めるとのことです。サービスプロバイダはユーザの求めに応じて、中小企業とブランチオフィス市場向けビジネスゲートウェイ機器などのバンドルサービスを進化させ、2007年までに提供を開始すると予想されています。

同社の予想では、今後12-24ヶ月の間に、このような新しいマルチサービス・デバイスの市場規模は急増し、2008年には166億米ドル市場に成長することが見込まれています。

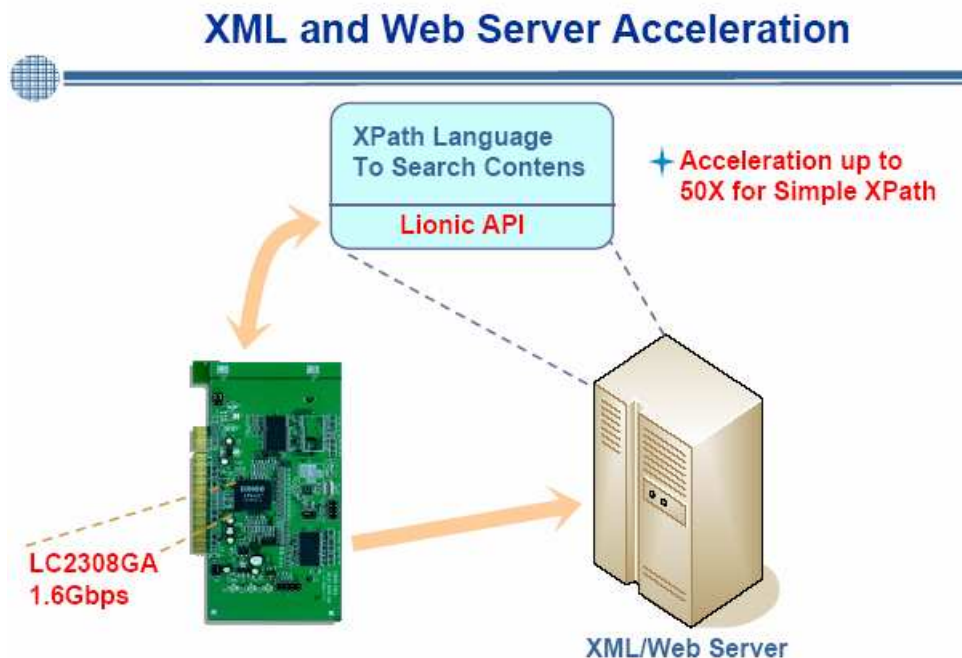


図20 LionicチップとAPI ライブラリによる汎用XML処理の高速化



参考文献

- 1. Keith Nissen, The Next-Generation Multi-Service Business Gateway, In-stat/MDR, September 2004**
- 2. Yu-Cheng Chang, The trend and application of prevented system, product management & development Division, D-link, January 2005**
- 3. Santosh Pawar, Understanding Network Security, Lucid Security**
- 4. Dr. Hsieh, Firewall and Intrusion Detection system, Distributed system & Network Security Lab., National Chiao Tung University, Hsinchu, Taiwan, R.O.C.**
- 5. Dr. Hsieh, Virtual Private Networks, Distributed system & Network Security Lab., National Chiao Tung University, Hsinchu, Taiwan, R.O.C.**
- 6. Percy, Symantec-the solution of enterprise information security, SecureUni Technologies Co., Ltd.**