数十ギガ～数テラ bps の超高速ネットワークに対応するセキュリティー装置

ー　有害サイト、ネットワーク侵入、コンピューターウイルスなどを即時に遮断　ー

平成 22 年 6 月 9 日
独立行政法人 産業技術総合研究所
株 式 会 社　KDDI 研 究 所

■ ポイント ■

- **60 ギガ bps の光通信機能を搭載した FPGA ボードによるセキュリティー装置**
- **FPGA ボードの追加で、数十ギガ～数テラ bps の超高速ネットワークでも処理可能**
- **有害サイトのリストを自動的に生成・配信するシステムにより即時性と高精度を実現**

■ 概　要 ■

独立行政法人 産業技術総合研究所【理事長 野間口 有】（以下「産総研」という）知能システム研究部門【研究部門長 比留川 博久】統合知能研究グループ【研究グループ長 神徳 徹雄】戸田 賢二 主任研究員、情報技術研究部門【研究部門長 関口 智嗣】センサーコミュニケーション研究グループ 高橋 栄一 研究グループ長らは、株式会社 KDDI 研究所【代表取締役所長 秋葉 重幸】と共同で、数十ギガ（10^9）～数テラ（10^{12}）ビット毎秒（bps）の超高速ネットワークに対応したセキュリティー装置を開発した（図 1）。

この装置は、専用に開発した 60 ギガ bps の光通信機能（10 ギガビットイーサネットポート×6）を備えた FPGA ボード（図 2）をベースとしており、有害サイトの遮断、ネットワーク侵入の遮断、コンピューターウイルスの遮断、パケットキャプチャーなどの機能を搭載できる。この FPGA ボードは PCI-Express カード型であるため、1 台の PC 内で複数枚使用でき、簡単に規模を拡張できる。よって数十ギガ bps～数テラ bps の通信速度でセキュリティー対策ができる。また、本装置の応用例として、パケットキャプチャーによって収集する通信情報と外部の信頼情報を組み合わせることにより、有害サイト遮断のためのフィルタリングリストを自動的に生成・配信するシステムを開発した。

＿＿＿＿は別紙【用語の説明】参照

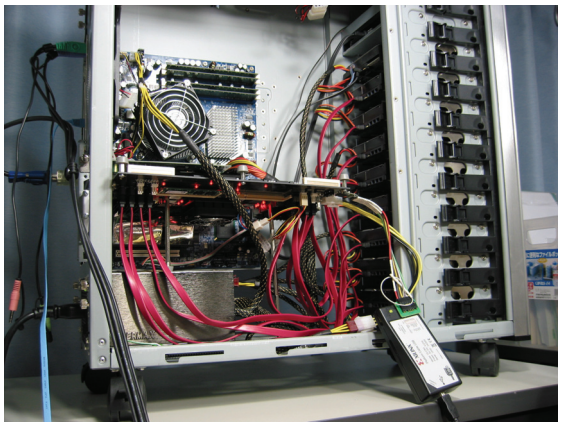

図 1 開発したネットワークセキュリティー装置

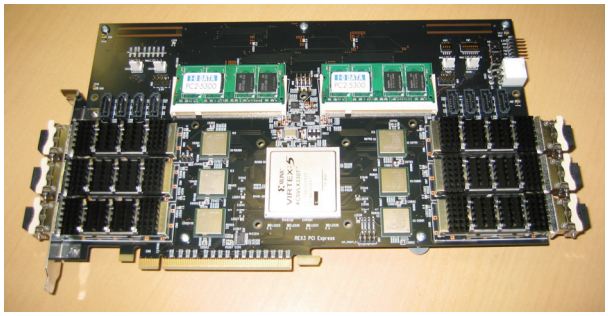

図 2 拡張可能 60 ギガ bps 光通信 FPGA ボード（15 cm × 27 cm）

■ 開発の社会的背景 ■

情報通信インフラは、現代社会の主要な柱となっているが、Web サイトの改ざん・情報漏洩、なりすましによって銀行口座やクレジットカード情報などを詐取するフィッシングサイト、DoS 攻撃などによるサービスの停止、コンピューターウイルスなど「悪意のある通信」による被害が大きな社会問題となってきている。今後は、高精細の画像・映像の配信、スマートフォンやタブレット型端末の普及など、通信が高速化かつ広帯域化し、また、エネルギーの制御に情報通信技術を用いることも期待されており、通信速度とともに安全性の確保が不可欠である。このような情報量の増大に伴い、ソフトウエアによるセキュリティー対策では、本来の PC としての機能の大部分をセキュリティー対策に占有されてしまうので、個人レベルでの対策には限界がある。この状況に対処するためには、情報通信サービスやデータセンターなどの超高速ネットワークで、「悪意のある通信」をエンドユーザーに渡る前に遮断する技術の開発が必要である。また、有害サイトは、短期間で発生と消滅を繰り返すため、これまでの人間による確認作業では追いつかず、即時性のあるフィルタリングリストの収集更新が課題となっている。

■ 研究の経緯 ■

産総研は、これまで大規模ネットワークの安全性を高めるため、ネットワーク侵入遮断装置やコンピューターウイルス遮断装置の開発を行ってきた。本研究開発は、総務省 戦略的情報通信研究開発推進制度「超高速ネットワークに対応した悪意のある通信の遮断技術の研究開発(072003008)」（平成 19 年度～平成 21 年度）により実施されたものである。

■ 研究の内容 ■

今回、開発を行ったネットワークセキュリティー装置のハードウエアは、専用に開発した拡張可能な 60 ギガ bps 光通信 FPGA ボード（図 2）および PC で構成される。今回開発した FPGA ボードは、有害サイトの遮断、ネットワーク侵入の遮断、コンピューターウイルスの遮断など高速ネットワークへの応用を行うことを主眼としたもので、10 ギガビットイーサネットポートを 6 ポート、フィルタリングリストなどの処理データを格納するための DRAM（Dynamic Random Access Memory）用ソケットを 2 個搭載している。さらにハードディスクなどへデータを蓄積するための SATA（Serial Advanced Technology Attachment）を 8 ポート備えている。PC との接続には PCI-Express を用い、内蔵カードとして使用する。図 1 は、PC の PCI-Express ソケットに本ボードを装着したネットワークセキュリティー装置の試験中の様子である。ネットワークセキュリティー装置には、有害サイト遮断、侵入遮断、コンピューターウイルス遮断、パケットキャプチャーの各回路を搭載でき、さらに自動フィルタリングリスト生成ソフトウエアをインストールできる（図 3）。

<table>
<tr><td></td><td></td><td colspan="2">自動フィルタリングリスト生成（ソフトウエア）</td></tr>
<tr><td>ネットワーク
侵入遮断
（回路）
30 ギガ bps
（予測値）</td><td>コンピューター
ウイルス遮断
（回路）
30 ギガ bps
（予測値）</td><td>有害サイト遮断
（回路）

60 ギガ bps
（実測値）</td><td>パケットキャプチャー
（回路）

～10 ギガ bps</td></tr>
<tr><td colspan="4">拡張可能 60 ギガ bps 光通信 FPGA ボード</td></tr>
</table>

図 3 ネットワークセキュリティー装置の概要

・有害サイト遮断

現在、コンピューターウイルスに感染させるサイトやフィッシングサイトなどの有害サイトが問題となっており、企業などの組織ネットワーク内における遮断が必須となっている。しかし、有害サイトは短期間で発生と消滅を繰り返すため、フィルタリングに用いるブラックリストの収集更新が課題であった。そこで、パケットキャプチャーした情報と外部の信頼情報を組み合わせて、候補となる URL を自動的に生成・配信するシステムを開発した。

フィルタリングリストとの高速マッチングを実現するエンジンについては、必要なメモリーのバンド幅を押さえることのできるハッシュとバイナリーサーチを組み合わせた方式を考案し、60 ギガ bps を超える性能を達成した。フィルタリングリストは、上記の自動生成・配信システムの実験によって得られた 34,000 個の URL を用いたが、リストを格納しているメモリーは 4 ギガバイトであり、ハッシュ値の重複時はバイナリーサーチを用いるため、大規模データにも十分に対応できる。

・ネットワーク侵入遮断

攻撃に関する情報が登録されたシグネチャとパケットとを比較して、シグネチャに適合する場合に検知もしくは遮断する。ネットワーク侵入検知システムのソフトウエアのひとつである Snort におけるシグネチャのサブセット 1200 個を採用し、非決定性有限オートマトンとその並列処理によって、1 ポートで 10 ギガ bps を実現した。3 ポートを並列に処理することにより 30 ギガ bps の速度を達成できる見込みである。

・コンピューターウイルス遮断

コンピューターウイルスのシグネチャとパケットを比較して、シグネチャに適合する場合に検知もしくは遮断する。アンチウイルスソフトのひとつである ClamAV のシグネチャが使用可能であり、パケットとシグネチャの適合判定回路の並列化によって、旧型のボードでは、6.4 ギガ bps の処理速度を実現した。今回開発したボードでは、シミュレーションにより、1 ポートにつき 10 ギガ bps の速度を確認した。3 つのポートを並列に処理することにより 30 ギガ bps の速度を達成できる見込みである。

・パケットキャプチャー

通信路を流れるパケットをハードディスクなどの記録媒体に書き込む機能である。ボード 1 枚当たり SATA でハードディスク 8 台に同時にアクセスできるため、十分な書き込み速度が期待できる。RAID や SSD など高速なディスクを用いれば 10 ギガ bps での記録が可能である。

・ボードの組み合わせにより機能と性能を自由に向上可能

今回開発したボードは、60 ギガ bps という広帯域の光通信機能を備えているため、ボード間の接続の自由度が高く、ボードを複数組み合わせることで、必要な機能と性能を提供できる高い拡張性を有している。有害サイトの遮断、ネットワーク侵入の遮断、コンピューターウイルスの遮断の 3 種類の機能が必要であれば、各機能を搭載したボードを 3 枚直列に接続すればよく、デスクトップ PC 1 台に内蔵することができる。有害サイト遮断専用であれば、ボード 1 枚の処理速度

は 60 ギガ bps であるため、17 枚を並列に使用することで、1 テラ bps の性能が得られる。PCI-Express が 6 枚装着可能なマザーボードを用いれば、3 台のデスクトップ PC で 1 テラ bps が処理可能となる。また、本ボードは SATA でハードディスク 8 台に同時にアクセスでき、PCI-Express や 10 ギガビットイーサネットで、複数組み合わせて利用することが可能である。

■ 今後の予定 ■

今回開発したネットワークセキュリティー装置は、コンパクトかつ省電力でありながら、テラ bps の超高速ネットワークに対応できることが実証された。本装置は設置も容易であるため、大規模ネットワークのセキュリティーを向上させ、安心安全な IT 社会の実現に大きな寄与が期待できる。今後は、実際の使用状況を模擬した試験を行い、製品化を目指す予定である。また、本装置は FPGA の回路の書き換えにより、ルーター、スイッチ、ネットワークカード、ネットワークストレージなどの幅広い応用が期待される。

■ 本件問い合わせ先 ■

独立行政法人 産業技術総合研究所
知能システム研究部門　統合知能研究グループ
主任研究員　戸田 賢二　〒305-8568 茨城県つくば市梅園 1-1-1　中央第 2
TEL：029-861-5875　FAX：029-861-5971
E-mail：k-toda@aist.go.jp

株式会社 KDDI 研究所
営業企画グループ
広報担当　前川 敦子　〒356-8502 埼玉県ふじみ野市大原 2-1-15
TEL：049-278-7545　FAX：049-278-7317
E-mail：inquiry@kddilabs.jp

【プレス発表／取材に関する窓口】
独立行政法人 産業技術総合研究所 広報部 広報業務室 小林 達哉
〒305-8568 茨城県つくば市梅園 1-1-1 中央第 2
つくば本部・情報技術共同研究棟 8Ｆ
TEL：029-862-6216　FAX：029-862-6212　E-mail：presec@m.aist.go.jp

【用語の説明】

◆ ビット毎秒（bps）

情報伝送能力の単位であり、1 秒間に伝送されるビット数を表す。10 ギガ bps は、CD-ROM を 1 秒間に約 2 枚転送することのできる速度で、1 テラ bps は、DVD を 1 秒間に約 26 枚転送することのできる速度。日米間の光通信回線容量は、現在 1.28 テラ bps である。

◆ イーサネット

イーサネットとは、コンピューターネットワークの通信規格のひとつで、OSI モデルにおけるデータリンク層にあたる。オフィスや家庭内からインターネットのコアに至るまで、幅広く使用されている技術規格である。

◆ FPGA（Field Programmable Gate Array）

FPGA とは、論理回路が書き換え可能な LSI（高密度集積回路）チップのことである。一般の LSI は製造後に機能を書き換えることができないが、FPGA は論理素子レベルでの再構成が可能で、機能を自由に変更できる。

◆ パケットキャプチャー

イーサネットでは、パケットと呼ばれる単位で情報が送受信されている。パケットキャプチャーとは、通信路を流れるパケットの全てもしくはヘッダの一部をハードディスクに記録することである。通常は、スイッチやルーターにおいて、通信を複製してパケットキャプチャー装置に入力することによって実施する。

◆ PCI-Express

パソコン用高速シリアルインタフェースの規格である。マザーボードとグラフィックカードなど拡張ボード間の接続に用いられる。

◆ フィルタリング・フィルタリングリスト

有害情報などを掲載している特定の Web サイトやアドレスへのアクセス要求を遮断し、アクセスできないようにすること。Web サイトの IP アドレス、ドメイン名、URL をフィルタリング対象のリストとしてあらかじめ登録する。

◆ DRAM（Dynamic Random Access Memory）

コンデンサーとトランジスタにより電荷を蓄える回路を記憶素子に用いたメモリー。回路が単純で、集積度も簡単に上げることができ、価格も安いため、コンピューターのメインメモリーはほとんどが DRAM である。

◆ SATA（Serial Advanced Technology Attachment）

パソコンとハードディスクなどの記憶装置を接続する高速シリアル通信規格「IDE(ATA)規格の拡張仕様」で、現在も最も多く使われている。

◆ ハッシュ

さまざまな種類や長さを持ついくつかのデータを整理するとき、ある計算によって固定の長さのデータ（ハッシュ値）に変換する方法。計算方法をハッシュ関数と呼び、ハッシュ値で参照するテーブルのことをハッシュテーブルと呼ぶ。

◆ バイナリーサーチ

探索空間を毎回 2 分割できるようにする探索方法であり、2 等分できる場合は最速の探索方法である。

◆ シグネチャ

侵入検知システムやアンチウイルスソフトウエアでは、攻撃の情報をシグネチャとして登録して、シグネチャに適合するファイルやパケットを攻撃と判断する方式が主流である。侵入検知システムでは、攻撃に固有のビット列やバイト列がシグネチャとして利用される。また、アンチウイルスソフトウエアでは、実行ファイルのハッシュ値がシグネチャとして利用される。

◆ Snort

ソフトウエアによる侵入検知システムのひとつ。オープンソースであるため広く用いられている。シグネチャが理解しやすいために、新たな攻撃手法が発見されると早急に新しいシグネチャを作ることができる特徴を持つ。

◆ 非決定性有限オートマトン

文字列のパターンマッチング処理で用いられているアルゴリズムのひとつ。ソフトウエアに比べて、ハードウエアによる実装が比較的容易であり、並列化による処理速度の向上ができる。

◆ ClamAV（Clam Antivirus）

Clam Antivirus は、オープンソースのアンチウイルスソフトのひとつ。シグネチャによるウイルス検知方式を採用している。

◆ RAID（Redundant Arrays of Inexpensive Disks）

複数のハードディスクを用いて仮想的に 1 台のハードディスクを構成する技術。耐故障性やアクセス速度の向上が行える。

◆ SSD（Solid State Disk）

フラッシュメモリーをディスクの記憶素子として用いたもので、可動部分がなく、アクセス速度が速く、衝撃にも強い。シリコンディスクとも呼ばれる。