サイバー攻撃から大規模ネットワークを防御するシステムの実現

--- 侵入検知ルールの変更に素早く対応でき、百ギガ bps にも拡張可能 ---

平成 19 年 2 月 20 日

独立行政法人 産業技術総合研究所
国立大学法人 筑波大学

■ ポイント ■

1. **1200 種類の侵入・攻撃の検知ルールを 10 ギガ bps で連続処理するネットワーク侵入防御装置を開発**
2. **試験用の侵入・攻撃パターンを送出し、システムの脆弱性を検査できる模擬攻撃装置を開発**
3. **自動的な防御と漏れのない検知により、大規模ネットワークシステムの安全性が大幅に向上**

■ 概　要 ■

独立行政法人 産業技術総合研究所【理事長 吉川 弘之】（以下「産総研」という）情報技術研究部門【部門長 坂上 勝彦】実時間組込システム研究班の戸田 賢二 班長と片下 敏宏 特別研究員および国立大学法人　筑波大学【学長 岩崎 洋一】システム情報工学研究科【研究科長 熊谷 良雄】コンピュータサイエンス専攻の山口 喜教 教授と前田 敦司 助教授は、共同で 10 ギガ bps イーサのネットワーク侵入防御装置の試作に成功した。これは、筑波大学での研究をもとに、産総研でハードウェア試作を行ったもので、1200 種類の検知ルールを 10 ギガ bps で遅滞なく連続処理し、自動的な防御と漏れのない検知によって大規模ネットワークの安全性を高める装置である（図１）。

併せて、産総研は、東京都立産業技術研究センター、デュアキシズ株式会社、株式会社ビッツらと協力して 10 ギガ bps イーサのネットワーク模擬攻撃装置を開発した（注）。これは、擬似的な侵入・攻撃を含んだ通信データを連続して 10 ギガ bps で生成・送出し、セキュリティシステムで侵入や攻撃が正しく除去されているか検査したり、処理性能の測定を行うための装置である（図２）。

侵入防御装置および模擬攻撃装置とも、FPGA（回路が書き換え可能な LSI）と呼ばれるデバイスを用いる新方式を開発したことにより、世界最高水準の性能と新しい検知ルールへの適応性を両立し、次世代の超高速ネットワーク（百ギガ bps）にも対応することが可能になった。

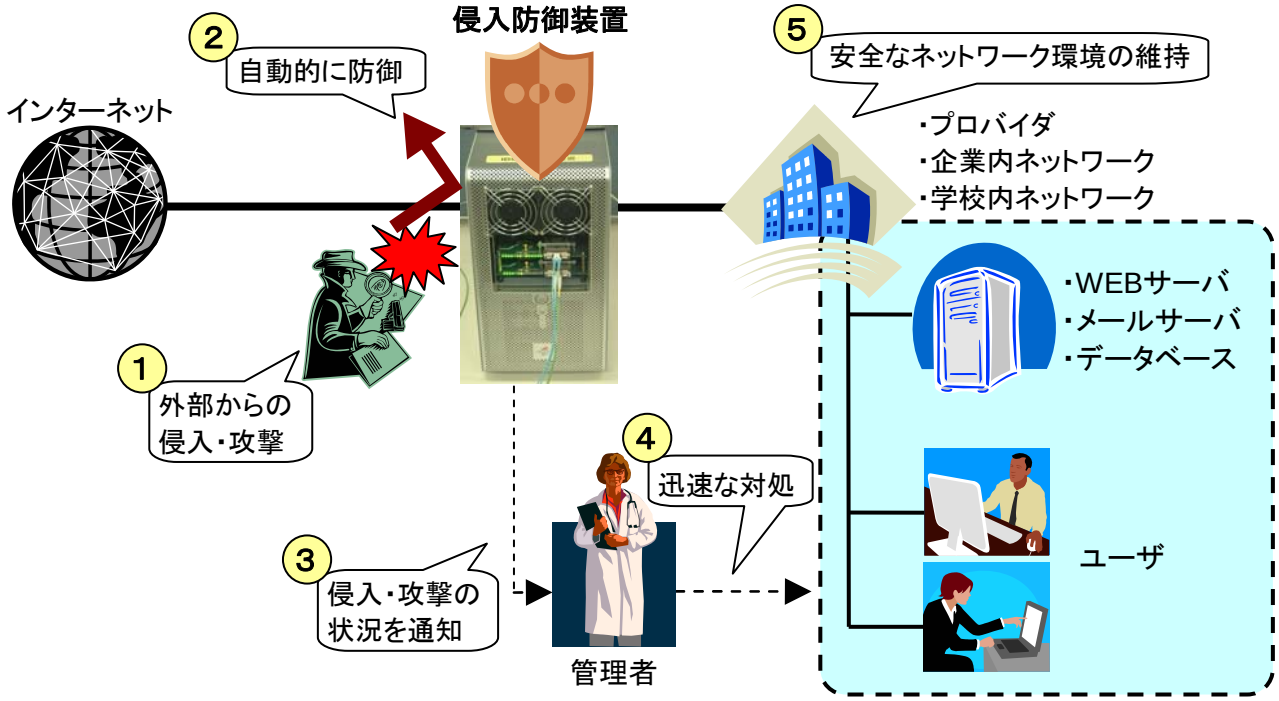

図１：ネットワーク侵入防御装置の概要

（注）模擬攻撃装置は、経済産業省の地域新生コンソーシアム研究開発事業による研究「パターンマッチング回路の超高速化とフィルタリング装置への応用」(H16～H17 年度) の研究成果を発展させたものである。

＿＿＿＿＿は別紙【用語の説明】参照

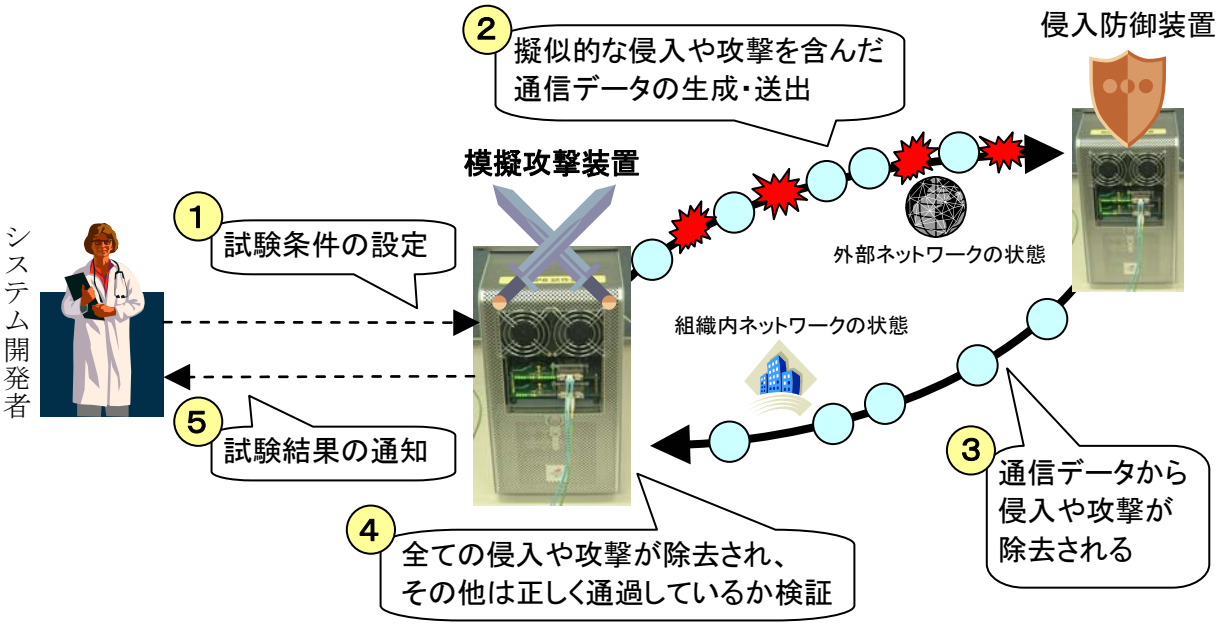

図２：ネットワーク模擬攻撃装置の概要

■ 研究の背景・経緯 ■

ネットワークプロバイダや企業・学校など組織ネットワークへのサイバー攻撃は、サービス不能やホームページの改ざん、情報漏洩など甚大な被害をもたらし、電子化社会の大きな脅威である。実際に、DDoS 攻撃（分散型使用不能攻撃）によって Yahoo!、e-Bay、Amazon.com などの米国大手の Web サイトが長時間アクセス不能の事態に陥ったことがある。また、スーパーボウルのスタジアム公式サイトのハッキングがなされ、アクセスした利用者にトロイの木馬をダウンロードさせる悪質な改ざんがなされたことも記憶に新しい。

このように組織ネットワークはサイバー攻撃にさらされているが、その被害を極力抑えることが組織の信用を高めるだけでなく、利用者を被害から守る観点からも重要である。被害を最小限にするためには、まず、サイバー攻撃を検知し迅速に対処することが必須である。

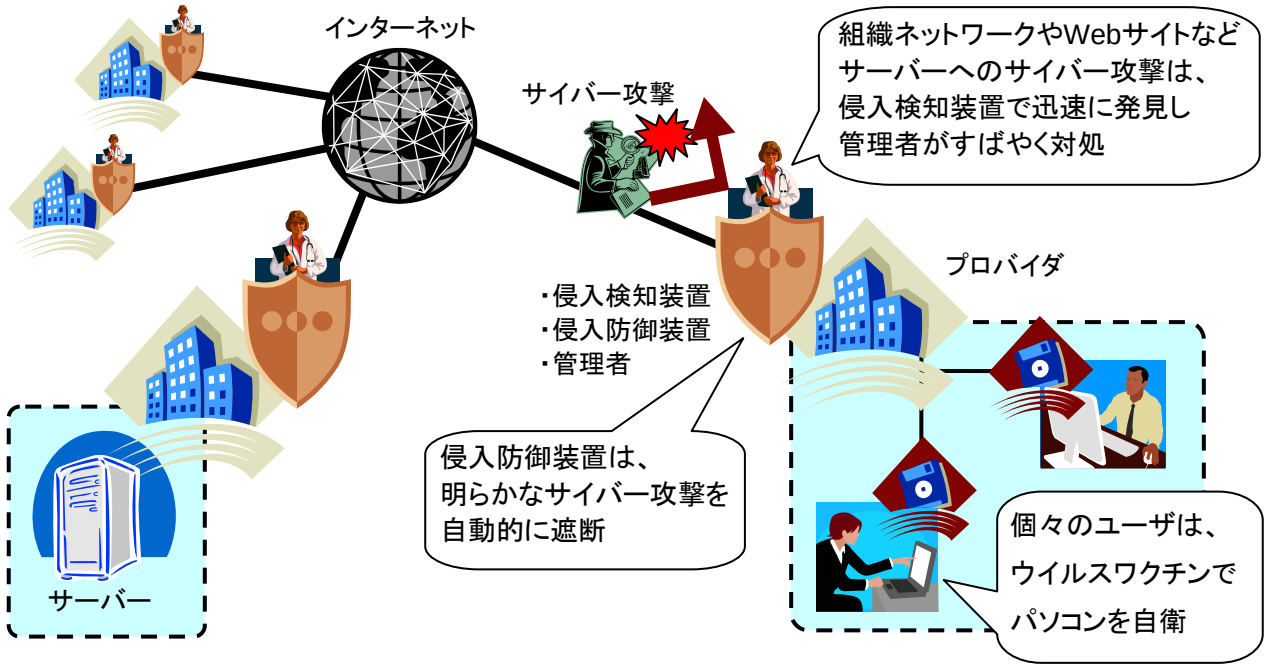

図３：サイバー攻撃に対する対処の概要

サイバー攻撃を検知するシステムとして、ネットワーク上の通信データを検査する IDS（Intrusion Detection System、侵入攻撃検知システム）が利用されている。また IDS の派生システムとして、明らかな攻撃は自動的に遮断する IPS（Intrusion Protection System、侵入防御システム）が開発されている。近年では、既知の侵入や攻撃をデータベース化し同様の攻撃を検知する方式（以下、シグネチャ方式と呼ぶ）の Snort と呼ばれるシステムが広く知られている。しかし、Snort はソフトウェアによる処理のためスループットが低く、組織の基幹ネットワークに利用される 10 ギガ bps イーサネットの通信データを漏れなく検査する事は困難であった。専用ハードウェアによる高速化されたシステムも開発されているが検査可能な侵入・攻撃の数が少ないのが現状である（注）。侵入や攻撃を見逃さず検知し被害を最小限にするためには、高速ネットワークでも通信データを漏れなく検査し、かつ、多くの侵入や攻撃を検知できるシステムが必要である。

（注）米国 Force10 社の IDS システム P10 は、Snort の検知ルール 650 種類を 10 ギガ bps で処理する。

■ 研究の内容 ■

[ネットワーク侵入防御装置]

１．検知ハードウェアの方式の開発

シグネチャ方式の IDS では、既知の侵入・攻撃のデータベース（以下、検知ルールと呼ぶ）中の文字列と通信データを１つ１つ照合するパターンマッチングと呼ばれる処理によって検査を行う。例えば、文字列「Attack」が通信データに含まれていれば攻撃と検知する。本研究による検知ハードウェアの方式は、主に以下の３つの工夫がなされている。

（１）高速化に適した NFA を採用

検知ハードウェアは様々な方式が研究されているが、処理速度の向上に有望な NFA（Nondeterministic Finite Automaton、非決定性有限オートマトン）の方式を採用した。NFA 方式は回路の並列化により容易に処理速度を向上でき、10 ギガ bps イーサネットの通信データを漏れなく検査するハードウェアも達成可能となる。しかし、従来研究されている NFA 方式では並列度に比例してハードウェアの規模が非常に大きくなり、少数のルールしか処理できないという欠点があった。そこで次のハードウェア規模の削減方式を開発した。

（２）ハードウェア規模の大幅な削減に成功

検知ルール中の文字列には、アルファベットなどある特定の文字が頻繁に含まれている。従って、頻出する文字を共有化することにより検知ルールを縮小する余地が大いにある。また、文字列の平均長が短く、文字の共有化による効果が大きいと期待される。

このような検知ルールの性質を利用し、検知ルールに含まれる冗長な要素を抽出・共有してからハードウェア化する新方式を開発した。この方式により処理速度を低下させることなくハードウェアの規模を従来方式の半分以下へ削減することに成功した。ハードウェア規模を削減した分多くの検知ルールに対応可能となり、検知可能な侵入・攻撃の数が大幅に向上した。

（３）検知ルールの更新に容易に対応

検知ハードウェアを再構成可能なデバイス FPGA へ実装することにより検知ルールの更新を可能とした。さらに侵入・攻撃の検知ルールから自動的に検知ハードウェアを生成するソフトウェアを開発し、検知ルールの変更を容易にした。

２．侵入防御装置の試作

今回開発した検知ハードウェアの方式を用い、1200 種類の侵入・攻撃に対応し 10 ギガ bps イーサネットの通信データを漏れなく検査する侵入防御装置を試作した。本装置は 10 ギガ bps イーサネットの光インタフェースを２基備えており、基幹ネットワークに設置することができる。検出された侵入・攻撃やネットワーク速度の情報をリアルタイムに通知する（図４）ほか、明らかな侵入や攻撃である通信データは除去することも可能である。試作システムでは全ての侵入・攻撃を除去する設定としている。

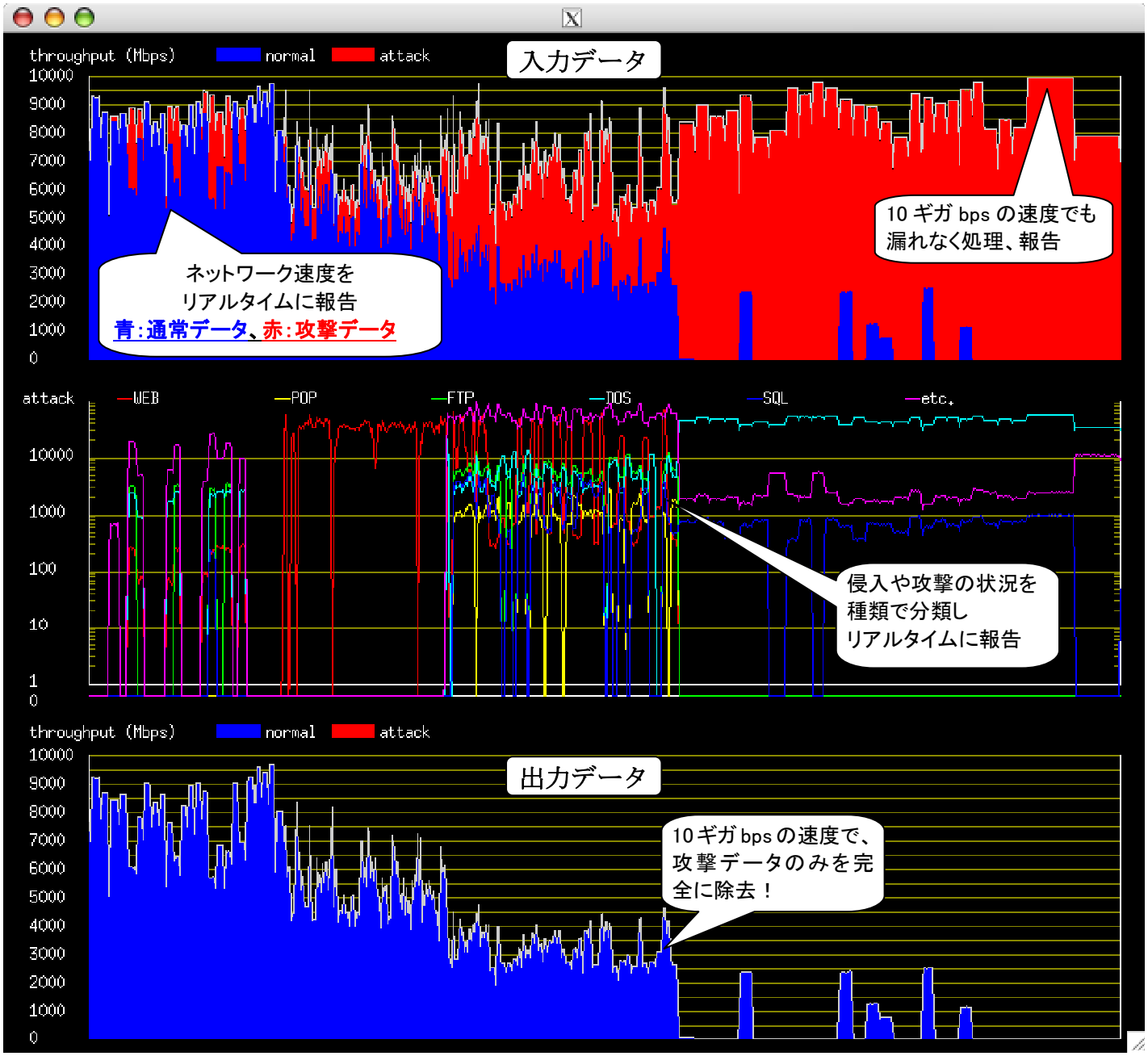

図４：侵入防御装置で検出されたサイバー攻撃の通知画面

［ネットワーク模擬攻撃装置］

１．模擬攻撃装置の開発

今回開発したネットワーク侵入防御装置は 10 ギガ bps という非常に高い処理性能を持つため、これを同等の速度で試験する装置が無く詳細な性能評価が困難であった。そこで、10 ギガ bps イーサネットの回線速度で攻撃用の通信データを生成・送出するネットワーク模擬攻撃装置の開発を行った。本装置は通信データ送出と同時に試験対象となる装置からの出力を監視して、通信データの中から攻撃データだけが検出・除去されており通常の通信データは通過していることを検証する機能を持つ。

10 ギガ bps の速度を実現するため、ハードウェアでネットワーク物理層チップを直接制御する機能を持たせ、さらに、独自に開発したハッシュテーブル方式による通信データの検証機能を搭載した。

開発したハッシュテーブル方式は３つの特徴：（１）通信データの検証処理が高速、（２）小さいハードウェア量で実装できる、（３）通信データの中で攻撃のみが正しく除去されているか検証できる、という特徴を持つ。

この方式では、ハッシュテーブルを用いることでハードウェア量の削減と通信データ記録の高速化を達成している。通信データの出現回数は種類別に分類され、送出と入力それぞれにテーブル上へ記録されており、この２つのテーブルを照らし合わせて通信データの中で攻撃だけが除去されているか検証する。異なる種類の通信データ間で起こるハッシュ値の重なりは、通信データを加工することにより回避している。

２．侵入防御装置を擬似攻撃した試験

試作した侵入防御装置の機能を試験するため、攻撃が含まれた通信データを生成し、模擬攻撃装置を用いて 10 ギガ bps イーサネットの回線速度で試作システムに入力する実験を行った。その結果の一部を図５に示す。

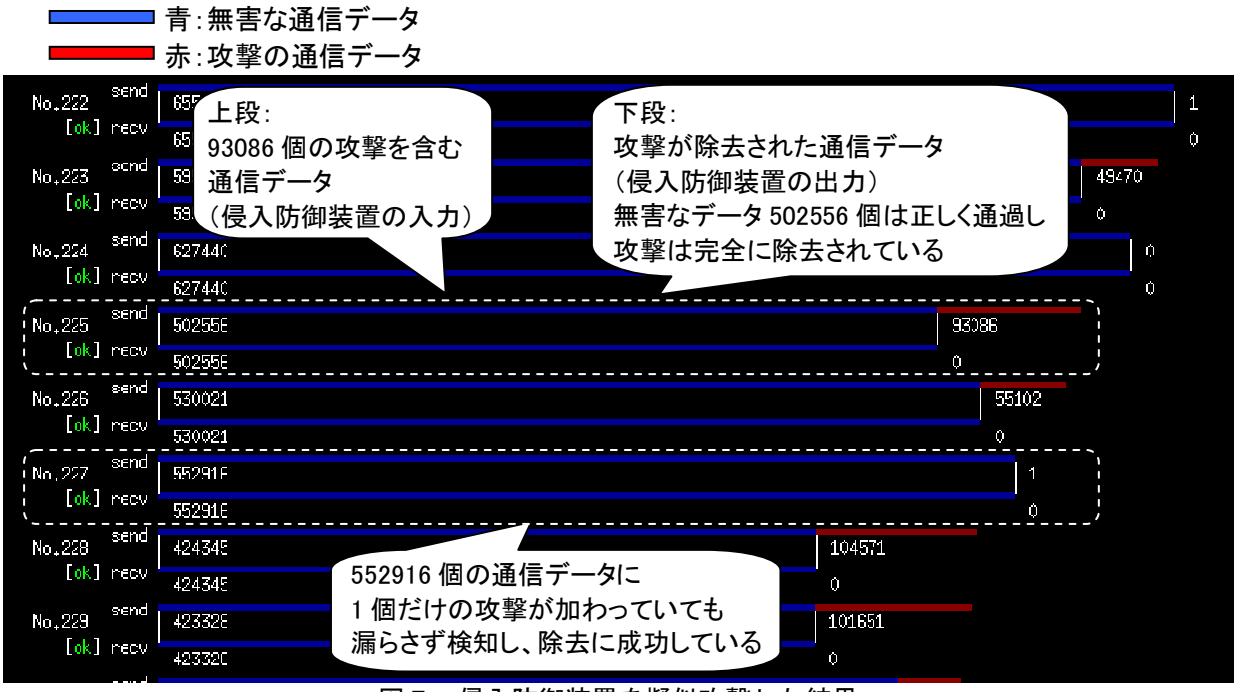

図５：侵入防御装置を擬似攻撃した結果

この実験により、試作装置は全ての攻撃を正しく遮断し、無害な通信データのみ通過させることが 10 ギガ bps の速度において可能であることが分かり、我々の開発方式による検知ハードウェアの処理速度と機能を実証した。

■ 今後の予定 ■

侵入防御装置及び模擬攻撃装置とも、大変コンパクトで省電力でありながら、超高速ネットワークに対応できることが実証された。すなわち、従来は両装置とも複数のＰＣからなるクラスタによっても実現し難かった攻撃および防御の性能が、それぞれ一台のＰＣ大の装置によって実現出来た。設置も容易であるため、両装置は、大規模ネットワークのセキュリティを向上させ、安心安全な IT 社会の実現に大きな寄与が期待できるものであり、市場の要求も強い。ユーザインタフェースの整備などを進め製品化を急ぐ予定である。

（問い合わせ先）

独立行政法人 産業技術総合研究所
情報技術研究部門 実時間組込システム研究班
班長　　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：029-861-5909
E-mail：k-todaｱｯﾄﾏｰｸaist.go.jp
国立大学法人 筑波大学
システム情報工学研究科　　〒305-8577 茨城県つくば市天王台 1-1-1
教授　　山口 喜教　　Tel:029-853-2425
E-mail: yamagutiｱｯﾄﾏｰｸcs.tsukuba.ac.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 村松 賢一 〒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ｱｯﾄﾏｰｸm.aist.go.jp

国立大学法人 筑波大学 総務・企画部
広報課 和田 雅裕 〒305-8577 茨城県つくば市天王台 1-1-1
TEL：029-853-2040 FAX：029-853-2014
E-mail：sk.prｱｯﾄﾏｰｸsec.tsukuba.ac.jp

【用語の説明】

◆サイバー攻撃
インターネット経由で他のコンピュータに不正アクセスを行い、相手の組織や国にダメージを与えようとする行動のこと。

◆bps (bits per second)
１秒間の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 のおよそ２枚分にあたる 10 ギガ bit の情報を１秒間に転送する速度。

◆FPGA (Field Programmable Gate Array)
論理回路が書き換え可能な LSI チップ。一般には LSI は製造後に機能を書き換えることができないが、FPGA は機能を自由に変更可能である。

◆DDoS (Distributed Denial of Service、分散型使用不能) 攻撃
多数のコンピュータから一斉にサーバへ不正アクセスすることにより、サーバの能力をあふれさせて機能を停止させる攻撃。2000 年 2 月に、Yahoo!、Amazon.com、Buy.com、eBay、CNN、E*TRADE、ZDNet などアメリカの大手 Web サイトが次々と DDoS の攻撃を受け、注目を集めた。現在も、主要なサイバー攻撃の１つである。

◆IDS (Intrusion Detection System、侵入検知システム)
ネットワークでの侵入や攻撃を検知するシステム。

◆Snort
ソフトウェア IDS。無料であり導入も容易であることから広く用いられている。検知ルール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検知ルールを作ることができる特徴を持つ。日本にも Snort ユーザ会があり、情報交換や普及活動を行っている。
（本発表の侵入防御装置は、Snort のルールセットをハードウェア化したもの）
Snort オフィシャルサイト：http://www.snort.org/
日本 Snort ユーザ会：http://www.snort.gr.jp/

◆NFA (Nondeterministic Finite Automaton、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、機械の一つ。ソフトウェアでは NFA を処理することが難しい。一方、ハードウェアでは簡単な回路で実装されるため並列化による処理速度の向上が簡単にできる。(しかし回路規模が非常に大きくなるので、本侵入防御装置では独自の工夫を行っている。)

◆ハッシュ
様々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ぶ。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。(異なるデータから計算されたハッシュ値が同じになるとデータの見分けができなくなるため、本模擬攻撃装置では独自の工夫を行っている。)