分散処理型侵入検知システムの検討

倉橋 孝雄　曽場 昭之　松浦 宣彦　茨木 久†
日本電信電話株式会社 ＮＴＴサイバーソリューション研究所‡

１．はじめに

近年のブロードバンド NW(Network)や常時接続 NW の普及によって，パソコン環境だけでなく，インターネットを用いる家電製品や NW アプライアンス製品が増加すると予想されている．

一方，不正侵入の報告数は増加傾向にあり，NW 利用犯罪者による様々な犯罪によって，企業や国家機関が多くの被害を受けている．更に，対象のターゲットは国家機関や企業だけでなく，上記家庭環境へ攻撃の対象や攻撃手法も多角化しつつある．そのため，家庭と外部を結ぶ入口に Firewall 機能付きのブロードバンドルータを設置し，外部からのアクセスをコントロールするユーザが増えている．

また，多様化する不正アクセスに対するセキュリティシステムとして注目されている IDS 装置は，Firewall 機能と平行して利用することでセキュリティ強化に貢献する重要な機能として，普及に向けた研究開発，例えば，IDS に対する帯域を調整するロードバランス機能の研究や，IDS 処理量を減らすアルゴリズムの検討[1]などが行われている．しかし，攻撃の種類は増加の一途を辿り，効率よいアルゴリズムだけでは対処が難しいという課題も存在している．

本稿では，上記 IDS 装置を家庭向けに適用することを狙い，まず IDS 装置に必要な処理量を定量的に測定し，装置構成上の課題を明確にする．その上で今後ますます増加する攻撃を想定した解決手段を提案し，その基本システム構成について述べる．

２．IDS 家庭内配置の必要性

前述のように常時接続 NW の普及に伴い，ホーム NW に接続された複数の家庭内端末も脅威にさらされることになる．ホーム NW 環境のセキュリティ対策ポイントとしては，NW の基幹網での対策と家庭の出入り口での対策が考えられる．しかし，前者は多様化するサービスに対して個別に対処することが難しく，処理量もより膨大となる．処理量については，NW の基幹網内で処理装置を共有する方法も考えられるが，e メールや Web 閲覧の内容までフィルタリングする機能に関しては，できるだけ家庭の出入り口に配置することが望ましい．しかし，現在普及しているブロードバンドルータの Firewall 機能だけでは，ワームや DoS 攻撃のような偽装されたパケットによる不正アクセスに対しては無力であるため，本検討では IDS をブロードバンドルータ機能として実装することを考える．

３．IDS 評価実験

Firewall は固定長データ(パケットヘッダ情報)をマッチングするため，実装は容易なものとなっている．しかし IDS は可変長データ(ペイロード部も含む)をマッチングするため，実装するにはプログラム負荷が大きい．そこで本検討では，IDS 機能に必要なリソースの調査を行った．

“Study of a distributed processing type intrusion detection system”

†Takao KURAHASHI, Teruyuki SOBA, Norihiko MATSUURA, Hisashi IBARAKI

‡NTT Cyber Solutions Laboratories, NTT Corporation

３．１．IDS 実装の課題と実験項目

IDS は，NW 上のパケットを監視し，侵入・攻撃となるパケットを発見すると Alert を上げる機能を持つシステムであり，一般的なシグネチャベース型の IDS は，シグネチャルール(シグネチャ)と呼ばれる攻撃パターンとパケットとを照らし合わせることで侵入・攻撃となるパケットを識別している．一般的な IDS 処理は，ソフトウェア実行時に大きなメモリ量，CPU 処理能力が必要なため，ブロードバンドルータなどの限られたリソース(50～200MIPS(Million Instruction Per Second)前後)上では起動はしても侵入検知動作までは出来ないことが考えられる． 本検討では，シグネチャベース型 IDS(以下，単純に IDS と呼ぶ)の中でポピュラーであり，プログラムのソースが公開されている「Snort2.0.5」を用いてプロファイリングを行い，IDS におけるリソース指標を求めることとした．プロファイリングとは，ソフトウェアの実行時間を分析することであり，プログラム実行のためのリソース指標がわかる．

本プロファイリングでは，Snort を攻撃が行われる NW 環境下に設置し，実行時間およびメモリ使用量の計測を行った．もともと IDS は，スループットによって処理しなければならないパケット量が変わり，IDS 処理に必要な CPU 能力が変わる．また，シグネチャ数によっても必要な CPU 能力が変わるため，容易に必要な CPU 能力を把握することは難しい．そのため本検討では，流れてきたパケットを取りこぼしなく検知できることを前提とし，スループットとシグネチャ数をパラメータとして IDS 処理に必要な CPU 処理能力を求めることとした．

３．２．実験環境

実験環境を Fig.1 に示す．IDS は攻撃用 PC と攻撃対象となっているサーバ PC が接続される NW 上を流れるパケットをスニフィングする形で設置されており，IDS 実装 PC は，以下のスペックのものを用いた．

- ✣OS : RedHat Linux 7.3　Kernel : 2.4.18-3
- ✣CPU：Pentium4 2.5GHz FSB:400MH z
- ✣メモリ：PC2100 DDR SDRAM 512MB CL2.5　32*8bit

また，攻撃用 PC から攻撃用パケットを送出するために「snot 0.92」を用いた．Snot は，Snort のルールファイルから攻撃パケットを生成するパケットジェネレータである．生成した攻撃パケット は全て Snort にて検知できることを確認している．

実験は，Snort の基本処理量を計るため Pre-processor の ON/OFF も含め，加えてシグネチャの数を変化させた評価を行った．また，結果は CPU 温度やパケット間隔によって誤差が生じるだけでなく，シグネチャの内容による誤差も発生するため，試行を 100 回ずつ行ない，その平均と平均偏差を結果とすることにした．

また，以下の式に基づいて結果を出すこととした．

★　プログラムステップ数＝実行時間×CPU 能力

★　パケット当りの処理量＝
プログラムステップ数／送出パケット数

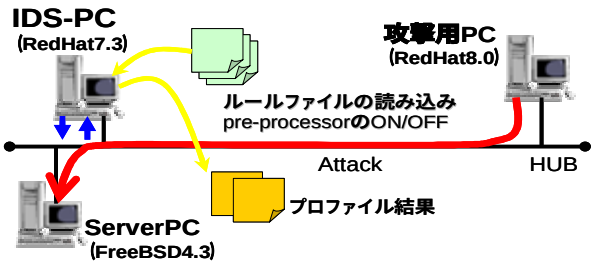

Fig.1　実験環境

Table.1　L1/L2 キャッシュの影響

	キャッシュ有効	キャッシュ無効
CPU-MIPS値	2150.99	10.462
MI/Packet	159.3×10^{-3}	85.4×10^{-3}

3．3．実験内容

Snort を実装した PC で用いられる CPU のスペックは，本検討におけるプロファイリング結果に大きな影響を与えると予測される．そのため，IDS 実装用 PC 内蔵 CPU の L1/L2 キャッシュの影響について予備実験を行った．予備実験は，Snort の Pre-processor と全シグネチャを有効にした状態で L1/L2 キャッシュを ON/OFF することで結果を得た．Table.1 にその結果を示す．CPU 能力を示す CPU-MIPS 値は， Dhrystone v2.1 にてベンチマークを行った結果を用いて VAX MIPS 値へと変換したものを用いた．結果としてキャッシュ OFF における MI/packet（1 パケット当りの CPU 負荷）は「0.085」であり，キャッシュ ON における MI/packet は「0.159」の結果を得られた．この結果においてキャッシュ ON 時には，Dhrystone v2.1 のプログラムが完全にキャッシュ内に入ってしまうため，キャッシュ OFF 時とくらべ 2 倍の値になっているが，参考文献 2)より上記の結果は誤差許容範囲内であると考えられる．よって以降の評価では，Dhrystone を用いた CPU 能力値を用いて得られたパケット当りの処理量は妥当なものとして評価を行った．

3．4．実験結果

実験結果を IDS 処理能力としてまとめた．Fig.2 に平均と平均偏差をグラフ化したものの一部(キャッシュ OFF)を示す．また，使用メモリ量は最大で 54MB と大きい結果となった．しかし，現在の市販ブロードバンドルータのメモリを考えると許容範囲と考えられる．Pentium3 の CPU を用いた PC 上で Snort を実行させトラヒック量に対する検知率が報告されている [3)4)]．この報告にある CPU-MIPS 値は 1204MIPS であり，トラヒック量は 50Mbps である．この結果を Fig.2 に当てはめると 55Mbps

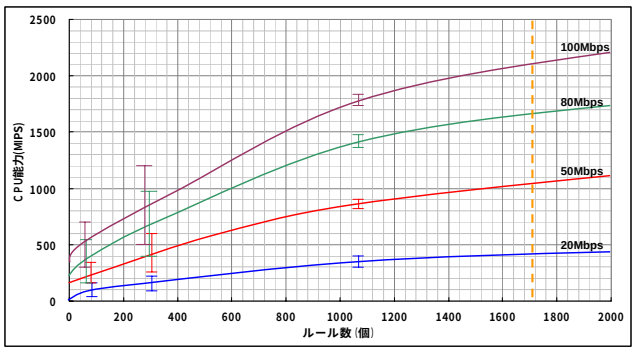

Fig.2　Snort の評価結果

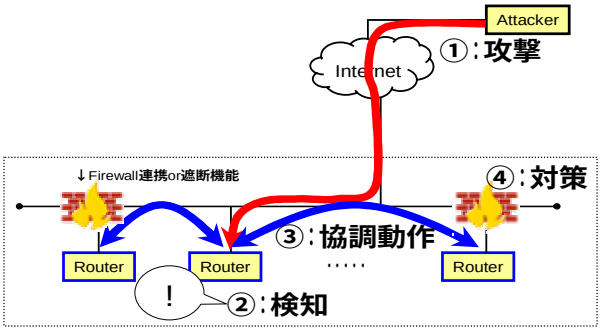

Fig.3　分散型侵入検知システム

と実験環境の平均偏差範囲内であり，Fig.2 の結果は信頼できるものと考えられる．

4．実験の考察と提案

実験結果によって，100Mbps 環境での検知率 100%を実現するには，ブロードバンドルータへ数 GH z 単位の CPU 実装が必要となることがわかった．また，先に述べた IDS 処理量を減らすアルゴリズムでは，今後増加する攻撃に対して対応が厳しいことが評価結果からも推測され，コスト的な観点からも IDS の効率的な実現方式が望まれる．そこで本検討では分散協調処理による侵入検知システムを提案する．

本検討で提案するシステムのコンセプトは，

- 複数の IDS にシグネチャを分散する．(分散 IDS と呼ぶ)
- 分散 IDS は相互に通信を行う機能を持つ．
- 各分散 IDS が検知した情報を共有する．
- 分散IDSの集合(クラスタ)全体で攻撃に対して検知を行う．

である．Fig5 は上記分散型侵入検知システムを示したもので，「ある攻撃に対して，その攻撃に対するシグネチャを持っている分散 IDS が攻撃を受けた場合，その分散 IDS は検知を行い，検知情報を同一クラスタ内の分散 IDS へ通知する．そして，通知を受けた他の分散 IDS は Firewall と連携を組み「ポートを閉じる」などの対処を行う．」という機能を有する．

また，上記機能によって，流行の攻撃に対処することで被害の拡大を防ぐこと可能となる．

5．まとめ

本検討では，家庭向け IDS 提供に向けて，現状の IDS 全てを実装することが困難であることを明らかにし，実装するための手法として分散処理の概念を提案した．上記概念を基に今後の検討としてシグネチャを減らすことによる被害リスクを評価パラメータとし，

・シグニチャ分散アルゴリズム
・分散装置間通信・同期プロトコル

などの方式検討を実施するとともに，分散 IDS の横方向のみの通信だけでなく，網側ルータも含めた縦方向の分散・協調動作などもついても検討を進める予定である．

6．参考文献

1)Tsunemasa Hayashi ,Motoki Yokoyama. Evaluation of IPS with Snort usion a high-speed hardware/software detection architecture IPSJ SIG Technical Report.2003

2) PERFORMANCE FLAW
http://www.intelligentfirm.com/membench/index.shtml

3) SOURCE fire Snort2.0-Detencion Revisited

4)Snort 処理能力検証 http://jem.serveftp.com/security/