社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (29)
2008－CSEC－ 40 (29)
2008／3／7

通信の双方向性を利用した DDoS 攻撃遮断システムの提案

鎌田 暢広† 寺田 真敏†† 土居 範久†

† 中央大学大学院 理工学研究科 情報工学専攻 〒112-8551 東京都文京区春日 1-13-27
†† 中央大学研究開発機構
〒112-8551 東京都文京区春日 1-13-27 中央大学後楽園キャンパス 3 号館 12 階

あらまし 今日，ボットネットの流行により，コンピュータ利用者の意図にかかわらず DDoS（Distributed Denial of Service）攻撃の実行に加担してしまう危険性が高まっている．それに対し，現在実施されている DDoS 攻撃対策は，専用ファイアウォールの設置などサーバ側でおこなうのもがほとんどであり，意図しない攻撃参加やインターネット上を不要なパケットが流れるなどの問題を解決することはできない．そこで，本稿では正常な通信における特徴である双方向性に着目し，クライアント側に存在するルータにて通信を監視し，DDoS 攻撃を発信元で検知，遮断する手法を提案する．そして，プロトタイプシステムを用い，様々なデータを適用した結果から提案手法の動作効率を検討する．

A Proposal of DDoS Attack Blocking System using Interactive of Communication

Nobuhiro kamata† Masato Terada†† Norihisa Doi†

† Graduate School of Science Engineering, Chuo University.
1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551, Japan
†† Research and Development Initiative Chuo University.
12th Floor, Chuo University Korakuen Campus,
1-13-27 Kasuga, Bunkyo-ku Tokyo 112-8551, Japan

Abstract The risk of participating in DDoS (Distributed Denial of Service) attacks involuntary is rising under the influence of the spread of BOTNET over these years. But, current measures for DDoS attacks can't avoid unintentional participation of DDoS attacks and outflow of redundant packets into the Internet. Because, current measures such as an exclusive firewall almost put into practice at the victim server. In this paper, we propose a method which blocks DDoS attacks at the source of the attacks by monitoring interactive of communication at the router close to client computers. And we show efficiency of the proposed method by the result for various data using the prototype system.

1. はじめに

今日，インターネットの普及に伴い，多くの企業がサイトを開設し，情報の公開や様々なサービスの提供をおこなっている．一方では，そうしたサービスの妨害を目的とした攻撃が増加しており，中でも DDoS（Distributed Denial of Service）攻撃が問題となっている．DDoS 攻撃は標的に対して大量のパケットを送信し，システムの処理能力を超えさせる．また，攻撃者は攻撃実行用プログラムを複数のコンピュータに仕掛け踏み台として利用し，そこから攻撃パケットを一斉に送信する．したがって，踏み台として利用されるコンピュータは，所有者の意図に関わらず攻撃に参加してしまうことになる．特に，ボットネットと呼ばれるネットワークを利用した DDoS 攻撃が増加しているため，そのような危険性が高まっている．

DDoS 攻撃に対して現状でおこなわれている対策としては，サーバ及びネットワーク機器の性能強化や DDoS 攻撃専用ファイアウォールの導入などがあげられる．しかし，これらの対策ではインターネット上に流れる不正なトラフィックを軽減することはできない．また，踏み台として利用されたコンピュータの所有者が意図していない攻撃への参加も防ぐことはできない．したがって，利用者の意図や知識に関わらず DDoS 攻撃を発信元で止めるシステムが必要とされる．

そこで，本研究では，クライアント側のネットワー

クとインターネットの境界となるルータ上にシステムを構築し，インターネット上に DDoS 攻撃のパケットが発信されることを検知，遮断する手法を提案する．攻撃の検知は，ルータを通過する通信の状態を解析し，パケットが双方向に交換されていないなどの DDoS 攻撃発生時にみられる特徴を利用することでおこなう．攻撃の遮断は，検知時の情報をもとに IP アドレスによるフィルタリングをおこなう．また，提案システムでは，通信の状態を単位時間ごとに区切り解析することで，監視にかかる負荷や資源を軽減する．そして，単位時間に区切ることで発生する誤検出を，直前の正常な通信と比較することにより回避する．

本稿では，プロトタイプシステムを用い，様々な通信データを適用した結果から，提案手法の動作効率を検討する．

2. DDoS 攻撃に関する動向

2.1 DDoS 攻撃の発生状況

DDoS 攻撃は複数個所から一斉に DoS（Denial of Service）攻撃を実行する攻撃である．DoS 攻撃には複数の攻撃手法が存在し，DDoS 攻撃に主に用いられる手法のひとつに SYN flood がある．SYN flood は，TCP の 3 ウェイハンドシェイクにおける SYN パケットのみを標的に対して大量に送りつける攻撃である．通常の通信に使用されるパケットを用いているため，攻撃パケットの判別が非常に困難である．

警察庁の調査[1]によると，ファイアウォールに送信された SYN/ACK パケットを分析した結果から得られた SYN flood の検知件数は，平成 19 年度上半期では，前期と比較して 67%減少しているが，約 25,900 件もの攻撃が検知されている．また，ボットネットにおいて指令サーバから出される命令は，全体では前期と比較し約 55%減少し 6,441 件となっているが，SYN flood に関しては 4,836 件と前期より約 102%増加している．

3. DDoS 攻撃遮断システムの提案

3.1 既存の手法を利用する際の課題

DDoS 攻撃のパケットはパケット自体に異常な点が存在しないため，正規アクセスのパケットとの差異を判別することが困難である．それに対し，DDoS 攻撃対策専用のハードウェアを使用することにより，正規アクセスのパケットと攻撃パケットを選別することも可能だが，導入するためには非常に費用がかかるという問題点がある．また，これらのサーバ側でおこなう対応では，攻撃の規模が大きくなるほど防御が難しく，インターネット上に流れる不要なパケットを軽減することもできない．

さらに，ボットネットの流行により，コンピュータの利用者が意図していないにもかかわらず，DDoS 攻撃活動に加担してしまう危険性が高まっている．ボットネットを構築するボットでは，OS やセキュリティソフトウェアの機能を無効化する機能を持つボットの存在が報告されている[2]．この機能を持つボットは，感染したコンピュータにおけるボットの検知，削除を実施するウイルス対策ソフトや，外部とおこなう通信のアクセス制御を実施するファイアウォールの実行を妨害する．その結果，ボットの存在や活動状況が隠ぺいされ，DDoS 攻撃が発信されていることを，コンピュータ上で検知できなくなってしまう．

3.2 DDoS 攻撃遮断システムの概要

本研究では，双方向に通信が発生するという正常な通信における特徴に着目し，DDoS 攻撃を検知，遮断するシステムを提案する．本研究における提案システムの概要を図 1 に示す．本システムではクライアント側のネットワークとインターネットの境界となるルータ上にて通信の監視をおこなう．通信をおこなっているホスト間ごとに，通信の状態を判定することで，インターネット上への DDoS 攻撃パケットの流出を防ぐ．

また，提案手法を実現するシステムは通信をおこなっているホストと独立して動作しているため，内部ネットワークに存在するコンピュータの状態にかかわらず，攻撃に対応することができる．

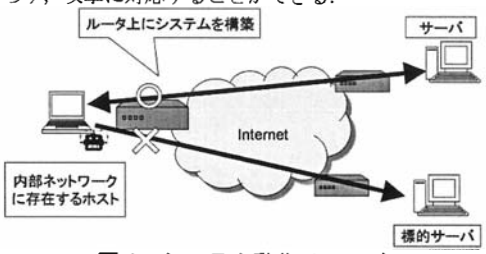

図 1　システム動作イメージ

3.3 DDoS 攻撃検知手法

提案手法では，ルータを通過してやりとりされる通信の状態を解析することにより DDoS 攻撃を検知する．まず，キャプチャしたパケットを通信しているホスト間ごとにまとめるため，送信元／宛先 IP アドレス，ポート番号の組み合わせでひとくくりの通信とする．そして，まとめた通信の状態を単位時間ごとに区切り解析する．本稿では，ホスト間ごとに単位時間で区切った通信をフローと呼び，フローの記憶する情報はつぎの項目である．

①送信元／宛先 IP アドレス
②送信元／宛先ポート番号
③送信／受信パケット数の総計
④送信／受信パケットのサイズの総計
⑤通信記録時間

つぎに，得られた情報をもとに，DDoS 攻撃の種類に応じた特徴を利用して，正常なフローと不正なフローに判別する．DDoS 攻撃に利用される DoS 攻撃の

主な種類と，判定に使用する条件を表 1 に示す．判定条件の詳細については，条件 1 を 3.3.1 節に，条件 2 を 3.3.2 節にて述べる．最終的に，同一の IP アドレスに対して，条件に合致するフローの合計パケット数が閾値を越えた時点で DDoS 攻撃の発生とみなす．

表 1　DDoS 攻撃の種類と対応

DDoS 攻撃の種類	判定条件
SYN flood , UDP flood , ICMP flood	双方向通信の有無（条件 1）
Connection flood	パケットのサイズ（条件 2）
HTTP GET flood	未対応

3.3.1　双方向通信の判定

ネットワークを介したホスト間でおこなわれる正常な通信では，リクエストとそれに対するレスポンスが存在し，図 1（A）のように双方向にパケットを交換することにより成立している．それに対し，DDoS 攻撃に用いられる SYN flood，UDP flood，ICMP flood などの攻撃手法では，図 2（B）のようにパケットを一方的に相手に送りつけるという特徴が見られる．この特徴を利用し，内部ネットワークからインターネットに向かって一方的にパケットが送信されているフローを検知した場合，つまり，受信パケット数が 0 の場合は不正なフローとして検出する．この判定条件を条件 1 とする．

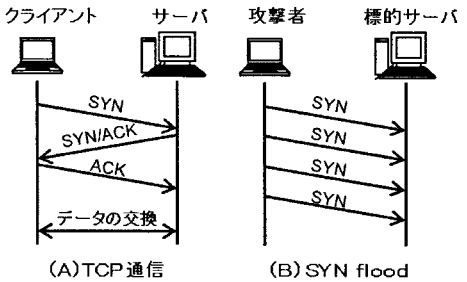

図 2 正常な通信と DDoS 攻撃の例

提案手法では，通信監視をおこなうルータにかかる負荷や資源を軽減するため，通信の状態を単位時間に区切ったフローとして解析している．そのため，図 3 のように単位時間におさまらないパケットが不正なフローとして誤検出される可能性がある．

そこで，つぎに述べる手順で直前におこなわれた正常な通信を正常通信リストとして保存し，単位時間で区切ることにより発生する誤検出を回避する．

1. 判定条件に合致しないフローを正常なフローとみなし，正常通信リストに保存する．
2. 判定条件に合致するフローは，まず正常通信リストと比較をおこなう．
3. リストに送信元／宛先 IP アドレス，ポート番号の一致する通信が存在する場合，正常な通信と判定し無視する．
4. 正常通信リストに一致する通信がない場合，不正なフローとして検出する．

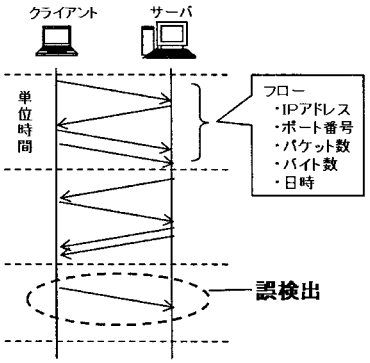

図 3　単位時間に区切ることによる誤検出

3.3.2　パケットサイズの判定

Connection flood と呼ばれる DoS 攻撃は，標的となるサーバと TCP における 3 ウェイハンドシェイクを大量に確立させ，サーバの持つ資源を占領し，他のクライアントに対して応答できない状態にする攻撃である．そのため，双方向通信の判定では，SYN flood，UDP flood，ICMP flood は検知することが可能だが，Connection flood を検知することができない．そこで，交換されるパケットの数とサイズを利用する．Connection flood で交換されるパケットは TCP の 3 ウェイハンドシェイクに利用されるパケットのみであるため，TCP プロトコルを利用した通信のうち，つぎの条件に合致するフローを不正なフローと判定する．この条件を条件 2 とする．

- 送信／受信パケット数がそれぞれ 2 以下である．
- 送信／受信パケットの平均サイズが IP 及び TCP ヘッダを合わせたサイズに収まっている．

また，条件 1 と同様に単位時間に区切ることによる誤検出が発生する可能性があるため，正常通信リストと比較をおこない誤検出を回避する．

3.3.3　DDoS 攻撃発生の判定

提案手法による DDoS 攻撃の判定は，それぞれの条件ごとに用意した不正通信リストを用いておこなう．

不正通信リストに記録されている通信は，図 4 に示す流れで検出された不正なフローにより更新する．更新は，条件 1 では宛先 IP アドレス，条件 2 では送信元／宛先 IP アドレスが一致する通信に対しておこない，最終更新時間の変更と送信パケット数の加算をおこなう．本稿では，送信パケット数の加算された数値

をカウント数と呼び，設定した閾値を越えた時点でDDoS攻撃の発生と判定する．

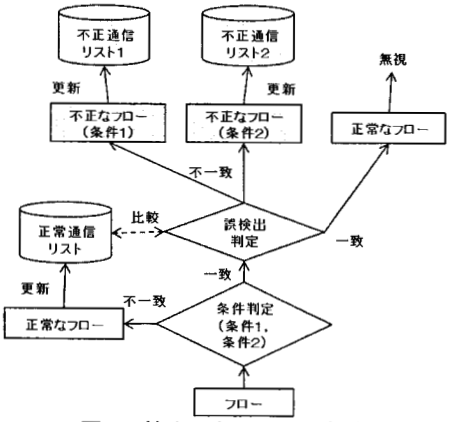

図4　検出したフローの処理

4. DDoS攻撃遮断システムの実装

本節では，前章で述べた手法を実現するためのプロトタイプシステムの実装方法について述べる．ここで，プロトタイプシステムではLinux（FedoraCore5）をルータとして利用し，そのうえにシステムを構築する．

4.1 システムの構成

本システムの全体像を図5に示す．主な機能を通信監視，情報解析，攻撃遮断の3つにわけて実装をおこなう．DDoS攻撃を検知，遮断するまでの処理フローをつぎに示す．

(1) ルータを通過するパケットから，フローごとに必要な情報をまとめる．
(2) 得られた情報を3章で述べた手法で解析する．
(3) 攻撃が検知された場合，遮断命令および，ログへの出力をおこなう．
(4) 攻撃発生情報をもとに，直ちにDDoS攻撃を遮断する．

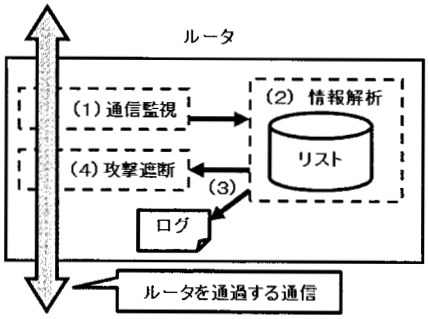

図5　システムの構成

4.2 各機能の詳細

各機能の動作，及び機能を実装するにあたって使用したソフトウェアについて述べる．

4.2.1 通信監視

ホスト間の通信を監視し，解析に必要な情報を得るためにつぎの機能を持つ．

① 通過するパケットをキャプチャする．
② パケットをフローにまとめる．
③ フローごとに必要な情報を記録する．
④ 解析に使用する形式で情報を抽出する．

①から③までの機能を，トラフィックモニタリングソフトであるargus[3]を用いて実装する．また，argusの記録するレコードはバイナリデータであるため，argusレコード読解用ソフトウェアであるraを機能拡張し，解析に使用する形式にまとめた情報を取り出す．

4.2.2 情報解析

通信監視機能により抽出した情報を受け取り，フローごとに3.3節で述べた手法で解析をおこなう．DDoS攻撃が検知された時点で攻撃遮断命令を発行する．

また，不正通信リストの内容は定期的にチェックし，最後に不正なフローを検出してから一定時間が経過しているものは削除する．攻撃遮断命令が発効されている通信においては，攻撃が停止してから一定時間経過後に解除命令を発行し，リストから削除する．さらに，監視している通信の状態を把握するため，ログとしてつぎの情報を記録する．

- 攻撃検知情報
- リスト更新情報（削除時）
- 攻撃遮断，解除情報

4.2.3 攻撃遮断

攻撃遮断命令が発行された時点で，不正通信リストに記録されている情報をもとに，ルータを通過してインターネット上へ出ていく攻撃パケットを遮断する．パケットを遮断する際にはiptables[4]を用いて，IPアドレスをもとにしたフィルタリングをおこなう．

条件1で検知された攻撃は同一宛先IPアドレスへのパケットをフィルタリングする．また，条件2で検知された攻撃は，Connection floodの特性上送信元IPアドレスを詐称することが困難なため，送信元／宛先IPアドレスの組み合わせでフィルタリングする．

5. 評価

構築した仮想ネットワークでプロトタイプシステムを用い，本提案システムの動作を検証した結果，DDoS攻撃の検知は問題なくおこなえることを確認した．つぎに，本システムにおける動作効率は適用するパラメータの設定によりに変化することから，発生

する誤検出の状況を利用し，システムの動作効率を最適にするパラメータの検討をおこなった結果を示す．ここで，誤検出とは，正常な通信から抽出したフローが不正なフローとして検出されることを指す．

5.1 評価内容

本稿にて検討をおこなうパラメータと，パラメータごとの最適化条件をつぎに述べる．

(1) 通信をフローとして区切る際の単位時間
提案手法では，単位時分の情報をまとめてから解析するため，新規に通信が開始されてから解析を開始するまで，設定した単位時間の経過が必要である．つまり，DDoS 攻撃の発生から検知まで，少なくとも設定した単位時間を要してしまう．よって，攻撃への対応を早くするために，フローを区切る単位時間は誤検出が増加しない範囲で短く設定する．

(2) 不正通信リストの保存時間
不正通信リストに記録された通信は，設定した保存時間更新されていない場合，リストから削除する．リストに記録された通信の量を減らし，リスト更新時の負荷を軽減するため，保存時間は DDoS 攻撃の判定に影響を与えない範囲で短く設定する．

(3) DDoS 攻撃検知に利用する閾値
不正通信リストのカウント数が閾値を越えた時点で攻撃と判定するため，攻撃判定を早めるために，正常な通信との誤判定を起こさない範囲で小さい値を設定する．

条件を満たすパラメータの設定を検討するため，パケットをキャプチャした通信データに対し，プロトタイプシステムを用いて解析をおこない，パラメータの変更に伴う不正なフローの発生状況を，つぎの 2 点から評価する．

- 不正なフロー検出比率
解析したフローに全体おいて，不正なフローとして検出されたフローの割合．正常な通信をおこなっている際の数値は，誤検出の割合となるため，ゼロに近づくことが望ましい．
- 不正通信リスト最大カウント数
不正通信リストに登録された通信のカウント数のうち，解析時に記録された最大値．カウント数は攻撃発生判定に利用されるため，正常な通信をおこなっている際に最大カウント数が増加すると，その分 DDoS 攻撃の誤検知が発生する可能性が高くなる．

評価に利用した通信データの内容を表 2 に示す．それぞれ異なる環境で，一定時間キャプチャしたパケットを記録した．A と B の通信データを取得した際に外部とおこなった通信内容は，WEB サイトの閲覧や，メールの送受信である．また，F はワームによる感染活動の通信のみをおこなった．ここで，A～E の通信データ取得中は攻撃を発信していないため，検出したフローは誤検出といえる．

表 2 使用データ内容

	取得環境	パケット数	フロー数	取得時間（分）
A	直接外部と通信	273390	2258	85
B	プロキシを利用して外部と通信	196239	32932	443
C	ハニーポットを稼働	27000	5716	1 日と 126
D	P2P プログラム①を稼働	63973	2430	43
E	P2P プログラム②を稼働	64144	2019	22
F	ワームを稼働	50967	50967	10

5.2 評価結果

5.2.1 不正なフロー検出比率

単位時間を変化させ，通信データを解析した結果を図 6 に示す．A と B の通信データにおいては，単位時間にかかわらず 1%以下の誤検知となっていた．C～D の通信データでは，取得環境によって検出比率の増減も異なる結果となった．また，検出比率の最大値は，通信データ D に対して単位時間を 7 秒と設定した際に 7.4%を記録した．

ここで，F の通信データに対する結果はすべての単位時間で検出比率が 100%であったため，図 6 には記載していない．

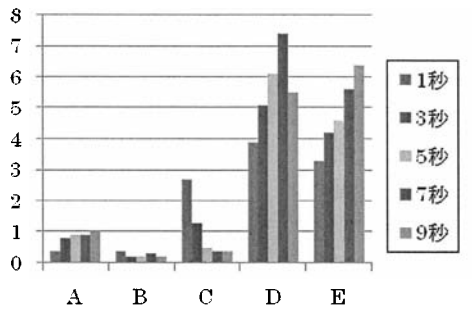

図 6 不正なフロー比率（%）

5.2.2 不正通信リスト最大カウント数

単位時間を変化させ，通信データを解析した結果を図 7 に示す．C 以外の通信データでは，単位時間の変更による最大カウント数への影響はほぼみられなかった．しかし，データ C に対する結果では，単位時間の変更による影響が顕著に現れた．特に，単位時間を 5 秒から 3 秒に短縮すると，誤検出された最大カウント数が 2 から 25 へ急激に増加した．

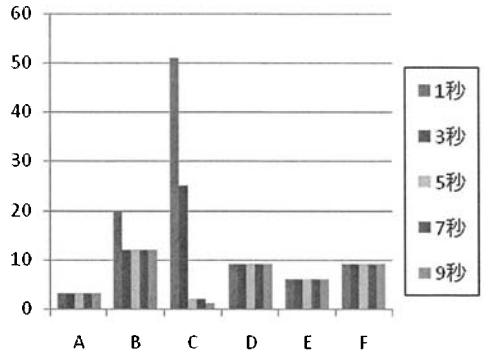

図 7　最大カウント数（単位時間変更時）

つぎに，単位時間を 5 秒に固定し，不正通信リストの保存時間を変化させ，通信データを解析した結果を図 8 に示す．全ての通信データにおいて，保存時間が 20 分以上の設定では，最大カウント数の変化はみられなかった．また，解析時に記録された最大カウント数は，全ての通信データを通じて高々12 であった．

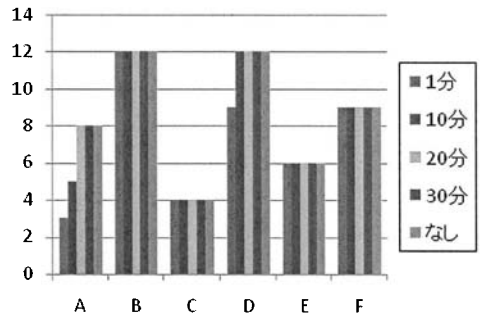

図 8　最大カウント数（保存間隔変更時）

5.2.3　考察とパラメータ設定の検討

評価結果から，それぞれのパラメータにおける最適な設定値に対して検討した結果をつぎに述べる．

(1) 通信をフローとして区切る際の単位時間
　最大カウント数においては，3 秒より短くすると誤検出数が急増する通信データが存在していた．誤検出比率は通信データの種類で増減の様子が異なり，単位時間を決定することはできなかったため，誤検出の増加を抑える範囲での最短の単位時間は 5 秒である．

(2) 不正通信リストの保存時間
　不正通信リストに登録された通信を 20 分以上リストに保存した場合，最大カウント数は変化しなかった．よって，カウント数の判定による DDoS 攻撃の検知に影響しない最短の保存時間は 20 分である．

(3) DDoS 攻撃検知に利用する閾値
　単位時間を 5 秒に固定した場合，攻撃パケットを含まない A～E の通信データでは，最大カウント数が高々12 であった．よって，DDoS 攻撃の誤検知を発生させない閾値は 13 である．

また，不正なフロー検出比率に対する評価結果から，WEB サイトの閲覧や，メールの送受信をおこなう通信では，ほぼ誤検出を発生させることなくシステムを動作できることがわかった．

最後に，通信データ F における検出比率が 100%となった理由は，ワームが感染活動として SYN パケットを大量に送信しているためだと推測できる．しかし，パケットの宛先 IP アドレスがランダムに変更され，本提案システムではカウント数が高々9 となり，閾値を越えないため攻撃と判定されない．よって，本提案システムによりワームなどのウイルスによる感染活動を検知するためには，宛先 IP アドレスごとに不正通信をまとめるリストを追加する必要がある．

6.　おわりに

本稿では，クライアント側のルータで通信の状態を監視することにより，DDoS 攻撃を発信元で検知，遮断する手法を提案した．また，提案手法を用いてプロトタイプシステムを作成し，異なる環境下で取得した通信データに適用することで評価をおこなった．評価結果から，WEB サイトやメールの閲覧時には，不正なフローの誤検出を 1%以下に抑えることが確認できた．また，通信を区切る単位時間を 5 秒，不正通信リストの保存時間を 20 分，攻撃判定に利用する閾値を 13 と設定することにより，正常な通信に対する誤検出がシステムの動作効率に与える影響を最も抑えることがわかった．

今後の課題として，つぎに示す内容に対して検討をおこなっていく予定である．

- 標的となるサーバに対して HTTP プロトコルの GET リクエストを大量におこなう攻撃である HTTP GET flood への対応
- SYN flood，UDP flood，ICMP flood の検知後，正常な通信も含め一時的に標的サーバに対する全ての通信を遮断してしまう利便性低下の改善

参考文献

[1] 警察庁：平成 19 年上半期におけるインターネット治安情勢について，
http://www.cyberpolice.go.jp/detect/index.html
[2] 松木 隆宏，寺田真敏：セキュリティ無効化機能を逆用したマルウェア活動抑制手法の検討
[3] argus，QoSient
http://www.qosient.com/argus/
[4] netfilter/iptables，http://www.netfilter.org/