Pushback 機構の一提案とそのモデル化に向けて

寺田剛陽† 双紙正和† 宮地充子†

標的サーバへのパケットの大量送信によってサービスを妨害する Denial of Service（DoS）攻撃は，近年の商取引や行政サービスの積極的なインターネットの活用にとって大きな脅威となっている．pushback とはネットワーク上のルータで行う帯域制限の情報を隣接する子のルータに伝えることで，DoS 攻撃のパケットによるネットワーク帯域の浪費を防ぐ技術である．既存研究における pushback 機構の性能評価は，攻撃に用いるホストの数，各ホストが送るパケットの流量を固定して行っているため，その他の DoS 攻撃に対する有効性を検証できなかった．そこで本論文では，pushback 機構の理論的なモデル化に向けて，その挙動を一般的に評価できる方式を提案する．提案方式では，完全 2 分木のネットワークトポロジを想定し，標的ホスト宛てのパケットの経路上の各ルータが子に対する流量制限を行う．これにより様々な DoS 攻撃に対する pushback 機構の評価が可能になった．

Toward Modeling of a Pushback Mechanism

Takeaki Terada,† Masakazu Soshi† and Atsuko Miyaji†

Denial of Service (DoS) attacks that disturb on-line services by sending large quantities of packets to a target host. Pushback is a technology that propagates rate-limiting information to adjacent child routers and prevents a network from being wasted on the packets by DoS attacks. In existing study, an efficiency test of a pushback mechanism has been performed under the condition that the number of attack hosts and the amount of the packets sent by each host have been fixed. Therefore, its result has not been useful for verifying the efficiencies of its mechanism against other DoS attacks. In this paper, toward theoretical modeling of Pushback mechanism, we propose a scheme that can generally evaluate its behavior against verious patterns of DoS attacks. In the proposed scheme, on the assumption of a network topology of a perfect binary tree, each router on the routes of the packets destined for a target host performs rate-limiting for its adjacent child routers. As a result, it becomes possible to evaluate pushback mechanism against verious DoS attacks.

1. 背　　景

商取引や行政サービスなど様々なサービスがインターネットの積極的活用を行うようになった昨今，DoS 攻撃は大きな脅威であり，その対策の確立およびインターネットへの実装が待たれている．DoS 攻撃対策として，攻撃に用いられた経路を復元し，その発信源を突き止める経路復元方式と，ルータが協調して DoS 攻撃によるネットワーク全体の帯域の浪費を防ぐ負荷軽減方式がある．

経路復元方式の代表として，確率的パケットマーキング（Probabilistic Packet Marking: PPM）がある．これはパケットにそれ自体の経路を確率的に記録させておき，これらのパケットを収集したサーバが経路復元を行うというもので，IP トレースバック技術ともよばれる．経路復元方式は，攻撃経路を ICMP パケットに埋め込む Bellovin[2] によるプロトコル化に続き，2000 年に Savage らにより初めてモデル化された[8]．これを雛形として多くの PPM の改良方式が提案された．なかでも 2001 年に提案された，Dean らの代数的方式[3] はトレースバック情報を埋め込むパケットのサイズを大幅に縮小し，IP トレースバックの第 2 の雛形となっている．しかし IP トレースバック技術の共通する欠点は，攻撃者を特定する間，DoS 攻撃によるネットワークの輻輳を抑えることができない点にある．

負荷軽減方式は，攻撃の発信源を突き止めるのではなく，攻撃によるネットワーク全体の高負荷を軽減しようというのが目的である．DoS 攻撃はネットワークが公共のものであるからこそ発生するという考えから 2002 年に Keromytis らは認証が必要なネットワークにより DoS 攻撃を防ぐ Secure Overlay Service（SOS）というアプローチを行った[6]．一方でネットワークは

† 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

公共のまま管理主体を越えて高負荷なトラフィックを縮減しようとするものに pushback 技術がある．

pushback は 2002 年に Ioannidis らによって提案された[5]．Aggregate Congestion Control（ACC）機構[7] の 1 つで，各ルータで行う帯域制限の情報を隣接する子のルータに伝えることでネットワーク全体の帯域浪費を抑えようとする技術である．文献 5) で Ioannidis らはパケットに埋め込む pushback 情報の仕様を提案し，さらに同年，pushback 機構の実装を行っている[7]．しかし機構の設計上，その評価はあらかじめ攻撃用ホスト数とそれらの送信量を定量的に与えることでしか行えず，特定の DoS 攻撃に対する有効性のみを検証するにとどまっている．

そこで本論文では pushback 機構の理論的なモデル化に向けて，その挙動を一般的に評価できる方式を提案する．提案方式では，完全 2 分木のネットワークトポロジを想定し，標的ホスト宛てのパケットの経路上の各ルータが子に対する流量制限を行う．これにより様々な DoS 攻撃に対する pushback 機構の評価が可能になる．

本論文は以下のように構成される．2 章において pushback の既存研究について述べる．3 章では既存研究の問題点を解決する方式を提案する．4 章でその評価を行い，5 章で提案方式の拡張について述べる．

2. Pushback の既存研究

この章では pushback の既存研究[5),7)] について議論する．ネットワーク上を流れるパケットは攻撃を受けるホストの立場から 3 つに分類できる．攻撃者が標的ホストに向けて送るパケットは bad パケットとよばれる．また不運にも DoS 攻撃の発生中に標的ホストと正規の通信をするべく送られたパケットを poor パケット，標的ホスト以外の宛先のパケットを good パケットとよぶ．

2.1 ACC 機構

ACC 機構とは，突発的なトラフィックの増加への対処をネットワーク上のルータが行うことで DoS 攻撃を防ごうとするものである．通信の輻輳を引き起こしホストのシステムをダウンさせるようなパケット群を *aggregate* とよぶ．aggregate を構成する各パケットには送信元および宛先 IP アドレス，ポート番号などの情報（*congestion signature* とよばれる）が入っており，DoS 攻撃と思われる aggregate を検出した際はこの情報を用いてパケットを選別し，aggregate の大部分を構成するパケットを破棄する．パケットを破棄するモジュールを rate-limiter とよぶ．各ルータでのパケットの選別は以下のように行われる．

2.1.1 攻撃の検出と帯域制限量の決定

ルータは流入するパケットを送信元アドレス（32 bits）ごとに分類したリストを作る．次にリストにあるアドレスのうち，DoS パケットを送っていると思われる複数のアドレスを，24 bit 前後の共通のネットワークアドレスを持つものどうしで縮約する．これらの縮約した 1 つ 1 つを prefix とよぶ．そして各 prefix を送信パケット量が多い順にソートする．ある aggregate によってルータの許容流量 p_{high} を上回る状態が K 秒間続くと，超過分 R_{excess} のパケットを破棄するために，以下の式により prefix のリストの上位にある prefix を持つパケット $Agg[k]$ $(k = 1, 2, \cdots)$ を上位から選び，それらを帯域制限（rate-limit）の対象とする．

$$\sum_{k=1}^{i}(Agg[k] - L) = R_{excess}$$

ただし L は rate-limit を受けなかった種類のパケットの最大流量を表し，$Agg[k] \geq Agg[k+1] \geq L > Agg[i+1]$ である．

2.2 Pushback

pushback は ACC 機構の 1 つであり，その起動は選択的である．pushback が適用されるネットワークトポロジは pushback を最初に呼び出したルータを根とする木であり，aggregate の発信源（= 攻撃者）は葉に分布する．aggregate を中継するルータは節にあたる．pushback は以下の要素から構成される．

2.2.1 帯域制限の子ルータへの分配

標的ホストに直接つながるルータは子ルータからの rate-limit の対象としたパケットの流量に応じて，超過分の流量 R_{excess} を子に振り分け，これを congestion signature とともに *pushback request message* として子に送る．rate-limit の要求を受けとった子はその要求に基づき，該当パケットの rate-limit を行い，必要に応じて自分の子にその要求を中継する．

2.2.2 Pushback の解除条件

子ルータは rate-limit を行う前の aggregate の流量を *pushback status message* として，一定時間ごとに親に送信する．親はこれを標的ホスト V を直接つなぐルータ R に中継する．R はこのメッセージにより aggregate が収束したかどうかを判断する．収束していなければ，*pushback refresh message* を子に送信し pushback の更新を要求し，収束していれば送信しない．このメッセージには rate-limit の実行期間の情報が書かれており，メッセージの受信がなくなれば子は

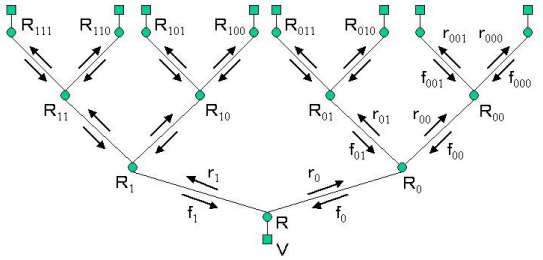

図 1 想定するネットワークトポロジ
Fig. 1 Supposed network topology.

rate-limit を終了する．

2.3 既存研究の問題点

DoS 攻撃が発生したとき，ルータは ACC 機構により aggregate を検出しその大部分を占めるパケットを選出する．そして選択的に pushback を起動して超過分の流量を子ルータに振り分けるが，その方法として max-min cut の定理を用いるとしている．これは，ルータに閾値を超える流入量があったときのルータの挙動のみを提案しているにすぎない．このことは pushback 機構の評価が，pushback 機能を実装したネットワークシミュレータにおいて，bad，poor，good パケットを送るホストを固定し，送信量の具体値を与えることでしか行うことができないことを意味している．つまり既存研究は特定の DoS 攻撃に対する pushback 機構の性能を評価したにすぎず，発信源の数，送信量の異なる DoS 攻撃に対しては何ら評価を行うことができない．そこで我々は pushback 機構の理論的なモデル化に向けて，その挙動を一般的に評価できる方式を提案する．

3. 提 案 方 式

3.1 想定するネットワークトポロジ

本論文で想定するネットワークトポロジは高さを h とする完全 2 分木とする．**図 1** に $h = 3$ の場合を示す．末端の各ルータには標的ホスト V に向けてトラフィックを送るホストあるいは中継ルータがつながっているとする．ルータ R は V とネットワークをつなぎ，$R_{b_1 b_2 \cdots b_i} (1 \leq i \leq h,\ b_i \in \{0,1\})$ はネットワーク上のルータ，$f_{b_1 b_2 \cdots b_i}$ は子から親への V 宛てのパケットの送信量，$r_{b_1 b_2 \cdots b_i}$ は pushback 機構により親から子へ要求するパケット送信量である．

3.2 提案 Pushback 機構

本節では pushback 機構の 1 機能である，rate-limit の子ルータへの分配方法について提案を行う．

標的ホスト V をネットワークにつなぐルータ R が，V 宛てのトラフィックに設定する許容量を t とする．ルータ $R_{b_1 \cdots b_{i-1}}$ $(i \leq h,\ b_j \in \{0,1\},\ 1 \leq j \leq i-1)$ は次節の方針に基づくアルゴリズムにより，子 $R_{b_1 \cdots b_i}$ に対し，決定した送信量 $r_{b_1 \cdots b_i}$ を要求する．この要求は congestion signature とともに pushback request message として $R_{b_1 \cdots b_i}$ に送られる．

3.2.1 方　　針

送信制限量 $r_{b_1 b_2 \cdots b_i}$ を以下の方針で決定する．

- 子ルータが中継するトラフィックのうち，t を超えないものについては，DoS 攻撃のトラフィックと見なさず，rate-limit の要求を pushback しない．
- 子ルータが中継するトラフィックのうち，t を超えるものについては，DoS 攻撃と見なし，送信量に比例した rate-limit の要求を pushback する．
- ルータ $R_{b_1 \cdots b_{i-1}}$ は親から要求された送信量 $r_{b_1 \cdots b_{i-1}}$ を子に振り分ける．すなわち $b_{i_1}, b_{i_2} \in \{0,1\}$ に対して
$$r_{b_1 \cdots b_{i-1} b_{i_1}} + r_{b_1 \cdots b_{i-1} b_{i_2}} = r_{b_1 \cdots b_{i-1}}$$
とする．
- pushback を最初に呼び出したルータ R は，子 R_0，R_1 からの送信量 f_0，f_1 と R が許容する送信量 t との大小関係によって場合分けを行う．場合分けを行うことで，DoS 攻撃に関わっていない，通常量のパケットを送っている正規ユーザの標的ホスト V への通信を妨げないようにする．
- ルータ $R_{b_1 b_2 \cdots b_i}$ $(i = 2, \cdots, h)$ での場合分けの際の比較値 $t_{b_1 b_2 \cdots b_i}$ は，想定するネットワークトポロジが完全 2 分木であり，レベルごとのノード数は葉に近づくほど増えることを考慮して定める．レベル $i-1$ に属するルータ $R_{b_1 b_2 \cdots b_i}$ での比較値 $t_{b_1 b_2 \cdots b_i}$ を $t_{b_1 b_2 \cdots b_i} = t/2^{i-1}$ とする．

以上の方針に基づき，提案方式のアルゴリズムを次項に記述する．

3.2.2 アルゴリズム

(1) R の 2 つの子を R_{i_m} $(i_m \in \{0,1\},\ m \in \{1,2\})$ とする．このとき

(a) $f_{i_1} > t$ かつ $f_{i_2} \leq t$ のとき
$$r_{i_1} = t - f_{i_2}, \quad r_{i_2} = f_{i_2}$$
とする．この式が示すように，R_{i_2} には送信量の制限を行わない．すなわち R_{i_2} には pushback request message を送らない．

(b) $f_{i_1} > t$ かつ $f_{i_2} > t$ のとき
$$r_{i_m} = f_{i_m} \cdot \frac{t}{f_0 + f_1}$$
とする．

(2) $R_{b_1\cdots b_{i-1}}$ $(2 \le i \le h)$ の 2 つの子を $R_{b_1\cdots b_{i-1}b_{i_m}}$ $(b_{i_m} \in \{0,1\},\ m \in \{1,2\})$ とする．

(a) $f_{b_1\cdots b_{i-1}b_{i_1}} > t/2^{i-1}$，$f_{b_1\cdots b_{i-1}b_{i_2}} \le t/2^{i-1}$ のとき

$$r_{b_1\cdots b_{i-1}b_{i_1}} = r_{b_1\cdots b_{i-1}} - f_{b_1\cdots b_{i-1}b_{i_2}},$$
$$r_{b_1\cdots b_{i-1}b_{i_2}} = f_{b_1\cdots b_{i-1}b_{i_2}}$$

とする．この式が示すように，$R_{b_1\cdots b_{i-1}b_{i_2}}$ には送信量の制限を行わない．すなわち $R_{b_1\cdots b_{i-1}b_{i_2}}$ には pushback request message を送らない．

(b) $f_{b_1\cdots b_{i-1}b_{i_1}} > t/2^{i-1}$，$f_{b_1\cdots b_{i-1}b_{i_2}} > t/2^{i-1}$ のとき

$$r_{b_1\cdots b_{i-1}b_{i_m}} = f_{b_1\cdots b_{i-1}b_{i_m}} \cdot \frac{r_{b_1\cdots b_{i-1}}}{f_{b_1\cdots b_{i-1}}}$$

とする．

4. 評　　価

従来の pushback 機構は DoS 攻撃によるネットワーク帯域の占有を軽減しながらも poor パケットの損失も抑えるという目的で提案された．したがって，pushback 機構を評価する指標の 1 つとして，発信源の数，送信量の異なる様々な DoS 攻撃が発生した際，pushback を呼び出したことによる poor パケットの損失の少なさをあげることができる．そこで本章では，提案方式の利用によって起こる poor パケットの損失量の上限と下限を求める．

高さ h の 2 分木のネットワークトポロジにおいて，葉に属するルータ $R_{b_1\cdots b_h}$ につながる末端のマシンのうち，標的ホスト V への poor パケットを送るマシンの集合を S_L とする．

ルータ $R_{b_1\cdots b_h}$ につながる末端のマシンが V に送る流量を $f_{b_1\cdots b_{h-1}b_h}$ $(1 \le i \le h,\ b_i, \overline{b_i} \in \{0,1\},\ b_i \ne \overline{b_i})$ とする．提案方式を適用したとき，V によって受け入れられる流量 $r_{b_1\cdots b_{h-1}b_h}$ は以下の式で表される．

- $f_{b_1\cdots b_{h-1}b_h} \le t/2^{h-1}$ のとき
$$r_{b_1\cdots b_{h-1}b_h} = f_{b_1\cdots b_{h-1}b_h} \quad (1)$$
- $f_{b_1\cdots b_{h-1}b_h} > t/2^{h-1} \wedge f_{b_1\cdots b_{h-1}\overline{b_h}} \le t/2^{h-1}$ のとき
$$r_{b_1\cdots b_{h-1}b_h} = r_{b_1\cdots b_{h-1}} - f_{b_1\cdots b_{h-1}\overline{b_h}}$$
- $f_{b_1\cdots b_{h-1}b_h} > t/2^{h-1} \wedge f_{b_1\cdots b_{h-1}\overline{b_h}} > t/2^{h-1}$ のとき
$$r_{b_1\cdots b_{h-1}b_h} = f_{b_1\cdots b_{h-1}b_h} \cdot \frac{r_{b_1\cdots b_{h-1}}}{f_{b_1\cdots b_{h-1}}}$$

ここで次の定理が成り立つ．

定理 1 $i < j \le h$ に対し，$f_{b_1\cdots b_i} \le \frac{t}{2^{i-1}} \wedge f_{b_1\cdots b_i\cdots b_j} > \frac{t}{2^{j-1}} \wedge f_{b_1\cdots b_i\cdots b_{j-1}\overline{b_j}} \le \frac{t}{2^{j-1}}$ であるとき

$$r_{b_1\cdots b_h} = f_{b_1\cdots b_h}$$

となる．

証明） $i < j \le h$ に対し，$f_{b_1\cdots b_i\cdots b_j} > \frac{t}{2^{j-1}}$ かつ $f_{b_1\cdots b_i\cdots b_{j-1}\overline{b_j}} \le \frac{t}{2^{j-1}}$ であるので

$$\begin{aligned} r_{b_1\cdots b_h} &= r_{b_1\cdots b_{h-1}} - f_{b_1\cdots b_{h-1}\overline{b_h}} \\ &= r_{b_1\cdots b_{h-2}} - f_{b_1\cdots b_{h-2}\overline{b_{h-1}}} - f_{b_1\cdots b_{h-1}\overline{b_h}} \\ &= r_{b_1\cdots b_i} - \sum_{j=i+1}^{h} f_{b_1\cdots b_{j-1}\overline{b_j}} \end{aligned}$$

ここで $f_{b_1\cdots b_i} \le \frac{t}{2^{i-1}}$ であるので $r_{b_1\cdots b_i} = f_{b_1\cdots b_i}$．このことと $f_{b_1\cdots b_i} - f_{b_1\cdots b_i\overline{b_{i+1}}} = f_{b_1\cdots b_{i+1}}$ より

$$\begin{aligned} & r_{b_1\cdots b_i} - \sum_{j=i+1}^{h} f_{b_1\cdots b_{j-1}\overline{b_j}} \\ &= f_{b_1\cdots b_i} - \sum_{j=i+1}^{h} f_{b_1\cdots b_{j-1}\overline{b_j}} \\ &= f_{b_1\cdots b_i} - f_{b_1\cdots b_i\overline{b_{i+1}}} - \cdots - f_{b_1\cdots b_{h-1}\overline{b_h}} \\ &= f_{b_1\cdots b_{i+1}} - \cdots - f_{b_1\cdots b_{h-1}\overline{b_h}} \\ &= \cdots \\ &= f_{b_1\cdots b_h} \end{aligned}$$

となる．題意は示された． ∎

したがって定理 1 により，ホスト V を根とする完全 2 分木のネットワークにおいて，葉に位置するホスト H から V への送信量 $f_{b_1b_2\cdots b_h}$ が，比較値 $t_{b_1b_2\cdots b_h}$ を上回ったとしても，経路上のあるルータ $R_{b_1b_2\cdots b_i}$ に流れ込むパケットの合計 $f_{b_1b_2\cdots b_i}$ が $t/2^{i-1}$ を下回ればホスト H に送信制限は課されないことが分かる．ゆえに $r_{b_1\cdots b_h}$ が最小，すなわち poor パケットの損失が最大になるのは，すべての i に対して $f_{b_1\cdots b_i} > t/2^{i-1} \wedge f_{b_1\cdots b_{i-1}\overline{b_i}} > t/2^{i-1}$ がつねに成り立つときである．

このとき

$$\begin{aligned} r_{b_1\cdots b_{h-1}b_{h_1}} &= f_{b_1\cdots b_{h-1}b_{h_1}} \cdot \frac{r_{b_1\cdots b_{h-1}}}{f_{b_1\cdots b_{h-1}}} \\ &= f_{b_1\cdots b_{h-1}b_{h_1}} \cdot \frac{f_{b_1\cdots b_{h-1}} \cdot \frac{r_{b_1\cdots b_{h-2}}}{f_{b_1\cdots b_{h-2}}}}{f_{b_1\cdots b_{h-1}}} \\ &= f_{b_1\cdots b_{h-1}b_{h_1}} \cdot \frac{r_{b_1\cdots b_{h-2}}}{f_{b_1\cdots b_{h-2}}} \\ &= \cdots \\ &= f_{b_1\cdots b_{h-1}b_{h_1}} \cdot \frac{t}{f_0 + f_1} \end{aligned}$$

が成り立つ．よって提案方式によって破棄される poor パケットの上限 $\max\{r_{drop}\}$ は，以下の式で表される．

$$\max\{r_{drop}\} = \sum_{i \in S_L} (f_i - r_i)$$
$$= (1 - \frac{t}{f_0 + f_1}) \sum_{i \in S_L} f_i. \qquad (2)$$

よって式 (2) より，提案方式は $\forall i \in S_L$ について $f_i > t/2^{i-1}$ が成り立つとき，poor パケットを最も多く失い，その量はルータ R への流入量 $f_0 + f_1$ の単調増加関数となる．

一方，$r_{b_1 \cdots b_h}$ が最大，すなわち poor パケットの損失が最小になるのは，式 (1) と定理 1 より，ある i に対して $f_{b_1 \cdots b_i} \leq t/2^{i-1}$ が成り立つときである．よって提案方式によって破棄される poor パケットの下限 $\min\{r_{drop}\}$ は以下の式で表される．

$$\min\{r_{drop}\} = \sum_{i \in S_L} (f_i - r_i) = 0 \qquad (3)$$

よって式 (3) より，提案方式は $\exists i$ $(b_1 \cdots b_i \cdots b_h \in S_L)$ について $f_{b_1 \cdots b_i} \leq t/2^{i-1}$ が成り立つとき，poor パケットの損失は 0 となる．よって次の定理を得る．

定理 2 pushback を呼び出すルータ R を根とする完全 2 分木のネットワークトポロジにおいて，R の 2 つの子 R_0，R_1 から R への送信量をそれぞれ f_0，f_1，R での許容量を t，R への poor パケットを送るマシンの集合を S_L とする，とする．このとき提案方式による poor パケットの損失量 r_{drop} は

$$0 \leq r_{drop} \leq (1 - \frac{t}{f_0 + f_1}) \sum_{i \in S_L} f_i$$

となる． ∎

既存の pushback 機構では，bad，poor，good パケットの発信源を固定し，シミュレーションを行うことで pushback 機構の性能評価を行っていた．つまり既存研究には理論的なモデルがなく，発信源の数や送信量の異なる DoS 攻撃に対する各ルータの挙動を検証することが困難であった．本論文では pushback 機構の理想的なモデル化に向けて，ネットワーク上の各ルータが自身へのパケットの流入量によって流量制限を行う方式を提案した．結果，様々な DoS 攻撃に対する各ルータの挙動を一般的に評価することが可能になったとともに，各攻撃における poor パケットの損失量の上限値を明らかにした．

5. 今後の課題

本研究では，パケットの流入量と流量制限の基本的な場合の評価を行った．今後，各ルータが確率的にパケットの流量制限を行うなどの一般化により，さらに効率の良い pushback の設計への発展が望まれる．

参 考 文 献

1) Adler, M.: Tradeoffs in Probabilistic Packet Marking for IP Traceback, *Proc. 34th ACM Symposium on Theory of Computing* (*STOC*) (2002).
2) Bellovin, S.: ICMP Traceback Messages (Mar. 2000). http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt
3) Dean, D., Franklin, M. and Stubblefield, A.: An Algebraic Approach to IP Traceback, *Network and Distributed System Security Symposium* (*NDSS '01*) (Feb. 2001).
4) Huang, Q., Kobayashi, H. and Liu, B.: Analysis of a New Form of Distributed Denial of Service Attack, *Conference on Information Science and Systems*, The Johns Hopkins University (Mar. 2003).
5) Ioannidis, J. and Bellovin, S.M.: Implementing Pushback: Router-Based Defense Against DDoS Attacks, *Proc. Network and Distributed System Security Symposium* (*NDSS*) (Feb. 2002).
6) Keromytis, A., Misra, V. and Rubenstein, D.: SOS: Secure Overlay Services, *Proc. ACM SIGCOMM'02*, Pittsburgh, PA (Aug. 2002).
7) Mahajan, R., Bellovin, S., Floyd, S., Ioannidis, J., Paxson, V. and Shenker, S.: Controlling High Bandwidth Aggregates in the Network (Extended Version). http://www.icir.org/pushback/pushback-Jul01.pdf
8) Savage, S., Wetherall, D., Karlin, A. and Anderson, T.: Practical network support for IP traceback, *Proc. 2000 ACM SIGCOMM Conference* (Aug. 2000).

(平成 15 年 12 月 4 日受付)
(平成 16 年 6 月 8 日採録)

寺田 剛陽

2002 年北陸先端科学技術大学院大学情報科学研究科情報システム学専攻博士前期課程修了．同大学院博士後期課程在学中．主として，情報セキュリティに関する研究に従事．

双紙 正和（正会員）

1991 年東京大学工学部卒業．1993 年同大学大学院理学系研究科情報科学専攻修了．電気通信大学大学院情報システム学研究科助手を経て，1999 年から 2003 年 1 月まで北陸先端科学技術大学院大学情報科学研究科助手．2003 年 2 月から同研究科特任助教授．現在に至る．情報セキュリティの研究に従事．博士（工学）．

宮地 充子（正会員）

1988 年大阪大学理学部数学科卒業．1990 年同大学大学院修士課程修了．同年松下電器産業株式会社入社．1998 年北陸先端科学技術大学院大学・情報科学研究科助教授．現在に至る．2002 年〜2003 年カリフォルニア大学デービス校客員研究員．情報セキュリティの研究に従事．博士（理学）．SCIS93 若手論文賞，科学技術庁注目発明賞，坂井記念特別賞，標準化貢献賞各受賞．電子情報通信学会，IACR 各会員．