サービス妨害攻撃の現状と対策技術の動向

非会員 富士 仁*   非会員 Eric Y. Chen*,**

Service Attacks and their Countermeasures

Hitoshi Fuji*, Non-member, Eric Y. Chen*, **, Non-member

Denials of Service (DoS) attacks are one of the most alarming threats on the Internet. A typical DoS attack disrupts the services of its target by usurping network bandwidth and overtaxing server resources to prevent legitimate access from getting through. Effective protection from DoS attack involves tackling the prevention, detection, traceback and mitigation at various levels. This article surveys DoS attacks commonly seen on the Internet, and a number of promising countermeasures against them.

キーワード：サービス妨害攻撃、ネットワークセキュリティ、攻撃検知、攻撃元探知

Keywords : Denial of Service attack, network security, attack mitigation, traceback

1. はじめに

昨今、インターネットを利用する際のセキュリティの脅威が広く認知されるようになってきており、ウイルス対策としてアンチウイルスソフトウェアを端末にインストールすることや、不正侵入対策としてローカルネットワークの入り口にファイアウォールや IDS(Intrusion Detection System)を設置することが行われてきている。

また、ビジネスに関連したクリティカルな業務などでは、一般の利用者に比べると進んだセキュリティ対策が採られており、情報の盗聴や改ざん対策として、インターネット経由の通信での盗聴防止のためのVPN等の暗号通信が利用されたり、情報を暗号化して保存、あるいは通信するといった対策が行われている。

しかし、これらの脅威のように、ネットワークの利用者が対策を実施するだけでは、十分な効果が得られない脅威としてサービス妨害攻撃(DoS: Denial of Service)、あるいは分散サービス妨害攻撃(DDoS: Distributed Denial of Service)と呼ばれるものがある。本稿では、DoS/DDoS 攻撃の現状、その対策技術の動向について述べる。

2. サービス妨害攻撃の脅威

DoS/DDoS 攻撃とは、サーバやネットワーク宛てに不正

なパケットを送信することによって、サービスを妨害する攻撃である。2000 年 2 月に多発した米国の商用 Web サービス提供者 (Yahoo, amazon, e-Bay 等) への DDoS 攻撃では、各 Web サービス提供者は多額の経済的な損失を被ったとされている。最近では、2002 年 10 月にインターネットの基幹サービスともいえるドメインネームシステム (DNS: Domain Name System) のルートサーバへの DDoS 攻撃が発生したことや、2004 年になってからは米国のマイクロソフトや SCO グループへの攻撃が発生したことが知られている。

あるサーバが **DoS/DDoS** 攻撃を受けると、サーバの **CPU** やメモリといった資源が無駄遣いされ、通常のサービスが提供できなくなったり、サーバが **ISP** へ接続しているアクセス回線の帯域が、大量のパケットにより消費されてしまうことになる。このうちサーバのリソース消費だけであれば、ファイアウォールなどでパケットを破棄してある程度の効果が得られる。すなわち、インターネットの利用者が、自衛のために対策することが可能である。しかし、ネットワーク帯域が消費されてしまう事象が発生するほどの大量のパケットが **ISP** に流れ込むと、途中のルータなどのネットワーク機器にも負荷が掛かるなど、攻撃を受けているサイトに対してアクセスしている利用者ばかりではなく、攻撃を受けているプロバイダを経由して通信を行っている他者にも悪影響が及んでしまう可能性がある。

また、CSI/FBI のレポート^①によれば、図 1 に示すように DoS/DDoS 攻撃を受けた被害者の割合も増加傾向にあり、また、被害額としても情報漏えいについて額が大きく、約 6,500 万ドルにもものぼる。この被害額は、ウイルスによる被害額が約 2,700 万ドルであることと比較すると、大きい。

* 日本電信電話(株)NTT 情報流通プラットフォーム研究所
〒180-8585 東京都武蔵野市緑町 3-9-11
NTT Information Sharing Platform Laboratories
3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585

東京大学大学院情報理工学系研究科
〒113-0033 東京都文京区本郷 7-3-1
Department of Information Science, University of Tokyo
7-3-1, Hongo Bunkyo-ku, Tokyo 113-0033

図1 一年間に DoS/DDoS 攻撃を受けた割合
Fig. 1. Percentage of respondents reporting DDoS attacks.

図2 DoS/DDoS 攻撃のパケットの流れ
Fig. 2. DoS/DDoS attack model.

な額であることがわかる。

3. DoS/DDoS 攻撃手法

DoS/DDoS 攻撃は、大別するとサーバ上のソフトウェアの脆弱性を狙う攻撃と、大量のアクセスによってサーバやネットワーク機器の処理負荷、またはネットワーク帯域を消費させる **Flood** 型の攻撃に分けられる。これらの攻撃の典型的なパケットの流れを示したのが図2である。

図2では、脆弱性を狙う攻撃のパケットを「①脆弱性攻撃パケット」として示してある。この種のパケットは、悪意のある **Cracker** などが、不正侵入をした端末から攻撃先のサーバなど(図中の **Victim**)へ直接送信することが多い。

一方、大量のアクセスによってサーバ等のリソースやネットワーク帯域の消費を起こさせる攻撃は、一台の端末では攻撃の効果が限られるため、多数の端末から同時に行われることが多い。このとき、攻撃を行う端末に埋め込まれているプログラムのことは“**Zombie**”と呼ばれ、**Cracker** などにより不正に埋め込まれたり、ウイルスによって自動的に大量にばら撒かれることがある。最近の例では、**MyDoom** というウイルスが、米国マイクロソフトのホームページなどを攻撃する機能を備えていた。**Zombie** には、特定のコマンドを受信すると攻撃を開始するトロイの木馬型と、前述の **MyDoom** で使われたような一定の時間になると攻撃を開始するタイマ型がある。前者の場合は、図2のように、「②制御パケット」が **Zombie** に送られ、その後に「③攻撃パケット」が **Victim** に送られるが、後者の場合には、制御パケットを受信しなくても **Zombie** は攻撃パケットの送信を開始する。

以下に、それぞれの攻撃方法の例を示す。

〈3・1〉 **脆弱性を狙う攻撃** このタイプの攻撃は、IP のプロトコルスタックなどに内在する脆弱性を狙う攻撃で、少ないパケットでDoS攻撃を成立させることができる⁽³⁾。

(1) Ping of Death

ping コマンドを使って一定サイズ以上の大きな IP パケットを送信することにより、サーバなどをクラッシュさせる。

(2) LAND

IP パケットの送信元アドレス及びポートを、送信先アド

図3 SYN Flood の概要
Fig. 3. SYN flood overview.

レス及びポートと同じ内容に詐称したパケットを送り、IP パケットの処理プログラムの脆弱性を狙う攻撃である。

(3) Teardrop

IP パケットのフラグメンテーションのオフセットをオーバーラップさせ、IP パケットを処理するプログラムに存在する脆弱性をつく攻撃である。

〈3・2〉 **Flood 型の攻撃** このタイプの攻撃は、大量にパケットをターゲットに送ることによって攻撃を成立させるため、攻撃に加担する端末の台数が多いほど効果的であり、DDoS 攻撃として行われることが多い⁽³⁾⁽⁴⁾。

(1) SYN Flood

TCP プロトコルのセッション確立時に行われる3ウェイハンドシェイクを悪用する攻撃方法である。図3のように、**Cracker** が **Victim** へ TCP コネクションの接続要求として SYN を送信した後、**Victim** からの応答として戻ってきた SYN/ACK を無視して、通常は **Victim** へ戻す ACK を送信しない。このとき **Victim** では、SYN/ACK を送信した後、再度 ACK 送られて来るのを待つ **half open** という状態になる。**half open** 時にはメモリなどを消費しているため、大量の SYN が送られて来ると、**Victim** がハングアップすることや、ハングアップしなくとも一定以上の数の **half open** が溜まった後には、それ以降の新規の SYN に対する処理ができなくなってしまう。これによって、正規にアクセスしてきた通信が確立できなくなりサービスを妨害する。

(2) Smurf

Cracker は Victim の IP アドレスを送信元に偽装した ICMP Echo Request パケットを作成し、そのパケットを踏み台とするサブネットのブロードキャストアドレス宛に送信する。このパケットを受信した各々の端末は、受信パケットの送信元アドレス、すなわち、Victim の IP アドレスに向かって、応答メッセージを返す。この応答メッセージが多数の踏み台マシンから送られることによって、結果的に Victim に対する DDoS 攻撃となる。

(3) DrDoS

Smurf と類似しており、Cracker が Victim の IP アドレスを送信元に偽装した SYN パケットを、多数の踏み台に送信する。踏み台にされた端末は、SYN/ACK パケットを

図4 Smurf の概要

Fig. 4. Smurf overview.

Victim に送信するが、Victim は元々 SYN パケットを送信していないため、ACK パケットは返さない。このとき踏み台の端末では、ACK パケットが返ってこないことから SYN/ACK の再送を行う。しかも、この再送は何度か繰り返して行われるため、Victim には SYN/ACK パケットが大量に送られて DDoS 攻撃となる。

4. DoS/DDoS 対策技術の動向

前述の通り、DoS/DDoS 攻撃には様々な種類があるため、対策も一つの方法で全てを網羅することは不可能である。さらに、攻撃を受ける可能性のあるサーバでの対策や、インターネットへの接続点での対策など、エンドユーザが実施できる対策だけでは不十分でもある。図5に、DoS/DDoS 対策を行う位置の分類を示す。

また、DoS/DDoS 対策に関連する技術は、攻撃の事前から実施できる対策と、攻撃開始後に実施する対策がある。攻撃開始後は、攻撃の検知、攻撃元の探索、そして攻撃を止めるための対策、というステップで実行する。これらの分類で、DoS/DDoS 対策の技術を分類したのが表1である。

〈4・1〉 事前対策

(1) サーバ及び LAN 側機器での事前対策

事前対策では、DoS/DDoS 攻撃を受けてもサービスが停止しないように、サーバなどの攻撃対象となる機器の脆弱性を修復することが必要である。ルータやファイアウォールで攻撃につながるパケットを破棄することは、脆弱性の修復までに時間が掛かるといった場合に、一時的な対処として行われるものであり、根本的な解決策にはならない。

図5 DoS/DDoS 攻撃対策の実施位置

Fig. 5. Locations of DoS/DDoS countermeasure deployment.

表1 DoS/DDoS 対策技術分類

Table 1. Types of DoS/DDoS countermeasures.

	(1) サーバ	(2) LAN 側機器	(3) ユーザ NW 接続点	(4) 他 NW 接続点
事前対策	・セキュリティホール対策 (パッチあて)	・不要パケットの遮断	・偽装パケット流入防止	・偽装パケット流入防止
攻撃検知	・ホスト IDS	・ネットワーク IDS	・ネットワーク IDS	—
攻撃元探知	—	—	・IP トレースバック	・IP トレースバック
防御・対策	・攻撃耐性向上	・パケットフィルタ ・帯域制限	・パケットフィルタ ・帯域制限	・パケットフィルタ ・帯域制限

(2) ネットワークでの事前対策

DoS/DDoS 攻撃では、攻撃元の分析を困難にすることや、攻撃対策を難しくすることを狙って、送信元アドレスを偽装したパケットが使われることが多い。送信元アドレスを偽装したパケットは、通常の通信では使われることは無いことから、ISP のネットワークに流入させないための技術として、Ingress Filter⁽⁶⁾と言われる技術がある。この技術は、ISP がダウンストリームネットワークの経路情報を持っている場合に、これらの経路情報以外から来たトラフィックを防ぐ。しかし、基本的には、エンドユーザを収容しているネットワークのエッジでなければ効果が得られない。そこで、他 ISP や IX との接続点でも利用できる方法として考えられているのが、DPF(Router-based distributed packet filtering)⁽⁶⁾である。DPF は、ボーダールータと接続されるネットワークは固定であることから、そこを通過するパケットの SA も固定的でありほぼ予想できる、という考えに基づき、過去に通過したパケットの履歴やルーティングテーブルなどの情報を分析して、それに合致しないパケットを破棄しようとするアプローチである。

〈4・2〉 攻撃検知 攻撃を検知するシステムには、表 1 に記述したようにホスト IDS とネットワーク IDS という、システムの設置箇所に着目した分類があるが、その他に、検知する手法に着目して Signature-based IDS と Anomaly-based IDS という分類もできる。Signature-based IDS は、攻撃を検知する基準となる Signature とパケットを比較することによって攻撃の検知を行う。一方、Anomaly-based IDS は、検知しようとする攻撃の種類ごとに異常を検知できる方法が様々な角度から検討されている。

DoS/DDoS 攻撃の検知では、Signature-based IDS は、パケットのパターンマッチで行われるという機構上、ビット単位での詳細な比較が可能であるが、処理負荷が高く大量のパケットを検査するのには向かないという面がある。このため、図 1 に示した典型的な攻撃の場合は、①脆弱性攻撃パケットや②制御パケットには、Signature-based IDS が、③攻撃パケットには Anomaly-based IDS が適している。

ここでは、DDoS 攻撃を検知するための Anomaly-based に分類される手法を紹介する。

(1) 通常時のトラヒックの状態との比較による検知

MULTOPS⁽⁷⁾は、サブネットごとに入出力のトラヒックを観測し、(1)式によって通常時比率を計算する。この通常時比率が、事前に人によって決められた閾値を超えた際に、攻撃として検知する。この手法では、2 台の端末の間でやり取りする通信は、通常時はトラヒック量の比率が大きくは変化しないということが前提となっており、大きく変化するということは攻撃が行われているという判断をしている。しかし、普段はあまり使わない大量のトラヒックが流れるアプリケーション（例えばストリーミングで）を急激に比率が変化すると、誤検知になる恐れが高いという課題

が残っている。

$$\text{通常時比率} = \frac{\text{サブネットへ送られてきたトラヒック量}}{\text{サブネットから送られていくトラヒック量}} \dots\dots\dots (1)$$

また、L. Feinstein が提案⁽⁸⁾している方法では、送信元アドレスのランダム性 H を(2)式で計算し、その値が異常になった場合に DDoS 攻撃として検知をしている。異常と判断するための基準は、MULTOPS と同様に人が事前に閾値を決めておき、それを超えるか否かによっている。

$$H = -\sum_{i=1}^n p_i \log_2 p_i \dots\dots\dots (2)$$

これらの方法は、いずれも異常を判断する基準は閾値になっており、閾値の決め方によって検知精度、誤検知確率が変わってくる。この閾値の決め方まで含めてトータルに考えて、異常検知方式としての評価をする必要がある。

(2) プロトコルの特性に着目する検知

Spectral Analysis⁽⁹⁾は、一定時間内にやり取りされる TCP プロトコルのトラヒックは、プロトコルの特性から傾向が予測できるという前提を持っている。そして、この検知方法を実装した機器に到着するパケット量の時間遷移を、PSD(Power Spectral Density)で分析すると、正常な TCP プロトコルだけで通信が行われている場合と、プロトコルの手順を守らない異常な通信が行われた場合を区別できるため、通常の TCP プロトコルだけの通信が行われている状態と異なる状態になると、攻撃が行われていると検知する。また、Wang's Method⁽¹⁰⁾は、TCP プロトコルでは、セッションが開始されてから終了するまでの間に二者間でやり取りされる SYN と FIN パケットの比率が 1 対 2 であることに着目し、その比率が異常な状態になったときに、異常な状態になっていると検知する。しかし、FIN パケットは必ずしも送信しないソフトウェアが現実には存在しており、SYN と FIN の比率が 1 対 2 から、どれだけ乖離した場合に異常なのかを決めるのは難しい。

〈4・3〉 攻撃元探索 前述のとおり、DoS/DDoS 攻撃には送信元アドレスを偽装したパケットが使われることが多く、攻撃元を見つけるために、攻撃の上流となるリンクをルータで特定し、それを何段階にも渡って繰り返すことが行われる。しかし、これを人手で実施するには時間がかかることなどから、効率的に方法が求められており、IP トレースバックと呼ばれる技術が検討されている。IP トレースバック技術から、2 種類の方法を以下に示す。

(1) マーキング方式

基本的な考え方としては、ルータを通過するパケットに逆探知のための情報を付加し、攻撃を受けているサーバなどでどの情報を分析することにより、攻撃元を突き止めようとする方法である。IP ヘッダの identification フィールドは、パケットのフラグメント時に利用されるだけのため、ここに逆探知に必要な情報を付加する方法が、Song⁽¹¹⁾、や Dean⁽¹²⁾によって考えられている。これらの方法は、IPsec の AH によるヘッダの認証が機能しなくなることや、

identification フィールドが IPv6 にはないため、他の方法を考える必要があるといった問題点が指摘されている。

(2) ダイジェスト方式

ルータでパケットの通過記録を残し、それをネットワークの複数地点から収集した上で、攻撃パケットが攻撃先へ到着するまでに辿った経路を分析する方法が、Snoeren⁽¹³⁾から提案されている。この方式の場合、パケットの通過を記録しておくために、パケットそのものを保持した場合、記憶容量が膨大になるため、IP パケットのヘッダの一部からハッシュ値を計算し、それを保持することで容量の削減を図っている。マーキング方式と比較すると、パケットに付加的な情報を加えることはないため、先に挙げた問題点は解決されることになる。

〈4・4〉 防御対策

(1) サーバでの対策

SYN Flood 攻撃に対するサーバでの対策の一つとして、SYN パケット受信後の処理を工夫し、攻撃に対する耐性を向上させようとする SYN Cookie⁽¹⁴⁾という技術がある。通常は、SYN パケットを受信後に SYN/ACK を返信すると、再度 ACK パケットを受信するまでの間、TCP のシーケンス番号を記録するためにメモリ領域を消費する。そこで、シーケンス番号をハッシュ関数で算出することで、メモリ領域に記録しておく必要がないようにすることで、メモリ領域の消費を無くすものである。しかし、ハッシュ関数の計算に CPU を利用する負荷は別途必要となる。

(2) ネットワークでの対策

表 1 に示したように、攻撃が発生した後の防御対策は、基本的にパケットフィルタリングか帯域の制限しかない。しかし、どのパケットに対して、どの地点で、どれだけの帯域制限や破棄を行うか、ということは攻撃ごとに千差万別であり、固定的に決めておくことは不可能である。

そこで、攻撃の検知、攻撃元の探索、防御という一連の機能をシステムとして構築し、攻撃に応じて必要な地点でパケットの破棄や帯域制限を試用とするアプローチをとっている研究に Pushback⁽¹⁵⁾、MovingFirewall⁽¹⁶⁾⁽¹⁷⁾がある。

両者の共通している考え方は、攻撃トラフィックが集中す

る攻撃先のサーバの近傍にあるルータなどのネットワーク機器で攻撃を検知し、その攻撃の情報を攻撃の上流のネットワーク機器に hop by hop で伝達することにより攻撃元を探知し、攻撃元近くの機器で対策を実施しようとするというものである。一方、大きな違いとしては、対策において、Pushback では攻撃によって帯域制限の値を調整するが、MovingFirewall では、帯域制限値の調整に加えて、攻撃パケットは破棄し、正規ユーザの通信パケットは帯域制限を解除するという正規ユーザの通信保護機構が加わっていることがあげられる。次章では攻撃検知から防御までを実施する DDoS 防御システムの典型的な例として、MovingFirewall について動作を詳しく述べる。

5. MovingFirewall の概要

〈5・1〉 ネットワーク全体での防御 MovingFirewall の動作シーケンスを図 6 に示す。

① MovingFirewall が DDoS 対策を開始するトリガーは攻撃の検知である。保護するサーバのネットワーク接続地点に設置されている MovingFirewall 装置が DDoS 攻撃を検知すると、攻撃を起こしているトラフィックからパケットの特徴となる識別情報を抽出する。そして、この識別情報を元に、同装置にて保護対象サーバへのトラフィック帯域の制限を開始する。

② 次に、同装置を始点として、攻撃元の探索を開始する。攻撃元の探知は、各 MovingFirewall 装置から隣接している MovingFirewall 装置へ攻撃の識別情報の伝達を行い、識別情報を受け取った MovingFirewall 装置が、さらに隣接している MovingFirewall 装置へも攻撃の識別情報を伝達する、という動作を繰り返し行う。このように、再帰的に攻撃元の探知を繰り返すことで、一番攻撃元に近い MovingFirewall 装置を特定することが可能である。これは、4.3 攻撃元探索で述べたルータでのリンク検査を自動化していることになる。

③ 探知した先の各 MovingFirewall 装置では、攻撃の識別情報を利用し分散して攻撃トラフィックを抑制する。この結果として、DDoS 攻撃トラフィックは、攻撃元の近くで局所

図 6 MovingFirewall の動作概要

Fig. 6. MovingFirewall overview.

図7 MovingFirewall における攻撃パケット制御

Fig. 7. Mitigating attack packets with MovingFirewall.

的に閉じ込められ、ISP のネットワーク全体で DDoS 攻撃を防ぐと共に、ネットワークに無用なトラフィックが流れて他の利用者へ悪影響を及ぼすことも防止する。

〈5・2〉 正規ユーザの保護 MovingFirewall の DDoS 攻撃防御機能では、先に述べた防御地点を分散させること加えて、攻撃パケットを遮断しながら正規ユーザのパケットは通過させるという適応型対策を実施する。

各 MovingFirewall 装置における適応型対策は、図 7 に示すように、“Normal”、“Suspicious”、“Malicious” という 3 種類のクラスに分けた処理である。異常を検知した直後は、異常の原因となった容疑トラフィックに対して“Suspicious”クラスで帯域を制限しながら、トラフィックの分析を行う。この結果として、攻撃をしているパケットと判別したもののについては、“Malicious”で破棄し、正常な通信を行っているトラフィックは“Normal”クラスに移行し帯域制限の対象から除外する。適応型対策では、トラフィックの転送をこのように動的に制御することにより、従来の DDoS 対策方法では発生してしまう「正規ユーザの遮断」を回避する仕組みになっている。

6. おわりに

この解説では、DoS/DDoS 攻撃の現状として、いくつかの有名な攻撃方法の概要と示すことで特徴を説明すると共に、攻撃対策の動向を、対策の実施箇所を 4 種類に、攻撃の発生前から発生後の防御までの技術を 4 種類に分類し、具体的な内容を示した。

これらから言える事は、DoS、あるいは DDoS 攻撃といっても様々な攻撃があり、対策は一種類だけでは十分ではないということである。また、それとあわせて、根本的な解決策が見出されていない攻撃も存在することを理解すべきである。

DoS/DDoS 攻撃は、ウイルスのように日々新種の攻撃が生み出されているわけではないが、現在確認されている攻撃を組み合わせただけでも、対策がさらに困難になることが予想される。今後は、エンドユーザ、ISP がそれぞれ単独で対策を実施するだけではなく、複数の ISP が連携して対策を実施することなども視野にいれていく必要があるだろう。

(平成 16 年 5 月 18 日受付)

文 献

- (1) CSI/FBI: “COMPUTER CRIME AND SECURITY SURVEY 2003”
- (2) D. Moore, G. M. Voelker, and S. Savage: “Inferring Internet Denial-of-Service Activity”, Proc. 10th USENIX Security Symposium, pp.9-22, Aug (2001)
- (3) 警視庁技術対策課サイバーテロ技術対策室: 「DDoS 攻撃の防御について」(2003)
- (4) 警視庁技術対策課: 「DoS/DDoS 対策について(検証)」(2004)
- (5) P. Ferguson and D. Senie: “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, IETF RFC-2827 (2000)
- (6) K. Park and H. Lee: “On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets”, Proc. of the ACM SIGCOMM’01, pp.15-26 (2001)
- (7) T. M. Gil and M. Poletto: “Multops: a data-structure for bandwidth attack detection”, USENIX Security Symposium (2001)
- (8) L. Feinstein: “Statistical Approaches to DDoS Attack Detection and Response”, DARPA research project
- (9) C.-M. Cheng, H. T. Kung, and K.-S. Tan: “Use of spectral analysis in defense against DoS attacks”, In Proceedings of IEEE GLOBECOM (2002)
- (10) H. Wang, D. Zhang, and K. G. Shin: “Detecting SYN flooding attacks”, IEEE INFOCOM (2002)
- (11) D. X. Song and A. Perrig: “Advanced and Authenticated Marking Schemes for IP Traceback”, IEEE INFOCOMM ’01 (2001)
- (12) D. Dean, M. Franklin, and A. Stubblefield: “An Algebraic Approach to IP Traceback”, NDSS ’01 (2001)
- (13) A. C. Snoeren, et. al: “Hash-Based IP Traceback”, ACM SIGCOMM ’01 (2001)
- (14) <http://cr.yip.to/syncookies.html>
- (15) R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker: “Controlling High Bandwidth Aggregates in the Network”, ACM SIGCOMM CCR, Vol. 32, No. 3, July (2002)
- (16) Eric Chen・柏 大・富士 仁・米澤明憲: 「Moving Firewall における DDoS 攻撃対策システムの評価」, 電子情報通信学会情報ネットワークシステム研究会予稿集, 信学技報, NS2002-121, pp.73-78, Sep. (2002)
- (17) D. Kashiwa, et.al: “Active Countermeasure Platform against DDoS Attacks”, IEICE TRANS. INF. & SYST. Vol. E85-D, No.1 (2003)

富 士 仁

(非会員) 1993 年東京理科大学工学研究科修士課程修了。同年、NTT に入社。ソフトウェアの品質管理・保証に関する研究に従事し Ph.D. 取得。現在、ネットワークセキュリティを中心とする研究に従事。2004 年日経 BP 技術賞受賞。電子情報通信学会、プロジェクトマネジメント学会等会員。情報流通プラットフォーム研究所主任研究員。

Eric Y. Chen

(非会員) 1997 年カナダ国 McGill University, Computer Science 学部卒業。2000 年同大学院 MBA 修士課程修了。1997 年、NTT に入社。東京大学大学院情報理工学系研究科在学中。情報流通プラットフォーム研究所社員。現在、ネットワークセキュリティおよびアクティブネットワークに関する研究に従事。2004 年日経 BP 技術賞受賞。IEEE Communications 会員。