2.1 DoS/DDoS攻撃観察日記(1) ～DDoSは身内からもやってくる～

専

高倉弘喜（名古屋大学）

前哨戦―騒ぎの前の静けさ

■ ボット駆除作戦開始

1週間前から準備していたボット感染マシンの一斉駆除を開始．対象ボットネットの指令サーバ（Command and Controlサーバと呼ばれている．以降，C&Cサーバ）リストを事前入手．さらに，各種セキュリティシステムの観測結果を集計．それを受けて，対外接続スイッチに，C&Cサーバとの通信を遮断するACL（Access Control List）の設定を一斉投入．並行して，ボット感染マシンの管理者に，当該マシンのキャンパスネットワークからの切り離し，アンチウイルスソフトでの駆除を依頼．

■ 作戦の目的

最近のボットやRAT（Remote Administration Tool, Remote Access Trojanと呼ばれることもある）といったマルウェアは以下のような機能を備えている．

- 複数のC&Cサーバを準備
  C&Cサーバを多重化し，通信中のC&Cサーバとの接続を遮断されても，直ちにバックアップ系に切り替えられる．
- 数種類のマルウェアの同時感染
  感染当初はアンチウイルスソフトで検出できないマルウェアも，時間経過に伴い，検出パターンが対応し，検出できる可能性は高まってくる．このため，数種類のマルウェアを同時に感染させ，そのうちの1つが駆除されても残りが機能を維持する，あるいは，未検出となる新たなマルウェアを外部から導入するようになっている．

確実な駆除を目指すのであれば，OSからのクリーンインストールが理想的な措置となるが，業務再開を急ぎたいユーザとしては，できれば避けたい．そこで，アンチウイルスソフトでの検査の後，暫定的に再接続を認める一方で，セキュリティシステムの監視を強化し，C&Cサーバへの接続などの不審な挙動を起こさないかを確認する．

なお，最近のキャンパスネットワークでは，グローバルIPアドレスでインターネットに直結されている一部のサーバマシンを除けば，ほとんどのマシンがブロードバンドルータ（以降，BBルータ）によるNAT（Network Address Translation）を介して接続されている．このため，ボット感染マシンの切り離しでは，BBルータではなく，その配下のマシンが対象となる．

■ 不吉な前兆（今にして思えば…）

感染マシンの切り離しをもって，夕方までにはボット駆除作戦はほぼ完了．C&Cサーバへのアクセスも観測なし．しかし，22時を過ぎたあたりから，TCP SYNやUDP，ICMP echo requestによるスキャンが増加．気のせいか，スキャンに対する応答パケットが多いように見える．

このときは，ボット駆除に気付いたボットネット指令者（複数のPCを羊の群れのごとく操ることから「羊飼い（Herder）」と呼ばれている）が，感染マシンの接続確認や新たな感染候補マシンの探索を行っていると判断した．過去の経験から，報復のDDoS（Distributed Deny of Service）攻撃はあり得ると想定していたが……．

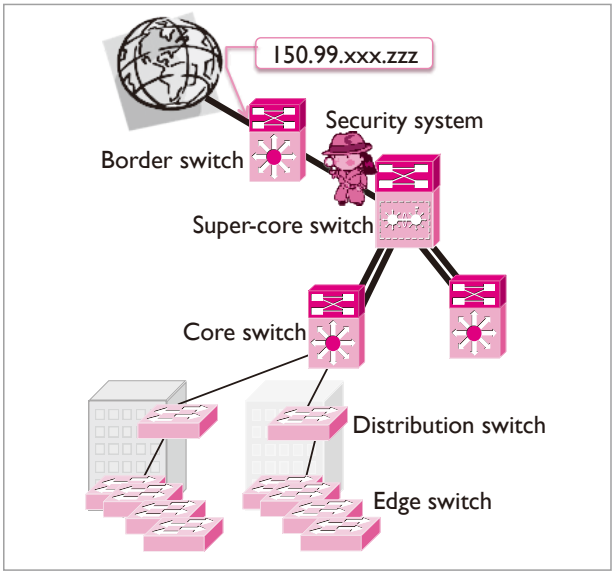

図-1　キャンパスネットワークの構成

キャンパスネットワーク構成

図-1 にキャンパスネットワーク構成の概略を示す．筆者が所属する大学のネットワークも，一般的なネットワークと同様にツリー構成となっている．太線は 10Gbps 回線，細線は 1Gbps 回線をそれぞれ表している．

キャンパスネットワークは Border スイッチ（Cisco Catalyst6506E．以降，対外接続スイッチと呼ぶ）を介してインターネットに接続されている．対外接続スイッチでは BGP（Border Gateway Protocol）4/BGP6 により外部と経路情報の交換を行っている．バックボーンネットワークは，対外接続スイッチ，Super-core スイッチ（Catalyst6506E），Core スイッチ（Catalys4500E）の L3 スイッチで構成．L2 スイッチとして，建屋の入口に Distribution スイッチ（Catalyst3560G）を，建屋内のフロアごとに Edge スイッチ（Catalyst2960G）を設置している．また，対外接続スイッチと Super-core スイッチ間のトラフィックは，評価機等を含め，IDS（Intrusion Detection System）など 10 種類のセキュリティシステムが監視している．

本学のネットワークの場合，1Gbps 程度の DoS/DDoS 攻撃では，バックボーンネットワークへの影響は軽微である．一方，建屋内の通信への影響は注意が必要となっている．最近の L2 スイッチは耐久性が向上し，昔のように DoS/DDoS 攻撃で L2 スイッチがダウンするネットワークヒューズ[1] 現象は起こさなくなった．そのため，各建屋への回線と建屋内の回線でも 1Gbps が淀むことなく流れ込み，建屋内で通信障害を引き起こすことが懸念される．

DDoS 攻撃―想定通り

■ ブロードバンドルータ被弾

その夜，そのまま残置した BB ルータへの TCP SYN Flood，UDP Flood，ICMP Flood による DDoS 攻撃が発生．攻撃はボット駆除を実施した数個の IP アドレスに集中．DDoS の規模は全体で 1Gbps 程度．発信元 IP アドレスによれば，発信元は南米に大きく偏っている傾向はあるが，世界各地に分散．TTL（Time To Live）の揃い具合から見て，発信元 IP アドレスの詐称と推定．約 10 分周期で攻撃元の一斉切り替え．攻撃は 30 分程度継続．休息をはさんで攻撃再開の繰り返し．

■ DDoS 攻撃の特徴

今回のフラッディング型の DDoS 攻撃は，攻撃対象となったマシン（BB ルータ）のダウンかキャンパスネットワークが輻輳状態に陥るのを狙ったものである．

TTL 値は OS ごとに初期値が異なる．したがって，24 ビットネットマスク単位でネットワークに所属する攻撃元のパケットを調べて，その TTL 値が揃っていれば，1 台のマシンが IP アドレスを詐称している可能性が高い．DDoS 攻撃の規模が 1Gbps と安定していること，攻撃元の切り替え周期が世界規模で同期していること，発信元 IP アドレスは全体的には世界中に分布しているが，均一ではなく，24 ビットネットマスク単位のブロックに偏っている傾向があること，大学からの traceroute の結果ではあるが☆1，攻撃元と大学の経路が分散しており，インターネット中の特定の回線にトラフィック集中

☆1 往路と復路で異なる経路となるのは珍しくない．

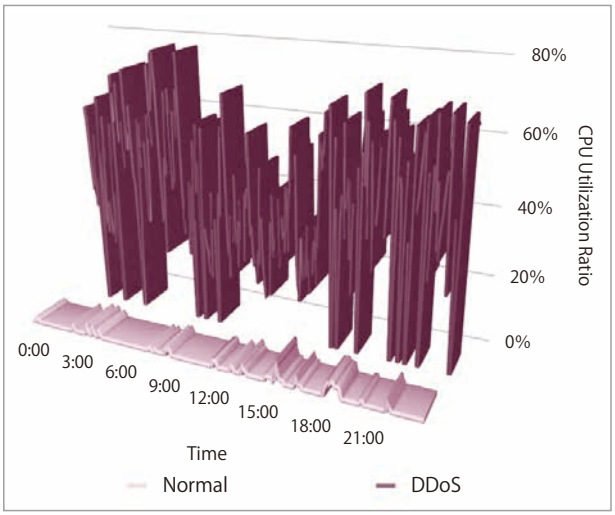

図 -2　CPU 使用率の変化

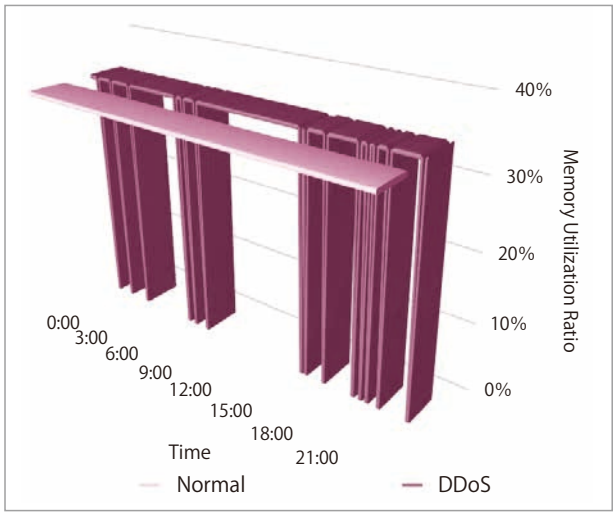

図 -3　メモリ使用率の変化

が生じないようにしていることから，DDoS 請負業者による攻撃かもしれない．

DDoS 請負業者は，攻撃の品質保証を売りにしているところが多く，利用者の要求を満たせなかった場合は料金を請求しないなど，顧客満足度を非常に重視している．このため，ボットネットを用いて攻撃する際，攻撃元から攻撃先に至る経路において，一部の回線やネットワーク装置に過度の負荷がかからないようにし，攻撃パケットが効果的に着弾するよう配慮している．また，発信元 IP アドレスを詐称する場合でも，ボット感染マシンが自身の繋がっているネットワークセグメントで使用可能なアドレスすべてを詐称するのではなく，少数のアドレスに絞ることで，当該セグメントの管理者に DDoS 攻撃の参加を察知されにくくする．

前述の通り，建屋に数百 Mbps の DDoS 攻撃パケットが流入すれば，「ネットワークが重く感じる」等それなりの影響を受けることになるので，ユーザから苦情がくる前に対策を，と考え始めたとき，攻撃の挙動が一変した．

対外接続スイッチダウン

■ 未使用アドレスへの分散攻撃

攻撃元 IP アドレスはそのままだが，流量が減少．一方で，攻撃先の IP アドレスが次々と変化．dig コマンドで攻撃先の IP アドレスのホスト名を確認したが，軒並み該当なし．試しに ping を打っても無応答．さらに，駆除作戦に関係しなかったネットワークセグメントにも，DDoS 攻撃が及ぶようになってきた．しかし，その大部分が未使用の IP アドレスであった．「DDoS 攻撃の効果が出ないので自暴自棄になったか？」という印象を持った．

その直後に，キャンパスネットワークに異常発生．間欠的に，対外接続スイッチが機能停止．当該スイッチに telnet しようとするが応答劣化．ネットワーク分析管理システム☆2 で調査．CPU 使用率，メモリ使用率ともに異常を確認．

■ CPU・メモリ使用率の異常

図 -2 に DDoS 攻撃時と平常時の対外接続スイッチの CPU 使用率の 1 日の変化を，図 -3 に同じくメモリ使用率の 1 日の変化を示す．両図とも，手前のピンクが平常時，奥の紫色が DDoS 攻撃時を示している．

平常時の CPU 使用率を見ると，散発的な負荷上昇はあるが，それでも 10% を超えることはない．これに対し，DDoS 攻撃時は使用率が最小 0% から最大 78% の間を激しく乱高下した．0% に落ち込む現象は 14 回発生し，1 回あたりの継続時間は 10 分

☆2 http://www.fivefront.com/products/genie/atm6000/overview.html

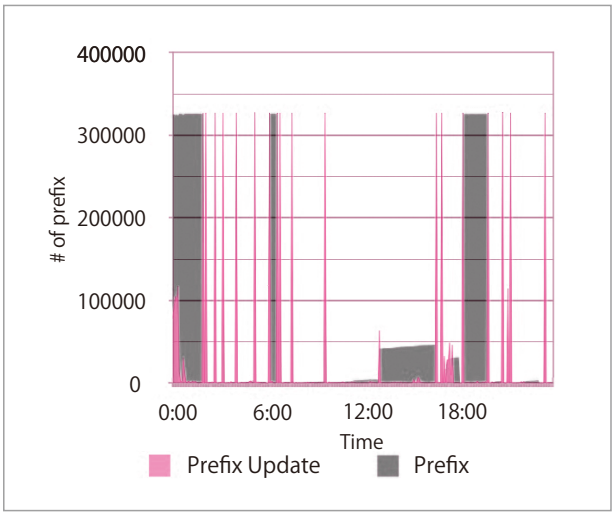

図 -4　BGP 経路情報数の変化

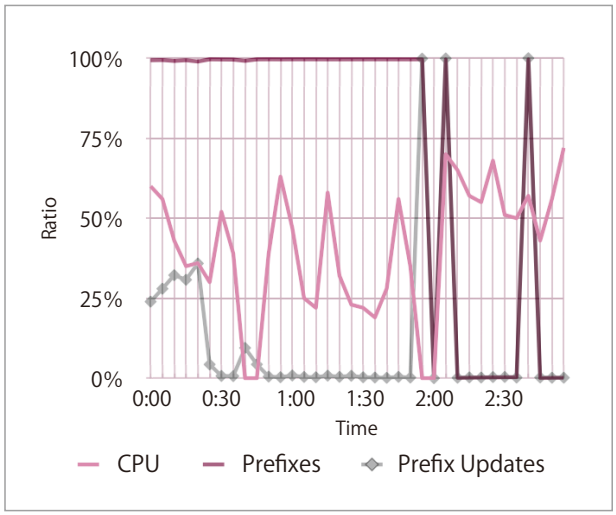

図 -5　CPU 使用率と経路情報変化率

未満であった．

一方，DDoS 攻撃時のメモリ使用率は CPU 使用率とは異なる傾向を示した．平常時，DDoS 攻撃時ともにメモリ使用率は 34% を維持していた．ただし，CPU 使用率が 0% になるときに限りメモリ使用率も 0% に急落し，CPU 使用率が上昇すれば 34% に戻る現象を繰り返した．このことから，CPU 使用率／メモリ使用率が 0% に急落した現象は，実際には対外接続スイッチが CPU の過負荷によりネットワーク分析管理システムへ SNMP（Simple Network Management Protocol）応答を返せなくなったと考えられる．

■ 断続的な通信速度の低下

対外接続スイッチの過負荷に伴い，学外との通信に支障発生．通信中セッションは応答性劣化．新規セッションは通信開始までの待ち時間増．ping/traceroute 等での RTT（Round Trip Time）の大幅遅延と RTT のばらつきが増大．

図 -4 に，対外接続スイッチにおける BGP の Prefix 数の変化を示す．ピンクは Prefix 更新数（新たに受信した Prefix 数）を，灰色は対外接続スイッチの保持 Prefix 数をそれぞれ示す．なお，平常状態で，対外接続スイッチの保持 Prefix 数は約 32 万であった．

図 -4 より，

- ほぼすべての保持 Prefix を瞬時に喪失
- 喪失数直後に Prefix 更新の試行

を繰り返していることが読み取れる．ほとんどの場合で，喪失した Prefix 情報に相当する更新 Prefix 数を直ちに取得して回復しているが，それを維持できないことが分かる．特に，12:00 ～ 18:00 にかけては，喪失した Prefix 情報を一度の更新では取得できず，さらに，段階的な回復を試みるも，遅々として進まない状況に陥っていることも読み取れる．

図 -2, 3 に関して述べたように，CPU 使用率が 0%，すなわち，SNMP の応答がなくなった時間は 10 分未満であることから，図 -4 における保持 Prefix 情報の喪失は，対外接続スイッチが経路情報を本当に失ったことを意味する．

図 -5 は，DDoS 攻撃中の観測結果から 00:00 ～ 02:55 の間を抽出したものである．ピンクは CPU 使用率（図 -2），紫色は対外接続スイッチの保持 Prefix 数（図 -4），灰色は更新 Prefix 数（図 -4）を示している．ここでは，比較を容易にするため，保持／更新 Prefix 数については，平常時の 32 万 Prefix に対する比率で表している．なお，02:00 以降については，保持 Prefix 数と更新 Prefix 数がほぼ同じ値となり，重なってしまっている．

図 -5 から，00:00 ～ 01:55 の間は，CPU の高負荷が続き，更新 Prefix 数も非常に多い時期があることが読み取れる．ただし，この時点では，保持

Prefix 数にわずかな変動が見られるだけであり，保持 Prefix 情報の減少を更新 Prefix で補えていたと判断される．

01:55 以降の結果から，経路情報を失ったときの挙動を読み取ることができる．

[01:55] CPU 使用率が 0% に急落．
[02:00] 保持 Prefix 数も急落（実際には 0.01%）．
[02:05] ほぼ 100% の更新 Prefix により
保持 Prefix 数も 100% に回復．
[02:10] 再び保持 Prefix 数が急落（0.1%），
その後，徐々に更新 Prefix を受信
（5 分間あたり 400 ～ 1200Prefix）．
[02:35] 保持 Prefix 数が若干回復（0.3% 程度）．
[02:40] ほぼ 100% の更新 Prefix 数を受信し，
一瞬回復．しかし，再度急落（0.1%）．

いずれにしても，CPU 過負荷との因果関係があることは明らかであった．

DDoS 攻撃の犯人は？

■ 攻撃元の謎

まず突き止めなければならないのは，攻撃元がどこなのか？　ということであった．対外接続スイッチでは経路情報を失っているはずなのに，学外からのパケットは流入している．インターネット上では本学への経路情報は有効なままということか？　モバイルルータを使って確認すると，大学への経路情報は消えていない．しかし，インターネット回線の流量は平常時と変わらず，対外接続スイッチが DDoS 攻撃を受けているとは思えない．

■ わけが分からないよ

セキュリティシステムで何かを検知していないかと思い，監視画面を確認．4 種類の IDS すべてで ICMP Flood の警報を発している！　ICMP パケットの数，毎秒数万？　ちょっと待て，監視ポイントは図 -1 の対外接続スイッチと Super-core スイッチ間のはず．ということは，学内から対外接続スイッチが攻撃を受けているのか？　文字通り滝のように流れる警報を眺めていて，ふと気になった 1 つをチェックする．

SRC: 133.6.aaa.bbb
DST: 150.99.xxx.zzz
ICMP redirect
133.6.aaa.ccc to host 133.6.aaa.ccc

思わず呟いてしまった．「わけが分からないよ」ICMP パケットの発信元は学内の 133.6.aaa.bbb，送信先は対外接続スイッチの外向けインタフェースの IP アドレス 150.99.xxx.zzz だ（図 -1）．つまり，学内のマシンが対外接続スイッチに経路変更を指示していることになる．しかも，「133.6.aaa.ccc 宛のパケットは 133.6.aaa.ccc に送った方が最適」という指示！？　気を取り直して，別の警報をチェック．

SRC: 133.6.ddd.eee
DST: 133.6.ooo.ppp
ICMP redirect
133.6.ddd.fff to host 133.6.ddd.fff

なんで，学内のマシン間の通信が監視ポイントを通過してるんだ？　しかも，経路変更の指示はやっぱり意味不明．さらに，警報を眺めていると，対外接続スイッチが発信元となっている ICMP パケットも攻撃として検知されている．

SRC: 150.99.xxx.zzz
DST: 133.6.fff.ggg
ICMP time exceeded in-transit

対外接続スイッチの外向きインタフェースが学内へパケット投げとる？　IP アドレスの使用状況を確認．133.6.aaa.ccc，133.6.ddd.fff，133.6.fff.ggg のいずれもが使用されていない．

■ 見覚えのある IP アドレス

呆然と警報を眺めていて，ふと気がついた．最適経路を指示している学内の IP アドレス，ボット駆除作戦にかかわった BB ルータが含まれている．さらに，経路変更の対象となっている IP アドレスは，「未使用アドレスへの分散攻撃」で見かけたものだ！

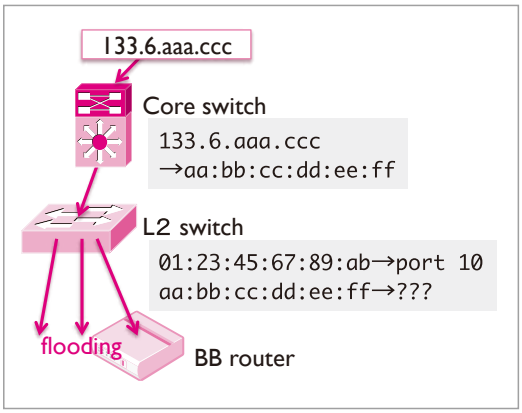

図 -6　MAC アドレス未学習時のフラッディング

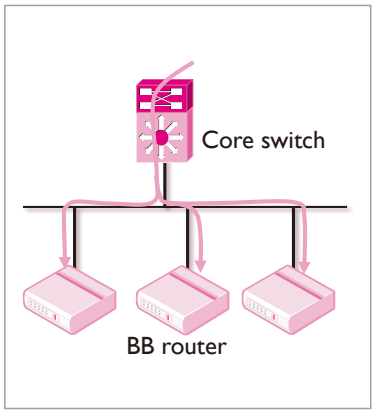

図 -7　バス化したネットワークセグメント

原因究明

■ 家庭用ブロードバンドルータ

問題を起こしている BB ルータを確認．家庭用 BB ルータ．パケットキャプチャの許可を得て，BB ルータの上流側で数分間 tcpdump 実行．直ちに持ち帰って解析開始．

■ フラッディング？

キャプチャデータに不自然な状況を確認した．直上の L2 スイッチから，BB ルータのものではないグローバル IP アドレス宛のパケットが大量に流れ込んでいる．このネットワークセグメントのすべての IP アドレス宛のパケットが流れてきているようだ．

L2 スイッチは，MAC アドレステーブルを参照することで，必要なポートにのみイーサフレームを転送する☆3．しかし，MAC アドレス学習のタイミングのズレなどにより，L3 スイッチの arp テーブルでは IP アドレス -MAC アドレスの対応を保持しているのに，L2 スイッチでは該当する MAC アドレスが未学習になってしまう図 -6 のような状況が発生する．この場合，L3 スイッチは arp request を出すことなく，イーサフレームを送出する．一方，MAC アドレスを学習するチャンスが得られなかった L2 スイッチは，転送先ポートを決定できず，イーサフレームを全ポートに転送するフラッディングを行う．この際，別の VLAN ID が設定されているポートにもフラッディングしてしまう癖がある☆4．

フラッディングが多発していることは，L2 スイッチで MAC アドレス学習が機能しておらず，このセグメントは，図 -7 のようなバス型ネットワークの状態になっていることを意味する．つまり，1 つのパケットがセグメントすべての機器に配られることになる．BB ルータも含めて．

■ 上流に投げ返す BB ルータ

さらに解析は続く．フラッディングされた 133.6.aaa.ccc 宛のパケットを BB ルータが投げ返している！　よく見ると，パケットの送信者 IP アドレスはそのままなのに，イーサフレームの送信者 MAC アドレスは BB ルータのものに書き変わっている．

分かった，こういうことだ！　IP アドレス -MAC アドレスの対応付けができている Core スイッチは，到着した IP パケットについて，発信元 MAC アドレスを自身のものに書き換え，対応付けを参照した送信先 MAC アドレスを指定してイーサフレームを送出する．しかし，このセグメントはバス化しているため，図 -7 のように，ほかの BB ルータにもイーサフレームが到着してしまう．

BB ルータが管理するネットワークはプライベート IP アドレスを使用しており，本来は，このイーサフレームを受け取らない．しかし，図 -8 のように，BB ルータは誤って受け取ってしまうようだ．しかも，イーサフレームを転送できないため，上流側

☆3　さらに，最近のハイエンドな L2 スイッチは，MAC アドレス学習時に IP アドレス情報も取得し，L3 層も参照して機能するようになっている．
☆4　この癖を活用すると，regeneration TAP なしで多くのミラー出力を得ることができる．

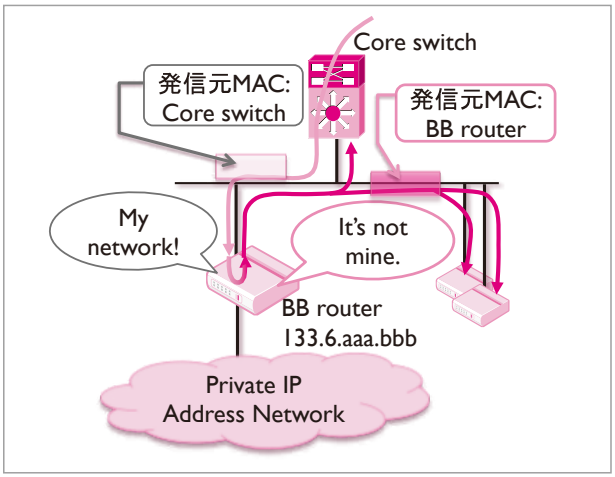

図 -8　BB ルータによるパケット異常転送

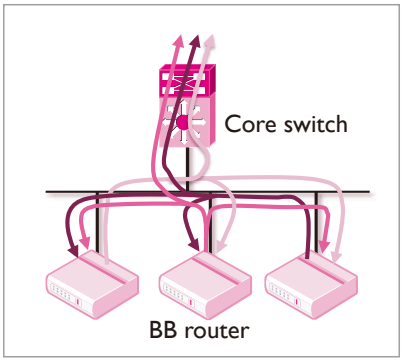

図 -9　イーサフレームの増殖

へ投げ返している．投げ返した先には，Core スイッチだけでなく，複数台の BB ルータが接続されている☆5．

その結果，図 -9 のように，異常動作をする BB ルータすべてでこの状況が発生してしまい，1 つのイーサフレームは，発信元 MAC アドレスと TTL だけが変更されたイーサフレームとなって，BB ルータの台数だけ増殖することになる．さらに，増殖したイーサレームを受け取った BB ルータは，TTL 値が 0 でなければ，再び上流へ投げ返す，という動作を繰り返す．この状態に陥ると，L2 スイッチでの MAC アドレス学習は阻害され続け，セグメントのバス化が延々と続くことになる．

■ 対外接続スイッチとのピンポン

この状況下では，Core スイッチの L2 機能にも

☆5　実際には十数台の BB ルータが存在した．

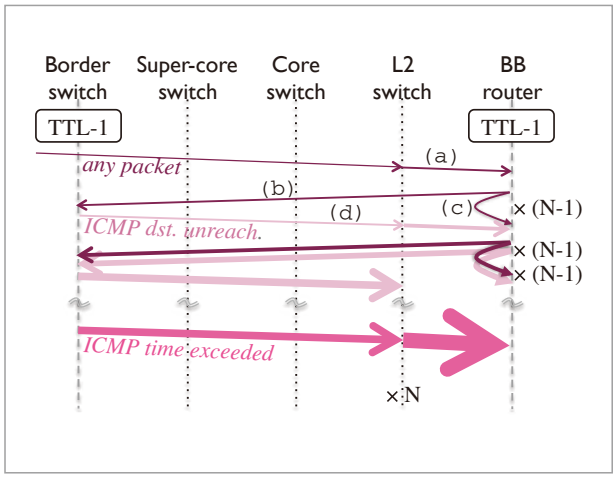

図 -10　対外接続スイッチとのピンポン増幅

影響が出る．図 -9 に示す通り，セグメントから上がってきたパケットは，転送先が見つからず，かつ，前述の VLAN ID を超えたフラッディングにより，バックボーンネットワークやほかのセグメントに流れ込む．バックボーンへ流れ込んだパケットは，最終的に対外接続スイッチに到達する．

一般に，発信元 IP アドレスを詐称したパケットが外部に漏れ出ないように，対外接続点において Egress filtering を行う．本学の場合も，対外接続スイッチの外向けインタフェースに Egress filtering を設定している．今回これが，事態を悪化させる要因となった．

学外から到達したパケットは，図 -10 のように，各 L3 スイッチを経て，L2 スイッチに到達する．バス化したセグメントに問題となる BB ルータが N 台存在したとすると，L2 スイッチでフラッディングされ，BB ルータに到達するたびにパケット数が N 個に増殖することになる（図 -10 の (a)）．次に，図 -9 で示したセグメント内での投げ返しにより，N 個のパケットが直接 Core スイッチへ向かい（図 -10 の (b)），N-1 個のパケットが BB ルータ間で交換される（図 -10 の (c)）．

対外接続スイッチに届いたパケットは Egress filtering により，『ICMP unreachable host unreachable』，『ICMP unreachable port unreachable』を送出する（図 -10 の (d)）．この ICMP パケットの発信元 IP アドレスは，対外接続スイッチの外向け

インタフェースのものとなり，観測結果と一致する．

さらに，セグメント内部での折り返しを繰り返すたびに，パケットの TTL 値は減少する．その結果 TTL 値が 0 になると，パケットは破棄される．L3 スイッチや BB ルータでは，TTL 値が 0 になれば，『ICMP time exceeded in-transit』を送信する．この際，TTL 値をセットし直すため，セグメント内での折り返しが再発することになる．また，バックボーンネットワークに漏れ出たパケットに対する ICMP パケットが BB ルータに到達すると，BB ルータは『ICMP unreachable host unreachable』,『ICMP redirect（133.6.aaa.ccc to host 133.6.aaa.ccc)』を送信する．これも観測結果と一致する．で，これを受け取った……（以降，ピンポンの繰り返し）．

■ ICMP のソフトウェア処理

ハイエンドなルータや L3 スイッチでも，ICMP の処理は苦手である．ICMP の type のうち，利用頻度が低いものはソフトウェア処理となる．ソフトウェア処理の場合，毎秒数十パケットの処理能力しかない．問題となった ICMP type のほぼすべてがソフトウェア処理の対象であった．これらのパケットが毎秒数万の規模で対外接続スイッチに押し寄せ，当該スイッチの CPU 資源を食い潰した．

■ VLAN インタフェースの罠

ネットワークから出てはならないパケットを抑止するために，Egress filtering を実施する．一般には，対外接続スイッチに設定し，自組織内のネットワークセグメントには設定しない．とはいえ，この現象を止めるにはこれしかないと判断し，前職の経験[1]をもとに Egress filtering を検討した．しかし，今回のようなフラッディングでは役に立たなかった．

図 -11 に物理インタフェースと VLAN インタフェースの仕組みの違いの概要を示す．右側の物理インタフェースでは，L3 層がパケットを直ちに処理する．したがって，RACL（Router Access List Control）で入力／出力を区別したアクセス制御を設定でき，Egress filter は機能し，別セグメントにパケットが漏れ出ることを阻止できる．

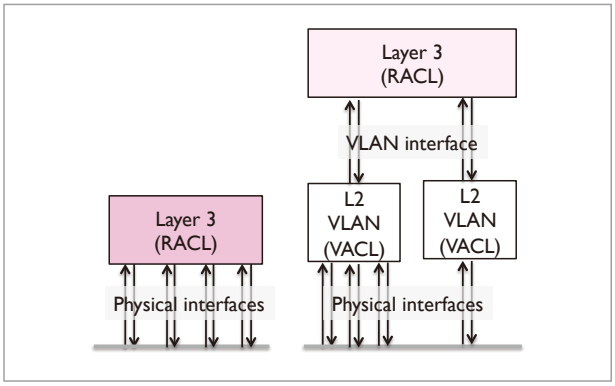

図 -11　Access List Control の違い

一方，左の VLAN インタフェースでは，L2 層で処理できないパケットのみ L3 層に送られる．このため，ある VLAN から別の VLAN にパケットが L3 層で転送される場合に限って RACL が機能する．一方，フラッディングは L2 層が処理するため，L3 層は関与できない．したがって，RACL は Egress filter として機能しない．VLAN 内でフィルタリングをする VACL（VLAN ACL）はあるが，VLAN からの出力とは物理インタフェースへの出力（図 -11 の下向き矢印）と VLAN インタフェースへの出力（上向き矢印）の両方を意味することになり，結果として BB ルータ自身の IP アドレスでの VLAN 内通信を拒否する設定しかできないため，BB ルータの正常な通信も遮断してしまう．

■ 暫定回避策

根本的な対策は BB ルータの撤去，あるいは，ファームウェア改修しかない．そこで，メーカと相談☆6．とりあえず，暫定ファームウェアの提供を受ける．同時に，対外接続スイッチで，問題を起こしているセグメント限定で，ICMP パケットを返さない設定に変更．

本件から学んだこと

家庭用 BB ルータの多くは，PPPoE（Point-to-

☆6 後日，正式なファームウェアが公開され，問題は解決した．

Point Protocol over Ethernet）等のインターネットサービスプロバイダ（ISP）接続での利用を想定した設計となっている．今回の主役となったBBルータのWAN（Wide Area Network）側インタフェースは，ネットワークセグメントのIPアドレス宛の通信すべてに応答するようになっていた．一方で，大学のような環境では，1つのセグメントのネットワーク領域が/20～/26マスク程度となっていることが多い．このようなセグメントに，BBルータを多数接続した結果，それぞれのBBルータはセグメント全体が自身の配下にあるものとして機能し，異常な挙動を起こすことになった．

今回，ボット撲滅作戦の報復として，BBルータが設置されたセグメントに対して，未使用アドレスへのDDoS攻撃が観測された．おそらく，その際に，このような挙動を示すBBルータの存在に気づかれ，悪用されたものと推定される．

このDDoS攻撃は，複数台のBBルータが設置されたセグメントに数秒に1パケットを送信するだけで成功する．1パケットを送れば，後は，内部でパケットが増殖し続け，ネットワークを自滅させることができる．特に，未使用IPアドレスにパケットを送れば，BBルータがCoreスイッチのarp requestに応答してしまい，CoreスイッチとL2スイッチのMACアドレス学習のタイミングのずれを引き起こしやすくなる．DDoS攻撃による影響が間欠的な機能停止にとどまったのは，対外接続スイッチとBBルータがピンポンに耐えきれずに一瞬停止してしまい，その際に増殖したパケットが消滅したからであった．

このように，通常の想定とは異なるDDoS攻撃を受けることもある．今回の事例もそうであるが，内部からの攻撃を受けた場合，2009年に韓国で発生した77DDoS[2]のようにサーバだけでなく，広範囲にわたる障害になる恐れがある．想定外の事態を想定することは難しく，柔軟な対応をいかに迅速に取れるかが問われる時代になったと考えられる．

参考文献

1) 高倉弘喜，江原康生，宮崎修一，沢田篤史，中村素典，岡部寿男：安全なギガビットネットワークシステムKUINS-IIIの構成とセキュリティ対策，電子情報通信学会論文誌B，Vol.J86-B No.8，pp.1494-1501（2003）．
2) International Workshop on DDoS Attacks and Defenses, http://caislab.kaist.ac.kr/77ddos/

（2012年12月28日受付）

■高倉弘喜（正会員） takakura@itc.nagoya-u.ac.jp

1990年九大卒業，1992年同修士課程修了，1995年京大博士課程修了，同年奈良先端助手，1997年京大講師，2000年同大助教授，2010年名大教授（現在に至る）．情報セキュリティ，次世代ネットワークの研究に従事．博士（工学）．電子情報通信学会，地理情報システム学会，システム制御情報学会，ACM各会員．