研究論文

鳴門教育大学情報教育ジャーナル No. 8 pp. 39-42 2011

ウイルススロットリングを用いたウイルス検知の試み

曽根直人*，佐藤知津**

コンピュータウイルスによる感染被害は社会問題にもなっており，学内でも多く報告されている。情報基盤センターでは端末にウイルス対策ソフト導入するほか，全学的に対策ソフトのライセンスを提供することによりウイルスの検出，駆除を行っている。しかしまだ学内ではウイルスに感染した PC が持ち込まれ，学内 LAN を介して感染活動を行っている場合がある。本稿ではそのような PC を発見し，ウイルスを駆逐するため，コアスイッチに備わるウイルススロットリング機能を用いたウイルス検知の試みについて報告する。

［**キーワード**：ウイルススロットリング，ウイルス検知，トラフィック監視］

1. はじめに

コンピュータウイルスやボットなどのマルウェアはネットワークや USB メモリを介して脆弱性の残っている PC に感染が拡がる。脆弱性が放置されたままの PC であれば，ほんの数分間インターネットに接続することで感染すると言われている。従来より，情報基盤センターではウイルス対策ソフトをセンターが管理する端末室の PC に導入するほか，希望のあったユーザにも対策ソフトを導入していただくことでウイルス対策を行っていた。このような対策により，セキュリティ意識の高いユーザはウイルス感染を防止することができたが，そもそもコンピュータウイルスに関する意識の低いユーザに関しては対策ソフトの導入による予防効果が見込めない問題があった。その結果，ウイルスに感染した PC が学内 LAN に接続され，他の PC へ感染活動を繰り返すような状況もしばしば発生した。

このように，学内ネットワークには多様な管理体制の PC が接続されており，その中には脆弱性への対応が十分なされていないものもある。それらがウイルスに感染してしまい他の PC への感染活動を行うことは学内 LAN のユーザにとって多大な迷惑行為となる。そこで情報基盤センターでは従来の端末に対策ソフトを導入して感染を防止することに加えて，ネットワークを観測することにより，ウイルスの活動と思われる挙動を検知し，感染が疑われる PC の利用者へウイルス対策を行うように連絡を行う取り組みを試みた。本稿ではこの試みについての報告を行う。

2. ウイルススロットリング

2.1. ウイルススロットリングの概要

ウイルススロットリングとは，HP 社製の L3 スイッチの一部製品にて提供されるセキュリティ機能の一つである。本学 LAN においてコアスイッチとして利用している HP 社製 8212zl スイッチはこの機能に対応しており，今回はコアスイッチにてウイルススロットリングを行った。ウイルススロットリングの原理はウイルスが新たな感染先を求めて短時間に多くの異なる IP アドレスへ通信を試みる特徴的な通信を検知し，通信を遮断することである。実際には単位時間当たりに特定の端末が一定の閾値を超える異なる通信相手へのアウトバウンド IP コネクションを確立しようとすると，その通信をウイルスによるものと見做し，以後一定時間その端末からの通信を遮断する動作を行う。設定により，閾値や検知時の対応（警告（notify-only），一定時間通信を遮断（throttle），検知後の通信をすべて遮断（block））を変更できる。

2.2. 設定

本学の学内 LAN 構成を図 1 に示す。このように本学の学内 LAN はスター型の構成となっており，全てのトラフィックは基本的に 1 台のコアスイッチにてルーティング処理されている。そのため，コアスイッチ上でウイルススロットリング動作を有効にすることで，学内 LAN に接続された端末が感染し，ウイルス感染的な挙動を効率よく監視できる。

コアスイッチではウイルススロットリングを行うポートおよび感度を設定する。設定可能な感度を表 1 に示す。

表 1　ウイルススロットリングの感度設定

感度	接続先閾値	ペナルティ
low	54/0.1 秒	30 秒未満
medium	37/1 秒	30～60 秒
high	22/1 秒	60～90 秒
aggressive	15/1 秒	90～120 秒

* 鳴門教育大学 大学院 自然・生活系教育部／情報基盤センター
** 鳴門教育大学 情報基盤センター

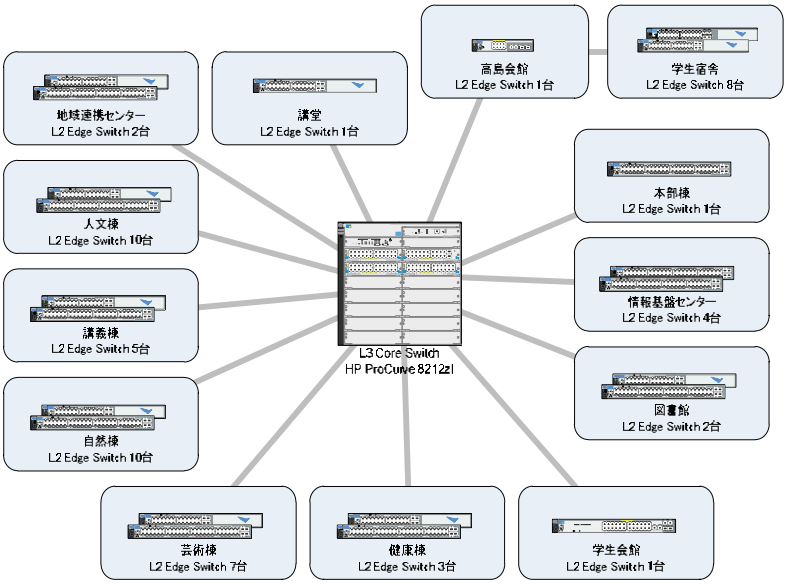

図 1　高島地区学内 LAN 構成

コアスイッチでのウイルススロットリング監視は，対象ポートとして各棟のエッジスイッチが接続されたポートを指定し，感度は low，検知時には一定時間遮断を行う throttle を設定している。検知時の対応として throttle を指定しているのは，block では誤検知時に利用者へ与える不利益が大きく問題があると判断したためである。

ウイルススロットリングにより検知されたホストはイベントログ（syslog）に記録されるほか，snmptrap により警告を発信することができる。図 2 に実際にウイルススロットリングが発生した際のイベントログを示す。

```
I 01/12/11 20:30:00 00806 connfilt: AM1: Src IP
160.204.103.253 unblocked
W 01/12/11 20:29:19 00695 connfilt: AM1: Src IP
160.204.103.253 throttled, port
```

図2　ウイルススロットリング発生時のイベントログ

3.　感染 PC の追跡

ウイルススロットリングの対象となった PC は throttle により一時的な接続制限のペナルティを受ける。しかし検知された通信がウイルスによるものであれば，原因となったウイルスの駆除といった対応が必要となる。そのためには，対象となった PC を追跡し，PC 管理者に対してウイルス感染の確認，今後の予防策についての依頼などを行う必要がある。

3.1.　追跡手法

ウイルススロットリング発生時のイベントログからは，

- 事象発生時刻
- 対象 PC の IP アドレス

の情報しか得られない。学内 LAN は複数の VLAN に分割され，それぞれ DHCP によるアドレス割り当てを行っている。そのため IP アドレスの情報のみから所有者や設置場所を求めることが困難である。そこで，対象 PC の MAC アドレスを用いて追跡することを考えた。スロットリング発生時にコアスイッチの ARP テーブルを参照することで該当 PC の MAC アドレスを求めることができる。MAC アドレスが判明すればエッジスイッチを辿り該当 MAC アドレスが接続されているポートを突き止めることができる。ポートが分かれば学内 LAN の配線記録から接続された部屋番号を求めることができる。当初，これらの処理は telnet などを利用し手動で行っていた。しかし複数のコマンドを実行するため非常に煩雑であり，さらに検知直後に追跡を開始しなければ ARP テーブルから該当 MAC アドレスの情報がすでに削除されている場合もあり，追跡に失敗することもあった。検知直後に追跡を行うために現在は ruby スクリプトにより追跡を自動化している。rsyslog にて virus throttle のログを受信した場合に追跡スクリプトを起動している。

3.2.　追跡の自動化

自動化された追跡処理の流れを示す。

1. コアスイッチによりウイルススロットリングが検知されると syslog サーバに検知メッセージが送られる。
2. syslog サーバでは送られたメッセージを rsyslogd により処理している。rsyslogd では拡張機能を利用し，メッセージに特定の文字列が含まれていた際に追跡用スクリプトを起動する。
3. 追跡用スクリプトは L3 スイッチの ARP テーブルから検知された PC の IP アドレスに対応する MAC アドレスを求める。次に得られた MAC アドレスが L3 スイッチのど

のインタフェースに接続されているか確認する。L3 スイッチではインタフェースの description に接続先エッジスイッチの IP アドレス情報を設定しているため，次にそのエッジスイッチに対して MAC アドレスがどのインタフェースに接続されているか確認する。エッジスイッチの各インタフェースの description には接続先の部屋番号を設定している。そのため，接続インタフェースが分かれば部屋番号を求められる。

4. 得られた結果は管理者にメールで送信する。

スイッチからの情報収集には SNMP を利用している。PC の追跡を自動化したことにより，昼夜を問わずスロットリング対象の PC がどの部屋で利用されていたのかを把握することができるようになった。

3.3. ウイルススロットリング検知の連絡

情報基盤センターシステム分野担当者はスクリプトにより報告される部屋番号から，部屋の管理者もしくはコース長あてにウイルススロットリング検知のお知らせをメールにて行っている。お知らせメールでは該当 PC の MAC アドレスや検知時刻といった情報とともに，

- 対象パソコンの特定
- ウイルスチェック
- 不必要なソフトウェアのアンインストール
- 情報基盤センターへ対応作業結果の連絡

といった一連の対策作業を依頼している。ウイルスチェックはすでに PC がウイルスに感染していた場合，rootkit などでウイルスの存在が隠ぺいされていることを考慮し，CD-ROM ブートで OS とは独立にウイルス検査が可能な AVG Rescue CD を利用するように依頼している。実際にいくつかの PC では rootkit によりウイルスの存在が隠ぺいされており，ウイルス対策ソフトではウイルスの存在が検出されなかった事例があった。

4. ウイルススロットリングの運用

4.1. ウイルス検知の効果

8 月 1 日から 12 月 6 日の期間におけるウイルススロットリングによる検知件数を図 3，表 2 に示す。日によってばらつきはあるものの，スロットリング対象となる PC は依然学内に存在している。ただし，検知件数が 10 を超えるような事象は減少傾向にある。これは 3.3 節で紹介したように，検知後には該当 PC の検査依頼をしており，実際に感染していた PC からウイルスが駆除されていることを示していると考えられる。また，検知が 0 にならないのはウイルスが原因ではないスロットリング，つまり誤検知があるためと考えている。

表 2 から検知回数は 942 回であるが，検知対象となっているのは 52 個の MAC アドレスであることがわかる。つまり特定の PC が複数回検知されている。また通知により少なくとも 6 台の PC がウイルスに感染していたという報告があった。またウイルスチェックを行わずに再インストールを行った PC もあるため，実際の感染台数はもう少し多かったと考える。

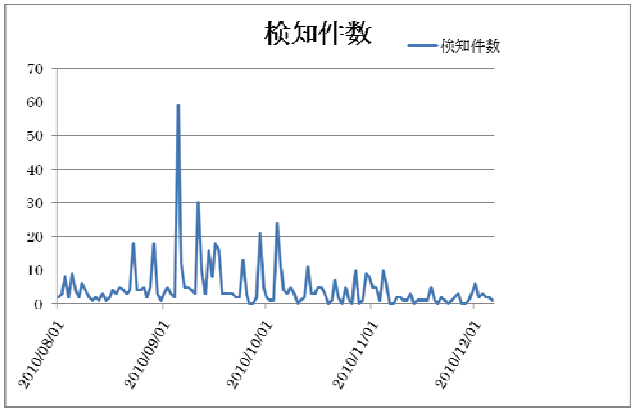

図 3　スロットリング検知件数

表 2　ウイルス検知回数(8/1-12/6)

検知回数	942
ユニーク MAC	52
通知回数	59
ウイルス検出数	6

4.2. 誤検知の考察

ウイルススロットリングで検知されたものの原因がウイルスではなかった誤検知の事例を紹介する。

P2P を利用したアプリケーションは複数のノードと通信を行うことがあり，スロットリング対象となる場合がある。いくつかの端末では AVG Rescue CD による検査ではウイルスは検出されないものの，P2P を利用した IP 電話ソフト skype をインストールして利用しているものがあった。これは skype の通信を誤検知したのではないかと考えている。また P2P による動画配信サービス(PPShare)も非常に多くの宛先にむけて UDP パケットを送信するため誤検知の対象となる。また P2P ソフトの一部には WindowsXP SP2 以降に設けられた tcpip.sys の接続上限(不完全な外向け接続上限 10)を変更し，多くの接続先と通信しようとするソフトウェアも存在している。制限を解除された端末からの通信も検知した。

ウイルススロットリングは単純な仕組みゆえに L3 スイッチで動作させることができるが，ネットワークを多数のアプリケーションが利用している現状では誤検知が多い。誤検知を減らしながら不正な通信を検出するためには，より高度な処理を行う機材の導入が不可欠である。

5. まとめ

ウイルススロットリングによるウイルス検知を実施した。その結果，すくなくとも 6 個のウイルスを検出することができた。ウイルス以外にもネットワークに負担が大きい P2P アプリケーションを見つけることもできた。また，ウイルス対応の依

頼を続けていくことで，検知そのものも減少傾向にある。ウイルススロットリングは，ネットワークに対する端末の振る舞いからウイルスの可能性を判断しているため，誤検知が避けられない。特に skype などの P2P を利用したアプリケーションは誤検知されるようである。

Bot に代用される最近のウイルスは感染しても静かに活動を行うため，ウイルススロットリングによる検知は難しい。そのため，運用開始以前はウイルスを検知することは難しいのではないかと考えていたが，実際にはウイルスを見つけることができた。大学のネットワークには様々なセキュリティレベルの PC が接続されている。そのため，ウイルススロットリングのような単純な仕組みでも検知されるようなウイルスに感染したままの PC も存在しており，今回の試みでウイルスを検知できたのは学内のセキュリティ向上に有益であったと考える。ただし，今回利用したウイルススロットリングはネットワークの単位時間当たりの接続先を計数するという単純な処理ゆえに誤検知も多くある。今後はより一層高度な監視を行う IPS などを導入することで，より確実に不正な通信を検知し学内 LAN のセキュリティを向上させることを検討したい。

参考文献

HP 社,アクセスセキュリティガイド,参照日: 2011 年 1 月 11 日，参照先: http://h50146.www5.hp.com/products/networks/procurve/pdfs/ProVision_ACS_SEC(2006_09_R1).pdf

情報基盤センター(2009) 鳴門教育大学におけるコンピュータウイルス感染状況，曽根直人，林秀彦，鳴門教育大学情報教育ジャーナル，No.6 pp.57-58