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

2004－DSM－35 (10)
2004／9／24

差出人詐称型ウィルスメールの発信源自動追跡

大隅 淑弘　宮下 卓也　岩井 俊道　山井 成良　森川 良孝
岡山大学 総合情報基盤センター

{oosumi,t_myst,t-os,yamai,morikawa}@cc.okayama-u.ac.jp

概　要

岡山大学では，コンピュータウィルスの蔓延を防止するため，メールゲートウェイで学外から学内および学内から学外への電子メールについてウィルスチェックを行っている．しかし，最近多く見受けられる差出人詐称型ウィルスメールは，メールゲートウェイでこれを検出しても，直ちにはその発信源を特定できず，短時間での対処が困難であった．本稿では，アンチウィルスサーバとMTAのログを照合することにより，差出人詐称型ウィルスメールの発信源を実時間で追跡するシステムを報告する．本システムの導入により学内の発信源を直ちに発見してウィルス駆除を行ったり，学外の発信源に対してその管理者に通報したりすることが可能になる．

Automatic Sender Tracing of Virus E-mails with Spoofed Sender Addresses

Yoshihiro Oosumi, Takuya Miyashita, Toshimichi Iwai,
Nariyoshi Yamai and Yoshitaka Morikawa

Information Technology Center, Okayama University

{oosumi,t_myst,t-os,yamai,morikawa}@cc.okayama-u.ac.jp

Abstract

In Okayama University, in order to prevent wide spread of computer viruses, mail gateways are introduced for checking virus infection of both inbound and outbound e-mails. However, if an e-mail is infected by a kind of virus that spoofs its sender address, it is difficult to specify and correct the sending host immediately. In this paper, we address a system that traces the sending hosts of sender spoofed virus e-mails in short time by referring to the logs of the antivirus software and those of MTAs. By introducing the system, we can find and correct the sending host in short time if it is inside of our domain, or notify the administrator of the sending host if it is outside of our domain automatically.

1 はじめに

コンピュータウィルス（以下，ウィルス）[1] という言葉が初めて使われたのは 1984 年と言われている．初期のウィルスはフロッピーディスクなどの外部媒体を介して感染が広がっていたが，インターネットが普及してくると，電子メールやネットワークによって感染が広がるようになり，その被害はますます深刻化している．独立行政法人情報処理推進機構 (IPA) の調査 [1, 2] によると，1992 年の届出件数が 253 件に対して，2003 年では 17,425 件と被害の件数は急速に増加している．

文献 [2] によると，ウィルスの感染・発見経路のうち最も多いのが電子メール (51.9%) である．最近のウィルスは，W32/Klez，W32/Netsky，W32/Mydoom[2]など，大量のウィルス付き電子メール（以下，ウィルスメール）を発信して感染拡大を図るもの（マスメール型ウィルス）が多く，感染した計算機をそのまま放置しておくと短時間のうちに広範囲にウィルスが蔓延したり，ネットワークやメールサーバに多大な負荷をかけたりする危険性がある．したがって，このようなウィルスの早期発見および早期駆除はウィルスによる被害を最小限に抑えるために非常に重要である．

ところが，このようなマスメール型ウィルスの多くは差出人アドレスを詐称するため，たとえウィルスメールを検出したとしても発信源を直ちに特定するのが困難であり，早期駆除等の対策が難しい状況がある．すなわち，検出箇所から配送経路を遡る必要があるため，従来は管理者がアンチウィルスソフトウェアやメールサーバのログを照合して追跡調査する必要があり，最近のように大量のウィルスメールが外部から送られる状況では発信源の特定にかなりの時間を要していた．

本稿では，上記のような問題を解決するために我々が開発した，差出人詐称型ウィルスメールの発信源自動追跡システムについて報告する．本システムでは，特に学内の計算機が発信源である場合には，その計算機を即座に発見して管理者に通報することが可能になる．また学外の計算機が発信源である場合でも，発信源ドメインの管理者に通報したり，発信源からの電子メール受信を拒否したりすることが可能になる．

[1] 一般にウィルスという用語は，既存のプログラムやファイルに寄生するプログラムを指す狭義と，これにワームやトロイの木馬などを含めたプログラムを指す広義の両方の意味で用いられるが，本稿では特に断りのない限り後者の意味で用いるものとする．

[2] 本稿における名称はいずれも IPA[3] による．

2 岡山大学の電子メール環境

岡山大学は 2004 年 5 月現在で学生数が 13,857 人，教職員数約 2,715 人で 11 学部を擁する総合大学である．キャンパスとしては，9 学部を擁する津島キャンパスと 2 学部を擁する鹿田キャンパスの 2 つの主要なキャンパスがあり，その他にも県内外に 10 以上のキャンパスがある．このうち，津島，鹿田，倉敷，三朝，東山，芳賀，牛窓の各キャンパスには，総合情報基盤センター（以下，センター）が管理・運用するメールサーバが存在し，各キャンパスの登録者が利用できるようになっている．メールサーバプログラムとしては，津島キャンパスでは SUN Enterprise 3500(OS は Solaris 2.6) 上で sendmail-8.9.3 を，他の 6 キャンパスでは，NEC Express 5800/120Mc(OS は TurboLinux Server 6.1) 上で sendmail-8.9.3 を運用している．この他に，各キャンパスには，学部，学科，あるいは研究室単位で独自に運用されているメールサーバが多数存在するが，大学全体ではセンター管理のメールサーバの利用者が大部分を占める状況である．

岡山大学では，独自運用しているものを含めた学内の全てのメールサーバに対するセキュリティ対策を行うためアンチウィルスソフトウェアを導入したメールゲートウェイを設置し，学外から発信された学内宛のメールは原則として全てメールゲートウェイを経由するようにしている [4]．図 1 に岡山大学のネットワーク構成を示す．メールゲートウェイはスループットと可用性の向上を図るために二重化されている．この構成において，対外接続ルータでは学外から学内への SMTP コネクションは，メールゲートウェイ宛のものを除き原則として遮断するように設定されており，また，学内の全てのメールサーバは原則としてセカンダリ MX としてメールゲートウェイが指定されている．このため，学外から学内宛に電子メールが配送される場合には，学外のメールサーバはまず末端メールサーバに直接配送を試みて失敗し，その結果セカンダリ MX であるメールゲートウェイに配送されることになる．一方，学内から発信される電子メールについてもできる限りウィルスの検出・駆除を行えるようにするため，センターが管理する 7 台のメールサーバから発信されるものはメールゲートウェイを経由して配送されるようにしている．

2 台のメールゲートウェイでは，それぞれにおいてアンチウィルスソフトウェアとしてトレンドマイクロ社の InterScan VirusWall v3.81 for UNIX（以下，

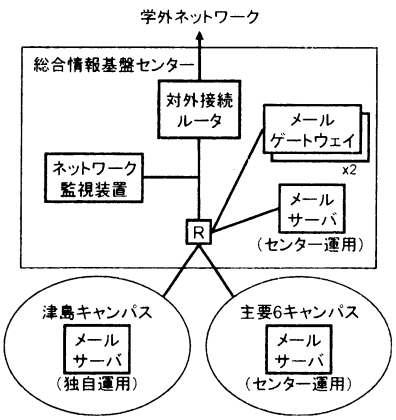

図 1: 岡山大学のネットワーク構成

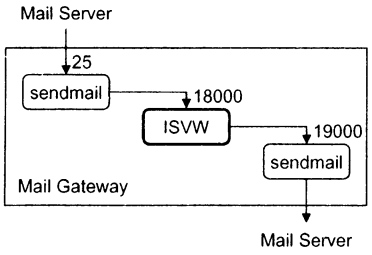

図 2: メールゲートウェイの構成

ISVW）を導入している．この製品はウィルスを検出して削除する機能は有するが，中継機能が不十分であったり，メール配信に関するログ機能がなかったりするなど，メールゲートウェイとして単独で運用するには問題が多いことが導入段階で判明した．そこで我々はメールゲートウェイの構成として，図 2 に示すように ISVW の前後に前処理用 sendmail および後処理用 sendmail を配置した構成を採用することにしている．ここで，前処理用 sendmail はポート 25 番で SMTP コネクションを待ち受け，SMTP コネクションが確立されると従来の中継サーバと同じ基準で受信を許可するか拒否するかの判定を行い，許可と判定すれば受信したメッセージを ISVW（ポート 18000 番）に中継する．ISVW は受け取ったメッセージを検査し，必要であればウィルスを除去した後にメッセージを後処理用 sendmail （ポート 19000 番）に引き渡す．これにより，従来の中継サーバと同等の不正中継防止機能，配送機能およびログ機能を有しながらウィルス対策機能をも実現することが可能となる．

3 差出人詐称ウィルスメールの発信源特定における問題点

1 章で述べたように，最近のウィルスの多くはマスメール型ウィルスであり，ウィルスによる被害を最小限に抑えるためにはまずウィルスの発信源を早期に特定することが非常に重要である．ところが，ウィルスメールの発信方法はウィルスの種類によって異なるため，発信源の特定にはウィルスの種類に応じた方法を用いる必要がある．

ウィルスメールの発信方法としては，W32/Netsky や W32/Sobig で用いられているようにウィルス自身が宛先への直接ウィルスメールを配送する方法（直接配送）と，W32/Klez や W32/Badtrans で用いられているように感染した計算機が通常利用するメールサーバを経由して配送する方法（間接配送）の 2 種類に大別できる．

このうち，直接配送については，現在のネットワーク構成では ISVW でウィルスメールを検出することができない．すなわち，前章で述べたように，学内からの電子メールのうち ISVW を経由するのはセンター管理のメールサーバから発信されるものに限られるため，直接配送されたウィルスメールは ISVW を経由しない．しかし，直接配送に伴う大量の通信は対外接続セグメントにおけるネットワーク監視で検出することが可能であり，また検出したパケットの送信元 IP アドレスにはウィルスメール発信源のものがそのまま現れるため，その特定は容易である[3]．

一方，間接配送については，大多数の利用者がセンター管理のメールサーバを利用しており，かなりの割合で ISVW でウィルスメールを検出することが可能である．このため，センターでは従来よりウィルス検出時にはウィルス名，差出人，宛先，動作を管理者に電子メールで通知するように ISVW を設定し，管理者はこのうち特に学外宛メールに関する通知（発信拒否通知）を受け取った場合には発信源を特定して対処するような体制を整えていた．

ところが，最近のマスメール型ウィルスの多くは感染した計算機から送信先アドレスを収集するため，実際には学内から学内宛にウィルスメールが発信される場合を無視できないにもかかわらず，上記の体制ではこのようなウィルスメールに直ちに対処することはできなかった．これは，このようなウィルスメールの検出通知が大量に発生する学外からのウィルスメール

[3]NAT(Network Address Translation) 機能が用いられている場合はこの限りではない．

```
Date:    MM/DD/YY hh:mm:ss
Method:  SMTP
From:    差出人アドレス
To:      <宛先アドレス>
File:    添付ファイル名
Action:  実行された処置内容
Virus:   ウィルスの名称
```

図 3: アンチウィルスソフトウェアのログ形式

の検出通知に紛れてしまうためである．したがって，管理者は上記のウィルス検出を通知するメールを受け取るとメールゲートウェイ上の sendmail の送受信ログと照合してまず発信源が学内か学外かを識別し，学内であれば次に中継に使われたメールサーバを特定して，さらにはそのメールサーバのログを調査して発信源を特定する必要があり，ウィルス検出を通知するメールを受け取ってから発信源を特定するまで相当の時間を要するなどの問題があった．

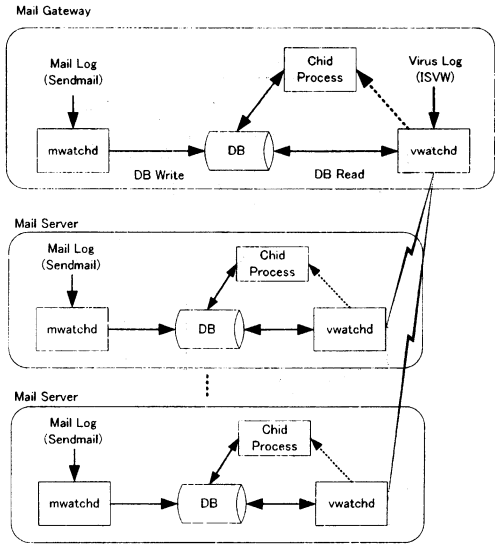

図 4: システムの構成

4 差出人詐称ウィルスメールの発信源自動追跡

前節で述べた問題を解決するため，我々はアンチウィルスソフトウェアのウィルス検出ログと sendmail の送受信ログを照合することによりウィルスメールの発信源を自動的に追跡するシステムの開発を行った．本章では本システムの設計・実装について述べる．

4.1 システムの概要

ISVW では，ウィルスメールを検出すると図 3 のような形式のウィルス検出ログを出力する．前述のように，このログにはウィルスメールの発信源あるいはウィルスメールを中継したメールサーバに関する情報は含まれていないため，このログから発信源や中継メールサーバを特定するには，検出日時（Date），差出人アドレス（From），宛先アドレス（To）を鍵として sendmail の送受信ログを検索する必要がある．また，検索の結果，ウィルスメールがセンター管理のメールサーバのいずれかを経由したことが判明した場合，同様の方法でそのメールサーバの送受信ログを検索すればよい．

そこで，本システムでは sendmail の出力するログを監視するプログラム mwatchd と，ISVW および mwatchd の出力をもとにウィルスメールの発信源を特定するプログラム vwatchd の 2 種類のデーモンプログラムを作成し，これらが互いに連携しながらウィルスメールの発信源を特定できるように構成した．本システムの構成を図 4 に示す．なお，これらのプログラムの記述には Perl-5.005-03 を用いた．

4.2 システムの動作

次に，システム全体の動作を述べる．本システムは以下の手順で動作する．

(1) メールゲートウェイおよびセンター管理メールサーバの mwatchd は sendmail のログを監視し，最近受信したメールに関するデータベースを作成・更新する．

(2) メールゲートウェイの vwatchd は ISVW のログを監視し，ウィルスメールが検出された場合にはデータベースを検索して送信元 IP アドレスを得る．

(3) 上記の結果，送信元 IP アドレスがセンター管理メールサーバのものであれば，メールゲートウェイの vwatchd は当該メールサーバの vwatchd にウィルス情報を通知する．当該メールサーバの vwatchd はデータベースを検索して 1 段階前の送信元 IP アドレスを得る．

(4) メールゲートウェイあるいは当該メールサーバのvwatchdは，得られたIPアドレスを管理者に通知する．

(5) もし，(2)や(3)の段階で送信元IPアドレスを得られなかった場合には，子プロセスでデータベースの再検索を行う．

以下の各節では，上記の各操作の詳細を示す．

4.2.1 データベースの作成

sendmailのログは電子メールの送受信のたびに追加されて巨大なファイルとなるため，ウィルスメール検出時に毎回ファイル全体を検索するのは非効率的である．そこで，本システムでは各メールサーバ上にデータベース（DBM）を導入し，受信した電子メールに関する情報を登録するようにした．具体的には，各mwatchdはsendmailのログを監視し，追加があれば，差出人，宛先，送信元IPアドレス，サイズ，受信日時を1レコードとしてデータベースに登録するようにした．その際，通常時にはウィルスメールはsendmailで受信された直後にISVWで検査され，さらにISVWの検査結果は直ちにvwatchdに伝わるため，同一レコードに対する登録と参照の時間差はそれほど大きくないと思われる．そこで，データベースには最近のもの100件程度を記録しておき，それ以外のレコードは随時削除することで無用な計算機資源の浪費を防止する．

4.2.2 ウィルスメール送信元の特定

メールゲートウェイ上のvwatchdはISVWのログを監視し，図3の項目のうちDate，From，Toを鍵としてデータベースを検索する．ここで，Dateについては，ISVWのログとsendmailのログとの間で多少の違いが生じる場合があるため，ある程度の時間差を許容する．検索の結果，該当するレコードがデータベースから見つかれば，vwatchdはそのレコードから送信元IPアドレスを取得する．

4.2.3 センター設置メールサーバでの検出

上記の動作で得られたIPアドレスがセンター管理メールサーバのものであった場合，メールゲートウェイのvwatchdは当該メールサーバのvwatchdにIO::SOCKETを通じて以降の処理を依頼する．依頼

```
Date: Fri, 27 Aug 2004 15:20:46 +0900
From: root <root@********.cc.okayama-u.ac.jp>
To: virus-alert@cc.okayama-u.ac.jp
Subject: virus detected

Virus Detected / Interscan VirusWall
--
08/27/2004 15:20:40 (1093587640)
from = ******@***.ne.jp
to   = ****@***.okayama-u.ac.jp
Virus= WORM_MABUTU.A

↓↓

<From MailLog>
--
8/27/2004 15:20:40 (1093587640)
from = ******@***.ne.jp
to   = ****@***.okayama-u.ac.jp
relay= [150.46.xx.xx]
size = 45587
ID   = PAA02989
--
```

図5: 通知メールの例

を受けたvwatchdはそのメールサーバ上のデータベースを検索し，送信元IPアドレスを取得する．

4.2.4 管理者への通知

メールゲートウェイあるいはセンター管理メールサーバのvwatchdは，管理者宛にウィルスメールを検出したことを通知する電子メール（通知メール）を送付する．そのとき，送信元IPアドレスが学内のものであれば，管理者にその旨を警告する[4]．図5に通知メールの一例を示す．

なお，現在は未実装であるが，ウィルスメール検出時の処理としては，単に管理者に通知メールを送付するだけでなく，発信源計算機の管理者に自動的に通報したり，レイヤ2スイッチやレイヤ3スイッチの設定を変更して発信源計算機の通信を制限したりする方法も考えられる．

4.2.5 データベースの再検索

メールゲートウェイやセンター管理メールサーバのvwatchdでは，データベースの参照で該当するレコードが見つからなかった場合は，子プロセスを起動し，規定の回数だけメールデータベースを再検索する．し

[4]実際には，発信源が学内かどうかで通知先アドレスを使い分けている．

表 1: 発信源が学内のウィルスメール検出件数

ウィルス名	検出件数
W32/Netsky	398
W32/Mabutu	70
W32/Lovgate	3
MIME_Tag_Overflow	3
合　計	474

かし，メールゲートウェイが非常に高負荷となったときには再検索をしても見つからないことがある．これは，sendmail が受信は受け付けるものの，ISVW の検査が追いつかず，待ち行列に入ってしまうことが原因と思われる．このような場合，子プロセスはこのレコードを別ファイルに記録しておき，定期的にまとめて sendmail のログを検索する．

5　システムの運用

本システムは 2004 年 8 月 4 日から試験運用を開始し，8 月 27 日まで（8 月 10 日から 15 日までは都合により休止）の計 18 日間に 23,608 件のウィルスメールを検出した．そのうち，学内が発信源であるものは 474 件であった．その内訳を表 1 に示す．

表 1 のうち，MIME_Tag_Overflow は実際のウィルスメールの検出を表すものではないが，添付ファイルの名前が長すぎるためバッファオーバフローの危険性があることを示すものである．この警告については，管理者とは別に差出人にも再発信を促す通知メールが自動的に送られるようにしている．残りの 3 種類のウィルスメールのうち，特に W32/Netsky の検出件数が多いが，これは 8 月 23 日午前 8:15 から 9:03 の 48 分間の間に発信されたものである．このとき，管理者は出勤後にこのウィルスメールに関する通知メールが大量に届いていることに気づき，その後直ちに発信源の計算機が接続されているレイヤ 2 スイッチのポートを停止し，比較的短時間に対処することができた．また W32/Mabutu や W32/Lovgate についてもウィルスの感染活動が異なるため検出件数は少なくなっているが，同様に短時間で対処を行うことができた．本システムの導入前では，差出人を詐称しない W32/Lovgate などを除き，このような短時間での対処は困難であったことから，本システムの有効性が確認できたといえる．

6　まとめ

本稿では，従来のアンチウィルスソフトウェアの運用において差出人詐称型ウィルスメールの発信源の特定が困難であることを示し，これを解決するためにアンチウィルスソフトウェアやメールサーバのログを照合してウィルスメールの発信源を自動的に追跡調査するシステムについて報告した．また，試験運用を通じて，本システムを用いれば，管理者がウィルスメール検出後比較的短時間にその発信源を特定して対処できることを示した．

今後の課題としては，4.2.4 節でも述べたように，本システムを拡張して発信源計算機の管理者に自動的に通報したり，レイヤ 2 スイッチやレイヤ 3 スイッチの設定を変更して発信源計算機の通信を制限したりする機能を実装することが挙げられる．

参考文献

[1] 独立行政法人情報処理推進機構:　コンピュータウイルスに関する届出について，http://www.ipa.go.jp/security/outline/todokede-j.html，2004 年 7 月．

[2] 独立行政法人情報処理推進機構:　国内におけるコンピュータウィルス被害状況調査報告書，http://www.ipa.go.jp/security/fy15/reports/virus-survey/documents/2003_virus_domestic.pdf，2004 年 4 月．

[3] 独立行政法人情報処理推進機構: IPA に届けられたウイルスの概要，http://www.ipa.go.jp/security/virus/virus_sub.html，2004 年 6 月．

[4] 山井成良，宮下卓也，大隅淑弘，林伸彦: “岡山大学における電子メールシステムのセキュリティ対策”，情報処理学会分散システム/インターネット運用技術研究会研究報告，2002-DSM-26-11，pp.61-66，2002 年 8 月．