ウイルス防御システムとその対策

車古　正樹

金沢大学総合情報処理センター

〒　920-1192 金沢市角間町

TEL:076-234-6912　　FAX:076-234-6918
shako@gipc.kanazawa-u.ac.jp

キーワード

コンピュータウイルス，ウイルス防御対策，ウイルス感染

はじめに

最近のコンピュータウイルスの動向は悪質化し社会的な問題に発展する可能性がある。コンピュータを破壊するもの，重要なファイルを勝手に送付するもの，爆発的に感染しネットワークやサーバに支障をきたすものがある。これらのウイルスから如何に防御するか，また，ウイルス感染者を如何に減少させるか対策を講じる必要性がある。

ここで，金沢大学におけるウイルス防御システムとその対策について報告する。

1. ウイルス感染防御システム

メールによるウイルス感染防御のために下記のようなシステムを構築した。

1.1 ウイルス感染防御

ウイルスを防御するために 12 式のトレンドマイクロ社製 InteScan VirusWall を導入し, 次のようなメールの流れで運用している。

1) 学外からのメールの流れ
　学外メールゲートウェイ(学外向け DNS サーバの MX レコードで取り込み), 学外用ウイルスチェッカー, 学内メールゲートウェイ，学内メールサーバ

2) 学内からのメールの流れ 1
　部局ファイアウオール外メールサーバ，部局用ウイルスチェッカー，部局ファイアウオール内メールサーバ「，部局用ウイルスチェッカー，学内メールサーバ」

3) 学内からのメールの流れ 2
　部局ファイアウオール外メールサーバ，部局用ウイルスチェッカー，部局ファイアウオール内メールサーバ「，学内メールサーバ」

4) 学内からのメールの流れ 3
　中継専用ウイルスチェッカー付き SMTP サーバ，学内外メールサーバ

1.2 ウイルス感知システム

ウイルス及びウイルスと思われるものを検知するために学内と学外を接続するところに 2 式の snort を設置し次のように運用している。

1）学外検地システム
　学外用ウイルスチェッカーを通過する前に設置し，1 時間毎にレポートをセキュリティ対策専門委員にメールで通知する。

2）学内検地システム
　学外用ウイルスチェッカーを通過した後に設置し，1 時間毎にレポートをセキュリティ対策専門委員にメ

ールで通知する。
両方のメールを比較することにより，送受信におけるウイルス除去漏れが確認できる。

1.3 smtp サーバの数

当大学はサーバ構築が自由であり，利用者用 smtp サーバが次の数が設置されている。

通常接続サーバ　　163 式
部局 DMZ 内サーバ　　26 式

2. ウイルス除去件数

上記の運用により外部からのウイルスの駆除件数は次の数である。

2002/7　合計　2,782 件　　最大/日　324 件　　最小/日　56 件　　FRETHEM(15.16)
2002/6　合計　2,346 件　　最大/日　114 件　　最小/日　44 件
2002/5　合計　3,392 件　　最大/日　188 件　　最小/日　61 件
2002/4　合計　1,846 件　　最大/日　192 件　　最小/日　8 件
(2002/4/-14 前半)　合計　190 件　最大/日　22 件　　最小/日　8 件
(2002/4/15- 後半)　合計　1.656 件　最大/日　192 件　　最小/日　46 件　KLEZ

上記の運用で内部からのウイルスの感染者数は次の数である。

2002/8/16　　1 人　KLEZ　　プロバイダー利用による
2002/7/15,16　６人　FRETHEM　　実際の感染者数　19 人　　(感染はパターンファイル以前)
2002/6/18　　1 人　JS_SEEKER　　ホームページと思われる

3. 問題点と対策

ウイルス感染防御に関して下記のような問題がある。

3.1 新種ウイルスに対する防御

2002 年 1 月 28 日の MYPARTY，7 月 15 日の FRETHEM のような新種ウイルスの場合はパターンファイルが更新される以前に大量のウイルスが学内に入り感染者が多数でる可能性がある場合の対策が必要である。

7 月 15 日の経過を次に記す。

07/15-11:42　最初のウイルスメール受信
13:02　新種ウイルスと断定，メーカに調査依頼
13:10- いたる所から多数のウイルスが送信されてくる
13:20　メーカに電話でパターンファイルが早急に更新されないか問い合わせる
13:25　専門委員会で外部メールゲートウェイの停止を検討，現段階では困難
13:49- 学内の感染者から外部にウイルスメールの発信が始まる（1 時間内で 10 人以上感染)
13:50　サポートセンターにウイルスを送付し調査依頼
14:38　学内に注意文書を発送
15:35　学内に再度注意文書を発送
18:03　ウイルスパターンが更新される

対策：8 月 6 日のセンター委員会で緊急時における学外とのメール送受信の停止についての権限を専門委員会に委任することが了承された。
現在，専門委員会で緊急時の対策を検討するための原案を準備中である。

3.2 二次感染防御

FRETHEM の感染において約 20 人もの感染者が出たのは次の理由によるところが大きい。

事務総務部の人が感染し，そのアドレス帖にあった全総務宛のアドレスにメールが発信され，一部の部局でさらに部局構成員に発信されたためである。

対策１：部局ファイアウオール外のメールサーバは必ず DMZ 上のメールサーバに中継する。中継設定を依頼しているが設定変更に応じないサーバについて，近い将来，要請に応じない場合はファイアウオールで遮断する方向で検討中である。これによりファイアウオールでの制御などにより防御が可能となる。

対策２：利用者端末にウイルスチェッカーが無いのにもかかわらず pop サーバと smtp サーバを同一のサ

ーバで利用している人がいる。感染者が出た場合に同一サーバ利用者に対するウイルス感染防御ができない。別サーバを利用するように指導を継続する以外方法がない。同一サーバ利用者の洗い出しが困難なため，完全な防御は難しい。

3.3 学外利用者の感染防止

外部 pop サーバ利用者がかなりおり，1 日 10 件以上のウイルスを利用者が受信している。2002 年 1 月から 7 月までに，これにより 2 人の感染者の報告を受けている。

対策：利用禁止について検討したが結果，学生用情報コンセントからの利用は禁止とするが現段階では職員の利用禁止措置は思わしくないとの結論に至った。このため完全な防御対策は困難であり，現状では利用者を洗い出しセキュリティ対策のアンケートを取り，ウイルス防御未対策者に防御方法の指導を行っている。

プロバイダーの Web メール利用者が多い。洗い出しが困難であり，指導ができない。

3.4 Web からの感染防止

Web による感染について 2002 年 1 月から 7 月までに 1 人の感染者の報告を受けている。

対策：Web についてもメールと同様にウイルスチェックを行えるシステムとなっているが，一部で http,ftp のウイルスチェックのテストを行ったところ非常にレスポンスが悪い，あるいは検索サイトを利用するとタイムアウトで切断される。という支障があり現実的でなく各個人で対策をとるしか方法がない。

3.5 学外者のウイルス感染警告

最近のウイルスは発信元が詐称されているため，受信者が発信者に警告できない。しかしながら，ウイルス駆除済みメールを受信した一部の人が不安をセンターに訴えてくる。

対策：当センターでは snort のウイルスメールのヘッダーを調査し，同一端末やサーバから大量に送信されてきた場合や，2，3 日続いた場合はそのサイトに対して駆除対策をお願いしている。

まとめ

ウイルスチェックにおいては，学外からのメールのウイルスチェックを行うことで 99%以上の感染を防御でき非常に効果的である。一方、学内の各部局に設置したウイルスチェッカーではほとんど駆除することがないため部局ごとに設置する場合はコストを十分考慮し配置する必要がある。また，新種ウイルスについてはウイルスチェッカーでは効果が全くないため，緊急措置を取る体制やマニュアルを整備しておく必要がある。しかしながら，ネットワーク管理者がどのような対策を施してもウイルス感染防御には限界がある。ウイルス感染の絶滅を図る最善の方法は，各個人のネットワーク利用の知識向上と端末のセキュリティ対策の向上を，周知徹底することである。そのためには，センターが積極的にセキュリティに関する情報をユーザに広報していく必要がある。