セキュリティ対策状況

学術情報処理センター　江藤博文

1　はじめに

学術情報処理センター (以下、センター) ではセキュリティ対策として、ファイアーウォールの設置、ウィルスチェックサーバの設置、ウィルス対策ソフトのサイトライセンス契約を行っています。

これらの対策状況を報告します。

2　ファイアーウォール

ファイアーウォールはネットワークの出入口に設置し、そこに流れるパケットをルールに従って制御するネットワーク装置です。

センターで設置したファイーアウォールは表 1 のルールで運用しています。

表 1: ファイアーウォールルール

学外から学内	開放	外部からのネットワーク利用に最低限必要なポート (DNS 等)
		教育研究に必要なサーバの特定ポート
	閉鎖	上記以外の全てのポート
学内から学外	開放	下記以外の全てのポート
	閉鎖	パスワードが平文で流れるアプリケーションが使用するポート (POP3 等)
		著作権などの問題があるアプリケーションが使用しているポート
		その他セキュリティ上問題のあるポート

学外から学内へのアクセスはほとんどが閉鎖されています。これは学外からの不正アクセスを防御するのが目的です。

学内にサーバを設置する場合には「サーバ学外公開申込書」や「ファイアーウォール特殊設定申込書」の提出をお願いします。但し、セキュリティ上問題がある場合には開放できない場合もありますので、事前にご相談下さい。

2.1　ファイアーウォール統計

ファイアーウォールは学内から学外、学外から学内を通過するネットワークをチェックしているため、その統計データは膨大な量になります。ここでは、2003 年 1 月 30 日 (木) のデータの統計情報を掲載します。図 1 に拒否した学外からのパケットの割合を示します。なお、拒否された総パケット数は 1,772,903 件でした。

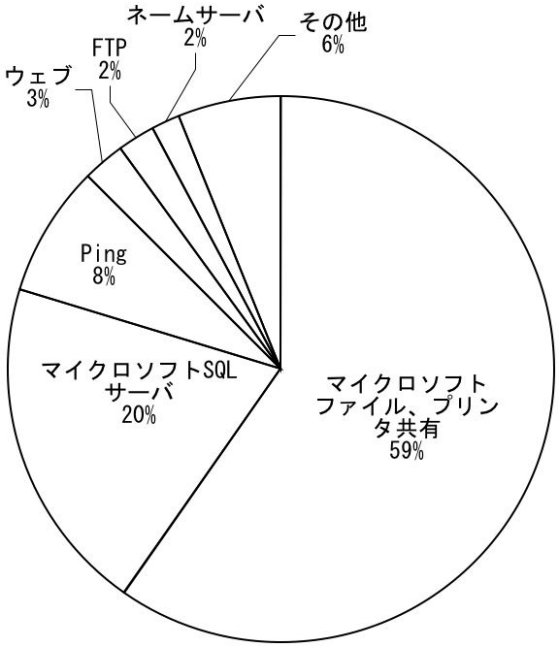

図 1: 拒否した学外からのパケットの割合 (2003 年 1 月 30 日 (木))

3　ウィルスチェックサーバ

ウィルスチェックサーバは登録されたメールサーバのメールを検査し、ウィルスが添付されている場合には除去を行うネットワーク装置です。

センターではこのサーバを 2002 年 10 月に導入しました。現在のところ学術情報処理センター及びいくつかの学部学科のメールサーバのウィルスチェックを行っています。

このウィルスチェックサーバの仕様による制限事項として、分割メールは送受信できませんのでご注意下さい。特にメールソフトによっては自動的にメールを分割する場合がありますので、設定をご確認下さい。

自組織でメールサーバを運用しており、ウィルスチェックを希望される組織はセンターに御相談下さい。

3.1　ウィルス駆除統計

図 2 に導入から 2003 年 1 月末までのウィルス駆除の統計を示します。

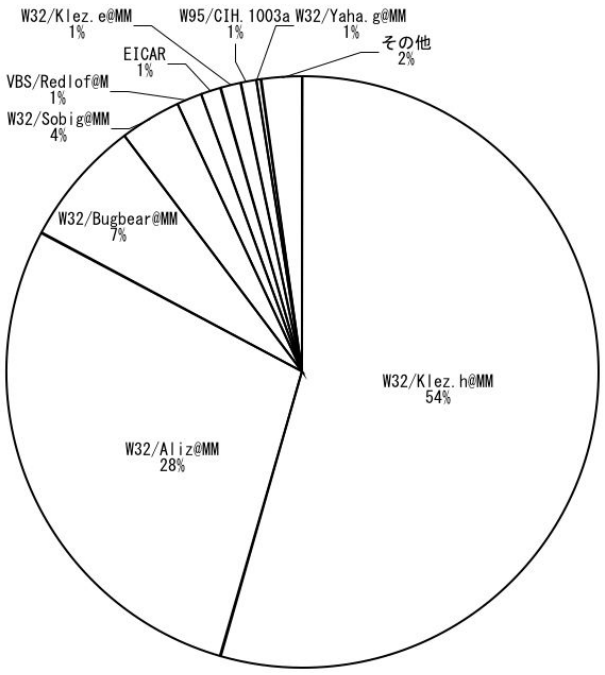

図 2: 2002/10〜2003/1 間に駆除した主なウィルスの割合

図 3 は 1 日のウィルス駆除件数の推移グラフです。

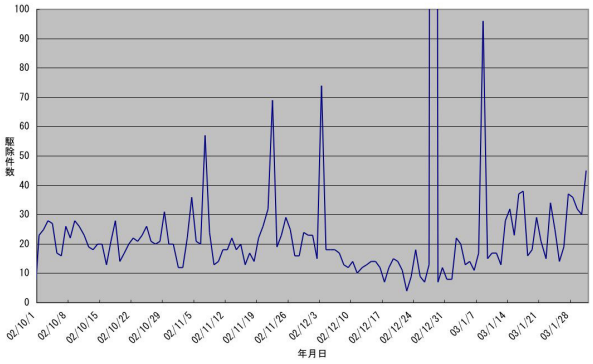

図 3: 1 日のウィルス駆除件数の推移

2002 年 12 月 28 日の 942 件はデータが大きすぎるため、グラフ外となっています。

2002 年 10 月から 2003 年 1 月の期間に合計 3,548 件、1 日平均で 29 件弱のウィルスが駆除されています。

3.2　メール不正中継防止統計

ネットワーク上の不正アクセスには外部のメールサーバを不正に経由させるものあります。

このウィルスチェックサーバにも数多くの不正中継のアクセスがあります。図 4 は 1 日のメール不正中継防止件数の推移グラフです。

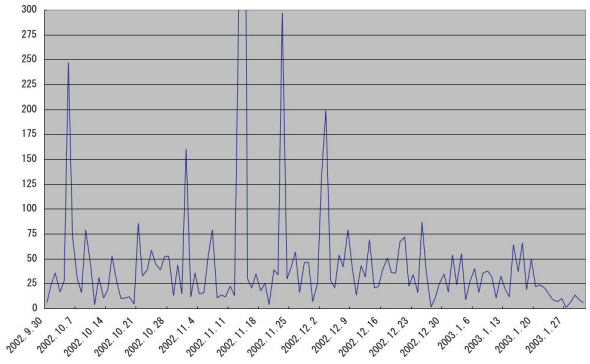

図 4: 1 日のメール不正中継防止件数の推移

2002 年 11 月 14 日の 840 件はデータが大きすぎるため、グラフ外となっています。

2002 年 10 月から 2003 年 1 月の期間に合計で 5,809 件あり、1 日平均で 47 件弱の不正中継がありました。

このように不正中継の攻撃は常に行われています。メールサーバを運用している管理者の方はメールサーバの設定に十分注意して下さい。

4　ウィルス対策ソフト

センターではウィルス対策ソフトのサイトライセンス契約を結んでいます。このソフトは対応 OS は表 2 の通りです。

表 2: ウィルス対策ソフト対応 OS

Windows 系	Windows98
	WindowsME
	WindowsNT4.0
	Windows2000
	WindowsXP
Macintosh 系	MacOS8.1〜9.x
	MacOSX v10.1 以上

サイトライセンス契約により、学内の公費で購入したコンピュータにはインストールが可能となっています。インストールを希望される方はセンターまでご相談下さい。

なお、2003 年 1 月末までに学内でインストールしている台数は 1,051 台です。

5　個人でのセキュリティ対策

上記のようにセンターではさまざまなセキュリティ対策を行っています。

しかしながら、コンピュータウィルスは日々新しいものが発見され、ネットワーク攻撃の手段も巧妙になっています。このためセンターの対策だけでは学内の全てのコンピュータを守ることは難しいのが現状です。特にコンピュータは個人個人でのセキュリティ対策が重要となってきます。

以下に個人でできるセキュリティ対策を記します。

1. **ウィルス対策ソフトをインストールする**
   公費で購入したコンピュータには 4 をご利用下さい。個人で購入したコンピュータには最初からお試し版のウィルス対策ソフトが添付されていることが多いですが、正式に契約を結ぶか新規で購入することをお勧めします。また、フリーのウィルス対策ソフトもいくつかありますのでそれらを使用することも可能です。

2. **パターンファイルを常に最新のバージョンにする**
   ウィルス対策ソフトはウィルスのパターンファイルを使用してウィルスを検知します。このパターンファイルが古いものだと最新のウィルスを検知できないことがあります。パターンファイルは常に最新のものにバージョンアップして下さい。通常ウィルス対策ソフトには自動アップデート機能がありますので、この機能を有効にしておくことをお勧めします。

3. **添付ファイルをむやみに開かない**
   ウィルスは通常メールに添付されるファイルとして来ます。このファイルを開いた時点でウィルスに感染しますので、添付ファイルはむやみに開かないで下さい。また、特に最近のウィルスは差出人を偽り、知合いのアドレスを使用してメールを送信することがあります。たとえ知合いからのメールであっても、添付ファイルはむやみに開かないで下さい。

4. **持ち込みのデータはまずウィルスチェック**
   ウィルス感染は上記のようなメールからの他に、フロッピーディスクを介して感染することがあります。他の人からフロッピーディスクなどを借りた場合には必ずウィルスチェックを行って下さい。

5. **ソフトを最新のバージョンを使用する**
   ソフトウェアは不定期にバージョンアップが行われます。このバージョンアップには重要なものが含まれていることがありますので、ソフトはなるべくバージョンアップを行い最新のバージョンのものを使用して下さい。

6. **感染が判明したらネットワークから切り離す**
   最近のウィルスは感染したコンピュータを乗っ取り、他のコンピュータに攻撃を行います。感染が判明した場合にはすぐにコンピュータをネットワークから切り離してから対処して下さい。

6　おわりに

　セキュリティ情報を提供しているサイトは多く存在します。ここではいくつかのセキュリティ情報の提供サイトを掲載します。

- コンピュータ緊急対応センター
  http://www.jpcert.or.jp
- IPA セキュリティセンター
  http://www.ipa.go.jp/security