Frethem ウィルス騒動の顛末

長谷川　明生

7月15日の昼過ぎ，複数の方から「電子メールウィルスチェックシステムのチェックにかからない新種のウィルスがあるようだ」という電話報告がありました。私自身もメーリングリスト等を通じて，複数の「Re: your password」という表題の添付ファイル付メールを複数受け取っていました。その電話以降も，センター内外から，ウィルスらしいメールを大量に受け取っているという情報が寄せられてきました。この時点で，昨年の CodeRed や Nimda の悪夢のような騒動が頭に浮かびました。新種ウィルスの場合，感染経路が既知のものかどうか不明なため，その感染力や影響範囲が不明で，緊急度の判定がつけにくいのですが，まわりからの声やウィルス対策ソフトの WWW ページ等をモニタしながら，CodeRed 並みの被害を想定して，当日の15時すぎに学内の管理者にウィルス情報を流しました。また，久しぶりに WWW ページのセキュリティ情報の更新を行いました。この時点では，Frethem の亜種らしい情報はあったのですが，確信はなくウィルス対策ソフト等のパターン更新はなされていませんでした。

このウィルスは，「Re: your password」という表題のメールで，password.exe や password.txt というファイルが添付しています。これらを開くと感染するのは当然として，場合によっては Outlook や Outlook Express で問題のメールをプレビューするだけで感染するというものでした。このウィルス/ワームは感染に成功すると，アドレス帳やエクセルファイル等のメールアドレスに対して，自分自身を添付した電子メールを発信します。

早めに sendmail 等に手を入れて，メールの表題のチェックを実施したところもありました。やきもきして待つうちに，夕刻に，Frethem の変種として解析され，各社のウィルスチェックソフトウェアのウィルスパターンが更新されました。また，19時には NICE 入り口のメールウィルスチェックシステムのパターンも更新されて，それ以後は目に見えてウィルス騒動も落ち着きはじめました。メールウィルスチェックシステム導入後初めて体験する大規模なウィルス出現だったので，システムの処理能力やログの容量に不安があったのですが，その点も杞憂に終わりました。

ただし，Frethem には，短時間に変種が多く出現し，数日はウィルスソフトウェアのパターン更新の頻度があがりました。それでも，昨年の CodeRed や Nimda ほどの問題にはなりませんでした。

このウィルスの終息が早かったのは，以下の要因が考えられます。

1．NICE でも導入しているような電子メールのチェックシステムの普及が全国的に進んでいること。実際に，そのようなシステムの発する警告メールを複数見ました。
2．ウィルス対策ソフトウェアが個々のパソコンにも普及したこと。

3．ウィルスやワームに関する知識が普及したこと。

4．Windows update 等の利用が普及したこと。

しかしながら，学内での感染は決してゼロではありませんでした。さらなる利用者教育が必要とされるところです。

一方で，Frethem の拡大の防止に威力を発揮した電子メールのウィルスチェックシステムですが，その発信する警告メールが，新たな問題を起こしました。

この種のシステムでは，電子メール中にウィルスを発見すると，多くの場合，問題のメールの発信者と受信者の両方に警告メールを送るように設定されているのが普通です。そのような設定は，アドレスが詐称されていないことを前提条件にすると正しいものです。しかし，最近のウィルスやワームでは，発信者のアドレスを適当に偽造したり，アドレス帳から抜いてきたアドレスを使ったりします。このような例では，ウィルスにアドレスを使われた被害者が，身に覚えのない警告メールを受け取ることになります。筆者のアドレスがワームの発信アドレスに使われたのでしょう。このような警告メールを何通も受け取りました。さらに問題なのは，ワームの発信者アドレスが大規模なメーリングリストのアドレスだった場合です。このようなケースでは，あちらこちらに設置されているウィルスチェックシステムの発する警告でメーリングリストの機能がそこなわれることがあります。今回の騒動の場合，活発な活動をしているメーリングリストの参加者は，ウィルスメールだけでなく，無関係なウィルス警告メールをたくさん受け取った様子です。

本学のシステムでは，導入時の議論で，このような問題が指摘されたこともあり，外部からのメールにウィルスがついていた場合，警告メールを学内の受信者にのみ配送する設定としていました。したがって，学内のサーバをホームとするメーリングリストを除いて，この問題は発生しなかったと考えています。

警告メールの文面がわかりにくく，どのシステムから来たものかが判定できないという指摘も複数ありました。警告メールの文面がわかりにくいという点に関しては，今後改善の余地があります。

と同時に，利用者は，パソコン等のウィルス検出ソフトウェアやウィルスメールチェックシステムの問題点，特にウィルス/ワーム検出からパターンファイルの更新までの時間差の問題を承知しておく必要があります。

また，このようなシステムの維持管理には，緊急時対応のための労力やソフトウェアのライセンス料等のコストの問題が付随していることをご理解ください。今回のウィルス騒動は，問題の発覚が平日の昼間だったので対処が可能だったのですが，これが深夜だったり連休中だったりすると，どう対処するか，体制の問題も含めて，未解決の課題として残っています。

（はせがわ　あきうみ：名古屋大学情報連携基盤センター大規模計算支援環境研究部門）