情報セキュリティ歳時記

Melissaウイルス騒動

前川　徹
情報処理振興事業協会（IPA）

ウイルスによるメール洪水

IPAが1999年3月中に受理したウイルス被害届出件数は，455件と過去最高を記録した．ちなみに1998年の届出件数は月平均170件弱である．届出が一番多かったのは，先月号で紹介したメールの添付ファイルの形で伝染するW32/Ska（Happy99）で，これまで1種類のウイルスの月間最多届出件数であったXM/Laroux の140件（1997年7月）を上回る181件を記録した．

こうして日本でW32/Skaが大流行している中，米国では新たなウイルスが大繁殖していた．このウイルスの名前は「Melissa（メリッサ）」[1]．Microsoft Wordのマクロ機能を利用したウイルスで，ウイルスに感染しているWordファイルを開くと，そのパソコン上のWordに感染し，それ以降に作業したWordファイルにも感染する．やっかいなのは，このマクロ感染型ウイルスは電子メールソフトであるMicrosoft-Outlookを利用して，Outlookのアドレス帳に登録されている宛先上位50に対してウイルスに感染しているWordファイルを添付した電子メールを自動送信することである．

もし，アドレス帳にメーリングリストのアドレスやグループが登録されている場合は，それも1つとしてカウントするので，実際に自動送信されるメールは50を超える可能性がある．もちろん，メール送信の処理は画面上に表示されないようにできているので，ユーザがメール送信に気付く可能性は小さい（ただし送信簿には記録が残る）．メールの件名は「Important Message From "ユーザ名"」，本文が「Here is that document you asked for ... don't show anyone else ;-)」となる．

なになに，Aさんからの重要なメッセージというメールが届いているぞ，「頼まれた文書を送ります，他の人には見せないでください」だって，さて，何だっけ．そう言いながら添付書類をクリックするとウイルスに感染する．感染した人がOutlookを利用していれば，また50人以上にウイルスに感染した添付書類付きのメールが送られる．もし仮に，ウイルスに感染した添付書類を受け取った人の20％がウイルスチェックをせずにファイルを開き，かつOutlookを利用していると仮定すると，8サイクル目にはウイルスに感染した添付書類付きのメールがネットワーク上を5億通以上も飛び交うことになる．20％ではなく40％と仮定すると8サイクル目に送られる電子メールの数は640億以上となる．そういう仕組みでネズミ算式にウイルスが広がっていったのである．

米国の緊急対応センターの1つであるCERT/CCに，このウイルスに関する連絡が入ったのが3月26日（金）の午後2時（米国東海岸標準時）．CERT/CCは，3月27日にMelissaに関する最初の警告（CERT Advisory）を出した[2]．翌3月28日には，NIPC（National Infrastructure Protection Center）からも異例の警告が発表された[3]．NIPCは，国家の重要なインフラを不正アクセスなどの脅威から守るために1998年2月に司法省とFBIによって創設された組織で，連邦政府におけるネットワーク犯罪対策の中心的役割を担っている．CERT/CCや連邦政府が警告を発した理由は，Melissaによる被害が従来のウイルスによる被害を遙かに超える可能性があったからだと考えられる．すなわちMelissaは，データを改竄したりファイルを消去したりするような発病機能は持っていないが，前述のように，ネズミ算的な感染力のためにメールの洪水を引き起こし，ネットワークやメールサーバを麻痺させる可能性があったからである．

容疑者の逮捕

Melissaがマスコミに登場してから約1週間後の4月2日，捜査当局はニュージャージー州在住のDavid L. Smithを逮捕した．犯人探しは3月末から始まっており，当初はWordファイルに含まれるGUID（Global Unique Identifier）が重要な手がかりになるのではないかと期待された．GUIDはMicrosoftのWordやExcelなどのMicrosoft Officeのアプリケーションで作成されたファイルにつくユニークな番号で，これを調べればどのパソコンで作成されたファイルかを特定できる可能性がある．おまけにMelissaは潜伏機能を持っていないため，発病したときに開いていたファイルをそのまま添付書類として50の宛先に送る．このため，ほとんどの場合，オリジナルのファイルがそのまま添付書類となる．したがって，

ウイルスを媒介しているWordファイルのGUIDは，そのウイルス作成者が使っているWordのGUIDだということになるはずである．

しかし，現実にはGUIDは，ほとんど役に立たなかったといわれている．Melissaが最初に投稿されたニュース・グループであるalt.sex上のWordファイルのGUIDは，いくつかのウイルスの作者として有名なVicondisES（ハンドル名）が作成しインターネット上で公開しているマクロ感染型ウイルスを含むWordファイルのGUIDと一致した．

考えられることは，Melissa作成の容疑で逮捕されたSmithがVicondisES本人であるか，SmithがVicondisESが作成したウイルスをベースにMelissaを作成したかである．現時点では，後者の可能性がきわめて高いと考えられている．他人が作成したWordファイルを利用してマクロ感染型ウイルスを作成すれば，そのGUIDは最初のWordファイルを作成した人が利用しているWordのGUIDになる．したがって，GUIDはMelissaのようなタイプのウイルスであっても作者を特定する決め手にはならない．

では，どのようにしてMelissa事件の犯人探しは行われたのだろうか．マスコミによれば，ニュージャージー州検事総長の広報官は，Smithを逮捕できたのはアメリカ・オンライン（AOL）の助力と電話の逆探知によるものであると語っている．AOLからどのような情報が提供されたかは明らかにされていないのだが，Melissaがalt.sexに投稿されたときに利用されたアカウントはAOLのもので，「skyroket@aol.com」であることは3月末に判明していた．このアカウントの持ち主であるワシントン州の土木技師は，マスコミのインタビューに対して，Melissaの作成や流布には一切関与していないと言明している．ここからは素人の想像であるが，Smithはウイルス作者やクラッカーとしては比較的アマチュアで，盗んだアカウントを，Melissaをニュース・グループに投稿した後も引き続き利用していたのではないだろうか．もしそうなら，skyroketのアカウントでアクセスしてくる人物が，どこのアクセスポイントを利用しているかを調べるのは難しくない．さらに，Smithが警戒せずにskyroketのアカウントの利用を続けていたと仮定すれば，電話の逆探知によって居所は容易に突き止めることはそう難しくない．もし，Melissaの作者がこの道のプロなら実在するアカウントからウイルスを投稿しなかっただろうし，手がかりになるような痕跡は残さなかっただろう．

Melissaの功罪

では，Melissaはどの程度の被害を与えたのだろう．CERT/CCによれば，300社以上の企業，10万台以上のパソコンが感染したという．わずか1週間の被害としては，おそらく史上最高に違いない．しかし，不思議なことに（この原稿を書いている時点では）日本ではほとんど流行した形跡はない．IPAにもいくつか被害届出が届いているが，ウイルスに感染しているファイルを海外から受け取ったという報告だけで，メールの自動送信が行われたとか，2次感染が起きているといった届出はまったくない．

現在も調査中であるが，オリジナルのMelissaは日本語環境では発病をしないのではないかと思われる．だからといって安心してはいけない．マクロ感染型ウイルスは，一部を改変した亜種が数多く発生する傾向がある．すでにMelissaの亜種もいくつか見つかっている．こうした亜種の中には，日本語版のアプリケーションで発病するものがあるかもしれないし，誰かがそうした亜種を作るかもしれない．

前述したようにMelissaの発病機能が，データを改竄したりファイルを消去したりするような悪質な発病機能を持っていなかったのは不幸中の幸いである．もし，重要なファイルを破壊するようなウイルスであったら，もっと甚大な被害が出ていただろう．ウイルスの作者がその気になれば，そうした悪質な機能を付加することは簡単なことである．そう考えると，Melissaの流行はウイルスの被害に人々の注意を向ける警鐘の役割を果たしたといえるかもしれない．米国では，3月末から4月にかけて，多くのパソコンユーザがワクチンソフトを用いてウイルスチェックを行い，従来型のウイルスを数多く発見したと伝えられている．

とはいっても，ウイルスに感染したファイルを添付したメールを大切な顧客に送っては，企業や組織の信頼は少なからず傷つくに違いない．ワクチンソフトを利用すると同時に，アプリケーションのマクロウイルスの検出機能を有効に設定し，アプリケーションがマクロを起動してよいか聞いてきたら，ウイルスに感染している可能性をまず考えていただきたい．

今月の参考文献等
1）IPAのMelissaに関するページ: http://www.ipa.go.jp/SECURITY/topics/melissa.html
2）CERT/CCのMelissaに関するAdvisory: http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html
3）NIPCのMelissaに関する警告: http://www.nipc.gov/nipc/w97melissa.htm

（平成11年4月15日受付）