セキュリティに関する話題から

長谷川　明生

Ⅰ．情報セキュリティ対策推進室の設置について

これまで，本学のネットワーク・セキュリティ対策は，情報連携基盤センターのネットワーク関係者や部局のネットワーク委員会の担当者等が協力して，半ばボランタリーで行われてきました。ネットワークトラブルやセキュリティインシデントは，夜間や休日，関係者の出張といった場合に限って集中発生すると感じているのは関係者の気のせいでしょうか？

このたび阿草センター長をはじめとする多くの先生方の御尽力で，全学の情報セキュリティに関する事柄を専門に扱う組織として，「情報セキュリティ対策推進室」が発足することとなりました。情報セキュリティ対策推進室とともに，情報戦略を全学的に考える専門の委員会もできそうです。

今年度内は，情報セキュリティ対策推進室は，坂部情報担当総長補佐を室長に，兼任室員として筆者と情報科学研究科の竹内助手の３人体制で活動します。今年度の活動は，来年度以降のセキュリティ対策室の本格的な活動のための準備期間という位置づけと考えていますが，年度内に目に見える成果を上げるために以下のような活動案が上がっています。

- セキュリティ対策推進室の長期的活動目標と計画の策定
  - ✓セキュリティ教育・啓発活動の企画立案と実行
  - ✓セキュリティに関する情報収集と発信体制の構築
  - ✓インシデントチームの設置と危機管理体制の構築
  - ✓デジタル文書管理規程等の各種規程整備の発案
- 部局セキュリティガイドライン策定の補助
- セキュリティ情報共有の手段としてのホームページ作成
  - ✓過去のインシデント情報の整理
  - ✓侵入検知システムのログ整理と公開
  - ✓過去のセキュリティ講習会資料の整理と提供
  - ✓リンク集
- 無線LANアクセスポイントの設置状況調査

上記の項目に上げる活動のうちのいくつかは，このニュースが皆様の手元に届くころには，実施に移されているかもしれません。少なくとも，情報提供優先の手作りホームページは，一部工事中かもしれませんが，公開されていると思います。

このような活動の企画や立案は，情報セキュリティ対策推進室だけでなく，情報連携基盤セン

ター，情報メディア教育センター，図書館や情報処理課と密接に協力して実行することになっています。また，実際の日常のセキュリティ維持活動は，情報連携基盤センターのネットワーク部門やネットワーク掛と密接に連携して行っていきます。

今年度の活動，来年度以降の活動案作りと並行して，現在，推進室自体の活動場所の確保や今年度及び来年度以降のための予算計画の立案をしています。当面，限られた人員での活動ですが，皆様からもアイデアや意見をお寄せいただき，情報セキュリティ対策推進室の今後の活動方針立案の参考にしたいと考えています。

是非，発足したばかりの情報セキュリティ対策推進室の活動にご協力をお願いします。

Ⅱ．その後のBlasterウィルス

８，９月に猛威をふるったBlasterやWelchiaは，2003年12月初旬沈静化しつつあります。それでも，３日に一度は，特定のサブネットで数台まとめて発症するケースが後をたちません。この原因として，以下の場合が考えられます。

１．感染状態のパソコンが放置されているところに未対策のパソコンが持ち込まれる。

２．未対策のパソコンがあるところに感染パソコンが持ち込まれる。

これから年度末にかけて，パーソナルコンピュータを研究室等でまとめて購入する機会も増えるかと思いますが，新規に購入したコンピュータについては，必ず以下の手順で対策をしてください。

１．購入時に必ずBlaster対策用のCD-ROMをもらう。

２．このCDを使って，ネットワークに接続せずに，最低限のOSのバージョンアップとパッチを当てる。この際，必ずCD-ROMの説明書にしたがって作業してください。

３．上記の作業後，ネットワークに接続して，Windows updateを，パッチが表示されなくなるまで繰り返します。

４．Officeソフトウェアを導入している場合は，Officeのアップデートを忘れないようにしてください。ついつい忘れがちになりますが，Officeにも問題がないわけではありません。

上記のような注意を払わないと，だらだらと１年以上にわたってBlasterやWelchia及び，これらの亜種が全学的に蔓延し続けることになります。早く学内だけでも絶滅宣言を出したいところです。

Blasterとは別のマイクロソフトのアップデートを装った電子メールが出回っています。このメールの中身は，本当にマイクロソフト社のセキュリティページと紛らわしい雰囲気の凝ったHTML形式で，ウィルスの本体がパッチのような名前で添付されています。マイクロソフト社のパッチだと思って実行すると感染してしまいます。本学では，メールゲートウェイでウィルス部分は検出及び削除されています。しかし，家庭でブロードバンドを楽しむ場合には，くれぐれも注意してください。マイクロソフト社から，利用者宛に直接アップデートが電子メールで送られることはありません。

これらのウィルスとは別に，いわゆる「デマ・ウィルス」が流行しています。これは，不幸の

手紙と同様のチェーンメールで,「○○という名前のファイルがシステムのフォルダにある場合は,ウィルスなので削除してください。また,ウィルスの蔓延を防ぐために,可能な限り多くの知り合いにメールを転送してください」といった内容です。実際のメールの内容は,こんなに簡単なものではなく,よりもっともらしく詳細に「問題のウィルスの対策」について記述してあります。しかし,正規のウィルス情報は,チェーンメールのような形で伝送されることはありません。また,指示どおりにファイルを削除しないようにしましょう。でないとシステムを損傷することがあります。

Ⅲ．SPAMの加害者にならないために

SPAMの手口がますます巧妙になっています。最近,いわゆるオープンPROXYサーバを使ったSPAM発信が問題となっています。PROXYサーバの設定が,不十分だと外部から接続でき,メール中継も可能な場合があります。PROXYサーバを立てる場合には,中継を許可するIPアドレスだけでなく,中継を許可するポート設定にも注意してください。Webキャッシュもアクセス制限を再度確認しておいてください。

NICEでは,外部からのメールを直接受けられるサーバを限定していますが,オープンなPROXYとメール中継制限のされていないメールサーバの組み合わせが,SPAM発信源に利用される例があるようです。学内にオープンPROXYが存在しないという保証はありませんので,学内専用のメールサーバであっても,オープンリレー対策はしておいてください。

これらの手口に加えて,ウィルスやワームとともに,SPAM中継用のプログラムを埋め込み,外部からコントロールするという悪質な手法も蔓延しています。

Ⅳ．著作権等の知的権利の保護について

いわゆるP2Pソフトウェアを使った音楽・映画といったコンテンツの違法なやりとりが急増しています。P2Pは,ソフトウェアの作者も含めて捜査の対象となり,昨年11月末には,逮捕者も出て世間の注目を集めました。

P2P（Peer to Peer,ピア　ツー　ピア）技術では,P2P網に参加するコンピュータにサーバとかクライアントといった概念は存在しません。P2Pソフトウェアを導入したら,近くのP2Pソフト網に参加しているホストに接続するだけです。いったん接続できれば,適当にリクエストを出しておけば,リクエストが網上を転送され,網上にリクエストしたコンテンツがあれば直接リクエストを出したホストにコンテンツが送られます。これがP2P（Peer to Peer）の所以です。最新のP2Pソフトでは,ポート番号を自由に変更できるだけでなく,発見を困難にするための暗号化等まで工夫されています。P2P技術そのものは,非常に高い可能性を持ったコンテンツ流通形態であったり,コンテンツ共有や検索形態ですが,著作権等で守られたコンテンツの不正流通手段として使われているところに問題があります。いろいろな工夫のために直接の検出は困難なので,P2Pの特質を逆用したおとりがあちらこちらに仕掛けられています。そこまでしなくても,日常的なトラフィック監視や,IDSのログの異常（最近,奇妙なポート番号を使った通信があります）

で，完全ではないにしろ，発見できます。大学・家庭を問わず著作権等の諸権利を侵害する行為は，絶対にやめてください。

Ⅴ．安全のコスト

通信の秘密を守るために，SSHが当たり前のように利用されるようになりました。しかし，ある種の作業には，このような暗号化には大変高いコストがかかるという例を紹介します。

発端は，統計処理用アプリケーションの起動に数分かかるという現象でした。厄介なことに，人によって，この症状が出たり出なかったりします。このように人や端末によって発生したりしなかったりする障害は，問題点を発見しにくいものです。関係者一同で何日も悩んでいたのですが，SSHに関係していそうだと思い当たりました。SSHを利用していない利用者及びSSH利用者でもDISPLAY環境変数を設定していると問題の現象が発生しないということから，SSHによるXウィンドウの自動ポートフォワーディングによる暗号化処理の時間だったわけです。通信の秘密を守ることと，効率について考えさせられるトラブルでした。

並列コンピューティングをインターネット上で実現していこうとすると，通信の秘密の確保は重要です。しかし，CPU間やプロセス間の通信を逐一暗号化・複合化していたのでは，早いコンピュータの性能を通信が生かせないという，今回の問題と類似のことが発生します。セキュリティと性能のトレードオフの問題は，今後のグリッドコンピューティングの実用化に向けて克服しなければいけない重要な問題です。

（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）