低温研ネットワークインシデント報告 2008

千貝 健[1,2]、小野 数也[1]、福士 博樹[1,2]

1. 技術部先端技術支援室
2. 所内ネットワーク運用委員会

1　序

コンピュータ・ネットワーク資源の円滑な運用は、研究活動に必要不可欠である。しかし、操作ミスなどを含めたなんらかの原因により、たびたび円滑な運用が出来なくなる（ネットワークインシデントの発生）。所内で起こったネットワークインシデントに対し、所内ネットワーク運用委員会は技術部先端技術支援室とともに対応している。2006 年の報告 [1] では、2005 年 4 月から 2006 年 1 月まで低温研内で起こったインシデント例と 2006 年 1 月に多かったインシデントを報告したが、今回はそれ以降に起きたインシデントの中から数例を報告する。

2　低温研全体へ影響を与えたインシデント

2.1　USB メモリを介して感染するウイルス

- 状況：教員同士が USB メモリを用いてファイルをやりとりしていた。2008 年 2 月 14 日 10:00 頃、USB メモリを PC に接続したところ、トレンドマイクロ・ウイルスバスターにより、POSSIBLE_OTORUN2（不正プログラムを実行させる疑いのある autorun.inf ファイルを発見した際の検出名）が検出された。調査したところ、USB メモリを介して感染するウイルスに感染したことがわかった。ウイルスバスターでは、不正プログラムを実行させる疑いのあるファイルを発見することは出来たが、ウイルス感染を防ぐことは出来なかった（新種のウイルスであったため、ウイルスバスターがまだ対応していなかった）。POSSIBLE_OTORUN2 が検出された時点ですぐにネットワークから切り離したため、ネットワークを介して他の PC への攻撃・ファイルのアップロード（情報の流出）等は最小限に抑えられたと思われる（もし、ウイルスにその機能があればだが）。確認できたウイルスの動作は、以下である。
  - Windows で、USB メモリを PC に接続し、ファイルを見るとウイルス感染する。Windows の標準設定では、USB メモリを接続するだけで感染する。
  - 全ファイルシステム（外付けハードディスク、USB メモリも含む）に自身をコピー。
  - フォルダオプションの変更を無効にする。（例：隠しファイルを見えるように設定変更しても、自動的に見えないように設定が変更される）
  - autorun.inf ファイルを隠蔽する。
  - レジストリの関連部分を書き換えても元に戻す。
  - My Document フォルダ内の全ファイルを USB メモリにコピーする。

  教員同士がやりとりしていたファイルは、感染した USB メモリごと所外に持ち出す予定だったため、感染に気がつかなかった場合は所外に感染が広がったおそれがあった。
- 障害原因：教員の一人が、以下のような状況で PC を使用していた。
  - OS のアップデートを行っていない。
  - ウイルス対策ソフトを使用していない。

    - 自宅の PC との間で、ウイルスチェックをせずに、USB メモリを使用してファイルのやりとりをしていた。

  この教員の PC にウイルス対策ソフトをインストールし、ウイルス検索・削除を 2 月 18 日に行ったところ、100 件以上のウイルス・スパイウェアが確認された。この教員がこれらのウイルス等をどこから持ち込んだのかは不明である。学内の感染した PC からのセキュリティホールを狙った攻撃を受けた、自宅からウイルスを持ち込んだ、メールに添付されたウイルスを実行した等、ウイルスの感染経路はいろいろ考えられる。また、過去に感染したウイルスが、ウイルス自身のアップデート機能で機能強化した可能性もある。さらに、この PC がネットワークを介して他の PC を攻撃していた可能性もある。後述の同様なウイルスに感染したマシンは、この PC 経由で感染したかもしれない。
- 対処状況：
  別のウイルス対策ソフト（F–Secure）で、駆除できた。ウイルス情報をネットで調べ、レジストリを手動で修正した。
  ウイルスバスターは 2 月 15 日のアップデートで対応したことを確認した。
- 事後改善策：メールで所内に注意を促した：新種のウイルスが出ていること、OS のアップデートをすること、ウイルス対策ソフトを使用すること等。
- USB メモリを介して感染する同様なウイルスが、2008 年 3 月 7 日にも発生した。上記ウイルス、またはその亜種と思われる。
- その他のウイルス感染は、2006 年 2 月から 2008 年 9 月まで 10 件あった。その原因のほとんどが、Windows アップデートを行っていなかったためセキュリティホールをつかれた、メールに添付されたウイルスを実行した、である。

2.2　改修工事中のネットワーク切断

2007 年度、研究棟の改修工事が行われた。改修工事に伴い研究所内のネットワーク配線が大きく変更されたが [2]、その際、以下のような予期していなかったトラブルが発生した。仮の部屋への一時退避や引越し後の居室内での LAN 配線のトラブルが多かった。居室内での LAN 配線のトラブルは日常的に起きているが、改修に関連して集中した形である。ハブや光ケーブルを建物内に残したまま改修工事を行ったため、それに関するトラブルも多かった。改修工事を行っている場所には、工事業者立ち合いでなければ入れないため、原因の究明や対応にいつもより時間がかかった。

- 2007 年 9 月 10 日：昼前にネットワークが停止した。数分で復帰した。原因不明。
- 2007 年 9 月 25 日 17:00 頃：研究棟から分析棟で通信が出来なくなった。研究棟改修工事中、誤って研究棟と分析棟間の光ケーブルを損傷したためであった。9 月 26 日 10:40 頃復旧した。
- 2007 年 11 月 15 日：ある部屋で LAN が使えなくなった。部屋の移動作業後、ハブに接続する LAN ケーブルの種類を間違っていた（クロスとストレートを逆に使う）。
- 2007 年 11 月 19 日：改修作業中の避難場所である講堂で有線 LAN が使えなくなった。部屋の移転時に、誰かが情報コンセントと仮設のハブ間の LAN ケーブルを外して持っていったようだ。別の LAN ケーブルを使い復旧した。
- 2007 年 11 月 21 日：ある部屋で LAN が使えなくなった。部屋の移動作業後、一つのハブに LAN ケーブルの両端が接続されていたため、ループが起きていた。部屋の住人の配線ミスだった。

- 2007 年 11 月 22 日：講堂で無線 LAN につながりにくくなった。新住人が持ち込んだ無線 LAN のチャンネルが、既設の無線 LAN のチャンネルに重なっていた。片方を設定しなおして回復した。
- 2007 年 11 月 27 日：講堂で無線 LAN が使えくなった。仮設の無線ルータにつながっていた LAN ケーブルを誰かが勝手に外したようだ。
- 2008 年 1 月 12 日：低温研のネットが数時間停止、原因不明。
- 2008 年 1 月 18 日：低温研の光ケーブルの移設作業で、当初 3 分程のネットワーク停止予定だったが、移設作業が終わらず、移設前の状態に戻した。調査の結果、光ケーブルの配線ミスがあったようだ。
- 2008 年 2 月 5 日：17:40–18:00、研究棟 2F のネットワークがつながらなくなった。改修工事中、ハブの電源コネクタが緩んだとのこと。
- 2008 年 2 月 10 日：08:40–13:40、研究棟、新棟のネットワーク停止。原因不明。
- 2008 年 2 月 13 日：13:26–13:36、研究棟、新棟のネットワーク停止。ハブの電源ケーブル抜けが原因。
- 2008 年 2 月 19 日：8:00–10:30、研究棟・新棟、ネットワーク切替え工事終わらず、元の状態に戻して後日に持ち越し。後日、auto–auto ネゴシエーションで接続不可、1G Full–1G Full 固定で接続可能を確認したので改めて工事を行った。
- 部屋の移転後に DHCP ルータを設置する際に、WAN 側と LAN 側の接続を逆にしたため、不正 DHCP サーバが所内に設置された状況になったことが、３件あった。

2.3 無線 LAN チャンネル重複、オープンアクセス等

最近、無線 LAN を設置する研究グループが多くなってきた。関連するトラブルも増えている。

- 2006 年 12 月 22 日：ある研究グループから、昨日まで使えていた無線 LAN がつながらない、と報告を受けた。となりの部屋に、FON[*1]の無線 LAN ルータが、既設の無線 LAN と同じチャンネルを使用して動作していた。FON の無線 LAN ルータ設置者に撤去してもらった。北大内での FON の使用の可否は不明である。
- 2008 年 2 月 4 日：オープンアクセス（部外者を含む不特定多数の者が無断で使用できる状態）の無線 LAN があるとの報告を受け、調査した。使用場所が確認できたので、管理者に連絡した。2 月 12 日、パスワードが設定されているのを確認した。
- 2008 年 5 月 14 日：所内にオープンアクセスの無線 LAN ルータがあるという報告を受け調査したところ、所外（学内他部局）に設置されたオープンアクセス無線 LAN ルータを発見した。情報基盤センターネットワークチームに連絡して、対応してもらった。
  ⇒ 低温研- 他部局間の距離に比べ、低温研- 大学敷地外の距離が短い。所内に無線 LAN を設置する場合、学外からのアクセスも考慮しなくてはならない。

[*1] http://www.fon.com/jp/

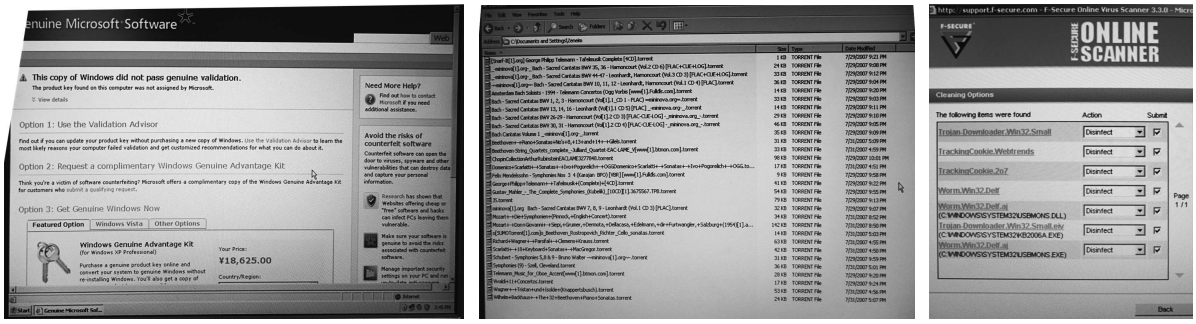

図 1　左）海賊版 Windows **が** Windows Genuine Advantage（WGA）**で確認された様子、中）**P2P **でダウンロードまたは共有していた音楽ファイル、右）発見されたウイルス。**

3　外国人客員研究室設置の PC について

外国人客員研究室設置の PC **の設定（ネットワーク設定、プリンタ設定、英語版** Windows **と** MS Office **がインストールされているかの確認）を依頼された。インストールされているソフトの種類・バージョンの把握の為に調査を行ったところ、**2 **台あるうちの** 1 **台（古い方の** PC**）が以下のようなとんでもない状況にあることがわかった。**

- MS Windows 98 **英語版を勝手にアップグレードし、海賊版** Windows XP **英語版** + Office 2003 Professional **ロシア語版をインストールしていた。 ⇒ 図** 1 **左**
- **北大で使用が禁止されている** P2P **ファイル交換ソフト（**BitTorrent client**）がインストールされていた。また、音楽ファイルを共有していた。 ⇒ 図** 1 **中**
- **ウイルス対策ソフトがインストールされていなかった。**
- **ウイルスに感染していた。 ⇒ 図** 1 **右**
- **リカバリ用** CD **等が散逸していた。**

PC **を設置してから置きっぱなしであったため、いつからこのような状況になっていたのかは、不明である。**PC **を持っていない研究員が二人以上同時に研究所を訪れ** PC **を使用したとき以外は電源が入っていなかった（**LAN **に接続されていなかった）ことが唯一の救いである。これに対し、以下のように対処した。**

- **ただちにこの** PC **を、フォーマットし、破棄した。**
- **リカバリ用** CD **等の散逸を防ぐため、**CD **等は事務部倉庫に保管することとした。**
- **置きっぱなしを止め、定期的（研究員の入れ替わりのタイミングで）にリカバリ** CD **等からの再インストールとアップデート、必要なソフトの再インストールをすることとした。これらは、技術部先端技術支援室で行うこととした。**
- **外国人客員研究室に設置する** PC **は、基本的なもの（**OS（MS Windows）**と** MS Office（Word、Excel、PowerPoint）**、ウイルス対策ソフトだけをインストール、自動アップデート機能を有効、ネットワークとプリンタ設定）とする。設置までは事務部と技術部で責任を持つ。その他の研究で必要なソフトウェア等の購入・インストールについては、研究員を招いた研究グループの責任で行ってもらうこととした。**
- **セキュリティマニュアル英語版** [3] **を外国人客員研究室に設置することとした。**

4 おわりに

2008 年、所内ネットワーク運用委員会では低温科学研究所情報セキュリティ対策手引を作成した。その中にあるように、サポートの終了している OS を搭載した PC を使用しない、OS のセキュリティアップデートを欠かさず行う、ウィルス対策ソフトを導入しパターンファイルの更新を欠かさず行う、等の基本事項を行ってくれれば、新種のウイルスには完全に対応できないかもしれないが §2.1 のように「ウイルス対策ソフトを使用していたからウイルスに感染したことにすぐ気がつくことが出来た」となることもある。コンピュータ管理の基本を確実に身につけてほしい。

§3 の外国人研究員室は、「管理されていなかった」ことが最大の問題であった。「PC を学生が管理している」研究室では、管理していた学生が卒業する直前に設定した PC をアップデート無しで使っている場合が多々ある。観測装置制御用 PC のように、OS をアップデート出来ない（OS をアップデートすると、装置制御ソフトが動かなくなる）PC がそのままネットワークに接続されていたりする。PC を廃棄したのに IP アドレスの返還をしていない場合もある。「管理されていない」というのは、表に現れていないだけでとても多いのかもしれない。

所内に設置されているハブ（各研究グループが独自に設置しているものを除く）は、ほぼ全てギガビットイーサネット対応となった。障害ではないが、ギガハブに接続されているにもかかわらず、ギガハブ- 各部屋の情報コンセント間で、フル結線されていない（8 線中 4 線のみの結線）ツイストペアケーブル（100BASE–TX までしか使用出来ない）が使用されているところがある。使用実態を調査し、ケーブルの引き直しをしなければならないだろう。

参考文献

[1] 千貝 健, 低温研ネットワークインシデント報告, 北海道大学低温科学研究所技術部技術報告, **11**, 22–25, 2006

[2] 小野 数也, 千貝 健, 福士 博樹, 改修工事に伴って変更した低温研のネットワーク, 北海道大学低温科学研究所技術部技術報告, **13**, 53–56, 2008

[3] 小野 数也, 千貝 健, 福士 博樹, 低温科学研究所情報セキュリティ対策手引の作成, 北海道大学低温科学研究所技術部技術報告, **14**, 51–52, 2008