医学情報基盤室の業務紹介

-インターネットインシデント対応の一例-

樺山　綾子、安達　苗生美、大神　宏路
筑波大学医学医療系技術室
〒305-8575 茨城県つくば市天王台 1-1-1

概要

医学情報基盤室の業務は、主に、1.医学サブネットの維持管理およびトラブル対応、2.医学医療系 Web サイト（の一部）とメールサーバの維持管理、3.医学地区に導入されているセキュリティドアシステムの維持管理、4.医学コンピューター室の維持管理、及び大型プリンター印刷サービス、である。

医学情報基盤室は、技術職員の所属部局であるが、医学サブネット委員会の内部組織でもある。その為、医学地区で発生したインターネットインシデントが起きた時、速やかに対応処理しなければならない。

今回は、1.の中で、最近問題になっているインターネットインシデントへの対応を紹介する。

キーワード：インターネット、インシデント、コンピュータウイルス

１．はじめに

最近、教育関係者がデジタルデータを紛失する、あるいは流出させるニュースに事欠かない。その一端となるコンピューターウイルスの侵入経路は、様々である。

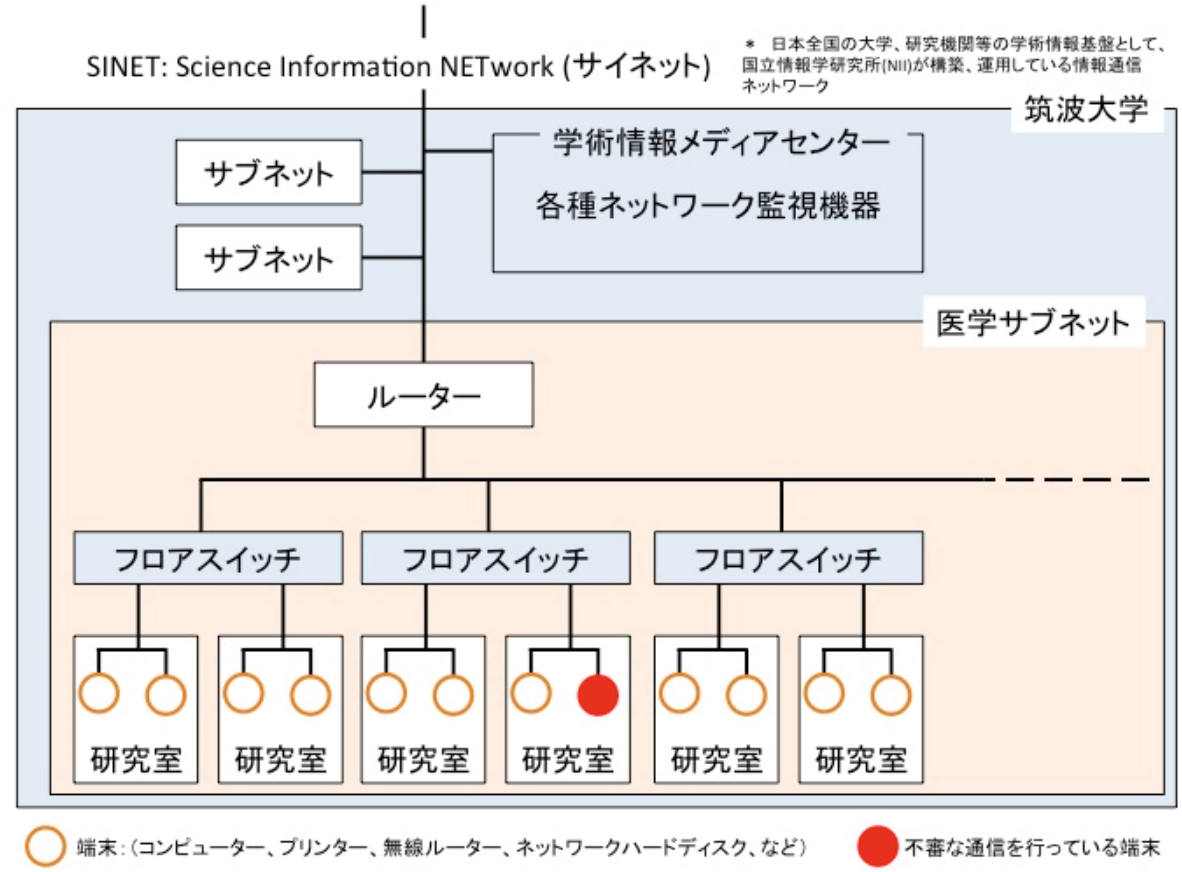
- 知人や業者、省庁を装ったメールに添付ファイルとして送られてくる。
- USB メモリーなどの外部データ保存機器が媒介する。
- 無料ソフトを装う。
- Web サイトを閲覧しただけで感染する。

などがある。

コンピューターウイルスに感染した機器の影響も多種多様である。

- コンピューターを起動できなくする。
- ハードディスクに保存されたデータを破壊、あるいは暗号化し本来の使用者が開けなくなる。

医学サブネットの概略図



・ 怪しいメッセージを画面上に表示させる。

などは、まだ判り易い。

データ（メールのアドレス帳、写真、文書ファイルなど）を外部に送信する、遠隔操作によって他のコンピューターを攻撃するのに利用される、などの場合は、感染コンピューターの使用者が気付かないことがほとんどである。

但し、管理されたネットワークでは、不審な通信として感知できる場合もある。

医学情報基盤室では、学術情報メディアセンターをはじめとした各部局と協力して、インシデントに対応している。

以下､平成 28 年 6 月に医学サブネットで発生した事例を報告する。

作業者の氏名が入っていない用件は、医学情報基盤室の技術職員が対応している。

1 日目

大学外部から本学情報基盤課経由で医学サブネット委員会宛に､｢不審なサイトにアクセスを繰り返す端末が医学地区内のネットワークに存在していて、なおかつインターネットバンキングに関連したマルウェア（コンピューターウイルスの一種）に感染している可能性が高い」との情報が入った。

ルーターの通信情報（ログ）を解析し、アクセスを繰り返す端末の物理アドレスを調べ、学術情報メディアセンターに依頼して、どのフロアスイッチのどのポートに接続しているかを特定した（讃岐勝先生)。

ポート番号と部屋の対応表を元に、不審端末の存在する部屋を訪問するも、部屋の使用者が不在だったため、フロアスイッチから該当の部屋に繋がっている LAN ケーブルを抜いた。

2 日目

部屋を訪問し、在室していた教員から事情聴取した。

知人を装っていたメールの添付ファイルを不審に思わずに開封したら､感染した模様｡受信したメール及び端末の動作ログを確保した（讃岐勝先生)。

次に、USB にて持参した別種のアンチウイルスソフトを実行した。

スキャンしたファイルのうち、感染ファイルを駆除した。インストールされている McAfree LiveSafe も実行した。感染ファイルの検出は無かったので、様子を見るために LAN に接続した。

午後、再び不正アクセスがあったことを確認した（讃岐勝先生）。該当ユーザーの部屋に伺い、不在だったため、フロアスイッチと部屋を繋ぐ LAN ケーブルを抜いた。

3 日目

該当ユーザから連絡があり、在席中だというので部屋に赴いて作業を開始した。コンピューターの動作をチェックしたところ、アンチウイルスソフトが削除した筈のコンピューターウイルスが稼働していて、駆除しきれていなかったことを確認した。

利用者の了承を得て、アンチウィルスソフトを本大学で契約している Symantec Endpoint Protection に変更した。

インストールした時点で、上記ウィルスが隔離されたことのメッセージが表示された。

その後、一時的にネットワークに接続させて定義ファイルを更新し、またネットワークから隔離して再起動させた。

再起動後、完全スキャンを実行したら、1 日目には検出されなかった別種のコンピューターウイルス（トロイの木馬）を複数ファイルで検出した。

再度､再起動後､アクティブスキャン（完全スキャン）を実行し、問題のないことを確認した。

＊ 週末を挟んだため、作業日が飛んでいる。

6 日目

コンピューターをネットワークに接続したところ､Endopoint Protection が マルウェアを検知､処置後に強制再起動がかかった。

Microsoft Safety Scanner、Spybot、F-Secure でスキャン実行したが、両方ともウィルスやマルウェアの類は検知されなかった。

7 日目

6 日目に Endpoint Protection が駆除したマルウェアは、感染 PC をネットに繋いだことで 既設置のバックドアから呼び込まれた可能性を考慮して、コンピューターのリカバリを提案し、利用者本人が作業した（讃岐勝先生）。

レポートを取りまとめ(讃岐勝先生)､情報セキュリティインシテント対応チーム（筑波大学 ISIRT）に提出した（浅野美礼先生）。

２．補足

同年 9 月にも､医学サブネット内から不審な通信を起こすインシデントが発生しており、3 日後に報告書を提出している。

３．考察

医学情報基盤室スタッフとして、インシデント発生件数を減らすために、日頃の注意喚起と万が一発生した時の的確な対応を心掛けたい。

一方、サーバーやルーター、コンピューターからの情報収集や解析は、ボランティアで協力している教員が本来の業務の合間を縫って作業している状態である。医学情報基盤室所属の技術職員および技術専門職員は、教員の指示に現場へ赴いての説明やアンチウイルスソフトの実行などの補助作業を行っている。なお、医学情報基盤室スタッフのコンピュー

ターウイルスへの対応は、一般ユーザーとほぼ同程度の情報収集能力であり、より詳細な対応を求められた場合、サーバー管理を委託している業者や上記の教員らと相談している。

４．謝辞

浅野美礼先生（医学医療系　准教授：医学情報基盤室室長）
市川政雄先生（医学医療系　教授：医学医療系広報・情報委員会委員長）
讃岐勝先生（医学医療系　助教）
大神明子（シニアスタッフ：医学情報基盤室勤務）
照井直人（医学医療系　特命教授）

Introduction of the Medical Information Technology Office, University of Tsukuba: An Example of Internet Incident Response

Ayako Kabayama, Naomi Adachi, Hiromichi Oogami

Technical Service Office for Medical Sciences, University of Tsukuba,
1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8575 Japan

Keywords: Internet, Incident, Computer Virus