

学校名	鶴岡工業高等専門学校	NO. 1	
氏名	横田 礼	職名	技術職員
研究開発 技術等の題名	最近のウイルスの形態について		

1. きっかけ

今春、鶴岡高専でウイルスが活動していることが判明した。それは **BOT** ウイルスと呼ばれるもので、外部へネット経由の**攻撃**をしていたらしい。幸いにも私の所属している部署のコンピュータには感染は無かったが、鶴岡高専の教育研究技術支援センターと機械工学科のホームページの更新に携わる者としてウイルス対策を考えてみたいと考えた。

2. ウイルス動向

2000年頃より急激に増加をしている。一般家庭にもネットに繋がるパソコンが普及してきた時期でもある。この頃よりウイルスがネットワークに強く依存するタイプが増えた。愉快犯よりも**犯罪性の強い**のが特徴である。

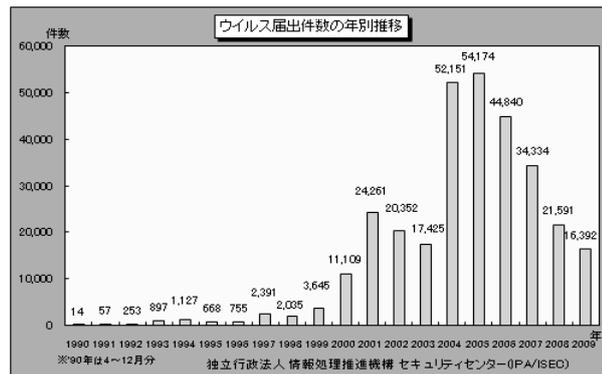


図 1 IPA によるウイルス届出件数の推移

3. ウイルス形態

最近の目立つウイルス形態には次の三つのタイプがある。

(i) USB 感染型ウイルス

パソコンに USB メモリが接続されると、その USB メモリの中に置かれたプログラムを自動的に実行する機能がある。この機能を悪用したものである。

「AutoRun.inf」の中身を改変し、感染を増やしていく。

中には WEB から更に不正プログラムをダウンロードするタイプがあり、そこから多重感染している事例もある。

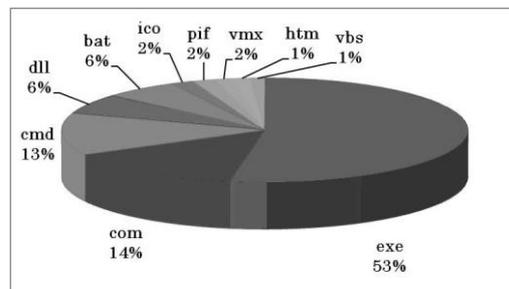


図 2 Trendmicro によるウイルス分析

学校名	鶴岡工業高等専門学校	氏名	横田 礼
-----	------------	----	------

(ii) GUMBLAR (ガンブラー)

2009 年後半に発生を確認された。感染した WEB を通じて感染を拡げていく。正規 Web サイトを改ざんしサイト訪問者を不正な Web サイトに誘導、不正プログラムに感染させようとするものである。日本では別名の「GENO ウイルス」の方が有名。

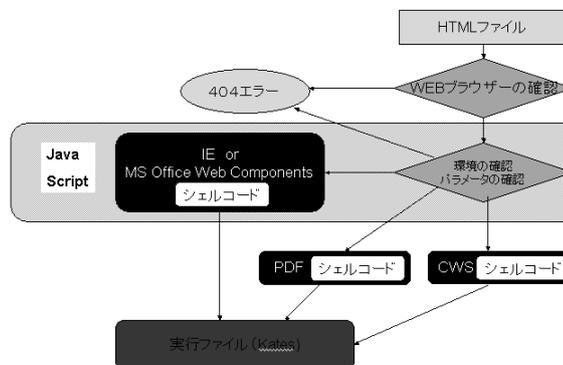
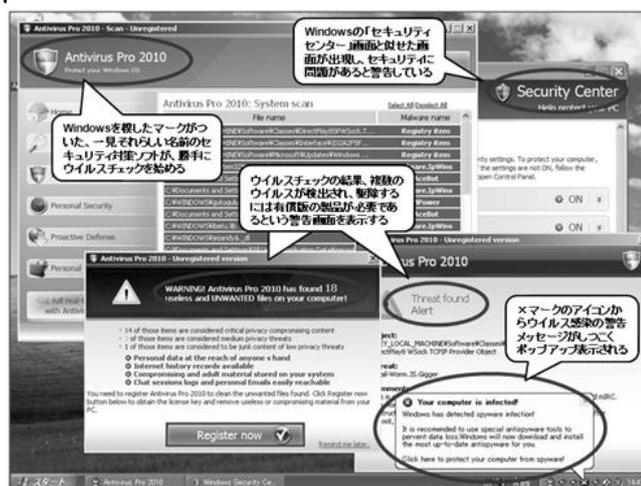


図 3 GUMBLAR の攻撃フローチャート

「PC がウイルスに感染している」という偽の警告でユーザーの恐怖心をあおり、問題を解決するには有償版を購入する必要があるというメッセージを表示して金銭をだまし取ろうとするもの。不正ウイルスが後ろにあることも非常に多い。



ルス対策

ウイルスに感染しないための対策として以下のことが挙げられる。

- アンチウイルス製品の導入
- OS のバージョンアップ
- セキュリティホールを塞ぐ
- 無用なソフトはインストールしない
- 敵（ウイルス）の特徴を知っておく

5. 鶴岡高専の取り組み

発表内で紹介します。

機 器 等 使 用 の 有 無	有 (PowerPoint 2007) ・ 無
-----------------	--------------------------