情報流出の原因となる三種類のウィルスの比較

佐世保高専情報処理センター

１．Antinny
（別名：ぬるぽワーム）

・P2P ファイル交換ソフト（Winny, Share 等）による通信で蔓延したウィルスで、P2P ファイル共有機能を利用して情報を流出させる。
・感染したパソコンのデスクトップ画面を写し取った画像ファイルや、デスクトップ上のファイルを P2P 通信網に公開してしまう。
・感染しても P2P ファイル交換ソフトを使っていなければ情報流出は無い。
・本校ではファイヤーウォールで外部とは P2P 通信はできないので、感染しても校内からの直接の情報流出は防ぐことができる。しかし、感染したパソコンを外部に持ち出したら、そこから流出する。

２．山田ウィルス
（別名：TROJ_DROPPER、TROJ_MELLPON、Generic）

・Antinny と同様に P2P ファイル交換ソフト（Winny, Share 等）による通信で蔓延したウィルスだが、Web サービス機能を持ったプログラムなので、P2P ファイル交換ソフトの有無に関係なく情報を流出させてしまう。
・デスクトップ画面を写し取った画像ファイルを Web 公開（http 通信）し、その URL を２ちゃんねるなどの掲示板に書き込む。
・バックドアと呼ばれるセキュリティホールを作り、外部からの操作を可能にする。
・本校ではファイヤーウォールで外部からのアクセスは出来ないので感染しても外部への情報流出は防ぐことができる。しかし、校内のパソコン間でのアクセスは可能なので、情報流出の危険はある。また、感染したパソコンを外部に持ち出したら、そこから流出する。

３．山田オルタナティブ
（別名：Backdoor.Nodelm、BKDR_AGENT.BOG、BackDoor-CYC）

・山田ウィルスの機能に加え、そのパソコンのディスク全体を Web 公開してダウンロード可能にする。
・感染したコンピューター間でリンクを貼り、更に他の感染者リストを作成する。
・P2P 通信網に加え、メールの添付ファイルや Web ページからのダウンロードからも感染する。校内のパソコンが直接感染する危険がある。
・本校ではファイヤーウォールで外部からのアクセスは出来ないので感染しても外部への情報流出は防ぐことができる。しかし、校内のパソコン間でのアクセスは可能なので、情報流出の危険はある。また、感染したパソコンを外部に持ち出したら、そこから流出する。