P2P 対策
–対策装置による検出結果–

江藤博文* , 田中芳雄†
総合情報基盤センター‡

1　P2P

1.1　仕組み

P2P はファイル共有の仕組みの一つです。特定のサーバを利用せず、各クライアントがサーバ機能も持つことでファイルを共有・交換します。特定のサーバを必要としないために簡単に参加でき、また匿名性が高いことで爆発的に普及しました。

1.2　危険性

もともとは他の不特定多数の人とファイルを簡単に共有・交換することが目的でしたが、共有するファイルのほとんどが違法コピーされたソフトや画像・動画のため著作権侵害問題が発生しました。これらのファイルは各クライアントで自動的に共有されるため、意図せずに自分の PC に著作権侵害のファイルが置かれることになります。

共有・交換されるファイルにウィルスやスパイウェアまでも存在したため、爆発的に感染が広がる結果ともなりました。ウィルスの中には暴露ウィルスという種類のウィルスがあり、P2P の仕組みを利用して意図しないファイルを勝手に共有・交換します。このため、P2P ソフトをインストールした PC による企業や自衛隊などの情報漏洩事例が後を絶たたないのが現状です。個人の PC であっても住所録などを管理している場合があるので、知人の生年月日や住所などの個人情報も漏洩する可能性があり注意が必要です。

*etoh@cc.saga-u.ac.jp
†yoshirin@cc.saga-u.ac.jp
‡http://www.cc.saga-u.ac.jp/

2　学内の対応

P2P の法律的な解釈はまだはっきりしませんが、現状のままでは大学内でも情報漏洩や著作権侵害を引き起こしかねません。このため、平成 18 年 3 月に学長名により学内での P2P の使用を禁止しました。

学内では P2P ソフトは利用しない様にお願いします。また、教職員の方々には研究室の学生への指導をお願いいたします。

3　対策

3.1　対策装置

総合情報基盤センターには以前からファイアウォール装置を設置して、学外からの攻撃を防ぎ、学内からの不要なパケットを制御しています。しかし、P2P のパケットは通常の通信装置では検出が難しいため、P2P 専用の対策装置を平成 19 年 9 月より設置しました。

3.2　P2P 検出ログ

P2P 装置より出力されるログの平成 19 年 11 月から平成 20 年 3 月までの結果をグラフとしてまとめました。P2P 検出結果 1 回を 1 として表示しています。ログの容量の関係で、1 日最大約 25000 が最大回数となります。

3.2.1 検出数

日別検出数を図 1 に示します。

当初はかなり多くの数の検出がありましたが、徐々に検出数は減少しています。これは、検出される毎に当該端末の管理者や端末設置部局のネットワーク管理者に連絡して対応をして頂いた結果だと思われます。これらの対応の結果、たまに多く検出される場合がありますが全体的には減少傾向にあります。

3.2.2 検出プロトコル

P2P プロトコル別検出割合を図 2 に示します。

Edonkey と BitTorrent で 8 割強となっています。

3.3 考察

図 2 で分かる通り、最も多く検出されているプロトコルは Edonkey で、全体の半分以上を占めています。Edonkey が検出された際に調査を行った結果、ほとんどの場合が FlashGet と言うソフトでした。FlashGet はダウンロードソフトだと紹介されていますが、実際には P2P ソフトの一種であり、このソフトを介して感染するスパイウェアなども確認されています。FlashGet はインストールされているだけで自動的に通信が始まりますので、大学のネットワークに接続する PC には絶対インストールしない様にしてください。

次に多い BitTorrent ですが、これは各種ソフトに組み込まれている場合が多いために検出数が多くなっていると思われます。

Winny は全体の 1%にとどまっていますが、これはニュースなどで情報漏洩の際に良く出てくるため、利用者が注意をしているのだと思われます。

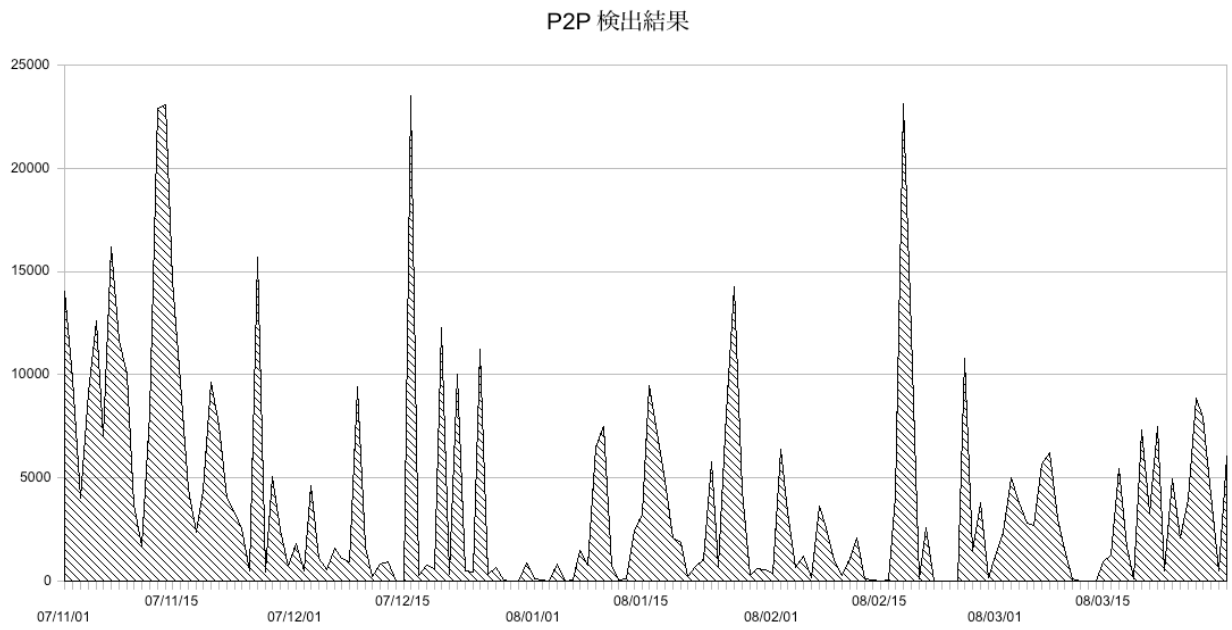

図 1: 日別検出数

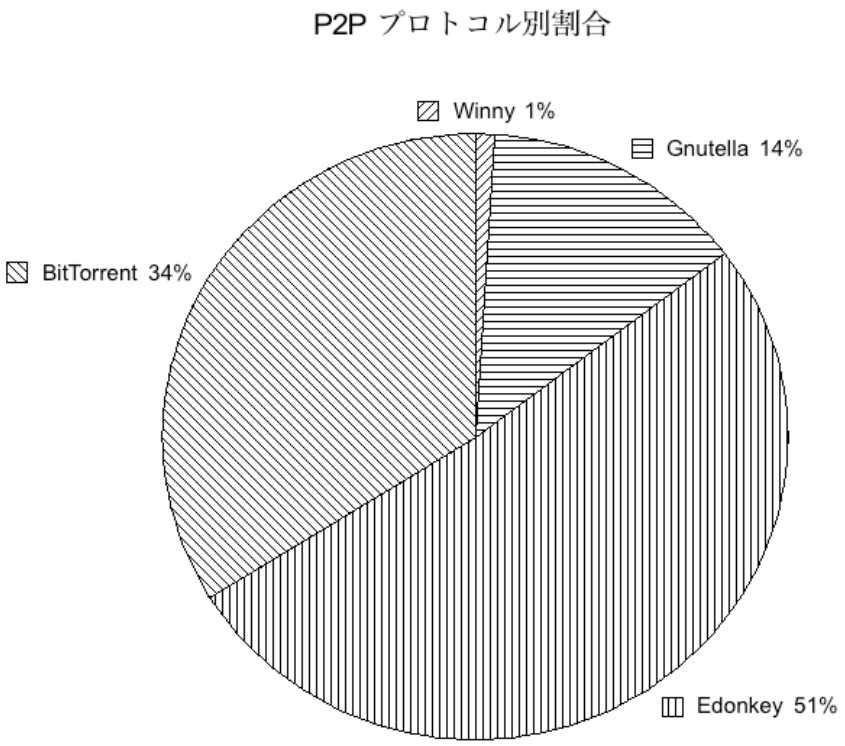

図 2: プロトコル別検出割合