佐賀大学 CNC Computer and Network Center
総合情報基盤センター・ニュース

CNC News No.68 2013.6.26

http://www.cc.saga-u.ac.jp/

問い合わせ
メインセンター（本庄地区） :8592
医学サブセンター（鍋島地区） :2154

1. セキュリティ対策装置 IDS の運用
2. ステルス型ウィルス感染に対する注意と対策

1. セキュリティ対策装置 IDS の運用

総合情報基盤センターでは、ウィルスに感染した学内端末の調査とウィルス感染の被害拡大を防ぐため、セキュリティ対策装置 IDS の運用を行っています。

この装置の通信ログを解析し、ウィルス感染らしき通信を発見した場合は、該当 PC 端末の管理者、該当 PC 端末の利用者が学生の場合は指導教員に、随時、ウィルス感染の調査依頼を行っています。

総合情報基盤センターより、「ウィルス感染の疑いのある PC 端末の調査依頼」で、メールが届きましたら、速やかに該当 PC 端末を調査し、ウィルス対策ソフトによるウィルスチェック・駆除等を行って頂くようにお願いします。

なお、校費で購入した PC については、総合情報基盤センターで貸し出しをしていますウィルス対策ソフトをインストールすることができますので、ご利用ください。

2. ステルス型ウィルス感染に対する注意と対策

学内でウィルス感染した PC の中に、ウィルス対策ソフト（最新のバージョン・パターンファイル）で検知できないウィルスに感染している PC 端末が複数台ありました。

このようなウィルスは、一般的に「ステルス型ウィルス（マルウェア）」と呼ばれており、ルートキット（root kit：コンピュータに不正侵入した後、その痕跡を消すソフトウェアのこと）と呼ばれる機能を持っています。

このルートキットの機能により、ウィルス対策ソフトではウィルスを検知・駆除できず、長期間ウィルスが常駐した状態でネットワーク、システムを利用するため、非常に危険なウィルスとなっています。

このようなステルス型ウィルスに感染した場合は、ルートキットスキャン（ルートキットがコンピュータ内に仕掛けられていないか？を検索）を行う必要があります。

ルートキット検査ツールとしては、以下の3つが利用できることを把握しており、これらは無償で利用できます。

(1) McAfee ルートキット駆除ツール Rootkit Remover
https://www.mcafee.com/Japan/mcafee/support/faq/answer_p_other.asp?wk=OT-00037
(2) Kaspersky ルートキット駆除ユーティリティ TDSSkiller
http://support.kaspersky.co.jp/faq/?qid=208288215
(3) RootkitRevealer
http://technet.microsoft.com/ja-jp/sysinternals/bb897445.aspx

総合情報基盤センターのウィルス感染の調査依頼により、ウィルス対策ソフトでウィルスが検知されなかった場合は、ルートキット検査ツールを使ってウィルス感染の調査を行ってください。