佐賀大学
学術情報処理センター
Computer and Network Center
NEWS

CNC News No.24
2005.2.4
http://www.cc.saga-u.ac.jp/

問い合わせ
本庄キャンパス(メインセンター)　:8592
鍋島キャンパス(医学サブセンター)　:2154

パスワード変更URL
https://intauth1.edu.cc.saga-u.ac.jp/

1. ウィルス侵入によるネットワーク過負荷のお知らせ

本庄キャンパスでは、複数のウィルスが侵入し多数のPCが被害にあっており、学内LANのトラフィック過負荷が発生しています。また、鍋島キャンパスでもウィルスが原因と思われる学内LANのトラフィック過負荷が起こっています。

ネットワークを介して拡散するウィルスは、感染したPCが感染できるPCを探すときに大量の通信を行います。そのため、ウィルスに感染したPCが多ければそれだけネットワークに過負荷がかかり通信障害を引き起こす原因となります。ウィルスを持ち込まないこと、ウィルス対策を怠らないことなど日ごろから注意を払うように教職員、学生の皆さんのご協力をよろしくお願いします。

さらに、MSNメッセンジャーからウィルス(W32.Bropia.J)が侵入するという事例がありました。学内にウィルスを侵入させないようにMSNメッセンジャーを利用しているユーザは利用を控えるなどご注意ください。

2. AntiVirusによる緊急ウィルススキャンのお願い

本庄キャンパスで確認されているウィルスは、W32_SPYBOT.WORM、W32.Randex.D、W32.Randex.gen、Adware.Istbar、WORM_SDBOT.AFI、WORM_SDBOT.ALB、WORM_SPYBOT.HH、W32.Bropia.J です。

これらのウィルスは、Windowsのファイル共有機能を使って感染を広げており、一度感染するとウィルスを駆除してもファイル共有を使って何度でも感染します。

学情センターでは、AntiVirusの貸し出しを行っていますので、ウィルス対策ソフトをインストールしていないユーザは、必ずAntiVirusをインストールしてください。

本庄、鍋島両キャンパスの教職員、学生の皆さん、下記の手順でウィルススキャンを行ってください。

(1) AntiVirusの定義ファイルを最新版にする
(2) PCをネットワークから切り離す
(3) WindowsXP/Meは、システムの保護機能をオフにする
(4) PCをセーフモードで再起動する(起動時にF8キーを押す)
(5) AntiVirusでウィルススキャンを行う

ウィルススキャンでウィルスの感染状況を確認してください。次に、AntiVirusのウィルススキャンでウィルスが検出できない場合もありますので、セーフモードの状態で下記のファイルがシステムフォルダ上に存在するか［スタート］→［検索］→［ファイルやフォルダ］を開きファイル検索で調べてください。
lmhosts.exe、msxml.exe、winfirewall.exe、mscrtl.exe、mscrt1.exe(数字が1～9のファイルが存在する場合もあり)

上記のファイルがシステムフォルダ上にあった場合は、AntiVirusのウィルススキャンで検出されなかったウィルスですので、手作業でウィルスの駆除を行ってください。

これらのウィルスに感染したPCは、再度ウィルスに感染しないようにするための対策として、Windowsのファイル共有を止めることが最善の方法です。Windowsのファイル共有を止める方法は、ローカルエリア接続のプロパティを開き、「Microsoft ネットワーク用ファイルとプリンタ共有」を選択し［削除］ボタンをクリックします。この対策を行うと他のPCとのファイル共有とWindowsのプロトコルを使ったプリンタの利用ができなくなりますが、ウィルス感染を未然に防ぐ方法としては効果的です。