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

CNC News No.36
2005.10.25
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/
ｼｽﾃﾑ更新作業のためﾒｲﾝｾﾝﾀｰ演習室・ﾛﾋﾞｰの
利用停止期間:**2006年2月1日～28日**

1. 学内部署名（架空）を偽ったウィルスメールの注意

ユーザから「学内から変なメールが届いている」と問い合わせが数件寄せられました。学情センターで調査したところ、メールの英文中に学内部署（架空のユーザID@cc.saga-u.ac.jpなど）からと偽ったウィルス付きメールであることがわかりました。このウィルスメールは、メールの件名が「注意を促す」ような英文になっていることが多く、メールの本文にはあたかも存在しているかのような学内部署(実は架空)から送信したように装っています。このようなウィルスメールを受信した場合は、不用意に添付ファイルを開かず直に削除してください。また、AntiVirusの「ウィルス定義ファイル」を常に最新版にするなどウィルス対策を行ってください。

```
ウィルスメールの件名
  "Returned mail: see transcript for details" や "Hello" など
ウィルスメールの本文
  Dear user *****  ←  ***** が受信者のユーザIDまたはメールアドレスなど
  本文の中身（英文）は省略
  架空のユーザID@cc.saga-u.ac.jp     ←┐ この部分が詐称されています
                                      │ 架空のユーザIDとしてadmin,serviceなどを使用
  The Cc Support Team                ←┘ cc.saga-u.ac.jpのccがcc以外の記述もあります
```

2. Spybot系ウィルスの感染注意

本庄キャンパスでは、Spybot系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Spybot系ウィルスは、感染したPCが次に感染できる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があれば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。

また、Spybot系ウィルスは、一度感染すると再感染する場合があります。Spybot系ウィルスに感染したPCは、定期的に「最新のウィルス定義ファイル」でウィルスチェックを行うようにしてください。

ウィルスの感染を防ぐため、WindowsUpdateを必ず行い、ウィルス対策ソフトをインストールし「ウィルス定義ファイル」を常に最新版にする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。なお、学情センターでは、ウィルス対策ソフト（AntiVirus）の貸し出しを行っています。