



CNC News No.7

2004.3.1

<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. 学外者による学生 ID の不正利用容疑者逮捕までの経緯
- 2. 部局等で設置している公開端末の管理

1. 学外者による学生 ID 不正利用容疑者逮捕までの経緯

学外者による学生 ID の不正利用について、容疑者逮捕の新聞報道が2004年1月27日にありました。容疑者逮捕までの経緯は下記のとおりです。

- ・2003年10月21日、附属図書館内の端末で学生 ID を使って利用していた学外者を見つけた。
- ・翌日、使用 ID に該当する学生を呼び、聞いたところ、この学外者は知らないとのことであったため、パスワード変更を指示した。別の学生も、ID 不正利用を受けた恐れがあったためパスワード変更を指示した。その後、該当する二つの ID による認証失敗の大量のログがあった。
- ・この件について、佐賀県警に相談し、2003年11月11日に事情聴取および現場検証(附属図書館および経済学部内就職相談室)があった。
- ・2004年1月26日に容疑者が逮捕され、27日に ID を取得したと思われる経済学部内就職相談室の捜査があった。その際、キーボード打鍵の記録を採取するソフトウェアおよびその記録が発見され、証拠として押収された。

2. 部局等で設置している公開端末の管理

学情センターでは、経済学部内就職相談室のコンピュータにキーボード打鍵を記録するソフトウェアが仕掛けられていたことは非常に重大な問題と受け止めています。利用者管理が行われていない Windows 端末にこのようなものを仕掛けて、個人情報抜き出すことは、あまり難しくありません。インターネットカフェで、クレジットカード情報が盗まれた事件をご記憶でしょう。また、他の部局では、公開端末が利用不可能な状態にまで利用者によって改変されている事例やウイルスだらけになる事例が起っています。

端末を設置する場合には、以下の点に十分な注意をしていただけるように、各部局にお願いいたします。また、学情センターでは技術的な相談を行います。

(1) 原則として利用者認証を行うこと。

佐賀大学では、全学生、全教職員に学情センターから利用者 ID が配布されていますので、利用者ごとの認証を行うことは可能です。

(2) 職員の目の届かないところに設置しないこと。

今回の容疑者は、経済学部内就職相談室に非常に長期間にわたって出入りしていたようです。

(3) 利用者によるシステム変更が困難な仕組みを導入すること。

何も対策をしていない端末にキーボード打鍵を記録するようなソフトウェアを入れることは非常に簡単なので、システム変更が困難なハードディスクキーパーなどの導入を検討してください。

(4) 利用終了ごとに電源を切るように指導すること。

ハードディスクキーパーを導入しても、キーボード打鍵を記録するようなソフトを起動した状態で放置し、次の利用者の情報を盗むことは可能です。電源がオンになった端末を触らないような指導が必要です。