

宛：NPO 情報セキュリティフォーラム

FAX：045-311-8747

連絡先

名 前： 情報 太郎
学校名： セキュリティ高等学校
E-Mail： isef@isef.or.jp
TEL： 045 - 311 - 8777
FAX： 045 - 311 - 8747

被害状況

- 被害ならびに被害状況 -
- ・生徒 A が授業で作成していたファイルが、本人の知らない間に内容が書き換えられていた。被害を受けた生徒 A は、なぜ自分のファイルが書き換えられているのか、状況を把握できないでいた。
- ・生徒 A のファイルを見ると、生徒 A をからかう内容に変更されていたため、学校内の他の生徒が生徒 A のファイル内容を意図的に書き換えたものと推測した。ファイルサーバでは、アクセスログを取得していないため、犯人の特定は難しいものと考えられる。

学校のコンピュータ環境・利用状況・セキュリティ対策について

- 校内のパソコン環境 -
- ・校内 LAN が敷設されており、パソコン教室で作成したファイルは、ファイルサーバに保存するルールとなっている。
ファイルサーバ：Windows2000
パソコン教室のクライアントマシン：Windows98
- 校内のパソコン利用状況や利用形態 -
- ・パソコン教室は情報の授業時以外の利用は原則として禁止している。
- ・授業では、教員の指導のもと、操作を行うこととしている。
- 校内のセキュリティ対策 -
- ・生徒側の LAN から教職員側の LAN へはアクセスできない仕組みにしている。
- ・生徒へは、情報授業時に情報モラル指導を行っている。
- ・ファイルサーバは生徒個々人のアクセス権は設定せず、生徒がアクセスできる領域へはパソコン教室のマシンから誰でもフルアクセスできる設定となっている。
- ・ファイルサーバへのアクセス状況を調べるためのログデータは取得していない。

発見の経緯

- ・発見方法：ファイルを書き換えられた生徒 A 本人から、授業実施時に直接申し出があった
- ・発生日時：平成 16 年 5 月 20 日 13 時頃
- ・発見日：平成 16 年 5 月 20 日 13 時頃
- ・事実確認：平成 16 年 5 月 20 日 13 時頃

被害への対応

- ファイルを改ざんされた生徒 A への対応 -
 - ・対応日：平成 16 年 5 月 20 日 13 時頃
 - ・対応担当者：情報担当教員（授業を担当している教員）
 - ・対応方法：ファイル改ざんを行った者の特定はできない旨を伝えた。
5 月 20 日の授業は、教員が作成したファイルを利用して授業を進めることとした。
今後は、授業が終了時にバックアップファイルを作成することを指導した。
- 在校生への対応 -
 - ・対応日：平成 16 年 5 月 24 日～28 日 情報の授業時
 - ・対応担当者：情報担当教員
 - ・対応方法：情報の授業時に改ざんが行われた事実と問題点の説明を実施。
なぜ改ざんを行ってはいけないのか、情報モラルの再確認を実施。
大切なファイルは、定期的にバックアップを取得する習慣を身に付けるよう指導を実施。

今後の対策と効果

- ・システムの対策として、生徒個々用のネットワークアカウントを作成し、ファイルサーバのフォルダやファイルにアクセス権を設定し、作成者本人のみがアクセスできる環境を導入することを検討中。また、アクセスログを取得することを検討したが、生徒を監視することにもなりかねないので、アクセスログ取得の導入は見送った。
- ・パソコン教室の利用に際して利用ルールを作成し、ルールを遵守するよう情報の授業時に情報担当教員が情報モラル指導とあわせて徹底的に行うようにする。

ご提供いただく情報は、できるだけ細かく事例を記載してください。不必要な項目は削除してください。ご提供いただきました情報につきまして、事務局より詳細を伺う場合がございます。その際にはご協力いただけますよう、お願い申し上げます。

ご提供いただいた情報につきましては事例集作成のためだけに使用させていただき、ご提供いただいた個人・事象事例が発生した学校名が特定できる形式では公表いたしません。