津山高専の情報セキュリティに対する取り組み

○三木勝*
*津山工業高等専門学校　技術部　第三技術班　技術専門職員

近年，情報セキュリティの重要性は非常に高まっている．著者の務める津山高専においても情報を安心安全に扱うために，情報セキュリティに対する様々な取り組みが行われている．情報セキュリティをより強固にするためには，技術的に対策を施すのと同時に利用者に対する教育も重要である．本論文では，技術面での取り組みと教育面の取り組みの２つについてそれぞれの事例を報告する．

1. はじめに

近年スマートフォン等の高性能なモバイル端末が急速に普及し，津山高専においても多くの学生が利用している．また個人のノートPCを持参して，実験実習に活用する学生も徐々に増えてきている．

津山高専では無線LANが整備されており，学生は申請書を提出する必要があるが，誰でも利用することができる．しかし利用中に悪意のあるサイトにアクセスしてしまいウイルスに感染したり，不正なソフトウェアをインストールしてしまったという報告も少なくない．

またSNS(Social Networking Service)での学生間のトラブルや，学生に相応しくない情報を発信して外部の方から指摘を受ける，といったケースも多い．

このような背景から，情報セキュリティに対する重要性が非常に高まってきた．安全に情報を扱うためには技術的に対策を施すのと同時に，学生自身のセキュリティ意識を高める教育が必要である．

本論文では技術的な対策と学生に対する教育の２つの事例について報告する．

2. 技術的な取り組み

(1) アンチウイルス

本校ではESET EndpointProtection Standard スクールパックを契約しており，学生は学内での使用に限り個人 PC にもインストールすることができる．特に支障がない限り学生の PC にはインストールさせている．

ウイルスが検出された PC からは著者を含むネットワーク管理者にアラートメールが送信され，PCの利用者が即座にわかる仕組みになっている．さらに当該 PC の利用者に対して直接指導を行う．

学内のESETが導入されたPCの状況を把握するため，クライアント管理用サーバ(図-1)を構築し，すべての PC を一元管理できるシステムとした．

図-1 ESET管理サーバ Webコンソール

(2) ファイアウォール

高専統一ネットワークシステムで設置されたファイアウォール(FortiGate 500D)を運用しており，不正アクセスに対する防御を行っている．

学内からインターネットへの通信も監視しており，学生が問題のあるサイト等へアクセスしようとした際に通信を遮断する，といったポリシーを状況に合わせて設定している．

表-1は学生の１日における通信先を，通信量の大きい順にファイアウォールの集計機能にを使用してまとめたものである．この表からSNS や動画サイトの利用が非常に多いことがわかる．

表-1 1日における通信先と通信量

通信先	カテゴリ	通信量
Youtube	Video/Audio	132.17GB
Amazon.Video	Video/Audio	12.86GB
Apple.Store	General.IN	15.56GB
Twitter	Social.Media	4.78GB
HTTP.Video	Video/Audio	2.78GB
Instagram	Social.Media	2.44GB
Naver.Line	Collaboration	2.07GB

3. 教育に関する取り組み

(1)インターネットについての教育

近年，実験実習でインターネットを活用することが増えてきているが，利用する学生の情報セキュリティに対する意識は決して高いとは言えない．SNS で重要な個人情報を含む内容を公開してしまい，外部の方から指摘を受けるという事例も増加してきている．

そこで本校の1年生が全員受講する「情報リテラシー」の講義で情報セキュリティ教育を取り入れることとなった．

情報セキュリティを学ぶためには，まずインターネットについて正しい知識を身に着けている必要があると考え，初学者向けでも理解が容易な教材を導入することとした．実際に導入したのが，JPRS が無償で配布している「ポン太のネットの大冒険」(図-2)であり，この教材を2週間かけて学習する．ストーリー形式で学ぶことができて，学生からもまずまずな評価を得ている．

図-2 JPRS ポン太のネットの大冒険

(2)情報セキュリティ教育

本校の1年生が全員受講する「情報リテラシー」は通年で24回行っているが，その中の12回は情報セキュリティに関する内容となっている．

前期は主に情報モラルや情報セキュリティ意識に関する内容が中心であり，またSNSを利用する学生が非常に多いことから，SNS の利用に関する内容も盛り込んでいる．以下に前期の主要な内容を抜粋する．

a) パスワードポリシー
b) 情報の発信
c) SNS を利用する上での注意
d) スマホ関連で逮捕される可能性
e) 情報発信後の責任と評価
f) 情報の管理とセキュリティ
g) ネットワーク利用のマナー

後期は内容がやや技術よりになっている．これは具体的な仕組みを知ることで，セキュリティ対策がイメージしやすくなるという狙いがある．以下に後期の主要な内容を抜粋する．

a) セキュリティを守る技術
b) 暗号化の仕組み
c) 公開鍵暗号方式
d) デジタル署名の役割
e) 認証局
f) SSL

講義を行ったあと，グループで今回のテーマについて議論を行いレポートにまとめて提出させている．

4. まとめ

情報セキュリティは個人の意識によるところが大きく，今後も継続して教育を続けていく必要がある．そのためには教える立場である教職員も情報セキュリティに対する意識をしっかりと持ち，取り組み続けていくことが重要であると考えられる．