授業実践

科目「情報セキュリティ」の授業実践

三重県立亀山高等学校主幹教諭　村山　佳之

１．はじめに

本校では平成30年度から２年間，国立教育政策研究所より教育課程研究指定校事業の指定を受け，高等学校学習指導要領（平成30年告示）で設置される科目「情報セキュリティ」を「情報」の専門学科であるシステムメディア科３年生の学校設定科目（２単位）として設置し，研究を進めている。

今回は研究の中で取り組んだ授業実践について報告させていただく。

２．新科目「情報セキュリティ」

高等学校学習指導要領（平成30年告示）では専門教科「情報」の科目として「情報セキュリティ」が設置されている。以下は学習指導要領の抜粋である。

１　目標

情報に関する科学的な見方・考え方を働かせ，実践的・体験的な学習活動を行うことなどを通して，健全な情報社会の構築と発展を支える情報セキュリティの確保に必要な資質・能力を次のとおり育成することを目指す。

(1) 情報セキュリティについて体系的・系統的に理解するとともに，関連する技術を身に付けるようにする。
(2) 情報セキュリティに関する課題を発見し，情報産業に携わる者として合理的かつ創造的に解決する力を養う。
(3) 情報セキュリティが保たれた情報社会の構築を目指して自ら学び，情報システムの運用と管理に主体的かつ協働的に取り組む態度を養う。

２　内容

１に示す資質・能力を身に付けることができるよう，次の〔指導項目〕を指導する。

〔指導項目〕

(1) 情報社会と情報セキュリティ
　ア　情報セキュリティの現状
　イ　情報セキュリティの必要性
(2) 情報セキュリティと法規
　ア　情報セキュリティ関連法規
　イ　情報セキュリティ関連ガイドライン
(3) 情報セキュリティ対策
　ア　人的セキュリティ対策
　イ　技術的セキュリティ対策
　ウ　物理的セキュリティ対策
(4) 情報セキュリティマネジメント
　ア　情報セキュリティポリシー
　イ　リスク管理
　ウ　事業継続

３．授業実践

授業実践を行った講座の生徒は経済産業省のITパスポート試験や基本情報技術者試験の取得も視野に入れて情報システムについて専門的に学ぶ系列の選択者であったため，セキュリティに関する基礎的な知識については２年次までに学習している。

そのため，各単元の最初に行う講義は内容の確認と深化を促す程度にとどめ，実習やレポート作成，グループ討議など主体的に取り組める内容を多く取り入れるようにした。

また，専門的な内容に特化しすぎず，共通教科情報や他教科の情報関係科目でも実践できるような内容となるよう工夫して，教材開発や授業実践を行うようにした。

3.1 「(1)情報社会と情報セキュリティ」

3.1.1　情報セキュリティの現状

情報セキュリティの3要素（機密性，完全性，可用性）について，それぞれが損なわれたセキュリティ事故の事例をネットで調査し，レポート形式にまとめた。

3.1.2　情報セキュリティの必要性

身近な事例からセキュリティ事件まで，不正のトライアングル（機会，動機，正当性）について考え，グループで互いに発表した。

【課題】以下の不正行為について「不正のトライアングル」を**想像**してみよう。

	機会	動機	正当性
高校生がお酒を飲む			
他人の物を盗む			
他人の情報を盗む			

図1　「不正のトライアングル」授業プリント

NHKの「プロフェッショナル仕事の流儀『サイバー攻撃に挑む』」を視聴し，セキュリティの必要性について考えた。

3.2 「(2)情報セキュリティと法規」

3.2.1　情報セキュリティ関連法規

自分自身が個人情報保護法に違反してしまいそうな場面を想定し，実際に起こったらどのような悪影響が起きるか考え，グループで互いに発表した。

また，三重県警察本部生活安全部サイバー犯罪対策課から「みなさんに知って欲しい『サイバー犯罪』のこと」と題した講演と，「SNSのアカウントを乗っ取られた高校生の被害者から相談を受け付ける」という想定で，警察官の方が被害者役，高校生が警察官役になって演習を行った。

図2　サイバー犯罪対策課による講演

図3　被害の聞き取り実習

3.2.2　情報セキュリティ関連ガイドライン

高校生がソーシャルメディアの使いすぎで困る場面を3つ設定し，対応するガイドラインを作成した。

3.3 「(3)情報セキュリティ対策」

3.3.1　人的セキュリティ対策

ア　パスワードクラック

Excelの旧形式ファイルに文字種や桁数が違うパスワードを複数設定し，総当たり攻撃ができるマクロを使ってパスワードが解析されるまでの時間を計測，その後必要なパスワード強度について考えた。

イ　標的型攻撃メール

実際に送られてきた標的型攻撃メールについてメールのヘッダ情報を解析し，メール送信に用いられたサーバのIPアドレスと，そのIPアドレスがどの国に所属しているかを調べた。

ウ　セキュリティ啓発ビデオの評価

独立行政法人情報処理推進機構（以下「IPA」）が提供しているセキュリティ啓発のためのビデオを複数視聴し，自分がセキュリティ啓発を実施する立場で評価した。

エ　「ひろげよう情報モラル・セキュリティコン

クール」への応募

IPAが行っている「ひろげよう情報モラル・セキュリティコンクール」の標語部門に応募することを，夏季休業中の課題とした。

3.3.2　技術的セキュリティ対策

ア　利用者認証（生体認証）

静脈による認証装置を使用して静脈パターンを登録し，自分のアカウントは認証が成功し，他人のアカウントは認証されないことを実習した。

図4　静脈認証装置での認証実習

イ　暗号技術

共通鍵暗号と公開鍵暗号について，それぞれ簡易的な内容で自ら計算して暗号化，復号を行った。

ウ　マルウェア・不正プログラム

EICARが提供しているワクチンソフトの動作テスト用のファイルをダウンロードし，パソコンにインストールされているマルウェア対策ソフトがどのような動作をするか確認する実習を行った。

図5　マルウェア対策ソフトの警告

また，ファイル名の偽装手法についても「RLO」という手法で実際にファイル名の拡張子を見た目上変更する実習を行った。

エ　ディジタル証明書

実際にhttpsで通信が行われているWebサイトからディジタル証明書をダウンロードし，表示される内容について確認する実習を行った。

図6　ディジタル証明書 授業プリント

オ　脆弱性体験学習ツールでの実習

IPAが「脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べるツール」として提供している「AppGoat」を使用した実習を行った。

LAN内に用意したサーバに対して，クロスサイトスクリプティング，ディレクトリトラバーサル，OSコマンドインジェクション，SQLインジェク

図7　「AppGoat」実行画面

図8　「AppGoat」実行結果画面

ションの4種類の攻撃を擬似的に体験し，脆弱性への対応方法について確かめる実習を行った。

3.3.3　物理的セキュリティ対策

ア　トラッシング・窃視実習

疑似パスワードが書かれたプリントを，手で破いたりシュレッダーにかけたりしたシュレッダーダストを使って，元のパスワードが再現できるかの実習を行った。また，疑似パスワードを入力する人の背後からキーボード操作だけをみて窃視することができるかを，文字種や桁数を変えたパスワードで行う実習を行った。

図9　トラッシング・窃視実習

イ　情報媒体からの漏洩対策

USBフラッシュメモリに保存したファイルを削除してから，復元ソフトによる復元を行い，その後，情報媒体消去ソフトによる消去を行うことにより復元ができなくなることを確認する実習を行った。

3.4 「(4)情報セキュリティマネジメント」

リスク管理について，トレンドマイクロ社から提供されている「インシデント対応ボードゲーム」をアレンジし，グループでCSIRTを想定した役割分担を決め，カードに書かれたイベントが発生したと想定して，現状分析や初動対応の選択についてグループで考え発表した。

図10　リスク管理実習

4．全体を通して

当初の想定より生徒はセキュリティに関する関心・意欲が高く，少し高度な実習内容でも意欲的に取り組む様子が見られた。

セキュリティに関する実習は他のPC実習に比べ事前の動作確認に多くの時間が必要になるなど大変ではあったが，意欲的な生徒の姿勢を見ると有意義な授業実践であったと感じている。

ただ，学んだ情報セキュリティ技術を悪用したりすることがないよう，モラル面の指導は今後も常に充実させていく必要性を感じている。

参考文献・参考サイト

［1］高等学校学習指導要領（平成30年告示）（文部科学省）
［2］「情報セキュリティ」（独立行政法人情報処理推進機構）https://www.ipa.go.jp/security/index.html
［3］「EICAR（European Institute of Computer Anti-virus Research）」http://www.eicar.org/

通巻第50号
2020年4月1日　発行

ⓒ編修・発行　実教出版株式会社
代表者　小田　良次

発行所　〒102-8377　東京都千代田区五番町5
TEL.03-3238-7777
http://www.jikkyo.co.jp/