情報セキュリティに対する意識向上を図る授業実践 ~辞書攻撃視覚的体験ツールの開発~

山本　周
聖学院中学校高等学校
s-yamamoto@seig-boys.jp

大谷　孟宏
電気通信大学
t-ootani@uec.ac.jp

昨今，様々なシステムやツールの登場により個人情報やパスワードを日々入力する場面が多々ある．情報社会における個人の責任及び情報モラルについて理解することは，大人のみならず中高生も必要である．中高生のSNSを使用したネット上のトラブルで多い不正アクセス行為の禁止等に関する法律など，また，情報セキュリティの3要素である機密性・完全性・可用性の重要性，情報セキュリティを確保するには組織や個人が行うべき対策があり技術的対策だけでは対応できないことなどを理解する．そこで本実践では，ソーシャルエンジニアリング，パスワード推測・作成のワークに加え，昨年度パスワードの重要性は理解できたが実際にどのように解読されているのか想像できないという課題に対し，今年度は総当たり攻撃・辞書型攻撃されている様子を視覚的に見ることができるテストツールを開発することで更なる情報セキュリティに対する意識向上の効果の検討とする．

キーワード：情報モラル，情報セキュリティ，パスワード，総当たり攻撃，辞書型攻撃

1. はじめに

2011 年 3 月の東日本大震災以降，災害時の安否確認や情報収集の手段として LINE や Twitter などSNS（ソーシャル・ネットワーキング・サービス）の利便性が注目され，スマートフォンとともに急速に普及した．迅速かつ広範囲に情報を伝達できるSNSは社会的インフラになり，高校生にとっても一般的なコミュニケーションツールである．内閣府による令和元年度「青少年のインターネット利用環境実態調査報告書」[1]では、高校生のスマートフォン利用率は 93.2%であり，スマートフォンでのインターネットの利用内容についても「コミュニケーション（メール・メッセンジャー・ソーシャルメディアなど）」の回答が最多である．一方で，高校生を含む若年層のSNS利用をめぐっては，ネットいじめや不適切な投稿による炎上など，問題や事件も多く発生しており，公共性・記録性・拡散性といったインターネットの特性を理解しないままSNSを利用することには大きなリスクが伴うことが考えられる．これらについては，学習指導要領[2]の情報社会に参画する態度において，「社会生活の中で情報や情報技術が果たしている役割や及ぼしている影響を理解し，情報モラルの必要性や情報に対する責任について考え，望ましい情報社会の創造に参画しようとする態度」と定義付けている．さらに，全ての人間が情報の送り手と受け手の両方の役割を持つようになるという現状を踏まえ，情報の送り手と受け手としてあらゆる場面において適切な行動をとることができるようにするために必要なルールや心構え及び情報を扱うときに生じる責任について考えることであると述べられている．

また，学習指導要領[2]の情報社会との問題解決の，ア（イ）情報に関する法規や制度，情報セキュリティの重要性，情報社会における個人の責任及び情報モラルについて理解することでは，情報社会で生活していくために，知的財産に関する法律，個人情報の保護に関する法律，不正アクセス行為の禁止等に関する法律などを含めた法規，更に，マナーの意義や基本的内容，情報を扱う上で個人の責任があること，情報セキュリティの 3 要素である機密性・完全性・可用性の重要性，情報セキュリティを確保するには組織や個人が行うべき対策があり技術的対策だけでは対応できないことなどを理解することが求められている．その際，法を遵守すること，情報モラルを養うこと，情報セキュリティを確保することの重要性，大量かつ多様な情報の発信・公開・利用に対応した法規や制度の必要性が増していることを理解するようにするとともに，人の心理的な隙や行動のミスにつけ込み情報通信技術を用いずにパスワードなどの重要な情報を盗み出すソーシャルエンジニアリングにも触れることの重要さが述べられている．

そこで本実践では，生徒にとって身近なツールである SNS を例にとり，ソーシャルエンジニアリング，パスワード解読・推測・作成のワークに加え，昨年度パスワードの重要性は理解できたが実際にどのように解読されているのか想像できないという課題に対し，総当たり攻撃・辞書型攻撃の視覚的な体験を通じて，情報セキュ

リティの重要性を学ぶ授業実践を行った. 今回はその授業実践と生徒の意識変容についての報告をする.

2. 研究目的

本研究では, ソーシャルエンジニアリング, 総当たり攻撃・辞書攻撃を視覚的に体験, パスワード解読・推測・作成のワークを通じて, 情報セキュリティ(情報モラル)に対する意識向上の効果の検討とする.

3. 開発ツール

提案の教材では, 生徒が使用する各コンピュータの内部において, 4 桁の数字で構成されるパスワードでログイン可能な Web サービスを稼働させ, それに対して総当たり攻撃を試みるテストツールを動作させる. Web サービス及びテストツールは, 実行されているコンピュータ内で動作し, ネットワークを経由してコンピュータ外部から通信を受け入れたり, 通信を行うことはない. 生徒はあらかじめ, コンピュータ上にインストールされている Web ブラウザを経由して, 任意のパスワードを設定する. 次にテストツールを起動して, 自身が設定したパスワードが解読できるかどうかを試してもらう. テストツールでは, 前述の Web サービスのパスワード入力欄およびログインボタンを Web ブラウザ上で自動制御し, 総当たりを行う. そのため, 攻撃が行われている様子を視覚的に見ることができ, 4 桁の数字の場合において, どの程度の速度で解読できるかを視覚的に把握できる. Web サービスでは, 実際の Web サービスと同様に, パスワードをハッシュ化して保存する. 本提案では暗号学的ハッシュ関数に MD5 を使用している. そのため, パスワードの解析時間の議論に必要となる, 暗号学的ハッシュ関数の計算速度を基にした授業の展開も可能となる. また, 提案では, 4桁の数字を総当たり攻撃する前に, 1234 や 1111 といった, 簡単なパスワードを辞書攻撃する. そのため, 辞書攻撃の概要やその危険性を体験することができる. テストツールは攻撃を行うツールとしてではなく, 一般に脆弱性を検証するペネストレーションテストにも用いられる. そのため, ”ホワイトハッカー”の存在や"ブラックハッカー"の脅威を説明を行うための補助として用いることも可能である.

4. 実践報告

4.1 対象生徒

高校 3 年生(週 2 コマ(1 コマ : 45 分)), 全 6 コマ
文系 : 3 クラス, 理系 : 2 クラス

4.2 実践時期

2022 年 5 月 28 日～6 月 24 日

4.3 実践環境

実践校は Google Workspace 環境が整っており, 生徒1人に1アカウントが配布されている. Google Workspace とはグループウエアサービスで, 以下の機能を使用する.

- Google Classroom:授業プラットフォーム(ネット上にクラスを作成し, 効率的に進捗管理・評価を行えるツール)
- Google Form:アンケートフォーム

4.4 授業カリキュラム

主な授業の流れは, 以下表1の通りである. 最終課題を「強固で覚えやすいパスワードを作る」という各自オリジナルのパスワード作成とした. 1,2 コマ目でパスワードの流出の危険性と企業と個人それぞれにおけるパスワードの扱い方によりパスワードの重要性の意識付け, 3 コマ目に開発ツールの体験, 4 コマ目でパスワード作成の手順書を作成し, 解読, 5 コマ目で再度作成する.

表 1 授業カリキュラム

授業数	内容
1	パスワードの流出の危険性と身近さ
2	企業のパスワード保管, 個人が安全性を高めるには
3	開発ツール体験
4	手順書作成, 解読ワーク
5	手順書作成(2 回目)・リフレクション

5. おわりに

急速な情報化社会の発展の中で中高生に必要とされる情報セキュリティの意識向上のため, 生徒にとって身近なツールであるSNSを例にとり, ソーシャルエンジニアリング, 総当たり攻撃・辞書型攻撃を視覚的に体験, パスワード解読・推測・作成のワークを設計した. 授業前後で情報セキュリティに関する意識アンケートを取り, 授業における妥当性を検討する.

参考文献

(1) 内閣府, 青少年のインターネット利用環境実態調査 https://www8.cao.go.jp/youth/youth-harm/chousa/r01/net-jittai/pdf/2-1-1.pdf (2022年5月29日確認)
(2) 文部科学省. 学習指導要領解説 (情報編) https://www.mext.go.jp/content/1407073_11_1_2.pdf (2022年5月29日確認)