5ZG-03

セキュリティ教育のためのセキュリティインシデント体験型教材の開発

伊藤 祐輝 †1　Peteri Santtu†2　坂元 晴彦 †1　和泉 諭 †1
†1 仙台高等専門学校　†2 オウル応用科学大学

1　はじめに

現在，世界中でランサムウェアを始めサイバー攻撃による被害が多発し，社会や経済にも大きな影響が及んでいる．この影響下にあるのは日本も例外でなく，増加しつつあるサイバー攻撃の脅威，およびそれによって引き起こされるセキュリティインシデントへの対策が必要とされている．2015 年には，国民へのサイバー安全保障強化が必要と判断した内閣が，サイバーセキュリティ月間の施策を開始した [1].

サイバー攻撃の影響下にあって，セキュリティインシデントによる損害を特に大きく受けるのは，セキュリティインシデントの防止および発生後の適切な対応に関する知識を持たない人間である．この現状を解決するための一手法として，サイバーセキュリティに関する知識の少ない人間に最低限のリテラシーを身につけさせる教育を行うことが必要となる．本研究は，そのために必要な教材，すなわち疑似的なセキュリティインシデントの体験を通して利用者のセキュリティ意識を向上させる教材を作成する．

2　関連研究

人間は見たことおよび聞いたことについては 20% 身につき，実際に手を動かして学んだことは 90% 身につくという研究結果をもとにサイバーセキュリティの基礎知識に関する教材を作成した文献がある [2]．教材のテーマはセキュリティ教育であり，攻撃手法と防御手法の対応付けをタワーディフェンスゲームやカードゲームの形式で教えるものになっている．

ここで，教材への没入感を強めることによって内容を学習者に身につかせるというアイデアを本研究の参考とした．

3　研究内容

3.1　概要

関連研究の項目で挙げた例において，没入感を強めることを目的としてタワーディフェンスゲームやカードゲームの形式をとっていたが，これは実際にセキュリティインシデントが発生する状況とは異なる．本研究で開発する教材は、より実際のセキュリティインシデントに近いシナリオを用意し、複数の攻撃手法を連続的に体験させるものとする．特に，サイバーセキュリティの知識が少ない人間がセキュリティインシデントに遭いやすいという考えから，特に小学生や高齢者をターゲットとして教材の作成を行う．実装予定のシナリオ例を図 1 に示す．

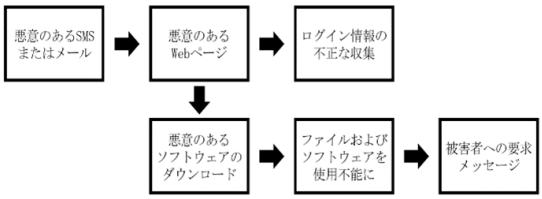

図 1: 教材のシナリオ例

3.2　実装方法

ランサムウェアのシナリオを例とした実装を示す．シナリオの開始地点となる悪意のあるメールは，教材側で用意した学習者の Gmail アカウントに送信している．メール内のリンクにアクセスすることで，シナリオの分岐点となる「悪意のある Web ページ」が開かれる．図 2 に悪意のある Web ページの実際の画像を示す．

図 2: 悪意のある Web ページ

学習者には図 2 の赤い文字と枠は見えていない．このため，何も仕組まれていないように見える画面が学習者に表示されるにも関わらず，悪意のある Web ページ内のどこをクリックしてもランサム

Developing of interactive learning materials for building cyber security awareness
Yuki ITOU†1, Peteri SANTTU†2, Haruhiko SAKAMOTO†1, and Satoru IZUMI†1
†1National Institute of Technology, Sendai College
†2Oulu University of Applied Sciences

ウェアがダウンロードされるようになっている．ランサムウェアが起動すると，教材の一部として作成したファイルの内容が書き換えられる．ファイル内容の書き換えには C++ におけるファイルポインタを用い，書き換え前の文章は学習者が自分で記述できるようにした．これは，「自分が手を動かして記述したファイルの中身が意思に関係無く書き換えられている」という事実を学習者に示し，教材への没入感を強めるためである．

ランサムウェアのシナリオで最後に表示される要求メッセージ（ファイル内容復旧の対価を要求するメッセージ．以降ランサムノートと呼ぶ．）は，学習者が使用している端末の画面を覆う大きさとし，消去と移動ができないように設定した．C++ を用いたランサムノートの動作原理を図 3 に示す．

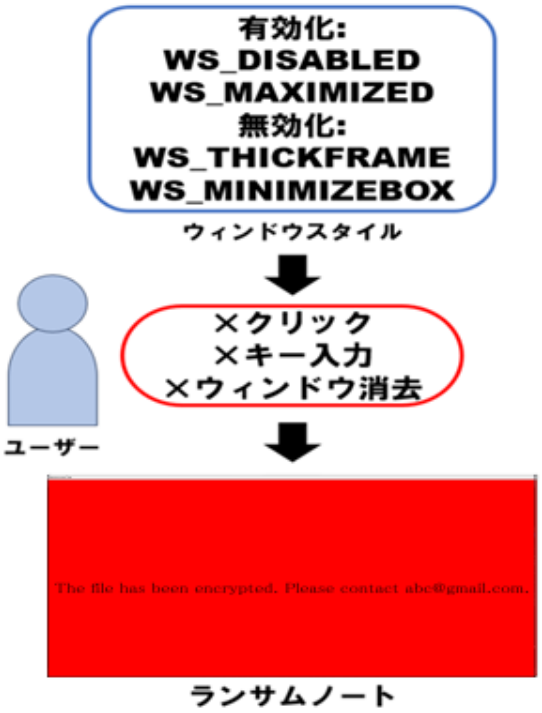

図 3: ランサムノートの動作原理

図 3 のウィンドウスタイルにおいて，THICKFRAME および MINIMIZEBOX を設定しないことでランサムノートのサイズ変更を防いでいる．また，MAXIMIZE および DISABLED によってランサムノートは最大化され，学習者からの操作を受け付けなくなる．これらは，学習者が手を動かして何かを成し遂げるのとは逆に，「自分がどんな操作をしても画面を切り替えることができない」という事実を学習者に示し，通常の操作はランサムノートに通用しないことを学習者自身の手を動かせながら学ばせるためである．

図 3 に示した通り，本研究のセキュリティインシデント体験型教材を起動したユーザーの端末において，ランサムノートへのマウス入力・通常のキー入力・ウィンドウ消去（ウィンドウ切り替えを含む）は不可能になっているが，現在のシステムではキーボードから「0」の入力があった際にシナリオを中断できるようにしている．これは，教材が不正にコピーされ，端末の動作を制限するという部分が本物のランサムノートとして悪用されることを防止するためである．また，何らかの不具合によってキーボードからの中断が行えなかった場合に備え，ランサムノートの表示開始から 30 秒が経過すると自動的にシナリオが中断されるようにしている．加えて，教材のランサムウェア部分によって改ざんされるファイルについては，編集内容が失われる可能性があることをユーザーに周知するものとする．

実装時，ランサムウェア部分の作成にプログラミング言語 C++ を用いた．その他，Web アプリケーションの制御に JavaScript を用いた．ハードウェア面の実装には Raspberry Pi を用いた．

3.3 評価手法

教材への評価は，第一に関連研究 [2] を参考として学習者を対象としたアンケートによって行う予定である．ただし，それだけでは学習者の主観的な意見のみが反映される結果となるため，事前テストと事後テストを行う．事前テストは，教材の利用前に教材でカバーする内容について学習者に質問を行うものである．事後テストは，教材の利用後に事前テストと同じ内容について学習者に問うものである．事前テストと事後テストの結果を比較することにより，教材の有効性を客観的に評価できる [3].

4 おわりに

今後，C++ および Python を用いて未完成のシナリオである「ログイン情報の不正な収集」の実装を行う予定である．また，現在は最低限の機能だけが実装されている教材用 Web ページを，HTML および CSS を用いて修飾する予定である．

謝辞 本研究は JSPS 科研費 JP22K18607 の助成を受けて実施した．

参考文献

[1] サイバーセキュリティ戦略本部：サイバーセキュリティ月間における松野内閣官房長官メッセージ，首相官邸（オンライン），入手先 ⟨https://www.kantei.go.jp/jp/tyokan/101_kishida/20230201message.html⟩（参照 2023-12-29）.

[2] Ge Jin, Manghui Tu, T.-H. K. J. H. J. W.: Evaluation of Game-Based Learning in Cybersecurity Education for High School Students, *Journal of Education and Learning*, Vol. 12, No. 1, pp. 150–158 (2018).

[3] 鈴木克明：HyperCard を使った教育用スタックの作り方—大学教員のための実践的教材設計入門—，東北学院大学教養学部（オンライン），入手先 ⟨https://www.gsis.kumamoto-u.ac.jp/ksuzuki/resume/books/1996a04.html⟩（参照 2023-12-29）.