6ZD-03

CTF を用いた情報セキュリティ学習手法の検討

坂木佳菜　鈴木松卓　宮内雄太　千葉尭　寺田真敏
東京電機大学

1. はじめに

JUAS の東証一部上場企業とそれに準じる企業の計 4,499 社を対象にした調査[1]によると，すべての情報セキュリティの役割において人材が不足していると回答している企業の割合は 4 割以上である．このように情報セキュリティに関する人材は不足しており，人材育成が急務である．

本研究では，情報セキュリティ技術を競う競技である競技用 CTF を，情報セキュリティ教育で活用するためのアプローチを検討していくことにある．本稿では，競技用 CTF が持つメリットを活かし，若者を対象とした情報セキュリティ教育に用いるために，出題者の意図(解答者に身に付けてほしい知識や技術)の伝達に着目したアプローチである教育用 CTF について報告する．

2. 関連研究

2.1 CTF の教育利用

picoCTF[2]や SECCON[3]などの競技用 CTF では，課題の中から隠された答えとなる FLAG を見つけ出し，得点を稼ぐことで情報セキュリティの技術を競う競技である．競技用 CTF には，学習面で次のような特徴がある．

- 情報セキュリティに対する幅広い知識が身につく
- 実際に手を動かすことで実践的なスキルが身につく
- クイズゲーム感覚で学習に臨むことが出来る

その一方，CTF を教育に活用する目的で，赤木[4]らは，出題レベルの適切化を図るために CTF 問題の分類とパターン化について報告している．また，企業では，CTF を社内教育用として利用している．例えば，一般社団法人 金融 ISAC（以下，金融 ISAC）では金融機関で働く人を対象に，独自で CTF 問題を作成し運用している．

2.2 解決したい課題

CTF を情報セキュリティ教育に活用していくためには，競技用 CTF の持つ学習面での特徴を活かしつつ，次に示す課題を解決する必要があると考えている．

- 問題には出題者の意図(解答者に身に付けてほしい知識や技術)があるが，この意図が解答者に伝わらないと，問題を解いても解答者に知識や技術が十分に身に付かない．すなわち，より高い学習効果を得るためには，ただ解答させるだけでなく，出題の意図を踏まえた解法をさせる必要がある．

3. 出題者の意図の伝達に着目したアプローチ

本章では，競技用 CTF のメリットを活かしつつ，情報セキュリティ教育に適用するために，出題者の意図の伝達に着目したアプローチを取り入れた教育用 CTF について述べる．

(1) タグを通して出題者の意図を伝達する

本教育用 CTF で扱うタグは，問題の解き方の方向性を示す役割と，解答者に学んで欲しい知識や技術のキーワードを示す役割がある．具体的な例を図 1 を用いて説明する．

図 1 の CTF 問題は 2 回パーセントエンコーディングをデコードすると「flag{電大}」という文字列になる問題である．これは二重エンコード(Double Encoding)[5]と呼ばれ，URL のパラメータを 16 進数形式で 2 回エンコードし脆弱性を攻撃する手法として 2000 年代前半から知られている．Web サーバが 1 回のみエンコードされたことを前提として処理した場合，予期しない動作を引き起こしてしまう．この CTF 問題の場合，「二重エンコード」というワードに着目し，調査して二重エンコードとはどのようなものなのか，二重エンコードの何が問題なのかを知って欲しいという意図を含めてタグを設定している．

図 1　教育用 CTF 問題とタグの例題

(2) 解説動画を通して出題者の意図を伝達する

本教育用 CTF で扱う解説動画は，出題の意図を踏まえた解法を説明する役割と，出題者の意図を解説する役割がある．具体的な例を図 1 の CTF 問題を用いて説明する．

図 1 は FLAG が二重エンコードされた問題である．解説動画の前半は解法を説明するパートで，復号ツールの使い方を実際の利用画面と音声を用いて解説することで感覚的にツールの使い方を理解してもらえるよう作成する．解説動画の後半は出題者の意図を解説するパートで，パーセントエンコードとは何か，「%25」という文字列に着目した二重エンコードについて解説する．基本は音声で解説をし，重要な内容はテロップとして表示することで，解説がより印象に残るよう作成する．

4. 提案手法の評価

4.1 評価方法

金融 ISAC から提供を受けた CTF 問題を使用した．提案手法の評価にあたっては，タグと解説動画を準備し，教育用 CTF に挑戦した被験者を対象にアンケート調査(表 1)を実施した．被験者は，東京電機大学情報セキュリティ研究室に所属する学生 24 名である．

- タグ
  金融 ISAC から提供を受けた CTF 問題から 24 問を選択し，解答者に学んで欲しい知識や技術のキーワードであるタグを 1～2 個追記した．

Feasibility of information security learning approach using CTF
KANA SAKAKI, MATSUTAKA SUZUKI, YUTA MIYAUCHI,
TAKASHI CHIBA and MASATO TERADA, Tokyo Denki University

- 解説動画
  24 問中，最も正解率が低かった 1 問について，2 種類の解説資料を準備した(表 1)．CTF 問題の内容は Windows レジストリファイルの中から FLAG を見つけ出すもので，ツールの使い方がポイントとなる．

表 1　評価用に作成した解説資料

区分	内容
解説動画	4 分 30 秒．動画の前半はツールを使い問題を解く過程を音声で解説したものであり，後半は出題者の意図を音声と画像で解説したもの．重要な内容はテロップをつけた．
解説文書	プレゼンテーションライクな資料で，解説動画と同じ内容を文字と画像のみでまとめたもの．

表 2　アンケート内容

区分	質問内容
タグ	[質問 1] タグから出題者の意図は読み取ることはできましたか？(できた～できなかったを 5 段階評価) [質問 2] 問題を解く過程でタグに書いてある知らないワードを調べましたか？(一つ選択：全て調べた，問題に躓いたら調べた，特に調べなかった)
解説動画	[質問 3] 解説動画と解説文書どちらを利用したいですか？(一つ選択：解説動画，解説文書) [質問 4] 質問 3 で答えた理由を教えてください．(自由記述)
全般	[質問 5] 教育用 CTF を利用して学習する際に良かった点悪かった点を教えてください．(自由記述)

4.2 評価結果

(1) タグを通して出題者の意図を伝達する

半数以上がタグから出題者の意図が読み取れたと回答しており(図 2)，解答者にとって難易度が高い問題は全員がタグのワードを自ら調べている(図 3)．

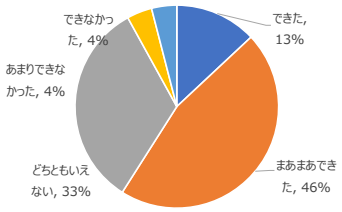

図 2　質問 1(タグから出題者の意図を読み取る)

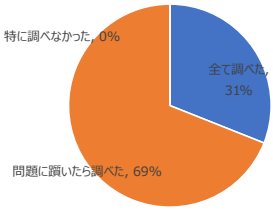

図 3　質問 2(タグに書いてある知らないワードを調べる)

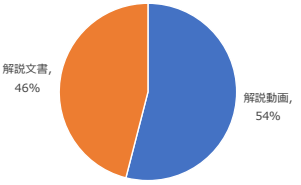

図 4　質問 3(動画，文書どちらを利用したいか)

(2) 解説動画を通して出題者の意図を伝達する

解説については，解説動画，解説文書それぞれ回答数は半々であった(図 4)．解説動画については，問題を解くのに利用するツールの操作を直感的に理解できる，解説文書については，繰り返し見やすい，自分のペースで理解することが出来るなどが回答されており，どちらにもメリットがあることを示している(表 3)．

4.3 考察

- 本教育用 CTF で準備したタグは，出題者の意図を伝達する方法として有効であると考える．特に，解答者はタグの知らないワードを自ら調べるなど，解答者に学んで欲しい知識や技術につながるきっかけを提供していることが挙げられる．
- 新たな知見として得られたことは，自由記述の回答(表 3)「出題者の意図がくみ取れない問題はモチベーションの維持が難しかった」から，タグが解答者のモチベーションの向上にもつながる可能性があること，「出題者の意図を理解せずに正解してしまうことがあった」から，教育用 CTF に解説は必要不可欠であることが挙げられる．

表 3　自由記述の回答で多くみられた意見

#	内容
質問 4	解説動画について ●問題を解くのに利用するツールの操作を直感的に理解できる 解説文書について ●繰り返し見やすい ●自分のペースで理解することが出来る
質問 5	**良かった点** ●幅広い分野を勉強するきっかけになった ●ゲーム感覚で挑戦でき，モチベーションの維持につながった ●知らなかった知識を，問題を解く過程で自ら調べることによって，勉強した内容が知識として身に付きやすい **悪かった点** ●出題者の意図がくみ取れない問題はモチベーションの維持が難しかった ●通常では使わないサイトやツール利用して解く問題は特に難しかった ●出題者の意図を理解せずに正解してしまうことがあった

5. おわりに

本稿では，出題者の意図の伝達に着目したアプローチを取り入れた教育用 CTF を提案し，評価を通して，タグならびに解説による出題者の意図の伝達が有効であり，効果的な学習につながることを示した．

今後も，情報セキュリティに関する能力を高める素地を創るための手段として教育用 CTF というアプローチを活用し，改善していきたいと考えている．

参考文献

[1] JUAS,”企業 IT 動向調査報告書 2022”，入手先（https://juas.or.jp/cms/media/2022/04/JUAS_IT2022.pdf)，(参照 2023-01-06)
[2] picoCTF，入手先（https://picoctf.org/)，(参照 2023-01-06)
[3] SECCON, 入手先(https://www.seccon.jp/2022/)，(参照 2023-01-06)
[4] 赤木智史，中矢誠，富永浩之，“ハッキング競技 CTF を取り入れた情報セキュリティ教育の導入イベントの実践報告”，情報教育シンポジウム，2014 年，p169-172
[5] OWASP: Double Encoding, https://owasp.org/www-community/Double_Encoding