7ZF-05

情報セキュリティの導入教育を目的とした 出題型ハッキング競技 CTF における競技者の振舞の傾向分析

西村拓海[†1]　中矢誠[†2]　富永浩之[†3]

香川大学[†1]　アキュトラス[†2]　香川大学[†3]

1. はじめに

ハッキング競技 CTF(Capture The Flag)は，情報セキュリティをテーマとするゲーム大会である．出題者がサーバ上に隠した情報を旗(フラッグ)に見立て，解答者が情報系の知識や技能を用いて，その旗を見つけるものである．日本でも，SECCON CTF[1]が開催されている．また，CTF はセキュリティ教育においても注目を集めている．

本研究では初心者を対象とするセキュリティの導入教育を目的とした CTF 大会を提案している．本論では，試行実践の解答ログを分析する．これにより，競技者の振舞の傾向分析を行う．オープンキャンパスに来場した高校生に対する試行実践を対象とする．

2. 情報セキュリティの導入教育の CTF 大会

本研究室では，初心者を対象とする情報セキュリティの導入教育として，出題型(ジェパディ型)の CTF の大会イベントを提案している[2]．大会運営サーバ BeeCon を開発している[3]．ハッカーのための本格的な CTF と異なり，ゲーム感覚で楽しみながら，誰でも気軽に参加できる大会を目指す．

3. カテゴリと分野に基づく問題区分

BeeCon で出題する問題は，学習の段階と対象者に応じて， 6 つのカテゴリに区分する(表 1)．さらに，情報セキュリティおよび情報リテラシの内容に応じて，分野を細分化している[4]．カテゴリ 1 は，初心者が日常的に起こす操作ミスや，知っておくと便利なチップスに関連する．カテゴリ 2 は，不審なデータや安易な操作の危険性を実感させる．カテゴリ 3 は，情報系の新入生が，情報処理の仕組みを理解するための問題である．カテゴリ 4 は，セキュリティに大きく関係する内容である．文字列や，ビット列などを扱い，バイナリエディタも必要となる．カテゴリ 5 は，専用のツールやコマンドを利用して，各種のデータの特徴を分析する問題である．カテゴリ 6 は，CGI や DBMS など，Web サイトの脆弱性を突く問題などである．

Analysis of Player's Behaviour in Hacking Competition CTF with Jeopardy Style for Introductory Learning about Information Security

[†1]Takumi NISHIMURA, Kagawa University

[†2]Makoto NAKAYA, Aqutras Inc.

[†3]Hiroyuki TOMINAGA, Kagawa University

4. 4 つの問題特性

問題の難易度に関わる要素を検討し，特性情報として付与する．これを問題特性と呼ぶ[4]．問題特性は，知識，計算，技能，作業の 4 つとする(図 1)．知識は，セキュリティに関する知識を要するか．計算は，2 進数の加算などの計算が必要か．技能は，プログラミングやセキュリティに関する技能を用いるか．作業は，大量の単純作業を行うかである．

5. 試行実践の概要

試行実践は，本学のオープンキャンパスで実施した．高校生 33 名に競技者として参加してもらった．出題する問題は，カテゴリ 1 を 7 問，カテゴリ 2 を 4 問，カテゴリ 3 を 2 問，カテゴリ 4 を 2 問の計 15 問とした(表 2)．プログラミングなどの技能を要求するため，技能の問題は出題しなかった．競技形式は，個人対戦とした．競技時間は 70 分とし，競技開始から 30 分後に用意したすべてのヒントを開示した．

試行実践の結果から，知識の問題の振舞と，計算，作業の問題の振舞との関係性を調べる．これにより，競技者の知識や情報検索の能力と問題特性ごとの傾向との関係を分析する．

6. 試行実践の分析結果

図 2，図 3 に，知識(問題番号 005)，計算(010)，作業(015)の解答状況を時系列順に示す．四角点が，問題ページ閲覧時間，三角点が誤答提出時間，丸点が正答提出時間である．図 2 は知識と計算を比較した図である．左側が知識，右側が計算である．図 3 は知識と作業を比較した図である．左側が知識，右側が作業である．

知識の問題の競技者の振舞と，計算，作業の競技者の振舞の関係性を調べる．図 2 から，知識の問題で正答するのに時間を要した競技者，正答できなかった競技者は，計算の問題に着手できていないことがわかる．これにより，情報検索ができる競技者は，計算を行うような問題でも，インターネット上に答えがあるのではないかと思い付き，情報検索を正しくできているの

ではないかと考える．この結果から，高校生や文系大学生に出題する場合は，情報検索の問題の比重を高める必要があると考える．これにより，わからないことがあれば，一人で考え続けるのではなく，情報検索を行う姿勢を身に着けさせることができるのではないかと考える．図 3 から，知識と作業の問題には，関係性があまり見られなかった．

今回は，各問題特性から，１問ずつを分析に利用した．今後は，より多くの問題に対し分析を行い，競技者の振舞の傾向について分析する．

7. おわりに

大学新入生などを対象とし，セキュリティを意識させる情報リテラシ教育として，CTF 競技を取り入れた大会イベントを提案している．大会運営サーバ BeeCon を開発している．CTF は，ジェパディ型で，分野と難易度に応じて，6 段階の問題カテゴリを設ける．また，問題の特性情報として 4 つの問題特性を提案している．本論では，高校生を対象としたコンテストを編成し，オープンキャンパスで試行実践を行った．

分析結果から，知識の問題で正答までに時間がかかった競技者は，計算の問題に着手することができていないことがわかった．

今後は，大会に出題した問題すべてに対して，競技者の振舞を分析する．将来的には，競技者や競技環境から自動で出題する問題を編成する機能を運営サーバに組み込む．

表 1 問題のカテゴリと出題分野

カテゴリ	対象者	出題分野
1	一般の大学生	1 キーボードのキー配置とシフト操作 2 マウスやタブレットの操作 3 Web ページの閲覧や URL 指定の構成 4 Web ブラウザと情報検索エンジンの機能 5 セキュリティ関連の用語
2	理系の高校生	1 様々なユーザ認証とパスワードの重要性 2 圧縮ファイルや実行ファイルのバイナリ 3 マルチメディアのファイル形式の復元再生 4 Web ページの HTML ソースの閲覧 5 オープンな SNS からの情報入手 6 二進数やビット列の変換と計算
3	情報系新入生	1 文字化けのテキストと文字コードの変換 2 合同式や素因数分解の計算 3 簡単な暗号解読やエンコード文字列の復元 4 悪意のある Web ページへのアクセス回避 5 PC の OS のコマンドのコマンド操作
4	意欲的高校生	1 文字列とハッシュ値の変換 2 文字列の検索と正規表現の利用 3 バイナリエディタによるビット列の走査 4 C 言語のプログラムの実行
5	情報系上級生	1 Linux のコマンド操作と簡単なスクリプト 2 バイナリデータの特徴の分析 3 ネットワーク通信のパケットの解析 4 オブジェクト指向言語の実行
6	意欲的新入生	1 クライアント側スクリプトの脆弱性（JS） 2 Web CGI の脆弱性(XSS) 3 DBMS の脆弱性(SQL インジェクション) 4 本格的なフォレンジックス

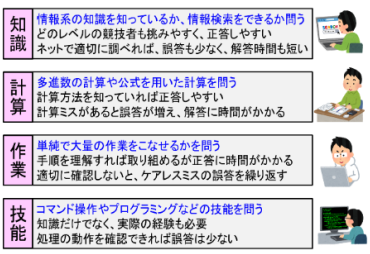

図 1 4 つの問題特性

表 2 出題した問題の分野と問題特性

番号	問題名	分野	難度	配点	知識	計算	技能	作業
001	キーボードの入力ミス	1-1	A	50	△	×	×	×
002	チープな暗号	1-1	A	50	△	×	×	×
003	何かが違う	1-3	C	150	○	×	×	△
004	google イースターエッグ	1-4	A	50	△	×	×	×
005	セキュリティについて知ろう	1-5	A	50	△	×	×	×
006	攻撃手法の名前を答えよ	1-5	A	50	△	×	×	×
007	コンピュータの 5 大要素	1-5	A	50	△	×	×	×
008	サイトに隠された格言	2-4	C	150	○	×	×	△
009	見えないフラッグ	2-4	C	150	○	×	×	△
010	100 番目の素数は?	2-6	B	100	×	○	×	×
011	計算せよ	2-6	D	200	○	○	×	×
012	暗号を復号してみよう	3-3	C	250	○	×	×	○
013	Yahoo のサイト	3-4	A	150	△	×	×	△
014	MD5 restore	4-1	B	200	○	×	×	△
015	情報を見つけろ	4-2	C	250	○	×	×	○

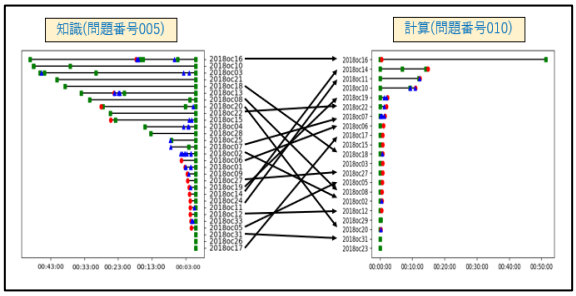

図 2 知識(問題番号 005)と計算(010)の比較結果

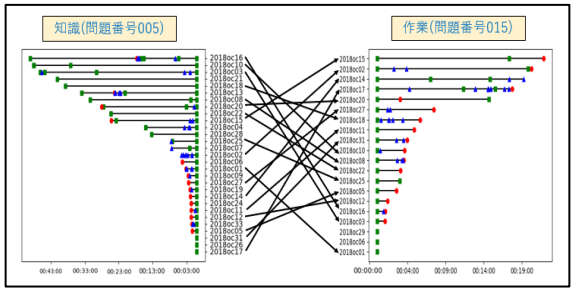

図 3 知識(問題番号 005)と作業(015)の比較結果

参考文献

1) SECCON : SECCON CTF, http://www. seccon. jp/.
2) 中矢誠, 富永浩之 : 情報セキュリティの教育機会としてのハッキングゲーム CTF, ゲーム学会 第 9 回合同研究部会 研究報告, Vol.9, No.2010-GE-1, pp.1-2 (2011).
3) 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の教育イベント - グループ対抗のコンテストの実施方法と大会運営サーバ BeeCon の機能 - , 情処研報, Vol.2013-CE-120, No.12, pp.1-6 (2013)
4) 西村拓海, 中矢誠, 富永浩之 : 情報セキュリティの導入教育を目的とした出題型ハッキング競技 CTF の試行実践における解答ログからの問題の特性分析, 情報処理学会情報教育シンポジウム SSS2018 論文集, Vol.2018, No.2, pp.68-75 (2018).