

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 試行実践における問題難度の検証

Hacking Competition CTF with Jeopardy Style for Introductory Learning about Information Security and Verification of Problem Difficulty in a Trial Practice

西村 拓海^{*1}, 中矢 誠^{*2}, 富永 浩之^{*3}

Takumi NISHIMURA^{*1}, Makoto NAKAYA^{*2}, Hiroyuki TOMINAGA^{*3}

^{*1} 香川大学

^{*1}Kagawa University

^{*2} アキュトラス

^{*2}Aqutras

Email: s15t253@stu.kagawa-u.ac.jp

あらまし：情報セキュリティの導入教育として，初心者を対象とする出題型の CTF の大会を開催している．カテゴリごとの分野に応じて様々な問題を構築している．本論文では，解答に必要な要件から，4 つの難度特性に着目する．試行実践を行い，問題ごとの解答状況を分析した．その傾向から，問題難度の妥当性を検証した．これにより，目的と対象者に応じた問題セットの編成，効果的なヒント機能の指針に役立てる．

キーワード：出題型ハッキング競技 CTF，セキュリティ導入教育，試行実践の結果分析，問題難度の検証

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，その旗を見つける．

常設で CTF の問題を公開している Web サイトも増えてきた．国内では，ksnctf⁽¹⁾や akictf⁽²⁾が有名である．また「セキュリティコンテストチャレンジブック」⁽³⁾などの参考書も出版されている．

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，大会運営サーバ BeeCon を開発し，出題型(ジューパディ型)の CTF の大会イベントを 2011 年から提案している⁽⁴⁾．ゲーム感覚で，誰でも気軽に参加できる大会を目指す．競技者は，チーム単位で取り組む．

3. 6 つの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，図 1 のように，カテゴリを設けている⁽⁵⁾．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．カテゴリ 1 は，初心者が日常的に起こす操作ミスや，便利な Tips 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し，積極的に体験してもらいたい問題である．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．さらにカテゴリ 5，6 は上級者向けの内容である．

4. 問題の 4 つの難度特性と問題の配点

BeeCon は情報セキュリティの初心者が，チーム単位で取り組むことを念頭に置いている．これまで，メンバ間の連携がうまくいかず全員がうまく取り組めないなどのケースが見られた．そこで，問題の難易度に関わる要素を吟味し，特性情報として付与する．これを難度特性と呼ぶ．難度特性は，知識，計算，技能，作業の 4 つとする．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，多くの情報から 1 つを見つけるなどの単純作業を行うかである．これらの難度特性から，問題の難易度を設定し，配点も決める．各問題に対し，4 つの難度特性の必要度を×，△，○の 3 段階で与える．難易度への寄与度として，難度特性ごとに要素点を定める．要素点の合計値から，各問題の難易度を A～E の 5 段階で設定する．さらに，問題の配点を決定するにあたり，各カテゴリに基礎点を設定した．また，問題ごとに設定されている難易度 A～E に対して，傾斜点を設定し，基礎点に加算する．

5. 試行実践の概要

試行実践では，本学の情報系サークルの 1～2 年生 12 名が競技者として参加した．今回は，余興ゲームを行わず，個人対抗の大会とした．競技時間は，90 分とし，競技開始から 60 分後にヒントを開示した．今回の試行実践では，カテゴリ 1 からカテゴリ 4 を網羅するように問題を 20 問用意した．

6. 試行実践の考察

大会運営サーバ上に保存されている競技者の各問題に対する解答ログから、正答率(全体)、正答率(着手数)、平均解答数を算出する。正答率(全体)は、競技者 12 人に対する正答数の割合である。正答率(着手数)は、解答を 1 回でも提出した競技者数に対する正答数の割合である。平均解答数は、問題に対して競技者が提出した解答数の平均値である。算出したこれらのデータを用いて、4 つの難度特性の解答状況を分析する。分析結果を表 1 に示す。

知識を問う問題は、着手数率、正答率(全体)、正答率(着手)が高い傾向にある。これは、用語に関する知識を知らなかったとしても、情報検索を行うことが可能であるからだ考える。また、平均解答数が低い。これは、情報を検索することが可能なため、用語に関する解釈の違いが生まれにくいからだ考える。

次に計算を要する問題に着目した。問題番号 14 の問題は、ブラウザで答えを検索することができるため、着手数率、正答率がともに高かった。次の試行実践では、検索しても答えがでないオリジナルの計算問題を用意し、傾向を見る必要があると考える。

次に大量の単純作業を行う問題に着目すると、平均解答数が高い傾向にあることが分かった。これは、ひっかけや解釈の違いによって誤答を提出しやすいからだ考える。この結果から、問題を正しく解釈させる、または、正答への一歩目を踏みださせるようなヒントが必要になると考える。

問題番号 1, 2 は正答率(全体)が低い。これは、作業というよりは、ひらめきが必要な問題であるからだ考える。以上により、難度特性ごとに解答状況の傾向が見られた。また、技能を有する問題は着手数率、正答率(全体)が低くなることがわかった。

7. おわりに

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、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、問題を 6 つのカテゴリに分類する。本論では、問題ごとの 4 つの難度特性について検証した。

試行実践から、難度特性ごとに問題の解答状況に傾向がみられた。技能を有する問題は、ほかの 3 つの難度特性を有する問題よりも、着手数率、正答率が低い傾向にあるがわかった。

今後は、難度特性を競技者にも提示し、問題の取捨選択や、メンバ間の分担、協力を支援し、コンテストの活性化に役立てる。また、ヒントの出し方や内容のルールを定め、競技者を適切に誘導することで、BeeCon の教育効果を高める。

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

図 1 問題のカテゴリと出題分野

表 1 試行実践の問題と解答状況

番号	分野	難度	配点	知識	計算	技能	作業	着手数率	正答率(全体)	正答率(着手)	平均解答
1	1-1	A	50	×	×	×	△	1.00	0.50	0.50	12.58
2	1-1	B	100	×	×	×	○	0.17	0.00	0.00	4.50
3	1-3	A	50	△	×	×	×	1.00	1.00	1.00	1.33
4	1-3	D	250	△	△	×	○	0.92	0.83	0.91	3.00
5	1-4	B	100	△	×	×	△	1.00	1.00	1.00	1.25
6	1-4	D	200	○	×	×	○	1.00	1.00	1.00	3.67
7	1-5	A	50	△	×	×	×	1.00	1.00	1.00	1.42
8	2-1	A	50	×	×	×	△	1.00	1.00	1.00	1.42
9	2-2	C	150	○	×	×	△	1.00	0.92	0.92	4.08
10	2-2	D	200	○	×	×	○	0.92	0.92	1.00	1.36
11	2-3	B	100	○	×	×	×	0.42	0.42	1.00	1.40
12	2-4	D	200	○	×	×	○	0.67	0.58	0.88	3.75
13	2-4	D	200	○	×	×	○	0.50	0.42	0.83	1.00
14	2-6	D	200	○	○	×	×	0.83	0.83	1.00	1.10
15	3-3	C	250	○	×	×	○	0.75	0.67	0.89	2.44
16	3-3	D	300	○	△	×	○	0.58	0.00	0.00	2.57
17	3-4	B	200	○	×	×	△	0.92	0.42	0.45	9.27
18	4-2	B	250	△	×	×	○	0.83	0.83	1.00	1.40
19	4-3	D	300	○	×	○	×	0.00	0.00	0.00	0.00
20	4-4	D	300	○	×	○	×	0.42	0.17	0.40	5.40

参考文献

- (1) ksnctf, ksnctf: <http://ksnctf.sweetduet.info/>.
- (2) akictf, akictf: <http://ctf.katsudon.org/>.
- (3) 碓井利宣, 竹迫良範, 廣田一貴, 保要隆明, 前田優人, 美濃圭佑, 三村聡志, 八木橋優: セキュリティコンテストチャレンジブック, マイナビ出版 (2015) .
- (4) 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) .
- (5) 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の分析, 情報処理学会 第 80 回全国大会講演論文集, Vol.2018, No. 5ZE-01 (2018) .