Vol.2018-CE-147 No.6
2018/12/1

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 の環境構築と運用実践 － 高校生への試行実践の分析と問題編成の支援機能 －

西村拓海[†1]　　中矢誠[†2]　　富永浩之[†3]

概要：近年，ハッキング競技 CTF が注目を浴びている．システムの開発者やサーバの管理者だけでなく，一般ユーザにもセキュリティへの意識が必要となってきている．本研究では，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ハッキング競技 CTF の大会を提案している．そのため，運営サーバ BeeCon を開発している．また，分野と難度に応じて様々な問題を構築している．今回，実際の対象者である高校生を対象に試行実践を行った．本論では，その解答ログとアンケートから，問題特性ごとの解答状況の分析や，問題の難易度設定の妥当性を検討する．これにより，目的と対象者に応じた問題セットの編成を支援する機能を検討する．

キーワード：出題型のハッキング競技 CTF，初心者向けのセキュリティ導入教育，高校生を対象とした試行実践の解答状況の分析，目的と対象者に応じた問題編成機能，競技に関するアンケート分析

Support Environment and Educational Practices of Hacking Competition CTF with Jeopardy Style for Introductory Learning about Information Security - analysis by in a Trial Practice for high school student and assistance features for problem set -

TAKUMI NISHIMURA[†1]　MAKOTO NAKAYA[†2]　HIROYUKI TOMINAGA[†3]

Abstract: Recently, the hacking competition CTF is spotlighted.The importance of security education for not only developer and server administrator but general users is increasing. in this study, we have proposed CTF competition with Jeopardy Style for Introductory Learning of information security. We develop competition management server BeeCon. We construct various problems according to field each category and difficulty. we conducted trial practice for actual subject's high school students. we analyze answers status each problem elements and considered validity of difficulty of problems from answers log and questionnaire. Herewith, We consider assistance features to configure problem set according to purpose and target.

Keyword: hacking competition CTF with jeopardy style, Introductory Learning of information security, analysis by Answer Logs in a Trial Practice for high school students, assistance featuresproblem set according to purpose and target, Questionnaire Analysis about competition CTF

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(図 1)．ほとんどの大会は，数名のメンバが組んだグループ同士のチーム対抗で得点を競う．インターネット上で参加できることが多く，遠隔にいるメンバ同士が協力したり分担して取り組むことができる．

表 1 のように，世界の各国で CTF が開催されている．CTF は，ハッカー達の腕試しの機会や交流の場にもなっている．セキュリティ関係の国際シンポジウムの行事に取り入れられることもある．政府機関も大会に協賛するなど，悪意のクラッカーへの対策のため，善意のハッカーが実践的な技能を習得する場として，認知されている．

2. セキュリティ教育とハッキング競技 CTF

2.1 ハッキング競技としての CTF

代表的な CTF をいくつか紹介する．もっとも古い CTF イベントは，1993 年に開催された．これは米国の有名な情報セキュリティのカンファレンスである DEFCON[1]の行事である．CODEGATE [2] は，2004 年から韓国政府の支援を受けて開催されている．他にも，ロシア，スペイン，フランス，インドなどで，様々な CTF が開催されている．

日本では, 2012 年から開催の SECCON[3]が有名である．情報セキュリティ会社の技術者や大学教員が実行委員となり，大会が運営されている．初回は，学生のみを対象とし

†1 香川大学工学部
Faculty of Engineering, Kagawa University
†2 アキュトラス
Aqutras
†3 香川大学創造工学部
Faculty of Engineering and Desgin, Kagawa University

ていたが，一般の技術者も参加できるようになった．チーム参加で地区予選から本予選に進む．地区予選は，会場でのオフライン予選と，インターネット上の地区予選に分かれ，2000 人以上が参加する規模となっている．マスコミにも取り上げられ，着実に裾野が広がっている．

CTF Time[4]という Web サイトでは，世界各国で開催されている CTF を紹介している．国内外についてまとめているブログもある[5]．さらに，常設で CTF の問題を公開している Web サイトも増えてきている．国内では，ksnctf[6]や akictf[7]が有名である．どちらも，40 問前後の問題が公開されており，出題ジャンルも多岐にわたる．Flaggers[8]というサイトでは，参加者同士が問題を出し合うという形をとっている．他にも数多くの常設コンテストが増えており，また CTF の解説書「セキュリティコンテストチャレンジブック」[9]や CTF の問題集「セキュリティコンテストのための CTF 問題集」[10]も出版されている．

2.2 情報セキュリティ教育のための CTF の利用

認知度が高まるにつれ，初心者の参加に向けたワークショップも開催されるようになってきた．そのため，これまでは上級者を対象とした大会が主流であったが，初心者を対象とする大会も増えてきた．2014 年には SECCON 実行委員会と JNSA(日本ネットワークセキュリティ協会)によって CTF for Beginners[11]と女性限定の CTF for GIRLS[12]が開催された．これらは定期的に開催されており，毎回定員を超える大盛況を見せている．

さらに，CTF はセキュリティ教育においても注目を集めている．国際的にも，CTF をテーマとするセキュリティ教育に関する情報カンファレンスが開催されている．特に，2014 年と 2015 年に，米国の USENIX が主催した 3GSE(Gaming, Games and Gamification in Security Education)が有名である[13]．2016 年以降は，ASE(Advances in Security Education)に名称を変えて，開催されている[14]．その流れを受け，高校生や大学生への教育イベントとして，教育機関で実施するところも出てきている．例えば，米国の高校生を対象に 2013 年に実施された picoCTF[15]などがある．2013 年版は，RPG を通じて，サイバーセキュリティについて学べる[16]． CTF の問題は，物語の場面で起こる事件として出題される．

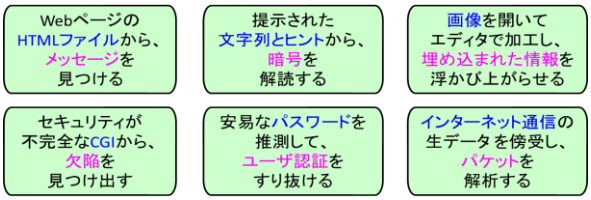

図 1 一般的な CTF の出題例

図 2 BeeCon の GUI

表 1 世界の主な CTF 大会

大会	開催国	開催年
DEF CON	米国	1993～
UCSB iCTF	米国	2002～
CSAW CTF	米国	2011～
US Cyber Challenge	米国	2005-
CODEGATE	韓国	2004～
ISEC CTF	韓国	2009～
smpCTF	Russia	2010-
PHD CTF	ロシア	2011～
CCCAC CTF	ドイツ	2012～
panda challenge	スペイン	2009/10
Nuit du Hack	フランス	2010～
Insomni'hack	スイス	2013～
InCTF	インド	2010～
IFSF CTF	チュニジア	2012
AVTOKYO CTF Project	日本	2008～
SECCON CTF	日本	2012～
NetAgent Security Contest	日本	2008～10

3. 初心者向け CTF と大会運営サーバ BeeCon

3.1 本研究の提案と大会運営サーバ BeeCon

本研究室でも，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 2011 年から提案している[17][18][19][20]．また，図 2 のような大会運営サーバ BeeCon を開発している[21][22]．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．現在は，BeeCon の試作版を実装し，200 問程度の問題を構築している．本研究室を主催者とし，情報系サークルの新人歓迎も兼ねて，実際の運用を行っている[23]．競技者は，チーム単位で取り組む．大会の進捗状況を Web で公開し，観戦者にも広く関心を持ってもらう．大会の後は，講評の時間を設け，復習を促す．参加が難しい入門者には，サポーター制のように，特定の競技チームへの応援者という役割を与える．応援者は，競技者と協調して取り組める余興ゲームに参加する(図 3)[24][25]．余興ゲームは，CTF と連動し，ゲームのポイントが競技の過程や結果に影響を与える(図 4)．競技者とともにゲームに参加することで，興味や関心を沸かせ，次回以降の CTF への参加を促している．

3.2 大会の教育目的

本コンテストの教育目的は，以下の通りである．まず，故意または無知の言動からセキュリティホールを招き，被

害者だけでなく加害者になり得る状況を防ぐ．そのためには，クラッカーの手口も知っておく．次に，不適切な操作や頻繁な質問により，管理者に余計な作業を必要にさせて煩わせたりせず，最低限は自分で考えて対処できる心構えを身に付ける．そして，情報セキュリティに関心と興味を持ってもらい，将来のセキュリティ技術者への道を示す糸口になればよいと考えている．

3.3 大会の開催意図

本コンテストは，大学における情報関連ガイダンスの一環として運用されることを念頭に置いている．ただし，一定の教科書やカリキュラムに沿った知識や技能の復習やテストに用いるという性格は薄い．むしろ，学内外での情報機器やネットワークの利用において，遭遇する可能性のある事案を幅広く取り上げる．すなわち，学んだ知識を再確認するというより，初めての用語や知らない概念にも諦めず，Web 上の情報検索で解決方法に迫っていくことを推奨する．本コンテストは，教育的な配慮から，何回かの開催を想定している(図 5)．その際， 応援者と競技者の立場を変えながら，4 回程度の開催が望ましい(表 2)．最初の 1 回目は，全員が競技者とし，簡単な問題に取り組む．2 回目は，ガイダンスの途中で，中級者を中心に開催する．3 回目は，ガイダンスの最後に，初心者を競技者とし，中級者は応援者に回る．最後の 4 回目は，再び全員で取り組む．時期は，夏休み前後など，「忘れた頃」や「慣れてきた頃」が適切である．

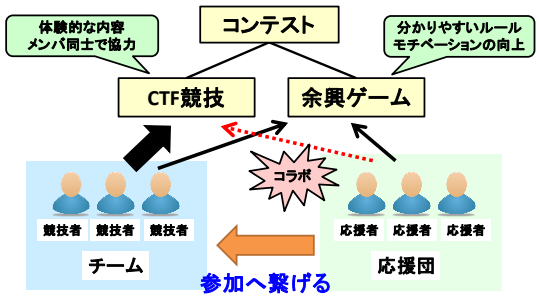

図 3 サポーター制による競技者と応援者の協調

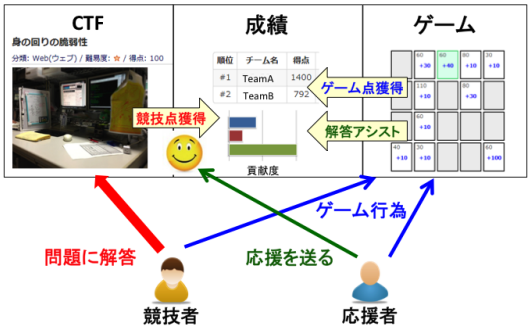

図 4 CTF 競技と余興ゲームの連携

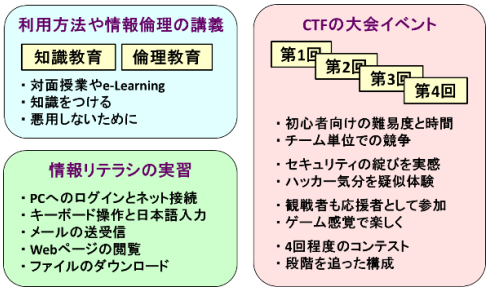

図 5 CTF の大会イベントの位置付け

表 2 CTF の大会における参加者の役割

回目	時期	意図	応援者	競技者
1	最初	各自の現状の把握		全員
2	途中	中級者への刺激	初心者	中級者
3	最後	初心者も参加	中級者	初心者
4	事後	忘れた頃に復習		全員 (中級者)

4. 問題の難易度の体系化

4.1 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，表 3 のように，6 つのカテゴリを設けている．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[26]．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．キーボードとマウス，標準的な Web ブラウザやファイルビューワがあれば解答できる．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として理解し，積極的に体験してもらいたい問題である．自分で計算したり，テキストエディタや電卓などの活用が必要である．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．バイナリエディタを用いて，バイナリデータの特徴を分析する．カテゴリ 6 は，CGI や DBMS など，Web サイトの脆弱性を突く問題である．JavaScript のソースを見て，フォーム送信するデータを書き換えたり，SQL インジェクションを行う．

また，大会ごとの問題構成は表 4 のようになる．一般に，CTF の問題は，解法を明示せず，あえて不親切な出題とすることが多い．解答へのアプローチは，試行錯誤を通して見つける必要がある．そのため，実際には，難易度の高い問題を，コンテストの開催中に解くことは難しい．また，無駄に時間や労力を費やしてしまいがちである．初心者向けの BeeCon では，そうしたフラストレーションを減らすため，一定時間の後にヒントを提示することにしている．

4.2 問題の 4 つの問題特性

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．これを問題特性と呼ぶ[27]． 問題特性は，知識，計算，技能，作業の 4 つとする(図 6)．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．これらの問題特性から，問題の難易度を設定する．各問題に対し，4 つの問題特性の必要度を×，△，○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(表 5).

表 3 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

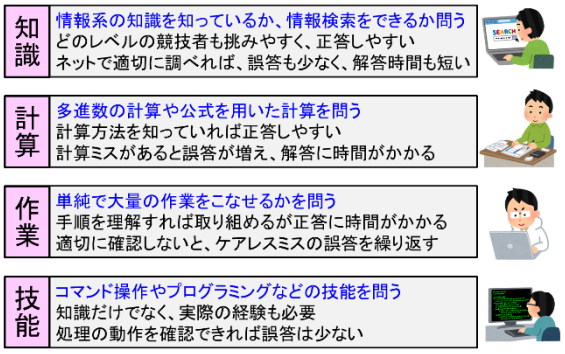

図 6 4 つの問題特性

表 4 各コンテストの実施意図と出題構成

回目	意図	時期	初心者	中級者	カテゴリごとの出題の割合					
					1	2	3	4	5	6
1	各自の現状の把握	最初	競技者	競技者	◎	◎	○	○	×	×
2	中級者への刺激	途中	応援者	競技者	△	◎	◎	○	○	×
3	応援者を引き込む	最後	競技者	応援者	○	◎	◎	○	×	×
4	忘れた頃に復習	事後	競技者	競技者	△	◎	◎	◎	○	△

表 5 カテゴリごとの難易度の基準点

カテゴリ	A	B	C	D	E
1,2	2	4	6	8	10
3,4	4	6	8	10	12
5,6	6	8	10	12	14

5. 高校生を対象とした試行実践

5.1 試行実践で検討すべきこと

試行実践の結果から，問題特性とカテゴリごとの解答状況の傾向分析と BeeCon の教育効果について検討する．今回の試行実践は，過去の試行実践とは違い，実際の対象者である高校生(非 IT 系)が競技者となっている．問題ごとの解答時間や正答率などを算出し，高校生がどのような問題を難しいと感じているのか，解答時間が長い問題にはどのような特徴があるのかを分析する．また，自由記述式で，難しかった問題について質問することで，より具体的に特徴を分析できると考える．分析結果から，問題セット編成に必要な事項を検討し，支援機能の設計に役立てる．

BeeCon の教育効果は, 競技終了後のアンケートから分析する．BeeCon を行うことで，IT やセキュリティに関する興味関心が変化しているかを分析する．

5.2 試行実践の概要

試行実践では, オープンキャンパスに参加した高校生 33 名に競技者として参加してもらった．競技者のレベルは，カテゴリ 1~4 に該当すると考える．そのため，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 問を出題した(表 6)．また，チーム対抗ではなく，個人対抗で問題に取り組んでもらった．競技時間は 70 分とし，競技開始から 30 分後にヒントを開示した．今回は，競技者の解答ログから問題のレベル設定の妥当性や問題の特性を検討することが目的のため，観戦者は存在せず，余興ゲームも行わなかった．

表 6 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	○	×	×	○

6. 解答ログ分析

6.1 対象データと分析手法

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，着手数，解答数，正答数，正答率(全体)，正答率(着手数)，正答時間を算出する．着手数は，問題の解答を一度でも提出した人数である．解答数は，各問題に対して，競技者が提出した解答数の合計である．競技者は，同じ問題に何回でも解答を提出することができる．正答数は問題を正答した人数である．正答率(全体)は競技に参加している競技者数に対する正答数の割合である．正答率(着手数)は，各問題の着手数に対する正答数の割合である．解答時間は，最初の解答を提出してから，正答または最後に誤答の解答を提出するまでの時間を平均した時間である．また，サーバのアクセスログと解答ログから，問題ページを閲覧した時間，解答を提出した時間を取得し，時系列順にプロットすることで，競技者の振る舞いを分析する．

6.2 解答ログの分析結果

今回，出題した問題に対して，6.1 節で述べた各種データを算出した．結果を表 7 に示す．また，表 7 の各種データをカテゴリごとに分類し，平均した結果を表 8 に示す．表 8 から，カテゴリが上がるごとに着手率が低くなっていることがわかる．カテゴリ 2，3，4 は，着手率が 5 割を切ってしまっている．また，正答率(全体)もすべてのカテゴリにおいて，5 割を下回っている．今回の競技者は，高校生であり，IT 系に関する知識をあまり有していないことから，なにをすればよいのかわかっていないことが原因であると考える．しかしながら，正答率(着手)はどのカテゴリも 5 割から 6 割であることから，一度着手してしまえば，正答する競技者が比較的多いのではないかと考える．今後，高校生といった非 IT 系を対象とする場合は，問題文に具体的な用語をつけることで競技者を正答に導くことができるのではないかと考える．例えば，今回出題したシーザー暗号を復号する問題では，問題文に「暗号を解け」としか書いていなかった．今後は「シーザー暗号を解け」という問題文にする．競技者は問題文の暗号がどの暗号なのか悩むことがなくなり，シーザー暗号がどのような暗号なのか，解読方法を調べることに集中することができる．結果，競技者の知識や意欲の向上につながるのではないかと考える．また，表 7 の各種データを問題特性ごとに分類し，平均した結果を表 9 に示す．今回，技能の問題は出題しなかった．これまでの情報系大学生を対象とした試行実践では，知識の問題は，着手率，正答率が高いという結果が出ていた．しかしながら，今回の結果では，着手率も正答率も低いことがわかる．表 7 のデータと合わせると，競技者のレベルによって問題特性やカテゴリごとの解答の傾向は変化するのではないかと考える．また，知識の問題である問題番号 005 と作業の問題である問題番号 008 の，競技者ごとの問題ページを閲覧した時間，解答を提出し誤答した時間，正答した時間を時系列順にプロットした．問題番号 005 の結果を図 7，問題番号 008 の結果を図 8 に示す．図 7 の結果から，問題番号 005 のような google 検索等により解答に迫っていく問題では，適切な検索ができている競技者とできていない競技者で正答までにかかった時間にかなりの差が出ていることがわかる．この問題は，カテゴリ 1 の問題であり，着手率，正答率が高く，正答するまでの時間は短くなると予想していた．しかしながら，着手率は 0.59，正答率は 0.44 であり，50 分を経過しても解くことができなかった競技者もいることがわかった．また，問題番号 012 のような，あるサイトから，フラグを見つけてくるような問題では，間違った情報をフラグと勘違いし，誤答を繰り返す競技者が一定数いることがわかる．また，問題番号 005 の結果に比べ，問題ページを閲覧する回数が多いことがわかる．今後は，着手率や正答率といったデータのほかに問題ごとの競技者の振る舞いから，競技者のレベルごとのカテゴリや問題特性の解答状況を分析していく．

表 7 問題ごとの解答状況

番号	着手	解答	正答	着手率	正答率(全体)	正答率(着手)
001	28	481	16	0.82	0.47	0.57
002	29	316	11	0.85	0.32	0.38
003	15	270	2	0.44	0.06	0.13
004	33	307	31	0.97	0.91	0.94
005	20	57	15	0.59	0.44	0.75
006	24	179	18	0.71	0.53	0.75
007	30	612	22	0.88	0.65	0.73
008	16	61	8	0.47	0.24	0.50
009	17	41	5	0.50	0.15	0.29
010	17	31	18	0.50	0.53	1.06
011	14	55	6	0.41	0.18	0.43
012	9	43	5	0.26	0.15	0.56
013	23	164	12	0.68	0.35	0.52
014	8	16	2	0.24	0.06	0.25
015	16	48	15	0.47	0.44	0.94

表 8 カテゴリごとの解答状況

カテゴリ	着手	解答	正答	着手率	正答率（全体）	正答率（着手）
1	25.57	317.41	16.43	0.75	0.48	0.61
2	16.00	47.00	9.25	0.47	0.27	0.56
3	16.00	103.50	8.50	0.47	0.25	0.54
4	12.00	32.00	8.50	0.35	0.25	0.60

表 9 問題特性ごとの解答状況

問題特性	着手	解答	正答	着手率	正答率（全体）	正答率（着手）
知識	19.10	137.00	14.00	0.56	0.41	0.70
計算	18.06	121.00	12.20	0.53	0.36	0.64
作業	16.00	103.50	8.50	0.47	0.25	0.54

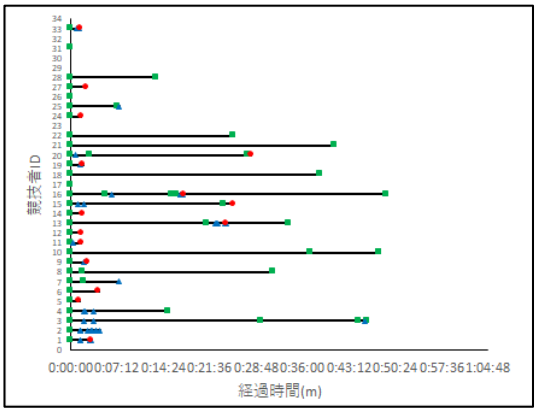

図 7 問題番号 005 に対する競技者の振る舞い

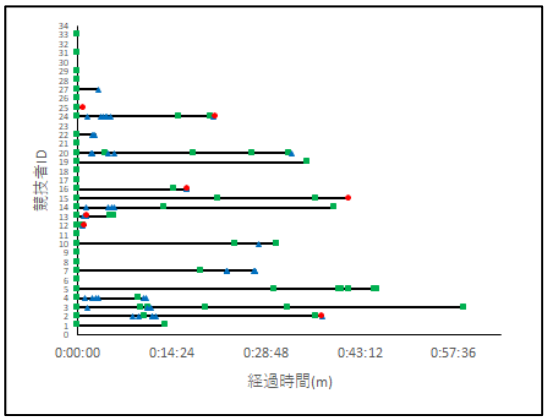

図 8 問題番号 008 に対する競技者の振る舞い

7. アンケート分析

7.1 質問内容

コンテスト終了後にアンケートによるユーザ評価を実施する．アンケートでは，4 つの質問を行う．1 つ目は，過去の CTF への参加経験について質問する． 2 つ目は，問題の難易度について質問する．また，自由記述式の質問として，一番難しいと感じた問題と感想について質問する．問題ごとに難しいと感じている競技者の数を集計し，どのような問題を難しいと感じているかを分析する．なお，一番難しいと感じた問題は複数回答を認めている．

7.2 選択式のアンケート結果

1 つ目の質問として，過去の CTF への参加経験について質問した．解答は，「初めて知った」，「聞いたことがある」，「参加したことがある」，「何度も参加している」の 4 つとした．解答者 29 人中 24 人が「初めて知った」，5 人が「聞いたことがある」と解答しており，「参加したことがある」，「何度も参加している」と答えた競技者はいなかった． 2 つ目の質問として，出題された問題の難易度について質問した．解答は，「とても簡単だった」，「簡単だった」，「ちょうどよかった」，「難しかった」，「とても難しかった」の 5 つとした．「とても簡単だった」，「簡単だった」と解答した人はおらず，29 人中 4 人が「ちょうどよかった」，16 人が「難しかった」，9 人が「とても難しかった」と解答した．BeeCon で出題する問題は，授業の確認としてのものではなく，初めての単語や概念に対して，web 検索などを用いて解決法に迫っていくような問題を考えている．今回，簡単だったと解答した人がいなかったこと，1 問も解けていない競技者はいなかったことから，出題した問題の難易度は妥当であったと考える．

7.3 自由記述式のアンケート結果

自由記述式のアンケートでは，一番難しいと感じた問題と感想を述べてもらった．難しい問題に関する意見の例を図 9 に示す．一番難しかった問題として，問題番号 003，問題番号 012，問題番号 013 を挙げている競技者が多かった．問題番号 003 は，リンク先の URL が間違っており，正しい URL を直接指定することでフラグを獲得できる問題である．リンク先の URL は必ず正しいという固定観念により解けなかったのではないかと考える．また，フラグを「BEECON{URL}」にしていたのだが，URL の部分にフラグのページの URL を入れている競技者が一定数存在した．紛らわしいフラグは，競技者の意欲をなくしてしまう恐れがあるため，設定するフラグにも注意する必要がある．問題番号 012 はシーザー暗号を復号する問題である．6.2 節でも述べた通り，問題文には，「暗号を復号せよ」としか書かれていないため，何をすればよいのかわからなかったのではないかと考える．問題番号 013 は，問題番号 003 と同様で，リンク先がダミーのサイトであり，正しいサイトの html の 1 行目がフラグとなっているものである．難しいと感じた理由は，問題番号 003 と同様であると考える．

BeeCon に関する感想を図 10 に示す．感想として，「楽しかった」，「また挑戦したい」という意見が多かった．また，「家でも CTF に挑戦したい」，「大学でもっと知識をつけたい」という意見もあった．問題の難易度についての質問結果と合わせると，いまの自分の知識では太刀打ちできない問題に遭遇することで，その分野について調べ，知識をつけたいという意欲が向上するのではないかと考える．また，BeeCon や大会運営に関する要望を図 11 に示す．要望とし

て,「解答方法がわからなかった」,「問題ページに 2 ページ目があることに気が付かなかった」という意見があった．このことから，競技開始前に問題の解答方法や，フラグの形式，問題数等について細かく説明する必要があると考える．

- Yahoo のソースコード(問題番号 013)
- 何かが違うっていう問題(問題番号 003)
- 暗号復号する問題(問題番号 012)
- シーザー暗号と url の間違いを探す問題 (問題番号 012 と問題番号 003)
- 全部

図 9 難しかった問題に関する意見

- 全問正解に至らなかったので自宅でも続けたい
- コンピュータの知識をもっと付けたらもう一度やってみたい
- ためになる問題ばかりで楽しかった
- 全然わからなかった

図 10 BeeCon や CTF 大会に関する感想

- 2 ページ目に気づかなかった
- 定期的に参加者の巡回をお願いします。 これからどうしたらよいのか、というのがなかなか聞けなかったです。
- 回答方法が最初わからなかった

図 11 BeeCon や CTF 大会に関する要望

8. 問題編成の支援機能の検討

8.1 問題編成の支援機能の目的

本システム BeeCon は，他の多くの教育機関でのオープン利用を実現し，実践的な運用を目指している[28]．BeeCon サーバおよび問題データベースは本研究室で管理し，大会を開催したいクライアントの教育機関に対して，必要なサービスを提供する形態である(図 12)．現段階では，大会の編成，出題する問題の選択は管理者である研究室が行っている．しかし，教育機関に対して必要なサービスを提供するオープン利用では，大会の編成や管理は，教育機関側が行うことになる．教育機関によっては，教員側にセキュリティに関する知識がない場合もある. このような場合でも，競技者のレベルや競技環境に応じた適切な問題を出題するために，出題する問題セットの自動編成機能が必要になってくる．

8.2 対象者と競技環境に応じた問題セット自動編成機能

BeeCon の教育効果を高めるために競技者のレベルや競技環境に応じた適切な問題を出題する必要がある. 例えば，アクセス制限がある教室では，情報検索を必要とする知識の問題は控える．代わりに，電卓や手計算で解ける問題を増やす．プログラミングの経験がある生徒が多ければ，技能の問題の比重を高める．文系など，IT 系の事項を習得していない場合は，作業的な問題の比重を高める．一人 1 台の PC が使えるか，共有の場合でも，このような調整が必要である．これらを考慮して，問題セットを編成する機能を検討する．問題数，競技者のレベル，競技の環境，競技時間等を入力することで，カテゴリや問題特性から出題する問題を編成する機能である．また，BeeCon は複数回実施することを想定しているため，実施回数も考慮する必要がある．また，今回の試行実践により，同じカテゴリ，問題特性でも，競技者のレベルによって解答状況の傾向が変化することが分かった．そのため，カテゴリ，問題特性のみを考慮する編成方法ではなく，競技者が非 IT 系か，IT 系か，高校生か大学生かなどの情報も考慮する．コンテストを前半と後半に分け，前半の解答状況から，後半に出題する問題を編成するという運営方法も検討する．

9. 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．サポーター制を導入し，CTF 競技と連携する余興ゲームも組み込んで，観戦者を応援者として巻き込む．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 段階のレベルを設ける．また，問題の難易度を決める要素として 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．BeeCon のアクセスログと解答ログから，競技者の解答状況と，一部の問題の競技者の振る舞いを分析した．競技者が，非 IT 系であることから，こちらの想定よりも正答率が低く，正答までにかかる時間も長かった．また，競技終了後にアンケートによるユーザ評価を実施した．アンケート結果から，競技者の IT やセキュリティに対する興味を高められていることがわかった．
以前までは，問題特性とカテゴリのみで，出題する問題を選択していた．今回の試行実践から，競技者のレベルによって解答状況の傾向が変化することが分かったため，今後，大会を実施する際には，競技者のレベルとカテゴリ，問題特性により，出題する問題を選択していく．大会を前半後半に分け，前半の解答状況から，後半に出題する問題を変えるという運用方法も検討する．

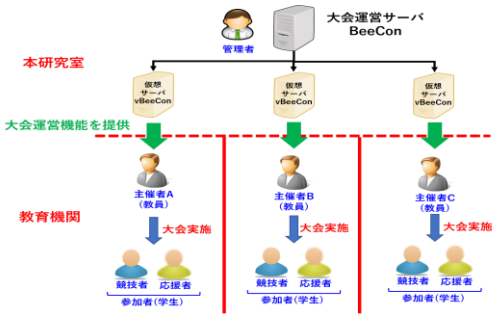

図 12 BeeCon システムの全体構成

参考文献

1) DEF CON, DEF CON : https://www.defcon.org/ (2018 年 7 月 10 日 閲覧)
2) CODEGATE, CODEGATE : http://www.codegate.org/ (2018 年 7 月 10 日 閲覧)
3) SECCON CTF 実行委員会, SECCON CTF : http://www.seccon.jp/. (2018 年 7 月 10 日 閲覧)
4) CTF Time, CTF Time : https://ctftime.org/. (2018 年 7 月 10 日 閲覧)
5) nanuyokakinu, WTF!? : http://nanuyokakinu.hatenablog.jp/entry/2015/08/24/213158. (2018 年 7 月 10 日 閲覧)
6) ksnctf, ksnctf : http://ksnctf.sweetduet.info/. (2018 年 7 月 10 日 閲覧)
7) akictf, akictf, : http://ctf.katsudon.org/. (2018 年 7 月 10 日 閲覧)
8) Flaggers, Flaggers : http://ctf.nash-dev.com/entrance.
9) 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).
10) 清水祐太郎, 竹迫良範, 新穂隼人, 長谷川千広, 廣田一貴, 保要隆明, 美濃圭佑, 三村聡志, 森田浩平, 八木橋優, 渡部裕 : セキュリティコンテストのための CTF 問題集, マイナビ出版 (2017)
11) SECCIN CTF 実行委員会, CTF for Beginners : https://2017.seccon.jp/about/beginners.html (2018 年 7 月 10 日 閲覧)
12) SECCON CTF 実行委員会, CTF for GIRLS : http://girls.seccon.jp/ (2018 年 7 月 10 日 閲覧)
13) USENIX, 3GSE'15 : https://www.usenix.org/conference/3gse15. (2018 年 7 月 10 日 閲覧)
14) USENIX, ASE'16 : https://www.usenix.org/conference/ase16. (2018 年 7 月 10 日 閲覧)
15) picoCTF, picoCTF : https://picoctf.com/. (2018 年 7 月 10 日 閲覧)
16) K. Zhang, S. Dong, G. Zhu, D. Corporon, T. McMullan, S. Barrera, “picoCTF 2013 - Toaster Wars: When interactive storytelling game meets the largest computer security competition”, IEEE Consumer Electronics Society's International Games Innovations Conference, IGIC, art. No.6659158, pp.293-299, 2013.
17) 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).
18) 中矢誠, 富永浩之 : 初心者への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, 信学技報, Vol.112, No.66, pp.45-50 (2012).
19) 中矢誠, 富永浩之 : ハッキングゲーム CTF を取り入れた情報セキュリティ教育の提案, 教育システム情報学会 第 37 回全国大会 講演論文集, Vol.37, pp.378-379, (2012).
20) 中矢誠, 富永浩之 : The Outline of an Educational Experience with Hacking Game CTF for Information Security Learning, 電気関係学会四国支部 平成 24 年度連合大会 講演論文集, No.16-18, p.319 (2012).
21) 中矢誠, 富永浩之 : 情報セキュリティの導入教育としてのゲーム要素を取り入れたハッキング競技 CTF, ゲーム学会 研究会報告, Vol.6, 2012-GE-1 (2013)
22) 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)
23) 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, 情報処理学会 情報教育シンポジウム SSS2014 論文集, Vol.2014, No.2, pp.169-172 (2014).
24) 赤木智史, 中矢誠, 富永浩之 : 初心者のためのハッキング競技 CTF への観戦者を巻き込んだ余興ゲームの導入, ゲーム学会 第 12 回 合同研究部会 研究報告, Vol.12, No.2013-GE-1, pp.4-9 (2014).
25) 阿部隆幸, 中矢誠, 楠目幹, 富永浩之 : 初心者向けのハッキング競技 CTF による情報リテラシとセキュリティの導入教育のためのオープンな大会イベント - クイズ形式のアドベンチャー型の余興ゲームの問題構築と試行実験 - , 信学技報, Vol.116, No.517, pp.123-128 (2017)
26) 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).
27) 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).
28) 中矢誠, 富永浩之 : 情報リテラシとセキュリティの導入教育のための初心者向けのハッキング競技 CTF による大会イベント - オープン利用のための仮想化の導入と運用方法 - , 情処研報, Vol.2015-CE-133, No.16, pp.1-8 (2016).