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

西村拓海[†1]　中矢誠[†1]　富永浩之[†1]

概要：近年，一般ユーザに対しても，セキュリティ教育の重要性が高まっている．また，ハッキング競技 CTF が注目を浴びており，初心者への裾野が広がっている．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 CTF の大会を提案している．大会運営サーバ BeeCon を開発し，情報系学科の学生を対象に，これまで，チーム対抗の大会を幾つか開催してきた．そのため，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，問題の難易度を適切に設定するため，解答に必要な要件から，4 つの難度特性に着目する．また，カテゴリごとの基準を設け，問題ごとの配点のルールも与える．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，問題の難易度の妥当性や，難度特性の特徴を考察した．これにより，目的と対象者に応じた問題セットの編成，チーム内のメンバの協力と分担の指針，効果的なヒント機能に役立てる．

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，大会運営サーバのオープン利用
問題の難易度の適切な設定，試行実践の解答状況の分析，目的と対象者に応じた問題セット

Hacking Competition CTF with Jeopardy Style for Introductory Learning about Information Security and Problem analysis by Answer Logs in a Trial Practice

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

Abstract: Recently, the importance of security education for general users is growing. Moreover, the hacking competition CTF in the spotlight and being expanded a range for beginners. in this study, we have proposed CTF competition with Jeopardy Style for Introductory Learning of information security. We develop competition management server BeeCon and, have hosted some team competition for student of computer science. We construct various problems according to field each category for that. In this study, we focus on the four difficult elements necessary for answers to properly set difficulty of problems. Moreover, we set basis for each category and, establish a rule of allocation of points each problem. We do trial practice moreover, analyze response status each problem. We examine peculiarity of difficulty element and validity of difficulty problems from this tendency. From this analysis, we help to configure problem set according to purpose and target, to set guidelines for cooperation and sharing of members within the team and, to implement effective Hint giving function.

Keyword: hacking competition CTF with jeopardy style, Introductory Learning of information security,
Open Investment of competition management server, properly set difficulty of problems,
analysis by Answer Logs in a Trial Practice, problem set according to purpose and target,

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
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．

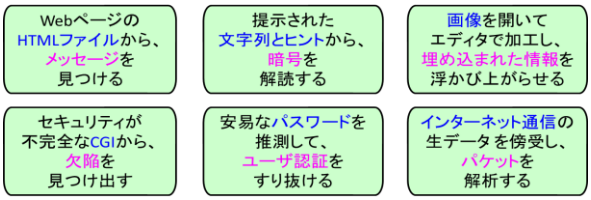

図 1 一般的な CTF の出題例

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

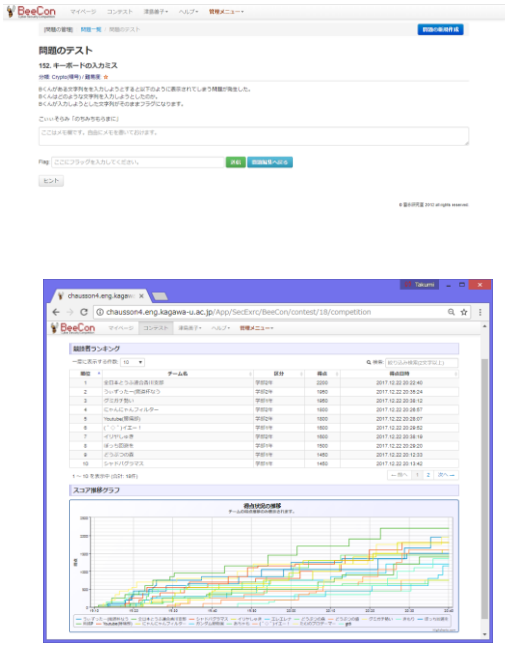

図 2 BeeCon の GUI

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，100 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．

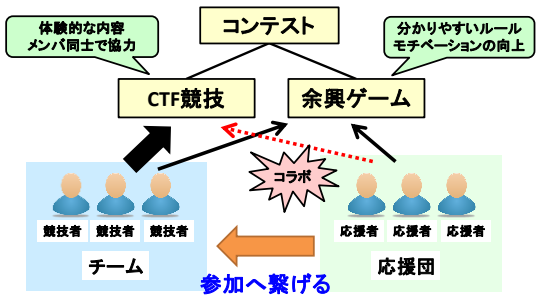

図 3 サポーター制による競技者と応援者の協調

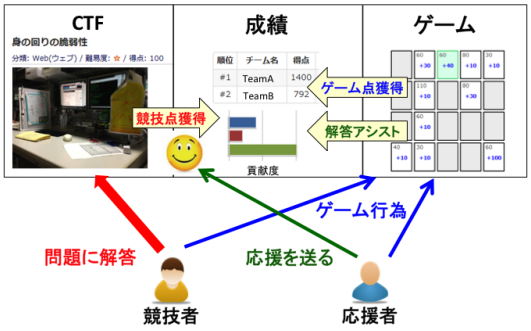

図 4 CTF 競技と余興ゲームの連携

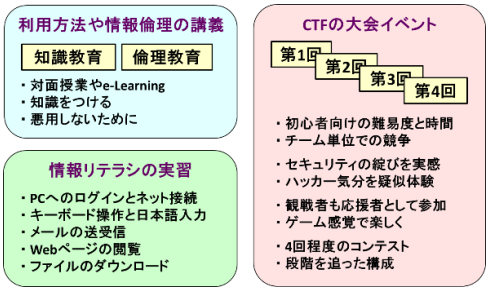

図 5 CTF の大会イベントの位置付け

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について

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][27]. 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．

各カテゴリの問題の事例を図 6~11 に示す．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 問題の難易度の精密化

以前は，問題を登録するときに，問題の作成者が適当に難易度を決めていた．しかし，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，特定の問題に固執しすぎて時間が足りなかった，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．コントストの運営者は，問題ごとの特性情報を用いて，難易度を求め，配点を定める．また，解答作業にかかる時間を推測し，所要時間の目安を得る．これらを基に，コンテストの目的に沿ったバランスの良い問題編成を行う．それにより，チームとしての問題の取捨選択や，メンバ同士の協力，分担を円滑にし，競技者の意欲の向上に繋げたい．

4.3 問題の 4 つの難度特性

本論では，各カテゴリの問題について，その難易度を決める要素を吟味する[27]. その観点としては，単純ながら大量の作業を必要とするか，情報系の知識が必要か，プログラミングなどの技能が必要か，計算が必要かの 4 つが考えられる．これを難度特性と呼ぶ．知識を問う問題の場合，競技者に必要なのは問題に関する知識，または，問題に関する情報を適切に検索する能力である．後者があれば，一般的な試験の形態よりも正答は得やすくなる．知らない用語や習っていない概念も出題できる．技能を問う問題の場合，競技者に必要なのはプログラミング経験と，それを問題解決に応用できる能力である．そのため，知識のみを問う問題よりも技能を必要とする問題の方が，難易度が高いと考える．また，簡単で単純ながら大量の作業を必要とする問題の場合，時間と手間がかかる．競技者がケアレスミスをしやすく，集中力を必要とする．また，メンバによる協力も必要になる．計算を必要とする問題は，計算に対する知識，計算を間違えずに行う能力が必要となる．後者の 2 つは，必ずしもネットワークやパソコンを必要としない問題も含まれる．メンバの能力や適性による，チーム内での分担も重要である．

4.4 難度特性からの問題の難易度と配点の設定

4 つの難度特性は，知識，計算，技能，作業と呼ぶ．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．これらの難度特性を用いて，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．また，難易度への寄与度として，0，2，4 の要素点を定める．ただし，技能の要素点のみ 0，3，6 としている．これは，他の 3 つの特性より，難易度を決める比重が高いと考えるからである．この 4 つの要素点の合計から，各問題の難易度を A~ E の 5 段階で設定する(表 5).

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する．カテゴリ 1 と 2，カテゴリ 3 と 4，カテゴリ 5 と 6 それぞれ 150 点，250 点，350 点である．また，問題ごとに設定されている難度 A, B, C, D, E に対して，それぞれ-100, -50, 0, +50, +100 点の傾斜点を設定し，基礎点に加算する(表 6).

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

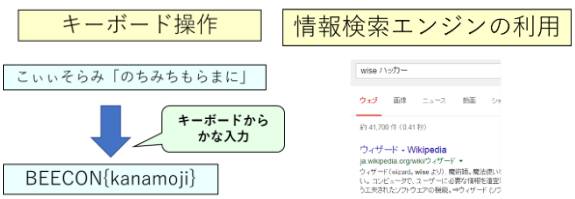

図 6 カテゴリ 1 の問題例

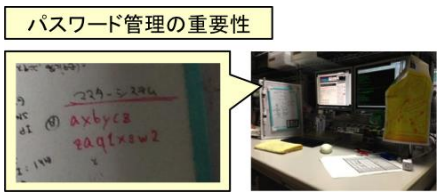

図 7 カテゴリ 2 の問題例

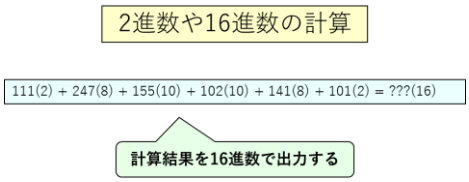

図 8 カテゴリ 3 の問題例

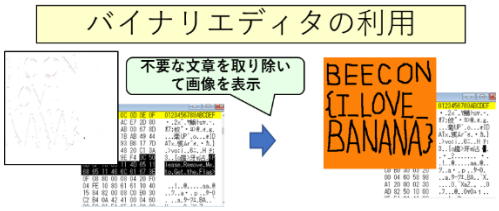

図 9 カテゴリ 4 の問題例

図 10 カテゴリ 5 の問題例

図 11 カテゴリ 6 の問題例

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	5	8	10
3,4	4	6	8	10	12
5,6	6	8	10	12	14

表 6 配点の表

	難度				
カテゴリ	A	B	C	D	E
1,2	50	100	150	200	250
3,4	150	200	250	300	350
5,6	250	300	350	400	450

5. 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，問題ごとに設定したカテゴリと難度の妥当性と，問題の特性情報の検討を行う．カテゴリの妥当性では，カテゴリが高い問題ほど難易度が高くなっているのかを検討する．難度の妥当性では，同じカテゴリでも難度が高い問題ほど難易度が高くなっているのかを検討する．これにより，本論で吟味した難易度の要素が妥当か議論する．また，吟味した問題の特性情報の妥当性を検討し，精密化や修正を行う．

5.2 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や解答状況から，閲覧数，着手数，解答数正答数，正答率(着手数)，正答率(解答数)，着手時間，正答時間を算出する．閲覧数は，問題を閲覧した人数，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(着手数)は，各問題の着手数に対する正答数の割合である．正答率(解答数)は，各問題に対して提出された解答のうち正答の割合である．着手時間は，問題ページを閲覧してから，最初の解答を提出するまでの時間を平均した時間，吟味時間は，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．算出したこれらのデータを用いて，カテゴリや難度の妥当性，問題ごとの難度特性による解答状況の傾向について分析する．

5.3 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 18 名に競技者として参加してもらった．情報系大学の学生であること，情報系サークルのメンバであることから，競技者のレベルはカテゴリ 3 からカテゴリ 6 に該当すると考える．

今回は，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，90 分とし，競技開始から 60 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．

5.4 試行実践における問題セット

今回の試行実践では， 図 7 の分野を網羅するように問題を 20 問用意した(表 7)．カテゴリ 1 を 6 問，カテゴリ 2 を 6 問，カテゴリ 3 を 3 問，カテゴリ 4 を 3 問，カテゴリ 5 を 1 問，カテゴリ 6 を 1 問，用意した．しかし，2 つの問題に不備があった．問題番号 8 は運営者の問題の読解ミスにより，振分けを誤った．本来は 2-2 ではなく，5-2 に所属すべき問題であった．問題番号 12 は解くことができない問題であった ．

5.5 難易度の妥当性の検討

表 8 の解答状況から、基礎点別の平均値を算出した．それぞれの平均値を表 9 に示す。表 9 から，基礎点の違う問題の解答状況を比較し，分析する．基礎点が高いほど，閲覧数, 着手数, 解答数, 正答数の平均値が低くなっている．特に，着手数，解答数，正答数には明確な差が見られる．着手数と正答数から，基礎点が高くなるにつれて，問題を見ただけであきらめたり，知識や技術が足りず，解答や正答ができない競技者が多くなっていることがわかる．

また，カテゴリ 1,2 とカテゴリ 3,4 の着手時間と吟味時間に着目すると，着手時間は，カテゴリ 3，4 の方が長いにもかかわらず，吟味時間は，カテゴリ 1，2 の方が長くなっている．カテゴリ 1，2 には，正答するのに知識や技術はあまり必要ないが，手間がかかったり，ひっかけがある問題が多い．そのため，競技者は，着手することは簡単にもかかわらず，誤答が多くなってしまい，正答まで辿り着くまでに時間がかかってしまっているのだと考える．一方カテゴリ 3，4 は，知識や技術に基づいて，正答を得るような問題が多いため，1 回目の解答で正答しやすいと考える．これは，解答数の平均値を比べても明らかである．

次に,同じ基礎点で難度が違う問題の解答状況を比較し，分析する．表 8 の解答状況から，同じ基礎点で難度別の平均値を算出した．平均値を表 10 に示す．表 10 を見ると，閲覧数は，同じ基礎点の場合は，ほとんど変わらない．しかし，着手数，正答数，正答率(解答数)については，難度に従い，少なくなる．しかしながら，解答率(着手数)は，難度によってあまり差が見られない．以上のことから，難度が上がるにつれ，着手する競技者は少なくなるが，着手した競技者のうち，正答できる競技者の割合はあまり変わらないことがわかる．

5.6 難度特性による解答状況の傾向

競技者の解答状況から，問題ごとの特徴を分析する．表 8 から，難度特性別の解答データの平均値を算出した．平均値を表 11 に示す． 表 11 から，知識のみを問うような問題と計算を必要とする問題は，作業や，技能を必要とする問題に比べ，閲覧数，着手数，解答率(着手数)が高いことがわかる．これは，知識があれば，すぐに正答できるほか，検索エンジンを活用すれば，容易に正答に辿り着けるからだと考えられる．技能を必要とする問題は，知識，計算，作業を要する問題と比べて，閲覧数，着手数，正答率(解答数)，正答率(着手数)がとても低いことがわかる．技能を必要とする問題は，難易度が高くなりやすいため，配点が高くなりやすい．そのため，解答できる技能を有してない競技者は，そもそも問題を見ない，見たとしても着手することができず，解答するのを諦めていることがわかる．

大量の作業を必要とする問題は，問題のカテゴリにかかわらず，正答率(解答数)が低く吟味時間が長いことがわかる．これは，競技者がケアレスミスを起こしやすく，間違った解答を提出してしまい，正答に辿り着くまでに時間がかかってしまっているからだと考えられる．また，着手数は少ないが，解答率(着手数)は 0.70 と高い値を示していることから，時間をかければ比較的正答しやすい問題だといえる．

5.7 考察

試行実践の結果から各カテゴリと難度 A~E により, 問題の難易度の差別化ができていると考える．そのため，カテゴリごとの基礎点と，難度 A~E による傾斜点により，配点を決める方式は，適切であると考える．また，難度特性を個別に分析した. 知識のみを問う問題は, 閲覧数, 着手数, 正答数が高かった．知識を知らなかったとしても，検索エンジンで調べることができるためだと考える．そのため，情報系のことをあまり知らない競技者にも，セキュリティについて自分で調べて，興味をもってもらう問題として，適切でないかと考える．今回出題した計算の問題は，多進数を扱う問題である．多進数は，情報系の学生が最初に学ぶ要素の一つであるため，正答率が高くなりやすかったのだと考える．また， BeeCon に登録されている問題で計算を問う問題が少ないため，計算を問う問題を 1 問しか用意できなかった．今後は計算の問題を多く作成することが必要である．技能を必要とする問題は，問題ページを見ない競技者や，着手できない競技者が多かった．このような競技者に対し，ヒントで正答まで誘導するのは困難だと考える．BeeCon は 1 回ではなく，4 回程度開催することを想定している．そのため，大会終了後に解法の説明を行い，次の大会で似たような問題を出題し，競技者の技能が向上しているか確認することが重要だと考える．作業を必要とする問題は, 競技者のケアレスミスを誘いやすく正答率(解答数)や吟味時間が長くなる傾向にあることがわかった. また, 着手数が低いにもかかわらず，正答率(着手数)が高いことから，適切なヒントを与えることで，正答に誘導しやすいのではないかと考える．

表 7 試行実践の問題の特性による難度と配点

番号	問題名	分野	難度	配点	知識	計算	技能	作業
1	かな文字入力	1-1	B	100	△	×	×	○
2	友人からの奇妙なメール	1-2	B	100	△	×	×	○
3	何かが違う	1-3	B	100	○	×	×	△
4	記事を探そう	1-4	C	150	△	×	×	△
5	攻撃手法の名前の検索	1-5	A	50	△	×	×	×
6	セキュリティ用語の検索	1-5	A	50	△	×	×	×
7	パスワードの使いまわし	2-1	C	150	△	×	×	○
8	Only one	2-2	C	150	○	×	○	×
9	開けない画像ファイル 初級編	2-3	B	100	○	×	○	×
10	見えないフラグ	2-4	B	100	○	×	×	×
11	Infinity Links	2-4	D	200	○	×	△	○
12	SNS に気をつけろ	2-5	B	100	×	×	×	○
13	メッセージを読め！	3-1	C	250	○	×	×	△
14	計算せよ	3-2	B	200	○	○	×	×
15	暗号!?!?	3-3	C	250	○	×	×	○
16	MD5 can restore!	4-1	B	200	○	×	×	△
17	正規表現を使おう	4-2	B	200	○	×	○	×
18	開けない画像ファイル 上級編	4-3	D	300	○	×	○	×
19	履歴からパスワードを検索	5-1	B	300	○	×	×	○
20	SQL インジェクション	6-3	C	350	○	×	○	×

表 8 各問題の解答状況

番号	閲覧	着手	解答	正答	正答率（解答数）	正答率（着手数）	着手時間	吟味時間
1	18	18	173	18	0.10	1.00	03:43	03:34
2	18	18	61	17	0.28	0.94	03:15	02:17
3	18	17	81	11	0.14	0.65	06:05	26:45
4	17	12	23	9	0.39	0.75	10:25	07:43
5	18	18	44	18	0.41	1.00	06:47	15:09
6	18	18	30	17	0.57	0.94	13:40	05:48
7	18	18	66	18	0.27	1.00	02:05	13:31
8	17	0	0	0	0.00	0.00	03:13	00:04
9	17	12	20	12	0.60	1.00	00:00	00:00
10	18	15	43	13	0.30	0.87	00:50	00:51
11	15	4	4	3	0.75	0.75	12:38	05:06
12	15	14	352	0	0.00	0.00	04:25	00:20
13	16	12	29	11	0.38	0.92	05:31	00:50
14	18	18	36	17	0.47	0.94	16:26	00:00
15	17	7	24	0	0.00	0.00	15:08	02:37
16	16	13	14	11	0.79	0.85	35:17	02:40
17	15	1	2	0	0.00	0.00	07:51	04:40
18	10	4	5	2	0.40	0.50	18:38	04:18
19	17	10	37	8	0.22	0.80	33:53	00:03
20	12	1	3	0	0.00	0.00	01:52	24:57

表 9 カテゴリ別の解答データの平均値

カテゴリ	閲覧	着手	解答	正答	正答率（解答数）	正答率（着手数）	着手時間	吟味時間
1,2	17.27	14.91	81.55	12.36	0.35	0.81	07:11	07:21
3,4	15.33	9.17	18.33	6.83	0.34	0.53	17:01	01:52
5,6	15.33	3.67	13.33	2.67	0.07	0.27	06:50	09:45

表 10 難度別の解答データの平均値

カテゴリ	難度	閲覧	着手	解答	正答	正答率（解答数）	正答率（着手数）	着手時間	吟味時間
1,2	A	18.00	18.00	37.00	17.50	0.49	0.97	03:29	02:55
	B	17.33	15.67	121.67	11.83	0.24	0.74	07:02	11:30
	C	17.50	15.00	44.50	13.50	0.33	0.88	06:44	02:58
	D	15.00	4.00	4.00	3.00	0.75	0.75	16:26	00:00
3,4	B	16.33	10.67	17.33	9.33	0.42	0.60	08:21	01:16
	C	16.50	9.50	26.50	5.50	0.19	0.46	21:34	03:40
	D	10.00	4.00	5.00	2.00	0.40	0.50	33:53	00:03
5,6	B	17.00	10.00	37.00	8.00	0.22	0.80	18:38	04:18
	C	14.50	0.50	1.50	0.00	0.00	0.00	00:56	12:29

表 11 難度特性別の解答データの平均値

難度特性	閲覧	着手	解答	正答	正答率（解答数）	正答率（着手数）	着手時間	吟味時間
知識	18.00	17.00	39.00	16.00	0.43	0.94	03:01	06:27
計算	18.00	18.00	36.00	17.00	0.47	0.94	05:31	00:50
技能	14.33	3.67	5.67	2.83	0.29	0.38	09:58	04:14
作業	16.82	13.00	78.55	9.64	0.30	0.70	13:04	06:52

6. 今後への利用

6.1 仮想環境 vBeeCon による外部機関でのオープン利用

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[27]. 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．すなわち，BeeCon の大会運営の機能をパッケージ化し，必要なサービスを個別に各機関に利用させる運営方法である(図 12).

6.2 利用機関の目的に応じた問題セットの適切な編成

本論で検討した難度特性を用いて，より適切な問題セットを編成できるようにする．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．また，チームの編成方法や，メンバの友好関係によって分担や協力の形態も変わってくる．それに応じた問題の調整が必要である．将来的には，問題の分野や特性の条件指定による自動編成を実現する．

6.3 適切なヒントの検討

現在，BeeCon に登録されている問題のヒントは，問題登録時に，問題作成者が適当に用意したものである．そのため，ヒントの種類が統一されておらず，問題によっては，適切なヒントになっていない可能性がある．今回の試行実践では，解答数に対する正答数の割合が低い問題や区分が低いにも関わらず正答数が低い問題が存在した．このような問題は，ヒントが適切に機能していないか不十分な可能性がある．着手数は低いが，着手数に対する正答率が高い問題は，問題の難易度を競技者が高く見積もりすぎている可能性があるため，ファイル編集の方法などをヒントに盛り込み，難易度を適切にとらえさせることが重要ではないかと考える．今後，ヒントの有無に関する解答状況の分析も行い，今回の試行実践の結果と合わせて，ヒントの体系化を行う．

6.4 コンテストの活性化

問題の特性情報を競技者側にも提示し，チームでの問題の取捨選択や，メンバ間での協力，分担の支援を行う．これ

により，競技者全員がコンテストに取り組むことができ，競技者の意欲の向上や，コンテストの活性化につながると考えられる．

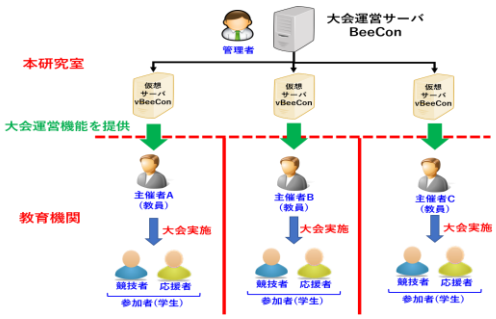

図 12 BeeCon システムの全体構成

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．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．本論では，問題の登録時に考慮すべき特性情報を検討した．すでに，BeeCon に登録されている問題に対して，特性情報を付与した．特性情報に基づいて，難度を導入し，配点のルールを定めた．実際にコンテストを編成し，試行実践を行った．競技者の解答状況から特性情報による予測が妥当であるかを確認した．試行実践の結果から，特性情報の修正や調整を行う．今後は，特性情報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(図 12)．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．

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) 中谷誠，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) 中谷誠，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) 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).