Vol.2018-CE-144 No.12
2018/3/17

Web ゲームサイトを題材とした 攻防型ハッキング競技の環境構築と運用実践 - 試行実践に基づいて改善を行った本番実践の結果と分析 -

中矢誠[†1]　富永浩之[†1]

概要：Web サービスを提供する企業において，システムの開発者やサーバの管理者には，実践的なセキュリティ教育が求められている．本研究では，複数人でプレイする Web ゲームサイトを題材とし，攻防型ハッキング競技としての体験的な演習を提案する．主催者は，脆弱性を残したサイトを競技環境として用意する．攻撃側は，ゲームのプレイヤとして，サイトにアクセスし，脆弱性を突いたチート行為を行う．防御側は，サイトの運営者として，ログを監視し，チート行為への対処を行う．主催者は，両者の状況をポイント化して勝敗を競わせ，事後に講評と検討を行う．本論では，試行実践に基づいて改善を行った本番実践の状況と結果の分析を述べ，今後の課題を議論する．

キーワード：ハッキング競技大会，情報セキュリティ教育，攻防型 CTF

Support Environment and Practices of Hacking Competition with Attack and Defense Style on a Game Website - Functions of a Trial Version and Discussions about the Result -

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

Abstract: Practical education about information security is needed for system developers and administrators in Web service supplier. We propose a hacking competition CTF as attack and defense type with a Web site for a multiple online game. The contest promoter prepares a game server site as a contest environment which contains several vulnerabilities. The contest participants are divided into an attacker team as game players and a defender team as game Web site operators. While the attackers access the game site with normal actions, they find vulnerabilities and try cheat actions. While the defenders monitor server logs, they detect illegal events and prevent them for maintenance. An action of each side is calculated as a point and makes each score for victory or defeat by the contest rule. The promoter reviews the progress situation with all participants. In this paper, we introduce several functions of a trial system and discuss the result of a trial practice.

Keywords: Hacking competition CTF, Information security learning, Attack and defense type

1. はじめに

近年，情報セキュリティに関する様々な社会問題が広がりを見せている．公的機関や大手企業の情報システムだけでなく，中小企業や個人が運営する Web サイトも，攻撃を受けるケースが多く報告されている．標的型メールによる攻撃は，技術者だけに限らず，一般のユーザにも大きな影響を与えた．2017 年 5 月には，情報を人質にとって身代金を要求する WannaCry と呼ばれるランサムウェアが猛威を振るった．一旦，攻撃を受けてしまうと，被害状況の調査だけで，数年の歳月がかかることもある．このような背景を受け，政府は，セキュリティ技術者の育成を急務としている．

一方で，セキュリティ技術者の育成には，実践的な学習が不可欠である．座学による知識学習だけでは，現実感が薄く，定着しづらい．リアルタイムに進行する攻撃へ対応するには，精神的な経験値も大きく影響する．何らかの場で実習して，経験を積むことが重要である．

2. 典型的な CTF の分類と特徴

2.1 ハッキング競技 CTF の概要

近年，ハッキング競技 CTF(Capture The Flag)が注目を浴びている．CTF は，サーバ上に隠された情報を旗(フラッグ)に見立てて，出題者の挑戦を受ける形で解答者がそれを見つける競技である．解答者は，数名のメンバからなるチーム対抗の形式が多い．世界最大規模のセキュリティ会議 DEFCON では，1996 年の DEFCON4 から毎年，会議内のイベントとして CTF が開催されており，人気を博している[1]．日本では SECCON が有名である[2]． CTF の主な開催形式には，出題型，突撃型，攻防型がある(図 1).

2.2 出題型 Jeopardy

図 1(a)の出題型(JPD)では，主催者が，フラッグを隠した問題を用意する．参加者は，問題を解いて，フラッグを見

†1 香川大学工学部
Faculty of Engineering, Kagawa University

ⓒ 2018 Information Processing Society of Japan

つけていく．問題ごとに配点が決まっている．1 度の開催につき，10 問～20 問前後が出題されることが多い．問題からフラッグを見つけるには，SQL インジェクションなどの脆弱性を用いる必要がある．問題を解くために，試行錯誤したり，情報を検索することで，脆弱性に関する知識や技術を身につける．セキュリティについての勉強を始めたばかりの人から，詳しい人まで，幅広い人が対象である．

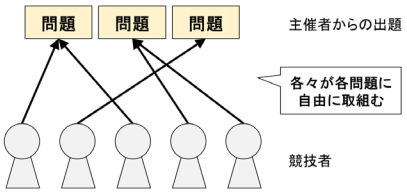
出題型は，競技のバランス調整が，他の開催形式と比べて楽である．出題数は，競技の様子を見ながら調整することが多い．ただし，問題の準備が手間である．論理だった構成になっていない解法が求められる問題は，エスパー問題と呼ばれ，あまり好まれない傾向が強い．また，スポット的な技術や知識のみを問う問題が多く，現実に即していないケースも少なくない. 出題に対する応答という性質上，出題型で防御行為を実践することは難しい．

2.3 突撃型 King of the Hill

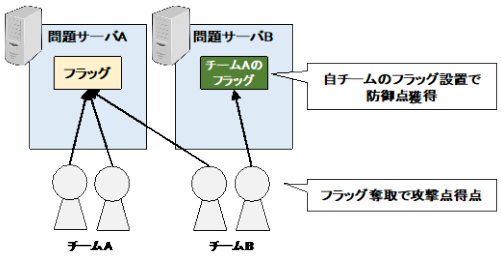
図 1(b)の突撃型(KoH)は，主催者が，脆弱なサービスが稼働しているサーバを用意する．サービス上には，主催者によるフラッグが隠されている. 参加者は, サーバを攻撃し，フラッグを見つけて，得点する．更に，参加者は，脆弱性をうまく利用して, 自チームのフラッグを書込んでおくと，継続的に得点する．出題型と違い，脆弱性を利用してデータを改竄する手法に関する知識や技術を身につける．対象は，出題型をある程度はこなせる人である．主催者は，脆弱なサービスを用意する際に，意図しない脆弱性を含まないように注意しなければならない．また，フラッグを見つけたときの得点と，フラッグを設置している間の得点のバランス調整も重要である．

2.4 攻防型 Attack & Defense

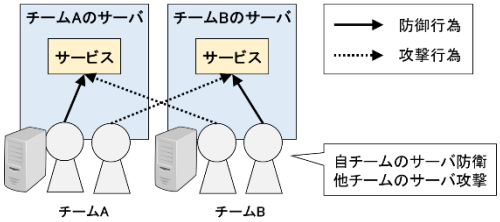
図 1(c)の攻防型(A&D)は，主催者が用意したサーバを，参加者の各チームが，構える．サーバ上には，複数の脆弱なサービスが稼働している．参加者は，自チームのサービスの脆弱性を修正して安定稼働させることで，得点する．また，他チームのサービスを攻撃し，情報を盗んだり，サービスをダウンさせることでも，得点する．限られた競技時間で，システムを把握する必要がある．出題型や突撃型と違い，リアルタイムな攻撃から守るという，実践に近い形を体験できる．突撃型のような，攻撃に関する学習だけでなく，サービスをいかに落とさないようにしながら脆弱性を修正するかという，実践的な内容も学習する．参加者は，攻撃だけでなく，防御も必要なため，ある程度の経験が求められる．主催者は，競技用のサーバとサービスを用意する必要がある．また，突撃型と同様に，意図しない脆弱性を作り込まないようにしなければならない．どちらかに偏ると，攻防型としての意味をなさなくなるため，攻撃と防御のバランスをうまく調整する必要がある．ネットワークに負荷がかかることが多く，競技ネットワークの運用コストが高いことも特徴的である．



(a) 出題型 (Jeopardy style)



(b) 突撃型 (King of the Hill style)



(c) 攻防型 (Attack & Defense style)

図 1 CTF の代表的な大会形式

3. CTF のセキュリティ教育への適用

3.1 著者らのこれまでの研究

本研究では，これまで，出題型による初心者向けの CTF の大会イベントを提案している[3][4][5][6]. 問題管理, ユーザ登録とコンテスト編成，出題と解答，採点結果の順位表示などを行う大会運営サーバ BeeCon を開発している[7][8]．初心者向けの技術項目を整理して問題を分類し，実際に問題を構築した[9][10][11]．大学新入生を主な対象に，幾つかの試行実践を行ってきた[12][13]. 教育機関での幅広い利用に向けて，システム利用のオープン化を進めている[14][15]．ビジネス向けとして，株式会社アキュトラスでの製品としての実績もある[16].

CTF 競技とは別に，余興ゲームを通して，間接的に競技へ参加できる間口として，応援者という役割を導入した[17][18][19]．応援者は，余興ゲーム上でセキュリティに関するクイズに答えることで，特定の競技チームをアシストする．また，高大連携のイベントにも広げるため，CTF の前段階として，余興ゲーム単独の実施も提案している[20][21]．これは，セキュリティをテーマとするクイズ形式で，参加者の固有情報も埋め込んだ学校を舞台とする AVG(アドベンチャーゲーム)である[22][23][24].

ⓒ 2018 Information Processing Society of Japan

3.2 CTF の関連研究

CTF に関する研究は，教育手法，開催形態，セキュリティ対策としての有効性について論じたものが多い．特に近年，教育手法についての研究が盛んである．セキュリティの国際会議 USENIX[25]では，CTF をテーマとしたワークショップも併設されている．2014 年と 2015 年には 3GSE(Gaming, Games and Gamification in Security Education)が，2016 年からは ASE(Advances in Security Education)と名前を変えて開催されている．これは，企業などのセキュリティ対策だけでは不十分であり，一般ユーザへのセキュリティ意識の必要性が高まっていることが背景として考えられる．開催形態については，より CTF やセキュリティに興味をもってもらい，モチベーションを高めるための工夫や，安定的な，または効果的な CTF の開催について検討が重ねられている．

Cowan らは，DEFCON CTF に参加し， Immunix を用いて好成績を得た[26]. Immunix は，ホストベースの Linux アプリケーション・セキュリティシステムである．この結果は，Immunix のセキュリティ面での信用を高めることに繋がったと同時に，改善すべき点も示されたと述べている．Immunix に使われている，様々な防衛技術や戦略について論じられている．DEFCON での CTF は，とてもレベルが高く，企業でのセキュリティ対策や，卓越した技術者による競技となる．

3.3 CTF と教育に関する研究

Eagle らは，CTF によって，脆弱性を見つける能力が身に付けられると論じている[27]. 更に，構築者と防御者からの視点以外に，破壊者という新しい視点の必要性を結論づけている．破壊者の視点では，システムの脆弱な点をいかに発見するかに焦点をあて，未知の脆弱性を発見する．そして，構築者や防御者と協力し，堅牢なシステムを目指す．

3.4 CTF の普及に関する研究

CTF を普及させるためには，観戦者の興味を惹き，未来の参加者へ繋げていく必要がある．しかし，競技を外部から見たときに．どういう状態か分かりづらい．また，CTF はチーム単位での競技形態をとることが多いが，個人での作業が多く，チームメンバの活動が分かりづらい．そこで，原田らは，セキュリティコンテストの可視化について論じている[28]．カメラを利用して参加者の様子を分かるようにし，正誤表示をチーム全体で共有している．これにより，どの程度の効果があるのかは，検討中のようである．

近年では，開催形態として，ゲーミフィケーションを取り入れた CTF も，多く検討されている．Zhang らは，高校生向けに picoCTF を実施し，肯定的なアンケート評価を得ている[29]. Chapman らは，picoCTF をオープンソースとして公開し．多くの教育機関で利用されていることを報告している[30]. Boopathi らは，ゲーミフィケーションを通じてセキュリティを学ぶことについて，InCTF を事例として論じている[31]．いずれも，ゲーム風の UI を取り入れつつ，レベルごとに題材が分かれており，テーマに集中して取り組める工夫が凝らされている．ストーリーも織り交ぜ，参加者の没入感も高められている．また，picoCTF は，1 万人を超える大規模な開催実績もある．

3.5 CTF システムに関する研究

JPD 形式と KoH 形式に対応した CTF 開催システムを，Facebook がオープンソースで公開している[32]．活発に開発が進められており，UI なども洗練されている．環境構築の手順も分かりやすく，管理画面も整備されており，手軽に主催できるようになっている．多言語化にも対応しているが，2017 年 6 月 9 日時点では日本語に対応していない．

iCTF を開催している UC Santa Barbara Seclab は，A&D 形式の CTF 開催システムを，オープンソースで公開している[33]. 全チーム専用のサーバを VM として生成する．また，スコアサーバ用の VM も生成する．このソースを元に，VM ではなく Docker で稼働するバージョンを InCTF の Amrita University と Amrita Centre for Cybersecurity Systems and Networks が開発している[34].

4. 攻防型 CtFrog の概要と教育での位置付け

4.1 CtFrog の概要と対象

BeeCon は，情報セキュリティへの認識を一般のユーザにも高め，裾野を広げることが目的である．そのため，情報セキュリティに強い関心がある中上級者には，物足りないイベントとなっている．そこで，本研究では，図 2 のような攻防型 CTF を開催するシステム CtFrog を新たに開発中である[35]．CtFrog は，攻防型 CTF における，攻撃者と防御者を分離して競技を行う．ゲーム感覚で，より実践的なセキュリティ実習を体験できるイベントを目指す．

CtFrog は，Web サーバの管理者，Web サービスの開発者，Web サイトの運営者などが対象である．企業研修の一環としての利用を想定する．もちろん，個人のハッカーも対象である．参加者は，ネットワーク通信の仕組みに関する知識が必要である．また， JSON によるデータ表現の知識，HTML，CSS，JavaScript など，フロント側に関する基礎事項も必要である．

オンラインゲームによる攻防型 CTF は，Linux などへの専門知識や，ネットワークの低レイヤに関する知識よりは，論理的な実装を読み解く力を必要とする．そのため，敷居が低く，コンテストに参加できる対象者が広いと考える．ゲームの規模や開示するコードを限定することで，対象とするスクリプトやコードの規模を小さくできる．一般人がゲームプレイに参加することで，ユーザとしての被害を体験でき，攻撃抑止への啓蒙もできる．

本イベントは，Web ゲームを題材とし，運営者と利用者との対決を模している．最近は，個人でゲーム系の Web サ

ⓒ 2018 Information Processing Society of Japan

イトを運営していることも多く，悪意を持ったクラッカー的な利用者への対策に悩まされているケースも少なくない．筆者も同様の経験がある．そこで，利用者の一部に，クラッカーが混じっており，その不正行為(チート)に対処するという設定を取り上げる．

このような攻防型 CTF は，事前の準備やバランス調整に多くの労力がかかる．イベント自体の主催者に対し，ゲーム内の役割としてのサイト運営者とゲーム利用者がいる二重構造になっている．そのため，これまでに，出題型ほど実施例は多くはない．安全で円滑な実施のためには，仮想環境の構築が望ましい．

4.2 イベントの題材

本イベントの題材は，複数人でプレイする Web ゲームサイトとする．イベントの主催者は，脆弱性を残したサイトを競技環境として用意する．イベントの参加者は，防御側のサイト運営者と，攻撃側のゲーム利用者に分かれる．それぞれ，3〜5 人程度とする．前者の方が技術力が必要である．希望を聞きながらも，参加者の力量に応じて，主催者が割り振る．

役割が決まったら，主催者は，サイトの運営権限を防御側に与える．攻撃側は，ゲームのプレイヤとして，サイトにアクセスする．脆弱性に気付いたら，チート行為を行い，サイトの運営を撹乱させる．防御側は，ログやデータベースを監視し，チート行為への対処を行う．主催者は，両者の状況を競技点に換算し，勝敗を競う．ゲームの終了後，主催者を司会役として，参加者全員で講評と検討を行い，セキュリティに対する技術と意識を高める．参加者の人数が多ければ，2 チームが互いに同時に，自分のサイトの防御と，相手のサイトへの攻撃を行う方式も考えられる．

4.3 システムの全体設計

主催者が，防御側に用意したサイトは，Node.js とそのライブラリである Express や Socket.IO を用いて実装され，データベース管理システム(DBMS)は MySQL を用いる(図 4)．ゲーム要素として，表 1 の脆弱性を残しておく．これらの脆弱性は，修正の難度と影響を検討し，費用対効果の高いものから対処する必要がある．サーバ側の DB 処理は，300 行程度の JavaScript ファイルで構成される．クライアント側の GUI 処理も，主に JavaScript ファイルで構成され，300 行程度である．

サーバ側の脆弱なプログラムの例と，その修正例を，図 3 に示す．これは，プレイヤのレベルアップに関する処理である．最初の状態では，クライアントからレベルアップ要求信号を受け取った際に，問答無用でレベルアップしてしまうようになっている．本来であれば，経験値が一定に達していなければ，レベルアップしてはならない．そこで，プレイヤの現在の経験値をチェックし，必要値に達していなければ，レベルアップ処理を行わないように修正している．この脆弱性は，修正難度は低いが，深刻で影響度が高いため，最優先で直されるべき内容である．

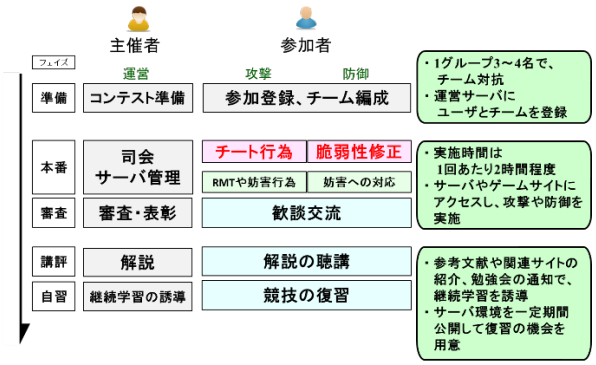


図 2 攻防型 CTF の大会イベントの進行

表 1 脆弱性の内容

内容	所在	難度	影響
蛙との距離判定がない	S	中	大
プレイヤの移動速度の異常検出がない	S/C	大	中
チャットの連投制御がない	S/C	中	小
レベルアップ処理に経験値判定がない	S	中	大
他のプレイヤとの衝突判定がない	S	中	小
マップの全領域を返却している	S	中	中
プレイヤの行動ログが記録されていない	S	小	大
ソースコードが難読化されていない	S/C	小	中

(a) 修正前

```
// レベルアップイベント
socket.on('levelUp', function() {
  (中略)
  if (user.level >= config.expBorders.length)
    return;
  User.updatePlayer(
    uuid,
    {level: user.level + 1, exp: 0}
  ).then(function() {
    (後略)
```

(b) 修正後

```
// レベルアップイベント
socket.on('levelUp', function() {
  (中略)
  if (user.level >= config.expBorders.length)
    return;
  if (user.exp < config.expBorders[user.level])
    return;
  User.updatePlayer(
    uuid,
    {level: user.level + 1, exp: 0}
  ).then(function() {
    (後略)
```

図 3 脆弱なプログラムの事例

5. コンテストのゲームのルール

5.1 ゲームの基本設定

現在の試作版では，Capture the Frog という独自の Web ゲームを題材としている(図 5)．プレイヤがフィールド内の蛙(フロッグ)を捕獲して得点を稼ぐ．プレイヤが登録したア

ⓒ 2018 Information Processing Society of Japan

カウントのキャラクタが 2D 格子のフィールド内を上下左右に移動し, 隣接するマス目の蛙をクリックして捕獲する. 試作版では，サーバ起動時に一定数の蛙がランダムにフィールド上に配置され，捕獲された後も，一定時間後に同じ場所へ出現する．プレイヤ同士では，蛙の取合いになる．

ゲームのプレイヤは，アカウントを登録してゲームに参加する．アカウントは，1 つのキャラクタに対応し，各キャラクタには得点に応じた育成レベルがある．各アカウントは，ゲーム中の蛙の捕獲数で，そのキャラクタがレベルアップする．アカウントをより強いキャラクタに育て，仮想の現金取引でアカウントを売って得点を稼ぐ．プレイヤは，次のアカウントを登録し，ゲームを続行する．

一般に，運営者にとって，この種のゲームでは，チート行為が横行し，ゲームバランスが崩れやすい．そのため，善意のプレイヤが迷惑を被って嫌悪感を抱き, 離れていく. また，不正に育成したキャラクタが現金取引され，大きな損失になる．他の犯罪行為を誘発する恐れもある．具体的なチート行為には，ゲームプレイを自動化する BOT やマクロ，スピードハック，メモリハッキング，パケットハッキング，クライアント改変などがある．

5.2 競技における各種行為

CtFrog では, 通常のゲームプレイ行為を通常行為とする. ゲームサービスに対する攻撃は，抜道行為とし，更に，ネットワークに負荷をかけ，競技の進行を困難にする行為を反則行為とする．通常行為には，ゲーム内操作と，ゲーム外操作がある. ゲーム内操作は， "Capture the Frog" の操作である．ゲーム外操作は，アカウントの生成やチャットに関する行為である. RMT に関する行為は, 抜道行為となる.

ゲームに対して，通常行為のみを行うユーザ(一般ユーザ)は，保護されなければならない．保護している間は，防御側に，得点が順調に加算される．もし，防御側が，通常運用を停止したり，通常運用できなくなるなどの原因で，一般ユーザを妨害した場合，防御側の減点となる．抜道行為は，防御側に気づかれない限り，攻撃側の得点となる．気づかれた場合は，攻撃側の得点が止められたり，場合によっては，減らされる．抜道行為を行ったユーザを摘発したり, ユーザを追放(BAN)すれば, 防御側の得点が増える. 反則行為は, 攻撃側でも防御側でも, 厳重注意を受けたり，大幅に減点される．以後の競技への参加を禁じられることもある．

5.3 攻撃側の想定行動

攻撃側は，まず，ゲームを通常プレイし，通信内容を見ながら，チートの目星をつける．次に，プレイを半自動化しつつ，チート行為を試行する．チートがうまく動作している間はよいが，運営側によって防がれた場合に備え，プレイの完全自動化を目指す. または, 新たなチートを探す. 競技時間内に，すべての脆弱性を修正されてしまった場合は，自動プレイの品質によって，攻撃側の防御側に対する有利不利が決定する.

5.4 防御側の想定行動

防御側は，事前にソースコードを確認したり，ゲームをプレイし，できるだけ早く脆弱性を見つける必要がある. 脆弱性を見つけ次第, 対処する. サイトの運用を開始後は, ゲームの Web ページやログを監視し, 攻撃側の抜道行為を見抜き，早急に対処する．例えば，クライアントからサーバへ送信された値が，通常プレイの範疇かどうかを確認する．脆弱性を修正するだけでなく，不正な行為を無効化したり，不正なユーザを追放する．必要があれば，データやログをリセットしたり，サービスの運用を一時的に停止してもよい.

5.5 競技点としての攻防スコア

CtFrog における攻撃側の競技点は，ゲーム上のアイテムやアカウントを，現金を用いて取引する RMT(リアルマネートレード)をイメージし，アカウントを仮想 RMT で売却することで攻撃点とする．防御側は，サーバを正常に運用させることで，防御点を得る．また，不正なアカウントを追放(BAN)することで, 攻撃側のチート行為を未然に防ぐ.

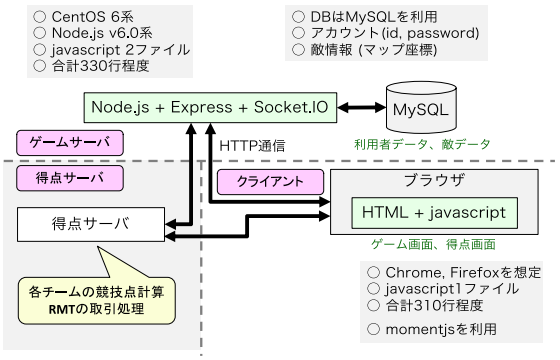


図 4 攻防型 CTF のシステム構成

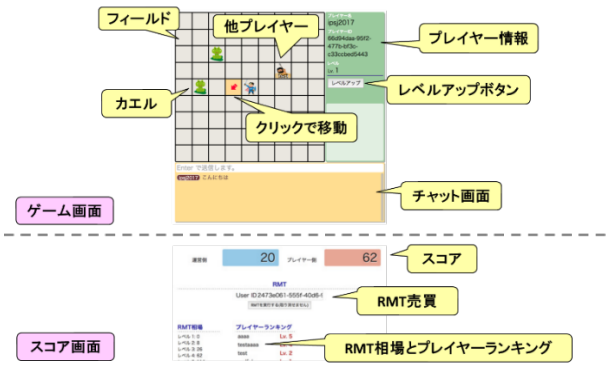


図 5 試作版 Capture the Frog の GUI

6. 試行実践に基づく本番実践

6.1 セキュリティ・キャンプについて

セキュリティ・キャンプとは，セキュリティ・キャンプ実施協議会が開催している，国をあげたセキュリティ人材

育成に関する取組の一環である[36]．5 日間程度の期間で，合宿形式で開催される．セキュリティの専門家や，セキュリティ関係の講師を招き，特色ある講義を実施する．全国の学生から応募を受付け，選考によって，50 人程度の人が参加者として選ばれる．多くは大学生であるが，高専生や高校生，ときには中学生も選ばれることがある．初日に，倫理的な講義が行われることが多く，技術の悪用を防ぐことにも注力されている．

6.2 試行実践

セキュリティ・キャンプでの本番実践に先立ち，アーヴァインシステムズ社と香川大学の学生サークル SLP の協力の下，試行実践を行った[37][38][39]．試行実践では，競技として競うことより，システムの問題点や改善点を見つけることを目的とした．進行については，事前にソースコードを読む時間がなければ，攻撃側が圧倒的に有利となってしまうことや，事前の作戦会議などが必要であるということが分かった．試行実践では，DBMS に SQLite3 を用いていたが，システム的には不便であることが分かった．また、ステージング環境が必要であることなども分かった．

6.3 本番実践

試行実践でのフィードバックを受けて，システムを改良し，本番実践に臨んだ．2016 年 8 月のセキュリティ・キャンプでは，希望者の 17 名に対する講義の一環として実施した．事前にソースコードを読む時間を設けるため，講義開催の 5 日前に，ソースコードとプレイアブルな環境を公開した．5 日間のうち，2 日間は，既にセキュリティ・キャンプが始まっており，1 日中，講義を受けることになる．また，その前の 2 日間は，移動時間や準備時間に必要となると考える．よって，参加者が読める実質的な時間は，1 日間程度だと考え，5 日前に公開した．DBMS は SQLite3 から MySQL に変更した．更に，本番環境とステージング環境を用意し，開発に専念できるようにした．参加者同士は，キャンプを通して 2 日間，交流の機会があったため，こちらから別段の作戦会議などの機会は設けなかった．

当日は，4 時間の講義時間を利用し，CtFrog を 2 回，実施した．最初の 30 分は，競技の説明と準備を行った．次の 1 時間で，1 回戦を行い，30 分の休憩の後，1 時間 30 分で 2 回戦を行った．最後の 30 分は，講評とディスカッションの時間とした．事前に参加者から，JavaScript の扱いにどの程度の自信があるかと，攻撃側と防御側のどちらを希望するか，アンケートをとった．その結果に基づいて，チーム内にある程度は JavaScript が扱えるという人が最低でも 1 人は含まれるよう，編成した．特に強い希望がない限りは，ほぼ全員が，1 回戦と 2 回戦で，攻撃側と防御側を体験した．参加者の人数が多かったため，2 つのグループに分け，グループごとに，運営者と利用者に分かれた．1 回戦と 2 回戦では，チーム編成を変えて実施した．

7. 本番実践の結果とログ分析

7.1 競技の状況

1 回戦では，2 グループともに利用者が圧倒的に勝利していた．2 回戦では，運営者が勝利していた．1 回戦では，レベルアップチートにより，利用者が大きく得点したため，運営者は巻き返せなかった．2 回戦では，初期の段階で，運営者が，サーバの JavaScript を編集して，レベルアップチートを修正した．他の脆弱性についてもほぼ修正され，安定した運用がなされていた．そのため，利用者は，プレイの自動化などを行う必要があった．

レベルアップチートについては，レベルを上げる JavaScript のコードを削除し，正常なプレイができない状態にしてしまうチームがあった．正常にプレイできるかどうかのチェックは，自動化されていた．しかし，レベルアップについては確認していなかったため，正常稼働と判定されてしまった．結果，競技システムの穴を突かれた形となった．他にも，RMT されたアカウントを BAN する際に，同一のアカウントを何度でも BAN できてしまう不具合が競技システムにあった．シェルコマンドを利用し，その不具合を突いて，大幅に得点されるという場面があった．

攻撃側は，ブラウザ上で JavaScript を直接実行することで，様々な攻撃を実現していた．画面全体をランダムに走査し，カエルを捕まえるチートを行ったチームもいた．画面上を明滅するようにキャラクタが移動するため，ゲーム画面を見ればすぐに気付く状態だった．運営者の対抗策として，JavaScript の setTimeout 関数を利用し，1 回あたりの通信に待ち時間を設けるチームもあった．この対策はとても有効であり，短時間での急激な得点を防ぎつつ，正常なゲームプレイを提供できる．しかし，ゲームの動作が重く感じるという難点があった．

ゲームクライアントでは，JavaScript のグローバル領域に，プレイヤデータなどの変数が公開されていた．それを利用し，JavaScript を書いて，自動プレイを試みるケースが見受けられた．プログラムの実装力が試されるため，実装に慣れているかどうかが，自動化の成否を分けているように思われる．画面上のカエルまでプレイヤを移動させ，自動で捕獲するスクリプトもあった．しかし，運営者によって，通信に待ち時間を設けられ，短時間での得点には至らなかったようである．

セキュリティ・キャンプの参加者とは別に，2 回戦では，チューターにも CtFrog で競技を行ってもらった．その結果，運営者によってリソースファイルの変更が行われ，プレイヤの画像がカエルの画像に置き換えられていた．また，カエルは不可視の画像に変更され，カエルの位置が見えないようにされていた．人間にとっては，正常なプレイが困難になるが，正常にプレイできるかどうかの機械的なチェックでは，正常ではないと見抜くことが難しそうである．あ

ⓒ 2018 Information Processing Society of Japan

る意味，運営者による競技システムへの攻撃といえる．

7.2 アンケートの結果

参加者からのアンケート結果を図 6 に示す．参加者の感想の傾向としては，中級者レベルは楽しめていた様子であった．しかし，上級者は，攻撃側としては物足りず，初級者は，防御側も攻撃側もハードルが高い様子であった．それでも，初級者は，上級者の様子を傍から観察し，どういったことを行っているのか積極的に質問するなど，積極性が見られた．防御側は，リアルタイムで続く攻撃を防がなければならないという，普段はなかなか体験することのできない焦りを体験することができていたようである．しかし，サービスの正常判定が甘く，ゲームバランスが良くないという声もあった．

7.3 セキュリティ教育の効果としての考察

試行実践と本番実践の結果より，セキュリティ教育としての効果は，技術的な面と精神的な面において，多少は認められると考える．試行実践では，「業務としてやっているように感じる」という感想が出ているため，題材としては，実務に近い体験を提供できていると言える．また，本番実践では，初級者が中上級者から学ぶといった場面が見られた．防御側は，実務と似たリアルタイム性を体験しており，セキュリティ教育において重要な体験を得ていると言える．プログラムのコードが参考になったという声もあったため，技術的にも教育の効果はあったと言える．

長期的には，参加者が何らかの形でオンラインゲームの開発や運営に携わった際に，本講義の内容を思い出してもらうことで，何かしらの反省を活かせるのではないかと考える．何故なら，どのようなバグが脆弱性を引き起こすのかについてや，プレイヤがどのような行動をとるのかについて，いくらかの体験を得ているからである．予備知識や経験がない状態では，攻撃者やプレイヤの思いもよらぬ行動に翻弄されてしまうことも少なくない．この点だけでも，教育としての意義は十分に認められると考えている．

7.4 攻防型 CTF イベントとしての考察

攻防型 CTF イベントとして見たときに，本番実践については，あまりよい結果とは言えないと考える．その理由として，攻防のアンバランスが挙げられる．今回は，主催者として，意図的に，1 回戦では攻撃側が圧勝し，2 回戦では防御側が勝てるように調整していた．しかし，参加者にはその意図が見えないため，1 回戦における防御側の圧倒的な不利に対し，大きな不満を与えてしまっていた．また，スコアサーバによるオンラインゲームの正常稼働判定に問題が多数あることも相まって，2 回戦における防御側の圧倒的な有利が発生していた．この点でも，参加者に対して不満を抱かせてしまった．攻防型 CTF では，バランス調整が難しいため，うまくバランスをとるための工夫が必要である．

本番実践の結果がよいとは言えない別の理由として，主催側で用意した脆弱性の少なさが挙げられる．2 回戦においては，防御側は，すべての脆弱性を修正しきってしまい，手持ち無沙汰になってしまっていた．そして，攻撃側が攻撃できる脆弱性がなくなってしまい，両チームともにやるべきことがほとんどない状態となってしまっていた．脆弱性の数や幅を増やし，より広い視点で挑戦できる題材が望ましいと考える．また，競技時間を余らせるよりは，作戦会議の時間や，事後対応の策定など，CSIRT が行うような演習を取り入れることで，より実のあるイベントにできたのではないかと考える．

8. まとめと今後の課題

Web ゲームサイトを題材とする攻防型 CTF の大会イベントを提案した．ゲームサイトの運営者とチート行為を試みるサイト利用者とのチーム対抗である．企業や個人の Web 系の技術者の研修を目的とする．試行実践のアンケート結果を踏まえ，システムを改良した．

セキュリティキャンプでの本番実践では，受講者の感想から，中級者にとっては良い題材となっていたようだが，初級者には少し厳しく，上級者には不満の残る内容となった．今後，初級者に対しては，事前の講義を行ったり，対象となるソースコードを部分的に開示するなどの対策を考えている．上級者に対しては，競技としての面白さに直結する，サービスの正常判定の品質が肝と言えそうである．よって，より高精度な正常判定を考えていきたい．

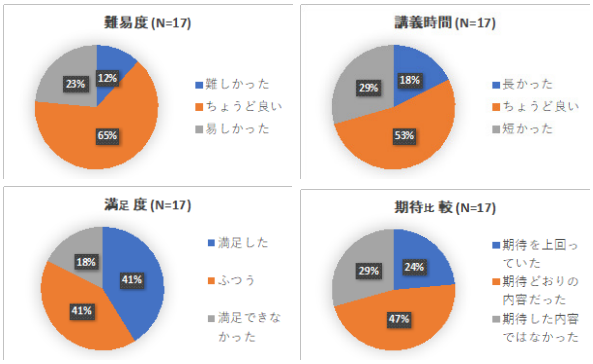


図 6 本番実践のアンケート

参考文献

[1] DEFCON, "DEFCON", https://www.defcon.org/, (参照 2018-02-09).
[2] SECCON, "SECCON". http://2016.seccon.jp/, (参照 2018-02-09).
[3] 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 研究会報告，Vol.4, 2011-GE-1, pp.1-2 (2012).
[4] 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，信学技法，Vol.112, No.66, pp.45-50 (2012).
[5] 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).

ⓒ 2018 Information Processing Society of Japan

[6] 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導入教育の支援システム, ゲーム学会 研究会報告, Vol.6, 2012-GE-1, pp.1-4, (2013).
[7] 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).
[8] 中矢誠, 赤木智史, 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 - 大会運営サーバ BeeCon の設計と実装 - , 信学技報, Vol.115, No.223, pp.53-60 (2015).
[9] 赤木智史, 中矢誠, 富永浩之 : セキュリティを意識させる情報リテラシ教育のためのハッキング競技CTFの問題分類と出題形式, ゲーム学会 研究会報告, Vol.8, No.2014-GE-1, pp.1-4 (2014).
[10] 赤木智史, 中井智己, 中矢誠, 富永浩之 : ハッキング競技 CTF を取り入れたセキュリティを意識させる情報リテラシ教育の大会イベント - 大会運営サーバの機能と初心者向けの問題設定 - , 信学技報, Vol.114, No.513, pp.39-44 (2015).
[11] 楠目幹, 阿部隆幸, 中矢誠, 富永浩之 : 情報セキュリティの導入教育のための大会イベント BeeCon におけるハッキング競技 CTF の問題構築, 情報処理学会 第 79 回全国大会 講演論文集, Vol.79, No.7ZC-07, pp.739-740 (2017).
[12] 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 講演論文集, Vol.2014, No.2, pp.169-172 (2014).
[13] 赤木智史, 中矢誠, 富永浩之 : セキュリティを意識させる情報リテラシ教育のためのハッキング競技CTFの大会サーバと運営方法, 情報処理学会 第 77 回全国大会 講演論文集, pp.919-920 (2015).
[14] 中矢誠, 赤木智史, 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).
[15] 中矢誠, 田澤征昭, 堀内晨彦, 田中翔也, 富永浩之 : セキュリティの導入教育のためのハッキング競技 CTF の IT 系イベントによるオープン実践とユーザ評価, 情報処理学会 第 78 回全国大会 講演論文集, Vol.78, No.1ZC-04, pp.821-822 (2016).
[16] アキュトラス, "BeeCon". https://beecon.aqutras.com/, (参照 2018-02-09).
[17] 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 研究会報告, Vol.7, No.2013-GE-1, pp.4-9 (2014).
[18] 中井智己, 赤木智史, 中矢誠, 富永浩之 : セキュリティを意識させる情報リテラシ教育のためのハッキング競技CTFと融合させる余興ゲームの事例と要件, 情報処理学会 第 77 回全国大会 講演論文集, pp.917-918 (2015).
[19] 中矢誠, 赤木智史, 富永浩之 : ハッキング競技 CTF と余興ゲームを組み合わせたセキュリティを意識させる情報リテラシ教育の導入イベントの運営サーバ, 情報科学技術フォーラム FIT2015 講演論文集, pp.399-400 (2015).
[20] 阿部隆幸, 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としての RPG, ゲーム学会 第 14 回全国大会 講演論文集, pp.31-34 (2016).
[21] 阿部隆幸, 中矢誠, 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 - 高大連携に向けたクイズ形式のアドベンチャー型の余興ゲームの設計と問題に関する調査 - , 信学技報, Vol.116, No.126, pp.39-44 (2016).
[22] 阿部隆幸, 太田翔也, 中矢誠, 富永浩之 : 情報セキュリティの導入教育としての学校情報をシナリオに含んだクイズ形式のアドベンチャーゲーム, ゲーム学会 第15回全国大会 講演論文集, pp.27-30 (2016).
[23] 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 - 高大連携に向けたクイズ形式のアドベンチャー型の余興ゲームの試作と予備実験 - , 信学技報, Vol.116, No.517, pp.123-128 (2017).
[24] 阿部隆幸, 中矢誠, 太田翔也, 富永浩之 : 学校機関ごとの個別情報を組み込んだ情報セキュリティの導入教育のためのクイズ形式のアドベンチャーゲームの試作, 情報処理学会 第 79 回全国大会 講演論文集, Vol.79, No.7ZC-06, pp.737-738 (2017).
[25] USENIX, “USENIX”. https://www.usenix.org/, (参照 2018-02-09).
[26] C. Cowan, S. Arnold, S. Beattie, C. Wright and J. Viega: Defcon capture the flag : Defending vulnerable code from intense attack, In DARPA Information Survivability Conference and Exposition, 2003, Proceedings, Vol.1, pp.120-129 (2003).
[27] C. Eagle and J. L. Clark : Capture-the-flag: Learning computer security under fire, NAVAL POSTGRADUATE SCHOOL MONTEREY CA (2004).
[28] 原田悠我, 豊田美咲, 近藤秀樹, 小出洋 : リアルタイムセキュリティコンテスト可視化システムの提案, 第 55 回プログラミング・ シンポジウム予稿集, pp.89-95 (2014).
[29] K. Zhang, S. Dong: picoCTF 2013-Toaster Wars: When interactive story telling game meets the largest computer security competition, Games Innovation Conference (IGIC), pp.293-299 (2013).
[30] P. Chapman, J. Burket, D. Brumley : PicoCTF: A Game-Based Computer Security Competition for High School Students, 2014 USENIX Summit Gaming Games Gamification Security Education (3GSE) (2014).
[31] K. Boopathi, S. Sreejith, A. Bithin : Learning Cyber Security Through Gamification, Indian Journal of Science and Technology, Vol.8, No.7, pp.642-649 (2015).
[32] fbctf, “fbctf, https://github.com/facebook/fbctf, (参照 2018-02-09).
[33] Vigna, Giovanni, et al., Ten Years of iCTF : The Good, The Bad, and The Ugly, 3GSE (2014).
[34] Raj, Arvind S., et al. : Scalable and Lightweight CTF Infrastructures Using Application Containers, 2016 USENIX Workshop on Advances in Security Education (ASE 16), USENIX Association (2016).
[35] 中矢誠, 大川昌寛, 中島雅弘, 富永浩之 : Web ゲームサイトを題材とした攻防型ハッキング競技の提案, 情報処理学会 第 79 回全国大会 講演論文集, Vol.79, No.4D-03, pp.517-518 (2017).
[36] セキュリティ・キャンプ実施協議会, "セキュリティ・キャンプ", http://www.security-camp.org/, (参照 2018-02-09).
[37] 中矢誠, 大川昌寛, 中島雅弘, 富永浩之, “Web ゲームサイトを題材とした攻防型ハッキング競技の提案”, 情報処理学会 第 79 回全国大会講演論文集, Vol.79, No.4D-03, pp.517-518 (2017).
[38] 中矢誠, 大川昌寛, 中島雅弘, 富永浩之 : Web ゲームサイトを題材とした攻防型ハッキング競技の環境構築と運用実践 - 試作版の機能実装と試行実践による今後への検討 - , 信学技法, Vol.117, No.65, pp.7-12 (2017).
[39] M. Nakaya, M. Okawa, M. Nakajima and H. Tominaga : A Support Environment and a Trial Practice of Hacking Contest with Attack and Defense Style on a Game Website, Proceedings of International Conference Information Visualisation, IV2017, pp.360-365 (2017).
[40] M. Nakaya and H. Tominaga : Hacking Contest Rule and an Official Practice of Information Security Event with Attack and Defense Style on a Game Website, Proceedings of WCTP 2017, pp. 260-277 (2017).

ⓒ 2018 Information Processing Society of Japan