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

赤木智史[†1]　中矢誠[†2]　富永浩之[†1]

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，攻撃側と防御側が競い合う競技である．ハッカー達の腕試しや交流の場として，各地で CTF 大会が開催されている．本論では，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を提案した．CTF の現状を概観し，問題の分類とパターン化を試みた．大会支援システム BeeCon を開発し，CTF 競技と余興ゲームによって，観戦者を巻き込む大会を目指した．余興ゲームとして，ゲーム性が高く，ルールが単純な神経衰弱を実装した．情報系学生に対してコンテストを試行し，ユーザ評価を行った．

A Practical Report of an Introductory Educational Experience with Hacking Competition CTF for Information Security Learning

SATOSHI AKAGI[†1]　MAKOTO NAKAYA[†2]
HIROYUKI TOMINAGA[†1]

Recently, a hacking competition CTF is paid attention, which means “Capture The Flag”. The competition is to find hiding information as a flag in a Web site. There are held a lot of CTF events in the world to compete in IT skill and have communication among hackers. We propose an easy CTF event as an introductory educational experience of information security. We classify questioning style and pattern of CTF and discuss educational contents and the purpose. We developed support system BeeCon. It offers CTF exercises and gaming factor for cooperation between competitors and supporters. For a gaming factor, we adopt a card game concentration which has highly contingency and simple rule and participants are familiar with it. We carried out some educational practices with students in information engineering college. We introduce the situation and the result.

1. はじめに

近年，公共機関や大手企業の情報システムを狙ったクラッキング事件が増え，情報セキュリティの重要性が認識されるようになってきた．そのため，管理者だけでなく，個人サイトの運用者や一般ユーザも含めた幅広い層に対する情報セキュリティ教育の必要性が高まってきた．このような教育では，関連するネットワークやサーバの知識だけでなく，何らかの場で実習して，経験を積むことが求められる．例えば，ペネトレーションテストのように，擬似的な攻撃と防御のシミュレーションが効果的である．

大学においても，情報処理教育の初期段階から，体験的な情報セキュリティ教育の場が求められている．問題が起こってからではなく，最初からセキュリティを重視したモノづくりを意識させる必要がある．しかし，体系的なカリキュラムを組んで，このような機会を用意することは環境整備などの点で労力がかかり難しい．一方，初心者の関心と興味を惹くには，何らかのゲーム要素を取り入れ，当事者としての意識を高めさせる工夫が必要である．

†1 香川大学
Kagawa University
†2 インターシティ
InterCity

2. ハッキング競技 CTF の概要と現状

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に見立てて，攻撃側と防御側が競い合うゲームである．ハッカー達の腕試しや交流の場として，各地で CTF 大会が開催されている．有名なものとして，米国の DEFCON や韓国の CODEGATE がある．

日本では，以前から「sutegoma2」というチームが CTF 大会で好成績を収めていた．2012 年になって，2 月(九州工業大学情報工学部)と 5 月(筑波大学)に，SECCON CTF が開催され，遅ればせながら注目が高まってきている[1].

3. 教育イベントとしての実施形態

先行研究では，教育イベントとしての CTF を提案した[2][3][4]．教育イベントの位置づけを集中演習としての大会とし，講義や実習との関係を図 1 に示す．この位置づけを元に，情報セキュリティの導入教育の支援システム BeeCon を提案する．

BeeCon におけるコンテストは，CTF 競技と余興ゲームを織り交ぜたものとする[5][6]．競技へ参加する競技者と，競技を観戦する観戦者に加えて，競技者をサポートする応

援者という立ち位置を導入する．応援者は競技を行わないが，競技と連動しているゲームへ参加し，競技者をサポートする．応援者は，競技の結果に影響を与えることになり，間接的な競技への参加を体験する．このように，観戦者を巻き込み，未来の競技者へとつなげる（図 2）．

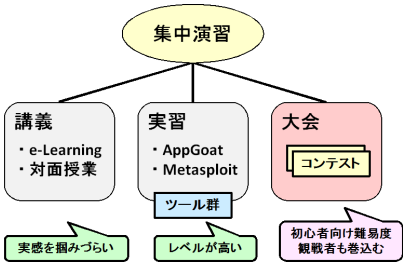

図 1　情報セキュリティの集中演習

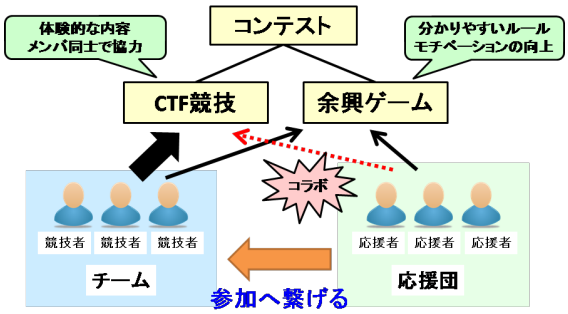

図 2　教育イベントとしての CTF 大会

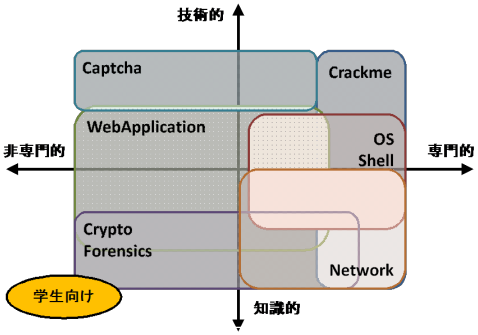

図 3　CTF の問題の分類

レベル	学習内容
1	キーボードのキー配置とシフト操作 WebページやHTMLソースを閲覧
2	画像や音声のファイル形式 ユーザ認証とパスワードの危険性
3	二進数やビット列の変換と計算 文字コードの変換
4	ハッシュ関数、文字列処理 バイナリエディタでビット列を眺める

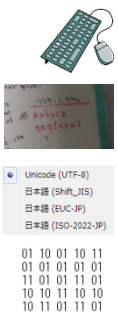

図 4　レベルと学習内容

4.　CTF 問題のパターン化

先行研究では，CTF の問題を図 3 のように大まかに分類した[5]．CTF の問題を考案するには，情報セキュリティに精通している必要がある．出題者のハードルを下げるために，問題のパターン化を試みる．学生向けと考えられる分類 Crypto や Forensics，Web Application に着目してパターン化の例を述べる．

(1)　**Crypto**

Crypto では，パスワード管理に関する問題が挙げられる．パスワードの文字列長を短く設定した圧縮ファイルや Office ファイルを提示し，復号化させる．パスワードの文字列長が短ければ，専用ソフトを使うことで瞬時に解析されてしまうことを体験する．

(2)　**Forensics**

Forensics では，メディア情報の管理に関する問題が挙げられる．EXIF タグが埋め込まれた JPEG ファイルを提示し，撮影場所を答えさせる．ファイルには，目に見えない情報が含まれており，安易に写真をアップロードすることの危険性を体験する．

(3)　**Web Application**

Web Application では，さまざまな Web サービスに関する問題が挙げられる．IP アドレスを提示し，その接続元のおおよその所在地を答えさせる．IP ひろばなどの Web サービスを用いることで，ある程度の所在地が分かってしまうことを体験する．

また，問題を解くために必要な技術などによって，難易度を設定する．難易度設定の例を，図 4 に示す．複数の技術を組み合わせて解く問題は，問題の解答ステップを想定し，各ステップの難易度を設定する．その和を，問題の難易度とする．ただし，これは目安であるので，出題者の裁量で適当な設定を行う必要がある．

5.　システムの設計と実装

BeeCon の実装には，Ruby on Rails を用いた．CTF 競技と余興ゲームについては，モデルでの分離を行った．コンテストとゲームは，インタフェースを通じて処理を行う．動作概念図について図 5 に示す．

競技者と応援者とのコミュニケーションツールとして，エモーション機能を実装した．応援者が問題の解答を競技者に教えることのないよう，あらかじめ用意されたエモーションのみで意思疎通を図る．コンテストページの GUI を図 6 に示す．

管理機能としては，図 7 のようなコンテストの管理ページと，図 8 のような問題の管理ページを実装した．問題の管理では，問題ごとにヒントや講評を設定できる．コンテストの管理では，解答状況の確認などができる．

余興ゲームには，神経衰弱を採用した．神経衰弱は，ル

ールが単純で，逆転性などのゲーム性が高い．得点ランキングおよび得点の遷移をグラフ表示として実装した．各チームの得点状況が視覚的に分かり，競技者のモチベーションの向上が期待される．余興ゲームの GUI を図 9 に示す．

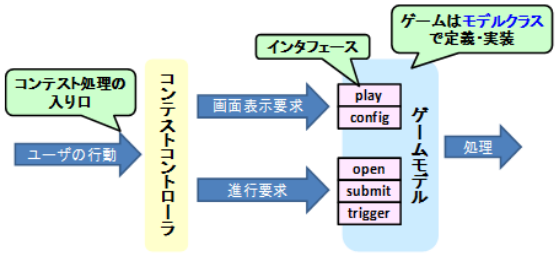

図 5　ゲームインタフェースの概念モデル

図 6　コンテストページの GUI

図 7　コンテストの管理機能の GUI

図 8　問題の管理機能の GUI

図 9　余興ゲーム神経衰弱の GUI

6. コンテストの実施概要と出題

実装したシステムを用いて，コンテストの試行を行った．BeeCon を用いたコンテストは，これまでに 4 回行っている．5 回目の今回を含むコンテストの実施概要を表 1 に示す．前回までの実施におけるアンケートでは，問題が全体的に易しいので，難しい問題を出題してほしいという意見が多く見られた．そこで，今回は，難易度の幅を持たせた多くの問題を出題し，競技者が飽きないよう工夫した．以前は，標準的な解答時間を，1 問あたり平均 5 分としていたが，今回は，1 問あたり約 3 分の設定とした．なお，問題の評価を主な目的とするため，応援者は設けていない．以下に，今回のコンテストで出題した問題の例を挙げる．

(1) **Trivia**

OSI 参照モデルの第 2 層は何か，システムの信頼性評価の要素をまとめた RASIS は何という単語の頭文字か，といった知識的な問題を出題した．情報系の事項を学習する上での基本的な用語に触れさせる目的がある．

(2) **Forensics**

MS Office 2010 の Word ファイル（拡張子 docx）からフラッグを探せという問題を出題した．Office 2007 以降のファイルは，拡張子を zip に変更して解凍することで，個々のデータが抽出できる．解凍すると，文書上には表示されていない画像が現れ，そこにフラッグが書かれている．

(3) **Miscellaneous**

排他的論理和を用いた論理演算を行う問題（図 10）や，動画の 1 フレームにだけ表示されるフラッグ文字列を読み取る問題を出題した．前者は，論理的思考の初歩となる考え方を学習させる目的がある．後者は，動画に個人情報などが一瞬でも映ってしまうと，漏えいする危険性があることを認識させる目的がある．また，このカテゴリの問題は，CTF の導入として，興味をひくという意図もある．

(4) **Crypto**

シーザー暗号や換字式暗号を解読させる問題を出題した．今回の換字式暗号は，英小文字の o, i, z を，数字の 0, 1, 2 に置換するといった，見た目にも判別しやすい簡単なものである（図 11）．安易な暗号化では，簡単に復号化されてしまうことを体験させる目的がある．

(5) **Network**

CTF 経験者向けに，パケットダンプファイルから，閲覧している Web ページを特定させる問題を出題した．ネットワーク上を流れるデータは，アプリケーションのユーザには見えない．しかし，通信データ自体を記録すれば，どのようなデータがやり取りされているかを見ることができる．それを解析することにより，閲覧したデータを特定することができる．そのような方法を学ばせることが目的である．

表 1　コンテストの実施概要

回	開催日	参加者数			出題数
		競技者	応援者	合計	
1	2013.02.15	2	3	5	10
2	2013.03.14	10	0	10	9
3	2013.03.18	11	11	22	17
4	2013.05.22	28	9	37	20
5	2014.05.17	20	0	20	30

(+) という特殊な記号を使った計算の謎を解き、最後の問題の答えを求めよ。

101 (+) 110 = 011
1001 (+) 0101 = 1100
11001 (+) 10011 = 01010

1010010101 (+) 1100111101 = ??????????

図 10　論理演算を行う問題の例

あるユーザのIDとパスワードが流出した。
ここから、Twitterのパスワードを推測しろ。
◎楽天
ID：kanamezyunn0221
password：kaname2yunno z z i
◎Google
ID：nakamurayuuiti0220
password： nakamurayuu1t1ozzo
◎Twitter
ID：udon0141

図 11　換字式暗号の問題の例

7. コンテストの実施とユーザ評価

今回，実施したコンテストの参加者は，情報系の大学生 20 名で，9 つのチームに分けた．各チームは 3 人以下のメンバである．チーム単位で得点を競うコンテストとして開催した．コンテスト時間は 90 分とした．出題した問題は 30 問で，技術的な知識がなくても解けるようなものから，複雑な手順を要求されるものまで，幅広く用意した．過去のコンテストで使用された問題も，難易度が程よく，参加者の知識の増加や技術の向上に役立つと判断したものについては，出題した．また，参加者の中には CTF 経験者もいたので，複雑な手順を要求する問題も 5 問ほど出題した．

コンテスト開始時には，用意した 30 問の問題のうち，20 問だけを公開した．残りの 10 問はコンテスト途中で公開し，解答意欲をかき立て，競技に飽きないよう工夫した．

結果として，どのチームも最低 13 問，平均 19 問程度を解いた．全問を解いたチームはなかった．競技終了後は，参加者から要望のあった問題について，解法と出題の意図を説明した．併せて，参加者に対してアンケート調査を行った．出題した問題への意見，システムの機能への意見を求める設問を用意し，それぞれ自由記述式で回答を求めた．

出題した問題については，難易度が幅広く楽しかったという意見が全学年から挙がった．一方，主に 1 年生から，配点の高い問題が難しすぎるという意見も挙がった．また，数人の 1, 2 年生から，各問題のヒントの充実や，問題を解くのに必要なツールの提示およびそのツールの解説といった，問題を解く足掛かりを増やしてほしいという意見があった．過去のコンテストに参加した経験を持つ参加者からは，以前の問題の使い回しを減らし，新しい問題の割合を増やしてほしいという意見があった．

システムの機能については，競技の残り時間のリアルタイムでの表示といった機能の追加を望む意見や，個別の問題の別タブでの表示といった機能の修正を望む意見があった．また，チームごとの得点推移のグラフによって，リアルタイムで得点状況が分かりモチベーションの向上につながったという回答を得た．

8. おわりに

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 BeeCon を提案した． CTF の作問のハードルを下げるため，問題のパターン化を試みた．新作の問題を追加し，コンテストを試行した．ユーザ評価のアンケートを実施し，システム改善のための意見を得た．

今後の課題として，システムのインタフェースの改善がある．特に，競技者と応援者との意思疎通について，どのようなエモーションが必要なのかを再検討する．問題については，より初心者向けの体系的な分類とパターン化を試みる．4 回程度のコンテストからなる大会の運用実験を情報系学科の新入生に対して行い，教育効果を検証する．

参考文献

1) SECCON CTF 実行委員会, http://www.seccon.jp/.
2) 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, No1.66, pp.45-50, (2012).
3) 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, pp.378-379, (2012).
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 GE 研究部会 研究報告, Vol.5, 2011-GE-1, pp.1-4, (2012).
5) 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 GE 研究部会 研究報告, Vol.6, 2012-GE-1, pp.1-4, (2013).
6) 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 GE 研究部会 研究報告, Vol.7, 2013-GE-1, pp.1-6, (2014).