7ZC-07

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の初中級レベルの問題構築

楠目幹† 阿部隆幸† 中矢誠† 富永浩之†
香川大学† 香川大学† 香川大学† 香川大学†

1. はじめに

ハッキング競技 CTF は，サーバ側に隠された情報を旗(フラッグ)に見立て，ハッカーとしての知識や技能を総動員して，それを探し出すものである(図 1)．インターネット上で参加できるチーム対抗の大会が多い．世界各地で開催され，マスコミでも注目されている．インターネット上での参加も多い．日本でも，SECCON[1]が開催され，参加者の裾野も広がっている．

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，CTF を中心とする大会イベントを提案している[2]．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．大会運営サーバ BeeCon を開発し，試行的に運用している[3]．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．

サポーター制のように，観戦者にも，特定の競技チームへの応援団という役割を与える(図 2)．そして，競技者と応援者が協調して取り組む余興ゲームを取り入れている．余興ゲームは，ハッキング競技 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．

大学などで実施する場合，大会は，時期を空けて，4回程度の実施を想定している(図3)．各大会では，競技チームと応援団のメンバの変更や，参加者の入替えがある．それに応じた出題の分野と難易度に調整する．最初は単なる観戦者だった利用者も，次回の大会からは応援者，そして競技者へと，より積極的な参加を促していく．逆に，過去の大会で既に競技者を務めた先輩が，後輩にエールを送る形で応援者になってもよい．

Problem Construction of Hacking Competition CTF in BeeCon Contest as Introductory Educational Experience for Information Security Learning
†Motoki KUSUME, Kagawa University
†Takayuki ABE, Kagawa University
†Makoto NAKAYA, Kagawa University
†Hiroyuki TOMINAGA, Kagawa University

3. CTF の問題の分類と構築

BeeCon の CTF は，防御側が出題者のサーバで，攻撃側が解答者である，最も基本的なジェパディ方式である．出題する問題は，情報セキュリティおよび情報リテラシにおける学習内容で分類し，難度に応じて 6 段階のレベルとする(図 4).

(1) レベル 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．1-1 の例として，半角の英数字と記号からなる文字列が与えられ，各文字に対応するキーをかな入力で打鍵するとフラッグが得られる．1-3 の例として，ヒントから URL を推定し，直接入力して該当ページを見つける．1-4 の例として，Google の AND/OR 検索，日付特定や除外機能を活用して，目的の Web ページを呼び出し，Web ブラウザのページ内検索で，フラッグを見つける．

(2) レベル 2 は，不審なデータや安易な操作の危険性を実感させる．2-1 の例として，誰かの作業机の写真が提示され，そこから ID とパスワードが書かれたメモを見つけ，認証ページにログインしてフラッグを得る．様々な Captcha を提示して，正しく入力する．2-2 の例として，添付ファイルの誤った拡張子を修正して，中身を閲覧し，フラッグを得る．2-3 の例として，同様であるが，画像・音声・動画を再生してフラッグを得る．2-4 の例として，指定された Web ページの HTML ソースの 1 行目を入力させる．2-5 の例として，Twitter のつぶやきからアカウントを特定し，プロフィール情報を入手する．

(3) レベル 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．3-1 の例として，文字化けのテキストを提示し，文字コードを推測して正しい文章を表示する．3-2 の例として，二進数やビット列の変換と計算でフラッグを得る．3-3 の例として，シーザー式や換字式といった古典暗号や，base64 エンコードされた文字列の解読を行う．

(4) レベル 4 は，セキュリティに大きく関係し

てくる．バイナリエディタも必要となる．4-1 の例として，ツールを用いて文字列をハッシュ値に変換したり，ハッシュ値をクラックして平文を割り出す．4-2 の例として，文字列の検索と正規表現を利用して，サーバのログから不審なアクセスを見つけ出す．4-3 の例として，添付された写真ファイルをバイナリエディタで開き，表示されたバイナリデータからフラッグを得る．

(5) レベル 5 は，専用のツールやコマンドを利用して，データの特徴を分析する問題である．5-1 の例として，Linux コマンドの履歴からパスワードを探し出す．5-2 の例として，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．かなり高度であるが，簡単なフォレンジックスも含まれる．5-3 の例として，パケットキャプチャソフトを用いて，パケットデータから閲覧していたサイトを特定する．

(6) レベル 6 は，CGI や DBMS など，Web サイトの脆弱性を突く問題である．実際に経験がないと難しい．意欲的な学生への挑戦的な出題である．6-1 の例として，JavaScript のソースを見て，フォーム送信するデータを書き換える．6-2 の例として，入力フォームに対して XSS を行い，Web ページの中からフラッグを取得する．6-3 の例として，ログイン画面等の入力フォームに対して SQL インジェクションを行い，パスワードやフラッグを取得する．

一般に，CTF の問題は，解法を明示せず，不親切な出題が多い．そのため，実際には，上位のレベルの問題を，コンテストの開催中に解くことは難しい．そこで，一定時間の後や，多少の減点の代わりにヒントを提示することを導入する．特に，応援団が余興ゲームを通して，ヒントの獲得に貢献できるようにする．

4. おわりに

情報セキュリティの導入教育の一環として，初心者を対象とする CTF 大会を提案し，大会運営サーバ BeeCon を開発している．競技チームに対する応援団という立場を導入し，余興ゲームに参加して，CTF 競技の得点に関与する．CTF は，ジェパディ型で，分野と難度に応じて，6 段階のレベルを設ける．大会ごとに，出題の割合を変え，主な対象者への適応や性格付けを行う．これまで，試行的な開催を行っているが，十分な問題を用意し，運用実験を実施して，システムの教育効果を検証したい．

参考文献

1) SECCON : SECCON CTF, http://www. seccon. jp/.
2) 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 - , 信学技法, Vol.115, No.223, pp.53-60 (2015).
3) 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).

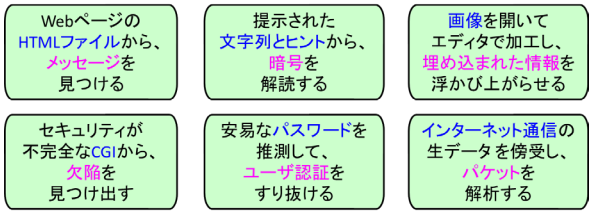

図 1 一般的な CTF の出題例

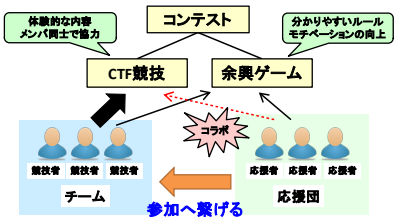

図 2 サポーター制による競技者と応援者の協調

回	意図	時期	初級	中級	出題の割合					
					1	2	3	4	5	6
1	各自の現状把握	最初	競技	競技	◎	◎	○	○	×	×
2	中級者への刺激	途中	応援	競技	△	◎	◎	○	○	○
3	応援者を誘引	最後	競技	応援	○	◎	◎	○	×	×
4	忘れた頃に復習	事後	競技	競技	△	◎	◎	◎	○	○

図 3 大会ごとの出題構成と参加者の遷移

段階	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
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
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 二進数やビット列の変換と計算 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
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
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
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)

図 4 問題のレベル設定と出題分野