4D-03

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

中矢誠† 大川昌寛‡ 中島雅弘‡† 富永浩之†
香川大学† 北陸先端大学院大学‡ アーヴァイン・システムズ‡† 香川大学†

1. はじめに

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．日本ではSECCONが有名である[1].

現在の CTF は，上述の主催者からの出題に競技者が解答する出題型(Jeopardy)が多い．しかし，主催者を防御側とし，サーバ自体に競技者が攻撃を仕掛け，最も早くフラッグを獲得する突撃型(King of Hill)もある．さらに，競技者が各自のサーバを構え，防御と攻撃で対戦する攻防型(Attack&Defense)もある．

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[2]. 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．大学新入生を主な対象に，簡単な問題を構築し，幾つかの試行実践を行ってきた.

2. 攻防型 CTF の大会イベントの提案

BeeCon は，情報セキュリティへの認識を一般ユーザにも高めるため，裾野を広くす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，本論は，攻防型 CTF を開催するシステムを，新たに開発中である．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.

こちらは，Webサーバの管理者，Webサービスの開発者，Web サイトの運用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．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．すなわち，利用者の一部に，クラッカーが混じっており，そのチート行為に対処するというものである.

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用者とゲーム利用者がいる二重構造になっている．安全で円滑な実施のためには，仮想環境の構築が必須である．そのため，出題型ほど実施例は多くはない.

3. 攻防型 CTF の大会イベントのルールと進行

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，防御側のサイト管理者と，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，サイトの管理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，勝敗を競う．ゲームの終了後，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チームが互いに自分のゲームサイトの防御と，相手への攻撃を同時に行う方式も考えらえる.

4. 試作版のゲーム題材と技術項目

現在の試作版では，Capture the Frog という独自のマルチプル・オンライン型の Web ゲームを題材としている(図 1)．これは，ゲームの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ものである．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．蛙は，マス目にランダムに出現する．捕獲数でプレイヤのキャラクタがレベルアップする．プレイヤ同士で，蛙の取合いをする．より強いキャラクタを育て，仮想の現金取引でアカウントを売って競技点を稼ぐ(図 1).

運営者にとっては，このようなゲームでは，チートが横行し，ゲームバランスが崩れやすい.

Trial Practices of Offensive and Defence Hacking Competition for Game Website
†Makoto NAKAYA, Kagawa University
‡Masahiro OKAWA, JAIST
‡†Masahiro NAKAJIMA, Irvine Systems Inc.
†Hiroyuki TOMINAGA, Kagawa University

それにより，善意のプレイヤが迷惑を感じ，利用しなくなる．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．具体的な不正行為には，自動操縦の 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．

主催者が，防御側に用意したサイトは，Node.js + Express + Socket.IO で実装され，DBMS は SQLite を用いている．以下のような脆弱性を残しておく．

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

防御側は，事前にソースコードを読むことができる．この時点で，脆弱性を見つけ，対処を始めなければならない．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，プレイヤからの不審な行為を見抜き，早急に対処する．脆弱性のバグを修正するだけでなく，管理者として，不正行為を無効にしたり，不正ユーザのアカウントを停止する．必要ならば，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．

一方，攻撃側のプレイヤには，本イベントのルール上，以下のようなチート行為を認めている．プレイヤ同士もチャットで相談できる．脆弱性を見つければ，複数で攻撃を仕掛けることもある．特に，クライアント側の JavaScript 処理に対しては，サーバ側に送信するデータの改竄が容易である．サーバ側で，範囲チェックなどを行わないと，予期しないチート行為を許容してしまう．ただし，DoS 攻撃など，ネットワークに負荷をかける行為は，厳禁とする．

- 他のプレイヤのデータを改竄する
- チャットを荒らす
- 他のプレイヤの行為を妨害する
- 複数のアカウントを取得する
- システムを多重起動する

5.試行実施の状況と結果

本システムは，IPA が 2016 年 8 月に開催するセキュリティ・キャンプ全国大会での実施に向けて開発した．これに先立ち，本学科の学生サークル SLP と Irvine Systems 社の協力の下，2016 年 7 月に，試作版で試行実施を行った．

競技時間は 2 時間程度とした．東京の企業の技術者 4 人を防御側の運営者，高松の学生 6 人を攻撃側のプレイヤとした．防御側は，若手 2 人が主に参加し，上司の 2 人はオブザーバー的な立場であった．ただし，事前にソースコードを読む時間は設けられなかった．攻撃側は，修士生 3 名と学部生 3 名である．主催者も，モデレータとして，東京と高松に待機した．両地点は，Skype でビデオ接続し，質疑も可能とした．今回は，実際に競争するというより，双方からシステムの問題点を洗い出してもらうことが目的であり，そのための情報交換も行った．

実施後，防御側の技術者へのインタビューとして，以下の意見が寄せられた．全般的には，防御側の負荷が大きく，事前準備の時間が必要であるとの声が多かった．

- DBMS が SQLite では不便
- オンラインゲームの運営経験を要求しすぎ
- 複数人で開発できる環境は欲しい
- 修正したものをデプロイする方法を用意する
- 修正の確認にステージング環境がほしい
- 事前にコードを読む時間がほしい
- 防御側にチームとしての体制を作る場が要る
- インセプションのフェーズがあるべき
- 事前に簡単なペンテストをかけておきたい
- 時間を決めて攻撃と防御をターンベースにする
- ターンの間でモデレータが誘導する

6. おわりに

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．企業や個人の Web 系の技術者の研修を目的とする．試作版の大会運営サーバを開発し，実際に IT 企業の協力の下で，試行実践を行った．参加者へのインタビューを行い，改良点を得た．将来的には，仮想環境を整備し，互いに攻防型として実施する．

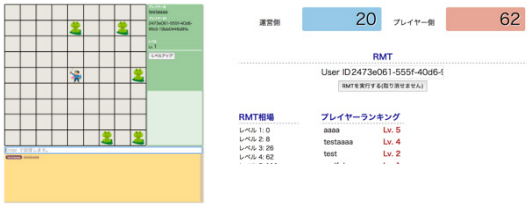

図 1 攻防型 CTF の題材の Web ゲーム

参考文献

1) SECCON : SECCON CTF, 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, No.66, pp.45-50 (2012).