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

A Proposal of an Educational Experience with Hacking Game CTF for Information Security Learning

中矢 誠，富永 浩之
Makoto NAKAYA, Hiroyuki TOMINAGA
香川大学工学部
Faculty of Engineering, Kagawa University
Email: s06t254@stmail.eng.kagawa-u.ac.jp

あらまし：近年，ハッキングゲーム 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．本論では，著者自身が参加したり実施した経験を踏まえ，CTF の現状を概観し，問題の分類を試みる．また，初心者への情報セキュリティの教育機会としての意義を論じる．
キーワード：ハッキングゲーム，CTF，初心者向けの教育イベント，情報セキュリティ

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，疑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なく，最初からセキュリティを意識したモノづくりを認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．

2. ハッキングゲーム CTF の概要と現状

近年，ハッキングゲーム 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，世界各地で CTF 大会が開催されている．

米国の DEFCON は，1993 年から毎年開催されており，セキュリティの専門家やジャーナリストが集まる，世界で最も有名なイベントである[1]．その CTF 大会は，各チームにネットワーク環境が与えられ，自分のチームの環境を攻撃から守りつつ，他のチームの環境を攻撃するというものである．大会の流れとして，最初にインターネット上で予選が行われ，上位 10 チームが本選に参加する．

韓国の CODEGATE は，ハッカーの育成を目的として，政府の後援などを受け，2004 年から開催されている[2]．本戦は，双六のようなゲーム要素も取り入れている．こちらも優秀なハッカー達が海外から参加し，熱戦を繰り広げている．

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[3][4]．

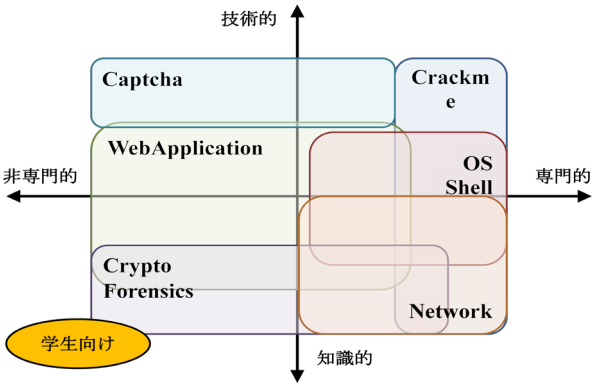

図 1 CTF 問題の分類

3. CTF の問題例

CTF の様々な問題を，以下のように大まかに分類する[5]．これらの分類は，図 1 のように，専門的か非専門的か，技術的か知識的かの 2 軸で整理すると分かりやすい．

(1) Crackme

ソフトウェアの実行バイナリに隠されたメッセージを発見する．そのために，ソフトウェアの認証をすり抜けたり，プロダクト ID を抽出したりする．

(2) Shell

指定されたサーバにログインし，バッファオーバーフロー等の脆弱性を突く．

(3) Web Application
Web ページに隠された情報を探す．また，データベースの情報を得るために，SQL インジェクションなどの技術を用い，Web サイトの脆弱性を突く．
(4) Crypto
提示された暗号を解いて，フラッグを見つける．ただし，暗号に関する高度な知識や数学を必要とするより，隠されたヒントを手掛かりに，復号の鍵や方法を見つける．
(5) Forensics
何らかのファイルが与えられ，そこからフラッグを見つける．内容は，HDD のイメージファイル，画像ファイル，音声ファイルなどである．ファイル形式の特徴となるビット列に着目したり，不自然なパターンを見つけて埋め込まれたメッセージを探す．
(6) Captcha
キャプッチャは，システムによる連続的な自動アクセスを防止するため，人間でなければ判別しにくい情報を入力させる仕組みである．CTF では，これをハッキングする問題として出題される．OCR 技術などを用いる必要がある．
(7) Network
ネットワーク上を流れるパケットデータ情報を解析する．通信されたファイルを探し出したり，どういった意図の通信が行われたのかを解析したりする．
(8) OS
OS の脆弱性を攻撃する．脆弱性が修正される前のバージョンの OS が入った環境などを攻撃する．Kernel など，低レベル層の知識や技術を問う．
(9) Miscellaneous
上記分類には入らない，余り知識や技術を必要とせず，誰でも解けるような問題である．CTF に対する興味を惹くために，導入として用意されたり，参加者に対するボーナス問題として出題される．

4. 教育イベントとしての実施形態

情報セキュリティ教育の場としての CTF には，以下のような利点がある．グループでの参加で，メンバ同士の協力が必要となる．防御側との知恵比べで達成感を刺激する．チーム間の競争意欲を刺激する．映画や小説のハッカー気分を満喫する．防御側の立場に立つと，攻撃の脅威を実感できる．これらを踏まえ，教育イベントとしての CTF を提案する．対象者と学習範囲は，表 1 の通りである．本論では，特に初心者向けの CTF について，実施形態を議論する．

CTF の問題は，以下のように，プログラム以前の学習内容とする．キーボードのキー配置とシフト操作を学習する．二進数やビット列の変換と計算を行う．文字コードの変換，ハッシュ関数，文字列処理を行う．Web ページと HTML の関係を理解する．ユーザ認証とパスワードの暗号化の仕組みを理解する．画像や音声のファイル形式を加工する．

グループ編成と出題については，以下の通りとする．1 チームあたりの人数は，2～3 人とする．実施時間は，1 回あたり 2 時間程度とする．予備知識の前提は，情報処理の基礎知識とエディタ操作とする．全体で 5～6 問を用意するが，2～3 問はすぐに解ける問題とする．単に解答数を競うだけでなく，ビンゴ形式や双六，RPG などの要素も取り入れ，ゲーム性を高める．4 回程度の実施で情報セキュリティの入門コースとして設定する．

実施の際には，運営サーバを用意し，事前にユーザとチームを登録する．サーバ上の出題ページにアクセスし，解答をサーバから提出する．チームの得点状況をランキングで表示する．コンテスト後に講評と表彰を行う．今後に向け，参考文献や関連サイトの紹介，勉強会の通知を行う．

表 1 CTF の対象者と学習範囲

対象者	学習範囲
パソコンをよく使う大学生	キーボードやマウスの操作 電卓や手計算での処理 ブラウザで Web ページや HTML ソースを閲覧
情報系の学生	テキストの加工や文字コードの変換 バイナリエディタでビット列を眺める
SE，プログラマ	脆弱性の少ない設計，開発 CGI やスクリプト言語の知識 データベースや Web サーバの設定
システム管理者	攻撃に強いシステムの構築 システムのログ解析 バグやアップデートの情報サイトとの連携
ネットワーク管理者	攻撃に強いネットワークの構築 攻撃の検知や防御をリアルタイムに対応 パケット解析

5. まとめ

情報セキュリティの重要性が増し，技術者の養成が急務である．このような教育には体験的な演習の機会が必要である．そこでハッキングゲーム CTF に着目し，初心者への入門として活用する．様々な CTF の出題を分類し，学習内容と教育目標を整理した．筆者らが運営する勉強会コミュニティ X-Lab では，情報セキュリティに関する知識や技術を共有し，互いに高め合う活動を行っている[6]．その一環として，一般人でも楽しく参加できる CTF 大会を開催している．単なるイベントで終わらせず，事前講習や事後総括も取り入れ，継続的な教育の機会を目指す．

参考文献

(1) DEF CON Communications, Inc.: DEF CON, https://www.defcon.org/.
(2) CODEGATE, http://yut.codegate.org/.
(3) SECCON CTF 実行委員会: 第 1 回 SECCON CTF 福岡大会（九州地区）, http://www.seccon.jp/p/2012ctffukuoka.html.
(4) SECCON CTF 実行委員会: 第 2 回 SECCON CTF つくば大会（関東地区）, http://www.seccon.jp/p/20125tsukuba.html.
(5) 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 研究会, 2011-GE-1, pp.1-2, (2012).
(6) X-Lab: X-CTF, http://ctf.iruca.cc/.