Using *Capture the Flag* Events as Training Opportunities

本稿は，米国で開催されているコンテストを題材に寄稿されたコンピュータセキュリティに関する随筆である（日本語訳を79ページに掲載）。

INTRODUCTION

Capture the flag（CTF）is a traditional children's outdoor game in which two teams attempt to protect their own flag, while at the same time trying to locate their opponent's flag, capture it, and return it to their own home base in order to win the game. An increasingly popular adaptation of this game has spawned an entire subculture within the computer security community. At Defcon [(1)], the capture the flag competition is one of the longest running of many well-known competitions, having been introduced in 1996 at Defcon 4.

CAPTURE THE FLAG VARIATIONS

There are two primary variations of CTF as played in computer security circles. Each offers competitors a chance to put into practice skills from all facets of the computer security field with the ultimate goal of retrieving "flags" that may be delivered to the contest organizers in order to demonstrate that a particular challenged has been solved or a particular goal met.

Perhaps the most well-known version of CTF is the version that has come to be known as the "Defcon-style" CTF. The Defcon CTF is a *full-spectrum* CTF played by a limited number of teams in a live, head-to-head event. At Defcon, the scale of this game has grown from eight teams to its current size of 20 teams that compete at a live event over the course of three days in Las Vegas, Nevada every summer. In a full-spectrum CTF, the event organizers provide each team with identical server images pre-configured with custom software developed by the organizers. Each team's server is connected into an isolated game network dedicated to the competition. Each team is required to simultaneously administer and defend their own server while attempting to penetrate the defenses crafted by each of the other teams in order to capture flags which are turned in to the organizers in exchange for points.

The rules for a full-spectrum CTF are intentionally unrestrictive in order not to limit the creativity of each team in building novel defenses. In order to prevent teams from shutting down vulnerable software as a means of defending it, teams are typically graded on their ability to continue providing these "services" to the public, which includes the organizers who periodically test whether each team's software remains accessible both to the organizers and to other teams. There is an expectation that teams patch any flaws that they find in their assigned software rather than simply shutting the software down.

As teams find flaws in their own software and come to understand how they may themselves be vulnerable to attack, they also understand that every other team playing the game is also vulnerable to the same attack. Consequently, teams attempt to use each flaw to penetrate their opponent's servers and, following each successful penetration, retrieve a flag from their opponent. Flags are placed on each team's server by the organizers and are periodically replaced in order to provide new flags to capture throughout the game. This periodic rotation of flags forces teams to repeatedly demonstrate that they can maintain access into their opponent's servers and allows for the gradual evolution of both defenses and offenses as the game progresses.

The Defcon CTF has become so popular that hundreds of teams attempt to qualify to play in the Defcon CTF every year with many of these teams spending months of preparation time in the hopes of earning a trip to Las Vegas. Increasingly the Defcon CTF is becoming an international event. Prior to 2006 competitors at Defcon

consisted solely of American teams. In 2006, the first international team, from South Korea, qualified and participated in the Defcon CTF. In 2013, two-thirds of the participating teams at the Defcon CTF were international teams including teams from Japan, South Korea, China, Russia, and mixed European teams.

A number of other full-spectrum CTFs have developed since the first Defcon CTF. Most of these are open primarily to academic institutions with the most well-known of these being the University of California, Santa Barbara's iCTF（International CTF） competition which has become the largest scale full-spectrum CTF in existence. In 2013, the iCTF hosted 90 teams from around the world in an eight-hour live event.

The second variation of CTF is based on the concept of solving puzzles in order to be awarded points. In a puzzle CTF, organizers develop a number of security-related challenges and make them available to participants for solving. Participants do not interact with one another; instead teams race to be the first to solve puzzles and to gather the most points.

The infrastructure to host a puzzle CTF resembles a traditional web site on which the puzzles are posted more than a live network battle ground. This makes it somewhat easier to host puzzle CTFs and allows far more teams to participate in a live puzzle-style event. In many cases 500 or more teams may be competing simultaneously to see who can win the event. A puzzle-style event is used as a qualifying event for the Defcon CTF, allowing hundreds of teams the opportunity to compete for a chance to compete in the live Defcon event.

Because they lack a head-to-head component, puzzle-style events often offer a wider variety of challenges across a larger number of security-related skills than full-spectrum events. Categories present in puzzle-style events often include reverse engineering, cryptography, forensics, packet analysis, web security, network reconnaissance, and many others.

Between these two types of events, CTF has become so popular that it is possible to find a CTF of one type or the other taking place almost every week of the year. In fact an entire online community has emerged and is tracked by sites such as ctftime.org [3] , which offers both a comprehensive calendar of events as well as results tracking and team ranking. The ranking system in particular highlights both the popularity of CTF and the increasingly competitive nature of the events.

BEYOND THE COMPETITIONS

While CTF events themselves are great fun for all participants, there is much more to CTF than just solving challenges. CTF offers a small window into the computer security field and the games and the excitement surrounding the games are both a great way to introduce new people to the computer security field, identifying talented individuals within specific security disciplines, and a way for established security professionals to showcase their skills.

One of the great opportunities available through CTF is to be able to introduce computer security to young students as a non-traditional introduction to the computer science field. When appropriately packaged, a CTF for young students can both demonstrate the dynamic nature of the computer security field and gently introduce young people to the security problems they are faced with through their everyday interaction with technology. In particular, the media often speaks of the dangers that are present when using social media. Younger users often see social media

as a convenience, a necessity, and an expectation without understanding the risk they may be exposing themselves to through reckless use of such technologies. A well designed CTF can go a long way towards raising awareness and increasing interest in computer security at ages where traditional computer programming may be too difficult to introduce.

As CTF evolves, or more specifically as organizers consider how they might evolve their games, one of the most important ways that CTF can become even more useful is to package CTF as a complete training opportunity in which the organizers provide training in CTF-specific skills, which mirror the skills of everyday security practitioners, leading up to an actual CTF event. Since the organizers typically have complete visibility into their CTF infrastructure, they are uniquely situated to utilize the data they collect, to include packet capture and event timelines, in order to conduct after-event training with participants in which feedback on procedures may be provided along with addressing any shortcomings noted during the event. Used in such a manner, CTF can be a valuable tool both in the workplace as a training opportunity and for the general public as a recruiting tool.

CONCLUSIONS

Japan like many nations faces a critical shortfall in the workplace for skilled computer professionals. Many studies show that it is increasingly difficult to reach younger students and motivate them to pursue education and jobs in the computer field and more specifically in the computer security field. CTF is used in many organizations as a motivational tool as well as a great source of pride when an organization's teams perform particularly well in large competitions. In the United States, companies boast of successful participation in CTF and individuals proudly list CTF on their resumes when applying for jobs in the security field.

As a means of introducing anyone to the computer security field CTF provides a highly interactive way to generate both involvement and interest. While CTF alone is certainly not going to solve the personnel shortage faced by many companies and nations, in a field that lacks innovative ideas for stimulating interest, CTF certainly looks like a good place to start.

REFERENCES

(1) Defcon Computer Security Conference, http://www.defcon.org.
(2) University of California, Santa Barbara iCTF, http://ictf.cs.ucsb.edu/
(3) CTF Time, https://ctftime.org/

ABOUT THE AUTHOR

Christopher Eagle

Christopher Eagle (Chris Eagle) is a Senior Lecturer of Computer Science at the Naval Postgraduate School (NPS) in Monterey, CA. A computer engineer/scientist for 28+ years, his research interests include computer network operations, forensics and reverse engineering. He has been a speaker at conferences such as Black Hat, Defcon, Infiltrate, and Shmoocon and is the author of "The IDA Pro Book", the definitive guide to IDA Pro. He is a multiple winner of the Defcon Capture the Flag Competition and was the organizer of that competition from 2009-2012. He is currently working with DARPA to build their Cyber Grand Challenge competition.

セキュリティスキル競技としての Capture The Flag イベント

はじめに

子どもの頃，野原に集まって旗取り合戦（Capture The Flag，以下「CTF」）で遊んだことはないだろうか。敵と味方に分かれて，味方の陣地の旗を守りつつ敵陣の旗を奪い，味方の陣地に持ち帰れば勝ちである。このCTFがコンピュータセキュリティ専門家たちの注目を集めており，すでに一種のサブカルチャーを形成している。世界最大のセキュリティコンテスト「Defcon」[1]においても，1996年のDefcon 4からCTFが連続で開催されており，著名なセキュリティ競技の中で最長の部類に入る。

2つの競技形式

コンピュータセキュリティ専門家のコミュニティで行われるCTFには，大きく分けて2つの種類がある。とはいえ，競技者がコンピュータセキュリティ分野に関するスキルをすべて駆使し，主催者によって設定された「旗」を奪って，問題解決や目標達成のスキルを示す点は同じである。

恐らく，最も著名なCTFは，「Defconスタイル」と呼ばれているものだろう。Defcon CTFは「CTFの総合競技」である。選抜された複数のチームが，リアルタイムで総当たり戦を行う。Defcon CTFは，毎年の夏にネバダ州ラスベガスで3日間のライブイベントとして開催されている。規模は年々拡大しており，参加チーム枠は1996年の8チームから現在の20チームにまで増えている。「総合CTF」では，主催者が用意する同一のサーバイメージが参加チームに提供される。このサーバは，主催者が開発したカスタムソフトウェアを事前に構成したうえで，Defcon CTF専用のゲームネットワークに接続されている。参加チームは，みずからのサーバを管理・防御しつつ，相手チームの守備を打ち破って「旗」を奪う。旗を主催者に提出すると，相応のポイントを獲得することができる。

Defconの総合CTFでは，意図的にルールを緩くしてある。これは，各チームの発想に制限をかけず，新たな防御法を編み出せるようにするためである。ただし，脆（ぜい）弱なカスタムソフトウェアを守る手段として，ソフトウェアのサービス（機能）自体を停止してしまうことは望ましくない。そこで，ソフトウェアのサービスの公開を継続できる能力に対して点数が与えられる。主催者は定期的にアクセステストを実行して，各チームのソフトウェアが主催者および相手チームからアクセス可能であることを確認している。提供されたソフトウェアの脆弱性を見つけた場合でも，単にソフトウェアを停止するのではなく，不具合を修正することが求められるのである。

ソフトウェアに不具合を発見し，どのような攻撃に対して脆弱であるかを知れば，それは相手チームの弱点を知ることと同じである。すなわち，発見した不具合を逆手にとって，相手チームのサーバへの侵入に成功すれば，相手の「旗」を奪うことができる。旗は主催者によって各チームのサーバに設置され，ゲームの進行に応じて，定期的に新しい旗と置き換えられる。旗が置き換えられるたびに相手のサーバにアクセスする必要が生じるため，ゲームが続いている間は，防御と攻撃を強化し続けなければならない。

Defcon CTFは有名な競技となり，毎年ラスベガスで開催されるCTFへの参加権を得るには，準備に数か月をかけて，数百チームの中から勝ち上がる必要がある。また，国際的なイベントへの変貌も果たしつつあり，当初は米国内からの参加のみであったが，2006年に韓国からのチームが初参加した。2013年には，日本，韓国，中国，ロシア，欧州混成などの海外チームが3分の2を占めた。

第1回Defcon CTF以来，総合CTFはさまざまなタイプが開発されており，それらのほとんどは，主に教育機関に公開されている。中でも，カリフォルニア大学サンタバーバラ校のiCTF（International CTF）は最大規模のCTF大会に成長し，2013年には世界中から90チームが8時間のライブイベントに参加した。

Defcon CTFと並ぶもう1つのCTFは，パズルを解いてポイントを獲得するパズルCTFである。セキュリティ関連の課題が主催者によって複数提示され，参加チームには

これらを解くことが求められる。対戦型ではない個別競技として，各チームはいち早くパズルを解き，より多くのポイントを獲得することを競う。

パズルCTFの主催者は，パズル問題をWebサイトに掲載するのと同じ要領でインフラを整えればよい。ネットワーク対戦ゲームのライブイベントよりも簡単に準備できるため，より多くのチームが参加できる。ほぼ毎回，パズルCTFのライブイベントでは500以上のチームが勝敗を競い合う。パズルCTFはDefcon CTFの予選として開催され，ラスベガス本会場でのDefcon CTFライブイベントへの出場権を獲得する機会となっている。

対戦要素のないパズルCTFイベントの課題には，Defcon CTFよりも多くのセキュリティ関連スキルを盛り込むことができる。例えば，リバースエンジニアリング，暗号化，フォレンジック，パケット分析，Webセキュリティ，ネットワーク偵察といった，多様なカテゴリーの問題が提示される。

Defcon CTFもパズルCTFも非常に人気が高く，毎週のように各地でイベントが開催されており，ctftime.org[3]のように，CTFのイベントカレンダーとチームのランキングが確認できるオンラインコミュニティもある。こうしたランキングの存在は，CTFの人気の高まりと，イベントが徐々に真剣味を帯びてきていることの証明でもある。

単なる競技イベントではなく

課題の解決を競うCTFは，それ自体が参加者にとって非常に楽しいイベントである。しかし，CTFの利用価値はそれだけにとどまらない。CTFのゲーム性と競技の楽しさをきっかけに，コンピュータセキュリティ分野に新しい人材が関心を持つようになる。すなわち，CTFは，特定のセキュリティ分野の才能がある個人を発見する場としても，セキュリティのプロがスキルを証明できる場としても有用なのである。

例えば，CTFイベントを活用すれば，若い世代にコンピュータセキュリティの重要さを新鮮な方法で伝えることができる。若い学生を対象にCTFを適切に設定すれば，コンピュータセキュリティ技術の移り変わりの速さを実際に感じつつ，日常生活において情報技術を利用する際に，どのようなセキュリティ問題に気をつけるべきかを学ぶことができる。特に，ソーシャルメディアの危険性についてはマスコミでもよく取り上げられている。多くの若者が，便利であるとか，必要であるとか，周囲が使っているとかいった理由でソーシャルメディアを利用しているが，このようなテクノロジーを不用意に使うことでどのようなリスクがあるか，よく理解していないことが多い。コンピュータプログラミングを学ぶには早すぎる世代でも，適切に設定されたCTFイベントを通じて，コンピュータセキュリティへの意識と関心を高めることができる。

今後もCTFが発展し，主催者がゲームの内容を吟味して厳選すれば，トレーニングとしても大きな役割を果たすようになるだろう。日常のコンピュータセキュリティに関するスキルを反映したトレーニングを，実際のCTFイベントに向けたトレーニングとして開催するのである。主催者はCTFのインフラを管理しているため，パケットキャプチャやイベントのタイムラインなどのデータを収集して，イベント後にトレーニングを開催し，フィードバックを提供して，競技中に気づいた弱点を補強することができる。このように用いれば，職場でのトレーニングや人材発掘の機会としても大いに有益である。

おわりに

世界的な傾向として，熟練技能を持つコンピュータの専門家が業務の現場で絶対的に不足しており，日本も例外ではない。大学でも職場でも，コンピュータ分野，特にコンピュータセキュリティ分野への若い世代の関心が低いと言われている中，多くの企業が，CTFを活用して，若い世代の関心をつかもうとしている。大規模なイベントで自社チームが勝てば，企業の知名度向上にもつながる。米国の企業は，CTFへの参加を宣伝材料として利用している。また，セキュリティ分野への就職を希望する者が，CTF参加経験を自己PRとして履歴書に記入することもある。

積極的に競技に参加し，実際にやり取りすることで，関心を高めることができるCTFは，コンピュータセキュリティ分野を紹介する手段として非常に有効である。多くの企業や国家が抱える人材不足をCTFだけで解消することは不可能だが，関心を高めるための新しい方法としては，非常に良いスタート地点である。

参考文献など

1) Defconコンピュータセキュリティ会議，http://www.defcon.org
2) カリフォルニア大学サンタバーバラ校iCTF，http://ictf.cs.ucsb.edu/
3) CTF Time，https://ctftime.org/

執筆者紹介

クリストファー イーグル

カリフォルニア州モントレーの米国海軍大学院にて上級講師として活躍中。コンピュータエンジニア／研究者として28年以上のキャリアを持ち，研究内容はコンピュータネットワーク運用，フォレンジックとリバースエンジニアリングに関連する。Black Hat，Defcon，InfiltrateやShmooconなどのカンファレンスにて講演し，また，IDA Proに関するハンドブックの決定版と呼ばれる「The IDA Pro Book」の著者でもある。DefconのCTF競技では，チームリーダーとして生徒らのチームを複数回優勝に導いており，2009年から2012年までは，同CTF競技の開催運用側で活躍した。