［セキュリティ人材育成の現状と実践］

⑤ 実践形式によるセキュリティ人材育成の取組み

応般

園田道夫 | 国立研究開発法人情報通信研究機構（NICT）

サイバーセキュリティ分野において，即戦力としての人材を求める声は年々高まっている．それには実践的な経験が必須だが，性質上真の実践が難しいのがこの分野である．そうした前提を踏まえてどのような試みがなされてきたか，本稿では筆者が主としてかかわったイベント等を中心に実践的な人材育成の取組みを紹介する．

セキュリティ・キャンプ事業

2004 年より開催しているセキュリティ・キャンプは経済産業省から（財）日本情報処理開発協会（現：（一社）日本情報経済社会推進協会（JIPDEC））を経て（独）情報処理推進機構（IPA）☆1 および（一社）セキュリティ・キャンプ協議会（旧：セキュリティ・キャンプ実施協議会）☆2 に主催が変わりながらも 2019 年現在 16 年目を迎える学生対象のイベントである☆3．その中心は全国大会☆4 という 8 月開催の 4 泊 5 日の合宿研修であり，そのほかに全国大会と同時期に開催するネクストキャンプ（旧：コアキャンプ）☆5，またセキュリティ・ミニキャンプ☆6 という地方開催のイベントや，中学生以下向けのセキュリティ・ジュニアキャンプ☆7，そこから発展した全国大会内のジュニア開発ゼミ，あるいは韓国，台湾，シンガポールと連携して開催する Global Cybersecurity Camp（GCC）☆8，セミナー＋修了生の優秀研究発表や活動の表彰を行うセキュリティ・キャンプフォーラム☆9 など，事業範囲を年々拡大している（表 -1）．全国大会の規模は 80 名程度．現在は募集が分かれているので単純に計算できないが，例年募集定員に対して 6 倍から 8 倍の参加申し込みがある．

なお，この事業が学生を対象としているのは，税金を使う事業として営利企業に所属する人材の育成を行うのはどうか，という考えがあったからである．また，当初はより若い人を発掘したいとのことから 20 歳以下を対象としたが，当時の日本の大学教育におけるセキュリティ事情から目覚める時期が学部 3 年以降であることが多い様子だったので，数年後

表 -1　セキュリティ・キャンプ事業のイベント

イベント名	内容
セキュリティ・キャンプ全国大会	22 歳以下学生対象．4 泊 5 日の合宿形式
セキュリティ・ミニキャンプ	25 歳以下学生対象（イベントによる）．1 泊 2 日の合宿形式，または 1 日のみの開催
セキュリティ・ジュニアキャンプ	中学生以下対象．1 泊 2 日の合宿形式
ジュニア開発ゼミ	全国大会内の中学生以下対象ゼミ
セキュリティ・ネクストキャンプ	セキュリティ・キャンプ修了生が対象．全国大会と併催
Global Cybersecurity Camp	韓国，台湾，シンガポール等アジア各国と共催．移動日含む 6 泊 7 日の合宿形式
セキュリティ・キャンプフォーラム	セキュリティ・キャンプ修了生の活動報告や LT，ゲストによる特別講演があるセミナー形式のイベント

☆1 https://www.ipa.go.jp/jinzai/camp/index.html
☆2 https://www.security-camp.or.jp/
☆3 https://www.ipa.go.jp/jinzai/camp/index.html
☆4 https://www.security-camp.or.jp/camp/index.html
☆5 https://www.ipa.go.jp/jinzai/camp/2019/next2019_index.html
☆6 https://www.security-camp.or.jp/minicamp/index.html
☆7 https://www.security-camp.or.jp/minicamp/kochi2018.html
☆8 https://www.security-camp.or.jp/event/gcc2018.html
☆9 https://www.ipa.go.jp/jinzai/camp/2018/forum2019.html

には22歳以下とした．さらにミニキャンプでは大学院生も含む25歳以下とすることが多い．

セキュリティ・キャンプの特徴はまさに実践である．当初より「手を動かすこと」をコンセプトに，座学オンリーの講義は可能な限り避けて構成してきた．一番長い全国大会でも4泊5日しかないイベントなので，理論にじっくり時間を割くのは難しい．それならいっそサイバーセキュリティに興味をひくことを最大化すべく，学生にとって面白いテーマで可能な限り手を動かすコンテンツにする．そこにフォーカスした．

もう1つコンテンツを構成する際に意識しているのは，学校ではやらない，できない講座をやろう，ということである．学校は体系的に整理された基礎をたたき込む場だが，逆にいえば旬なテーマを追いかけづらい．キャンプでは変化の早いサイバーセキュリティの分野でその「追いかけづらい」部分を少しでも補完したいと考えている．

現在の全国大会は，初日に倫理や法律，基礎的なセキュリティの講義，最終日に成果発表会などがあり，その間の3日間は，多数の講義を受講可能な「選択コース」と，小規模なゼミに分かれて3日間開発し続ける「集中開発コース」がある[☆10]．当初はサーバの要塞化から攻撃検知などのネットワークセキュリティ的なテーマが中心だったが，近年は幅広くマルウェア解析からハードウェア，Webサービス，コンパイラやOS開発，制御システムとの連携やAIなどの領域もカバーしている[☆11]．数年前より修了生を対象としたネクストキャンプも併催していて，コンテンツ面ではさらに深掘りしたもの，たとえばGPSをハックする講座とか，AI系技術を使ってWeb Application Firewallを作る講座なども用意している．

全体的にもの作りに寄っている理由は，日本オリジナルなサイバーセキュリティ製品を生み出せていないという現在の日本の課題を反映したためである．もの作りとサイバーセキュリティ領域の間にある溝を埋め，セキュリティを専門とする技術者以外にもセキュリティの考え方を拡げていく必要があると考えているが，この方針は全国大会におけるゼミ制による3日間ハッカソンの導入と，それを発展させた集中開発コースの増設から1年かけて何かを作り出すことを目的とするSecHack365（後述）にも繋がっている．

インフラ面も特徴的で，ウィルスなどを扱うことまで想定し，伝統的に分離型のネットワーク構造をとり，リスク管理を徹底している．現在はその構築管理も修了生チームに任せている．

また，セキュリティ・キャンプに限らず，セキュリティを扱うイベントでは特に，法的な側面をフォローすることが重要である．犯罪的行為などの明らかな悪いことはもちろんのこと，たとえば，脆弱性の指摘など「良いこと」と思われるものであってもリスクを伴う，ということを学ぶ機会を作るべきと考えている．そのため，前述したが倫理面や法的な面のフォローのために，毎年警察や弁護士などに講演してもらっている．

近年では，修了生のフォローアップ強化の一環で，ミニキャンプに積極的に若手を登壇させている．さらにはその企画や運営も修了生＋αのチームで行っている．これまで修了以降の活躍の機会はチューターとして全国大会等に参加するか，講師になるか，あるいは別ルートでのフォーラムにおける表彰のみだったが，新たな試みで事業が拡大していく中，これまでのようにメインキャストが負う責任や負担が増えていくのをただ見ているだけではスケールしない，という課題に応え，コミュニティの中で活動的な人材の数を増やすことも兼ねている．持続的なコミュニティとするためには，常に新しい人材を発掘し，取り入れることができる仕掛けが必要だと考えている．

元々セキュリティ・キャンプは経済産業省から直

☆10 https://www.ipa.go.jp/jinzai/camp/2019/zenkoku2019_program_timetable.html

☆11 https://www.ipa.go.jp/jinzai/camp/2019/zenkoku2019_program_list.html

接，あるいは情報処理推進機構を経た予算のみで企画運営されていたが，2012年にセキュリティ・キャンプ実施協議会を設立し，一般企業のスポンサーを募り始めた．公的な資金と民間の資金を併用することは，手間はかかるがメリットも多く，特に企画の自由度を高めるのに役立っている．2018年より旧実施協議会も一般社団法人化し，スポンサー獲得活動をより一層強化している．

情報危機管理コンテスト

サイバー犯罪に関する白浜シンポジウム内のイベントとして開催される情報危機管理コンテスト（旧称：危機管理コンテスト）は2019年で14回を数える[☆12]．学生が対象で，2019年は22の学校から33チームが参加し，2次にわたる予選を経て決勝は5チームで争われた．

コンテストの形式はシナリオ型で，各チームにはサービスの維持運営が求められる．次々と起こるトラブルの原因を究明しつつ，封じ込めや設定変更などを関連組織と調整を図りながら実施する．技術力だけでなくコミュニケーションの力やきちんとした段取りを踏まえた調整力などが求められる．競技の最後にはトラブルチケットという報告書をまとめて提出するが，その内容や質は年々向上している．常連チームはうまくノウハウを継承している様子で，単に勝利を目指して選抜チームで臨むのではなく戦略的に先輩後輩で組ませて複数チームで挑む学校もある．

企画運営側のメインキャストが学生であるのも特徴で，「劇団」と呼ばれる彼らは調整先組織の役で電話対応したり，進捗チェックを行ったり，各チームの技術サポートを行ったりという働きぶりで毎年称賛されている．ベースとなるシナリオは当然ながら現実に起こり得る可能性をすべて網羅できるわけではないので，相応のアドリブ力が求められる．ほぼ1年かけてさまざまな準備を行う過程の中で，彼らは鍛えられるのである．

筆者は初回から審査委員として参加しているが，毎年感心させられるのはその劇団の優秀さとシナリオのリアリティである．たとえば今年は「あるユーザのWebページがどうやってもリダイレクトされてしまう」とか，「とあるWebサイトが表示できなくなってしまう」とか，「データがごそっと抜かれて掲示板に貼られてしまった」とかの災難が各チームに降りかかった．どれも一見すると事象を抑え込んだり，回復・改善させるのは簡単そうに見えるが，無体な経営者が「なんかヤバそうだったのでこの箱物買ったのでそれ使って」と言い出したりする．参加者は組織の立場上それを拒否できず，その上での対応を適切にこなす必要がある．南紀白浜で行われる決勝ではこうしたシナリオが3本，4本と用意されていて，これを5時間でこなすというハードさだ．事象特定から原因の追及・分析と封じ込めを行い，その傍ら関係組織や関係者（ユーザ，オーナー等）と密に連絡をとり，打診に先行して処置を施したりすることのないように対処する，というのがこのコンテストの目指すところである．そのためのリアリティは徹底して追求されており，企業向け研修や大学連携教育プログラムenPiT Security（SecCap）などにそのまま転用されるほど高い評価を得ている．

Hardening Project

WASForum Hardening Project実行委員会が主催するHardening Project[☆13]のコンセプトはオープン版「情報危機管理コンテスト」と言ってもよいだろう．中身はより実際的である．実際に売られているプロダクトやサービスを，ベンダサポート付きで導入できたり，本物のマルウェアを競技に使用することも

☆12 http://www.riis.or.jp/symposium23/crisismanagement/purpose/

☆13 https://wasforum.jp/hardening-project/

ある．競技は情報通信研究機構（NICT）の仮想インターネット環境 StarBED 上で行われるため，それでも危険はない．セキュリティの演習やトレーニングに実際の環境を使うのは，内容がリアルであればあるほど本当の攻撃に近くなるためとても難しい．攻防戦などが行われるセキュリティ競技 CTF（Capture The Flag）のように閉じた環境で行えれば安全だが，一般企業がそのような環境（サイダーレンジ）を用意することは，開発工数や要件などを考えるなら自力では難しい．となると限られた環境下でリアリティを犠牲にして部分練習をすることになるが，いつかはスキルアップが頭打ちになってしまう．

現実に限りなく近い環境下で，導入が難しいサービスやプロダクトを使ったシミュレーションができるコンテスト．ここが Hardening の強みである．チームは混成で知らない者同士が組むことも珍しくないが，実際の競技とその後の分析や反省を共有することで良いチームワークが醸成される．そこもまた強みだ．チームワークがコミュニティに繋がり，コンテストのいわば復習である MINI Hardening という活動にも繋がっている．

また，情報危機管理コンテストの場合は 1 日という時間的制約があるためトラブルチケット（報告書）をまとめるところまでだが，Hardening の場合は毎回振り返りの Softening Day が開催され，各チームの戦略や対応，分析を共有できる．CTF でも Writeup としてプレイヤ自身が解法をブログ等にアップして広く情報を共有する文化があるが，それをさらに鮮度高く深めたものだといえる．こうした企画面での工夫が数多くのリピータを呼び，コンテスト全体を活性化させているといえるだろう．

SECCON

SECCON[☆14] は 2012 年から開催されている日本最大級（世界最大級でもある）の CTF である．CTF の歴史は古く，最初の公開競技 DEF CON CTF[☆15] は 90 年代前半に開催されている．今や世界中で開催され，ポータルサイト CTFtime.org[☆16] に掲載されている国際大会の数は年間 150 以上である．これだけ流行る理由は簡単で，良いエンジニアのリクルーティングと実践的経験値の積み上げに繋がるからである．

前述したが，サイバーセキュリティにおいて効果的な演習を行うことはとても難しい．

OJT（On the Job Training）のように実地の環境を使った演習は，大きなリスクを伴う．とはいえ実際にシステムを攻撃したり，攻撃されるのをリアルタイムで防御したりする経験を積めなければ，犯罪者には対抗し得ないだろう．そうした危機感から CTF という競技が生み出された．

最初の CTF は，OS がインストールされたコンピュータを渡されて，さぁハックしてみよう！というものだった．その後 OS の品質も上がり，数日の間で容易に脆弱性を発見できるようなものではなくなったこともあり，競技形式は変化してジョパディと呼ばれるクイズ形式，仮想マシンを渡される攻防戦形式，そして仮想マシンイメージ（VM）を主催者が管理する形となる King of the Hill という形式で行われている．運営の難易度は形式によって相当異なり，最も難しいのは攻防戦である．国際大会の大半は運営しやすいジョパディ形式で行われている．

SECCON は例年オンライン予選（ジョパディ形式）と東京で開催する決勝大会（King of the Hill 形式）の二段構えで行われる．ジョパディは参加もしやすいので集客力が見込めるし，King of the Hill 形式は攻防戦に比べてスコアリングがクリアなので運営しやすい．しかし世界では攻防戦形式をベストと見る傾向も強いので今後どう取り組むかが課題である．数年前には国内の学生限定で，攻防戦形式で

☆14 https://www.seccon.jp/

☆15 https://www.defcon.org/html/links/dc-ctf.html

☆16 https://ctftime.org/

開催したこともあるが，国際大会での実践にはもう少し準備や経験値が必要だと考えている．

SECCON の場合，King of the Hill 形式を選ぶ理由には可視化も絡む．SECCON の競技可視化は Hardening でも協力している NICT のサイバーセキュリティ研究室が開発している，NIRVANA 改（SECCON カスタム．最新は Mk-V）というシステムを使っている（図 -1）．

筆者を含む主催者は NIRVANA 改 SECCON カスタムのビジュアルは世界最高峰のクオリティであると自負している．このシステムでは攻撃のインパクトを表現しているが，そのための情報収集は VM にソフトウェアを入れて行っているため，VM を運営側が握っていないとさまざまな偽装工作や攻撃の可能性がある．これは攻防戦形式のスコアリングシステムの抱えるリスクと同じであり，可視化システムの性質上異なるプロセス（プログラム）を使わざるを得ないためリスクは 2 倍になってしまう．

とはいえ各種イベントで経験値は積んできているので，形式の検討は改めて行うことになるだろう．

近年，ゲームの仕組みを利用してたとえば社内教育の効果を上げる手法についてゲーミフィケーションという言葉が使われるようになってきたが，CTF はゲームそのものであり，実際開催してみると参加した人の技術的モチベーションを大いに刺激する効果が実感できる．CTF には解法をブログ等で共有する文化があるが，感想を読むと SECCON に限らず CTF 全般で「やる気になった」とか「技術的な立ち位置が認識できた」というフレーズが多い．そういう効果に目を付けて企業が CTF を技術者向けの社内教育に使うケースも増えていて，最近は警察等も CTF を開催し始めており，SECCON 開始当初からは隔世の感がある．

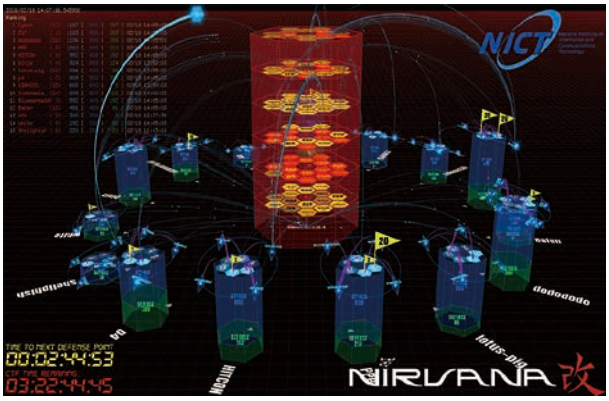

図 -1　NIRVANA 改 SECCON カスタム Mk-V

CTF の場合も単純にプレイするだけでなく実際に作問したり運営したりすると力がつく．その一環として，実行委員になってもらうだけでなく，ワークショップや独自 CTF の開催という活動もサポートしている．

その 1 つ，初心者向けワークショップ，SECCON Beginners は年数回の頻度で開催している．セキュリティ的な総合力を必要とする攻防戦や King of the Hill に比べると，技術的な部分練習であるクイズ形式のジョパディは取っ付きやすいが，それでも初心者にはハードルが高いことは否めない．その最初のハードルを超えさせるためには考え方や必要な技術・知識について学ぶワークショップが重要だと考え，主には学生（現在は多くが卒業し，社会人も増えてきたが）の CTF プレイヤに声を掛けてワークショップの企画運営，コンテンツ作成を行ってもらっている．全国でどこか引き合いがあると開催する，という形をとっているがオファーは多く，すべてに応えられないほどの人気をいただいていて，大人が別途ワークショップを開催するほどである．また，中級者向けのワークショップ SECCON Beginners NEXT や SECCON Beginners の CTF も開催している．

また，SECCON 実行委員の中の女性委員の発案で女性限定ワークショップ，CTF for GIRLS[☆17] も開催している．これは，IT 業界やサイバーセキュリティの業界に圧倒的に少ない女性のエンジニアの，気軽に情報交換などを行いたいという要望を踏まえた企画であり，2019 年 6 月現在 11 回を数えている．講師役も運営スタッフもすべて女性である．

☆17　http://girls.seccon.jp/

SECCON Beginners は週末の半日を使ってさまざまな分野の講義演習とミニ CTF というパッケージで開催しているが，CTF for GIRLS は主に平日夜で，ワンテーマのワークショップという形をとっている．こちらも好評で，毎回多数の参加者がある．こちらも発展して最近は CTF for School GIRLS という学生向けワークショップを開催したり，攻殻機動隊 REALIZE PROJECT とコラボレーションして SECCON CTF for GIRLS（略称：攻殻 CTF）を開催したりしている．攻殻 CTF の 3 回目は世界大会として国際的カンファレンス CODE BLUE とコラボレーションして開催し，注目を浴びた[☆18]．

また最近，CTF for GIRLS の発起人である NTT セキュアプラットフォーム研究所の中島明日香氏が CTF 問題解説の雑誌連載を始めるなど，各方面で意欲的な活動を行っている．

AVTOKYO

最後に少し毛色の違うイベントを紹介しよう．セキュリティのカンファレンスである AVTOKYO[☆19] は 2007 年に初回が開催され，2018 年で 12 回を数える．2019 年も 11 月 2 日に開催予定で，企画等準備中である．

このイベントのモットーは「no drink, no hack.」である．以前開催されていた Black Hat Japan の後の飲み会で，せっかく海外からハッカーやエンジニアが来てくれているので Lightning Talk（LT）とかやるか，というのが発端となり，イベント化していった．drink することで心の壁も薄くなり，技術で語る LT で交流する，というのがイベントの狙いである（そのため，会場と調整して現在は飲み放題としている）．

メインは講演で，講演者は Call For Paper（CFP）を吟味して決めている．若干であるが渡航費を補助しているので海外からの応募も増えている．CFP ではなく独自企画で講演者を呼ぶこともあり，2017 年はオープンソースのソフトウェア解析ツール radare2（r2）のメイン開発者 pancake 氏を，2018 年はフォレンジック解析の最新 Linux ディストリビューションである TSURUGI Linux のメイン開発者 Giovanni Rattaro 氏をそれぞれ招聘した．両氏ともに，翌日別会場でワークショップも開催していただいた．

また近年，Call for X としてイベント内イベントの企画も募集している．2018 年には，SECCON スタッフによるクイズ大会 SEQCON，UEFI Reverse Engineering，Open xINT CTF などが開催された．毎年好評をいただき，近年のセキュリティ熱も手伝ってチケットも早めに売り切れるのが現状である．要望に応じて会場をさらに大規模にすることも毎年検討はしているが，会場の確保が難しいのが課題である．

技術的テーマにフォーカスしたカンファレンスは日本国内では少ないが，「no drink, no hack.」というカジュアルなモットーでありつつも技術の尖ったテーマの講演を供給する，この役目は続けていきたいと考えている．

(2019 年 7 月 2 日受付)

園田道夫（正会員） sonodam@nict.go.jp
（独）情報処理推進機構専門委員，国立研究開発法人情報通信研究機構ナショナルサイバートレーニングセンター長，SECCON 実行委員（事務局長）．

☆18 https://2017.seccon.jp/news/-realize-project-seccon-ctf-for-girls-in-code-blue.html
☆19 http://ja.avtokyo.org/