

若い突出したセキュリティ人材育成に向けて

— IPA セキュリティ・キャンプと今後の取り組み —

神島万喜也

(独) 情報処理推進機構 (IPA) IT 人材育成本部産学連携推進センター

セキュリティ・キャンプとは

□ 背景

インターネットの急激な拡大・普及に伴って、世界中のコンピュータが1つのネットワークに繋がるようになり、私たちの暮らしの隅々までとけこんでいる。インターネットを利用することにより、利便性が高まる一方で、国、企業、個人の情報と、それらの情報を扱うコンピュータが、悪意ある人やプログラムによる脅威にさらされており、そこにセキュリティリスクが発生している。

2000年代初頭、職場、家庭等へのパーソナルコンピュータの導入が急速に進み、各企業・家庭においてもウィルス対策ソフトウェアを導入するなどさまざまな対策を施しつつあった状況下、コンピュータやネットワークに関する深い知識や高い技術を持つ人材（いわゆる悪意のある活動をする「ブラックハッカー」）に対し、善意で活動する「ホワイトハッカー」が必要であるという機運が高まった。高まるセキュリティリスクに立ち向かい日本の安心・安全なIT社会に貢献する若い優れた逸材を輩出することの必要性がにわかにクローズアップされた。

□ 目的と概要

若年層のセキュリティ意識の向上と優秀なセキュリティ人材の早期発掘と育成を目的として、「セキュリティ・キャンプ」（以下「キャンプ」という）を2004年度から経済産業省主催で開始した。また

2008年度からIPAの主催となり、「セキュリティ&プログラミングキャンプ」として実施してきた。

このキャンプは、22歳以下の就業前の学生・生徒を対象に、第一線で活躍している技術者を講師として合宿形式で行う研修である。

2004年度から2011年度まで8回開催したキャンプには、延べ1,700名弱の応募者があり、約360名（応募倍率約4.7倍）が受講している。

参加希望者が応募要領に記載した設問回答内容を講師が査読し、参加に値する技術力・それまでの活動実績等を加味して選定にあたる講師の合議制で参加者候補を選考し、有識者で構成される「実行委員会」にて議論し参加者が決定される。

キャンプ終了後も、主催者による「セキュリティキャラバン」や企業・学校関係者・卒業生等が参画する「キャンプ報告会」等を開催している。また講師・卒業生有志による各種イベントも随所で開催されており、講師・卒業生のみならず将来キャンプに参加を希望する学生・生徒も参加しキャンプを通じたネットワークが形成されつつある。

キャンプ卒業生の中には米国ハッカー競技会の1つで優勝した者、日本のソフト技術者によるAndroidセキュリティコミュニティを立ち上げた高校生、OSの改ざんを防止する手法の論文が難関といわれているコンピュータ関連国際学会で採択された者等、際立った活躍をしている若者もでてきている。キャンプ卒業後、セキュリティ関連企業、ITベンダ企業、Eコマース企業、ゲーム関連企業等に

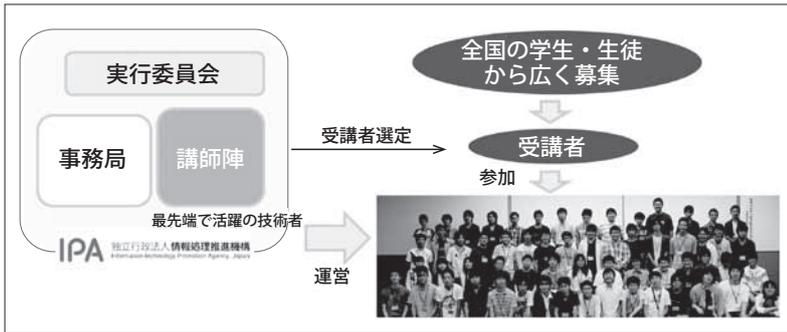


図-1 セキュリティ&プログラミングキャンプ 2011 実施形態

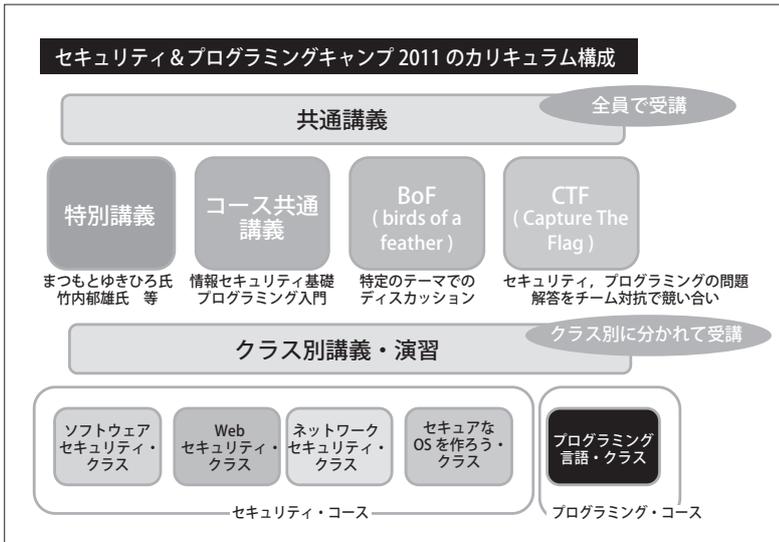


図-2 セキュリティ&プログラミングキャンプ 2011 カリキュラム構成

学校種別	受講者数	年齢	
大学	30名	最少年齢	13歳
高等専門学校	12名	最高年齢	22歳
専門学校	3名	平均年齢	18.2歳
高等学校	10名		
中学校	5名		
合計	60名		

表-1 受講者の学校別と年齢集計

たい。

実施形態とカリキュラム構成を図-1および図-2に示す。また受講者の学校別集計と最少・最高・平均年齢を表-1に示す。

キャンプ参加者からのアンケートによると「将来の目標を見つけた」「モチベーションが高まった」「意識が変わった」という回答が大半で、また講師等に対しても「前々から憧れていた講師・チュータたち、凄まじい技術を持つ参加者たちと出会って、自分もこうありたい！と強く意識した」との声があった。

就職し、各企業で活躍している者もでてくる。

また、IPAで実施している優れたアイデア・技術を持った若い突出した人材を発掘・育成する「未踏IT人材発掘・育成事業」にこのキャンプ受講後挑戦する若者も増加し、2011年度公募において、4名のキャンプ受講者を採択した。

2011年度の取り組み

□ 全体概要

2011年度のキャンプを2011年8月10日～14日（4泊5日）に「セキュリティ&プログラミングキャンプ2011」として「ホテルコスモスクエア国際交流センター」（大阪市住之江区）で実施した。

受講者60名、講師24名、チュータ16名、事務局等関係者17名（特別講師含む）の計117名が参加した。詳細は以下IPAのWebページ^{☆1}を参照され

☆1 <http://www.ipa.go.jp/jinzai/renkei/spcamp2011/index.html>

□ 講義カリキュラム構成

キャンプ受講者全員が受講する共通講義と受講者がクラス別に分かれて受講するセキュリティコース、プログラミングコースに区分されたクラス別講義・演習のカリキュラム構成でキャンプを実施した。

講義実施にあたり、セキュリティ関連企業、IT企業等の第一線で活躍中の最先端技術を有する技術者を講師として選任した。また講師の補佐役として過去のキャンプ卒業生から選抜したチュータも配置した。講師構成については以下のWebページ^{☆2}を参照されたい。

● 共通講義

キャンプ受講者全員が受講する以下の共通講義を実施した。

① 特別講義

竹内郁雄氏（早稲田大学教授、東京大学名誉教授）、田中慎司氏（(株)はてなCTO）、まつもと

☆2 <http://www.ipa.go.jp/jinzai/renkei/spcamp2011/instructor/index.html>

ゆきひろ氏(Ruby 開発者)等による講演を行った。

② コース共通講義

脆弱性(ぜいじゃくせい)はなぜ作り込まれてしまうのか、ウィルス感染の最新トレンド、ネット詐欺の手口と対策等に関する「情報セキュリティ基礎」および、デバッグの方法論等に関する「プログラミング入門」の共通講義を行った。

③ グループディスカッション

受講者全員をシャッフルしたグループに分け、グループごとにテーマを設定したディスカッションを実施し、最終日に発表した。また講師が特定のテーマを設定し、BoF (Birth of a Feather) と呼ばれるグループディスカッションも行った。キャンプに参加する前に受講者には名刺を準備させ、講師を含む全員が名刺交換を通じての交流の場面も設けた。

④ CTF (Capture The Flag)

セキュリティおよびプログラミングに関する設問を講師により用意し、グループ対抗で知識を競う競技を行い、最終日に優勝したグループ、個人優秀賞等の表彰を行った。

● セキュリティコースのクラス別講義・演習

情報セキュリティを中心としたITについての意識が高く、将来的に優秀なIT人材として期待される若い人材に対して、情報セキュリティを中心としてIT化実現のための技術的な目標と高い技術修得への励み、および安全かつ信頼性の高いIT化の進展について正しい知識を与えることを目的とした以下の4クラスを設け、受講者はそれぞれのクラスに分かれて、講師による講義・演習を受講した。

① ソフトウェア・セキュリティ・クラス

マルウェアを解析してマルウェアの動作、OS等への影響、特徴などを解析結果から抽出し、その目的や性質、過去の傾向などを踏まえて抽出した材料を吟味できるレベルを目指した。ソフトウェアに含まれる脆弱性を通して、ソフトウェア全般のセキュリティについて学ぶとともに、脆弱性を悪用した攻撃の原理、および防御・解析手法の修得や、実際のソフトウェア開発に

おいて脆弱性が作り込まれてしまう原因の考察を、演習を通じて行った。また、新たなソフトウェア動作プラットフォームであるスマートフォンなどについても演習素材とした。

② Web セキュリティ・クラス

現在のWebアプリケーションを構成する要素技術や仕組み、そしてそれらに付随する脆弱性や課題について考察し、新たな対応技術や、対応のための攻撃技術を進化させるレベルを目指した。実在する脆弱性を例にして、演習形式で調査・解析を行い、発見した脆弱性の適切な扱い方を学ぶとともに、Webブラウザごとの「方言」や、HTTPのプロトコル仕様に基づいた攻撃の仕組みについても講義や演習で取り扱った。

③ ネットワーク・セキュリティ・クラス

実際のネットワークにおける攻撃の検知や、適切な防御策を講じられるとともに、今後出現する新しい攻撃やその対応技術について考察・提案できるレベルを目指した。具体的には、現在のコンピュータネットワークにおけるセキュリティや弱点などについて学ぶとともに、広く利用されている防御技術の課題について考察し、ネットワークプロトコルを体感しながらネットワークセキュリティを学習した。この際に、事件対応の実例を素材としたネットワーク攻撃のメカニズム理解や、実際のネットワークにおける攻撃の検知・防御策の策定についても演習のスコープに含めた。

④ セキュアなOSを作ろうクラス

これまでの数多くのOSの概念にとらわれない自由な発想でOSカーネルからの攻撃の検知や、適切な防御策を考え、実装するとともに、今後発見されるであろう未来的な攻撃手法に対しても考慮されたまったく新しいセキュリティモデルをOSに組み込むことができるレベルを目指した。具体的には、OSの設計や実装をセキュリティという観点から学び、実装するとともに、今後発見されるであろう新しい攻撃手法と、それに対する防御技術を考察し、CPUとソフトウェアの

セキュア機能を意識しながらの、新しく堅牢な OS を創造する。セキュリティ技術を「ものづくり」の設計の段階から取り入れることで、今後起こり得る攻撃に対する検知・防御策を提示する演習を行った。

● プログラミングコースのクラス別講義・演習

高度な IT 人材を発掘・育成する場の 1 つとして、高度なソフトウェアを設計・開発できる『可能性』がある若い人材を早期に発掘し、その可能性を現実のものに近づけていくために、オープンソースソフトウェアを題材にプログラミングの楽しさやソフトウェアを開発して広く活用してもらうことの喜びを理解すること、および安全かつ信頼性の高い IT 化の進展について正しい知識を与えることを目的とし、「プログラミング言語クラス」を設けて行った。プログラミング言語 (Ruby などの言語を想定)、およびその言語処理系を題材に、座学と実習によって言語処理系の基本、ソフトウェア構成手法の基本、性能改善手法の基本を学び、開発コミュニティで活躍できるレベルを目指した。具体的には、処理系のコンパイルからビルドの方法、ソースコードの読み方、テスト、デバッグ方法、コミュニティとのかかわり方までを講義と実習を通して学んだ。

□ クラス別講義・実習の様子

● セキュリティコースの様子

セキュリティコースではそれぞれのクラスに分かれ計 45 名が受講した。

基礎となる考え方や専門的なツールの使い方、さらに実習までと濃縮されたカリキュラムが用意され、その合間に、たとえばほかのサイトの脆弱性を見つけてしまったときどのような対応をすればよいか現実的なシナリオとリスクを鑑みながらの議論や、講義によっては講師の中でも見解の分かれる事柄もあえて扱うなど、表面的な知識の習得だけでなく、参加者自身が自分なりに深く考えをめぐらす場面も設けた講義・実習を行った。セキュリティコースのクラス別講義・実習の様子を図-3 に示す。



図-3 クラス別講義・実習の様子

● プログラミングコースの様子

「プログラミング言語クラス」は 15 名が受講し、プログラミング言語処理系、ソフトウェア構成手法、性能改善手法などを学んだ。ソースコードの読み方からデバッグ、ソースコード管理までひと通りのベースとなるノウハウを習得後すぐに実践的な講義に移った。特別講義を受け持ったまつもとゆきひろ氏が引き続き授業を担当するなど、カリキュラムの多くが Ruby 言語に割かれたが、Ruby 言語によるプログラミングを学習するというより、プログラミング言語がどのように作られ、どうすればその性能を改善し機能を拡張できるかを学ぶ題材として Ruby 言語が利用された。

日本から登場した Ruby 言語は、コアメンバとして開発に直接関与している人材を講師としてアサインできる利点もあり、またオープンソース系のソフトウェアの利活用では不可欠な開発コミュニティとのかかわりについても学ぶことができた。

□ CTF の様子

4 日目の午後から夜にかけて CTF (キャプチャー・ザ・フラッグ (Capture The Flag)) という競技が開催された。CTF はセキュリティ知識を競うゲームとして、米国の大規模カンファレンス DEFCON をはじめとして、世界中でさまざまな大会が開かれている。日本ではそれほど盛んではなかったものの、キャンプ直前に開催された DEFCON19 の CTF に日本の sutegoma2 チームが予選 2 位通過で参加したことで注目された。

大会議室に集合した受講者は A から F まで 6 チームに分かれ、さらにチュータのみで構成された Z チームと、帰国後間もないところを駆けつけてくれた sutegoma2 チームを合わせて 8 チームが、講師陣



図-4 CTFの様子

NO	企業・団体名 (50音順)	NO	企業・団体名 (50音順)
1	(ISC) 2 Japan	14	トレンドマイクロ (株)
2	伊藤忠テクノソリューションズ (株)	15	(社) 日本情報システム・ユーザー協会
3	(株) インテリジェントウェイブ	16	日本電気 (株)
4	SCSK (株)	17	(株) 野村総合研究所
5	エヌ・ティ・ティ・コミュニケーションズ (株)	18	(株) 日立製作所
6	(株) エヌ・ティ・ティ・データ	19	富士通エフ・アイ・ピー (株)
7	(株) オービックビジネスコンサルタント	20	フューチャーアーキテクト (株)
8	グーグル (株)	21	マカフィー (株)
9	CompTIA 日本支局	22	(株) ミクシィ
10	(株) サイバーエージェント	23	(株) 三菱総合研究所
11	サイボウズ (株)	24	三菱電機 (株)
12	(株) シマンテック	25	楽天 (株)
13	ソニー (株)	26	(株) ラック

特別会員 (独) 情報処理推進機構

表-2 セキュリティ・キャンプ実施協議会 賛同企業・団体一覧



図-5 官民連携によるセキュリティ・キャンプのイメージ

が腕によりをかけて作成した100以上の難問に挑戦した。複数のクラスの受講者が協力しつつ、6時間という長丁場の競技だったが、緊張感は途切れることなく、まさに静かな熱気というにふさわしい熱戦が繰り広げられた。黙々とPCに向きあう者、チームで相談して解法を考える者、Wi-Fiの電波で出題されている問題を捕まえるためにPCを持って館内をうろつく者、ネットワークで検索してヒントを見つける者など、さまざまな取り組み方が見られた。1人で17問(2,800点)を正解するなど、問題を作成した講師陣が驚くほどの解答率を見せた受講者もいた。

最終的には、Eチームが最後の5分で300点の問題と500点の問題を解いて大逆転勝利する劇的な幕切れとなった。CTFの様子を図-4に示す。

今後の取り組みは官民連携で

昨今、サイバー攻撃の複雑化・高度化などにより情報セキュリティ上の脅威がますます顕在化されてきている中、セキュリティ人材育成の必要性が高まってきている。このような情報セキュリティを取り巻く環境を考慮し、いままで実施してきたキャンプをセキュリティ人材の育成にフォーカスし、官民連携による若年層セキュリティ人材の発掘・育成の場として実施することとした。

このため国内外の企業・団体26社(表-2参照)で構成される「セキュリティ・キャンプ実施協議会」を2012年2月22日に設立し、今後は同協議会とIPAが対等の立場で密に連携を語り、高度な技術と実践力を持った若年層セキュリティ人材発掘の裾野を広げ、それら人材と産業界との交流機会の拡大を図っていく。また、日本の国際競争力強化や快適な国民生活の発展に貢献する世界レベルの「セキュリティの若い突出した人材」の発掘・育成に官民が連携して取り組んでいく。官民連携によるセキュリティ・キャンプのイメージを図-5に示す。

なお、従来のキャンプは「セキュリティ・キャンプ中央大会」と位置付け、IPAの事業として運営する。

(2012年2月29日受付)

神島万喜也 m-kami@ipa.go.jp

岡山県倉敷市出身。1979年岡山大学工学部合成化学科卒業。同年某電機会社に入社。プラント・工場等の生産管理システムのシステムエンジニアリング、営業技術等の業務に従事。2000年情報処理振興事業協会(IPA:現(独)情報処理推進機構)に出向。2002年IPAに移籍。現在に至る。セキュリティ・キャンプ事業、未踏IT人材発掘・育成事業の責任者を担務。