ARTICLE

# 実践的演習を伴うサイバーセキュリティ公開講座の取り組み

丸山一貴　明星大学
佐々木伸彦　ストーンビートセキュリティ（株）
高谷宏幸　マカフィー（株）

## 興味の入口としての公開講座

一般の方にとってはサイバーセキュリティというと高度に複雑であり，理解が難しく恐いものであると思われがちである．また，報道される際には事件としての側面から，個人情報漏洩の規模や被害額，責任の追及といった部分が大きく取り上げられ，技術的な側面は置いてきぼりになることが多い．そうした中，2014 年にサイバーセキュリティ基本法が成立し，セキュリティ分野の人材育成に一層注目が集まるようになった．企業では社内の人材を教育するため，サイバーセキュリティに関する演習付きの研修を外部に委託するケースが増えた．その一方で，大学では，学生向けに同様の機会を設けたり教材を準備したりするのは難しいこと☆1や，CTF（Capture The Flag）☆2のようなイベントは専門性が高く未経験者が初めに学ぶ題材としてはハードルが高いという問題があった．

セキュリティではプログラムや OS，ネットワークといった幅広い分野の理解が必要なことから，学生が自身の専門分野を活かせる可能性があることと，専門分野以外にも興味を持つことの必要性を感じてもらうことが重要である．そこで我々は，PC の操作は問題なくできるが，セキュリティについては素人である 10 代の生徒・学生を主な対象として，実践的な演習形式でその一端に触れる機会を設けようと考えた．2015 年に第 1 回を開催して以降，毎年 1 回，明星大学情報学部主催の無償の公開講座としてこれを運営している（図 -1）．2019 年のアンケートでは参加者の約 90% が「非常に満足」「満足」と回答し，後述する演習参加者に限定すると「満足」以上は 100% であった．本稿ではこの取り組みの概要と課題について述べる．

☆1　一部の学科にカリキュラムとして導入している大学は存在する．
☆2　サイバーセキュリティ技術に関する競技であり，ネットワークやバイナリ解析等の幅広い分野の技術が必要とされる．

## 講座の構成と参加形態

公開講座は休日午後の約 4 時間を利用して開催しており，大きく分けて 3 部からなる．第 1 部は講演として，サイバーセキュリティに関する基礎と最新情報を，その年のテーマに合わせて簡単に紹介する．第 2 部は公開講座のメインイベントである演習を行う．前半は前提知識やツール類の紹介をハンズオン形式で行い，後半は用意した課題に取り組んでチームごとの成果を競う．前半で扱う内容は，後半の課題に取り組むためのヒントを兼ねており，参加者は教材に例示されたコマンドの使い方等を参考にしながら課題に挑戦していく．第 3 部は演習内容の講評と全体の総括，質疑応答を行

図 -1　公開講座の様子

うとともに，優秀な成果を上げたチームを表彰する．

参加形態は演習参加と聴講参加の 2 種類を設定している．演習参加は，第 2 部で実際に 1 人 1 台のノート PC を使って課題に取り組むことができる．生徒・学生の優先枠を設け，2019 年は 36 名の演習参加者を募集した．演習参加者は 3 人で 1 チームを構成し，協力して課題に取り組む．聴講参加は演習を行わず，第 2 部では演習参加の様子を見守る形になる．

講座の運営には 2 つの課題があり，1 つは参加者の前提知識やスキルの違いである．演習参加者は高校生と大学生（大学院生を含む），社会人からなるが，間口を広くするという意図から，参加募集の際に専門的な知識や経験を要求していない．結果として，(1) 教材に出てくる用語等が分からない参加者や，(2) キー入力により起動するコマンドラインツールの取り扱いに不慣れで，第 2 部前半のハンズオンをスムーズに進められない参加者が存在している．

(1) の対策として，用語等の必要な知識を事前に学習できる簡易な予習教材を準備し，明星大学の学習管理システム☆3 を通じて演習参加者に配布している．2019 年は，事前登録した演習参加者の約 84% が予習課題にアクセスしていた．(2) に対しては，いわゆるティーチングアシスタントのようなサポートスタッフを数名配置して，個別の質問に対応しながら演習を進めることで解決を図っている．

講座運営のもう 1 つの課題は，聴講参加者の支援である．聴講参加者は，演習中は室内を自由に移動して演習参加者の PC 画面を見ながら，進捗状況を見守る形になる（図 -2）．しかし，画面内のコマンドの表示などは見づらく，また，各チームの進捗状況を把握することは難しい．この対策については後述する．

## 演習のテーマ

第 2 部の演習で出題する課題のテーマは年により異なり，サイバー攻撃を扱う回とディジタルフォレンジックスを扱う回に分けられる．ここではそれぞれの課題の概要と，いずれの回でも共通して課しているレポーティングについて述べる．

### ❑ サイバー攻撃

サイバー攻撃を扱う回では，演習参加者は攻撃者の立場になり，運営側である我々が用意した攻撃対象のシステムを外部から調査する．システムには典型的な脆弱性☆4 が残されており，そこからシステム内部に侵入して重要情報を取得する，というシナリオである．攻撃者の視点を学ぶことで，防御側，すなわち攻撃を受ける側としてどのような対策が必要か，何を学ぶべきかを考えるきっかけを提供している．

2015 年の第 1 回は，当時のマカフィー(株)がトレーニングプログラムのために用意していた課題をベースにしており，演習参加者は攻撃側と防御側に分かれていた．しかし，防御側の参加希望者が少ないため，現在は攻撃側のみを募集している．防御側の視点は，後述するフォレンジックスの回で取り上げている．

### ❑ フォレンジックス

フォレンジックスを扱う回では，演習参加者は企業の情報システム部門の立場になる．運営側である我々は，攻撃を受けて情報漏洩が発生した状態の情報システムを準備しておく．演習参加者には社の重

図 -2　演習中の聴講参加者

☆3 講義資料の配布やレポートの提出を管理できる Web システム．いわゆる LMS（Learning Management System）．

☆4 もろくて弱い状態のこと．セキュリティホールのこと．

役から，社外からの通報により個人情報の漏洩が発覚したため，原因と漏洩の経緯を調べるよう業務指示があった，というシナリオである．

現実には，フォレンジックスの作業そのものは社内スタッフでは行わず，専門的な外部企業に委託するケースも多い．しかし，フォレンジックスの作業を理解しておくことで，情報システムの企画や設計，運用において何に注意が必要であるか，意識を高めるきっかけになると考えている．

### ❑ レポーティング

演習の最後は，どちらのテーマを扱った回でも，必ずチームごとに簡単なレポートを提出する．レポートには，いつ，どんな原因で何が起こったか，どんな対策が考えられるかを，簡潔に記載してもらう（図 -3）．客観的な事実に基づいて，具体的な対策まで含めて報告することで，演習で取り組んだ内容を効果的に振り返ることができる．第 3 部の講評では，レポートの内容について簡単に触れ，課題の進捗がよかったチームや適切な対策を報告したチームを紹介して表彰する．

## IoT サイバーセキュリティ演習

ここではより具体的な内容の紹介として，2019 年に実施した IoT サイバーセキュリティ演習について，テーマ設定の背景と当日の進行や参加者の様子を紹介する．

図 -3　レポートの記入

### ❑ テーマ設定の背景

IoT（Internet of Things，モノのインターネット）は，あらゆる機器がインターネットに接続することで，我々の生活や仕事などを豊かにしてくれることが期待されている一方で，サイバーセキュリティの脅威が懸念されている．2018 年に公開された映画『名探偵コナン ゼロの執行人』でも IoT デバイスが登場し，話題になった．

実際，IoT デバイスに対するサイバー攻撃は年々増加傾向にあり，2016 年には Mirai[☆5] と呼ばれる IoT デバイスをターゲットとしたマルウェアが出現している．Mirai は脆弱な IoT デバイスへ不正侵入し，ボットネット[☆6] と化して，かつてないほどの大規模なサイバー攻撃（DDoS 攻撃[☆7]）を発生させた．その後，Mirai のソースコードがインターネットで公開されたこともあり，Mirai の亜種が次々と発生し，今もインターネット上で活動を続けている．

Mirai の攻撃は，典型的な ID とパスワードの組合せで次々とログインを試みるという非常に古典的な手法だったが，世界中で何十万台もの IoT デバイスがこの方法で不正侵入されてしまった．より身近になる IoT デバイスへの侵害は，これまで以上に，我々の生活に直結する甚大な被害を与えかねない脅威となり得るが，IoT デバイスにおけるセキュリティ対策やその理解は，まだまだ十分な状況とは言えない．デバイスが多様化しても，いつの時代も，セキュリティ対策は基本が重要であることを理解してもらうため，2019 年は IoT に関するサイバーセキュリティをテーマとして演習を実施した．

### ❑ 演習の題材

第 2 部の演習は，架空の鉄道事業者が運用する

☆5 Mirai は，脆弱な IoT デバイスへ不正侵入し，それらデバイスをボットネットとして悪用するマルウェア．ターゲットとするシステムや Web サイトに対して大量の通信トラフィックを送信し，サービス妨害攻撃（DDoS 攻撃）を行う．

☆6 マルウェア感染や不正侵入などによって，攻撃者の指令によって動く端末のことをボットと呼ぶ．ボットが大量に構成されたものをボットネットという．

☆7 Distributed Denial of Service attack，分散型サービス妨害攻撃．

「鉄道の運行管理システム」をテーマとした．この事業者では，離れた事務所からも電車の走行を把握できるようにして監視業務の運用を効率化したいという要望があり，監視用の IoT カメラが新設された，という状況を設定した☆8．

演習では，走行する鉄道模型（N ゲージ）と信号機に見立てた LED ライト，これらを制御する運行管理システム（Raspberry Pi）からなる演習セットを各チームに提供し，シナリオに沿って課題に取り組んでもらった．シナリオは，IoT カメラを調査して脆弱性を発見し，それを利用することで内部の運行管理システムへアクセスするという流れである．最終的に運行管理システムの認証を突破することができれば，鉄道模型を動かしたり，LED ライトを自由に点灯させたりすることが可能になる（図 -4）．

例年の演習とは異なり，鉄道模型や LED ライトといった目に見える変化を生む機器があることで，より積極的に課題に取り組む様子が見られた．特に，ほかのチームが鉄道模型を動かし始めると，「うちのチームも頑張らないと」という反応があり，会場全体が盛り上がっていた印象を受けた．

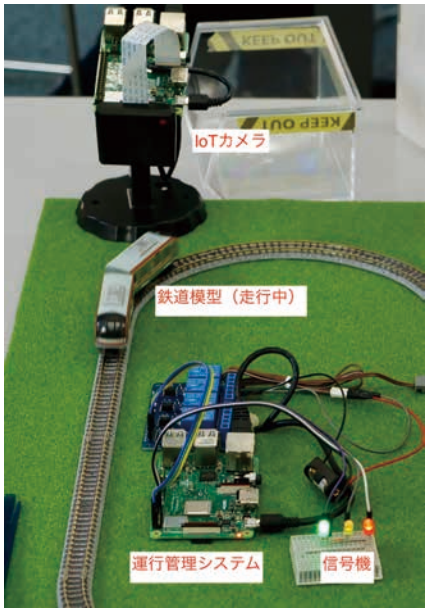

図 -4　鉄道模型を使用した演習セット

☆8 実際の鉄道運行システムはインターネットから隔離されているため，今回のテーマのような事態は発生しない．あくまで，IoT の脅威を勉強するための架空の設定である．

## 課題と今後の計画

講座の運営については大きく 2 つの課題があり，1 つは演習参加者の前提知識やスキルの違い，もう 1 つは演習中の聴講参加者の支援である．前者の対策についてはすでに述べたが，後者の対策として演習の進捗状況の可視化と解説を検討している．

可視化については Facebook CTF☆9 の利用を試みた回もあったが，単に課題の到達度を表示するだけでなく，チーム内のコミュニケーションの状況や試行錯誤の様子を見せられるとより効果的であると考えている．演習中の講師やサポートスタッフがそれらの表示を指し示しながら解説することで，聴講参加者の理解度向上を期待している．

2020 年度はハードニング（hardening，堅牢化）に焦点を当てた内容を検討しており，これらの改善案を盛り込んで実施することを目指している．

（2020 年 2 月 15 日受付）

**丸山一貴（正会員）** kazutaka@acm.org

2004 年東京大学大学院修了．博士（情報理工学）．同大情報基盤センター助教等を経て，2013 年明星大学情報学部情報学科准教授．プログラム開発環境やユーザインタフェースの研究，大学における ICT サービスの設計と運用に従事．

**佐々木伸彦** sasaki@stonebeat.co.jp

2015 年にストーンビートセキュリティを設立，代表取締役．2016 年から外務省最高情報セキュリティ責任者（CISO）補佐官を務める．脆弱性診断や情報セキュリティコンサルティング，トレーニング講師など幅広く活躍中．CISSP，CISA，GCFA，LPIC-3 Security.

**高谷宏幸** Hiroyuki_Takatani@McAfee.com

2005 年マカフィーに入社し，セールスエンジニアとして営業活動の技術的支援業務に従事．2014 年以降，プロフェッショナルサービス本部のシニアトレーナーとしてセキュリティ研修サービスを展開している．

☆9 CTF の運営を支援する Web アプリケーション．現在はオープンソース化されている．