第２部

特集2　JAISTにおけるセキュリティ人材育成への取り組み

宇多 仁

第１章　はじめに

北陸先端科学技術大学院大学(JAIST)では、WIDE Project参加研究者を中心に、セキュリティ人材育成活動として次のような活動を行っている。

■高度セキュリティ技術人材の輩出

JAISTはenPiT-Securityに参加し、連携各大学(東北大学、北海道大学、静岡大学、京都大学、大阪大学、奈良先端科学技術大学院大学、和歌山大学、岡山大学、九州大学、長崎県立大学、慶應義塾大学、東京電機大学、情報セキュリティ大学院大学)とともに、高度セキュリティ技術人材の輩出を目指した教育プログラムを実施している。

■人材育成プログラムへの技術支援・協力

セキュリティ人材育成プログラムは、内容的にも、技術力の向上を目指したものからインシデント対応の組織力まで幅広く、また、対象も、ある程度の技術力を有するエンジニアを対象としたものから情報リテラシーすら怪しい初心者を対象としたものまで様々である。共同研究などを通じて、CYDER[*1]、都立高専、国立高専機構、中小企業向けセミナー[*2]などさまざまなプログラムへ技術支援・協力を行っている。

■サイバーレンジに係わる研究開発

サイバーセキュリティに取り組む人材(サイバーセキュリティ人材)を育成するためのサイバーレンジ(サイバー空間の演習場)の構成技術を研究開発するとともに、これを用いた教育プログラムの設計および教材開発を行なうことを目的として、サイバーレンジ構成学講座(CROND: Cyber Range Organization and Design)を設置して研究開発を行っている。

特に、CROND のサイバーレンジに係わる研究開発活動はWIDE Projectとも密に連携しており、本年度はWIDE内にもサイバーレンジに係わる議論・研究を進めるNBCAワーキンググループを設立し、さらなる連携強化を図っている。本稿では、このCROND の活動を中心に報告する。

第２章　サイバーレンジ構成学講座(CROND)

CROND は、2015年4月に日本電気株式会社の寄付でJAISTに設置された寄付講座である。サイバーレンジとは演習を行うために特別に計算機上に構築された仮想空間を指し、多くの場合はセキュリティに関する解析、防御あるいは攻撃の演習が行われる。サイバーセキュリティが社会問題となっている現代では、サイバーセキュリティ人材が必要であり、そのような人材をより多く・より早く育成するためのサイバーレンジが重要となっている。

CROND はサイバーセキュリティ人材を育成するためのサイバーレンジの構成技術を研究開発するとともに、これを用いた教育プログラムや教材の設計を行なっており、次のような方向性をもって研究開発を進めている。

■サイバーレンジ構成の体系化、構築自動化

一般利用者のリテラシー教育から専門家向けの高度な演習まで、様々な対象や用途があるサイバーレンジを体系化する。また、現状では手作業の多いサイバーレンジ構

＊1　https://cyder.nict.go.jp/
＊2　http://www.htnet.co.jp/workshop/

築を自動化可能となるよう設計する。その検証のために、自動化を進めた構築ツールを設計・実装している。

■教育プログラムや教材の設計

教育機関、民間企業の人材育成部門やセキュリティイベントなどの組織と連携し、サイバーセキュリティ人材向け教育プログラムを設計している。

第３章　サイバー演習システムCyTrONE

CyTrONE（Integrated Cybersecurity Training Framework）はJAIST CRONDが開発しているサイバー演習システムで、クイズ形式のサイバー演習の構築・運用を実現する。CyTrONEはクイズ内容やサイバーレンジ構成を自由に編集できる。また、BSDライセンスで公開されているオープンソースソフトウェアなので、低コストので利用可能なのも利点である。

3.1　対象演習と提供機能

CyTrONEはセキュリティ技術者を目指す初心者〜中級者を育成することを念頭において開発されている。そのために鍵となったのが、「手軽に演習を実施できること」である。そのため、CyTrONEはクイズ式の演習を仮想環境で行う機能を提供している（図1）。クイズ形式とは、CTF（Capture The Flag）という競技でよく行われる形式で、順次出題される問いに対し指定された形式（選択式、記述式、等）で回答していく一問一答式の演習である。このような演習を実施するために、演習専用の環境（計算機やその上で動作するソフトウェア、ネットワーク）を仮想空間上に生成する。この仮想空間のことをサイバーレンジと呼ぶ。サイバーレンジを用いることで、物理的な計算機の構成にとらわれず柔軟にネットワーク構成などを指定することができる。さらに、セキュリティ演習では演習環境上で攻撃が行われることがあるため、これらを外部から隔離するという重要な機能も提供する。

3.2　システム構成

CyTrONEはCyLMSとCyRISという2つのサブシステムを利用している。CyLMSはトレーナーが作成した問題文・ヒント・解答などをLMS用に変換し、Moodleへの登録を行う（図2）。CyRISはトレーナーが定義した構成の演習環境を作成する。CyTrONEは上記2つのシステムを統合管理することにより、演習を立ち上げるプロセスを簡素化する（図3）。さらに、演習の立ち上げや削除はGUI操作で行うことができる（図4）。

図1　CyTrONEで作成した演習の例

```
---
- training:
  - id: L1-JA
    title: デスクトップコンピュータのセキュリティ調査
    overview: |
      <p>本日はシステム管理者として初めての仕事の日です。</p>
      <p>あなたの上司は、誰かがあなたの会社のネットワークに攻撃しようとしたことを疑っており、あなたにダニエル・グレイグ(Daniel Craig)と呼ばれる男が管理者だった頃に起こった可能性のあるサイバー攻撃を調査するよう頼みました。上司は前任のシステム管理者のコンピュータの前にあなたを座らせて、上手くいくことを望んでいます。</p>
      <p>このコンピュータは以前 WEBサーバも兼ねていました。WEB の脆弱性も調べてください。<p>
      <button class="open" value="VNC" onClick="window.open('http://150.65.117.115:3000/userinfo.php')">ログイン情報</button>
    level: 1

    questions:
    - id: L1-JA-001
      body: オペレーティングシステムとカーネルリリース番号でそのコンピュータにどの脆弱性を知ることができます。コンピュータのカーネルリリース番号を探してください。（例：3.4.5-6.7.8.abc.x86_64 ）
      answer: 3.10.0-693.21.1.el7.x86_64
      hints:
        - あなたは<code>uname</code>コマンドを使ってOSの詳細を探すことができます。
        - <code>$ uname -r</code>
        - 別の方法として、<code>/proc/version</code>ファイルから必要な情報を探すことができます。

    - id: L1-JA-002
```

図2　問題定義ファイル

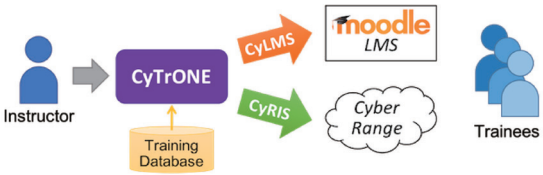

図3　CyTrONEのシステム構成

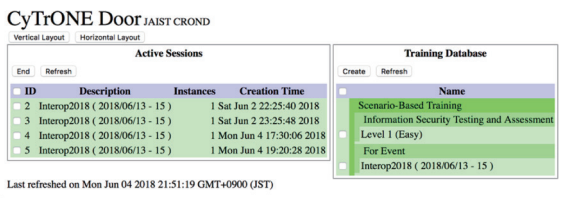

図4　CyTrONEの管理者（講師）向けUI

第４章　本年（2018年）の活動

本節では、本年の活動について、システム開発の状況、研究成果を中心にまとめる。

4.1　システム開発の状況

CROND で開発を行っているCyTrONE（ならびに周辺ツール群）は、オープンソースとして開発を実施しており、ソースコードはGitHub上で公開している。随時、リリースエンジニアリングも実施しており、現在の最新リリース版はCyTrONE v1.0である。

https://github.com/crond-jaist

また、CROND で開発を行っている一連のシステム群の普及活動の一環として、学生を中心にインストールガイドを作成した。これまでのプログラム群のそれぞれのマニュアルでもインストールは可能だが、使用するハードウェアやOS、アプリケーション構成には様々な組み合わせがあり、実際のインストール作業が難しい旨の指摘が多いため、新たに作成した。

このインストールガイド [23] では、アプリケーション構成を定め、一連の作業手順を具体的に記述したため、インストールが容易となった。このガイドは国立高専の教員向け講習会でその有用性が確かめられた。参加者がインストール作業にまごつかず、早い場合は約3時間でインストール作業を完了できた。

4.2　研究成果

CyTrONEの開発に係わる研究活動について、本年発表された主な論文等を取り上げ、その概要を示す。なお、CyTrONEの拡張に関する研究に関しては、必ずしも最新のCyTrONEリリース版に研究成果が既に含まれているわけではなく現段階では実験的実装のものも含まれるので注意されたい。

この論文 [24] は、我々の研究開発活動の中核であるCyTrONEについて、詳細概要をまとめたものである。CyTrONEの設計と実装、機能面ならびに性能面からの評価について記されている。

この論文 [25] は、サイバー防衛訓練を想定したCyTrONEの拡張に関するものであり、訓練参加者のシナリオ進捗管理の自動化について提案するものである。

東京都立産業技術高等専門学校との共同研究の成果を国際会議論文 [26] として発表したものであり、サイバーレンジ上で様々なOSを用いたPCの構築を可能とした。その例として、既に対応していたCentOSに加えて、新たにWindows系列OSのPCが利用可能となった。これを実現するツール群は、第一著者坂本氏により実装されたものである[*3]。

この成果をCyTrONE / CyRIS本体へフィードバックすべく、その差分の反映作業を進めている。

この論文 [27] は、サイバーセキュリティへの応用を伴う、高等教育のための教育プログラムの設計に関する方法論の体系化を行っている。

この論文 [28] は、Linked Open Data（LOD）データセットを用いたサイバーセキュリティ意識向上訓練に関する研究についての、中間進捗を報告している。

この論文 [29] は、我々が取り組んでいるセキュリティ演習をより高い視点で考察するため、それらの一般化を試みている研究の中間報告である。今後、修士論文として研究成果がまとめられる予定である。

この論文 [30] は、CyTrONEの拡張に関するものであり、制御を柔軟にするフレームワークを設計している。今後、修士論文として研究成果がまとめられる予定である。

この論文 [31] は、実環境に即したセキュリティ教育の一つして、インシデント再現に取り組む研究である。今後、修士論文として研究成果がまとめられる予定である。

＊3　https://github.com/motya1121

4.3 研究交流やイベント

サイバーレンジ技術の研究開発においては、利用者(受講者のみならず講師/運営者も含め)からの要求要件のヒアリングや開発システムに関するフィードバックを収集することも重要である。その重要な役割の1つをWIDE Projectを通じた研究者間の交流が担っているわけであるが、その他にも様々な交流やイベントを通じて知見の収集ならびに普及活動を図っている。ここでは、そのうちのいくつかを紹介する。

4.3.1 高等専門学校との交流

高等専門学校はCRONDの成果の適応先として有力である。本年は以下のように東京都立産業技術高等専門学校や国立高等専門学校と交流した。国立高等専門学校に関しては、国立高専機構を中心に交流している。

■東京都立産業技術高等専門学校との共同研究セキュリティ教育に取り組んでいる東京都立産業技術高等専門学校とCRONDは共同研究を続けてきた。この共同研究から前述文献[26] のような成果も導かれている。本年度は、高専生が1)我々のシステムに組み込むサブシステムや協調するシステム、2)セキュリティ教育コンテンツ、などを開発している。また、これまでと同様にセキュリティ教育の体制やコンテンツを議論してきた。加えて、8/20-23には合宿として、高専生と教員が本学へ訪問し、教育コンテンツ作成などを行った。

■国立高専機構との情報交換・講習会昨年までは国立高専機構との情報交換が中心であったが、本年は国立高専各校の教員へ、本講座が開発したシステムのインストール方法や教育コンテンツ作成方法などの講習会を開催した(10/18-19)。実際に教育に従事している教員がインストールする状況を観測でき、貴重な知見を得た。また、この講習会を機会にインストールガイドが整備できた。

4.3.2 「セキュリティ・ミニキャンプin石川2018」の運営参加、情報交換

セキュリティ・ミニキャンプはセキュリティ・キャンプと称するプログラムの一環で、25歳未満の学生を想定したセキュリティ教育イベントである。石川大会はJAIST高信頼IoT社会基盤研究拠点が主催団体の一つとなっている。我々は現地での会場作りなどを手伝い、開催者・講師達との交流を深めた。CRONDが目指す「若年層のセキュリティ教育」の視点で大いに参考となった。

4.3.3 Interop 2018 Tokyoでのデモ展示

Interop 2018 Tokyoに出展し、「CyTrONE v1.0を使用したサイバー演習体験」と題したデモンストレーション展示を行った。本デモンストレーションでは、一般の来場者の方々にCyTrONEで構築された訓練環境を受講者として体験してもらい、CyTrONEの幅広い層に対する認知度向上を図りつつ、体験者からのフィードバックを集めることができた。

第5章 まとめ

本年はWIDE内にもサイバーレンジに係わる議論・研究を進めるNBCAワーキンググループも設立するなど、より幅広い議論ができる場としてWIDEとの連携強化を図っている。興味を持たれた方々には、NBCAワーキンググループを通して、あるいは、JAIST CROND へ直接連絡を頂き、これからのサイバーセキュリティを担う人材の育成ひいてはサイバーセキュリティの向上に資する活動に共に参加頂きたい。