第10部

サイバーレンジ基盤技術の研究

砂川 真範、太田 悟史、阿波 史和、加藤 大弥、古寺 雄馬、知念 賢一

第１章　活動目的

活動目的は，サイバーレンジに関する議論と実装，普及活動などである．サイバーレンジとは，コンピュータネットワークに関するセキュリティ技術の練習場である．

第２章　現在の活動内容

現在の活動内容として，昨年に引き続きWGの各メンバーが行なっている研究の意見交換や，JAISTCROND Cyber Security Training Systemの研究・開発，サイバー演習[*1]で使用する用語の統一，普及活動を行っている．さらに，一部メンバーにより，昨年あげたマイルストーン上にある，CRaaSの実現に向けた，オリジナルのサイバーレンジ構築システムの設計・実装なども行っている．

現在WGの各メンバーが行なっている主な研究は，以下の通りである．

1)インシデントの再現を目的としたサイバーレンジ構築支援システムの設計[92]
インシデントの再現で必要となる要件を明らかにする．

2)サイバー演習コンテンツの比較
インシデント対応演習コース向けコンテンツやCTF出題コンテンツの分析・開発を通して，サイバー演習のあるべき姿を明らかにする．

第３章　2019年度の活動実績

2019年度の活動実績を以下に示す．

1）2019年 3月信学会IN研究会
セキュリティ演習に関する調査，および実際に運営した知見から，不正利用や形骸化の対策として正解の多様化に着目してきた．この研究会では，具体的な正解の多様化を実現するシステムを紹介した[93]．このシステムはJAISTCROND がこれまで開発してきたツール群の更新として実現されている．サイバーレンジの構築時に定まる事項(IPアドレスなど)を利用した正解を作れる，という副産物も得られた．

2)WIDE 3月合宿BoF
(a) NICTのサイバーセキュリティ人材育成・サイバーレンジ研究開発の取り組みと課題
WGメンバーの安田がNICTにおけるサイバーセキュリティ人材育成やサイバーレンジ研究開発について発表した．国内外のセキュリティ人材育成プログラムの現状に始まり，人材育成に関する国の方針と企業のニーズとのミスマッチ，NICTが取り組む人材育成事業とサイバーレンジ研究について，その具体的な内容や問題点・課題について発表した．

(b) CyTrONE用演習コンテンツの作成体験ワークショップ
CyTrONE用演習コンテンツの作成を実際に体験するワークショップを開催した．参加者は事前に用意された演習コンテンツのサンプルを編集すること

＊1　コンピュータネットワークに関するセキュリティ技術の演習

で，コンテンツの記述方法や編集結果がサイバーレンジにどのように反映されるかを確認することができた．

3）JAIST冬期集中講義

JAISTでは冬期集中講義としてセキュリティ関連科目を開講しているが，その科目でCyTrONEを使用したサイバー演習を実施した．演習内容はIPAの情報処理安全確保支援士試験問題を元にしたシチュエーションをサイバーレンジ上に再現したものである．CyTrONEを講義で実際に使用することで，講義に必要な準備に関する知見を得ることができた．また，CyTrONEに一部の不具合があることも判明した．

4）WIDE 5月研究会ワークショップ

(a) SecCapでのCyTrONE活用事例の紹介

CyTrONEの活用事例として，enPiTSecurity[*2]で基礎知識習得のためCyTrONEを活用した事例を慶應義塾大学の加藤が発表した．enPiT-Securityは，実践セキュリティ人材の育成を目的としているが，必ずしもセキュリティを専門とする学生が受講するわけではないため受講生の知識やスキルにばらつきが生じる．慶應義塾大学では基礎知識を習得し，受講生のセキュリティに関する基礎知識を底上げするためCyTrONEを活用した課題を実施した．ターミナルでの操作が不慣れな受講生が多い，受講者が演習を実施した結果を採点しにくいという問題があったため，CyTrONEを利用した演習へシフトすることとした．2019年度に行われた実際の演習の規模としては，受講生が16名，演習数が1つと小規模な取り組みではあったが特段の問題もなく実施することができた．結果としては，受講生はターミナル操作ではなく，Webブラウザを用いることですべての演習を実施し，CyTrONEを用いることで採点業務の効率化を実現した．

また本演習では，現状のCyTrONEでは実装されていないブラウザ上でのターミナル操作を実装し，CyTrONEへの技術的な貢献を果たした．

(b) CTFイベント開催

JAIST CROND はInterop Tokyo 2018でCTFを体験できるデモを出展したが，その際使用した問題及びCyTrONEをアップデートして新たにCTF[*3]ライクな演習を体験できるイベントを開催した．本イベントで参加者から得られたフィードバックを元に演習コンテンツの改良を更に進め，翌月にCyTrONE用CTFスタイル演習コンテンツをリリースした（後述）．

5）CyTrONE 用CTFスタイルサンプルコンテンツ公開

CyTrONEにはサイバー演習コンテンツのサンプルとしてNIST Level 1相当の問題が同梱されているが，追加サンプルとしてCTFスタイルの問題セットを6月にリリースした．[*4]．問題セットはバイナリ解析・暗号解読・ネットワーク・OS・ウェブの5分野からなり，CyTrONEがインストールされた環境に追加する形で利用することを想定している．

6）Interop Tokyo 2019

JAIST ブースでCROND の研究を紹介した．サイバーレンジ関連のビデオが中心であった．

7）CODE BLUE 2019

JAIST CROND が寄附講座の縁でNECのブースを借りて出展した．出展内容はCROND の開発物の紹介が中心である．セキュリティ分野のイベントであることから，参加者とより専門的な議論を交わすことができた．それ以外のメンバーがCapture The Packetのワークショップに参加した．このワークショップでは，AriesSecurity社のサイバーレンジに基づいたサイバーディフェンスの競技のほかトレーニングが提供された．トレーニングに参加し，Aries Security社のサイバーレンジで使われているコンテンツの一部や受講者の操作など体験しサイバーレンジやコンテンツに関する知見を得ることができた．

＊2　SecCap
＊3　Capture The Flag
＊4　https://www.jaist.ac.jp/misc/crond/achievements-ja.html

8）WIDE 12月研究会BoF

（a）CyPROMの紹介

JAIST CROND の最新ツールであるCyPROMを紹介し，CyPROMを使用する際の前提知識と実行手順を具体的に説明した上で，デモを行った．

（b）次世代サイバーレンジシステム（案）

研究内容の紹介として，次世代サイバーレンジシステムの草案を発表した．開発方針，既存システムでの課題を含めた追加の要件など挙げた上で，全体像や利用イメージなどを説明した．

第４章　マイルストーン

4.1　2020年度の目標

- セキュリティ演習の新しい形の検討
  新しいセキュリティ演習の形式を考案し検討を行う．
- セキュリティ演習用コンテンツの開発
  セキュリティ演習に使用できるシナリオ等のコンテンツを開発・実装を行う．

4.2　中・長期的な目標

- 様々なサイバーレンジの比較
- 様々な用途向けコンテンツを検討
- 外部の組織との連携
- 一般向けにイベントを開催
- WIDE内の他のWGとの連携
- CRaaS（CyberRange as a service）の実現
  クラウドサービスのように，いつでも・どこでも・誰でも使えるサイバーレンジサービスを実現させる．

第５章　今後の活動

定期的なミーティングの他に，WIDE研究会やWIDE合宿でのBoFやイベント開催，随時用語集の更新，不定期開催のサイバーレンジ見学会を予定する．