

4 サイバーセキュリティに関する人材育成

4 Human Resource Development on Cybersecurity

4-1 ナショナルサイバートレーニングセンター研究開発報告

4-1 National Cyber Training Center Research and Development Report

園田 道夫

SONODA Michio

ナショナルサイバートレーニングセンターは人材育成事業を展開しているが、独自開発の LMS である CYDERANGE によって演習環境を提供している。その CYDERANGE に組み込むべき実装として、仮想環境の利用に関する詳細なログ等を活用した学習効果の可視化やスキルの可視化について研究を行っている。また、対応分析等の分析手法を用いて CYDER 演習にて収集したアンケートデータから、潜在的な評価をあぶり出す手法の開発を行っている。開発した手法を用いてアンケートデータよりサービス改善の手がかりをつかみ、事業改善に役立てている。

The National Cyber Training Center is developing a human resource development project and provides an exercise environment through CYDERANGE, a proprietary LMS. As we incorporate an implementation into CYDERANGE, we are researching the visualization of learning effects and skills by utilizing detailed logs in the virtual environment. We are also developing a method to uncover potential evaluations from the questionnaire data collected in the CYDERANGE exercise using analytical techniques such as correspondence analysis. Using the developed method, we have obtained clues for service improvement from the survey data and are using it for business improvement.

1 マウス、キーボードの利用ログなどを用いたツールの習熟性についての研究開発

ナショナルサイバートレーニングセンターでは主に地方公共団体や独立行政法人、中央省庁等にインシデントの初動対応をテーマとした演習を提供している(実践的サイバー防御演習 CYDER)。他には国家資格である情報処理安全確保支援士向けに CYDER の流れをくむシナリオベースの演習を展開し(実践サイバー演習 RPCI)、2024 年現在、2025 年日本国際博覧会協会向けにも演習を提供している(CIDLE)。これら実務者向けの演習とは別に、25 才以下の若手研究者・技術者向けにセキュリティ・イノベーター育成事業として SecHack365 も展開している。

これらの教育の事業展開に係るソフトウェア、システム開発として、NICT が持つ仮想インターネットを実現可能なテストベッド StarBED (<https://starbed.nict.go.jp/>) 上に構築する LMS (Learning Management System) である CYDERANGE (<https://www.nict.go.jp/>

[press/2018/03/08-1.html](https://www.nict.go.jp/press/2018/03/08-1.html))を開発している。CYDERANGE は多数の仮想マシンを展開可能な演習環境を提供するシステムでもあり、CYDER や RPCI のような 4 人 1 チームで組む集合演習で各チームに 100 台以上の仮想端末など組織の実環境を模した演習環境を提供している。また仮想マシン上での操作ログをシステムコールレベルで収集していて、その中で主にマウスとキーボードの動きに関するログデータを基にツールの習熟性に関して可視化につながる研究を行っている。これらの研究は、GUI ベースのツールの場合、習熟度によってマウスの動きのパターンが異なり、パターンごとにグループ化が可能ではないか、さらにそれらを機能の呼び出しログと照らし合わせることでデジタル的な 1 - 0 ではなくアナログ的に表現(可視化)できるのではないか、という仮説の検証をテーマとしている。パケットデータの収集・分析ツールとして広く使われている Wireshark (<https://www.wireshark.org/>) を題材に、エキスパートと初心者との動きのパターンについてモデル化を行った [1]-[3]。ほかにキーボードとマウ

スの動きをもとにしたログ解析の習熟度のモデル化[4]や、検索サイトの利用に関する習熟度に関しては視線のトラッカーを補助的に用いるなどの研究を行った[5]。

これらの研究成果は将来的に CYDERANGE に分析・可視化機能として実装していく予定である。

2 CYDER のアンケート分析による潜在的評価の抽出

主たる事業の CYDER では年間 100 回以上の集合型演習を開催しているが、必ず事後にアンケートを記入してもらい、収集している。近年、そのアンケートデータを主に潜在的な評価をあぶり出すことを目的として分析・評価する研究を行っている。

論文「多重対応分析とアスペクトベース感情分析を組み合わせた受講者満足度調査データの分析手法の開発」において報告した手法は、多重対応分析 (MCA) とアスペクトベース感情分析 (ABSA) を組み合わせなおむね「満足」の結果をあらわしているデータから改善すべき課題を抽出するものである。ここではまず MCA を用いて受講生空間を生成し、そこに満足度関係の変数を投影することで、満足及び不満の構造を可視化したのち、自由記述回答に埋もれている両儀的な語を ABSA によって抽出、それをタグ付けし、MCA によって生成された空間上の個体へのマッピングを行なった。結果として全体的に「満足」の回答から課題を抽出することが可能になった[6]。続いて論文「クラスタリングによる自由記述回答の要約と選択肢回答空間に射影による解答群間の連関の可視化」においては、非階層型クラスタリングによって自由記述回答を「要約」、それを構造化データ解析 (MCA/SDA) の手法で生成された選択肢回答空間に射影し、この二つの回答群の連関を幾何学的に可視化する手法を開発した。この手法は選択肢回答によって生成された変数 / 個体空間上にクラスタ番号として「要約」された自由記述回答をプロットすることを可能とし、自由記述部分の分析条件が拡大することを示した[7]。

今後も主に対応分析を用いて、アンケートの分析及びそれに資する手法の開発を進めていく予定である。

【参考文献】

- 1 T. Matsuda, M. Sonoda, M. Etou, H. Satoh, T. Hanada, N. Kanahama and H. Ishikawa; "Mathematical Model on Wireshark Operation Skill Evaluation," IMA Conference on Mathematics in Defence, pp.1-7, 2017.
- 2 松田 健, 園田 道夫, 衛藤 将史, 佐藤 公信, 花田 智洋, 金濱 信裕, 石川 大樹, 池田 克己, 加藤 大貴, "PC 操作ログ解析による作業効率の可視化に向けた一考察," 情報処理学会研究報告, vol.2018, MPS-118,no.21, pp.1-2, June 2018.
https://jglobal.jst.go.jp/detail?JGLOBAL_ID=201902259471052685
- 3 平井 美穂, 松田 健, 園田 道夫, 衛藤 将史, 佐藤 公信, 金濱 信裕, 花田 智洋, 石川 大樹, 池田 克己, 趙 晋輝, "キーボードとマウス操作ログ

分析に基づくユーザー特性の考察," JSiSE 研究会研究報告, vol.32, no.5, pp.103-106, Jan. 2018.

<https://www.jsise.org/society/committee/2017/5th/TR-032-05-016-A.pdf>

- 4 Takeshi Matsuda, Michio Sonoda, Masashi Eto, Hironobu Satoh, Tomohiro Hanada, Nobuhiro Kanahama and Hiroki Ishikawa, "User Skill Characteristics Analysis by Mouse Operation Log Analysis Based on Algebraic Method,"
https://link.springer.com/chapter/10.1007/978-3-319-94947-5_25
- 5 Takeshi Matsuda, Ryutaro Ushigome, Michio Sonoda, Hironobu Satoh, Tomohiro Hanada, Nobuhiro Kanahama, Masashi Eto, Hiroki Ishikawa, Katsumi Ikeda & Daiki Katoh "Investigation and User's Web Search Skill Evaluation for Eye and Mouse Movement in Phishing of Short Message," Takeshi Matsuda, Ryutaro Ushigome, Michio Sonoda, Advances in Intelligent Systems and Computing, AISC, volume 960.
- 6 大畑 和也, 藤本 一男, "多重対応分析とアスペクトベース感情分析を組み合わせた受講者満足度調査データの分析手法の開発," 言語処理学会 第 29 回年次大会 発表論文集, pp.255-260, 2023.
- 7 根本 颯汰, 藤本 一男, "クラスタリングによる自由記述回答の要約と選択肢回答空間に射影による解答群間の連関の可視化," 言語処理学会 第 30 回年次大会 発表論文集, 2024 年 3 月.



園田 道夫 (そのだ みちお)

サイバーセキュリティ研究所
ナショナルサイバートレーニングセンター
センター長
博士(工学)
サイバーセキュリティ、教育
【受賞歴】

2024 年 電波の日・情報通信月間、情報通信月間推進協議会会長表彰 (情報通信功績賞)

2018 年 情報セキュリティ文化賞受賞
2012 年 SecureAsia@Tokyo 2012 Asia-Pacific Information Security Leadership Achievements (ISLA) Senior Information Security Professional表彰