

令和2(2020)年度 スマートネイチャーシティ(SNC)ちとせ事業 実績報告書

令和3年3月20日

報告者 (所属学科・職名・氏名) : 情報システム工学科・講師・深町 賢一 助教・砂原 悟事業名 : サイバーセキュリティにおける橋渡し人材育成のための演習教材の開発とサイバーレンジ(演習環境)の構築**事業報告 :**

1. 今年度の活動実績・報告

サイバーセキュリティ人材が全国的に不足している現在において、特に若手の人材育成が急務となっている。千歳市においても高度なセキュリティ人材育成が可能な拠点として認識されることを目指し、北海道地域情報セキュリティ連絡会(HAISL)を中心とした産学官連携を行い、演習環境の開発や若手向けの講習会を実施した。

2. 実践的なサイバーレンジ環境と教材の開発

情報セキュリティ事故につながる要因として世界的に問題となったbashの脆弱性(CVE-2014-6271等)を疑似体験できる演習教材を開発した。演習教材では次の4点を重視している。

- (1) 学習者がひとり1台、自分専用のサイバーレンジ環境を自力で(簡単に)用意できること
- (2) 不正アクセスを受けたかもしれない状況において、調査、防衛策、関係各所への報告やそれらの優先度について組織的な観点から学習者が考えること
- (3) コマンダー、マネージャー、トリアージなどのCSIRT的な役割分担可能なシナリオであること
- (4) 演習が「防災訓練」の役割を果たし、未来において適切な行動を素早く行えること

演習はシナリオベースとなっており、学習者が手元で構築するサイバーレンジ環境は2014年9月24日にCVE[1]やNVD[2]にて脆弱性の情報が公開されたときの状況を再現している。シナリオでは、より実践的な訓練を行うために攻撃者の活動も疑似的に再現している。したがって、この演習は倫理教育とセットで行う必要がある。専門用語やコンピュータの操作など、受講に必要な前提知識は理工系大学2~3年生を想定している。学習者が自分の手元で用意する環境のイメージを図1に示す。

3. 講習会の実施について

2020年8月29日に北海道地域情報セキュリティ連絡会(HAISL)が主催する「次世代育成プロジェクト Security College for Youth」の第1回目として北海道警察サイバーセキュリティ対策本部と連携し、講習会を実施した。当初計画では千歳市民文化センターで実施予定であったが、新型コロナウイルスによる感染症対策のため、実施形式をオンラインに切り替えて開催した。演習にはTAなどのサポートを受けることが可能なzoom枠15名、YouTube Liveによる見学者35名、計50名が参加した。

環境構築時のネットワークイメージ図

LAB環境を悪性の通信から守るために
外部からの通信は遮断
自ホストのループバックアドレスからのみ通信可能

| 送信元 | 送信元IP | 宛先IP | 通信 |
|------------|--------------------------|--------------|----|
| 外部(黒服) | グローバルIP | 192.168.0.10 | NG |
| 宅内(ウサギ) | 192.168.0.11 | 10.0.2.15 | NG |
| 自ホスト(ペンギン) | 192.168.0.10 | 10.0.2.15 | NG |
| | 127.0.0.1 port 22, 80 | 10.0.2.15 | OK |

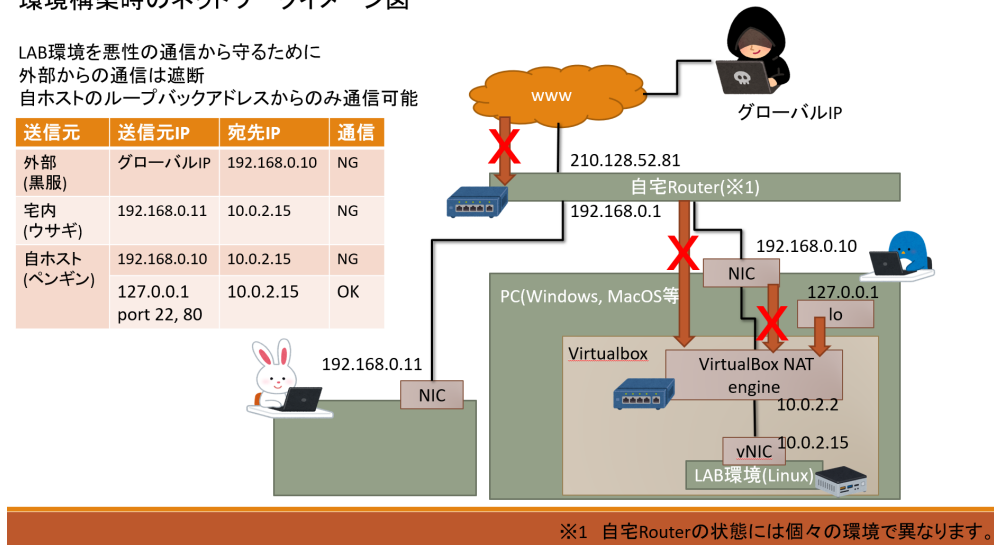


図1 学習者が自分の手元で用意するサイバーレンジ環境のイメージ

4. 参加者からの評価

演習実施後に受講者へのアンケートを行った。完全オンライン形式のため、学習者は配布される資料を読み、自力で環境を構築する必要があったため、サポート体制を必要とすると思われていた。しかし実際には特に質問もなく、図2のとおり環境構築はおおむね容易であったという評価が得られた。演習内容については図3のとおり、多くの参加者から学びにつながったという評価が得られた。

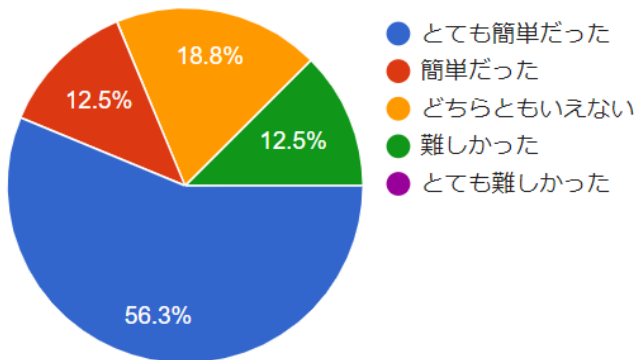


図2 サイバーレンジ環境の構築難易度

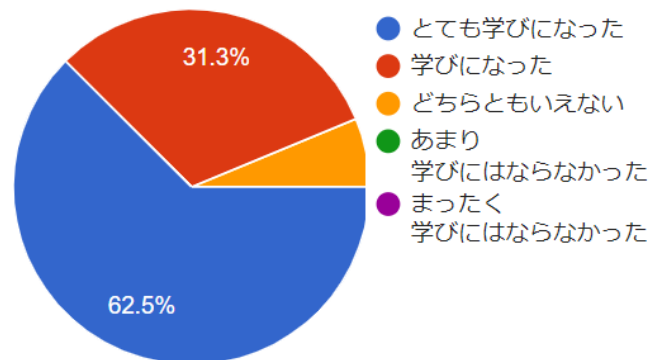


図3 今回の演習が自身の学びにつながったか

5. 今後の展開

2021年度も北海道地域情報セキュリティ連絡会(HAISL)との産学官連携は継続する見込みである。演習で学んだ知識や技術をより実践的な場で活用できる取り組みとしてセキュリティ競技であるCTFやWAS Forumが実施するHardening Projectなどとも連携し、学習者の学びの場を広げていくことが重要であると考えている。今年度の取り組みを足掛かりとして、サイバーセキュリティの学びの場として、千歳市のプレゼンスを高めていきたい。

[1] CVE: Common Vulnerabilities and Exposures <https://cve.mitre.org/>

[2] NVD: National Vulnerability Database <https://nvd.nist.gov/>