令和 4 年度実績報告書

令和 5 年　3 月　20 日

公立千歳科学技術大学
学長　宮永　喜一　様

公立千歳科学技術大学特別研究等助成要綱第 7 条に基づき、下記のとおり報告いたします。

報告者	所属	共通教育科	職名	助教
	氏名	砂原 悟	ふりがな	すなはら さとる
研究課題名	ネットワークインフラセキュリティを学ぶためのサイバーレンジ環境開発とその検証			
本研究費による発表論文、著書など	令和 6 年度 発表予定			

研究成果報告

コロナ禍においてテレワークの重要性が高まっており、今後も継続的に活用されることが期待されている一方で、VPN などのネットワーク接続機器を狙ったサイバー攻撃が実際に観測されている。サイバー攻撃を防ぐ、あるいは影響を緩和させる方法として、サイバー攻撃の再現及びその対策や対応を繰り返し行うことができる安全な環境(サイバーレンジ)での訓練が有効であると考えられる。現在では、サイバーレンジを用いた実践的な演習を作成及び維持するコストを低減させるために、サーバの仮想化環境を用いて構築することが一般的である。 1 台のサーバ上にハイパーバイザを構築した場合、OS は仮想マシンによる高い分離レベルを確保することが可能であるが、ネットワークのコントロールはハイパーバイザの管理から分離できないため、学習者にネットワークの変更を伴うような演習シナリオを提供することが困難であるという問題点がある。本研究では、ハイパーバイザ上にソフトウェアネットワークルータを組み込むことによって、それぞれのサイバーレンジ環境に新たなネットワークレイヤーを作成するというアプローチで問題の解決を試みた。

本研究で開発したサイバーレンジ環境の構成を図 1 に示す。サイバーレンジ環境は繰り返し何度も利用することを想定し、Terraform による自動構築を行った。環境内の仮想マシンを悪用されないための対策として、インターネットとの接続ポイントに VPN とユーザ認証を設置した。演習用のテンプレート環境として架空の企業ネットワーク及びデスクトップ、サーバ、攻撃再現用の仮想マシンを用意した。演習環境操作インターフェイス(Apache Guacamole)から演習用のデスクトップ、サーバ、ネットワーク機器の全ての操作が可能である。学習者が演習を受けるために必要な環境は VPN とブラウザ接続のみであり、Windows、MacOS、Chromebook、Android タブレット及び iPad から演習に参加が可能であることを確認した。サイバーレンジ環境内のネットワークルータ、ファイアーウォール及び VPN は VyOS を使用しており、学習者は演習にてこれらのネットワークを自由に編集することが可能である。演習環境で使用するネットワークはハイパーバイザのネットワークとは分離されているため、演習中にネットワークの破壊的な設定変更を行っても他のサイバーレンジ環境に影響が出ないことを確認した。本環境では次の 4 つのサイバー攻撃について実行が可能であることを確認した。(1)ポートスキャンによる偵察活動、(2)ファイアーウォール及び VPN の設定不備による不正アクセス、(3)標的型攻撃による VNC での不正な遠隔操作及びワームの拡散　(4)DDoS 攻撃によるサービス停止。(1)～(4)全て実行することが可能であるが(4)を実行した場合は、負荷によって学習者が演習環境を操作できなくなるため、演習のためには 10 秒サイクルで攻撃と停止を繰り返すなどの加減が必要であることがわかった。(1)～(4)の演習シナリオを体験した理工系の大学生 4 年生 3 名にアンケート及びヒアリングを行ったところ、楽しんで学ぶことができると感じている一方で、ネットワークの実技を行った経験がほとんどなかったため、事前学習用にネットワーク用語と設定の意味を理解する資料が欲しい、また、コマンド操作に慣れていないためグラフィカルなネットワーク操作のインターフェイスが欲しい、ネットワークルータの設定をミスすると自力での復旧が難しいため、設定をリセットする機能が欲しいなどの意見が得られた。今後は、今回得られた意見を参考に、より規模の大きい演習を行い、環境の評価や学習の効果について検証を行う予定である。

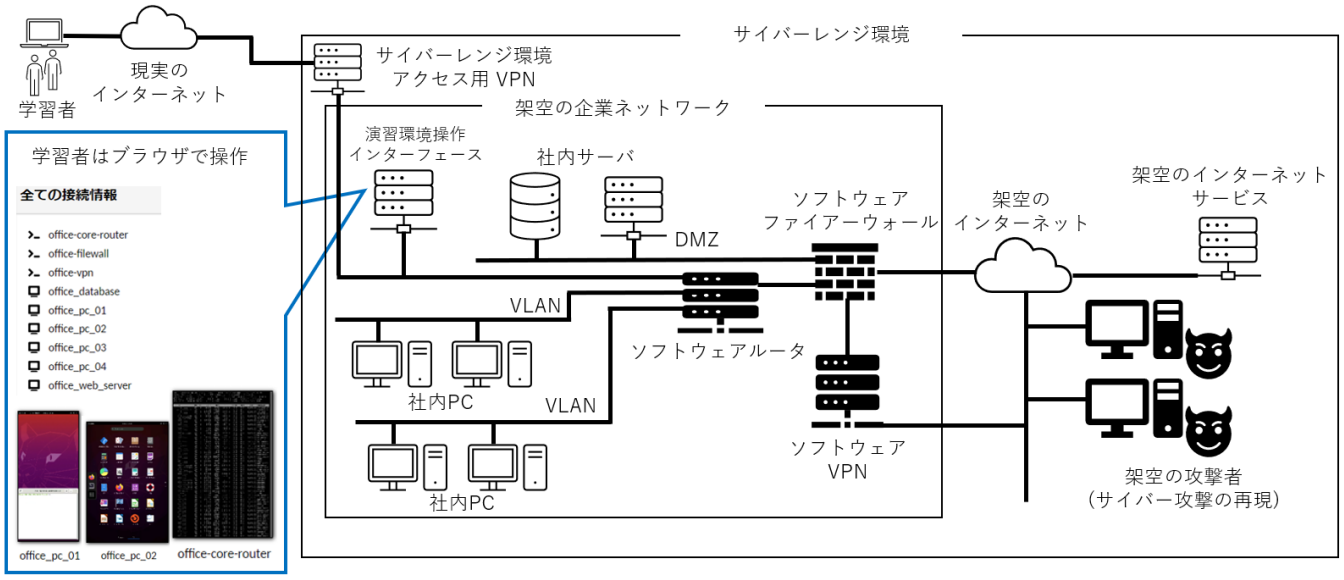

図 1 開発したサイバーレンジ環境の構成図