分散環境における拡張性を持つ サイバーレンジの構築手法の提案と評価

寺嶋　友哉[1,a)]　小出　洋[1]

概要：社会生活に IT 技術が浸透，発展するとともにサイバー攻撃の脅威が増加しているが，セキュリティ人材は慢性的に不足しており，サイバー攻撃に対応できる人材の育成の必要性が高まっている．人材育成の取り組みとしてサイバー攻撃対応演習を行うことは実際に攻撃への対処を経験できるため効果的である．サイバー攻撃対応演習においてサイバーレンジを用いた演習は仮想環境を構築して実環境を再現することで実際のインシデントに近い状況を再現できるため，高い演習効果が期待できる．一方で，サイバーレンジを構築，運用するためには高性能なハードウェアやネットワーク機器が必要であり，高い費用がかかる．さらに演習環境に接続するために特定の演習会場に移動する必要があるなど，参加者に地理的制約を課してしまう．これらの理由から気軽にサイバーレンジを用いた演習を企画，参加することが難しい．そこで，本論文ではサイバーレンジを構成するサーバ群やネットワークをコンテナ型仮想化システムとソフトウェア VPN を用いて物理機器を用いずにクラウド上に構築することによりサイバーレンジを用いた演習のコストや地理的制約などの諸課題を解決する拡張性を持ったサイバーレンジ構築手法を提案，評価した．その結果，通常の演習環境と同様の演習環境を提案手法に基づきクラウド上に構築，演習を行うことができた．

Proposal and evaluation of an adaptable cyberrange construction method in a distributed environment

1. はじめに

本研究では，サイバーレンジを用いたサイバー攻撃に対する攻防演習における物理的・地理的な制約を軽減することを目的として，より柔軟性と拡張性を持ったサイバーレンジの構築手法を提案し，評価を行う．

1.1 提案

セキュリティインシデント対応能力を向上させるための訓練として，サイバーレンジを用いた演習を実施することは効果的である．しかし，サイバーレンジを用いた演習は構築，運用にかかるコストが高く，演習環境に参加するためには演習会場に移動する必要があり演習企画者や参加者に対して金銭的や物理的，地理的に制約を課すこととなる．そのため，本論文ではサイバーレンジ構築に必要なプライベートネットワークと演習用サーバをクラウドの仮想マシン上に構築することで，サイバーレンジ演習にかかる制約を軽減し，拡張性を持ったサイバーレンジを構築する手法を提案する．

1.2 実験と結果

提案する手法を用いてクラウド上に構築した演習システムを用いて実際に演習を行った．仮想プライベートネットワークの構築にはソフトウェア VPN，演習サーバにはコンテナ型仮想化システムである Docker を使用した．演習は開始時に参加者の接続が集中したことにより一時的に接続障害が発生し，接続が困難になった参加者が少数存在したものの，その後は概ね通常の LAN 環境で構築した演習システムと同様に進行することができた．また，改善すべき点についても複数得ることができた．

1.3 サイバー攻撃演習

サイバーレンジとは，自治体や企業のシステムを模倣した情報システムを仮想環境を用いて構築した演習システム

[1] 情報処理学会
IPSJ, Chiyoda, Tokyo 101–0062, Japan
[†1] 現在，九州大学
Presently with Kyushu University
[a)] terashima.tomoya.988@s.kyushu-u.ac.jp

である．サイバーレンジを用いた演習では仮想環境内でシステムに対して実際に攻撃を行い対応を訓練することにより演習を進行する．セキュリティインシデント対応の演習は大きく分けて２種類の演習方法がある．IPA が発行している IT 計画および IT 対応能力のためのテスト、トレーニング、演習プログラムのガイド [2] によると，セキュリティインシデント対応についての教育方法として，机上演習とサイバーレンジを用いた機能演習がある．机上演習とは議論ベースの演習で，担当者が会議室に集まって緊急時の対応を議論する演習である．用意したシナリオをベースとして参加者が各自の役割，責任，決定事項などを議論することで進められる．機能演習とは，実際の環境を模したシミュレーション環境を用意してシナリオに沿ったインシデント対応を仮想環境の中で実践することができる．サイバーレンジを用いた演習は機能演習に分類される演習で，実際のインシデントに近い状況を再現した上で演習を行うことができるため得られる効果が高い．その一方で商用に販売されているサイバーレンジは費用が高い．また，オープンソースでのサイバーレンジの開発も進んでいるが，サイバーレンジを構築するためには仮想マシンを多数運用するための高性能ハードウェアや，ネットワーク機器の用意が必要である．そのため，演習参加者に金銭的，物理的，また地理的制約がかかることが多く，演習企画の障害となっている．

1.4 サイバー攻撃の現状

現在の社会において IT 技術は我々の生活と密接に結びついており，社会にとって必要不可欠なものとなっている．一方で，IT 技術と生活の結びつきが強くなるほどサイバー攻撃が社会に与える影響は増大している．総務省が発行している情報白書の令和元年度版 [3] によると，2017 年度サイバー犯罪による損失は全世界で 6,080 億ドルにのぼり (McAfee 社による分析)，日本においても，一社あたり数億円単位の損失が発生すると報告されている．また，サイバー攻撃の種類も多様で，発生したインシデントの分類も年々変化している．情報セキュリティ白書 2019[5] によると，個人向けの脅威第一位は”クレジットクレジットカード情報の不正利用”，組織向けでは”標的型攻撃による被害”が一位であった．昨年度はランクインしていなかった”サプライチェーンの弱点を悪用した攻撃”がランクインしているなど，攻撃は多様化，複雑化している．

1.5 サイバーセキュリティ人材の現状

サイバー攻撃の脅威が高まり，セキュリティインシデントに対応することのできるサイバーセキュリティ人材の需要が増加している．しかし，サイバーセキュリティ人材は慢性的に不足しており，総務省が平成 30 年に発行した我が国のサイバーセキュリティ人材の現状について [4] には，2016 年時点で情報セキュリティ人材が 13.2 万人不足と推定．2020 年には，不足数が 19.3 万人に増加するとも見込まれている．とあり．実際にサイバー攻撃に対応できる人材の不足は深刻なものとなっている．従って，サイバーセキュリティ人材を育成することが必要とされている．同資料によると，企業のサイバーセキュリティ人材の不足の原因について，“トレーニングの余裕がない”，“専門人材を公募しても必要なスキルを持つ応募者がいない”，“採算が取れない”，“適切な教材や講座”がないといったものが挙げられており，時間・対費用効果・教育の質などの要員が人材育成の障害となっている．このような現状において，サイバーレンジを用いた演習を気軽に行えることは，人材育成に対して有効な対策となり得る．

2. 研究の目的

IT 技術の発展と社会への浸透とともに，サイバー攻撃に対する脅威は年々増加している．しかし，セキュリティインシデントに対応できるサイバーセキュリティ人材は不足しており，2020 年には 19.3 万人が不足すると試算 [4] されている．その背景として，サイバー攻撃に対応するためには専門的なスキルを必要とするため教育が難しく，時間がかかるということがある．サイバー攻撃対応の演習の手法として，サイバーレンジを用いた機能演習がある．サイバーレンジ [13] とは，実際の環境を模したシミュレーション環境を仮想計算機などを使用して演習用に再現するシステムのことである．このサイバーレンジを使用して演習を行うことにより，参加者は実際のサイバー攻撃と同様の状況と体験，対応することができる．実際のインシデントに近い演習を行えるため，サイバーレンジを用いた演習は非常に教育効果が高いと言える．しかし，演習環境を構築する際には，様々な要件がある．サイバーレンジには実際に脆弱性を持ったサーバを動作させ，様々なサーバを連携して動作させたり，実際の企業などの内部ネットワークなどを模したネットワーク環境を構築することからプライベートネットワークであることが望ましい．これらの要件により商用のサイバーレンジは非常に高価である．また，参加者はサイバーレンジのネットワークに接続できる会場に移動する必要がある．サイバーレンジを用いた演習は高い教育効果がある一方で，参加者や企画者に地理的・物理的また金銭的に制約を課してしまう．これらの制約により，サイバーレンジ演習は非常に敷居の高いものとなっている．本研究では，サイバーレンジ演習の制約を軽減し，より柔軟性と拡張性を持ったサイバーレンジを構築する手法を提案し，評価することを目的とする．

3. 研究の概要

3.1 クラウド上に構築

サイバーレンジの構築に必要な主な要素は演習用プライ

ベートネットワークと演習用のサーバ群である．本研究では，これらの要素を物理機器でなく，クラウド上の仮想計算機上で構築することで環境のスケーリング，再現性などを容易にし，サイバーレンジ構築・運用の負担を軽減する．クラウドを利用することで演習の内容や規模に合わせたコンピューティングリソースを確保することができ，拡張性・柔軟性を実現する．**図 1** に提案手法のシステム図を示す．

3.2 プライベートネットワークの構築

サイバーレンジ演習では仮想システム内で脆弱性を持ったサーバやアプリケーションを稼働させるため，インターネットや外部のネットワークから隔離されたプライベートネットワークが必要である．既存のサイバーレンジはプライベートネットワークを構築するためにルーターやスイッチなどの物理機器を使用するのが一般的である．これらの機器を用いて LAN を構築する場合，LAN に参加できる場所が電波の届く範囲に限定されてしまう．また，VLAN や VXLAN[14] を用いて地理的に離れた場所でも仮想的に LAN に参加させることは可能だが，参加者側のネットワーク機器がこれらに対応している必要があり，制約を軽減できているとは言えない．そこで，本研究では，サイバーレンジ構築に必要なプライベートネットワークをソフトウェア VPN を用いて構築する．現在の PC には標準機能として VPN クライアントが搭載されているので，クライアントは VPN に参加するだけで地理的な制限を受けずに演習を行うことができる．また，ソフトウェア VPN を使用することにより，Linux などの汎用サーバ上に VPN サーバを構築することができるため，専用の物理機器を用意することなく構築できるため，サイバーレンジ構築のコストを抑えることができる．

3.3 演習用サーバの構築

演習用サーバの構築には，コンテナ型仮想化技術を使用する．コンテナ型仮想化システムはホスト型やハイパーバイザ型の仮想化システムと比較して軽量でオーバーヘッドが少ないという特徴がある．コンテナ型仮想化システムを用いて演習用のサーバをコンテナとしてクラウド上のインスタンスに動作させる．これによって効率的にクラウドリーソースを使用することができる．

4. 関連研究

4.1 リモートデスクトップを用いたサイバーセキュリティ演習システムに関する研究

地理的制約を軽減した分散した環境においてのサイバーレンジ演習の手法として，リモートデスクトップを用いたシステムが提案されている．体験型サイバーセキュリティ学習システムの提案と構築 [6] によると，架空の企業を模したネットワークと仮想的なインターネットをサイバーレンジのネットワーク内に構築する．仮想的なインターネットには攻撃者のサーバやその他のサーバが配置されている．企業のネットワークには DNS サーバやプロキシサーバ，Web サーバが配置されていて，架空の企業の社員の PC が配置されている．参加者は，サイバーレンジとインターネットの両方のネットワークに接続されたサイバーレンジ接続用の PC に RDP(Remote Desktop Protocol) を使用して接続し，社員の PC や DNS サーバなどに RDP を用いて接続することで，演習に参加する．RDP とはユーザがネットワークで接続されたコンピュータのデスクトップ環境を遠隔地から接続して操作するためのプロトコルである．RDP を使用することでインターネットを介して参加者は地理的・時間的制約を受けることなく演習を行うことができる．実際に提案された手法を用いて構築されたシステムで約 300 人の受講者が演習を受講している．この研究で提案されている手法では，RDP を用いることでサイバーレンジを用いた演習における制約を軽減しているが，RDP は予め演習システムに用意された端末を使用して行うため各自の端末にインストールされているソフトウェアを使用できない．これは演習の効率や利便性を低下させるとともに，実環境の再現度を損なっている．本研究では演習ネットワークに参加者各自の端末を接続するために参加者は各自の端末にインストールされたソフトウェアを使用して演習を行うことができる．

4.2 コンテナ型仮想化技術を用いたサイバーレンジの提案

サイバーレンジへのコンテナ型仮想化技術を活用するシステムが提案されている．情報セキュリティ演習環境サイバーレンジへのコンテナ型仮想化活用の提案 [7] によると，サイバーレンジにコンテナ型仮想化システムを導入することにより, サイバーレンジ構築にかかる負担を軽減できるとしている．コンテナ型仮想化システムを使用する場合の優位性として，ハイパーバイザ型の仮想化やホスト型の仮想化システムと比べて軽量でオーバーヘッドが少ないため，ハードウェアリソースを削減することができる．また，コンテナはホスト型などの仮想化システムの仮想マシンイメージより軽量で環境の廃棄や再構築などが容易であり，運用面においても，従来のサイバーレンジに対して優位性がある．一方でコンテナ型仮想化を使用したサイバーレンジの課題は，コンテナシステム自体の脆弱性を再現するようなシナリオが作成できないというものや，コンテナ型仮想化はその他の仮想化と比べてシステムの分離レベルが低いため，ホスト OS や他のコンテナの影響を受けてしまう可能性があるというものである．しかし，コンテナを使用した脆弱性の再現性について，コンテナ型仮想化のサイバーレンジにおける脆弱性の再現性評価 [8] では，コンテナ型仮想化とホスト型仮想化におけるサイバーレンジ運用時の脆弱性の再現性を評価したところコンテナ型仮想化

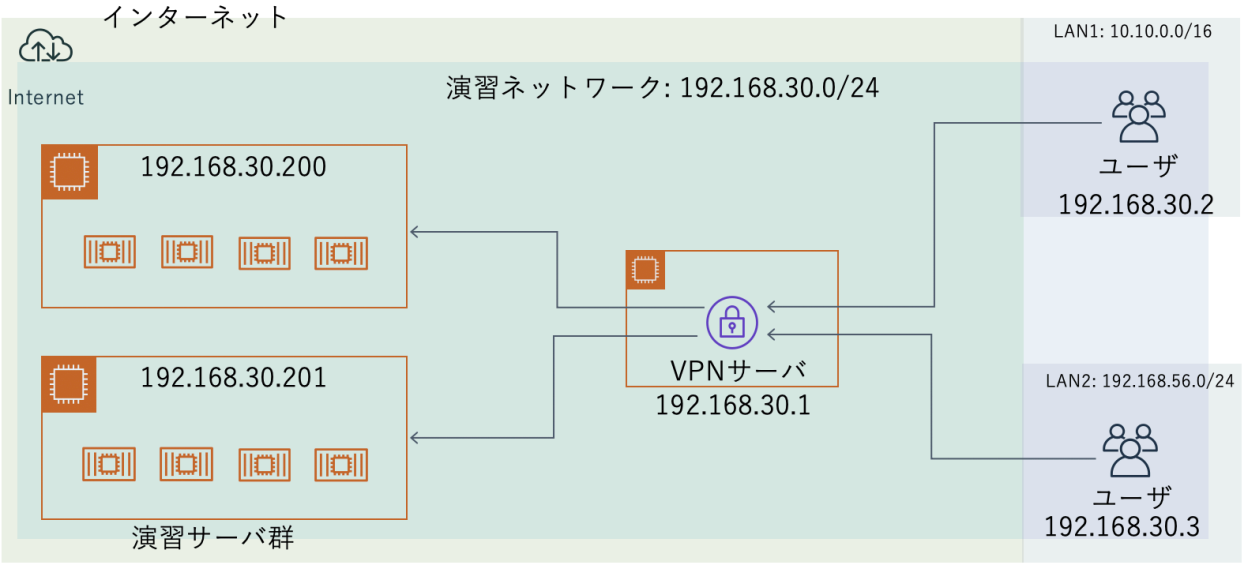

図 1 提案システム
Fig. 1 proposed system

は各種脆弱性の再現に必要な設定を追加することでホスト型仮想化を用いたシステムに対して約 97%の一致率を得たと報告している．よって，コンテナ型仮想化システムをサイバーレンジの構築に活用することは有用である．

4.3 VPN を用いたサイバーセキュリティ演習環境の構築

Arvind S. Raj らは Scalable and lightweight CTF infrastructures using application containers[9] で実際に VPN を用いて開催された CTF 大会について言及している．CTF とは Capture The Flag の略で，チーム，または個人でサイバーセキュリティの技術を競い合う競技である．地理的に分散した環境において CTF のように攻撃パケットを送受信する環境を構築する際に，VPN を用いることは有効である．競技用ネットワーク内に VPN サーバを設置して競技参加者，またはチームが VPN クライアントや VPN ゲートウェイを用いて競技ネットワークに VPN 接続することにより分散した環境においても影響を受けずに競技を行うことができる．しかし，演習環境の構成は VPN サーバや，VPN ゲートウェイのために専用機器を用いるため，物理機器への依存度が高い．本研究では，同様に VPN を用いて演習用ネットワークを構築することで演習参加者の地理的制約を軽減したサイバーレンジを提案する．さらに，演習ネットワークを物理機器を使用せずにクラウドを用いて構築することで物理機器への依存度を削減している．これにより拡張性や柔軟性を持ったサイバーレンジを構築することが可能である．

表 1 使用したソフトウェアとバージョン
Table 1 software and version

ソフトウェア	バージョン
SoftEther VPN Server	Ver 4.31, Build 9727, beta
Docker	18.09.9-ce
docker compose	1.25.0

5. 提案手法

本章では，クラウド上に VPN サーバと演習用サーバ群を稼働させることにより目的の章で述べた各種制約を軽減するサイバーレンジ構築手法を提案する．提案手法では 1 に記載する無償で利用できる外部ソフトウェアを使用してサイバーレンジを構築する．

5.1 クラウド上に VPN サーバを構築する

本研究で提案する手法では，サイバーレンジを構成するための仮想プライベートネットワークをクラウド上に設置した VPN サーバを用いて構築する．演習参加者は VPN に接続することによって，地理的な距離を意識することなくサイバーレンジ用に構築されたプライベートネットワークに参加することができる．

5.1.1 VPN(Virtual Private Network)

VPN(Virtual Private Network) とは，物理ネットワーク上に仮想的なプライベートネットワークを構築する技術である．VPN には，インターネットを経由して仮想的なプライベートネットワークを構築するインターネット VPN と，プロバイダなどが提供する専用の閉域網を利用する VPN

が存在する．本研究では，インターネット VPN を使用するため，以後 VPN とはインターネット VPN を指すものとする．VPN とは，インターネット上に仮想的なトンネルを張ることで実現される．具体的にはパケットをカプセル化・暗号化，することでプライベートな通信を実現する．

5.1.2 SoftEther VPN

VPN を実現する手法は様々な物が存在し，それぞれの手法により機能は様々である．本研究での VPN の要件は汎用サーバ上で専用の物理機器を用いることなく構築できること，仮想的なプライベートネットワーク (LAN 環境) を構築できることである．仮想的な LAN 環境を地理的に分散した環境で構築するためには，データリンク層のプロトコルである Ethernet をカプセル化して通信を行う必要がある．これらの要件を満たすソフトウェア VPN が SoftEther VPN である．従って，本研究では仮想ネットワークの構築に SoftEther VPN(https://ja.softether.org/) を使用する．SoftEther VPN とは，筑波大学の研究プロジェクトとして開発され，ソフトイーサ株式会社の製品である PacketiX VPN の制限バージョンとして公開されているオープンソースのソフトウェア VPN である．SoftEther VPN の特徴は Ethernet を仮想的にソフトウェアでエミュレートしている点である．仮想 NIC や仮想スイッチングハブをソフトウェアとして実装することで L2 VPN を実現している点である．SoftEther VPN は IPSec による暗号化や SSL による暗号化の機能を備えている．

5.1.3 SoftEther VPN を用いた仮想プライベートネットワーク

SoftEther VPN を用いて仮想ネットワークを構築するためには，SoftEther VPN Server を動作させたサーバが必要である．提案手法では，この VPN サーバをクラウド上に構築する．インターネットを介してアクセスできるクラウド上に VPN サーバを構築することで演習参加者は地理的な制約を気にすることなく VPN に接続することができる．演習参加者はその VPN サーバに VPN 接続することで演習用に構築された仮想プライベートネットワークに参加することができる．演習用ネットワークで TCP/IP のようなプロトコルを用いた通信をするためには IP アドレスが必要である．SoftEther VPN Server には仮想 DHCP の機能が備わっており，VPN 接続しているクライアントに対し，重複しないプライベート IP アドレスを自動で割り振ることができる．そのため，参加者は特別な操作をすることなく，VPN に接続するだけで演習を開始することができる．しかし，仮想 DHCP の機能が Linux 上では正常に動作せず，IP アドレスが自動で割り当てられないという状況が発生したため，Linux においては手動で同一セグメント内の重複しないアドレスを割り当てる必要があった．

5.2 クラウド上に演習サーバを構築する

演習に必要な脆弱なサーバやアプリケーションを動作させるサーバをサイバーレンジ内に構築しなければならない．提案手法では VPN によるプライベートネットワークを演習用ネットワークとして用いるため，サーバを配置する場所に地理的制約はない．従って，演習用サーバもクラウド上で構築することができる．クラウド上に構築することで，コンピューティングリソースの管理やスケーリング・トラブルシューティングを容易に行うことができる．一方で，クラウド上に演習サーバを構築する際は，サーバが外部からアクセスできないように適切にファイアーウォールなどを設定しておく必要がある．全ての演習パケットは VPN サーバを介して送信されるため，VPN サーバのアドレス以外からの不必要なトラフィックは全て拒否する設定をしなければならない．

5.2.1 コンテナ型仮想化

提案手法では演習用サーバにコンテナ型仮想化を用いる．コンテナ型仮想化とは仮想化手法の一種で，通常の仮想化とは異なり，ホスト OS 上でプロセスを分離することにより専用のリソースを確保する仮想化手法である．ハードウェア資源などをホスト OS と共有するため，その他の仮想化手法と比べてオーバーヘッドが少なく，軽量であるという利点がある．演習用サーバの構築には，コンテナ型仮想化ソフトウェアの Docker(https://www.docker.com/) を用いる．Docker を用いることで，Dockerfile と呼ばれるコンテナを起動するための設定ファイルを作成することにより，特定の環境を再現したコンテナを容易に構築することができる．また，環境の複製や再構築などにおいてもコストを削減することができる．一方で，関連研究にあるようにコンテナ自体の脆弱性を再現できないことや，リソースの分離レベルがその他の仮想化技術と比較して低いことによりハードウェアに依存するような環境を再現することができないという欠点が存在する．そういった場合は，ホスト型の仮想化などと組み合わせてサイバーレンジを構築することが必要である．

5.3 サイバーレンジの構築

上述した SoftEther VPN とコンテナ型仮想化を用いてサイバーレンジを構築する．手順は以下の通りである．

(1) クラウド上にインスタンスを用意して，SoftEther VPN Server をインストールして動作させる．
(2) クラウド上のインスタンスに Docker をインストールし，演習用サーバの Docker イメージを動作させる．
(3) 演習用サーバが動作しているインスタンスに SoftEther VPN Client をインストールする．
(4) 演習用サーバが動作しているインスタンスが VPN 接続するためのユーザーを VPN サーバに登録して，VPN 接続を確立させる．

表 2　使用したクラウドリソース
Table 2　cloud resource

用途	タイプ	メモリ	vCPU	OS
ホストサーバ	m5ad.4xlarge	64GB	16	Amazon Linux
VPN サーバ	t3a.xlarge	16GB	4	Amazon Linux

(5) 演習参加者を VPN 接続させるためのユーザーを VPN サーバに登録する．

構築手順は以上である．演習参加者は，VPN サーバに登録されたユーザー情報を元に各端末から標準の VPN クライアントを用いて VPN サーバに接続する．以後の演習時の通信は VPN 接続時に割り当てられたプライベートアドレスを用いて通信を行う．

6. 実験

2019 年 12 月 21,22 日に東京・秋葉原で開催された SECCON Akihabara 2019 (https://www.seccon.jp/2019/akihabara/) で実施されたワークショップにて，提案手法を用いて構築した演習環境を用いて演習を行った．演習参加者は一般から募集した約 80 人，演習時間は 1 時間 30 分であった．

6.1 実験内容

今回の実験は本研究で提案する柔軟性と拡張性を持ち，サイバーレンジを用いたサイバーセキュリティ対応演習における地理的・物理的制約を軽減するサイバーレンジ構築手法を評価するために行った．VPN を用いて各参加者がクラウド上の演習サーバに接続して演習を行うため，分散環境においても同様の結果が得られると考える．演習内容は，各演習参加者が一人一台ずつ割り当てられた演習サーバに SSH を用いて接続して Python を用いて予め用意された脆弱性のある Web アプリケーションを動作させ，その脆弱性を実際に各自の端末にフォワーディングして確認し修正するというというものである．

6.2 演習システム

6.2.1 構成

演習用に起動したクラウドのインスタンスの性能は 2 のように選択した．使用したクラウドのベンダーは Amazon Web Service(https://aws.amazon.com/jp/) である．ホストサーバでは Docker を動作させ，参加者が利用する演習用サーバとなるコンテナを 100 個動作させる．VPN サーバでは演習ネットワークを構成する VPN サーバを動作させる．また，演習補助アプリケーションを動作させる．

6.2.2 実装

演習内容の要件を満たす演習環境を構築するにあたり，SSH 接続・Python3・SQLite が動作する Ubuntu ベースの Docker イメージ A.1 を作成し，演習用サーバとしてクラウド上のホストサーバ (以下ホスト) で稼働させた．各コンテナは SSH 接続をするために 22 番ポートを開いており，ホストサーバの 10022 番から 19922 番ポートにマッピングされている．また，コンテナ内の通信ログを取得するためにコンテナ内では tcpdump を動作させている．ホストサーバは VPN サーバからのトラフィックのみを受け付けるようにファイアーウォールを設定しており，外部ネットワークからのアクセスはできない．VPN サーバには SoftEther VPN Server と演習補助アプリケーションを動作させる．仮想的なプライベートネットワークを構成するために SoftEther VPN Server の仮想 DHCP 機能を用いて参加者に対してユニークなプライベートアドレスを割り当てる．ホストサーバには DHCP により割り当てられる IP セグメントと同一となる DHCP 割り当て IP アドレス範囲外のアドレスを割り当てることでアドレスの重複を防止する．また，ログ収集機能を用いて VPN サーバを通るトラフィックを記録する．演習を行うにあたり，参加者は VPN に接続するための認証情報や演習用サーバが動作するアドレスとポートの情報を事前に取得する必要がある．また，VPN に接続するためには事前に VPN サーバにアカウントを登録する必要がある．これらを解決するために演習補助アプリケーションを作成した．演習補助アプリケーションにアカウント登録機能を実装することで，アプリケーションへのアカウント登録が VPN サーバのアカウントと紐ついて登録される．VPN サーバへのアカウント登録には SoftEther VPN Server の API を用いて補助アプリケーションのアカウント情報を元に VPN ユーザ作成リクエストを発行してユーザ登録を行った．参加者は演習補助アプリケーションにアカウント登録することで同一の認証情報で VPN 接続時の認証情報を登録できる．また，参加者は演習補助アプリケーションにログインすることで VPN サーバのアドレス情報や事前共有鍵，演習用サーバのアドレスとポートを取得することができるように実装した．実装した演習システムの構成は 2 のようになっている．

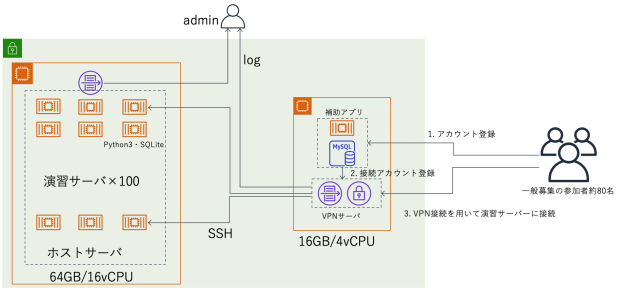

図 2　演習システムの構成図
Fig. 2　infrastructure configuration

6.2.3 演習手順

参加者は演習開始時に演習補助アプリケーションにアカウント登録，ログインすることで必要な VPN サーバや

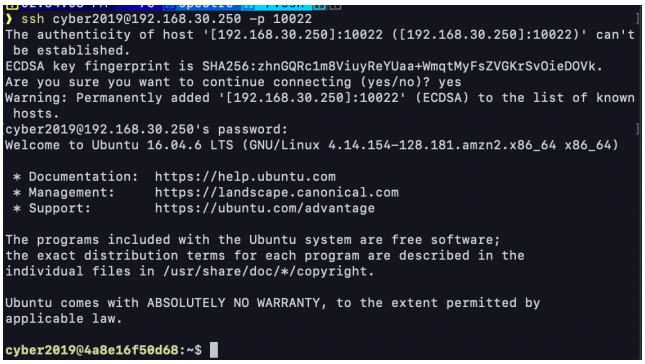

図 3 ssh 接続画面
Fig. 3 ssh connection

演習用サーバの情報を取得する．取得した VPN 接続情報を用いて各自の端末に標準搭載されている VPN クライアントを用いて演習ネットワークに VPN 接続を行う．演習ネットワークに参加し，各自に割り当てられた演習用サーバの情報を用いて演習用サーバに SSH を用いて接続する．3 以後は演習用サーバ上で Web アプリケーションを動作させ，ポートフォワーディングを用いて各自の端末の Web ブラウザに表示させながらアプリケーションの脆弱性を修正する形で演習を進行させる．

7. 実験結果

本実験全体において VPN サーバに流れたパケットの総量は約 7GB であった．一方で演習サーバとして各演習参加者が使用したコンテナ内部に到達したパケットの総量は約 253MB であった．演習中にネットワーク内を流れたパケットのうち，演習に関連したパケットは全体の約 3.6% であったことから，演習中のほとんどの通信は演習に関係のない通信であった．各演習サーバに流れた通信のうち最も多くパケットを受信していたサーバは 113MB を受信しており，総パケット量の約半分を通信していた．通信量が他の演習サーバと比べて極端に多いサーバでは，何かしらのソフトウェアをインストールしていたと思われる．ほとんどの参加者の演習サーバは 1.5MB 以内の通信量であり，中央値は 658KB であった．通信量が 1.5MB 以内であった演習サーバの通信量の分布は 4 のような分布となっていた．100KB から 1.1MB まで幅広く分布しており，参加者によって演習の進み具合は違いが現れていたと考えられる．また，演習開始時に演習参加者が一斉に補助アプリケーションと VPN サーバに接続したことにより一時的にアプリケーションへの接続や VPN 接続が困難になる障害が発生した．補助アプリケーションを VPN サーバと同一のサーバ内で動作させていたためにそれらが動作しているサーバインスタンスへ接続が集中したと考えられる．演習開始時の接続障害は一時的なもので，以後は問題なく演習を進行することができた．参加者は VPN 接続後は通常の LAN 環境と同様の手順により SSH 接続を行い演習用サーバへと接続ができていた．一方で，VPN を普段使用しない参加者にとって，VPN 接続は慣れないものであるので接続方法についての質問がいくつか挙げられた．さらに，VPN 接続は一定時間通信を行わないと接続を切断するために，最後の操作から一定時間空いた後操作する際は再度接続する必要があり，通信が途切れる場合があった．

8. 考察

本研究ではサイバーレンジを用いたサイバーセキュリティ対応演習にかかる地理的，物理的制約を軽減する柔軟性と拡張性を持ったサイバーレンジ構築手法を提案し，提案手法を用いて構築した演習システムで実際に演習を行った．演習は開始時に参加者が一斉に VPN サーバと補助アプリケーションが動作しているサーバに接続したことにより一時的に接続障害が発生した以外は問題なく進行した．本実験は分散環境ではなかったものの，提案手法では VPN を用いて演習システムに接続するため，地理的な制約を受けることなく演習を行うことができたと言える．また，本実験を行うにあたって必要なシステムは全てクラウド上の仮想計算機上で動作させたため，物理的制約を軽減している．演習システム構築に必要な機器をクラウド上にソフトウェアとして動作させることで演習の規模によってクラウドのリソースを選択することでネットワーク，演習サーバ群共に対応することができる．一方で，本演習システムでは VPN サーバに大量の通信が流れることとなる．そのため，予め演習時の通信量を予測して VPN サーバのクラウドリソースを選択したり，VPN サーバの負荷分散が必要である．また，参加者の端末に演習に関係する通信以外の通信を VPN を経由しないような設定を追加するという対策がある．従来の演習環境と比較して，提案手法による演習システムはネットワークに接続する際に VPN に接続するというステップを踏まなければならない．これは VPN に慣れていない参加者にとっては負担となりうる操作である

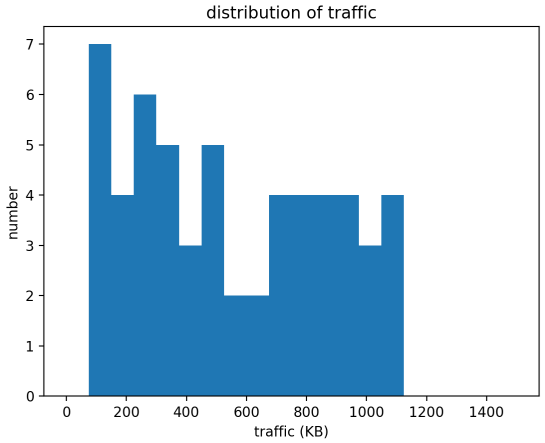

図 4 通信量の分布 (distribution of traffic)

と考える．演習用サーバを Docker を用いてコンテナとして動作させる手法は演習用サーバがコンテナであることを参加者に意識させることなく演習を進行できたため，コンテナを演習用サーバとして使用することは有効であった．

9. おわりに

本論文ではサイバーレンジを用いた演習にかかる制約を軽減したより拡張性と柔軟性を持ったサイバーレンジ構築手法を提案し，実際に提案手法を用いて演習システムを構築し演習を行い，評価を行った．提案手法では演習用ネットワークにソフトウェア VPN を用いてクラウド上に VPN サーバを動作させ，VPN によって演習用プライベートネットワークを構築することにより，演習参加者は地理的な制約を受けることなく演習に参加することができる．さらに，クラウド上にネットワーク機器をソフトウェアとして動作させることにより演習の規模や内容によって演習システムを柔軟に拡張，複製または再構築が可能となる．本研究で提案した手法には課題も見られた．VPN を使用して演習ネットワークを構築しているため，普段 VPN を使用していない演習参加者にとって VPN 接続設定のステップは負担である．演習ネットワークに VPN を使用することにより演習時の通信が VPN サーバに集中する．そのため，VPN サーバを動作させるインスタンスには十分な処理性能を持つインスタンスを選択する必要がある．今後の課題，展望として，演習ネットワークを意識させない演習ネットワークを構築手法の開発や，今回は一時的な演習用として構築した演習環境を大規模な演習プラットフォームとして長期にわたり運用することを予定している．

謝辞 本論文の作成にあたり終始丁寧な指導と適切な助言を賜りました小出洋教授に感謝申し上げます．また本論文の執筆にあたり実験の場を提供していただいた SECCON 実行委員会の皆様に感謝申し上げます．論文の執筆方法や実験の補助などの支援をしていただいた九州大学サイバーセキュリティセンター学術研究員藤岡福資郎氏に感謝申し上げます．本研究の一部は日立システムズと国立情報学研究所 SINET 広域データ収集基盤プロジェクトの支援を受けている．

参考文献

[1] IPA 独立行政法人 情報処理推進機構:情報セキュリティ白書 2019,IPA 独立行政法人 情報処理推進機構 (2019)
[2] IPA 独立行政法人 情報処理推進機構:IT 計画および IT 対応能力のためのテスト、トレーニング、演習プログラムのガイド,page 25-32,IPA 独立行政法人 情報処理推進機 (2006)
[3] 総務省:情報白書,page-96, 総務省 (2019)
[4] 総務省:我が国のサイバーセキュリティ人材の現状について, 総務省 (2019)
[5] IPA 独立行政法人 情報処理推進機構:情報セキュリティ 10 大脅威 2019,IPA 独立行政法人 情報処理推進機構 (2019)
[6] 八代哲, 高橋和司, 渡辺亮平, 角田祐太, 田邊一寿, 横山雅展, 斎藤裕太, 斎藤孝道:体験型サイバーセキュリティ学習システムの提案と構築, コンピュータセキュリティシンポジウム 2017 論文集 (2017)
[7] 中田亮太郎, 大塚玲:情報セキュリティ演習環境サイバーレンジへのコンテナ型仮想化活用の提案, 情報教育シンポジウム論文集 page 198-205(2019)
[8] 中田亮太郎, 大塚玲:コンテナ型仮想化のサイバーレンジにおける脆弱性の再現性評価,2020 Symposium onCryptography and Information Security(2020)
[9] Arvind S. Raj and Bithin Alangot and Seshagiri Prabhu and Krishnashree Achutha:Scalable and Lightweight CTF Infrastructures Using Application Containers (Prerecorded Presentation,2016 USENIX Workshop on Advances in Security Education (ASE 16)(2016)
[10] 登大遊:SoftEther の内部構造, 情報処理 vol45 number10 page 1057-1-62(2004)
[11] 登大遊:SoftEther による Ethernet の仮想化とトンネリング通信, 情報処理学会第 45 回プログラミング・シンポジウム論文誌 page 147-158(2004)
[12] SoftEther Project at University of Tsukuba, Japan:SoftEther VPN, 入手先 ⟨https://ja.softether.org/⟩
[13] V. E. Urias and W. M. S. Stout and B. Van Leeuwen and H. Lin:Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper,2018 International Carnahan Conference on Security Technology (ICCST)(2018)
[14] RFC Editor:Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, 入手先 ⟨https://rfc-editor.org/rfc/rfc7348.txt⟩

付　　録

A.1 演習サーバコード

```
1  FROM ubuntu:16.04
2  RUN apt-get update \
3      && apt-get -y install python3 python3
           -pip sqlite3 openssh-server sudo
           vim tcpdump nano \
4      && pip3 install bottle peewee \
5      && mkdir -p /work \
6      && mkdir /var/run/sshd \
7      && mkdir -p /var/log/research
8
9  RUN sed -i 's/PermitRootLogin prohibit-
       password/PermitRootLogin yes/' /etc/
       ssh/sshd_config
10 RUN sed 's@session\s*required\s*
       pam_loginuid.so@session optional
       pam_loginuid.so@g' -i /etc/pam.d/
       sshd
11
12 ENV NOTVISIBLE "in users profile"
13 RUN echo "export VISIBLE=now" >> /etc/
       profile
14
15 RUN groupadd -g 1000 cyber2019 \
16     && useradd -g 1000 -m -u 1000
           cyber2019 \
17     && chsh -s /bin/bash cyber2019 \
18     && echo 'root:toor' | chpasswd \
```

```
19          && echo 'cyber2019:apple8086' |
                chpasswd
20
21      COPY /work /home/cyber2019/work
22      COPY ./startup.sh /startup.sh
23      RUN tar zxvf /home/cyber2019/work/web0X.
            tar.gz -C /home/cyber2019/work
24      RUN chown -R cyber2019:cyber2019 /home/
            cyber2019 \
25          && echo "cyber2019 ALL=(ALL) ALL" >>
                /etc/sudoers \
26          && chmod +x /startup.sh
27      EXPOSE 22
28      CMD ["/startup.sh"]
```

A.1.1 起動スクリプト

```
1  #!/bin/bash
2  #tcpdump
3  tcpdump -C 1000 -Z root -w /var/log/research
       /`date "+%Y%m%d"`.pcap &
4
5  ##ssh
6  /usr/sbin/sshd -D
```