Vol.2021-CSEC-93 No.15
Vol.2021-IOT-53 No.15
2021/5/14

KAKOI: クラウドを利用したサイバーレンジをシンプルかつ安全に構築する新しいツール

寺嶋　友哉[1,a)]　仲山　昌宏[2]　横山 輝明[3]　小出　洋[4]

概要：サイバー攻撃の脅威は増加している．一方，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．サイバーレンジとは，実際の情報システムなどの環境を模擬したシミュレーション環境をセキュリティ演習用に再現して構築するシステムのことである．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高い演習効果が期待できる．しかしサイバーレンジを構築・運用するためにはネットワーク設計やサーバ構築などの高度な知識が要求されたり，煩雑な設定に手間がかかり容易ではない．本論文では筆者がクラウド上にサイバーレンジを構築するための負担を軽減することを目的として開発している KAKOI というツールを提案する．

KAKOI: A new tool to make simple and secure build cyber ranges using cloud environments

Tomoya Terashima[1,a)]　Masahiro Nakayama[2]　Teruaki Yokoyama[3]　Hiroshi Koide[4]

Abstract: The threat of cyber attacks is increasing year by year. On the other hand, there are not enough specialists for counterpart to the cyber attacks. Conducting cyber attack exercises for human resource development is effective because participants can experience how to deal with actual attacks. In the cyber attack response exercise, the exercise using cyber ranges can produce the situation close to the actual incident by constructing virtual environments and producing the real environments, so a high exercise effect can be expected. However, in order to build and operate the cyber ranges, advanced knowledge such as network design and server construction will be required, and complicated settings will be troublesome and not easy. So, in this paper, the authors propose a set of tools to reduce loads of building cyber ranges on cloud.

1. はじめに

本論文ではセキュリティ演習を実施する際の負担となるサイバーレンジの構築と運用をパブリッククラウドを活用し演習環境の構成をテンプレート化することで削減することを目的として筆者が開発している KAKOI というツールを提案し，評価までを行う．

1.1 目的

サイバー攻撃が発生した際に正しく対応することのできる知識や技術を持ったセキュリティ人材は慢性的に不足している．2020 年にはセキュリティ人材は約 19.3 万人の不足と試算 [1] されている．人材育成が進まない背景としてセキュリティ分野の教育の難しさがあげられる．セキュリティ分野の教育は専門的な知識や技術を要求されることが多い．そのため，適切な教材が用意することが難しく，教育に時間がかかる．セキュリティ教育における効果的な教育方法として演習を実施することが挙げられる．演習を実

[1] 九州大学大学院システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University
[2] 株式会社 WHERE
WHERE, Inc.
[3] 情報通信研究機構 ナショナルサイバートレーニングセンター
National Institute of Information and Communications Technology, National Cyber Training Center
[4] 九州大学情報基盤研究開発センター
Research Institute for Information Technology, Kyushu University
[a)] terashima.tomoya.988@s.kyushu-u.ac.jp

施して攻撃や防御の手法を実際に手を動かすことで体験することは高い教育効果が期待できる．セキュリティ演習を実施するためにはサイバーレンジという専用の環境を構築する必要がある．サイバーレンジとは，実際の情報システムなどの環境を模擬したシミュレーション環境をセキュリティ演習用に再現して構築するシステムのことである．しかし，サイバーレンジを用いた演習は高い学習効果が期待できる反面，サイバーレンジ構築や演習シナリオ作成など演習実施における負担が演習企画者，参加者共に大きく，演習を気軽に実施することが難しい．

本論文ではサイバーレンジをパブリッククラウド上に構築し，構成をテンプレート化することで構築，運用の負担を軽減するために開発している KAKOI を提案，評価することを目的とする．

1.2 セキュリティ演習環境構築ツール: KAKOI

KAKOI はクラウド上にサイバーレンジを構築するための構成管理ツールである．クラウド上にサイバーレンジを構築することにより資源や構成の管理にかかる負担を削減し，環境の再現性や拡張性を向上させることができる．また，KAKOI は演習環境の定義を yaml(https://yaml.org) ファイルに記述することでクラウド上にサイバーレンジを構築する際の構成や設定をテンプレート化することにより考慮事項や手順を削減することでサイバーレンジ構築にかかる負担を軽減する．

クラウド上に計算資源を構築する際に構成管理ツールを利用することは一般的である．構成管理ツールを利用することで宣言的に構築，運用を行うことが可能となり，設定の保存や拡張が容易となる．構成管理ツールの例として Terraform(https://www.terraform.io/) や Ansible(https://www.ansible.com/) がある．これらのような既存のツールを利用することで KAKOI が実現するサイバーレンジと同等の環境を構築することは可能である．しかし，既存のツールで構築する場合，設定ファイルの生成やクラウド資源の作成順序など，全ての資源や手順を宣言的に記述することはできない．また，既存の構成管理ツールは汎用的にクラウド資源を扱うことができるために選択肢が多く，設計において考慮すべき事項が増えてしまう可能性があり，既存の構成管理ツールの使用では必ずしもサイバーレンジ構築における複雑さを解消できていない．KAKOI はこれらの既存の構成管理ツール使用時に発生する複雑さを解消し，簡潔にサイバーレンジを構築できる．

1.3 評価

KAKOI を用いて構築した環境に対して接続性や環境に反映される設定の正確性，サイバーレンジ構築における利便性などについて検証を行った．KAKOI を用いて構築される演習環境への接続方法は VPN(Virtual Private Network) のみである．検証では VPN を経由して演習環境に接続できること，VPN 以外の手段では演習環境に接続できないこと，演習環境内部から外部の環境に接続できないことを確認した．KAKOI を使用してサイバーレンジを構築する手順は演習に使用する仮想マシンイメージのビルドと演習ネットワークの構築の２つの手順で構築できる．これは通常の手順と比較して大幅に手順を削減できていると考えられる．

2. サイバーレンジとその課題

サイバーレンジとは，実際の情報システムなどの環境を模擬したシミュレーション環境をセキュリティ演習用に再現して構築するシステムのことである．サイバーレンジを用いた演習では構築した演習用仮想環境内で対象となるシステムに対して実際に攻撃を行うことで攻撃手法や対処方法を学習することができる．

独立行政法人情報処理推進機構 (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，実際のセキュリティインシデントに近い状況を再現して演習を行うことができるため学習効果が高いと考えられる．

サイバーレンジは大きく演習用ネットワークと演習用サーバによって構成される仮想システムである．一般的な情報システムと異なる点は安全なサイバー攻撃やマルウェアの動作を目的として構築されるというところにある．そのため，安全性を確保するためインターネットなどの外部ネットワークから独立したネットワークとして構築される必要がある．さらに，演習用サーバは外部ネットワークに接続できない状態においても演習に必要となるソフトウェアなどを導入することが可能である必要がある．

サイバーレンジを構築する手法は様々存在する．最も一般的な手法は演習会場にネットワーク機器やサーバなどの物理機器を持参することで会場に隔離環境となるローカルネットワークを構築し，必要に応じてインターネットなどに接続して必要なソフトウェアを導入することでサイバーレンジを構築するという手法である．この手法はサイバーレンジを柔軟に構成，管理することができ，物理機器を使用することからより実環境に近い環境を再現できる．一方

で手作業によるオペレーションが複雑かつ大量である場合が多く，物理機器の用意，管理にコストが多くかかる．また，演習時に参加者はサイバーレンジが構築された演習会場に集合しなれば演習に参加することができない．

異なる手法として仮想環境上にサイバーレンジを構築する手法がある．クラウドなどの仮想環境上にサイバーレンジを構築し，安全な接続方法を用いてネットワーク越しに接続することで演習を実施することができる．さらに，仮想環境を利用する利点として環境の可用性と拡張性があげられる．物理機器を使用しないため資源をより柔軟に選択することができ，管理も容易となる．しかし，仮想環境上に構築する手法も同様に手作業や設定が複雑である場合が多く，ネットワーク上に構築することになるため安全性への配慮がより求められる．

このように，サイバーレンジの構築，運用はどの手法においても複雑である場合が多く，十分な知識や技術がなければ構築，運用を行うことが難しい．

3. 関連研究

3.1 Alfons: ビルディングブロック型模倣環境構築システム

マルウェア解析やサイバー攻撃演習の環境を支援する模擬環境構築システム Alfons が安田ら [4] により提案されてる．Alfons は国立研究開発法人情報通信研究機構（NICT）が運用する StarBED[5] という大規模ネットワークシミュレーション基盤において模擬環境におけるインスタンスの構築における手作業による人的コストの削減を目的として開発されている．

Alfons は模擬環境構築におけるテンプレートの管理，インスタンスの作成，設定を単一のシステムで管理することができる．演習時に模擬環境で使用する OS イメージはある程度共通であることが多いため，ベースとなる OS イメージをテンプレート化し，各アプリケーションサーバなどで必要となる差分を挿入することでイメージを作成することができる．Alfons では yaml, XML 形式の論理構成ファイルを基準に物理リソースの割り当てから環境への配置までを CLI(Command Line Interface) により実行することができる．これにより環境の再構築や一部改変での再利用などを容易に行うことができる．

これまでに，Alfons を利用して文部科学省の教育プログラムである enPiT-Security(https://www.seccap.jp/) や WASForum Hardening Project 実行委員会が開催する Hardening Project(https://wasforum.jp/hardening-project/) にて大規模な演習用の環境を構築する際に使用されている．Alfons は演習や検証に使用する環境の構築時の負担を軽減し，管理を容易にしている．

Alfons はサイバーレンジにおける演習サーバ (インスタンス) を作成する機能を有したツールである．論理構成定義をファイルに記述することでサイバーレンジの構築，管理を容易にしている．一方，Alfons は StarBED での運用を前提として開発されており，他の環境で利用することが難しく，StarBED のような特別な環境を持たないような組織，個人がサイバーレンジを構築する負担は軽減されていない．

3.2 CyRIS: A Cyber Range Instantiation System for Facilitating Security Training

サイバーレンジの構築における手作業の負担を軽減するために CyRIS というツール [6] が提案されている．CyRIS は北陸先端科学技術大学院大学が開発するセキュリティトレーニング支援システムである CyTrONE[7] の構成要素である．

CyRIS は構成管理ツールとして動作し，一般的な構成管理ツールに存在する機能の他にセキュリティインシデントを再現して設定するセキュリティ機能が存在する．サイバーレンジのネットワーク構成や演習ノードの OS といった基本的な設定から DDoS 攻撃やマルウェアのエミュレーション，トラフィックのキャプチャ設定などのセキュリティ機能を設定して構築を行うことができる．また，セキュリティ演習では脆弱性のあるバージョンのソフトウェアを動作させなければならない場合がある．そのようなソフトウェアのバージョンは一般的なパッケージとして配布されていない場合が多い．CyRIS はそのような場合にバージョンを指定してソースからインストールする機能を有している．CyRIS はサイバーレンジにおけるネットワーク構成の管理から演習ノードに配置するソフトウェアの管理までを宣言的な定義によって実現している．

CyRIS は上述した Alfons と比較してサイバーレンジにおけるネットワーク構成やノードの配置といった役割を担うツールである．ネットワーク構成の定義やノードの配置，ソフトウェアの供給を機能として有している．CyRIS はセキュリティ演習のための独自機能として攻撃のエミュレーション機能を有している．一方，CyRIS は Alfons と同様に StarBED での運用を前提として開発されている．そのため，特別な環境を持たない組織，個人がサイバーレンジを構築する負担は軽減されていない．

3.3 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

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 [3] 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プライベートな環境に接続して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．また，RDP 接続をするための PC を演習システム内に用意しなければならず，費用や資源面で負担が大きい．

4. KAKOI の提案

本章ではパブリッククラウド上にサイバーレンジの構築を支援するツールである KAKOI について詳しく説明する．

4.1 概要

KAKOI はサイバーレンジをクラウド上に構築するための構成管理ツールである．

サイバーレンジにおける構成管理ツールとして前章で Alfons と CyRIS を紹介した．Alfons や CyRIS が特別な実験基盤上にサイバーレンジを構築するためのツールであるのに対して，KAKOI はパブリッククラウド上にサイバーレンジを構築するためのツールである．パブリッククラウドを使用することにより誰でもサイバーレンジを構築することができる．

KAKOI では，yaml 形式でサイバーレンジの論理構成を定義し KAKOI に入力として渡すことによりクラウド上に定義したコンピューティング資源が作成される．KAKOI はサイバーレンジ構築における複雑さや負担の大きさをテンプレート化と自動化により軽減する．

サイバーレンジの重要な要件である外部ネットワークとの隔離を実現する手法はいくつか存在するが，KAKOI ではクラウドサービスが提供する VPC(Virtual Private Cloud) を使用し，独立した演習用ネットワークへの安全な接続方法として VPN(Virtual Private Network) を使用することでテンプレート化する．前章では RDP を使用したネットワーク越しの演習について紹介した．これに対し，VPN を使用する手法は演習参加者が各自の端末からサイバーレンジに接続することができ，通信量や設定などの負担を軽減することができる．また，設計をテンプレート化することによりユーザーの設計における考慮事項を削減し，安全にサイバーレンジを構築することができる．さらに，テンプレート化することにより，構築時に必要となる設定を自動化することができる．

4.1.1 パブリッククラウドサービス

パブリッククラウドサービスとはインターネット経由で様々なコンピューティング資源を利用することのできるサービスである．代表的なパブリッククラウドサービスに Amazon 社の Amazon Web Service(AWS)，Google 社の Google Cloud Platform，Microsoft 社の Microsoft Azure などがある．クラウドサービスを利用することの利点として，物理機器の使用に伴う費用や調達における手間や運用にかかる手間を削減することができる．また，各クラウドサービスが提供，管理するソフトウェアサービスを利用することでユーザーは管理を最小限に止め，柔軟に環境を構築することができる．KAKOI は現在 AWS を対象として開発を行っており，VPC や VPN サービスといった様々な AWS が提供するサービスを連携させることでサイバーレンジを構築，管理する．

4.1.2 構成管理ツール

構成管理ツールとは情報システムを一貫性のとれた望ましい状態に保つためのツールである．一貫性のとれたシステム設定をコードとして定義することによって大規模なシステム構成であっても管理者はシステムがどのような状態であるかを簡単に管理することができる．また，構成管理を行うことで環境の違いによる問題の発生を防ぐことができ，正しい構成により環境を複製することができる．

代表的な構成管理ツールとして RedHat 社の Ansible や HashiCorp 社の Terraform，Amazon 社の AWS CloudFormation などが存在する．ツールによって提供している機能や管理対象となるコンピューティング資源は様々である．特に，クラウド資源を管理するツールとして Terraform や AWS CloudFormation がある．これらは構成定義をファイルとして記述することでクラウド資源を宣言的に管理することができる．KAKOI も同様にクラウド資源を構成管理することが必要であるため，バックグラウンドに Terraform を採用してクラウド資源の管理を行っている．

Terraform をバックグラウンドに利用することによりクラウド資源を柔軟に管理することができる．また，Terraform は様々なクラウドサービスに対応しているためクラウドサービスによる差異を吸収し，共通化することが容易となる．

4.1.3 VPN

VPN 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．

4.1.4 クラウドと VPN を利用したサイバーレンジ

KAKOI はサイバーレンジの構成をテンプレート化することによってユーザーである演習企画者の負担を削減する．設計の負担軽減のため，KAKOI はサイバーレンジにおける隔離ネットワークをクラウドサービスが提供する VPC を使用し，環境内への安全な接続方法として VPN を使用する．

筆者は以前，パブリッククラウドと VPN を使用したサイバーレンジ構築手法を提案，評価した [8]．その際に評価実験として SECCON Akihabara 2019 にて AWS 上に構築した演習システムを使用した演習を実施した．実験の結果，問題なく演習を実施することができた．このことから，パブリッククラウドと VPN を利用したサイバーレンジは運用可能である．したがって，KAKOI における隔離ネットワークの実現に本手法を採用している．

4.2 特徴

KAKOI は図 1 に示すように一般的な構成管理ツールと同様にユーザーとなる演習企画者が自身の端末で構成を記述し，実行することでサイバーレンジを構築する．
現在，KAKOI は以下のコマンドを実行することでサイバーレンジを構築，管理する．

(1) init
定義に基づいて演習用サーバのための仮想マシンイメージをクラウド上に作成する．

(2) create
init の結果と定義に基づいて演習用ネットワークの作成，演習用サーバの配置を含めたサイバーレンジの構築を行う．

(3) destroy
構築したサイバーレンジを破壊する．

4.2.1 演習環境定義記述

KAKOI はサイバーレンジを yaml 形式の定義記述で管理する．定義記述は以下のセクションに分かれている．

- provider
  provider セクションではサイバーレンジを構築するクラウドサービスと構築するリージョン，クラウド資源を使用するアカウントを定義する．
- service
  service セクションではサイバーレンジの構成を定義する．演習用ネットワークの定義と演習用サーバの定義のサブセクションにより構成される．
  - network
    network セクションにて演習用ネットワーク構成の定義を行う．演習用ネットワークとして VPC のアドレス範囲を定義することで大元となるネットワークを構築する．subnet として演習ネットワーク内でサブネットワークを定義する．サブネットワークを演習ネットワーク内に定義することで企業ネットワークなどの複数のサブネットワークから構成されるネットワークを柔軟に定義することができる．また，KAKOI ではサイバーレンジへの接続手段として VPN を使用するため，vpn_gateway で VPN の設定を定義する．
  - hosts
    hosts セクションにて演習用サーバの定義を行う．演習用サーバは配置するサブネットワークやクラウド上に作成するインスタンスのサイズ，同一サーバの配置数などを定義することができる．演習用サーバとして起動する仮想マシンは init コマンドにより作成される仮想マシンイメージを使用する．init コマンドのより作成される仮想マシンイメージユーザーである演習企画者が自身の端末から既に出来上がっている仮想マシンイメージをアップロードする方法と定義記述にシェルスクリプトを基に仮想マシンイメージをクラウド上で作成する方法の二つの手段をサポートしている．

以下に定義記述の例を示す．

```
1  provider:
2  name: "aws"
3  profile: "example-profile"
4  region: "ap-northeast-1"
5  service:
6  name: "example"
7  network:
8    name: "example-network"
9    range: "10.10.0.0/16"
10   subnets:
11   - name: "subnet1"
12     range: "10.10.10.0/24"
13     private: true
14     vpn_gateway_associated: true
15     routes:
16     - from: "0.0.0.0/0"
17       to: "10.10.10.0/24"
18   - name: "subnet2"
19     range: "10.10.20.0/24"
```

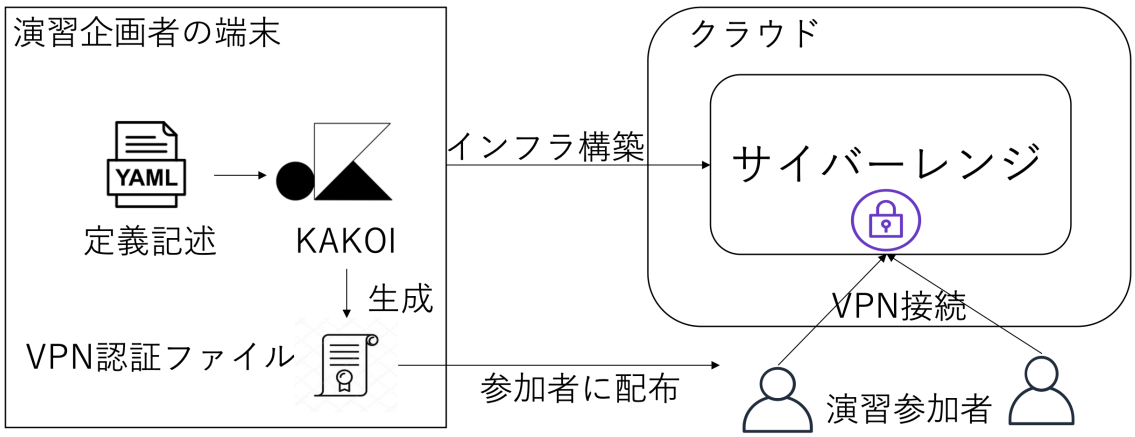

図 1 KAKOI 動作図.
Fig. 1 KAKOI operation flow.

```
20      private: true
21      routes:
22      - from: "0.0.0.0/0"
23        to: "10.10.20.0/24"
24    vpn_gateway:
25        range: "10.10.30.0/22"
26        domain: "example.com"
27        associated_subnet: "subnet1"
28  hosts:
29    key:
30    name: "example-key"
31    servers:
32    - name: "example-host1"
33      subnet: "subnet1"
34      image:
35      image_path: "~/example-host1.ova"
36    - name: "example-host2"
37      subnet: "subnet2"
38      image:
39      custom: true
40      scripts:
41        - "example-host2.sh"
```

この定義記述例によって構築されるサイバーレンジの概要図が図 2 である．例示した定義記述例では演習用ネットワークとして二つのサブネットワークを持ったネットワークを構築し，その中に一つずつサーバが配置されている．

4.2.2 演習ネットワークの構築

サイバーレンジを構築する上で重要な要素の一つが演習用ネットワークの構築である．KAKOI は入力として与えられた定義記述に基づき演習用ネットワークを自動で構築する．KAKOI によって構築されるネットワークはクラウドサービスによって提供される VPC(Virtual Private Cloud) である．クラウド上に構築された VPC はインターネットへの接続手段を持たず，独立したネットワークとして構築することができる．VPC の中でサブネットワークを切り分けることにより柔軟に演習を実施するために必要なネットワークを表現する．

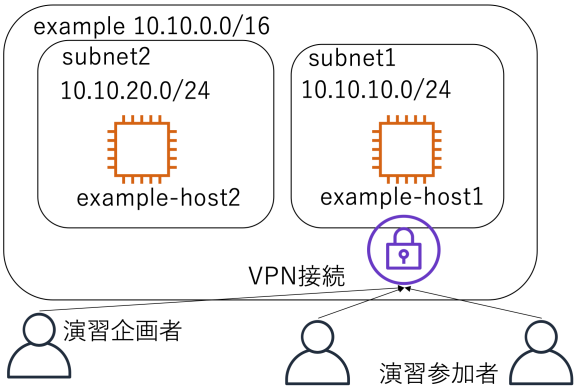

図 2 例示した記述から構築されるサイバーレンジの概要図.
Fig. 2 Overview of cyber range made from example.

一方，VPC はインターネットに接続されないため，演習参加者が安全にサイバーレンジに接続するための手段として VPN ゲートウェイを使用する．演習実施者は KAKOI によって生成される VPN 接続用の認証ファイルを演習参加者に配布し，VPN によって安全な接続手段を提供する．KAKOI は VPC と同様に VPN ゲートウェイも自動で構築する．VPN ゲートウェイの構築は一般的に手順や設定ファイルが多く，複雑である．KAKOI はこの複雑さを解消するために VPN ゲートウェイの設定を range, domain, associated_subet の三つのフィールドのみで可能である．構築に必要なクラウド資源の設定や作成，独自証明書の生成を自動で行うことによりユーザーの負担を軽減している．

4.2.3 演習サーバの構築

サイバーレンジを構築する上でもう一つの重要な要素が演習用サーバの構築である．KAKOI により構築されるサイバーレンジは内部からインターネットに接続できない．したがって，演習用サーバはサイバーレンジ内に配置された後に必要なソフトウェアやコンテンツを外部から取得す

ることができない．KAKOI はサイバーレンジ内に配置する前に予め演習サーバに必要となるパッケージやコンテンツを事前に導入した仮想マシンイメージを作成することで解決している．KAKOI は仮想マシンイメージ作成に対して二つの手段をサポートしている．

一つはユーザー自身が予め保持している仮想マシンイメージをクラウド上にアップロード，適切なフォーマットに変換する手法である．この手法は既存の仮想マシンイメージを利用して演習用サーバを構築することができる．しかし，ユーザー自身の端末から仮想マシンイメージをアップロードするため，使用するネットワークによっては実行に非常に時間がかかる場合がある．

もう一つはユーザーが演習用サーバを構成するために実行すべきコマンド群を記述したシェルスクリプトのファイルを指定することで，そのファイルを基に仮想マシンイメージを作成する手法である．この手法はユーザーが自由に演習用仮想マシンイメージを作成することができる．また，仮想マシンイメージの作成はクラウド上で実行される．

さらに，演習用サーバは同一イメージのサーバを複数台配置したり，配置するサーバのサイズをクラウドサービスの規格にしたがって選択したりすることができる．これらのパラメータは定義記述ではデフォルト値が設定されており，特に指定する必要なく実行することができる．

5. 評価

本章では KAKOI によるサイバーレンジの構築手順と KAKOI によって構築されるサイバーレンジを評価する．評価のために図 3 に示す環境を KAKOI を用いて構築した．

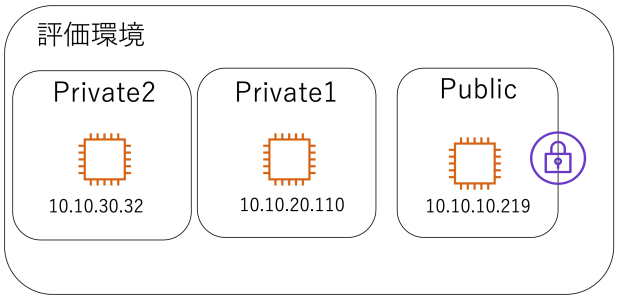

図 3 評価環境の構成図.
Fig. 3 evaluation environment.

5.1 構築時における評価

KAKOI はクラウド資源の構築に Terraform とクラウドサービスの API コールを使用しており，同様の構成を Terraform やクラウドサービスのコンソール操作などにより KAKOI を使用することなく構築することも可能である．本項では KAKOI を使用した場合に構築にかかる手順や作成すべき設定ファイルなどと KAKOI を使用しなかった場合に同様の構成を構築するために必要な手順，設定ファイルなどを比較，評価した．ここで，KAKOI を使用しない場合とは KAKOI のバックグラウンドで実行する Terraform やクラウドサービスの操作を個別に行う場合のことを指す．

5.1.1 構築手順

はじめにサイバーレンジ構築における手順について評価した．KAKOI を用いた構築手順は以下である．

(1) サイバーレンジ構成定義ファイル，仮想マシンイメージ作成のためのスクリプトの記述
(2) init コマンドによる仮想マシンイメージの作成
(3) create コマンドによるサイバーレンジの構築
(4) 生成される VPN 接続用ファイルを参加者に配布

KAKOI を使用しない場合の構築手順は以下である．

(1) 仮想マシンイメージ作成のためのスクリプト，Terraform，その他設定ファイルの作成
(2) 仮想マシンイメージ作成のためのクラウド資源の作成 (Terraform 実行)
(3) 仮想マシンイメージの作成と確認
(4) サイバーレンジ構成を記述した Terraform のファイル記述
(5) 演習用サーバ接続のための鍵や VPN のための証明書類の発行
(6) サイバーレンジの構築 (Terraform 実行)
(7) VPN 接続用ファイルの作成
(8) 生成される VPN 接続用ファイルを参加者に配布

二つの手順を比較すると KAKOI を用いた場合，手順が大幅に削減されていた．KAKOI を使用しない場合，Terraform の使用やクラウドサービスのコンソール操作，コマンドライン操作によるファイルの生成など複数のサービスを組み合わせた構築手順となる．これは様々なサービスの知識が必要とされるため，考慮すべき事柄が多くユーザーがサイバーレンジの構成に集中することを妨げてしまう．一方，KAKOI は手順が削減され，単一のツールとしてサイバーレンジの構築が完結するため，ユーザーはサイバーレンジの構成により集中することができる．

5.1.2 記述・ファイル量

次に KAKOI を使用する場合とそうでない場合に必要となる設定ファイルやその記述量を評価した．表 1 に示すように，評価環境を KAKOI を用いて構築するために必要となる設定ファイルは定義記述ファイルのみであった．一方，KAKOI を使用しない場合評価環境を構築するために必要となる Terraform の設定ファイルを 350 行記述しなければならなかった．また，KAKOI を使用しない場合構築に際して以下のようなファイルを生成する必要がある．

- 演習用サーバ SSH 用公開鍵・秘密鍵
- VPN ゲートウェイ認証用証明書

- VPN 接続用認証ファイル
- 仮想マシンイメージ作成用設定ファイル

これらのファイルは KAKOI では実行時に自動生成されるためファイルの生成や手順の間違いによってエラーが発生する可能性を削減している．

表 1 ファイル数・記述量の比較.
Table 1 comparison of files and descriptions.

手法	ファイル数	形式	合計行数
KAKOI 使用	1	yaml	50 行
KAKOI 不使用	16	Terraform	350 行

KAKOI は yaml 形式の定義記述ファイルからサイバーレンジ構築のために必要な値を取り出しバックグラウンドで動作する Terraform などに値を渡す．

yaml 形式に設計を構造化することによりサイバーレンジを構築する上での柔軟性が低下するという欠点がある．一方で記述すべきファイルの数やその量が削減でき，設計を大幅に簡略化することができる．また，設計を構造化して考慮事項を減らすことにより設計時のミスが発生する箇所も削減することができる．

5.2 サイバーレンジの接続性における評価

本項では KAKOI を使用して構築した評価環境がサイバーレンジとして運用するために要求される接続性について評価した．サイバーレンジは環境内で攻撃を行ったりマルウェアを動作させたりするためインターネットなどの外部ネットワークから独立したネットワークとして構築する必要がある．KAKOI はこの要件を満たす演習用ネットワークをクラウドサービスが提供する VPC と VPN を利用して実現する．KAKOI を使用して構築した評価環境に対して以下の検証を行った．

- VPN 接続なしでサイバーレンジに接続できない
- VPN 接続ありでサイバーレンジ内の各サブネットワークに接続できる
- VPN 接続ありでサイバーレンジ内の VPN ゲートウェイが配置されていないサブネットワークに直接接続できない
- サイバーレンジ内から外部ネットワーク (インターネット) に接続できない

接続性の検証には ping コマンドを使用し，評価環境内のサーバへのログインは VPN 接続を行った上で SSH を用いて行った．検証の結果，全ての項目において意図した結果が得られた．

これにより，KAKOI を使用して構築するサイバーレンジが外部ネットワークとの接続性を分離しつつ，演習参加者は VPN を用いた安全な接続手段を用いて接続することが可能であることがわかった．

6. おわりに

本論文ではクラウドを利用することでサイバーレンジ構築，運用における複雑さを解消し，シンプルかつ安全にサイバーレンジを構築するためのツールである KAKOI を提案した．KAKOI はサイバーレンジ構築，管理用の構成管理ツールである．クラウド上にサイバーレンジを構築することでコンピュータ資源をより柔軟に使用することができ，構成の管理にかかる負担を削減することができる．KAKOI はサイバーレンジの設計をテンプレート化することによって設定を簡略化し，ユーザーが設計について考慮するべき事項，構築における手順を削減する．

本論文では KAKOI がサイバーレンジ構築における複雑さを解消していること評価として KAKOI を使用した場合と使用しなかった場合でのサイバーレンジ構築の手順や設定ファイルの記述量に関して比較した．比較の結果，構築手順や設定ファイルの記述量，使用数などにおいて削減されており，サイバーレンジ構築における複雑さが軽減された．また，KAKOI を使用して構築した演習環境がサイバーレンジとして運用するために必要なネットワークの分離が行われているか検証した．検証の結果，要求されるネットワークの分離が行われていることを確認した．

既存の手法によるサイバーレンジ構築，管理における課題は手順や設定が複雑で十分な知識や技術がなければ構築，管理することが難しいという課題があった．KAKOI は評価の結果よりその複雑さを解消し，簡潔かつ安全にサイバーレンジを構築することを可能にしていると言える．

現在 KAKOI は yaml 形式の定義記述からクラウド上にサイバーレンジを構築し，破棄する機能を有している．一方，実現していない機能が多数存在する．構成管理ツールとして，動的な環境の状態管理や構築した環境を監視，検証する機能を実装する必要がある．

今後はサイバーレンジ構築，管理のための構成管理ツールとして機能を充実させることを進める．また，シナリオ作成や演習時の状態管理など，演習を補助する機能のサポートも検討している．

謝辞

本研究の一部は，NICT SecHack365 (https://sechack365.nict.go.jp/)，NII SINET 広域データ収集基盤実証実験，科研費（21K11888）の助成を受けたものである．

参考文献

[1] 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, https://www.soumu.go.jp/main_content/000591470.pdf (2021/4/7 参照).
[2] 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, pp. 25-32, https://www.ipa.go.jp/files/000025350.pdf

(2006).
[3] 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).
[4] 安田 真悟:ビルディングブロック型模倣環境構築システム Alfons とその応用事例〜セキュリティ検証環境構築基盤と人材育成への貢献〜, 情報通信研究機構研究報告 (2016).
[5] 宮地 利幸, 中田 潤也, 知念 賢一,Razvan Beuran, 三輪 信介, 岡田 崇, 三角 真, 宇多 仁, 芳炭将, 丹 康雄, 中川 晋一, 篠田 陽一:StarBED：大規模ネットワーク実証環境 (2008).
[6] Razvan Beuran,Dat Tang,Cuong Pham,Ken-ichi Chinen,Yasuo Tan,Yoichi Shinoda: Cybersecurity Education and Training Support System: CyRIS, IEICE Transactions on Information and Systems, Vol. E101.D, No. 3, pp. 740-749 (2018).
[7] Razvan Beuran,Dat Tang,Cuong Pham,Ken-ichi Chinen,Yasuo Tan,Yoichi Shinoda:Integrated framework for hands-on cybersecurity training: CyTrONE,Computers & Security (2018).
[8] 寺嶋 友哉, 小出 洋: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，情報処理学会火の国シンポジウム 2020 予稿集 (2020).