

## セキュリティ演習環境構築ツール 開発駆動コース 仲山ゼミ 寺嶋友哉

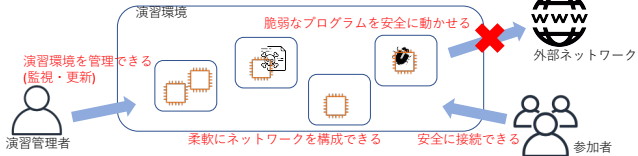


### Motivation

セキュリティ演習の構築・運用をシンプルに!

### Background

セキュリティ演習環境とは?



セキュリティ演習環境構築の課題

複雑で考えることが多い

設計・安全性の確保・管理・コスト etc..

設計不備  
大変さ

専門家(詳しい人)がいないと気軽かつ安全に演習ができない!

### KAKOI

#### Concept

演習環境構築の複雑さを減らして簡単に!

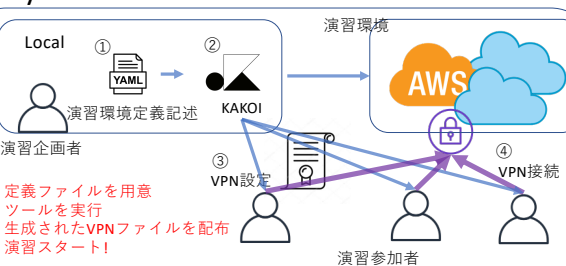
構成のテンプレート化・自動生成

設計の考慮事項  
構築時の手順  
DOWN

安全性  
環境の再現性  
UP

Public Cloud **X** Infrastructure as Code

#### System



1. 定義ファイルを用意
2. ツールを実行
3. 生成されたVPNファイルを配布
4. 演習スタート!

#### Features

デモで使った環境の場合

- tfファイル**
  - finaldemo-key.tf
  - finaldemo-kakoi.terassyi.net.tf
  - image\_builder-finaldemo-target.tf
  - image\_builder-finaldemo-web.tf
  - image\_builder-finaldemo-worker.tf
  - image\_builder-finaldemo-target-0.tf
  - image\_builder-finaldemo-worker-0.tf
  - image\_builder\_role.tf
  - provider.tf
  - s3.tf
  - kakoi-finaldemo-target-0.tf
  - kakoi-finaldemo-web-0.tf
  - kakoi-finaldemo-worker-0.tf
  - kakoi-vpn.tf
  - subnet-private1.tf
  - subnet-private2.tf
  - subnet-public.tf
  - terraform.tfstate
  - terraform.tfstate.backup
  - vpc-finaldemo.tf
- サーバー鍵**
  - finaldemo-key.pem
  - finaldemo-key.pub
- 証明書**
  - ca.finaldemo.kakoi.terassyi.net.crt
  - ca.finaldemo.kakoi.terassyi.net.key
  - client.finaldemo.kakoi.terassyi.net.crt
  - client.finaldemo.kakoi.terassyi.net.key
  - server.finaldemo.kakoi.terassyi.net.crt
  - server.finaldemo.kakoi.terassyi.net.key
- VMビルドファイル**
  - finaldemo-target
    - buildspec.yml
    - image\_builder.json
  - finaldemo-web
    - buildspec.yml
    - image\_builder.json
  - finaldemo-worker
    - buildspec.yml
    - image\_builder.json

隔離環境をVPC+VPNに限定  
設計における考慮事項を削減  
VPNに必要な設定を自動化することで負担削減

演習用サーバー構築の自動化

鍵の自動生成  
VMイメージビルドの自動化

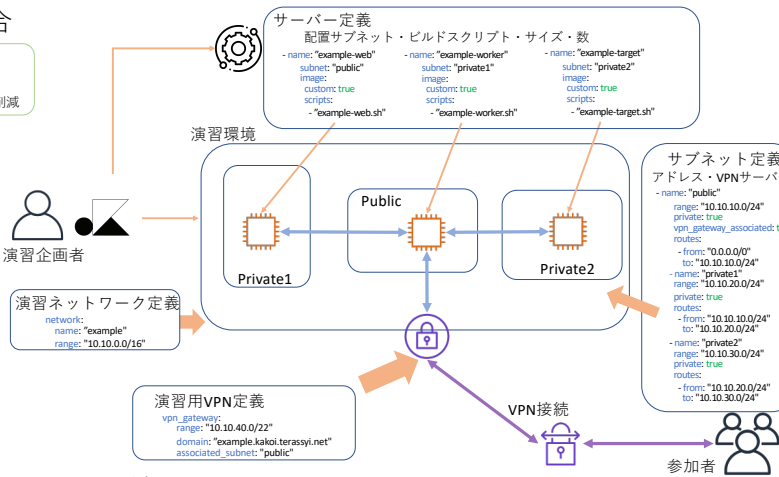
KAKOIを使用すると  
必要だったファイルが一つにまとまる

example.yml

演習ネットワーク定義  
サブネットワークを自由に定義可能

演習VPN定義  
VPN接続時の使用可能アドレス  
VPNにしようとする証明書ドメイン  
配置するサブネット

演習サーバー定義  
配置するサブネット  
サーバーサイズ  
台数  
ビルド(2パターン指定可能)  
イメージのパス  
スクリプトのパス



KAKOIが実現したこと

- Public Cloud と Infrastructure as Code を用いて...
- 演習環境をテンプレート化
- 設定ファイルの自動生成
- 構築の自動化
- 記述量の削減

ユーザーが考慮すべき事項を削減し  
構築における複雑さを解消、  
設計不備の危険性を削減!!

演習環境の表現力とのバランスを保ちつつ環境構築をシンプルにすることができた

#### Use Setup

1. ビルド (Required Go >= 1.13)
 

```
$ git clone https://github.com/terassyi/kakoi
$ cd kakoi
$ sudo ./setup.sh
```
2. AWS Credentialファイル作成

#### Command

Init: VMビルド	\$ kakoi init -p example.yml
Create: 演習インフラ作成	\$ kakoi create -p example.yml
Destroy: 演習インフラ破壊	\$ kakoi destroy -p .kakoi

#### Procedure

1. 演習環境の定義記述をymlで記述
2. Initコマンドで使用するイメージをビルド
3. Createコマンドで演習環境を構築
4. 生成されるVPN接続ファイルを配布して演習開始
5. 終了したらDestroyコマンドで環境を破壊

### Future Work

演習環境管理・検証機能サポート  
演習環境へのssh機能  
構築時の環境検証機能

シナリオ作成支援機能サポート  
演習に使用する脆弱性の管理機能  
バージョン指定でのソフトウェアインストール機能

他のクラウドへの対応  
使用できるプラットフォームの追加

演習環境構築・運用の複雑さを解消しより気軽かつ安全に演習を実施することができるように開発を継続

