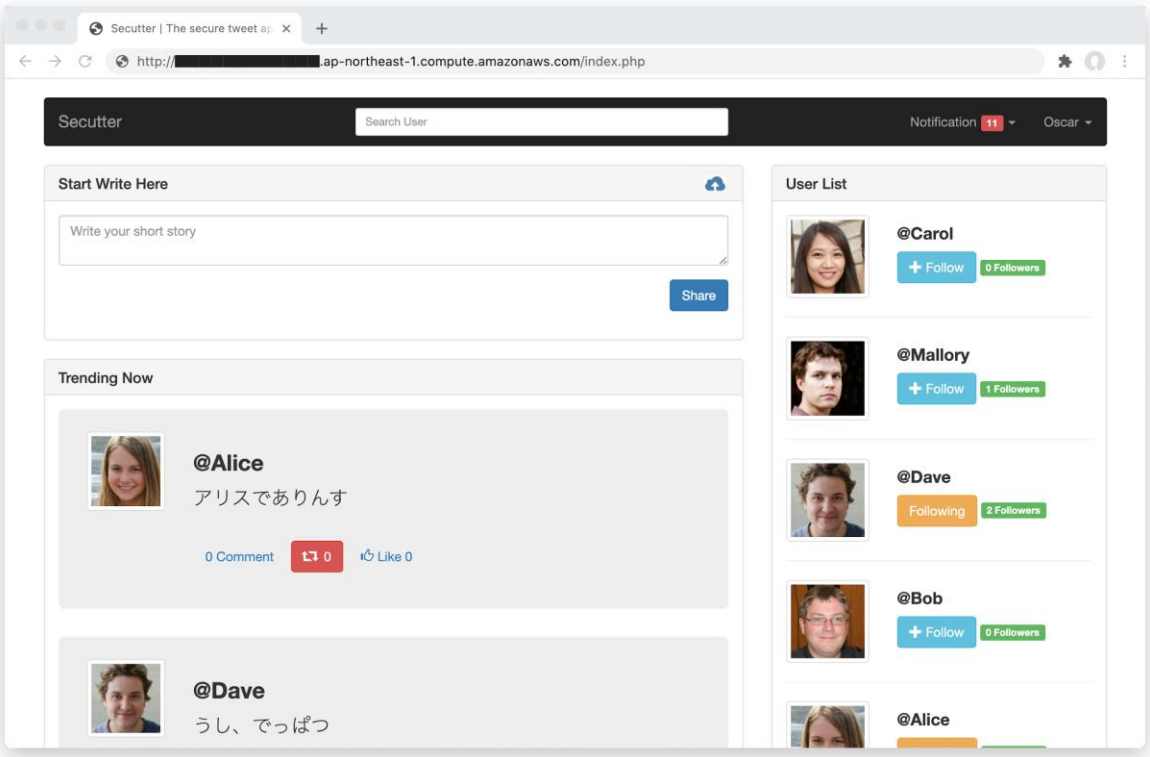
とある診断員とSecurity-JAWS #02

イベント事前配布資料

システム概要

講義の中で登場するWebサイト「Secutter」は、セキュアなつぶやきを投稿できるSNSアプリケーションです。



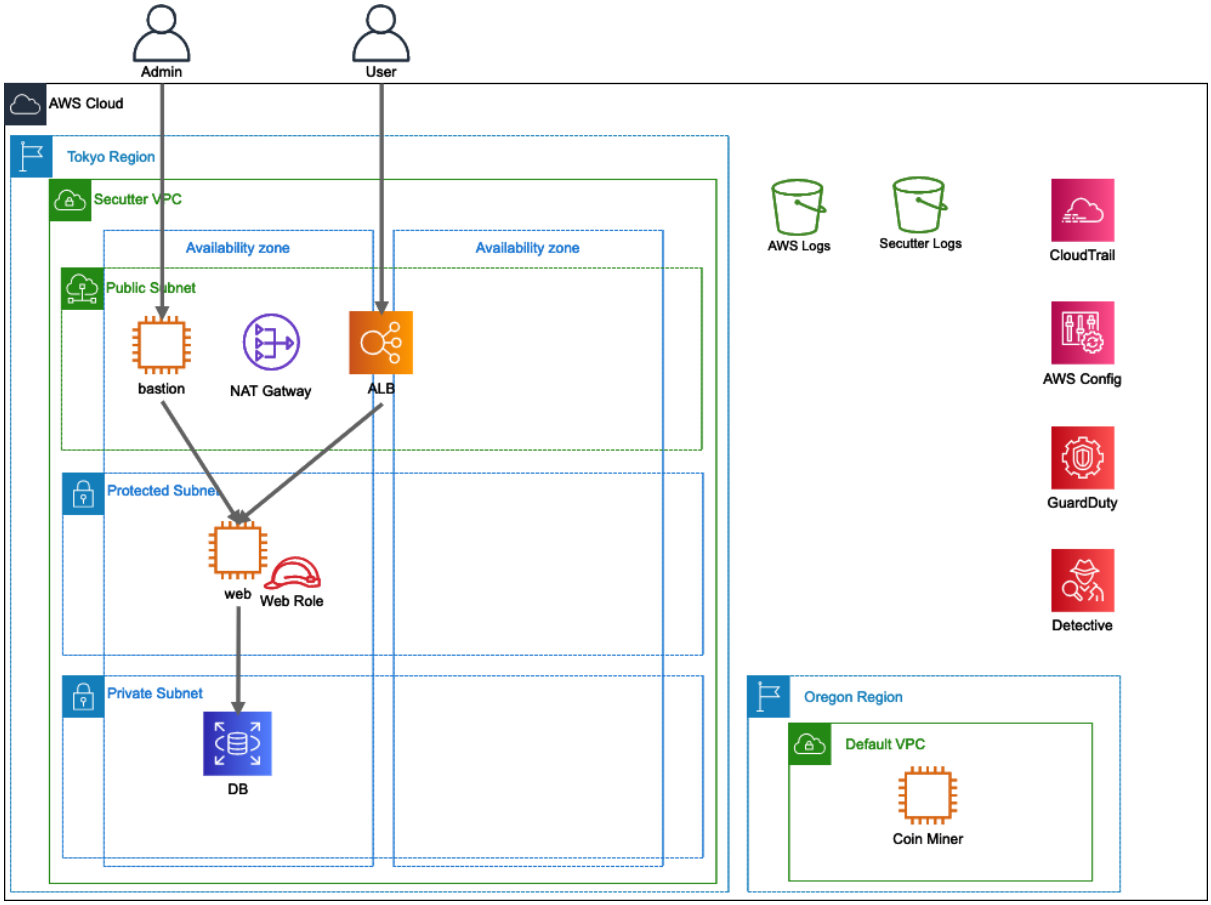
Secutterには、以下のような機能が存在しています。

- IDとパスワードによるログイン

- プロフィール画像の設定
- 画像を含めたつぶやきの投稿
- 他ユーザーのつぶやきへのいいね

AWS環境説明

- 構成図



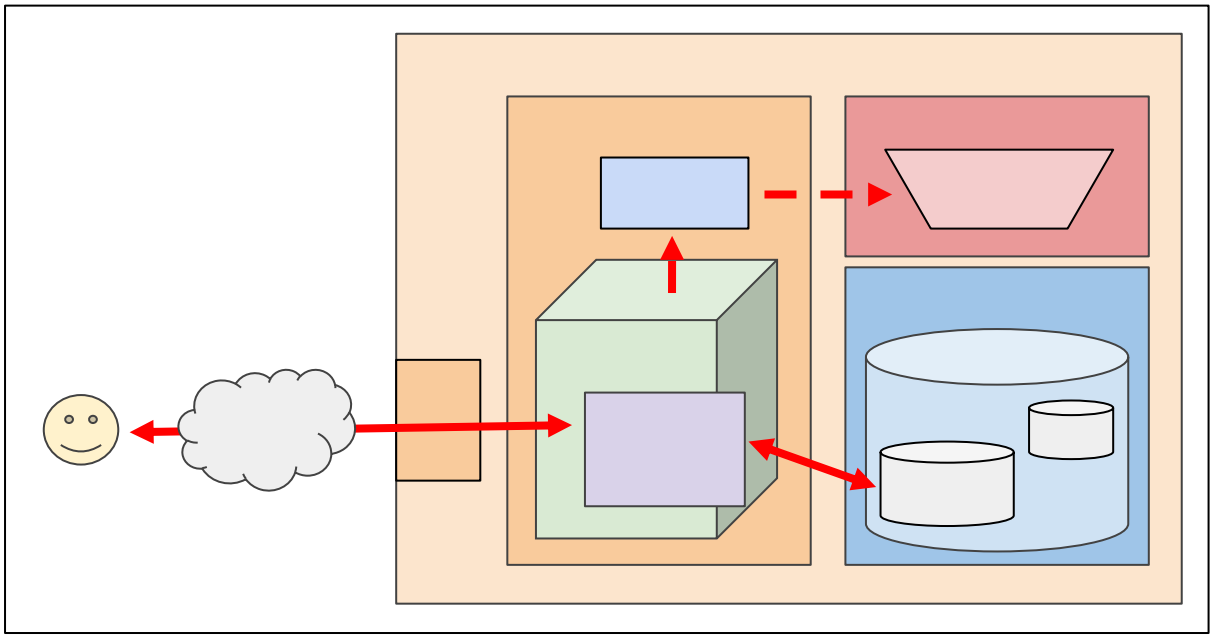
- 構成要素
  - ○ ALB
    - ■ Name: secutter-prd-ALB
    - ■ DNS: secutter-prd-ALB-1797007934.ap-northeast-1.elb.amazonaws.com
  - ○ Webサーバー(EC2)
    - ■ Name: secutter-prd-web

        - インスタンスID: i-0e6921bc7de8aa9e9
        - IP: 10.0.30.91
        - IAM Role: read-s3-ec2-role
    - RDS
        - Name: secutter-prd-db
        - DNS: secutter-prd-db.chch2ezj5tkn.ap-northeast-1.rds.amazonaws.com
        - エンジン: MySQL5.7
    - bastion(EC2)
        - 踏み台サーバー
    - IAM Role
        - Name: read-s3-ec2-role
        - EC2用のRole
        - S3やSecretsManagerなどが読み込める権限がアタッチされています。
    - AWS Logs(S3)
        - Name: awslogs-xxxxxxxxxxxx
        - CloudTrail / Configのログが保存されています。
    - Secutter Logs(S3)
        - Name: secutter-logs-xxxxxxxxxxxx
        - ALB / Nginxのログが保存されています。
    - その他
        - IAM User: ke-ni-, tigerszk, akaの3つは管理者ユーザーであり、このユーザーの操作ログはインシデントには関係ありません。
        - マネージドプレフィックスリストは必要なもののみ作成、アタッチしており変更されていません。

- super-developer(人物名兼IAM User名)が環境構築にあたり、色々作業を行っていたようですが、管理者は詳細を把握していないようです。
- 管理者の把握していないリソースも存在する可能性があります。
- Secutterの構成要素についてはap-northeast-1（東京）リージョンで作成されています。

アプリケーション説明

Secutterは、PHPで実装されたWebアプリケーションです。WebサーバーにはNginxを採用し、Nginxで発生するログはfluentdを経由してS3バケットに保存しています。また、DBサーバーにはMySQLを採用しています。MySQLには「testing」と「credit」という2つのデータベースが存在します。「testing」ではSecutterが利用する全てのデータを管理しています。一方、「credit」で管理しているデータは別のサービスが利用するものであり、このデータをSecutterは利用しません。



MySQL上の各データベースに存在するテーブルは以下の通りです。

データベース名：testing

テーブル名：tbl_comment

カラム名	データ型	Not Null	主キー	属性	説明
comment_id	int(11)	○	○	AUTO_INCREMENT	コメントの識別子
post_id	int(11)	○			コメントされたツイートの識別子
user_id	int(11)	○			コメントしたユーザーの識別子
comment	text	○			コメントの内容
timestamp	datetime	○			コメントした日時

テーブル名：tbl_follow

カラム名	データ型	Not Null	主キー	属性	説明
follow_id	int(11)	○	○	AUTO_INCREMENT	フォローの識別子
sender_id	int(11)	○			フォローされたユーザーの識別子
receiver_id	int(11)	○			フォローしたユーザーの識別子

テーブル名：tbl_like

カラム名	データ型	Not Null	主キー	属性	説明
like_id	int(11)	○	○	AUTO_INCREMENT	いいねの識別子
user_id	int(11)	○			いいねしたユーザーの識別子
post_id	int(11)	○			いいねされたツイートの識

					別子

テーブル名：tbl_notification

カラム名	データ型	Not Null	主キー	属性	説明
notification_id	int(11)	○	○	AUTO_INCREMENT	通知の識別子
notification_receiver_id	int(11)	○			通知されたユーザーの識別子
notification_text	text	○			通知の内容
read_notification	enum('no','yes')	○			通知が読まれたか否か

テーブル名：tbl_repost

カラム名	データ型	Not Null	主キー	属性	説明
repost_id	int(11)	○	○	AUTO_INCREMENT	リツイートの識別子
post_id	int(11)	○			リツイートされたツイートの識別子
user_id	int(11)	○			リツイートしたユーザーの識別子

テーブル名：tbl_samples_post

カラム名	データ型	Not Null	主キー	属性	説明
post_id	int(11)	○	○	AUTO_INCREMENT	ツイートの識別子
user_id	int(11)	○			ツイートしたユーザーの識別子
post_content	text	○			ツイートの内容

post_datetime	datetime	○			ツイートした日時

テーブル名：tbl_twitter_user

カラム名	データ型	Not Null	主キー	属性	説明
user_id	int(11)	○	○	AUTO_INCREMENT	ユーザーの識別子
username	varchar(150)	○			ユーザーの識別名
password	varchar(150)	○			ユーザーのパスワードのハッシュ値
name	varchar(150)	○			ユーザーの名前
profile_image	varchar(150)	○			ユーザーのプロフィール画像
bio	text	○			ユーザーの自己紹介
follower_number	int(11)	○			フォローされたユーザーの数

データベース名：credit

テーブル名：tbl_credit

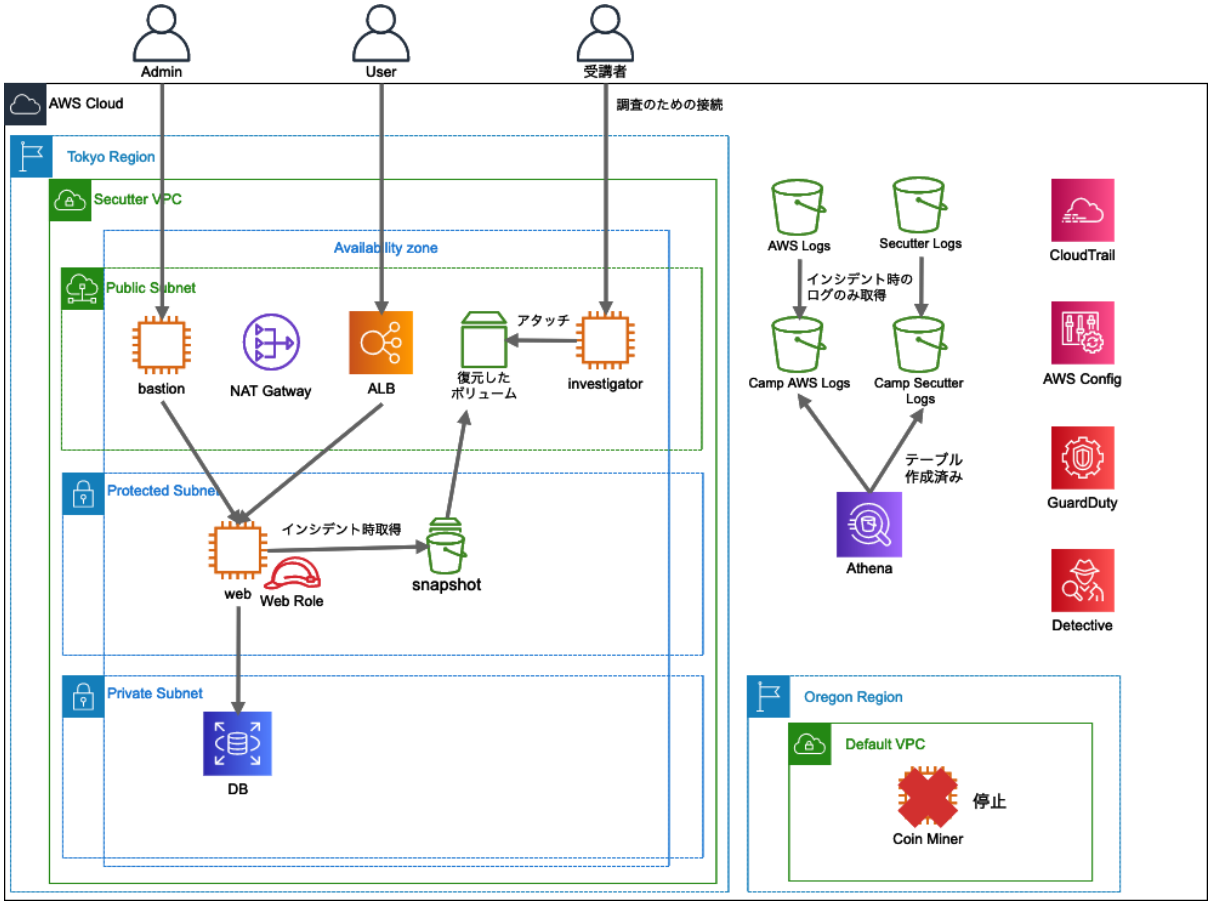
カラム名	データ型	Not Null	主キー	属性	説明
credit_id	int(11)	○	○	AUTO_INCREMENT	クレジットカードの識別子
card_user_name	text	○			クレジットカードの登録者の名前
card_number	bigint	○			クレジットカードの番号
card_cvv	int	○			クレジットカードのセキュ

					リティコード
card_expiry_date	date	○			クレジットカードの有効期間

インシデント説明

- インシデント発覚の経緯について

  2020/10/03 16時頃AWSからのAbuseレポート(メール)にてインシデントが発生したことを確認しました。
- 初動対応
  - ○ us-west-2（オレゴン）リージョンで、作成した覚えがない不正なEC2が動作しているのを発見しました。
  - ○ GuardDutyにて不正なEC2では仮想通貨が採掘（マイニング）されていることを検知していました。
  - ○ 動作していた不正なEC2を即時停止しました。
  - ○ Secutterサービスも侵害されている可能性が高いため、あわせて停止しています。
  - ○ 環境保全のため、secutter-prd-web EC2のAMIバックアップを取得しました。
  - ○ 該当時間のSecutterアプリログをcamp-secutter-logs-xxxxxxxxxxxxバケットに複製しています。
  - ○ 該当時間のAWSログをcamp-awslogs-xxxxxxxxxxxxバケットに移動しています。
- 初動対応後のイメージ



- 各種ログの調査対象時刻範囲

  15:00 ~ 16:00を調査範囲としてください(※)。

  ※メタ要素ですが、15時以前は環境構築時のログであるため無視してください。

課題説明

現時点では、具体的に何が起きたのか不明です。Secutterサービスを早く再開させたいため、各種ログを調査し、以下の観点で調査内容をまとめてください。

- 今回のインシデントについてSecutterサービスへの影響の有無を確認して報告してください。
  - ○ Secutterサービスは何か影響を受けているのか？
  - ○ 影響を受けているのであれば具体的にどのようなものなのか？また、そう判断した根拠は何なのか？
  - ○ 直ぐにサービスを再開しても良いのか？

- 不正なEC2が動作していた原因について調査をしてください。
    - ○ いつ、誰によって作成されたのか？
    - ○ そもそもインシデントが発生してしまった根本的な原因は何か？

- サービス再開のための対策案について提案してください。
    - ○ サービスを復旧するために対応すべきことは何か？
    - ○ 対策の優先度は？直近で対応しなければならないことは何なのか？

調査方法

当日のハンズオンでは以下2点の調査を実施します。

1. ハンズオン用に発行したIAMユーザーを利用して、AWS環境にログインし、侵害されたAWS環境の状況確認や各種ログの調査を実施
2. 侵害されたEC2環境のディスクイメージをダウンロードしていただき、参加者のローカル環境で解析を実施

１．AWS環境にログインしての調査について

- AWS環境ログイン方法
    - ○ Slackで連絡します。
- AWSレイヤーの調査
    - ○ 発行したIAM Userを利用して実際のAWS環境上におけるリソースや設定状況などを確認してください。
    - ○ 仮想通貨のマイニングについてはus-west-2（オレゴン）リージョンのGuardDutyにて検知しています。そちらも起点に調査をしてください。

- ○ CloudTrailのログは該当時間のものがcamp-awslogs-xxxxxxxxxxxxにあり、ap-northeast-1（東京）リージョンのAthenaにてcloudtrail_logs_camp_awslogs_xxxxxxxxxxxxテーブルを作成済みとなります。
- ○ Athenaを初めて使う時は[Settings] - [Query result location] に s3://aws-athena-query-results-xxxxxxxxxxxx-ap-northeast-1/を設定します。(儀式)
- ○ サンプルクエリ
  - ■ 特定のユーザーのAPI実行一覧を取得
  - ■ SELECT eventTime, eventName, eventSource, awsRegion, sourceIpAddress, userAgent, errorCode, errorMessage, requestParameters, responseElements FROM "default"."cloudtrail_logs_camp_awslogs_xxxxxxxxxxxx" WHERE userIdentity.userName = 'xxx-user' ORDER BY eventTime DESC;
- ○ 各イベントがどこから実行されているのか、どんな強力なAPIを実行しているかに注目してください。

- ● Secutterアプリ関連のログについての調査
  - ○ Nginxのログはcamp-secutter-logs-xxxxxxxxxxxxにありap-northeast-1（東京）リージョンのAthenaにてnginx_access_logsテーブルを作成済みです。
    - ■ サンプルクエリ
      - ● ELBヘルスチェック以外のログ一覧を取得
      - ● SELECT format_datetime(date_parse(time, '%d/%b/%Y:%H:%i:%s +0900'),'YYYY-MM-dd HH:mm:ss') AS datetime, * FROM "default"."nginx_access_logs" WHERE user_agent != 'ELB-HealthChecker/2.0'
  - ○ RDSのログはCloudWatch Logsに出力されておりクエリを検索することが可能です。auditログの調査に最適ですので、そちらを利用してください。

2. 侵害されたEC2環境のディスクイメージに関する調査について

調査対象のEC2はsecutter-prd-webのみとなります。こちらの解析を実施するためには、ddコマンドでバックアップした侵害されたEC2のディスクイメージを解析できる環境を事前に用意していただく必要があります。Linux環境もしくはWindows環境をご準備いただくことを推奨いたします。本ドキュメントではそれぞれの環境でのディスクイメージの解析方法について説明いたします。

なお、ディスクイメージは約8.3GB程度の容量となりますので、ハンズオン事前にダウンロードいただくことを推奨いたします。

- victime_ec2_backup.img
  侵害されたEC2環境のディスクイメージです。
- filehash
  ディスクイメージのファイルハッシュが記載してあります。

Linux環境

Linux環境にダウンロードしたディスクイメージをmountコマンドを利用してマウントし、調査を行います。なお、タイムスタンプをJSTで表示したい場合にはあらかじめマウントする側のLinux環境のタイムゾーンをJSTに設定してください。

以下のコマンドはroot権限で実行してください。

マウントポイントとなるディレクトリを作成
mkdir /mnt/victim_root

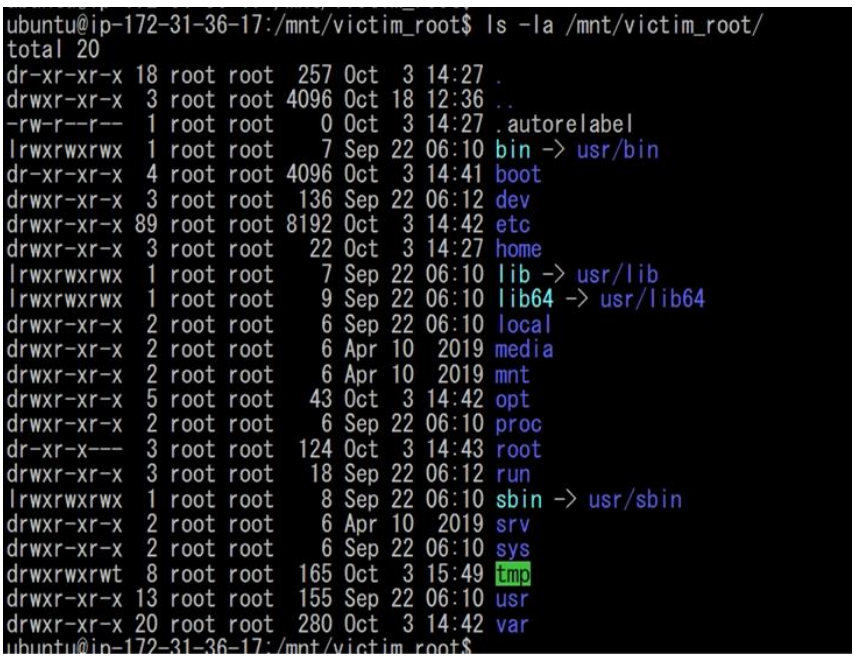
mountコマンドを実行してダウンロードしてきたディスクイメージを指定して、作成したディレクトリをマウントポイントとしてマウントしてください(※)。

mount -o ro,noexec,nodev -t xfs /home/tigerszk/victime_ec2_backup.img /mnt/victim_root

※実行しているmountコマンドのオプションについて

- ro: 読み取り専用
- noexec: バイナリの実行を不許可にする
- nodev: ファイルシステム上のキャラクタスペシャルデバイスやブロックスペシャルデバイスを利用できないようにする

mountコマンドの実行が成功していれば、以下の用にマウントポイントより侵害されたEC2環境のファイルを確認することができます。Linuxコマンドなどを利用して、調査を行ってください。



Windows環境

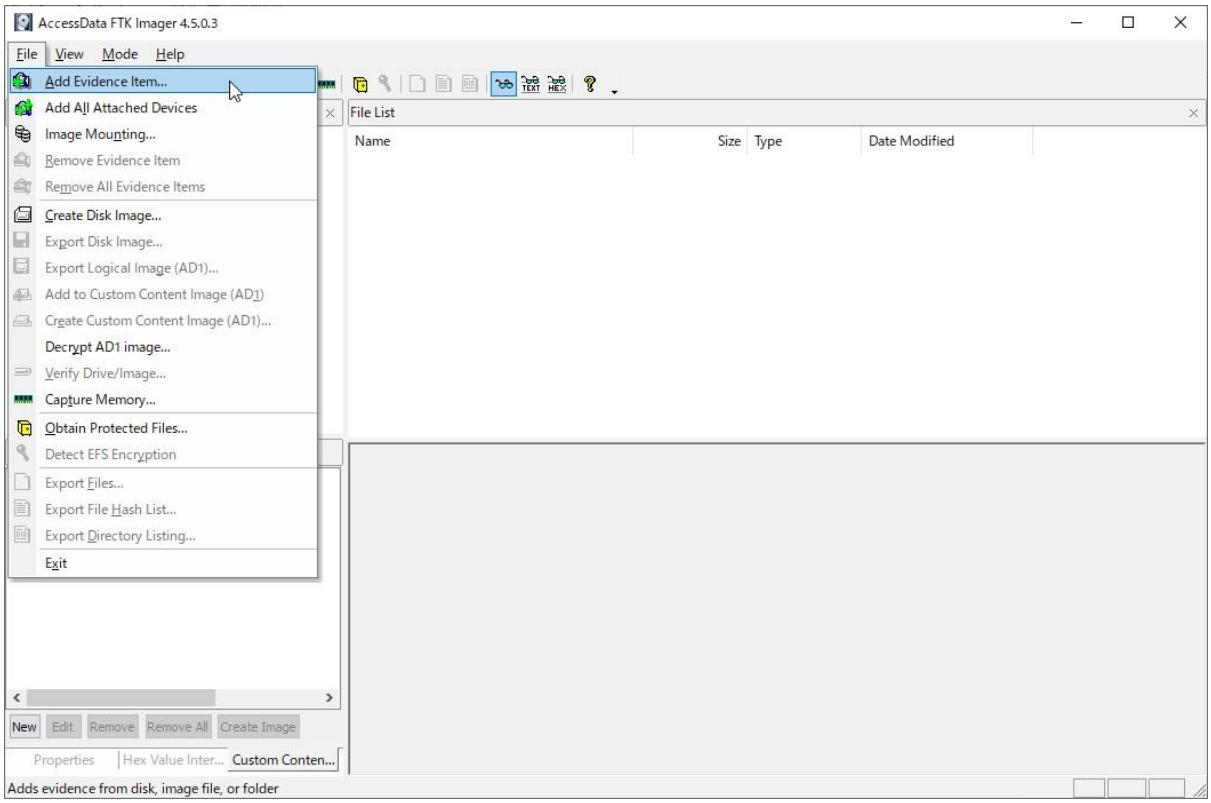
Windows環境ではデータ保全などに利用されるフォレンジックツールであるFTK Imager を利用した読み込みの方法を説明します。

FTK Imagerは以下からダウンロードが可能です。

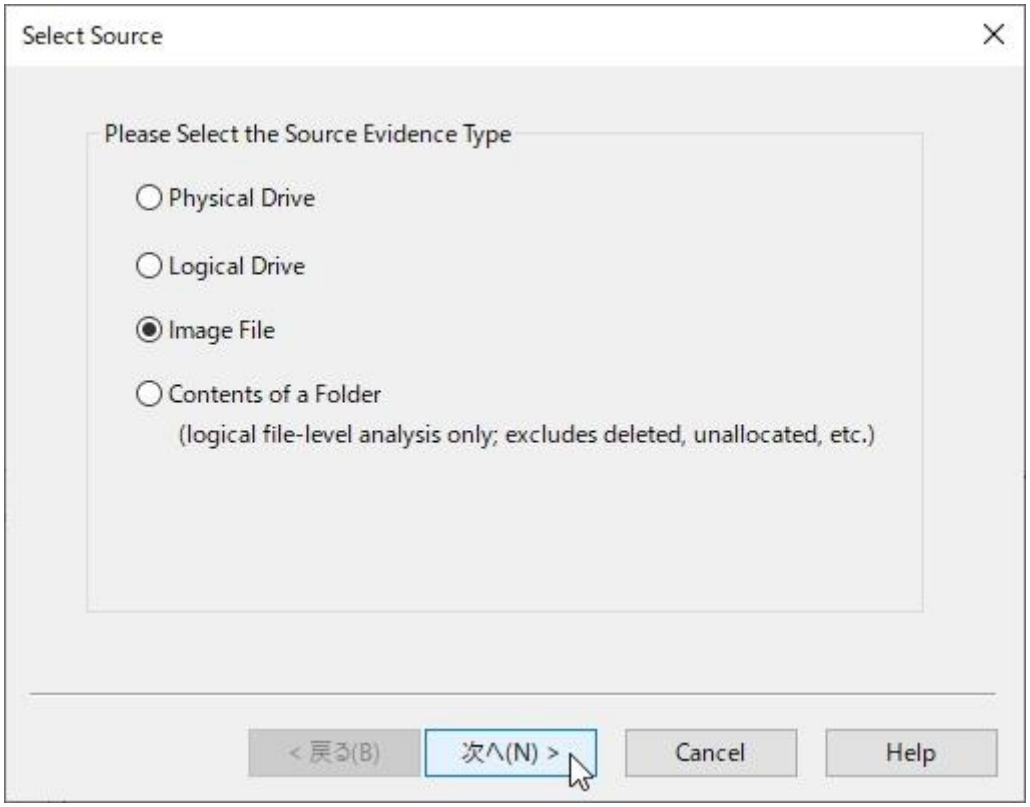
https://accessdata.com/product-download/ftk-imager-version-4-5

上記よりインストーラーをダウンロードしてインストールしてください。

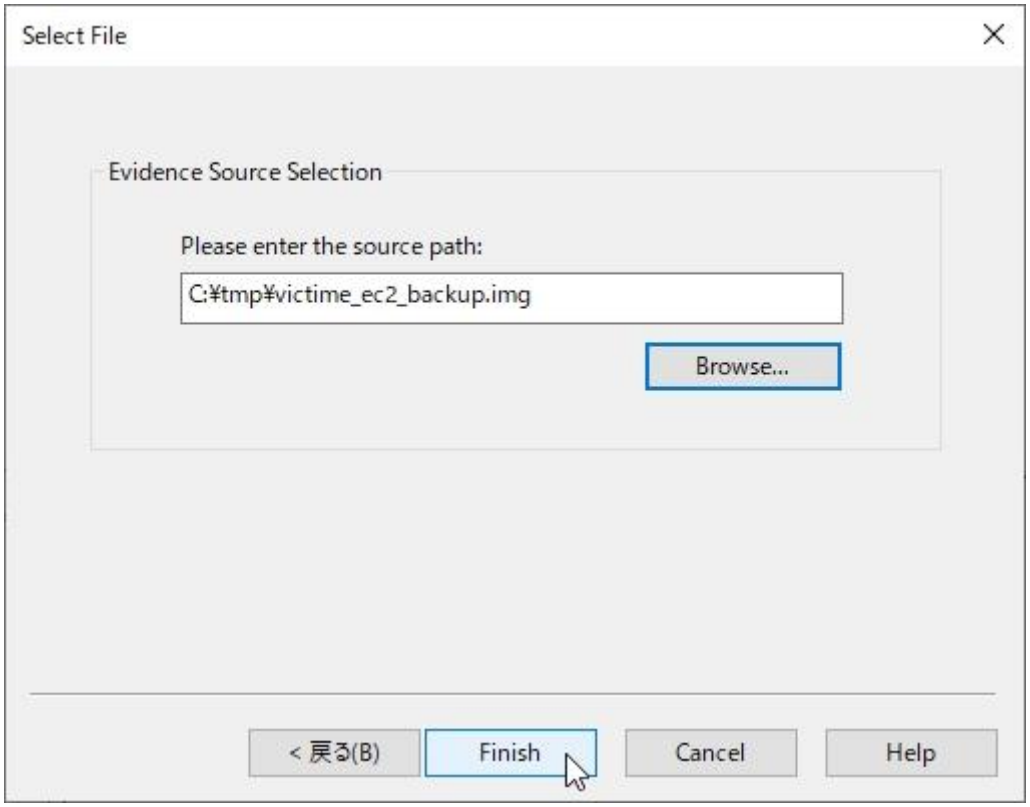
FTK Imager を起動し、［File］⇒［Add Evidence Item...］を選択します。



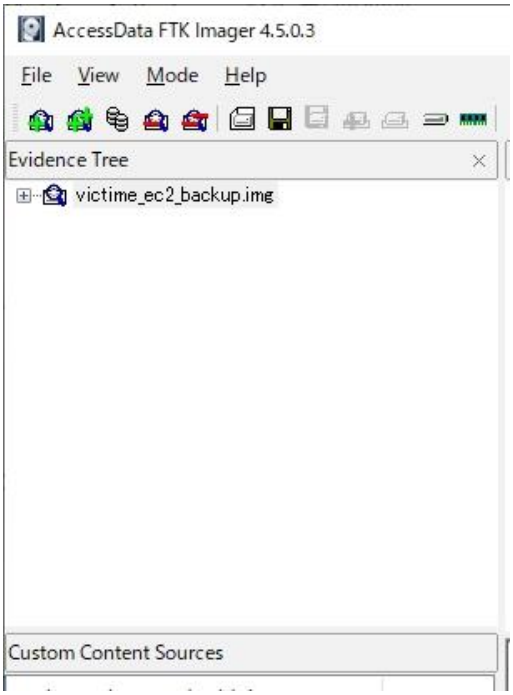
[Image File]を選択し、[次へ]をクリックします。



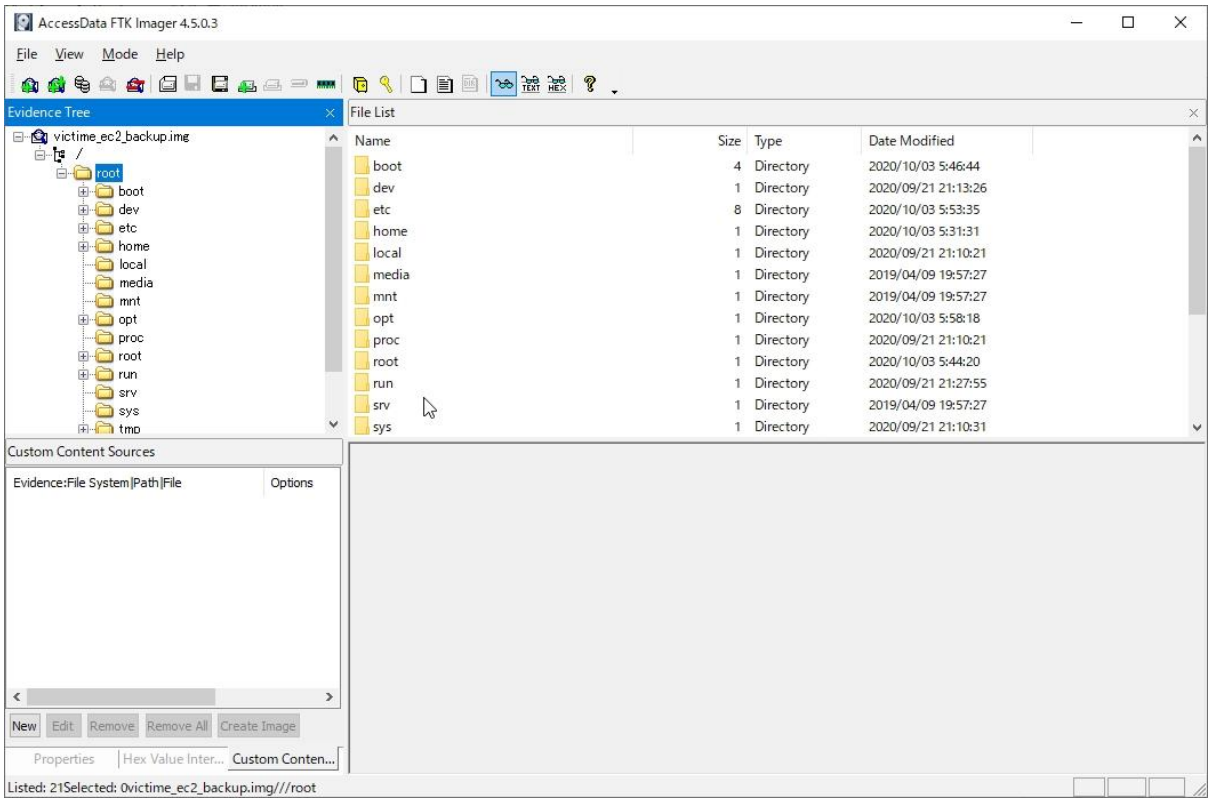
[Browse]ボタンをクリックし、ダウンロードしたディスクイメージのファイルを選択します。イメージファイルを選択し終えたら[開く]をクリックし、[Finish]をクリックします。



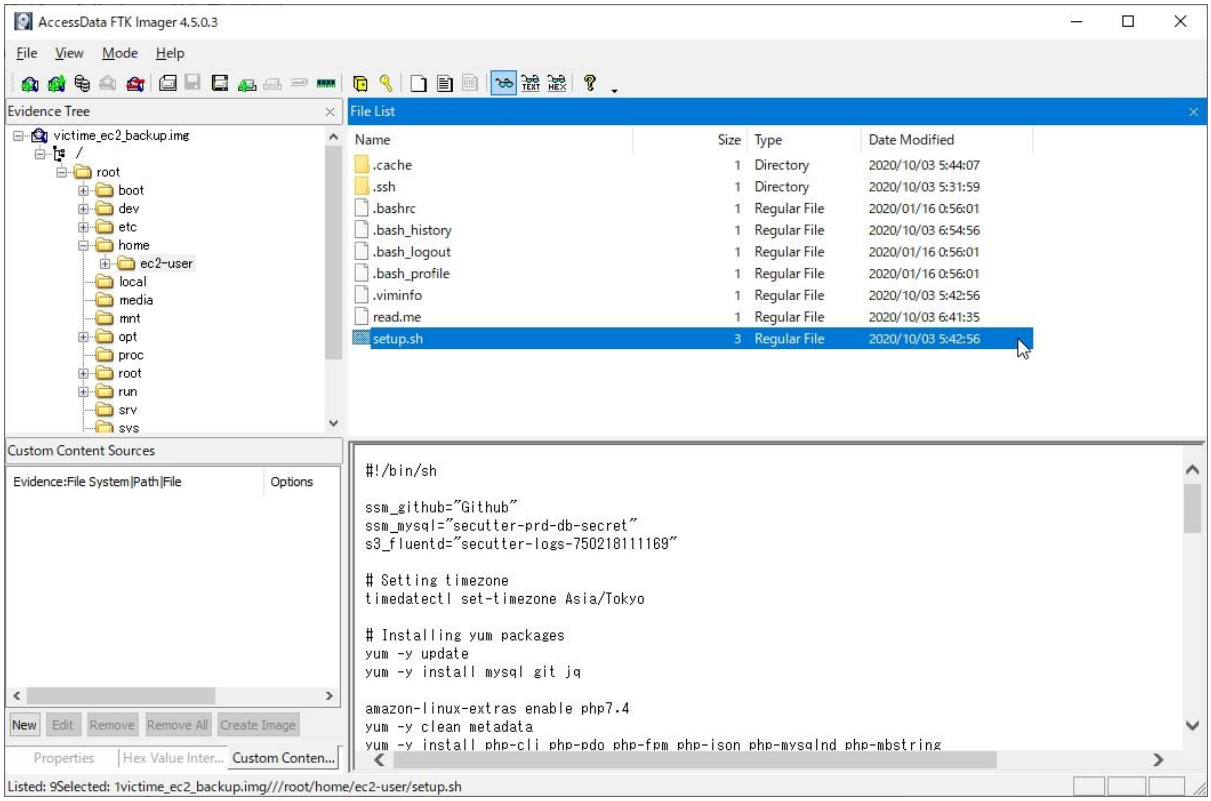
FTK ImagerのEvidenceTreeペインに選択したディスクイメージがマウントされます。



左側にある＋ボタンを押すことで、ディスクイメージのディレクリ構造がツリー形式で表示されます。



フォルダを選択すると、選択したフォルダ内のファイルやフォルダのリストがFile Listペインに表示されます。File Listペインで選択したデータの中身は、File Listペインの下の画面(コンテンツペイン)で確認することが出来ます。タイムスタンプはUTC表示のため，日本時間に換算するには+9時間してください。


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
victime_ec2_backup.img
/
root
boot
dev
etc
home
ec2-user
local
media
mnt
opt
proc
root
run
srv
sys
File List
Name Size Type Date Modified
.cache 1 Directory 2020/10/03 5:44:07
.ssh 1 Directory 2020/10/03 5:31:59
.bashrc 1 Regular File 2020/01/16 0:56:01
.bash_history 1 Regular File 2020/10/03 6:54:56
.bash_logout 1 Regular File 2020/01/16 0:56:01
.bash_profile 1 Regular File 2020/01/16 0:56:01
.viminfo 1 Regular File 2020/10/03 5:42:56
read.me 1 Regular File 2020/10/03 6:41:35
setup.sh 3 Regular File 2020/10/03 5:42:56
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conten...
#!/bin/sh
ssm_github="Github"
ssm_mysql="secutter-prd-db-secret"
s3_fluentd="secutter-logs-750218111169"
# Setting timezone
timedatectl set-timezone Asia/Tokyo
Installing yum packages
yum -y update
yum -y install mysql git jq
amazon-linux-extras enable php7.4
yum -y clean metadata
yum -y install php-cli php-pdo php-fpm php-json php-mysqlnd php-mbstring
Listed: 9Selected: 1victime_ec2_backup.img///root/home/ec2-user/setup.sh