〔様式第４号の１〕

令和６年３月 22 日

令和５年度　学生自主研究成果報告書

教　育　本　部　長　様

学生自主研究グループ名	White Poo	
研究課題名	Honeypotを用いたサイバー攻撃の可視化	
研究代表者（学生）	学籍番号	B25P025
	氏　名	庄司　はな
指導教員	学　科	情報工学科
	氏　名	光澤　敦

学生自主研究の報告書を別紙のとおり提出します。

〔様式第４号の２〕

Honeypot を用いたサイバー攻撃の可視化

システム科学技術学部　情報工学科
１年　庄司　はな
１年　石塚　杏佳
指導教員　システム科学技術学部　情報工学科
教授　光澤　敦
助教　橋浦　康一郎
学生支援スタッフ　システム科学技術研究科　総合システム工学専攻　情報工学コース
博士前期１年　中林　舜葵
システム科学技術学部　情報工学科
４年　加藤　久

はじめに

1.1 背景

近年，インターネット上での個人情報の抜き取りが増えている．サイバー攻撃とは，パソコンやスマートフォンなどの情報端末に対し，ネットワークを介してシステムの破壊や情報の改ざん，窃取などをする行為である．NICT が運用している大規模サーバーが観測したサイバー攻撃関連通信数は 5 年前と比較して 3.7 倍に増えている．[1]この攻撃の内容は IoT 機器を狙った通信，Windows を狙った攻撃などである．サイバー攻撃の分析をすることで，サイバー攻撃に強いシステムを作る必要がある．だからサイバー攻撃の理解を深める必要がある．そこで今回はアマゾンウェブサービス（AWS）というクラウドサービスを利用し，仮想サーバーの一つである Honeypot を構築してサイバー攻撃の種類を調査する方法を考えた．

1.2 目的

サイバー攻撃のパターンや手法を T-pot を用いて可視化する．そこからサイバー攻撃の特徴を理解する．

実験

2.1 実験の概要

インスタンスがうけた攻撃に対して一か月ごとに二回調査し，実際にどのようなサイバー攻撃があるのか確認する．実験結果から攻撃の特徴について考察する．最後に実験のまとめを行う．

2.2 実験に使用したもの

Amazon EC2 と T-pot を使用する．Amazon EC2 は Amazon Elastic Compute Cloud の略称で，アマゾンウェブサービスが提供する仮想サーバーサービスである．これを使用することで環境構築作業をすることなく手軽に仮想サーバーを用意することができる．今回使用した仮想サーバー（インスタンス）のメモリ容量は 8GB である．

T-pot とは，複数の Honeypot を運用し，そこから得たログを可視化するサービスである．Honeypot とは、あえてシステムへの不正侵入を許して攻撃手法や何をターゲットとしているのかを分析するおとりのような

システムのことである．

T-Pot の管理画面（図 2.1）にはブラウザからアクセスすることができ，管理画面で Attackmap（図 2.2）や国，サービス，port 番号ごとの攻撃数を確認することが可能である．Attackmap とはどの国からどの国へ攻撃が飛んでいるのか一目で知ることができるサービスである．

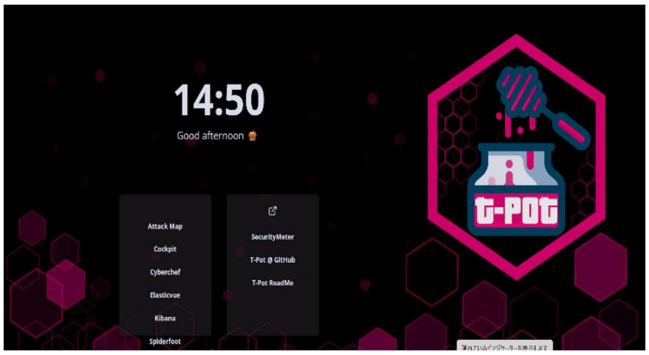

図 2.1　T-Pot の管理画面

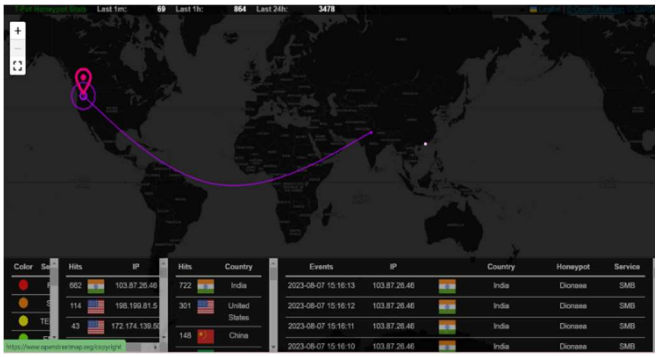

図 2.2　Attackmap

2.3 実験の手順

実験の手順として，5 つの手順がある．

① AWS アカウントを作成し，オレゴンに新しい仮想サーバー(EC2 インスタンス)を設置する．EC2 インスタンスを選択しさらにインスタンス名 t3.large,vCPU が Any vCPUs,メモリは 8GiB,Family:t3 を使用する．

② インスタンスへ接続する．Windows PowerShell を起動する．作成したインスタンスに SSH でリモートアクセスする．

③ T-Pot をインストールする．HoneyPot を構築するために，T-Pot をインストールする必要がある．そのために git-hub の T-pot に関するページ（https://github.com/telekom-security/tpotce）からコマンドを入手し手順に従ってインストールする．

④ 管理画面にアクセスする．ブラウザを使用して，作成したユーザー名とパスワードを用いて T-Pot の管理画面にアクセスする．

⑤ 攻撃を分析する．管理画面を通じて，HoneyPot が収集したデータやログを分析する．今回は 2023 年 9 月 2 日から 2023 年 10 月 2 日と 2023 年 10 月 3 日から 2023 年 11 月 2 日の 2 つの期間で攻撃の観測を行う．期間が違うことでどのような違いがあるのか明らかにする．

⑥ 考察とまとめを行う．

2.4 実験結果

2023 年 9 月 2 日から 2023 年 10 月 2 日を期間①，2023 年 10 月 3 日から 2023 年 11 月 2 日を期間②とする．

最初に期間による攻撃数を比較する．

期間①は合計 65,851 回，期間②は合計 578,440 回であった．

次に国ごとの攻撃数を比較する．

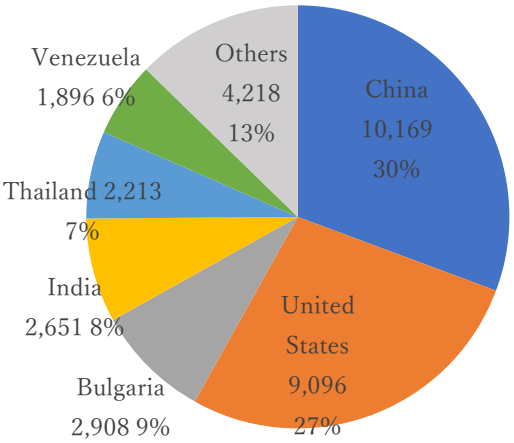

図 3.1　国ごとの攻撃数(期間①)

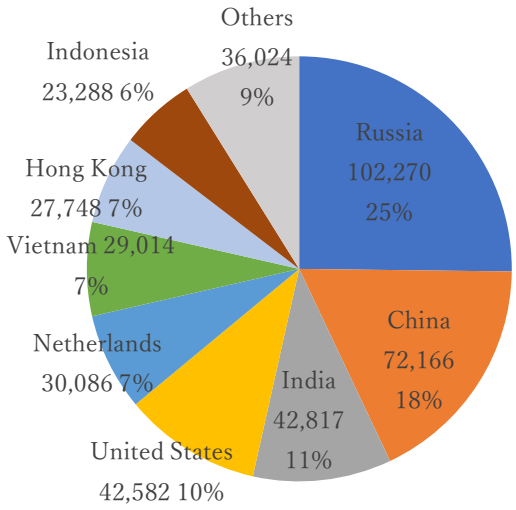

図 3.2　国ごとの攻撃数(期間②)

期間①は中国が 10,169 回で最も多く，次いでアメリカの 9,096 回であった．期間②はロシアが 102,270 回で最も多く，次いで中国の 72,166 回であった．

最後にサービスごとの攻撃数を比較する．

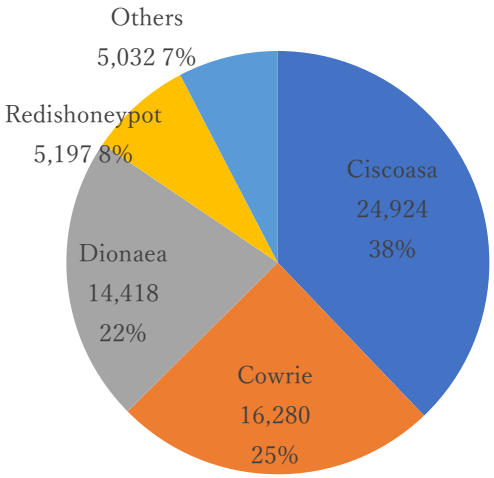

図 3.3　サービスごとの攻撃数(期間①)

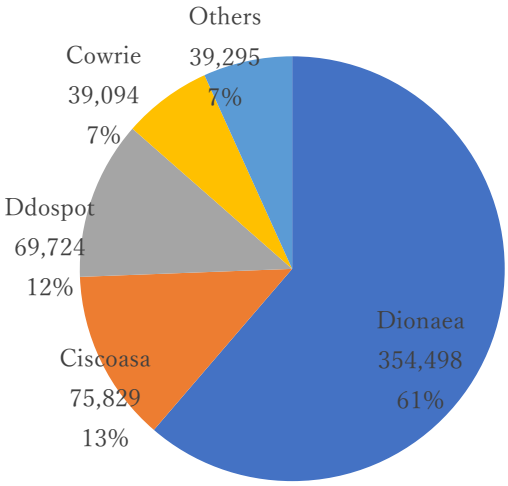

図 3.4　サービスごとの攻撃数(期間②)

期間①は Ciscoasa の 24,924 回で最も多く，次いで Cowrie の 16,280 回，Dionaea の 14,418 回であった．期間②は Dionaea の 354,498 回で最も多く，次いで Ciscoasa の 75,829 回，Ddospot の 69,724 回であった．

2.5 考察

2 つの観測期間では，攻撃された数が大幅に違う理由として，期間①ではインスタンスが止まっている期間があったためだと考える．攻撃データの収集には，ある程度容量が必要である．観測期間の違いによって，攻撃元の国は様々であった．しかし，攻撃元の国は中国，ロシア，アメリカなどの主要な国からの攻撃が多いことから，国の経済状況が比較的に高い国が多く攻撃していると考える．サービスごとの攻撃数の結果から，Ciscoasa と Cowrie，Dionaea がどちらの期間でも攻撃数が特に多かったため，この 3 つに焦点を当て

てみる．Ciscoasa とはシスコシステムズ合同会社が提供するファイアウォール製品のファームウェアである．つまり，企業や組織がネットワークを保護し，第三者からの不正アクセスや攻撃からシステムを守るために使用されている．しかし，ASA には脆弱性が存在し，攻撃者に悪用されると，情報が取得されることや情報の改ざん，サービス不能(DoS)状態になる可能性がある．Cowrie の特徴として攻撃者が SSH で接続試行するときのアカウント情報・ログイン後に実行したコマンド等を収集することができることがあげられる．Dionaea の特徴としては名前の意味がハエトリグサを意味している．この Honeypot は攻撃者からマルウェア（悪意を持ったソフトウェア）のコピーを手に入れることを目的としたマルウェア収集用 Honeypot である．Ciscoasa は不正アクセスされた攻撃を保護するためのファイアウォールであるためここを突破することができれば情報が簡単に取得できてしまうため攻撃数が多いのではないかとも考えられる．また，Cowrie と Dionaea は攻撃によって得られる情報を収集するためのものであり，実際のシステムやデータを保護するものではないため，この二グループを比較するのは難しい．

終わりに

3.1 まとめ

今回の研究に興味を持ったきっかけは，”はじめに”にもあるようにサイバー攻撃による被害をどのようなシステムで対抗することができるのかだった．システム自体を作ることは私たちでは作ることがまだできない．そのため，考察にもあるがこのサービスの特徴から，サイバー攻撃の特徴や種類を知るためにインスタンスを設置し，攻撃の統計を調査した．実験の結果からインターネットでの個人情報の抜き取りが多いことがわかった．サイバー攻撃のパターンや手法を理解することはセキュリティに対する理解を深める上ではとても重要だと今回の研究では理解することができた．

3.2 今後の展望

今後の展望として，今回の研究では測定期間が 2 か月と短かったこと，また，ハニーポットの停止により何日間かのデータ収集ができなかったことから正確なデータをとれたといえる実験ではなかったといえる．データを収集できる容量を増やすことによって，の停止を防ぐ Honeypot ことが可能である．予算の関係もあるため AWS のサービスを利用する際はある程度の知識を持ってからのほうがやりやすいと感じた．また，Honeypot が稼働しているか毎日確認することも正確なデータを取るために必要だと感じた．

参考文献

[1]”総務省　令和 4 年版情報通信白書第 2 部第 7 節”(2024 年 3 月 17 日 18:00 参照)
[2]“さくらのナレッジ　高機能ハニーポット(T-Pot22.04)をさくらのクラウドに構築して攻撃を観測する”,https://knowledge.sakura.ad.jp/35289/#T-Pot (2024 年 3 月 6 日 10:00 参照)
[3]“AWS の Amazon EC2 とは？機能とメリットをわかりやすく解説”,https://www.itechh.ne.jp/blog/column/ec2-explain.html (2024 年 3 月 6 日 10:00 参照)
[4]”EC2 上に Honeypot:Dionaea を建ててマルウェアを収集する話”,
https://kobaltlog.hatenablog.com/entry/2023/12/23/030607https://kobaltlog.hatenablog.com/entry/2023/12/23/030607_(2024 年 3 月 6 日 10:00 参照)
[5]須藤啓介，向井宏明，”T-Pot を用いたサイバー攻撃の分析” (2024 年 3 月 15 日 14:00 参照)