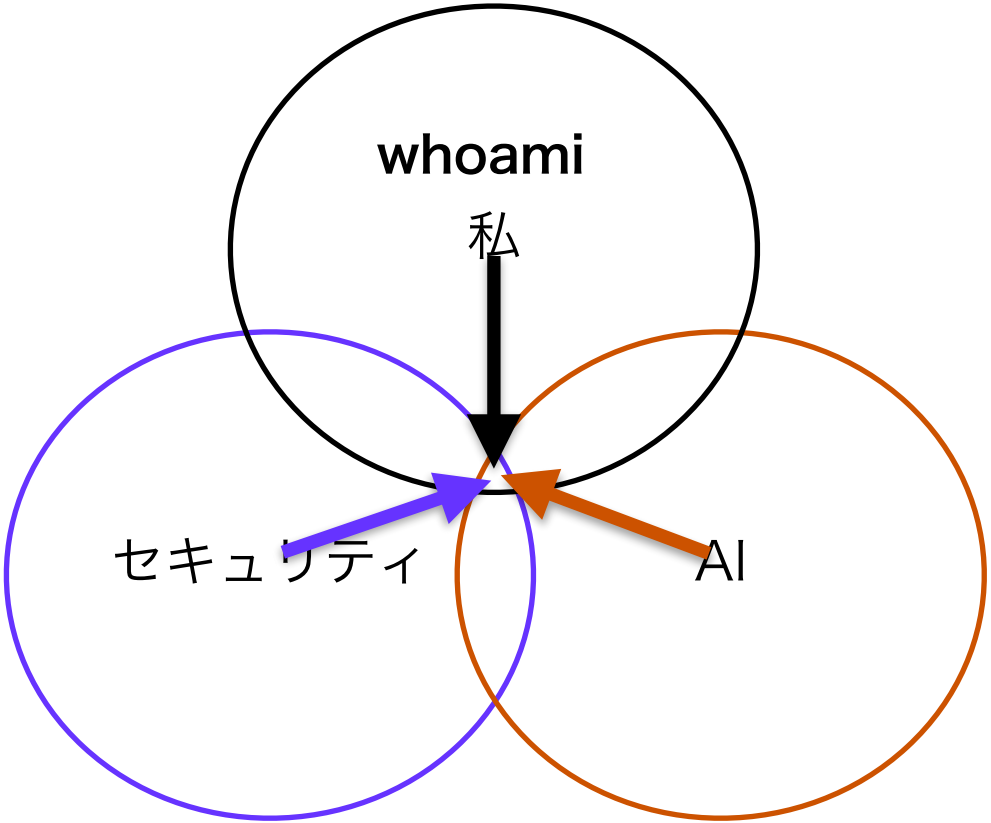
IIJ Internet Initiative Japan

セキュリティとAIと私

株式会社インターネットイニシアティブ
セキュリティ本部
守田 瞬

本日のお話



whoami

- 2017年2月 IIJ 入社（中途入社）
- Background
  - ➡ 光学シミュレーション用の数値（物理）計算エンジンの開発
  - ➡ アルゴリズム改良
  - ➡ 機械学習もブームに乗って少し
- セキュリティ、ネットワーク？
  - ➡ なにそれ？
- 使命はセキュリティ×AIの実現

IIJのSOCで何をやっているの？

セキュリティ機器から得られるログの情報を元に、脅威を見つける

- **ログとは？**

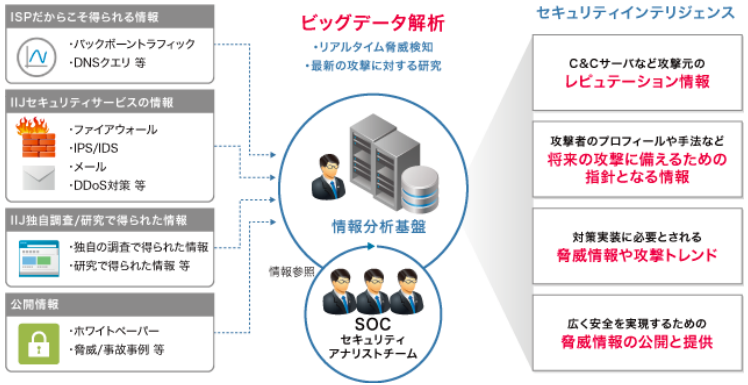
  マネージドセキュリティサービス（MSS）のログ
  （IPS / IDS、ファイアウォール、メール etc）

- **どうやって？**

  情報分析基盤（データベース）

- **どんな脅威？**

  マルウェアの通信、DDoS 攻撃 など



IIJのSOCで何をやっているの？（もう少し具体的編）

安全をあたりまえに wizSafe

Input と Output は様々なんです

ISPだからこそ得られる情報
- バックボーントラフィック
- DNSクエリ etc

IIJセキュリティサービスの情報
- ファイアウォール、IPS/IDS
- メール、DDoS対策 etc

IIJ独自調査/研究で得られた情報
- 独自の調査で得られた情報
- 研究で得られた情報 etc

ビッグデータ解析
- リアルタイム脅威検

情報分析基盤

セキュリティインテリジェンス

C&Cサーバなど攻撃元の
レピュテーション情報

攻撃者のプロフィールや手法など
将来の攻撃に備えるための指針となる情報

対策実装に必要とされる
脅威情報や攻撃トレンド

情報参照

インターネット
- SNS（Twitterなど）
- 企業や個人のWebサイト

情報収集

セキュリティ
アナリストチーム

情報発信

データ分析を起点とした方法で見つけている

- **データ分析を起点とした？**

  可視化や分析から傾向を掴む

  可視化や分析結果を元にルールを作成

  自動化して、通知を受け取る

  詳細な分析

具体例は後ほど

C2 通信の検知

概要

- 通信先に依存せず、通信の振る舞いから C2 通信の検知を行う
- 通信先の情報が未知である場合にも有効
- C2 通信の振る舞いと類似する、正常な通信との区別は困難

検知技術

- 機械学習

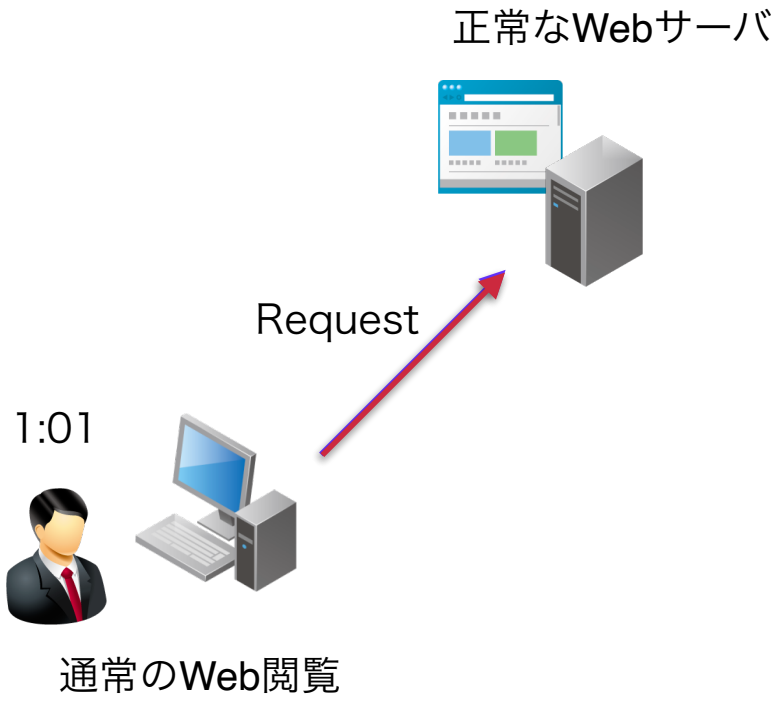
活用技術の選定ポイント

- C2 通信の振る舞いを定式化することは困難
- 機械学習モデルの評価に用いるデータがある

具体的には、どんな脅威を見つけてるの？（part 1）

C2 通信の検知

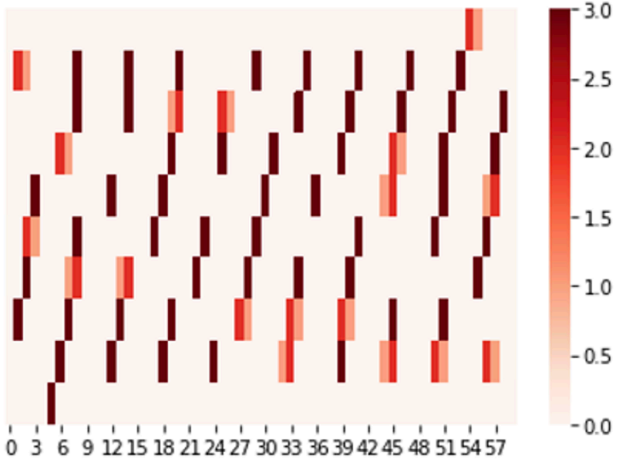
	1分	2分	‥	60分
1時	1	0		
2時				
:				
24時				

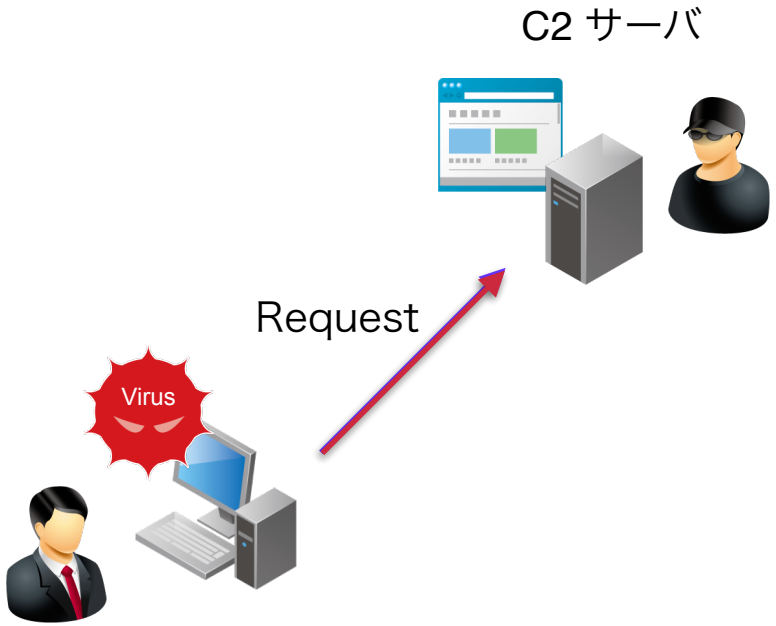


具体的には、どんな脅威を見つけてるの？（part 1）

C2 通信の検知

C2 通信の例





攻撃訓練/攻撃演習で使用された仮想の C2 通信、実際に使用された**標的型攻撃**の C2 通信を検知

DDoS 攻撃の観測（SYN/ACK Reflection 攻撃）

概要

- リフレクション型の DDoS 攻撃で、Web Server などがリフレクターとして悪用される恐れがある
- 正常通信に紛れて、Three-way handshake の仕組みを悪用した攻撃
- 単一のリフレクターを監視していても、リフレクターとして悪用されていることに気が付きにくい

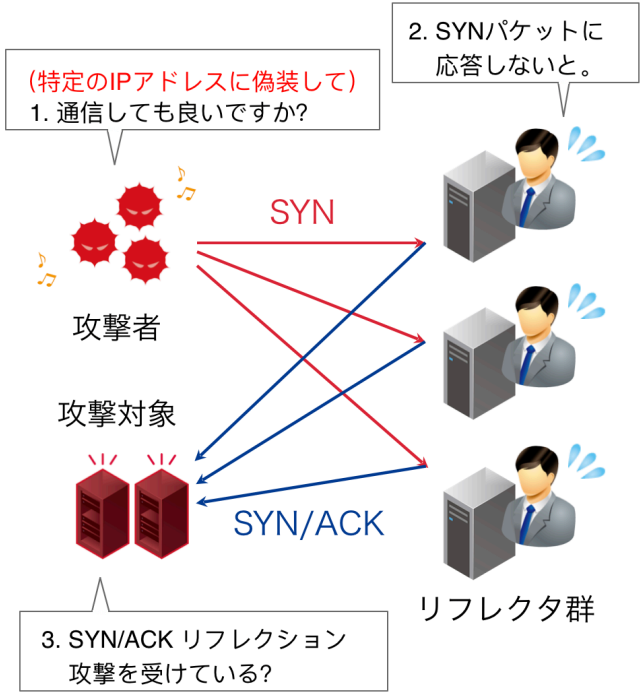
検知技術

- 可視化と分析による検知ロジックの定式化

活用技術の選定ポイント

- 過去の事例として、教師として存在するデータがない
- 観測事例の頻度が増加した時期があったため、早く自動化したかった

SYN/ACK Reflection 攻撃の概要



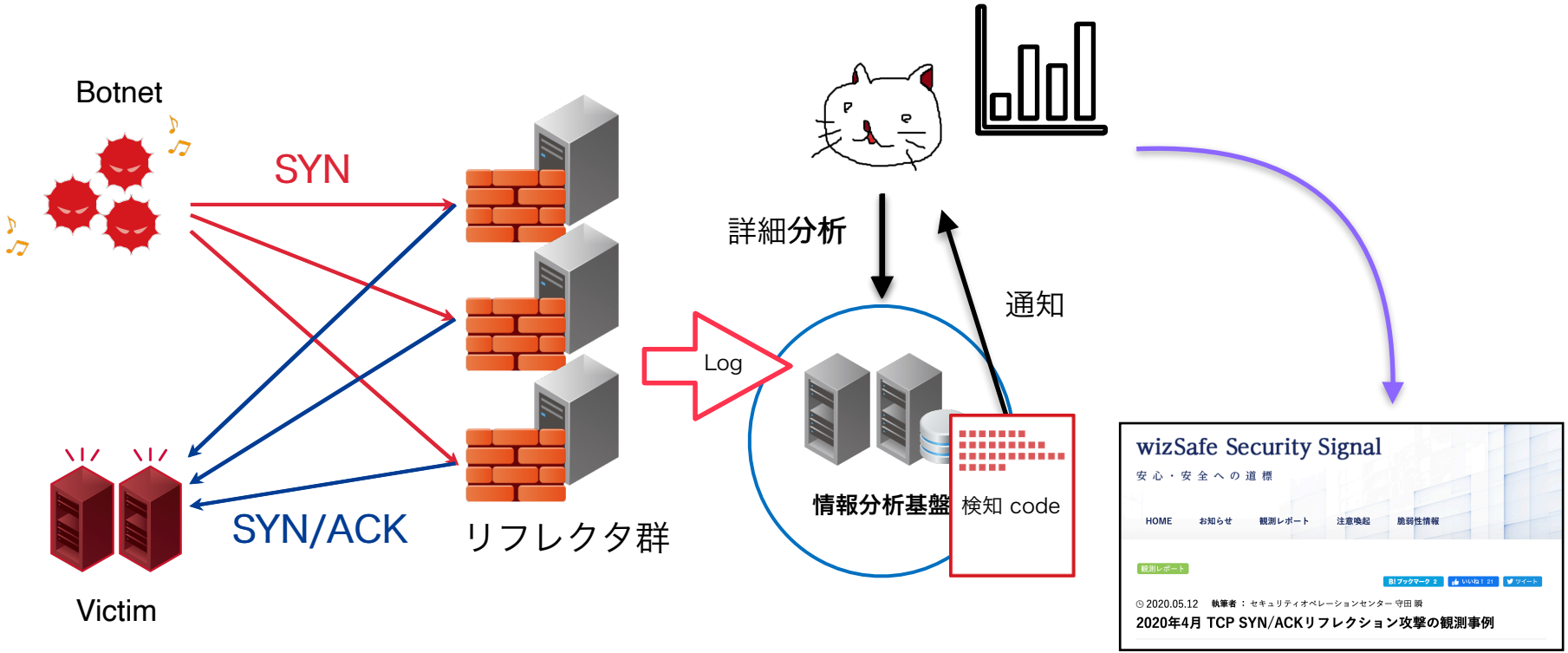
1. 攻撃に用いられる **SYN パケット**は送信元が攻撃対象となる宛先に偽装されている。

   ※基本的に、SYN/ACK Reflection 攻撃を発生させるための SYN Packet を送信する Actor は不明。

2. 上記 1 のような **SYN パケット**を受け取った端末は、その応答として **SYN/ACK パケット**を偽装されたIPアドレスに返す。
3. 身に覚えのない **SYN/ACK パケット**を処理する端末に負荷がかかり、Denial of Service (DoS) となる。

具体的には、どんな脅威を見つけてるの？（part 2）

SYN/ACK Reflection 攻撃を検知して Output するまで



安全をあたりまえに wizSafe

IIJのSOCだからできること

- データ分析を起点として、脅威の検知・分析を行うことができる。
- チャレンジングに活動でき、データ分析だけでなくドメイン知識（セキュリティ、ネットワーク）となる技術も習得できる。

wizSafe

安全をあたりまえに