IoT Security Systemの開発

2018/04

情報科学科 小山研究室

1

キーワード

- IoT
- セキュリティ
- マルウェア
- 機械学習

2

研究紹介の前に・・・

3

3

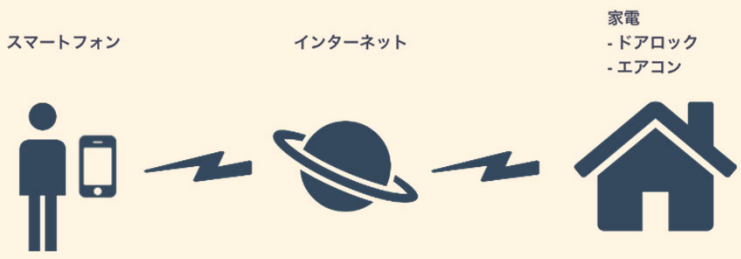
IoTについて

IoTとは？

- Internet of Thingsの略で「モノのインターネット」と呼ばれる
- 身の周りのあらゆるモノがインターネットに繋がる仕組み

IoTの活用事例

- 携帯端末を用いて家電を遠隔制御



4

4

IoTのセキュリティについて

なぜセキュリティが重要なのか

- 発展途上の概念なのでセキュリティ意識の甘いIoT機器が多数存在する
- IoT機器をターゲットにしたマルウェアの存在が確認された（Mirai / Hajime 等）
- 自分のIoT機器がマルウェアによって踏み台にされ、知らない間にサイバー攻撃の加害者になっている可能性がある

5

5

マルウェアについて

マルウェアとは？

- ユーザーに害をなす不正なソフトウェアの総称
  - ウイルス、ワーム、トロイの木馬、キーロガー、 etc..
- ネットワーク、メール、外部メディア等から感染

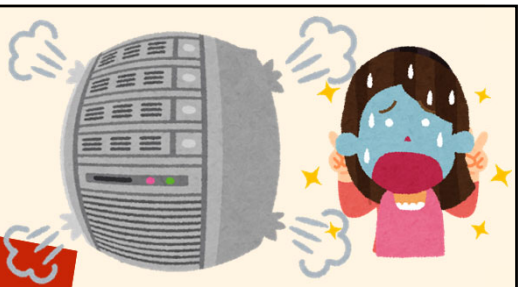
マルウェアの目的

- 個人情報を盗む
- 感染した端末を不正に遠隔操作
- 端末のデータを改竄、消去

6

6

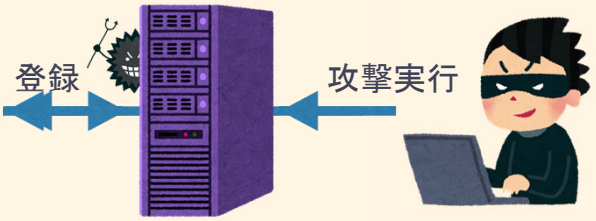
攻撃方法例



大量のアクセス

多数のIoT機器

第三者のサーバー



攻撃者のC&Cサーバー

攻撃者

7

現実

2016年09月29日 21時00分00秒

毎秒1テラビットという史上空前のDDoS攻撃が発生、攻撃元はハッキングされた14万5000台ものウェブカメラ

参考: GIGAZINE

IoT機器を踏み台にした史上最大規模のDDoS攻撃が続々発生

2016/09/28

シェア 0　ツイート

参考: 日経BP

nds for this listing. I will let my previous Alph

a 40 cent test attack. These attacks are goo
pending 25 dollars on a 1-day attack.
ne for 1-day attacks, just make multiple orde
antity over "1" (which is really 6 test keys if t

参考: NHK News

8

研究背景

マルウェアの感染拡大を抑止したい

↓

マルウェアによって引き起こされる通信に着目

↓

全ての通信の中からマルウェアによって引き起こされる通信を検知出来ればよさそう

9

9

研究内容

- IoT Security Systemの開発
  - ネットワーク内のIoT機器の把握、監視
  - マルウェアによる通信の検知
  - ユーザーが扱いやすいUIや通知機能

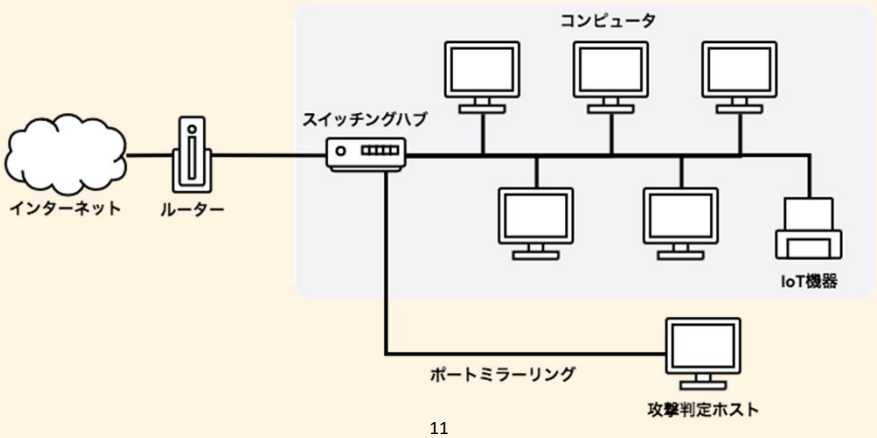
10

10

研究内容

ネットワーク内のIoT機器の把握、監視

- ネットワーク上の通信を傍受 (パケットキャプチャ)
- 通信データのアドレスから機器を識別し、監視する



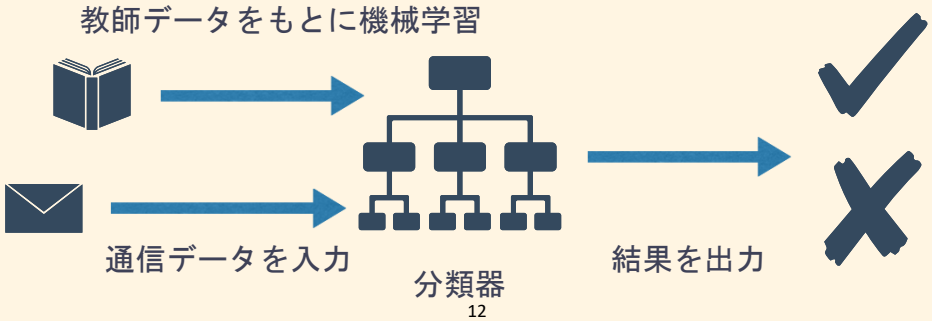
11

11

研究内容

マルウェアによる通信の検知

- 機械学習により、マルウェアによる通信かどうかを分類する分類器を生成
- 通信データを判定器にかけることで検知を行う



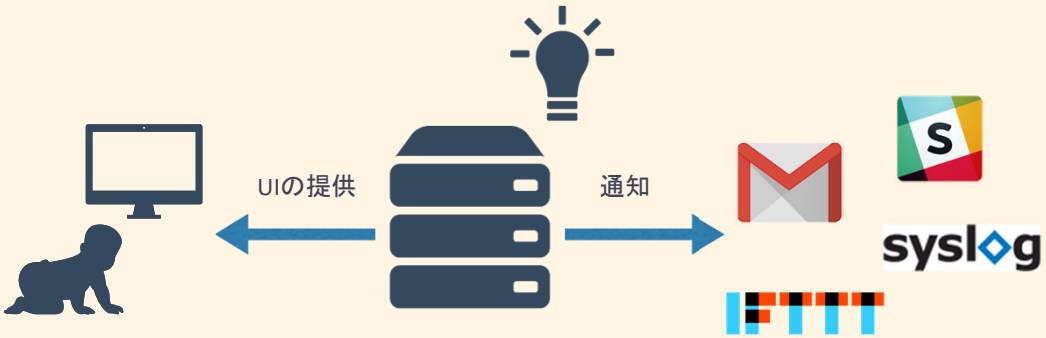
12

12

研究内容

ユーザーが扱いやすいUIや通知機能

- ウェブブラウザから扱えるUI
- メール、Syslog、IFTTT、Slackによる通知機能



13

13

補足

機械学習とは具体的に何をしているのか？

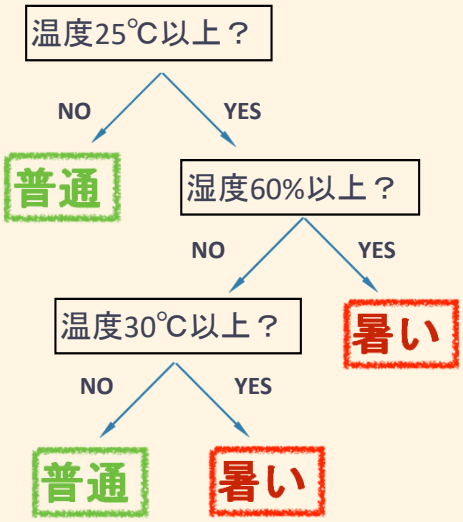
- ディープラーニング、クラスタリング、ニューラルネットワーク、教師あり学習、etc…

様々なアルゴリズムが存在しているが、
今回はランダムフォレストを使用する

14

補足

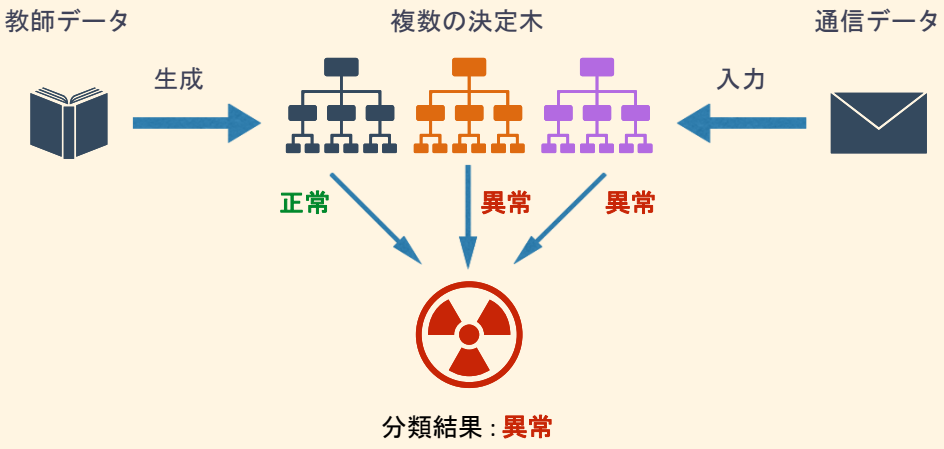
決定木とは



15

補足

ランダムフォレストとは



16

終わり

17