岩手県立大学
Iwate Prefectural University

成田研の紹介： 成田 匡輝（なりた まさき）

- 自己紹介
  - ■ 本学部と大学院の出身
  - ■ 専門分野：ネットワークセキュリティ
- 研究室のテーマを一言で
  - ■ **“IoT時代のサイバーセキュリティ”**

- IoT (Internet of Things)
  - ■モノのインターネット
  - ■あらゆる「モノ」がインターネットに接続する時代

セキュリティ対策が今後の課題

脆弱なIPカメラの例
（組み込みLinux搭載）

- 簡単なIDとパスワードで侵入可能
- インターネット上で攻撃活動に加担させられる

サイバー攻撃被害とこれから

- サイバー攻撃を受けると，経済的損失だけでなく，社会的信用も失う
  - ■ サービスの停止，顧客情報の流出　等
- 家電等の身近な「モノ」が攻撃対象になることにより，被害がサイバー空間から人への直接被害へ移行

Black Hat USA 2015
で発表されたクルマの遠隔操作実験

人命に関わる可能性

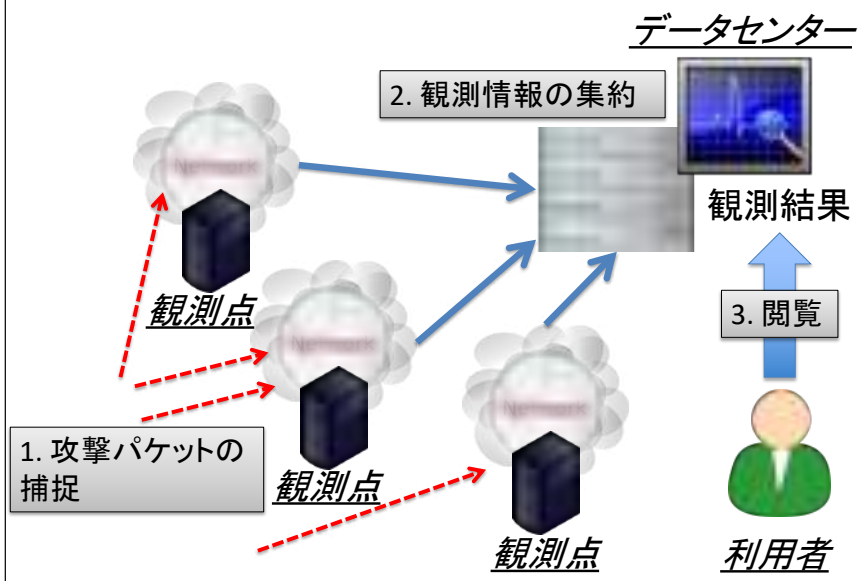
デバイスをインターネットに直接つないで放置するとどうなる？

- 様々なパケットが勝手に到着
  - ■コンピュータウイルスが次の感染先を探して
  - ■自分とは無関係な攻撃によって生じたパケット
  - ■設定ミスによるパケット

そこで，囮のネットワーク機器をインターネットに接続しておけば，到着パケットから攻撃傾向が分かる

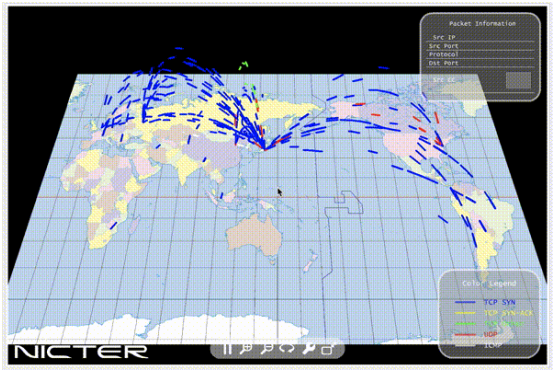
→ ダークネット観測システム

ダークネット観測システムの概要



システムの一例:

nicter（情報通信研究機構の例）



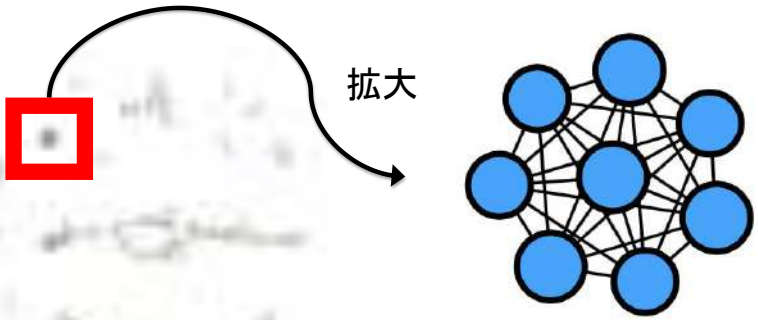
近年の傾向として. . .

特にIoT機器が狙われています

参考:nicter, http://www.nicter.jp/atlas

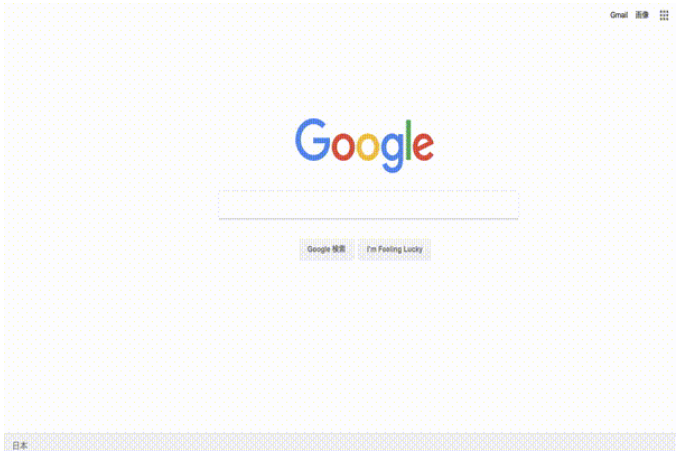
研究テーマの例（1） 攻撃パケットの観測

- ビッグデータ化する攻撃パケットに対処する試み
  - ➢新たな攻撃分析手法の開発
  - ➢データの形に着目する (Topological Data Analysis)



➢ 7021番ポートへの攻撃
→ NetWin SurgeFTP の脆弱性を狙ったもの

研究テーマの例（1）



研究テーマの例（2）

IoT機器の保護

- 家庭内のIoT機器に侵入されてしまったら？

➢ 何が起こるか
➢ どのようにして攻撃者から機器を保護するか

研究テーマの例（3）

AI作成画像によるCAPTCHA

CAPTCHAとは「人間と機械を判別するチューニングテスト」

人間にとって理解できるが、機械にとっては認識が難しい

応答者にコンピュータでは対応できない問題を出して答えさせる

研究テーマの例（3）

既存のCAPTCHA

研究テーマの例（3）

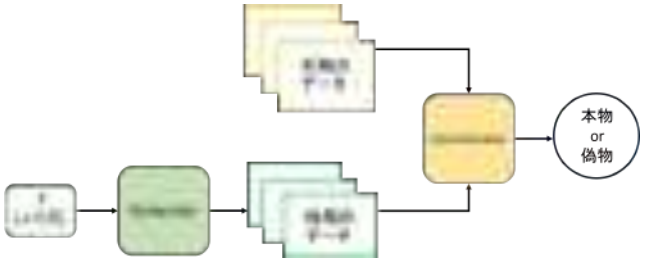
GAN（敵対的生成ネットワーク）

Generative Adversarial Network

入力した画像データを学習して

Generator と Discriminator を
競い合わせて画像を生成

©Picture on [Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks] 2015

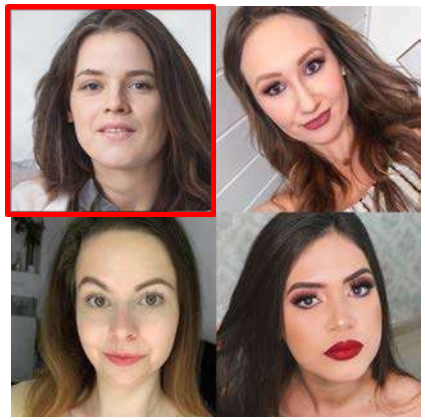


研究テーマの例（3）

AIを用いて作成した顔画像を利用したCAPTCHA

- 人間の違和感を感じる能力を利用
  - ■ 人間だからこそ直感的にクリアすることが可能な新しいCAPTCHAを提案
  - ➢ 人間の直感のほうが，まだAI性能を上回るだろうという前提

研究テーマの例（3）
AIで生成された顔画像はどれでしょうか？



https://www.photo-ac.com/main/genface

研究テーマの例（3）
プロトタイプによる評価実験

◆人間でも正答率が低すぎる結果になった（想定外）
◆その為，コンピュータによる攻撃実験が未実施

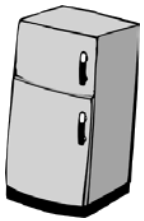
右図はSNS上での実験の様子

- 50%～70%程度の正答率
- 100%の正答率を出す被験者も

経験・慣れによるものなのか，
先天的な感性なのか解明できていない

研究テーマの例（4）
IoT機器とプライバシー

- IoTデバイスからの個人情報推定
  - – あらゆる「モノ」がインターネットに接続する時代
  - – 特に個人のプライバシーという観点から弊害はないのだろうか



研究テーマの例（4）

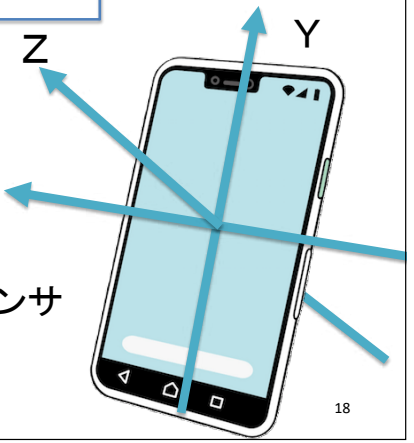
実験してみた想定シナリオ

- ネットワークに接続されたドアがある
  - 攻撃者がネットワークを流れるパケットデータを盗める・盗聴できると仮定

➢データを分析することで個人を特定したり個人の行動を把握する問題が発生するのではないだろうか

研究テーマの例（4）

スマートドア（仮称）



スマホ内蔵のセンサでやってみた

研究室のドアに設置

研究テーマの例（4）

着目した特徴量

- ドアの開閉時刻
  - どの学生にも生活パターンがある
  - 夜型や朝型
- 加速度
  - 乱暴に力強く開ける人
  - 最小限の開閉で出入りする人

➢この研究はドアに着目したが，外部環境の値が収集・突合・分析されることで個人のプライバシーが侵害される可能性は今後増えていくだろう

過去の研究

SNS + Blockchain

SNSへの画像投稿に応用

➢ 投稿，画像の差し替え，削除などを全て記録

個人間の物品の貸し借り
（シェアリングエコノミーへ応用）