IoTとセキュリティと、時々、機械学習

- NICTにおけるIoTセキュリティと機械学習応用の取り組み -

井上 大介
国立研究開発法人 情報通信研究機構

サイバーセキュリティ研究所
サイバーセキュリティ研究室

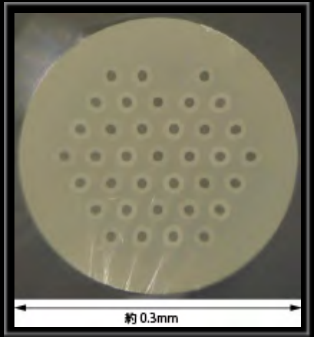
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

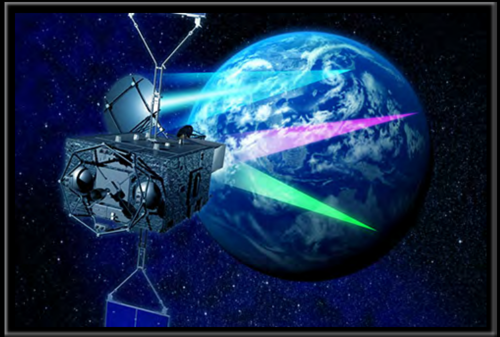
国立研究開発法人 情報通信研究機構とは？

- 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）

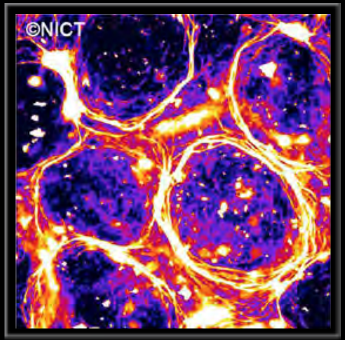


光通信システム
（ペタbps級 マルチコアファイバ）


宇宙通信システム
（超高速インターネット衛星きずな）


サイエンスクラウド
（ひまわり8号リアルタイムWeb）

電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）



バイオ・ナノICT
（生体分子の自己組織化）


脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）


超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）


サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

サイバーセキュリティ研究室 研究マップ

インシデント分析センタ（ニクター）

NICTER

対サイバー攻撃アラートシステム（ダイダロス）

DAEDALUS

受 Passive

サイバー攻撃統合分析プラットフォーム（ニルヴァーナ・カイ）

NIRVANA改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

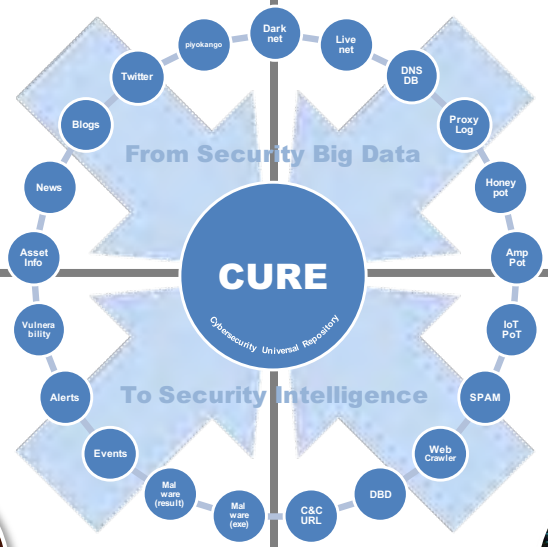
NIRVANA改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

局



サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

Active

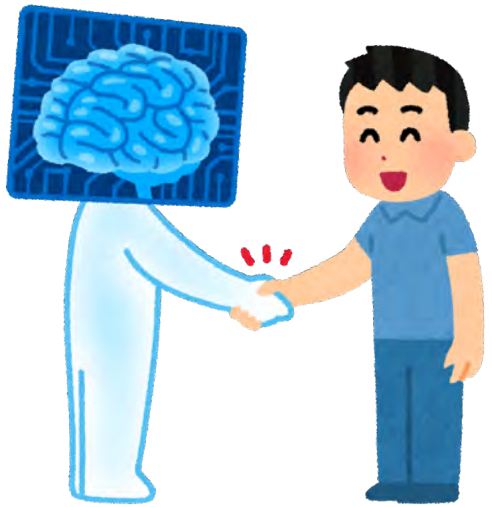
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

本日のアジェンダ

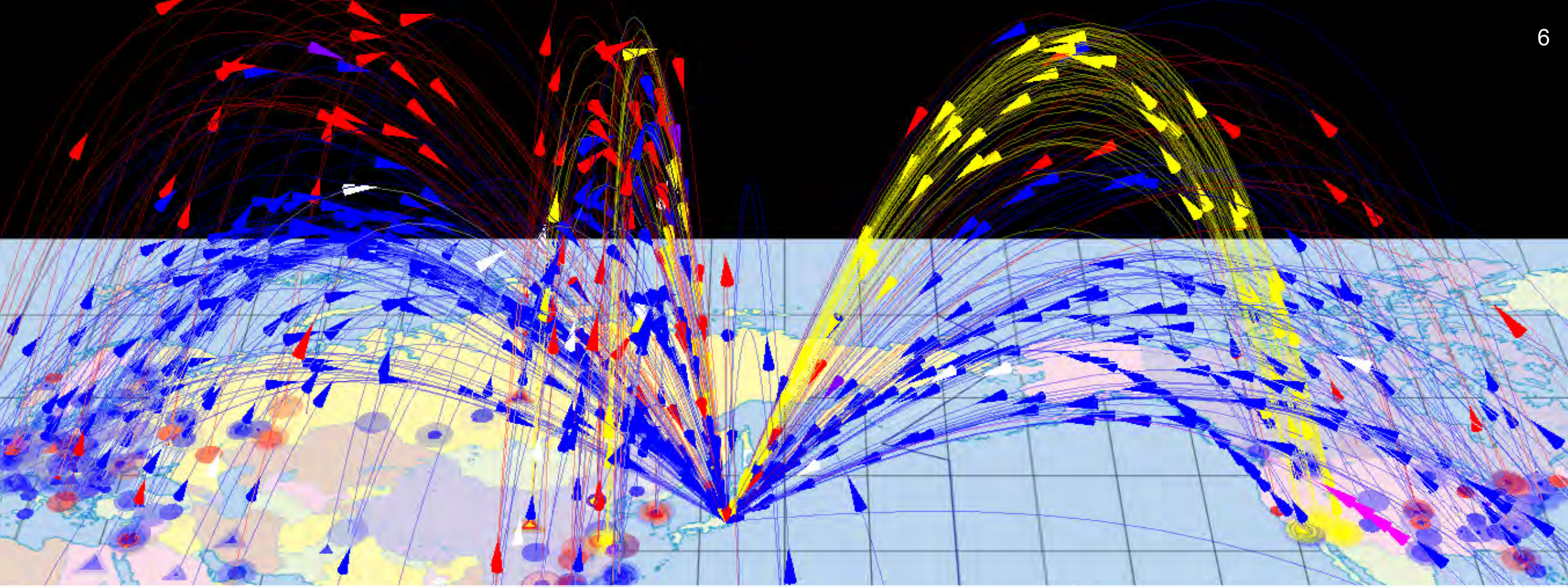
1. IoTセキュリティ

2. AIとサイバーセキュリティ



IoTセキュリティ

- 感染IoT機器の現状とその対策 -

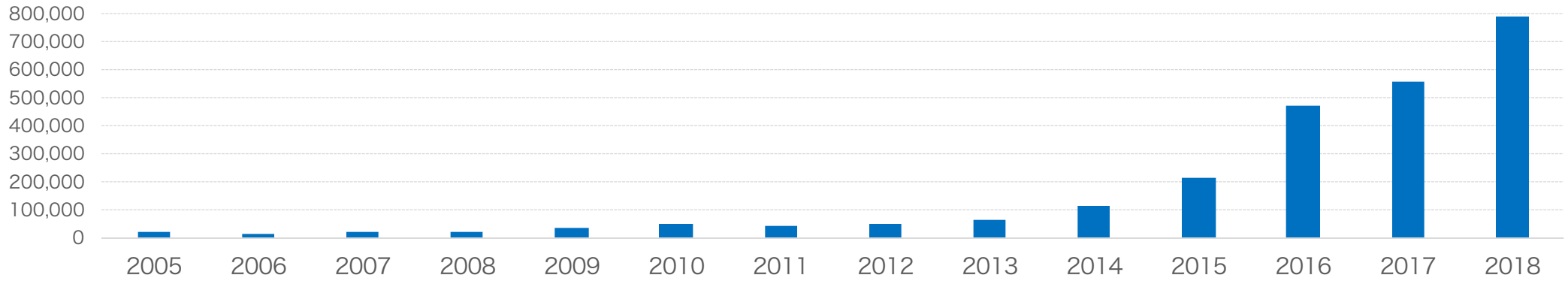


NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

NICTER観測統計（2005-2018）

年	年間総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	**約2,121億**	約30万	**789,876**



1 IPアドレスあたりの年間総観測パケット数


IoT
Internet of Things
横浜国立大学
吉岡研究室による調査
National University
YOKOHAMA
YNU
HG8245
HUAWEI
Account:
Password:
Login
Copyright © Huawei Technologies Co., Ltd 2009-2011. All rights reserved
嵌入式電話錄音主機WEB管理系統
V1.0
設備IP地址 1.34.155.239
用戶名稱 AAAA
密碼
主端口 12345
FTP端口 21
Connect
Close
Record System Copyright2008
Java Application
Web Application
pandora
BUSINESS SUITE
Username:
Password:
Login
Security Equipment
HOT box
Login
Login
Password
Save login and password
Apply
BISBOX
BUSINESS INTERNET
IP: 107.190.198.86
Username:
Password:
Login
Clear
User Name: admin
Password:
Network: WAN
RouterOS v5.22
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.
WebFig Login:
Login: admin
Password:
Login
Winbox
Telnet
Graphs
License
Help
DiskStationPlay
Aanmelden
Username
Password
Login
WPA2-Personal
WEB 1.0
User Name:
Password:
11n 150Mbps WLAN ADSL2+ Modem Router
Status
Network
Wireless
Tek Corp. All Rights Reserved.
DrayTek
ZTE中兴
F460
Please login...
Username
Password
Login
TM
Welcome To Streamyx Connection Setup
Login
Password
Quick Setup mode
Login
Modem model: ADSL-RIGER-DB120WL
Page : DIR-868L
Hardware Version : A1
Firmware Version : 1.03SHC
D-Link
LOGIN
Network video client
Username: admin
VOIP
Login>>>>

感染IoT機器の分類（2016年9月）

- 横浜国立大学 吉岡研究室による調査結果 -

- **Surveillance camera**
  - IP camera
  - DVR
- **Network devices**
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances
- **Telephone**
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters
- **Infrastructures**
  - Parking management system
  - LED display controller







- **Control system**
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)
- **Home/individuals**
  - Web cam, Video recorders
  - Home automation GW
  - Solar Energy Control System
  - Energy demand monitoring system
- **Broadcasting**
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box
- **Etc**
  - Heat pump
  - Fire alert system
  - Medical device(MRI)
  - Fingerprint scanner



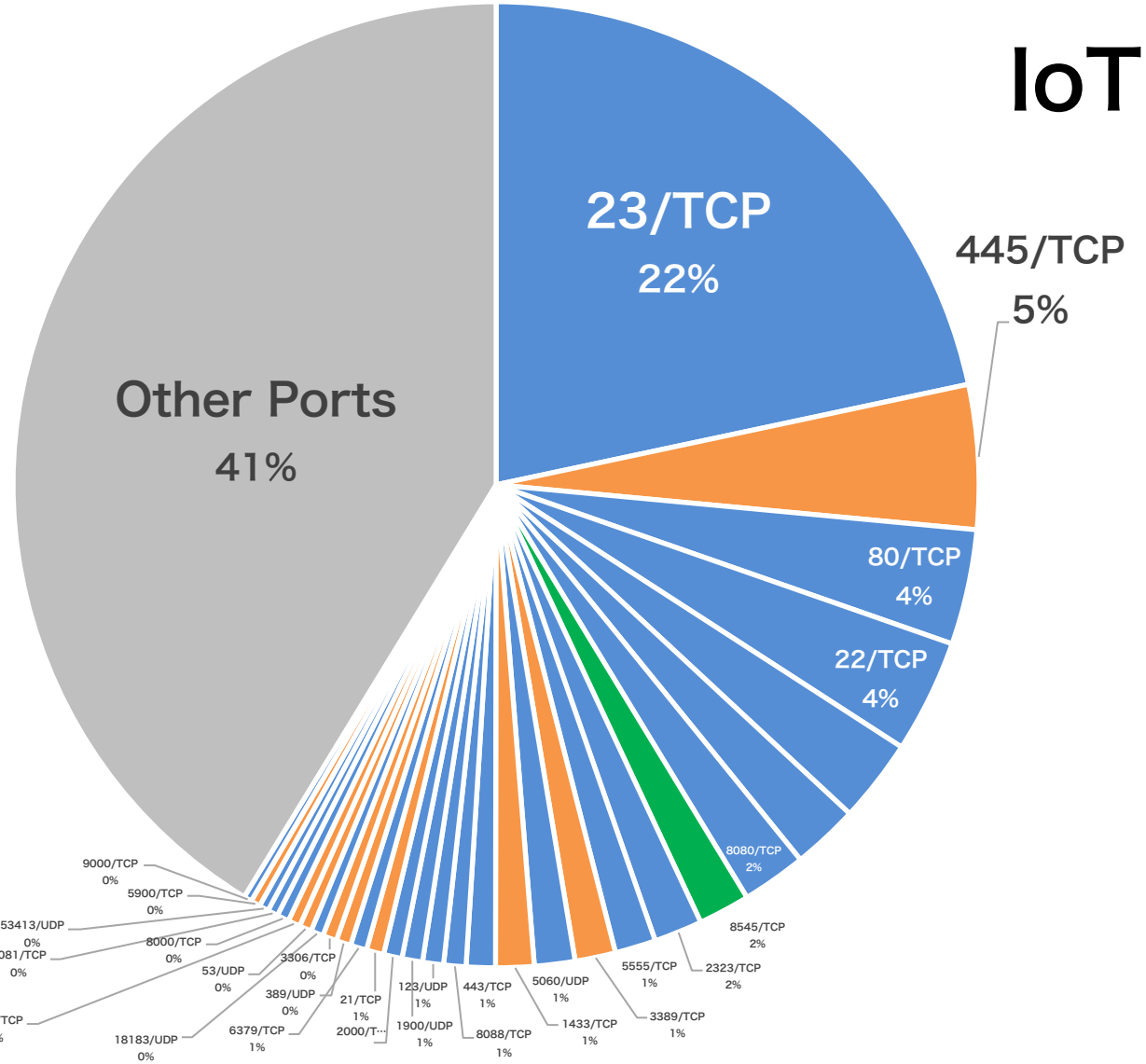




NOTE: Devices are inferred by telnet/web banners

感染機器の分布（2018年）

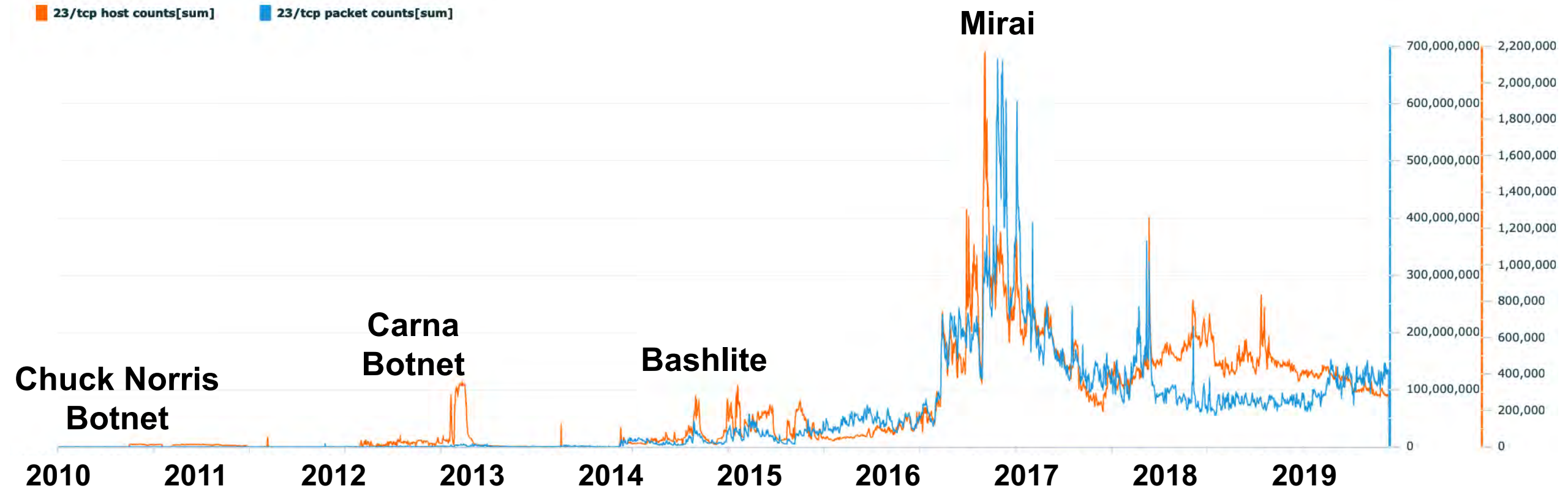
- NICTER 観測レポート 2018：宛先ポート番号別パケット数分布 -



IoT = 47.7%（上位30ポート中）

ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android機器 （セットトップボックス等）

23/TCPのダークネット長期観測（2010-2019）



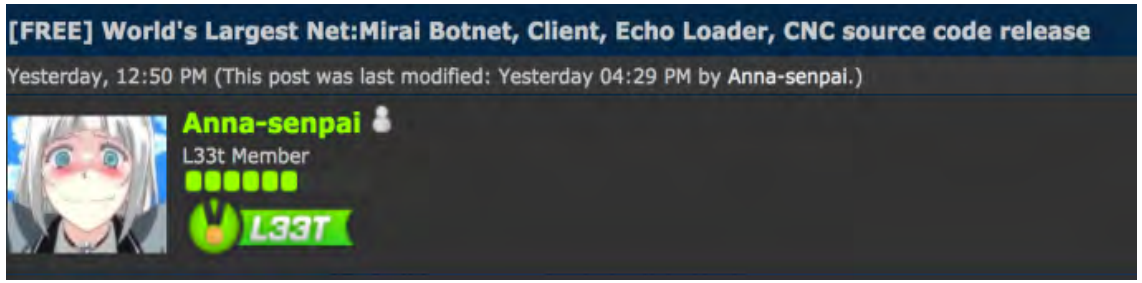
Webカメラ等を悪用した大規模DDoS攻撃（2016）

2016年10月21日

- 米国のDNS事業者Dynに対し大規模なDDoS攻撃が発生
- Amazon, Twitter, PayPal, Spotifyなど多数のサイトに影響
- マルウェア “**Mirai**” に感染したWebカメラ等を悪用して攻撃
- 数百GbpsクラスのDDoSが現実に

Miraiの作者：Annna-sempai

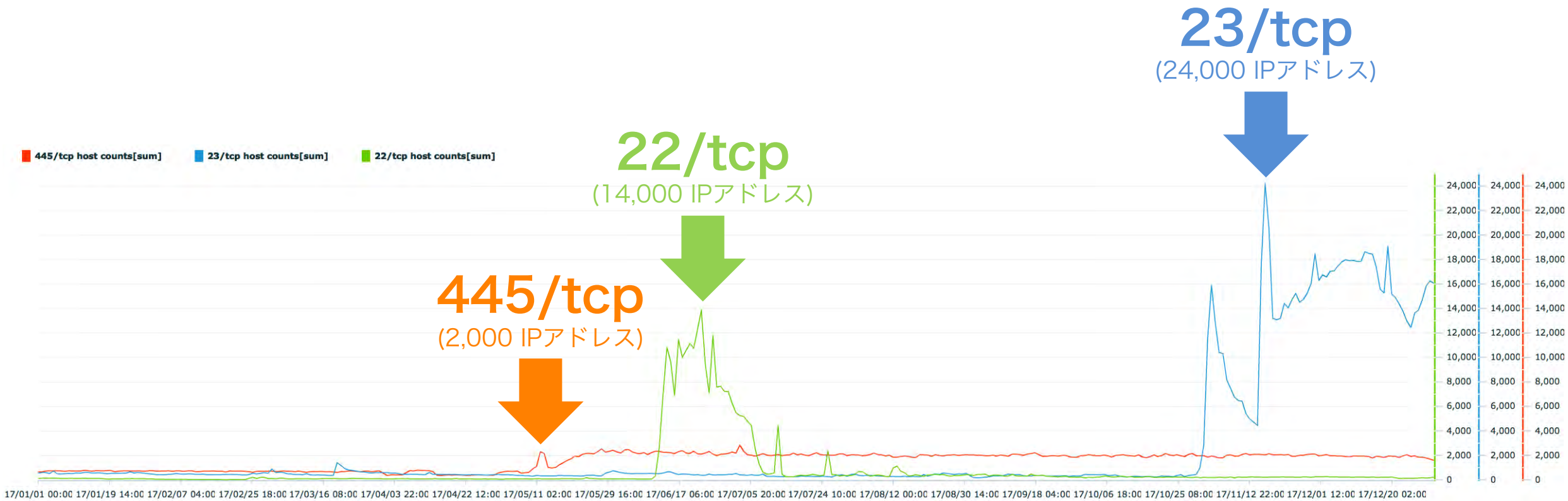
- 2016年9月：MiraiのソースコードをGitHubで公開
- 2017年12月：容疑を認める（米国司法省公表）
- Protraf Solutions LLC（DDoS対策会社）の共同創業者



https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/

日本国内の大規模感染 Top 3（2017）

- 日本国内の送信元IPアドレス数/日 -



2017年1月1日～12月31日

国内の主な感染端末（2017）

- **445/tcp (SMB)**
  - ✓ 2017年5月～
  - ✓ Windows（WannaCry）

出典：Symantec
https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99

- **22/tcp (SSH)**
  - ✓ 2017年6月～
  - ✓ 国内モバイルルータ

出典：週刊アスキー
http://weekly.ascii.jp/elem/000/000/404/404196/

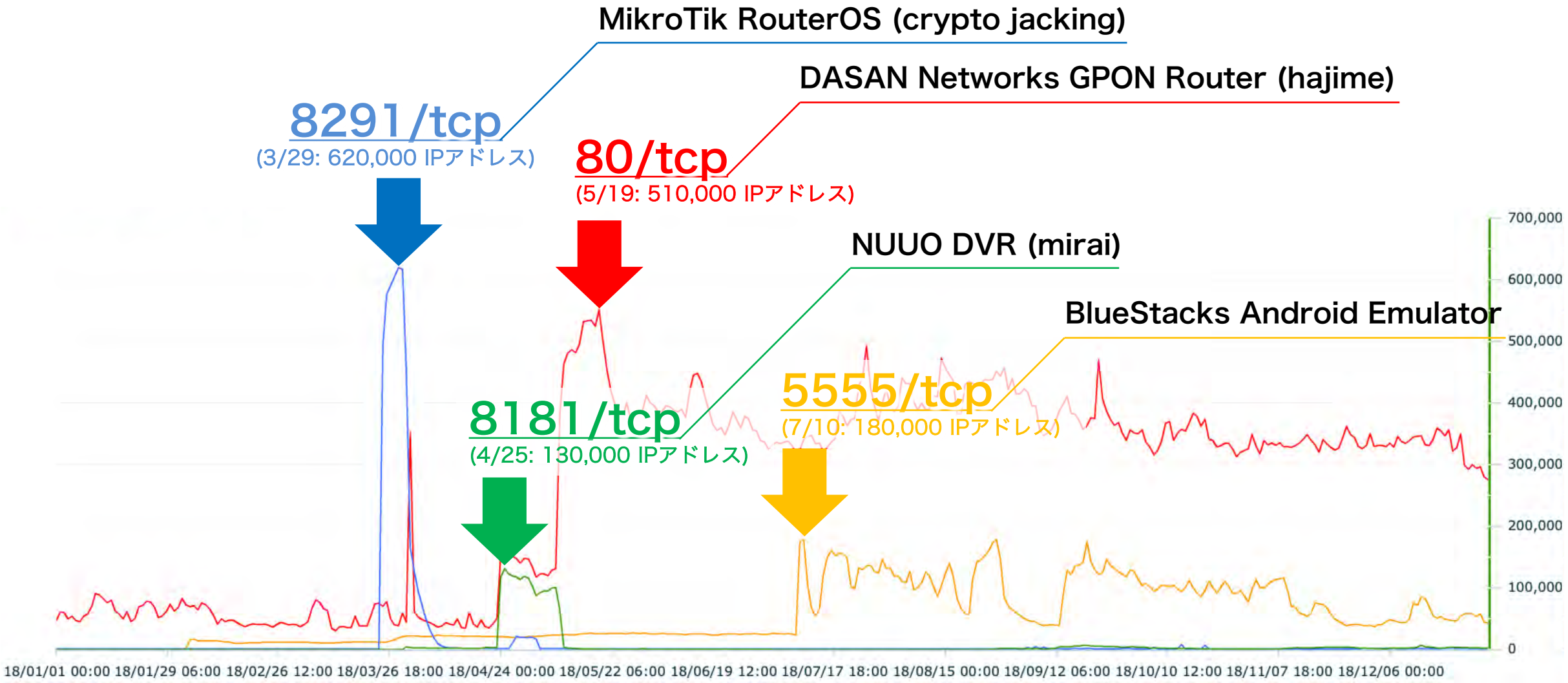
- **23/tcp (telnet)**
  - ✓ 2017年11月～
  - ✓ 国内ホームルータ

出典：Logitec
http://www.logitec.co.jp/info/wireless-router.html

国内における脆弱性ハンドリング

- Coordinated Vulnerability Disclosure -

2018年の主な大規模感染事例



ユニークホスト数/日（2018年1月～12月）

NASAからの機密データ流出（2019）

- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」

米航空宇宙局（NASA）のジェット推進研究所（JPL）の研究データが昨年、サイバー攻撃により盗まれていたことが、米連邦政府の監察総監室（OIG）が6月18日付で公開した報告書（リンク先はPDF）で明らかになった。

2018年4月にJPLのネットワークに侵入した攻撃者が約10カ月の間ネットワーク内の多数の脆弱性を利用して行動範囲を広げ、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ。深宇宙通信情報網DSN（ディープスペースネットワーク）のデータにもアクセスした痕跡があるため、JPLのネットワークからDSNの宇宙飛行関連システムを切断したという。

DSNのパラボラアンテナ（画像：NASA）

攻撃者の侵入口はJPLのネットワークに無許可で接続していたRaspberry Pi端末だった。本来ならば最高情報責任者室（OCIO）がネットワークに接続するすべての端末を管理しているはずだが、正常に機能していなかった。管理者の1人はOIGに対し、新たに端末を接続する際はセキュリティデータベースに手動で登録することになっているが、更新機能がうまく動かないことがあり、そのまま登録を忘れることがあると語ったという。

GIZMODO

NASAの機密文書を盗んだハッカー、利用したのはRaspberry Pi

2019.06.27 20:00

Victoria Song - Gizmodo US［原文］（岡本玄介）

Image: Getty Images

GIGAZINE

19万点超 著作権フリー音楽

日本最大級のBGM・効果音販売サービス「オーディオストック」 - Audiostock

2019年06月25日 19時00分　セキュリティ

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明

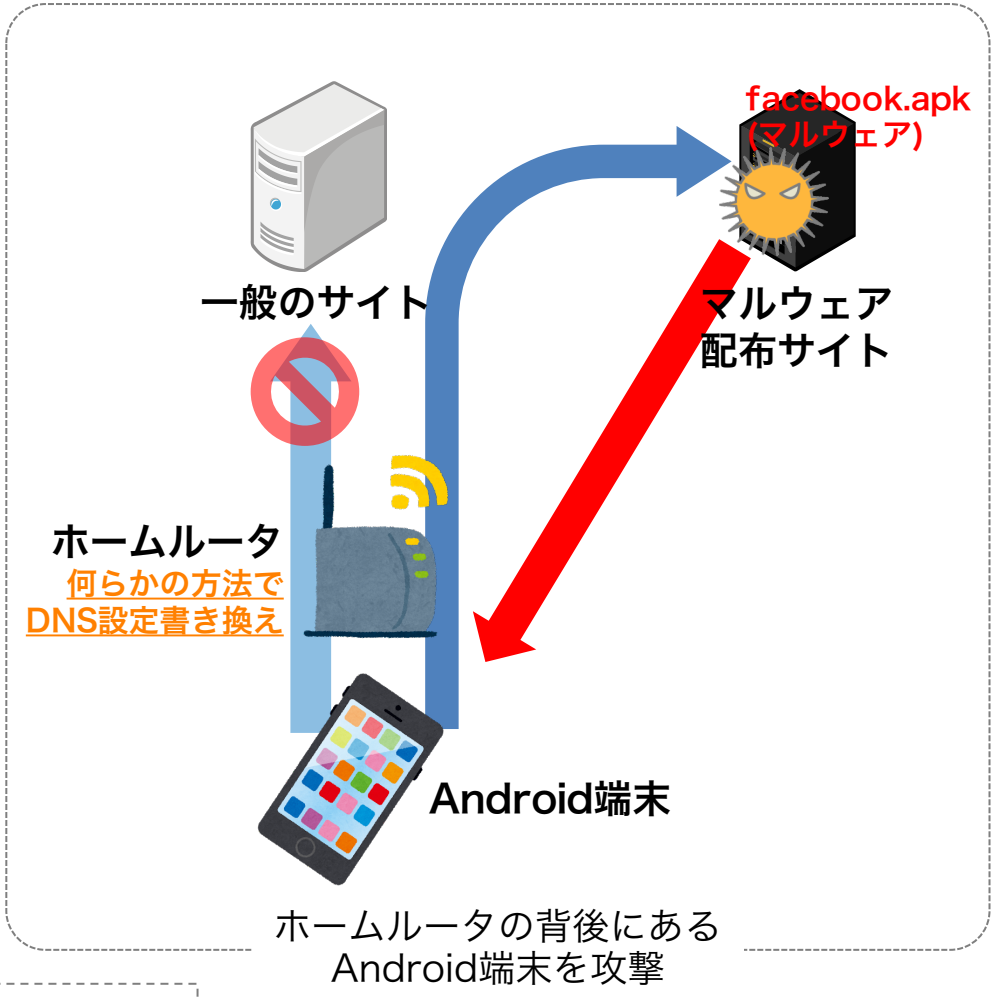
by Les Pounder

アメリカ航空宇宙局(NASA)は、2018年にジェット推進研究所(JPL)のネットワークがハッキングされたことを確認しました。報告によると、ハッキングをしかけたクラッカーは、JPLのネットワークに無許可で接続されたRaspberry Piを侵入口として、データを盗み出したとのことです。

https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/
https://www.gizmodo.jp/2019/06/nasa-hacker-raspberry-pi.html

高度化するIoT機器への攻撃

- **2016年以前**
  - デフォルトID/パスワードでログインし感染
- **2017年**
  - デフォルトID/パスワードでログインし感染
  - IoT機器の**脆弱性を攻撃**して感染
- **2018年**
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
  - IoT機器の**背後にある機器を攻撃**



ホームルータの背後にある
Android端末を攻撃

NICTER Blog
"Wi-Fi ルータの DNS 情報の書換え後に発生する事象について,"
https://blog.nicter.jp/2018/03/router-dns-hack/ (Posted on 2018-03-26)

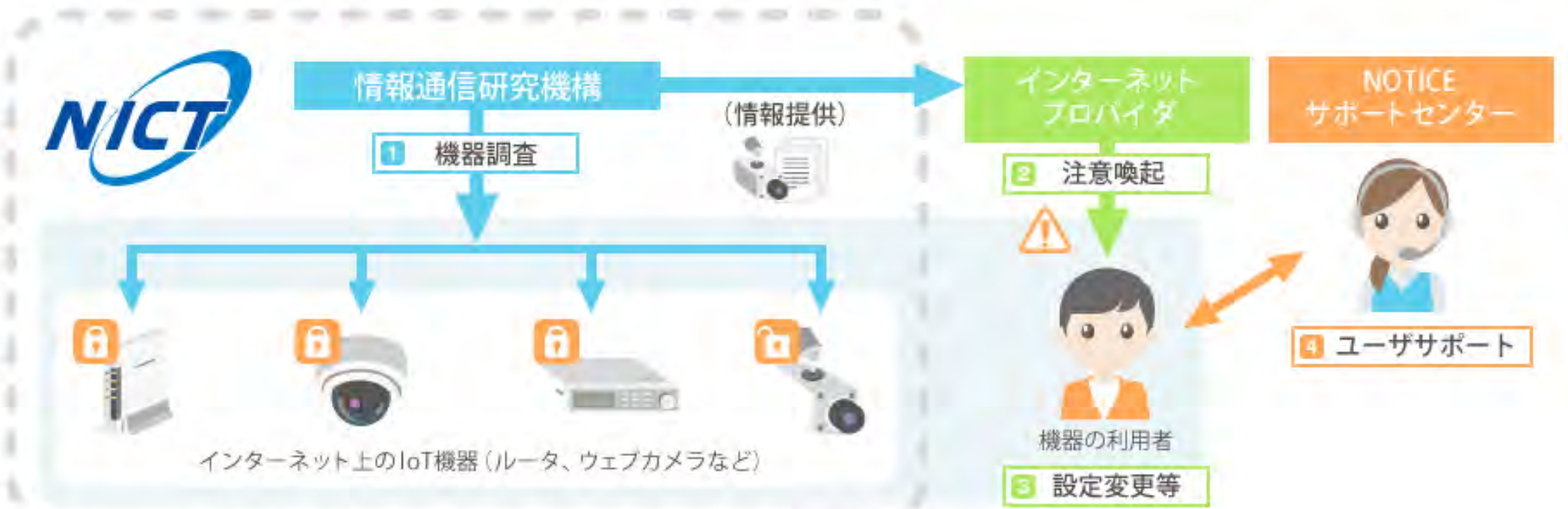
まずは…

容易に推測されるID/パスワード

で動いているIoT機器をなんとかしたい！

NOTICE

- NOTICE: National Operation Towards IoT Clean Environment
- 総務省、NICT、ISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組



https://notice.go.jp/

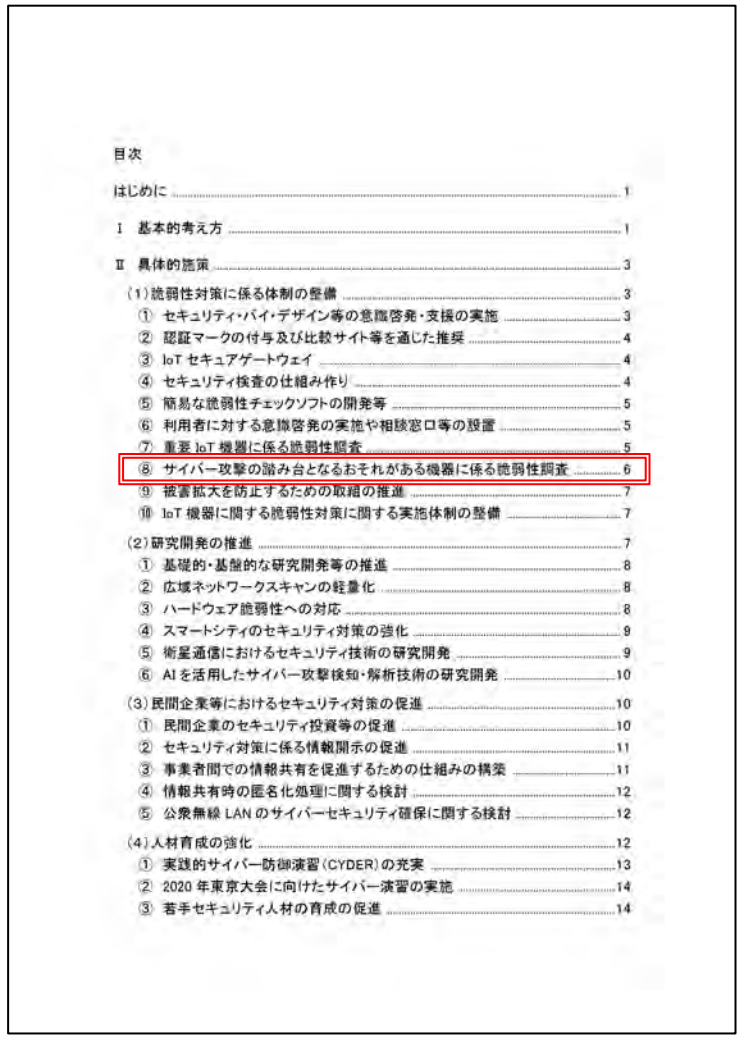
IoTセキュリティ総合対策（2017年10月3日公表）

別紙

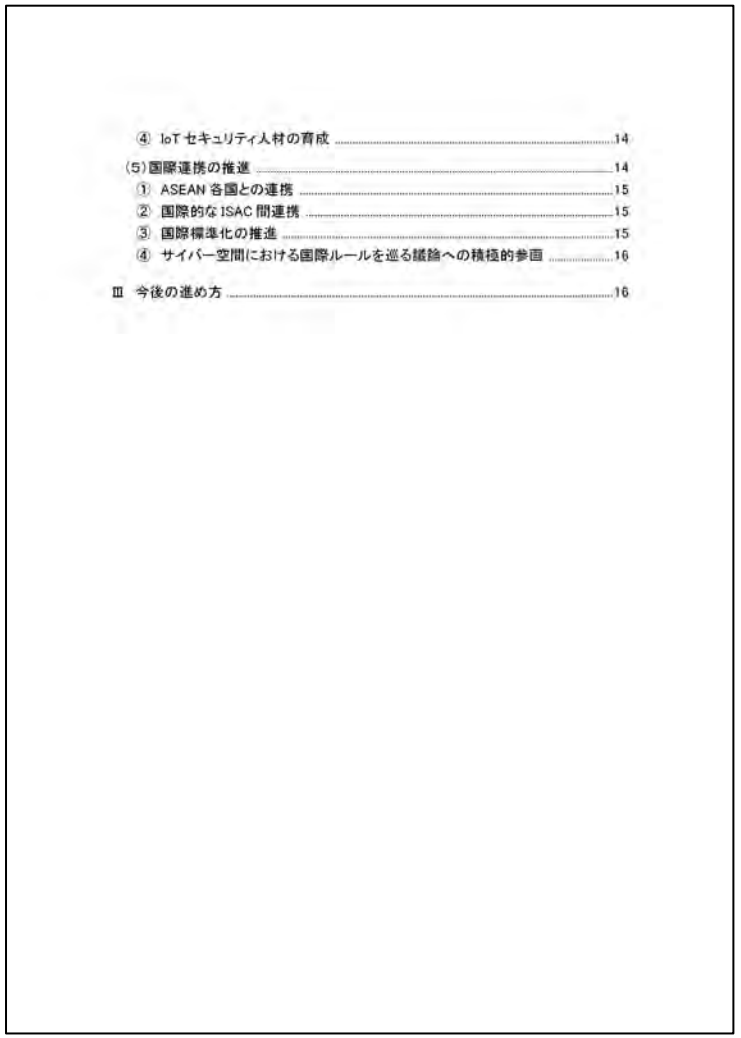
IoT セキュリティ総合対策

平成 29 年 10 月

サイバーセキュリティタスクフォース



目次



出典：総務省 サイバーセキュリティタスクフォース「IoTセキュリティ総合対策」
http://www.soumu.go.jp/main_content/000510701.pdf

NICT法改正のタイムライン

2017/10/3 総務省 サイバーセキュリティタスクフォース「 IoTセキュリティ総合対策」 公表

2018/3/6 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」 第196回国会（常会）提出

5/23 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」 公布

8/24 総務省「識別符号の基準並びに実施計画への記載事項及び認可手続等を定める省令」 意見募集

10/19 総務省「識別符号の基準並びに実施計画への記載事項及び認可手続等を定める省令」 意見募集結果公表

11/1 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」 施行

2019/1/25 業務実施計画書 認可日

2/20 NOTICE調査業務開始

国立研究開発法人情報通信研究機構法（NICT法）

第十四条

機構は、第四条の目的を達成するため、次の業務を行う。

一　情報の電磁的流通及び電波の利用に関する技術の調査、研究及び開発を行うこと。

二　宇宙の開発に関する大規模な技術開発であって、情報の電磁的流通及び電波の利用に係るものを行うこと。

三　周波数標準値を設定し、標準電波を発射し、及び標準時を通報すること。

四　電波の伝わり方について、観測を行い、予報及び異常に関する警報を送信し、並びにその他の通報をすること。

五　無線設備（高周波利用設備を含む。）の機器の試験及び較こう正を行うこと。

六　前三号に掲げる業務に関連して必要な技術の調査、研究及び開発を行うこと。

七　第一号に掲げる業務に係る成果の普及としてサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）に関する演習その他の訓練を行うこと。

八　前号に掲げるもののほか、第一号、第二号及び第六号に掲げる業務に係る成果の普及を行うこと。

九　高度通信・放送研究開発を行うために必要な相当の規模の施設及び設備を整備してこれを高度通信・放送研究開発を行う者の共用に供すること。

十　高度通信・放送研究開発のうち、その成果を用いた役務の提供又は役務の提供の方式の改善により新たな通信・放送事業分野の開拓に資するものの実施に必要な資金に充てるための助成金を交付すること。

十一　海外から高度通信・放送研究開発に関する研究者を招へいすること。

十二　情報の円滑な流通の促進に寄与する通信・放送事業分野に関し、情報の収集、調査及び研究を行い、その成果を提供し、並びに照会及び相談に応ずること。

十三　科学技術・イノベーション創出の活性化に関する法律（平成二十年法律第六十三号）第三十四条の六第一項の規定による出資並びに人的及び技術的援助のうち政令で定めるものを行うこと。

十四　前各号に掲げる業務に附帯する業務を行うこと。

国立研究開発法人情報通信研究機構法（NICT法）

附　則

第八条

２　機構は、第十四条及び前項に規定する業務のほか、平成三十六年三月三十一日までの間、次に掲げる業務を行う。

一　特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。

二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと。

イ　電気通信事業者　当該電気通信事業者

ロ　電気通信事業者（電気通信事業法（昭和五十九年法律第八十六号）第百十六条の二第二項第一号イに該当するものに限る。第八項において同じ。）の利用者　当該電気通信事業者

三　前二号に掲げる業務に附帯する業務を行うこと。

国立研究開発法人情報通信研究機構法（NICT法）

附　則

第八条

７　第二項から第四項までの規定により機構の業務が行われる場合には、次の表の上欄に掲げる規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句とする。

不正アクセス行為の禁止等に関する法律第二条第四項第一号	及び当該	、当該
	を除く	及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第九条の認可を受けた同条の計画に基づき同法附則第八条第二項第一号に掲げる業務に従事する者がする同条第四項第一号に規定する特定アクセス行為を除く

特別法は一般法に優先する。

(NICT法)　(不正アクセス禁止法)

不正アクセス行為の禁止等に関する法律

第二条

４　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

不正アクセス行為の禁止等に関する法律

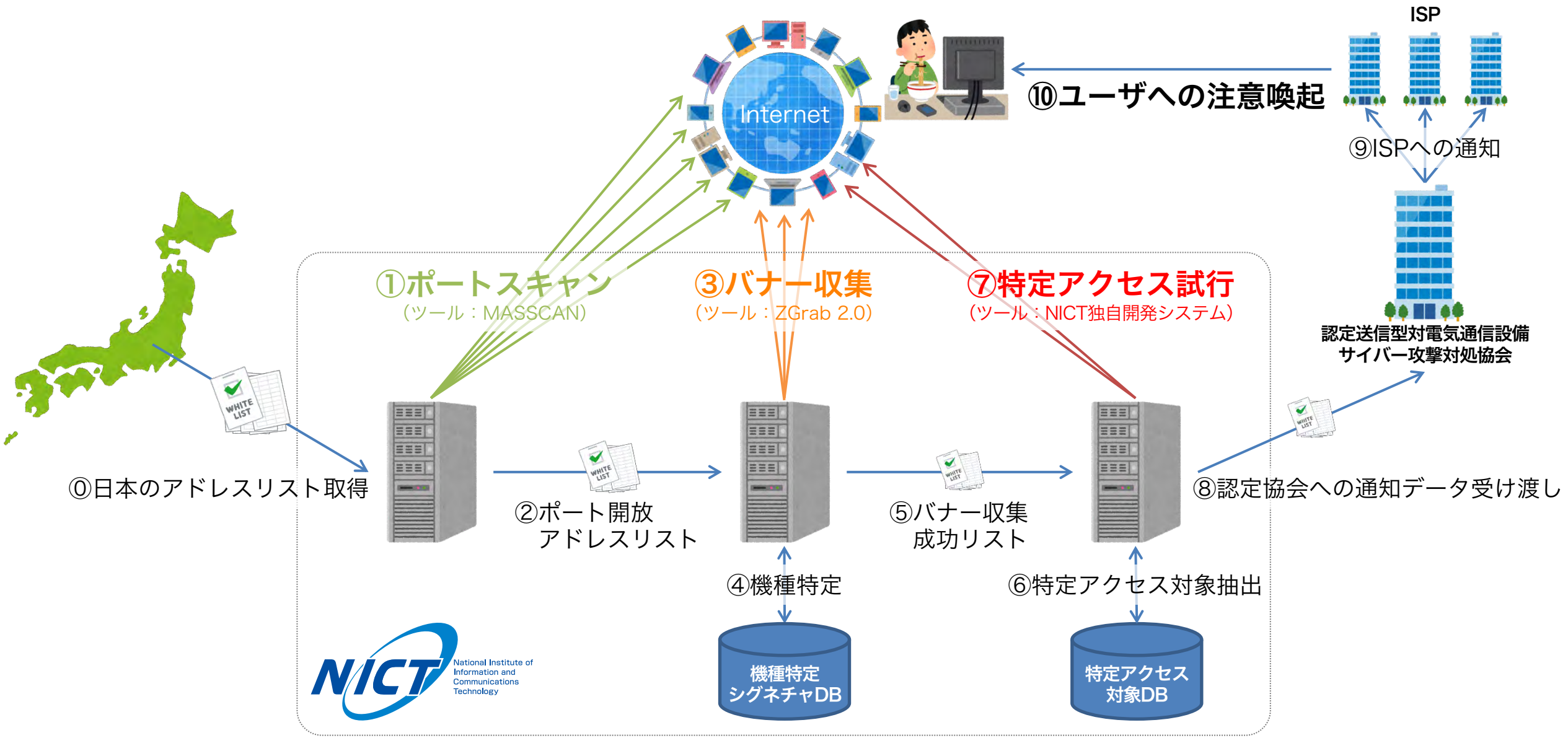
第二条

４　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの、当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするもの及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第九条の認可を受けた同条の計画に基づき同法附則第八条第二項第一号に掲げる業務に従事する者がする同条第四項第一号に規定する特定アクセス行為を除く。）

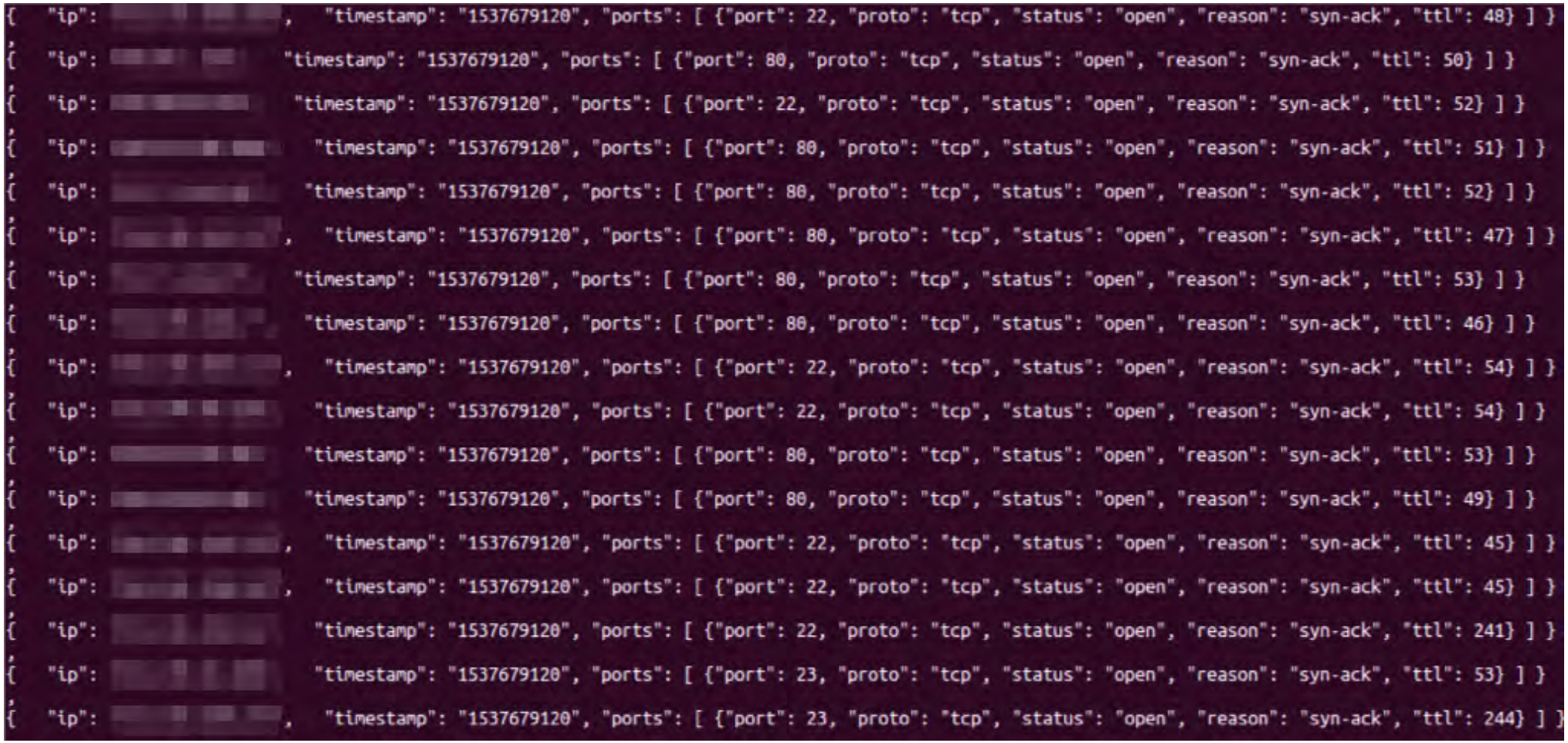
NICTの特定アクセス行為は
不正アクセス行為からは除外される。

NICTによるIoT機器調査の技術詳細



ポートスキャン（MASSCAN）結果例

- ポート開放状態のIPアドレスが1行で記述される



MASSCANの結果ファイル（JSON出力）のサンプル

バナー収集（ZGrab 2.0）結果例

- 1つのIPアドレスの各ポートのバナー収集結果が記述される


```
{
  "ip": [redacted]
  "data": {
    "23/telnet": {
      "status": "success",
      "protocol": "telnet",
      "result": {
        "banner": "\r\r\nmdm MDM9607.LE.2.0-00055-STD.PROD URoad-FHC100\r\n\r\r\n\r\r\nURoad-FHC100 login: ",
        "will": [
          {
            "name": "Echo",
            "value": 1
          },
          {
            "name": "Suppress Go Ahead",
            "value": 3
          }
        ],
        "do": [
          {
            "name": "Echo",
            "value": 1
          },
          {
            "name": "Negotiate About Window Size",
            "value": 31
          }
        ]
      },
      "timestamp": "2018-12-10T14:26:44+09:00"
    },
    "[redacted]": {
      "status": "connection-timeout",
      "protocol": [redacted],
      "result": {},
      "timestamp": "2018-12-10T14:26:55+09:00",
      "error": "dial tcp [redacted] connect: connection refused"
    },
    "[redacted]": {
      "status": "success",
```


Zgrab 2.0の結果ファイル（JSON出力）のサンプル

能動的対策と受動的対策

能動的対策

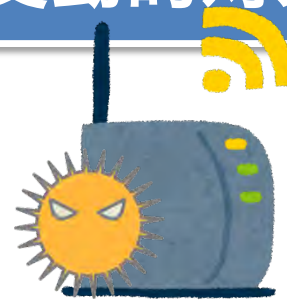
パスワード設定等に
不備があるIoT機器

能動的観測

NOTICE
National Operation Towards IoT Clean Environment

通知

受動的対策

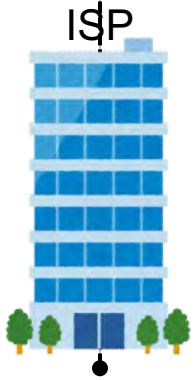


感染IoT機器

受動的観測

NICTER

通知



ISP

NOTICE 注意喚起の実施状況（2019年10月25日）

NOTICE National Operation Towards IoT Clean Environment（アクティブスキャン）　NICTER（パッシブモニタリング）

NOTICEの取組結果	マルウェアに感染しているIoT機器の利用者への注意喚起の取組結果
調査対象となったIPアドレスのうち、 ID・パスワードが入力可能であったもの → **約98,000件** 上記の内、ID・パスワードによりログインでき、 注意喚起の対象となったもの → **延べ505件**	ISPに対する通知の対象となったもの → **1日当たり80～559件**

出典：総務省、NICT、ICT-ISAC “脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況（2019年度第2四半期）”
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html

まとめ： IoTセキュリティ

●NOTICEの舞台裏

- ✓IoT機器への攻撃の激化
- ✓NICT法改正
- ✓IoT機器調査の技術詳細

●NOTICEのこれから

- ✓これまで：抑制的なIoT機器調査
- ✓これから：
  - 調査対象ポートの拡大
  - ID/パスワードの増加
  - 機器特定能力の強化
  - 効果測定　　etc. etc...

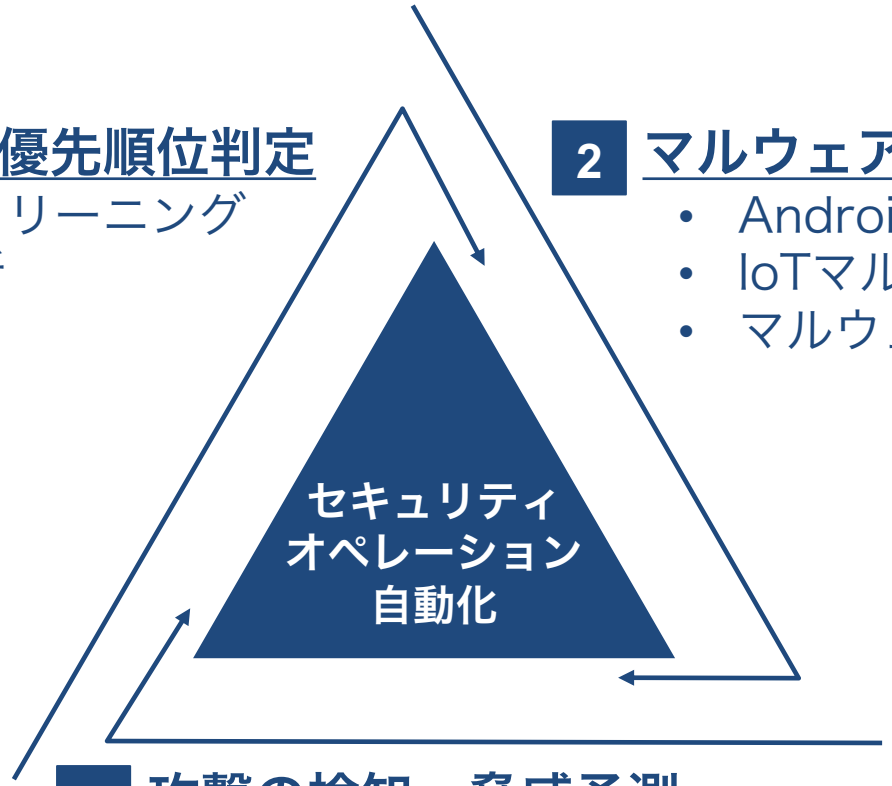
IoT機器調査業務は試行錯誤を重ねつつ
NICT職員が厳粛に進めておりますので
ご理解の程よろしくお願いいたします。

AIとサイバーセキュリティ

- NICTにおけるサイバーセキュリティと機械学習の融合研究 -

NICTにおけるAIとサイバーセキュリティの融合研究

- AIとサイバーセキュリティの融合で、各種の**自動分析技術**や**セキュリティ・オペレーションの自動化**について研究開発を推進



1 インシデントの優先順位判定
- アラートスクリーニング
- 脆弱性の分析

2 マルウェア機能分析自動化
- Androidアプリおよびマーケット分析
- IoTマルウェア分析
- マルウェア自動分析ツール開発

3 攻撃の検知・脅威予測
- ダークネット分析
- ユーザトラフィックの異常検出
- 脅威予測

NICTが保有するサイバーセキュリティ関連情報例

カテゴリ	蓄積データの具体例
ダークネット関連情報	未使用IPアドレス空間で観測したパケット、その統計情報、など
ライブネット関連情報	NICT内部のトラフィックやフロー情報、など
アラート情報	NICT内部のセキュリティ機器群のアラート情報、など
エンドポイント情報	NICT内部のPC端末内のプロセス情報、通信履歴、感染情報、など
マルウェア関連情報	マルウェア検体、静的解析結果、動的解析結果、など
スパム関連情報	スパム（ダブルバウンス）メール情報、など
Android関連情報	Android APK、カテゴリや説明文などアプリのメタデータ、など
ブログ・SNS情報	セキュリティベンダーブログ、ツイート、など
Webクローラ取集情報	URLリストやWebコンテンツ、それらの評価結果、など
ハニーポット収集情報	高対話型/低対話型/DRDoSハニーポット観測情報、など
脅威情報	有償/無償の脅威情報、IP/URLレピュテーション、C&C情報、など

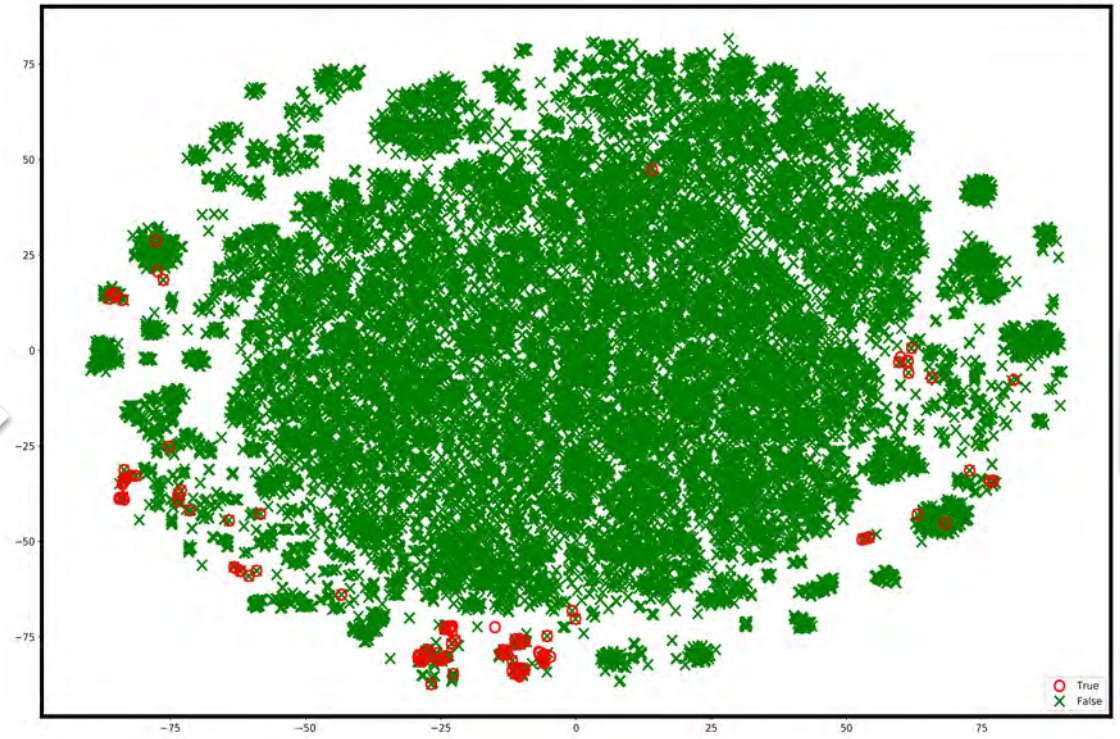
機械学習によるアラートのスクリーニング

- セキュリティ機器群から出る**大量のアラートを機械学習**※1**を用いて自動分類**
- 重要度の低いアラートをスクリーニングして**87%のアラートの削減に成功**[3]

※1 isolation forest

セキュリティ機器群

大量のアラート



t-SNEによるアラート情報の2次元マッピング
（赤：True Positive、緑：False Positive）

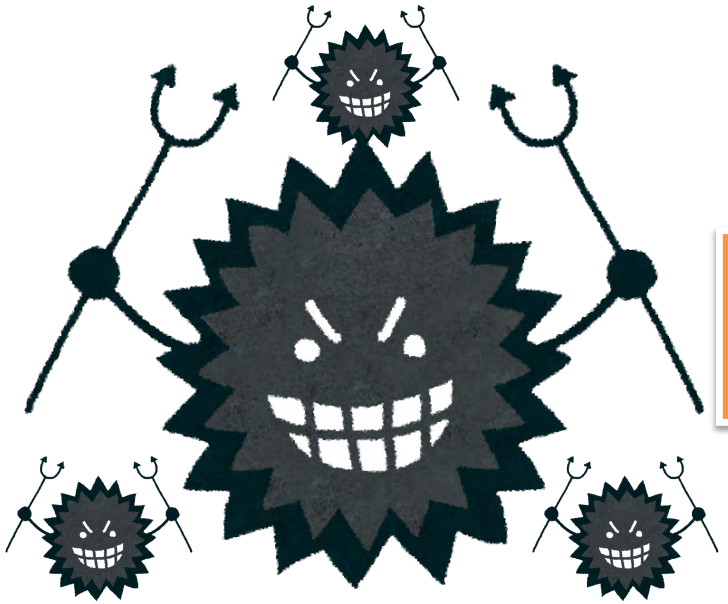
アラートの大幅削減

セキュリティオペレーションの効率化

[3] M. E. Aminanto et al., “Combating Threat-Alert Fatigue with Online Anomaly Detection using Isolation Forest,” ICONIP’19, Dec 2019. (to appear)

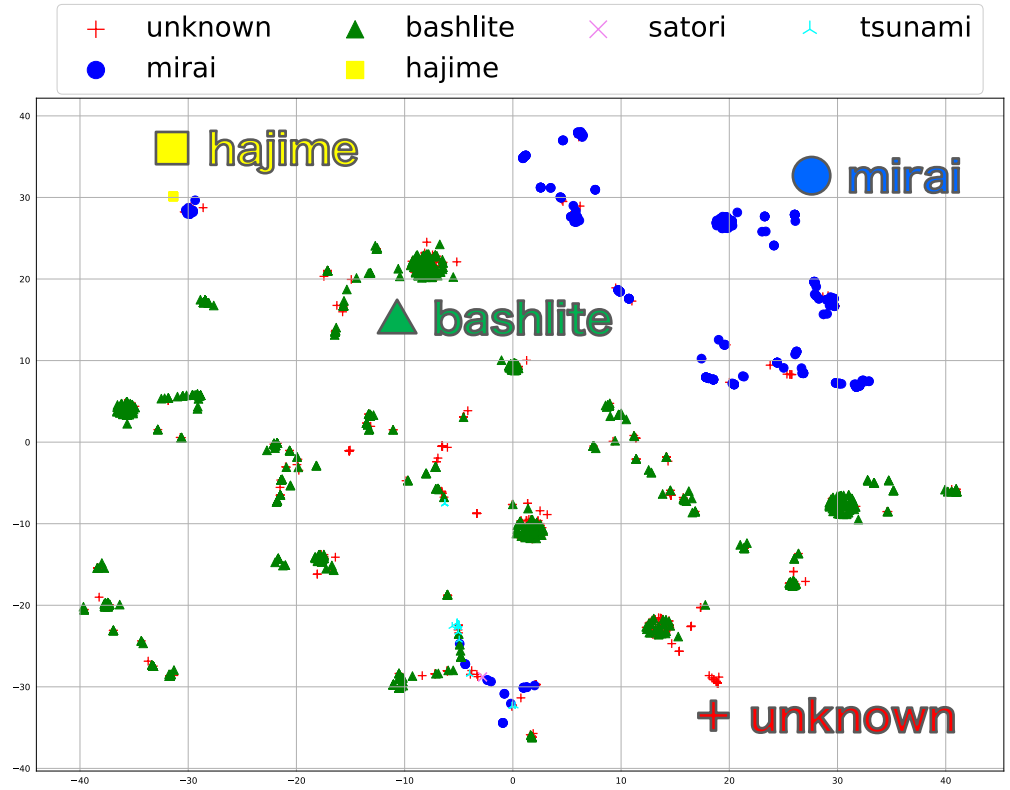
機械学習によるIoTマルウェアの自動分類

- IoTマルウェアの**プログラムコードを分割して特徴抽出**[4]
- 機械学習※2を用いて**99%以上の精度でIoTマルウェアの分類に成功**[5] ※2 SVM



未知のIoTマルウェア

特徴抽出し
機械学習で分類



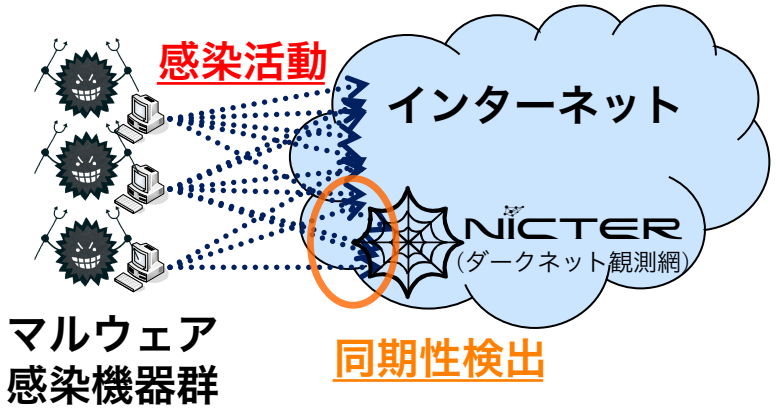
t-SNEによるIoTマルウェアの2次元マッピング

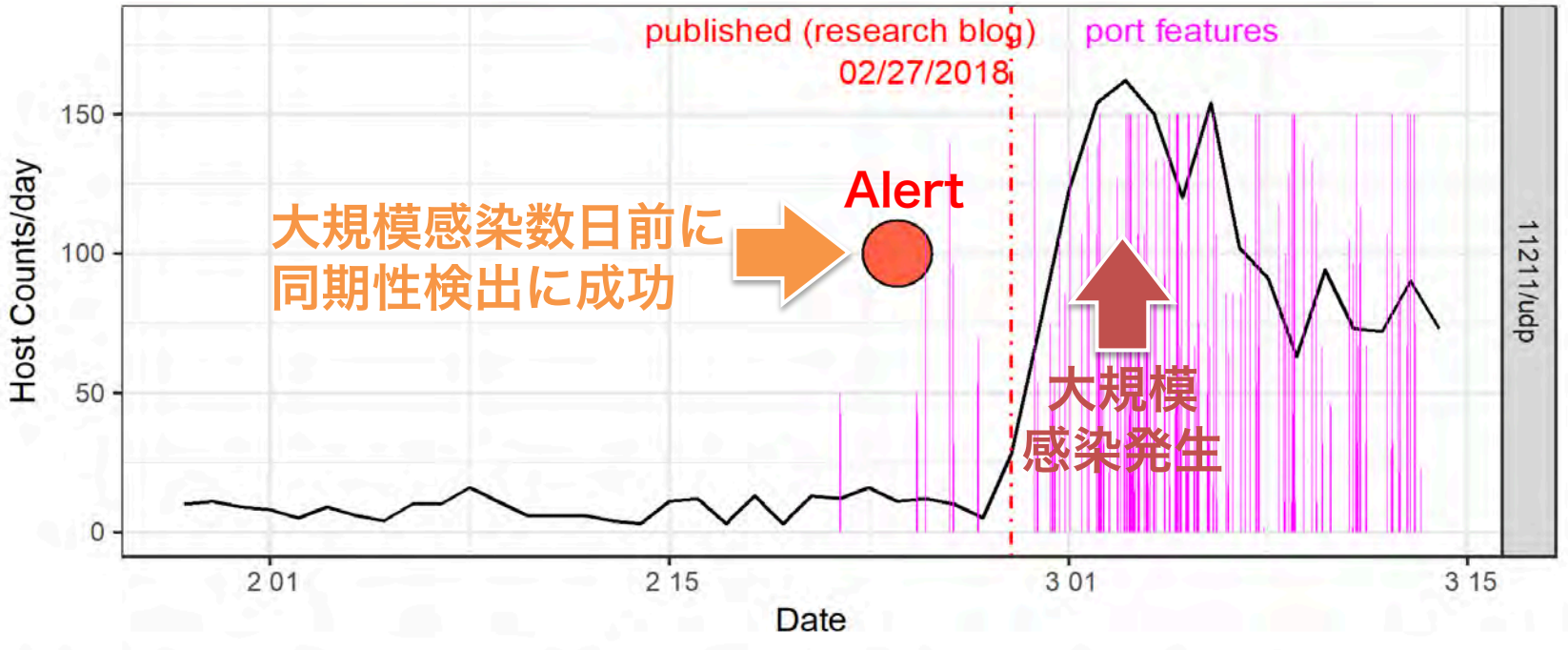
[4] R. Isawa et al., “Evaluating Disassembly-code based Similarity between IoT Malware Samples,” AsiaJCIS 2018, Aug 2018.
[5] T. Ban et al., “A Cross-Platform Study on IoT Malware,” ICMU2018, Oct 2018.

機械学習によるマルウェア大規模感染の早期検出

- マルウェアの感染活動の同期性を機械学習※3によって検出
- マルウェアの大規模感染数日前に同期性の早期検出に成功[6]

※3 tensor decomposition





[6] H. Kaneharaet al., "Real-Time Botnet Detection Using Nonnegative Tucker Decomposition," ACM SAC, 2019, Apr 2019.

AI x Cybersecurity：今後の課題

- **Ground Truth**
  - ✓ 正解ラベル（教師データ）をどう得るのか？
- **誤検知率の低減**
  - ✓ True Positive 99.9% → 8億件のアラートの場合、80万件の誤検知
  - ✓ 6N（99.9999%）のTPは可能か？
- **Explainable AI (XAI)**
  - ✓ 機械学習エンジンの出力の説明可能性をどう向上させるのか？
- **リアルタイム機械学習エンジン**
  - ✓ 動き続ける機械学習エンジン

まとめ：AIとサイバーセキュリティ

- **AIを使ったサイバー攻撃はまだ観測されていない**
  - ✓ 少なくともNICTの各種観測網では未観測
- **AIとサイバーセキュリティの融合研究は世界的トレンド**
  - ✓ NICTはAIとサイバーセキュリティの融合研究を10年以上前から推進
- **実用化までの課題は多い**
  - ✓ 教師データをいかに作るか
  - ✓ リアルタイム性
  - ✓ 説明可能性（XAI）
  - ✓ 研究人材確保　　etc., etc...