セキュリティフォーラム2019@中央大学後楽園キャンパス
3/14/2019

IoT・AIの未来とセキュリティの課題
～CCDSとNICTの視点から～

（一社）重要生活機器連携セキュリティ協議会(CCDS)会長
国立研究開発法人 情報通信研究機構理事長
慶應義塾大学名誉教授
徳田英幸
Hideyuki Tokuda
tokuda@nict.go.jp, hxt@ht.sfc.keio.ac.jp

hide tokuda

CCDSの概要

CCDS

名称：一般社団法人 重要生活機器連携セキュリティ協議会
英名：Connected Consumer Device Security council (CCDS)
設立：2014年10月6日
会長：徳田英幸（情報通信研究機構　理事長、慶應大学 名誉教授）
代表理事：荻野 司（情報セキュリティ大学院大学　客員教授）
理事：後藤厚宏（情報セキュリティ大学院大学 教授、SIP：PD）
松本 勉（横浜国立大学先端科学高等研究院 教授）

会員数：182（正会員以上：50、一般会員：102、学術系：16、協賛:14）（2018年11月）

主な事業：

1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
2. 生活機器の安全と安心を両立するセキュリティ技術の開発
3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

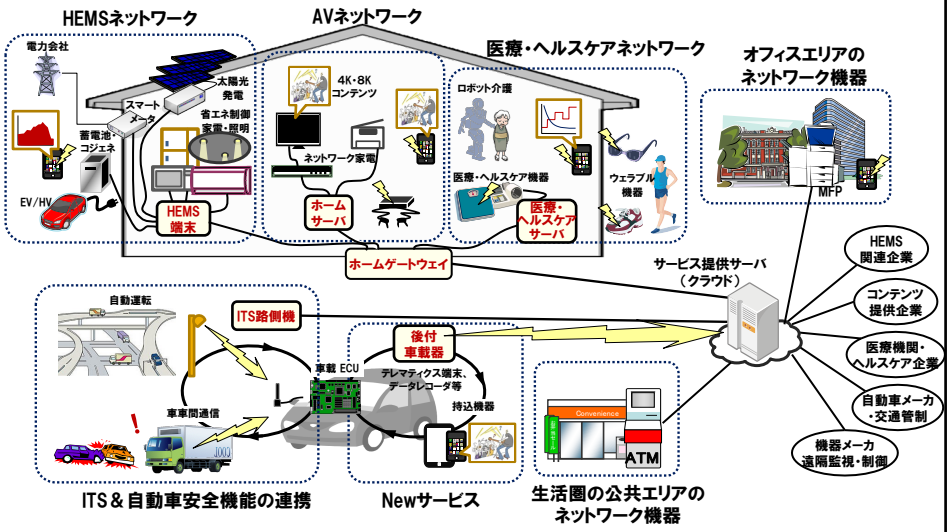
Copyright 2019 Connected Consumer Device Security Council Proprietary

CCDSとは：
重要生活機器におけるセキュリティ事業の創生

CCDS

一般民生機器など あらゆるモノが繋がる “モノのインターネット”

HEMS、AV家電、医療・ヘルスケア、自動車関連機器（ナビ、AV機器等）製品・サービス



Copyright 2019 Connected Consumer Device Security Council Proprietary

CCDSの事業分野

CCDS

検証基盤構築
- 検証業務をサポートする共通基盤開発
  －組込み機器評価・検証基盤システム
- セキュリティ検証ツール開発
  －車載、IoT-GW、ATM、POS分野
- テストベット検討

標準化推進
- セキュリティガイドライン策定
  －セキュリティガイドラインWG
  （車載、IoT-GW、ATM、POS-SWG）
- IoTセキュリティ対策技術の体系化
  －デバイスセキュリティ技術SWG
  －ユーザビリティWG
- ガイドライン国際標準化検討

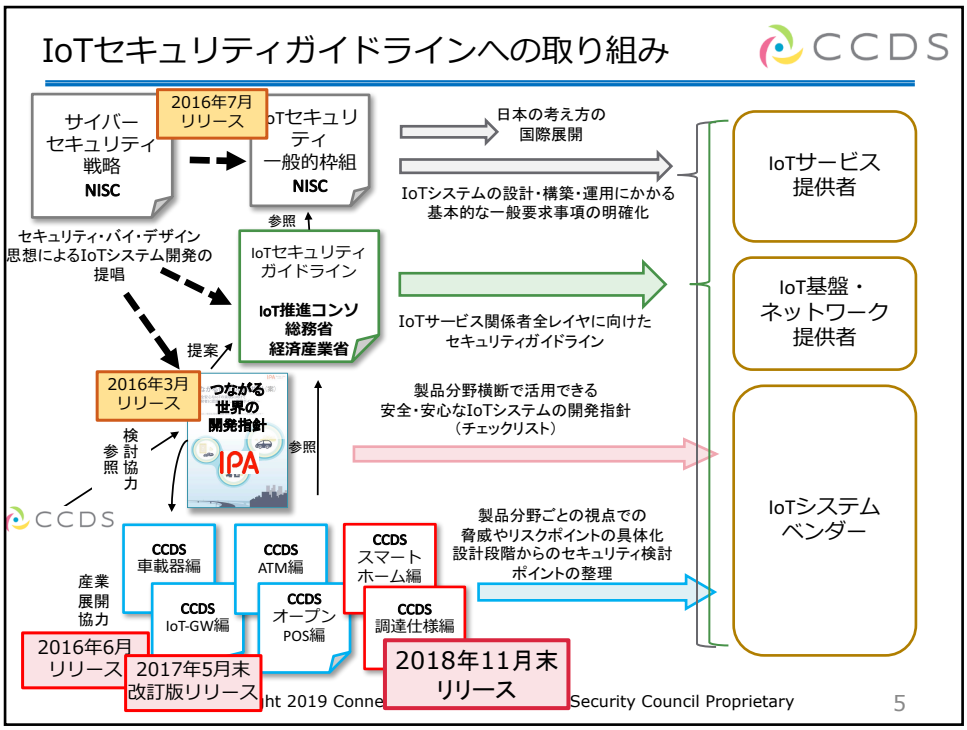
人材育成
- オープンセミナーの開催
  －セキュリティシンポジウム
  －検証技術セミナー
  －CCDSガイドライン勉強会　.etc
- ワークショップの開催
  －検証ツールハンズオン講習会
  －IoTセキュリティ評価検証
  技術講習会

CCDS

動向調査・研究
- 国内外のガイドライン、標準化動向
- 検証手法、検証ツールの調査・研究
- 脅威事例の収集、ハッキング技術調査
- 認証制度の実現に向けた調査

普及啓発
- シンポジウム、セミナーの主催
- 調査資料、ガイドラインの公開
- 提携団体での講演活動

© Connected Consumer Device Security Council Proprietary



IoTセキュリティガイドラインから標準化へ

ISO/IEC JTC 1/SC27

hide tokuda 6

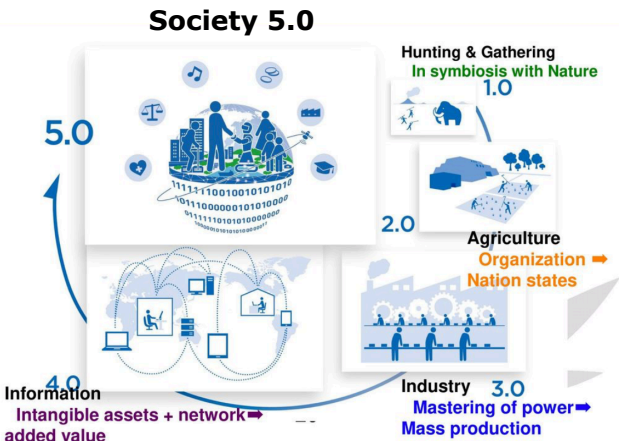
Outline

- IoT・AIの進化のかたち
  - Society 5.0と戦略的課題
- IoT機器への攻撃
  - Connected Car and Wireless Infusion Pump
- IoTセキュリティの課題
  - IoT環境の脅威とリスク
  - セキュリティ人材育成
- まとめ

IoT・AIの進化のかたち

Shaping the Future Society

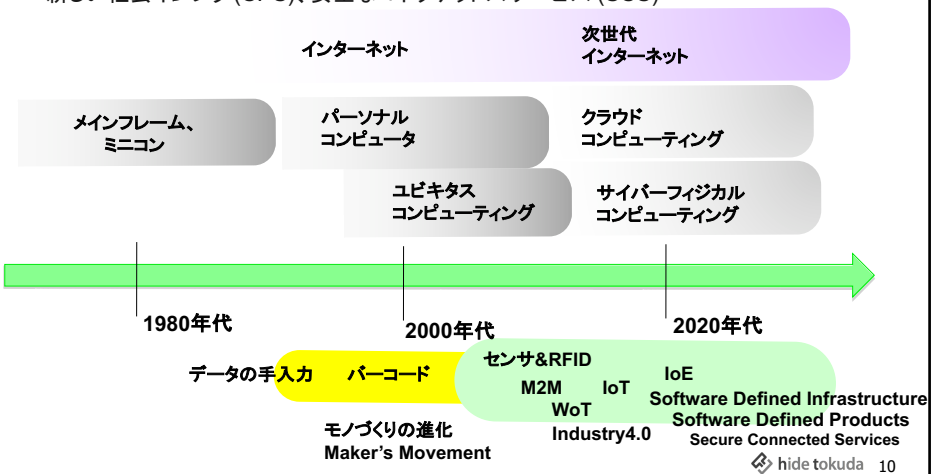
Safe and Secure Society 5.0



hide tokuda 9

2020年-2030年の社会: Society 5.0

- 情報化社会 ―> 高度情報社会 ―> 知能化社会 (機械との共創社会)
- 物理空間と情報空間は融合へ
- 新しい社会インフラ (CPS)、安全なコネクテッドスサービス (SCS)



hide tokuda 10

AI戦略

深層学習を超える次なる信頼できるAI技術(ブレイン指向AI)
公平性, 説明責任, 透明性 and 倫理的/法的/社会的課題（ELSI)

ICT/IoT戦略

センシング/処理・解析(プロセッシング)/作動・制御(アクチュエーション）技術
/Beyond 5G/革新的ネットワーク/量子コンピューティング・量子通信

Data戦略

Data流通促進のためのプラットフォーム
データマーケットプレイス／GDPR-JGDPR/
オープンサイエンスの推進

Security戦略

高度なセキュリティ／プライバシー保護技術開発、セキュリティ人材／質と量
非対称性問題／研究者のセキュリティ

人材戦略

100年時代のジュニア、シニアの育成

テクノロジー シェーピング

新しい技術の創出と社会的受容性の向上

&

社会的イノベーション

新しい社会的枠組みの創出
道路交通法、保険制度、著作権、知的財産権など

IoT・AI環境の光と影

技術的課題と制度的課題

テクノロジーシェピングとソーシャルイノベーション

BlackBox AI vs. Explainable AI

“In-The-Wild” Test, フライトレコーダー, 保険

Mobileye ADAS system’s response image

(https://newsroom.intel.com/editorials/experience-counts-particularly-safety-critical-areas/)

Prof. Amnon Shashua, SVP Intel, CEO & CTO of Mobileeye

EXPERIENCE COUNTS, PARTICULARLY IN SAFETY-CRITICAL AREAS

Now Is the Time for Substantive Conversations about Safety for Autonomous Vehicles

By Prof. Amnon Shashua

Society expects autonomous vehicles to be held to a higher standard than human drivers. Following the tragic death of Elaine Herzberg after being hit last week by a self-driving Uber car operating in autonomous mode in Arizona, it feels like the right moment to make a few observations around the meaning of safety with respect to sensing and decision-making.

First, the challenge of interpreting sensor information. The video released by the police seems to demonstrate that even the most basic building block of an autonomous vehicle system, the ability to detect and classify objects, is a

Mobileeyeによると公開された事故当時の映像を分析すると被害者の人物を衝突の1秒前に検出できてる。Uber車は、何らかの原因で検出できていなかった！

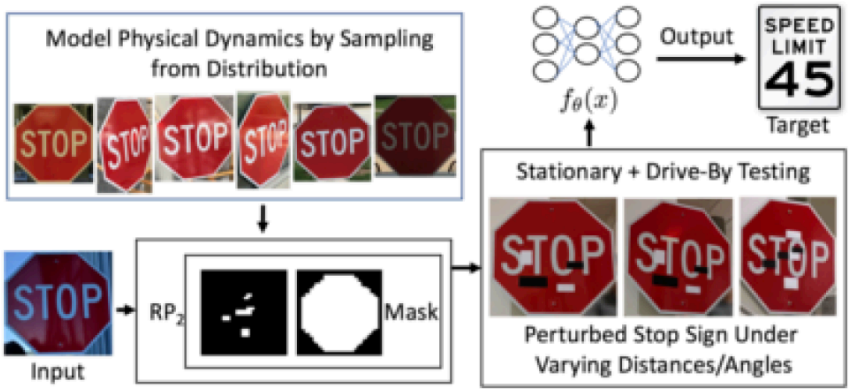
1）Experience Counts (経験）

2) Transparency （透明性）

3) Redundancy （冗長性）

AI(Deep Learning)への攻撃

自動運転車のストップサイン認識への攻撃事例
(by K. Eykholt et al., from CVPR2018)



Outline

- IoT・AIの進化のかたち
  - Society 5.0と戦略的課題
- IoT機器への攻撃
  - Connected Car and Wireless Infusion Pump
- IoTセキュリティの課題
  - IoT環境の脅威とリスク
  - セキュリティ人材育成
- まとめ

IoT機器への攻撃

つながるメリット
vs.
つながるリスク

事例：JEEPハッキング (BlackHat2015)

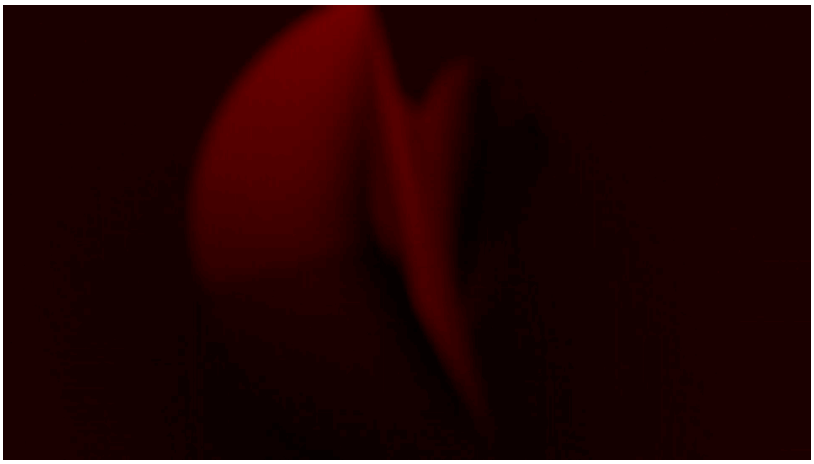
- Jeepを物理的改造なく遠隔から操作できる研究
  - エアコン、ワイパー、ブレーキ、変速、ステアリングに干渉、自動車の情報が常時取得可能 (http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/)
  - 脆弱性：
    - 車載器WiFiが覗けた
    - Sprint3Gネットワーク上のIP網が覗けた
    - V850ECUのファームウェアを改造版に入れ替えられた
  - リコール１４０万台で数十億円規模の損害が発生

- Chryslerのコネクテッドカーシステム「UConnect」の脆弱性を利用
  - エンタメシステムのチップセットのファームウェアを更新
  - エアコン、ワイパー、ブレーキ、変速、ステアリングに干渉
  - バック中にはハンドル操作も奪取
  - ファームウェアの更新なしでもネットワーク内の他の自動車の情報も取得可能
- Chryslerではパッチ提供して対応
  （USBまたは整備工場での更新）

画像.ブレーキ不能で溝に(出典:WIRED)

Jeep2015ハッキング (from wired.com)

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway



セキュリティ研究者のセキュリティ (11/2/2016)

The FTC authorized changes to the Digital Millennium Copyright Act (DMCA) that will allow Americans to do hack their own electronic devices. Researchers can lawfully reverse engineer products and consumers can repair their vehicle's electronics, but the FTC is only allowing the exemptions for a two-year trial run.

engadget

You can now legally hack your own car or smart TV

The FTC's "security research exemption" to the DMCA has kicked in.

Steve Dent , @stevetdent
14h ago in Security

4 Comments

826 Shares

Library of Congress Renewed DMCA Section 1201

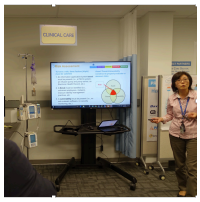
"Smartphones", "home appliances", "home systems"

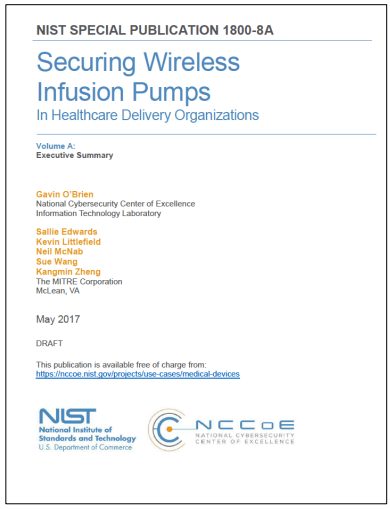
Sponsored

Tiny De
into a B

無線輸液ポンプの脆弱性 (by NIST NCCoE 2017)

- NIST-NCCoEのSP1800-8A レポート
- ヘルスケア提供側のリスク分析
  - 脆弱性をついた攻撃者による侵入
  - 病院情報システムへの攻撃
  - 患者情報やヘルスレコードの漏洩や改ざん
  - ヘルスサービスへの攻撃
  - 組織のレピュテーションへのダメージ





NIST SPECIAL PUBLICATION 1800-8A

Securing Wireless Infusion Pumps
In Healthcare Delivery Organizations

Volume A:
Executive Summary

Gavin O'Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

May 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use-cases/medical-devices

NIST National Institute of Standards and Technology U.S. Department of Commerce
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Outline

- IoT・AIの進化のかたち
  - Society 5.0と戦略的課題
- IoT機器への攻撃
  - Connected Car and Wireless Infusion Pump
- **IoTセキュリティの課題**
  - **IoT環境の脅威とリスク**
  - **セキュリティ人材育成**
- **まとめ**

IoTセキュリティの課題

国、企業・組織、コミュニティ、個人

＜技術的課題と制度的課題＞

コネクテッドサービス
クラウド
ネットワーク
スマートデバイス

hide tokuda 25

新たなサイバーセキュリティ戦略 (by NISC in 2015)

1 サイバー空間に係る認識
- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがインターネットに連接され、サイバー空間と実空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的
- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安定及び我が国の安全保障」に寄与する。

3 基本原則
① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策
①後手から先手へ　／　②受動から主導へ　／　③サイバー空間から融合空間へ

経済社会の活力の向上及び持続的発展
～ 費用から投資へ ～
- 安全なIoTシステムの創出
  安全なIoT活用による新産業創出
- セキュリティマインドを持った企業経営の推進
  経営者の意識改革、組織内体制の整備
- セキュリティに係るビジネス環境の整備
  ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現
～ 2020年・その後に向けた基盤形成 ～
- 国民・社会を守るための取組
  事業者の取組促進、普及啓発、サイバー犯罪対策
- 重要インフラを守るための取組
  防護対象の継続的見直し、情報共有の活性化
- 政府機関を守るための取組
  攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定 及び 我が国の安全保障
～ サイバー空間における積極的平和主義 ～
- 我が国の安全の確保
  警察・自衛隊等のサイバー対処能力強化
- 国際社会の平和・安定
  国際的な「法の支配」確立、信頼醸成推進
- 世界各国との協力・連携
  米国・ASEANを始めとする諸国との協力・連携

横断的施策
- 研究開発の推進
  攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発
- 人材の育成・確保
  ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制
- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会に向けた対応

1

hide tokuda 26

IoT環境の脅威

コネクテッドサービス
DoS攻撃
データ盗み出し/標的型メール攻撃
データ改竄
仮想イメージ改竄・管理コンソール攻撃
＜対策＞
＜予防＞＜検知＞＜診断＞＜追跡＞
＜回復＞＜更新＞＜予知＞

Security by Design
Privacy by Design
クラウドセキュリティ
データ暗号化／暗号化演算技術
プライバシー保護技術

コネクテッドサービス
クラウド
ネットワーク
スマートデバイス

IoTセキュリティの問題点

- 問題点：非対称性問題
  - 攻撃側のコスト << 守備側のコスト
  - 攻撃側人数 >> 守備側人数
  - 攻撃スピード >> 守備スピード
- 流れを変えるには
  - Game Changeをどう進めるか？
    - Security by Design & Privacy by Design
  - デフェンダー・ムーブメントの動き
  - IoTリテラシー教育の普及・啓蒙／人材育成

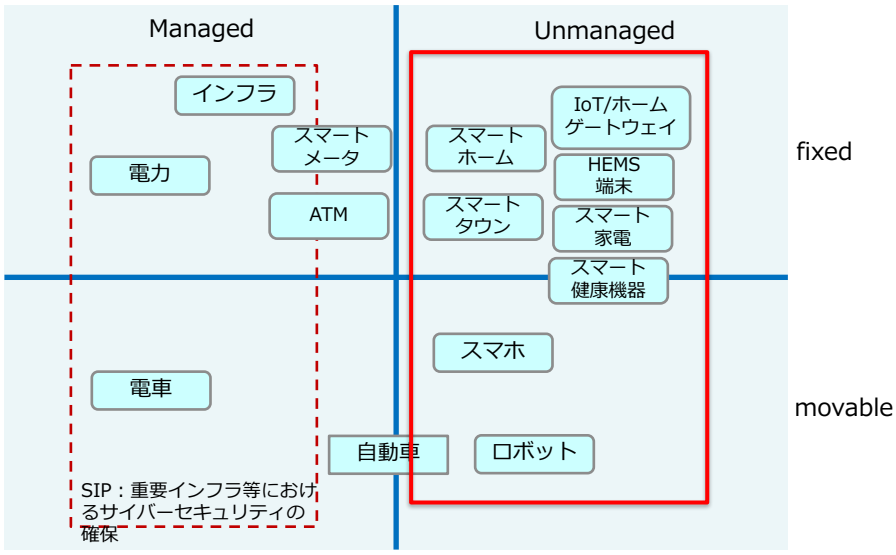
IoT時代のセキュリティ
何が今までと違うのか？

before and after
攻撃のターゲット
攻撃の質と量

“のらIoT”の脅威

管理が行き届いていない“のらIoTデバイス”への攻撃増加
e.g. 横浜国大への攻撃例：2016年1月～6月
約60万台、500種類以上のIoTデバイスから

IoT環境で対象とするシステム



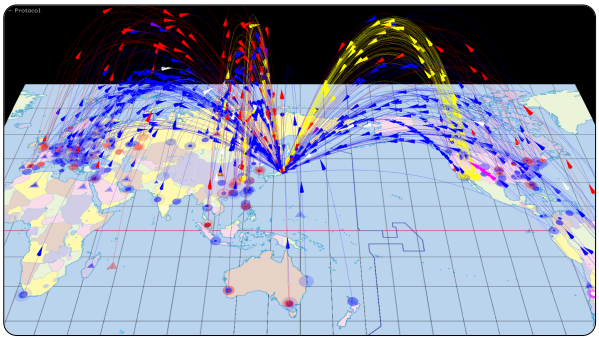
インシデント分析センタ（ニクター）

NICTER

●サイバー攻撃大規模観測・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

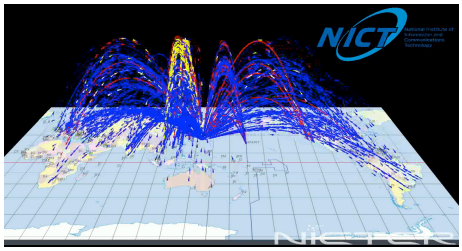


Scanning observation by nicter-Atlas

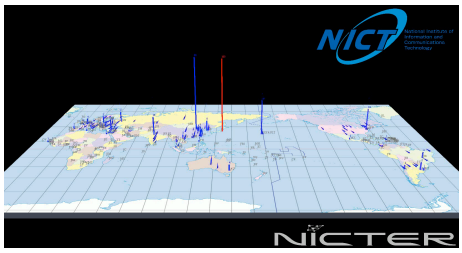
Recently, scanning to IoT related Ports (including Port 23 (telnet)) is getting larger.

- Capturing packets through dark-net in real time basis.
- Color indicates the protocol types.

UDP
TCP SYN
TCP SYN/ACK
TCP Other
ICMP



Atlas All view

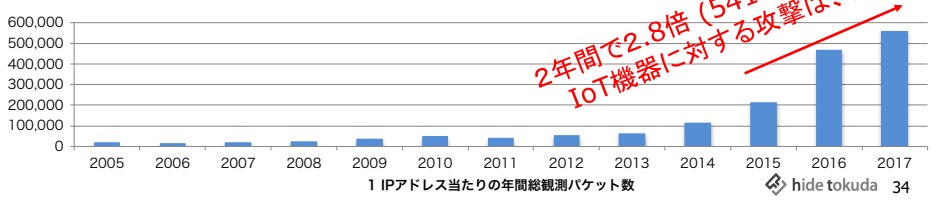


Atlas only IoT related ports

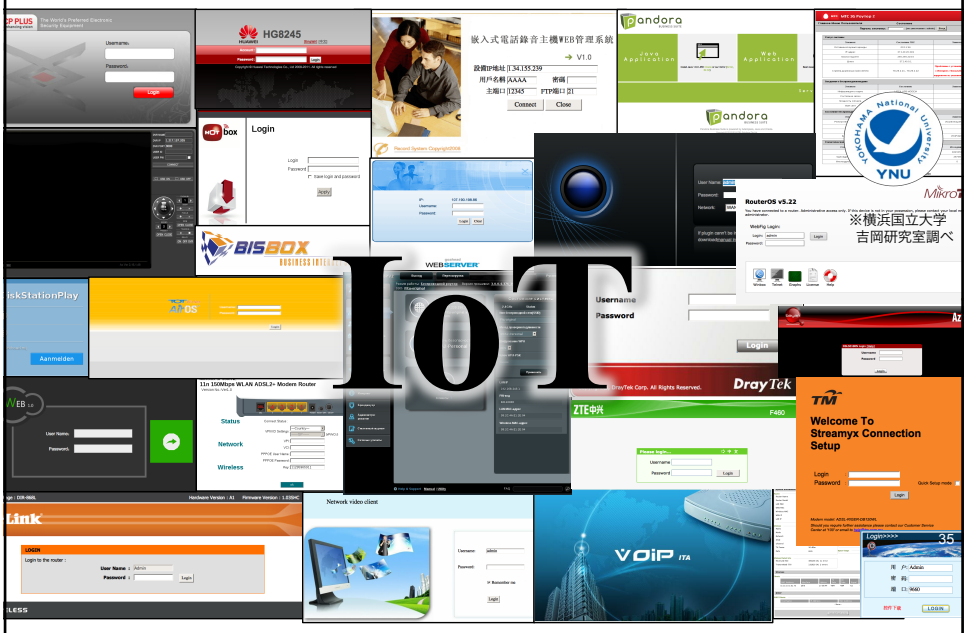
hide tokuda 33

NICTER観測統計（2005-2017）

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



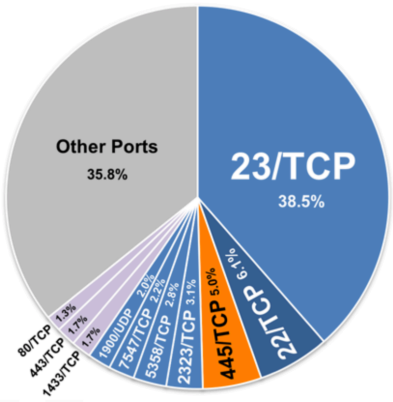
hide tokuda 34



hide tokuda 35

感染機器の分布（2017年）

- 宛先ポート番号別パケット数分布 - (by NICT)



ポート番号	攻撃対象
23/TCP	IoT機器（Webカメラ等）
22/TCP	IoT機器（モバイルルータ等） 認証サーバ（SSH）
445/TCP	Windows（サーバサービス）
2323/TCP	IoT機器（Webカメラ等）
5358/TCP	IoT機器（Webカメラ等）
7547/TCP	IoT機器（Webカメラ等）
1900/UDP	IoT機器（ホームルータ等）
1433/TCP	データベースサーバ（SQL）
443/TCP	Webサーバ（SSL/TLS）
80/TCP	Webサーバ（HTTP）

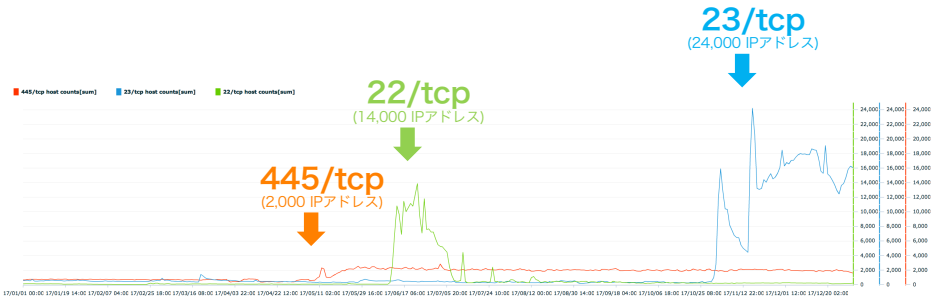
2017: IoT > 54%

(23/TCP + 22/TCP + 2323/TCP + 5358/TCP + 7547/TCP + 1900/UDP)

hide tokuda 36

日本国内の大規模感染 Top 3（2017）

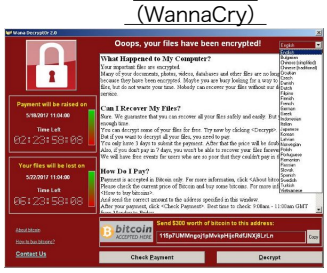
- 日本国内の送信元IPアドレス数/日 -



1/1/2017　～12/31/2017

国内の主な感染端末（2017）(by NICT)

- 445/tcp (SMB)
  - ✓ May 2017～
  - ✓ Windows PC (WannaCry)



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

- 22/tcp (SSH)
  - ✓ Jun. 2017～
  - ✓ Domestic Mobile Router

From: Weekly ASCII
http://weekly.ascii.jp/elem/000/000/404/404196/

- 23/tcp (telnet)
  - ✓ Nov. 2017～
  - ✓ Domestic Home Router

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

IoTデバイスへの攻撃の進化 (2016～2018)

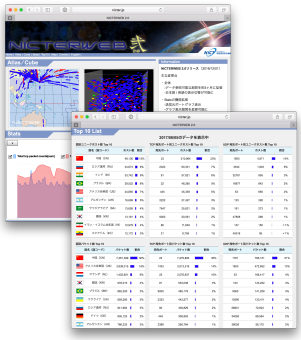
- ●2016年以前
  - ▸デフォルトID/パスワードでログインし感染
- ●2017年
  - ▸デフォルトID/パスワードでログインし感染
  - ▸IoT機器の脆弱性を攻撃して感染
- ●2018年
  - ▸デフォルトID/パスワードでログインし感染
  - ▸IoT機器の脆弱性を攻撃して感染
  - ▸IoT機器の背後にある機器を攻撃

出典：NICTER Blog
http://blog.nicter.jp/reports/2018-02/router-dns-hack/

NICTER観測情報の提供

nicter.jp

- ●セキュリティ関連組織への観測情報提供
  - ✓SIGMON (定点観測友の会)
    - JPCERT/CC、IPA、@Police等との観測結果共有（2004年～）
  - ✓ICT-ISAC Japan (DoS攻撃即応-WG)
    - DoS攻撃関連情報共有（2011年～）
  - ✓オリパラ体制検討会 (NISC、オリパラ組織委員会、関連組織、他)
    - DoS攻撃関連情報共有（2015年～）
- ●観測情報一般公開
  - ✓NICTERWEB (http://www.nicter.jp/)
  - ✓NICTER Blog (http://blog.nicter.jp)
  - ✓NICTER 観測レポート (http://www.nict.go.jp/cyber/report.html)



NICTERWEB

IoT機器等に関する調査業務

日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

2018年11月7日

国立研究開発法人情報通信研究機構

ツイート　いいね！ 174

hide tokuda　41

IoT機器の調査業務 (2018-)

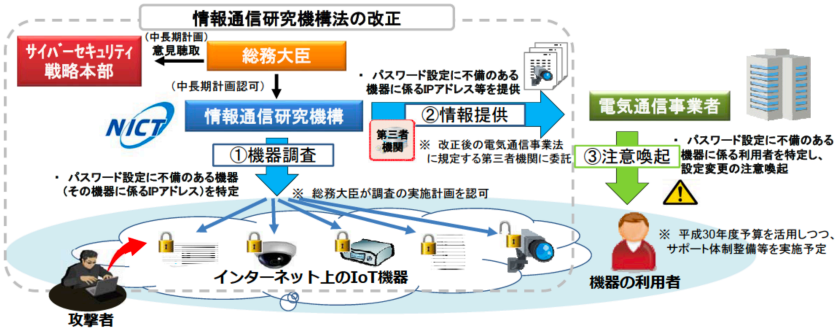
国立研究開発法人情報通信研究機構法の改正について　（by　総務省）

○　IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構(NICT)の業務に、**パスワード設定に不備のあるIoT機器の調査**等を追加(**5年間の時限措置**)する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行うもの。

サイバー脅威の深刻化
- IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。
※IoT機器を狙った攻撃は全体の3分の2(2016年)

対策の必要性
- パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備
- NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進(下図)。



42

NOTICE (National Operation Towards IoT Clean Environment) https://notice.go.jp

hide tokuda 43

NOTICE広報活動：車内ポスター

hide tokuda 44

セキュリティ人材の育成

量と質の問題 (ITKeys, SecCap)
Security by Design教育の実践
育成側とユーザ企業側ニーズとの乖離
経営への橋渡しができるセキュリティ人材
トップノッチ人材
産官学の連携体制

hide tokuda 45

NICTナショナルサイバートレーニングセンター

(2017年4月スタート)

CYDER
Cyber Defense Exercise with Recurrence

国の行政機関、地方公共団体、重要インフラ等を対象とする実践的なサイバー防御演習(CYDER)

cyber colosseo

2020年東京オリンピック・パラリンピック競技大会の適切な運営に向け、大会開催時を想定した模擬環境下で行う実践的なサイバー演習(CYBER COLOSSEO)

SecHack365

若手セキュリティエンジニアの育成を目的として、NICTが若年層のICT人材を対象に、セキュリティの技術開発を本格的に指導する新規プログラム(SecHack365)

まとめ

- IoT・AIの進化のかたち
  - サイバーフィジカル空間を支える基礎技術と社会基盤
  - AI戦略, ICT/IoT戦略, Data戦略, Security戦略, 人材戦略
  - テクノロジーシェーピングとソーシャルイノベーション
- IoT攻撃の質と量の変化
  - のらIoT機器の問題、Dataへの攻撃
  - IoT機器等に関する調査業務: NOTICE
  - セキュリティ人材育成
    - NICTのCYDER, Cyber Colosseo, SecHack360
    - 産官学の連携体制

ご清聴ありがとうございました

http://www.nict.go.jp/