# IoT Marketplace in Japan

Kosuke Ito
Founder & Strategic Advisor,
Connected Consumer Device Security Council (CCDS)
Supporting Researcher, NICT
Visiting Researcher, IISEC
PSIRT Leader, JVC Kenwood

# Contents

- Introduction of CCDS
- IoT Market Situation of Japan
  - IoT Market Category
  - IoT Market Size Projection
- Challenge of New Service Development with “IoT”
- IoT Security Guideline and Regulation in Japan
  - Guidelines
  - Regulations and Certification

# CCDS Overview

- Name: Connected Consumer Device Security council
- Est:　2014年10月6日
- Chairman: Dr. Hideyuki Tokuda
  - Prof. of Keio University
  - Special Advisor of Cyber Security to the Cabinet
- Representative Director: Dr. Tsukasa Ogino
  - Kyoto University
- Director: Dr. Atsuhiro Goto
  - Prof. of Inst. Of Information Security
- Director: Dr. Tsutomu Matsumoto
  - Prof. of Yokohama Nat'l University
- Member: 173（Principal/Regular:47, General:97, Academic:16, Supporting Org:13）

# CCDS Members

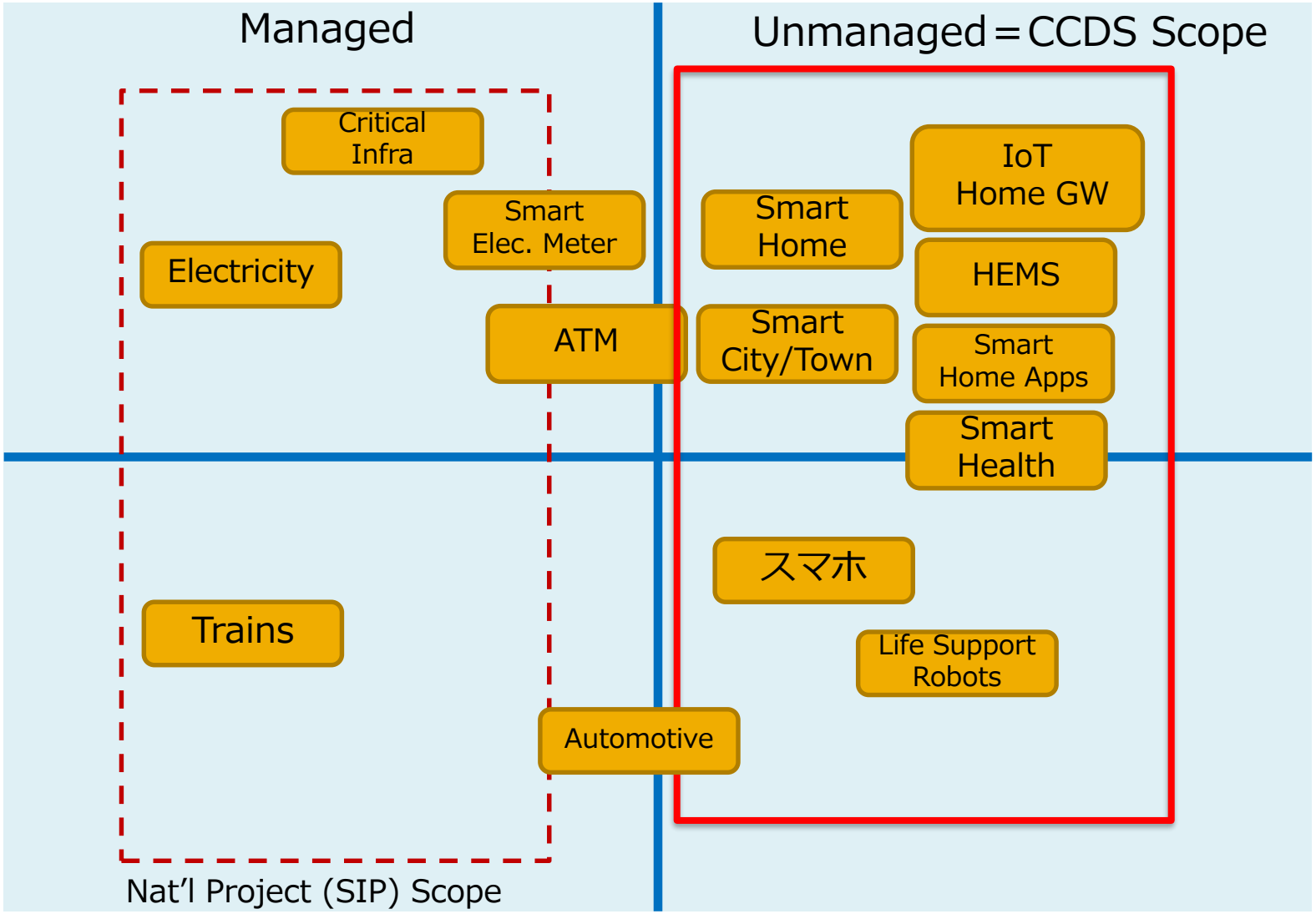
- Total number of members: 173 (as of Sep, 2018)
  - Executive Members: 22 such as

    DNP Deloitte. HITACHI Inspire the Next JVCKENWOOD creates excitement & peace of mind LIXIL SEKISUI HOUSE
    OKI OMRON SYNOPSYS TREND MICRO LAC
  - Regular Members: 25 such as

    AISIN comCruise ALPHA BUNKA SHUTTER FUJITSU Canon muRata NRI SECURE TECHNOLOGIES NTT Communications Transform. Transcend.
    Paloma Panasonic Soliton TEC
  - General members: 97 such as

    ALPINE Driving Mobile Media Innovation ALPS Anritsu Calsonic Kansei Driven by Inspiration and Innovation clarion DENSO EPSON EXCEED YOUR VISION FUJISOFT FURUKAWA ELECTRIC
    gemalto security to be free INTEC TIS INTEC Group I-O DATA KASPERSKY lab KOKUYO KDDI KDDI Research NEC NISSHO ELECTRONICS
    NTT AT NTT東日本 Pioneer SONY THALES TOKIO MARINE GROUP TOSHIBA Underwriters Laboratories
  - Academic members: 16
    - Hiroshima City Univ., Keio Univ., Nagoya Univ., Univ. of the Ryukyus, Yokohama Nat'l Univ., Inst. of Information Security (IISEC), Japan Adv. Inst. of Science and Technology (JAIST), Nat'l Inst. of Adv. Industrial Science and Technoloty (AIST), Nat'l Inst. of Information and Communications Technology (NICT), Nat'l Inst. of Informatics (NII), etc.
  - Liaison members: 13
    - Computer Software Assoc. of Japan, Internet Assoc. of Japan , Japan Network Security Assoc., Japan Cloud Security Alliance, etc.

# IoT Business fields




SIP: Strategic Innovation Promotion Project by Cabinet Office, Gov. of Japan

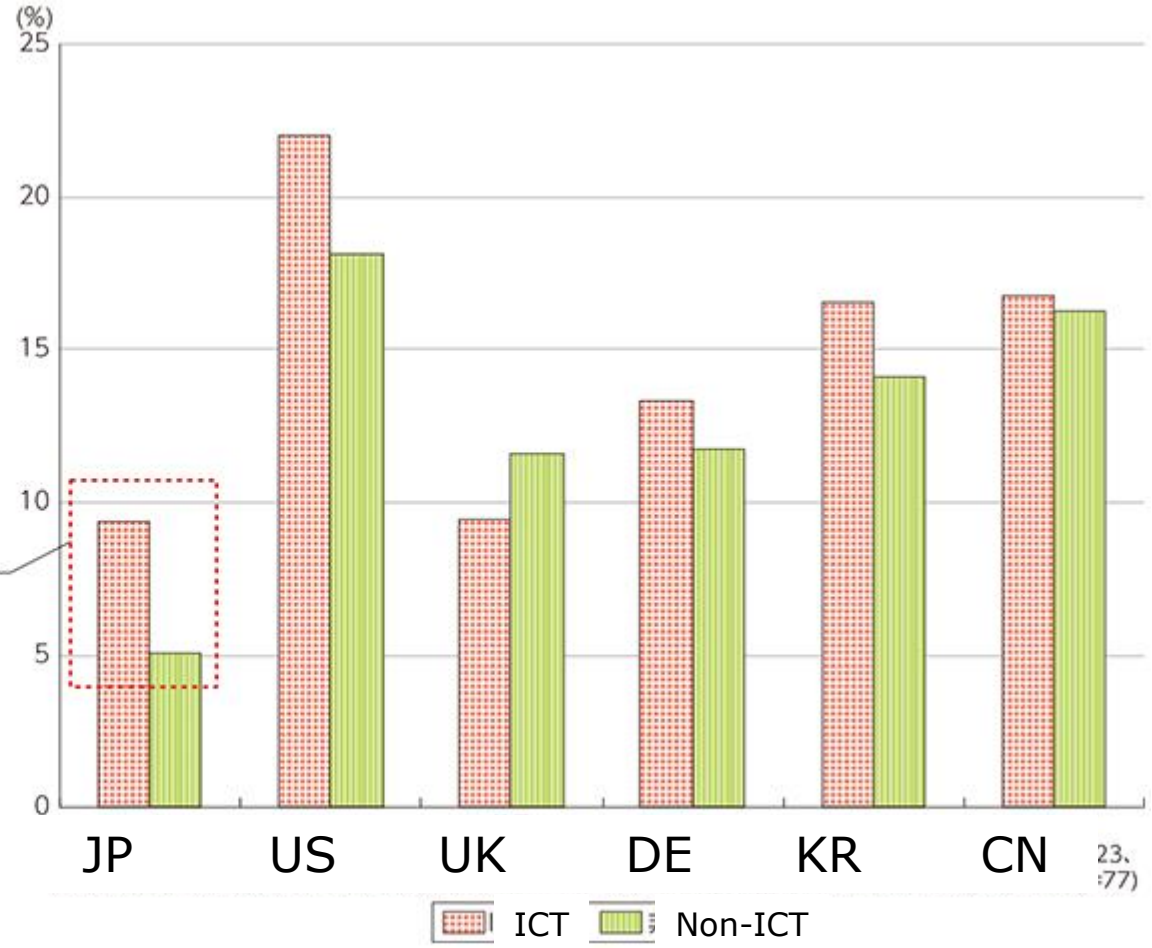
ref: Dr. Tokuda, Keio Univ.

# IoT Market

- IoT Market Growth rate prediction, 2015 to 2020
  - Stronger in ICT than non-ICT

「IoTの進展・普及によって、貴社が属する業界全体(国内)の市場規模は先5年程度(2020年頃まで)どの程度拡大すると思いますか。」という質問に対する回答結果より作成。

● 非ICT企業のIoTによる自産業の市場拡大率(予測)はICT企業の自産業の市場拡大率(予測)半分程度にとどまっている。

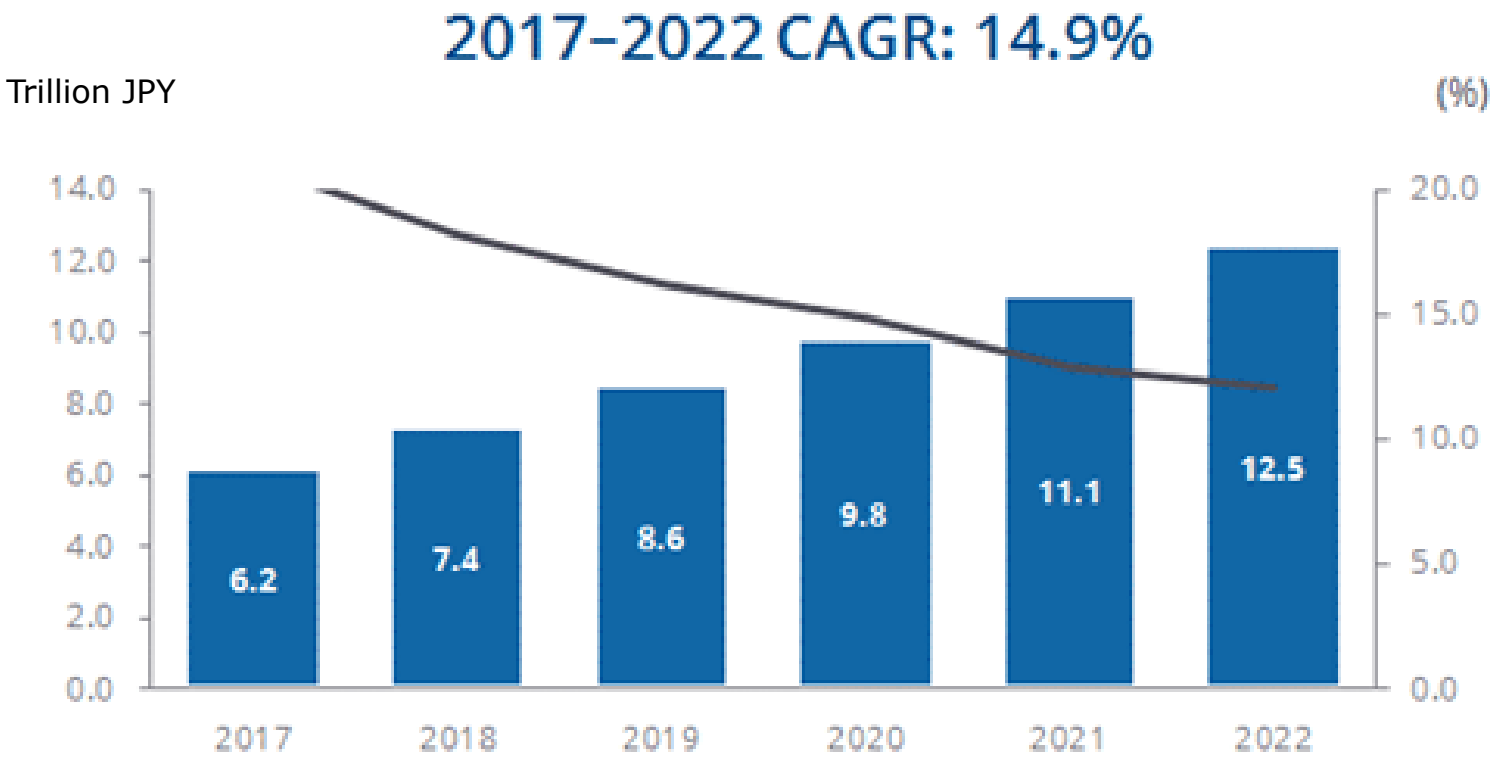



**Market Growth Prediction of IoT in 2020**

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc123330.html

# Domestic IoT Market in Japan

- Double in 5 years

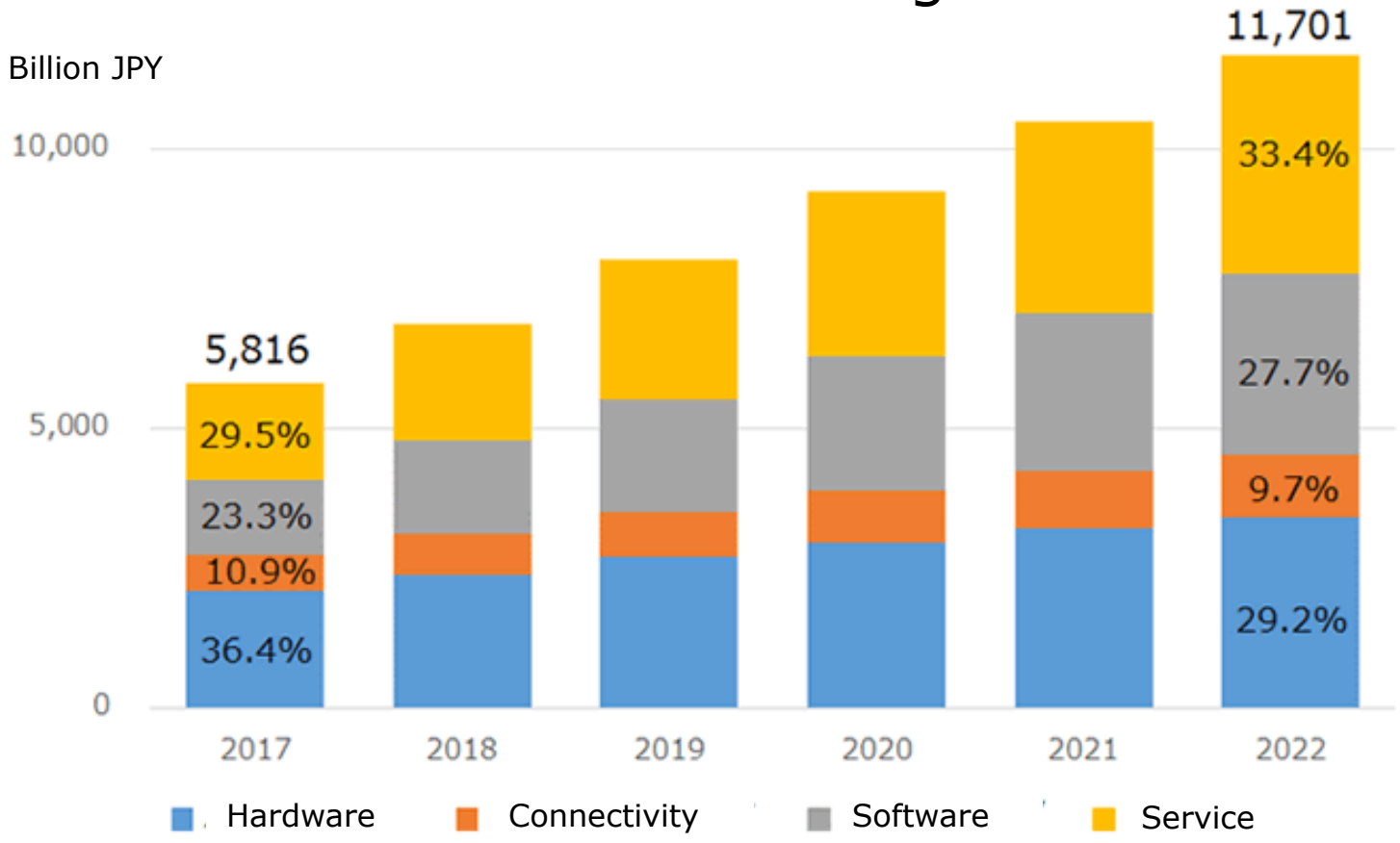



**Domestic IoT Market Investment Prediction, 2017～2022**
2017: Actual, 2018～2022: Prediction
（Source：IDC Japan）

https://businessnetwork.jp/Detail/tabid/65/artid/5981/Default.aspx

# IoT Market Segments in Japan

- Hardware centric, now
- but Service domain is increasing




Domestic IoT Market Investments Prediction: 2017～2022
（Source：IDC Japan）

https://japan.zdnet.com/article/35125558/

# IoT Applied Domain in Japan

**Tracking**
1. Automobile
2. Objects
3. Human
4. Livestock

**Monitoring Analysis**
5. Agri-Field
6. Factory
7. Home/Building
8. Shops
9. Public Facility
10. Energy Plant
11. Transport Condition
12. Truck Operation
13. Human Health
14. Livestock
15. Physical Security
16. Disaster
17. Nature Environment

**Optimization**
18. Energy Consumption
19. Factory Production
20. Supply-Chain
21. Delivery Route

**New Services**
22. Sharing service
23. Wearable Device
24. Smart Product
25. Connected Car
26. Smart/Telematics Insurance
27. Smart retails
28. IoT Payment Device

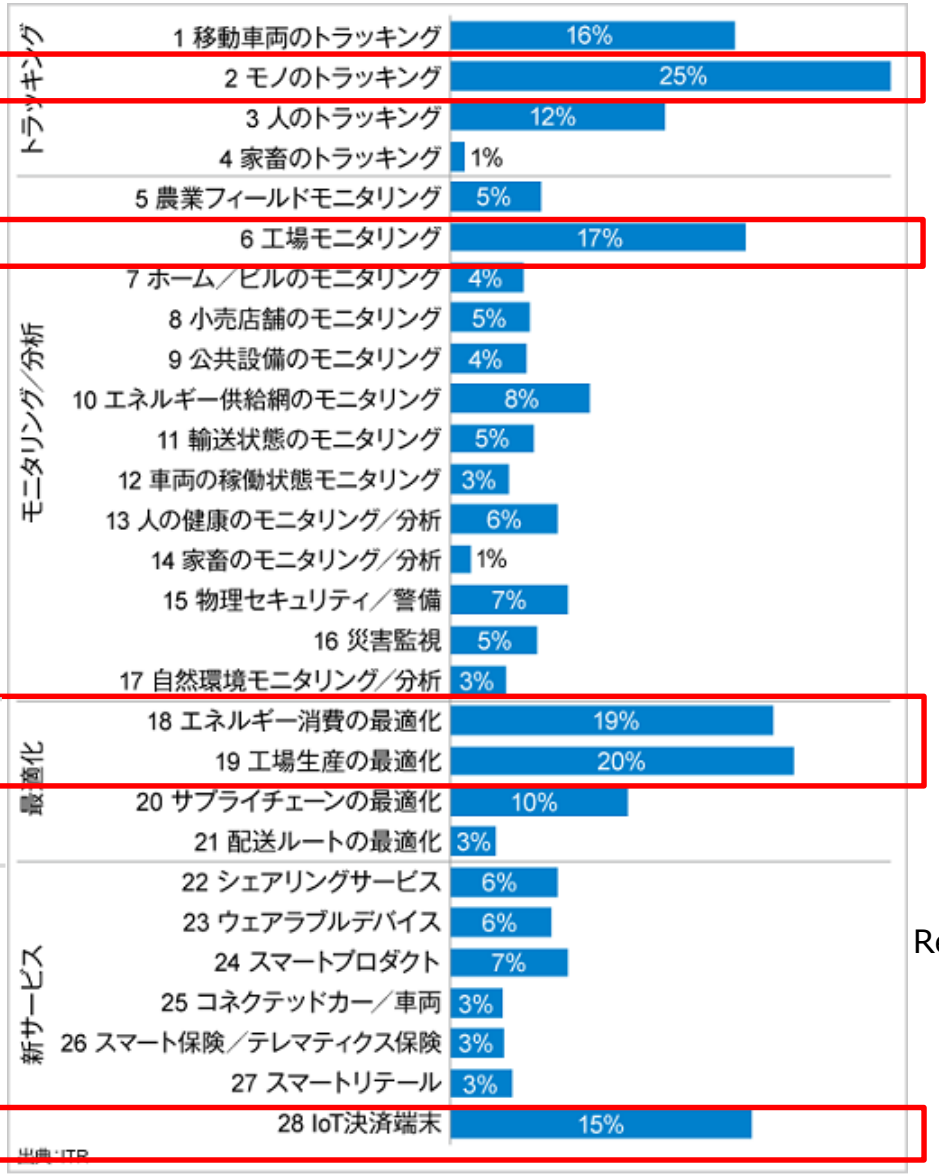


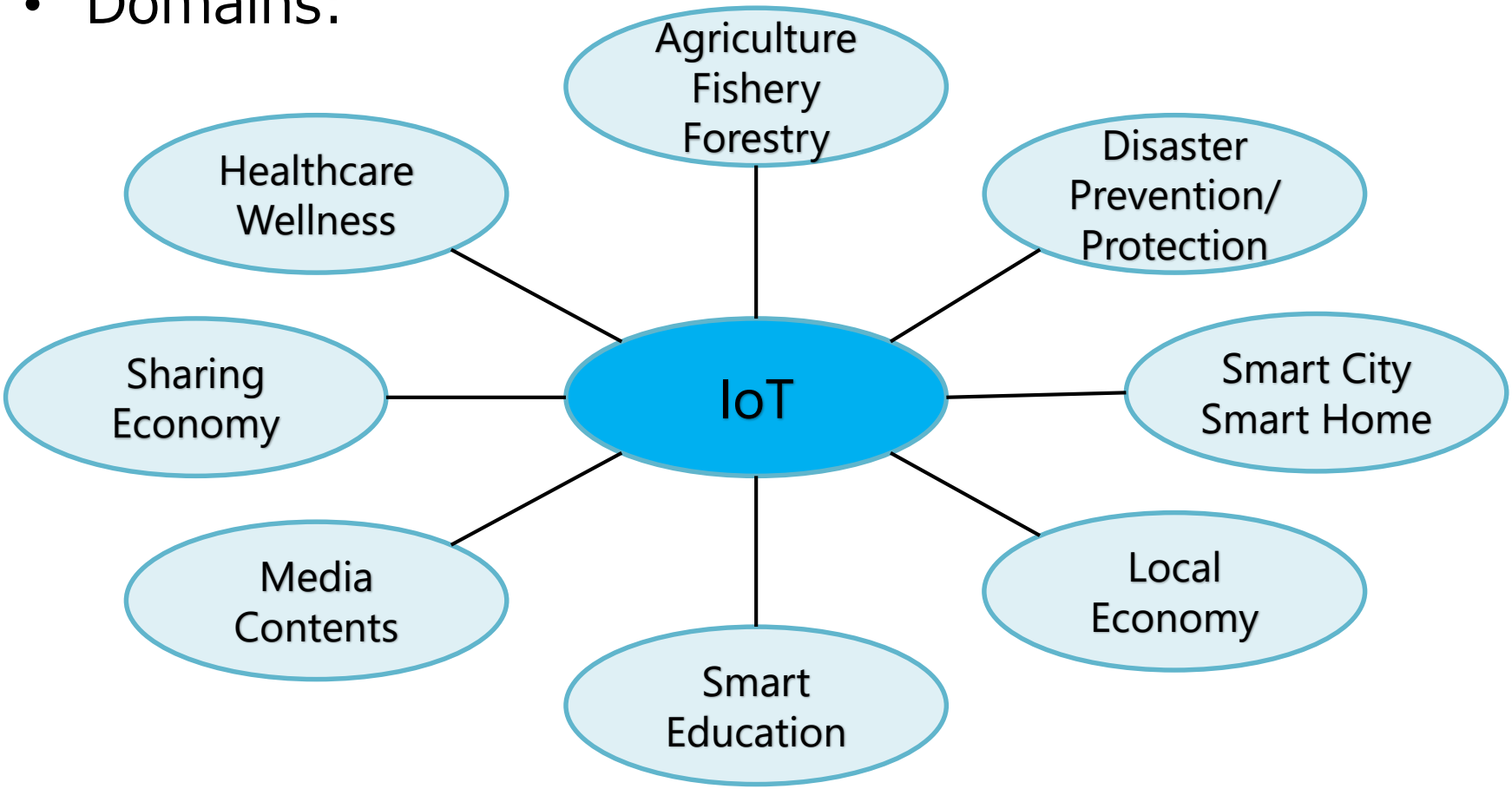

図. IoT導入企業における分野ごとの実施率（全業界平均）

Res：ITR/2017

https://www.itr.co.jp/company/press/171012PR.html

# “Midika-IoT” projects by MIC

- Projects started since 2016
- “Midika” = familiar to the life
- Domains:

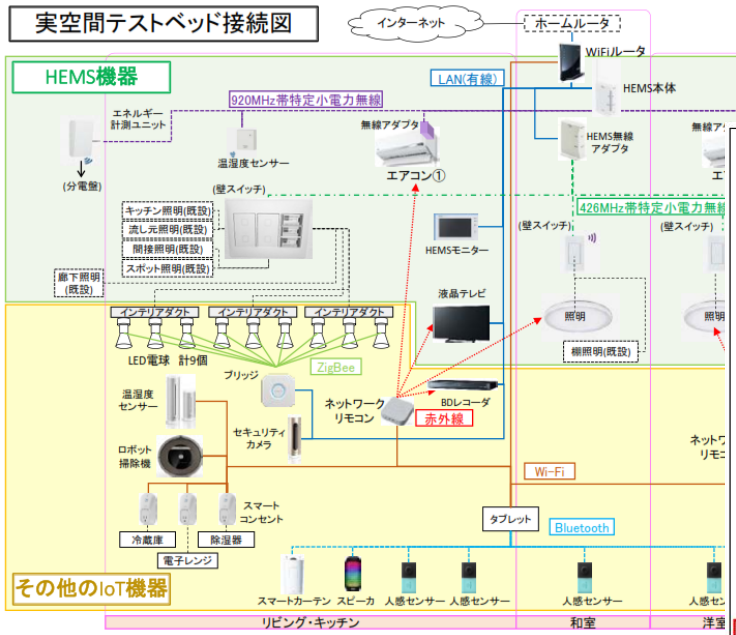


# “Midika-IoT” projects by MIC

- Private B&B Operation Supporting System
  - Reduction of Operating Cost
  - Reduction of Energy Cost
  - Preventing the noise trouble with neighborhood

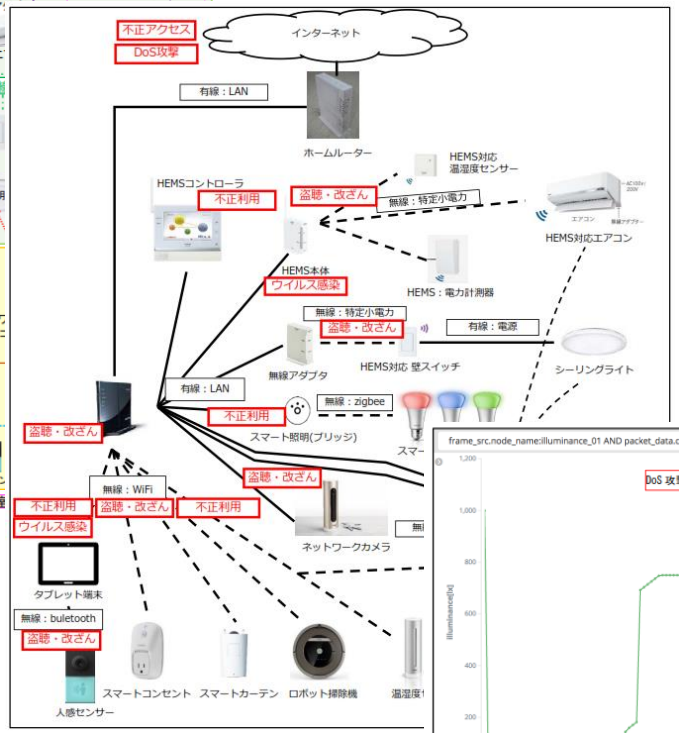
# “Midika-IoT” projects by MIC

- IoT Security on Smart Home
  - IoT Security Evaluation Guideline from the real attack experiences

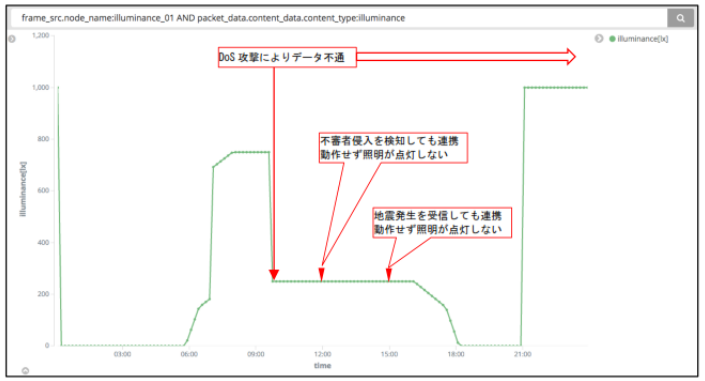



1) Smart Home Testbed System Building with Multi-Vendors
- Smart Lighting by motion sensor
- Smart A/C Control by motion sensor
- Auto A/C Control by Humidity sensor
- Smart Control programmed by IFTTT

2) Threat Analysis on the testbed
- Spoofing
- DoS Attack, etc.

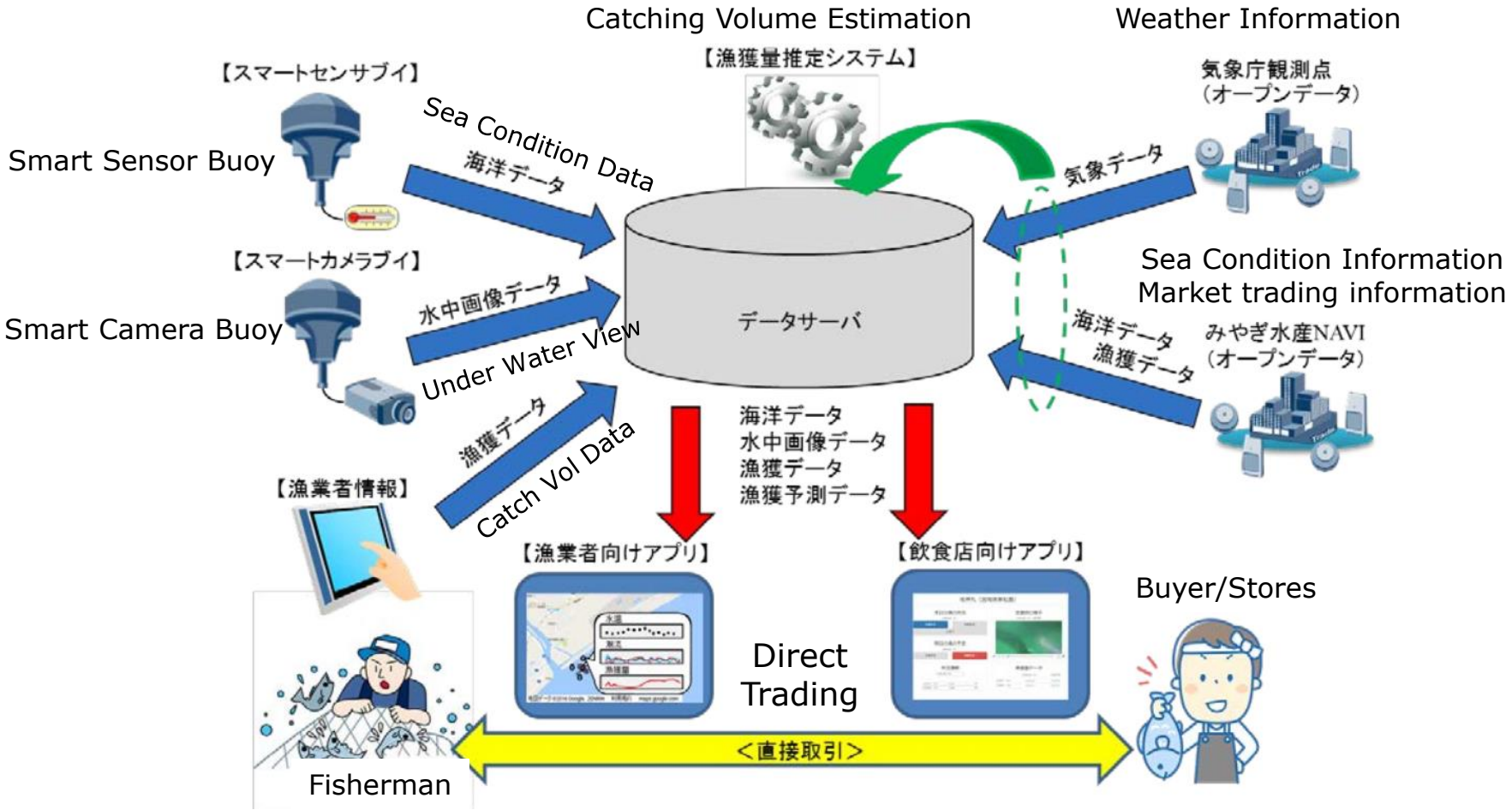



3) Attack Testing and Evaluation on the system
↓DoS Attack monitoring



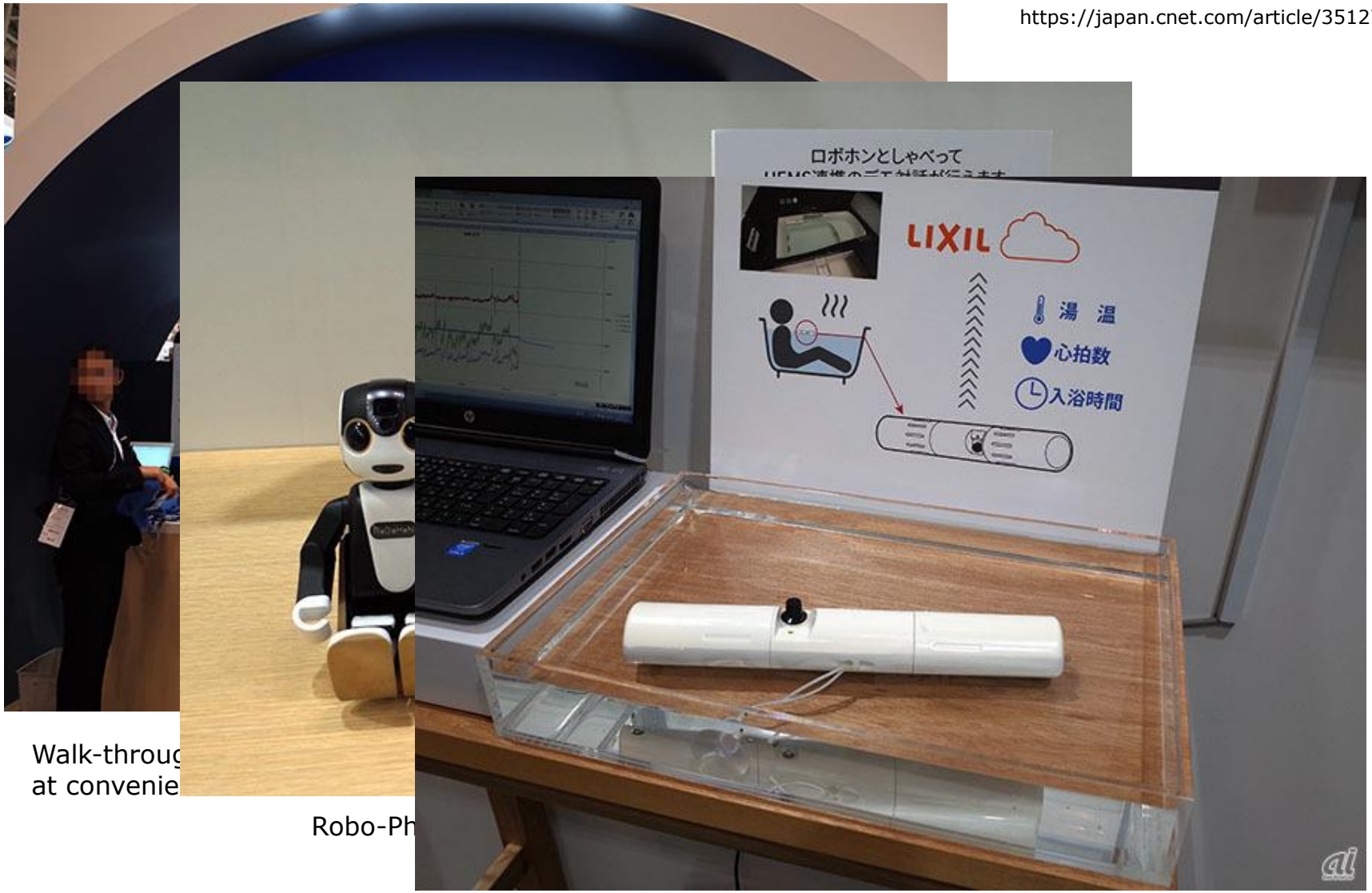
# “Midika-IoT” projects by MIC

- Smart Fishery
  - Efficient Fishing and catching volume on trip
  - Short-cut the distribution channel



# CEATEC 2018 cnet japan記事より

https://japan.cnet.com/article/35127302/




Walk-throug
at convenie

Robo-Ph

Bathroom Monitor (Vital-Heart rate, Water Temp, Time in Bath)

# CEATEC 2018 Internet Watchより

https://internet.watch.impress.co.jp/docs/event/1148031.html

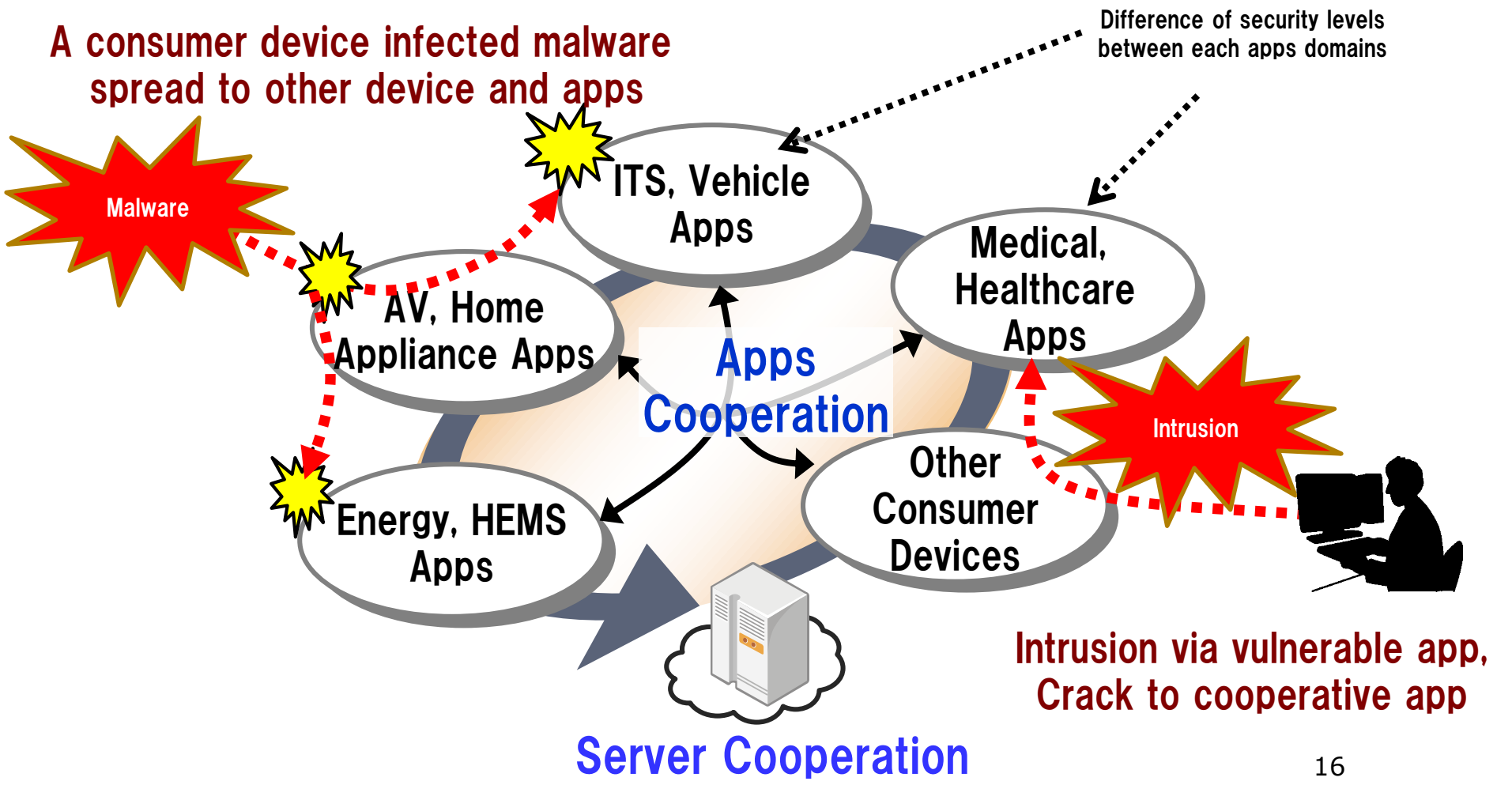

AI Guard m

Mobile

Remote Construction

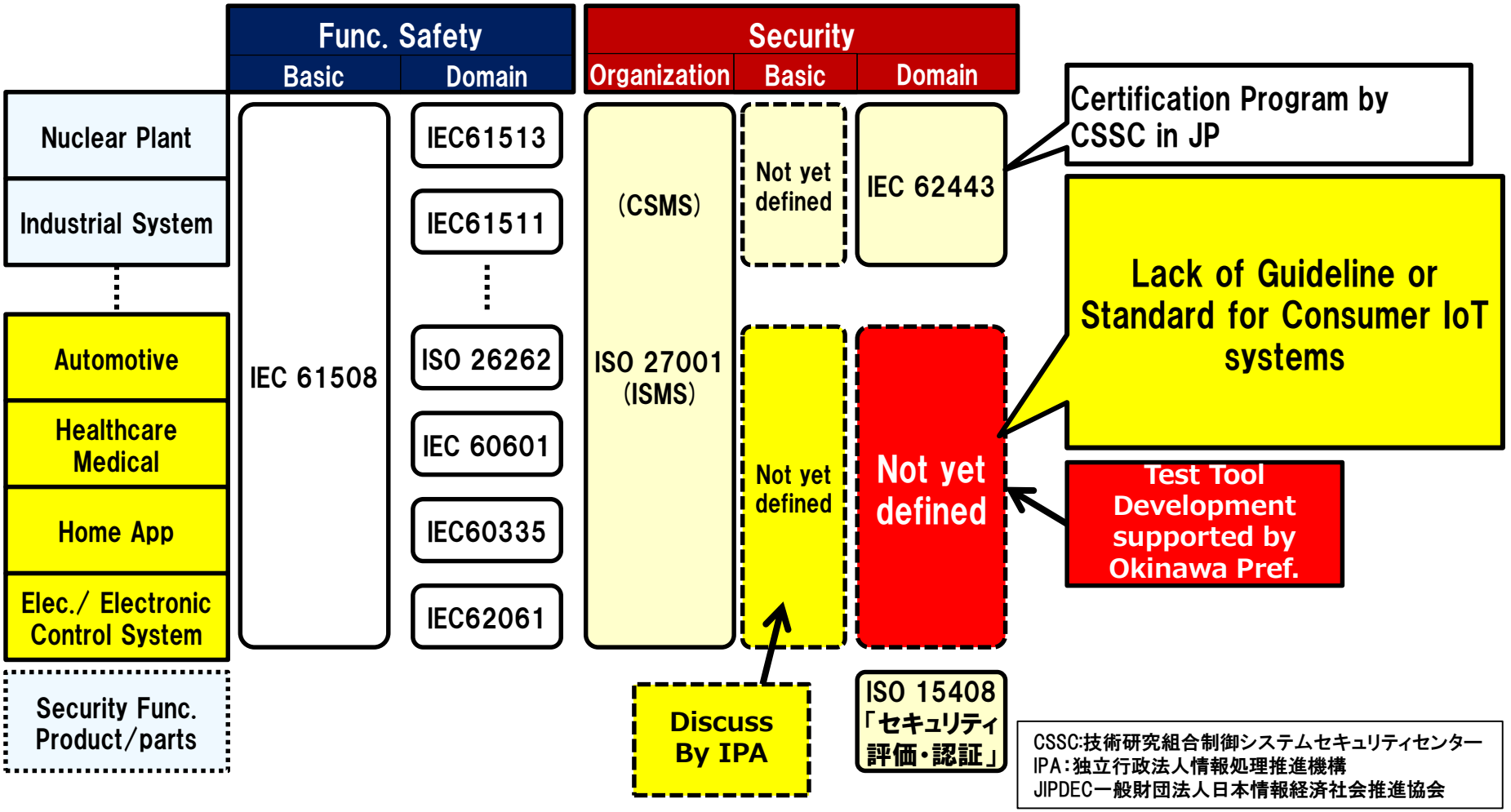
# ISSUE: Threats from Cooperated Devices

If even Single App is safe, but may be vulnerable in cooperated situation



# Lack of Security Standard for IoT in 2014

- Increasing the threats on IoT systems
- Lack of Security Standard for IoT



# Cyber Security Strategy in 2015 by NISC

CCDS

## 経済社会の活力の向上及び持続的発展

～費用から投資へ～

Security By Design (SBD)
System Design with Security Consideration from planning and design stage

■安全な

- 企画・設
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を整合的に実施するための体制等を整備
- エネルギー
- IoTシス

Preparation of the general guidelines to affect security on IoT system

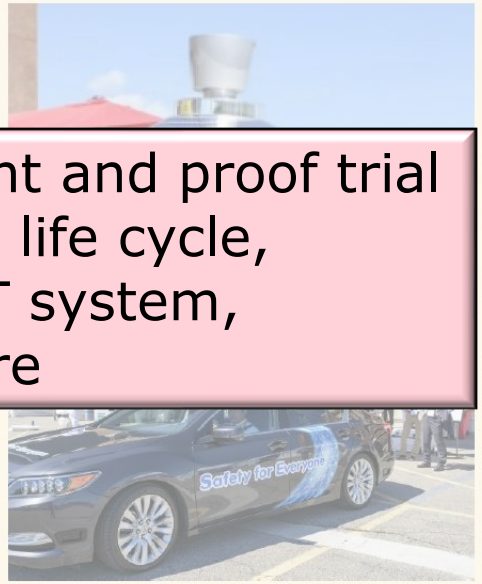
■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築
- 経営層と
- 民民間・

■セキュリ

- 政府系
- 中小企業等
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステム等のセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備

Enforcement of the technology development and proof trial in consideration of the characteristic (long life cycle, limit of the processing capacity) of the IoT system, importance of the hardware genuine nature




▲自動運転車の実証実験

出典：NISC：サイバーセキュリティ戦略（案）より

# Position of guidelines (CCDS perspective)

Cyber security strategy **NISC**

IoT security general framework **NISC**

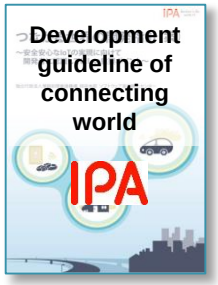
Reference

Proposal of IoT system development by **Security-by-design** concept

IoT security guideline

**IoT Promotion Consortium MIC and METI**

Proposal




Refer to review for cooperation

CCDS

Cooperation for industry deployment

**CCDS** Onboard unit

**CCDS** ATM

**CCDS** IoT-GW

**CCDS** Open POS

International deployment of Japanese idea

Clarification of general basic requirements related to design, building and operation of the IoT system

Security guideline for all layers of IoT service relevant persons

Safe and secure IoT system development guideline which can be used across product fields (checklist)

Specific threat or risk point in view of each product field
Summary of security review points from design stage

IoT service provider

IoT platform /network provider

IoT system vendor

## Purpose

**Since threats for each product field vary, security actions are summarized in view of each field based on IPA "Development guideline of connecting world" to easily disseminate the security-by-design concept in the industry.**

## Target field

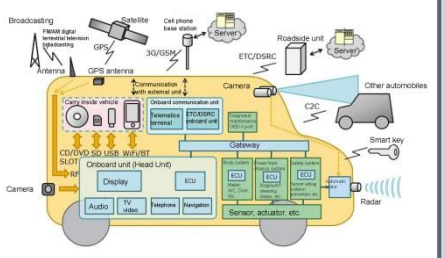
**Car Onboard unit**
**IoT gateway**
**Financial terminal(ATM)**
**Accounting terminal(POS)**

## Major contents of guideline

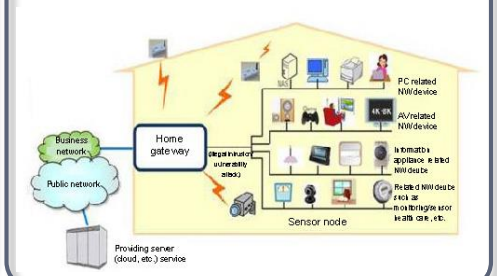
- **Target system configuration**
- **Anticipated security threat**
- **Security action in each phase of product life cycle**
  **(Relationship with IPA "Development guideline of connecting world")**
- **Threat analysis/risk evaluation method**
- **3rd party security evaluation for entire product and security measure function**


**English Versions are available!**

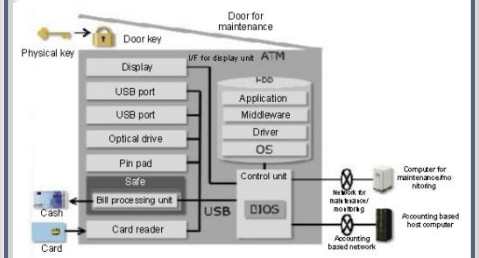
Onboard system configuration



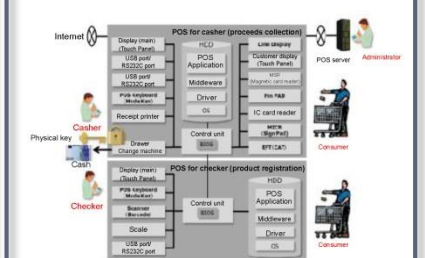

IoT-GW: Home GW case




ATM system configuration

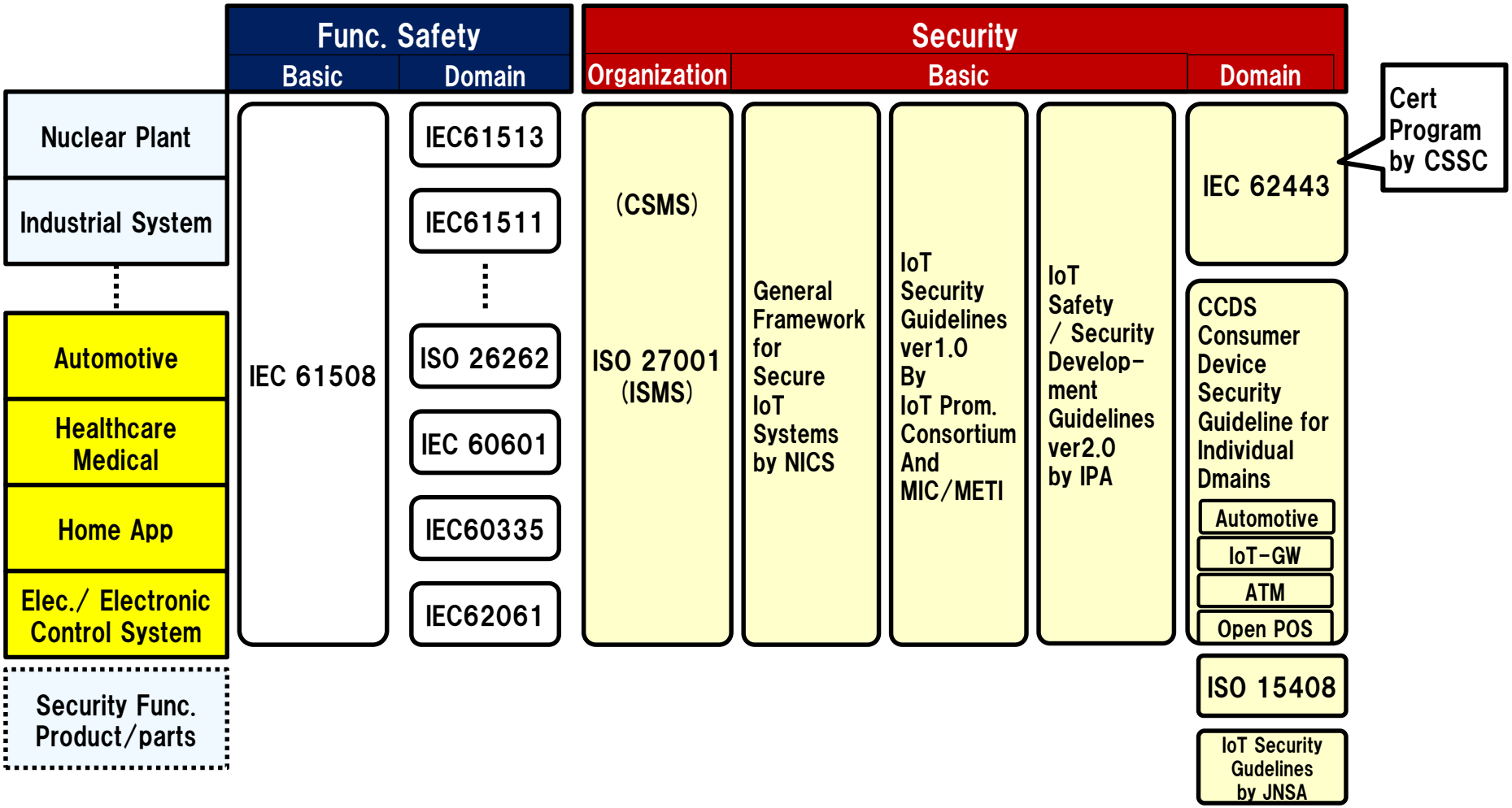



POS system configuration



# Results of CCDS Guideline Development

- Full-filling the lacking parts



# International Standard Development Efforts

- ISO/IEC JTC1 SC27/WG4, SC41
  - ISO/IEC JTC1 SC27/WG4 : ISO27030
    - Developing IoT Security Requirements and Controls
    - JP experts leads this development activity
    - Input the basic idea of “IoT Security Guideline” of IoT Promotion Consortium of Japan
  - ISO/IEC JTC1 SC41 : ISO30147
    - Developing the general requirements for IoT Trustworthiness
    - JP experts contributes this development
    - Also input the basic idea of “IoT Security Guideline”
- ISO/SAE 21434 (Automotive)
  - Standard of Security Engineering for Automotive from design to support in use
  - Planned to complete by May, 2020
  - JP Industry contributes to the EU-US harmonization

# International Standard Development Efforts

- ITU-T SG17
  - X.1373: Secure software update capability for intelligent transportation system communication devices
    - NICT (Nat'l Inst. of Information and Communication Technology) contributes to develop
  - NICT also starts New work on IoT Secure Update Scheme

# Discussion on IoT Security Certification

- MIC
  - Expressed the needs of IoT Security certification on “IoT Security General Package” summarizing the proposals raised by “Cybersecurity Task Force”, a group of experts.
  - Started discussion on extending the requirements of Technical compliance for Telecommunication Devices to IoT Security requirements.
  - It is under preparation for Public Comments.
- METI
  - Leads and promotes individual segment of industries to develop their own “IoT Security requirements”
  - Building, Smart Home, Power Supply, Automotive

# Discussion on IoT Security Certification

- IoT Security WG of IoT Promotion Consortium
  - Restarted the WG activity for the agenda of Certification after the release of IoT Security Guideline
  - WG Chair recommend to start the discussion on the Common IoT Security Requirements across the industries

- CCDS
  - CCDS also discuss the private certification program with our members
  - Extracting the baseline requirements among the members from Smart Home, Car on-board Device, ATM, POS/Cash Register
  - Planning to start a pilot program this year

# Summary

- IoT Market in Japan is growing as expected
- Major area of IoT is shifting from JP Specialty of Hardware shifting to Service
- Many Challenges on IoT with AI/Big Data are under development
- Developing Guidelines / Standards of IoT Security is active in JP
- Now, those activities are expanding to discussion on the regulation and a certification program