RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-W02

Japan’s new cybersecurity strategy to close an IoT gap

Mihoko Matsubara

Chief Cybersecurity Strategist
NTT Corporation
@M_Miho_JPN

Contents

- Cyber/IoT security pressure & Tokyo 2020
- Cyber/IoT security efforts
- What is next for Japan?
- Next steps for audience

RSAConference2019

Cyber/IoT security pressure & Tokyo 2020

Why is Japan under pressure for IoT security?

Tokyo Summer Olympic & Paralympic Games 2020

Tokyo was selected as the host city in September 2013

Tokyo 2020 leads to:

Innovation

Success for Tokyo 2020 requires:

- Physical security
- Cyber/IoT security

RSAConference2019

Cyber/IoT security efforts

Cybersecurity Strategy in 2015

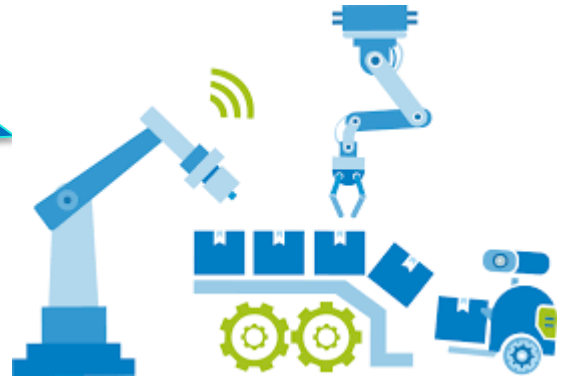
- Cyber/IoT security for Tokyo 2020 & economic growth
- Awareness raising among business leadership
- More collaboration

IoT in Japan: Manufacturing

- Productivity, efficiency

1. Monitor packet chains

2. Detect anomaly



3. Notify operators of recommended actions to take

IoT in Japan: retail & logistics

- Shrinking population → manpower shortage

The 1st unmanned convenience store opened in Japan in December 2018.

A Japanese logistics company has cut the number of vehicles in operation by 50% and hours of operation by 35%, using AI and IoT.

IoT in Japan: agriculture

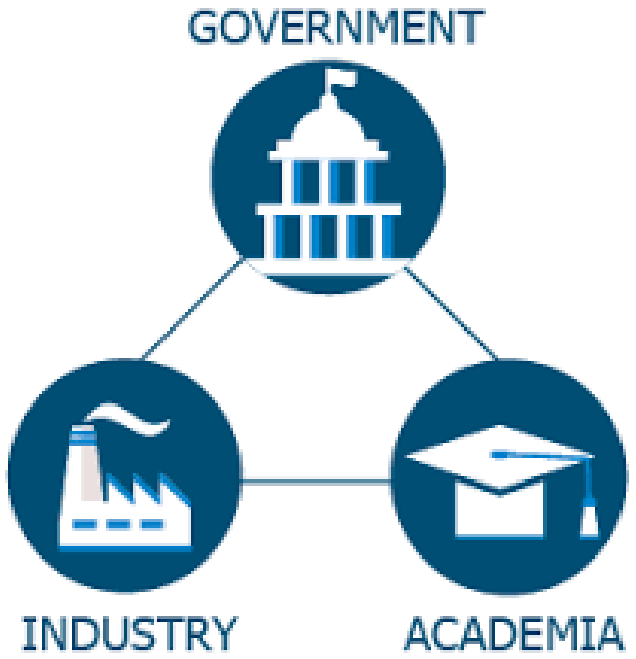
- Decreasing manpower: 60% down, compared to 1985
- Aging farmers: 65% of farmers are over 65 years old

Multiple vendors started to sell smart tractors in 2018

Sensing + Monitoring + Know-how

IoT Acceleration Consortium in 2015

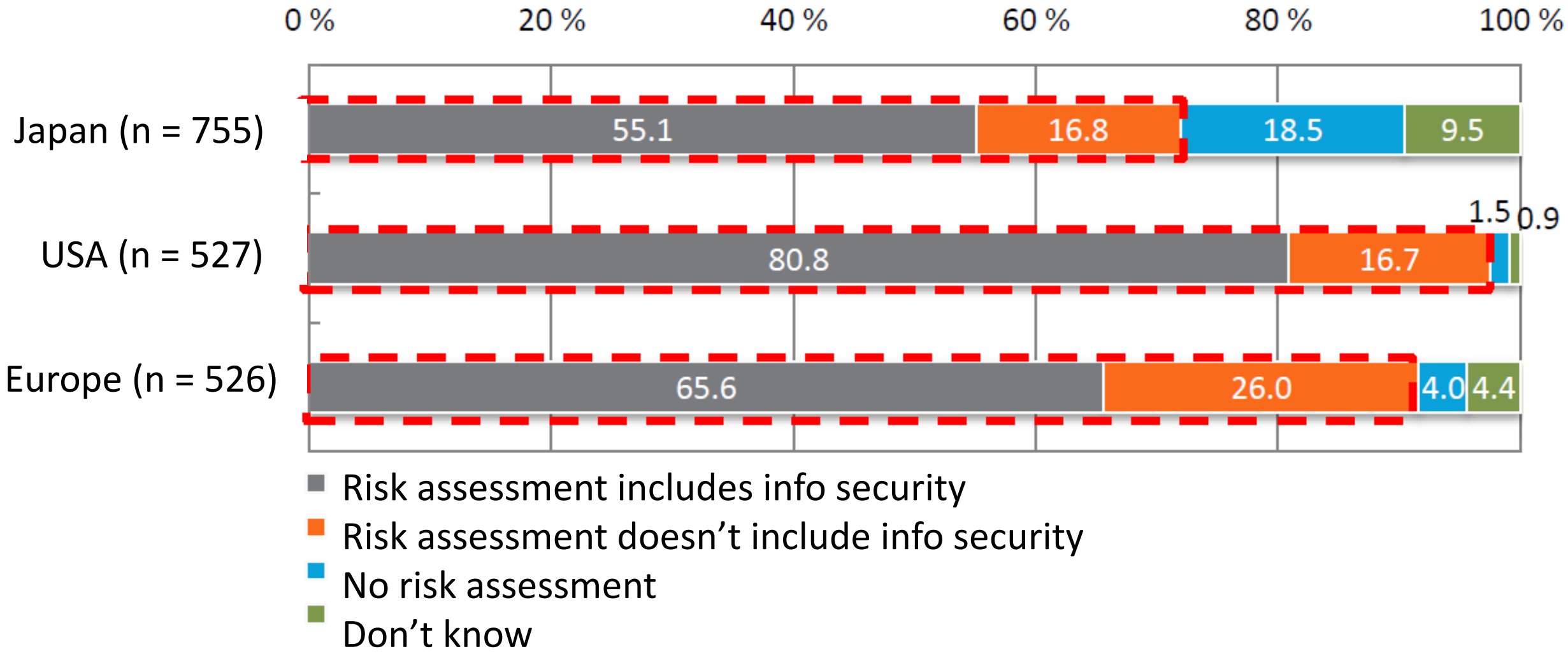
- Government-Academia-Industry collaboration
- IoT Security Guidelines in 2016



Cybersecurity Guidelines for Business Leadership in 2015

- Cybersecurity, not a cost center
- Business risk management
- Check list for the NIST Cybersecurity Framework (Version 2.0 in 2017)

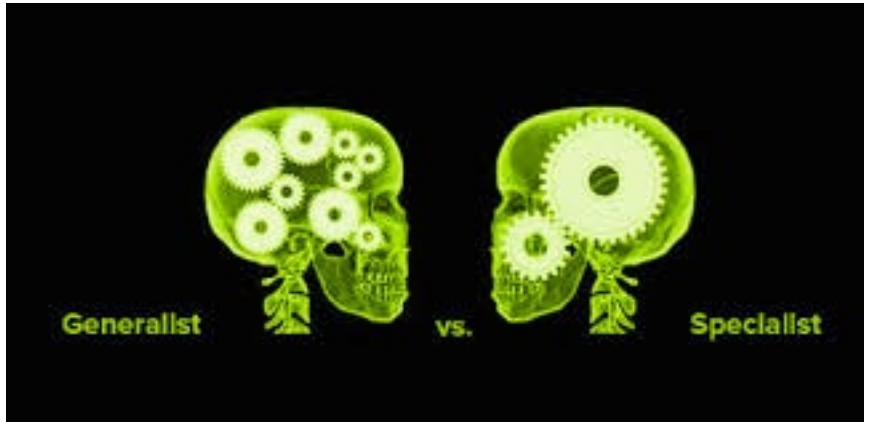
Cybersecurity & risk management in Japan



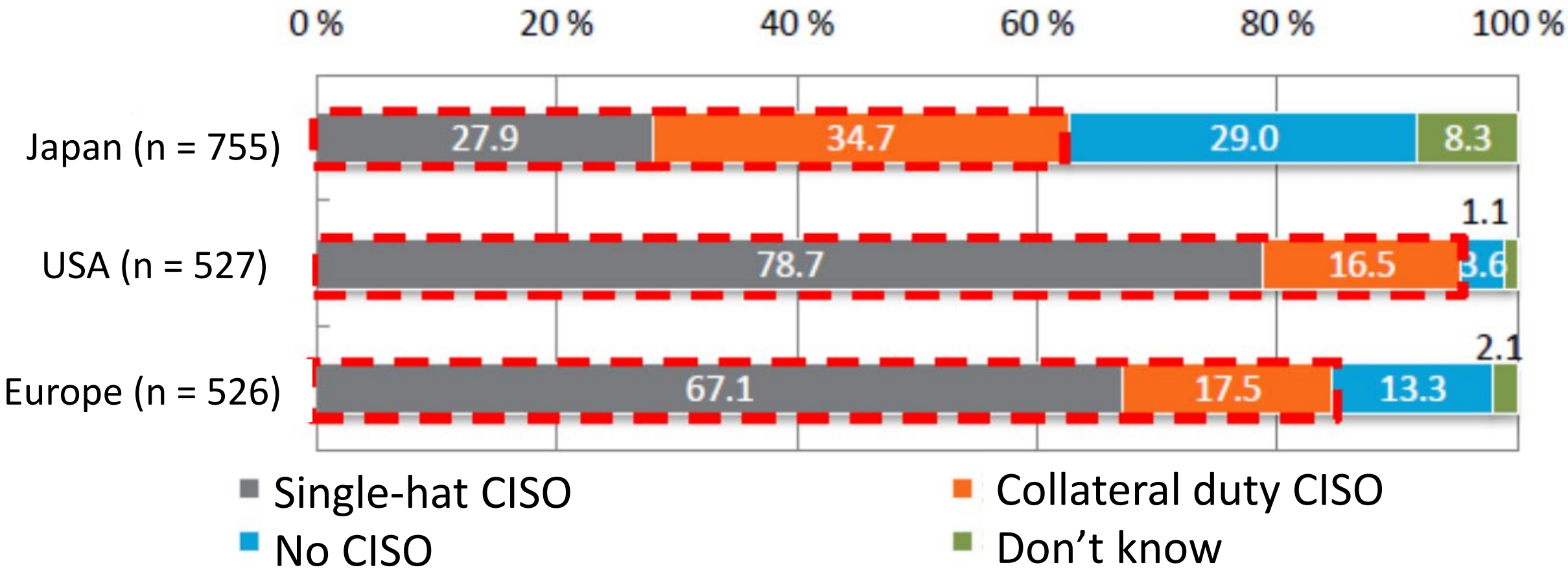
Source: IPA's report in April 2017, https://www.ipa.go.jp/files/000058850.pdf, 41

Japanese career paths

- Lifetime employment
- Rotation every 2-3 years within a same organization
- Generalist vs. Specialist



CISOs in Japan, USA, and Europe



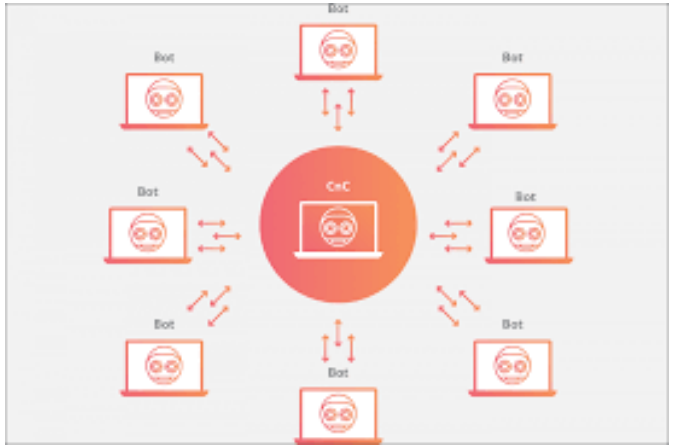
Source: IPA's report in April 2017, https://www.ipa.go.jp/files/000058850.pdf, 22

Japanese CISOs

- Collateral duty
- IT/Cybersecurity background
- Need a team to support CISO

Cybersecurity Strategy in 2018

- Fused cyber and physical domains
- Botnet mitigation
- Diversified cybersecurity professionals



Tax incentive for IoT & security in 2018-2021

- Corporate tax deduction: 3%
- Special depreciation: 30%
- Encouraging to industry's capital investment & security
  - Certified cybersecurity specialists

Japanese gov's POC to check vulnerable IoT devices in 2017

- Ministry of Internal Affairs & Communications + ICT-ISAC + Yokohama National University
- Findings in 2018
  - 150 vulnerable IoT devices found
  - 77 of them: GOJ was able to identify their contact information
  - 36 of them: GOJ was able to reach out to their owners

Revised NICT Act in 2018

- National Institute of Information & Communications Technology under Ministry of Internal Affairs & Communications
- Revised Act
  - NICT can scan IoT devices to find vulnerable ones (default password)
  - NICT shares that information with the ISPs cyber threat intelligence sharing framework

Revised Telecommunication Business Act in 2018

- Increase in IoT botnet
- Revised Act allows:
  - NICT to share cyber threat intelligence with ISPs via ICT-ISAC
  - ISPs to alert about infected IoT devices to customers
  - ISPs to block DDoS attacks

Previous efforts for botnet mitigation

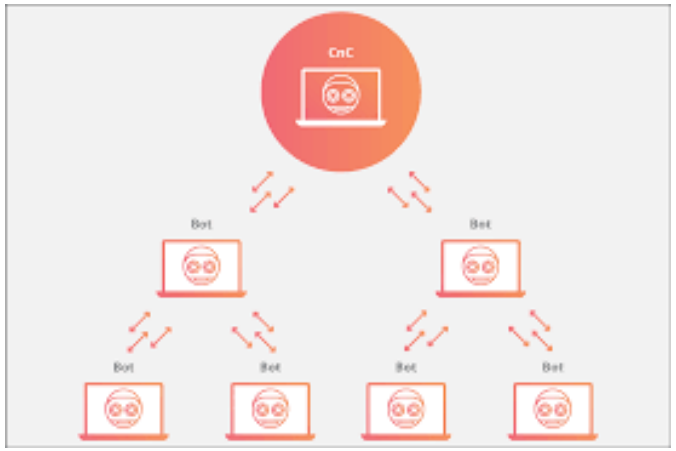
- Past collaboration between the government and ISPs
  - Cyber Clean Center between 2006 and 2011
  - ACTIVE (Advanced Cyber Threats response InitiatiVE) between 2013 and 2018
- Challenges
  - Effectively and efficiently reaching out to users
  - ISP costs for user communications
  - Need to address concerns over why ISPs are able to identify specific users under Constitution Article 21 (secrecy of communications)

ICT-ISAC Japan

- Information & Communications Technology – Information Sharing & Analysis Center
- Members are telecom, security vendors, and TV broadcasters
- International collaboration
  - IT-ISAC, Communications ISAC
  - DHS Automated Indicator Sharing (AIS)

Council to Secure the Digital Economy (CSDE)

- ICT companies work together to “combat increasingly sophisticated and emerging cyber threats through collaborative actions.”
- International Anti-botnet Guide 2018
  - Aims to offer baseline practices for tech companies
  - Encourages tech companies to keep their products, systems, and users secure to protect the internet from botnet



ICT-ISAC Japan & CSDE

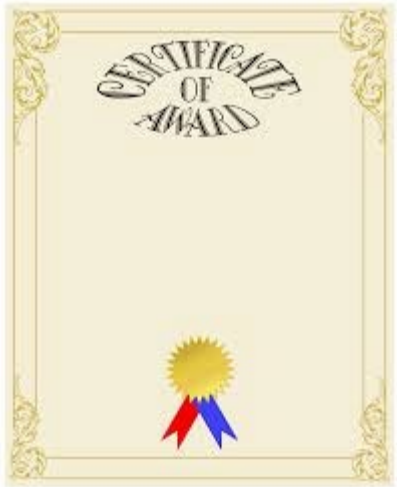
- NTT is a founding member of ICT-ISAC Japan and CSDE.
- NTT contributed to writing CSDE Anti-botnet Guide.
- ICT-ISAC Japan translated the Guide to Japanese.

RSAConference2019

What is next for Japan?

What does Japan need to do next?

- More IoT & AI
  - Aging society: agriculture, housing
- IoT security professionals
  - Bridge between operations, IoT, and security
- Open innovation
  - Better interconnectivity
  - International certificates

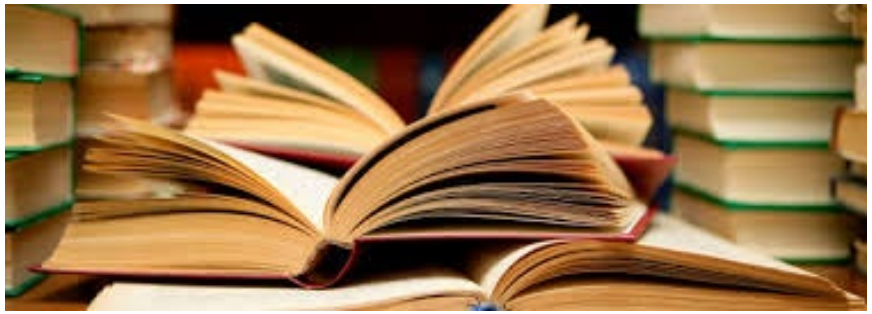


RSAConference2019

Next steps for audience

Next Steps for Audience 1/2

- Next week you should:
  - Check what Japan has done for cyber/IoT security.
  - Read the CSDE International Anti-Botnet Guide 2018.
- In the first three months following this presentation you should:
  - Identify how Japan and your country/organization can collaborate on cyber/IoT security.
  - Learn whom to work with in Japan.



Next Steps for Audience 2/2

- Within six months you should:
  - Reach out to your potential Japanese counterpart to start dialogues.
  - Discussions should include certificates, education/training, or security.

RSA®Conference2019