How to communicate with your government

- Lessons from Japan -

Dr. Suguru Yamaguchi

JPCERT/CC

Japan

Summary

- CSIRT can be a good liaison between government and industries.
  - "Cybersecurity" is emerging in various policy domain by the government, esp. for national security and critical infrastructure protection (CIP & CIIP).
  - Infrastructure and various components for ICT society are operated mainly by private sectors (private industries). But, classic regulations are not working well with this business structure for cybersecurity, because the situation changes very rapidly.
  - "Be a good catalyst", Nice & rich communication with your government is a key for more collaborations.

JPCERT/CC and others

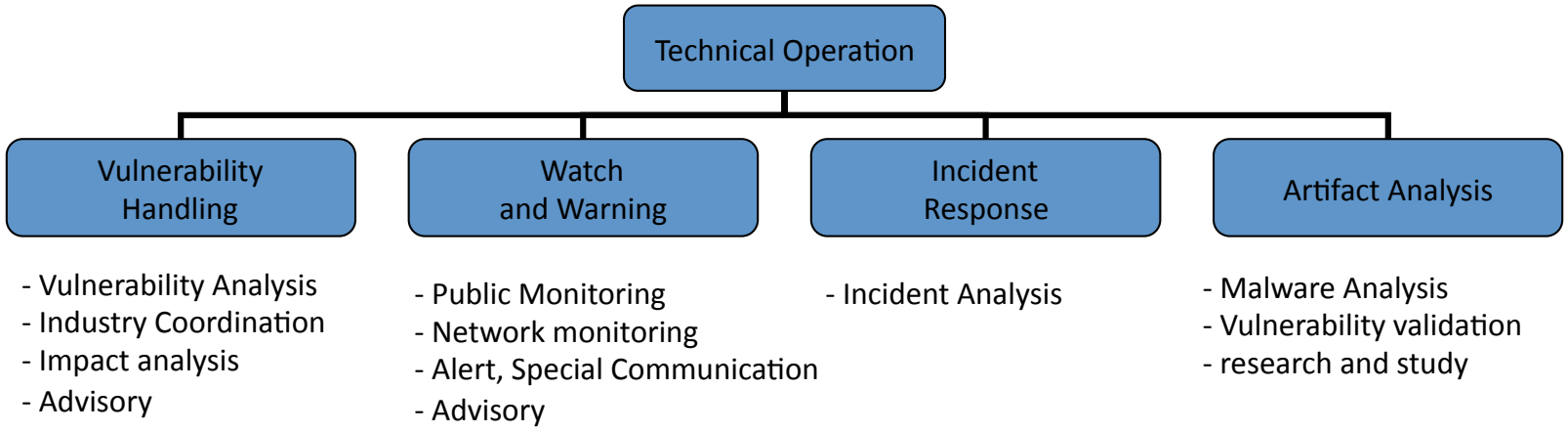
- Multiple “Point of Contact” (POC) Structure for JAPAN

- JPCERT – POC for Japan
  - Provide its service for Japan as its constituency
- NISC - Policy & Government related
  - National Information Security Center, Cabinet Secretariat, GOJ
- NPA – Law Enforcement
  - National Police Agency, GOJ

- More than 20 CSIRT’s in Japan
  - Enterprise CSIRT
  - 20 FIRST members.

Quick overview of JPCERT/CC

- Budget comes from METI (Ministry of Economy, Trade and Industry), but not 100%
- Non-governmental, Not for Profit Organization
- National POC CSIRT in Japan (Point of Contact for International relations)
- FIRST (Forum of Incident Response and Security Team) Full member since 1998
- APCERT (Asia Pacific Computer Emergency Response Teams) chair, Secretariat

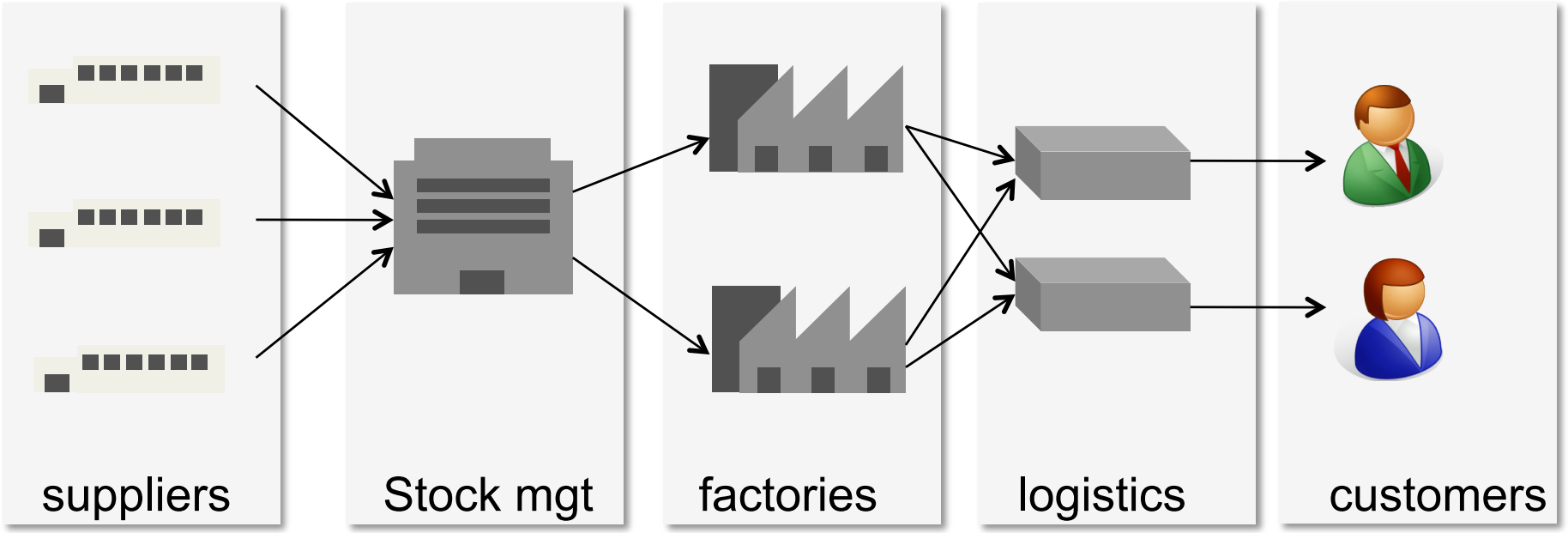


“No infonet, No business!”
so what our government can do?

Where we are heading?

- Widely ICT deployment to social infrastructures.
- We are living in “Connected world” where more information are exchanged and processed among vast number of computers and ICT devices.
- True “ICT society”
  - Covers our whole globe.
  - Knowledge based economy.
  - Global optimization.
  - High mobility of users, information processing and assets.

Supply Chain Management (SCM), today



Production Optimization

Financial Management

Integrated Business Management & ERP

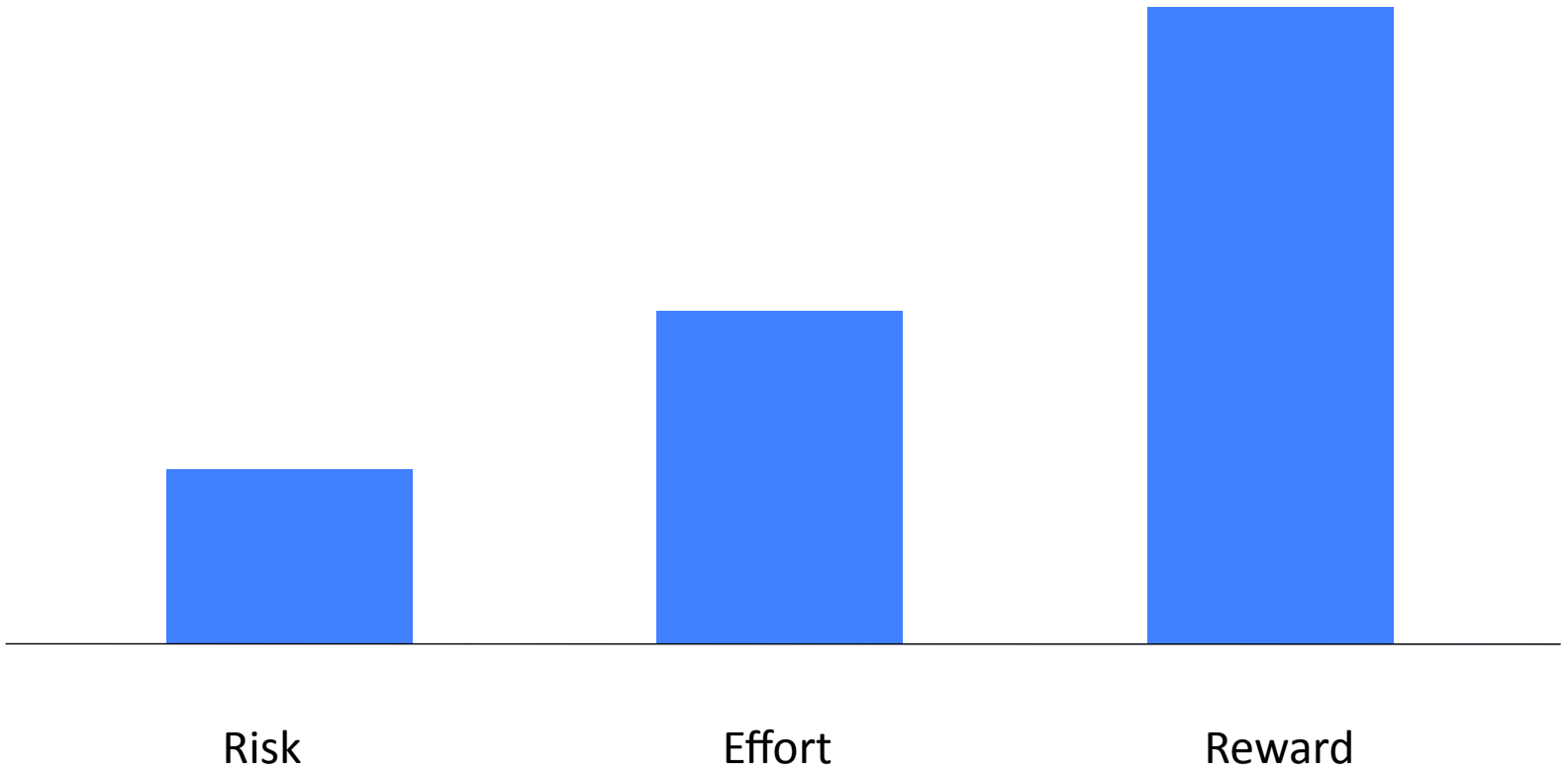
ICT platform

Security is our #1 priority

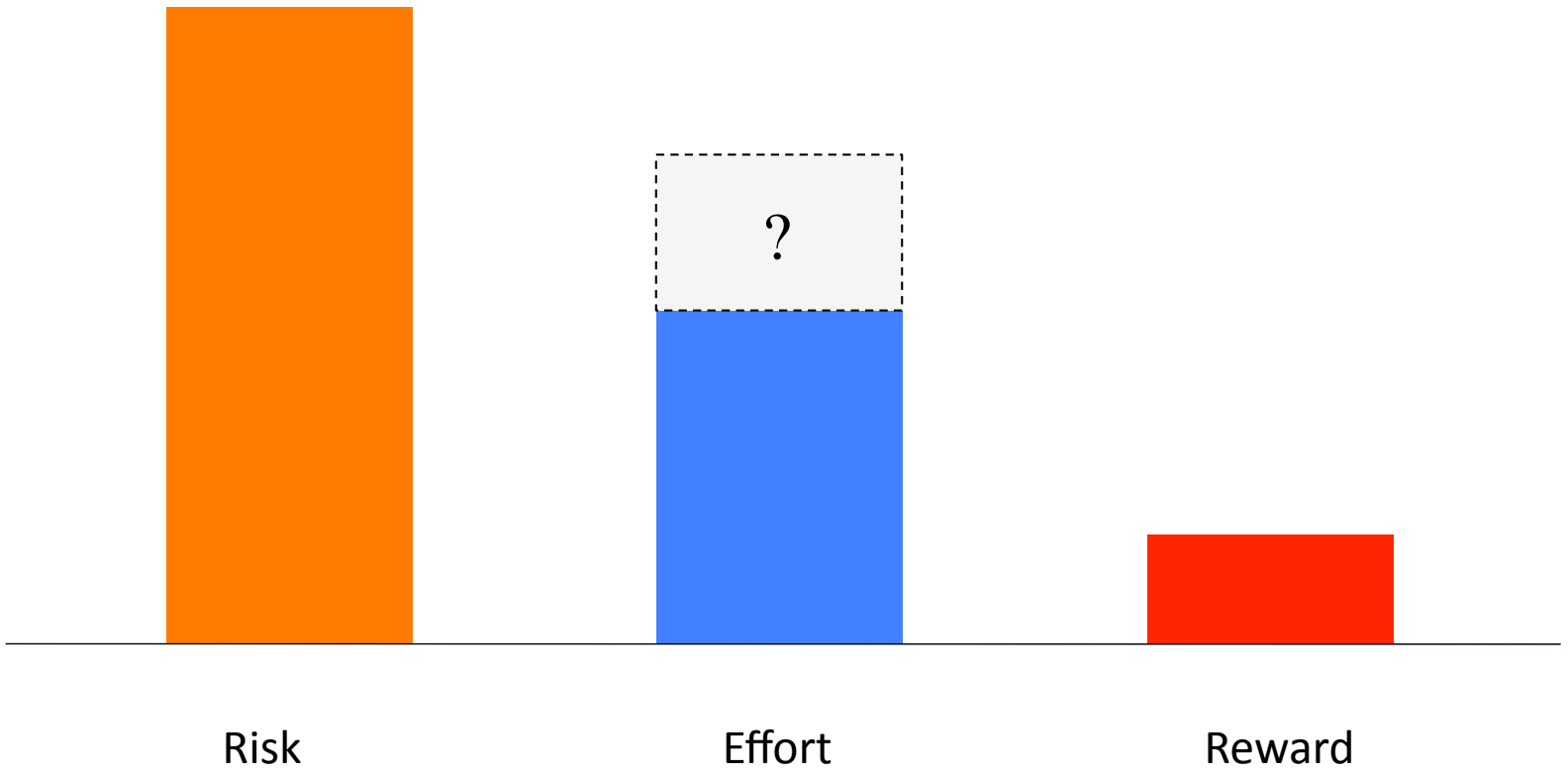
- Information systems are also "business enabler" for criminals.
  - Information systems are adding power for criminals in many ways, such as APT and attacks using cloud computing.
  - Global collaboration for making malwares, composing attacks and getting $$$.

- We have to change this game!
  - Good scheme to strengthen information security management.
  - More efficient measures against criminals.
  - Need changes on the structure.

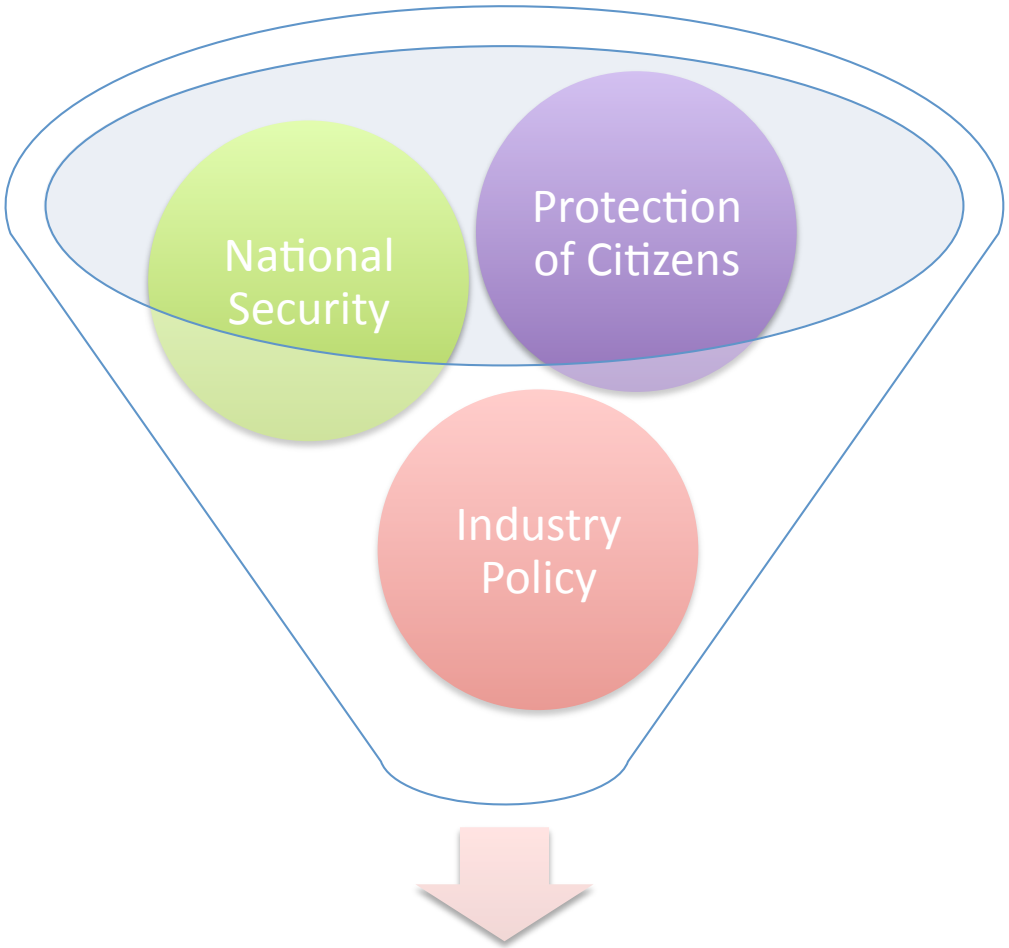
Economics of Cyber Crimes, Today



Economics of Cyber Crimes, Tomorrow



Areas we have to work today



National Cyber Security Policy

Policy Areas

- Industry Policy
  - Protection of ICT infrastructure as our business basis for various economic activities.
    - Data confidentiality, ID management, digital signature, commerce over the Internet
- National Security
  - Counter activities against malicious activities over the Internet.
    - Combating against cyber terrorism, high-tech crimes, …
    - Counter intelligence activities, …
    - Preparedness for large-scale state organized cyber attacks.
- Protection of Citizens
  - Protection of Citizens from malicious activities
    - Citizens as consumers in e-Commerce
    - Protection of Individual information & privacy data transferred over the Internet
    - Human rights protection

Japan's Directions

Industry Policy

- Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (2001)
- IT HQ (2001) & NISC (2005) in Cabinet Secretariat (PM office)

National Security

- National Cyber Security Master Plan, version 4 (2011)
- National Defense Program (2011)
- Legal framework for anti-cyber terrorism, high-tech crime, and the other malicious activities against our society
- CIP/CIIP basic plan by NISC (first ed. In 2006)
- Counter intelligence, counter espionage, (2009)

Protection of Citizens

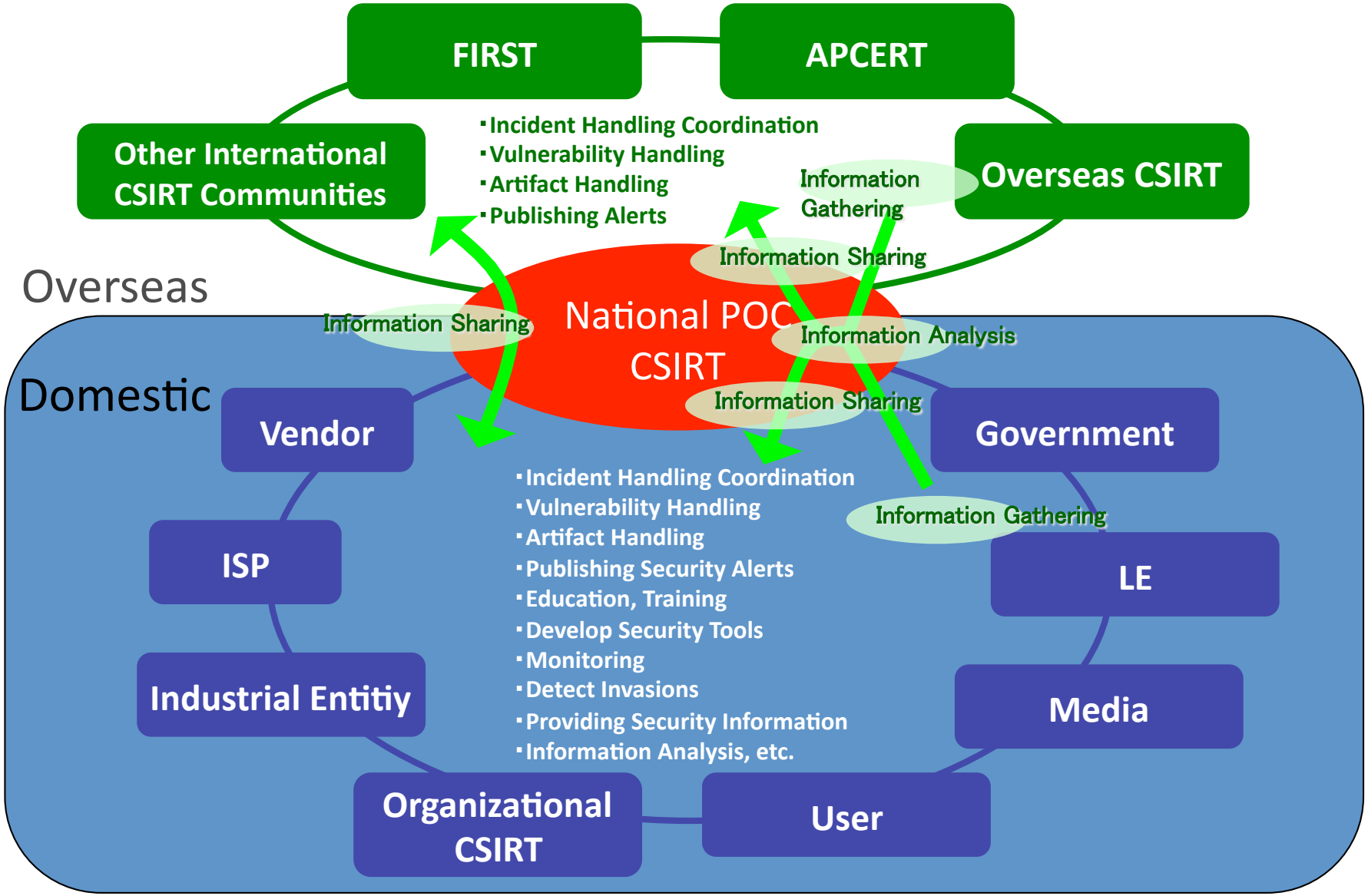
- Personal Information Protection Law (2004 etc.)
- Consumer Affairs Agency (CAA), est. 2009

But, the gov cannot do everything.

- The network infrastructure and their vital components are operated by private sectors.
  - The Internet and communication networks.
  - Information systems for our society
  - Today critical information infrastructure includes various business infrastructure including financial services, supply chain systems, and energy networks.
- Government has its own silo structure.
  - It comes from bureaucrat system, naturally.
  - However, cybersecurity is the common issue for all the ministries.
- Industries have their own legal framework for operations.
  - Confidentiality management of their operation is highly required, especially for farms on stock markets.
  - Government regulations controls many in the business area.

What can CSIRT do?

Main Operations of National POC CSIRTs



Information Security - Key Factors

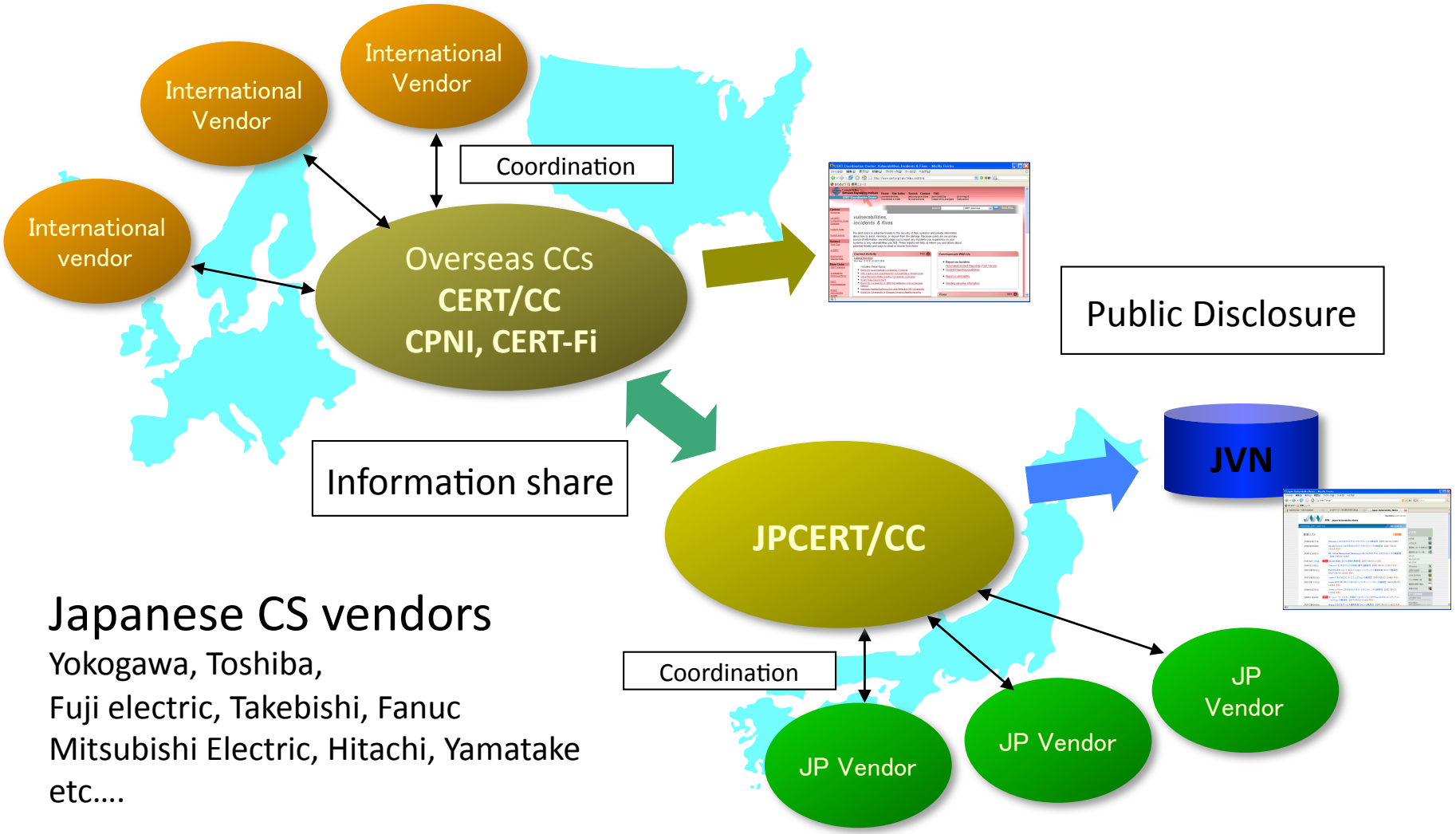
Areas we can work together with gov

- Dealing with the bureaucrat silo structure.
  - Cybersecurity is cross-sector agenda today, not limited to ICT.
  - Being a bridge among ministries is possible way to work together.
- Public Private Partnership (PPP) needs a good coordinator for information sharing.
  - CSIRT can be a clearinghouse of information for industries to be shared with government.
- The society needs more human resource development for cyber security management in various business area.
  - We can working together, including public awareness raising.
  - Global & international collaborations.

JPCERT/CC case, communications with JP Gov

- Sharing with our own analysis data with government.
  - Periodic & emergency report for government as "cyber hurricane center"
  - Update them for rapid changes of incidents.
- Collaborations for various areas
  - Technical capability development
  - Human resource development
  - Engineering & technical research, and standardizations.
  - Functions as ISAC. (information sharing & analysis center)
- Working as a primary contacts of industries for governments.
  - Especially for telecommunication infrastructure.
  - Escalation for specific cases, especially for international cases that need communication with the other countries' authorities (gov).

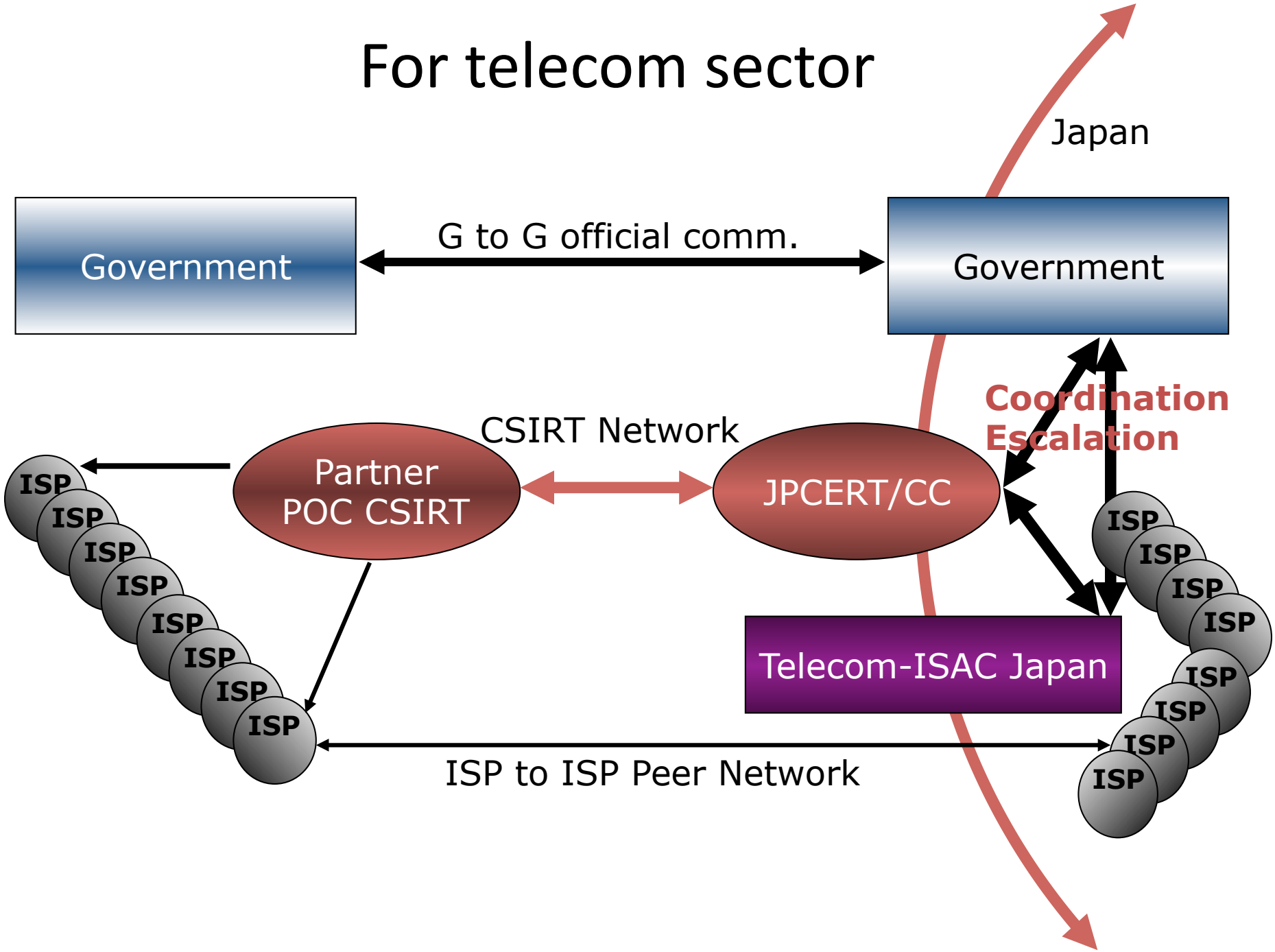
International partnership and framework for ICS security



Japanese CS vendors

Yokogawa, Toshiba,
Fuji electric, Takebishi, Fanuc
Mitsubishi Electric, Hitachi, Yamatake
etc….

For telecom sector



Summary

- Government has various concerns on “cybersecurity” policy, but it cannot do everything by itself alone.
- Industries always deal with multiple ministries and regulations for their business operation. They need a good coordinator for working with government.
- CSIRT is a specialized organization to deal with cyber security incidents, but today we have many capabilities to work with both gov and industries, as a catalyst for them.
- Gov / CSIRT / industries is a good formation to deal with cybersecurity issues.
  - Proofed with many cases in various countries, including JP.