Good Practices for ICS Supply Chain Risk Management

Special Expert at Cyber Tech Lab
Information-technology Promotion Agency, Japan (IPA)
Industrial Cyber Security Center of Excellence (ICSCoE)
Hiroshi Sasaki, CISSP

© Information-technology Promotion Agency, Japan
Industrial Cyber Security Center of Excellence

Self-Introduction

Hiroshi Sasaki, CISSP

Sr. Expert, Cyber Tech. Lab, ICSCoE (Industrial Cyber Security Center of Excellence since July/2017 (part-time)

IT Security Officer of Ministry of Economy, Trade and Industry (METI) since May/2016 (part-time)

Senior Security Advisor,
Cyber Strategic Initiative Office, CISSP
McAfee Co., Ltd. Email: Hiroshi_Sasaki@McAfee.com

Mission:
To Cultivate CULTURE of Critical Infrastructure (CI) Protection/ IoT Security

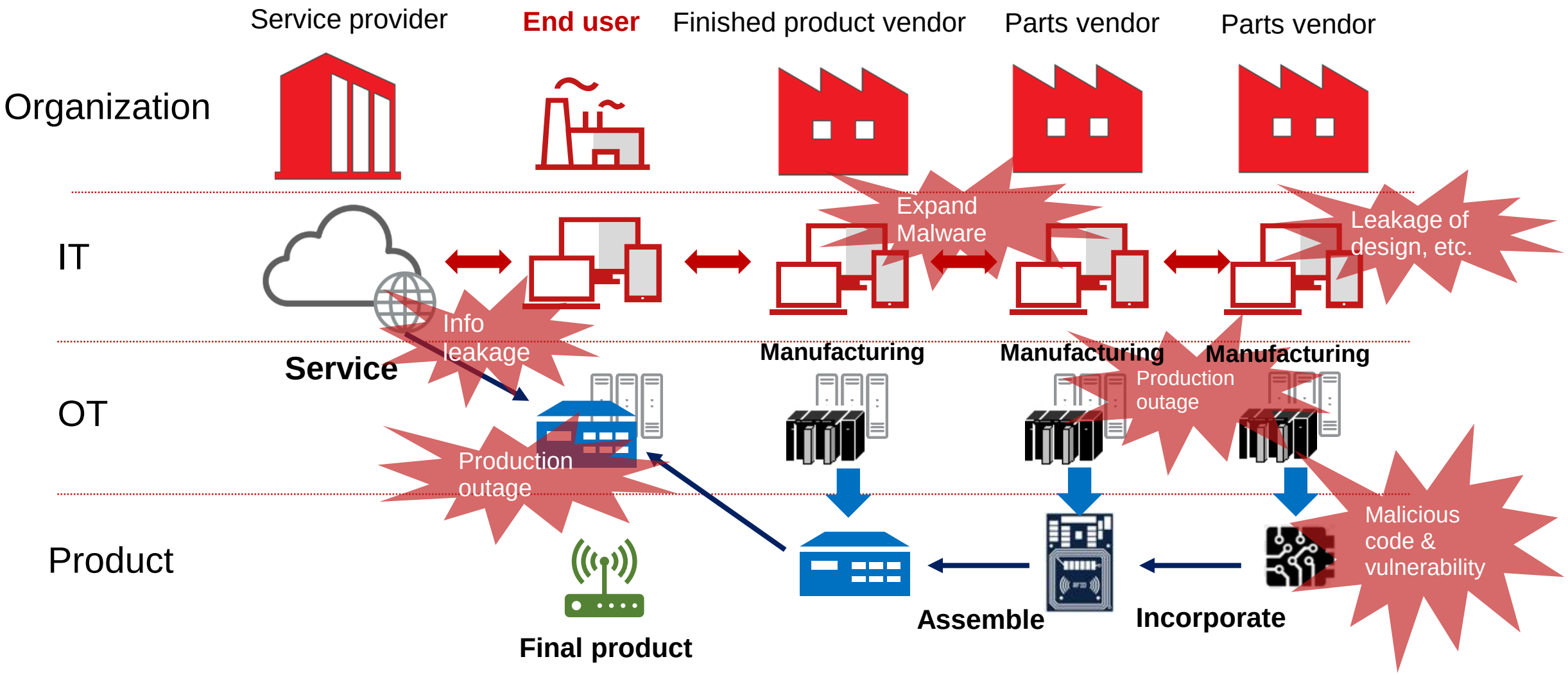
Joined McAfee in December 2012 after working for 14 years as a developer of industrial control system. Aiming to foster culture of industrial cyber security, providing enlightenment such as lectures, writing and consulting services.

Agenda

- Challenges of ICS SCRM
- 7 categories of the requirements for ICS supplier
- Good practices of ICS SCRM in Japan

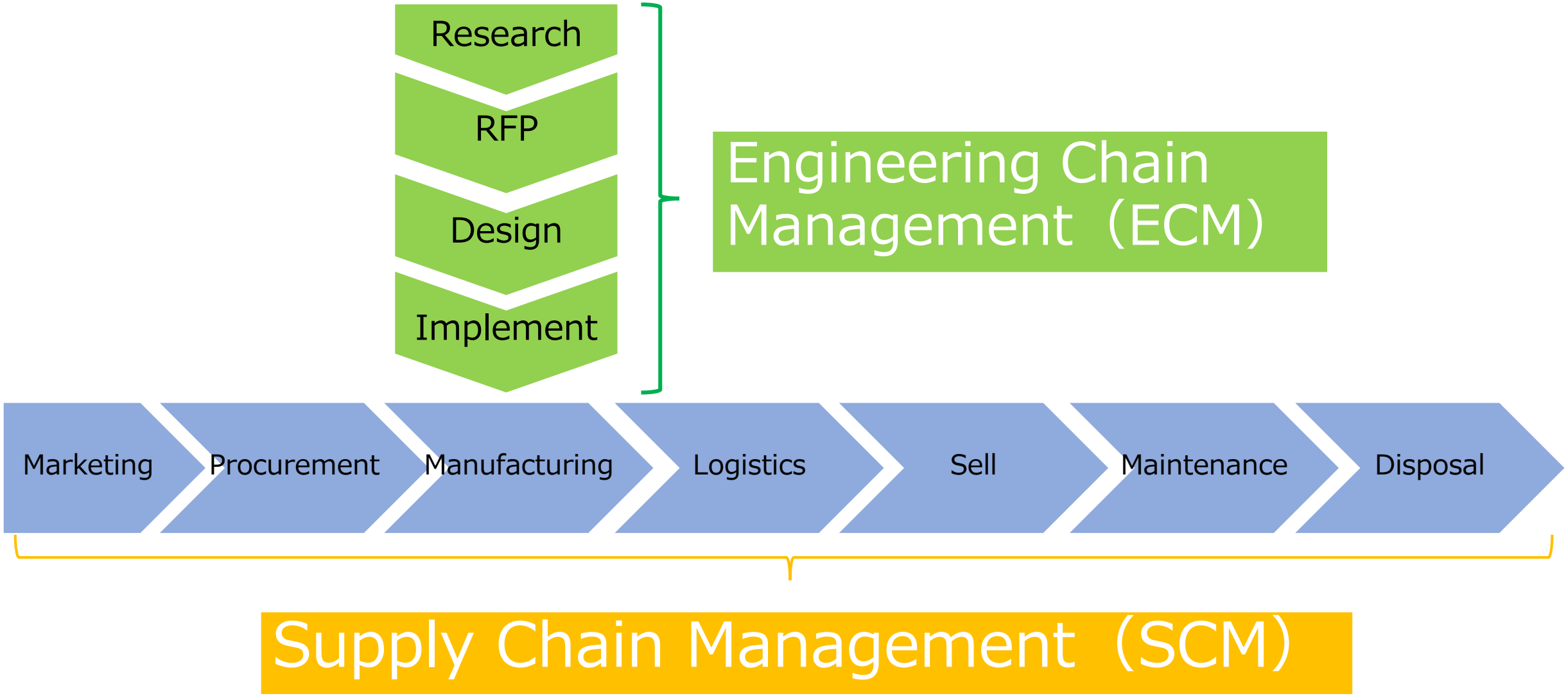
Challenges of ICS SCRM

ICS supply chain heavily relies on the **vendor reliability** and the **product reliability.**

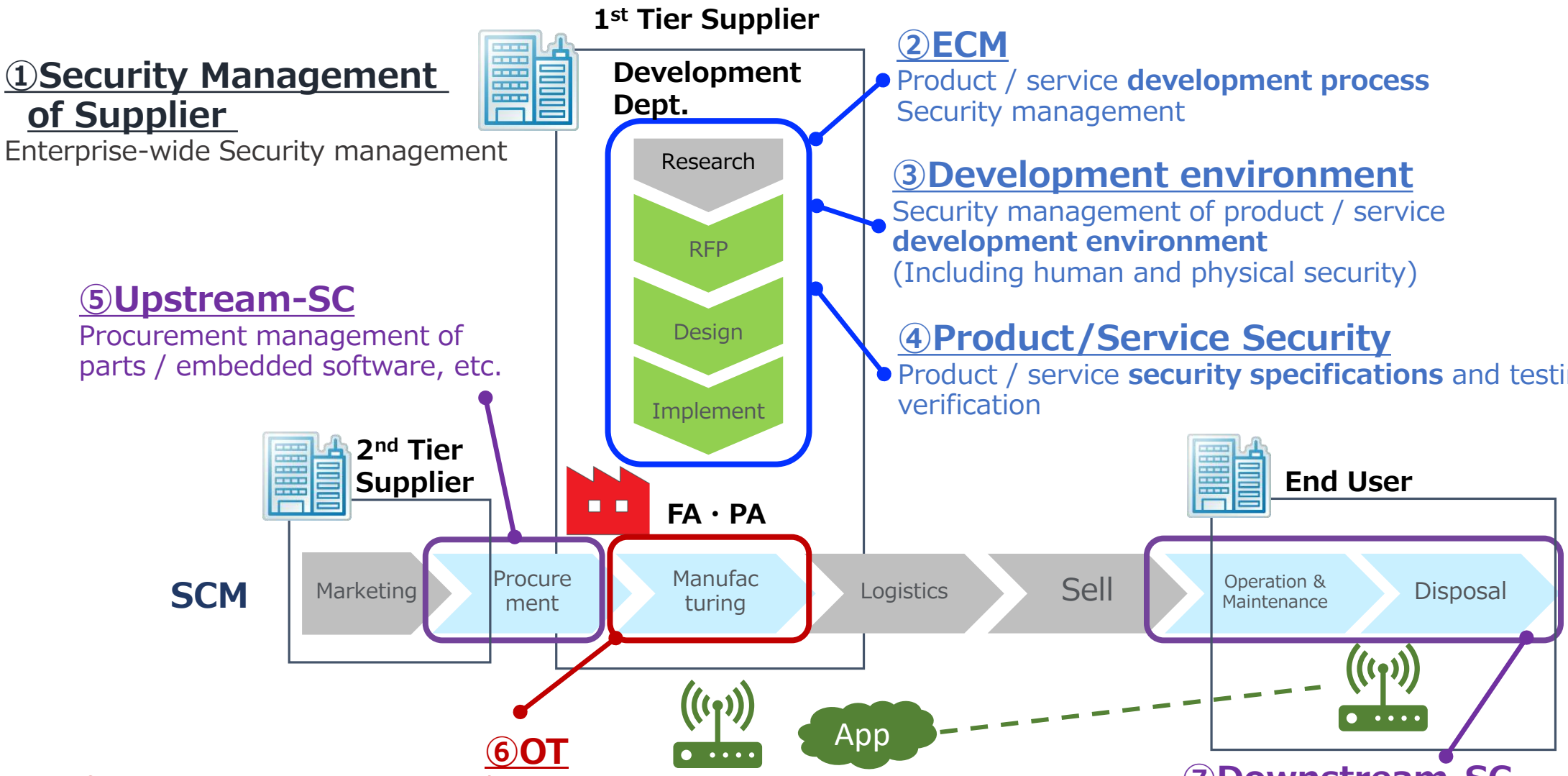


7 categories of the requirements for ICS supplier

ECM＆SCM


Research
RFP
Design
Implement
Engineering Chain Management（ECM）
Marketing
Procurement
Manufacturing
Logistics
Sell
Maintenance
Disposal
Supply Chain Management（SCM）

7 Categories for ICS SCRM



①Security Management of Supplier

Enterprise-wide Security management

②ECM

Product / service **development process** Security management

③Development environment

Security management of product / service **development environment** (Including human and physical security)

④Product/Service Security

Product / service **security specifications** and testing / verification

⑤Upstream-SC

Procurement management of parts / embedded software, etc.

⑥OT

Manufacturing equipment, personnel, etc. Security management

⑦Downstream-SC

Products / services **maintenance / operation / disposal** User support

Reference for 7 categories of SCRM

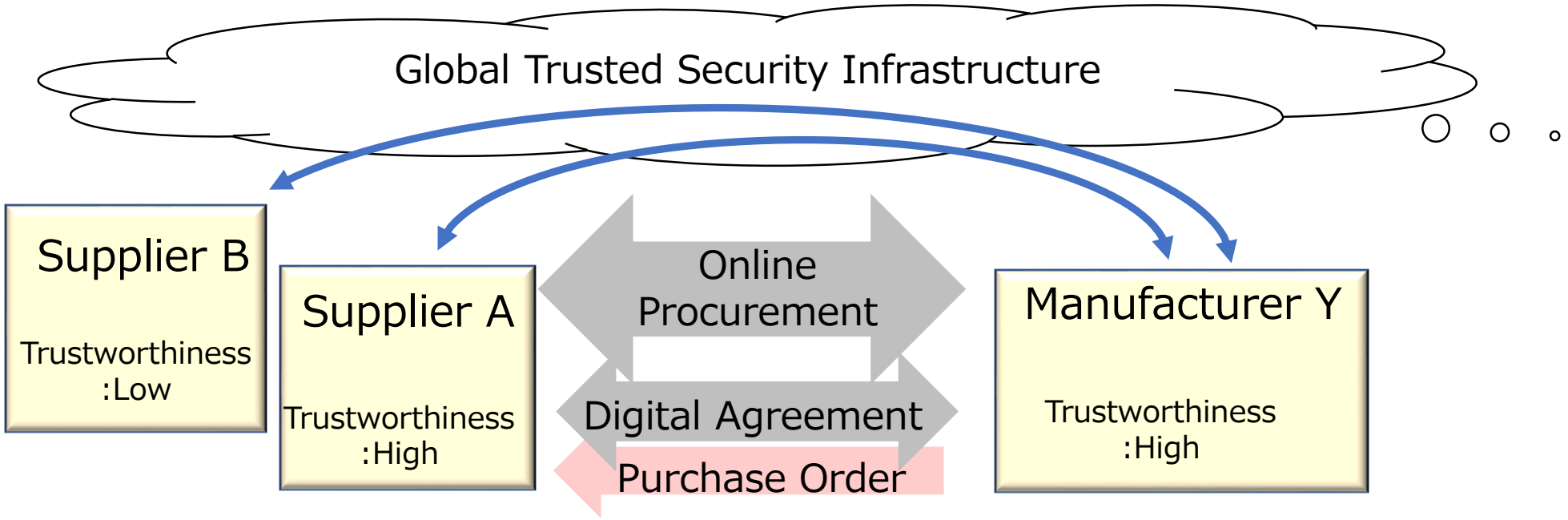
Categories		Reference
① Security Management of Supplier		NIST CSF, ISO/IEC 27001(ISMS),SANS Top 20 Critical Control, NIST SP800-171, NIST SP800-53、NIS Directive
② ECM		IEC 62443-4-1, ISO/IEC 21434
③ Development Environment		NIST SP800-171, NIST SP800-53
④ Product/Service	For IoT	NISTIR 8200, NISTIR 8228, NISTIR 8259(8259A), NIST Cyber-Physical Systems Framework, Considerations for a Core IoT Cybersecurity Capabilities Baseline(NIST), Cyber Security for Consumer Internet of Things(ETSI EN 303 645), IEC 62443-4-2,IEC/ISO 15408, UL2900 Series, Cyber/Physical Security Framework(CPSF, METI)*
	For Cloud	ISO/IEC 27017, ISO/IEC 27018, ISMAP(Information system Security Management and Assessment Program), FedRAMP, NIST SP800-190 (Container)
⑤ Upstream-SC		NIST SP800-161, NIST SP800-171, ISO/IEC 27036, NIST CSF(v1.1), CPSF, ISO/IEC 27001(ISMS), NERC CIP CIP-013
⑥ OT		IEC 62443-2-1(CSMS), IEC 62443-3-3, NIST CSF, NISTIR 8183, NIST SP800-82, NIS Directive, Good Practices for Security of Internet of Things in the context of Smart Manufacturing(ENISA),
⑦ Downstream-SC		IEC 62443-2-1(CSMS), ISO/IEC 21434, NIST CSF

*CPSF:Cyber/Physical Security Framework (CPSF) : https://www.meti.go.jp/english/press/2019/0418_001.html

Good practices of ICS SCRM in Japan

Security questionnaires for suppliers

- A template for security in the supply chain as baseline
- “Requirement” in the supply chain between the manufacturer and the supplier
- The answer for the questionnaire would be useful for the Manufacturer to determine “the supplier’s trustworthiness” and "how supplier’s in the value chain have the same trustworthiness level”



Select requirements in RRI questionnaire from CPSF

The total number of requirements in CPSF are 104

NIST CSF	METI/CPSF	
Identity	CPS.AM	ID.AM (Asset Management)
	CPS.BE	ID.BE (Business Environment)
	CPS.GV	ID.GV (Governance)
	CPS.RA	ID.RA (Risk Assessment)
	CPS.RM	ID.RM (Risk Management Strategy)
	CPS.SC	ID.SC (Supply Chain Risk Management)
Protect	CPS.AC	PR.AC (Identity Management and Access Control)
	CPS.AT	PR.AT (Awareness and Training)
	CPS.DS	PR.DS (Data Security)
	CPS.IP	PR.IP (Information Protection Processes and Procedures)
	CPS.MA	PR.MA (Maintenance)
	CPS.PT	PR.PT (Protective Technology)
Detect	CPS.AE	DE.AE (Anomalies and Events)
	CPS.CM	DE.CM (Security Continuous Monitoring)
	CPS.DP	DE.DP (Detection Processes)
Respond/ Recovery	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
	CPS.CO	RS.CO (Communications) RC.CO (Communications)
	CPS.AN	RS.AN (Analysis)
	CPS.MI	RS.MI (Mitigation)
	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

15 items

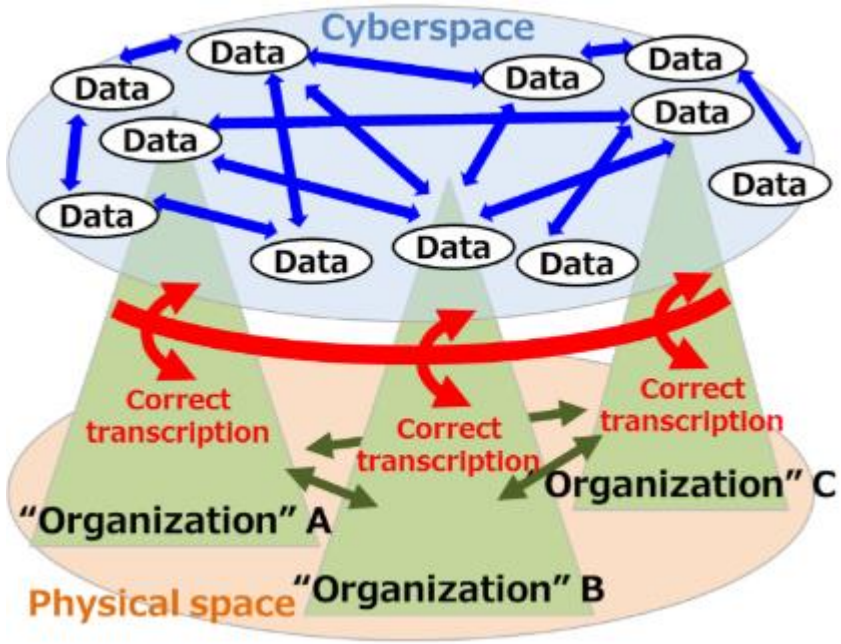
Select requirements in RRI questionnaire from CPSF

I . Why we had chosen METI CPSF (Cyber Physical Security Framework) as baseline:

- CPSF provides cybersecurity requirements focused on communications between companies and/or organizations categorized as 3 levels,
- The 1st layer ,The 2nd layer, The 3rd layer and six elements (organization, people, component, data, procedure and system).

- CPSF provides informative references of other standards (e.g. NIST CSF and IEC 62443) on each requirement and this information supports our tasks.

- CPSF is enterprise-wide security framework and security requirements are described for each entity in a company.



The 1st layer (Connections between organizations in physical space)
The 2nd layer (Mutual connections between cyberspace and physical space)
The 3rd layer (Connections in cyberspace)

The Cyber/Physical Security Framework (CPSF)
https://www.meti.go.jp/english/press/2019/pdf/0418_001a.pdf

Select requirements in RRI questionnaire from CPSF

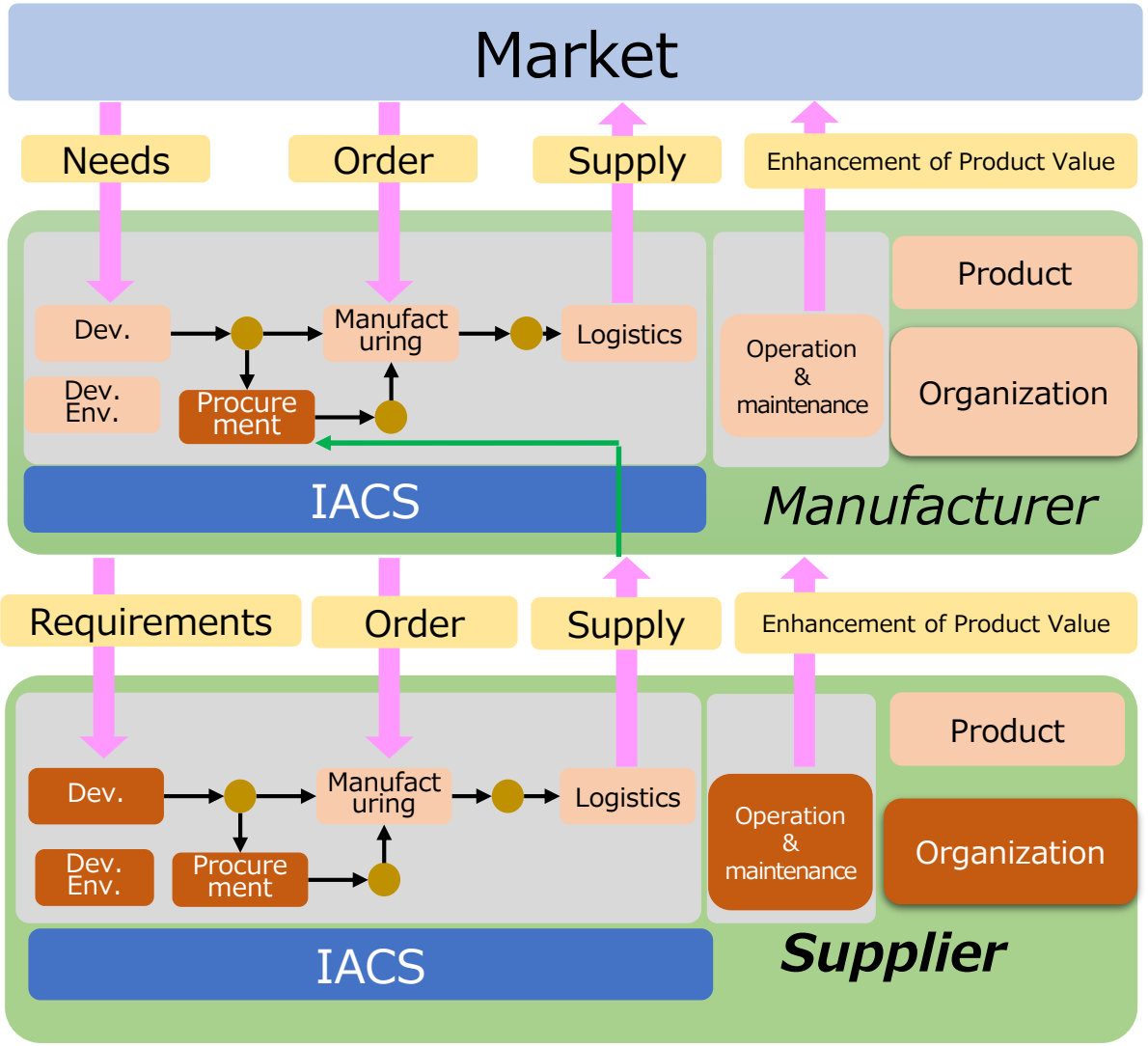
II. How we had prioritized requirements and selected 15 requirements is:

- Security requirements that we have already achieved in our companies.
- Security requirements that we require for product/system suppliers at least.
- Security controls in operation, management processes and organization.

(Technical security controls are out of scope because they depend on products)

- High(Policy)-level security requirements in the security risk management process.

Additional requirements



*IACS(Industrial Automation and Control System)
*Dev.(Development)
*Env.(Environment)

Selected category for questionnaire

I . We added additional requirements

-development,
-development environment,
-procurement,
-Operation & maintenance(O&M)
from the viewpoint of **product life cycle**.
e.g.) IEC 62443 2-1,2-4,4-1

II. How we had selected additional requirements is

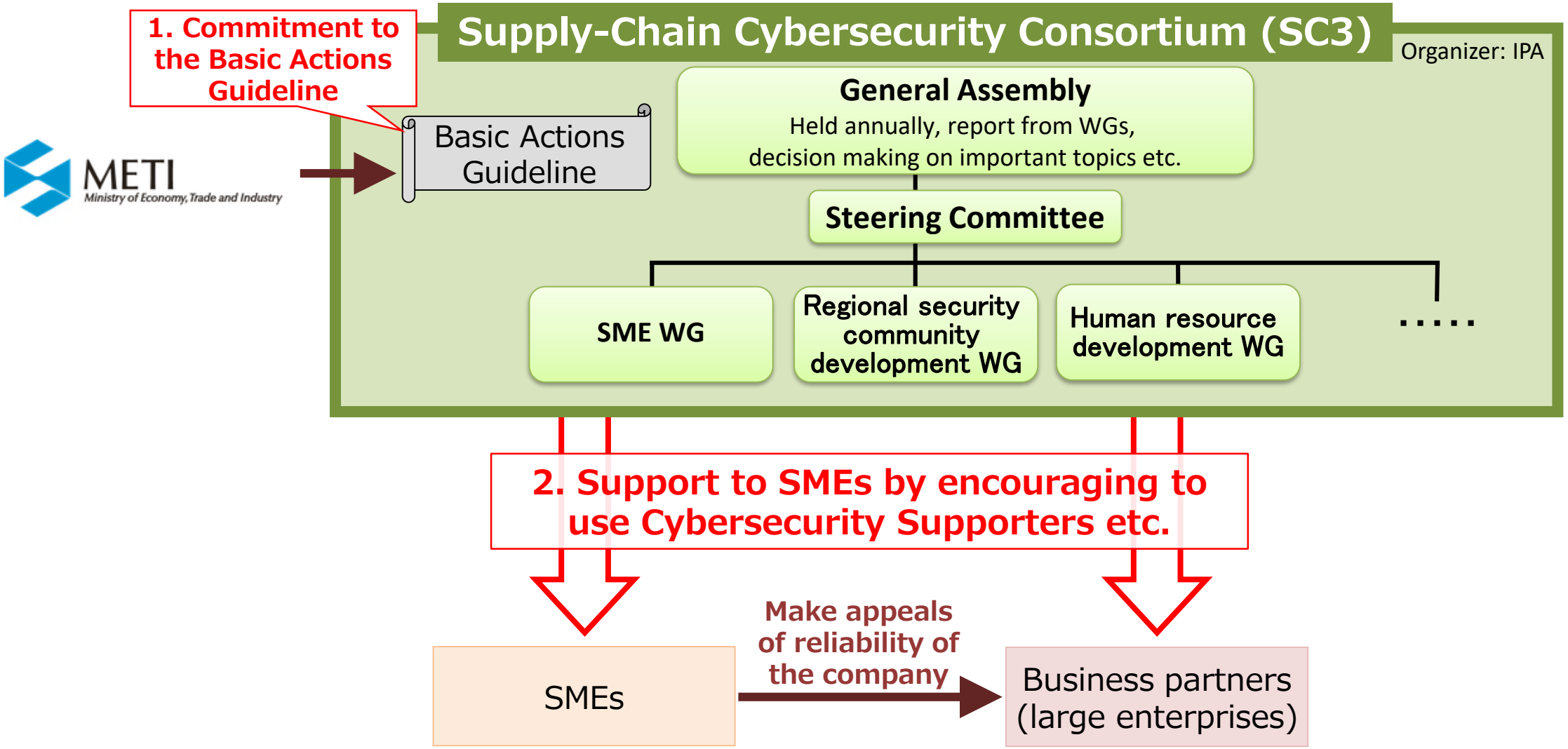
-already implemented by us
-appropriate to request the requirements to suppliers
-not technical but managing/operational
-not too specific but moderately general

Questionnaire in-practice- Example

Category			(5) Manufacturing site security - 1
Security requirement			Have you created a list of the hardware and software that make up the system and its management information? And is it properly managed?
Example : Answer	evidence		1)Including, but not limited to, an electronic or written list of assets, 2)including asset names, versions, network addresses, administrative responsibility, licensing information, and locations; operational policies, 3)including transportable media; asset bail line configuration and audit rules; automatic asset discovery and removal mechanisms; and more.
	Maturity level		Assets are identified, listed and prioritized according to their priority.
		1	☐Implemented ☐Planned to be implemented ☐Not applicable
			Maintain the asset list by regularly reviewing and updating it. Control and limit the use of portable media. Prohibit the removal of highly sensitive data.
		2	☐Implemented ☐Planned to be implemented ☐Not applicable
			The asset list is updated in real time. Regular audits for compliance with the organization's defined baseline structure. A mechanism is in place and operational to automatically detect and remove unauthorized assets.
		3	☐Implemented ☐Planned to be implemented ☐Not applicable

Supply-Chain Cybersecurity Consortium

- The industry-wide movement to practice the Basic Actions Guideline and strengthen cybersecurity of entire supply chains by both large enterprises and SMEs



Reference)
15 items of RRI questionnaires

Selected 15 security requirements for suppliers from CPSF

Identify	CPS.AM-1 **(Asset Management)**	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system.
	CPS.GV-1 **(Governance)**	Develop security policies, define roles and responsibilities for security across the organization and other relevant parties, and clarify the information-sharing method among stakeholders.
	CPS.RA-1 **(Risk Assessment)**	Identify the vulnerability of the organization's assets and document the list of identified vulnerability with the corresponding asset.
	CPS.RM-1 **(Risk Management Strategy)**	Confirm the implementation status of the organization's' cyber security risk management and communicate the results to appropriate parties within the organization (e.g. senior management). Define the scope of responsibilities of the organization and the relevant parties (e.g. subcontractor), and establish and implement the process to confirm the implementation status of security risk management of relevant parties.
	CPS.SC-1 **(Supply Chan Risk Management)**	Formulate the standard of security measures relevant to the supply chain in consideration of the business life cycle, and agree on contents with the business partners after clarifying the scope of the responsibilities.

*CPSF description(need to revise as questionnaire description) https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf

Selected 15 security requirements for suppliers from CPSF

Protect	CPS.AC-1 **(Identify Management & Access Control)**	Establish and implement procedures to issue, manage, check, cancel, and monitor identification and authentication information of authorized goods, people, and procedures.
	CPS.AT-1 **(Awareness &Training)**	Provide appropriate training and education to all individuals in the organization and manage the record so that they can fulfill assigned roles and responsibilities to prevent and contain the occurrence and severity of security incidents.
	CPS.DS-1 **(Data Security)**	If the organization exchanges protected information with other organizations, agree in advance on security requirements for protection of such information.
	CPS.IP-1 **(Information Protection Process & Procedures)**	Introduce and implement the process to manage the initial setting procedure (e.g., password) and setting change procedure for IoT devices and servers.
	CPS.IP-9 **(Information Protection Process & Procedures)**	Include items concerning security (e.g., deactivate access authorization and personnel screening) when roles change in due to personnel transfer.
	CPS.MA-1 **(Maintenance)**	Discuss the method of conducting important security updates and the like on IoT devices and servers. Then, apply those security updates with managed tools properly and in a timely manner while recording the history. Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable.

Selected 15 security requirements for suppliers from CPSF

Detect	CPS.AE-1 **(Anomalies & Events)**	Establish and implement the procedure to identify and manage the baseline of network operations and expected information flows between people, goods, and systems.
	CPS.CM-1 **(Security Continuous Monitoring)**	Conduct network and access monitoring and control at the contact points between corporate networks and wide area networks.
	CPS.DP-1 **(Detection Process)**	Clarify the role and responsibility of the organization as well as service providers in detecting security events so that they can fulfill their accountabilities.
Respond / Recover	CPS.RP-1 **(Response Planning)** **(Recovery Planning)**	Develop and implement previously the procedure of response after detecting incidents (security operation process) that includes the response of Organization, People, Components, System to identify the content of response, priority, and scope of response taken after an incident occurs.