日独連携で策定したメーカー・サプライヤー間セキュリティレベル合意プロトコル

２０２１年２月２２日

Robot Revolution & Industrial IoT Initiative(RRI)
三菱電機（株）　設計システム技術センター
コーポレートＰＳＩＲＴ　チーフエンジニア
米田　健

RRI and PI4.0's collaboration for Industrial Security

２０１６年４月に日独政府間の産業分野のサイバーセキュリティの連携スタート

- the RRI of Japan and the PI4.0, Germany, concluded an agreement on enhancement of collaboration（2016.4）
- Industrial cyber security is one of the areas for our collaboration to create synergy.

17年10月

Panelists

ロボット革命イニシアティブ協議会
Robot Revolution Initiative

WG1: "Manufacturing Business Reformation through IoT"

Industrial Security AG

Dr. Tsutomu Matsumoto

Dr. Takeshi Yoneda

European Commission

AIOTI
WG11: " Smart Manufacturing Industry "

PLATTFORM INDUSTRIE4.0

Plattform Industrie 4.0

WG3: " Security of networked Systems"

Dr. Wolfgang Klasen

Mr. Steffen Zimmermann

Mr. Lukas Linke

Mr. Thomas Walloschke

VDMA

ZVEI: Die Elektroindustrie

ドイツ経産省主催：Secure Global Industrial Value Networks

2018年５月

Securing Global Industrial Value Networks

synchronising international approaches

Programme Day 2 – 15 May

A deep dive into security aspects of global industrial value chains – Challenges and Approaches

from 08:00	Registration
08:15 – 9:15	Networking Breakfast // Speed-Dating Best Practice Poster Session on key question regarding Security 4.0
09:15 – 09:30	Introduction: Challenges of security aspects of global industrial value chains Michael Jochem, Robert Bosch // Plattform Industrie 4.0
09:30 – 10:30	Session 1: A secure ecosystem for smart manufacturing Dr. Wolfgang Klasen, Siemens // Plattform Industrie 4.0 Sebastian Piecha, Huawei
10:30 – 11:00	Coffee Break
11:00 – 12:00	Session 2: How can we guarantee a secure communication? Dr. Lutz Jänicke, PHOENIX CONTACT // Plattform Industrie 4.0 Takeshi Yoneda, Mitsubishi Electric // Robot Revolution Initiative
3:00 – 4:00	Panel: What to take away from the sessions and where to go **Dr. Wolfgang Klasen**, Siemens // Plattform Industrie 4.0 **Dr. Detlef Houdeau**, Infineon Technologies // Plattform Industrie 4.0 **Robert Martin**, The MITRE Corporation // Industrial Internet Consortium **Takeshi Yoneda**, Mitsubishi Electric // Robot Revolution Initiative
4:00	End of the conference

ドイツ経産省主催：Secure Global Industrial Value Networks(下記URL)より引用
https://www.bmwi-registrierung.de/Securing-Global-Industrial-Value-Networks/pdf/Programme.pdf
https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/2018-conference-report-securing-global-industrie-value-networks.pdf?__blob=publicationFile&v=5

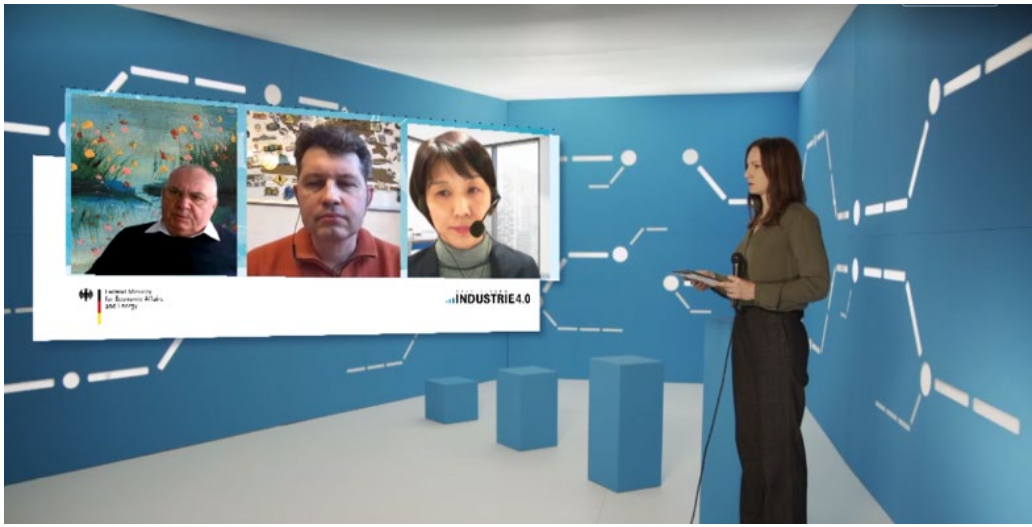
ドイツ経産省主催：Conference on Shaping a globally secure Industrie 4.0 Ecosystem

2021年1月

Day 1 – Trustworthiness and the way towards interoperability
27th January 2021

Moderation: Ina Karabasz

11:00 a.m.-11:05 a.m.	**Welcome and Introduction**
11:05 a.m.-11:15 a.m.	**Welcome Note from the Federal Ministry for Economic Affairs and Energy, Germany – Elisabeth Winkelmeier-Becker** (Parliamentary State Secretary)
11:15 a.m.-11:30 a.m.	**Welcome Note from the European Commission – Khalil Rouhana** (Deputy Director-General in DG CONNECT, European Commission)
	Session on "Trustworthiness" – Trustworthiness for secure supply chains within a framework of international standards.
11:30 a.m.-11:50 a.m.	**Dr. Wolfgang Klasen** (Siemens / Plattform Industrie 4.0): Achieving Trustworthiness of Secure Supply Chains for Industrie 4.0
11:50 a.m.-12:10 a.m.	**Ekaterina Rudina** (Kaspersky ICS CERT): Approaching industrial IoT trustworthiness in international standards and guidelines
12:10 a.m.-12:30 a.m.	**Ayaji Furukawa** (Toshiba Corporation / RRI): The Role of Trustworthiness in secure supply chain for connected industries
12:30 a.m.-12:45 a.m.	Q&A Session
12:45 a.m.-01:15 p.m.	**Prof. Dr. Georg Borges** (Institute for Legal Informatics, Saarland University) and **Benjamin Korth** (Fraunhofer Institute for Material Flow and Logistics IML): Towards the automation of trustworthiness: Basic concepts and practical demonstration from the „Industry 4.0 Legal Testbed"
01:15 p.m.-01:45 p.m.	**Break**



-The goal of our activity is:
*To identify new security requirements for Industrie 4.0.
*To incorporate trustworthiness in coming interconnected economies.

-PI4.0(Germany) and RRI(Japan) announced three common position papers," Facilitating International Cooperation for Secure Industrial Internet of Things/ Industrie4.0"
(16th March 2017, 16th May 2018, 3rd April, 2019)

-PI4.0 and RRI had discussed the role of trustiness intensively during FY19 and have provided the whitepaper "IIOT Value Chain Security – The role of Trustworthiness."

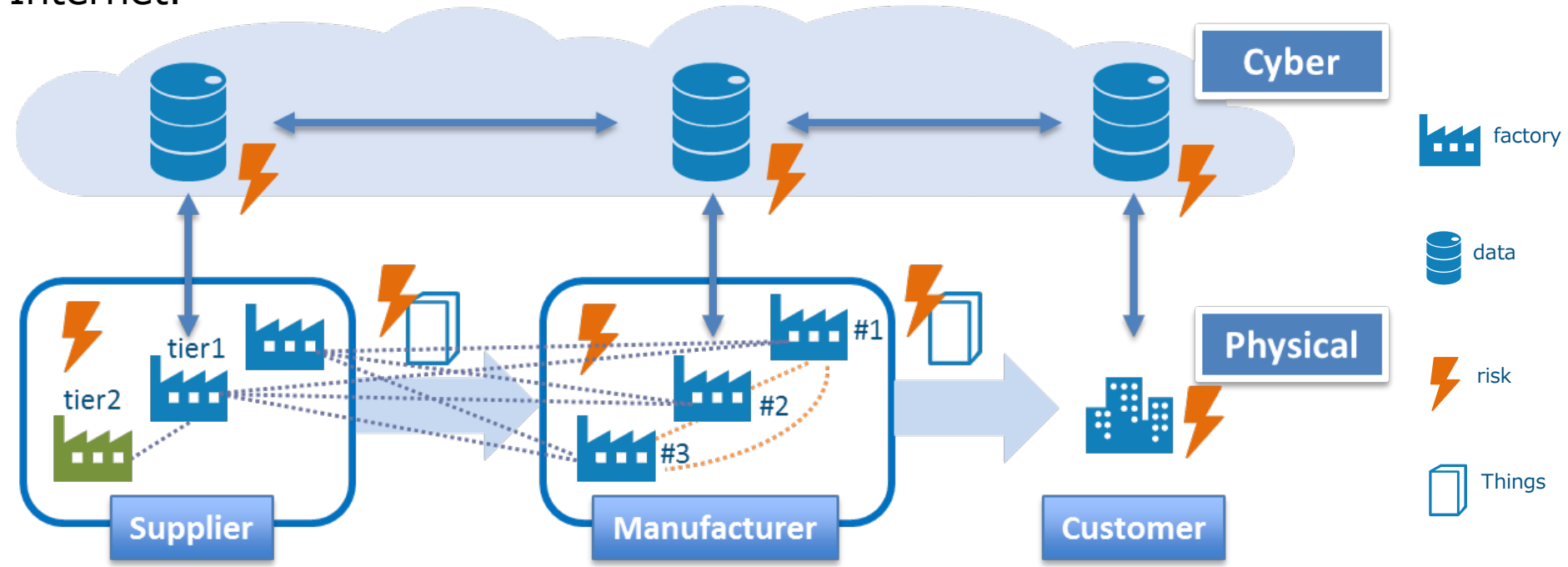
-Today what PI4.0 and RRI had discussed in FY19 is introduced.

PI4.0: Plattform Industrie4.0, RRI: Robot Revolution & Industrial IoT Initiative

Global Value Chain

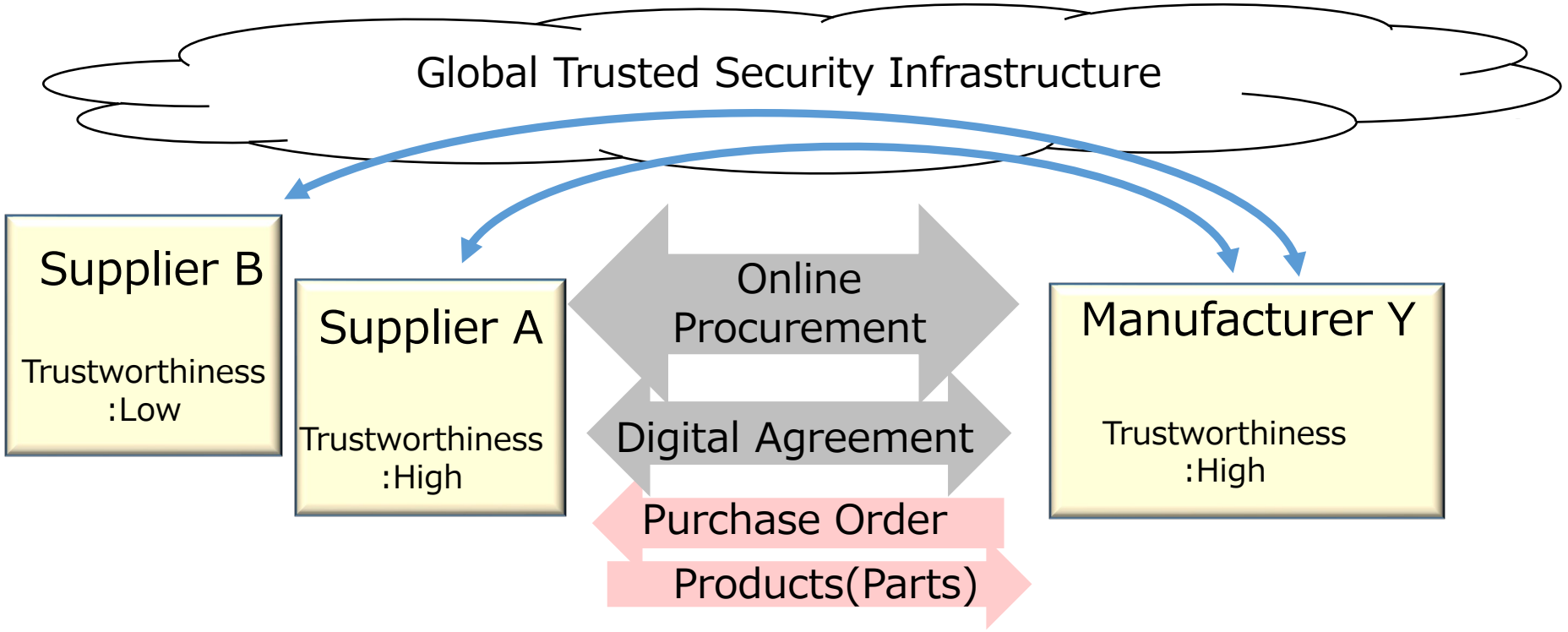
Information security has become an essential aspect of trustworthiness because manufacturers and suppliers are becoming interdependent as parties in the global value chain accelerated through the Internet.

1)Needs to develop products that satisfy rapidly changing customer needs.
2)Needs to collaborate with suppliers whose products are required to develop the products.
3)Needs to find appropriate suppliers from all over the world timely though the Internet.



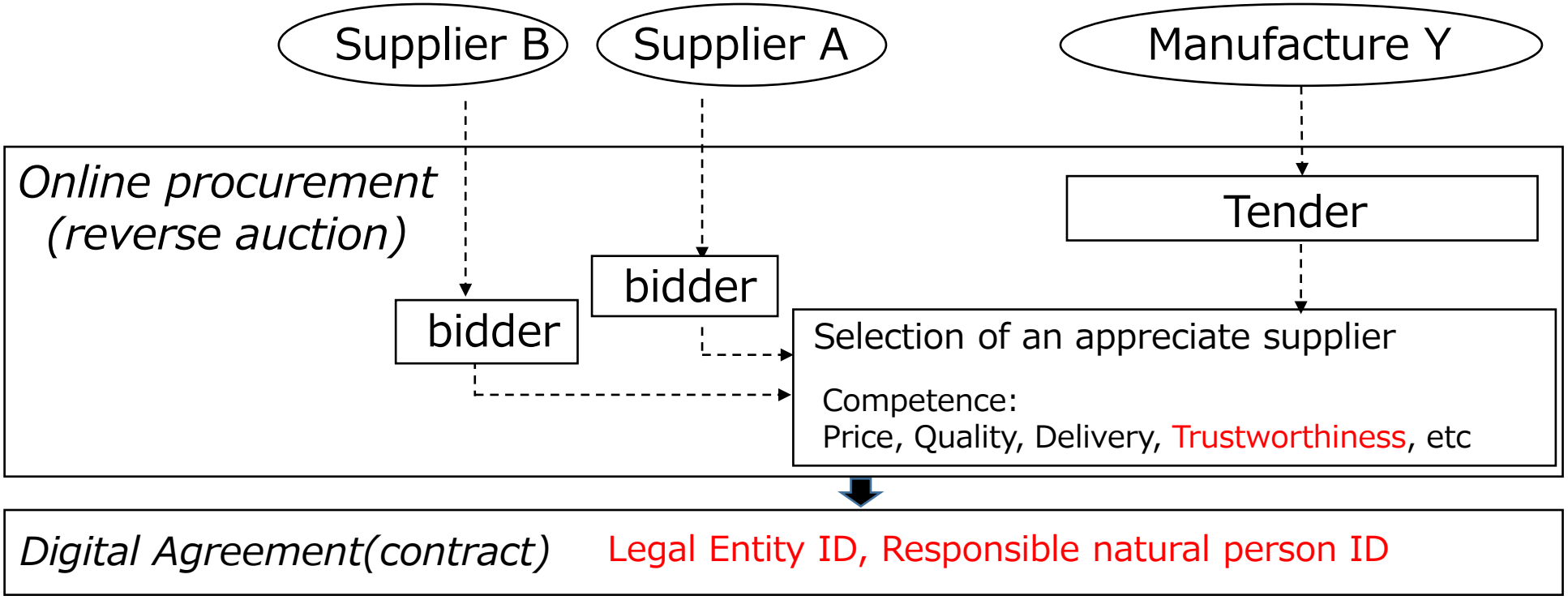
A use case for understanding the role of trustworthiness

-To find an appropriate supplier, what level of trustworthiness the supplier has is crucial because the supplier would share critical information and high availability among other parties in the value chain.
-So by using online procurement as a use case, we had discussed "what is trustworthiness" ,"how to determine the party's trustworthiness" and "how parties in the value chain have the same trustworthiness level" .

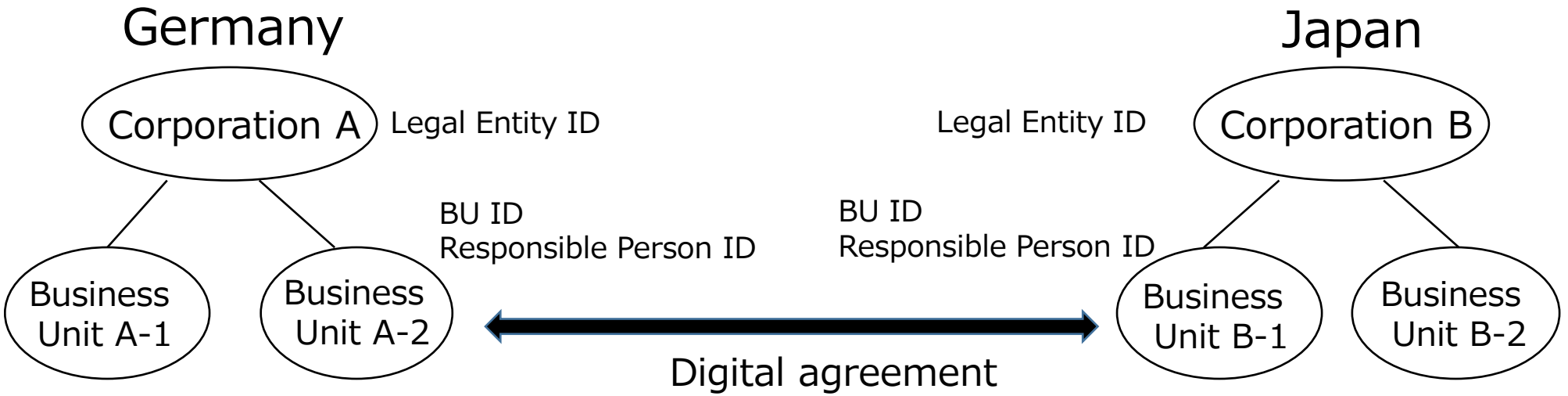


Online Procurement and Digital Agreement

- In **Online procurement** the following security aspects of the parties are the matter.
  *authenticity of parties
  *security level implemented in their organizations
  *security level of their products
- In **Digital agreement** the following security aspects are the matter.
  *authenticity of the organization as a legal entity represented by a legal entity ID
  *authenticity of the signer as a responsible natural person represented by a natural person ID



ID systems for online procurement

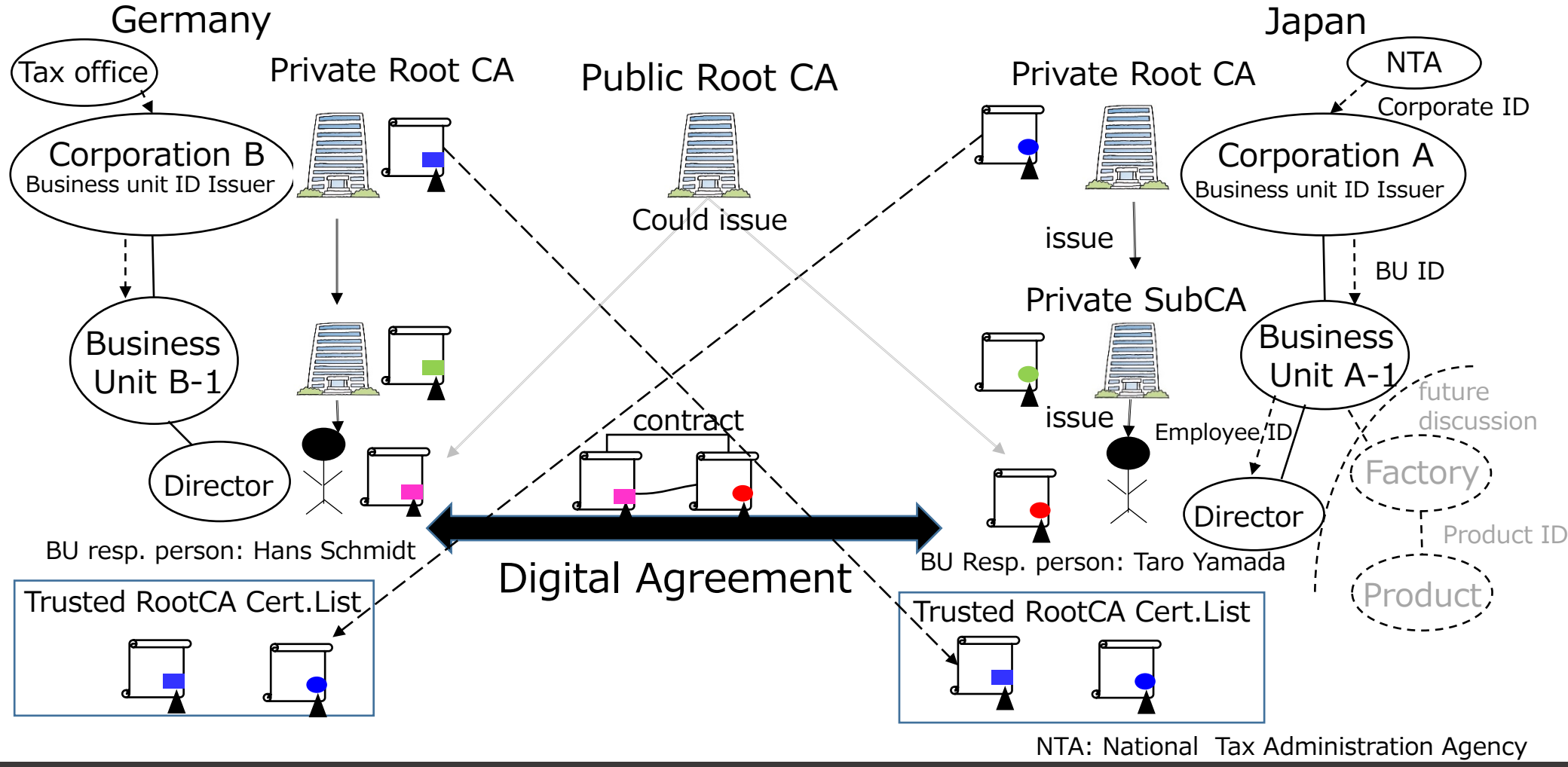


Discussion items	Germany	Japan	Technical Issus
Legal Entity ID and its provider	VATIN (USt-IdNr) The tax office	Corporate No. NTA	—
Natural person ID/BU ID and their provider	eIDAS	Employee ID Each Corp.	BU ID code system is not yet determined.
Digital Certificates for natural persons	eSignature, eIDAS	Each Corp.	Cross certification is needed.
Digital Certificates for legal entities	eSEAL, eIDAS	Each Corp.	Cross certification is needed.

NTA: National Tax Administration Agency

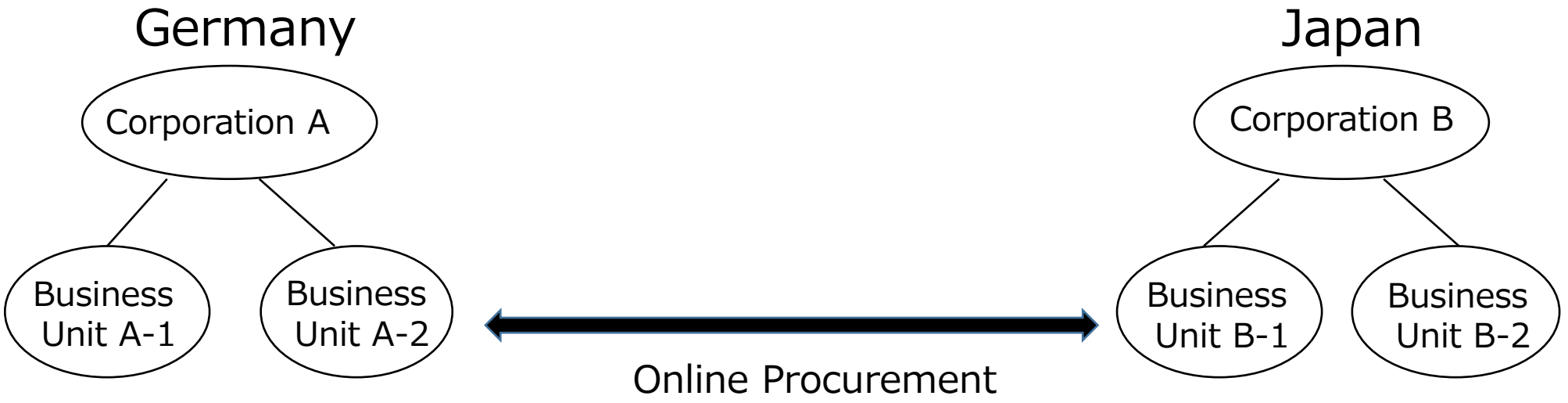
A Certificate Authority(CA) structure for online procurement

-Digital signatures of responsible persons are used for digital agreement.
-A CA structure for issuing digital certificates to responsible persons is needed for each side.
-A mechanism of trusting each other's Root CA is needed.



NTA: National Tax Administration Agency

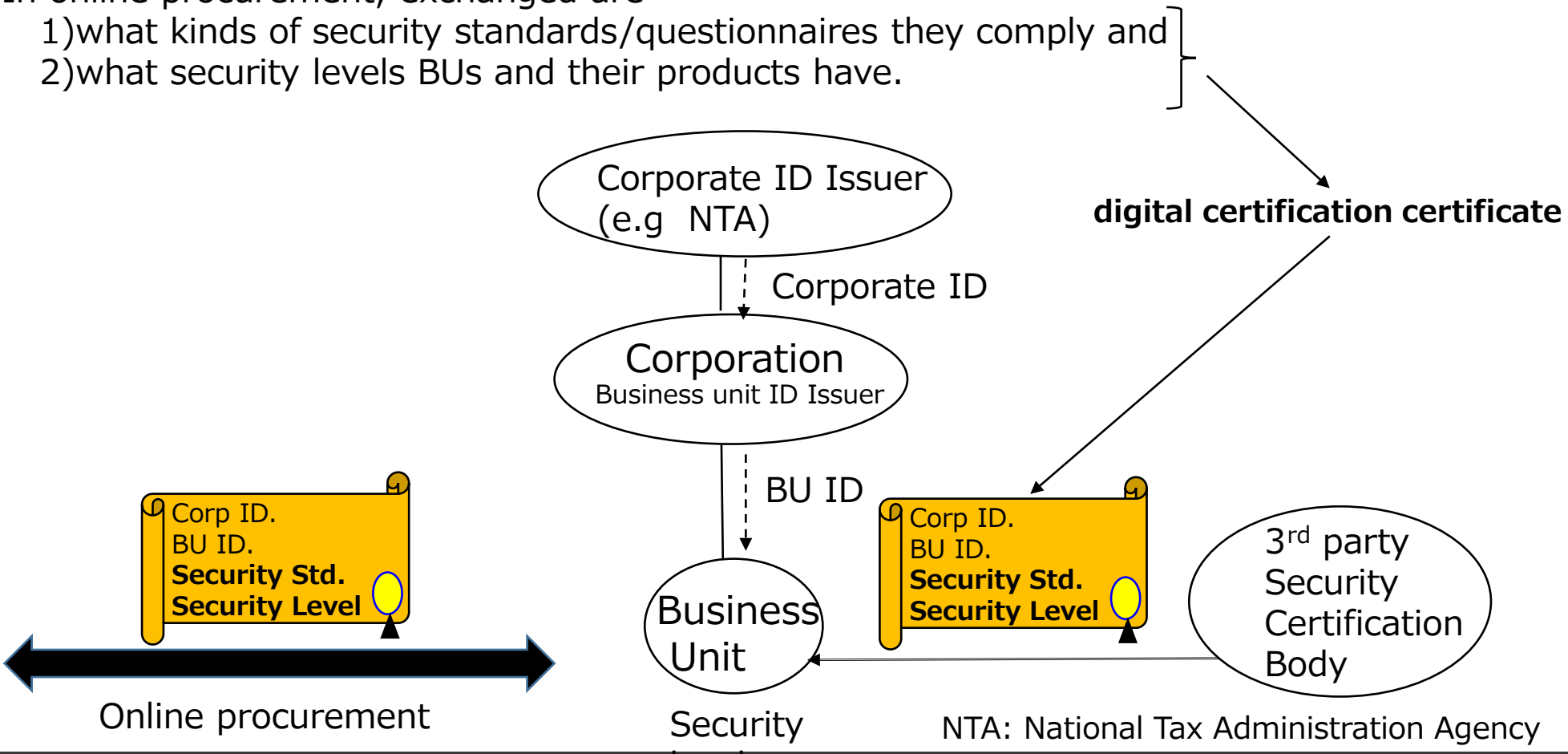
Security exchanged though online procurement



Discussion items	Germany	Japan	Technical Issus
Standards used for security(trustworthiness) assurance	ISO 27001,IEC 62443,etc		Machine readable certification certificate is not yet established
Security(Trustworthiness) level agreement	-	-	There is no agreement protocol

Security exchanged though online procurement

1.Corporate ID Issuers assure the existence of corporations.
2.Each corporation has responsible for assigning a BU ID to a BU.
3.Each corporation has a CA which issues digital certificates to employees with IDs and names.
4.Those certificates are used for digital signatures(by natural persons) on a digital agreement.
5.In online procurement, exchanged are
  1)what kinds of security standards/questionnaires they comply and
  2)what security levels BUs and their products have.

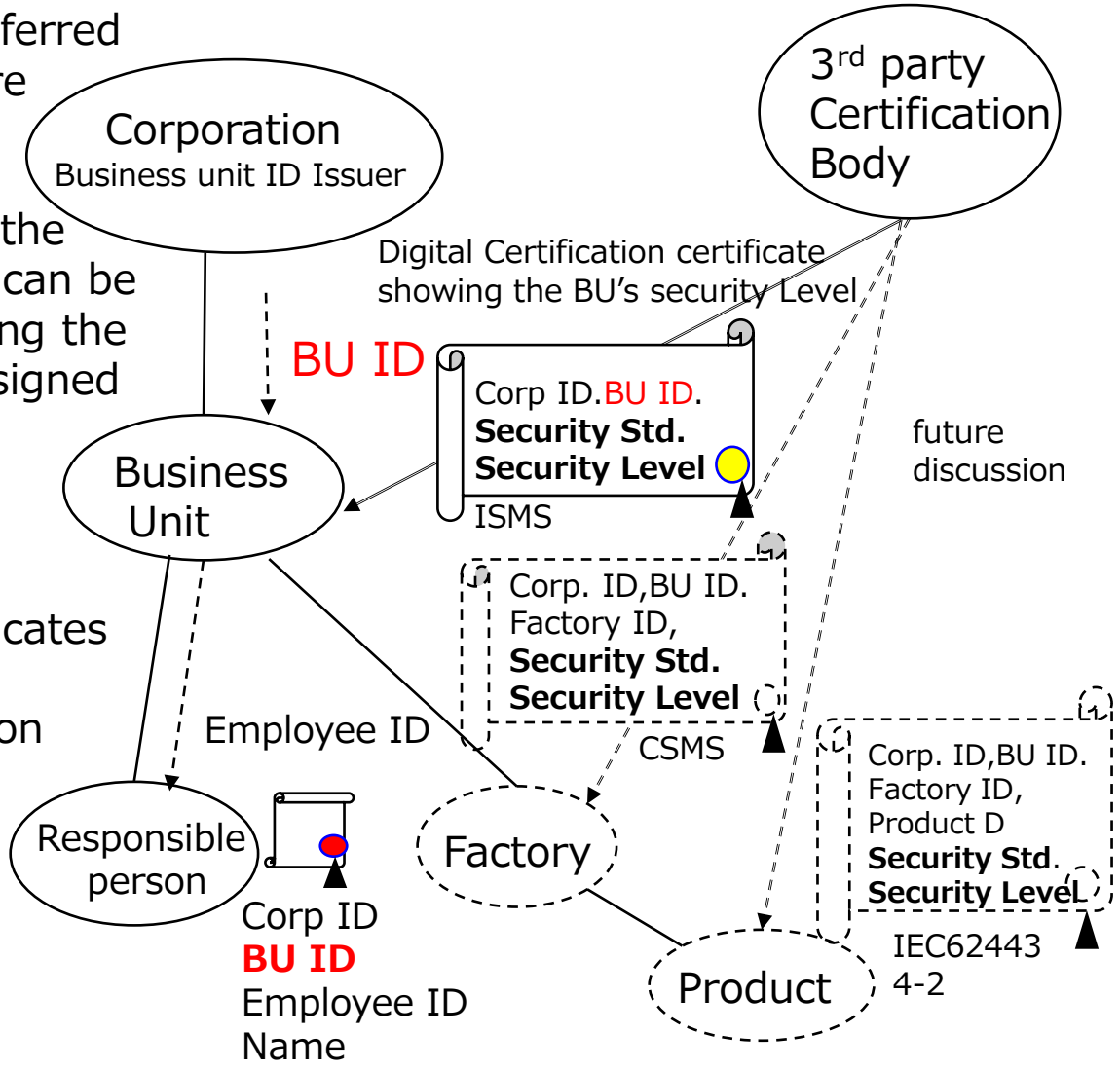


IDs and digital certification certificates

1. A Corp.ID should be globally unique and trusted, because they are used and referred to in various economic activities, where corporation identification is critical.

2. A BU ID should be globally unique for the same reason. Such global uniqueness can be achieved, for example, by concatenating the unique global Corp.ID and a BU ID assigned uniquely within the corporation.

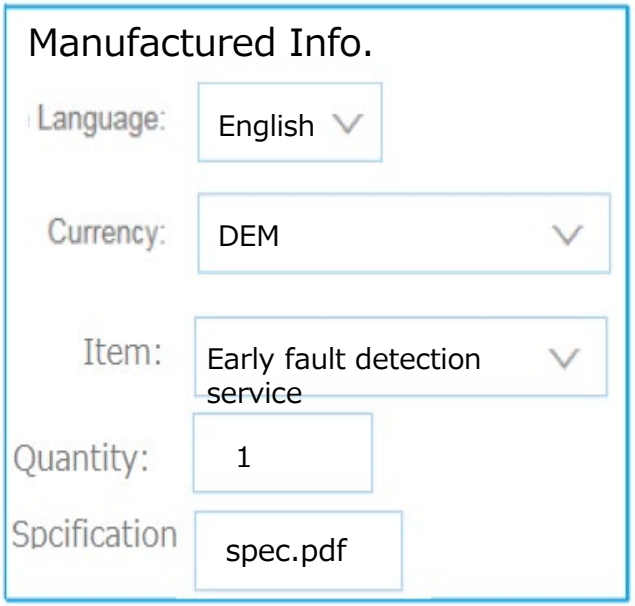
3. BU IDs would be used in at least two different applications.
   1) BU IDs included in the digital certificates used for digital agreements.
   2) BU IDs included in digital certification certificates.



A Sample GUI for Online Procurement

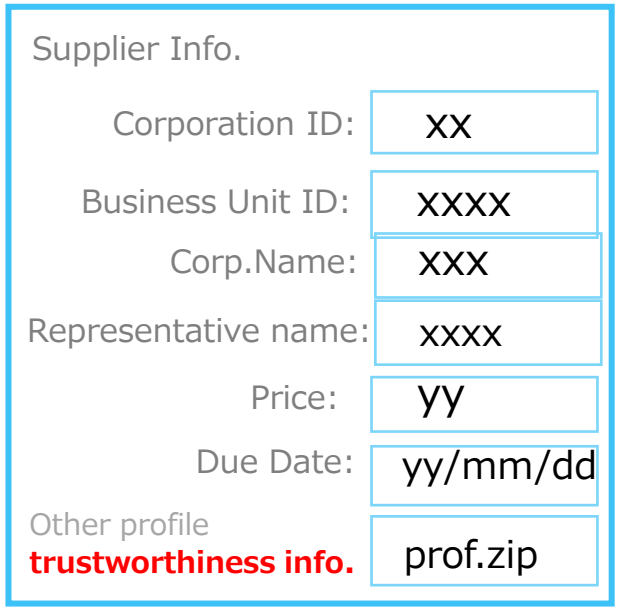
After assigning IDs and Digital certificates to corporations/BUs/responsible persons, manufactures and suppliers can participate in online procurement.

Request for work



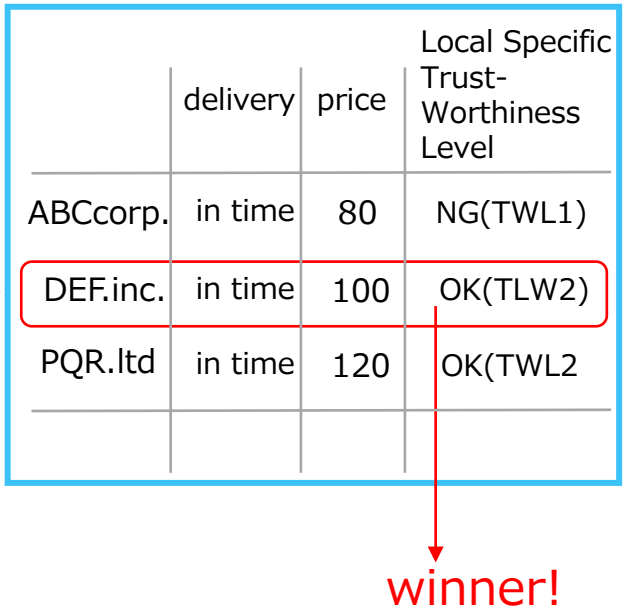
Manufacture(tender) side

Submission to bid



Supplier(bidder) side

Supplier selection



Manufacture(tender) side

A sample security requirements for online procurement

ISO 27001: Protection of development environment in supplier
IEC 62443: Implementing security of product in suppliers' development process

Organization Trustworthiness: ISO 27001 + Supply chain security

1. Information Security Policy	**(ISO 27001 A.5)**
2. Organization of Information Security	**(ISO 27001 A.6)**
3. Human Resources Security	**(ISO 27001 A.7)**
4. Asset management	**(ISO 27001 A.8)**
5. Access Control	**(ISO 27001 A.9)**
6. Cryptography	**(ISO 27001 A.10)**
7. Physical and Environmental Security	**(ISO 27001 A.11)**
8. Operations Security	**(ISO 27001 A.12)**
9. Communications Security	**(ISO 27001 A.13)**
10. System acquisition, development and maintenance	**(ISO 27001 A.14)**
11. Supplier Relationships	**(ISO 27001 A.15)**
12. Information Security Incident Management	**(ISO 27001 A.16)**
13. Information Security Aspects of Business Continuity Management	**(ISO 27001 A.17)**
14. Compliance	**(ISO 27001 A.18)**
15. Supply chain security	**(NIST CSF and CPSF)**

- Clarify, manage and continuously improve the role of the organizations in the supply chain
- Specify how to manage the components produced by the organization's supply chain

System/Component Trustworthiness: IEC 62443 3-3,4-1,4-2

- Integrity in Product Lifecycle
- Document/Secure Configuration, Testing for Security Vulnerabilities, Prevention of Undocumented Functions, Back Doors and Easter Eggs, Provide additional documents and so on (T.B.D).

Security levels used for online procurement

Types of security levels are categorized the following:
*Level of Maturity
*Level of Security: (A) Organization (B) System/Component (Technical)

Document	Type of security levels		
	Maturity	Security	
		Organization	System/Component (Technical)
NIST CSF	Framework Implementation Tier (4 levels)		–
NIST SP800-82 (FISMA)	–	ICS Impact level (3 levels)	
METI CPSF	–	Measure Requirement (3 levels)	
ISA/IEC 62443	ML (5 levels)	ISO/IEC directive verbal form(2 levels)	SL (4 levels)
VDA-ISA	Maturity Level (6 levels)	Required level (5 expressions)	
ISO/IEC 15408	–	CC EAL(7 levels)	
ISACA COBiTS	Process Capability Level(6 levels)		

White paper　released 2020.9
(IIoT Value Chain Security -The Role of Trustworthiness)

- PI4.0 and RRI had discussed the role of trustworthiness intensively during FY19 and have provided the whitepaper **"IIOT Value Chain Security –The role of Trustworthiness" 2020.9**

- *In the future, collaboration activities between RRI and PI4.0 plan to realize the TWP(Trustworthiness Profile) in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers.*

- On the Japanese side,
  establish a "Security questionnaires for suppliers"

5

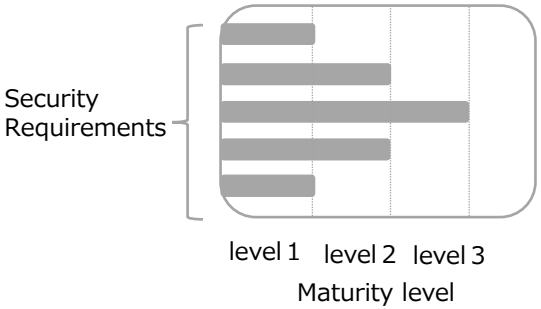
Use case of profile (Answer of questionnaire)

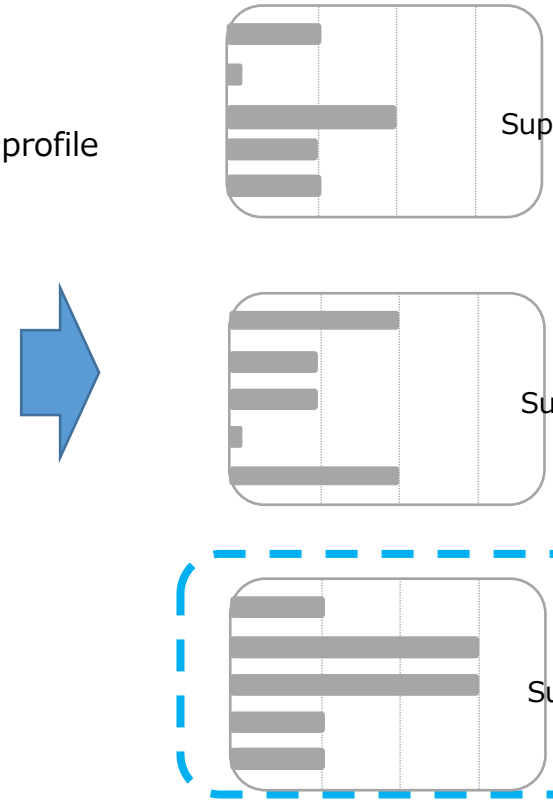
Supplier

Answer from supplier=Supplier's capability

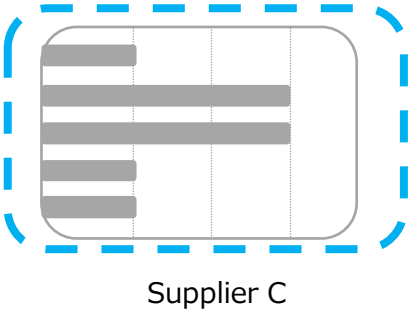
Manufacturer

Expected level for trustworthiness profile
= requirement





Selected supplier



Maturity level for Trustworthiness

◆ Check maturity level by two axes
①Management – layer process
Processes achieved by high-level management side
(Policies and procedures referred by senior managers)
②Operation-layer process
Security processes achieved by manufacturing and production side
(Policies and procedures referred by personnel in fields)

Partial

Level1

①Management
・Partially implemented by organization level

②Operation
・Documented

Risk Informed

Level2

①Management
・Implemented by organization and got approval by a chief security officer

②Operation
・Documented and developed

Repeatable

Level3

①Management
・Implemented, reviewed and adapted by organization
・Got approval by a chief security officer

②Operation
・Documented, developed
・Reviewed, updated

The contents and the number of evidences are developed

Risk management process is developed

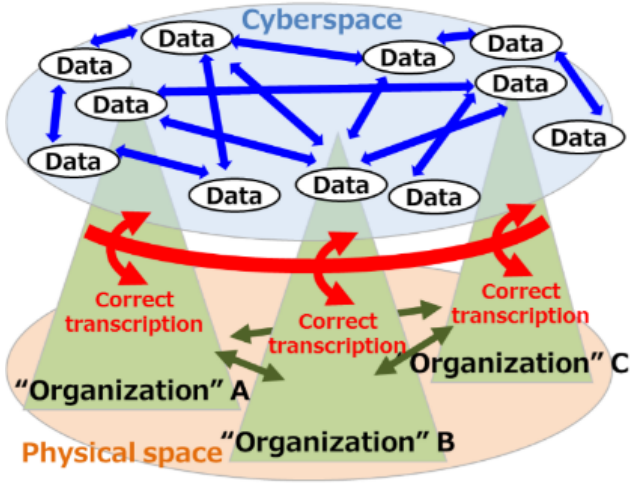
Selected requirements in RRI questionnaire from CPSF

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

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)

Selected requirements in RRI questionnaire from CPSF

II. How we had prioritized requirements and selected 17 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.

12

Select requirements in RRI questionnaire from CPSF

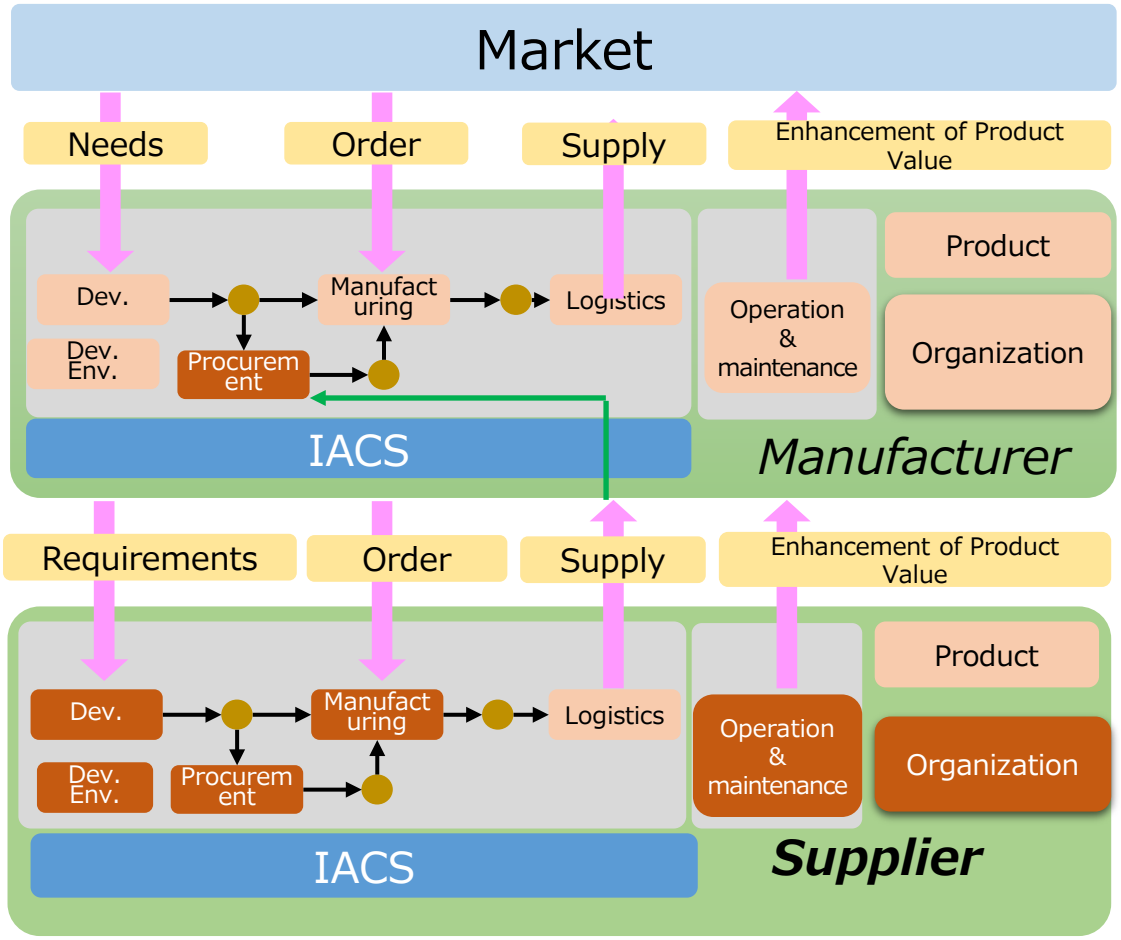
The total number of requirements in CPSF are 104

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

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)

4 domains
17 items

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)
-Production equipment

from the view point of product life cycle.
e.g.) IEC 62443 2-1,2-4,4-1

14

Additional requirements

ECM development process	IEC 62443-4-1 SM	Include security management requirements in the product development process.
Development environment	IEC 62443-4-1 SM	Manage product development environment according to security requirements.
	IEC 62443-4-1 SM	Confirm that the source code and data contents of the product are maintained correctly.
Procurement	IEC 62443-2-4 SP.02	Present documentation that ensure the security level of the products and services provided.
O&M	IEC 62443-4-1 SG	Provide manuals to securely set up and make the equipment robust.
	IEC 62443-4-1 SG	Provide manuals for secure use and disposal of equipment.
Production equipment	IEC 62443-2-4 SP.01.01, SP.01.02	Manage construction of production equipment according to security requirements.
	IEC 62443-2-1	Manage operation of production equipment according to security requirements.

◆ ***This requirement is added because it will become important when production facilities are connected to IT networks within the company in the Connected Industry in the near future.***

16

Questionnaire in-practice- Example

Category			Governance
Security requirement			Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
Example : Answer	evidence		History of security policy development and approval, and approval of revisions to the security policy. Describe the security roles and responsibilities of the organization and other relevant organizations (e.g., contractors), and any arrangements for security with contractors in the security policy.
	Maturity level	1	The security officer of the organization has developed (documented) a security policy.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		2	The organization's Chief information security officer has approved and implemented the security policy. The organization manages and implements the approved documents.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		3	The organization's security officers and Chief information security officer regularly review, update, and maintain security policies.
			☐Implemented ☐Planned to be implemented ☐Not applicable

17

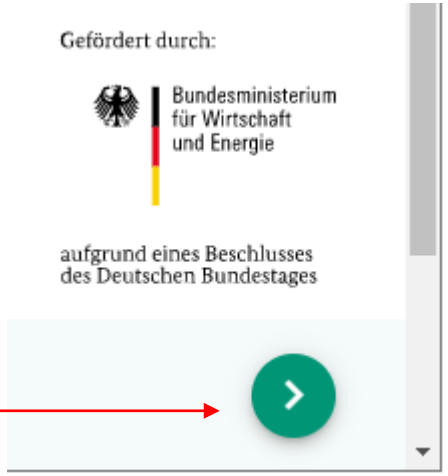
Next Step

- **RRI is developing security questionnaires for suppliers in FY2020 based on Cyber/Physical Security Framework issued by METI, Japan.**

- **RRI expects the questionnaire and the answer for the questionnaire would be standardized, would be used digitally for online contracts.**

DEMO from ドイツ：フランフォーファ研究所

https://legaltestbed.org/en/trust-demonstrator/
https://twp-demonstrator.legaltestbed.org/landingPage



上記ページのココをクリックしてスタート

Thank you!