CPSEC-WP-2020002

Building Trust in Supply Chains

Report Two:

Trust Building Technology

January 2020
Cyber Physical Security Research Center
National Institute of Advanced Industrial Science and Technology (AIST)

Abstract

In recent years, there have been many reported incidents (including security incidents) that damage the trust of products and services in supply chains. This paper, which is the second part of a white paper entitled "Building Trust in Supply Chains - Report One: Analysis of Incidents that Damage Trust and Basic Approach to Trust Building," describes technology for building trust that prevents such incidents. First, we introduce the basic concept of trust building and describe in detail the requirements for trust building and the presentation of evidence. Next, we describe the technology for realizing trust between companies and chain of trust along the supply chain, which are core technical processes for trust building. Furthermore, we describe the benefits of this technology by referencing and describing incident cases. Lastly, we explain that our basic policies for building trust share the same approach as "trust" described in the information technology (IT) field.

1. Basic Approach of Building Trust

In recent years, there have been reports of incidents (including security incidents) that damage the trust in products and services in diverse industrial fields, ranging from telecommunications equipment such as servers and routers to social infrastructure such as automobiles, railroads, and buildings.

With the globalization of trade and logistics, supply chains for products and services are increasing in size and complexity. Additionally, advancements in IT have led to the realization of the concept of the Internet of things (IoT), with hybrid systems called cyber-physical systems (CPS), which combine information and mechanical systems at a high level, becoming increasingly widespread.

As systems that support global supply chains become larger and more complex, there are

concerns that the probability of manufacturing or operational troubles or failures and the risk of damaging the trust of systems will both increase. Additionally, CPS have a greater attack surface (sum total of all targets of attacks), which is pointed out as increasing the chances of being attacked.

In White Paper - Report One [1], we investigated incident cases that damaged the trust of the supply chain; these involved various products and services, including CPU boards, foods, and aircraft operations. We analyzed the cases that we collected and obtained the following common characteristics.

Characteristics of Supply Chain Incident Cases

(1) Incidents occurred because of either a defect in the necessary work rules or a violation of the rules when executing business processes relating to the design, procurement, manufacturing, distribution, or operation of products and services.

(2) Incident causes can be created and incidents can arise in any business process along the supply chain. Additionally, incident causes can be created and incidents can arise in different organizations.

White Paper - Report One presents the basic approach to realizing trust building in the supply chain, as shown in Figure 1, based on the above analysis results.

(1) Trust Building between Organizations

Trust between organizations that deliver and receive products and services is built by the acquiring organization requesting the requirements related to the trust and function of products (“Request trust requirements” in Fig. 1), and as necessary, the supplying organization returning evidence that its own process is sufficient for the requirements (“Return evidence” in Fig. 1). In this paper, trust requirements refer to requirements that encompass trust-related requirements in addition to functional requirements.

(2) Trust Building in the Entire Supply Chain

Trust of products and services in an entire supply chain is built by the organizations participating in the supply chain chaining the trust between organizations (“Chaining trust along a supply chain” in Fig. 1).

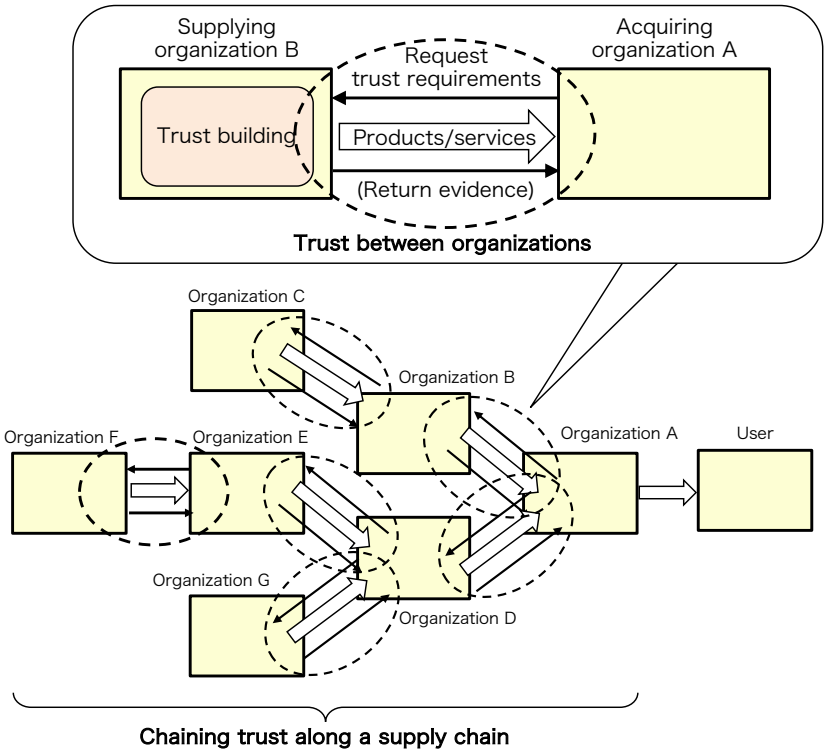

Figure 1. Basic Approach of Trust Building

The following constitutes the trust building technology that realizes the above basic approach. Chapter 2 describes the request of trust requirements, the return of evidence, and the building of trust of the entire supply chain, which are key to the basic approach to trust building for products and services. Since the chapter includes a detailed discussion, read and go through it as necessary. Chapter 3 describes the technology process for trust building between two organizations in the supply chain. Chapter 4 describes the technology process for trust chain building in the entire supply chain.

2. Considerations for Trust Building

2.1. Request of Trust Requirements of Acquiring Organizations

The acquiring organization requests the trust requirements for the products or services (hereafter collectively "products") it procures, as described in Chapter 1. Various necessary requirements concerning functions and properties are included in the normal requirements encompassed in trust requirements.

Trust-related requirements encompassed in trust requirements are those that concern the degree of certainty of supplying the product functions and properties needed by the acquiring organization. For example, if the product is a cryptographic module, the international standard *ISO/IEC 19790: 2012 Security techniques — Security requirements for cryptographic modules* can be cited as a technical requirement. Requirements that seek

assurance that the technical requirements stipulated by this standard are properly designed and implemented are trust-related requirements.

Aside from technical requirements, it is important for manufacturing operations to comply with management system standards for the product manufacturing and operating method, equipment, and personnel, etc., as shown by the analysis results for the incident cases in White Paper - Report One. Examples of management system standards are *ISO/IEC 27001: 2013 Security techniques — Information security management systems* — Requirements in the field of security, and ISO 9000 Quality management systems in the field of quality control. Requirements that seek assurance of manufacturing according to such management system standards are also trust-related requirements.

The examples given above are all international standards, but in some cases, industry standards are used as requirements. In addition, in some instances, requirements are presented as nonpublic arrangements appended to agreements between the acquiring and supplying organizations, rather than public standards information such as international and industry standards.

2.2. Return of Evidence of Supplying Organizations

The supplying organization manufactures products that meet the trust requirements of the acquiring organization. The supplying organization further returns evidence that the products, etc., were manufactured to meet the trust requirements. This section describes the processes executed by the supplying organization to perform manufacturing and returning evidence, as per Figure 2.

The first process is extraction of the product requirements (1. in Fig. 2). If the products are manufactured to order, the supplying organization prepares the product requirements in accordance with the trust requirements of the acquiring organization in 2.1. If the products are off-the-shelf or consumer products, the supplying organization has product specifications as the product manufacturer. Based on the product specifications or trust requirements of the acquiring organization, the requirements definitions for the product are prepared.

The second process is analysis of the requirements (2. in Fig. 2). To manufacture the products in accordance with the requirements in the requirements definitions, the supplying organization prepares operating procedures that detail what is processed, how it is processed, to what degree, and by whom or what it is processed, to a level that can be implemented. The supplying organization further decides what to measure and what should be preserved as the evidence data that manufacturing was performed in accordance with the operating procedures.

The third process is agreement on the operating procedures (3. in Fig. 2). The supplying organization engages in discussions with the acquiring organization to confirm that the contents of the prepared operating procedures satisfy the trust requirements of the acquiring organization and reaches agreement on the contents of the operating procedures.

The fourth process is the manufacturing and inspection of products (4. in Fig. 2). Manufacturing and inspection personnel manufacture and inspect the products in accordance with the operating procedures and preserve evidence of it. The supplying organization ships the products to the acquiring organization and returns evidence.

In some cases, the supplying organization may limit the evidence that can be disclosed to the acquiring organization among preserved evidence data, taking into account its own business constraints. For example, if the operating procedures themselves constitute business secrets or know-how that is specific to the organization, then it cannot disclose evidence data that reveal the operating procedures. The supplying organization must reach prior agreement with the acquiring organization regarding the suitability of the evidence data to disclose in the above process of reaching agreement on the operating procedures.

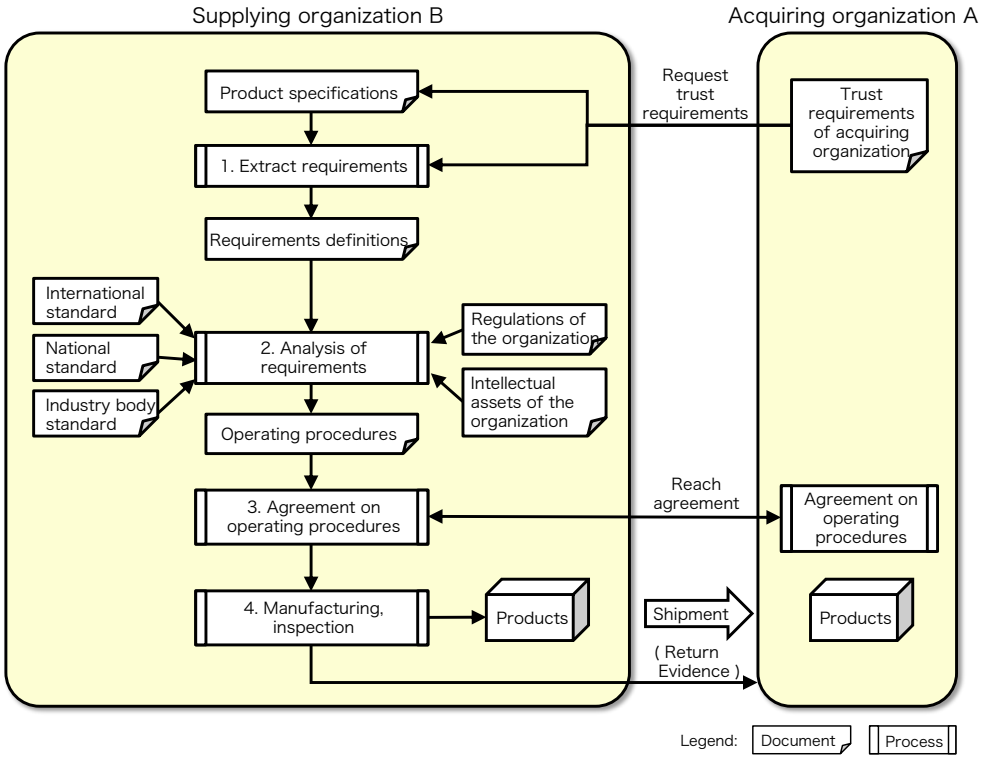

Figure 2. Analysis of Requirements of Supplying Organizations

2.3. Trust Building in the Entire Supply Chain

Figure 1 shows how, for example, an end product manufactured by organization A consists of components and products supplied by organizations B through F. As described in 1., trust between organizations is constructed by each organization presenting trust and trust requirements in the ordering and delivery of components and products. Constructing this relationship in the entire supply chain constructs trust in the entire supply chain. This shows that by shifting the perspective from organizations to products and components, the trust of an end product is achieved by the trust of all components that comprise the product. Constructing trust in the entire supply chain is nothing less than holding evidence as proof of the overall trust of the components and products that comprise the end product in the entire supply chain.

Conventionally, even if the trust of the end product were confirmed, the trust of the components and products that comprise the end product could only be inferred. However, if trust is constructed in the entire supply chain as described in 1., it is possible to arrive at evidence of the trust of the components and products that comprise the end product. Specifically, using the example in Figure 1, organization B not only presents evidence to organization A, but also is presented with evidence from organization C, so that it is possible to create an association between the two pieces of evidence. By applying this to the entire supply chain, it is possible to arrive at overall evidence for the components and products that comprise the end product.

3. Technical Process for Trust Building

This chapter describes the technical process for trust creation implemented to construct trust between organizations that deliver and receive products and services. In the following explanation, the business process that relates to design through procurement, manufacturing and inspection, distribution, operation, and maintenance implemented by an organization to realize the supplying products, etc., is referred to as the value creation process (VCP) [2].

Trust building is realized through steps (1) to (4) below. Each step is explained in accordance with Figure 3.

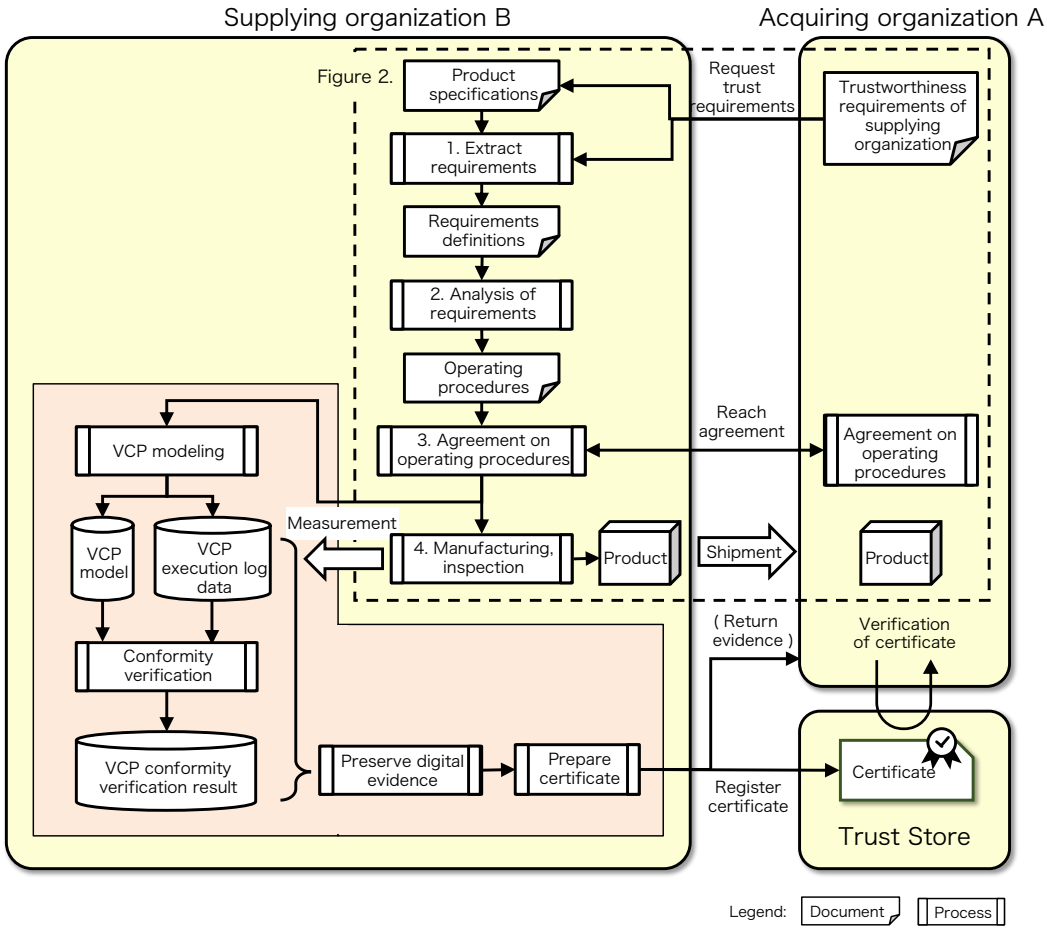

Figure 3. Technology Process for Trust Building

(1) VCP modeling: Design a proper VCP and prepare a VCP model.

- Supplying organization B analyzes the trust requirements contained in the requirements definitions and prepares a VCP model. Using a process model description language, the VCP model describes the correct operating procedures to manufacture products that meet the trust-related requirements. The VCP model is a reference model for verification of cyberspace IT systems to determine if business for physical spaces (VCP) is being implemented properly.
- The VCP model is prepared by analyzing the target business from the following perspectives: the business implementers (people, organizations), raw materials (things), standards (data), procedures (procedures), and facilities (systems). This is because business is an activity wherein organizations and people realize products and services in accordance with business procedures using systems that encompass things and data [2].
- The decision of the evidence data that people and things are properly executing the

business was described in 2.2. Furthermore, the supplying organization must decide on the measurement method for the evidence data. For example, data regarding the conduct of people in business processes can be obtained by capturing video footage of the worksite. In addition, the use of things such as tools, etc., in accordance with the work rules can be judged through data measurement using the IoT device function of things (for example, tightening torque data for torque wrenches).

(2) VCP conformity verification: The supplying organization, as shown below, verifies whether its own VCP execution status conforms with the VCP model.

- The evidence data are measured at the manufacturing site and collected as the VCP execution log data. The VCP execution log data are the basic data for verifying that the VCP is being executed according to the work rules in operating procedures.
- The VCP execution log data are compared with the VCP model from (1) to verify that the VCP execution status conforms with the VCP model. This result is called the "VCP conformity verification result."

(3) Preservation of digital evidence: The supplying organization, as indicated below, prepares the evidence using the VCP conformity verification result.

- Using the VCP model and VCP execution log data used for conformity verification in (2) and the VCP conformity verification result, prepare the digital evidence that the VCP conformity verification was performed.
- Typically, the supplying organization does not disclose the digital evidence to third parties. However, if a dispute, etc., arises due to an incident involving trust, it is anticipated that the digital evidence would be disclosed in accordance with the request of a third party such as an appropriate institution, etc., and used as evidence of the conformity of the executed business.

(4) Preparation of certificate: Use the digital evidence to prepare certificates in a standard format.

- The supplying organization, as shown in Figure 3, uses the VCP digital evidence to prepare a certificate in a standard format. The prepared certificates are stored in a certificate trust store that can be read and written to according to the authorities of the organization participating in the supply chain. Lastly, the supplying organization returns the certificate as evidence that the business was executed in conformance with the trust requirements of the acquiring organization. The acquiring organization verifies the certificates to verify whether the delivered products, etc., conform with its own trust requirements. The certificate verification by the acquiring organization completes the cycle for forming trust between organizations, which began with the

acquiring organization presenting its trust requirements.

- There are two possible organizational mechanisms for preparing a certificate with trust. Figure 3 shows the method whereby the supplying organization prepares the certificate. This method requires trust based on the assumption that the acquiring organization recognizes beforehand that the supplying organization has constructed a system for verifying VCP conformity, as shown in *3. Technical Process for Trust Building*. Under this assumption, the acquiring organization trusts the certificate prepared by the supplying organization and verifies the conformity of the products, etc. This method is a mechanism for the supplying organization to perform first-party authentication of the conformity of its own products, etc.
- As a separate organizational mechanism for preparing certificates with trust is the method whereby a third-party organization that can be trusted (trusted third party [TTP]; not shown in Figures 3 and 4) prepares the certificate. In this case, the aforementioned assumption of trust in the supplying organization must be substituted with the assumption of trust in the TTP. Under this assumption, the acquiring organization trusts the certificate generated by the TTP so that the conformity of the products, etc., is verifiable. This method is a mechanism for third-party authentication of the trust of the products, etc., of the supplying organization by the TTP. The TTP implements the conformity verification using the digital evidence and prepares the certificate. Accordingly, the supplying organization must disclose the digital evidence to the TTP.

4. Technology Process for Trust Chain Building

This chapter explains the technology process for trust chain building implemented by each organization involved in the supply chain to form the trust of products and services in the entire supply chain. Trust chain building is realized through steps (1) and (2) below. Each step is described in accordance with Figure 4.

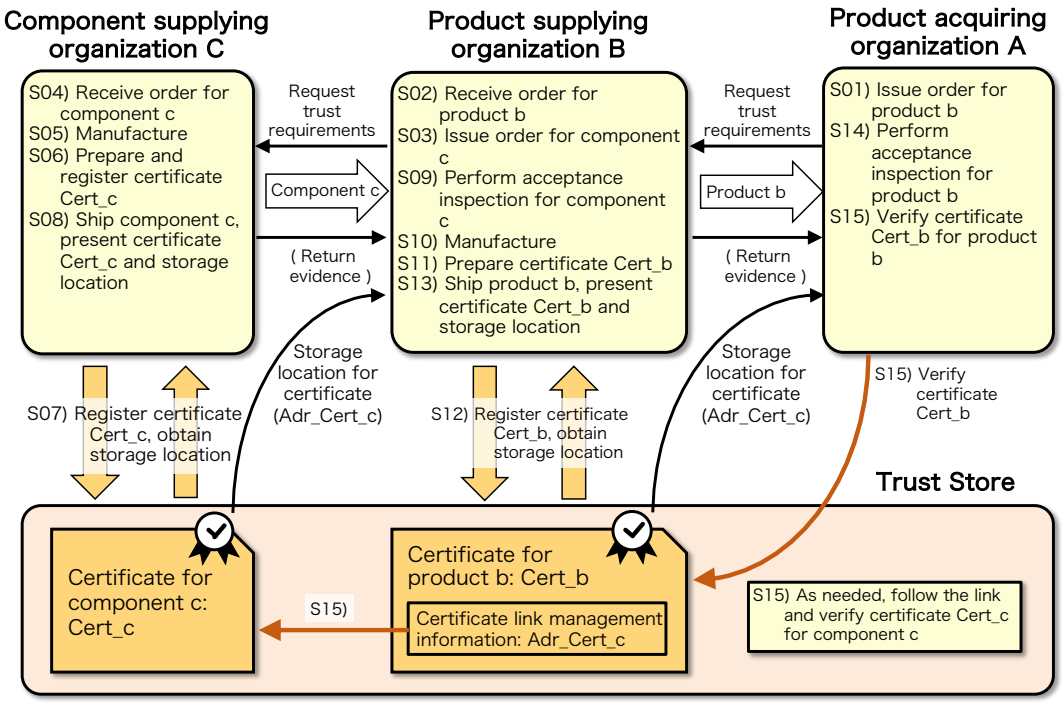

Figure 4. Technology Process for Trustworthy Chain Construction

(1) Inter-certificate chaining: Relating trust links in the supply chain to certificate links

- The trust between a pair of organizations involved in issuing and receiving orders is not sufficient to construct the trust of an entire supply chain. Consequently, it is necessary to build a trust chain, as described in 2.3. The following describes the mechanism for managing the certificate links, in accordance with Figure 4, which shows the steps for linking certificates between three parties comprising product acquiring organization A, product supplying organization B, and component supplying organization C, as indicated in sequences S01 through S15.

- Product supplying organization B registers the prepared certificate Cert_b in the trust store (S12) and presents it to product acquiring organization A (S13). The trust store is a storehouse of certificates that can be read and written to in accordance with the individual authorities of the organizations involved in the supply chain. Product supplying organization B, when returning evidence, returns storage location Adr_Cert_b in the certificate trust store to product acquiring organization A. All supplying organizations involved in the supply chain register certificates in the trust store and return the certificate storage location to acquiring organizations.

- When product supplying organization B prepares certificate Cert_b for its own product b (S11), storage location Adr_Cert_c for certificate Cert_c of component c that was used is stored in certificate Cert_b as certificate link management data. The process

expresses the trust link between organization B and organization C on the supply chain as the link between certificates Cert_b and Cert_c in the trust store. When product supplying organization B performs the acceptance inspection for component c (S09), component supplier organization C presents location position Adr_Cert_c so that it can be stored in the above certificate Cert_b.

(2) Verification of trust chain: The acquiring organization verifies the product certificates.

- The abovementioned mechanism for linking certificates makes it possible for the acquiring organization to verify whether the organizations involved in manufacturing implemented the manufacturing in conformance with the respective trust requirements across the entire supply chain of the products.
- This mechanism makes it possible to verify the trust of intermediate components, etc., even in the intermediary stages of manufacturing in the supply chain, in addition to verifying the trust of the end products or services.

It should be noted that the contents described in 3 and 4 are universally applicable, regardless of whether the products are made-to-order.

5. Benefits of Trust Building Technology and Issues

This chapter describes the benefits and issues when applying trust building technology to actual incident cases. Table 1 shows describes and presents the characteristics of six of the incident cases introduced in White Paper - Report One.

Table 1. Case Studies of Incidents That Damaged Trust

No.	Case	Description	Relation to Rules	Main Actor	Fraud/ Negligence
1	Excessive drinking by airplane copilot before boarding flight [3]	Inebriated pilot evades alcohol detection test and operates aircraft	Violation	Employee acting alone	Fraud
2	Fraud in inspections for industrial rubber products [4]	Inspector neglects to perform some of his/her inspection duties	Violation	Employee acting alone	Fraud
3	Suspicions of backdoor tool installed on network routers [5]	Third party opens product while it is in transit with outsourcing shipping company and installs malfeasant tool	Violation	Third party	Fraud (attack)
4	Noncompliant products labeled Halal-certified [6]	Insufficient review during manufacturing process design leads to manufacturing of non-Halal products	Defect	Internal organization	Negligence
5	Fraud related to exhaust gas emissions for diesel vehicles [7]	Automaker manufactures defective vehicles through malfeasant design, manufacturing, and inspection at the organizational level	Violation	Internal organization	Fraud

6	Suspicions of information-leaking chips embedded in server motherboards [8]	Malfeasant motherboards containing information-leaking chips manufactured by outsourcing motherboard manufacturer at the organizational level	Violation	Outsourcing organization	Fraud (attack)

5.1. Benefits of Trust Building Technology

Cases No. 1 and No. 2 in Table 1 are incident cases caused by rules violation. The incident causes were created by the intentional fraud of a company employee acting alone. In these cases, the things that need to be stipulated in the management work rules of the operating procedures are simple and obvious, for which our trustworthiness construction technology is highly effective as a countermeasure. The company can combine technical means and business process improvements to prevent fraud in these cases. Specifically, for Case No. 1, technical means such as alcohol detectors, etc., can be combined with improvements to the boarding roll call business process to prevent a person who has been drinking from wrongly evading an alcohol test. For Case No. 2, technical means such as surveillance cameras and inspection device monitoring., etc., can be combined with improvements to the inspection task process to prevent an inspector from intentionally neglecting inspection tasks.

In Case No. 3, a third party opened the product packaging while in transit with the outsourcing shipping company and installed a malfeasant tool. This case involved an intentional attack by a third party, and is an example of exploiting a vulnerability in a business process. Our trustworthiness construction technology is an effective countermeasure for this attack case. The outsourcer manufacturer can request the outsourcing shipping company to prevent an attack by third-party malfeasant access to products by incorporating into the transportation business process technical means such as surveillance cameras and devices to prevent packages from being opened. The outsourcing company presents a certificate that indicates the proper implementation of the outsourcing business to the outsourcer, enabling the verification of malfeasant behavior during distribution.

In summary, trust building technology can be said to have a certain degree of effectiveness in preventing fraud.

5.2. Issues with Trust Building Technology

Unlike the rules violation cases described in 5.1, the incident cause of Case No. 4 in Table 1 was a defect in the regulations. The incident cause was created by the organization that created the work rules and operation procedures, and by negligent conduct in the form of analysis oversights or errors in the operating procedures. In this case, since the Halal

certification is not easy to understand, there could have been oversights in the manufacturing processes and operational rules so that products not conforming with Halal certification were manufactured. The food manufacturer must have carefully examined the manufacturing work process and combined it with technical means in an attempt to realize manufacturing processes that conformed with Halal certification. Typically, if there is an insufficient understanding of the certification requirements, it is difficult to prepare proper business processes. It also becomes difficult to construct systems that verify the conformity of VCP properly.

Unlike Cases No. 1 through No. 4, the incident cause of Case No. 5 was created by organizational fraud by the company. The organization itself cannot be expected to prevent such organizational and intentional fraud. Our trust building technology is not an effective countermeasure when the technology is intentionally used to generate false evidence. Organizational fraud of this kind probably cannot be prevented except by having an authoritative third-party institution strictly implement inspections to verify the conformity with the legal regulations for the product.

The incident cause of Case No. 6 was created by organizational and intentional fraud by the outsourcing manufacturer. As in Case No. 5, the organization itself cannot be expected to prevent such organizational and intentional fraud. Accordingly, our trust building technology is not an effective countermeasure for malfeasance of this kind.

In summary, the construction of a system for VCP conformity verification is limited by the knowledge of the constructing organization, and it is difficult to counteract fraud that intentionally attempts to embed evidence that differs from the facts. These limitations in applicability are a future issue.

6. Relation to the Conventional Approach to Trust

Trust building technology is technology for build trust in supply chains. While there is "trust" and "trustworthiness," the former is a broader concept and closer to what is discussed in this paper. Trust and trustworthiness have been considered for more than 20 years in the field of IT.

[Quotation 1] National Research Council. "Trust in Cyberspace". 1999. [9]

> The degree of confidence one has that the system performs as expected in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks.

Additionally, an IoT-related industry body from recent years defines "trustworthiness" as follows.

[Quotation 2] Industrial Internet Consortium. “Vocabulary”. V2.1, August 2018. [10]

> Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks.

The common core description from these two quotations is “Degree of confidence one has that the system performs as expected.” This is nearly the same as in *Figure 1. Basic Approach of Trust Building*.

Figure 1 shows the building of trust of an acquiring organization by the supplying organization presenting the acquiring organization with evidence that the system performs as per the requirements of the acquiring organization. In this diagram, if “requirements” is substituted with “expectations” and “present evidence” with “grounds or evidence,” the trust building diagram can be seen as enhancing the “degree of confidence” mentioned in the two quotations.

[Quotation 3] NIST. “Framework for Cyber-Physical Systems”. Release 1.0., May 2016. [11]

> Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but not limited to, safety, security, privacy, reliability and resilience.

In this quotation, if we think of “requirements” as “design (requirements)” and “present evidence” as a “demonstrable likelihood that the system performs,” it is nearly the same as the diagram for trust building.

As indicated above, the approach to trust building in this report is nearly the same as the conventional approach to trust and trustworthiness.

7. Summary

Lastly, this chapter describes what added-value trust building technology creates and how it contributes to a cyber-physical age.

In addition to establishing trust in supply chains, trust building technology is expected to enhance the efficiency of overall business processes, bringing about added value by reducing costs. As we described at the start of this paper, modern supply chains continue to increase in complexity and are becoming more globalized. By using CPS to manage real-world manufacturing and operational work, it is first of all possible to reduce business management costs at manufacturing sites. Furthermore, even if an incident that damages the trust of products or services were to arise, downtime in production processes and the

cost of the incident response can be minimized by rapidly investigating the incident causes and simplifying the drafting of countermeasures.

The ultimate contribution of trust building technology to a cyber-physical age is the realization of a world that is friendlier and more livable for people. Trust building technology establishes the trust of products and services. The aforementioned IIC defines "trustworthiness" as the "degree of confidence one has that the system performs as expected with five characteristics—safety, security, privacy, reliability, and resilience—in the face of environmental disturbances, human errors, system faults, and attacks." When products and services that support our lives continue to behave as expected with respect to these five characteristics in the face of various disturbances and attacks as mentioned by the IIC, it is certain to support the realization of a world that is friendlier and more livable for people.

8. Acknowledgments

This research is partly conducted by the Cross-ministerial Strategic Innovation Promotion Program (SIP): Cyber-Physical Security for an IoT Society (management entity: New Energy and Industrial Technology Development Organization [NEDO]) led by the Cabinet Office, Government of Japan.

References

[1] National Institute of Advanced Industrial Science and Technology. "Building Trust in Supply Chains, Report One: Analysis of Incidents that Damage Trust and Basic Approach to Trust Building." October 2019. https://www.cpsec.aist.go.jp/achievements/CPSEC-WP-2019001.pdf

[2] Ministry of Economy, Trade and Industry. "Cyber/Physical Security Framework." Version 1.0, April 2019. https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

[3] BBC News Japan. "JAL Hands Disciplinary Dismissal Against Co-Pilot Who Boarded Flight Inebriated and Was Jailed in the U.K." November 30, 2018. https://www.bbc.com/japanese/46395567

[4] Toyo Tire Corporation. "Announcement of Investigation Into Causes of Industrial Rubber Products (Sheet Ring) Problem and Recurrence Prevention Measures." March 24, 2017. https://www.toyotires.co.jp/uploads/2017/03/20170324.pdf

[5] ITmedia News. "Revelations from New Book Related to Snowden: NSA Planted Backdoor Tools in Cisco Products for Export." May 15, 2011.

https://www.itmedia.co.jp/news/articles/1405/15/news096.html

[6] Ajinomoto Co., Inc. “Announcement Concerning Halal Issue in Indonesia.” January 6, 2001. https://www.ajinomoto.com/jp/presscenter/press/detail/2001_01_06.html

[7] United States Environmental Protection Agency. “Notice of Violation”. 2015.9.15 https://www.epa.gov/sites/production/files/2015-10/documents/vw-nov-caa-09-18-15.pdf

[8] Bloomberg Business week. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”. 2018.10.4 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[9] National Research Council. “Trust in Cyberspace”. The National Academies Press, 1999.

[10] Industrial Internet Consortium. “The Industrial Internet of Things Volume G8: Vocabulary”. V2.1, August 2018. https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf

[11] NIST. “Framework for Cyber-Physical Systems”. Release 1.0, May 2016. https://www.itmedia.co.jp/news/articles/1906/10/news049.html