CPSEC-WP-2020001

Building Trust in Supply Chains

Report One:

Analysis of Incidents that Damage Trust and Basic Approach to Trust Building

October 2019
Cyber Physical Security Research Center
National Institute of Advanced Industrial Science and Technology (AIST)

Abstract

Various types of incidents (including security incidents) that damage trust in products and services in supply chains have been occurring. This report introduces a variety of cases and analyzes the causes of those incidents. It is shown that the incidents in these case studies span the full lifecycle from manufacturing to operation and that the causes of these incidents can be broadly divided into defects in or violations of work rules established to follow at each stage of the lifecycle. Trust can be built up across the entire supply chain if each company in the supply chain endeavors to prevent defects in or violations of work rules and reduce the occurrence of incidents. Today, supply chains are making a major shift to cyber-physical space, so opportunities for exploiting the advantages of cyber-physical space and building trust are appearing.

1. Introduction

Our daily life would be impossible without the use of products and services produced by others. We purchase these products and services at a fair price, which also represents our expectations of those products and services. In other words, the more we pay the more we expect. However, that is not to say that there are no conditions attached to low-priced products and services. For example, it is implicitly understood that food products will not harm our health regardless of how inexpensive they may be. Consumer lives are predicated on this implicit trustworthy relationship. Nevertheless, there have been a number of cases in recent years that suggest that such a trustworthy relationship no longer exists.

It is the background of such change that supply chains are becoming increasingly complex and global in scale. The more the number of companies and people involved in supply

chains becomes the more diverse the attitudes on trust and on responsibility for upholding trust become. It depends on the product whether it is completely examined during the acceptance period or not that the product satisfies requirements and specifications so as to be worthy of trust. Products are used even if they are completely examined sufficiently to be trusted. However, the accumulation of such uses may lead to a breakdown in trust. Additionally, because a considerable amount of information exchanged in a supply chain shifts to the cyberspace, information tampering or leaks in the cyberspace can damage the trust of the supply chain. The increasing number and diversification of attack methods targeting IT devices that configure the cyberspace is expanding the attack surface (sum total of all targets of attacks), and as a result, opportunities of damaging trust in supply chains are increasing. On the other hand, incidents and problems are becoming all the more apparent as the corporate governance comes to place more importance on transparency. However, as long as uncertain trust is not rebuilt, it will be impossible to form supply chains in the cyber-physical space that merges the cyberspace and the actual physical space. Here, problem analysis should be performed before consideration of the rebuilding of trust. Let's take a look at several cases of problems on trust in supply chains, starting with those related to IT.

2. Case studies: incidents and analyses

Chip embedded on server motherboard for attacking [1]

Incident overview:

Time	October 2018
Location	United States (location of occurrence)
Business/field	IT
Damaged trust	Confidential information protected by products

A news agency reported that a certain country tampered with the servers of 30 companies in the United States. According to this report, a top global supplier of server motherboards had consigned the manufacture of motherboards to a contractor in that country, and those motherboards had been embedded with a microchip for attack purposes during the manufacturing process by a party related to that country's military. This opened up a backdoor to the OS enabling the leaking of confidential information. Two companies from among those whose servers the report claimed to have been altered denied that this happened.

Case analysis:

Process	Manufacturing
Rules	Violated

This case concerns the altering of a product. The embedding of a microchip for attack purposes deviated from work rules and was an intentional act by a power beyond the control of those rules, so it could not be avoided within the manufacturing company. An organization that purchased this server computer would think that the product would never leak confidential information of the organization. This case shows that such an assumption does not hold. In order to preventing this incident from occurring, should the purchasing organization open the housing of individual purchased products and check whether such an attack chip was actually embedded? It is the product manufacturing company that should to show that there are no problems with the product so that a purchaser can trust and use it. Furthermore, even if this news report were false, the trust of this server manufacturing company would still be severely damaged. It is desirable that a company be able to counter such trust issues.

Suspicion about addition of backdoor tools to routers [2]

Incident overview:

Time	April 2015
Location	Several countries around the world (where incident may have occurred)
Business/field	IT
Damaged trust	Confidential information protected by products

According to a book, a former employee of a certain national agency accused of the national agency of tampering of network equipment. It was written that this national agency intercepted routers for export along their distribution route, embedded them with backdoor tools, and repackaged and returned them to distribution. It is said that these tools made it possible to monitor traffic processed by those network routers and leak information to that national agency. The company manufacturing these routers issued a comment that it did not work with the government to intentionally weaken its products.

Case analysis:

Process	Distribution
Rules	Defective

This is also a case of product alteration. A supply chain cannot be completely trusted

unless the distribution route in addition to the participating manufacturing companies cannot be trusted. In other words, the trust of the entire supply chain including the distribution route should be questioned. Although mechanisms are available for checking whether a product has been unpacked during the time from shipment to arrival along the distribution route, such countermeasures were insufficient in this case.

Chip manufacturing line halted by WannaCry [3]

Incident overview:

Time	August 2018
Location	Asia
Business/field	Semiconductor manufacturing
Damaged trust	Information security measures of a company

A leading global company announced that the computer systems at several of its factories were infected with the WannaCry ransomware affecting its manufacturing facilities. The detail was that software contaminated with this malware was installed without a virus scan resulting in damage to more than 10,000 Windows computers connected to the in-house network. While the ultimate problem here was a malware infection, the fundamental cause of the incident was an operational mistake in the company. The company estimated that 2018 third quarter revenue would fall by about three percent due to shipment delays and countermeasure expenses.

Case analysis:

Process	Manufacturing
Rules	Violated

In this case, business continuity was impaired. While it could be viewed as just an internal problem of a company, it might indirectly delay activities of other companies purchasing the manufactured products due to shipment delays. If similar incidents occur often, the productivity of society on the whole will drop. Under such conditions, it is not sufficient to question just the trust of the product itself but also the trust of business partners' processes more than ever.

Trust has been viewed as an important concept in the field of security. However, it is not something that can be achieved simply by ensuring security. In supply chains, incidents damaging not only trust related to security but also trust related to other aspects have

been reported. In the following, let's take a look at several cases on trust related to safety.

Delivery of Shinkansen (bullet) train bogie frames out of specifications [4]

Incident overview:

Time	February 2018
Location	Japan
Business/field	Manufacturing of rolling stock
Damaged trust	Safety of product based on conformance to specifications

The company manufacturing the bogie frames for the N700 series Shinkansen (bullet) train announced the occurrence of a crack in a bogie frame due to defects during the manufacturing process. It is inferred that the work instruction card used in the manufacturing process of a bogie frame component was less than thorough, that a fissure arose due to various factors including the welding work, and that the fissure eventually developed into the crack. As specific causes, it is cited that the work instruction card was somewhat vague, that responsibility for guiding and training supplementary work fell on onsite workers, and that there were no records of carrying out and checking that work. In addition, checking of plate thickness at the location where the crack occurred was not included as a quality management or inspection item. Countermeasures proposed to prevent another occurrence of this problem include the establishment of a mechanism to prevent the shipping of any product not conforming to design drawings, checking of process of works, auditing of documentation including work instruction cards, and reconstructing of worker training.

Case analysis:

Process	Manufacturing
Rules	Defective

In this case, while defects in work rules could be compensated for based on onsite judgments, the essence of this problem is that proper judgments could not be made. The quality of onsite judgments depends on that site. Although work rules exist to eliminate such dependency, the end result here was to negate the meaning of such rules.

Fraudulent inspections of industrial rubber product [5]

Incident overview:

Time	March 2017
Location	Japan
Business/field	Manufacturing of industrial components
Damaged trust	Inspections conformant to standards, safety of product conformant to specifications

In the inspection process of an industrial rubber product (a sheet ring for seating a valve in a pipeline such as used in an oil tanker), it was originally agreed between the manufacturing company and its customer that a sampling inspection for measuring dimensions and hardness would be conducted one for every 5 items. Nevertheless, the sampling inspection was performed only one for every 10 or 20 items. According to a news release issued by the company, this pattern was caused by several problems, such as individual negligence on the part of inspectors, deterioration of the normative consciousness that fraud is unacceptable, insufficient management and supervision, and an inspection environment in which monitoring is difficult. The company presented measures to prevent recurrence, such as automating the inspection process and introducing video monitoring cameras as well as raising consciousness and improving corporate culture. In other words, these measures included both human-related and technology-related ones.

Case analysis:

Process	Testing
Rules	Violated

In this case, though rules existed, inspections were not correctly performed due to individual negligence. Controlling variation in individual consciousness regarding work norms is the responsibility of the company, and will heighten the trust of not only the product but also of the company. Here, raising employee consciousness of work norms requires thorough management and supervision. However, there are limits to what can be achieved if relying only on human activities.

Fraudulent inspection of emission gases in diesel vehicles [6]

Incident overview:

Time	September 2015
Location	Germany
Business/field	Automobile manufacturing

Damaged trust	Product conformant to environmental standards, inspections conformant to standards

The United States Environmental Protection Agency (EPA) issued a notice of violation of the Clean Air Act to a German automaker stating that it had installed software to bypass EPA emission standards in certain model of its vehicles. On receiving this notification, the automaker, amid clarification that the results of bench tests of emissions with that diesel engine software differed greatly from measurements taken under actual road conditions, announced four days later that the problem affected 11,000,000 vehicles worldwide. The state of California subsequently determined that this German automaker had installed illegal software in its vehicles to sense whether a vehicle was being inspected or being driven under actual road conditions so as to meet emission standards only during inspections, and that such a vehicle would actually emit up to 40 times more pollutants than that allowed by emission standards.

Case analysis:

Process	Design, manufacturing, testing
Rules	Violated

This is a case of a manufacturer designing a fraudulent function and installing it in a product to circumvent established regulations. It is technically difficult for regulatory agencies to completely clamp down on such complex and clever attempts at defeating regulations. This would require that regulatory agencies, consumers, etc. monitor the whole product/service lifecycle observing regulations, from design to operation, which is quite unrealistic.

The manufacturing industry is intimately associated with our daily lives in terms of food, clothing, housing, and other needs, which has the potential of creating problems that can involve general consumers. Let's take a look at several such cases.

Halal non-conformity in renewing halal certification of a food product [7]

Incident overview:

Time	September 2000
Location	Indonesia
Business/field	Food manufacturing
Damaged trust	Food product conformant to religious laws

A Japanese food-products company was informed on renewing their Indonesia halal certificate that they were using an enzyme originating from pigs in its manufacturing process for seasoning. The company used no substances at all that would violate halal in its main or auxiliary ingredients. The swine-derived enzyme is used as part of the medium for preserving a fermenter used in manufacturing process, and is regarded as a catalyst. It was also a product procured from an external source. The National Agency of Drug and Food Control of Indonesia issued a statement declaring that swine-derived substances were not included in the final product, but the Halal Fatwa Committee nevertheless judged the substance in question to be unsuitable from a halal perspective. As a result, The National Agency of Drug and Food Control issued a product recall directive, which the food-products company followed. In November of that year, the company switched to an enzyme extracted from soybeans and received an opinion from the Halal Fatwa Committee that this enzyme posed no problem.

Case analysis:

Process	Design
Rules	Defective

In this case, it appears that the in-house rules for halal certification lacked completeness. When a company goes global, it must adapt to the culture and values of the countries targeted for expansion. Still problems that could not be envisioned in the corporate activities in its own country may arise. A company that provides products or services to consumers lies at the end of an increasingly complex and long supply chain, and therefore bears the risk of taking primary responsibility for an incident originating in any raw material or component provided along the supply chain. In this case, the food-products company could probably not be held morally responsible, but it took responsibility from a business perspective in recalling the product. To prevent such confusion from occurring in the first place, the food-products company should perhaps have conducted a strict onsite inspection to the company supplying the enzyme, similar to that conducted by The National Agency when applying for a halal certificate.

Excessive drinking by airplane copilot before joining crew [8], [9]

Incident overview:

Time	November 2018, August 2003
Location	England, Japan
Business/field	Passenger transport

Damaged trust	Passenger safety

The copilot of an airplane flight was arrested after a breathalyzer test detected more than nine times the legal alcohol limit for a country 50 minutes before joining his crew for departure. He was given a prison sentence of 10 months and received a punitive dismissal by the airline company the next day. Before his arrest, he had fraudulently circumvented an in-house breathalyzer test. It appears that he had kept away from two chief pilots with whom he was scheduled to fly, preventing them from noticing his behavior. Six months before the incident, the airline company had announced that it would be introducing new alcohol breathalyzer equipment at overseas airports.

A similar incident occurred in relation to highway buses in Japan. A bus driver scheduled for an upcoming trip went to bed after drinking from late night until early the next morning and answered a roll call by the auxiliary dispatcher at around 7:00 that morning. The auxiliary dispatcher, though suspecting that the driver was hungover, nevertheless allowed him to board the bus so as not to get in trouble of arranging for a substitute driver. The police held the company responsible and sent the case to prosecutors.

Case analysis:

Process	Operation
Rules	Violation

In either of these cases, there were rules governing the safe transport of passengers, and checks had been made as to whether the state of the crew hindered them from carrying out their duties. However, the checking mechanisms established by those companies were ineffective against the copilot's and bus driver's lack of a sense of responsibility and mental weakness. Some rules can be broken if so desired, and whether to break such a rule or not depends on the individual. To gain public trust, a company must create rules and mechanisms that not only have no holes in them but also prevent the making of holes. Here, however, a solution depending solely on the human element would be difficult.

Reverse running of computer-controlled transport system [10]

Incident overview:

Time	June 2019
Location	Japan
Business/field	Passenger transport
Damaged trust	Safe service

In this incident, a computer-controlled unmanned automated train ran in reverse slamming into a station buffer and injuring 14 passengers, some of them seriously. The cause of the accident announced by the train operating company was a circuit disconnection. Here, a break in one circuit out of more than 100 circuits had the potential of preventing an instruction for reversing the direction of movement from being transmitted at all. There was no mechanism for detecting such a disconnection, and appeared that equipment for stopping the train at the time of an abnormality was not operating due to the wiring disconnection. The operating company admitted that there was a defect in the system. An expert on train control stated, "A means of detecting a circuit disconnection should definitely have been installed."

Case analysis:

Process	Design
Rules	Defect

This case concerns a design defect of not incorporating a disconnection detection function. The operating company owning the system should probably be held responsible for the accident, but the company that designed and built the system should also be responsible at least in part. In other words, this case as well deals with the problem of trust in supply chains. As described earlier, the primary responsibility for a product or service delivered via a supply chain lies with the company at the end of the supply chain. Similarly, this case has the form of a train operating company at the end of a supply chain bearing the responsibility for an accident.

3. Analysis summary

The case studies described above show that causes of damaged trust occur in a variety of processes within the lifecycle of a product, system, or service. The following table arranges these cases by type of process.

		Case	
Process	Design	Halal non-conformity in renewing halal certification of a food product, reverse running of computer-controlled transport system	Fraudulent inspection of emission gases in diesel vehicles
	Manufacturing	Chip Embedded on server motherboard for attacking, chip manufacturing line halted by Wannacry, delivery of Shinkansen train bogie frames out of specifications	
	Testing	Fraudulent inspections of industrial rubber product	
	(distribution)	Suspicion about addition of backdoor tools to routers	
	Operation	Excessive drinking by airplane copilot before joining crew	

Furthermore, while the rules governing the execution of a process are found within the companies described in these case studies, policies for building trust will likely depend on whether the breakdown in trust originates in a rule defect or rule violation. The following table arranges the cases from this perspective.

		Case study
Rules	Defect	Suspicion about addition of backdoor tools to routers*, delivery of Shinkansen train bogie frames out of specifications, halal non-conformity in renewing halal certification of a food product, reverse running of computer-controlled transport system
	Violation	Chip embedded on server motherboard for attacking*, chip manufacturing line halted by Wannacry, fraudulent inspections of industrial rubber product, fraudulent inspection of emission gases in diesel vehicles, excessive drinking by airplane copilot before joining crew

In the above table, cases marked with an asterisk (*) describe attacks, which in some cases damage the trust of the targeted organization.

As can be seen in these case studies, the process in which the cause of an incident originates is not necessarily the same as the process in which the problem occurs. In addition, an incident will not necessarily occur in a company that made the cause. For example, in the case of reverse running of a computer-controlled transport system, the design defect originating in the company that developed the transport system appeared as

an accident in the company operating the transport system.

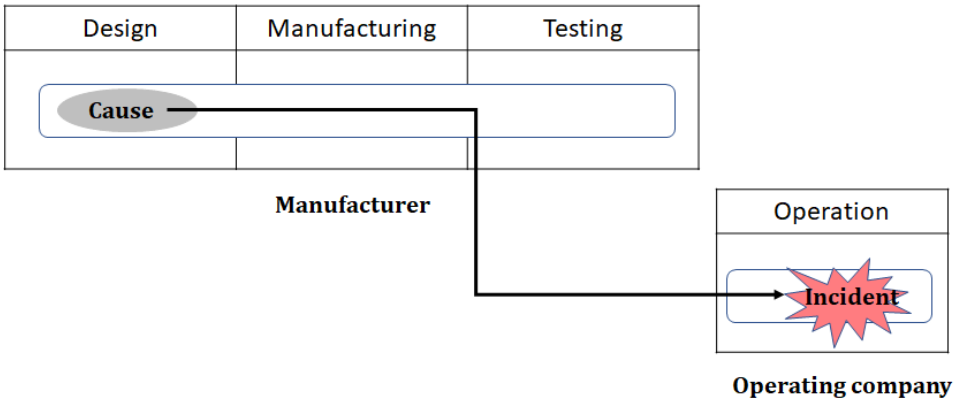

Figure 1 Example of incident cause and occurrence spanning multiple processes

Moreover, even if an incident were to occur in an organization which made the cause, care must be given to the possibility that an even bigger problem might occur at a client damaging the trust of the organization all the more. For example, the problem of fraudulent inspections of an industrial rubber product has the potential of causing a tanker accident later in the supply chain.

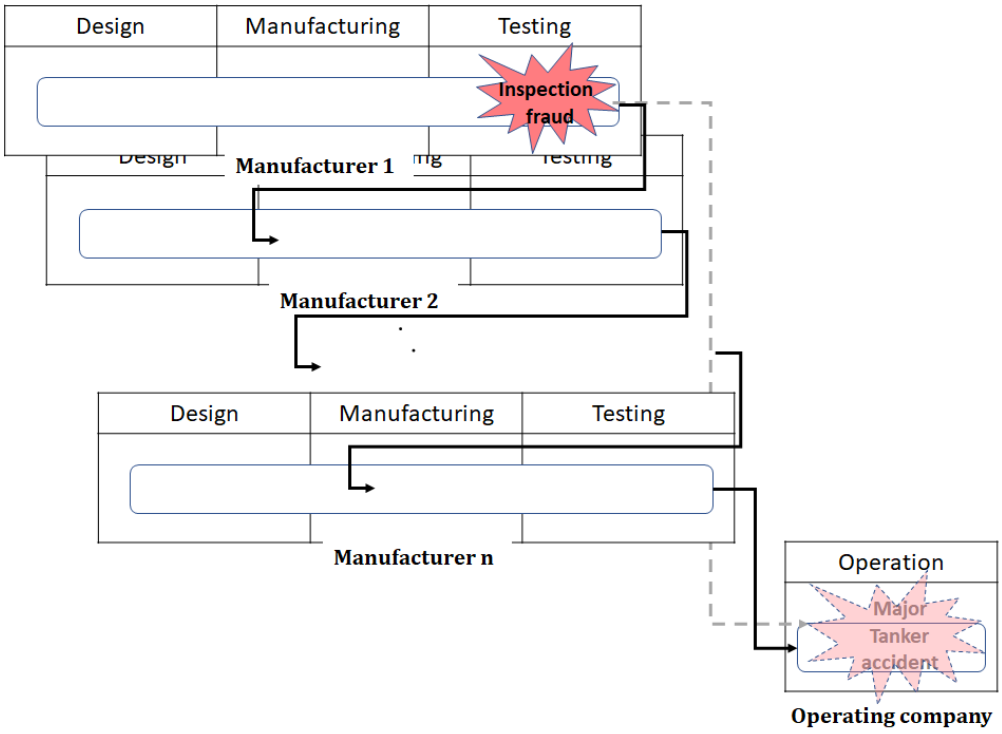

Figure 2 Example of an accident occurring via multiple companies after the cause was made earlier

4. Toward building trust in cyber-physical space

As explained above, a company on a supply chain may bear responsibility for all the companies below it on the supply chain. The closer a company gets to the endpoint of the supply chain, the greater is its responsibility and the greater is the severity of the problems it must deal with thereby magnifying business risk. Such risk can be mitigated through efforts taken along the entire supply chain—not just by the efforts of a single company. The companies making up a supply chain participate in an effort to increase the trust of the entire supply chain and mitigate risk. Specifically, trust between companies is established if the acquiring company requests clear requirements that include those related not only to functions but also to trust to the supplying company and if the supplying company returns evidence that its processes satisfy the requirements using evidence data if necessary. Connecting more companies in this way through inter-company trust can form a chain of trust along the supply chain.

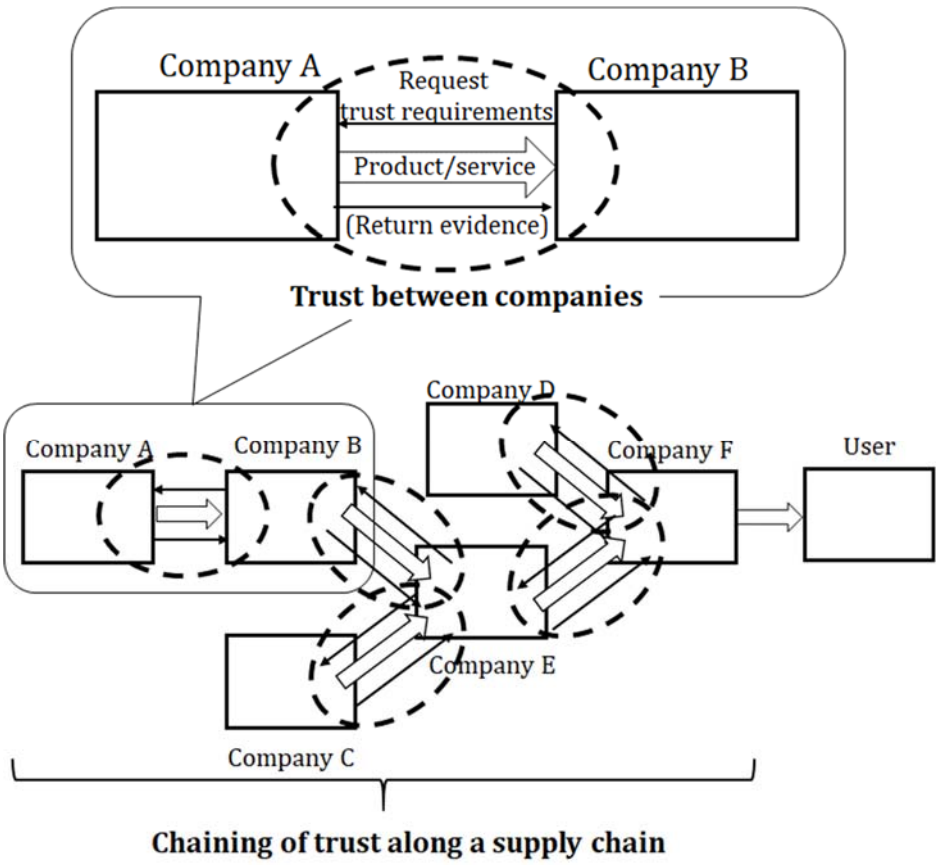

Figure 3 Chain of trust in a supply chain

Note: “Trust requirements” refers to clear requirements that include those related not only to functions but also to trust.

Trust between companies assumes that the supplying company executes its processes in conformance with its in-house rules and makes a decision how to fix a inapplicable rule when it finds it. Establishing trust between pairs of companies along the entire supply chain based on this assumption may take a certain time. For this reason, the entire chain of trust cannot be formed at one time—they can only be formed in a step-by-step manner starting with constructible sections of a supply chain. Taking into account the expansion of the attack surface in the cyber space, there should be no delay in getting started in building trust.

It may be thought that the increasing complexity of supply chains will increase the cost of chaining of trust and even make it difficult to achieve trusted chains. Nevertheless, the cyber-physical space that is now emerging incorporates supply chains and may even be an ideal space for building trust. In the cyber-physical space, the state of the physical space can be collected and digitized by appropriate sensors in each process and transferred to the cyber space. Such processing may incur initial costs, but automatically migrating work heretofore performed by people to the cyber space should reduce costs over the long term. In addition, determining whether rules are being observed and recording those judgments are simple to achieve in the cyber-physical space. Moreover, if a certain rule appears to be inapplicable, the people who must make a decision on that can do so in the cyber space. Requirements and evidence necessary for chaining of trust can also be automatically collected and recorded in the cyber-physical space. These data can help build a chain of trust by being disclosed as needed within an appropriate range. A chain of trust on a supply chain built in the cyber-physical space may give birth to new forms of trust different from those in the past, which may lead to less incidents and reduce costs for all the companies on the supply chain.

5. Acknowledgments

Part of this research is being conducted under the Cyber-security for Critical Infrastructure program (Managing Agency: New Energy and Industrial Technology Development Organization (NEDO)) of the Cross-ministerial Strategic Innovation Promotion Program (SIP) promoted by the Cabinet Office, Government of Japan.

References

[1] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-u

sed-a-tiny-chip-to-infiltrate-america-s-top-companies

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

[3] https://www.vice.com/en_us/article/3ky75b/windows-malware-wannacry-new-iphone-delays

[4] https://www.khi.co.jp/news/C3180228-1_2.pdf

https://global.kawasaki.com/news_C3180228-1.pdf (in English)

[5] https://www.toyotires.co.jp/uploads/2017/03/20170324.pdf

[6] https://www.epa.gov/sites/production/files/2015-10/documents/vw-nov-caa-09-18-15.pdf

[7] https://www.ajinomoto.com/jp/presscenter/press/detail/2001_01_06.html

[8] https://www.bbc.com/japanese/46395567

[9] https://response.jp/article/2003/09/26/54177.html

[10] https://www.itmedia.co.jp/news/articles/1906/10/news049.html