NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

3rd Quarter of 2020

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary

This report is the result of survey and analysis by NTTDATA-CERT on quarterly global trends from its own perspective based on cybersecurity-related information collected in the period.

Intensifying attacks on supply chains

Multiple organizations received supply chain attacks in the third quarter. Among them, the software supply chain attack on SolarWinds attracted major public attention. With supply chain attacks becoming a serious problem, the Ministry of Economy, Trade and Industry of Japan (METI) established Supply Chain Cybersecurity Consortium (SC3) on October 30, 2020. These events indicate that supply chain attacks are receiving increasing attention.

Attackers intrude a supply chain from a site that does not take sufficient security measures. To protect a supply chain, organizations must eliminate security vulnerabilities from the entire supply chain. However, eliminating all security vulnerabilities from the entire supply chain is not easy because the entruster cannot force entrustees to take security measures, and a supply chain is huge and complex. Also, there is no complete method for efficiently establishing supply chain attack countermeasures. Therefore, efforts are necessary to find patterns of supply chain attacks and methods for protecting the entire supply chain by analyzing a number of past supply chain attacks.

Increase of double-extortion ransomware attacks

Ransomware attacks are increasing and evolving from the data-encryption type to *the double extortion type*, which steals data and demands ransom. In the background of the increase of ransomware attacks, there are recent environmental changes such as the increase of telework, which contribute to the increase of intrusion paths for attackers. According to an awareness survey by CrowdStrike, more than half of the responding organizations in Japan have experienced ransomware attacks, and about 30% among them have paid ransom.

The most effective measure against double-extortion ransomware attacks is to take protection measures before receiving an attack. However, with ever-sophisticated attack methods, it is difficult to defend against all attacks. The trend of policies for double-extortion ransomware attacks is to prohibit paying ransom because it is an act of helping crimes. An example is a recommendation made by Office of Foreign Assets Control of the U.S. Treasury in October 2020. In the case of a double-extortion ransomware attack, it is important to have strong determination not to yield to the threat of the criminal.

Data breach attributable to defective setting of Salesforce

From the third quarter of 2020, there have been a number of data breach incidents attributable to defective setting of the Salesforce platform. An organization that uses the Salesforce platform should check the privileges settings of guest user access control according to the guideline of Salesforce.com.

According to the policy of the shared responsibility model, the cloud service customer is responsible for such data breach incidents caused by defective settings. However, insufficient support by Salesforce.com, a cloud service provider, is considered one of the causes of these incidents. For secure use of cloud service services, cloud service providers should provide support to cloud service customers to prevent defective settings, and cloud service customers should well understand cloud service specifications before using them.

Outlook

Incidents that require actions by cloud service providers, such as the Salesforce incident, will probably continue because cloud service providers not taking sufficient measures are considered to exist. As for supply chain attacks, which have happened frequently, attackers will have to make attacks through multiple organizations to make more attacks. So, techniques to evade detection are presumed to further advance, making it more difficult for businesses to detect attacks.

Bitcoin hit a record-high market price in the third quarter of 2020, and is on an upward trend. Cryptocurrency attacks may increase in the months ahead as they did in the first half of 2019.

2. Featured Topics

2.1. Intensifying attacks on supply chains

Following the 2nd quarter of 2020, many cases of damage by supply chain attacks have been reported. We introduced supply chain attacks a number of times in past quarterly reports, but they are getting more and more advanced and sophisticated.

Table 1: Supply chain attacks that happened and were reported in the 3rd quarter of 2020

Date	Target (entruster)	Target (entrustee)	Summary
11/17 *	Organization using the service	Japan / Event management / Peatix Japan Inc.	Peatix Japan Inc. suffered unauthorized access on October 16 and 17. In this incident, personal information of users managed by Peatix Japan was stolen. The number of affected users was a maximum of 6.77 million. [1]
11/26 *	Japan / Music / Everysing Japan Co., Ltd.	Japan / Application management / Dear U Co., Ltd.	Dear U was compromised by a third party. In this incident, the personal information of members registered for a karaoke app, Everything, which was entrusted by Everything Japan, was stolen in the period from November 5 to November 11. The number of affected members was 707. [2]
12/11 *	Japan / Power generation system / Mitsubishi Power, Ltd.	Japan / Information communication / Hitachi Systems, Ltd.	Unauthorized access was made through a managed service provider that Mitsubishi Power uses. In this incident, one server of the company was compromised and IT information was stolen. [3]
12/13 *	Organization that uses software (OrionPlatform)	U.S. / Software development / SolarWinds Worldwide, LLC.	There was a cyberattack that exploited Orion Platform, a network management software product of SolarWinds. In this incident, a maximum of 18 thousand companies were considered to have had damage. [4]

* Date published

Among these four incidents, the incident of SolarWinds has drawn special attention. According to a report, about 80% of the affected organizations to date are based in the United States. However, many companies in Japan also use products of SolarWinds, and malware infection by this attack has already been detected. We must be cautious of this attack

because damage by this type of attack of using supply chains may became more pervasive in the days ahead.

Against supply chain attacks, METI announced the establishment of Supply Chain Cybersecurity Consortium (SC3) [5] on October 30, 2020. SC3 is a consortium of organizations from diverse industrial sectors that promotes cybersecurity countermeasures against supply chain attacks. In *10 Major Security Threats*, which was published in 2019 and 2020 by the Information-technology Promotion Agency, Japan (IPA), attacks targeting the vulnerability of supply chains were ranked in the top 4. Supply chain attacks are receiving increasing attention [6].

2.1.1. Supply chain attack

With the advancement of digital transformation, IT business supply chains are growing in IT outsourcing, outsourcing of IT system construction, operation and maintenance, and the procurement of software. With these IT business supply chains, many companies are potential attack targets regardless of the industries they are in.

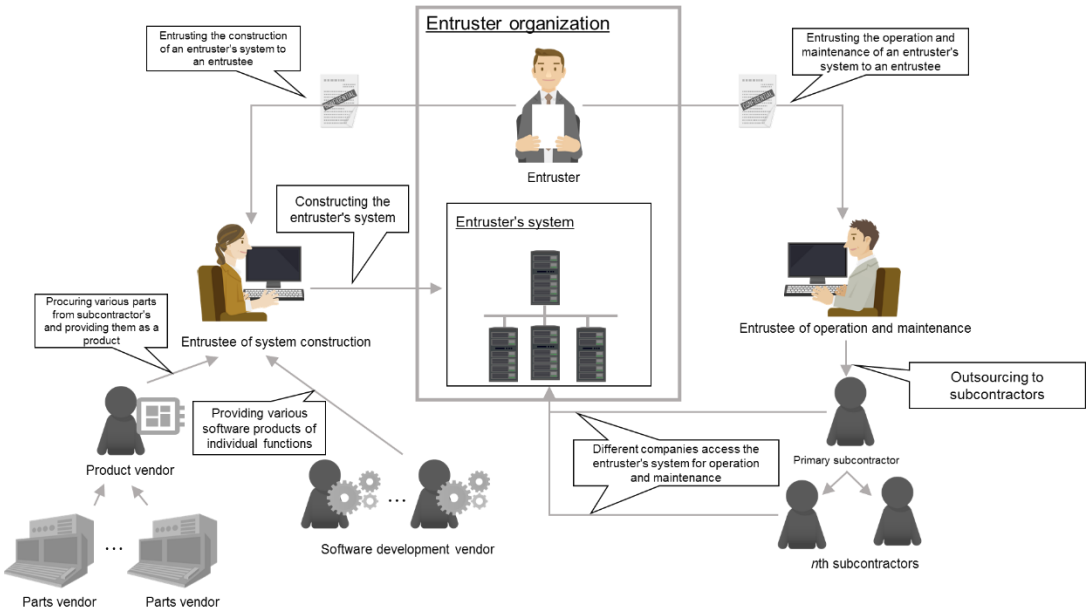


Figure 1: Example of IT supply chain

Companies must know supply chain attack methods that attackers use when they take countermeasures. The following section introduces three methods of supply chain attacks.

2.1.1.1. Methods of supply chain attacks

According to the incidents of supply chain attacks described in past quarterly reports, methods of supply chain attacks are categorized into three types: (1) attack using the entrustee as a launching pad, (2) software supply chain attack, and (3) information theft from an entrustee. Table2 describes cases of these three types of supply chain attacks.

Table2: Cases of three types of supply chain attack methods (from past quarterly reports) [7] [8] [9]

Category	Date	Target (entruster)	Target (entrustee)	Summary
(1) Attack using an entrustee as a launching pad	2019 /7/13 *	U.S. / Information communication / Sprint Corporation	Korea / Electrical instrument / Samsung Electronics Co., Ltd.	Sprint was compromised through samsung.com, the official site of the Samsung Group, resulting in the leak of personal information that Sprint manages. [10]
	2019 /9/18 *	Organization using the service	IT service company (Saudi Arabia)	A Saudi Arabian IT service company was attacked. With this attack, at least 11 organizations that use the service were compromised and an information collection tool was implanted in servers of at least two organizations. [11]
(2) Software supply chain attack	2019 /1/19 *	Organization that uses the software	PHP PEAR	A trace of an attack on the official site of PEAR, a package management tool, was found and a fabricated installer was implanted. [12]
	2019 /3/13 *	Organization that uses the software	Android SDK	Adware was implanted in RXDrioder, an SDK for advertisements, and the adware was implanted in over 200 applications developed by this SDK. [13]
	2019 /3/25 *	Organization that uses the software	ASUS Live Update	Malware was delivered with abuse of ASUS Live Update, automatic update software for computers manufactured by ASUS. [14]
(3) Information theft from an entrustee	2019 /7/13 *	Federal Security Service of Russia	SyTech Corporation	SyTech compromised from a third party. In this incident, information of the Russian Federal Security Service was stolen. [15]
	2020 /7/11 *	U.S. / Auction / LiveAuctioneers	Third party (details not disclosed)	A database of tenderers, which LiveAuctioneers outsourced to a third party, was compromised. In this incident, customer information was leaked. [16] [17]
	2020 /7/16 *	Saxo Bank Securities Ltd.	Third party (details not disclosed)	An outsourced server was compromised. In this incident, customer information was leaked. [18] [19]
	2020 /7/21 *	Israel / Video producer / Promo.com	Third party (details not disclosed)	User records leaked through a vulnerability of a third-party service. [20] [21]

* Date published

The third quarter of 2020 witnessed these three methods of supply chain attacks. Described below are cases of (1) attack using an entrustee as a launching pad, (2) software supply chain attack, and (3) information theft from an entrustee.

Attack using an entrustee as a launching pad

In this method, the attacker uses a vulnerable organization in a supply chain as a launching pad to attack and compromise a target organization such as a large company or governmental organization. The case of Mitsubishi Power is an example of an attack using an entrustee as a launching pad. Mitsubishi Power announced that it was compromised by a third party via a managed service provider (MSP, hereafter) on December 11, 2020 [3]. On December 12, the media reported that the attack was made via an operation monitoring service of Hitachi Systems [22]. The figure below illustrates the intrusion path.

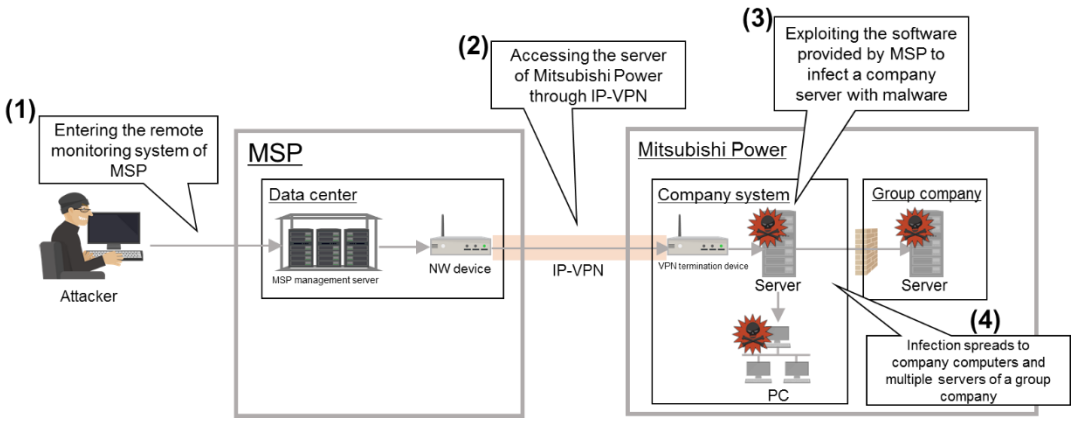


Figure 2: Flow of attacks that Mitsubishi Power received

The attacker entered an operation monitoring system (1), with which Hitachi Systems monitors customer systems, and then compromised a server of Mitsubishi Power through that system (2). After that, the attacker abused a vulnerability of software provided by Hitachi Systems to infect a company server with malware (3). Furthermore, because of inappropriate firewall settings of the company network, the malware propagated to computers of the company and multiple servers of group companies (4).

This attack did not cause the leak of highly confidential technical information, important business information of business partners, or personal information, but caused the leak of IT information such as server settings, account information, and a memory dump of an authentication process.

Software supply chain attack

In this method, attackers implant malware or an attacking code in a software product, deliver the software through a software supply chain that involves a software developer, software distributer, and other parties, and use the software as a launching pad for further attacks. The incident of SolarWinds announced on December 13, 2020 [4] is an example of

a software supply chain attack. The attacker implanted SUNBURST (Trojan horse malware) in Orion Platform, SolarWinds software for network management and remote monitoring, to distribute SUNBURST to users exploiting formal updates of the software. This software containing SUNBURST had a code signature of SolarWinds issued by Symantec, and this inhibited antivirus software of users to detect the infection, resulting in the spread of infection. The figure below illustrates the flow.

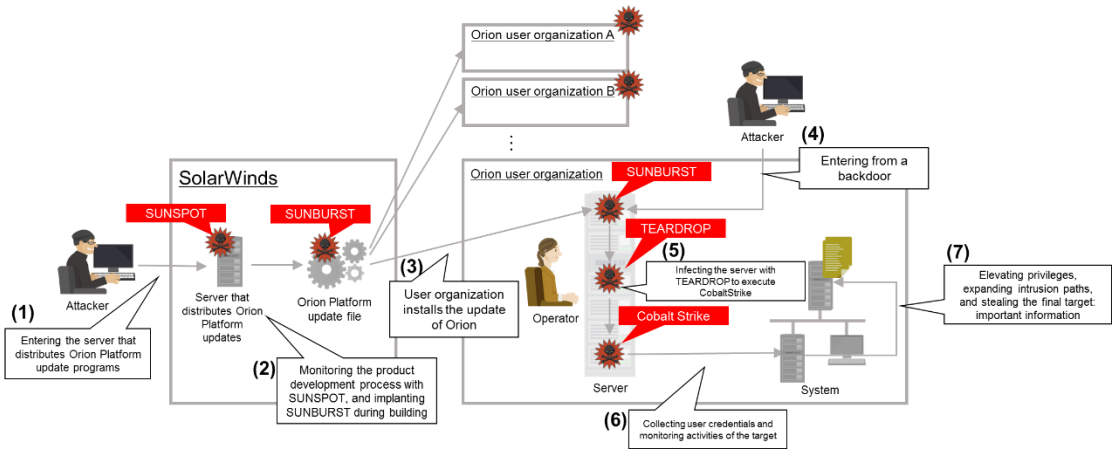


Figure 3: Flow of attacks that started from SolarWinds

First, the attacker entered the server that delivers update programs of Orion Platform software of SolarWinds (1). Next, the attacker monitored a process related to builds of Orion Platform using malware called SUNSPOT, and caught an unguarded point of the build to replace the source code file with a file that contained a Trojan horse, SUNBURST (2). After that, over 18 thousand organizations installed an update of the Orion Platform software that contained the malware (3). SUNBURST had a backdoor function, by which the attacker had access through the Internet to systems that run the Orion Platform software implanted with the malware (4). SUNBURST has a function that downloads programs from the attacker's server to the machine that runs SUNBURST and that function executes any programs. The attacker uses these functions to infect the machine with another malware called TEARDROP. TEARDROP downloads a penetration tool, Cobalt Strike, into the memory and executes it. The attacker uses Cobalt Strike to collect user credentials and monitor the behavior of the machine (5). As a result, the attacker gained privileged rights on the machine, entered other machines (6), and finally stole important information (7).

According to the paper [23] that SolarWinds submitted to the U.S. Securities and Exchange Commission (SEC), update programs implanted with SUNBURST are those delivered from March 2020 to June 2020, and over 18 thousand organizations installed these update programs. FireEye, Inc., one of the world's most well known cybersecurity companies, is one of them. This attack stole from FireEye a penetration tool and customer information, including that of government agencies [24].

Information theft from an entrustee

In this method, the attacker takes advantage of an entrustee that does not take sufficient security measures to steal personal information or important information that the entruster has entrusted to the entrustee. The attack on Peatix Inc. announced on November 17, 2020 [1], and the attack on Dear U announced on November 17, 2020 [2] are examples of information theft from an entrustee. For example, when an entruster entrusts system construction to an entrustee, confidential information such as system specifications is provided from the entruster to the entrustee. When an entruster uses a cloud service that an entrustee provides, personal information or important business confidential information is stored in the provided service in some cases. The environment of an entrustee or a cloud service without sufficient security measures is an easier target for the attacker than the system of the entruster protected by strict security measures.

2.1.1.2. Danger of supply chain attacks

The danger of supply chain attacks is that service recipients cannot completely control risks.

For example, the entruster cannot assess security measures of the entrustee in detail, nor can they instruct or force the entrustee to take detailed security measures. The entruster may include security measures in the contract, but it is difficult to have security control at an equivalent level to the company itself for many reasons. Furthermore, if the entrustee is a cloud service provider, it cannot respond to specific requirements of an entruster because it offers services of the same specification to multiple customers. With these backgrounds, security risks of the entrustee are overlooked, resulting in (1) attacks using an entrustee as a launching pad and (3) information theft from an entrustee.

Furthermore, in (1) attacks using an entrustee as a launching pad, the entruster can hardly detect unauthorized access made via the entrustee without a sophisticated behavior detection function, because the entruster trusts the entrustee. Cases that require special attention are attacks made through a managed service provider (MSP) such as the incident of Mitsubishi Power. Attackers recently tend to target operation monitoring systems. An operation monitoring system has rear-side access to systems through the operation management network, which is not segmented much. If the attacker can hijack an operation monitoring system, the attacker can easily enter various devices of the system to spread its range of activity. If the attacker succeeds in gaining unauthorized access to an MSP, information assets of many organizations will be attacked and damaged.

There are the following dangers in (2) software supply chain attacks. Users trust manufacturers of widely used software products, so they install product update programs downloaded from such a manufacturer without hesitation. Even if there is a user who does not trust update programs provided by manufacturers, it is very difficult to find fraudulent processing by analyzing update programs. Damage caused by successful intrusion of the software will be more significant if the software is well known and used by many users, as in the case of SolarWinds. This means that (2) software supply chain attacks can hardly be controlled by users if the compromised software product is well known and trusted.

2.1.2. Countermeasures against supply chain attacks

In supply chain attacks, attackers may exploit diverse objects as means of attack. Therefore, it is important to consider risks with suspicious eyes into group companies, business partners, and even your own company.

For example, it is important to try to verify every asset of the organization and external/internal communication of the supply chain, with the suspicion of the vulnerability of communication, fraudulent third parties, and malware infection of applications, data, and hardware of the organization, which may allow intrusion by attackers. Thus, important factors when considering countermeasures are not to be overconfident in the reliability of communication and assets managed by the organization, and to enumerate risks of supply chain attacks on the organization. Also, with the characteristics of (2) software supply chain attack and (1) attacks using an entrustee as a launching pad (especially, an attack exploiting an MSP as a launching pad), supply chain attacks tend to aim at an entrustee, that is, a software manufacturer or a service entrustee, as the first target.

The following sections introduce examples of security measures from the viewpoints of software development and service entrustment. Please note that they are only examples of numerous ways for reducing risks of supply chain attacks.

2.1.2.1. Security measures in software development

This section introduces measures to be considered for software manufacturers. There are two common causes in past cases of software supply chain attacks and the case of SolarWinds. They are the fact that the attacker succeeded in entering the build environment and the fact that the attacker succeeded in distributing malware by implanting it in an update program. Measures to be taken by entrustees to prevent software supply chain attacks are considered to be the strengthening of countermeasures against these common causes. Described below are some insights into these causes and plausible countermeasures, taking the example of the incident of SolarWinds.

(1) Intrusion into build environment

The actual cause is under investigation and has not yet been determined, but the attacker presumably entered the environment by bypassing multi-factor authentication or by cracking the vulnerable FTP password of GitHub. According to the SolarWinds paper submitted to the U.S. Securities and Exchange Commission and information from Volexity [25], the attacker presumably entered the environment by bypassing authentication and spoofing after getting the total secret key of Duo Security (multi-factor authentication system). As a result, the attacker probably succeeded in impersonating a qualified user of SolarWinds.

Software product manufacturers should ensure sufficient security in remote access to their build environments to defend against attacks that use commonly known vulnerabilities or attack methods. Also, cases are increasing in which attackers bypass multi-factor authentication. We should start considering risks of multi-factor authentication being bypassed or cracked.

(2) Implanting of malware in an update program and distributing it

The reasons that the attacker succeeded in implanting malware in an update program and distributing it are considered to be that the attacker was able to get permission to falsify the update program and put the code signature on the falsified update program.

- Acquisition of permission to falsify update programs

  If the attacker was able to impersonate a qualified user when entering the SolarWinds network, the attacker may have already acquired permission to modify update programs at that time. If this is true, the organization should introduce EDR to detect and take measures against the malware behavior of monitoring the build process of Orion Platform and suspicious behavior different from those of program developers. If the attacker has not acquired permission to modify update programs, damage can be prevented by detecting suspicious behavior such as privilege escalation by EDR.

  Even if the attacker impersonates a qualified user and enters the network, one effective measure is to provide separate accounts and authentication passwords for access to the development environment to put the development environment in a segment of a higher security level. However, because the cause is has not yet been clearly identified , we may need to reconsider after the actual cause is has been determined.

- Code signature on a falsified update program

  The falsified update program was signed by the code signing certificate of SolarWinds issued by Symantec. The attacker probably had stolen the code signing certificate of SolarWinds or had been able to code sign using the hijacked user privileges.

  If the code signing certificate was stolen and abused due to improper management, the company should manage it by an HSM. Some rules may be needed such as allowing code signing only to a restricted group of users, or requiring two users to be

involved for code signing.

We consider that the strengthening of countermeasures against these two common causes are actions to be taken by entrustees to prevent software supply chain attacks.

2.1.2.2. Security measures in service entrustment

Among attacks using an entrustee as a launching pad, one cause of the case of attack on Mitsubishi Power is that the attacker was able to enter the operation monitoring system of the entrustee, Hitachi Systems. Another cause is that the attacker was presumably able to use a privileged account. For these two causes, various countermeasures can be considered such as the control of external access, the protection of important assets such as accounts, and the prevention of unauthorized elevation of the privilege level.

Even if individual organizations involved in a supply chain make risk analysis and maintain a sufficient security level, just one organization without sufficient security measures can allow an attacker to succeed in a supply chain attack. Therefore, measures must be taken for all involved organizations, networks, and systems without missing anything. In taking such measures, there are two cases where the governance of the entruster (1) can be enforced to entrustees, and (2) cannot be enforced to entrustees. Here are measures in these two cases:

(1) Cases where the governance of the entruster can be enforced to entrustees

In the case where the entrustees and entruster are organizations of the same company or company group, the entruster may be able to grasp and control the entire supply chain by applying the security measures of the entruster to the entrustees. For example, the entruster would have all entrustees disclose their business procedures and security measures to verify their appropriateness, or have the entrustees employ security measures of the entruster. This ordinarily involves a great burden on entrustees because they have to take additional measures besides their own security measures. If the entrustees and entruster are organizations of the same company or company group, this method may be feasible because their security policies and measures are unified.

In recent years, there are services that unify the management of security measures of the whole complex supply chain and visualize vulnerabilities and points prone to attack. The use of these services is also an effective measure.

(2) Cases where the governance of the entruster cannot be enforced to entrustees

When entrusting something to an external organization, the entruster should confirm that the entrustee takes enough measures against supply chain attacks before signing a contract to ensure security. Here are steps of verifying and determining the security of the entrustee against supply chain attacks:

- The entruster verifies the actual security measures taken against supply chain attacks with regard to (1) attacks using the entrustee as a launching pad, (2) software supply chain attacks, and (3) information theft from the entrustee.

As a result of this security measure verification, if the entruster considers that the security measures for the entire supply chain are not sufficient, the entruster takes security measures in the following steps:

I. Enumerate risks in the entire supply chain.
II. Enumerate security measures for eliminating/mitigating the risks.
III. Between the entruster and entrustee, clearly define the party who takes the primary responsibility in implementing each security measure, as well as the scope of responsibility of each party. Then, with these definitions, assign different roles of security measures to both parties.
IV. The entruster and entrustee implement security measures.

In addition to the above, the entruster may check the third-party certificate acquisition status of the entrustee for ISMS, the Privacy Mark, etc. However, consider this as only a complementary means because security certificates alone may not ensure the security of the entrustee.

If there are still insufficient points in security measures for the entire supply chain after taking these measures, the entruster should consider additional measures. Here are some examples:

- Strengthen the company system in the ability to detect attacks in order to be prepared for attacks made via an entrustee.
- Keep the information given to the entrustee minimum to mitigate the damage of information leak from the entrustee.

2.1.3. Conclusion

In the *Quarterly Report on Global Security Trends, 2nd Quarter of 2020* [9], we forecast that supply chain attacks would continue. As anticipated, multiple organizations suffered damage from supply chain attacks in the third quarter. Especially, the case of supply chain attack on SolarWinds is remarkable. The new CEO of SolarWinds said that the case was one of the most complicated and sophisticated cyberattacks in history in view of the characteristics, magnitude, and potential damage of the attack [26]. Also, attackers found an efficient way as in the case of the supply chain attack of Mitsubishi Power [3], which is to enter an MSP to exploit an operation management system as a launching pad, and then enter the system of the target organization.

We must advance measures against supply chain attacks based on measures introduced in this report, as well as on guidelines and countermeasure frameworks of supply chain management provided by various organizations. Risks of supply chain attacks exist everywhere. So, organizations must consider not only conventional measures in their own domain but also of a wider scope involving entrustees. There are no complete measures that efficiently cover an entire supply chain that is huge and complicated. We should work to find patterns of supply chain attacks and progressively create methods for protecting the entire supply chain by analyzing multiple past incidents of supply chain attacks.

2.2. Increase of double-extortion ransomware attacks

2.2.1. Overall status of double-extortion ransomware attacks

There have been reports on damage from ransomware attacks in the past. In the 3rd Quarter of 2020, there were also many cases of damage reported worldwide, including Japan. Especially, cases of damage by double-extortion ransomware attacks were reported repeatedly. A double-extortion ransomware attack not only encrypts data and demands ransom, but also threatens to expose the data if the victim does not pay ransom. This section explains double-extortion ransomware attacks, which may bring greater damage in years ahead. Table 3 Below lists cases of damage caused by double-extortion ransomware attacks in the 3rd quarter of 2020.

Table 3: Cases of double-extortion ransomware attacks

Date published	Organization	Summary
10/22	Shionogi & Co., Ltd. (pharmaceuticals company in Japan)	A Taiwan subsidiary of Shionogi suffered a ransomware attack that corrupted a computer, exposed a part of the stolen information (the import permit of a medical instrument and permission of residence of an employee) on the Internet, and threatened to reveal more information if the company did not pay money. [27] [28]
10/27	Enel Group (energy company in Italy)	The company received a second ransomware attack in October 2020 following the first one in June 2020. Data of several TB was encrypted and stolen. The attacker threatened the company to expose the data unless the company paid a ransom of 14 million dollars. [29]
11/3	Campari (beverage company in Italy)	The attacker demanded a ransom of 15 million dollars for decrypting files. Also, the attacker threatened the company to expose the files stolen from the Campari network if the company did not pay the demanded ransom within one week of the intrusion. The crime group posted a Facebook advertisement announcing that the data was in jeopardy and Campari was refusing to pay [30].
11/12	Capcom Co., Ltd. (game manufacturer in Japan)	The cybercrime group demanded a large amount of ransom (1.1 billion yen) for the stolen confidential information. On the morning of November 11, files considered to be part of the stolen information were exposed. [31]

2.2.2. Double-extortion ransomware attacks

(1) Overview of double-extortion ransomware attacks [32]

While countermeasures against ransomware attacks such as careful backup of data are progressing, double-extortion ransomware attacks are increasing. In double-extortion ransomware attacks, the attacker not only encrypts data, but also steals the data and threatens to expose the data unless the victim pays ransom. Figure 4 and Figure 5 show the difference between conventional ransomware attacks and double-extortion ransomware attacks.

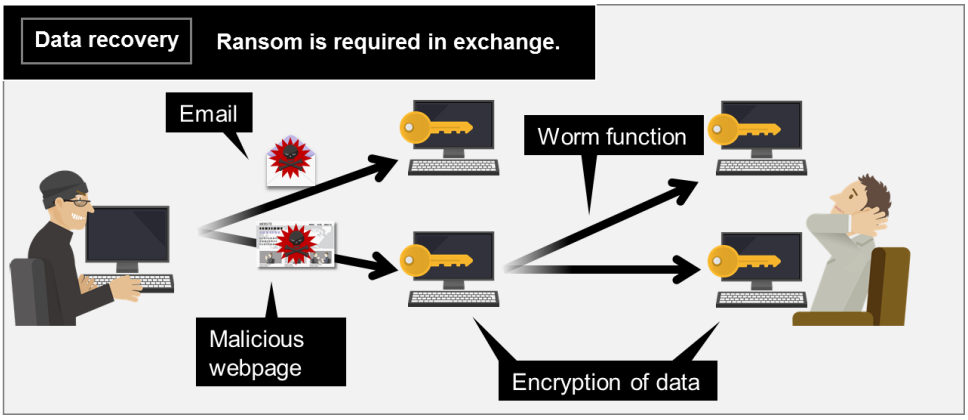


Figure 4: Conventional ransomware attack

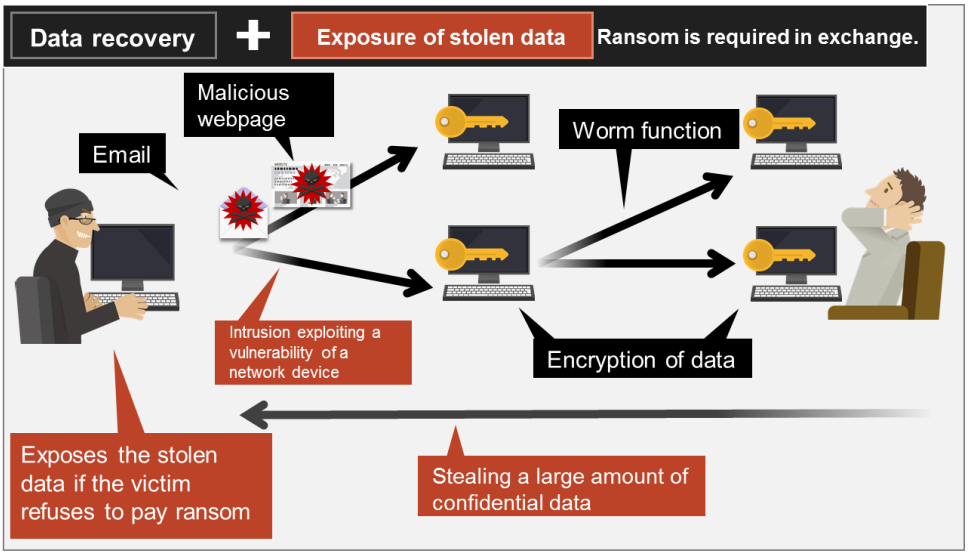


Figure 5: Double-extortion ransomware attacks

(2) Damage of double-extortion ransomware attack on Capcom

On November 16, 2020, Capcom Co., Ltd., a major game producer in Japan, announced that it received a targeted attack and was infected with order-made-type ransomware, which

stole personal information of nine individuals. On January 12, 2021, the company also announced that it found that personal information of an additional 16,406 individuals leaked. According to the announcement, the number of individuals of leaked personal information may amount to a maximum of 390 thousand. The number may grow even larger [33] [34].

According to Capcom, there was unauthorized access of a third party on November 4 and had a system failure on November 2, 2020. Through the investigation that followed, the company found that the cause of the system failure was a ransomware attack. Capcom announced the status of damage of the ransomware attack on November 16, 2020. Capcom explained that it took time to investigate and analyze the case because information on the server was encrypted and the access log was deleted [33] [35].

The crime group Ragnar Locker claims that it entered Capcom networks in Japan, U.S., and Canada, encrypted files on over 2,000 devices, and stole data of over 1 TB. Also, the attacker demanded 11 million dollars in bitcoin for the decryption of the encrypted data and the abandonment of the stolen data [36]. Capcom refused to pay ransom, and reported the case to the Osaka prefectural police. Because Capcom refused to pay ransom, the crime group exposed the data listed in Table 4 on the dark web. [37]

Table 4: Identified information leak

Date announced	Information type	Information details
11/16	Personal information	● Personal information of past employees (5 items) (1) Name, signature: 2 items (2) Name, signature: 2 items (3) Name, address: 1 item (4) Passport information: 2 items ● Personal information of employees (4 items) (1) Name and personnel information: 3 items (2) Name, signature: 1 item
	Other	● Sales report ● Financial information
1/12	Personal information	● Personal information of business partners, etc.: 3,248 individuals Name, address, phone number, and/or email address ● Personal information of retired individuals and related parties: 9,164 individuals Name, email address, and/or personal information ● Personal information of employees and related parties: 3,994 individuals Name, email address, and/or personal information
	Other	● Sales information, marketing information, development documents, business partner information, etc.

Table 5: Events of ransomware attacks on Capcom in chronological order

Date	Event
11/2	Connection failure to the company system was found before dawn, and the system was shut down for damage investigation. It was found that ransomware targeting Capcom encrypted files on the server. A threatening message was found to be sent from a crime group by the name of Ragnar Locker demanding ransom. The case was reported to the Osaka prefectural police.
11/4	Capcom posted a notice of system failure caused by unauthorized access.
11/9	Ragnar Locker posted a threatening message for Capcom at a leak site. [38]
11/11	Ragnar Locker exposed the data stolen from Capcom at the leak site. [38]
11/12	Capcom identified the leak of personal information of nine individuals and some company information.
11/16	Capcom announced the information that might have been leaked other than the nine items.
1/12	Capcom announced that it found an additional information leak of 16,406 individuals and the number of individuals of leaked personal information might amount to a maximum of 390 thousand. As of December 11, Ragnar Locker exposed data 11 times at the leak site, totaling nearly 200 GB. [39]

(3) Background of the increase of double-extortion ransomware attacks [40] [41]

Ransomware attacks have increased and evolved to the *double-extortion type*, which steals data and demands ransom. In the background of this situation, changes in the business environments of both victims and attackers are considered to exist.

- Increase in intrusion paths brought by the increase of telework

In conventional ransomware attacks, attackers use emails to infect victims. In recent years, attackers started to use the attacking method of infecting victims by entering the target network exploiting vulnerabilities of network devices. In 2019, many vulnerabilities were found in *VPN*. In 2020, the spread of COVID-19 infection made many companies employ telework through tentative construction of environments which used network devices without amendment of vulnerabilities. This situation is considered to have caused the spread of ransomware attacks that take advantage of vulnerabilities of network devices.

- Ransomware attacks becoming a business

Ransomware as a Service (RaaS, hereafter) provides an infrastructure equipped with ransomware, a downloader, a C&C server, etc., to attackers that intend to infect victims with ransomware to get ransom. RaaS is available on the dark web for tens to hundreds of thousands of yen depending on the granted usage period and functions. Attackers can make ransomware attacks easily by buying RaaS even if they do not have special development capabilities such as ransomware programing. Some RaaS sites make frequent update of functions, and functions attractive to attackers may emerge in the future. RaaS has already gained business feasibility, which is considered to be one of the reasons behind the increase of attacks.

- Inexpensive large-capacity storage is becoming widely available

In a double-extortion ransomware attack, the attacker steals data of tens to hundreds of GB, or sometimes even amounting to several TB. The major method of ransomware attacks has long been to demand ransom for the decryption of encrypted data, so cases of stealing a large amount of data were rare. The recent advent of inexpensive large-capacity cloud storage services has made it easy for attackers to store a large amount of stolen data. The availability of these inexpensive large-capacity storage services is considered to have contributed to the increase of double-extortion ransomware attacks.

2.2.3. How should we respond to double-extortion ransomware attacks?

(1) Percentage of companies that pay ransom [42] [43] [44]

CrowdStrike conducted a security survey on 2,200 individuals (200 from Japan) who are decision makers or IT security administers in IT-related departments of companies in 12 countries. The following survey results of ransomware attack damage are announced in 2020 Global Security Awareness Survey:

- ✓ Over half (52%) of the organizations in Japan that responded to the survey had a ransomware attack in the past year, and 28% among them suffered two or more attacks.
- ✓ Among organizations in Japan that suffered ransomware attacks, 42% attempted to negotiate with the attacker, and 32% paid ransom.
- ✓ The average amount of ransom paid by organizations in Japan that were attacked and paid ransom was 1.17 million dollars (approx. 123 million yen).

This survey revealed that damage from ransomware attacks is significant with facts such as that over half of Japanese organizations that answered the survey have suffered ransomware attacks. According to this survey, the percentage of worldwide answers that worry about risks of ransomware attacks increased sharply from 42% in 2019 to 54% in 2020. Among answers from Japanese organizations, 68% indicate increased concerns of ransomware attack risks related to COVID-19. The worldwide trend of discussions on actions to be taken for ransomware attacks is shifting from the prevention of ransomware attacks to negotiation with criminals for the recovery of data after infection.

(2) Points to consider when paying ransom [45]

- Will the data be returned in exchange for ransom?

A ransomware attack may encrypt files that are necessary for keeping the system running, causing system failure and business suspension. If the system is important and the amount of damage swells in proportion to the system suspension time, the damage may be minimized by paying ransom to restore the system. In such cases, many organizations would choose to pay ransom. Actually, as indicated in the awareness survey of CrowdStrike, many

organizations have paid ransom.

The party that receives ransom is a criminal. A criminal may not return data even if the victim pays ransom. According to a survey by Trend Micro, one in five organizations that paid ransom could not recover the data. Even if the data is returned, the data is not guaranteed to be free of falsification. Some type of data, such as financial information, has no value even if recovered unless it is guaranteed to have no falsification. Even if the data is returned without falsification, the attacker may threaten to expose a copy of the data again after the ransom was paid for decryption. Once an organization pays ransom, the name of organization is shared to the network of attackers as a once-paying organization, and another attacker may target the organization. One must know that, if the cause of ransomware infection is not identified, the same method may be used again.

- Paying ransom can mean supporting terrorists [46] [47] [48]

On October 1, 2020, the Office of Foreign Assets Control (OFAC) of the U.S. Treasury announced that companies, such as financial institutions and cyber-attack security insurance companies, that support ransomware victims in paying ransom may violate OFAC regulations and be subject to the following sanctions:

- ✓ The act of paying ransom to criminals benefits them, encourages unlawful purposes, and provides funds for activities that go against the security and foreign policies of the United States of America. Such acts violate the regulations of OFAC and are subject to fines and sanctions.
- ✓ A party damaged by a ransomware attack must report to and cooperate fully with law enforcement bodies.

The above instruction indicates that, if a paid ransom goes to a dangerous crime organization such as a terrorist, the company that paid the ransom is considered have helped them and can be subject to sanctions. In the 87th annual congress of the U.S. Conference of Mayors in July 2019, over 220 mayors signed a resolution that they will not pay ransom for ransomware attacks. The purpose of this resolution is to discourage attackers by rejecting to pay ransom [49]. The above OFAC instruction is considered to further promote the trend of rejecting ransom. An organization within the scope of the influence of the U.S. law must consider the above OFAC instruction when considering whether to pay ransom in the case of a ransomware attack.

(3) How can we prevent damage caused by double-extortion ransomware attacks? [50] [51] [52]

Damage caused by ransomware attacks is becoming worse and more complicated. Companies and organizations should take all measures they can to prevent serious damage caused by ransomware attacks.

As in the case of the double-extortion ransomware attack on Capcom, more attack cases now use targeted cyberattack methods to enter the network of a company or organization to make a double-extortion ransomware attack. Such double-extortion ransomware attacks are

made using the following four major steps:

1. Intrusion into a network
2. Expansion of the range of intrusion in the network
3. Theft of data
4. Encryption of data

American company MITRE Corporation published *ATT&CK* [53], which is a set of knowledge on cyberattack methods. *ATT&CK* consists of Tactic (purposes of attackers), Technique (methods of attacks) for realizing Tactic, and Mitigation/Detection as countermeasures against Technique. We should take measures against double extortion ransomware attacks on our organizations, with reference to the part of ATT&CK relevant to the four steps of double-extortion ransomware attacks described above, which are similar to targeted cyberattacks.

2.2.4. Conclusion

In the past several years, ransomware attacks have been ranked among the 10 Major Security Threats selected by the Information-technology Promotion Agency, Japan (IPA). Their attack methods have evolved from *the distribution type* to *the targeted type* that targets a specific organization, and then to *the double-extortion type*. According to a survey by CrowdStrike, among the responding organizations in Japan that have experienced ransomware attacks, about 30% have paid ransom. However, the trend of policies for double-extortion ransomware attacks is to prohibit paying ransom because it is an act of helping crimes. An example is a recommendation made by Office of Foreign Assets Control of the U.S. Treasury in October 2020. To prevent damage caused by double-extortion ransomware attacks, the most effective action for companies and organizations is to take all defending measures possible. However, with evolving attacking methods, it seems difficult to defend perfectly. We consider that an important attitude toward an incident is to have strong determination not to yield to the threat of the criminal, even if damaged by a double-extortion ransomware attack.

3. Data Breach

In the third quarter of 2020, there have been a number of data breach incidents attributable to defective setting of Salesforce. In such cases of data breach through a cloud service, the issue is which party is to take responsibility. In this section, we explain the overview of the case of data breach caused by defective setting of Salesforce, and the shared responsibility model, which is a security policy when using cloud services.

3.1. Data breach through Salesforce

In December 2020, PayPay Corporation and Rakuten Group, Inc. announced the possibility of an information leak caused by defective setting of a cloud business management system [54] [55]. Both PayPay and Rakuten announced that they were compromised by an overseas third party. The media reported that both companies were using a cloud business management service on the Salesforce platform of Salesforce.com [56]. The media also reported that the cause of the defective setting was insufficient provision of information from Salesforce.com at the time of product renewal [57]. Also, there have been a number reports on data breach incidents attributable to defective setting of the Salesforce platform in the 4th quarter [58]. In this situation, the Financial Services Agency and NISC called attention on defective setting of the cloud business management service of Salesforce.com [59] [60].

Salesforce.com announced that third parties can view some information of the following products and functions [61]:

- Community
- Salesforce site (former site: Force.com)
- Public site construction function on Site.com

An organization that uses the Salesforce platform, which may cause an incident, should check the privileges settings of guest user access control with reference to the best practices described in the guideline of Salesforce.com (https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/). If your company cannot check the settings without help, file a case in the Salesforce help link at Salesforce.com, or ask the SI partner who introduced the service or other helpers.

About this incident, Salesforce.com announced the following:

- The incident was not attributable to a vulnerability of the product.
- The incident was attributable to inappropriate privilege settings of guest user access control.
- Users must confirm that the privilege settings of guest user access control are made appropriately.

- About this incident, there was no fact that the settings were changed at the time of product update.
- A standard release note was published at the product update.

In this incident, guest users were able to have access to restricted information at public sites built on the Salesforce platform because of inappropriate privilege settings of access control for guest users, who do not have to go through an authentication process. Therefore, this incident would not have happened if the privilege settings of access control of the Salesforce platform were made appropriately. However, in view of a number of similar incidents that happened, the behavior of Salesforce.com may not have been satisfactory. When considering the locus of responsibility in this incident, one must consider it in the light of the shared responsibility model in cloud services and the cause of the incident.

3.2. Shared responsibility model

Responsibilities for the security of cloud services are basically considered based on the policy of the shared responsibility model (Figure 6). The shared responsibility model is a policy of clarifying the scope of responsibilities of the cloud service provider and the cloud service customer when starting the use of the cloud service. In this incident, the cloud service provider is Salesforce.com, and the cloud service customers are PayPay and Rakuten. There are two major types of the shared responsibility models depending on the type of the cloud service. The border of the scope of responsibility is called the responsibility demarcation point.

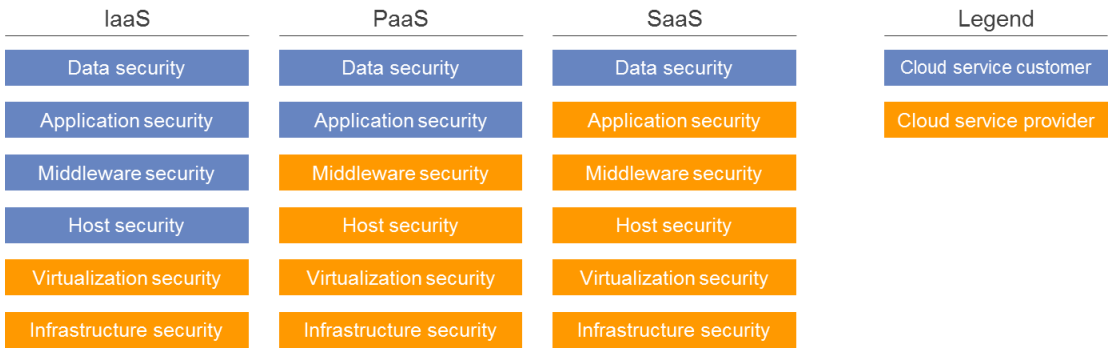


Figure 6: Shared responsibility model

Source: Excerpt from *Guideline on Effectively Managing Security Service in the Cloud*, Cloud Security Alliance [62]

This incident is a data breach caused by defective privilege settings of guest user access control in PaaS provided by a cloud service provider. Privilege settings of access control belong to data security in Figure 6, so that the prime responsibility lies with the cloud service customer. The data breach in this incident would not have happened if the cloud service customer had understood the cloud service used and set privileges appropriately.

In this incident, however, there have been many reports on data breaches caused by defective settings similar to the cases of PayPay and Rakuten. Therefore, these defective settings are unlikely to be simple human mistakes. Salesforce.com claims that the release note indicates the addition of the function that is considered to be related to this incident. This claim is considered to mean that the addition of the function had been explained to cloud service customers, and therefore, they were able to take an appropriate action. However, in the consideration of the fact that many companies made the same defective settings, Salesforce.com is not considered to have made sufficient explanation on the additional setting for the added function, nor have implemented a satisfactory access control mechanism. Cloud service providers are considered to owe duty of care for preventing defective settings that may cause a serious problem such as data breach. For cloud services that are widely used such as the Salesforce platform, it is important that they publicize setting changes that may cause serious problems because the impact is great if a problem occurs. If duty of care is not adequately fulfilled by the cloud service provider, we consider that the responsibility of data breach caused by a defective setting lies not only with the cloud service customers that made the defective setting, but also with the cloud service provider.

Because the responsibilities in the use of a cloud service are determined based on the shared responsibility model, we consider that the responsibility of this data breach incident in the Salesforce platform should be taken by cloud service customers. However, in the case of this incident, the cause lay with both parties: the cloud service customers who did not understand well the specification of the cloud service they are using, and the cloud service provider who did not provide sufficient explanation to cloud service customers.

As in this incident, there are cases in which the responsibility is determined to lie with one party based on the shared responsibility model even if the cause of the problem lies with both parties. However, we consider that a party that holds part of the cause should take some measures, even if the measures are not in the scope of responsibility of the party. Both the cloud service provider and cloud service customers must consider what measures to take regarding defective setting of the cloud service.

3.3. Data breach attributable to defective setting

As with the Salesforce platform, a cloud service such as cloud storage that stores confidential information has a risk of data breach by unauthorized access exploiting defective settings.

For example, when a cloud service customer cannot have access to a desired communication port or file, they may assign more access privileges than they need. As a result, users that should not have access to the communication port or file have access to it, leading to unauthorized access and data breach.

Such defective settings may be made due to a simple error or insufficient understanding of the specification by the cloud service customer. The cloud service customer should understand well the specification and the setting method of the cloud service to use, and should check the setting for any errors when they have changed the setting. One way of

preventing errors is to grant the right of making settings only to those who possess the skill certificate granted by the service provider. An access range verification test is also effective in finding defective settings.

Cloud service providers can mitigate the risk of defective settings in accordance with the architecture of the provided cloud service by minimizing the amount of tasks required by cloud service customers at the time of a cloud service specification change, or by defining safe values for the initial setting. Cloud service providers can also provide cloud service customers with sufficient information and support with an appropriate channel and timing. Especially, for a setting that may cause a serious problem such as data breach, the cloud service provider must provide support and best practice about the setting method so that cloud service customers will not make defective settings. Cases that involve a setting change to be made by cloud service customers require even more elaborate support and communication.

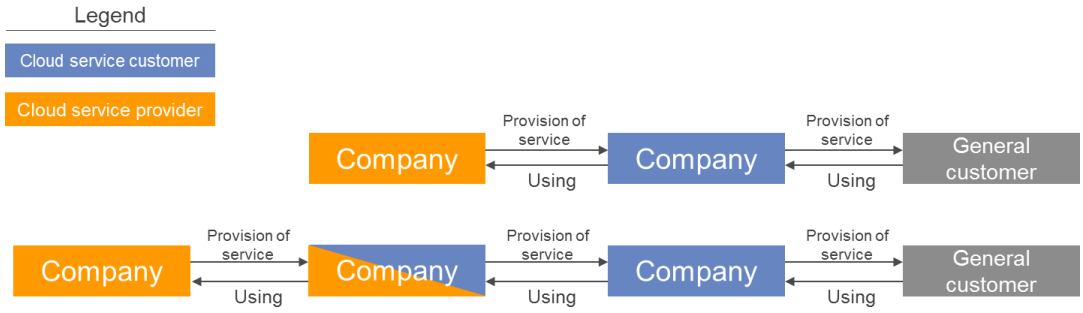


Figure 7: Cloud service provider and cloud service customer

A cloud service customer may provide the cloud service to its own customer, or the cloud service customer itself may act as a cloud service provider (Figure 7). In such a case, the company takes the roles of both the cloud service provider and cloud service customer, and therefore, must consider and implement the measures described above in both perspectives.

3.4. Conclusion

Many similar incidents have been identified regarding the defective setting of the Salesforce platform. An organization that uses the Salesforce platform should check that the privileges settings of guest user access control are made appropriately according to the guideline of Salesforce.com.

Responsibilities of cloud services are defined by the shared responsibility model. However, depending on the situation of the cloud service provider and cloud service customer, the cause of the problem may lie with both parties. Cloud service providers must provide support to cloud customers so that they do not make defective settings. Cloud service customers should understand the scope of their responsibility based on the shared responsibility model (Figure 6) and the specification of the cloud service in order to prevent defective settings.

4. Vulnerability

4.1. Summary of the 3rd quarter of 2020

Support for CentOS 6 ended on November 30, 2020 [63], and support for Adobe Flash Player ended on December 31, 2020 [64]. We recommend that organizations stop using these software products because updates and security patches will not be provided.

From a security company FireEye Inc., a tool used by its red team was stolen. This incident became a hot topic because it was a security company that was compromised and a tool of the security company was stolen and might be abused. The next section analyzes the impact of the theft of this tool.

4.2. Impact of the theft of the tool

On December 8, 2020, FireEye announced that it had a targeted attack and was robbed of a tool of the company's red team [65]. The attack method used was a supply chain attack that exploited the update of Orion Platform, the network management product of SolarWinds. Many organizations including U.S. government institutions were damaged by the same method [66]. Details of the attack itself are described in "2.1 Intensifying attacks on supply chains", so this section focuses on the impact of the theft of this tool.

The red team, the user of the tool stolen, is a specialist team that evaluates company security frameworks by simulated attacks. The stolen tool was a tool used for simulated attacks and contained attack codes that use known vulnerabilities [65]. It is highly possible that the attacker can compromise companies using vulnerabilities contained in this tool, which may lead to great damage to organizations that have not taken measures against the vulnerabilities. Table 6 lists high-severity vulnerabilities announced by FireEye that require prioritized action.

Table 6: List of vulnerabilities announced by FireEye that require prioritized action [67]

No	CVE	Product	CVSS	Vulnerability
1	CVE-2019-11510	Pulse Secure Pulse Connect Secure	10.0	Vulnerability related to permission
2	CVE-2020-1472	Microsoft Windows Server	10.0	Vulnerability that allows privilege escalation
3	CVE-2018-13379	Fortinet FortiOS	9.8	Vulnerability in path traversal
4	CVE-2018-15961	Adobe ColdFusion	9.8	Vulnerability related to unlimited upload of dangerous-type files

5	CVE-2019-0604	Microsoft SharePoint	9.8	Vulnerability that allows remote code execution
6	CVE-2019-0708	Remote desktop service of Microsoft Windows	9.8	Vulnerability that allows remote code execution
7	CVE-2019-11580	Atlassian Crowd and Crowd Data Center	9.8	Vulnerability in input check
8	CVE-2019-19781	Citrix Application Delivery Controller and Gateway	9.8	Vulnerability in path traversal
9	CVE-2020-10189	Zoho ManageEngine Desktop Central	9.8	Vulnerability related to deserialization of untrusted data
10	CVE-2014-1812	Microsoft Windows	9.0	Vulnerability that allows the theft of important credentials in group policy implementation
11	CVE-2019-3398	Confluence Server and Data Center	8.8	Vulnerability in path traversal
12	CVE-2020-0688	Microsoft Exchange Server	8.8	Vulnerability that allows remote code execution
13	CVE-2016-0167	Microsoft Windows	7.8	Vulnerability that allows privilege escalation for kernel mode driver
14	CVE-2017-11774	Microsoft Outlook	7.8	Vulnerability that allows arbitrary execution of commands
15	CVE-2018-8581	Microsoft Exchange Server	7.4	Vulnerability that allows privilege escalation
16	CVE-2019-8394	Zoho ManageEngine ServiceDesk Plus	6.5	Vulnerability related to unlimited upload of dangerous-type files

In WannaCry that broke out in 2017, an attack group used a tool that it stole from the United States National Security Agency. The case of FireEye also has the danger of causing a similar situation [68] [69]. However, with the lesson that organizations learned from the incident of WannaCry, they now properly apply security patches for serious vulnerabilities found to be exploited, such as those listed in Table 6. In consideration of the fact that many vulnerabilities listed in Table 6 , it had already been found to be abused and most organizations had taken countermeasures before the tool theft incident, and the fact that no attack using the tool has been identified after the incident, the possibility that this incident significantly increased the danger of these vulnerabilities is considered small at this point.

An organization that has not applied the security patch of any of the vulnerabilities listed in Table 6 should promptly apply it. If there are many vulnerabilities to be amended, one may wonder which vulnerability should be amended first. For reference, the next section describes a guideline of prioritization of actions.

4.3. Actions to be taken for vulnerability responses and points to consider

Among vulnerabilities listed in Table 6, all of those that require prioritized action are known vulnerabilities. Organizations that have not made regular vulnerability responses should take action promptly. Also, many vulnerabilities are found every day. Organizations that do not take care of them will be under threat of attack [70]. It is important to respond to vulnerabilities regularly to prevent a situation that the organization must take an emergency action to a vulnerability or receive an attack exploiting a vulnerability. However, vulnerability responses involve not only the continued execution of a series of tasks from asset management to the application of amendments, but also responses to many vulnerabilities found every day. The load of the task is heavy, and we consider that there are many organizations that cannot conduct the task sufficiently [71]. This section explains points to consider to take care of vulnerabilities efficiently every day.

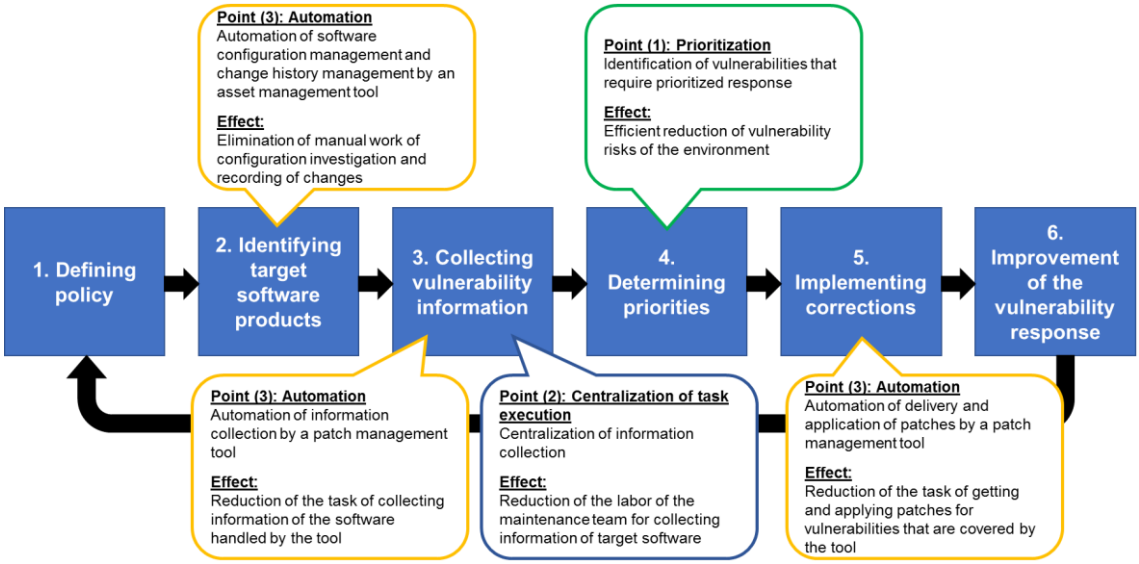
Table 7 lists actions to be taken as vulnerability responses that we prepare with reference to the NIST guideline [72] [73] [74] [75].

Table 7: Actions to be taken for vulnerability responses

No	Action item name	Description of action
1	Defining policy	Define the process and organization for vulnerability responses.
2	Identifying target software products	Manage the software configuration (type, version, and other properties of software) and the update history (application of patches, etc.) to clarify which software products require vulnerability responses.
3	Collecting vulnerability information	Check periodically the information of vulnerabilities, corrections, and threats of the identified software products.
4	Determining priorities	Prioritize corrections in view of the following: ✓ Current status of vulnerabilities (abuses, etc.) ✓ Importance of the confidentiality, integrity, and availability of the system ✓ Severity of the vulnerability in consideration of the system status
5	Implementing corrections	● Before implementing corrections in the production environment, do the following: ✓ Determine the action policy (final action or tentative action) ✓ Confirm that the correction has no problem by testing it in a non-production environment ✓ Back up the entire production environment ● Implement the correction. ● After implementing the correction, confirm that the vulnerability has been amended or mitigated as intended.
6	Improvement of the vulnerability response	Check how the vulnerability response was made, and review the process and organization.

Figure 8 describes some points for the effective implementation of the above action flow.

Figure 8: Flo



w of vulnerability response and points to consider

The first point to consider is prioritization. By prioritizing actions, one can first respond to vulnerabilities that truly need to be responded to. In prioritization, evaluate vulnerabilities in view of the following three points listed in Table 7.

- Current status of vulnerabilities (presence of attacks, levels of countermeasures, accuracy of information)
- Importance of the confidentiality, integrity, and availability of the system
- Severity of the vulnerability in consideration of the status of countermeasures on the system

One way of evaluating vulnerability risks is CVSS Environmental Metrics, which considers the three viewpoints above [76]. When calculating the CVSS Environmental Score using CVSS Environment Metrics, the evaluator evaluates a maximum of 14 CVSS items of the configuration, settings, countermeasure implementation status, and other aspects of the target system with the understanding of vulnerability exploitation methods. If the CVSS Environmental Score is difficult to calculate, one can also evaluate risks with their own method based on CVSS Base Metrics by focusing on specific points such as the possibility of attack over the network, attack information, and the presence of PoC. Also important is to make prior arrangement for the smooth execution of evaluation, such as saving time for persons in charge of system operation and maintenance by the central execution and automation of common tasks, the documentation of the procedure of vulnerability response, and the training of the system operation and maintenance persons.

The second point is the central execution of tasks. With the central execution of common

tasks such as the collection of vulnerability information conducted by different system operation and maintenance teams, their work load will be reduced. Especially, if different maintenance teams use the same software, the duplicated work load such as collecting vulnerability information can be reduced easily. Also, if software products that constitute different systems can be standardized, the effect of task centralization will be greater. When centralizing tasks to the center team, it is important to clearly define the scopes of work between the center team and different maintenance teams, such as target software subject to information collection and type of information to be collected, in order to cover all necessary tasks. For a team short of labor power and in such a situation that one person is responsible for both security response and system operation, we recommend outsourcing. By using a vulnerability information delivery service or other ways of outsourcing, the maintenance team can use the spare time to focus on tasks that cannot be outsourced such as prioritization of vulnerabilities and system operation verification before applying amendments.

The last point is automation. It takes much time to identify target software products, collect vulnerability information, and apply corrections if these tasks are not automated. The work load may be significantly reduced through automating tasks by using tools such as an IT asset management tool and patch management tool.

4.4. Conclusion

Many of the high-severity vulnerabilities announced by FireEye that require prioritized action had been publicized and abused before the announcement of the incident. Therefore, the incident is not a significant threat for organizations that properly apply security patches according to the lesson of WannaCry. Organizations should conduct vulnerability responses regularly to avoid being in a situation that they need to take emergency vulnerability measures in response to an incident such as the tool theft from FireEye, or in a situation that they receive an attack that exploits a vulnerability not amended.

We recommend that organizations consider a vulnerability risk evaluation method suitable for them and make preparations for smooth execution of vulnerability responses. We also recommend that organizations reduce the work load of the system operation and maintenance persons by centralizing and automating tasks to secure time for them to consider priorities or other important tasks.

5. Malware/Ransomware

5.1. Summary of the 3rd quarter of 2020

Damage cases caused by malware and ransomware in Japan continue from the 2nd quarter of 2020. In Japan, there was damage from ransomware and damage by Emotet, which is the malware that marked a record-high infection magnitude in September 2020. Overseas, there was damage from ransomware that targets the healthcare and education sectors and damage by Emotet, such as in Japan.

This section introduces the trend of Emotet, which continues to rage from the 2nd quarter of 2020, and malware named IcedID, which is similar to Emotet and has started to spread in Japan. Overseas, SANS Institute announced that it identified the infection of IcedID in mid-July 2020 and after [77]. In Japan, multiple cases of IcedID infection were found from late October of 2020, and the JPCERT/CC analysis center called for caution via Twitter in November 2020 [78]. IcedID is explained in this section because cases of its damage will probably increase and this malware can be handled by considering the points in common with and different from Emotet.

5.2. Trend of Emotet

Emotet became less active in November 2020, but Check Point Software Technologies, a security vendor, ranked it No.1 among the most infectious malware codes in the Global Threat Index issued in December 2020 [79]. In the 3rd quarter, Emotet used emails impersonating Windows Update of Microsoft [80] and emails using keywords of "Christmas" and "Bonus" matching the year-end period [81]. An Emotet email infects a computer when the user opens an attached word document and clicks [Enable Content]. The attacker crafts the email content to make the user want to click the button. An effective way against this attack is to identify attack emails by keeping yourself updated about attack email texts and attachment file names that are published by institutions such as the Information-Technology Promotion Agency. The attacker updates Emotet regularly. The version of Emotet found recently had an updated malicious payload and an improved detection-evasion function [79]. Some organizations probably use EmoCheck, a detection tool provided by JPCERT/CC in February 2020. However, according to JPCERT/CC, the infection of Emote that started activity from December 21, 2020 cannot be detect by EmoCheck v1.0 [82]. EmoCheck v2.0, capable of detecting the above Emotet version, has been provided since January 27, 2021.

According to the report issued by LAC Co., Ltd in November 2020, among Emotet-infected devices that the cyber emergency center of LAC investigated in September 2020, about 90% of them were also infected by malware called Zloader [83]. An attacker is considered to have used Emotet to distribute Zloader in order to steal online banking information. As explained in a past quarterly report, in the event of Emotet infection, one should suspect the infection of other malware, especially the infection of Zloader and accompanying leak of online banking information.

5.3. IcedID akin to Emotet

IcedID is a trojan-type fraudulent program for stealing information of email and browsers. As with Emotet, it has the function of secondary infection of other malware. According to Trend Micro, the malware started be detected from late October of 2020, and the number of infected devices in Japan detected by Trend Micro products was over 70 in the 10-day period from October 27 to November 6, 2020 [84]. IcedID shares many common characteristics with Emotet, so that measures for Emotet are effective if some different points are considered. We found the following common points and different points by comparing the characteristics of IcedID and Emotet published by a security vendor.

- The attacker sends an email with the attachment of a password-protected zip file. The password is indicated in the email text. [85]
- The subject starts with "Re:" as if the email is a response. [85]
- The device is infected by IcedID if the user unzips the file, opens the word document, and executes [Enable Content]. [85]
- IcedID steals information such as email credentials to log in to the email account, and distributes attack emails to organizations that have correspondence with the email account. [86]
- The malware may download a different malware code, magnifying the damage. [86]

The common points above of the attack methods suggest effective countermeasures that are common. For IcedID, the following countermeasures for Emotet are effective.

- Do not view suspicious emails or attachments.
- Do not click the [Enable Content] button. (Disable auto execution of macros.)
- Introduce a security product that detects emails and endpoints.
- Do not send/receive emails with an attachment of a password-protected zip file.

On the other hand, there are the following differences between Emotet and IcedID.

One difference is that Japanese texts of IcedID attack emails identified so far are less fluent compared with Emotet [85]. Therefore, looking at the fluency of Japanese text of the email is an effective measure. However, as with Japanese texts of Emotet, which have become increasingly sophisticated with a number of updates from the initial spread, IcedID emails are expected be updated so that they become difficult to discriminate from normal emails.

The second point is that IcedID emails are sent via organizations such as business partners. Some Emotet emails disguised the display name, so the presence of a disguise could be identified. However, IcedID hijacks an email account to send attack emails from that email account, so it does not disguise the display name. IcedID attack emails cannot be identified by checking the disguise [85].

The third point is that it has not been long since IcedID attack was first detected in Japan, so there are organizations that do not know of its existence. The attack method and effective countermeasures of Emotet are widely known, and there should be organizations that have introduced the detection tool EmoCheck mentioned above. Of course, EmoCheck cannot detect IcedID [86]. Organizations must introduce a security product effective for IcedID. We recommend that organizations do not rely only on pattern matching but consider the introduction of next-generation anti-virus products that detect abnormal behavior because the malware will probably be updated continuously.

In order to prevent damage from IcedID, organizations should collect the latest information about IcedID delivered by security institutions, grasp the existence of different versions and the latest attack method, and take measures with reference to the above-mentioned common and different points.

5.4. Cases of damage by malware/ransomware

As described in "5.1 Summary of the 3rd quarter of 2020", there are many cases of damage by malware and ransomware in Japan. Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) of the U.S. issued a warning on cyberattacks on medical institutions [87] and education institutions [88]. The cases listed below include damage cases of medical institutions and education institutions.

Table 8: Cases of damage by malware/ransomware

Date	Target	Summary
10/8 *	USA (Massachusetts)/ Springfield public school	The school identified a latent threat. The school was closed and remote classes were temporarily suspended. The school is considered have received a ransomware attack. [89]
10/10	USA / Law office / Seyfarth Shaw LLP	The office was infected with ransomware, and stopped the system. [90]
10/10	USA / Bookstore chain / Barnes&Noble	The bookstore chain was infected with ransomware, and had a system failure. There was a problem where users could not have access to the library of the electronic books they bought. [91]
10/16 *	Japan / Manufacturer of electronic parts and devices / Kyocera Corporation	The company was infected with Emotet, and delivered fraudulent emails. There may have been a leak of personal information such as email addresses, names, addresses, and phone numbers of related parties in and outside the company, as well as email texts. [92]

10/30 *	Japan / Educational institution / Kansai Medical University	The university was infected with Emotet, and fraudulent emails were sent from a server of an organization different from the university. Medical ICT systems of the hospitals that belong to the university were operated on an independent network, so that they were not affected. [93]
11/1	Italy / Liquor company / CampariGroup	The company was infected with Ragnar Locker ransomware, and its IT services and network were stopped. The attacker stole 2 TB of data. The attacker demanded a ransom of 15 million dollars. [94]
11/2	Japan / Game manufacturer / CAPCOM	The company was infected with Ragnar Locker ransomware, and the attacker stole 1 TB of data. Personal information including names and addresses also leaked. The attacker demanded a ransom of 11 million dollars. [95]
11/30 *	Japan / System integrator / ilovex Co., Ltd.	The company was infected with order-made-type ransomware, and data on its computers and file server were encrypted. [96]
11/25	USA (Maryland) / Educational institution / public school in Baltimore County	The institution was infected with ransomware. It temporarily suspended virtual learning and closed the school. [97]
11/29	Mexico / Manufacture of electronic devices / Foxconn	The company was infected with DoppelPaymer ransomware, and its website went down. The attacker exposed the stolen data on a leak site. [98]
11/30 *	USA / For-profit educational company / K12 Inc	The company was infected with Ryuk ransomware. It shut down its system. The online learning system was not affected. The company paid ransom with cyber insurance. [99]
12/6 *	USA (Maryland) / Hospital / Greater Baltimore Medical Center	The hospital was infected with ransomware, and the computer system and operation of the hospital were affected. [100]
12/16 *	China / Medical services / WellBe Holdings Limited	The company was infected with Emotet, and delivered impersonating emails. This incident may have caused the leak of 6,906 email texts. [101]
12/30 *	Lithuania / National Public Health Center (NVSC)	The company was infected with Emotet, and delivered fraudulent emails. The center temporarily stopped the email system to prevent the spread of virus. [102]

* Date published

5.5. Conclusion

We introduced malware named IcedID, which is similar to Emotet. IcedID is expected to get more sophisticated in Japanese texts and infection functions, as it was with Emotet. However, Emotet and IcedID have common points in attack methods and effective countermeasures, so that measures that have already been taken by many organizations are effective for IcedID. Organizations that have taken enough measures against Emotet do not have to be alerted to IcedID as a new threat. There will probably be increasing cases of similar malware and updated malware, but we consider that organizations can protect themselves from many attacks by understanding their characteristics and continuing to take security measures unless there is a significant change.

6. Outlook

Keep alerted to changing supply chain attacks

The incident of Mitsubishi Power was a supply chain attack that used an operations management system as a launching pad to efficiently enter multiple systems. In the supply chain attack on SolarWinds, the attacker used more sophisticated methods compared to past ones, such as *a technique to bypass multi-factor authentication for intrusion* and *technique of implanting a malicious software backdoor without being found by the organization*. These two supply chain attacks damaged organizations that take important roles in society, including companies that have business with the Ministry of Defense such as Mitsubishi Electric and NEC, IT companies such as FireEye, Microsoft, and Cisco, as well as multiple government institutions.

As these incidents indicate, supply chain attacks that enter target systems via an operation management system and supply chain attacks that exploit the distribution of updates of OS or other major software allow attackers to enter many systems efficiently, so attackers get very active when they use these methods. Therefore, companies that provide operation monitoring services, and companies that provide software especially need to strengthen countermeasures against supply chain attacks. Furthermore, in order to enter an organization from which efficient supply chain attacks are possible, attackers will make a separate supply chain attack. Thus, attackers will have to make supply chain attacks via multiple organizations, leading to further sophistication of disguising techniques. As a result, it will be more difficult for businesses to detect attacks.

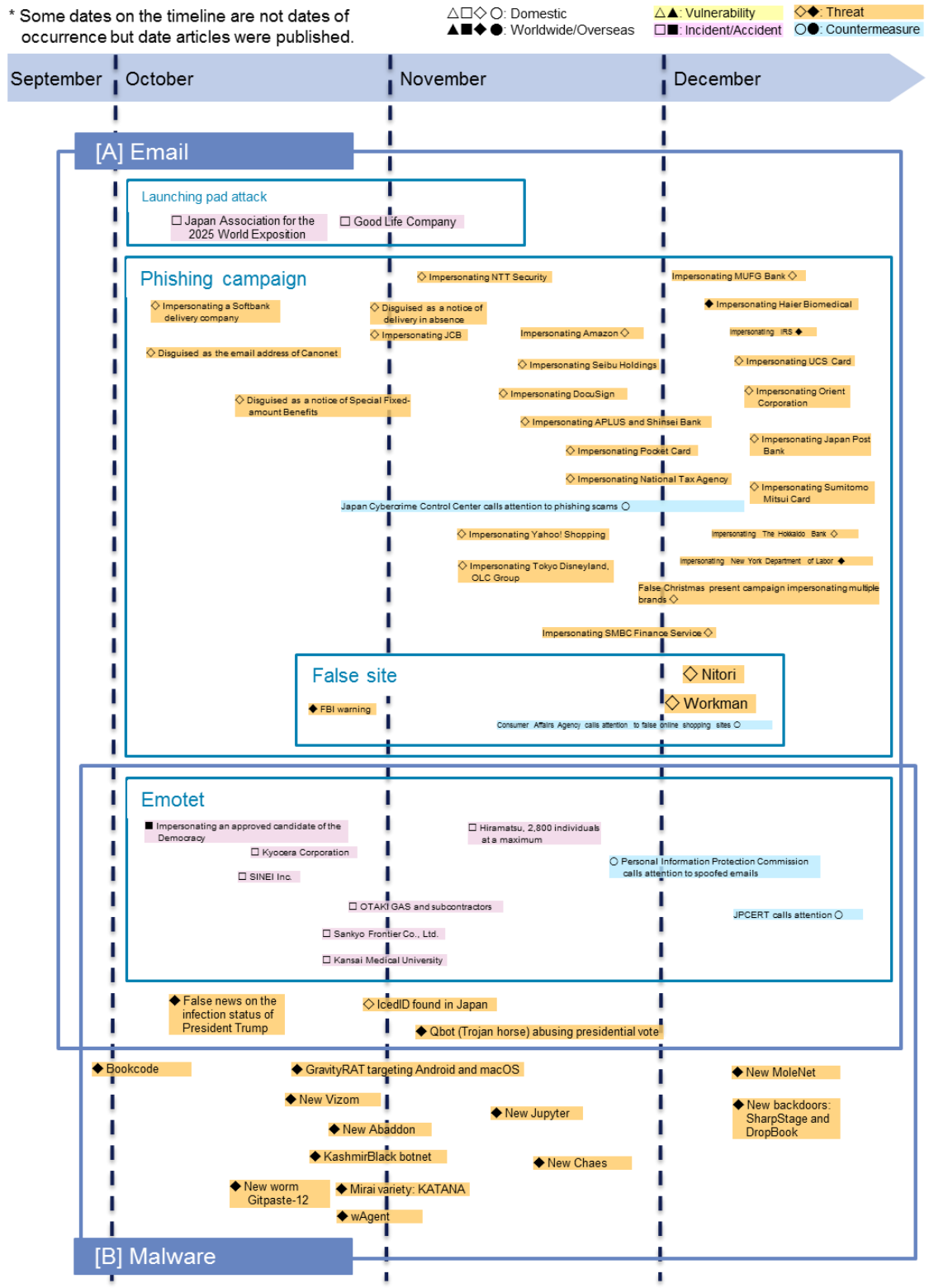
Incidents attributable to defective setting of cloud services

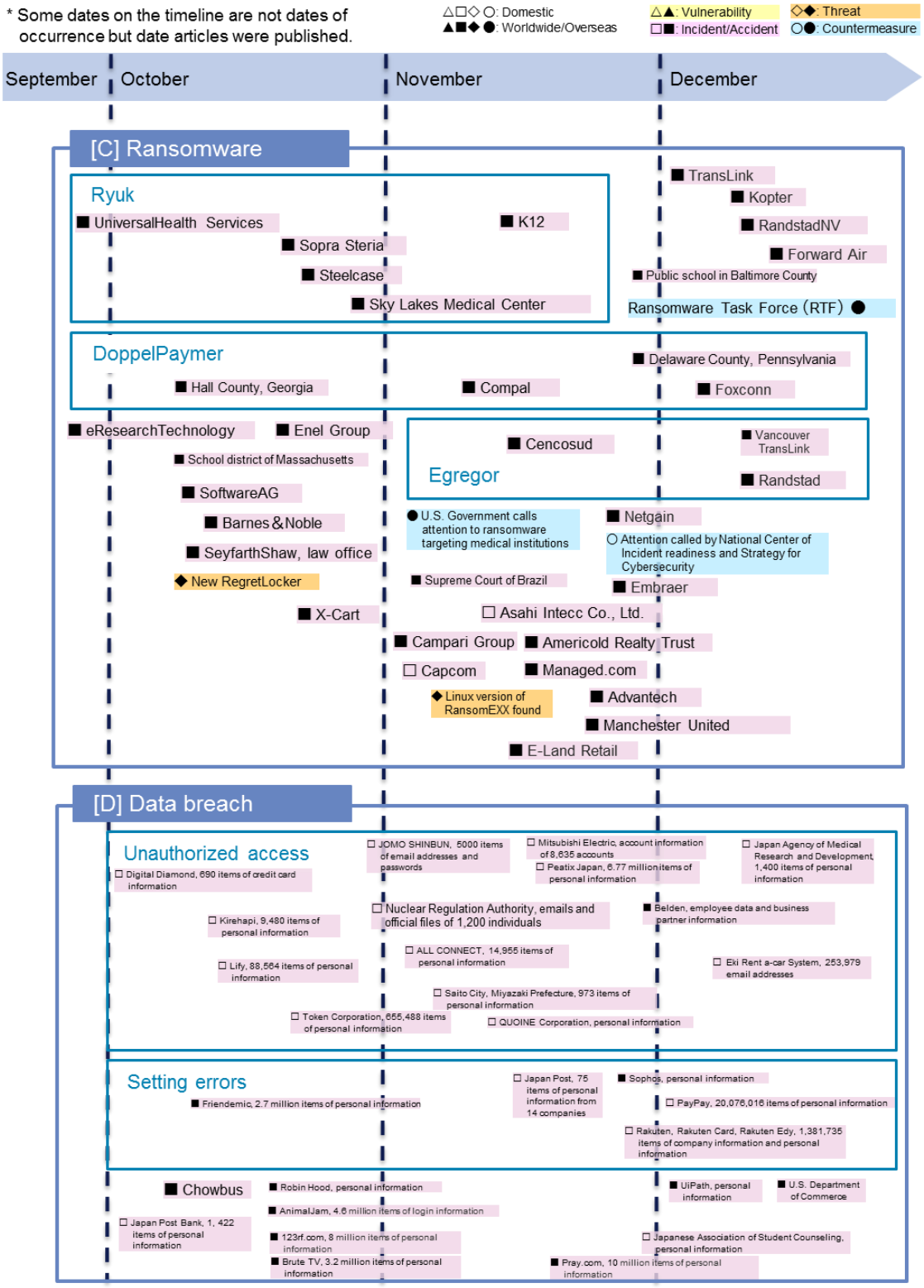
In the third quarter of 2020, there have been a number of data breach incidents attributable to defective setting of Salesforce. These incidents will probably subside if cloud service customers take measures according to the instructions. Simple setting errors can be avoided if the cloud service customers understand the specifications of the cloud service and make correct settings with reference to the information and mechanism provided by the cloud service provider. However, for an incident whose causes also lie with the cloud service provider, such as the incident introduced in this report, the cloud service provider must also provide services in consideration of security risks. Because cloud service providers not taking sufficient measures are considered to exist, incidents similar to those introduced in this report will probably continue to happen. With the continued increase of the use of cloud services due the progression of digital transformation and working practice reform in response to the COVID-19 pandemic, future similar incidents will potentially cause damage on a greater number of companies [103] [104] [105] [106] [107].

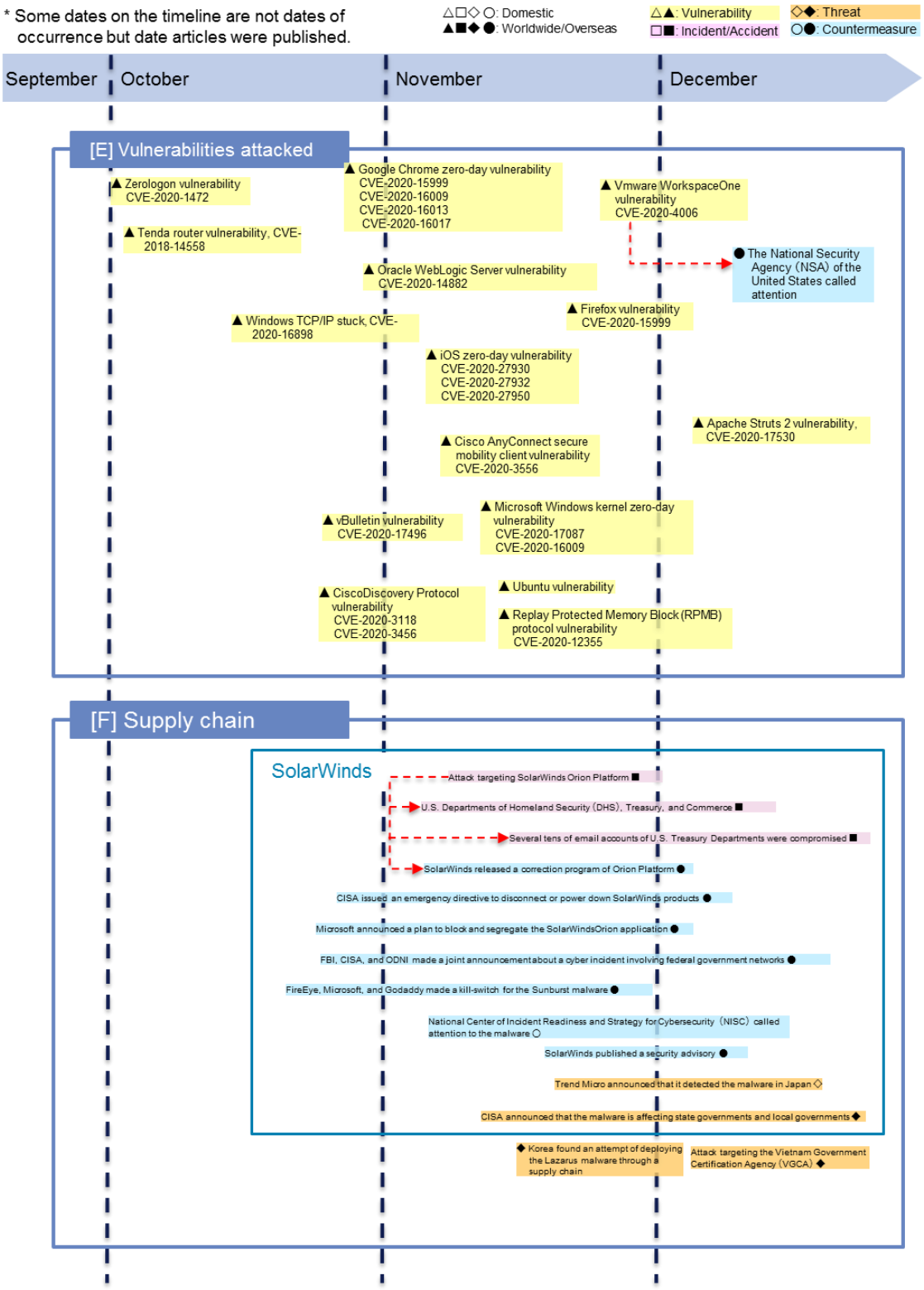
Attack on cryptocurrency

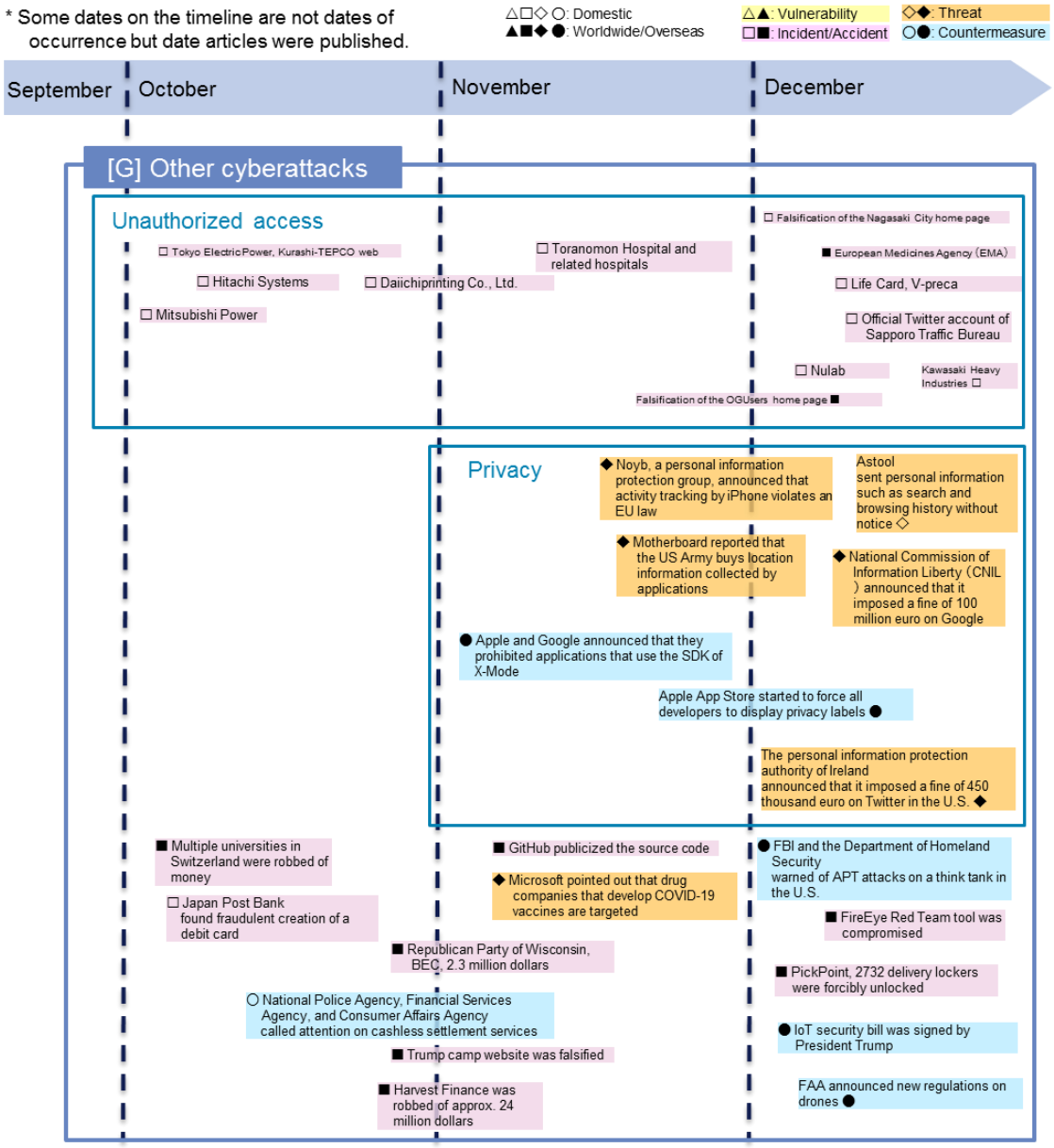
Bitcoin hit a record-high market price on 17 December, 2020. The price continues to be on an upward trend [108]. In May 2019, in which bitcoin was also on an upward trend, a cyberattack on Binance, a major virtual currency exchange, stole 7,000 bitcoin (equivalent to 4.4 billion yen at that time) [109]. The current upward trend of bitcoin with more than twice the value of 2019 may trigger an attack on cryptocurrencies if this situation continues.

7. Timeline









References

[1] Peatix Japan株式会社, “Peatixへの不正アクセス事象に関するお詫びとお知らせ,” 17 11 2020. [オンライン]. Available: https://peatix.com/event/1721625.

[2] 株式会社エブリシング, “弊社委託先への不正アクセスによる「エブリシング」個人情報流出に関するお詫びとお知らせ,” 26 11 2020. [オンライン]. Available: https://everysing.co.jp/2020/11/18/.

[3] 三菱パワー株式会社, “当社ネットワークに対するマネージド・サービス・プロバイダを経由した第三者からの不正アクセスに係る件,” 11 12 2020. [オンライン]. Available: https://power.mhi.com/jp/news/20201211.html.

[4] SolarWinds, Inc, “SolarWinds Security Advisory,” 13 12 2020. [オンライン]. Available: https://www.solarwinds.com/ja/securityadvisory.

[5] 経済産業省, “サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が設立されます,” 30 10 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html.

[6] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威 2020,” 28 8 2020. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2020.html.

[7] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2018年度版 第4四半期）,” 30 5 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2018_4q_securityreport.pdf.

[8] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2019年度版 第2四半期）,” 29 11 2019. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf.

[9] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート（2020年度版 第2四半期）,” 11 12 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/121100/121100-01.pdf.

[10] C. Cimpanu, “Sprint says hackers breached customer accounts via Samsung website,” CBS Interactive., 16 7 2019. [オンライン]. Available: https://www.zdnet.com/article/sprint-says-hackers-breached-customer-accounts-via-samsung-website/.

[11] S. S. R. A. I. Team, “Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks,,” Broadcom., 18 9 2019. [オンライン]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

[12] PEAR, “PEAR公式Twitterアカウント,” 19 1 2019. [オンライン]. Available: https://twitter.com/pear/status/1086634389465956352.

[13] Check Point Software Technologies LTD, “SimBad: A Rogue Adware Campaign On Google Play,” 13 3 2019. [オンライン]. Available: https://research.checkpoint.com/simbad-a-rogue-adwarecampaign-on-google-play/.

[14] AO Kaspersky Lab, “Operation ShadowHammer,” 25 3 2019. [オンライン]. Available: https://securelist.com/operation-shadowhammer/89992/.

[15] C. Cimpanu, “Hackers breach FSB contractor, expose Tor deanonymization project and more,” CBS Interactive, 20 7 2019. [オンライン]. Available: https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/.

[16] LiveAuctioneers, “July 11, 2020 - LiveAuctioneers Account Security,” 7 11 2020. [オンライン]. Available: https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security.

[17] G. Cluley, ““Millions of LiveAuctioneers passwords offered for sale followingdata breach,” 13 7 2020. [オンライン]. Available: https://grahamcluley.com/liveauctioneers-passwords-for-sale/.

[18] サクソバンク証券株式会社, “サイバー攻撃による個人情報流出に関するお詫びとお知らせ,” 17 9 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/personal-information-leakage.

[19] サクソバンク証券株式会社, “個人情報流出についてお客様からお寄せいただいたご質問ならびに回答,” 2020. [オンライン]. Available: https://www.home.saxo/ja-jp/about-us/security-incident/questions-and-answers.

[20] Promo, “Promo Data Breach July 21, 2020 FAQ,” 21 7 2020. [オンライン].

Available: https://support.promo.com/en/articles/4276475-promo-data-breach-july-21-2020-faq.

[21] Bleeping Computer, “Promo.com discloses data breach after 22M user records leaked online,” 27 7 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/promocom-discloses-data-breach-after-22m-user-records-leaked-online/.

[22] 日本経済新聞, “三菱パワーの不正アクセス、日立システムズ経由で侵入,” 12 12 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ121VP0S0A211C2000000.

[23] U.S. Securities and Exchange Commission, “Form 8-K Solarwinds Corp Current report, item 8.01,” [オンライン]. Available: https://sec.report/Document/0001628280-20-017451/. [アクセス日: 14 12 2020].

[24] FireEye, Inc., “Unauthorized Access of FireEye Red Team Tools,” 8 12 2020. [オンライン]. Available: https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

[25] Volexity, Inc., “Dark Halo Leverages SolarWinds Compromise to Breach Organizations,” 14 12 2020. [オンライン]. Available: https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/.

[26] CRN, “SolarWinds CEO: Attack Was ‘One Of The Most Complex And Sophisticated’ In History,” 7 1 2021. [オンライン]. Available: https://cloud.watch.impress.co.jp/docs/topic/special/1301088.html.

[27] 日本経済新聞, “塩野義製薬にサイバー攻撃　台湾現地法人、金銭要求も,” 22 10 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO65325770S0A021C2CR8000.

[28] 読売新聞, “塩野義製薬の台湾現地法人にサイバー攻撃…盗まれた情報の一部がネットに公開,” 23 10 2020. [オンライン]. Available: https://www.yomiuri.co.jp/national/20201023-OYT1T50124/.

[29] BLEEPINGCOMPUTER, “Enel Group hit by ransomware again, Netwalker demands $14 million,” 27 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/.

[30] DZNet, “Italian beverage vendor Campari knocked offline after ransomware

attack,” 5 11 2020. [オンライン]. Available: https://www.zdnet.com/article/italian-beverage-vendor-campari-knocked-offline-after-ransomware-attack/.

[31] 朝日新聞デジタル, “カプコンへのサイバー脅迫　記者はちらつく影を追った,” 12 11 2020. [オンライン]. Available: https://digital.asahi.com/articles/ASNCD3DNQNCCULZU00J.html.

[32] 独立行政法人情報処理推進機機構 セキュリティセンター, “事業継続を脅かす新たなランサムウェア攻撃について,” 20 8 2020. [オンライン]. Available: https://www.ipa.go.jp/files/000084974.pdf.

[33] 株式会社カプコン, “不正アクセスによる情報流出に関するお知らせとお詫び,” 16 11 2020. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/201116.html.

[34] 株式会社カプコン, “不正アクセスによる情報流出に関するお知らせとお詫び【第3報】,” 12 1 2021. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/210112.html.

[35] 株式会社カプコン, “不正アクセスによるシステム障害発生に関するお知らせ,” 4 11 2020. [オンライン]. Available: https://www.capcom.co.jp/ir/news/html/201104.html.

[36] BLEEPING COMPUTER, “Capcom hit by Ragnar Locker ransomware, 1TB allegedly stolen,” 5 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/.

[37] アサ芸Biz, “個人情報の身代金を支払い拒否！「カプコン」の強硬姿勢が称賛されたワケ,” 19 11 2020. [オンライン]. Available: https://news.nifty.com/article/economy/business/12277-866199/.

[38] ITmedia, “カプコン情報流出、ロシア周辺国が関与の可能性,” 24 11 2020. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2011/24/news045.html.

[39] NHK, “ハローカプコン！暴露型サイバー攻撃の衝撃,” 23 12 2020. [オンライン]. Available: https://www3.nhk.or.jp/news/special/sci_cul/2020/12/special/20201223capcom/.

[40] Security NEXT, “凶暴性増すランサムウェアの裏側 - 今すぐ確認したい「意外な設定」,” 12 11 2020. [オンライン]. Available: https://www.security-

next.com/120578.

[41] キヤノンITソリューションズ, “手頃な値段でランサムウェアを販売する業者がいる,” 11 7 2018. [オンライン]. Available: https://ascii.jp/elem/000/001/705/1705420/.

[42] 日本経済新聞, “クラウドストライク、2020年度版グローバルセキュリティ意識調査結果を発表,” 26 11 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXLRSP600746_W0A121C2000000/.

[43] DZNet Japan, “ランサムウェアの身代金支払い額、日本は平均で約1億2300万円,” 26 11 2020. [オンライン]. Available: https://japan.zdnet.com/article/35162969/.

[44] CROWDSTRIKE, “2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY,” [オンライン]. Available: https://www.crowdstrike.com/resources/reports/global-attitude-survey-2020/.

[45] 大元隆志 | クラウドセキュリティアナリスト/国士舘大学経営学部非常勤講師, “ランサムウェアの被害にあったら、身代金を支払うべきか?,” 18 11 2020. [オンライン]. Available: https://news.yahoo.co.jp/byline/ohmototakashi/20201118-00208356/.

[46] BLEEPING COMPUTER, “US govt warns of sanction risks for facilitating ransomware payments,” 1 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-govt-warns-of-sanction-risks-for-facilitating-ransomware-payments/.

[47] Digital Keeper, “【2021年最新】進化したランサムウェアの被害を防ぐ対策とは～身代金は支払うべきか？,” 13 1 2021. [オンライン]. Available: https://keepmealive.jp/ransomware-protection/.

[48] DRS, “ランサムウェアの身代金支払いへの勧告と制裁に関する米国事情,” 20 1 2021. [オンライン]. Available: https://www.drs.co.jp/column/security/20210120_100000.html.

[49] DZNet, “全米市長会議、ランサムウェア攻撃で身代金支払い拒否へ--年次総会で決議採択,” 16 7 2019. [オンライン]. Available: https://japan.zdnet.com/article/35139937/.

[50] 経済産業省, “最近のサイバー攻撃の状況を踏まえた経営者への注意喚起,” 18 12 2020. [オンライン]. Available: https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf.

[51] 内閣サイバーセキュリティセンター, “ランサムウエアによるサイバー攻撃について【注意喚起】,” 26 11 2020. [オンライン]. Available: https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf.

[52] 独立行政法人 情報処理推進機構, “事業継続を脅かす新たなランサムウェア攻撃について,” 20 8 2020. [オンライン]. Available: https://www.ipa.go.jp/files/000084974.pdf.

[53] MITRE, “MITRE ATT&CK,” [オンライン]. Available: https://attack.mitre.org/.

[54] PayPay株式会社, “当社管理サーバーのアクセス履歴について,” 7 12 2020. [オンライン]. Available: https://paypay.ne.jp/notice/20201207/02/.

[55] 楽天株式会社, “クラウド型営業管理システムへの社外の第三者によるアクセスについて,” 25 12 2020. [オンライン]. Available: https://corp.rakuten.co.jp/news/update/2020/1225_01.html.

[56] 日経クロステック, “楽天だけでなくPayPayでも、セールスフォース製品の設定不備を狙った不正アクセス,” 26 12 2020. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09412/.

[57] 日経クロステック, “楽天とPayPayがつまずいたセールスフォース製品の「設定不備」、被害は氷山の一角か,” 22 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/column/18/00989/012000044/.

[58] 日経クロステック, “セールスフォース製品「設定不備」による不具合続々、バンダイや日本政府観光局でも,” 1 2 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09570/.

[59] 日経クロステック, “金融庁の注意喚起で金融機関が対応急ぐ、セールスフォース製品への不正アクセスで,” 29 12 2020. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09416/.

[60] 日経クロステック, “NISCが「セールスフォース製品の設定不備」に注意促す、楽天などで不正アクセス,” 30 1 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/news/18/09560/.

[61] 株式会社セールスフォース・ドットコム, “Salesforceサイトおよびコミュニティにおけるゲストユーザのアクセス制御の権限設定について,” 21 2 2021. [オンライン]. Available: https://www.salesforce.com/jp/company/news-press/stories/salesforce-update/.

[62] 日本クラウドセキュリティアライアンス, “クラウドにおけるセキュリティサービスの効果的な管理のガイドライン,” 21 2 2021. [オンライン]. Available:

https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/09/Guideline-on-Effectively-Managing-Security-Service-in-the-Cloud-06_02_19_J_FINAL.pdf.

[63] The CentOS Project, “About/Product - CentOS Wiki,” The CentOS Project, 12 12 2020. [オンライン]. Available: https://wiki.centos.org/About/Product.

[64] アドビ株式会社, “Adobe Flash Player End of Life,” アドビ株式会社, 13 1 2021. [オンライン]. Available: https://www.adobe.com/jp/products/flashplayer/end-of-life.html.

[65] ファイア・アイ株式会社, “FireEye Red Team のツールに対する不正アクセスに関して | FireEye Inc,” ファイア・アイ株式会社, 9 12 2020. [オンライン]. Available: https://www.fireeye.com/blog/jp-threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

[66] WatchGuard Technologies, Inc., “FireEye の侵害は SolarWinds へのサプライチェーンハッキングが原因,” WatchGuard Technologies, Inc., 14 12 2020. [オンライン]. Available: https://www.watchguard.co.jp/security-news/solarwinds-supply-chain-hack-responsible-for-fireeye-breach.html.

[67] FireEye, Inc., “red_team_tool_countermeasures CVEs_red_team_tools.md,” FireEye, Inc., 9 12 2020. [オンライン]. Available: https://github.com/fireeye/red_team_tool_countermeasures/blob/master/CVEs_red_team_tools.md.

[68] 株式会社カスペルスキー, “WannaCry：情報まとめ,” 株式会社カスペルスキー, 18 5 2017. [オンライン]. Available: https://blog.kaspersky.co.jp/wannacry-faq-what-you-need-to-know-today/15594/.

[69] E. Moyer, “Stolen NSA hacking tool now victimizing US cities, report says,” CNET, A RED VENTURES COMPANY., 25 5 2019. [オンライン]. Available: https://www.cnet.com/news/stolen-nsa-hacking-tool-now-victimizing-us-cities-report-says/.

[70] 独立行政法人情報処理推進機構, “脆弱性対策情報データベースJVN iPediaの登録状況 [2020年第4四半期（10月～12月）]：IPA 独立行政法人 情報処理推進機構,” 独立行政法人情報処理推進機構, 20 1 2021. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/report/JVNiPedia2020q4.html.

[71] 株式会社ブロードバンドセキュリティ, 株式会社イード, “厳しい条件のもとでも高い意識で脆弱性管理に取り組む「一人情シス」たち ～ 日本企業の脆弱性管理実態探る５００名調査実施,” 23 10 2020. [オンライン]. Available:

https://www.bbsec.co.jp/news/pdf/20201023.pdf.

[72] National Institute of Standards and Technology, “Special Publication 800-40 Version 2.0 Creating a Patch and Vulnerability Management Program,” 11 2005. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-40ver2.pdf.

[73] 独立行政法人情報処理推進機構, “セキュリティ担当者のための脆弱性対応ガイド 第3版第2刷,” 3 2017. [オンライン]. Available: https://www.ipa.go.jp/files/000058493.pdf.

[74] 独立行政法人情報処理推進機構, “脆弱性対策の効果的な進め方（ツール活用編）～ 脆弱性検知ツール Vuls を利用した脆弱性対策 ～,” 21 2 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000071584.pdf.

[75] 独立行政法人情報処理推進機構, “脆弱性対策の効果的な進め方（実践編）第2 版～脆弱性情報の早期把握、収集、活用のスヽメ～,” 21 2 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000071660.pdf.

[76] 独立行政法人情報処理推進機構, “共通脆弱性評価システムCVSS v3概説,” 独立行政法人情報処理推進機構, 1 12 2015. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/CVSSv3.html.

[77] SANS Institute, “More TA551 (Shathak) Word docs push IcedID (Bokbot),” 14 10 2020. [オンライン]. Available: https://isc.sans.edu/forums/diary/More+TA551+Shathak+Word+docs+push+IcedID+Bokbot/26674/.

[78] JPCERT/CC 分析センター公式Twitterアカウント, 6 11 2020. [オンライン]. Available: https://twitter.com/jpcert_ac/status/1324561915738091522.

[79] Check Point Software Technologies Ltd., “December 2020’s Most Wanted Malware: Emotet Returns as Top Malware Threat,” 7 1 2021. [オンライン]. Available: https://blog.checkpoint.com/2021/01/07/december-2020s-most-wanted-malware-emotet-returns-as-top-malware-threat/.

[80] Bleeping Computer LLC, “Watch out for Emotet malware's new 'Windows Update' attachment,” 18 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/watch-out-for-emotet-malwares-new-windows-update-attachment/.

[81] 独立行政法人情報処理推進機構, “「Emotet」と呼ばれるウイルスへの感染を狙

うメールについて,” 22 12 2020. [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[82] 一般社団法人JPCERTコーディネーションセンター, “マルウエアEmotetへの対応FAQ,” 23 12 2020. [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html.

[83] 株式会社ラック, “分析レポート：Emotetの裏で動くバンキングマルウェア「Zloader」に注意,” 25 11 2020. [オンライン]. Available: https://www.lac.co.jp/lacwatch/people/20201106_002321.html.

[84] トレンドマイクロ株式会社, “「EMOTET」に続き「IcedID」の攻撃が本格化の兆し、パスワード付き圧縮ファイルに注意,” 9 11 2020. [オンライン]. Available: https://blog.trendmicro.co.jp/archives/26656.

[85] マクニカネットワークス株式会社, “IceID /IcedIDマルウェアへの対応について,” 12 11 2020. [オンライン]. Available: https://mnc.macnica.net/2020/11/iceid.html.

[86] トレンドマイクロ株式会社, “緊急セキュリティ速報：マルウェア「IcedID」に注意,” 10 11 2020. [オンライン]. Available: https://www.trendmicro.com/ja_jp/about/announce/announces-20201110-01.html.

[87] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “Ransomware Activity Targeting the Healthcare and Public Health Sector,” 28 10 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector.

[88] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data,” 10 12 2020. [オンライン]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-345a.

[89] Bleeping Computer LLC, “Massachusetts school district shut down by ransomware attack,” 8 10 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/massachusetts-school-district-shut-down-by-ransomware-attack/.

[90] Security Affairs by Pierluigi Paganini, “Leading Law firm Seyfarth Shaw discloses ransomware attack,” 13 10 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/109435/malware/seyfarth-shaw-ransomware-attack.html.

[91] Security Affairs by Pierluigi Paganini, “U.S. Bookstore giant Barnes & Noble hit by cyberattack,” 15 10 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/109511/hacking/barnes-noble-cyber-attack.html.

[92] 京セラ株式会社, “弊社を装った不審メールと個人情報等の流出の可能性に関するお詫びとお知らせ,” 16 10 2020. [オンライン]. Available: https://www.kyocera.co.jp/information/2020/1001_alpf.html.

[93] 学校法人関西医科大学, “本学職員を装った不審メールについてのお知らせとお詫び,” 30 10 2020. [オンライン]. Available: http://www.kmu.ac.jp/news/20201030_Emotet.html.

[94] Bleeping Computer LLC, “Campari hit by Ragnar Locker Ransomware, $15 million demanded,” 5 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/campari-hit-by-ragnar-locker-ransomware-15-million-demanded/.

[95] Bleeping Computer LLC, “Capcom: 390,000 people may be affected by ransomware data breach,” 12 1 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/.

[96] 株式会社アイロベックス, “【重要なお知らせ】不正アクセスの影響によるご迷惑をおかけしたことのお詫び,” 25 12 2020. [オンライン]. Available: https://www.ilovex.co.jp/event/20201225/ilovex20201225_release.pdf.

[97] Bleeping Computer LLC, “Baltimore County Public Schools hit by ransomware attack,” 25 11 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/baltimore-county-public-schools-hit-by-ransomware-attack/.

[98] Bleeping Computer LLC, “Foxconn electronics giant hit by ransomware, $34 million ransom,” 7 12 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/.

[99] Security Affairs by Pierluigi Paganini, “K12 education giant paid the ransom to the Ryuk gang,” 2 12 2020. [オンライン]. Available: https://securityaffairs.co/wordpress/111824/malware/k12-ryuk-ransomware.html.

[100] Security Affairs by Pierluigi Paganini, “A ransomware attack hit the Greater Baltimore Medical Center,” 7 12 2020. [オンライン]. Available:

https://securityaffairs.co/wordpress/112017/malware/greater-baltimore-medical-center-ransomware.html.

[101] WellBe Holdings Limited, “ウイルスメール感染に関するお詫びと注意喚起,” 16 12 2020. [オンライン]. Available: http://wellbemedic.com/topics/detail/post_86.html.

[102] Bleeping Computer LLC, “Emotet malware hits Lithuania's National Public Health Center,” 30 12 2020. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/.

[103] IDC Japan 株式会社, “国内パブリッククラウドサービス市場予測を発表,” IDC Japan 株式会社, 14 9 2020. [オンライン]. Available: https://www.idc.com/getdoc.jsp?containerId=prJPJ46845820.

[104] Gartner, Inc., “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020,” Gartner, Inc., 13 11 2019. [オンライン]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020.

[105] 佐藤由紀子, “Microsoftの10～12月決算、コロナ禍で売上高・純利益ともに過去最高,” アイティメディア株式会社, 27 1 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2101/27/news079.html#:~:text=Azure%E3%82%84%E3%82%B5%E3%83%BC%E3%83%90%E3%83%BC%E8%A3%BD%E5%93%81%E3%82%92,146%E5%84%84%E3%83%89%E3%83%AB%E3%81%A0%E3%81%A3%E3%81%9F%E3%80%82.

[106] 佐藤由紀子, “Amazon.com、巣ごもり需要による大幅増収増益で過去最高に,” アイティメディア株式会社, 3 2 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2102/03/news061.html#:~:text=2021%E5%B9%B4%E7%AC%AC1%E5%9B%9B%E5%8D%8A%E6%9C%9F,%E3%81%AF%E5%89%B5%E6%84%8F%E3%81%AE%E4%BC%81%E6%A5%AD%E3%81%A0%E3%80%82.

[107] R. Nieva, “Google discloses more on cloud business as it looks beyond search,” CNET, A RED VENTURES COMPANY. , 2 2 2021. [オンライン]. Available: https://www.cnet.com/news/google-discloses-more-on-cloud-business-as-it-looks-beyond-search/.

[108] V. Hajric, “最高値更新続いたビットコイン、21年は規制当局の監視強まる可能性,” Bloomberg L.P., 28 12 2020. [オンライン]. Available:

https://www.bloomberg.co.jp/news/articles/2020-12-28/QM03DST1UM0X01.

[109] Binance.com., “Binance Security Breach Update,” Binance.com., 8 5 2019. [オンライン]. Available: https://www.binance.com/en/support/articles/360028031711.

[110] The Hacker News, “Software Supply-Chain Attack Hits Vietnam Government Certification Authority,” 17 12 2020. [オンライン]. Available: https://thehackernews.com/2020/12/software-supply-chain-attack-hits.html.

[111] 防衛相, “三菱電機㈱による機微な情報の漏えいの可能性について,” 10 2 2020. [オンライン]. Available: https://www.mod.go.jp/j/press/news/2020/02/10a.pdf.

[112] 日本電気株式会社, “当社の社内サーバへの不正アクセスについて,” 31 1 2020. [オンライン]. Available: https://jpn.nec.com/press/202001/20200131_01.html.

[113] Data Centre Dynamics Ltd (DCD), “Tech companies like Intel, Nvidia, Microsoft, and Cisco installed SolarWinds malware,” 23 12 2020. [オンライン]. Available: https://www.datacenterdynamics.com/en/news/tech-companies-intel-nvidia-microsoft-and-cisco-installed-solarwinds-malware/.

[114] 独立行政法人情報処理推進機構, “情報セキュリティ5か条,” 19 3 2019. [オンライン]. Available: https://www.ipa.go.jp/files/000055516.pdf.

[115] J. LEMON, “Alleged Russian SolarWinds Hack 'Probably an 11' On Scale of 1 to 10, Cybersecurity Expert Warns,” Newsweek, 24 12 2020. [オンライン]. Available: https://www.newsweek.com/alleged-russian-solarwinds-hack-probably-11-scale-1-10-cybersecurity-expert-warns-1554606.

NTT DATA
Trusted Global Innovator

Published on Tuesday, March 16, 2021

NTT DATA Corporation
Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Ryo Hoshino / Akihiro Ito / Yohei Ozawa / Daisuke Miyazaki / Jun Kinoshita / Tsutomu Nakamura / Yuki Fukuda
nttdata-cert@kits.nttdata.co.jp