NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

4th Quarter of 2020

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary 2
2. Featured Topics 4
2.1. Revision of Personal Information Protection Law 4
2.1.1. Introduction—Summary of Revision of Personal Information Protection Law 4
2.1.2. Impact of the revision on business operators that transfer personal data to overseas locations 5
2.1.3. Overseas transfer of personal information by LINE Corporation 8
2.1.4. Treatment of personal information that corporations use and provision of information to users 12
2.1.5. Impact of toughened penalties on responses to be made by corporations 13
2.1.6. Conclusion 14
2.2. Embezzlement from customers' accounts by a member of securities trading system development team 15
2.2.1. Details of the incident 15
2.2.2. Distinctive feature of the incident 17
2.2.3. Countermeasures 19
2.2.4. Conclusion 21
3. Data Breach 22
3.1. Data Breach on SITA 22
3.1.1. Overview 22
3.1.2. Causes and countermeasures of information theft from an entrustee 23
3.1.3. Legal system applied to overseas entrustees 23
3.1.4. Comparison of media reports on SITA and LINE Corporation 24
3.2. Data breach through Salesforce (continued report) 24
3.3. Conclusion 26
4. Vulnerability 27
4.1. Vulnerabilities of Microsoft Exchange Server 27
4.2. Timeline 28
4.3. Attacking steps and countermeasures 28
4.4. Conclusion 29
5. Malware/Ransomware 30
5.1. Summary of the 4th quarter of 2020 30
5.2. Emotet takedown operation (Operation LadyBird) 30

5.2.1. Takedown of Emotet through international cooperation 30
5.2.2. Activities after the takedown of Emotet 31
5.3. Recent trend of smishing 32
5.3.1. Current status of smishing damage 32
5.3.2. Types of smishing 33
5.3.3. Countermeasures against smishing 34
5.4. Conclusion 35
6. Outlook 36
7. Timeline 38
References 42

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.

Enforcement of revised Personal Information Protection Law

The revised Personal Information Protection Law will be enforced in 2022. The revised law changes the treatment of personal data transferred to overseas locations in response to the increased overseas transfer of personal data due to the globalization and digitalization of corporate activities. In March this year, the media reported that the personal data possessed by LINE Corporation was stored at an overseas location. The Personal Information Protection Committee pointed out that LINE Corporation, on the grounds of the current Personal Information Protection Law, did not conduct sufficient supervision of its overseas entrustees. Also, there are some points LINE Corporation must take action on according to the revised law, although the current law does not require such action. In this report, we describe the difference between the old and new Personal Information Protection Laws about the overseas transfer of personal data and actions to be taken by corporations, taking the example of the LINE Corporation case. For a corporation to handle personal information properly, the corporation must have an organization for the management of personal information and must practice proper management methods. For this purpose, activities based on JIS Q 15001 (Management System for Personal Information Protection—Requirements) are effective. A corporation can acquire the Privacy Mark to make known their corporate compliance with JIS Q 15001 and its efforts for personal information protection.

Embezzlement from customers' accounts by a member of securities trading system development team

Matsui Securities Co., Ltd. announced that a former employee of an entrustee of the development and operation of a securities trading system unlawfully withdrew about 200 million yen from customers' securities accounts. This incident took two and a half years from the start of the criminal act to its discovery. Several factors have been found that prevented the criminal act from being discovered for a long time. In this paper, we will look into the details of this incident to describe security measures that should be taken by operation and development departments that engage in financial systems. Also, we will propose methods for preventing damage and prompt the finding of incidents from the viewpoint of customers.

Vulnerability of Microsoft Exchange Server

Microsoft released a non-regular security update program in March 2021. The vulnerabilities allowed attackers to have access to normally inaccessible Exchange Servers through port 443 from another server, break authentication, and impersonate an administrator.

Among seven vulnerabilities, four were zero-day vulnerabilities, which had been exploited by attacking groups and ransomware attacks actually causing damage before the release of the update program. A large number of Exchange Servers had been identified that had not been amended. They may already have suffered attacks. Quick action is required.

Outlook

Marriage hunting site "Omiai" had an incident of the leak of user identification documents including drivers' licenses. It is expected that the attacker will fabricate pictures of drivers' licenses from the stolen data to impersonate different individuals.

Many fraudulent acts have been identified related to COVID-19 vaccinations. Vaccination-related attacks are expected on a wider range of age groups from June, in which the vaccination target ages will be broadened.

The trend of policies for ransomware attacks is to prohibit paying ransoms. An example is a recommendation made by the Office of Foreign Assets Control of the U.S. Treasury (OFAC). However, as long as information disclosure has big damage on victim organizations, cases of paying ransom are expected to continue.

2. Featured Topics

2.1. Revision of Personal Information Protection Law

2.1.1. Introduction—Summary of Revision of Personal Information Protection Law

The Personal Information Protection Law is reviewed every three years, and a revised Personal Information Protection Law will be enforced in 2022. In this revision, the following six points listed in Table 1 are revised [1].

Table 1：Summary of revision of Personal Information Protection Law

Revised point	Description
1. Rights of individuals	• Enhancement of rights of individuals concerning the request of suspension of use, erasure, etc. • Allowing individuals to specify the way their personal data is made open on the Internet and other means • Allowing individuals to request the disclosure of the third-party-provided record on the exchange of their personal data • Inclusion of possessed personal data as short-term storage data that are to be erased within six months, and making such data subject to disclosure and suspension of use • Opt-out provision that restricts the scope of personal data to be provided to third parties
2. Responsibility of business operators	• Duty of business operators to report to the Personal Information Protection Committee and to notify the affected individuals when rights of individuals may be compromised due to leak of sensitive personal information or information leak by unauthorized access • Clarified prohibition of the use of personal information in improper ways that support unlawful or unjust behaviors
3. Mechanism of encouraging business operators to make spontaneous efforts	• Enhancement of the current certification institution system by enabling certification institutions to grant certification to specific sections (departments) of corporations
4. Use of data	• Relaxation of duties of disclosure, response to requests for usage suspension, etc., on the condition that the data is used only for internal analysis through anonymization of the data by erasing names and other identities

	• Duty of obtaining the consent of individuals when providing the data that is not considered personal data by the party that provides the data but is expected to be considered personal data by the third party that receives the data
5. Penalty	• Raising the level of criminal penalties for the violation of a directive from the committee and false report to the committee • Raising the maximum amount of penalties on legal parties that violate directives
6. Application of the law beyond the national border and transfer of information across the national border	• Making overseas business operators that handle personal information of domestic residents subject to reporting and directives with violation penalties • Enhancement of information provision and other duties related to the handling of personal information by third parties, for the case when personal information is transferred to third parties located in overseas countries

Source: Personal Information Protection Committee [1]

In March 2021, the media reported that user information of LINE Corporation was viewable from outside Japan and part of the user information was stored at an overseas location. This media report attracted public attention about how the transfer of personal data across the border should be. In this report, we explain how personal data should be handled when it is transferred to a third party across the border by considering the incident of LINE Corporation in view of the old and new versions of "6. Application of the law beyond the national border and transfer of information across the national border" (article 24, Act on the Protection of Personal Information). Details of the revision of the law including guidelines are not fixed yet. So, this report describes the revision of the law based on the direction of discussion publicized at this point.

2.1.2. Impact of the revision on business operators that transfer personal data to overseas locations

The revised Personal Information Protection Law has two changes described in Table 2 about "application of the law beyond the national border and transfer of information across the national border."

Table 2：Changes in the application of the law beyond the national border and transfer of information across the national border

No.	Description
(1)	Making overseas business operators that handle personal information of domestic residents subject to reporting and directives with violation penalties
(2)	Enhancement of information provision and other duties about the handling of personal information by third parties, for the case when personal information is

	transferred to third parties located in overseas countries

(1) of Table 2 makes an overseas corporation subject to penalties of the law if the corporation handles personal data of domestic residents. The current law allows authorities only to make non-binding instructions and recommendations, while the revised law allows authorities to collect reports and issue directives, as well as to publicize the fact of violation if the violating corporation does not observe the directive.

Revision (2) has an impact on domestic corporations that transfer personal data to overseas locations. Related cases include, for example, transferring employee data collected in Japan to an overseas BPO company and transferring customer data collected in Japan to the overseas parent company. The handling of personal information that LINE Corporation collected is subject to the revision (2).

Both the current and revised laws mandate three conditions for providing personal data to third parties in overseas countries: (a) first-person informed consent, (b) business operator that has the compliant organization, and (c) country that has the same level of regulations, as shown in Figure 1. To provide personal data to a third party in an overseas country, one of the three conditions must be satisfied.

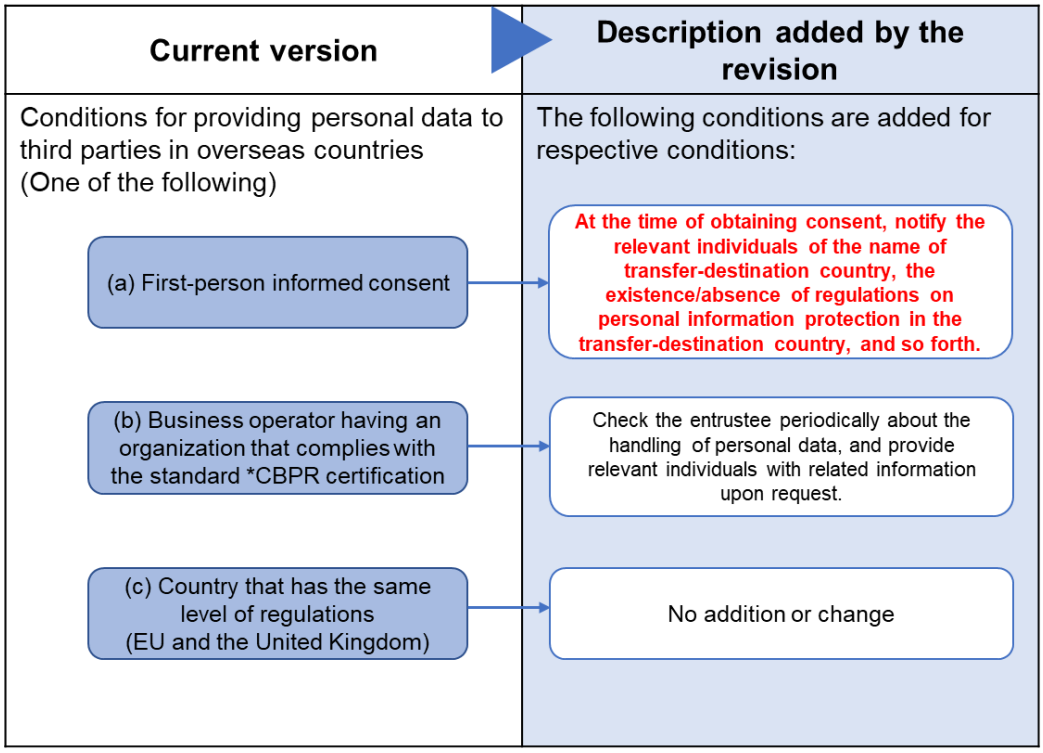


Figure 1: Revision of conditions for providing personal data to third parties in overseas countries [2] (source text with some modification by the author of this report)

Business operators that satisfy condition (b) of Figure 1 include business operators that have acquired the certification of CBPR (Cross Border Privacy Rules: APEC cross border

privacy rule system). As of May 2021, two corporations have acquired CBPR [3]. Countries and regions that satisfy condition "(c) country that has the same level of regulations" include the EU and the United Kingdom. In January 2019, the EU and the United Kingdom granted Japan with sufficiency acknowledgment based on article 45 of GDPR (General Data Protection Regulation) [4] [5]. In other words, Japan, the United Kingdom, and the EU mutually acknowledge the sufficiency of personal data protection. This point does not change by the revision.

The condition that significantly changed because of the revision is (a) first-person informed consent. The current law requires *business operators to obtain first-person informed consent to the provision of personal data to third parties in overseas countries before business operators do so*. The revised law requires, *in addition to the condition of the current law, business operators to provide the relevant individuals with information on regulations of personal information protection enforced in the relevant countries, personal information protection measures taken by business operators to which personal information is transferred, and other relevant information, when obtaining first-person informed consent* [6]. Details are being studied at this point in time, but the content of information to be provided at the time of obtaining first-person consent (Table 3) is described in *Discussion Points in Defining Ordinances and Regulations (Enhancement of Cross-Border Information Provision)* issued by the Personal Information Protection Committee in November 2020 [7].

Table 3：Information that the revised law requires to provide to relevant individuals (summary)

Revised point	Information to be provided to relevant individuals (considered outline)
(a) Regulations related to the protection of personal information enforced in the relevant country	• Information with the content and granularity that enables the identification of essential differences from the Personal Information Protection Law of Japan • Summary of regulations enforced in overseas countries is to be published by the Personal Information Protection Committee for business operators for reference
(b) Measures taken by relevant third parties for the protection of personal information	• Information that enables the identification of essential differences from measures required to be taken by business operators in Japan for the handling of personal data • In cases when the provision of information of measures taken by the third party for the protection of personal information is difficult at the time of obtaining first-person consent, information on the fact and reason of the difficulty should be provided.
(c) Other relevant information	• Name of the country that the third party to which the information is transferred is located in • In cases when the country to which the information is transferred cannot be identified, it is recommended that the corporation provides the information of the region of the country or provides information upon a first-person request if the country is identified at a later time.

The point considered important in (a), (b), and (c) is to let the relevant individuals know properly of risks in cross-border transfer of their personal data. The business operator must explain to relevant individuals which country the personal data is transferred to, what regulations there are for the protection of personal information in that country, and what measures are taken by the transferred-to business operator for the handling of personal

information.

2.1.3. Overseas transfer of personal information by LINE Corporation

In this section, we explain the difference between the Personal Information Protection Laws before and after the revision about the cross-border transfer of personal data, with the example of the March 2021 media report on problems in the handling of personal information by LINE Corporation. LINE Corporation, now offering a nationwide infrastructure, posed a social problem through many media reports. In this report, we explain the incident from the viewpoint of the Personal Information Protection Law and what to be observed with regard to the revised Personal Information Protection Law, although the incident also attracted public attention from the viewpoints of security and the Telecommunications Business Act.

In March 2021, an affiliate company of LINE Corporation located in China was able to access the personal data of users in Japan in order to develop services and monitor some contents. Also, the media reported that all photos and videos of posted talks in Japan were stored in servers of NAVER Corporation, a major company in Korea. According to these media reports, there may have been three problems as described in Table 4

Table 4：Three problems in cross-border transfer of personal information by LINE Corporation

No.	Description of problem
Problem 1	Personal data may have been entrusted to an overseas company without sufficient explanation to users.
Problem 2	Supervision of the overseas entrustee may have been insufficient.
Problem 3	Measures taken for storing personal data (pictures and videos) in the overseas cloud service may have been insufficient.

In the following sections, we explain problems 1, 2, and 3 of Table 4 in terms of the current and revised laws. Among matters that do not pose a problem in terms of the current law, we explain those that do pose a problem in terms of the revised law.

2.1.3.1 Problem 1: Insufficient explanation to LINE users about the cross-border transfer of personal information

LINE Corporation announced that the personal information policy presented to LINE users states that *personal information may be transferred abroad with the users' consent or with the compliance with the law*. However, LINE Corporation did not mention which country the information is transferred to in what situations [8].

The current law as of March 2021 stipulates that the business operator must take advanced action such as explaining to and obtaining consent from relevant individuals when providing personal data to a third party (including an entrustee) in an overseas country, but the law

does not require the disclosure of the name of the country to which the information is transferred. To be more specific, item 9-2 of the Q&A of the guideline of the Personal Information Protection Law states, "When obtaining the consent of relevant individuals about providing personal information to a third party in an overseas country, the way of obtaining the consent must be appropriate and rational for the relevant individuals to make a decision on the consent. Examples of ways of obtaining consent include indicating the name of the country and indicating the situation in which the personal information is provided to the third party in an overseas country." [9] However, as written by Mr. Sawaki, Q&A of the Personal Information Protection Law Revised in 2020, states, "The name of the relevant country and the regulations on the protection of personal information enforced in the relevant country were not always required to be disclosed," indicating that the requirements of the current law had limited effect [10]. In view of this statement, the current law did not require the disclosure of the name of the country to the relevant individuals.

Therefore, the LINE Corporation incident is unlikely to violate the current law in terms of the provision of personal information to a third party in an overseas country. On April 23, 2021, in the announcement by the Personal Information Protection Committee about *administrative responses based on the Act on the Protection of Personal Information*, the committee pronounced that it was hard to say that the users could not understand the situation in which the personal information was provided to a third party in an overseas country because the privacy policy about the first-person informed consent stated the use purposes of the users' personal information (provision and improvement of services, development and improvement of contents, and prevention of unauthorized use) and the provision of the information to a third party entrustee in an overseas country [11]. The Personal Information Protection Committee pronounced that problem 1 of Table 4 is not subject to accusation.

For cases in which messages or other personal information are obtained through LINE services, the Personal Information Protection Committee directed LINE Corporation to clearly notify users of the scope of personal information obtained and to establish a system for ensuring the proper display of such notifications. This directive was considered to have been issued for reasons that information handled by LINE Corporation has high confidentiality and the amount of personal data is large, although the incident does not violate the law.

What if the revised law was applied to the incident of LINE Corporation? According to the revised law, information listed in Table 5 below must be provided to relevant individuals in accordance with revisions (a), (b), and (c) listed in Table 3. China and Japan do not mutually acknowledge the sufficiency as it is with GDPR of the EU and the Personal Information Protection Law of Japan. Therefore, differences between China and Japan must be stated about (a) Regulations related to the protection of personal information enforced in the relevant country. If a business operator cannot find the difference, it may wait for the summary of regulations of overseas countries that will be publicized by the Personal Information Protection Committee for business operators for reference.

Table 5：Information that LINE Corporation should provide according to revised Law

Revised point	Information that should be provided to relevant individuals about personal information transferred to a third party in an overseas country, with the revised law applied to the case of LINE Corporation
(a) Regulations related to the protection of personal information enforced in the relevant country	Description of differences between the law for the protection of personal information of China (where the entrustee is based) and the Personal Information Protection Law of Japan The description may need to include the possibility of the intervention in personal data by the Chinese government.
(b) Measures taken by relevant third parties for the protection of personal information	Description of the actual policy of the entrustee on the handling of personal information including those that are the same as LINE Corporation and those unique to the entrustee
(c) Other relevant information	China, as the name of the country that the third party to which the information is transferred is located in

2.1.3.2 Problem 2: Insufficient supervision of overseas entrustee

"Problem 2: Potentially insufficient supervision of the overseas entrustee" means the problem that employees of a Chinese development company affiliated to LINE Corporation had access to servers in Japan to view user names, phone numbers, email addresses, and messages. According to LINE Corporation, no fraudulent access was identified and the setting was changed in late February of 2021 to prohibit access to the servers from China [12]. In response to this problem, the Personal Information Protection Committee instructed LINE Corporation to strengthen the supervision on entrustees. The instructions include detailed setting of access rights, periodical audit of entrustees, and review of the entrusted business. The rationale for issuing the instructions is article 22 of the Personal Information Protection Law, supervision of entrustees. The supervision of entrustees is required not only for overseas business operators to which personal information is transferred but also for domestic entrustees. This incident attracted attention because of entrustment to a Chinese company. However, whether oversees or domestic, the entrusting company must require the entrustee to conduct necessary and proper management so that personal data is handled safely by the entrustee.

From the standpoint of security measures, corporations should ensure that privileges assignment is made based on the policy of minimum privileges and remove any unnecessary privileges. It is not certain whether LINE Corporation intentionally granted viewing privileges of personal data for the development in China. However, it is questionable whether real Japanese user information was necessary for the development at an overseas site.

2.1.3.3 Problem 3: Insufficient measures for the protection of personal information on overseas cloud services

"Problem 3: Measures taken for storing personal data (pictures and videos) in the overseas cloud service may have been insufficient" means that the personal data of users in Japan was stored in servers of NAVER Corporation of Korea and employees of NAVER had the access rights of those servers. The media reports that stored data was put under special security measures such as distributed storage over multiple servers, and server administrators were not able to view videos and pictures stored [13].

When a corporation that handles personal data uses a cloud service, the corporation must check whether the use of the cloud service results in providing personal data to the cloud service provider. The guideline of the Personal Information Protection Law states that information retrieval using personal data as a retrieval key is an example of the provision of personal data to a cloud service provider [9]. Direct use of personal data in a cloud service is considered to be providing personal data to the cloud service. An application running on a computer or smartphone requires attention if it sends personal data to a SaaS-type cloud service.

Provision of personal data to a cloud service is entrusted to be the entrustment of personal data to the cloud service provider. Entrustment of personal data to a third party in an overseas country basically requires measures described in Figure 1 such as first-person informed consent. It is the same as the content of Table 3 in that the business operator must inform relevant individuals of the name of the country that the entrustee is based in and the existence of regulations in the country to which personal data is transferred.

On the other hand, the provision of personal data to a third party is not considered to exist in a case where the jobs of the business operator to which personal data is entrusted are only the maintenance of hardware and software and a case where personal data is not entrusted to a cloud service provider and the cloud service provider does not handle personal data stored in servers by contract [14]. As an example of a case that does not provide personal data, the guideline of the Personal Information Protection Law mentions the distribution and application of data for system amendment or as malware countermeasures [9].

LINE Corporation explains that NAVER Corporation, the cloud service provider to which personal data was entrusted, was not able to handle the personal data owned by LINE Corporation by access restrictions. This case of Japanese users' personal data being stored in servers of NAVER Corporation of Korea had not constituted the provision of personal data to a third party if, in addition to access restrictions, there had been a clause in the contract between NAVER and LINE Corporation that prohibited NAVER from accessing personal data on servers. In that case, LINE Corporation could have stored personal data in the cloud service without other conditions such as the consent of users.

2.1.3.4 Impact of the incident of LINE Corporation and measures to be taken by corporations

Many government institutions including central government offices had been using LINE as a formal tool, but the use of LINE Messenger was stopped after this incident. Among 23

government institutions, 18 were using LINE for their operations, and about 20% of those operations were handling confidential information including personal data [15]. In a press conference, President Idezawa of LINE Corporation said, "We should have considered that it was more of how clear it was to users and how they might feel uneasy, than compliance with the law [16]." As indicated by what he said, it is essential that a corporation provides information by which users will know how their data is used. In recent years, some corporations explain how personal data is handled in a manner clear to users. Apple Inc., a major IT company in the United States, provides in addition to a privacy explanation A Day in the Life of Your Data—A Father-Daughter Day at the Playground on the web, which explains the handling of personal data in a story. The story conveys deep consideration for users through an explanation from the users' perspective on the flow of personal data in data sharing, advertisements, and tracking that Apple makes.

2.1.4. Treatment of personal information that corporations use and provision of information to users

To comply with the article of the revised law about the transfer of personal information to third parties including those in overseas countries, corporations must grasp how they are using personal data in order to be able to handle it properly, as indicated in the incident of LINE Corporation. Also, corporations must establish a system that enables the continued protection of personal data. There are some corporations that suffer from the malfunctioning of the audit and correction process of personal data protection. With this revision of the law, the management of such a corporation should first recognize the protection of personal information as a corporate issue clearly, and assign an executive controller of personal information protection in a strong position such as to directly report to the president. With the strong authority of the controller of personal information protection, the information security control team can have practical power to exercise initiatives for proper personal data protection such as the strengthening of employee training and internal audits. For those who want to know the proper way for personal data protection, where to begin to establish an organization, or how well the company complies with the law, we recommend to start with activities according to general standards.

For the protection of personal information, there is JIS Q 15001 (Management System for Personal Information Protection—Requirements). A corporation handles a wide range of personal data including member sites on the Web, information of job applicants for the corporation, past sales data, and employee information. JIS Q 15001 requires corporations to list them up, evaluate risks, and take measures. The Privacy Mark is a system in which a third party certifies that a corporation complies with JIS Q 15001. If it is hard for you to list corporate information or to define a policy of personal information handling, you could go to a company that helps with the acquisition of the Privacy Mark to ask how you can comply with the revised Personal Information Protection Law. The Privacy Mark adds to social credibility because it is granted by a third party.

A common way of disclosing the corporate effort for personal information protection is to post the privacy policy in the public domain. Information about the transfer of personal data

to third parties in overseas countries should be included in the privacy policy. Many corporations post a plain template on their web site without changes. We hope that they use the revision of the law as an opportunity to establish activities and organizations for corporate personal data, and publicize them properly and clearly to earn trust from users and build corporate value.

2.1.5. Impact of toughened penalties on responses to be made by corporations

Penalties on corporations were significantly toughened by the revision of the law. Penalties of 100 million yen at a maximum are applicable to the violation of a directive of the Personal Information Protection Committee and the unlawful provision of a personal information database, as shown in Table 6. Penalties were significantly raised from a maximum of 0.5 million yen in the former law. Turning our eyes to overseas countries, penalties of GDPR are 20 million Euro (about 2,600 million yen) or 4% of annual earnings at a maximum. Also, according to the Personal Information Protection Law of China that was disclosed, the maximum penalty is 50 million RMB (about 800 million yen) [17]. In the background of the worldwide toughening of penalties of laws for personal information protection, there are lawsuit risks due to users' rising concerns on personal data protection and the intent of avoiding economic loss caused by differences from other countries.

Table 6：Changes of penalties by the revision of law

		Prison term		Fine	
		Before revision	After revision	Before revision	After revision
Violation to a directive of the Personal Information Protection Committee	Individual	6 months or less	**1 year or less**	300 thousand yen or less	**1 million yen or less**
	Corporation, etc.	-	-	300 thousand yen or less	**100 million yen or less**
Illegal provision of a personal information database, etc.	Individual	1 year or less	1 year or less	500 thousand yen or less	500 thousand yen or less
	Corporation, etc.	-	-	500 thousand yen or less	**100 million yen or less**
False report to the Personal Information Protection Committee	Individual	-	-	300 thousand yen or less	**500 thousand yen or less**
	Corporation, etc.	-	-	300 thousand yen or less	**500 thousand yen or less**

Source: Personal Information Protection Committee [18]

Also, the revised law requires corporations to report any potential leak of personal data to the Personal Information Protection Committee as soon as the leak is suspected. In consideration of penalties on missed and false reports to the Personal Information Protection Committee, corporations should establish a reporting system to be prepared for incidents. It is desirable to prepare a method to track what personal data leaked in what ways. Corporations have different content of personal data and different ways of handling them, but general methods to be taken are preparation of a registration book of taken-out personal

data, everyday collection of device logs and software logs, and preparation of a history storage of user activities related to emails and uploads.

2.1.6. Conclusion

According to *Report of Survey on Efforts of Business Operators on Personal Information Protection (2017)*, 12.3% of business operators make cross-border transfers of personal data [19]. Cross-border transfers are expected to increase in years to come due to the transfer of IT departments to overseas locations, the increase of offshore development offices, the increase of cloud sourcing, and the increase of overseas subsidiaries resulting from M&A.

All business operators that are subject to the Personal Information Protection Law must respond to the new law revised in 2020. Some corporations transfer personal data to third parties and some do not, but transfer may be taking place in an unexpected situation. Corporations should review company information on a regular basis, and establish a system for providing proper information to users as necessary.

2.2. Embezzlement from customers' accounts by a member of securities trading system development team

Matsui Securities Co., Ltd. announced that a former employee of a subcontractor (SCSK Corporation) that undertook the development and operation of a securities trading system unlawfully withdrew about 200 million yen from customers' securities accounts, and the former employee was arrested [20].

A distinctive feature of this incident is that it took two and a half years from the start of the criminal act to its discovery, and another year until the arrest of the criminal. In January 2020, Matsui Securities received a query from a customer that there was a transaction that the customer did not remember. Matsui Securities investigated and found that a former employee of a subcontractor (SCSK Corporation) had unlawfully accessed the information of multiple customers, impersonated them, and withdrawn money (Figure 2). Matsui Securities paid the whole amount to the affected customers, and SCSK paid damages to Matsui Securities.

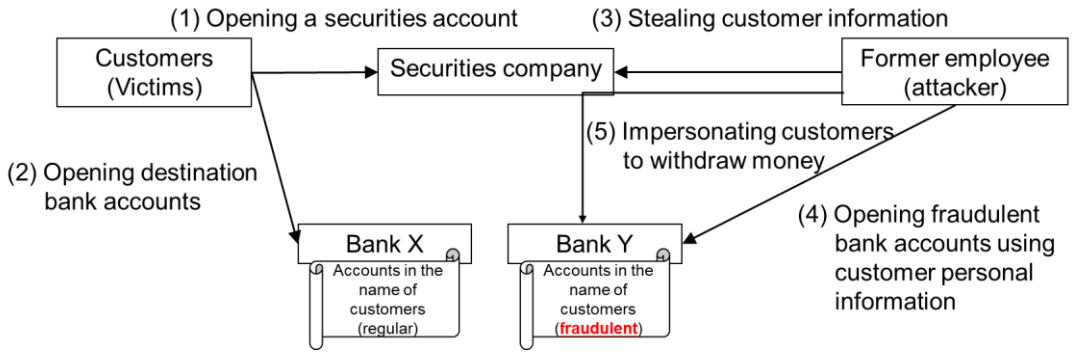


Figure 2: Overview of the incident

2.2.1. Details of the incident

Based on reports from Matsui Securities and SCSK [21], we will explain the flow of the preparation of fraudulent withdrawal (Figure 3) and the flow of the execution of fraudulent withdrawal (Figure 4).

◆ **Preparation of fraudulent withdrawal** (Figure 3)

The former employee that committed fraudulent withdrawal was an employee of SCSK Corporation, to which Matsui Securities entrusted the job of system development and operation. The person had access rights to the production environment and the development environment to conduct development and operation [22]. The former employee exploited these access rights to make a backup that contained customer IDs and passwords in the production environment and copied the backup to the development environment. The person extracted customer information from the backup to send it to the email address of the person. Then, the person impersonated the victims using obtained customer information, and opened

false bank accounts in the names of the victims.

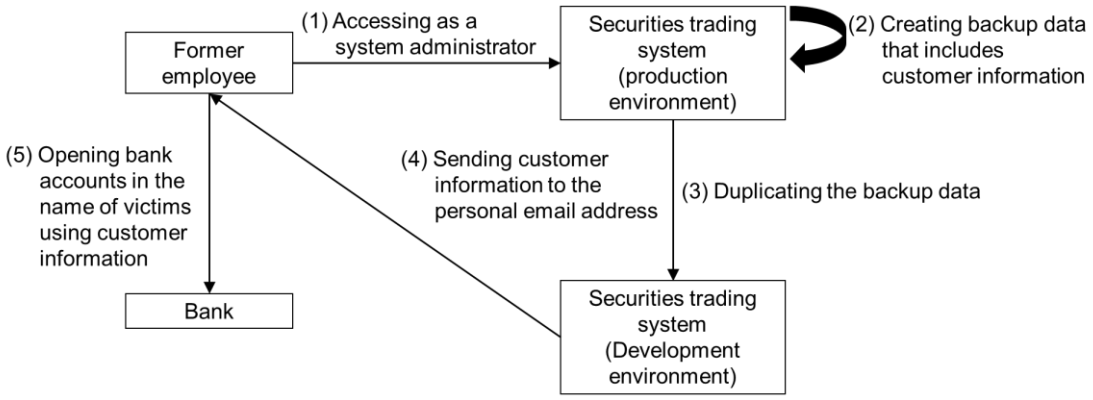


Figure 3: Flow of the preparation of fraudulent withdrawal ((1)–(5))

◆ **Execution of fraudulent withdrawal** (Figure 4)

The former employee used IDs and passwords contained in the obtained customer information to access the securities trading system, and raised cash from customers' securities through trading. The former employee transferred the cash converted from securities and the cash deposited in the securities accounts to the false bank accounts opened in the name of victims, and then withdrew the cash from those bank accounts. This incident was not found until a victim accessed the securities trading system and found a transaction that the victim did not remember.

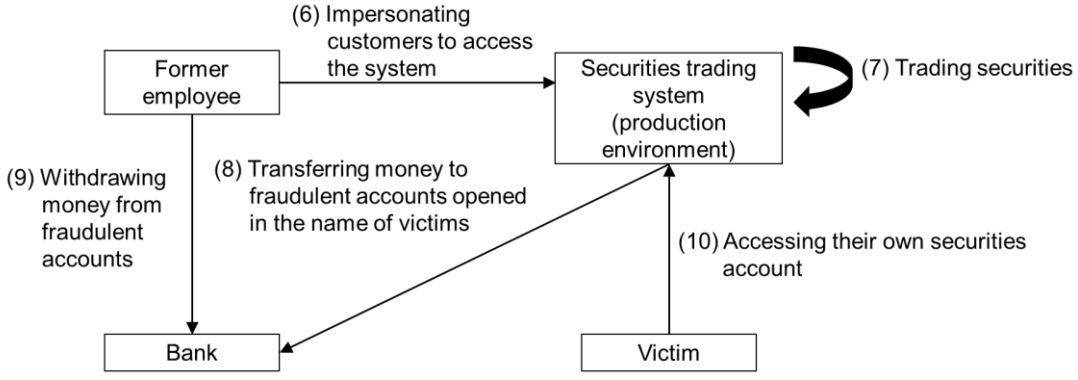


Figure 4: Flow of the execution of fraudulent withdrawal ((6)–(10))

This fraudulent withdrawal amounts to about 200 million yen affecting 15 customers. Matsui Securities announced that it had paid the whole amount to all affected customers.

2.2.2. Distinctive feature of the incident

◆ **Time elapsed from committing the crime to the revelation of the crime**

The former employee had been in charge of the system operation of Matsui Securities since joining SCSK for 18 years, and, as the project leader, was familiar with the business flow and the system structure [22]. Table 1 outlines the history of the former employee from joining the company until being arrested.

Table 1: History of the former employee from joining the company until being arrested

Date	Event
April 2002	The former employee joins the company.
June 29, 2017 to 12 November, 2019	Fraudulent withdrawal is executed.
January 2020	A customer makes a query.
	Matsui Securities starts investigation.
	Matsui Securities reports to the control authority and starts consulting the police.
September 2020	SCSK submits a written accusation to the police.
March 24, 2021	The former employee is arrested and dismissed by the company.

The former employee started the crime in June 2017 and it was not until January 2020 that a customer noticed it and made a query, which means a maximum of two and half years had elapsed. The reason that the crime was not found for a long time is presumed to be that the former employee studied the trading history and other information to select, as victims of fraudulent withdrawal, customers who had less frequent transfers from/to their accounts and less frequent access to the securities trading system. The former employee may have investigated the trading history and access history through the repeated retrieval of customer information to carefully select customers with which fraudulent withdrawal was unlikely to be found.

◆ **Taking out customer information from production environment to development environment**

The Control Standard of Description of Security Measure Standard for Computer Systems of Financial Institutions (Revision 9) [23] (Security Measure Standard, hereafter) issued by Financial Information System Center (FISC, hereafter) states the following for the prevention of fraudulent activities:

> Clarify the scopes of work, responsibilities, and authorities and establish a mutual supervision mechanism for the smooth and proper operation of jobs related to computer systems and for the prevention of fraudulent activities. (snip) If it is difficult to segment the operating organization, responsible persons must be rotated periodically to have the effect of mutual supervision

[24].

Matsui Securities is audited by the Financial Services Agency for compliance with the FISC Security Measure Standard, so Matsui Securities is considered to have taken measures against internal fraud according to the above Control Standard of the Security Measure Standard. However, in this incident, the criminal took out customer information that should have been strictly protected. To the former employee that had access to the development environment, access rights to the production environment were also given for system maintenance and operation, resulting in a period in which the same person has access to both environments. This situation presumably enabled the former employee to send customer information obtained from the production environment to the development environment without being noticed by other system operation personnel.

◆ Acquisition of IDs and passwords of customers

Even if one succeeds in taking out customer information from the production environment, the person cannot use customer information fraudulently if it is encrypted. The section of Practice Standard of the FISC Security Measure Standard states the following for data protection:

> Protect important data to prevent information leak through fraudulent duplication and theft. (Snip) Especially, a repository of personal data must be protected by means such as encryption and passwords so that the data content is not revealed even if it is duplicated fraudulently or stolen. Data accumulated through electronic transactions must also be protected by means such as encryption and passwords. [25]

In a publication, Matsui Securities says that it cannot answer questions on the security measures at the time of the incident because it affects security [26], but the company was presumed to have taken various data protection measures such as encryption of databases and access right restriction. If that is the case, the former employee had not been able to exploit customer IDs and passwords even if the person was able to transfer them from the production environment to the development environment. The former employee presumably found a security hole based on knowledge accumulated through long-standing system development to retrieve and decrypt the customer information. One possibility is that the decryption keys of the production environment and the development environment were the same so that decryption was possible once information was taken out.

◆ Reason that a third party was able to withdraw money

The law prohibits transactions under a name different from the owner of the account, so that cash transfer to a third-party account is also prohibited. Therefore, withdrawal from a securities account is possible only by the customer that owns the account. However, in this incident, the former employee, a third party, impersonated customers by stealing customer information submitted to Matsui Securities, opened bank accounts in the name of the

customers, and used those accounts as cash transfer destinations. The former employee used IDs and passwords of accounts that do not have multi-factor authentication setting for access to the security trading system to transfer cash, which is recognized as the same activities, in terms of the system, as real customers transferring money to their bank accounts, making it difficult to recognize those activities as a criminal act of a third party.

2.2.3. Countermeasures

In addition to preventive measures, another important thing about security measures is the prior consideration of ways for early detection and incident handling, on the assumption that incidents will happen. Described below are proposed measures to be taken by different parties.

A) Operation department

◆ Preventive measures

President Warita of Matsui Securities apologized in a press conference mentioning the insufficiency of fraudulent activity prohibition measures and the monitoring system. Mr. Warita also said that they would review the authorization procedure as a preventive measure against customer information transfer from the production environment to the development environment [27]. One thing that you should keep in mind is that making the entire authorization procedure too strict and complicated may result in a procedure of only formality and that does not function properly. Therefore, you should design operation procedures based on risks in consideration of handled information and the importance of operations—for example, using a strict authorization procedure for the application for access rights to files that contain personal information, and using a simple procedure for the application for the retrieval of application logs. You should aim for balanced preventive measures that do not burden the operation.

For example, the customer procedure may allow customers to use the online procedure to specify a transfer destination bank account only once after the opening of a security account, and for later changes of the bank account, the procedure may require a procedural document to be sent to the registered residential address. Appropriate levels of identity confirmation and authentication should be applied in accordance with the importance of different procedures. Quarterly Report on Global Security Trends of the 2nd quarter of 2020 describes an incident of fraudulent access to an online settlement system. That article explains a convenient authentication method that uses eKYC for online settlement services [28].

◆ Early detection

It is not practical to visually and meticulously check all operation logs of the production environment because of the burden of the work. The use of a detection system based on UEBA (User Behavior Analytics), which analyzes the behaviors of users and devices, is effective to automatically detect suspicious behavior that may be linked to internal fraud. A UEBA-based detection system can automatically detect unusual behaviors of users and devices through the analysis of operation logs. For that purpose, it is essential to understand the system comprehensively and design and configure the system so that access to sensitive

information and important operations are recorded in the operation log.

The FISC Security Measure Standard states, "5. When a financial institution entrusts an operation, the institution must evaluate and verify the execution of the entrusted operation and the observance of rules by workers of the entrustee [29]." When the development department of the entrustee accesses the production environment for special operations such as system troubleshooting and software version updates, the entrustor must make a visual examination of the operation log during the operation for any activities violating the rule.

B) Development department

◆ Preventive measures

You must create a mechanism for preventing sensitive information from being taken out and easy finding of fraudulent activities so that even employees that understand the system security design cannot make fraudulent activities. Internal fraud can be prevented by establishing a procedural mechanism in which multiple workers must attend in the execution of a command or file access that requires high privileges such as obtaining customer information from the production environment or sending customer information to the development environment, or a procedural mechanism in which the execution of a high privilege operation must be reported to the operation department, which is different from the department that the executing worker belongs to. Internal fraud can also be prevented by restricting data that can be taken out from the production environment, and segregating the environment used for the analysis of data that includes personal information from other environments. The operational burden becomes too heavy if you set a rule that require two workers for all operations or set a low detection level that causes too many notifications. Too many notifications may result in a looser visual check and overlooking of fraudulent activities. You should make a risk-based design and introduce multiple tier privileges. In the event of troubleshooting, the workers may apply for privileges that are higher than those required for the work to be done, in order to be prepared for unexpected additional work. Basically, they should apply for the lowest privileges that are necessary. We recommend that you break the work procedure down to a series of command executions, and based on it, make a mechanism for checking the operation log automatically.

The former employee had engaged in the same system from development to maintenance and operation. Latent risks can be reduced by a mechanism for distributing authority over multiple staff members and the rotation of persons in charge.

◆ Early detection

In system troubleshooting, an unexpected operation may become necessary that is difficult to foresee in advance such as retrieving data from the production environment and granting special privileges. In such an event, fraudulent activities can be identified by ensuring the traceability of data and involving multiple knowledgeable people from not only the operation department but also the development department to check the operation log.

C) Customers

◆ Preventive measures

In the preparation stage of this incident, the criminal obtained personal information and opened bank accounts to use as cash transfer destinations in a way that customers cannot notice. However, fraudulent login to the securities system could have been prevented and detected if a security function available in the system had been enabled. If multi-factor authentication had been enabled, the former employee would not have been able to log in by impersonating customers. Access from third parties can be prevented by enabling multi-factor authentication for account access and restricting source devices and IP addresses, although security functions that can be used depend on services that the financial institution provides.

◆ Early detection

As a method of detecting fraudulent login and transactions made by third parties, many systems send notifications to configured email addresses in the events of login, an operation on account setting, and a change of security settings. These settings help relevant customers to notice at an early stage any operations that they do not remember to have made. Also, the use of a money diary application to oversee the cash flow helps to recognize fraudulent activities.

2.2.4. Conclusion

We have considered countermeasures from multiple viewpoints based on the internal fraud incident at Matsui Securities. Financial services are more difficult than other systems to balance security and convenience—improving security by making identity verification stricter makes the customer procedure less convenient, and providing simple online procedures adversely affects security measures. To provide services that customers can use with peace of mind and consider to be convenient, a risk-based approach is effective, in which you conduct necessary and sufficient risk management for different functions and operations individually. The rate of the use of online services is increasing every year in settlement services. The government will also probably promote online procedures and digitalization for financial services by, for example, increasing types of taxes that can be paid online. We hope that corporations that engage in financial systems will consider security measures with reference to this report. We also hope that customers who use financial systems will properly reconfigure security settings of online financial services that they use to prevent cyber-attacks and internal fraud.

3. Data Breach

In March 2021, there was fraudulent access to a system of the Society of International Telecommunications of Airlines (SITA, hereafter), which compromised the member information of Star Alliance and Oneworld. Among the members of Star Alliance, there is All Nippon Airways, which is affiliated with ANA Holdings, which is an entrustor of SITA, and among the members of Oneworld, there is Japan Airlines, which is an entrustor of SITA. This report discusses the views of entrustor airline companies on the causes and countermeasures of the data breach on the entrustee SITA, compares different legal systems, and compares impacts of media reports on the SITA case and the LINE Corporation case. This report also follows up on the case of the data breach of Salesforce, which still continues due to improper settings.

3.1. Data Breach on SITA

3.1.1. Overview

The data breach of SITA damaged British Airways, which is a member of Oneworld, and United Airlines and Singapore Airlines, which are members of Star Alliance. Among Japanese airline companies, All Nippon Airways suffered a data breach of about 1 million items of the member information and Japan Airlines suffered about 0.92 million items. The content of member information leaked was the following [30] [31]:

- Full name in alphabet characters
- Membership number
- Member tier status

The damaged airline companies shared member information with partner airline companies through SITA to provide services to their member customers when they use partner airline companies, as illustrated in Figure5. A server of SITA located in the United States was compromised resulting in a data breach.

The cause of fraudulent access is not disclosed, but SITA has already disconnected the compromised system from the Internet and is now further investigating for any other data breaches. This incident is considered a supply chain attack because customer information of an entrustor leaked from an entrustee [32].

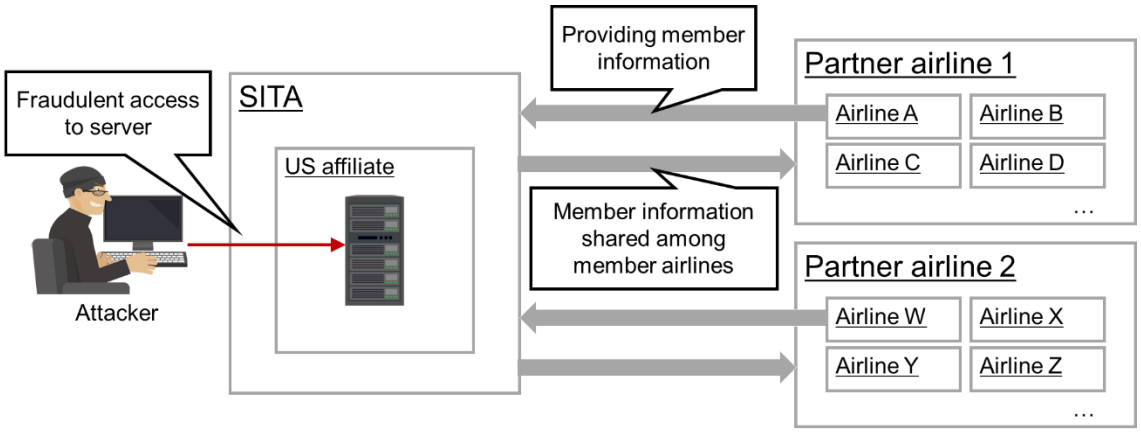


Figure5: Provision of member information and fraudulent access

3.1.2. Causes and countermeasures of information theft from an entrustee

The report of the 3rd quarter of 2020 introduced three types of supply chain attacks: (1) attack using the entrustee as a launching pad, (2) software supply chain attack, and (3) information theft from an entrustee. This incident is categorized in (3) information theft from an entrustee.

In the event of a data breach at an entrustee, the entrustor must respond to it according to the Personal Information Protection Law. Basically, the entrustor reports the incident to the Personal Information Protection Committee and other related institutions. Also, in the case of the leak of personal information, which may damage individuals, the entrustor should notify and alert affected individuals to prevent secondary damage.

In this incident, the system was shared by multiple partner companies. Therefore, building the system according to the governance policies of individual companies is considered to have been difficult for SITA. The fact that the data breach encompassed multiple groups of partner airline companies simultaneously indicates the possibility that administrative privileges of the system and database were not segmented into different groups or the database was not encrypted. When important information is entrusted, the entrustor should confirm that the entrustee is taking sufficient measures against supply chain attacks of (3) information theft from an entrustee. For example, the entrustee should take measures for protecting sensitive data even when an attacker compromised the administrative privileges of the cloud system or core system of the entrustee.

3.1.3. Legal system applied to overseas entrustees

Switzerland, the head office location of SITA, enforces the Federal Act on Data Protection (FADP, hereafter), whose revision was enacted on September 25, 2020 and will be enforced in the middle of 2022 [33]. The revised law consists of 74 articles, and largely reflects General Data Protection Regulation (GDPR, hereafter). However, the current version of the law, enacted in 1992 with only 39 articles, will continue to take effect until the enforcement of the

revision in 2022, so it is not good enough to maintain sufficient acknowledgment in terms of the current GDPR [34]. Therefore, if the system of SITA was designed, built, and operated based on the current law, its security measures may not have been sufficient. In a case of overseas entrustment, the entrustor should compare the legal system applied to the entrustee with GDPR and the Personal Information Protection Law to confirm that the security requirement level is high enough.

3.1.4. Comparison of media reports on SITA and LINE Corporation

In March 2021, there were intense media reports on the handling of personal information by LINE Corporation.

With the news that an entrustee in China had access to the data of registered email addresses, names, personal correspondence, etc. [12], concern about potential privacy invasion arose among LINE private users. Government agencies and local governments that had been using LINE in their operations and services stopped using it due to the fear of the violation of the Personal Information Protection Law about the storage location of highly confidential data handled through LINE and data exchange with overseas entrustees. The Ministry of Internal Affairs and Communications stopped the use of LINE although external fraudulent access or a data breach was not identified.

On the other hand, the incident of SITA was not covered widely by the media despite the data breach. This difference is considered to be owing to *the difference of the importance of data* and *the size of data leaked in the case of SITA*. While the data that LINE Corporation holds includes various important contents such as pictures (including those of insurance cards), videos, and transaction information of settlement services, the data that SITA holds only includes names in alphabet characters, member numbers, and member tier statuses. The number of members of ANA Mileage Club of All Nippon Airways amounts to about 37.02 million [35], and the number of members of JAL Mileage Bank of Japan Airline amounts to about 30 million [36]. Among them, personal information leaked in this incident is about 1 million items for All Nippon Airways and 0.92 million items for Japan Airlines. The impact on domestic users of All Nippon Airways and Japan Airline is considered small because the number of items of the personal information leaked was relatively small compared to the total numbers of users of these two companies and the types of personal information were less effective for identifying individuals for malicious purposes than those of LINE Corporation. These factors are considered to have made media reports less active.

3.2. Data breach through Salesforce (continued report)

The data breach attributable to the inappropriate settings of Salesforce described in the report of the 3rd quarter of 2020 continues to the 4th quarter with several reported incidents. For many cases of data breaches made through Salesforce listed in Table 2, causes were

the same as those reported for the 3rd quarter. The organizations that suffered a data breach may have been slow in responding to the information provided by Salesforce.com or took too long to analyze the data leading to delayed announcements. In the report of the 3rd quarter, we recommended that cloud service providers make a safe initial setting to prevent users' setting errors. In line with this recommendation, Salesforce.com started *granting minimum access rights to general users* and *forcibly applying the security policy that makes guest users' initial setting as safe as possible*, as countermeasures against inappropriate privileges setting in guest users' access control.

Incidents of freee K. K. and AEON Co., Ltd. in Table 2 have different causes than past incidents listed in the report for the 3rd quarter of 2020. Causes of past data breach cases of Salesforce were inappropriate privilege settings of guest user access control. However, freee K. K. explains that the incident affecting the company had a different series of events than those of other companies [37]. The cause of the incident of freee K. K. is presumed to be that the storage location of entry forms to be sent had inappropriate privilege settings of access control. As a result, the contents of forms to be sent became viewable from outside.

Table 2: Salesforce data breach cases in 4th Quarter of 2020

[38] [39] [40] [41] [42] [43]

Date published	Organization	Overview
1/27	AEON	A defective setting of a query form of AEON resulted in unauthorized access to 859 items of information that contains names, genders, email addresses, phone numbers, and query contents.
2/10	freee	A defective setting of a query form of freee K. K. made the sent contents viewable from outside.
2/10	Ryobi Systems	A third party accessed some customer information held by a local government system that Ryobi Systems offered. The access was shut off by changing the setting of the system. Details of access made before the setting change are now under investigation.
3/1	Konami Digital Entertainment Konami Amusement	A defective setting of a customer management system deployed on a cloud service allowed a third party to have access to customer personal information.
3/8	SMBC Trust Bank SMBC Nikko Securities	Personal information of customers who have just opened accounts leaked for a maximum of 101 customers of SMBC Trust Bank and a maximum of 50 customers of SMBC Nikko Securities.
3/16	Japan International Cooperation Agency	The international job-hunting site "PARTNER" operated by Japan International Cooperation Agency had access from a third party for viewing personal information.

3.3. Conclusion

For supply chain attacks, security measures are required to be taken by a wide range of organizations including entrustors and entrustees. However, in the incident of SITA, basic security measures for database systems may have been insufficient in the first place such as unencrypted databases and unsegmented administrative privileges of systems and databases, before worrying about supply chain problems. Fortunately, the impact on domestic users of All Nippon Airways and Japan Airlines was small because the magnitude of the data breach was insignificant compared to the total number of users of the two companies and the leaked personal information was not very effective for identifying individuals for malicious purposes. If a larger amount of information had leaked, the damage would have been enormous.

Most cases of data breaches made in the 4th quarter of 2020 made through Salesforce were attributable to the same causes as data cases reported for the 3rd quarter. As a countermeasure against defective privileges setting in guest users' access control, Salesforce.com started to enforce secure initial settings. It is difficult to eliminate setting errors just by calling users' attention and enlightening them, so service providers should introduce secure standard settings and system-based countermeasures. The cases of freee K. K. and AEON listed in Table 2 were owing to different causes than the Salesforce cases reported for the 3rd quarter of 2020. Details of their causes have not been announced, but we presume that insufficient understanding by cloud service customers and insufficient explanation by the cloud service providers were responsible for these incidents as it was with those reported for the 3rd quarter of 2020. We also suspect that similar problems still remain in Salesforce. Cloud service customers alone cannot find similar problems. We expect investigations to be made by security experts and Salesforce.com.

4. Vulnerability

In this report, we explain the vulnerabilities of Microsoft Exchange Server. Multiple vulnerabilities are combined in this case of Microsoft Exchange Server, and among them, the most significant one is listed in JVN with CVSS v3 base value 9.1, which is very severe. Some of them have already found to have been exploited. There is an urgent need for applying the correction program and taking mitigation measures.

4.1. Vulnerabilities of Microsoft Exchange Server

Microsoft released a non-regular security update program on March 3, 2021 [44]. Among seven vulnerabilities that this program amends, the following four vulnerabilities have already found to be exploited.

Table 3: Vulnerabilities of Microsoft Exchange Server found to have been exploited

CVE number	Overview
CVE-2021-26855	SSRF (Server Side Request Forgery: Attack on servers that cannot be accessed directly) vulnerability
CVE-2021-26857	Unsafe deserialization vulnerability of an undefined messaging service
CVE-2021-26858	Writing in arbitrary files
CVE-2021-27065	Writing in arbitrary files

Cybersecurity and Infrastructure Security Agency (CISA) issued an urgent directive for the above vulnerabilities [45]. Urgent directives of CISA are issued based on a law that allows CISA to issue them to government institutions when a severe cybersecurity threat is identified. Microsoft Exchange Server is a product that is listed for standard procurement made by the US government. CISA issued the urgent directive because such vulnerabilities of products may cause the leak of confidential information of the government.

4.2. Timeline

Table 4 shows the series of events that happened since the vulnerability was found.

Table 4: Events happened until the disclosure of vulnerabilities of Microsoft Exchange Server

Date	Event
December 10, 2020	DEVCORE found the vulnerability (CVE-2021-26855) of an authentication proxy. [46]
January 3, 2021	Volexity found a cyberattack that exploits the above vulnerably. [47]
January 5, 2021	DEVCORE reported to Microsoft. [46]
January 27, 2021	Dubex reported to Microsoft about an attack that exploits a deserialization vulnerability (CVE-2021-26857).
February 28, 2021	Exploitation of this vulnerability by multiple attacking groups were identified.
March 3, 2021	Microsoft distributed a correction program.

One of the vulnerabilities was found by Orange Tsai of DEVCORE (security company in Taiwan) on December 10, 2020, which is earlier than the publication by Microsoft on March 3, 2021. This is a zero-day vulnerability; that is, a vulnerability exploited before the publication of the vulnerability. After the distribution of the correction program on March 3, 2021, a PoC code was posted on GitHub and a sharp increase was found in attacks that exploit this vulnerability. Microsoft says that *HAFNIUM*, an attacking group that operates in China, and ransomware *DearCry* are exploiting this vulnerability [48]. Exploitation by other multiple attacking groups has also been reported. Being zero-day attacks, many cases of these attacks are considered to have made on organizations that have not amended the vulnerabilities. KrebsOnSecurity reports that at least 30,000 organizations have suffered attacks on these vulnerabilities [49].

4.3. Attacking steps and countermeasures

Attackers exploit the SSRF vulnerability (CVE-2021-26855) on port 443 to bypass the authentication of Microsoft Exchange Server, and then can exploit the deserialization vulnerability (CVE-2021-26857) to impersonate the administrator. This method of attack was named *Proxylogon* by DEVCORE because it exploits the proxy architecture and logon mechanism of Microsoft Exchange Server. Having impersonated an administrator, the attacker can execute any code. The attacker can write in any file exploiting vulnerabilities CVE-2021-26858 or CVE-2021-27065.

Microsoft publicized a correction program, mitigation measures, and a tool that checks for the SSRF vulnerability (CVE-2021-26855) [44]. Because this vulnerability is a zero-day vulnerability, systems that are open to the Internet may have been compromised before the delivery of the correction program. If an attacker has set a back door, the attacker can enter the system through the back door even if the system has the correction program applied. You

should investigate your system for any trace of an attacker that has compromised the system. If you find that an attacker entered the system, you must physically disconnect the system from the network to shut the attacker out and remove the back door before applying the correction program.

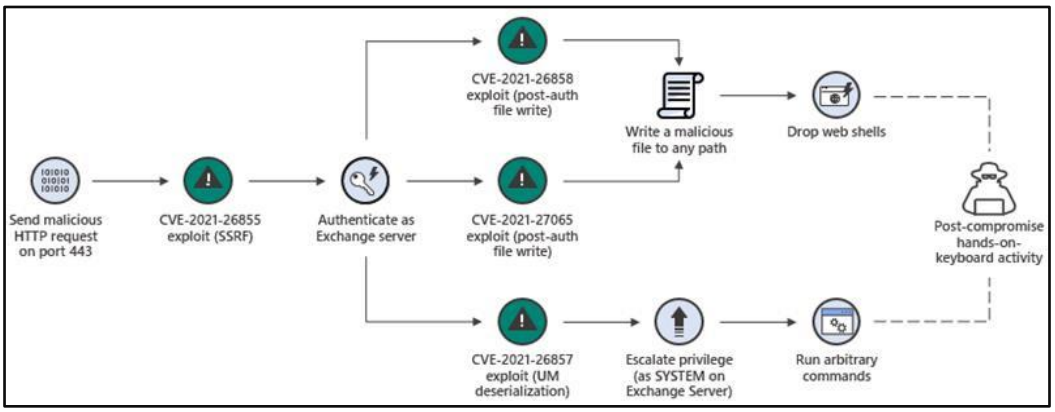


Figure 6: Exploiting chain of Microsoft Exchange Server [50]

4.4. Conclusion

In this report, we explained zero-day vulnerabilities of Microsoft Exchange Server. Palo Alto Networks postulates, from the result of the investigation by the Expands platform, that more than 125 thousand Microsoft Exchange servers open to the Internet were remaining around the world as of March 8, five days after the publication of the correction program [51]. Many organizations did not take timely actions against these dangerous vulnerabilities even though there were attacks causing damage.

The reason for delayed actions may be that these organization were not capable of taking action after the publication of the vulnerabilities. In the cyber risk survey made by the General Insurance Association of Japan on small business operators in 2019, many companies said that *they do not know how to respond to cyberattack*s and *they do not know who to consult*, compared to large companies. Also, 24% of these companies answered that they were not taking measures against cyberattacks. These companies may not be taking care of vulnerabilities as well [52]. Companies that do not take care of vulnerabilities should first check the software versions of company systems. If there are systems or software that has dangerous vulnerabilities remaining, you should apply patches as soon as possible. The application of patches does not end by applying them only once. You should continue the periodical checking of vulnerability information and the application of patches. Define an organizational system and an action cycle for vulnerability responses, and operate them continuously. Also, collect system and software vulnerability information as quickly as possible. If you cannot collect vulnerability information frequently, we recommend that you use a service that automatically delivers vulnerability information and a tool or service that supports version management.

5. Malware/Ransomware

5.1. Summary of the 4th quarter of 2020

Reports on damage cases caused by malware and ransomware continue from the 3rd quarter of 2020. Malware Emotet has caused great damage around the world from 2014 to recent years, but the European Police Office (EUROPOL) and the European Union Agency for Criminal Justice Cooperation (EUROJUST) announced that they succeeded in stopping the operation platform that remotely controls Emotet.

As for smishing that was described in the report of the 4th Quarter of 2019, damage is expanding in Japan due to the slow implementation of countermeasures [53] [54] [55].

In this report, we describe the sequence of events that terminated the operation platform of Emotet, which had been causing damage since 2014, and responses made to Emotet in Japan, as well as the changing attack method of smishing and its damage cases reported in Japan.

5.2. Emotet takedown operation (Operation LadyBird)

Malware Emotet infects a computer when the computer user executes an attached file of an attack email that is disguised as a legitimate email to steal information stored in the computer or infect the computer with other malware [56]. The attacker makes a targeted attack on an aimed, user using Emotet [57]. On 27 January, 2021, the operation platform of Emotet was stopped by the police agencies of the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine cooperating under the orchestration of EUROPOL and EUROJUST [58]. Operation LadyBird was carried out through the following events [58]:

(1) Seizure of the upstream C&C server that remotely operated Emotet
(2) Detoxification of Emotet by controlling it
(3) Arrest of members of Emotet operation and maintenance group

This report explains the details of the Emotet takedown operation.

5.2.1. Takedown of Emotet through international cooperation

The police agencies of the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine cooperated to investigate the operation platform of Emotet [59].

In August 2018, the German police started an investigation of Emotet, which had spread in Germany. Through the investigation, the police found multiple C&C servers that constituted

the Emotet botnet [60]. By analyzing the data stored in the seized C&C servers in Germany, the police found other C&C servers that were operated in multiple countries in Europe and identified the range of the infection of Emotet. Because the identified C&C servers were not located in Germany, the German police cooperated with the international police and the police agencies of other countries to proceed with the investigation. Consequently, they seized C&C servers in the Netherlands, Lithuania, and Ukraine that constitute the Emotet botnet [60]. By analyzing the data of the seized C&C servers, they finally located and seized two upstream C&C servers that remotely controlled Emotet through the botnet [61].

The Dutch police used the seized C&C servers to change the Emotet setting so that computers that were infected with Emotet communicate only with the C&C server that was controlled by the Dutch police [62]. After that, the police distributed a detoxified version of Emotet from the C&C server to update the infected computers with the detoxified Emotet [59] [61]. This operation detoxified a large number of Emotet codes to end the Emotet issue [62].

In addition to the seizure of the operation platform of Emotet, Operation LadyBird succeeded in arresting some members of the group that operated and maintained Emotet. The Ukrainian police officers that were engaged in Operation LadyBird arrested two suspects who were considered to have maintained the operation platform of Emotet [63]. From the information seized in this arrest, the police found that Emotet caused damage worth 2.5 billion dollars to financial institutions in the United States and Europe [63]. These two suspects may be sentenced to a maximum prison term of 12 years due to unauthorized access, the creation of malware, fraud, and so forth [63] [64]. The Ukrainian police identified other groups that committed the Emotet cyberattack and are working to arrest them [63].

5.2.2. Activities after the takedown of Emotet

Operation LadyBird seized and stopped multiple C&C servers but could not stop all C&C servers. So, the German police installed a sinkhole server for Emotet. A sinkhole server is a special DNS server that returns a harmless IP address as the response to a malware-originated name resolution request for C&C servers. In this way, the sinkhole server prevents communication from malware to the C&C servers and identifies the IP address of machines that are infected with malware.

The operation by EUROPOL and EUROJUST detoxified Emotet, but did not eliminate the secondary infection of malware Ursnif, Trickbot, Qbot, Zloader, and IcedID [65]. After Operation LadyBird stopped the operation platform of Emotet on January 27, 2021, the IP addresses captured by the Emotet sinkhole server controlled by the German police and the email addresses found in the data stored on the seized C&C servers were provided to the CSIRTs of individual countries. The CSIRTs of individual countries expelled secondarily infected malware using these IP addresses.

Communication data of computers in Japan infected with Emotet has started to be provided to JPCERT/CC when they computers communicate with C&C servers that the German police controls [58]. JPCERT/CC found based on the communication record that about 900 computers in Japan were infected with Emotet. Among them, 500 computers remained infected after February [58].

JPCERT/CC provided the IP addresses of infected computers received from the German police to Internet service providers. Internet service providers derived Emotet-infected computers from these IP addresses and informed the users of these computers about how to remove malware of secondary infection. Users that received this information removed malware of secondary infection [66] [67].

Stolen information that may have spread over the Internet has not been collected or deleted. The Dutch police collected stolen information stored in the seized C&C servers, and opened a website where the users of infected computers can investigate whether their information was stolen or not [62]. On this website, users can check whether their credentials. such as email addresses, account names, and passwords, or other information have been stolen or not by entering their email addresses. Users should change their passwords to prevent the exploitation of credentials for fraudulent login to different services if their credentials have been stolen.

The termination of the operation platform of Emotet is a great accomplishment achieved through the cooperation of the police agencies of the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine under the orchestration of EUROPOL and EUROJUST. Although Emotet was terminated by Operation LadyBird, Emotet-like malware IcedID, which was introduced in the report for the 3rd Quarter of 2020, is still active [62]. Attacks will not cease. We must continue to take action.

5.3. Recent trend of smishing

Smishing is a type of phishing scam that steals information. The attacker sends to smartphones an SMS message that impersonates a legitimate shopping site or service such as a courier notification of delivery in absence to lure users into a fraudulent website for the theft of personal information, credentials, and other information [68].

This report we will explain the attacking method, current status of damage, and countermeasures of smishing, which is now spreading and causing damage.

5.3.1. Current status of smishing damage

While cases of phishing scam damage are increasing overall, those of smishing are also increasing. As for the number of cases of overall phishing scam damage in the 4th Quarter of 2020, the number of reports in January 2021 exceeded that of January 2020, February had a lower number of reports, but the number reached the level of January in March [53] [54] [55]. The Council of Anti-Phishing Japan reports that smishing damage is on the increase, although they do not report the number of cases [53] [54] [55]. Japan is not the only country that suffers pervasive smishing damage. According to the FBI report on the survey of Internet crimes targeting American citizens, the year 2020 alone had 241,342 cases with the damage estimated at about 54 million dollars [69] [70]. Phishing scams including smishing are increasing also in the United States.

5.3.2. Types of smishing

Smishing messages that lure users into fraudulent websites can be categorized into *messages disguised as services* and *messages disguised as security functions of services* as shown in Table 5.

Table 5: Messages that lure users into fraudulent websites

Type	Description
Disguised as services	Sending a false SMS message disguised as a notification SMS message sent from a service [Example] ● Sending a message disguised as a notification of delivery in absence sent from a courier such as Kuroneko Yamato and Sagawa Express [71] ● Sending a message disguised as a shipment notification sent from a shopping site such as Rakuten Ichiba [72]
Disguised as a security function	Sending a message disguised as a message of multi-factor authentication or access confirmation for the use of a service [Example] ● Sending a message disguised as an alarm message sent from Sumitomo Mitsui Banking such as "An unauthorized access from a third party was detected. Please check your account." [73] ● Sending a message disguised as a message from Sumitomo Mitsui Banking for the approval for payment ● Sending a message disguised as a message for SMS access confirmation

Attackers use messages as listed above to lure users to fraudulent websites and have users execute fraudulent applications to steal their information. Table 6 explains methods of stealing user information.

Table 6: Methods of stealing information

Type	Description
Fraudulent website	The attacker includes the URL of a fraudulent website in an SMS message to have the user access the website and enter the user's personal information and credentials in order to steal information. [71]
Fraudulent application	The attacker includes in an SMS message the URL to have the user download a fraudulent application. Then, the user installs the fraudulent application and grants the application with privileges. As a result, the fraudulent application retrieves information from the address book in the smartphone and sends it to the attacker on the Internet. [72]

The attacker exploits the information obtained by the above methods for the malicious use

of services such as fraudulent transfer of money by online banking or for further smishing attempts.

5.3.3. Countermeasures against smishing

According to the report of Proofpoint, many users are still not aware of smishing attack methods. The report also states that more than half of the surveyed companies do not conduct security training for smishing [74]. In view of the above report, the reason that smishing damage continues to happen is insufficient awareness raising about smishing for users.

Users who do not know of smishing should first know the existence and danger of the cyberattack called smishing. General users probably do not often view the website of the Information-technology Promotion Agency (IPA), which provides information on information security. Therefore, financial institutions and service providers such as carriers that are exploited by smishing must actively raise awareness in service users. Service providers can let many users know of smishing by active raising awareness about smishing through their websites and applications used by users. Also, if service providers disclose real examples of smishing SMS messages to raise awareness, the probability and the number of cases of service users deceived by smishing SMS messages will decrease. Such support will also help to earn a sense of security and credibility from service users.

Organizations such as corporations can enlighten employees with knowledge and skills related to smishing by periodical security training and phishing simulation exercises.

In recent years, we have seen sophistication in smishing messages, phishing messages, fraudulent websites, and fraudulent applications. The prevention of damage is becoming difficult only with the above awareness raising on smishing SMS messages. In these circumstances, we recommend that users introduce the following functional and technical countermeasures:

- Enable the function to reject smishing SMS messages. Block SMS messages that match the condition of suspicious SMS messages provided by telecommunication service providers [75].
- Enable the URL filtering function of the smartphone. The filtering function automatically blocks access to known phishing sites when the user taps a suspicious URL in an SMS message [76].
- Install applications from the official store only. Install tested applications that are available in official stores such as AppStore and Google Play. The installation of applications to devices of iOS and Android is restricted to those in official stores. Do not disable this setting.
- Introduce EMM and MDM to control applications on company smartphones to allow the installation of only permitted applications and prohibit the installation of dangerous applications [77].

5.4. Conclusion

In this report, we introduced the takedown of Emotet and the trend of smishing. The operation platform of Emotet was detoxified by the takedown operation LadyBird conducted with the cooperation of the law enforcement agencies of eight nations in Europe and North America. This incident indicated that international cooperation is necessary for the thorough resolution of malware such as Emotet that causes worldwide damage. Emotet was terminated, but information stolen by Emotet cannot be retrieved, and malware implanted by secondary infection is not removed automatically. We should change passwords to prevent third-party unauthorized access by stolen passwords and remove malware implanted through secondary infection to prevent damage.

Many users still do not know about the cyberattack called smishing. Service providers should take the initiative in awareness raising activities to enlighten as many users as possible about the threat of smishing to have them take measures.

Users and corporations must continuously collect the latest information about security including malware to understand threats correctly and take appropriate measures. This applies to both Emotet and smishing.

6. Outlook

Secondary damage of data breach incidents to beware of

Data breach incidents continue to occur although activities of personal information protection are gathering momentum from the society situation and law systems. In May 2021, marriage hunting site "Omiai" (Net Marketing Co., Ltd.) had an incident of the leak of the image data in user identification documents including drivers' licenses. The number of pictures leaked from Omiai user identification documents is reported to be about 1.71 million [78]. The attacker can fabricate pictures of drivers' licenses from the stolen image data. With this incident, impersonation incidents using such image data of identification documents are expected to increase. For example, an online bank that authenticates customers with only one identification document may approve an application for account opening by an attacker who uses a picture fabricated from a driver's license. eKYC is widely used as a method of online user identification [79]. eKYC defines four levels of identity verification according to the Act on Prevention of Transfer of Criminal Proceeds. The lowest level of identity verification, which is made by a picture of an identity card and a picture of the person, may be broken by impersonation with a fabricated driver's license created from the leaked data. Identification methods provided by eKYC include multi-factor authentication methods that also require the use of other media such as the reading of IC chips and the matching of credit cards. If cases of impersonation increase, we must consider the use of identity verification methods of higher reliability.

The importance of identity verification varies depending on corporations and services. Corporations must evaluate the risk level of the fabrication of identification documents to take measures such as the avoidance, mitigation, and acceptance of risks.

Smishing scam disguised as vaccination

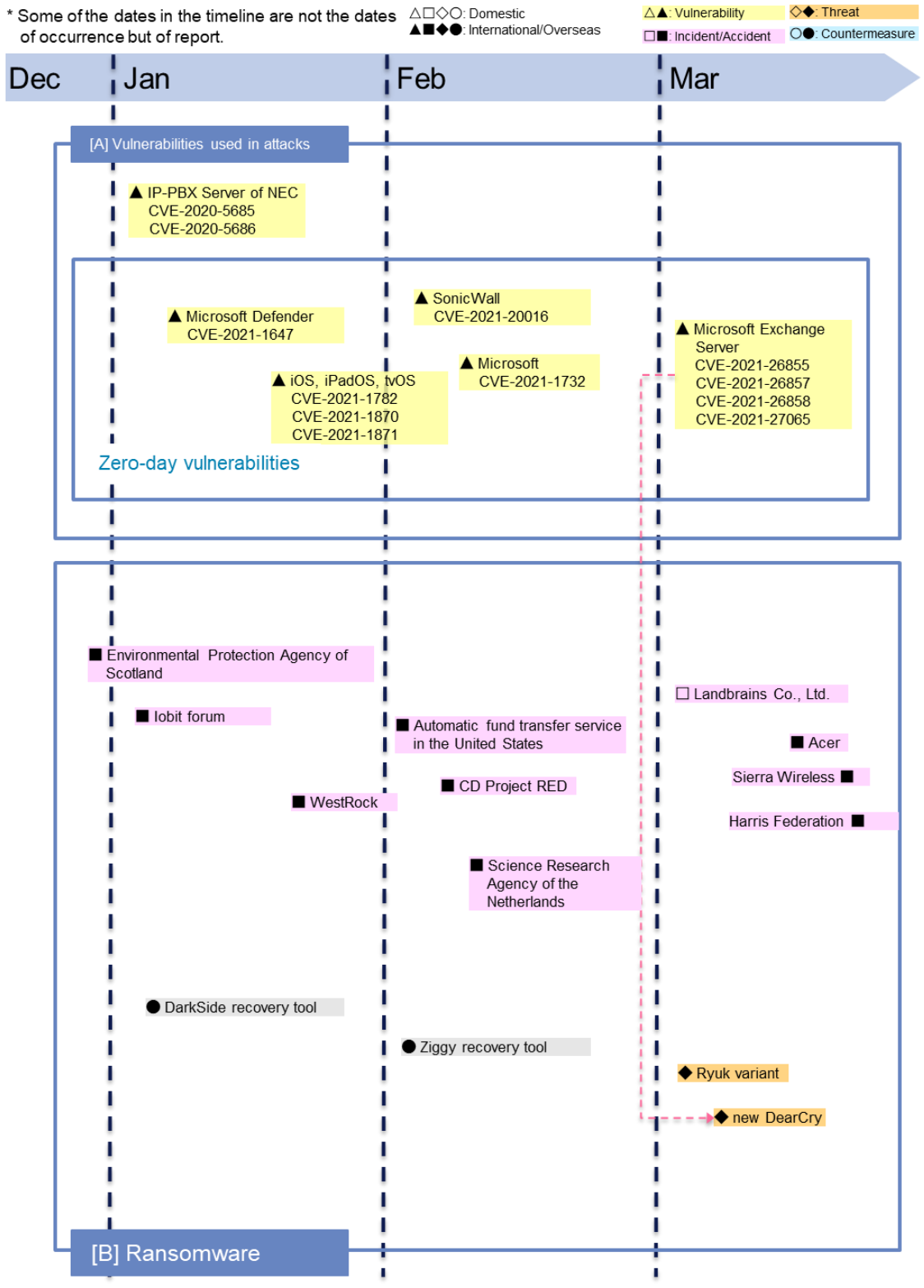
Many fraudulent acts have been identified related to COVID-19 vaccinations. Because of the currently prioritized vaccinations for senior adults, there are many fraudulent acts by phone calls and visits that target them. Because the ages for vaccinations will be widened from June, we presume that fraud through the Internet will increase instead of phone calls and visits. One of the methods considered to be used by attackers is smishing. For example, the attacker may impersonate a government agency to send messages such as "surplus vaccine for medical service workers is available for a price," [80] and "special vaccine with less side effects is available for a price," to smartphones to have receivers transfer money to an account of the attacker or enter personal information such as credit card information at a phishing site. Messages that require money for vaccinations are frauds. If you receive a message about COVID-19 and feel suspicious even if only a little, call the toll free number 0120-797-188 of the *Consumer Hotline on COVID-19 Vaccine Fraud* of the National Consumer Affairs Center of Japan [81].

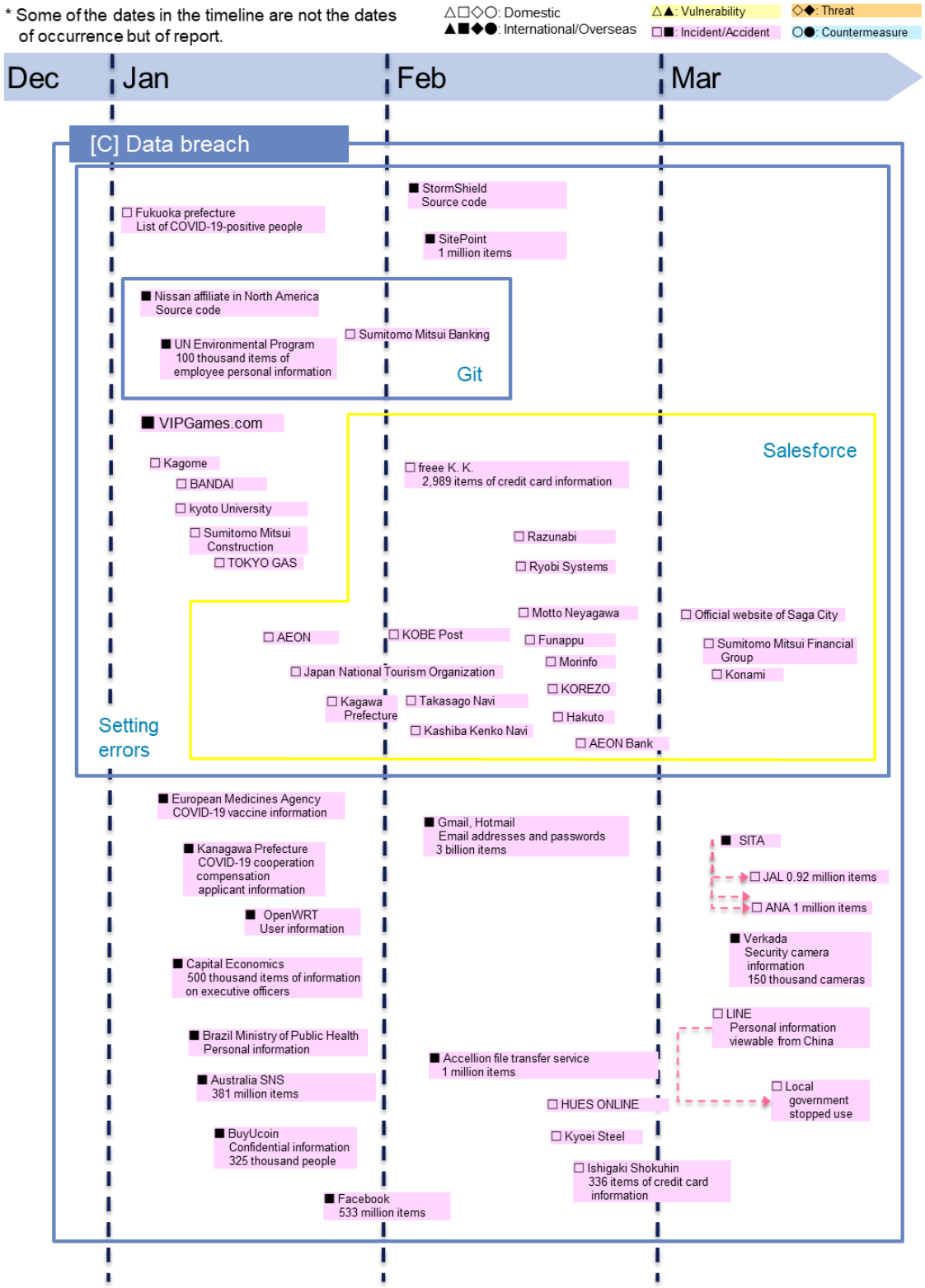
Continuation of double-extortion ransomware attacks

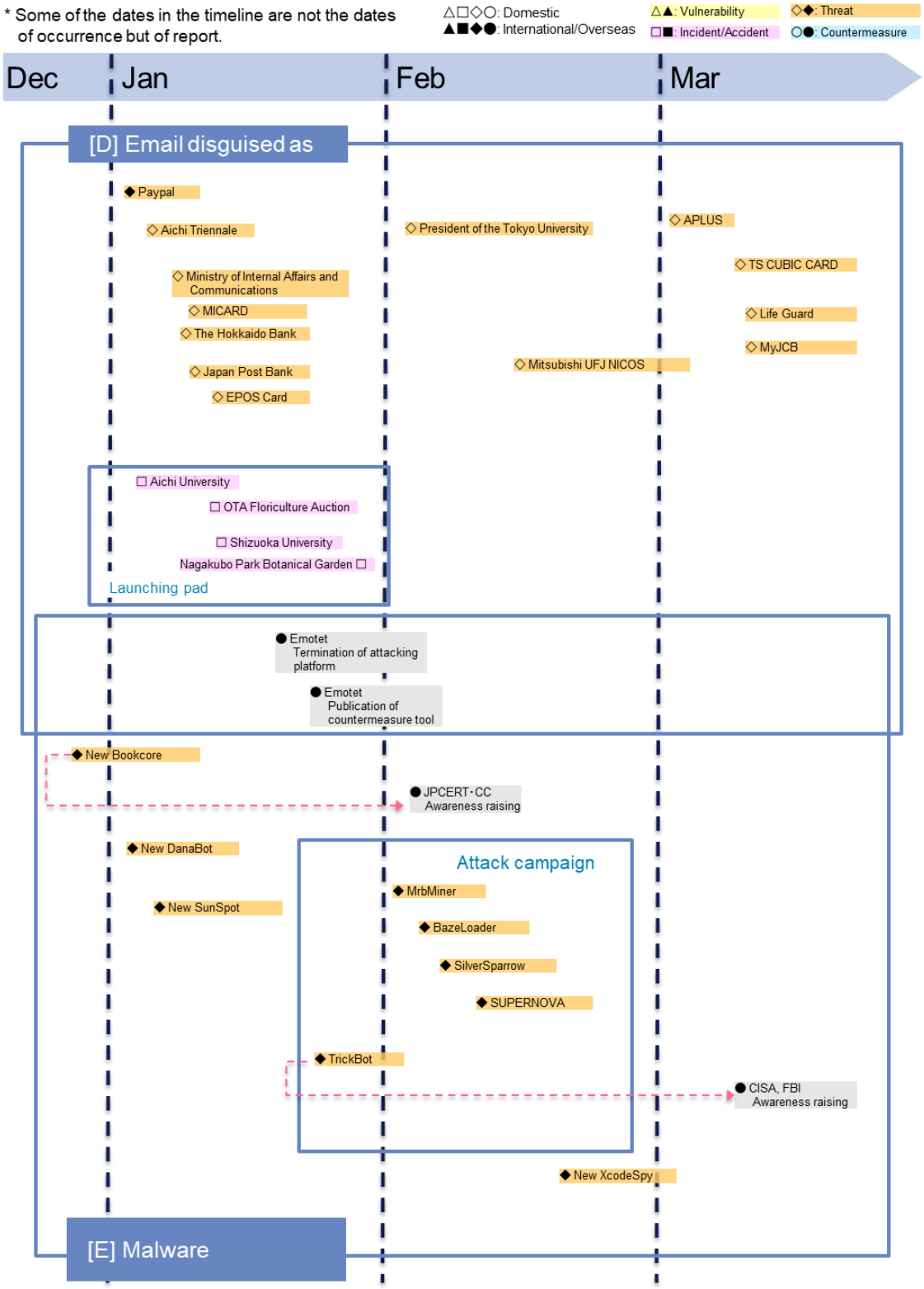
The report for the 3rd quarter of 2020 described double-extortion ransomware attacks. In the 4th quarter, there were also ransomware attacks on corporations including CD Projekt S.A., a company that develops games, and Landbrains Co., Ltd., a company trusted with a wide range of public projects [82] [83]. CNA Financial, an insurance company in the United States, was reported to have consented to the payment of 40 million dollars, the highest in 2020 [84].

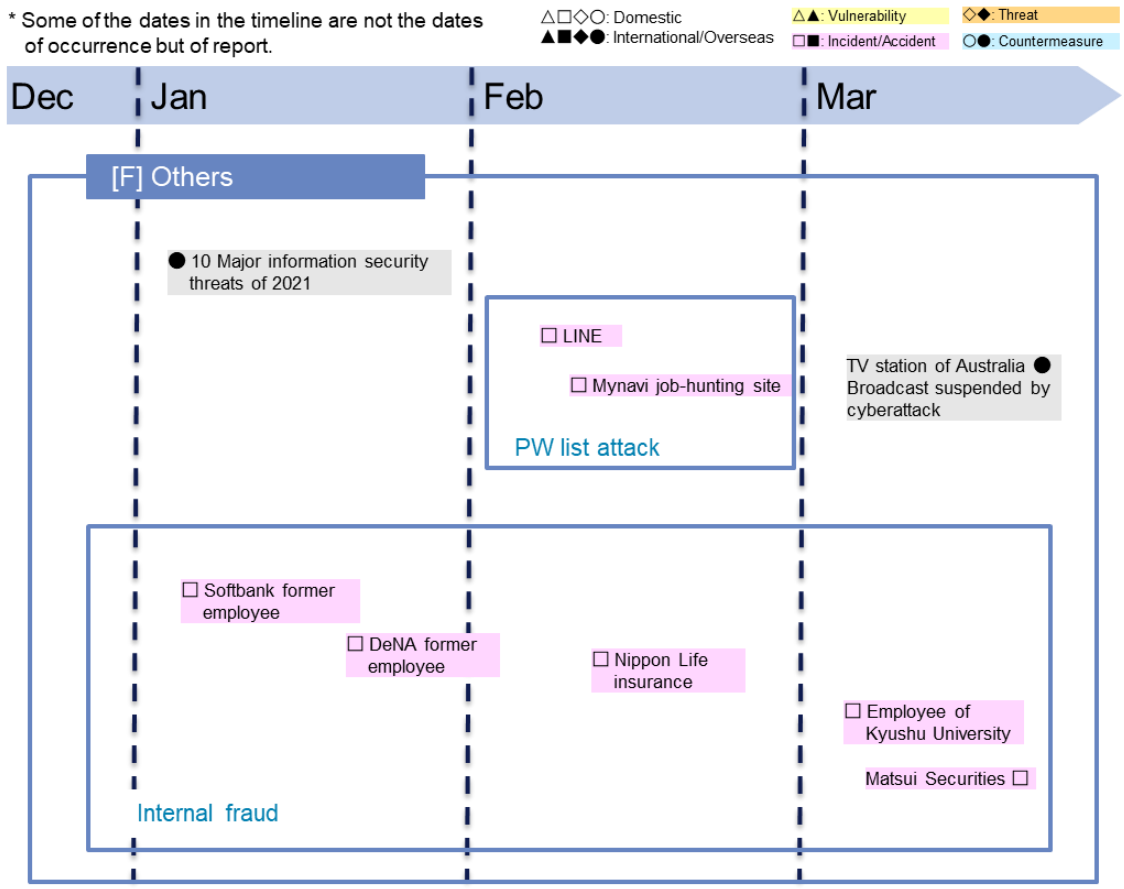
The trend of policies for double-extortion ransomware attacks is to prohibit paying ransoms because it is an act of helping criminal activities. An example is a recommendation made by Office of Foreign Assets Control of the U.S. Treasury in October 2020. Therefore, it is believed that cases where ransoms are paid will decrease in the years to come [85]. However, attacked organizations may suffer considerable damage by double-extortion ransomware attacks that expose information. As long as such cases remain, ransom payments are expected to continue.

7. Timeline









References

[1] 個人情報保護委員会, “「個人情報の保護に関する法律等の一部を改正する法律（概要）」より抜粋編集,” [オンライン].

[2] 佐脇紀代志, “一問一答 令和2年改正個人情報保護法,” 商事法務, 2020, pp. 53-4.

[3] 一般社団法人日本情報経済社会推進協会, “CBPR認証,” 17 5 2021. [オンライン]. Available: https://www.jipdec.or.jp/protection_org/cbpr/.

[4] 一般社団法人日本情報経済社会推進協会, “十分性認定後の日本企業のGDPR対応　越境データ移転を中心に,” 18 4 2019. [オンライン]. Available: https://www.jipdec.or.jp/library/report/20190418.html.

[5] 個人情報保護委員会, “個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール,” [オンライン]. Available: https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf.

[6] 佐脇紀代志, “一問一答 令和2年改正個人情報保護法,” 著: *一問一答 令和2年改正個人情報保護法*, 商事法務, 2020, p. 96.

[7] 個人情報保護委員会, “改正法に関連する政令・規則等の整備に向けた論点について（越境移転に係る情報提供の充実等）,” 4 11 2020. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/201104_ekkyouiten.pdf.

[8] NHK, “LINE社長 中国からの個人情報へのアクセス遮断を明らかに,” 23 3 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210323/k10012931491000.html.

[9] 個人情報保護委員会, “「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ＆A,” 個人情報保護委員会, 12 11 2019. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/1911_APPI_QA.pdf.

[10] 佐脇紀代志, 一問一答 令和2年改正個人情報保護法, 商事法務, 2020.

[11] 個人情報保護委員会, “個人情報の保護に関する法律に基づく行政上の対応について,” 23 4 2021. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/210423_houdou.pdf.

[12] 読売新聞オンライン, “「ＬＩＮＥ」個人情報が丸見え、管理委託の中国企業から…運用見直しを検討,” 17 3 2021. [オンライン]. Available: https://www.yomiuri.co.jp/national/20210317-OYT1T50123/.

[13] 朝日新聞DIGITAL, “日本のLINE利用者の画像・動画全データ、韓国で保管,” 17 3 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP3K64ZCP3KUHBI01W.html.

[14] 西村あさひ法律事務所 濱野 敏彦, “BUSINESS LAWYERS,” 4 1 2021. [オンライン]. Available: https://www.businesslawyers.jp/practices/1314.

[15] NHK, “LINE利用でガイドライン “機密情報 残さない仕組みを” 政府,” 1 5 2021. [オンライン]. Available: https://www3.nhk.or.jp/news/html/20210501/k10013007361000.html.

[16] 朝日新聞DIGITAL, “「漏洩は確認してない」 LINE社長の会見、一問一答,” 23 3 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP3R7R94P3QUTIL06F.html.

[17] 東洋経済オンライン, “中国が「個人情報保護法」制定に踏み出す事情,” 23 10 2020. [オンライン]. Available: https://toyokeizai.net/articles/-/382436.

[18] 個人情報保護委員会, [オンライン]. Available: https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/.

[19] 株式会社 野村総合研究所, “個人情報の保護に関する事業者の取組実態調査（平成２９年度）報告書,” 3 2018. [オンライン]. Available: https://www.ppc.go.jp/files/pdf/personal_report_3003_jigyosya.pdf.

[20] 松井証券株式会社, “業務委託先元従業員の逮捕について,” 24 3 2021. [オンライン]. Available: https://www.matsui.co.jp/parts/pdf-view/web/viewer.html?file=/company/ir/press/pdf/pr210324.pdf.

[21] SCSK株式会社, “https://www.scsk.jp/news/2021/pdf/20210324.pdf,” 24 3 2021. [オンライン]. Available: https://www.scsk.jp/news/2021/pdf/20210324.pdf.

[22] 日経クロステック／日経コンピュータ, “SCSK元社員の2億円不正出金事件はなぜ起こった？IT大手8社の内部不正対策を調査,” 16 4 2021. [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/column/18/00989/041400051/.

[23] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 3 2019. [オンライン]. Available: https://www.fisc.or.jp/publication/book/003930.php.

[24] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 2019, p. 統制基準（第９版）統９.

[25] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基

準・解説書（第9版改訂）,” 2019, p. 実務基準（第９版）実３.

[26] Security NEXT, “松井証券で顧客資産約2億円が不正引出 - 長年業務に携わる委託先SEが権限悪用,” 25 3 2021. [オンライン]. Available: https://www.security-next.com/124542.

[27] 日本経済新聞, “松井証券顧客の株式を無断売却か　SCSKエンジニア逮捕,” 24 3 2021. [オンライン]. Available: https://www.nikkei.com/article/DGXZQODG246R70U1A320C2000000/.

[28] 株式会社ＮＴＴデータ　セキュリティ技術部, “サイバーセキュリティに関するグローバル動向四半期レポート（2020年7月～9月）を公開,” 11 12 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/news/information/2020/121100/.

[29] 金融情報システムセンター, “金融機関等コンピュータシステムの安全対策基準・解説書（第9版改訂）,” 2019, p. 監査基準（第９版）監１.

[30] 日本経済新聞, “JAL、92万人分の情報流出　マイレージ会員対象,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ05ABI0V00C21A3000000/.

[31] 日本経済新聞, “ANAも100万人分流出　マイレージ情報、不正被害は未確認,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODZ060KO006032021000000/.

[32] SITA, “SITA statement about security incident,” [オンライン]. Available: https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/.

[33] Pestalozzi Attorneys at Law, “The revised Federal Act on Data Protection,” [オンライン]. Available: https://pestalozzilaw.com/en/news/legal-insights/revised-federal-act-data-protection/.

[34] 日本貿易振興機構, “スイス連邦データ保護法改正案の内容およびEU「一般データ保護規則」との比較,” [オンライン]. Available: https://www.jetro.go.jp/ext_images/_Reports/01/74c0fb55f759d238/20170108.pdf.

[35] 全日空商事, “ANA MEDIAKIT ANAメディアキットのご案内,” [オンライン]. Available: https://www.anahd.co.jp/ana-info/ana/mediadata/pdf/mediakit/ANA_MEDIA_KIT_outline.pdf.

[36] JALブランドコミュニケーション, “JAPAN AIRLINES MEDIA INFORMATION JAL広告メディアのご案内,” [オンライン]. Available: https://www.jalbrand.co.jp/common/pdf/adv_all.pdf.

[37] Security NEXT, “「Salesforce」利用の複数フォームに設定不備 - 他社事例と異なる部分,” [オンライン]. Available: https://www.security-next.com/123273.

[38] 日本経済新聞, “イオンでも不正アクセス、セールスフォース製品で,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQOFK280XJ0Y1A120C2000000/.

[39] freee, “クラウド型お問い合わせ管理システムに対しての第三者によるアクセスの可能性について,” [オンライン]. Available: https://corp.freee.co.jp/news/system-research.html.

[40] 両備システムズ, “クラウド型システムへの第三者からのアクセスについて,” [オンライン]. Available: https://www.ryobi.co.jp/news/notification20210210.

[41] 株式会社コナミデジタルエンタテインメント, “第三者のアクセスによる情報流出につい,” [オンライン]. Available: https://www.konami.com/games/corporate/ja/news/topics/20210301a/.

[42] 日本経済新聞, “三井住友FG傘下2社が顧客情報流出、システム設定不備で,” [オンライン]. Available: https://www.nikkei.com/article/DGXZQODF086CX0Y1A300C2000000/.

[43] 国際協力機構, “「PARTNER」への第三者による不正アクセスについて,” [オンライン]. Available: https://www.jica.go.jp/information/info/2020/20210316_10.html.

[44] Microsoft, “Microsoft Exchange Server 2019、2016、2013 用のセキュリティ更新プログラムについて: 2021 年 3 月 2 日 (KB5000871),” Microsoft, 2 3 2021. [オンライン]. Available: https://support.microsoft.com/ja-jp/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b.

[45] Infrastructure Security Agency, “Emergency Directive 21-02,” Infrastructure Security Agency, 3 3 2021. [オンライン]. Available: https://cyber.dhs.gov/ed/21-02/.

[46] DEVCORE, “ProxyLogon,” DEVCORE, 3 2021. [オンライン]. Available: https://proxylogon.com/.

[47] M. M. S. K. S. A. T. L. Josh Grunzweig, “Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities,” volexity, 2 3 2021. [オンライン]. Available: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/.

[48] Microsoft, “HAFNIUM targeting Exchange Servers with 0-day exploits,” Microsoft, 2 3 2021. [オンライン]. Available: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[49] KrebsOnSecurity, “At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft’s Email Software,” KrebsOnSecurity, 5 3 2021. [オンライン]. Available: https://krebsonsecurity.com/tag/microsoft-exchange-server-flaws/.

[50] Microsoft, “Analyzing attacks taking advantage of the Exchange Server vulnerabilities,” Microsoft, 25 3 2021. [オンライン]. Available: https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/.

[51] palo Alto Network, “Microsoft Exchange Server Attack Timeline,” palo Alto Network, 11 3 2021. [オンライン]. Available: https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/.

[52] 日本損害保険協会, “数字で見るサイバーリスクと保険,” 日本損害保険協会, 2020. [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/data/2019-01/pdf/cyber_report2019.pdf.

[53] フィッシング対策協議会, “2021/01 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202101.html.

[54] フィッシング対策協議会, “2021/02 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202102.html.

[55] フィッシング対策協議会, “2021/03 フィッシング報告状況,” [オンライン]. Available: https://www.antiphishing.jp/report/monthly/202103.html.

[56] 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,” [オンライン]. Available: https://www.ipa.go.jp/security/announce/20191202.html.

[57] サービス &セキュリティ株式会社, “Emotetテイクダウン成功後の現状と今後の対策,” [オンライン]. Available: https://www.ssk-kan.co.jp/topics/?p=11545.

[58] 一般社団法人JPCERTコーディネーションセンター, “マルウェアEmotetのテイクダウンと感染端末に対する通知,” [オンライン]. Available: https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html.

[59] Security Next, “「Emotet」を追い詰めた「Ladybird作戦」 - 攻撃者がバックアップ保有の可能性も,” [オンライン]. Available: https://www.security-next.com/122910.

[60] Bundeskriminalamt, “Infrastruktur der Emotet-Schadsoftware zerschlagen,” [オンライン]. Available: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html.

[61] POLITIE, “Internationale politieoperatie LadyBird: wereldwijd botnet Emotet ontmanteld,” [オンライン]. Available:

https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html.

[62] トレンドマイクロ株式会社, “サイバー犯罪の根本解決：EUROPOLによるEMOTETテイクダウン,” [オンライン]. Available: https://blog.trendmicro.co.jp/archives/27132.

[63] Національної поліції, “Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі комп’ютерного вірусу «EMOTET»,” [オンライン]. Available: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-ugrupovannya-xakeriv-u-rozpovsyudzhenni-najnebezpechnishogo-v-sviti-komp-yuternogo-virusu-EMOTET/.

[64] 日経XTECH, “最も危険なマルウエア「Emotet」が壊滅,” [オンライン]. Available: https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/042100139/.

[65] ZDNet Japan, “マルウェア「Emotet」の国内感染は推定約500台--駆除活動が本格化,” [オンライン]. Available: https://japan.zdnet.com/article/35166831/.

[66] Malwarebytes Inc, “Cleaning up after Emotet: the law enforcement file,” [オンライン]. Available: https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/.

[67] BLEEPINGCOMPUTER Inc, “Europol: Emotet malware will uninstall itself on April 25th,” [オンライン]. Available: https://www.bleepingcomputer.com/news/security/europol-emotet-malware-will-uninstall-itself-on-april-25th/.

[68] キヤノンマーケティングジャパン株式会社, “SMSを利用したスミッシングによるサイバー詐欺の危険性,” [オンライン]. Available: https://eset-info.canon-its.jp/malware_info/special/detail/201210.html.

[69] Proofpoint, Inc., “FBIインターネット犯罪報告書：2020年に最大の金銭的損失をもたらしたのはメール詐欺,” [オンライン]. Available: https://www.proofpoint.com/jp/blog/email-and-cloud-threats/fbi-internet-crime-report-shows-email-fraud-represents-largest.

[70] Federal Bureau of Investigation, “INTERNET CRIME REPORT 2020,” [オンライン]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[71] Whoscall株式会社, “スミッシンクづてなに?被害事例やその手口・対策方法をご紹介,” [オンライン]. Available: https://whoscall.com/ja/blog/articles/196-%E3%82%B9%E3%83%9F%E3%83%83%E3%82%B7%E3%83%B3%E3%82%AF%E3%82%99%E3%81%A3%E3%

81%A6%E3%81%AA%E3%81%AB%EF%BC%9F%E8%A2%AB%E5%AE%B3%E4%BA%8B%E4%BE%8B%E3%82%84%E3%81%9D%E3%81%AE%E6%89%8B%E5%8F%A3%E3%83%BB%E5%AF%BE%E7%AD.

[72] トレンドマイクロ株式会社, “偽装SMSから誘導される不正アプリをインストールしてしまったらどうなる？,” [オンライン]. Available: https://is702.jp/news/3803/partner/101_g/.

[73] ニフティ株式会社, “三井住友カードのなりすまし迷惑メールに注意|詐欺手口と見分け方について解説,” [オンライン]. Available: https://koneta.nifty.com/koneta_detail/1141008010565_1.htm.

[74] Proofpoint, Inc., “State of the Phish 2021,” [オンライン]. Available: 220252.37-pfpt-jp-a4-r-state-of-the-phish-2021.pdf.

[75] 株式会社NTTドコモ, “SMS拒否設定,” [オンライン]. Available: https://www.nttdocomo.co.jp/info/spam_mail/sms/.

[76] 株式会社Innovation & Co, “おすすめフィルタリングソフト８製品を徹底比較！選び方も解説！,” [オンライン]. Available: https://it-trend.jp/filtering/article/98-0002.

[77] 株式会社Innovation & Co, “EMMとは？MDMやMAMとの違いもわかりやすく解説！,” [オンライン]. Available: https://it-trend.jp/mdm/article/160-0005.

[78] 朝日新聞　DIGITAL, “婚活アプリの個人情報が流出か　免許証など171万件,” 朝日新聞社, 21 5 2021. [オンライン]. Available: https://www.asahi.com/articles/ASP5P5Q3PP5PULFA02S.html.

[79] 金融庁, “「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について,” 30 11 2018. [オンライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html.

[80] 消費者庁, “便乗悪徳商法の注意喚起,” 消費者庁, [オンライン]. Available: https://www.caa.go.jp/policies/policy/consumer_policy/information/notice/efforts_002.html.

[81] 独立行政法人　国民生活センター, “「新型コロナワクチン詐欺　消費者ホットライン」をご利用ください,” 14 5 2021. [オンライン]. Available: http://www.kokusen.go.jp/info/data/coronavirus_vshotline.html.

[82] L. Abrams, “CD Projekt's stolen source code allegedly sold by ransomware gang,” BleepingComputer, 13 2 2021. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/cd-projekts-stolen-source-code-allegedly-sold-by-ransomware-gang/.

[83] Security NEXT, “不正アクセス被害のランドブレイン、調査結果を公表 - ランサムウェアは「Cring」,” Security NEXT, 19 5 2021. [オンライン]. Available:

https://www.security-next.com/126310.

[84] K. M. a. W. Turton, “CNA Financial Paid $40 Million in Ransom After March Cyberattack,” Bloomberg, 21 5 2021. [オンライン]. Available: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

[85] U.S. DEPARTMENT OF THE TREASURY, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” 1 10 2020. [オンライン]. Available: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[86] aaa. [オンライン].

[87] 日本貿易振興機構（ジェトロ）, “GDPR適用開始から2年、域外適用の範囲を明示,” 4 6 2020. [オンライン]. Available: https://www.jetro.go.jp/biznews/2020/06/c81164d22cfa1274.html.

[88] MOTHERBOARD TECH BY VICE, “Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers,” 26 1 2021. [オンライン]. Available: https://www.vice.com/en/article/xgz7bd/facebook-phone-numbers-bot-telegram.

[89] I. NEWS, “5.33億人のFacebookユーザーの電話番号を含む個人情報、犯罪フォーラムで公開,” 4 4 2021. [オンライン]. Available: https://www.itmedia.co.jp/news/articles/2104/04/news016.html.

[90] LINE Corporation, “LINEプライバシーポリシー,” 31 3 2021. [オンライン].

NTT DATA
Trusted Global Innovator

Published on Friday, June 18, 2021

NTT DATA Corporation
Security Engineering Department
Hisamichi Otani, Chihiro Oyama, Ryo Hoshino, Junya Kawai, Yusuke Noro, Daisuke Miyazaki, Kazutaka Shimizu, Chiaki Endo, and Yuji Kamiya
nttdata-cert@kits.nttdata.co.jp