NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

1st Quarter of 2022

Table of Contents

1. Executive Summary

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

Cyberattacks on agricultural sector

In the U.S., cyberattacks targeting the increasingly IT-driven agricultural sector have been on the rise in recent years. We speculate that this is due to the increase in the number of IT systems in the agricultural sector that can be targeted for intrusion and cyberattacks by attackers, and the fact that the probability of a ransom being paid has increased as cyberattacks can now cause extensive damage to the entire food supply chain. At present, there have been no cyberattacks targeting farmers or agricultural corporations in Japan, but as the IT utilization in the agricultural sector advances in Japan, we expect that farmers and agricultural corporations will become targets of cyberattacks. Additionally, the Japanese agricultural sector is in the early stages of IT utilization, and education on information security has not yet spread to all farmers who are using smart devices. Therefore, it is important to educate farmers on how to prevent cyberattacks and how to respond in the event of a cyberattack while promoting IT in the agricultural sector. Furthermore, it is necessary to consider improvement in information security of IoT systems themselves so that farmers who are not IT experts can introduce IT safely.

New authentication mechanisms and countermeasure standards to prevent unauthorized online payments

Incidents of credit card information being compromised through attacks on e-commerce sites continue to occur. Taking this into account, the industry is promoting a transition to the new authentication mechanism, EMV 3-D Secure. EMV 3-D Secure is effective in preventing unauthorized use of credit cards, but it is insufficient as a measure against credit card data breaches. Even for e-commerce site systems that do not keep credit card information, it is necessary to strengthen the measures that conform to the new PCI DSS, which includes measures against web skimming attacks. This section explains what measures should be taken by organizations that build and operate e-commerce sites.

Security risks and solutions for the end of support for Internet Explorer 11

The support for web browser Internet Explorer 11 desktop application ("IE11") provided by

Microsoft ended in June 2022. After the end of support, there will be no security update program available and continuing to use IE11 will carry the risk of zero-day attacks. Corporate system administrators and web service providers should investigate whether there are any systems remaining in their companies that can only be viewed and operated using IE11. If there are any systems using IE11, please urge system personnel or developers to immediately modify the systems and migrate to systems that support the latest web browsers.

2. Featured Topics

2.1. Cyberattacks on agricultural sector

2.1.1. Increase in ransomware attacks on the agriculture and food sectors in the U.S.

In April 2022, the Federal Bureau of Investigation (FBI) issued an alert regarding the increase in ransomware attacks on the agriculture and food sectors [1]. According to the document, the technology and attack strategies of ransomware continued to evolve from 2021 to 2022, increasing the likelihood of attackers carrying out cyberattacks that have a serious impact on the food supply chain. The year before, in September 2021 as well, the FBI issued an alert on ransomware attacks targeting the agriculture and food sectors, indicating the severity of the issue [2]. Similar ransomware attacks targeting the agricultural sector have also occurred in Brazil, Canada, and Australia.

In recent years, the automation of farming operations using IoT and machine learning has been rapidly advancing. For example, IoT devices equipped with sensors and cameras are installed throughout the farm to collect information such as temperature, humidity, and hours of sunlight. Also, water and fertilizers are automatically applied to the farm based on the results of analyzing this information. In addition, pesticide spraying by drones and the use of unmanned tractors have saved labor in farming operations, and harvest and shipping quantities are now automatically managed using IT. The widespread use of IT technology in farming operations has led to improvements in the working environment and profitability.

Meanwhile, the agricultural sector has become a target of cyberattacks. Until now, sectors with a high dependence on IT, such as the critical infrastructure sector, the healthcare sector, and the manufacturing industry, have been the main targets of ransomware attacks. The agriculture sector had little connection with cyberattacks, as it was largely less dependent on IT. However, the increasing use of IT in agriculture has not only made it possible for attackers to launch cyberattacks, but has also halted various operations that rely on IT technology in the event of a successful cyberattack, seriously affecting the supply of agricultural products.

The FBI also reports that ransomware attacks in the agricultural sector are characterized by a concentration of the cyberattacks at specific times of the year, such as planting and harvesting. Not only is the crop production highly time-sensitive during planting, harvesting, and the period between harvesting and shipping, but the workload is also heavy during these periods, and any missed opportunities can result in significant losses. If IT-dependent farming and shipping operations were to stop due to a ransomware attack, they would have to be done manually until their restoration and the efficiency of the work would be significantly lower. Therefore, a ransomware attack that halts farming operations during these times can have a major negative impact on the entire food supply chain. As a result, farmers and agricultural corporations affected by ransomware are likely to pay the ransom to resume operations as soon as possible. Therefore, farmers and agricultural corporations have sufficient motivation to pay the ransom, and they are targeted by attackers.

Looking only at 2021 and beyond, various agricultural and food sector companies in the U.S., including agricultural cooperatives, have fallen victim to ransomware attacks. For example, in 2021, six grain cooperatives were hit by ransomware attacks in less than a month from September 15th to October 6th, during the harvest season. Some cooperatives suffered only a partial loss of administrative functions, while others experienced a complete shutdown of production activities. There have also been multiple cyberattacks on agricultural and food-related companies since the beginning of 2022, and the FBI warns that cyberattacks will continue to occur.

Attackers launch ransomware attacks in a variety of ways, but the FBI reports that the most common infection routes are email-based phishing and cyberattacks on remote desktops and software vulnerabilities. Secondary infections to related organizations through exploitation of shared networks and violations of managed services have also occurred [1, 2].

2.1.2. Cyberattacks in the agricultural sector in Japan

As for cyberattacks on the agricultural sector in Japan, data breaches through unauthorized access have been reported. In June 2022, an e-commerce site operated by an agricultural goods manufacturer was illegally accessed by an attacker, resulting in the leakage of over 5,000 pieces of personal information and 400 pieces of credit card information. In April 2022, an employee of an agricultural-related public interest incorporated association opened an email purporting to be from a related party, which led to EMOTET infection, causing email addresses and the contents of emails stored on the PC to leak. EMOTET is covered in our Quarterly Report on Global Security Trends for the third quarter of FY2021, so please refer to that report for more information [3].

Cyberattack trends such as ransomware attacks targeting farmers and agricultural corporations like those in the U.S. have not been seen in Japan yet. According to the number of companies and organizations by industry that suffered ransomware attacks in 2021 (Fig. 2-1) published by the National Police Agency, the largest number of such attacks occurred in the manufacturing industry, followed by the wholesale and retail industry, and none in the agriculture industry.

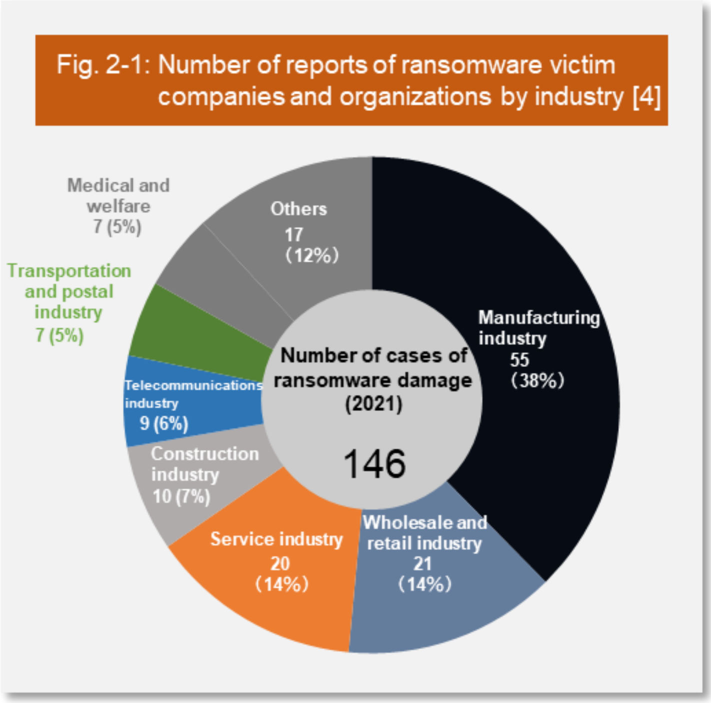


Fig. 2-1：Number of reports of ransomware victim companies and organizations by industry [4]

For the future, we believe it is extremely important to consider information security in the agricultural sector in Japan. The Ministry of Agriculture, Forestry and Fisheries has been leading the "The Smart Agriculture Demonstration Project" since 2019, with the goal of almost all farmers using data for agriculture by 2025 [5]. We predict that this will lead to further IT utilization in the future, beginning with the collection and use of data from sensors and cameras, followed by the automatic supply of water and fertilizers, and the automation of tasks using drones and robots. Such increasing use of IT in agriculture in Japan will create openings for cyberattacks, and increase the damage in the event of a successful cyberattack, making farmers and agricultural corporations more likely to become targets. In addition, we expect that farmers have not yet developed an awareness of information security, as the agricultural sector is in the early stages of IT adoption. Therefore, farmers and agricultural corporations are likely to be seen as soft targets by attackers, which increases the likelihood that they are targeted by cyberattacks.

Then what kind of cyberattacks are likely to be launched against the Japanese agricultural sector in the future? As mentioned earlier, there has been no trend of ransomware attacks targeting farmers and agricultural corporations in Japan. However, if the use of IT in the agricultural sector in Japan increases at this rate and attackers determine that Japanese farmers and agricultural corporations are willing to pay the ransom, we predict that they will launch ransomware attacks that will halt agricultural operations. In addition to ransomware attacks, there are also concerns about unauthorized access to IoT devices used in agriculture to alter data or change settings resulting in abnormal behavior that could cause damage. For example, if IoT devices are made to function abnormally, it may be possible to kill crops by giving them an inappropriate amount of water or fertilizer. As a specific problem in agriculture, the effects of such cyberattacks appear after the crops have grown over time, so there is a risk of not noticing the cyberattack or discovering it too late. Supply chain attacks are also a widespread problem in many industries. As in other industries, the agricultural sector may also see an increase in cyberattacks that use a company in the food supply chain as a stepping stone to launch secondary infections against other farmers and companies. In this supply chain attack, if any company in the food supply chain has weak security measures and allows a successful cyberattack, the entire food supply chain may be affected and products may not reach consumers. To avoid being affected by such cyberattacks, it is necessary to consider security as well as to promote the use of IT in agriculture.

2.1.3. Countermeasures against cyberattacks

To avoid becoming a victim of cyberattacks, it is important to first thoroughly implement basic security measures. For example, it is important to avoid carelessly opening files or hyperlinks attached to received emails, and to apply updates and patches for the OS, software, and firmware of all IT devices, including IoT devices, to eliminate vulnerabilities.

It is also important to take damage mitigation measures against malware infection. This includes regularly backing up data and servers, storing them disconnected from the network, and having a plan in place for recovering the system from the backups. It is also effective to identify critical functions and make a plan for operation in case the system goes offline.

The National center of Incident readiness and Strategy for Cybersecurity (NISC) operates a portal site to improve cybersecurity [6]. Please refer to the special page on the site that summarizes the measures and warnings provided by various public organizations against ransomware attacks [7].

2.1.4. Conclusion

In Japan too, the use of IT in agriculture has led to labor savings in farming operations and improvements in quality and yield. We expect that the probability of a cyberattack and its impact will increase accordingly. In the future, it will be necessary to take stronger information security measures to prevent cyberattacks, and to consider in advance how to contain the damage in the event of a cyberattack.

However, it is difficult for farmers to take sufficient security measures by themselves. According to a 2020 survey by the Ministry of Agriculture, Forestry, and Fisheries, more than 95% of agricultural businesses are run by individuals [8]. It would be difficult to expect farmers, who account for the majority of agricultural businesses, to consider, introduce, and operate adequate security measures. Therefore, in further promoting IT in agriculture in the future, it will be necessary not only to introduce IT devices but also to provide educational opportunities for farmers to acquire knowledge about security. In addition, to reduce the burden of introducing and operating security measures on individual farmers and agricultural corporations, we believe it will be necessary to bundle IoT devices with security features, for example, by installing security functions in agricultural IoT devices as standard features, making automatic log monitoring available, establishing a joint SOC, and including managed security service contracts. Furthermore, it is important to promote security measures throughout the entire food supply chain so that farmers can procure materials necessary for agricultural production and deliver their produce to consumers.

3. Data breach "New authentication mechanisms and countermeasure standards to prevent unauthorized online payments"

3.1. Current status of credit card data breach incidents

We have continuously discussed the incidents of credit card data breaches that exploited the vulnerability of EC-CUBE in this report for the first and third quarters of FY2021. In the first quarter of FY2022, there were still incidents of credit card data breaches as shown in Table 3-1, although it is unclear whether they were caused by the same vulnerability or not.

Table 3-1: Cases of credit card data breach incidents (Q1 FY2022)

#	Date Released	E-commerce site's name	E-commerce site's operator
1	2022/4/25	Iimono Aruyo!	Utsunomiya CATV corporation
2	2022/5/18	MACHATT ONLINE STORE	Machatt Co., Ltd.
3	2022/5/24	Minamoto Kitchoan Online Shop	Minamoto Kitchoan Co., Ltd.
4	2022/5/24	CHUOH Net Shop	Chuoh Kyouiku Kenkyusyo, Inc.
5	2022/6/7	Sweets Paradise Online Shop	Inoue Corporation
6	2022/6/7	Seiwa website, Seiwa Online Shop, Shinjidai Nogyojuku	Seiwa Co., Ltd.
7	2022/6/7	Tokyo Shirts Official Order Site	TokyoshirtCo.
8	2022/6/29	Sun City Online Mail Order Site	Sun City Co., Ltd.
9	2022/6/30	Doll Studio Hitotoe Online Shop	Matsunaga Co., Ltd.

Many of the incidents listed in Table 3-1 were caused by attackers exploiting vulnerabilities to gain unauthorized access and tamper with payment applications. In these incidents, credit card information was compromised even though the systems did not retain credit card information. From this, it is clear that simply not storing credit card information is insufficient as a security measure, and the system for e-commerce sites must take measures to prevent unauthorized access and tampering as described above.

Against this backdrop, the credit card industry is promoting the introduction of new authentication mechanisms and the establishment of security guidelines to prevent credit card data breaches and unauthorized use. Based on the trend of the industry, this section summarizes the security measures that should be taken by organizations building and operating e-commerce sites against credit card fraud and data breaches in online payment systems. First, the EMV 3-D Secure mechanism is described as a countermeasure against fraudulent use of credit card information, but this alone is not sufficient. To protect the system from attacks, it is necessary to take multilayered measures, and to prevent credit card data breaches, the security level of the system itself needs to be improved in the first place. In this issue, we will discuss the PCI DSS [9], which has been revised for the first time in about eight years as a countermeasure against credit card data breaches. In addition, a description of each organization listed in this section is provided in Table 3-2, Fig. 3-1, and Fig. 3-2.

Table 3-2: Description of each organization [10]

#	Name of Organization	Description
1	Issuer	A company that contracts with users to issue and provide cashless means of payment. Its main business is acquiring users and billing them.
2	Acquirer	A company that contracts with stores for the introduction of cashless payment methods and manages them. Its main business includes billing the issuer (a payment company contracted with credit card users) for the purchase amount and paying the merchants (stores).
3	Payment service provider (PSP)	A company that provides payment agency services. *Payment agency services are services that stand between merchants and credit card companies or payment service companies, handling contracts and settlements with multiple credit card companies and payment service companies on behalf of the merchants.
4	Merchant	A store or business that accepts payment by cashless means. Merchants are "affiliated" as they have a contract with a payment company and support its services.
6	International brand	A credit card brand that has a large number of merchants worldwide and is accepted internationally. Generally speaking, international brands refer to seven credit card brands: Visa, Mastercard, American Express, Diners Club, JCB, Discover Card, and UnionPay. (As of February 2019)

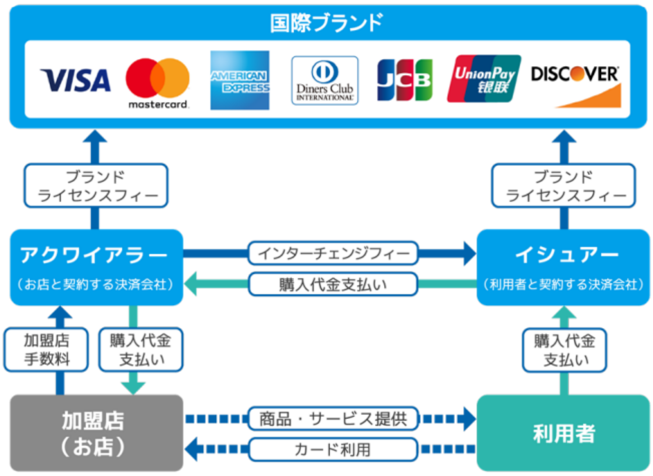


Fig. 3-1：Money flow in credit card payments [10]

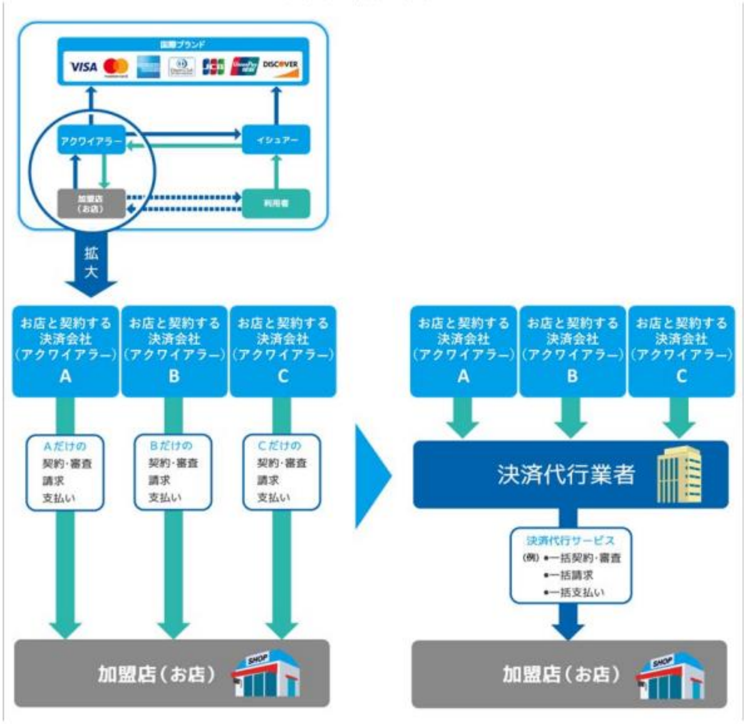

国際ブランド
アクワイアラー
イシュアー
加盟店（お店）
利用者
拡大
お店と契約する決済会社（アクワイアラー） A
お店と契約する決済会社（アクワイアラー） B
お店と契約する決済会社（アクワイアラー） C
Aだけの 契約･審査 請求 支払い
Bだけの 契約･審査 請求 支払い
Cだけの 契約･審査 請求 支払い
加盟店（お店）
SHOP
お店と契約する決済会社（アクワイアラー） A
お店と契約する決済会社（アクワイアラー） B
お店と契約する決済会社（アクワイアラー） C
決済代行業者
決済代行サービス
(例) •一括契約･審査
•一括請求
•一括支払い
加盟店（お店）
SHOP

Fig. 3-2：Role of payment service providers [10]

3.2. Discontinuation of old 3-D Secure and transition to EMV 3-D Secure

There is a service called 3-D Secure 1.0, which requires a password in addition to credit card information to perform authentication when making an online payment. This service was discontinued in October 2022, and after that, it was recommended to switch to a service that performs authentication in accordance with EMV 3-D Secure [11].

3.2.1. What is EMV 3-D Secure?

EMV 3-D Secure is a technology that improves on the shortcomings of conventional 3-D Secure 1.0 and incorporates mechanisms to improve usability and prevent fraudulent use, such as "reduction of the burden of password entry using risk-based authentication," "support for smartphone applications," "support for non-payment fields," and "introduction of multi-factor authentication [12]." In particular, "introduction of multi-factor authentication" helps prevent fraudulent use as it reduces the risk of impersonation by a malicious third party by requiring a one-time password or biometric authentication when requesting additional authentication.

3.2.2. Risk of owing compensation when EMV 3-D Secure is not installed

With this transition, there will be a change in the terms and conditions regarding the burden of compensation when the issuer (a payment company contracted with credit card users) makes a chargeback claim to a merchant or payment service provider (hereinafter, "PSP") [11]. The term "chargeback claim" refers to a claim by an issuer to a merchant or PSP through an acquirer (a payment company contracted with the store) for the reversal of credit card charges or sales in the event of unauthorized use of a credit card and the credit card user does not agree to pay the charges due to such use. Although it depends on the contract between the organizations and on each case that occurs, once a chargeback claim is approved, the merchant or PSP must pay for the unauthorized use, etc. In the past, with the introduction of 3-D Secure 1.0, a merchant could show that fraudulent use was not their responsibility, and the issuer compensated for the cost of fraudulent use incurred at the merchant or PSP that installed 3-D Secure. However, as shown in Table 3-3, after October 2022, under the rules of the major international brands, if the merchant does not have EMV 3-D Secure installed, the merchant will bear the cost, as the issuer will not compensate for it.

This means that if EMV 3-D Secure is not installed, there is a high risk that a malicious third party will succeed in fraudulent use, and the merchant will have to pay for the fraudulent use of the credit card by the attacker.

Table 3-3: Whether merchants/PSPs are responsible for payment in the event of fraudulent use [13]

Merchant security measures	Until October 2021	October 2021 to October 2022	October 2022 and thereafter
3-D Secure not installed	Responsible	Responsible	Responsible
Old 3-D Secure installed	Not responsible	Partially responsible	Responsible
EMV 3-D Secure installed	Not responsible	Not responsible	Not responsible

3.2.3. How EMV 3-D Secure works

Fig. 3-3 shows the flow of credit card online payment processing using EMV 3-D Secure.

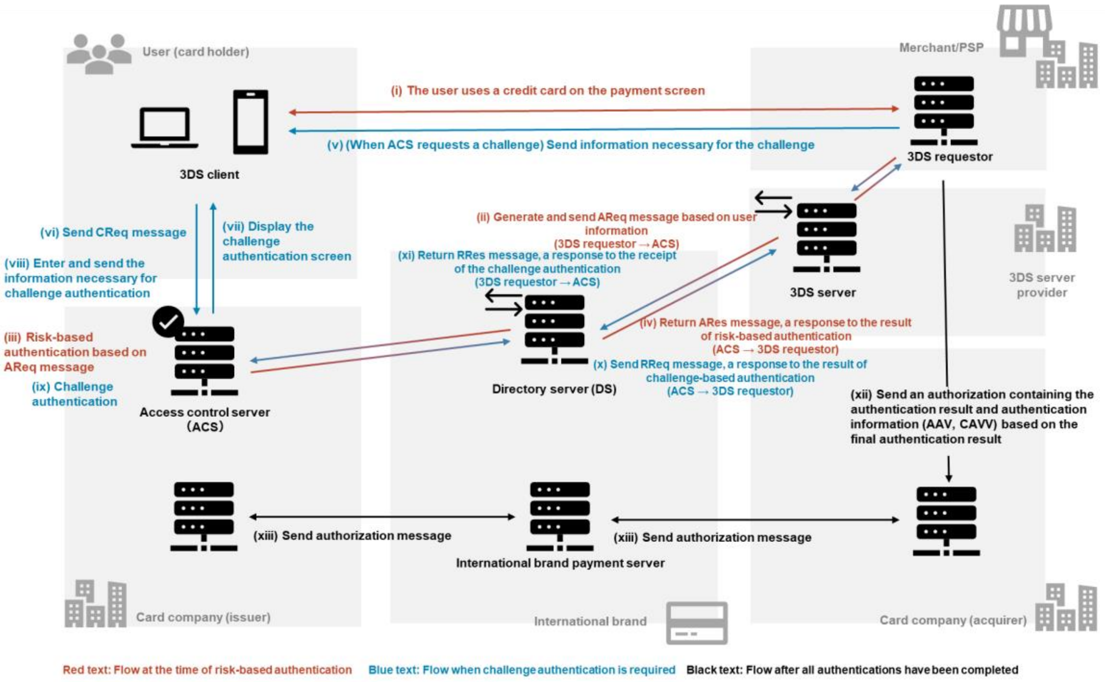

User (card holder)
Merchant/PSP
(i) The user uses a credit card on the payment screen
(v) (When ACS requests a challenge) Send information necessary for the challenge
3DS client
3DS requestor
(vi) Send CReq message
(vii) Display the challenge authentication screen
(viii) Enter and send the information necessary for challenge authentication
(ii) Generate and send AReq message based on user information (3DS requestor → ACS)
(xi) Return RRes message, a response to the receipt of the challenge authentication (3DS requestor → ACS)
3DS server
3DS server provider
(iii) Risk-based authentication based on AReq message
(ix) Challenge authentication
Access control server (ACS)
Directory server (DS)
(iv) Return ARes message, a response to the result of risk-based authentication (ACS → 3DS requestor)
(x) Send RReq message, a response to the result of challenge-based authentication (ACS → 3DS requestor)
(xii) Send an authorization containing the authentication result and authentication information (AAV, CAVV) based on the final authentication result
(xiii) Send authorization message
International brand payment server
(xiii) Send authorization message
Card company (issuer)
International brand
Card company (acquirer)
Red text: Flow at the time of risk-based authentication
Blue text: Flow when challenge authentication is required
Black text: Flow after all authentications have been completed

Fig. 3-3: Payment processing flow using EMV 3-D Secure [11]

As shown in Fig. 3-3, the basic payment processing follows the risk-based authentication flow ((i)-(iv)) indicated by the red arrows and red text. When the probability of fraudulent use is judged to be high during risk-based authentication and challenge authentication becomes necessary, the challenge authentication flow ((v)-(xi)) indicated by blue arrows and blue text is executed. After the two authentications have been successfully completed, the blackcolored flow ((xii)-(xiii)) is executed to determine that it is safe to settle the transaction with the credit card in question, and the merchant or the PSP contracted by the merchant sends a credit approval (authorization message) to the credit card company.

So what should an organization that builds and operates an e-commerce site, i.e., a merchant or an e-commerce site builder/operator contracted by a merchant, do when migrating from 3-D Secure 1.0 to EMV 3-D Secure?

Here, in the flow of online credit card payment processing, an organization that builds and operates an e-commerce site will be involved in new elements: the 3DS server provider and the 3DS server owned by the provider. When processing online payments using EMV 3-D Secure, a new communication connection is required from the 3DS requestor operating the e-commerce site to the 3DS server. Fig. 3-4 shows the other organizations and systems that an organization building and operating e-commerce sites must work with when establishing the new connection. Things to be addressed will vary depending on whether the system is built in-house or outsourced to a PSP.

3.2.4. What organizations that build and operate e-commerce sites should do

(1) In case the organization that builds e-commerce sites in-house introduces EMV 3-D Secure

If an organization builds its own e-commerce site, it is necessary to make some modifications to the system, such as implementing the 3DS SDK provided by the 3DS server provider in the system. In addition, there are some tasks that the organization needs to perform on its own, such as various applications related to the use of EMV 3-D Secure, and connection checks for functions that have been modified. The advantages of building in-house are that the organization can manage and understand the system and contracts by itself and can reduce the cost of outsourcing to a PSP. The disadvantages, on the other hand, are that the organization must perform many tasks in-house, which makes management more complicated, or that the organization must provide its own technical staff. Alternatively, the organization can outsource the system construction to other vendors, but in any case, it must have its own resources.

(2) In case the organization contracted with a PSP introduces EMV 3-D Secure

On the other hand, if an organization outsources some of its operations to a PSP, fewer changes need to be made to the system compared to building it in-house as the PSP will handle some of the connections and contract management related to the 3DS server on behalf of the organization. Also, there are two main types of contracts.

The first is where the merchant signs a merchant agreement directly with the acquirer and outsources only payment processing to the PSP. In this case, the merchant needs to sign a contract with both the acquirer and the PSP and deal with the system, but the PSP handles the other procedures with the 3DS server provider and information processing center on its behalf.

The second is when the merchant outsources both the merchant agreement with the acquirer and the payment operations to the PSP. In this case, the PSP also handles the contracting procedures between the merchant and acquirer, so the merchant only needs to sign the contract with the PSP and deal with the system in many cases.

The advantage of outsourcing to a PSP is that it simplifies handling contracts and systems. Conversely, the disadvantage includes the cost of outsourcing to a PSP and the fact that the contracts and some of the systems are outside the merchant's control. The details of outsourced operations vary depending on the contract with the PSP, but it is important to fully consider whether the PSP is a reliable company and whether there are any inconveniences in the contract.

Each organization that builds and operates an e-commerce site needs to consider the EMV 3-D Secure introduction according to the type of e-commerce site system they are operating. If the merchant has already outsourced payment services to a PSP, it is advisable to check the administrative aspects of the contract with the merchant's own rules, confirm the details with the outsourced company, and outsource part of the EMV 3-D Secure implementation work to them. Organizations that have built and are operating their own e-commerce sites may want to consider whether they should implement EMV 3-D Secure by themselves or outsource it to a PSP, taking into account their budget and their own rules.

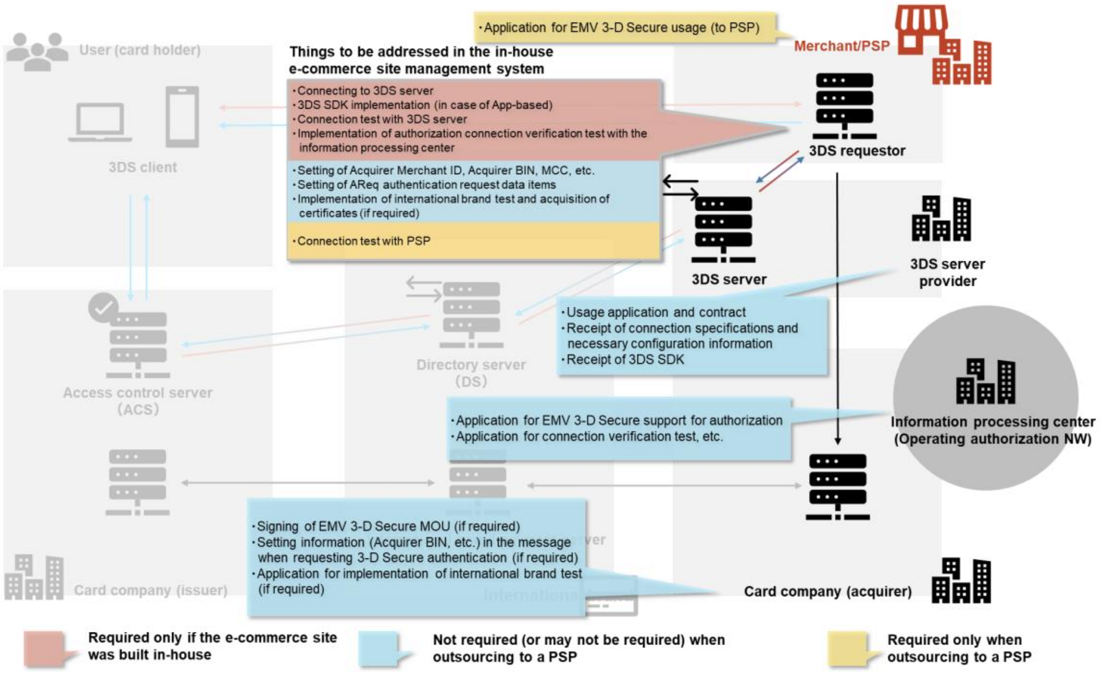

·Application for EMV 3-D Secure usage (to PSP)
User (card holder)
Things to be addressed in the in-house e-commerce site management system
·Connecting to 3DS server
·3DS SDK implementation (in case of App-based)
·Connection test with 3DS server
·Implementation of authorization connection verification test with the information processing center
·Setting of Acquirer Merchant ID, Acquirer BIN, MCC, etc.
·Setting of AReq authentication request data items
·Implementation of international brand test and acquisition of certificates (if required)
·Connection test with PSP
Merchant/PSP
3DS requestor
3DS client
3DS server
3DS server provider
Access control server (ACS)
Directory server (DS)
·Usage application and contract
·Receipt of connection specifications and necessary configuration information
·Receipt of 3DS SDK
·Application for EMV 3-D Secure support for authorization
·Application for connection verification test, etc.
Information processing center (Operating authorization NW)
·Signing of EMV 3-D Secure MOU (if required)
·Setting information (Acquirer BIN, etc.) in the message when requesting 3-D Secure authentication (if required)
·Application for implementation of international brand test (if required)
Card company (issuer)
Card company (acquirer)
Required only if the e-commerce site was built in-house
Not required (or may not be required) when outsourcing to a PSP
Required only when outsourcing to a PSP

Fig. 3-4: Things to be addressed by merchants when EMV 3-D Secure is introduced [11]

3.2.5. Attacks that EMV 3-D Secure cannot prevent

So far, we have described the changes that organizations that build and operate e-commerce sites should be aware of when migrating to EMV 3-D Secure. As explained in the introduction, EMV 3-D Secure is not a sufficient countermeasure. For example, if an attacker exploits a system vulnerability to gain unauthorized access to an e-commerce site and launch a web skimming attack, even if the e-commerce site uses EMV 3-D Secure, the credit card information can be intercepted by the attacker if the e-commerce site user enters the credit card information into the payment screen. EMV 3-D Secure is a system that detects and prevents unauthorized use based on the information and operations of the e-commerce site user and the credit card information entered into the payment screen. It does not detect or prevent an attacker from illegally entering an e-commerce site or inserting a intercepting function into the payment screen.

In other words, EMV 3-D Secure can prevent fraudulent use of credit card information after it has been compromised, but it cannot prevent the breach of credit card information itself. The only way to prevent the breach of credit card information is to take thorough security measures in the system itself, as has been done in the past.

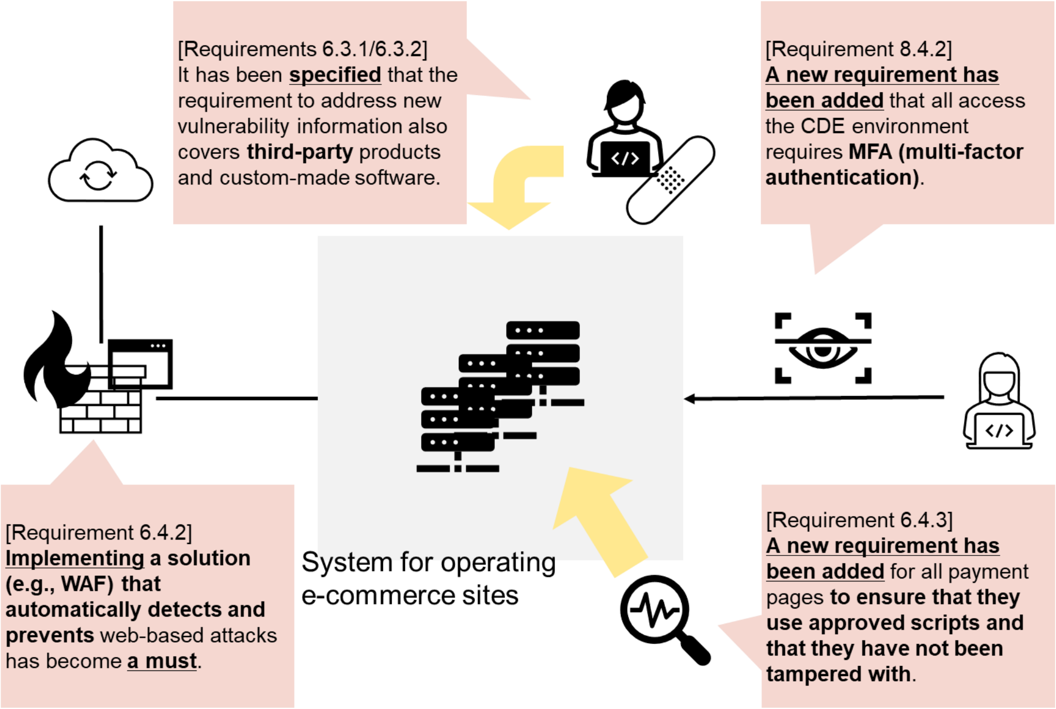
From the above, organizations that build and operate e-commerce sites need to strengthen measures against e-commerce site vulnerabilities and for e-commerce site security in order to prevent the breach of credit card information, in addition to the implementation of EMV 3-D Secure.

3.3. First major update of PCI DSS in about eight years

The Payment Card Industry Security Standards Council (PCI SSC), jointly established by five companies (American Express, Discover, JCB, Mastercard, and Visa), released PCI DSS v4.0, the first major update in about eight years, in March 2022 [9]. The update includes additional countermeasures against phishing and web skimming attacks related to credit card data breaches.

Fig. 3-5 picks up examples of requirements that have been updated in PCI DSS v4.0 based on a merchant's e-commerce site system. For example, as a countermeasure against web skimming attacks, a requirement to address script tampering, such as requirement 6.4.3, has been added. In addition, the requirements for vulnerability management of systems using third-party products or custom software, which were not specified before, are now specified as requirements 6.3.1/6.3.2. These requirements are designed to address the risk of vulnerabilities when using packaged software for e-commerce sites such as EC-CUBE.

There is no one-size-fits-all measure to prevent cyberattacks targeting e-commerce sites and it is important to implement a multilayered system protection mechanism for multiple possible attack points on the system to prevent various risks and attack methods. All entities that store, process, or transmit cardholder data or sensitive authentication data must comply with PCI DSS. However, we recommend that systems that comply with PCI DSS by not retaining cardholder data or sensitive authentication data also enhance e-commerce site vulnerability countermeasures and e-commerce site security measures in accordance with each requirement of PCI DSS.



[Requirements 6.3.1/6.3.2]
It has been **specified** that the requirement to address new vulnerability information also covers **third-party** products and custom-made software.

[Requirement 8.4.2]
A new requirement has been added that all access the CDE environment requires **MFA (multi-factor authentication)**.

[Requirement 6.4.2]
Implementing a solution (e.g., WAF) that automatically detects and prevents web-based attacks has become **a must**.

[Requirement 6.4.3]
A new requirement has been added for all payment pages **to ensure that they use approved scripts and that they have not been tampered with**.

Fig. 3-5: Examples of requirements updated in PCI DSS v4.0 [9]

3.4. Conclusion

In light of recent cases of credit card data breaches, the industry as a whole has been revising its systems and developing countermeasures. We recommend that organizations that build and operate e-commerce sites implement EMV 3-D Secure to prepare for risks such as unauthorized use and avoidance of chargeback obligations after a credit card data breach.

In addition, at the time of implementation, the organizations need to consider implementation according to the type of e-commerce site system they are operating. If the organization has already outsourced payment services to a PSP, it is advisable to check the administrative aspects of the contract with the organization's own rules, confirm the details with the outsourced company, and outsource part of the EMV 3-D Secure implementation work to them. Organizations that have built and are operating their own e-commerce sites may want to consider whether they should implement EMV 3-D Secure by themselves or outsource it to a PSP, taking into account their budget and their own rules.

Since EMV 3-D Secure alone cannot prevent card data breaches, guidelines such as PCI DSS should be consulted, and we recommend that systems that comply with PCI DSS by not retaining cardholder data or sensitive authentication data also enhance e-commerce site vulnerability countermeasures and e-commerce site security measures in accordance with each requirement of PCI DSS. It is important to protect the system in multiple layers with multiple measures, such as preventing data breaches by strengthening vulnerability countermeasures and security measures for e-commerce sites, and preventing unauthorized use with EMV 3-D Secure.

4. Data breach "Lessons learned from the OAuth token leak incident"

On April 15, 2022, GitHub, Inc. announced that an incident of unauthorized access to GitHub's private repositories using users' OAuth tokens had occurred. According to the company, dozens of private repositories, including not only those of GitHub but also of npm, were illegally accessed in this incident, and 100,000 users' information was leaked from npm's repositories [13]. This section examines the intentions of attackers and countermeasures against unauthorized access from this OAuth token leak incident.

4.1. Timeline of the OAuth token leak incident

In April 2022, a cyberattack occurred in which someone illegally accessed GitHub's private repositories and stole data by misusing stolen OAuth tokens of users [13]. The OAuth tokens stolen by the attacker were reportedly not held at GitHub, but were stolen from third-party applications Heroku and Travis-CI, which are integrated with GitHub. In addition, according to GitHub's analysis, this cyberattack was a highly targeted attack that carefully selected its targets by misusing OAuth tokens. Table 4-1 below shows the timeline of the OAuth token leak incident as announced by GitHub.

Table 4-1: Timeline of the OAuth token leak incident at GitHub

Date	Events
2022/4/7	The attacker gains unauthorized access to Heroku's database and steals OAuth tokens.
2022/4/9	The attacker misuses the OAuth token stolen from Heroku to illegally download data from private repositories on GitHub, etc.
2022/4/12	GitHub's security team begins investigation and discovers unauthorized access to npm's repositories.
2022/4/13, 14	GitHub notifies Heroku and Travis-CI of its findings.
2022/4/13	Heroku begins deactivating stolen OAuth tokens.
2022/4/15	GitHub and Heroku post this incident on their blogs.
2022/4/17	All Heroku Dashboard OAuth tokens have been disabled.
2022/4/18	Travis-CI posts this incident on its blog.
2022/4/18	GitHub notifies affected users and calls for action.
2022/4/27	GitHub releases results of analysis indicating that the attack was a targeted attack against multiple organizations.
2022/5/5	Heroku implements password reset.
2022/5/26	GitHub reports details of leaked data.

4.2. Explanation of this incident

(1) Causes

The overall picture of this incident is shown in Fig. 4-1. The OAuth tokens that were leaked were authorization tokens that allowed access to GitHub's private repositories. In this incident, the OAuth tokens issued by GitHub for the OAuth applications Heroku and Travis-CI were somehow leaked and ended up in the hands of the attacker, allowing him/her to illegally log in to GitHub's private repositories. According to Heroku's announcement, it is not clear how the intrusion was initiated, but it appears that the attacker somehow got into Heroku's internal machine, reached the database that manages OAuth tokens, and extracted information from the database [14].

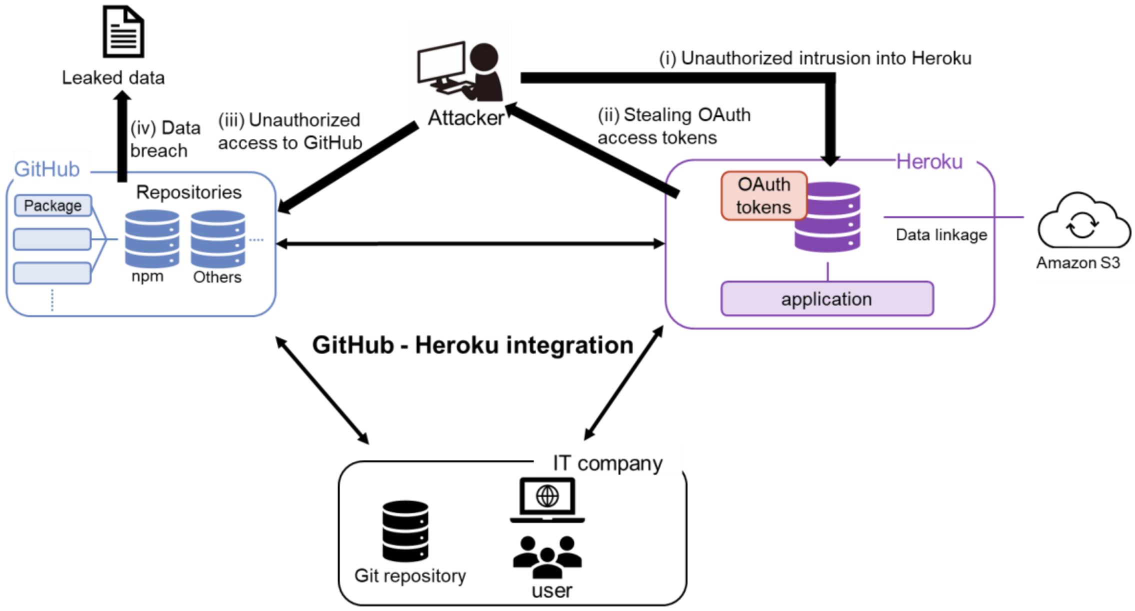


Fig. 4-1: Overview of the OAuth token leak incident

(2) Impact

What was the impact of this attack described in (1)? The following is a list of the information confirmed to have been leaked [15].

- OAuth tokens issued by GitHub
- Backup data for skimdb.npmjs.com
- Information on 100,000 registered users of the npm's repositories since 2015 (user names, password hashes, and email addresses)
- Manifests and package metadata for all private npm packages as of April 17, 2021
- A list of CSV data including the names, public version numbers, and archives of all private packages of npm as of April 10, 2022
- Private packages for two organizations

As mentioned above, npm-related leaks have been found. Information on 100,000 registered users and archives of all private packages have been leaked from npm's repositories. In this regard, GitHub stated that after analyzing logs and events and checking version hashes, the attacker was unlikely to have tampered with public packages on GitHub or released new versions for existing packages, but did not provide any further details about the damage to private repositories.

(3) How the companies responded

In this incident, GitHub, Heroku, and Travis-CI have taken several actions.

GitHub, through Heroku and Travis-CI, sent notification e-mails to the users concerned, informing them of the damage caused by this incident, the measures taken by GitHub, and emergency contact information. Additionally, GitHub has announced that two-factor authentication will be mandatory by the end of FY2023, a move that is seen as an attempt to strengthen security, although it is unclear whether this is related to the incident [16].

Heroku has refreshed the credentials of all accounts that could be logged in illegally with the leaked OAuth tokens [14]. Heroku has also informed users to check Heroku's official blog regularly for updates and respond appropriately.

Travis-CI has stated that there are no issues or risks regarding their customers, as there have been no unauthorized accesses to their repositories or data by misusing the leaked OAuth tokens. Therefore, they do not appear to have taken any particular measures [17].

4.3. Attacker's intent

According to information from GitHub, the attacker listed organizations that they could access by using OAuth tokens, and then selected target organizations and gained unauthorized access to those organizations' private repositories [14]. The attacker also successfully gained unauthorized access to npm's repositories, and there is information that the attacker was also able to access npm's S3 bucket. Although it is only speculation, based on the fact that the attacker listed and selectively targeted organizations, we do not think the primary goal of the attacker was to steal a large amount of personal information from GitHub. While stealing information such as access tokens and personal information from GitHub may indeed be one of the attacker's goals, obtaining such information and gaining unauthorized access to GitHub alone would not yield significant profits for the attacker. Therefore, we suspect that the attacker's main goal was to tamper with product code, install backdoors, infiltrate many organizations, and launch a supply chain attack against target organizations. Indeed, GitHub also reported analysis results suggesting that the attack was a highly targeted attack [13].

In this incident, as far as GitHub's investigation of repositories published on GitHub is concerned, no tampering with source code or suspicious files were found. However, private repositories on GitHub cannot be investigated because their owners restrict access. There is a concern that the attacker may have tampered with the source code in private repositories that are accessible to them.

4.4. Supply chain attacks on development environments

The following describes how software development companies should prepare for a software supply chain attack in which an attacker uses a development environment such as GitHub as a foothold.

(1) Comparison with similar incidents that occurred in a development environment

As mentioned in 4.3, GitHub reported that no tampering or other damage was found in the public repositories. If we only consider the scope of the investigation conducted by GitHub, the incident resulted in unauthorized access to GitHub and the theft of information from public repositories, but no further damage occurred. A case similar to this is the Mercari Inc. incident discussed in the Quarterly Report on Global Security Trends for the first quarter of FY2021 [18]. The Mercari incident [18] was a software supply chain attack in which the attacker attacked Codecov, a cloud service for developers, and attempted to infiltrate the development environments of the service's users, one after another. In the Mercari incident, the attacker was unable to intrude into Mercari's production environment, and their attempts to deploy a program with backdoors and web skimmers into the source code were unsuccessful.

However, in the case of the GitHub incident, the private repositories, which GitHub cannot check, are at risk of having programs with backdoors installed by the attacker. If a product with a backdoor was deployed and the breach was spread to multiple organizations, this incident would be similar to the incident of SolarWinds Worldwide, LLC. covered in the Quarterly Report on Global Security Trends for the third quarter of FY2020 [19]. In the SolarWinds incident [19], the attacker intruded into the SolarWinds' development environment and deployed a backdoor into the source code of the Orion Platform, an operational monitoring software. Several user companies downloaded and installed the Orion Platform update containing that backdoor, and the attacker got into the user companies through the backdoor and caused damage. In other words, this incident of the OAuth token leak appears to be of the type of the Mercari incident because GitHub has announced that there is no tampering in the repositories, but if the tampering occurred in a private repository that GitHub cannot investigate and the program is deployed without realizing it, it may have developed into a software supply chain attack like the SolarWinds incident.

(2) Countermeasures against software supply chain attacks on development environments

Based on the two past incidents, we propose security countermeasures against software supply chain attacks that target development and production environments.

There are multiple countermeasures against software supply chain attacks, but preventing the production environment from being compromised is most important. In past incidents too, damage has been limited by preventing the intrusion into the production environment. Therefore, to prevent attackers from entering the production environment, you should restrict who can connect, and control access. Even if only the production environment is made strong, in a DevOps environment, if an attacker is able to enter the development environment, they can alter the source code and deploy a program containing backdoors or malware to the production environment. This would allow the attacker to enter the production environment as well. Therefore, even for development environments, appropriate connection restrictions and access controls are necessary. Preventing identity theft using multi-factor authentication, which GitHub has announced will be mandatory in the future, is also an effective measure for DevOps environments. Even with the above measures in place, unauthorized access may still be possible. In such cases, serious problems will be avoided by finding any source code tampering or any backdoor or malware hidden in the program before the program is released. By properly managing changes and checking through an established review process, it is possible to identify source code tampering or malicious code before the release.

The measures listed here are numbers 5, 7, and 8 of the "Protect your code repository" within the UK National Cyber Security Centre's (NCSC's) "Secure development and deployment guidance." [20] [21] [22] In addition to these, the guidance provides effective measures in an easy to understand manner. It is also necessary to implement a wide range of operational and risk management measures, such as establishing a management system for the products and services being introduced and an incident response system. Various measures like these are documented and made available by public organizations. The U.S. National Institute of Standards and Technology (NIST) has published the document "SP800-161" on supply chain risk management, while the European Union Agency for Cybersecurity (ENISA) has published "Threat Landscape for Supply Chain Attacks," which summarizes the results of its analysis of supply chain attacks and their countermeasures. It is important to implement these measures as well.

4.5. Conclusion

The OAuth token leak incident was a large-scale software supply chain attack, if we assume that the attacker obtained numerous credentials from third-party applications and attempted to breach multiple organizations through their private repositories. And this is a complex and sophisticated cyberattack because it combines methods such as stealing credentials and OAuth tokens from third-party applications linked to GitHub, targeting DevOps environments in the cloud, and distributing tampered software to launch software supply-chain attacks. However, we can learn security measures to prevent OAuth token leak incidents from previous incidents like the Mercari and SolarWinds incidents. In other words, it may have been a complex and sophisticated cyberattack, but it was by no means an unpreventable attack.

Software development companies must strengthen their security measures by referring to other sophisticated incidents as well as the security guidelines of public organizations, such as the "Protect your code repository" included in NCSC's "Secure development and deployment guidance" in order to counter cyberattacks that could evolve from an OAuth token leak incident to a software supply chain attack.

5. Vulnerability "Security risks and solutions for the end of support for Internet Explorer 11"

As of June 16, 2022 (Japan Standard Time), support for the Internet Explorer 11 desktop application ("IE11"), a web browser provided by Microsoft Corporation, has ended. After the end of support, security updates are no longer provided, which may increase security risks. This section discusses the impact and security risks that users and companies will face as a result of the end of support for IE11, as well as countermeasures against these risks.

5.1. What are the impact and countermeasures for the end of IE support after about 27 years of history?

IE11 is a web browser developed and provided by Microsoft Corporation. The company started providing the first IE in 1995 as an extension of Windows 95, which also triggered the spread of the Internet. Since then, IE has led the Internet as the standard web browser for Windows, and by the year 2000, IE accounted for more than 90% of the market [23].

So why has IE support come to an end as of 2022? One reason is that IE did not conform to the standards set by the World Wide Web Consortium (W3C), a standardization body for web browser-related technologies. Microsoft responded by providing updates whenever vulnerabilities were found in IE, but each time an update or unique feature was added, problems arose, such as slow operation. Meanwhile, web browsers compliant with W3C standards emerged on the Internet one after another, and users dissatisfied with IE's usability shifted to Google Chrome and other browsers that were simpler, moved faster, and were updated more frequently, gradually reducing IE's market share. As a result, with IE's market share declining, in 2015 Microsoft terminated IE's development and announced Microsoft Edge, the successor web browser to IE. Edge is compliant with W3C standards. Then, on June 15, 2022, Microsoft discontinued support for IE11, and Microsoft Edge with "Internet Explorer Mode" ("IE Mode"), which is fully compatible with IE11, officially became the standard Windows web browser.

5.1.1. Affected targets

The end of support applies to IE11 that comes with Windows 10 client SKU version 20H2 or later and Windows 10 IoT version 20H2 or later [24]. Meanwhile, support for IE on Windows 7, Windows 8.1, Windows 10 LTSC/LTSB, and Windows Server is not yet terminated. Support for IE will continue until the end of support for the respective operating systems.

In addition, support for IE mode in Microsoft Edge on each OS will be discontinued along with the lifecycle of that OS. Microsoft has announced that IE mode will continue to be supported until at least 2029, if the OS support ends in 2029 or later. The end date of IE mode support after 2029 is not yet determined and will be announced by Microsoft one year prior to the end date of support.

Table 5-1: IE11/IE mode support termination schedule by OS [24]

OS version	Application	Support expiration
Windows 7	IE IE mode	January 2020* January 2022
Windows 8.1	IE/IE mode	January 2023
Windows 10 Enterprise Version 20H2	IE IE mode	June 2022 May 2023
Windows 10 Enterprise Version 21H1	IE IE mode	June 2022 December 2022
Windows 10 Enterprise Version 21H2	IE IE mode	June 2022 June 2024
Windows 11 Enterprise Version 21H2	IE mode	October 2024
Windows 11 Enterprise Version 22H2	IE mode	October 2025
Windows 10 Enterprise 2015 LTSB	IE/IE mode	October 2025
Windows 10 Enterprise 2016 LTSB	IE/IE mode	October 2026
Windows 10 Enterprise LTSC 2019	IE/IE mode	January 2029
Windows 10 Enterprise LTSC 2021	IE/IE mode	January 2027
Windows Server 2012	IE/IE mode	January 2023
Windows Server 2016	IE/IE mode	January 2027
Windows Server 2019	IE/IE mode	January 2029
Windows Server, version 20H2	IE/IE mode	August 2022
Windows Server 2022	IE IE mode	January 2031 January 2029

*OS support for Windows 7 ended in 2020. However, if an organization has purchased an Extended Security Update (ESU) license for corporate users, OS support will be extended through January 2023. In this case, support for the IE11 desktop application will also be extended until January 2023 to match the OS support expiration date.

5.1.2. IE security risks after the end of support

Microsoft's official blog had a post in February 2019 that recommended using the latest web browsers, saying that using IE as the default web browser is risky [25]. Chris Jackson, the company's cybersecurity architect, stated that by continuing to use IE, companies will have "technical debt." Despite the discontinuation of IE development in 2015, companies still continue to use IE. According to Statcounter, a global web browser share survey service, 1.71% of people in Japan were still using IE as of August 2022, when support was no longer available [23]. Although IE's share has been gradually declining from over 50% a decade ago, IE still has a certain share in Japan compared to the global IE usage rate of 0.79% as of August 2022.

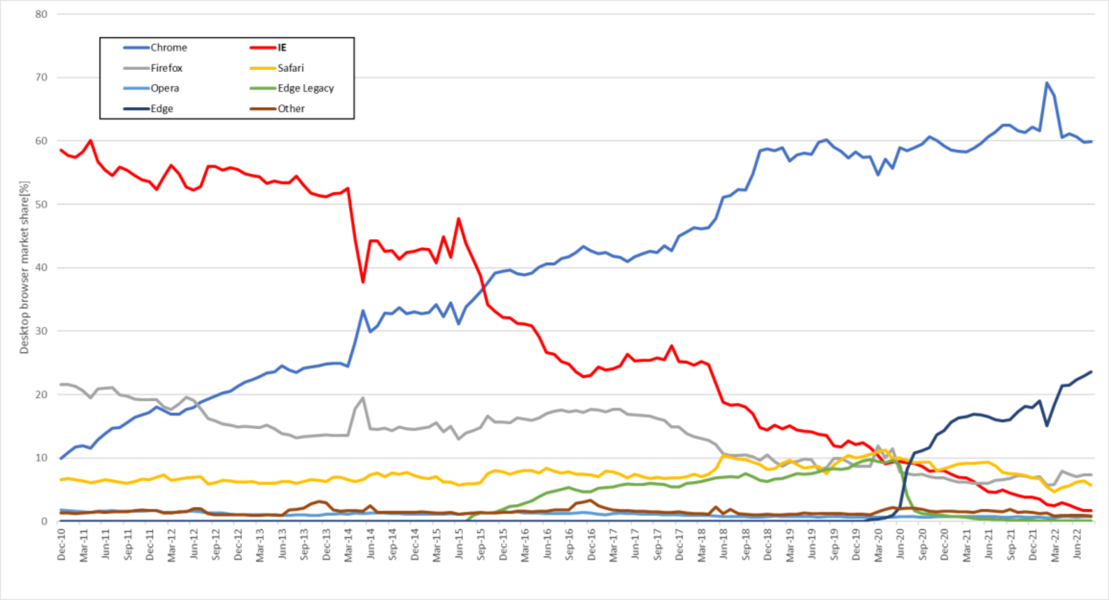


Fig. 5-1: Trends in desktop browser market share in Japan [23]

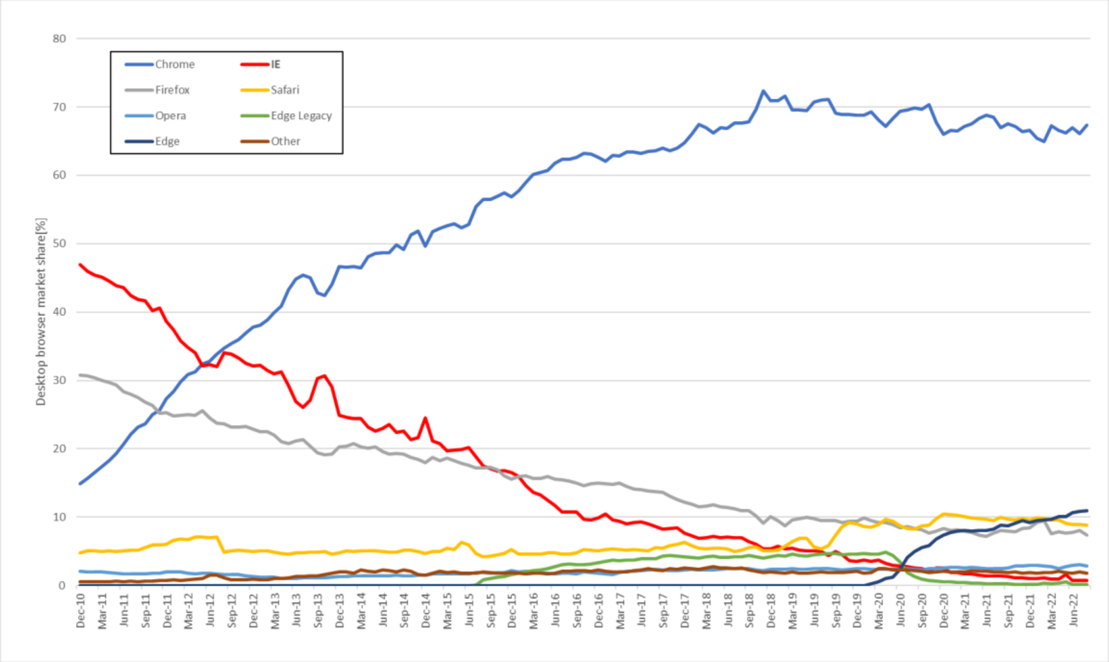


Fig. 5-2: Trends in desktop browser market share all over the world [23]

One of the reasons why IE maintains certain share in Japan is the existence of business systems and web applications that were developed assuming that they would be accessed with IE. As IE had a high market share from the early days of the Internet, it has been adopted as the user interface for many business systems. Changing from IE to the latest web browsers may cause concerns that the system may not work properly and may also burden on-site workers, who may have to change business operations to compensate for the lost functionality. Migration costs and a lack of resources may have delayed the migration from IE to Microsoft Edge or other web browsers. This may be why companies are still using IE.

However, continuing to use IE after its support has expired entails security risks. The leading security risk is zero-day vulnerabilities and zero-day attacks. A zero-day vulnerability is a vulnerability for which the software developer has failed to provide a patch or update, and a zero-day attack is an attack that exploits a zero-day vulnerability. Zero-day vulnerabilities could occur in any web browser or application. The risk of zero-day attacks is particularly high for IE, which is no longer supported, as no updates are provided even if a vulnerability is discovered. Examples of attacks that exploit web browsers include drive-by download attacks, in which users accessing a malicious website are infected by downloading spyware, ransomware, or other malicious programs via their web browsers, and watering hole attacks, in which sites frequently accessed by the attack target are tampered with to infect them with malware.

If malware exploits a zero-day vulnerability in IE to intrude into a corporate user's machine, there is a risk of information leakage, unauthorized access, damage from ransomware, or being used as a stepping stone for other attacks. IE, which is no longer supported, is an easy target for attacks, and even if vulnerabilities are discovered, security patches are not available, so the probability of a successful attack is high. While it is easy to imagine the significant costs involved in responding to a security incident, it is also important to remember that the negative impact on a company's brand image is also significant. If an incident occurs due to the continued use of IE, which is no longer supported by Microsoft, the loss of public trust and damage to business is immeasurable. From a long-term perspective, the risk of continuing to use the unsupported IE11 is significant, and if an incident should occur, the cost of damage could be much greater than the cost of migration.

5.1.3. Required countermeasures

This section describes the security measures that will be required following the end of IE support by Microsoft. Company employees/general users and system administrators/web service providers should implement the following countermeasures [26].

(1) Company employees/general users

According to Microsoft, after the end of support for IE on Windows 10 on June 15, 2022, if monthly cumulative updates are applied, attempting to launch IE on Windows 10 to display web pages will automatically redirect to Microsoft Edge. However, if the device has joined the company's Windows domain, the above automatic redirection may not occur because it is subject to the presence or absence of the IE disable policy in the group policy [24]. In that case, it is recommended to use a different web browser instead of using IE11. If users want to view web content with IE11, they can use IE mode in Microsoft Edge, which allows them to view web content in the same way as in IE11. Note that to use IE mode, the MSHTML engine of IE11 is required, so be careful not to uninstall or remove IE11.

(2) System administrators/web service providers

System administrators and web service providers should inform IE11 users to change their standard web browser to the latest supported web browser such as Microsoft Edge, Google Chrome, Safari, Firefox, etc. after the end of support. System administrators and web service providers should also check whether there are any systems, websites, or business applications in their company that can only be viewed or operated using IE11, and if so, ask system personnel or developers to modify them so that they can operate properly using an alternative web browser. System administrators should also set up an IE disable policy in the company's Windows domain group policy and instruct employees to apply the monthly cumulative Windows updates to disable IE11 as soon as they are ready to migrate from IE11. One thing to note is the expiration date for IE mode support. Microsoft will continue to support the MSHTML engine in IE, which will remain as IE mode. Microsoft has announced that they will support IE mode until 2029, but support after that is not yet determined, which means that there is a risk that IE content may become unviewable using IE mode. Please proceed with content modification and web browser migration as soon as possible.

5.2. Conclusion

Using services or applications that are no longer supported and will no longer receive program updates carries the risk of zero-day attacks. The end of support for IE11, Microsoft's web browser that has been widely used by individuals and companies for a long time since the early days of the Internet, is an issue that needs to be addressed urgently, especially for companies. Due to the fact that IE11 has been widely used as an interface for internal business applications, it may not be easy to migrate to the latest web browser. However, once an incident related to IE11 occurs, the negative impact on business in terms of damage cost, cost of incident response, and lost opportunities due to loss of public trust is immeasurable. System administrators and web service providers should investigate whether there are any systems remaining in their companies that can only be viewed and operated using IE11. If there are any systems using IE11, please urge system personnel or developers to immediately modify the systems and migrate to systems that support the latest web browsers. If possible, apply the IE disable policy after the migration is completed, and disable IE11.

6. Malware and ransomware "Ransomware damage increasing in SMEs"

Ransomware remains a major threat. While ransomware has attracted public attention with news stories about large corporations and critical infrastructure being victimized by ransomware, in reality, attacks occur regardless of industry or company size, so ransomware is a threat that everyone must take seriously. Small and medium-sized enterprises (SMEs), in particular, are experiencing an increase in ransomware damage due to insufficient security measures compared to large companies, and they need to promote overall security measures, including ransomware countermeasures, as soon as possible. This section examines the reasons why SMEs are frequently targeted by ransomware attacks, and then presents the actions that SMEs can take to combat ransomware.

6.1. Overview of ransomware damage among SMEs

6.1.1. Increasing ransomware damage to SMEs

According to the "10 Major Security Threats [For Organizations]" [27] released by the Information-technology Promotion Agency, Japan (IPA), "damage caused by ransomware" continued to be No. 1 from the previous year. According to a report by the National Police Agency [28], the number of ransomware damage cases has been steadily increasing since the second half of 2020 (Fig. 6-1). From this, we expect that ransomware damage will continue to increase in 2022.

Against this backdrop, ransomware damage to SMEs is on the rise. According to a National Police Agency report [28], the National Police Agency identified 146 cases of ransomware damage in FY2021, of which 79 (54%) were to SMEs (Fig. 6-2). In ExtraHop's survey on organizational cybersecurity [29], 20% of organizations surveyed said they would not disclose a cyberattack even if they had one. We also expect that SMEs tend to have incident response rules that are not as well developed as those of large companies, and that there are more cases of damage that are not reported than in large companies. Therefore, we think that the actual number of ransomware damage cases among SMEs is higher than that reported by the National Police Agency.

The report also found that 43% of the companies hit by ransomware attacks required more than 10 million yen in recovery costs, and that some companies required a recovery period of two months or more.

Ransomware may not only shut down a company's systems and halt its business activities, but can also cause secondary damage, such as data breaches and the spread of damage to business partners. In fact, double extortion, which involves threatening to publish stolen information if the ransom is not paid, is rampant, and the public disclosure of leaked personal information can lead to a loss of trust in the company. In recent years, a new technique called quadruple extortion has emerged that could corner companies even more than double extortion. Quadruple extortion is an extortion method that, in addition to double extortion, threatens to suspend services through a DoS attack or to contact the victim's customers, business partners, or employees to urge them to pay a ransom. These clearly have a negative impact on the survival of the business and the company's credibility. In other words, once infected with ransomware, significant damage can occur even without making ransom payments. Especially for SMEs, whose corporate strength is lower than that of large companies, damage from a ransomware attack and significant recovery costs can threaten the survival of their business.

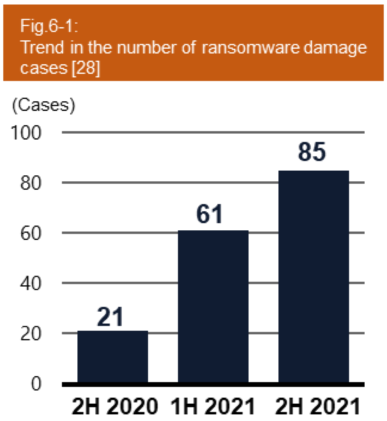


Fig. 6-1： Trend in the number of ransomware damage cases [28]

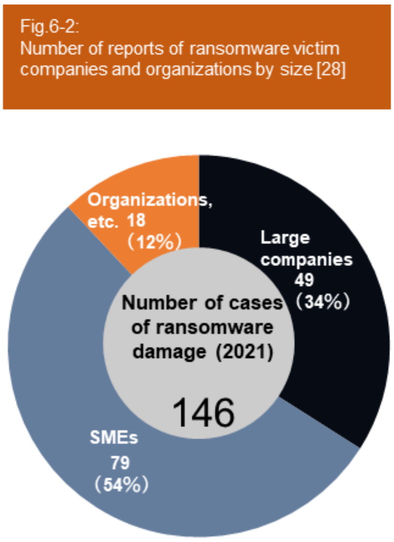


Fig. 6-2： Number of reports of ransomware victim companies and organizations by size [28]

6.1.2. SME ransomware cases (Q1 2022)

In the first quarter of FY2022 too, there were several reports of ransomware damage among SMEs (Table 6-1). None of the incidents had a significant impact on the companies' operations. However, since the attackers gained unauthorized access to the servers, the risk of secondary damage and loss of corporate credibility, as described in 6.1.1, remain. To prevent such risk from occurring, SMEs should promote security measures as soon as possible.

Table 6-1: Major cases of ransomware damage among SMEs in the first quarter of FY2022

No.	Date of incident	Victim	No. of employees	Incident overview
1	April 2	Gekkeikan Sake Company, Limited	365	The company announced that it had suffered a ransomware attack through unauthorized access, and that a large amount of personal information, including that of its customers, could have been leaked [30].
2	April 8	Keisei Construction, Inc.	326	The company announced that a server operated by the company had suffered unauthorized access and that some data had been encrypted [31].
3	May 11	Riken Nosan-Kako Co,. Ltd.	210	The company announced that the data in the server had been encrypted and that the company's internal systems had been shut down. The company explains that operations have resumed since May 12, but that it will take some time to fully restore the core system [32].
4	June 1	Iware, Co., Ltd.	63	A suspected ransomware attack on the server of JOBA, a service for returnee students operated by the company, resulted in the encryption of internal data [33].

6.1.3. Case of Handa Hospital

The following is a case of ransomware damage that occurred due to the failure of an SME to take appropriate security measures. In the early hours of October 31, 2021, the main information systems, including the electronic medical record system, at Handa Hospital, a municipal hospital in Tsurugi-cho, Tokushima Prefecture, were infected with ransomware, which encrypted files, as a result, rendering the systems unusable for about two months. Although the hospital was able to maintain its operations by reducing them, the lack of the system forced the staff to rely on manual procedures, resulting in a significant impact on the patients and the local medical system. On June 16, 2022, Handa Hospital released an investigative report [34] prepared by a panel of experts that summarized the details of the incident.

Based on the report, we can unravel the cause of the incident. The main cause was the lack of personnel to promote security measures. Handa Hospital had only one IT staff member and was unable to take appropriate security measures. As a result, the design, construction, operation, and maintenance of the system were all outsourced to a contractor. However, due to the ambiguity of responsibilities between the outsourcer and the contractor, vulnerabilities were left unaddressed, creating opportunities for attackers to carry out cyberattacks. In addition, the lack of personnel was also due to a shortage of budget. In the budget planning for the municipal hospital, improving profits took precedence, so it would have been difficult to secure a budget for security incidents that had not yet occurred.

In the Handa Hospital case, we believe that the lack of resources to implement security measures and the lack of management understanding of the importance of security measures were the causes behind the incident.

6.2. Why SMEs?

6.2.1. Background on why SMEs are heavily targeted

In 6.1, it was mentioned that ransomware attacks on SMEs have been increasing in recent years. In this section, we will examine the reasons why ransomware attacks target SMEs.

From the attacker's perspective, we consider the causes of targeting SMEs. The attacker's main goal is to gain money. Any industry and any size company can be the target of an attack, as long as the attacker can ultimately gain money. In other words, attackers are not targeting specific industries or company sizes, but instead attack various organizations with ransomware. As a result, ransomware attacks are successful and cause damage to companies that keep themselves open to attack. "Open" here means neglect of vulnerabilities in IT equipment and software, and insufficient employee security literacy due to lack of security training. In addition, "Cybersecurity Survey of Workplaces" conducted by Nikkei BP Consulting shows that the percentage of employees working for large companies who answered "Sufficient" to a question asking about the level of realization of cybersecurity measures at their workplace was nearly 20 points higher than that of employees working for SMEs. In other words, SMEs are more open to attack than large companies, hence them being more vulnerable to ransomware attacks.

For example, the main method of ransomware attacks that occurred in Japan in FY2021 was to exploit a VPN vulnerability to gain unauthorized entry and infect the system with ransomware. As described in the Quarterly Report on Global Security Trends [35] for the second quarter of FY2021, this type of attack indirectly utilized the vulnerability of the VPN device, FotiGate. The attacker first obtains the credentials that were leaked by someone exploiting a vulnerability in the VPN device, FotiGate. Then the attacker uses the obtained credentials to gain unauthorized access, and causes ransomware infection on the compromised system. Thus, it is clear that companies that keep themselves open to attack by leaving vulnerabilities unaddressed are more susceptible to attacks.

6.2.2. Causes of insufficient security measures in SMEs

So why are security measures in SMEs often inadequate compared to large companies? According to a survey on information security measures in SMEs in FY2021 [36], 33.1% of SMEs responded that they had not invested in information security measures in the past three fiscal years. The survey also asked these companies about the reasons for not investing in information security measures. It shows that "not feeling the need for it" was the most common reason (40.5%), followed by "not seeing the cost-effectiveness" (24.9%), "costing too much" (22.0%), and "not knowing where to start" (20.7%). Looking at the high percentage of companies that answered "not feeling the need for it" and "not seeing the cost-effectiveness," it is clear that many companies still do not understand the importance of security measures. On the other hand, from the answers "costing too much" and "not knowing where to start," it can be seen that some companies understand the importance of security measures but are unable to implement them due to the cost and lack of human resources.

We suspect that the main causes of insufficient security measures in SMEs are the following: first, they do not understand the security measures that they should take in the first place; second, they do not have enough security-related personnel; and third, they do not have enough budget to implement security measures. In the case of Handa Hospital introduced in 6.1.3, it can be seen that there is a shortage of personnel and budget for security measures, which corroborate the aforementioned causes. We believe that these three causes are hindering the promotion of security measures in SMEs.

6.3. How to promote security measures in SMEs

In 6.2, we considered that the cause of the increase in ransomware damage at SMEs is the insufficient security measures taken by them. They should understand the importance of security and promote security measures to avoid falling victim to ransomware attacks. We speculated that the three main causes hindering security measures in SMEs are: "not knowing what security measures to take," "lack of personnel," and "lack of budget." In this section, we will present solutions to these three causes hindering the promotion of security measures in SMEs.

(1) Case of not knowing what security measures to take

Those in charge of actually implementing security measures in SMEs often do not know what they should do to improve their company's security. There are countless security measures that can be taken to protect a company from cyberattacks. Those in charge must consider the effectiveness and feasibility of these measures and choose the ones that are appropriate for their company. To do this, they need to conduct a security risk assessment to identify their company's risks, develop security measures to address those risks, and then implement them. To successfully carry out this process, knowledge and experience in security are important. In SMEs, the lack of knowledge and experience in security among security personnel is considered one of the causes that hinder the promotion of security measures.

One solution to the lack of experience is to utilize the Information Security Measures Guidelines for SMEs [41] published by the IPA. These guidelines summarize specific procedures and methods for implementing measures so that even those without knowledge or experience in security can promote security measures suited to each company's circumstances. The guidelines provide four steps for promoting security measures. Step 1 provides the minimum five measures necessary for SMEs that have not implemented information security at all up to now. In Step 2, the guidelines instruct companies to understand the current status of their security and take measures to address areas where security measures are insufficient. The guidelines are accompanied by templates for proceeding with Step 2, making it easy for even those lacking significant experience in risk analysis to tackle the task. By completing Steps 1 and 2, SMEs that have not implemented security measures can make significant improvements. In Step 3, as a more serious security measure, the company first formulates information security regulations suited to itself. Then, the company informs and educates its employees to ensure that they comply with the regulations. Then, the company checks and evaluates compliance with the regulations and directs improvements as necessary. Step 3 involves more advanced information security measures, but since templates are available for this step as well, companies can start by adding to or revising the templates to suit their own situation. Step 4 explains how to implement additional measures to further strengthen security. Those in charge at SMEs who have been able to implement up to Step 3 can implement the additional measures necessary for their company.

In order to develop and continue improving security measures, it is important to develop those in charge as security personnel from a medium- to long-term perspective. For SMEs, we believe that the minimum necessary personnel are those who can oversee the company's information security. Specifically, they need to be able to lead the development of security policies, employee security education, and awareness-raising for management. This is because these tasks are closely related to the characteristics of each company and require a strong understanding of the company. Meanwhile, technical security measures such as log analysis and implementation and operation of security products require advanced expertise. If the company cannot secure personnel on its own, there are options such as utilizing MSS or outsourcing as described in (2) later.

So what can be done to develop personnel who can oversee the security of a company? To become such a person, we believe that a wide range of security knowledge and experience in promoting security within a company are necessary. To acquire a wide range of security knowledge, it is advisable to utilize certifications and educational programs. For example, there is a certification to become a Registered Information Security Specialist, which requires general security knowledge, as well as the IPA's Core Human Resource Development Program, a one-year program to train personnel to oversee security. To gain experience in promoting security measures, it is advisable to work on tasks such as developing security policies and conducting in-house education as part of one's job duties. Activities in line with the Information Security Measures Guidelines for SMEs can also be good experience. To develop security personnel, it takes at least one year just to acquire knowledge, and from there, experience must be gained, so the total time required is several years. Companies should make steady progress for the safety of their future.

(2) Case of personnel shortage

Shortage of personnel is a concern faced by many SMEs. Without personnel, it is not possible to develop personnel who can oversee security as mentioned in (1). In addition to personnel overseeing security, a diverse range of personnel is also necessary to implement security measures. Ideally, a system for developing cybersecurity personnel within the company should be established, and a career advancement system for cybersecurity personnel should also be put in place. In Tokyo, support is being provided to SMEs for the development of cybersecurity personnel and the establishment of an internal training system [37]. In addition, the Ministry of Economy, Trade and Industry (METI) has also released a "Guidebook for Establishing Cybersecurity Systems and Securing Necessary Human Resources," [38] which outlines key points for companies to establish a cybersecurity organizational structure and secure the necessary personnel. SMEs with the budget and personnel can take advantage of these measures to secure cybersecurity personnel. However, we believe that many companies do not have the resources to implement these measures. In such cases, the lack of in-house personnel can be covered by outsourcing to external parties such as managed security services (MSS). In the case of Handa Hospital in 6.1.3, one of the causes of the incident was delegating the whole security operation to a contractor. When outsourcing, select the contractor based on established selection criteria such as the abundance of business experience and whether or not the contractor has obtained external certification (ISMS, PrivacyMark, etc.), and clarify the details of the work to be outsourced. While outsourcing, do not leave the whole operation to the contractor, but supervise them by checking the progress and pointing out any mistakes or delays.

(3) Case of budget shortage

A shortage of personnel is also related to a lack of budget. In fact, in a survey on the actual situation of information security measures in SMEs in FY2021 [36], which was introduced in 6.2.2, there were many opinions such as "not seeing the cost-effectiveness" and "costing too much" as reasons for not investing in information security. As one solution, SMEs can receive subsidies from institutions or local governments. The Tokyo Metropolitan Small and Medium Enterprise Support Center provided Cybersecurity Measures Promotion Subsidies [39] for SMEs in FY2022. These subsidies cover the costs associated with the introduction of equipment, etc. necessary to implement cybersecurity measures and the use of cloud services. METI is also implementing a measure called the IT Introduction Subsidy for Security Measures Promotion [40] to support the implementation of cybersecurity measures for SMEs. This program subsidizes the fees for using the security measure service provided by the IPA, called Cybersecurity Help Desk Service. SMEs can take advantage of these subsidies.

After obtaining subsidies, it is important to gain the understanding of management in order to promote security measures and obtain continuous budgets for security measures. IT personnel need to continue their steady efforts to raise management's awareness about cybersecurity.

6.4. Conclusion

Ransomware damage is increasing every year and has now become a threat that no one can afford to ignore. In this section, we have mentioned that ransomware damage is increasing among SMEs, which tend to have inadequate security measures compared to large companies. As the security awareness of society as a whole increases, we expect to increasingly see attacks concentrated in areas where security measures are lax. SMEs that do not understand the importance of security measures or do not have the resources to implement them will be more vulnerable. Putting off ransomware countermeasures because of a lack of resources could result in an incident that could affect the survival of the company. First, companies should try implementing the content of the Information Security Measures Guidelines for SMEs. Then, in order to continuously improve their security, companies should promote security measures tailored to their own needs as well as train personnel to oversee security operations. In addition, where resources are lacking, it is a good idea to utilize MSS, outsourcing, and subsidy programs related to cybersecurity. To avoid becoming a victim of ransomware, let's advance security measures one step at a time, starting from where we can.

7. Outlook

My Number cards becoming de facto mandatory

The government has indicated that it plans to abolish the current health insurance card in principle and replace it with a new insurance card that is integrated with the My Number card, called the "Maina Insurance Card," as early as the fall of 2024. If this is realized, it will mean that obtaining a My Number card will become virtually mandatory, since Japan has adopted a universal health insurance system. The penetration rate of My Number cards can be expected to increase significantly from the 49.0% of September 2022.

The use of a My Number card is said to be highly secure in the event of theft or loss due to the fact that identification is required by photo and PIN, the card does not contain highly confidential information, and the IC chip is tamper-resistant. However, if the My Number card and the PIN are leaked at the same time, there is a risk that an attacker could illegally log in to the My Number Portal and acquire specific personal information, or impersonate the cardholder through private online authentication services to open bank accounts or create credit cards. With the expected increase in the penetration rate of My Number cards, it can be predicted that the number of private services that utilize My Number cards will increase in the future. Therefore, we predict an increase in cyberattacks that use the My Number card as a foothold to steal money. Even if the security level of My Number cards themselves is high, if the cardholder does not properly manage the card, there is a risk that an attacker will steal the My Number card and PIN and exploit them.

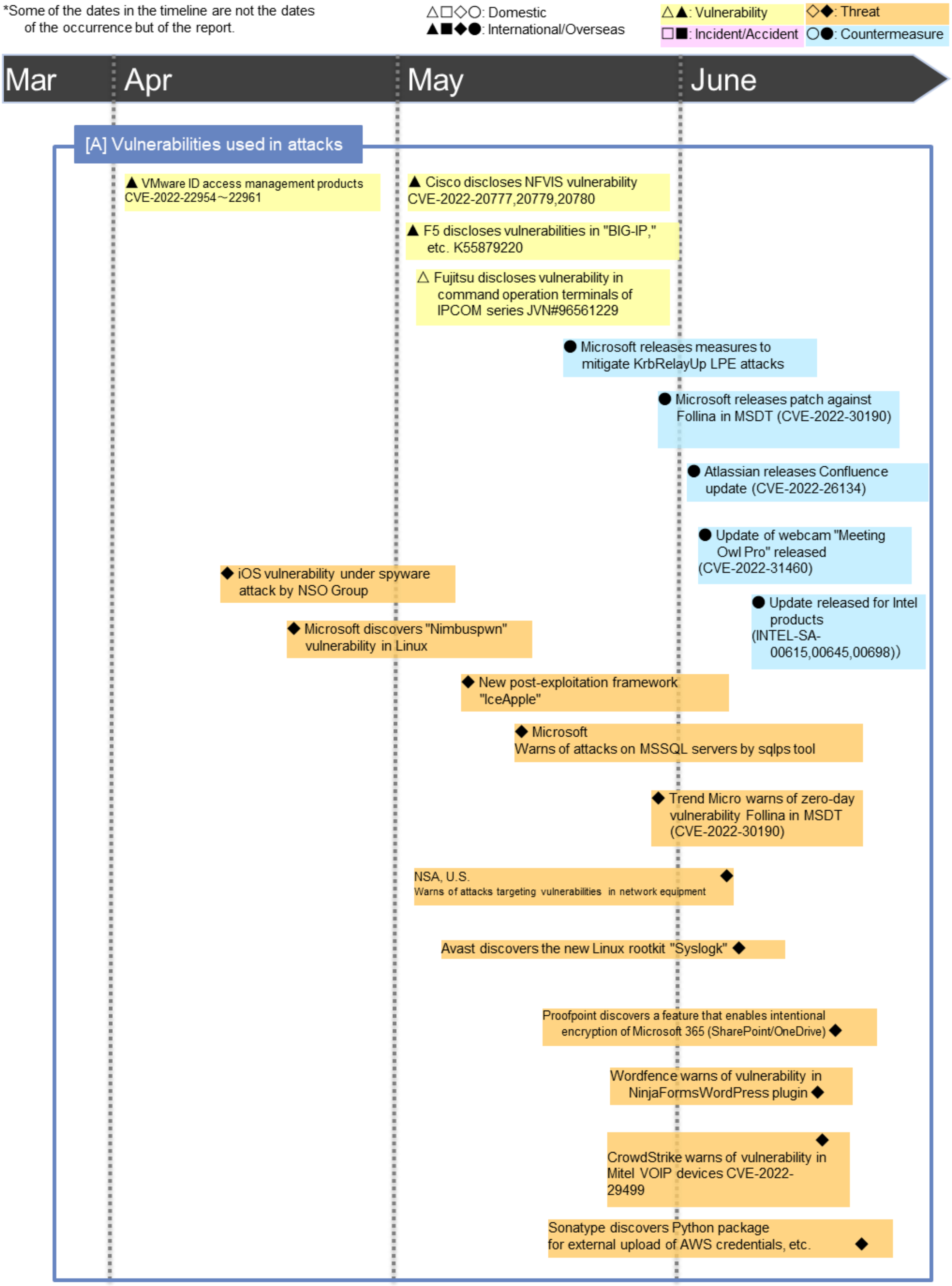
Before My Number cards become de facto mandatory, it is necessary to improve the security literacy of the Japanese people as a whole. In addition, it is imperative to develop a secure system that reduces the risk of the My Number card itself, such as by incorporating biometric authentication.

Cyberattack targeting FIFA World Cup Qatar 2022

The Qatar World Cup will be held for about a month starting on November 20, 2022. Such major events attract global attention and are therefore a target of cyberattacks. As similarly global sporting events, the Summer Olympics and Paralympics were held in Tokyo in 2021 and suffered 450 million cyberattacks, although there were no incidents that disrupted the operation of the games. Cyberattacks targeted not only the host organizations, such as the Organizing Committees for the Olympic and Paralympic Games, but also stakeholders such as outsourced systems companies in the supply chain and prospective spectators. In the case of the Qatar World Cup too, cyberattacks could also be directed at entities other than the organizing committee.

For example, attackers may prepare fake World Cup-related websites and launch phishing attacks against soccer spectators. Nowadays, more and more people watch sports live on the Internet and collect information about the events. During the World Cup, including the preparation period, attackers may lead sports fans to fake live broadcast sites or ticket reservation sites to steal their personal information. Phishing attacks are ranked first in the personal category in the "10 Major Security Threats 2022," and it is expected that cyberattacks following current trends will occur at the World Cup as well.

8. Timeline



*Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident/Accident
○●: Countermeasure

Mar Apr May June

[A] Vulnerabilities used in attacks

▲ VMware ID access management products CVE-2022-22954～22961

▲ Cisco discloses NFVIS vulnerability CVE-2022-20777,20779,20780

▲ F5 discloses vulnerabilities in "BIG-IP," etc. K55879220

△ Fujitsu discloses vulnerability in command operation terminals of IPCOM series JVN#96561229

● Microsoft releases measures to mitigate KrbRelayUp LPE attacks

● Microsoft releases patch against Follina in MSDT (CVE-2022-30190)

● Atlassian releases Confluence update (CVE-2022-26134)

● Update of webcam "Meeting Owl Pro" released (CVE-2022-31460)

● Update released for Intel products (INTEL-SA-00615,00645,00698))

◆ iOS vulnerability under spyware attack by NSO Group

◆ Microsoft discovers "Nimbuspwn" vulnerability in Linux

◆ New post-exploitation framework "IceApple"

◆ Microsoft Warns of attacks on MSSQL servers by sqlps tool

◆ Trend Micro warns of zero-day vulnerability Follina in MSDT (CVE-2022-30190)

NSA, U.S. Warns of attacks targeting vulnerabilities in network equipment ◆

Avast discovers the new Linux rootkit "Syslogk" ◆

Proofpoint discovers a feature that enables intentional encryption of Microsoft 365 (SharePoint/OneDrive) ◆

Wordfence warns of vulnerability in NinjaFormsWordPress plugin ◆

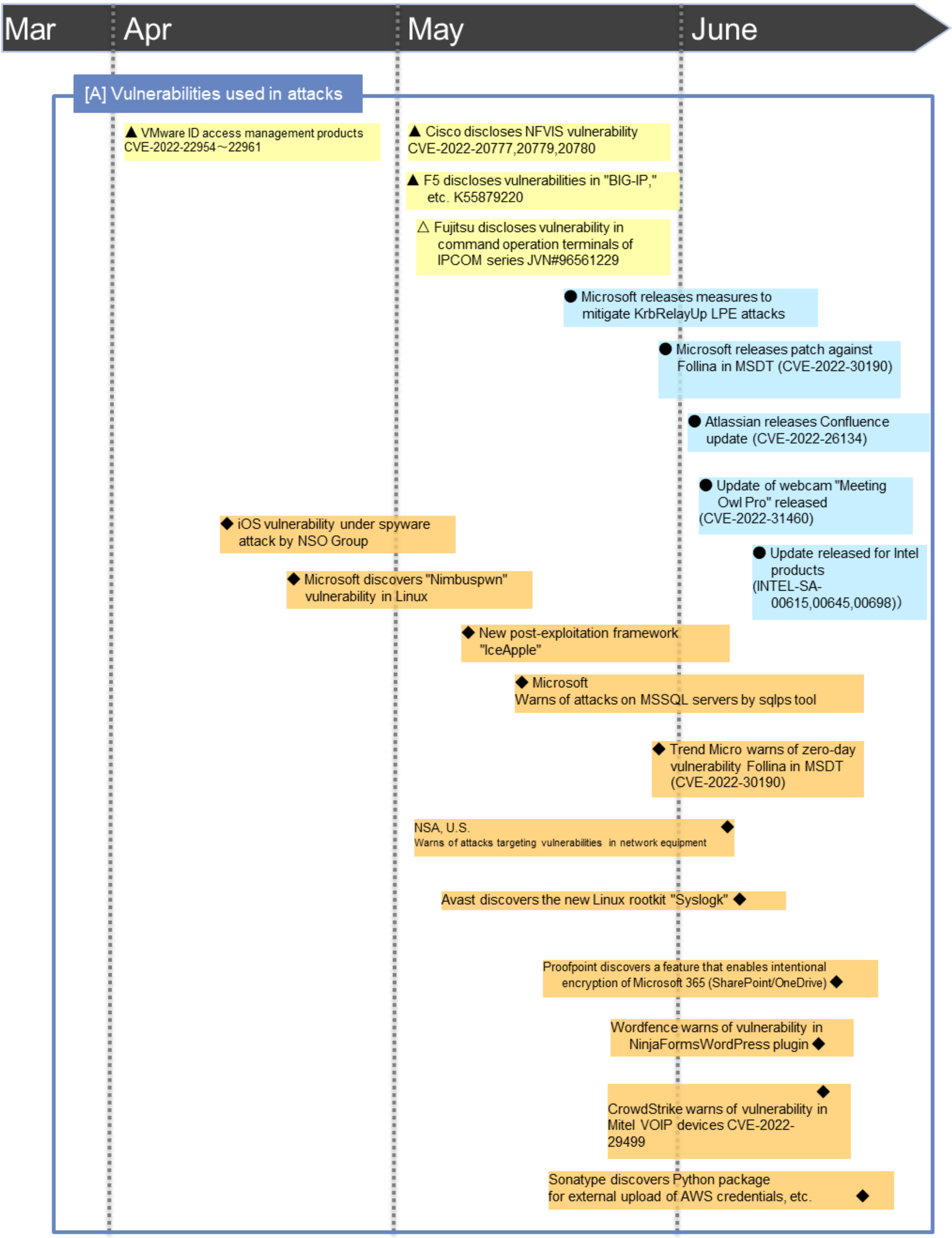
◆ CrowdStrike warns of vulnerability in Mitel VOIP devices CVE-2022-29499

Sonatype discovers Python package for external upload of AWS credentials, etc. ◆

*Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident/Accident
○●: Countermeasure



Mar Apr May June

[A] Vulnerabilities used in attacks

▲ VMware ID access management products CVE-2022-22954～22961

▲ Cisco discloses NFVIS vulnerability CVE-2022-20777,20779,20780

▲ F5 discloses vulnerabilities in "BIG-IP," etc. K55879220

△ Fujitsu discloses vulnerability in command operation terminals of IPCOM series JVN#96561229

● Microsoft releases measures to mitigate KrbRelayUp LPE attacks

● Microsoft releases patch against Follina in MSDT (CVE-2022-30190)

● Atlassian releases Confluence update (CVE-2022-26134)

● Update of webcam "Meeting Owl Pro" released (CVE-2022-31460)

◆ iOS vulnerability under spyware attack by NSO Group

● Update released for Intel products (INTEL-SA-00615,00645,00698))

◆ Microsoft discovers "Nimbuspwn" vulnerability in Linux

◆ New post-exploitation framework "IceApple"

◆ Microsoft Warns of attacks on MSSQL servers by sqlps tool

◆ Trend Micro warns of zero-day vulnerability Follina in MSDT (CVE-2022-30190)

NSA, U.S. Warns of attacks targeting vulnerabilities in network equipment ◆

Avast discovers the new Linux rootkit "Syslogk" ◆

Proofpoint discovers a feature that enables intentional encryption of Microsoft 365 (SharePoint/OneDrive) ◆

Wordfence warns of vulnerability in NinjaFormsWordPress plugin ◆

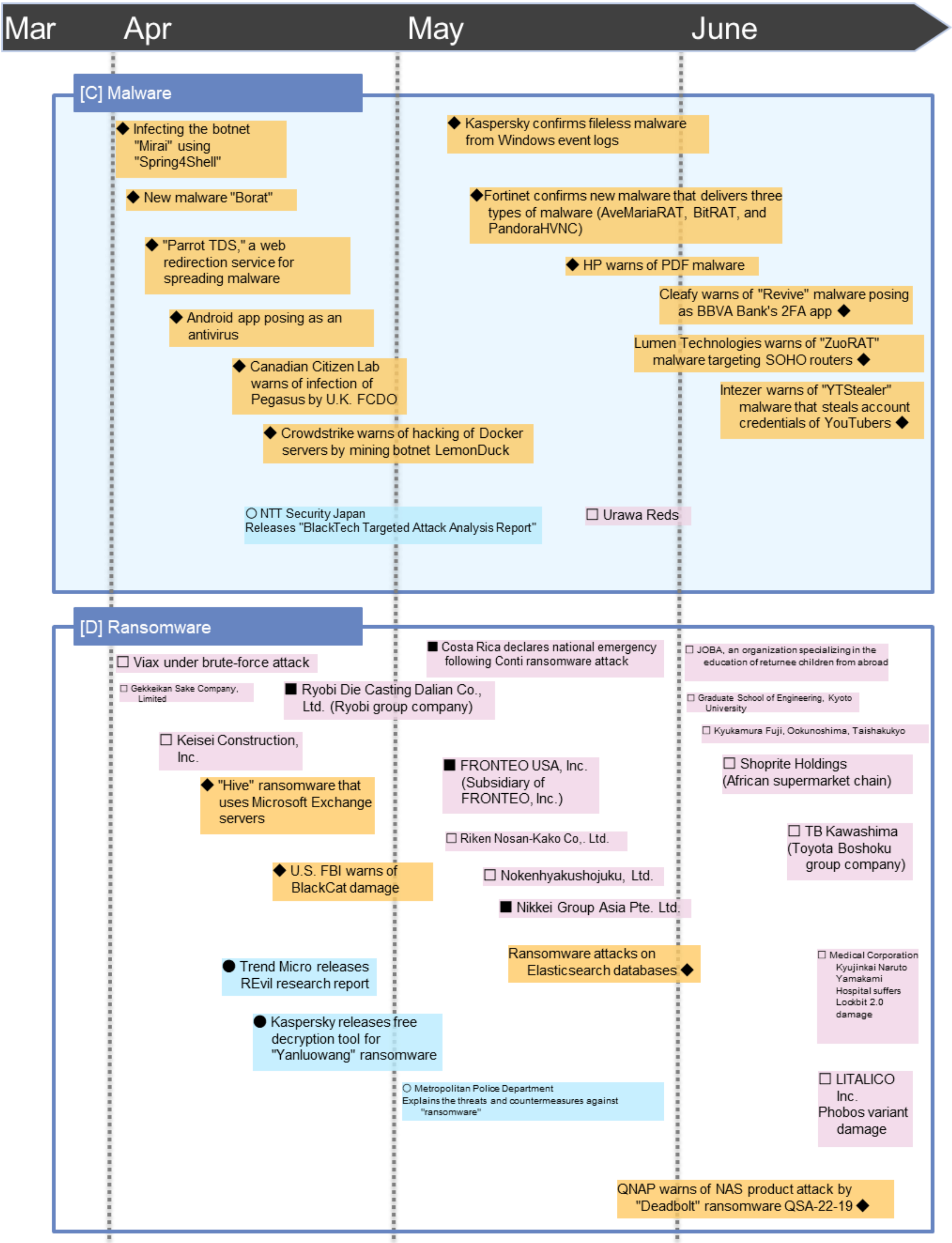
◆ CrowdStrike warns of vulnerability in Mitel VOIP devices CVE-2022-29499

Sonatype discovers Python package for external upload of AWS credentials, etc. ◆

*Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident/Accident
○●: Countermeasure



[C] Malware

◆ Infecting the botnet "Mirai" using "Spring4Shell"

◆ New malware "Borat"

◆ "Parrot TDS," a web redirection service for spreading malware

◆ Android app posing as an antivirus

◆ Canadian Citizen Lab warns of infection of Pegasus by U.K. FCDO

◆ Crowdstrike warns of hacking of Docker servers by mining botnet LemonDuck

○ NTT Security Japan Releases "BlackTech Targeted Attack Analysis Report"

◆ Kaspersky confirms fileless malware from Windows event logs

◆ Fortinet confirms new malware that delivers three types of malware (AveMariaRAT, BitRAT, and PandoraHVNC)

◆ HP warns of PDF malware

Cleafy warns of "Revive" malware posing as BBVA Bank's 2FA app ◆

Lumen Technologies warns of "ZuoRAT" malware targeting SOHO routers ◆

Intezer warns of "YTStealer" malware that steals account credentials of YouTubers ◆

□ Urawa Reds

[D] Ransomware

□ Viax under brute-force attack

□ Gekkeikan Sake Company, Limited

□ Keisei Construction, Inc.

◆ "Hive" ransomware that uses Microsoft Exchange servers

◆ U.S. FBI warns of BlackCat damage

● Trend Micro releases REvil research report

● Kaspersky releases free decryption tool for "Yanluowang" ransomware

■ Ryobi Die Casting Dalian Co., Ltd. (Ryobi group company)

■ Costa Rica declares national emergency following Conti ransomware attack

■ FRONTEO USA, Inc. (Subsidiary of FRONTEO, Inc.)

□ Riken Nosan-Kako Co,. Ltd.

□ Nokenhyakushojuku, Ltd.

■ Nikkei Group Asia Pte. Ltd.

Ransomware attacks on Elasticsearch databases ◆

○ Metropolitan Police Department Explains the threats and countermeasures against "ransomware"

□ JOBA, an organization specializing in the education of returnee children from abroad

□ Graduate School of Engineering, Kyoto University

□ Kyukamura Fuji, Ookunoshima, Taishakukyo

□ Shoprite Holdings (African supermarket chain)

□ TB Kawashima (Toyota Boshoku group company)

□ Medical Corporation Kyujinkai Naruto Yamakami Hospital suffers Lockbit 2.0 damage

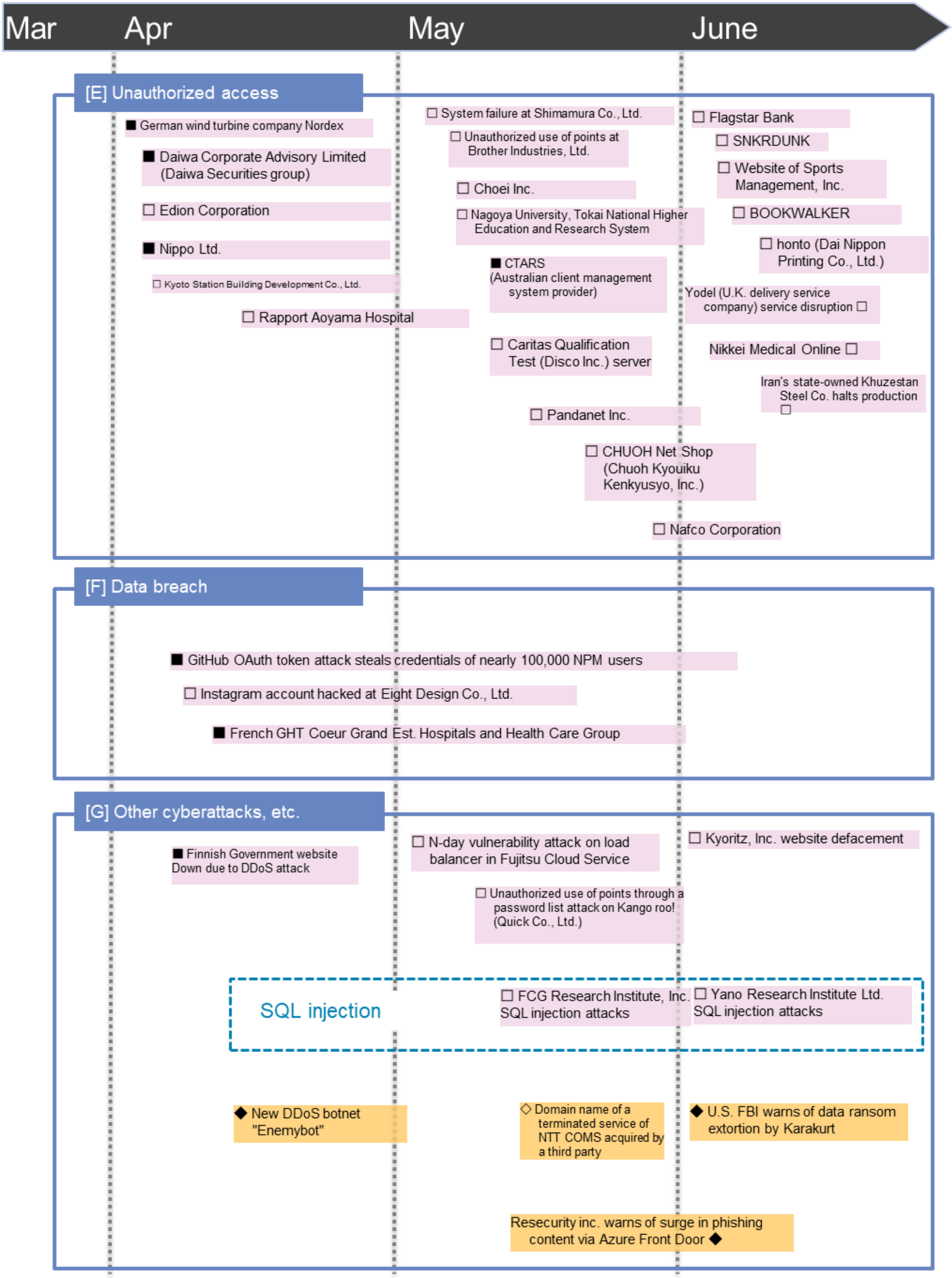
□ LITALICO Inc. Phobos variant damage

QNAP warns of NAS product attack by "Deadbolt" ransomware QSA-22-19 ◆

*Some of the dates in the timeline are not the dates of the occurrence but of the report.

△□◇○: Domestic
▲■◆●: International/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident/Accident
○●: Countermeasure



Mar Apr May June

[E] Unauthorized access

■ German wind turbine company Nordex

■ Daiwa Corporate Advisory Limited (Daiwa Securities group)

□ Edion Corporation

■ Nippo Ltd.

□ Kyoto Station Building Development Co., Ltd.

□ Rapport Aoyama Hospital

□ System failure at Shimamura Co., Ltd.

□ Unauthorized use of points at Brother Industries, Ltd.

□ Choei Inc.

□ Nagoya University, Tokai National Higher Education and Research System

■ CTARS (Australian client management system provider)

□ Caritas Qualification Test (Disco Inc.) server

□ Pandanet Inc.

□ CHUOH Net Shop (Chuoh Kyouiku Kenkyusyo, Inc.)

□ Nafco Corporation

□ Flagstar Bank

□ SNKRDUNK

□ Website of Sports Management, Inc.

□ BOOKWALKER

□ honto (Dai Nippon Printing Co., Ltd.)

Yodel (U.K. delivery service company) service disruption □

Nikkei Medical Online □

Iran's state-owned Khuzestan Steel Co. halts production □

[F] Data breach

■ GitHub OAuth token attack steals credentials of nearly 100,000 NPM users

□ Instagram account hacked at Eight Design Co., Ltd.

■ French GHT Coeur Grand Est. Hospitals and Health Care Group

[G] Other cyberattacks, etc.

■ Finnish Government website Down due to DDoS attack

□ N-day vulnerability attack on load balancer in Fujitsu Cloud Service

□ Unauthorized use of points through a password list attack on Kango roo! (Quick Co., Ltd.)

□ Kyoritz, Inc. website defacement

SQL injection

□ FCG Research Institute, Inc. SQL injection attacks

□ Yano Research Institute Ltd. SQL injection attacks

◆ New DDoS botnet "Enemybot"

◇ Domain name of a terminated service of NTT COMS acquired by a third party

◆ U.S. FBI warns of data ransom extortion by Karakurt

Resecurity inc. warns of surge in phishing content via Azure Front Door ◆

References

[1] Federal Bureau of Investigation, “Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons,” 20 4 2022. [オンライン]. Available: https://www.ic3.gov/Media/News/2022/220420-2.pdf.

[2] Federal Bureau of Investigation, “Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks,” 1 9 2021. [オンライン]. Available: https://www.ic3.gov/Media/News/2021/210907.pdf.

[3] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2021年度第3四半期）」,” 15 3 2022. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_3q_securityreport.pdf.

[4] 警察庁, “令和３年におけるサイバー空間をめぐる脅威の情勢等について,” 7 4 2022. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf.

[5] 農林水産技術会議, “「スマート農業実証プロジェクト」について：農林水産技術会議,” [オンライン]. Available: https://www.affrc.maff.go.jp/docs/smart_agri_pro/smart_agri_pro.htm.

[6] 内閣サイバーセキュリティセンター, “NISC | サイバーセキュリティ普及啓発・人材育成ポータルサイト構築,” [オンライン]. Available: https://security-portal.nisc.go.jp/.

[7] 内閣サイバーセキュリティセンター, “ランサムウェア特設ページ - NISC,” [オンライン]. Available: https://security-portal.nisc.go.jp/stopransomware/.

[8] 農林水産省, “2020年農林業センサス結果の概要（確定値）（令和2年2月1日現在）：農林水産省,” 11 6 2021. [オンライン]. Available: https://www.maff.go.jp/j/tokei/kekka_gaiyou/noucen/2020/index.html.

[9] PCI Security Standards Council, LLC., “Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards,” 3 2022. [オンライン]. Available: https://www.pcisecuritystandards.org/document_library/. [アクセス日: 26 10 2022].

[10] 経済産業省 商務情報政策局 商務・サービスグループ　キャッシュレス推進室,

“キャッシュレス関連用語集,” 6 2019. [オンライン]. Available: https://www.meti.go.jp/policy/mono_info_service/cashless/image_pdf_movie/cashless_glossary_R1_06.pdf. [アクセス日: 27 10 2022].

[11] クレジット取引セキュリティ対策協議会, “EMV 3-Dセキュア導入ガイド 1.0版,” 8 3 2022. [オンライン]. Available: https://www.j-credit.or.jp/download/news20220309b4.pdf. [アクセス日: 25 10 2022].

[12] EMVCo, “3-D Secure - EMVCo,” 8 2022. [オンライン]. Available: https://www.emvco.com/emv-technologies/3d-secure/. [アクセス日: 1 11 2022].

[13] 経済産業省 商務・サービスグループ 商取引監督課, “クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）,” 2 6 2022. [オンライン]. Available: https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf. [アクセス日: 18 11 2022].

[14] GitHub Inc, “Security alert: Attack campaign involving stolen OAuth user tokens issued to two third-party integrators,” 2022. [オンライン]. Available: https://github.blog/2022-04-15-security-alert-stolen-oauth-user-tokens/. [アクセス日: 25 10 2022].

[15] Salesforce , “Heroku Security Notification,” 2022. [オンライン]. Available: https://status.heroku.com/incidents/2413. [アクセス日: 25 10 2022].

[16] BLEEPINGCOMPUTER, “GitHub: Attackers stole login details of 100K npm user accounts,” 27 5 2022. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/github-attackers-stole-login-details-of-100k-npm-user-accounts/.

[17] GitHub Inc, “Software security starts with the developer: Securing developer accounts with 2FA,” 4 5 2022. [オンライン]. Available: https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/.

[18] Travis CI, “SECURITY BULLETIN; Customer repositories have NOT been accessed,” 18 4 2022. [オンライン]. Available: https://blog.travis-ci.com/2022-04-17-securitybulletin.

[19] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2021年度第1四半期）」,” 2 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_1q_securityreport.pdf.

[20] 株式会社NTTデータ, “「グローバルセキュリティ動向四半期レポート（2020年度第3四半期）」,” 16 3 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2020_3q_securityreport.pdf.

[21] National Cyber Security Centre, “Secure development and deployment guidance,” [オンライン]. Available: https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository.

[22] 株式会社セキュアベース, “ソースコードおよびリポジトリ保護のためのセキュリティガイダンス,” 22 12 2021. [オンライン]. Available: https://secbase.jp/report/20211222_protect-your-code-repository.

[23] PNC株式会社, “英国NCSC、ソースコード保護のためのセキュリティガイダンス解説【前半】,” 22 12 2021. [オンライン]. Available: https://www.pnc.jp/blog/ncsc-source-code-security/.

[24] Statcounter, “Statcounter Global Stats,” [オンライン]. Available: https://gs.statcounter.com/browser-market-share/desktop-mobile-tablet/japan/.

[25] Japan Windows Blog, “Internet Explorer 11 デスクトップ アプリケーションのサポート終了 - 発表に関連する FAQ のアップデート,” 21 2 2022. [オンライン]. Available: https://blogs.windows.com/japan/2022/02/21/internet-explorer-11-desktop-app-retirement-faq/.

[26] C. Jackson, “The perils of using Internet Explorer as your default browser,” 6 2 2019. [オンライン]. Available: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-perils-of-using-internet-explorer-as-your-default-browser/ba-p/331732.

[27] 独立行政法人情報処理推進機構, “Microsoft 社 Internet Explorer のサポート終了について,” 16 6 2022. [オンライン]. Available: https://www.ipa.go.jp/security/announce/ie_eos.html.

[28] IPA, “情報セキュリティ10大脅威 2022,” 27 1 2022. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2022.html.

[29] 警察庁, “令和３年におけるサイバー空間をめぐる脅威の情勢等について,” 7 4 2022. [オンライン]. Available: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf.

[30] ExtraHop, “サイバーセキュリティの信頼度指数,” 23 5 2022. [オンライン]. Available: https://assets.extrahop.com/whitepapers/ExtraHop2022CyberConfidenceIndex_AsiaPacific_J.pdf.

[31] 株式会社月桂冠, “当社サーバへの不正アクセスに関するお知らせ,” 26 5 2022. [オンライン]. Available: https://www.gekkeikan.co.jp/company/news/detail/326/.

[32] 京成建設株式会社, “当社サーバに対する不正アクセスに関するご報告,” 18 4 2022. [オンライン]. Available: http://keisei-const.jp/info/%e4%b8%8d%e6%ad%a3%e3%82%a2%e3%82%af%e3%82%bb%e3%82%b9%e3%81%94%e5%a0%b1%e5%91%8a/.

[33] 理研農産化工株式会社, “不正アクセスによるシステム被害について,” 20 5 2022. [オンライン]. Available: https://rikenf.sagafan.jp/e982686.html.

[34] 株式会社アイウエア, “システム障害に関するお知らせとお詫び,” 13 6 2022. [オンライン]. Available: https://www.joba.jp/public_relations/.

[35] 徳島県つるぎ町立半田病院, “徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書,” 27 6 2022. [オンライン]. Available: https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf.

[36] NTTデータ株式会社, “グローバルセキュリティ動向四半期レポート　2021年第2四半期,” [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2021_2q_securityreport.pdf.

[37] IPA, “2021年度 中小企業における情報セキュリティ対策に関する実態調査,” 31 3 2022. [オンライン]. Available: https://www.ipa.go.jp/security/fy2021/reports/sme/index.html.

[38] 東京都, “セキュリティ対策に取り組む中小企業の人材育成・社内体制整備を支援します！,” 25 5 2022. [オンライン]. Available: https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2022/05/25/08.html.

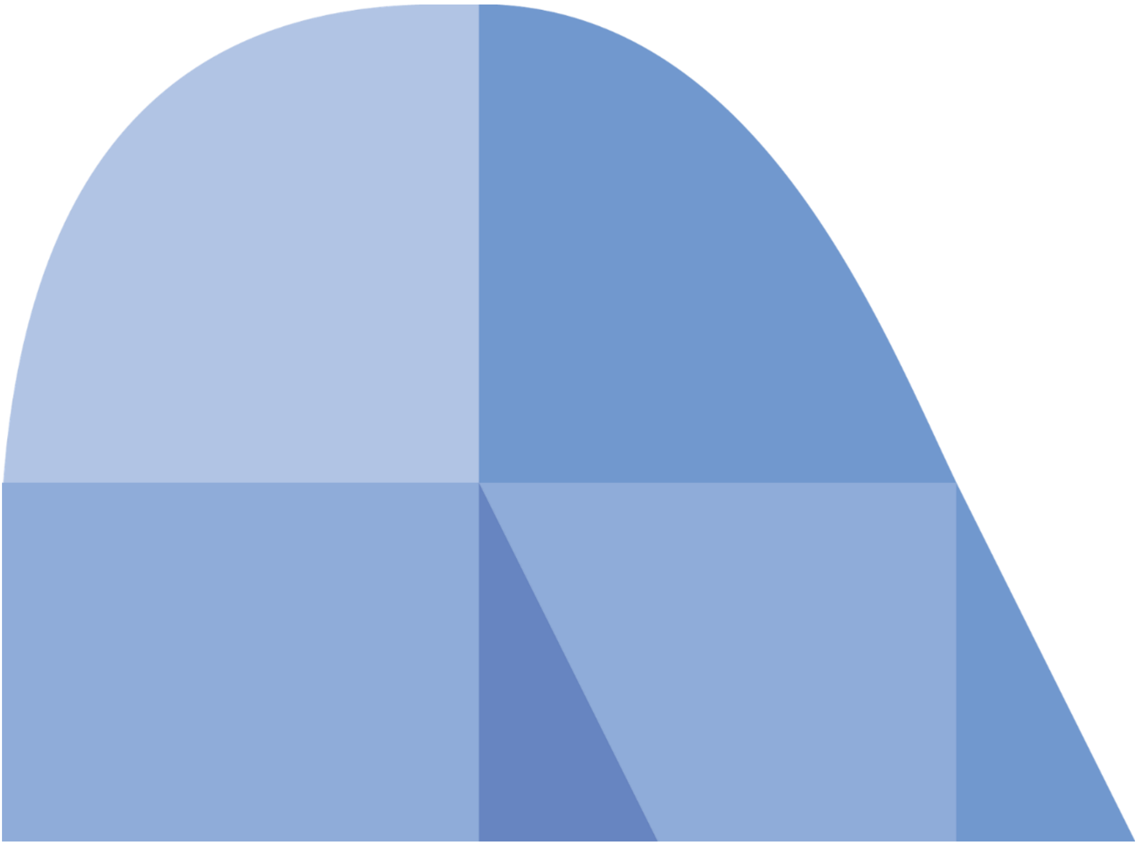
[39] 経済産業省, “サイバーセキュリティ体制構築・人材確保の手引き,” 15 6 2022. [オンライン]. Available: https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html.

[40] 東京都中小企業振興公社, “令和4年度 サイバーセキュリティ対策促進助成金,” 2022. [オンライン]. Available: https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html.

[41] 経済産業省, “IT導入補助金セキュリティ対策推進枠,” 2022. [オンライン].

Available: https://www.it-hojo.jp/security/.

[42] IPA, “中小企業の情報セキュリティ対策ガイドライン,” 19 3 2019. [オンライン]. Available: https://www.ipa.go.jp/security/keihatsu/sme/guideline/.



Published on January 31, 2023

NTT DATA Corporation
Cyber Security Department
Hisamichi Ohtani
Toshihiko Matsuo / Yuto Kihira / Naomi Sakuta / Chisa Saito / Naoki Murata / Tatsuya Takahashi / Masafumi Kuromiya / Kantaro Kudo
nttdata-cert@kits.nttdata.co.jp