

Quarterly Report on Global Security Trends



2nd Quarter of 2020



Table of Contents

1. Executive Summary.....	2
2. Featured Topics.....	4
2.1. Security which is required for payment service.....	4
2.1.1. Unauthorized use of payment and financial services	5
2.1.2. What is “identity verification”?	8
2.1.3. Security which is required for payment service	9
2.1.4. Conclusion	15
2.2. Zerologon (CVE-2020-1472)	16
2.2.1. Summary of Zerologon.....	16
2.2.2. Explanation of Zerologon vulnerability	16
2.2.3. Step-by-step response	18
2.2.4. Conclusion	21
3. Data Breach	22
3.1. Cases targeting the vulnerability of supply chain.....	22
3.2. Measures against supply chain risks	23
3.3. Impacts of data breach on organization.....	24
3.4. Information breach cases in the 2nd quarter of 2020	25
3.5. Conclusion.....	25
4. Vulnerability	27
4.1. Vulnerability which arose in several products of BIG-IP.....	27
4.1.1. Summary of vulnerability	27
4.1.2. Timeline	27
4.1.3. Attack-related cases.....	28
4.2. Conclusion.....	30
5. Malware/Ransomware.....	31
5.1. Summary of the 2nd quarter of FY 2020	31
5.1.1. Revival of Emotet.....	31
5.1.2. Worsening of damage caused by ransomware attacks.....	32
5.1.3. Other damage cases of malware.....	33

5.2. Conclusion.....34

6. Outlook.....35

7. Timeline37

References.....41

1. Executive Summary

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

Security which is required for payment service

In the "10 Largest Information Security Threats in 2020" published by the Information-technology Promotion Agency, Japan (IPA), the "unauthorized use of smart phone payment services" was ranked the top personal threat for the first time. During the 2nd quarter of 2020, unauthorized use of these services have occurred in a large scale at SBI Securities and NTT DOCOMO. Each company has announced that they will take several measures and both companies said they will strengthen "identity verification." This article explains which security measures should be installed in terms of identity verification regarding functions such as "account registration," "bank account registration" and "payment" which general payment services offer, based on the definition of "identity verification" stated by the Ministry of Economy, Trade and Industry.

Zerologon (CVE-2020-1472)

Zerologon is a vulnerability found when the authentication protocol used in Active Directory is installed on Windows. Attackers can steal the administrator's rights of a domain controller, take over all devices that are joining the domain, steal confidential information and spread malware by exploiting this vulnerability and illegally passing the authentication. Microsoft is planning to take 2 step measures against the vulnerability. This article outlines the vulnerability, setting changes required in each step and logs to be monitored.

Revival of Emotet and worsening of ransomware damage.

The spread of Emotet has been revived and it caused over 5.7 times more infected cases than the last peak in September 2020. One of the factors of the spread was a new attacking method by which Emotet sends a suspicious Word file containing malware by creating a password-protected zip file and attaching it in emails. Security products are unable to scan viruses in password-protected zip files. Emails with an attached zip file containing malware are sent to users without being removed. It is effective to stop using password-protected zip files as they are exploited by Emotet as well as being insufficient as a data breach countermeasure.

Damage caused by ransomware is also becoming worse. Ransomware caused the first loss of life by stopping the hospital healthcare system and failure in GPS service, which brought

chaos in the world. As it is highly likely that infection with ransomware causes a system to stop, it is important to take measures to prevent infection as early as possible using EDR, etc.

Outlook

There is an SMS identification proxy service where people can create an account of SNS and cloud services by illegally passing through SMS identification with concealed identity. By using this, one can easily pass through SMS identification. It is considered that more cases of unauthorized acts will emerge by combining cheap SIM cards and SMS identification proxy services. Businesses which provide services for which people can make a new account online should re-acknowledge that online "identification" such as SMS identification on smart phones alone can falsify identity by separating identity verification and authentication of the user. It is necessary for services with issues of users with falsified identity to use a method of identity verification such as eKYC. It was found that many organizations have not taken measures against supply chain attacks and the number of places which are easy for attackers to target increased because organizations which were connected through the supply chain changed their working style to telework. Therefore, attack cases targeting supply chains are expected to continue to occur. We recommend taking measures using guidelines and frameworks on supply chain management as well as services that evaluate supply chain risks.

Last but not least, vaccine-themed phishing attack cases are expected to emerge when coronavirus vaccination begins. Other than this, identity verification and authentication of users have become necessary for the first online communications in normal business activities. The number of swindles and cyberattacks targeting opportunities from identity verification acts through online communications is expected to increase.

2. Featured Topics

2.1. Security which is required for payment service

On August 25, 2020, the “10 Largest Information Security Threats in 2020” was published by the Information-technology Promotion Agency, Japan (IPA) [1]. The “10 Largest Threats” are discussed and determined by over 100 researchers and persons in charge of practical work in businesses based on various incidents occurred in the previous year which threaten information security. 10 threats against individuals and those against organizations are shown in ranking in order of higher priority as the entire society and can be referred to to prioritize measures as well as understanding trends. Threats against individuals in 2020 are as follows.

Table 1 Threats against individuals published in the “10 Largest Information Security Threats in 2020”

Ranking	Previous year Ranking	Comparison with the previous year's ranking	Threat
1	—	NEW	Unauthorized use of smart phone payment
2	2	→	Exploitation of personal information through phishing
3	1	↓	Unauthorized use of credit card information
4	7	↑	Unauthorized use of Internet banking
5	4	↓	Demanding of money by methods of threatening or swindle using email, SMS, etc.
6	3	↑	Damage to smart phone users caused by unauthorized applications.
7	5	↓	Slander, libel, false rumor on the Internet
8	8	→	Unauthorized logging in to Internet services
9	6	↓	Internet swindles through fake warnings
10	12	↑	Stealing of personal information from Internet services

“Unauthorized use of smart phone payment” was chosen as one of the 10 largest threats for the first time and it was designated as the threat of the highest social importance. “Unauthorized use of smart phone payment (No. 1)”, “unauthorized use of credit card information (No. 3)” and “unauthorized use of Internet banking (No. 4)” are all threats which are directly targeting money. “Exploitation of personal information through phishing (No. 2)” is an in-advance preparation to illegally use smart phone payment, credit card payment and Internet banking by pretending to be the user and it can also be considered a threat targeting money. Various incidents caused by these threats have occurred in recent years at home and abroad. This report considers necessary securities for “payment and financial services.”

2.1.1. Unauthorized use of payment and financial services

In order to consider securities necessary for payment and financial services, we will introduce 2 examples of unauthorized use of payment and financial services which occurred during the 2nd quarter of 2020.

(1) More than 90 million yen of customers' assets leaked through unauthorized access to security accounts (SBI Securities Co., Ltd.).

In this case, the fact that several unauthorized access and unauthorized withdrawals were found when a customer who has an account in SBI Securities inquired that "there was a transaction which I know nothing about." The attacking process is shown below based on the announcement [2] by SBI Securities.

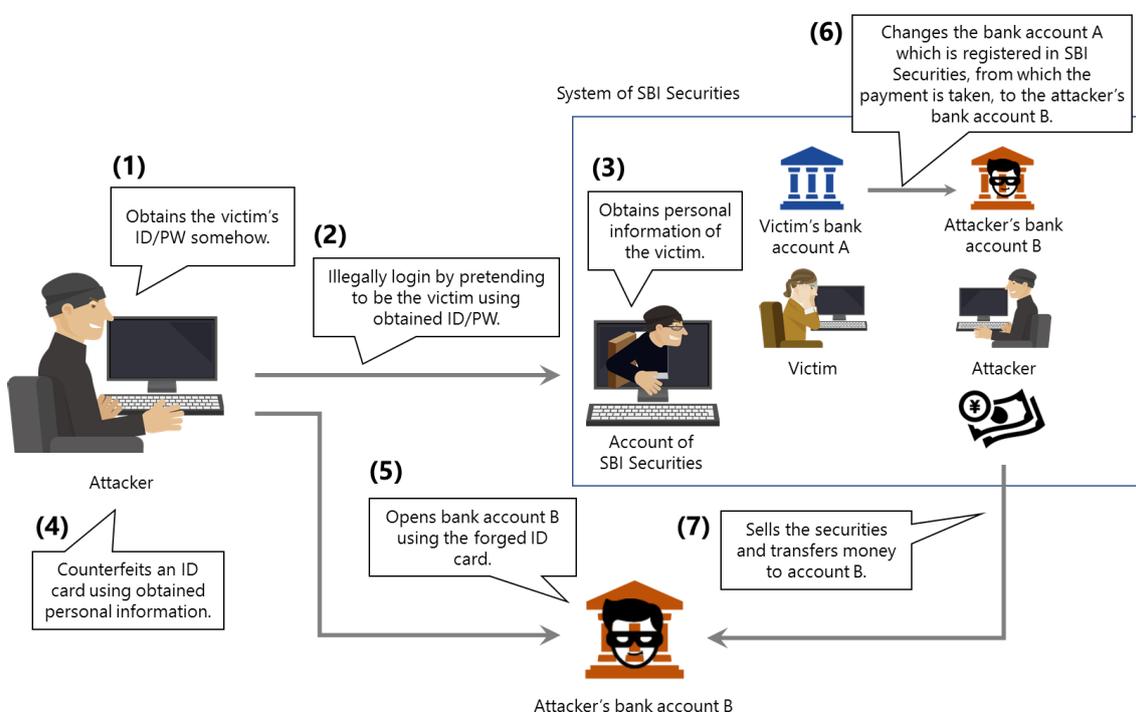


Figure 1: Process of unauthorized access to SBI Securities

An attacker illegally logs in to the customer website (2) using an SBI Securities customer's username (shown as "ID" in the figure) and log-in password (shown as "PW" in the figure) which they obtained somehow (1) and acquires the customer (victim)'s personal information (3). Using the personal information, the attacker counterfeits the victim's ID card (4) and opens another bank account (B) under the victim's name (5). Then, the attacker changes the bank account A to B, from which the payment is taken, on the My Page of the SBI Securities website (6). The attacker then sells the victim's securities and transfers the money from the sale to the account (B) (7). The total amount of damage from this illegal use was 98.64 million from 6 accounts and SBI Securities announced that all the damage will be compensated by the company.

Although SBI Securities has controlled bank accounts to be able to transfer to bank accounts under the same user only, the identification verification process when changing the bank account to be transferred was inadequate. The attacker was able to change the bank account for the money to be transferred to that which is not the victim's account and this illegal use was successful. After the incident, SBI Securities has changed the procedure of changing bank accounts for payment to the procedure only by post, which sends documents to the account holder's address. The company announced that they will take this measure and strengthen collaboration with the monitoring system against unauthorized access, login authentication, identity verification and banks.

(2) More than 20 million yen of customers' savings was illegally withdrawn via electric payment service (NTT DOCOMO, INC.)

Since September 2020, there has been several posts on SNS that people's savings were withdrawn under the name "docomokouza," which revealed the unauthorized use. Docomo accounts are a virtual wallet which can be opened by anyone if they have a "d-account" which can be registered with only an email address. It is a system where users can make payment online using charged balance or send money to other users [3]. The unauthorized use of Docomo accounts had already been carried out in May 2019, using the same method as this time [4]. Figure 2 shows the process of the unauthorized use.

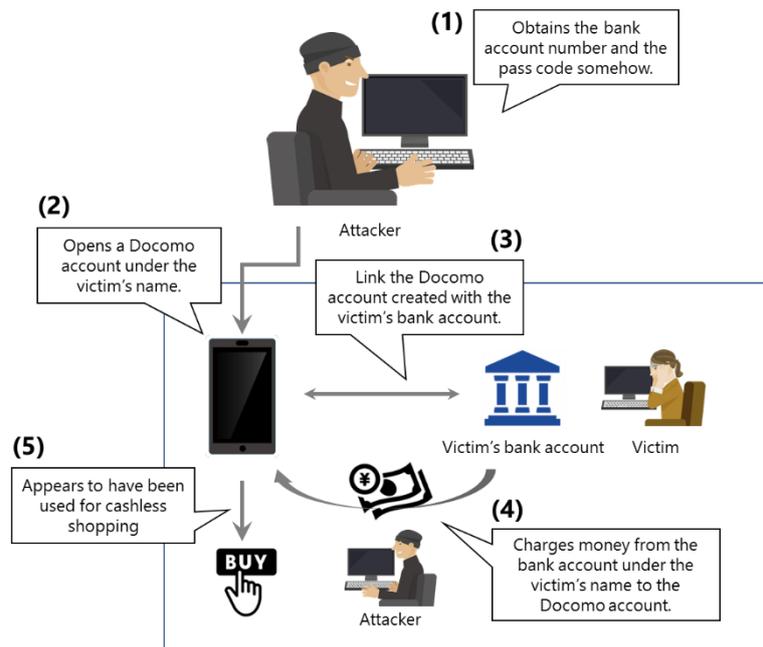


Figure 2: Process of unauthorized use of Docomo accounts

The attacker obtains the name of the bank account holder, account number and the pass code for cash card (1) somehow and opens a Docomo account under the holder's name (2). The attacker links the Docomo account and the bank account (3), and illegally takes the victim's savings by charging cash from the bank account to the Docomo account using the obtained cash card pass (4).

Eventually, it is considered that the attacker had been using “d payment,” a cashless payment method used by Docomo account, under the victim’s name. As of October 28, the total amount of damage from the unauthorized use was 28.85 million yen from 128 cases. It was announced that this damage was all compensated [5]. In response to a series of incidents, NTT DOCOMO has stopped the registration of new bank accounts in Docomo accounts for the time being. Through Docomo accounts, NTT DOCOMO tried to gain new users other than Docomo line contractors, and new users were able to open an account only with an email address. Therefore, it was in a structure where malicious attackers could use it illegally. NTT DOCOMO announced that they will take measures such as applying SMS authentication and carrying out identity verification by asking users to upload their portrait taken by themselves as well as a photo of their ID card [6].

Table 2 summarizes measures released by each company for the above 2 cases.

Table 2: Measures released by SBI Securities and NTT DOCOMO

Main measures released [2] [6]	
SBI Securities	<ol style="list-style-type: none"> 1. Monitoring <ul style="list-style-type: none"> ✓ Strengthening of monitoring system against unauthorized access, introduction of WAF*1 ✓ Further use of IP reputation service*2 2. Authentication <ul style="list-style-type: none"> ✓ Introduction of two-factor authentication*4 by OTP*3 and risk base authentication*5 ✓ Introduction of a function to limit devices which permit access 3. Identity verification <ul style="list-style-type: none"> ✓ Strengthening identity verification when registering a bank account to transfer money (changing the bank account to transfer money is only accepted by post with detailed identity verification) 4. Other <ul style="list-style-type: none"> ✓ Strengthening collaboration with the bank to be transferred ✓ Introduction of dynamic security technology*6
NTT DOCOMO	<ol style="list-style-type: none"> 1. Authentication <ul style="list-style-type: none"> ✓ Introduction of two-factor authentication by SMS 2. Identity verification <ul style="list-style-type: none"> ✓ Ensuring identity verification implementation by eKYC*7

*1 WAF

Web Application Firewall。 A security measure to protect a website from attacks that exploit web application vulnerability. It is installed at the step before the Web server. [7]

*2 IP reputation service

A service that blocks communication from suspicious IP addresses.

*3 OTP

One Time Password。 Disposable passwords which are automatically updated after a certain time.

*4 Two-factor authentication

An authentication method which uses two of three authentication factors: “Bio-information”

such as a fingerprint and iris, “knowledge information” such as passwords and secret questions and “carrying information” such as My Number Card, OTP and tokens.

*5 Risk base authentication

An authentication method which requests authentication with an added factor when there is an authentication act that is different from normal time, in order to prevent fraud and unauthorized logins. [8]

*6 Dynamic security technology

A distinctive application monitoring technology of EverSpin, which allocates a program of a security module with a time limit as running an application and the program is disposed when time runs out. [9]

*7 eKYC

electronic Know Your Customer. A system to complete identity verification procedure online.

As seen in the above cases of the two companies, the key word “identity verification” is frequently used as a measure against unauthorized use of payment and financial services. In particular, when the procedure is completed online, it is necessary to verify whether the account made by a username is of the real user. The Ministry of Economy, Trade and Industry suggests that “identity verification” should be carried out by combining two of the following.

2.1.2. What is “identity verification”?

The Ministry of Economy, Trade and Industry defines “identity verification” is successful when both of, “proofing” which verifies the user’s existence and “authentication of user” which verifies whether the user is operating are carried out [10]. eKYC, which was mentioned as a measure of NTT DOCOMO in Table 2, is one of the methods of “proofing” and two-factor authentication is a method of “authentication of user.” Proofing and authentication of user are divided in 3 levels respectively as shown in Table 3. This is developed based on the “Digital Identity Guidelines(NIST SP-800-63)” established by the US National Institute of Standards and Technology (NIST), and is a standard for carrying out online identity verification for administrative services. There is a trade-off relationship between proofing, levels and cost of authentication of user and convenience. It is necessary for online services to choose an appropriate level of identity verification after comprehensively deciding the balance of these by property.

Table3: Levels of proofing and authentication of user [10]

	Proofing	Authentication of user
Level 3	Implemented based on "public ID card" "in person"	Use multiple of the 3 factors Make sure to include authentication with hardware which makes it difficult to read information illegally, such as My Number Card.
Level 2	Implemented using "public ID card" "by post, not in person"	Use multiple of the 3 factors
Level 1	Implemented based on "self-assessment"	Use one of the 3 factors

2.1.3. Security which is required for payment service

We have explained unauthorized use cases of financial services including online payment services and "identity verification" which is often referred to as a measure. Unlike the actual money exchanges between a shopkeeper and customers in person or withdrawal of cash from ATM using the account holder's own ATM card, it is important to check the credit of users who accessed when handling money online. The afore-mentioned concepts of "proofing" and "authentication of user" are methods to realize this. From now, we will explain functions necessary for the safe practice of functions in general payment services. Figure 3 shows the outline of assumed services.



- Install
 - (1) Account registration on a smart phone application
- Charge
 - Charge by cash from a convenience store ATM
 - (2) Register a bank account and charge from the account balance
 - (3) Register a credit card
 - *Paid by credit card, not in a charge form
- Payment
 - (4) Show your QR code (or bar code) and the shopkeeper will read it.
 - Read the QR code displayed in the store and make payment by inputting the payment amount yourself.
- Withdrawal
 - (5) Transferring balance to the registered bank account (or account to be registered)
- Send money
 - Send money to another user who has an account.

Figure 3: Representative functions of payment services

First, users register their account (1) on an application (hereafter referred to as “app”) which operates on a smart phone. Users can charge money on the application by directly sending money from an ATM at a convenience store, transferring money from the registered bank account (2) or register a credit card (3) and pay later. To register a bank account or a credit card, users need to authenticate their proofing in addition to the authentication carried out at the registration of their account. For actual payment, users can display their QR code on their smart phone screen and have it read at the POS register of a store (4), or read a QR code of the store with their smart phone and input payment amount. Money on the application can be transferred to their bank account (5) or sent to another user who has the same application.

Table 4 summarizes factors of identity verification which are necessary for each function, and Table 5 shows requirements of each function and specific measures.

Table4: Identity verification and levels necessary for each function

Function	Proofing	Authentication of user
(1) Account registration	Recommendation It is recommended to authenticate when registering (1) as it is compulsory in (2) and (3). In cases where there are some users who only uses the point service without using payment function, they can at least carry out authentication of user. (In this case, proofing must be carried out in (2) and (3).)	Recommended ^{*(1)}
(2) Registration / change of bank account	Compulsory (Not necessary if completed in (1)) Level 2 ^{*(2)-1}	Compulsory Level 2 ^{*(2)-2}
(3) Registration/change of credit card information	Compulsory (Not necessary if completed in (1)) Level 2 ^{*(2)-1}	Compulsory Level 2 ^{*(3)}
(4) Users make payment by showing QR code	Assuming they completed processes (1) to (3).	— ^{*(4)}
(5) Transferring to bank account	Assuming they completed processes (1) to (3).	Recommendation

^{*(1)} According to the “Guidelines on the prevention of linking bank account illegally in code payments [11]” provided by “PAYMENTS JAPAN,” authentication of the user at registration of an account is important to collect information to check the correspondence between the user who tries to make payment and the person who made the account.

- * (2)-1 According to the "Guidelines on the linking of account with a fund transfer specialist, etc. [12]" provided by the "Japanese Bankers Association," it is important for the bank to be linked to check the verification process for the user existence and correspondence carried out by the payment service provider when users open an account. As the level 1 proofing is said to have little credibility [13], level 2 authentication is necessary.
- * (2)-2 The guidelines in *(1) prescribes that it is necessary to carry out a robust authentication process by combining multiple factor authentication methods when linking an account with a bank account.
- * (3) According to the "guidelines on the preventive measures of unauthorized use of credit card numbers, etc. breached illegally through code payments [14]" provided by "PAYMENTS JAPAN," it is compulsory to introduce a method to collate information known only by the credit card holder as well as authentication through information on the card to prevent unauthorized use at the time of credit card registration.
- * (4) According to the "unified technical specification guidelines on code payments [user display type] [15]" provided by "PAYMENTS JAPAN," it is compulsory to set a valid time on QR codes to prevent unauthorized use through the illegal copy of QR codes, etc.

Table5: Requirements and measures of each function

Function	Requirements	Measures
<p>(1) Account registration</p>	<ul style="list-style-type: none"> ➤ As in the case of NTT DOCOMO, actual users needs to assure that they have created their own account in order to prevent others from creating an account without permission. ➤ The Act on Prevention of Transfer of Criminal Proceeds prescribes that certain financial institutions should carry out identity verification in a certain method to prevent money laundering and funding to criminal organizations [16]. 	<p><Proofing></p> <ul style="list-style-type: none"> ● eKYC As NTT DOCOMO has announced, users must “take a photo for the identity verification document, upload the photo, and check the correspondence between the person in the photo and the person in the identity verification document [6].” This can prevent fraud as the identity of account users can be verified to be the same person as appears in the identity verification document. <p><Authentication of user></p> <ul style="list-style-type: none"> ● SMS authentication This is a method to verify that users attempted the operation by themselves by sending an SMS message with random 4-6 digit numbers to the phone number which the user wrote and users input the numbers. On June 24, 2020, PayPay which holds the No.1 share of QR code payment service introduced authentication numbers comprising 2 random letters + 4-digit numbers (e.g. AB-1234). This can prevent phishing damage since the 2 letters are displayed on the authentication screen [17]. *Although SMS authentication is a widely used method, it is not an adequate authentication method as there are ways known as SMS intercept (intercepting SMS authentication) [18] and SIM swap (taking over phone numbers) [19]. ● Social login (API link) A method to create an account using SNS account (Google, Twitter, Facebook, etc.) This can take over the security level used for SNS when the account is registered. When using a social login, fraud can be prevented at a certain level as a notification is sent through SNS. *This is not an adequate authentication method as a person can hold multiple SNS accounts and accounts can be handed over.

<p>(2) Registration/change of bank account</p>	<p>In order to prevent registration of account information by other users, the linked bank needs to verify that the account is of the actual user and the action was carried out by the user himself/herself.</p>	<p><Proofing> If not carried out in (1), carry this out in the method written in (1)</p> <p><Authentication of user></p> <ul style="list-style-type: none"> ● Two-factor authentication Authentication factors include passwords and secret questions registered when a bank account is opened (knowledge information), authentication using USB tokens “carrying information” and a method using OTP if the bank offers Internet banking. [20] <p>* Malware (Trojan) to steal authentication information on payment services with a function to intercept SMS and steal OTPs which are generated by application has been reported recently [21]. In many cases, these Trojans are infected by loading a phishing site (disguised website) by mistake, and it is crucial to have basic measures against phishing, such as not clicking suspicious URLs.</p>
--	---	--

<p>(3) Registration/change of credit card information</p>	<p>In order to prevent registration of credit card information by other users, the linked credit card company needs to verify that the credit card is of the actual user.</p>	<p><Proofing> If not carried out in (1), carry this out in the method written in (1)</p> <p><Authentication of user> Information written on a credit card including numbers, validity and security code can be stolen whenever there is a chance to see the credit card. It is dangerous if a credit card is registered to an account through this method.</p> <ul style="list-style-type: none"> ● 3D secure This is an authentication method using password registered separately on the credit card company's website as well as information written on one's credit card [22]. It is one of two-factor authentication combining carrying information (credit card number) and knowledge information (password). As the credit card company has verified proofing when issuing a card, prepare a system where only credit cards offering 3D secure are allowed to be linked.
<p>(4) Payment by CPM method</p>	<p>It is necessary to consider a way to prevent payment using another user's code.</p>	<p>Attacks which try to steal information by intruding in communication between 2 people are called Man-in-the-Middle (MITM) attacks. It is necessary to prevent physical MITM which makes payment using another user's QR code when people try to pay by CPM method.</p> <ul style="list-style-type: none"> ● Validity of code QR codes and bar codes displayed on devices should be updated in a short time (generally around 5 minutes) and old codes are discarded. By using this system, we can reduce the risk of payment by other users using a pre-captured screen. <p>*MITM is also possible by a method of inserting malware with a function to capture a device's screen shot. It is necessary for users to display codes only immediately before payment and check notifications from the app.</p>

<p>(5) Transferring to bank account</p>	<p>(2) Although risk of fraud can be reduced through proofing verification carried out in (1) and (2), it is possible to further strengthen authentication.</p>	<p><Authentication of user></p> <ul style="list-style-type: none"> ● Risk base authentication <p>When transferring money to a bank account, you can prevent fraud by attackers by requesting additional authentication factors when there is access different from usual usage pattern to the terminals and network which you normally use.</p> <p>*As in the case of SBI Securities, there is a measure to accept changing of bank account by post so that attackers are unable to change the account to be transferred.</p>
---	---	---

2.1.4. Conclusion

We have considered unauthorized use cases concerning payment and financial services and security to prepare in general payment services. Security level is in a trade-off relationship with convenience and process speed, we cannot sacrifice either of them. "Whether users can start using the service immediately" is important for services which can complete all transactions online, which is the factor to differentiate them from competing services. On the other hand, "whether users can use the service with relief" is important for services which handle money in particular, and security level can be the factor to differentiate them from competing services. It is therefore necessary for each business to correctly judge the security level to equip for each service. It is considered that there will be an increasing trend of promoting cashless payment. Based on this article, service providers should consider how they can provide QR code payment service safely and users should review which security measures the services they are using (or will use) take.

2.2. Zerologon(CVE-2020-1472)

Zerologon is a vulnerability (CVE-2020-1472) of Netlogon Remote Protocol, which is an authentication protocol used between a device in the domain and the domain controller. Attackers send an MS-NRPC request which is specially worked from a PC/device (which is able to communicate with the domain controller) to the domain controller and acquire the access right of the domain administrator by exploiting vulnerability and illegally passing through authentication. Microsoft is planning to take 2 step measures against this vulnerability and the administrator needs not only to apply patch but change settings.

2.2.1. Summary of Zerologon

Zerologon (CVE-2020-1472) [23] is a vulnerability published by Microsoft in August 2020. On September 11, 2020, a security firm in the Netherlands, Secura, published a technical report [24] on Zerologon. On September 19, 2020, the United States CISA (Cybersecurity and Infrastructure Security Agency) issued an emergency warning [25]to US administrative organs to apply the patch by September 21. On September 24, 2020, Microsoft observed the occurrence of an attack exploiting this vulnerability [26] and called for attention [27].

2.2.2. Explanation of Zerologon vulnerability

Zerologon is a vulnerability of Netlogon Remote Protocol (also known as MS-NRPC, hereinafter referred to as Netlogon), which is an authentication protocol used between each device in the domain and the Windows Server domain controller (hereinafter referred to as domain controller) to authenticate each of them in Active Directory. Netlogon uses a cipher use mode known as AES-CFB8 to cipher communications relating to authentication, and there was a problem in the generation method of initialization vector used for the encryption process. An initialization vector is random data to be added to plaintexts when they are enciphered. If the initialization vector is set to an unpredictable random value, it is difficult to predict plaintext from the ciphertext as a different ciphertext will be output even if the same plaintext is enciphered. However, the initialization vector was not a random value "0" has always been used in a program installed in Netlogon. As a result, when 64-bit plaintexts all comprising "0" are prepared and enciphered, 64-bit cryptogram all comprising "0" in the same way will be generated in a 1/256 probability.

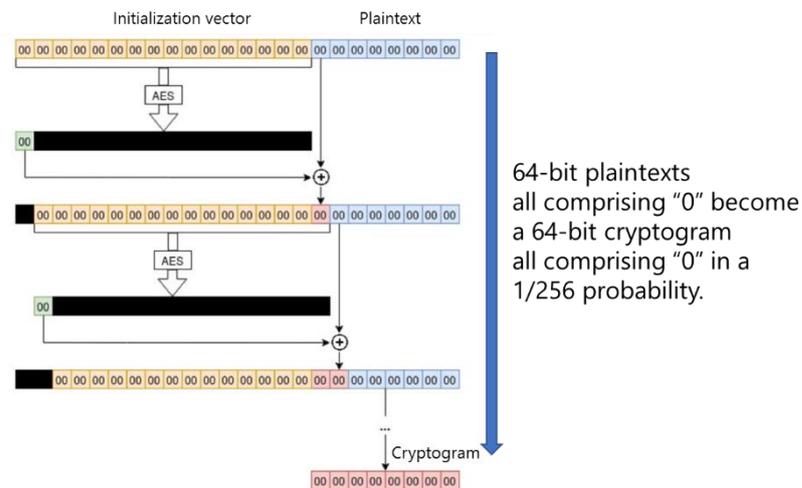


Figure 4: Impact of initialization vector being fixed to "0"

Created based on the figure of WHITEPAPER Zerologon by Secura

Authentication using Netlogon authenticates a client PC when the values obtained by decoding the Client challenge code which the domain controller received from the client PC and the Client credential code which the domain controller received from the same client PC using the session key on the domain controller match.

- Client challenge: any values which are sent from a client PC to the domain controller
- Client credential: values which a client PC enciphered Client challenge using the session key (client PC's password hash)

Attackers who do not have the session key, a secret key shared by a client PC and the domain controller, try to authenticate by sending the Client credential code same as the 64-bit Client challenge code which comprises all "0" numbers. As Netlogon does not limit the number of authentication failures, attackers repeatedly send Client challenge code and Client credential code which comprise "0" until when 64-bit decrypted text all comprising "0" is generated in a 1/256 probability. When decrypted text comprising all "0" is generated in a 1/256 probability, attackers are able to authenticate their client PC to log into the domain controller. CVE-2020-1472 is called Zero(0)logon because of this attacking method.

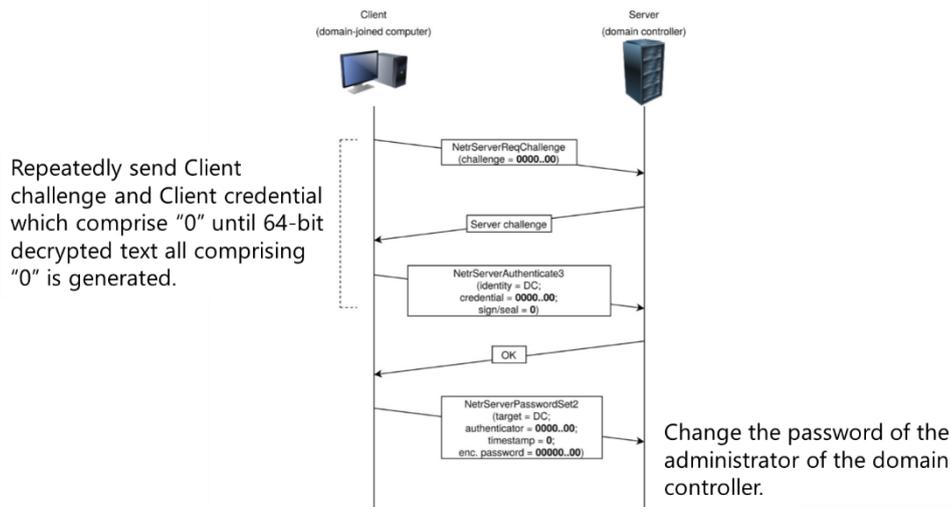


Figure 5: Authentication flow of Netlogon

Created based on the figure of WHITEPAPER Zerologon by Secura

Attackers repeat attacks targeting Zerologon from their authenticated client PC in the same way and successfully change the password of the administrator of the domain controller. Attackers can login to the domain controller as an administrator using the changed password. As attackers can steal the administrator's rights of a domain controller, they can take over all devices that are joining the domain, steal confidential information and spread malware. When they intrude in an internal network, a prompt response is required as the impact of exploitation is significant, given that they can directly access the domain controller.

2.2.3. Step-by-step response

The patch released on August 11, 2020 limits connections from part of devices using Netlogon. Applying this patch alone cannot prevent attacks targeting Zerologon completely. By making the use of Secure RPC compulsory in all devices, which is a safe authentication protocol as an alternative to Netlogon, attacks targeting Zerologon can be prevented. Currently, Secure RPC, not Netlogon, can be used in Windows OS which offers product support. If the domain controller prohibits the use of Netlogon and makes the use of Secure RPC compulsory, devices would not be affected by attacks targeting Zerologon.

However, if the use of Secure RPC is made compulsory, devices which are not adaptable to Secure RPC are unable to join the domain. Therefore, Microsoft is working on addressing this vulnerability in 2 phases - Initial Development Phase and Enforcement Phase [28]. Applying the patch released on August 11, 2020 is the Initial Development Phase. The Initial Development Phase is a tentative measure which makes the use of Secure RPC compulsory on devices mounting Windows OS which offers product support. Applying the patch which is planned to be released in February 2021 is the Enforcement Phase. The Enforcement Phase is a permanent measure which makes the connection using Secure RPC compulsory on any devices.

(1) Initial Development Phase

Applying the patch released in August 2020 alone allows devices mounted with an OS other than Windows OS to connect using Netlogon. Therefore, in the Initial Development Phase, additional measures are necessary including the detection of suspicious connections using Netlogon and changing Secure RPC to an available OS. If all devices in the domain can use Secure RPC even in the Initial Development Phase, you can prohibit the use of Netlogon and make to use of Secure RPC compulsory in all devices in the domain by setting the registry key of the domain controller as follows.

- Set the FullSecureChannelProtection registry key to 1.

This can reduce the risk of being attacked through exploitation of Zerologon even before applying the patch released in February 2021.

If there are devices which cannot use Secure RPC and there is a need to connect from Netlogon, you can allow the use of Netlogon to specific groups and accounts by setting the group policy as follows.

- Policy path: **[Computer Configuration], [Windows Settings], [Security Settings], [Local Policies], [Security Options]**
- Setting name: **Domain controller: Allow vulnerable Netlogon secure channel connections**

It should be noted that, if connections through Netlogon are allowed, there will be an increased risk of Zerologon exploitation.

By applying the patch which was released in August 2020, the following event ID will be output in the event log of the domain controller [29].

Table 6: Netlogon-related information recorded in the event log

Event ID	Category	Details
5827	Error (machine accounts)	Events recorded in the log when connections by Netlogon are rejected.
5828	Error (trust accounts)	
5829	Warning (machine accounts)	Events recorded in the log when connections by Netlogon from a device mounted with an OS other than Windows OS are allowed (Initial Development Phase only)
5830	Warning (machine accounts)	Events recorded in the log when connections by Netlogon are allowed.
5831	Warning (trust accounts)	

When a domain controller which has applied the patch rejects connections by Netlogon, Event ID 5827 or 5828 will be recorded in the event log. In this case, the following three cases are assumed.

1. It is connected from a device which is mounted with Windows XP or Windows 7 with expired product support. Upgrade OS to Windows 8.1 or 10.
2. A device which is mounted with Windows 8.1 or 10 uses Netlogon. Change the setting to use Secure RPC, not Netlogon.
3. Update the setting to use Secure RPC for devices which are mounted with an OS other than Windows.

When a domain controller which has applied the patch allows connections by Netlogon from a device mounted with an OS other than Windows, Event ID 5829 will be recorded in the event log. In this case, change the setting of the applicable device to use Secure RPC. If the applicable device cannot use Secure RPC, it is unable to join the domain after the Enforcement Phase. Consider updating the device.

When a domain controller which has applied the patch allows connections by Netlogon from a device mounted with an OS other than Windows while connection by Netlogon is allowed by setting a group policy, Event ID 5830 or 5831 will be recorded in the event log. If the applicable device can update OS to use Secure RPC, update the OS. If all devices can use Secure RPC, set the registry key of the domain controller, change the group policy to the default setting and make the use of Secure RPC compulsory.

(2) Enforcement Phase

The domain controller which has applied the patch which is planned to be released in February 2021 makes the use of Secure RPC compulsory to all devices to be connected. In the same way as in the Initial Development Phase, you can allow the use of Netlogon to specific groups and accounts by setting a group policy. If connections by Netlogon are allowed, there will be an increased risk of Zerologon exploitation. Identify connections by Netlogon by monitoring the event log.

Table 7: Response to be carried out and allowance/denial of connections by Netlogon

Phase	Response	Connection by Netlogon
Initial Development Phase	Patch application	Prohibit connections from devices other than those not using Secure RPC which are mounted with an OS other than Windows.
	Patch application Change registry key	Not allowed (No exceptions)
	Patch application Change registry key Change group policy	Prohibit connections from specific devices.
Enforcement Phase	Patch application (February 2021)	Not allowed (No exceptions)
	Patch application (February 2021) Change group policy	Prohibit connections from specific devices.

2.2.4. Conclusion

Zerologon is a critical vulnerability which can give a chance to steal the administrator's rights of the domain controller. Although you might think that there is no problem if attackers do not intrude in the internal network, intrusion cases into an internal network have still occurred and it is very risky to leave the vulnerability. If the patch released in August 2020 has not been applied yet, apply it immediately. Even if the domain controller has applied this patch, the domain controller can still be attacked from a device mounted with an OS other than Windows OS. It is recommended to change the setting of the domain controller without waiting for the patch which is planned to be released in February 2021 and prohibit connections by Netlogon in order to reduce the risk of attacks through the exploitation of Zerologon as early as possible. If there are devices which cannot use Secure RPC, it is recommended to change the device OS to OS compatible with Secure RPC as soon as possible.

When a vulnerability is published, it is important to apply the patch immediately. On the contrary, some cases are assumed where applying the patch alone is inadequate as a measure such as in the Zerologon case, and it is unavoidable to abandon patch application. In order to reduce the risk of vulnerability exploitation while controlling the impact on business, it is important to understand the details of vulnerability and the patch, verify the impact of the patch on business operation and then apply the patch. It is also necessary to try to reduce the risk of vulnerability exploitation as much as possible by taking tentative measures even when the patch cannot be applied immediately.

3. Data Breach

In the 2nd Quarter of 2020, data breach cases from attacks targeting the vulnerability of supply chain have occurred one after another and there were also cases of breaching important personal information including My Number and social security numbers. In recent years, the supply chain has become complex due to globalization and diversifying business models, which has led to many of these cases. The “10 Largest Information Security Threats” which is published annually by the Information-technology Promotion Agency, Japan (IPA), attacks targeting the vulnerability of supply chain were ranked in the top 4 in 2019 and 2020, and the significance of supply chain risk management has increased [30].

3.1. Cases targeting the vulnerability of supply chain

Table 8: Cases targeting the vulnerability of supply chain

Organization	Cases
Saxo Bank Securities (*Japanese Subsidiary of Saxo Bank A/S)	Personal data of about 38,000 customers including name, address, email address, etc. was leaked from an Internet securities company, Saxo Bank Securities. My Number Card information of 378 customers was disclosed. The login password required for the transaction is stored in the server managed by the parent company Saxo Bank A/S, which was not leaked. The cause was an overseas attacker’s group which illegally accessed the server storing the transaction tool outsourced by the company [31] [32].
LiveAuctioneers	In an auction site LiveAuctioneers, personal data of 3.4 million customers including name, email address, phone number, ciphered password, etc. was leaked and the attacker deciphered the password of 3 million cases. The cause was a supplier who suffered a cyberattack and the database of bidders was illegally accessed [33] [34].
Promo.com	In a video production site Promo.com, user records of 22 million cases including name, email address, hashed password, etc. were leaked and disclosed in a hacker’s forum. It is likely that the attacker deciphered passwords. Vulnerability of a third party service caused the leakage [35] [36].

Dave	In a digital banking service Dave, customer data including name, email address, phone number, enciphered social security number, etc. was stolen and about 7.5 million cases of customer information were provided free of charge in the hacker's forum RAID. The attacker intruded in database of Waydev, a Git analysis company and a former third party service provider, using the vulnerability of the blind SQL injection and obtained the access rights to GitHub or GitLab of Dave. The cause of the data breach was that the attacker illegally accessed customer data in the Dave application using the access right obtained [37] [38] [39].
------	---

3.2. Measures against supply chain risks

In the case of Saxo Bank Securities, the Financial Services Agency issued an Order for Business Improvement as preventive measures against re-occurrence were not taken enough concerning system risk management and outsourcing contractor management. The company had published measures of introducing two-factor authentication. However, it is considered that the Financial Services Agency decided that the company required an organizational review on the issue of the outsourced transaction tool having been operated with the existence of the vulnerability.

It is required to understand security measure status in the whole supply chain and fully reduce risks in order to prevent data breach from a third party with insufficient security measures or attacks (supply chain attacks) via a third party. We will introduce 2 methods which were covered as featured topics in past quarterly reports [40].

The first is a method of understanding the whole supply chain and manage the borders of responsibilities in a batch appropriately. It lets all clients to disclose their operation procedure and details of security measures and requests them to equip with security measures. The realization of this is extremely difficult as it is unable to fully understand the operation procedures and systems of other organizations and manage their security measures. This method is possible only if the organization is on the top layer of the supply chain and can fully take control of terminal organizations.

The second is a method of taking security measures in each organization by setting the operator and scope of responsibility for security measures in advance between partner organizations. Examining possible risks in advance and building consensus can prevent omission of measures in the whole supply chain. However, trusting partners is the only way of security measures in organizations other than your organization. Taking into consideration that an attacker can make attacks via a partner or information provided to a partner can be breached, it is necessary to take measures including identification of attacks and providing minimum required information.

3.3. Impacts of data breach on organization

Recognizing the impacts of data breach on organization is important in promoting security measures. When data breach has occurred, the following impacts can be felt by an organization.

Table 9: Examples of impacts of data breach on organization

Impact	Details
Compensation for damage	Compensation for damage to people and organizations caused by data breach
Handling cost	Expenses for the investigation of cause and preventive measures for re-occurrence, public relations cost for notice of apology
Loss of opportunity	Decreased sales and suspension of transactions due to service interruption or loss of social credibility
Legal remedy	Criminal penalty (fine, bidding ban) imposed by each country's laws and regulations (Act on the Protection of Personal Information, GDPR, etc.)

Breached account information such as personal information, password, etc. can be exploited for target-type phishing attacks and password list-type attacks. It is also considered that compensation for the secondary damage is demanded to the organization. Many countries in the world are developing laws on the protection of personal information with penalties including GDPR in European Union (EU). In Japan, the Amendment Act of the Act on the Protection of Personal Information, etc. was promulgated in June 2020 and part of the highest penalty amount was raised. Impacts of legal sanctions on organizations are expected to grow in the future.

The "Survey on Cost Incurred by Data Breach in 2020" released by IBM Security in July 2020 revealed that the cost incurred by data breach is 3.86 million dollars (about 400 million yen) per case on average. The survey result indicates that breach cases of customers' personal information saw the highest cost [41].

It is important to understand impacts on organization when promoting security measures and making decisions.

3.4. Information breach cases in the 2nd quarter of 2020

Table 10: Data breach cases in the 2nd quarter of 2020

Date published	Organization	Cause	Summary
7/10	Dunzo	Cyberattacks	A third party's server was illegally accessed and user information including phone number, email address, etc. was leaked. [42]
7/16	MyCastingFile	Misconfiguration	Information of about 260,000 registered users including name, address, phone number, email address, etc. was disclosed. [43]
8/7	Mitsubishi Heavy Industries, Ltd.	Social Engineering	An internal PC connected to an external network without going through the internal network and was infected with a virus when the user used SNS. Information of employees was disclosed. [44]
8/11	SANS Institute	Phishing	Staff received a phishing mail and about 28,000 pieces of data including personal information were breached. [45]
9/10	Nomura Securities Co., Ltd.	Internal improprieties	A former employee illegally breached 275 corporate customer information to other companies. [46]
9/12	LINE Corporation	Password list attacks	Unauthorized login to about 74,000 user accounts of LINE, a communication application. [47]
9/24	HJ Holdings, Inc.	Password list attacks	Unauthorized login to about 800 user accounts of Hulu, a video distribution service. [48]

3.5. Conclusion

In this document, we have introduced attack cases targeting vulnerability of supply chain and measures, and impacts of data breach on organizations.

2 methods to counter supply chain risks were introduced, but it is actually difficult to prevent attacks completely. Various organizations provide guidelines and frameworks on supply chain management. For example, there is "Cyber Physical Security Measure Framework" issued by the Ministry of Economy, Trade and Industry in 2019. It shows not only measures to be taken by organizations as a supply chain risk management but also

coordination with related standards at home and abroad (Cybersecurity Framework, etc. issued by NIST) [49].

In recent years, the number of services which evaluate supply chain risks has been increasing. These services are useful as they have a service to unify the management of security measure status in the increasingly complex whole supply chain and make vulnerabilities and points that can easily get attacks transparent.

In Japan, there are businesses to support incident responses in small and medium-sized enterprises, which have insufficient security measures due to the lack of human factors, etc. and can easily be targeted by attacks [50]. Efforts have continued to reduce risks using these methods.

4. Vulnerability

This Chapter explains the vulnerability (CVE-2020-5902) which arose in several products of BIG-IP. The CVSS Base Score of the applicable vulnerability which was published in JVN was 10, showing that it is an extremely serious vulnerability. Organizations which have introduced the said product are required to apply the patch immediately.

4.1. Vulnerability which arose in several products of BIG-IP.

4.1.1. Summary of vulnerability

On July 6, 2020, JPCERT/CC published a “reminder about the vulnerability (CVE-2020-5902) of several BIG-IP products” [51]. This vulnerability was found in the Traffic Management User Interface (TMUI), the management screen of BIG-IP products by F5 Networks. By exploiting this vulnerability, the attacker can remotely execute any arbitrary code regardless of the presence/absence of authentication. If TMUI of the products is set to be accessible from the Internet, the device used can be affected by the vulnerability [52].

As a permanent measure for the vulnerability, F5 Networks has provided an update to fix the vulnerability [52]. As a tentative measure, they also provided a method to execute access control to mitigate the impact of the vulnerability [52].

4.1.2. Timeline

Table 11 shows chronological events from the detection of the vulnerability (CVE-2020-5902) of several BIG-IP products to the release of the exploitation method of the vulnerability to the public.

Table 11: Timeline to the release of the exploitation method of CVE-2020-5902

Date	Events
Wednesday, April 1, 2020	Mikhail Klyuchnikov of Positive Technologies reported a vulnerability present in a BIG-IP product of F5 Networks [53].
Friday, April 3, 2020	F5 Networks reproduced the above vulnerability [53].
Wednesday, July 1, 2020	F5 Networks announced that they confirmed the vulnerability (CVE-2020-5902) present in BIG-IP products and released a fixing patch and advisory [54].
Thursday, July 2, 2020	Positive Technologies released its own advisory [55].

Sunday, July 5, 2020	A Proof of Concept code (PoC) was published on Twitter, which enables attacks through the exploitation of this vulnerability [56].
Monday, July 6, 2020	An exploit module for Metasploit was published on GitHub [57].

The vulnerability was published on July 1. 4 days after this, on July 5, an exploit module the PoC code was published on SNS as shown in Table 11, and an exploit module for Metasploit was published on GitHub on the following day, July 6. This means that, after the publication of the vulnerability information, the exploitation method became widely open to the public within a week.

Recently, there are cases where an attack begins the following day of the publication of the vulnerability [58], or where there is no measure including patch, etc. at the time of the vulnerability publication (Zero-Day Vulnerability). The time between the publication of vulnerability information and the release of exploitation method is short and the grace period for the response of vulnerability can be very short.

Therefore, the person in charge of information security in an organization needs to collect information on vulnerabilities regularly. If vulnerability information is detected in the product you use, it is important to take a mitigation measure or apply the patch immediately.

4.1.3. Attack-related cases

In early July 2020, after the vulnerability (CVE-2020-5902) of BIG-IP products was published, BAD PACKETS observed a significant amount of scanning on the vulnerability [59]. Several organizations in Japan also observed communications which seem to be attempts to scan or exploit the vulnerability [51] [60]. Vulnerability is scanned to check the existence of any system with a vulnerability or identify defects which might allow illegal intrusion into the system [61]. Scanning itself doesn't affect the system. However, if an attacker finds a system with a remaining vulnerability which he/she can exploit by scanning it, he/she is likely to attack the system.

Table 12 shows results of the survey for BIG-IP products published online by BAD PACKETS [59]. The survey revealed that a total of 8,204 products whose TMUI was published online as of July 5 (the vulnerability of 3,012 of the total has not been fixed) waccess limitas found. In this case, anyone can easily try to scan or access the product via the Internet and has an increased risk of being attacked.

TMUI is an interface for the administrator of BIG-IP products and it is not recommended to publish it on the Internet under ordinary circumstances. There are two access routes to TMUI: Management Port and Self IPs. For the former route, it is recommended to limit access through the connection source IP addresses [62]. In the default setting, access is permitted from all IP addresses. [63] In the latter route, accessible protocols and services are limited to

minimum necessary by default [64] HTTP and SSH which are necessary to access TMUI is permitted. In some cases, the product is used without changing the above default setting to an appropriate setting or the setting is misconfigured and TMUI is published on the Internet without knowing it. It is recommended to recheck the setting of the products and network design including the products as well as response to the vulnerability.

Table 121: Number of BIG-IP products with unfixed vulnerability [59]

Country	Number of unfixed products
USA	1,237
China	496
Taiwan	144
Thailand	114
South Korea	91
Malaysia	80
The Philippines	79
Indonesia	72
Brazil	65
Japan	60

Trend Micro found an IoT malware downloader which exploits the vulnerability [65]. The downloader searches BIG-IP products accessible from the Internet and intrudes inside by exploiting the vulnerability. Then, it connects to an illegal site and downloads and executes "SORA," a subvariety of IoT malware "Mirai" [66]. "SORA" intrudes in an IoT device via vulnerable BIG-IP products and develops an IoT bot net. It is also found that the downloader attacks by exploiting various vulnerabilities published in the same period as shown in Table 13.

Table13: Vulnerabilities which are exploited by downloaders [65]

Device	Vulnerability	CVE identifier
Apache Kylin 3.0.1	Command injection	CVE-2020-1956
Aruba ClearPass Policy Manager 6.7.0	Unauthenticated remote command execution	CVE-2020-7115
Big-IP 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, 11.6.1-11.6.5.1	Remote code execution using TMUI	CVE-2020-5902

Comtrend VR-3033	Command injection	CVE-2020-10173
HP LinuxKI 6.01	Remote command injection	CVE-2020-7209
Tenda AC15 AC1900	Remote code execution	CVE-2020-10987
Nexus Repository Manger 3	Remote code execution	CVE-2020-10204
Netlink GPON Router 1.0.11	Remote code execution	None
Netgear R7000 Router	Remote code execution	None
Sickbeard 0.1	Remote command injection	None

4.2. Conclusion

We picked up the vulnerability of BIG-IP products this time. According to a survey by Macnica Networks [67], there were 67 BIG-IP products which were published on the Internet by TMUI without fixing the vulnerability in Japan as of July 8, 2020 and measures remain necessary. The person in charge of information security in an organization needs to manage the status of the software structure of the organization, collect information on vulnerabilities and promptly apply the patch if a dangerous vulnerability is found. An intrusion might have occurred already when the patch is applied. It is also important to investigate if there was an intrusion using an IoC detection tool [68] rather than feeling secure after the patch application.

Teleworking which is expanding due to the novel coronavirus has led to the remote operation of system management from home. Unlike the time when all administrators accessed the system from the office, multiple administrators need to connect to the system management screen to manage things through a provider at home. It might be difficult to limit access to some from connection source IP addresses. A significant amount of TMUI without access limit might have existed for this reason. If it is impossible to set an access limit to the management screen, try to use the system securely by introducing measures to prevent unauthorized connections from attackers such as the use of login methods using SSL-VPN connection which uses a client certificate or two-factor authentication.

5. Malware/Ransomware

5.1. Summary of the 2nd quarter of FY 2020

Activities of malware Emotet, which caused many infection cases in the 3rd quarter of 2019 have been identified again. Following the 1st quarter of 2020, many damage cases caused by ransomware such as Maze and NetWalker have been reported. Illegal access and data breach damage from malware infection has been reported in Japan. Service damage caused by ransomware infection has been reported overseas. This chapter explains the worsening of damage caused by the revival of Emotet and ransomware attacks because the impact of future damage expansion is significant.

5.1.1. Revival of Emotet

Although many infection cases of Emotet have been reported from October 2019 to February 2020, the infecting activities have calmed down between March and July 2020. However, active infection activities have been identified again from the end of July 2020 and one of the largest infections was found in September [69].

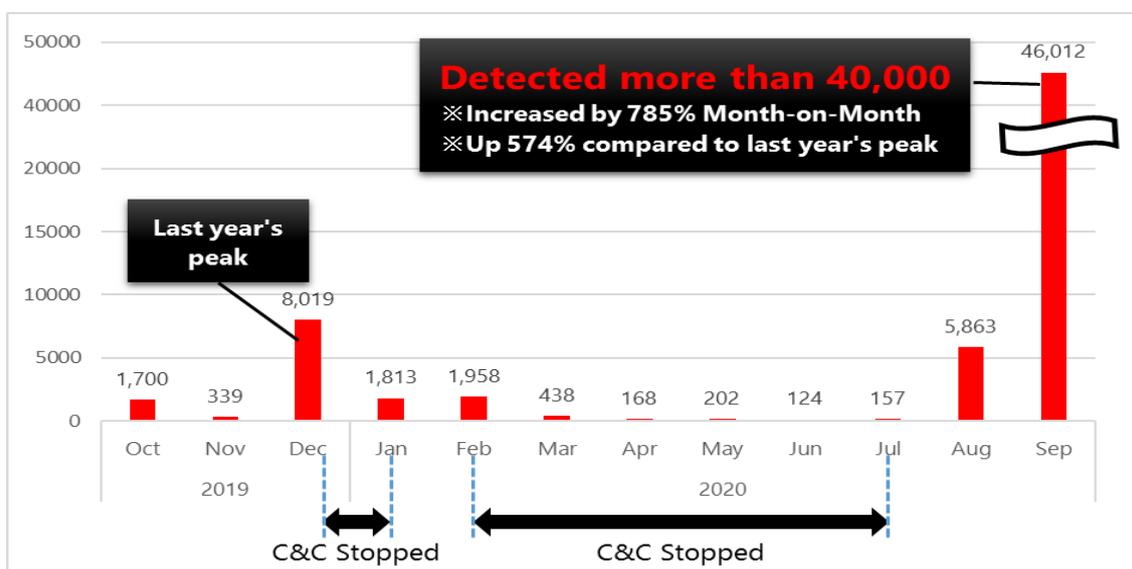


Figure 6: Changes in the number of Emotet detections in Japan [69]

The reason that Emotet infection is expanding is that the spreading method is becoming more sophisticated. Emotet emails after July 2020 copied the contents frequently seen in business emails in Japan. The body of email begins with "To Associated Companies" or the email title/attached file name is "Fire Services Inspection," "Notification of Payment and Request for Issuing the Bill" or "Subject of the Next Meeting." It is difficult to distinguish them from genuine emails at a glance.

After September 2020, a new method to spread Emotet using a password-protected zip file has been reported [70]. As password-protected zip files are encrypted, they can pass through virus detection of security products through email delivery and the files might not be removed. Therefore, there is a high probability that malicious files are delivered to receivers. When sending a password-protected zip file, a method to send 2 separate emails - sending the encrypted attached file in the first email and the unzip password in the second email - has widely been used in Japan as a measure to prevent data breach from the wrong transmission of emails. However, attackers who can intercept emails are highly likely to be able to obtain both the attached file and the password and it is said that this is not sufficient as a data breach measure. The central ministries and agencies announced the policy to abolish the use of password-protected zip files [71].

As a measure for the new method to spread Emotet, it is effective to take the plunge and stop sending/receiving emails with attached password-protected zip files. This will avoid the risk of malicious files to be open without being removed, in addition to the abolition of the above-mentioned deficient data breach measure.

The report of the 3rd quarter of 2019 estimated that the infection spread widely in small and medium-sized enterprises with insufficient security measures and training compared with large enterprises [72]. The same trend can be seen in the spread in the 2nd quarter of 2020. The highly effective measure for target-type attacks entering through emails including Emotet is to build a solution to detect and stop attacks on the email system. It is however difficult for small and medium-sized enterprises to introduce it as introducing the solution is costly and time-consuming. Using email services with functions to detect and sort malicious emails such as Gmail is an example of a measure suitable for small and medium-sized enterprises. It is reasonable and does not take time to introduce compared with introducing and operating a detecting and sorting solution in the existing server.

In the future, the method is expected to become more sophisticated and the expansion of damage from Emotet is concerned. IPA has published the title and body of Emotet emails together, which were actually used [70]. Keep a close watch on the latest information such as information sent by IPA and JPCERT/CC [73].

5.1.2. Worsening of damage caused by ransomware attacks

In September 2020, a university hospital in Dusseldorf, Germany was attacked by ransomware, which stopped the hospital's healthcare system and resulted in the tragedy of a patient's death while the patient was in transit [74]. There were ransomware attacks targeting medical institutions in the past, but this time a person's life was lost for the first time. Ransomware did not directly target the patient's life and it is assumed that the attacker did not intend to target human life in this case as the university which manages the hospital was the target. However, as many cyberattacks which take advantage of the global coronavirus pandemic have been reported from the 4th quarter of 2019 [75] [76], there will be an increasing chance of losing human life from ransomware attacks targeting medical institutions.

An attack to Garmin, a US GPS service company, which occurred in July 2020 caused service

damage from ransomware infection [77]. Services such as Garmin Connect which synchronizes user activities and data to clouds and other devices and fly Garmin which plans navigation of aircrafts and routes stopped and several million users in the world who use these services were affected for a week. If similar problem occurs in critical infrastructures such as air traffic control systems and plant control systems, the suspension of services can cause confusion in social activities and negative impacts all over the world.

As in above cases, ransomware attacks not only cause financial damage but also can cause damage relating to human life and worldwide confusion. In particular, as it is highly likely that infection with ransomware causes a system to stop, it is important to prevent infection as early as possible. It is effective to take measures at the end point, the origin of the ransomware outbreak. Specifically, detect and stop activities relating to suspicious shell script operations by detecting behaviors of EDR products. This can detect fileless malware attacks which avoid anti-malware software.

5.1.3. Other damage cases of malware

In the 2nd quarter of 2020, many organizations became a victim of malware and ransomware attacks. Many incidents caused by ransomware have been reported recently from overseas companies. Illegal access and data breach damage from malware infection has been reported in Japan. Service damage caused by ransomware infection has been reported overseas. Damage cases caused by malware and ransomware which were reported in the 2nd quarter of 2020 are shown in Table2.

Table2: Malware/ransomware damage cases * Date of announcement

Date	Target	Summary
7/7	USA/ Alabama/Chilton County	Computer network was closed temporarily due to a suspected ransomware attack. [78]
7/18	Argentina/Communications company/Telecom Argentina	Infected with ransomware. There was a problem with internal VPN and database access. [79]
7/23	Spain/National railway infrastructure management company/ADIF	Infected with REvil ransomware. There was no large impact from the attack. [80]
8/6	USA/Electrical equipment company/Cannon USA	Infected with Maze ransomware. Part of the data on the cloud platform they manage disappeared. [81]
8/7	Mitsubishi Heavy Industries, Ltd.	An internal laptop was infected with malware. The infection spread to an internal network and caused unauthorized access damage. [82]
8/16	USA/Sake brewery/Brown-Forman	Infected with Sodinokibi ransomware. They prevented encryption of system data. [83]

8/21	The Japan Association of Corporate Executives	Part of the secretariat system was infected with ransomware and had a system failure. [84]
8/28	Fukuoka Prefecture/Real estate sales/Dax Corporation	Infected with malware and the past email transmitting/receiving history was disclosed. Email transmitting records pretending to be company's employees and the company's email address were also found. [85]
9/5	USA/Cyber security company/Cygilant	Infected with Netwalker ransomware. [86]
9/7	Pakistan/Electric cooperative/K-Electric	Infected with Netwalker ransomware. There was a problem with an online billing service. [87]
9/14	USA/Fiber laser company/IPG Photonics	Infected with RansomExx ransomware. The internal IT system was shut down and caused failure in email, telephone, network connection, etc. [88]

5.2. Conclusion

Revival of malware Emotet has been identified in Japan. As a measure for the newly discovered Emotet which exploited password-protected zip files, it is effective to take the plunge and stop sending/receiving emails with attached password-protected zip files. In the 2nd quarter of 2020, a human life was lost because of a ransomware attack. As it is highly likely that infection with ransomware causes a system to stop, it is important to take measures to prevent infection as early as possible.

6. Outlook

Verifying proofing will become more important

We mentioned that, out of “securities required for payment services,” two-factor authentication using SMS is highly likely to be passed through by acts known as SMS intercept or SIM swap and it is not an adequate authentication method. However, there is another reason that SMS authentication is not adequate as a user authentication method. It is because there are “SMS authentication proxies.” Originally, it was a service which assumes cases such as when people would like to create an account on a device using a SIM card which is not compatible with SMS or when people would like to create several accounts but have only 1 phone number. However, there is an increasing number of cases where the service is used by application users to hide their identity and Saitama Prefectural police has issued a warning that it encourages crimes [89]. There is a SIM card which is available without proofing in the background. If the SIM card holder shares a phone number and an authentication code which the number received to a proxy agency, the agency can pass through authentication with hidden proofing. As the number of users of cheap SIM cards which do not need a contract with a major carrier is rising, it is considered that it will become easier to illegally pass through SMS authentication in the future. In order to gain trust from users, providers which complete services online need to reconfirm that identity verification process does not complete by “authentication” alone and carry out proofing including eKYC.

Continuous attacks to supply chain

Many attack cases targeting supply chains have occurred between June and September 2020. In 5 countries including USA and UK, there is a survey result that shows 80% of organizations were damaged by supply chain attacks in the past year. As a countermeasure to this attack, it is necessary to understand the security measure status over the whole supply chain first. However, a survey result shows that 77% of organizations in 5 countries including USA and UK has not identified the measure status [90]. This implies that many organizations in many countries have not taken measures and a number of organizations require a measure against supply chain attacks.

In addition, it is assumed that the development of measures have not progressed as it is estimated that the security market growth in 2020 will slow down [91]. Furthermore, organizations which were connected through the supply chain changed their working style to telework due to the spread of the novel coronavirus. As the remote access from home PCs increased, the number of points which attackers can target easily is increasing [92]. Under this circumstance, it is assumed that attackers continue to attempt supply chain attacks. Therefore, we recommend using guidelines and frameworks on supply chain management as well as services that evaluate supply chain risks as shown in “3. Data Breach” . In Japan, the Supply Chain Cyber Security Consortium was established as a group

to promote cyber security measures between large enterprises and small and medium-sized enterprises. It is effective to use information provided by such group [93].

Take precautions against cyberattacks related to novel-coronavirus

Although attacking emails including phishing mails, etc. which pretend to provide infection information of the novel coronavirus are still seen as of September, the number is decreasing compared to the peak in April [94] [95]. It is considered that this is because various organizations in the world brought new attention to attacking emails related to the novel coronavirus information while the number of infection cases and death rose and people became immune to fake information, and because there were themes such as telework and stay home which were easier to fake [96]. This type of attack mails will decrease if there is no big change in information related to the novel coronavirus. However, when vaccination of the novel coronavirus starts in many countries, people will strongly seek information on the vaccines. It is expected that the number of phishing, smishing and fake application attack cases will increase in the same way as the initial spread of the novel coronavirus. It is recommended for information receivers to always keep in mind the points to be noted written in the report of the 4th quarter of 2019 in order to avoid damage from attacking emails [97].

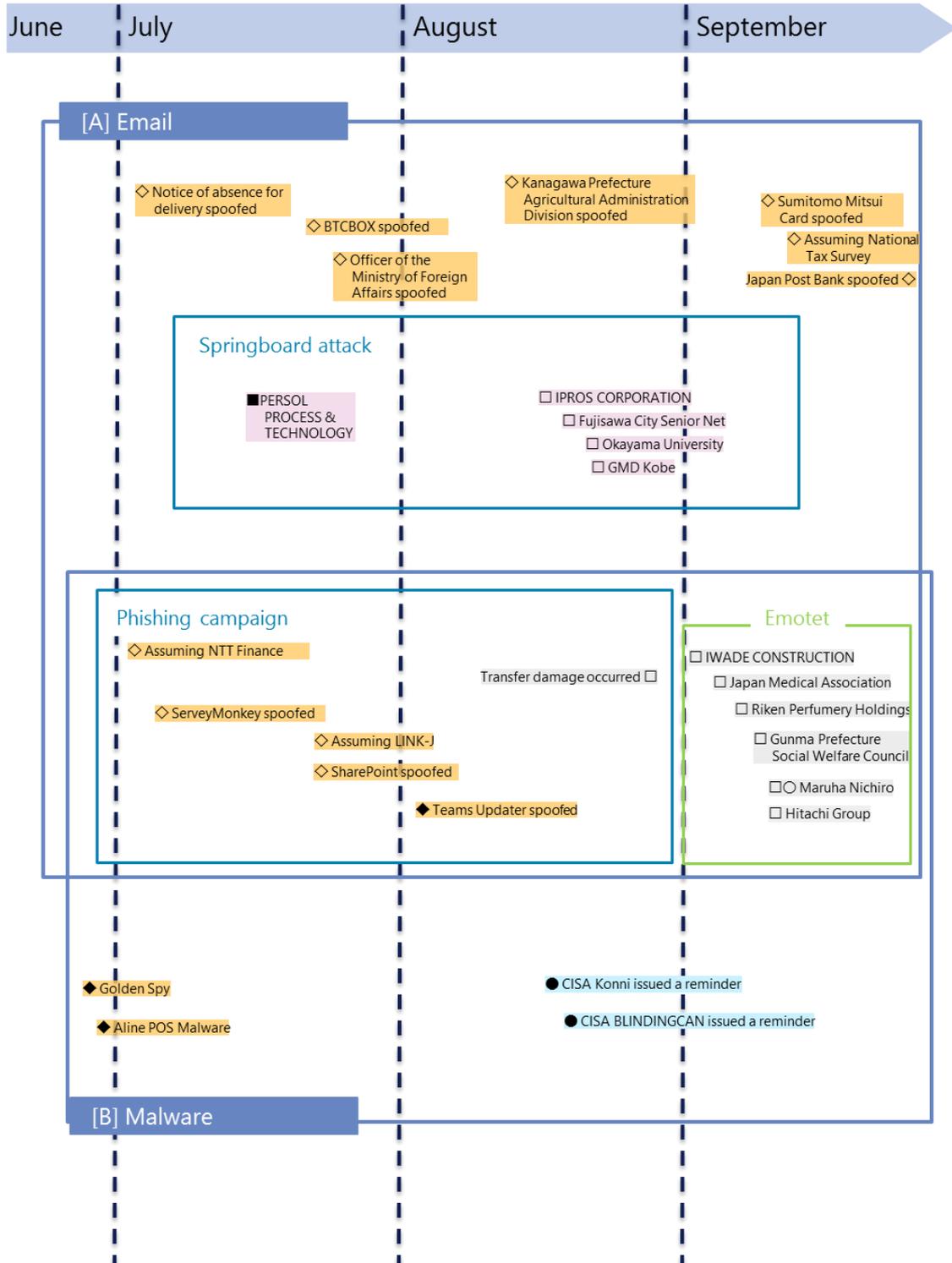
Make sure to remember there will be attacks to the New Normal as attacks related to the novel coronavirus. Various new risks were generated due to the change in working style to telework [92]. It is assumed that many organizations haven't taken sufficient measures against risks caused by the change to telework as there was not enough time after the change and the security budget was not fully prepared due to the impact of the novel coronavirus. Under this circumstance, it is assumed that attack cases targeting home PCs, cloud services and communication tools and the expansion of incident damage from communication difficulties will continue to occur. It is recommended to read the risks caused by the increased amount of telework and the points to be noted written in the report of the 1st quarter of 2020 and consider taking measures [92].

7. Timeline

* Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

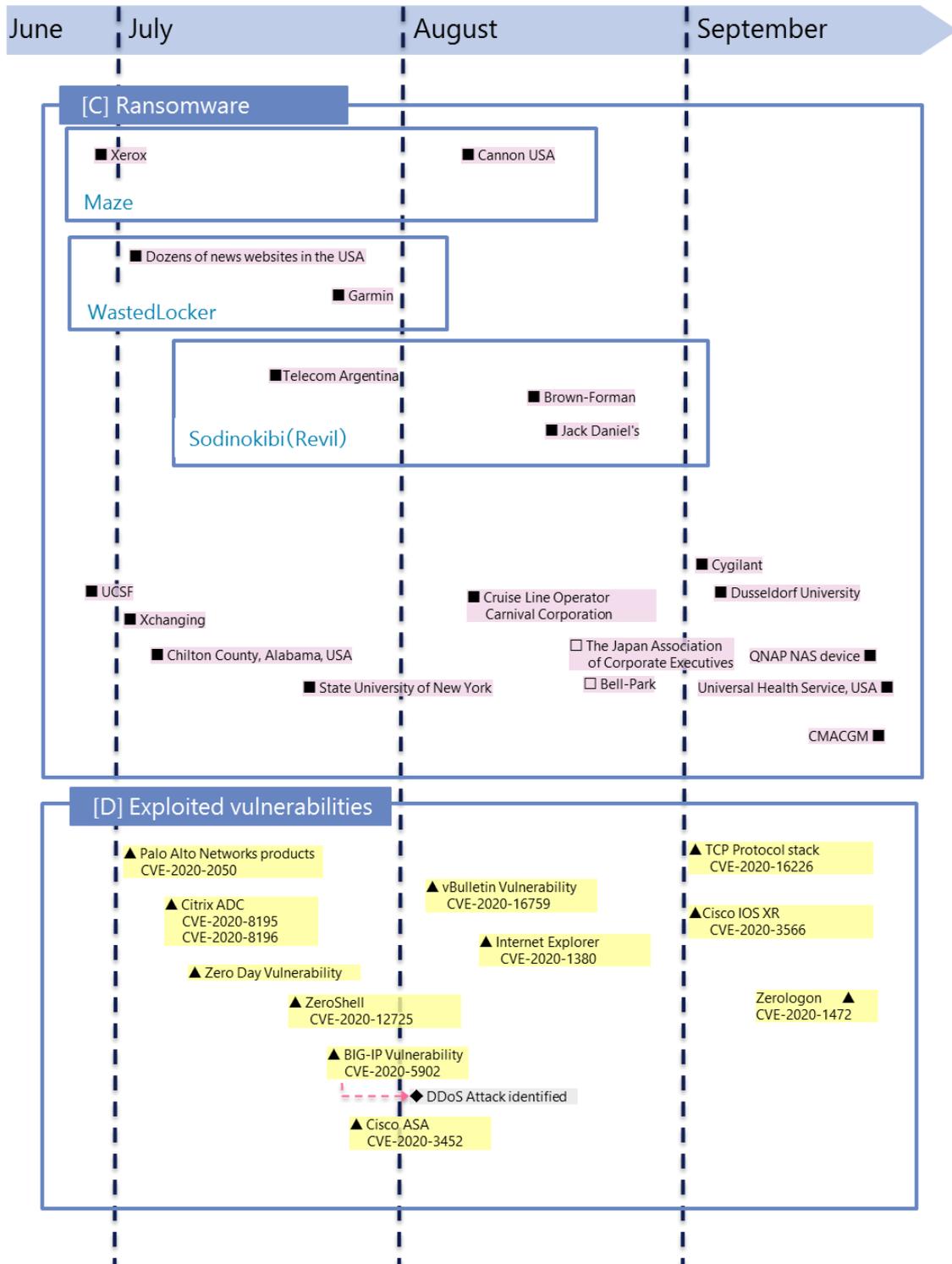
△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



* Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

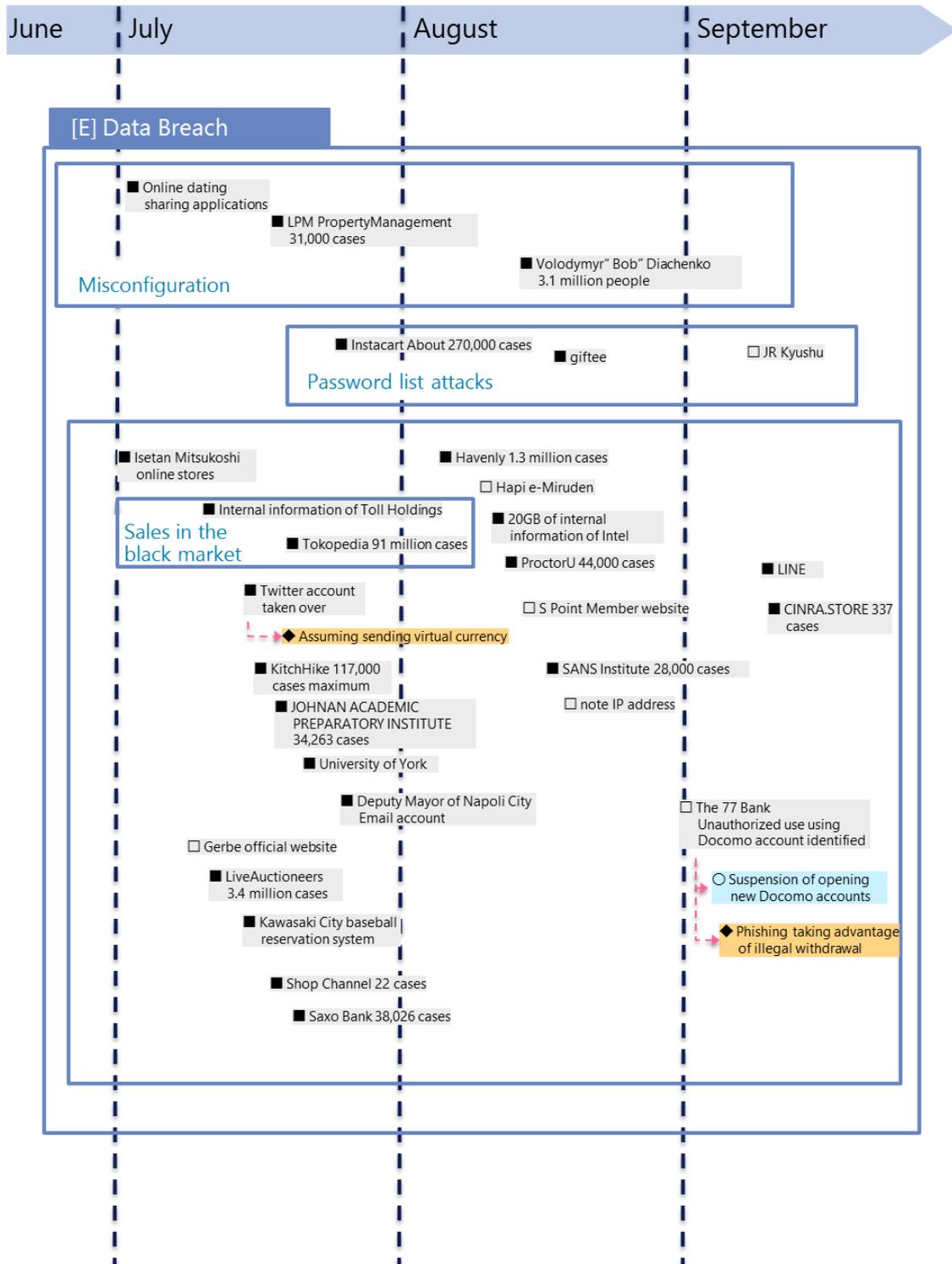
△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



* Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

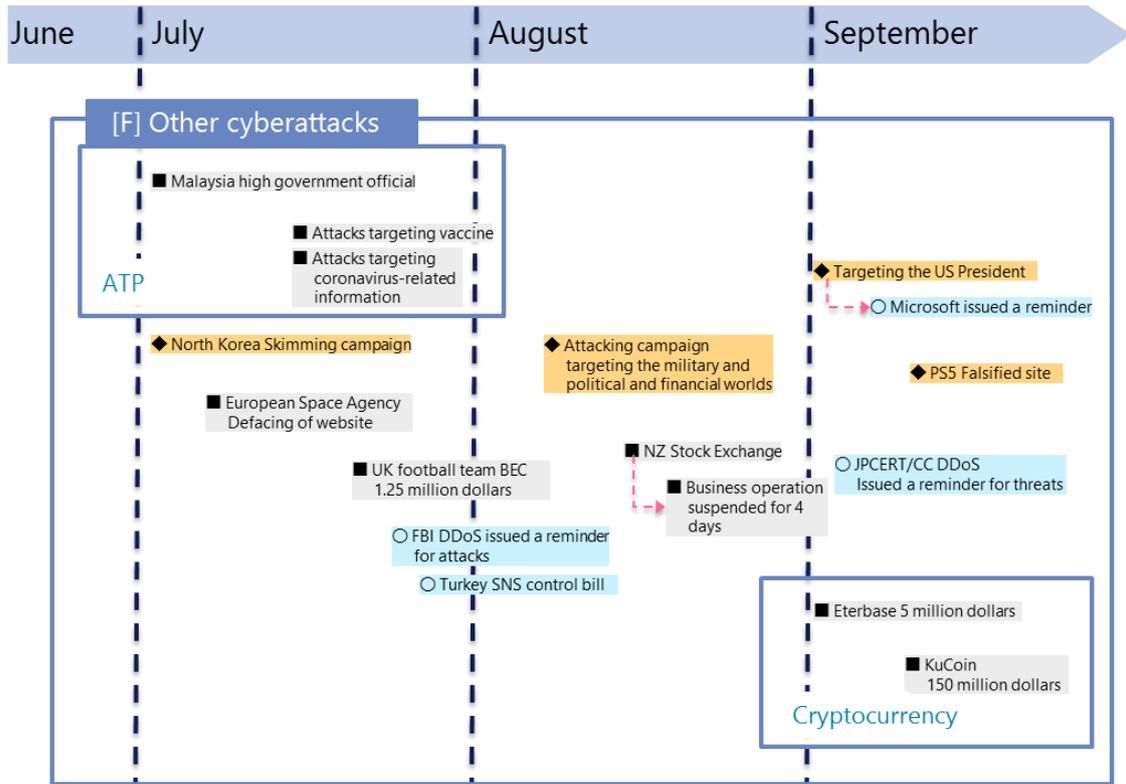
△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



* Some dates on this timeline are dates of article publication rather than dates of when the incident occurred.

△□◇○: Japan
▲■◆●: Global/Overseas

△▲: Vulnerability
◇◆: Threat
□■: Incident
○●: Measure



References

- [1] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威 2020,” 独立行政法人情報処理推進機構, 28 8 2020. [オンライン]. Available: <https://www.ipa.go.jp/security/vuln/10threats2020.html#download>.
- [2] 株式会社SBI証券, “悪意のある第三者による不正アクセスに関するお知らせ,” 株式会社SBI証券, 16 9 2020. [オンライン]. Available: https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html.
- [3] 株式会社NTTドコモ, “ドコモ口座とは?,” 株式会社NTTドコモ, [オンライン]. Available: <https://docomokouza.jp/detail/about.html>.
- [4] 株式会社日本経済新聞社, “ドコモ口座不正引き出し、りそな銀行で19年5月にも,” 株式会社日本経済新聞社, 9 9 2020. [オンライン]. Available: <https://www.nikkei.com/article/DGXMZO63655670Z00C20A9EE8000/>.
- [5] 株式会社日本経済新聞社, “ドコモ口座、判明被害の補償完了 128件で2885万円,” 株式会社日本経済新聞社, 28 10 2020. [オンライン]. Available: <https://www.nikkei.com/article/DGXMZO65570570Y0A021C2000000/>.
- [6] 株式会社NTTドコモ, “ドコモ口座への銀行口座の新規登録における対策強化について,” 株式会社NTTドコモ, 9 9 2020. [オンライン]. Available: https://www.nttdocomo.co.jp/info/news_release/detail/20200909_00_m.html.
- [7] “Webアプリケーションファイアーウォール (WAF) ,” キヤノン, [オンライン]. Available: <https://cweb.canon.jp/it-sec/solution/siteguard/waf/>.
- [8] NECソリューションイノベータ株式会社, “リスクベース認証,” NECソリューションイノベータ株式会社, [オンライン]. Available: <https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/24.html>.
- [9] “アジアナIDT フィンテック分野のセキュリティベンダーと協業 新たにセキュリティ事業を切り開く,” 11 2 2016. [オンライン]. Available: https://www.weeklybcn.com/journal/news/detail/20160211_14606.html.
- [10] “オンラインサービスにおける身元確認手法の整理に関する検討報告書を取りまとめました,” 経済産業省, 17 4 2020. [オンライン]. Available: <https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html>.

- [11] 一般社団法人キャッシュレス推進協議会, “コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン,” 一般社団法人キャッシュレス推進協議会, 18 9 2020. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2020/09/Fraud_Prevention_Guidelines_bkac_linked.pdf.
- [12] 一般社団法人全国銀行協会, “資金移動業者等との口座連携に関するガイドライン,” 一般社団法人全国銀行協会, 30 11 2020. [オンライン]. Available: <https://www.zenginkyo.or.jp/fileadmin/res/news/news321130.pdf>.
- [13] 各府省情報化統括責任者（CIO）連絡会議, “行政手続におけるオンラインによる本人確認の手法に関するガイドライン,” 各府省情報化統括責任者（CIO）連絡会議, 15 2 2019. [オンライン]. Available: <https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf>.
- [14] 一般社団法人キャッシュレス推進協議会, “コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン,” 一般社団法人キャッシュレス推進協議会, 16 4 2019. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/04/Fraud_Prevention_Guideline.pdf.
- [15] 一般社団法人キャッシュレス推進協議会, “コード決済に関する統一技術仕様ガイドライン【利用者提示型】,” 一般社団法人キャッシュレス推進協議会, 31 10 2019. [オンライン]. Available: https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2019/10/CPM_Guideline_1.2.pdf.
- [16] 金融庁, “「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について,” 金融庁, 30 11 2018. [オンライン]. Available: <https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html>.
- [17] PayPay株式会社, “「PayPay」のSMS認証機能のセキュリティ強化について,” PayPay株式会社, 24 6 2020. [オンライン]. Available: <https://about.paypay.ne.jp/pr/20200624/01/>.
- [18] “NISTが警告、SMSでの二段階認証が危険な理由,” ZDNetJapan, 27 1 2017. [オンライン]. Available: <https://japan.zdnet.com/article/35095393/>.
- [19] “欧米でも「決済アプリの不正出金・詐欺」多発、スクエアのCashAppやZelleでも——ドコモ、PayPayだけではない,” coindesk Japan, 19 10 2020. [オンライン]. Available: <https://www.coindeskjapan.com/84820/>.
- [20] 公益財団法人金融情報システムセンター, “口座振替による不正出金に対する金融情報システムへの安全対策のあり方,” 公益財団法人 金融情報システムセン

- ター, 2020.
- [21] “New 'Alien' malware can steal passwords from 226 Android apps,” ZDNet, 24 9 2020. [オンライン]. Available: <https://www.zdnet.com/article/new-alien-malware-can-steal-passwords-from-226-android-apps/>.
- [22] 株式会社ゼウス, “3Dセキュア (クレジットカード本人認証サービス),” 株式会社ゼウス, [オンライン]. Available: <https://www.cardservice.co.jp/service/creditcard/3d.html>.
- [23] Microsoft Security Response Center, “Netlogon の特権の昇格の脆弱性,” 11 8 2020. [オンライン]. Available: <https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2020-1472>.
- [24] Secura, “ZeroLogon: Instantly Become Domain Admin by Subverting Netlogon Cryptography (CVE-2020-1472),” 14 9 2020. [オンライン]. Available: <https://www.secura.com/blog/zero-logon>.
- [25] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, “WINDOWS SERVER VULNERABILITY REQUIRES IMMEDIATE ATTENTION,” 18 9 2020. [オンライン]. Available: <https://www.cisa.gov/blog/2020/09/18/windows-server-vulnerability-requires-immediate-attention>.
- [26] Microsoft Corporation, “ZeroLogon is now detected by Microsoft Defender for Identity (CVE-2020-1472 exploitation),” 1 10 2020. [オンライン]. Available: <https://techcommunity.microsoft.com/t5/microsoft-365-defender/zerologon-is-now-detected-by-microsoft-defender-for-identity-cve/ba-p/1734034>.
- [27] Microsoft Security Intelligence@MsftSecIntel, “Microsoft is actively tracking threat actor activity using exploits for the CVE-2020-1472 Netlogon EoP vulnerability, dubbed Zerologon.,” 24 9 2020. [オンライン]. Available: <https://twitter.com/MsftSecIntel/status/1308941504707063808>.
- [28] Microsoft Security Response Center, “[AD 管理者向け] CVE-2020-1472 Netlogon の対応ガイダンスの概要,” 14 9 2020. [オンライン]. Available: https://msrc-blog.microsoft.com/2020/09/14/20200915_netlogon/.
- [29] 日本マイクロソフト株式会社, “CVE-2020-1472 に関連する Netlogon のセキュリティで保護されたチャネルの接続の変更を管理する方法,” 20 11 2020. [オンライン]. Available: <https://support.microsoft.com/ja-jp/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc>.
- [30] 独立行政法人情報処理推進機構, “情報セキュリティ10大脅威 2020,” 独立行

- 政法人情報処理推進機構, 28 8 2020. [オンライン]. Available: <https://www.ipa.go.jp/security/vuln/10threats2020.html>.
- [31] サクソバンク証券株式会社, “サイバー攻撃による個人情報流出に関するお詫びとお知らせ,” 17 9 2020. [オンライン]. Available: <https://www.home.saxo/ja-jp/about-us/security-incident/personal-information-leakage>.
- [32] サクソバンク証券株式会社, “個人情報流出についてお客様からお寄せいただいたご質問ならびに回答,” 2020. [オンライン]. Available: <https://www.home.saxo/ja-jp/about-us/security-incident/questions-and-answers>.
- [33] LiveAuctioneers, “July 11, 2020 - LiveAuctioneers Account Security,” 11 7 2020. [オンライン]. Available: <https://help.liveauctioneers.com/article/496-july-11-2020-liveauctioneers-account-security>.
- [34] G. Cluley, “Millions of LiveAuctioneers passwords offered for sale following data breach,” 13 7 2020. [オンライン]. Available: <https://grahamcluley.com/liveauctioneers-passwords-for-sale/>.
- [35] Promo, “Promo Data Breach July 21, 2020 FAQ,” 21 7 2020. [オンライン]. Available: <https://support.promo.com/en/articles/4276475-promo-data-breach-july-21-2020-faq>.
- [36] Bleeping Computer, “Promo.com discloses data breach after 22M user records leaked online,” 27 7 2020. [オンライン]. Available: <https://www.bleepingcomputer.com/news/security/promocom-discloses-data-breach-after-22m-user-records-leaked-online/>.
- [37] Dave, “Notice of Data Breach,” 21 8 2020. [オンライン]. Available: <https://www.dave.com/blog/notice-of-data-breach/>.
- [38] ZDnet, “Tech unicorn Dave admits to security breach impacting 7.5 million users,” 26 7 2020. [オンライン]. Available: <https://www.zdnet.com/article/tech-unicorn-dave-admits-to-security-breach-impacting-7-5-million-users/>.
- [39] ZDnet, “Hackers stole GitHub and GitLab OAuth tokens from Git analytics firm Waydev,” 27 7 2020. [オンライン]. Available: <https://www.zdnet.com/article/hackers-stole-github-and-gitlab-oauth-tokens-from-git-analytics-firm-waydev/>.
- [40] 株式会社NTTデータ, “サイバーセキュリティに関するグローバル動向四半期レポート（2019年7月～9月）,” 株式会社NTTデータ, 29 11 2019. [オンライン]. Available: <https://www.nttdata.com/jp/ja/>

/media/nttdatajapan/files/services/security/nttdata_fy2019_2q_securityreport.pdf

- [41] IBM, “IBM、セキュリティーに関する調査レポートを公開,” 25 8 2020. [オンライン]. Available: <https://jp.newsroom.ibm.com/2020-08-25-ibm-security-concern-investigation-report-release>.
- [42] Dunzo, “Your Security is our Top Priority!,” 10 7 2020. [オンライン]. Available: <https://medium.com/dunzo/your-security-is-our-top-priority-def5ebe5db12>.
- [43] SafetyDetectives.com, “US casting site leaks personal data belonging to 260,000+ actors,” 16 7 2020. [オンライン]. Available: <https://www.safetydetectives.com/blog/mycastingfile-leak-report/>.
- [44] 三菱重工業株式会社, “当社グループ名古屋地区のネットワークに対する第三者からの不正アクセスに係る件,” 7 8 2020. [オンライン]. Available: https://www.mhi.com/jp/notice/notice_200807.html.
- [45] 朝日インタラクティブ株式会社, “セキュリティ教育機関で2.8万件のデータ侵害、フィッシングが原因に,” 朝日インタラクティブ株式会社, 13 8 2020. [オンライン]. Available: <https://japan.zdnet.com/article/35158096/>.
- [46] 野村證券株式会社, “法人のお客様の情報流出について,” 10 9 2020. [オンライン]. Available: <https://www.nomuraholdings.com/jp/news/nr/nsc/20200910/20200910.pdf>.
- [47] LINE株式会社, “LINEアカウントへの不正アクセスに対する注意喚起,” LINE株式会社, 12 9 2020. [オンライン]. Available: <https://linecorp.com/ja/security/article/330>.
- [48] H J ホールディングス株式会社, “Hulu「リスト型アカウントハッキング（リスト型攻撃）」による弊社サービスへの不正ログインの発生について,” 24 9 2020. [オンライン]. Available: <https://www.hjholdings.jp/release/20200924.html>.
- [49] 経済産業省, “サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました,” 18 4 2019. [オンライン]. Available: <https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html>.
- [50] 情報処理推進機構（IPA）, “サイバーセキュリティお助け隊（令和2年度中小企業向けサイバーセキュリティ対策支援体制構築事業）,” 27 10 2020. [オンライン]. Available: <https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html>.
- [51] 一般社団法人JPCERTコーディネーションセンター, “複数の BIG-IP 製品の脆弱

- 性 (CVE-2020-5902) に関する注意喚起,” 一般社団法人JPCERTコーディネーションセンター, 14 7 2020. [オンライン]. Available: <https://www.jpccert.or.jp/at/2020/at200028.html>.
- [52] F5, Inc., “K52145254: TMUI RCE vulnerability CVE-2020-5902,” 23 7 2020. [オンライン]. Available: <https://support.f5.com/csp/article/K52145254>.
- [53] M. Klyuchnikov, “Remote Code Execution in F5 Big-IP,” 15 7 2020. [オンライン]. Available: <https://swarm.ptsecurity.com/rce-in-f5-big-ip/>.
- [54] F5, Inc., “Protect Against the BIG-IP TMUI Vulnerability CVE-2020-5902,” 2020. [オンライン]. Available: <https://www.f5.com/services/support/big-ip-vulnerability-cve-2020-5902>.
- [55] Positive Technologies, “F5 fixes critical vulnerability discovered by Positive Technologies in BIG-IP application delivery controller,” 2 7 2020. [オンライン]. Available: <https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/>.
- [56] Twitter, Inc., “@x4ce Twitterアカウント,” 5 7 2020. [オンライン]. Available: <https://twitter.com/x4ce/status/1279790599793545216>.
- [57] GitHub, Inc., “Add F5 BIG-IP TMUI Directory Traversal and File Upload RCE (CVE-2020-5902),” 6 7 2020. [オンライン]. Available: <https://github.com/rapid7/metasploit-framework/pull/13807>.
- [58] 株式会社ラック, “Apache Struts2 の脆弱性(S2-016)を悪用した攻撃の急増について,” 18 7 2013. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20130718_000168.html.
- [59] Bad Packets LLC, “OVER 3,000 F5 BIG-IP ENDPOINTS VULNERABLE TO CVE-2020-590,” 5 7 2020. [オンライン]. Available: <https://badpackets.net/over-3000-f5-big-ip-endpoints-vulnerable-to-cve-2020-5902/>.
- [60] 株式会社ラック, “【注意喚起】 F5 BIG-IP製品の任意コード実行可能な脆弱性 (CVE-2020-5902) を狙う攻撃活動を観測,” 8 7 2020. [オンライン]. Available: https://www.lac.co.jp/lacwatch/alert/20200708_002231.html.
- [61] 一般社団法人JPCERTコーディネーションセンター, “攻撃を目的としたスキャンに備えて 2019年7月,” 一般社団法人JPCERTコーディネーションセンター, 22 7 2019. [オンライン]. Available: <https://www.jpccert.or.jp/newsflash/2019072201.html>.

- [62] F5, Inc., “K13092: Overview of securing access to the BIG-IP system,” 27 3 2019. [オンライン]. Available: <https://support.f5.com/csp/article/K13092>.
- [63] F5, Inc., “K13309: Restricting access to the Configuration utility by source IP address (11.x - 16.x),” 28 10 2020. [オンライン]. Available: <https://support.f5.com/csp/article/K13309>.
- [64] F5, Inc., “K17333: Overview of port lockdown behavior (12.x - 16.x),” 14 8 2020. [オンライン]. Available: <https://support.f5.com/csp/article/K17333>.
- [65]トレンドマイクロ株式会社, “「BIG-IP」の脆弱性「CVE-2020-5902」を利用するIoTマルウェアを確認,” 18 9 2020. [オンライン]. Available: <https://blog.trendmicro.co.jp/archives/26197>.
- [66]トレンドマイクロ株式会社, “ホームルータや監視カメラ用ストレージシステムを狙うIoTマルウェア:「SORA」と「UNSTABLE」,” 17 2 2020. [オンライン]. Available: <https://blog.trendmicro.co.jp/archives/23916>.
- [67]マクニカネットワークスセキュリティ研究センター, “BIG-IP等のNW機器の脆弱性まとめとSHODANでの観測状況,” 10 7 2020. [オンライン]. Available: <https://blog.macnica.net/blog/2020/07/big-ip-nw-shodan.html>.
- [68]GitHub, Inc., “CVE-2020-5902 IoC Detection Tool,” 22 7 2020. [オンライン]. Available: <https://github.com/f5devcentral/cve-2020-5902-ioc-bigip-checker/>.
- [69]安藤正芳, “Emotet検出数が前月比8倍の過去最大規模に、フィルタリングを巧妙に回避,” 日経クロステック, 22 10 2020. [オンライン]. Available: <https://xtech.nikkei.com/atcl/nxt/column/18/00001/04747/>. [アクセス日: 2020].
- [70]独立行政法人情報処理推進機構, “「Emotet」と呼ばれるウイルスへの感染を狙うメールについて,” 2 9 2020. [オンライン]. Available: <https://www.ipa.go.jp/security/announce/20191202.html>.
- [71]樋口隆充, “霞が関でパスワード付きzipファイルを廃止へ 平井デジタル相,” ITmedia, 17 11 2020. [オンライン]. Available: <https://www.itmedia.co.jp/news/articles/2011/17/news150.html>.
- [72]株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第3四半期,” 株式会社NTTデータ, 28 2 2020. [オンライン]. Available: https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/services/security/nttdata_fy2019_3q_securityreport.pdf.
- [73]一般社団法人JPCERTコーディネーションセンター, “マルウェア Emotet の感

- 染拡大および新たな攻撃手法について,” 一般社団法人JPCERTコーディネーションセンター, 4 9 2020. [オンライン]. Available: <https://www.jpccert.or.jp/newsflash/2020090401.html>.
- [74] L. Mathews, “史上初の身代金ウイルス攻撃による死者、ドイツの病院で発生,” Forbes Japan, 19 9 2020. [オンライン]. Available: <https://forbesjapan.com/articles/detail/37142>.
- [75] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019年度第4四半期,” 26 6 2020. [オンライン]. Available: <https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/062600/062600-01.pdf>.
- [76] 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1四半期,” 11 9 2020. [オンライン]. Available: <https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf>.
- [77] Z. Whittaker, “ランサムウェア攻撃によってGarminのサービスが世界的に停止,” Cech Crunch Japan, 26 7 2020. [オンライン]. Available: <https://jp.techcrunch.com/2020/07/26/2020-07-25-garmin-outage-ransomware-sources/>.
- [78] S. Coble, “Cyber-Attack Downs Alabama County's Network,” infosecurity, 9 7 2020. [オンライン]. Available: <https://www.infosecurity-magazine.com/news/cyberattack-downs-alabama-countys/>.
- [79] P. Muncaster, “Telecom Argentina Has Tuesday Deadline to Pay \$7.5m Ransom,” infosecurity, 21 7 2020. [オンライン]. Available: <https://www.infosecurity-magazine.com/news/telecom-argentina-tuesday-75/>.
- [80] Security Affairs by Pierluigi Paganini, “Spanish state-owned railway infrastructure manager ADIF infected with ransomware,” 24 7 2020. [オンライン]. Available: <https://securityaffairs.co/wordpress/106304/cyber-crime/adif-revil-ransomware-attack.html>.
- [81] Bleeping Computer LLC, “Canon confirms ransomware attack in internal memo,” 6 8 2020. [オンライン]. Available: <https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo/>.
- [82] ニュースガイア株式会社, “テレワーク環境でマルウェア感染、社内に拡大 - 三菱重工,” ニュースガイア株式会社, 11 8 2020. [オンライン]. Available: <http://www.security-next.com/117404>.

- [83] Security Affairs by Pierluigi Paganini, “Sodinokibi ransomware gang stole 1TB of data from Brown-Forman,” 16 8 2020. [オンライン]. Available: <https://securityaffairs.co/wordpress/107190/data-breach/sodinokibi-ransomware-brown-forman.html>.
- [84] ニュースガイア株式会社, “ランサムウェアに感染、障害が発生 - 経済同友会,” ニュースガイア株式会社, 26 8 2020. [オンライン]. Available: <https://www.security-next.com/117841>.
- [85] ニュースガイア株式会社, “マルウェアに感染でなりすましメール - 浄水器販売会社,” ニュースガイア株式会社, 3 9 2020. [オンライン]. Available: <https://www.security-next.com/118027>.
- [86] Z. Whittaker, “サイバー脅威スタートアップのCygilantがランサムウェア「NetWalker」に襲われる、身代金は支払い済みか,” TechCrunch Japan, 5 9 2020. [オンライン]. Available: <https://jp.techcrunch.com/2020/09/05/2020-09-03-cygilant-ransomware/>.
- [87] Bleeping Computer LLC, “Netwalker ransomware hits Pakistan's largest private power utility,” 8 9 2020. [オンライン]. Available: <https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/>.
- [88] Bleeping Computer LLC, “Leading U.S. laser developer IPG Photonics hit with ransomware,” 18 9 2020. [オンライン]. Available: <https://www.bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware/>.
- [89] 株式会社中日新聞社, “危険です、SMS 認証代行 アプリ利用時など不正横行 ツイッターで県警警告,” 株式会社中日新聞社, 6 10 2020. [オンライン]. Available: <https://www.tokyo-np.co.jp/article/59964>.
- [90] BlueVoyant, “Global Insights: Supply Chain Cyber Risk,” 2020.
- [91] 株式会社グローバルインフォメーション, “サイバーセキュリティの市場規模、COVID-19の影響で2020年の年間成長率CAGR1.83%に鈍化 2023年にはV字回復しCAGR11.02%で成長予測,” 株式会社グローバルインフォメーション, 3 8 2020. [オンライン]. Available: <https://www.value-press.com/pressrelease/249866>.
- [92] 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 1 四半期,” 11 9 2020. [オンライン]. Available: <https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/091101/091101-01.pdf>.

- [93] 経済産業省, “サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3) が設立されます (METI/経済産業省),” 経済産業省, 30 10 2020. [オンライン]. Available:
<https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html>.
- [94] Trend Micro Inc., “1H 2020 Cyber Security Defined by Covid-19 Pandemic,” Trend Micro Inc., 15 9 2020. [オンライン]. Available:
https://www.trendmicro.com/en_us/research/20/i/1h-2020-cyber-security-defined-by-covid-19-pandemic.html.
- [95] Trend Micro Inc., “Developing Story: COVID-19 Used in Malicious Campaigns,” Trend Micro Inc., 11 11 2020. [オンライン]. Available:
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains>.
- [96] 株式会社日本経済新聞社, “チャートで見る世界の感染状況,” 株式会社日本経済新聞社, 2020. [オンライン]. Available:
<https://vdata.nikkei.com/newsgraphics/coronavirus-chart-list/>.
- [97] 株式会社NTTデータ, “グローバルセキュリティ動向四半期レポート 2019 年度 第 4 四半期,” 株式会社NTTデータ, 26 6 2020. [オンライン]. Available:
<https://www.nttdata.com/jp/ja/-/media/nttdatajapan/files/news/information/2020/062600/062600-01.pdf>.
-

Published on Friday, December 11, 2020

Security Engineering Department, NTT DATA Corporation
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
Ryo Hoshino / Daisuke Miyazaki / Akihiro Ito / Jun Kinoshita / Takuya Katai / Risa Shishido /
Kazutaka Shimizu / Kantaro Kudo
nttdata-cert@kits.nttdata.co.jp