# Quarterly Report on Global Security Trends

## 3rd Quarter of 2022

# Table of Contents

# 1. Executive Summary

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

## Featured topic, "How to use the ISMAP-LIU system"

On November 1, 2022, the Digital Agency started operating ISMAP-LIU (ISMAP for Low-Impact Use). Compared to ISMAP, ISMAP-LIU is expected to lower costs through reduced cash outflow for external audits required before registration, but since internal audit reporting becomes mandatory, it is necessary for companies to prepare personnel and systems for conducting audits internally.

Government agencies have announced that they will primarily procure cloud services from services registered with ISMAP or ISMAP-LIU when acquiring cloud services, so it is expected that many companies will follow this trend in the future. When considering registration, it is important to consider the advantages and disadvantages, evaluate cost performance, and utilize the system.

## Featured topic, "Passkey support gaining momentum toward a world of passwordless authentication"

In May 2022, Apple, Google, and Microsoft jointly announced that they would provide multi-device compatible FIDO credentials, commonly known as "passkeys," to expand support for passwordless authentication.

Passkey support is expanding on both platforms and service providers, and in the future, users will be able to enjoy not only the improved convenience of using services on multiple devices, which is a feature of passkeys, but also the intended benefits of FIDO authentication, such as phishing resistance and passwordless authentication.

We recommended that companies and other entities collect information now and consider how to position passkey authentication in the authentication of the services they use.

## Data breach, "Learning from the Showcase data breach incident"

On October 25, 2022, Showcase Inc. announced that a third party had gained unauthorized access to several of its services and rewritten the source code, possibly leaking externally information of several companies using the services.

In recent years, e-commerce sites may utilize various external services to implement their services, and a software supply chain attack may cause multiple sites to suffer data breach. It is important for e-commerce sites to monitor external services and consider countermeasures in terms of preventing the spread of damage and avoiding and transferring risks.

## Vulnerability, "Remote code execution vulnerabilities in Microsoft Exchange Server"

We describe a remote code execution vulnerability in Microsoft Exchange Server, known as ProxyNotShell, for which a patch was distributed in November 2022.

The ProxyNotShell attack combines multiple vulnerabilities, and in the past, serious vulnerabilities such as ProxyLogon and ProxyShell were also discovered in similar attacks where multiple vulnerabilities were chained together.

It is necessary to continuously collect vulnerability information not only to reduce risks by reviewing Exchange Server configurations and settings and implementing other security systems, but also to apply patches to permanently address each vulnerability.

# 2. Featured topic, "How to use the ISMAP-LIU system"

On November 1, 2022, the Digital Agency started operating ISMAP-LIU (ISMAP for Low-Impact Use) [1]. ISMAP-LIU is a system within the framework of the Information system Security Management and Assessment Program (ISMAP) that targets SaaS services for processing low-risk operations and information.

Government agencies have also announced that they will primarily procure cloud services from services registered with ISMAP or ISMAP-LIU when acquiring cloud services. As services registered with ISMAP or ISMAP-LIU clearly meet the certain security level required by government agencies, it is expected that this trend will be followed not only in the public sector but also by many companies. Registration with ISMAP and ISMAP-LIU will play an important role in doing business with cloud products.

This article explains the contents and structure of ISMAP-LIU and its differences from ISMAP from the perspective of company personnel who handle SaaS products. We hope that this article will deepen your understanding of the ISMAP-LIU system and help you decide whether you should obtain ISMAP or ISMAP-LIU registration.

## 2.1. Overview of ISMAP-LIU

ISMAP-LIU is a new system that began operation on November 1, 2022. As mentioned above, ISMAP-LIU is a system within the ISMAP framework that targets SaaS services for processing low-risk operations and information.

ISMAP-LIU was created due to concerns that ISMAP's security requirements may be excessive for some services. Information systems that handle level 2 confidential information, which are subject to ISMAP, range from IaaS, PaaS, to SaaS. Among them, SaaS has a wide range of services, some of which are low-risk, such as services with extremely limited applications and functions, and services that only handle information of relatively low importance among level 2 confidential information. If all these services were treated uniformly under ISMAP, it would create excessive security requirements and hamper the utilization of these services.

Against this background, a system was established for SaaS services that handle level 2 confidential information and are used to process operations and information with low security risk. This system is ISMAP-LIU. [2]

*ISMAP (Information system Security Management and Assessment Program) is a security assessment system for government information systems.

*ISMAP aims to ensure the security level in government cloud service procurement by evaluating and registering cloud services that meet the government's security requirements in advance, thereby facilitating the smooth introduction of cloud services.

## 2.2. Details of the ISMAP and ISMAP-LIU systems

As explained in 2.1, ISMAP is closely related to the establishment of the ISMAP-LIU. In this section, we will provide the details of the ISMAP and ISMAP-LIU systems.

### 2.2.1. Details of the ISMAP system [3]

(1) Purpose of introducing the system

The purpose of the ISMAP system is to provide clear, unified security standards for cloud services and to establish an effective and efficient cloud security assessment system, so that a certain level of security can be ensured.

(2) Target

Cloud services in general

(3) Registration procedures

Internal audit → External audit → Application for registration → Service registration

*Internal audits are not required to be reported.

### 2.2.2. Details of the ISMAP-LIU system [2]

(1) Purpose of introducing the system

The purpose of this system is to create a security assessment system specific to SaaS, since the uniform treatment of SaaS under the existing ISMAP may result in excessive security requirements, thereby ensuring a certain level of security.

(2) Target

The system targets SaaS that handles operations and information with low security risks among level 2 confidential information.

A target operation list containing information of operations that ISMAP-LIU is designed for has been released by the Digital Agency. SaaS systems providing operations as released may be eligible for ISMAP-LIU. The following table provides eligible operations and their system examples.

Table 2-1: Operations eligible for ISMAP-LIU and system examples

| No. | Operations | System examples |
|---|---|---|
| 1 | Operations in cooperation with the private sector in the planning and coordination process of policies and systems intended to be made public<br>(For operating meetings through web conferencing and storing, managing, and sharing information through file sharing in order to operate council meetings, etc., with experts invited) | Web conference service<br>File sharing service |
| 2 | Operations that handle information on the titles and names of government employees in the course of their duties (For personnel management and talent management of government employees by using their title and name information)<br>*Except in cases where the nature of the operations requires strict confidentiality of the information of employees engaged in the operations | Human resource management service<br>Talent management service |
| 3 | Operations that handle information within the scope of information provided to the public at large, such as business card information, and information for managing distribution destinations, etc. associated with the distribution of public information<br>(For registration and management of business card information such as company, title, name, etc., and for registration and management of | Business card management service<br>Video and content distribution service |

| | | |
|---|---|---|
| | information for the purpose of identifying distribution destinations in connection with distribution of images, contents, etc., to customers such as government agencies, etc.) | |
| 4 | Operations that process information that is provided by the private sector and that is deemed low-risk by the relevant information provider (For storing and managing information provided by the relevant information provider by using SaaS for web conferencing and file sharing used by private companies and private organizations) | Web conference service<br>File sharing service |
| 5 | Cases in which the operations handle open source, publicly known facts, and publicly available information that still needs to be treated as confidential on an exceptional basis (For handling information that is scheduled to be made public, such as pre-publication information on a website, and for which a decision has been made to make the information public; and for translating and researching policy information, technical information, etc. of other countries using machine translation (in cases where research trends for specific government information are classified as confidential)) | Public information management service |
| 6 | Operations to confirm any damage to members of the organization in the event of a disaster, etc. | Safety confirmation service |
| 7 | Operations to educate members of the organization on organizational rules, business skills, etc. | Employee education service |
| 8 | Operations to handle routine and daily business correspondence, etc., among those falling under the retention period of less than one year in the "Guidelines for the Management of Administrative Documents"<br>(Routine and daily business correspondence, itineraries, etc. / documents compiled from publications and public announcements / responses to factual inquiries concerning affairs under the jurisdiction of the Ministry of XX / documents created in the process of decision-making that have an extremely small impact on the decision-making concerned) | Help desk automated response service<br>Business communication service |

(3) Registration procedures

Impact assessment conducted by user ministries and agencies → Pre-application → Approval that the SaaS is eligible for LIU → Internal audit → External audit → Formal application → Service registration

## 2.3. Notable differences between ISMAP and ISMAP-LIU

### 2.3.1. Differences in reporting items for external audits

External audit items defined by ISMAP include 18 items for governance criteria, 64 items for management criteria, and 1,074 items for controls criteria (due to the selective nature of the audit, there may be differences from the actual number of items audited). [3]

Meanwhile, ISMAP-LIU has the same number of items for governance and management criteria, with 18 items for governance criteria and 64 items for management criteria, but the number of items for controls criteria is approximately 148 questions*, less than 1/5 of the number of items for ISMAP's controls criteria. [2] [4]*For other controls criteria that are not required, items should be selected as necessary according to the organization, environment, technology, etc. in the service that is the subject of the statement.

In the external audit of ISMAP-LIU, the governance and management criteria follow ISMAP and cover all audit items, whereas the controls criteria mainly cover controls that can have a direct impact on the service infrastructure and configuration (some important controls), reducing the scope of the external audit.

This is expected to reduce the cash outflow for external audits and reduce the burden on SaaS service providers.

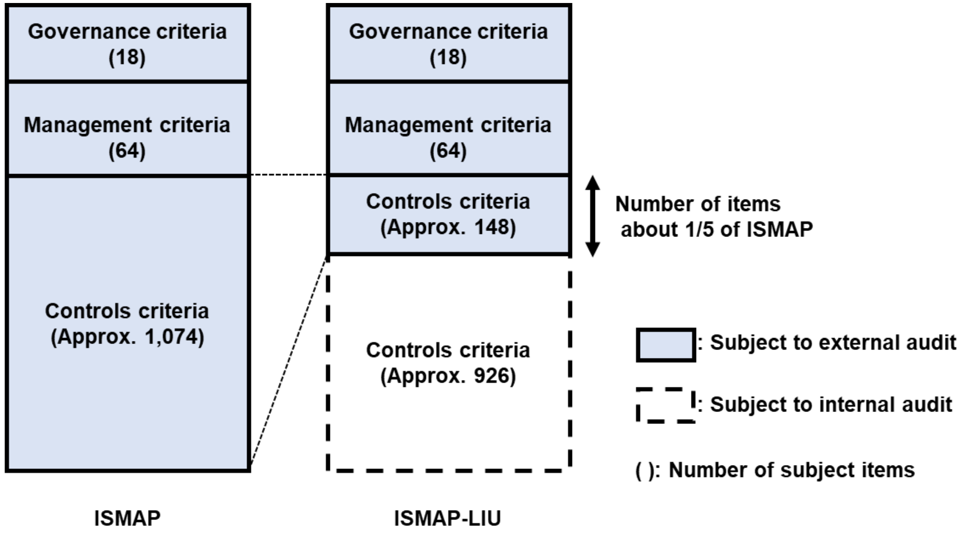

Governance criteria (18)
Management criteria (64)
Controls criteria (Approx. 1,074)
ISMAP
Governance criteria (18)
Management criteria (64)
Controls criteria (Approx. 148)
Controls criteria (Approx. 926)
ISMAP-LIU
Number of items about 1/5 of ISMAP
: Subject to external audit
: Subject to internal audit
( ): Number of subject items

Fig. 2-1: Comparison of the number of items subject to external audit

## 2.3.2. Reporting obligations for internal audits

In 2.3.1, it is noted that the number of external audit items in ISMAP-LIU is much smaller than in ISMAP. However, for items excluded from the scope of external audits in ISMAP-LIU, it is necessary to report them through internal audits. As described in 1.2.1(3), ISMAP also requires internal audits to be conducted, but since all items are externally audited and reported, there was no requirement for internal audit reporting.

ISMAP-LIU's internal audit requires that all control objectives in the controls criteria (excluding control objectives that are excluded in the statement) have been the subject of an internal audit at least once in the last three years. [2]

While there are some exceptions, ISMAP-LIU requires external audits of three-digit controls (items up to the third level, such as A, B, and C), which are control objectives in the controls criteria, and internal audits of four-digit controls (items at the fourth level, such as A, B, C, and D), which are detailed controls that provide means to achieve the control objectives. [2] [4]

Example:

[Subject to external audit] 8.1.2 Assets maintained in the catalog shall be controlled.

[Subject to internal audit] 8.1.2.1
In the process of ensuring the assignment of asset management responsibility without delay, assign management responsibility to eligible persons (individuals and organizations given management responsibility for the asset lifecycle) when the asset was generated or transferred to the organization.

[Subject to internal audit] 8.1.2.2 The person responsible for the management of the asset shall be responsible for managing the asset appropriately throughout the asset lifecycle.

Since there is no specific area that can only be audited by internal audits, even SaaS services that handle low-security-risk operations and information among level 2 confidential information (i.e., systems eligible for ISMAP-LIU) must go through an external audit for the items whose security levels need to be checked once a year, and an internal audit for the detailed security items once every three years. In ISMAP-LIU, it is possible to reduce the running costs of the overall audit by extending the inspection period of internal audits. However, extending the audit cycle can also lead to a delay in problem discovery, so it is important to set an appropriate period based on business risk considerations.

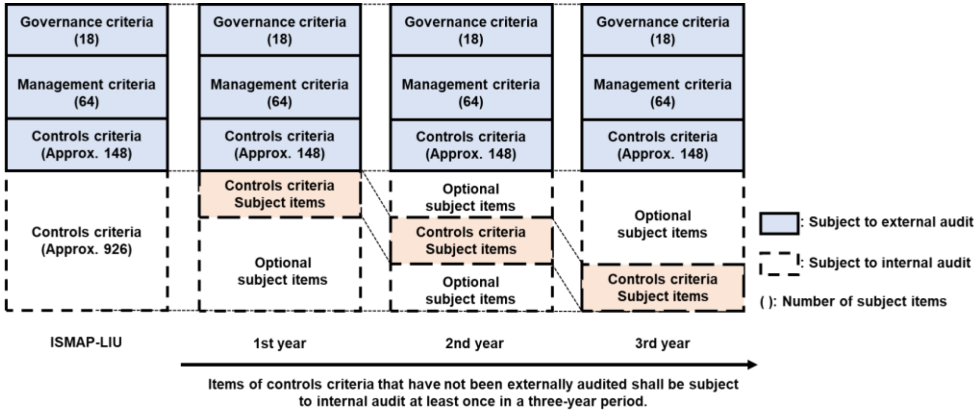

Governance criteria (18)
Management criteria (64)
Controls criteria (Approx. 148)
Controls criteria (Approx. 926)
Controls criteria Subject items
Optional subject items
: Subject to external audit
: Subject to internal audit
( ): Number of subject items
ISMAP-LIU
1st year
2nd year
3rd year
Items of controls criteria that have not been externally audited shall be subject to internal audit at least once in a three-year period.

Fig. 2-2: Items subject to annual internal audit

### 2.3.3. Cancellation and publication system

The process of cancellation and publication in ISMAP-LIU basically follows the process of re-audit and re-application in ISMAP. However, in ISMAP-LIU, when an incident occurs that could have a particularly serious impact, the ISMAP-LIU system operator will immediately suspend the registration of the service in question. [2]

Specific criteria for suspension have not been disclosed, but the addition of the suspension makes it impossible to procure during the suspension.

## 2.4. Conclusion

As mentioned in the introduction, registration with ISMAP and ISMAP-LIU enables system procurement by public agencies. Registration with ISMAP and ISMAP-LIU is expected to play an important role in the business of cloud service providers because it will help them promote the reliability of their cloud services.

Since ISMAP imposes high standards and many items for external audits, a large cost was incurred due to cash outflow for external audits before registration. Although eligible SaaS services are limited, the cash outflow for this external audit is expected to be reduced now that the ISMAP-LIU is in operation. In addition, since items that are excluded from external audits are replaced with internal audits once every three years, it is now possible to register while keeping the running costs of audits low.

However, there are some points that require attention in ISMAP-LIU, such as the need to prepare personnel and systems capable of conducting audits within the company since ISMAP-LIU requires internal audit reporting with higher accuracy, and the fact that procurement will not be possible during the suspension of registration.

It is important to consider the advantages and disadvantages, evaluate cost performance, and utilize the system.

# 3. Featured topic, "Passkey support gaining momentum toward a world of passwordless authentication"

In May 2022, Apple, Google, and Microsoft jointly announced that they would provide multi-device compatible FIDO credentials, commonly known as passkeys, to expand support for passwordless authentication [5]. At that time, it was expected to be available on each company's platform by the end of 2023, but the implementation has already begun in FY2022 Q3.

We will introduce the passkey, what is expected of it, and what will improve compared to the current situation, as well as future trends.

## 3.1. Challenges in popularizing FIDO authentication

Currently, the most commonly used authentication method, password authentication, has been plagued by various attacks such as password guessing, exploitation of leaked passwords, and phishing, and there have been many cases of damage in recent years.

FIDO (Fast Identify Online), an international standard, is an authentication method that aims to move away from such problematic password authentication toward a passwordless world [6].

FIDO is based on public key cryptography. Specifically, a key pair is created on the user's device for each service domain, with the private key stored in a secure area on the device, and the public key transmitted to the service provider's authentication server for registration [7]. Authentication is achieved through multi-factor authentication by a combination of device possession and identity confirmation based on the user's biometrics/knowledge. If the identity confirmation result is successful, the challenge sent from the server is signed with the private key and sent to the server, where it is verified with the user's public key to complete authentication.

This system overcomes the problems associated with password authentication. There is no way to guess the private key in the device, and even if the public key is compromised on the service side, the challenge cannot be signed, so authentication information cannot be generated illegally. In addition, keys are managed for each domain name of the service, so authentication information cannot be sent to phishing sites.

However, as of December 2022, it is difficult to say that this system has been widely adopted by many services. The main reason is that FIDO key registration is required for each device. For example, if a device is lost or replaced, users have to re-register their keys for each service, and service providers need to prepare means other than FIDO authentication for account recovery in case of loss, which can be cumbersome. There is also a method of registering multiple devices in advance to prepare for the loss of the authentication method, but this would require registering each service on each device, leading to a loss of usability for the user.

## 3.2. Resolving issues with passkeys

To resolve these issues with FIDO, the introduction of passkey was announced in March 2022 [8].

Passkeys are characterized by the fact that keys are backed up in the cloud tied to a platform vendor's account. Through this system, when a device is changed due to a model change or loss, or when multiple devices are used, keys are synchronized to the new device by logging into the platform vendor's account. This eliminates the need to re-register for the service when a device is changed or lost, which has been a problem with traditional FIDO. It also reduces the need to retain password authentication with low authentication strength for account recovery.

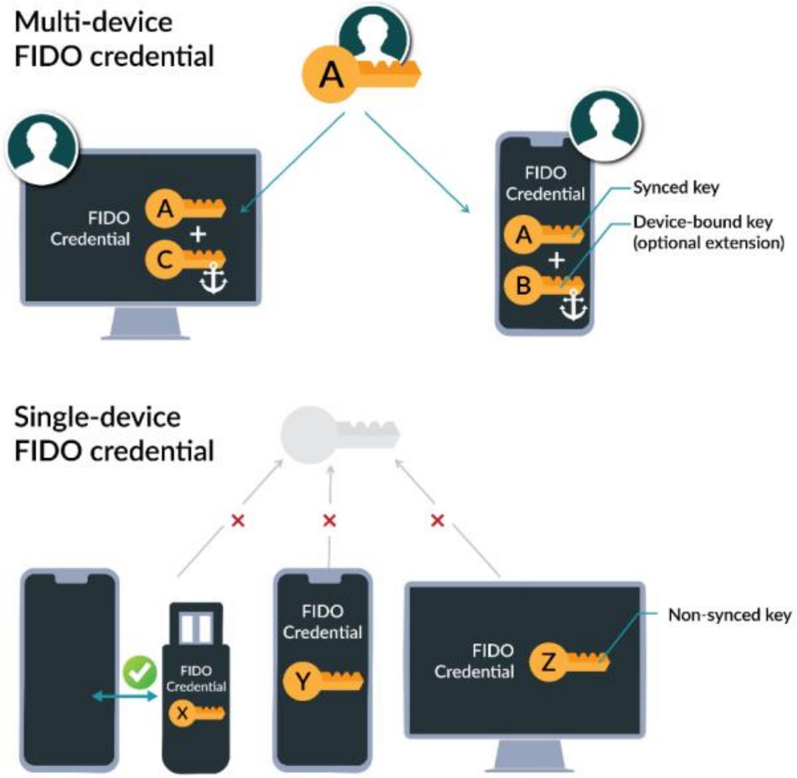


Fig. 3-1: Comparison of multi-device FIDO credentials and traditional FIDO [9]

On the other hand, with the introduction of a passkey, there is no longer a link between the device and the FIDO key, which was the premise of the previous FIDO. Therefore, an option is provided to create a key pair linked to the device so that when using a passkey on multiple devices, it is possible to identify which device the passkey came from. The private key of this device-linked key pair is securely stored on the device, cannot be extracted, and unlike a passkey, is not linked to or synchronized with the platform vendor's account.

To increase the number of cases where a passkey is used, a hybrid method is also available [10], where a passkey from another device can be used to log in. Using the hybrid method, passkeys can be used on different platforms (Apple, Google, Microsoft, etc.). To establish a connection with another device, a QR code and Bluetooth Low Energy (BLE) are used. First, display the QR code on the original device and then read it on the device with the passkey. Then, a path is created on the BLE for the authentication exchange. At this time, Bluetooth pairing is not necessary. The use of BLE enhances security by ensuring that both devices are in close proximity and that the same user is in possession of both devices.

## 3.3. Passkey implementation gaining momentum from October 2022

### 3.3.1. Status of support by major platforms in FY2022 Q3

The platform vendors that made progress in passkey support in FY2022 Q3 are Apple and Google. The status of each is as follows.

(1) Apple

Apple took the lead in platform support. Passkey support started with iOS 16, which was released on September 13th, just before FY2022 Q3, followed by macOS Ventura on October 24th, and iPadOS 16.1 on October 25th [11] [12] [13]. At the same time, support for browsers began with Safari 16.

Passkeys created on Apple-based platforms are stored in iCloud Keychain. This allows passkeys to be used across iOS/iPadOS/macOS that are logged in with the same Apple ID.

(2) Google

Google also started supporting passkeys for Android 9.0 and above over the latter half of FY2022 Q3 after releasing a beta version on October 12 [14]. In addition, Google Chrome also began supporting passkeys on Android/Windows11/macOS starting with Google Chrome 108 [15].

In Android, the passkey is saved in the Google Password Manager associated with the user's Google account. Therefore, it can be used across Android OS-enabled devices.

### 3.3.2. Status of cross-platform support

As shown in the examples of Apple and Google, passkey usage across devices within the same platform is progressing. While Windows does not yet support passkeys, support is expected in the future.

At present, cross-platform support has not yet begun in earnest. The only case in point is passkey sharing on iOS/iPadOS/macOS. Otherwise, a hybrid approach is the only option. This, however, requires caution, as the passkey is not shared in some cases, even if the same browser is used, but on different platforms. As an example, Google's Chrome is available on each platform, but the range of passkey sharing depends on the platform vendor account where the passkey is stored [16].

## 3.4. Assumed passkey trends for 2023

Passkey support was expanded in FY2022 Q3, but how will it continue to expand in 2023 and beyond?

On the platform side, Microsoft plans to support passkeys on Windows. If support starts as planned, passkeys will be available on all major platforms, including Android, iOS/iPad/macOS, and Windows.

As for cross-platform passkey use, password manager vendors such as 1Password and LastPass have also announced passkey support [17] [18]. This would be very beneficial, as it would allow passkeys to be used across platforms that support the same password manager. However, there have been incidents and hacking damage with LastPass [19]. If the cloud, where administrative accounts and passkeys are backed up, is damaged, significant impact can be expected. Therefore, the choice of platform accounts and password managers used to back up passkeys should be made carefully.

Service providers are expected to gradually begin support in 2023. Some services have already started or are planning to support it, such as Yahoo Japan's Yahoo! JAPAN ID and NTT DOCOMO's d account. It is expected that the introduction will start with ID providers and communication carriers like these, and spread to various services [20] [21].

To promote passkey support among service providers, it is expected that platforms will provide libraries to facilitate implementation, such as Credential Manager provided by Google for Android app developers [22]. However, to actually implement passkeys, it is necessary to decide how passkeys should be positioned within the authentication of your service. This decision will also be influenced by platform support, so it is likely that service providers will start using passkeys in earnest only after passkey support is provided on Windows.

## 3.5. Conclusion

Regarding the introduction of passkeys, platform support has just begun in the second half of 2022, and the specifications are still undefined, including those of device linkage, which is optional, as mentioned in 3.1.2. However, the remaining major platform, Windows, has been expressing support for passkeys from the beginning, and there is no doubt that the scope of use will expand. As these issues are resolved, the environment for passkey introduction is expected to become more favorable. As a result, users will be able to enjoy not only the improved convenience of using services on multiple devices, which is a feature of passkeys, but also the intended benefits of FIDO authentication, such as phishing resistance and passwordless authentication.

As a service provider, it may not be possible to immediately abandon password authentication for the entire service, but there are benefits such as providing a phishing-resistant authentication method for users who choose the passkey method. Therefore, we recommend that company personnel gather information and develop a plan for implementation. In planning, please consider how passkey authentication should be positioned in the authentication of services.

# 4. Data breach, "Learning from the Showcase data breach incident"

On October 25, 2022, Showcase Inc. announced that a third party had gained unauthorized access to several of its services and rewritten the source code, possibly leaking externally information of several companies using the services [23]. Subsequently, 12 companies that had been using the company's services announced one after another the details of the data breach and the extent of the damage. Given the characteristics of Showcase's services, it is presumed that they were mainly used on e-commerce sites. Therefore, this article explains the points that e-commerce site operators should consider when incorporating tools that process data on the service provider's server, such as Showcase's entry form optimization tool, into their own e-commerce sites.

## 4.1. Overview of the Showcase data breach incident

According to Showcase, there are three services that the attacker gained unauthorized access to and rewrote the source code for: "Form Assist," "Site Personalizer," and "Smartphone Converter." When companies use Showcase's services, they embed the JavaScript provided by the company into their website pages. "Form Assist," "Site Personalizer," and "Smartphone Converter" provide assistance for entering data into website forms, support for individual marketing, and optimization of website display, respectively. (Fig. 4-1)

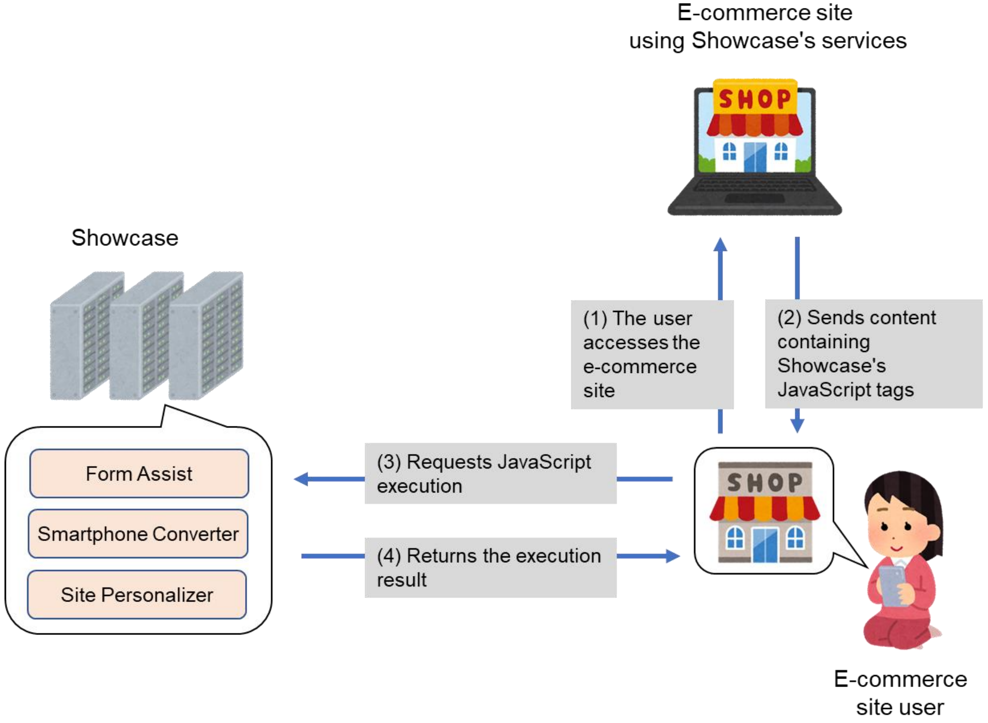

E-commerce site
using Showcase's services
Showcase
Form Assist
Smartphone Converter
Site Personalizer
(1) The user accesses the e-commerce site
(2) Sends content containing Showcase's JavaScript tags
(3) Requests JavaScript execution
(4) Returns the execution result
SHOP
E-commerce site user

Fig. 4-1: Service mechanism

Based on this mechanism, the attacker is believed to have stolen information in the steps shown in Fig. 4-2.

(1) The attacker exploits a vulnerability in the server that provides Showcase's "Form Assist," "Site Personalizer," and "Smartphone

Converter" to gain unauthorized access. The attacker tampers with the JavaScript of "Form Assist," "Site Personalizer," and "Smartphone Converter" on the said server.

(2) A user accesses an e-commerce site that uses Showcase's services.

(3) The e-commerce site sends content containing Showcase's JavaScript tags to the user's browser.

(4) The browser requests Showcase to execute the JavaScript.

(5) Showcase's server returns the results of the JavaScript execution to the browser.

(6) The browser displays the results of the Showcase server's processing. When the user enters information into the zip code field to purchase a product, for example, the Form Assist function converts the zip code to an address and displays it on the form for address entry. At this point, legitimate JavaScript would return the address converted from the zip code, but the attacker's tampered JavaScript had an additional process that would send the entered personal information to an external party.

(7) The personal information entered is sent to the attacker's server.

In this way, after the user's browser displays the contents of the e-commerce site, Showcase's JavaScript is executed on Showcase's server to provide the services. Therefore, it is difficult for the e-commerce site operator to notice that the JavaScript has been tampered with because no information about the JavaScript execution or communication to the attacker's server is left in the e-commerce site's logs. The information leaked this way was information related to credit cards, including credit card numbers, expiration dates, and security codes, according to the user companies' public disclosure.

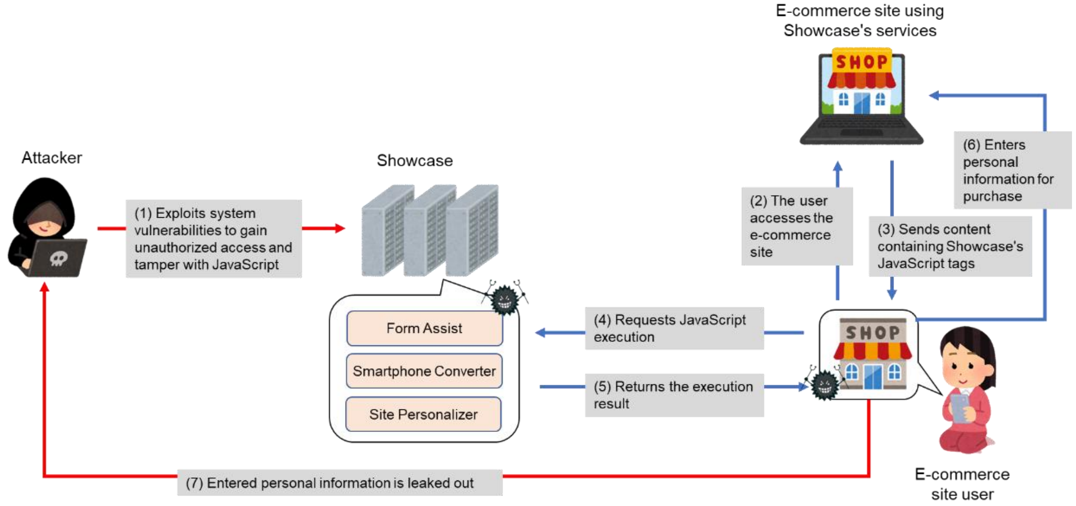

E-commerce site using Showcase's services
SHOP
Attacker
Showcase
(6) Enters personal information for purchase
(2) The user accesses the e-commerce site
(1) Exploits system vulnerabilities to gain unauthorized access and tamper with JavaScript
(3) Sends content containing Showcase's JavaScript tags
Form Assist
Smartphone Converter
Site Personalizer
(4) Requests JavaScript execution
(5) Returns the execution result
SHOP
(7) Entered personal information is leaked out
E-commerce site user

Fig. 4-2: Attacking steps

# 4.2. Consideration of this incident

## 4.2.1. Consideration of the cause of the cyberattack

This incident was a cyberattack in which the source code of an external service used by e-commerce sites was altered to efficiently steal credit card information from multiple e-commerce sites. This can be considered an attack that cleverly exploits the potential risks in the software supply chain of e-commerce sites.

A software supply chain attack is a technique of distributing software containing malware or attack code through the software's supply chain, such as the software's developer and distributor, to use it as a foothold for an attack. In the attack on Showcase, the attacker gained unauthorized access to a server of Showcase, a software developer, and tampered with the JavaScript on the server. Since the e-commerce site operator only adds the JavaScript tags from

Showcase's server to the HTML, we believe that no one was monitoring Showcase's JavaScript for any changes. Even if the e-commerce site operator did monitor the JavaScript, it would be difficult to determine if the changes were legitimate changes by the service provider or tampering by an attacker.

Meanwhile, from the perspective of Showcase, the service provider, the service whose source code was rewritten to allow the attacker to steal information, was not intended to be used for payment processing such as credit card transactions. Therefore, we suspect that the cyberattack was successful because the security measures and monitoring system of the server executing the JavaScript did not meet the strict security standards for payment services, etc.

### 4.2.2. Consideration of the resumption of credit card transactions

While some e-commerce sites announced their own damage and resumed credit card transactions immediately after Showcase announced the damage, others announced their damage much later or resumed credit card transactions several months after the damage was announced by Showcase. What caused the difference in response time among the e-commerce sites? The affected e-commerce sites added Showcase's JavaScript tags to the HTML of their web pages in order to optimize the display and support form input, etc. We suspect that by temporarily removing the JavaScript tags from the e-commerce sites, they could have stopped data breaches from the tool without having to make major changes to the design of the e-commerce sites themselves. The reason for the delay in reopening of some e-commerce sites, despite the fact that the modification only involved the deletion of the JavaScript tags in question, is that there is a risk of customer churn if the causes and countermeasures are not properly explained to the satisfaction of the users, and therefore it may have taken time to prepare an explanation of the causes of the data breach, support in case of damage, measures to prevent recurrence, etc. Responding to a data breach incident such as this one is different from simply updating the contents of an e-commerce site. It took a long time for some e-commerce sites to make announcements and reopen the sites, and we suspect this is because there were no personnel available to respond to data breach incidents, so they had to consult with a company specializing in information security quickly and establish a response system.

### 4.2.3. Consideration of the service provider's compensation

There are cases where an e-commerce site that uses Showcase's service claims compensation from the service provider Showcase for damages such as costs associated with data breach handling, system modifications, lost opportunities, etc. In this incident, it is not clear how much compensation Showcase paid to the e-commerce site operators, but in general, the amount of compensation paid for damage caused by failures or security incidents in SaaS services is not very high. According to the "ASP Service Model Terms of Use" [24] stipulated by the Japan Information Technology Services Industry Association (JISA), the upper limit is "actual ordinary damages" and "one month's average monthly fee for the past 12 months," and "damages arising from special circumstances and lost profits" are exempted. Service providers may include such a statement in their terms and conditions as part of their efforts to prevent large amounts of compensation. This is because if a security incident is deemed to be a special circumstance, there is a possibility that the compensation amount will not be high. In such a case, e-commerce sites have no means to compensate for the damages.

## 4.3. Points for e-commerce site operators to consider

Showcase's data breach incident was caused by tampering with source code managed by the service provider, so e-commerce site operators have no means to prevent the incident beforehand. One possible countermeasure is to develop an equivalent service in-house, but this is only possible for a few large-scale e-commerce sites that can secure the necessary personnel and bear the manufacturing costs. Then, what should other e-commerce sites consider?

### 4.3.1. Understanding the software supply chain

Given the possibility of such incidents, the first thing to consider is understanding the software supply chain.

Investigate whether your company's e-commerce site uses external services, and if so, clearly identify what functions are incorporated into which web pages and in what format. Anticipate what the impact would be in advance, should a problem occur with an external service. Ideally, you should list the cases of problems that may occur with external services and organize each case in detail. The more detailed the consideration, the more quickly a series of responses can be taken, including investigation of the cause, provisional measures, and restoration decisions, should an incident occur. Even if that is difficult, simply having an overview of the impact on the e-commerce site, such as the status of use of external services, whether the e-commerce site itself will be shut down when the external services used are shut down, or whether sales can continue as is, may contribute to shortening response time in the event of an emergency.

Note that e-commerce sites that retain credit card numbers are required to comply with 6.3.2 of PCI DSS Version 4.0 [25] which requires maintaining an inventory of bespoke and custom software.

### 4.3.2. Selection of a consultation partner for incident response and countermeasures

While it would be ideal for e-commerce operators to be able to handle incidents and take both provisional and full countermeasures by themselves, most of them are not able to do so. If this is the case, it is advisable to decide in advance on a company specializing in information security to consult with or request a response from in the event of an incident. Useful references include the "Information Security Service Standards Conforming Service List" [26] compiled by IPA, which includes services that have been recognized as compliant with the information security service standards established by the Ministry of Economy, Trade and Industry, and the "List of Companies for Emergency Response to Cyber Incidents" [27] by JNSA. It is a good idea to consider who to consult based on this information.

### 4.3.3. Use of cyber insurance

If there is a problem with an external service as a result of understanding the software supply chain, the e-commerce site operator may not be able to prevent information security incidents that occur on the external service. In addition, as discussed in 4.2.3, even if a dispute is made with the service provider regarding compensation for damages, compensation may be limited to a small amount based on the terms and conditions. A possible follow-up action would be to introduce another service, but this too is likely to be costly and time-consuming. In such a case, a way to transfer the risk of damage or loss incurred is to purchase cyber insurance. Cyber insurance generally covers not only damages to victims and litigation costs, but also investigations into the cause of incidents, establishment of inquiry call centers, lost profits, etc., so it serves as preparation in case an incident occurs. According to the General Insurance Association of Japan, cyber insurance is provided by eight companies [28], and there are insurance plans that provide support for incident prevention and response, such as simple risk diagnosis and emergency support in the event of an incident, as ancillary services. By comparing multiple insurance plans and purchasing the appropriate plan that matches the size of your system and business and provides the coverage you need, you can reduce your losses.

## 4.4. Conclusion

This article provided the overview of a credit card data breach incident caused by tampering with the services provided by Showcase, and discussed the causes of the cyberattack, resumption of credit card payments, and compensation from the service provider. As preparation in case such an incident occurs, we explained three points that e-commerce site operators should consider: understanding the software supply chain, selecting a company specializing in information security to consult with or request a response from, and cyber insurance. By considering these points in advance, you should be prepared to respond quickly and minimize damage in the event of a problem.

# 5. Vulnerability, "Remote code execution vulnerabilities in Microsoft Exchange Server"

## 5.1. Remote code execution vulnerabilities in Microsoft Exchange Server

This article describes a remote code execution vulnerability in Microsoft Exchange Server ("Exchange Server"), known as ProxyNotShell, for which a patch was distributed in November 2022. "ProxyNotShell" is the generic term used to refer to vulnerabilities CVE-2022-41040 and CVE-2022-41082, which can be exploited in sequence to enable remote code execution.

### 5.1.1. Timeline

The events leading up to the release of a patch by Microsoft for the vulnerability ProxyNotShell are listed in chronological order in Table 5-1.

On September 28, 2022, GTSC, a Vietnamese security firm, announced on its blog that an Exchange Server monitored by the firm had been attacked using a new vulnerability [29]. Microsoft announced the vulnerability and mitigation measures on September 30 of the same year, but it took more than a month to provide a patch for this issue.

Table 5-1: Timeline from ProxyNotShell discovery to patch release

| Date | Event |
|---|---|
| August 2022 | An attacker attacks a system monitored by GTSC. |
| September 28, 2022 | GTSC announces this vulnerability on its blog. [29] |
| September 30, 2022 | Microsoft announces the vulnerability and provides guidance on mitigation measures. [30] |
| Early October 2022 | Release of signatures for IDS/IPS and WAF by various security vendors |
| October 11, 2022 | Monthly security update for October is released.<br>(Not including a patch for this vulnerability) |
| November 8, 2022 | Monthly security update for November is released. [31]<br>(Including a patch for this vulnerability) |

### 5.1.2. Vulnerability details

(1) Attack target

The versions affected by this vulnerability are Exchange Server 2013/2016/2019 (Exchange Online is not affected).

(2) Vulnerability overview

By exploiting a combination of the two vulnerabilities shown in Table 5-2, attackers can execute remote code on Exchange Server.

Table 5-2: Vulnerability overview

| CVE no. | Details | CVSS score |
|---|---|---|
| CVE-2022-41040 | Vulnerability allowing to reach the PowerShell backend of Exchange Server by SSRF (Server Side Request Forgery) | 8.8 |
| CVE-2022-41082 | Vulnerability allowing remote code execution in Exchange Server | 8.8 |

(3) Attacking steps

The steps of the attack that exploits the vulnerability ProxyNotShell have been analyzed in detail by Mr. Piotr Bazydło at the Zero Day Initiative using PoC [32]. As shown in Fig. 5-1, the attack uses two vulnerabilities in sequence.

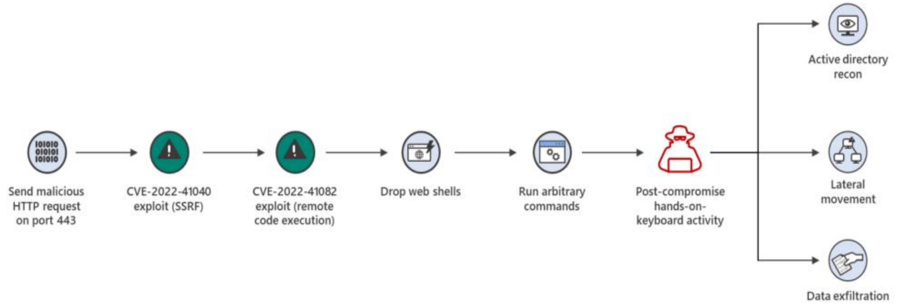

Send malicious HTTP request on port 443
CVE-2022-41040 exploit (SSRF)
CVE-2022-41082 exploit (remote code execution)
Drop web shells
Run arbitrary commands
Post-compromise hands-on-keyboard activity
Active directory recon
Lateral movement
Data exfiltration

Fig. 5-1: Diagram of ProxyNotShell attack [33]

Step 1 (CVE-2022-41040):

Exchange Server provides the Autodiscover service that allows clients such as Outlook to automatically set up configuration information. The Autodiscover service is a service that runs on the Internet Information Service (IIS), and an attack can be carried out using a vulnerability that allows access to Exchange Server's PowerShell backend through an SSRF attack that sends requests for exploitation to the Autodiscover service.

While authenticated access is required to perform an attack using this vulnerability, the attacker does not need to be a privileged user, but can use a general user account. The credentials (ID/password) could be obtained through phishing attacks or in the underground market.

Step 2 (CVE-2022-41082):

The attack is carried out by serializing the attack object using the remote protocol in PowerShell, which was made reachable in Step 1, and loading it onto the payload. Normally, PowerShell's deserialization process verifies the attack object and prevents it from being instantiated, but there is a problem with some serialization processes that allow an attacker to instantiate any object. Verification by Mr. Piotr Bazydło has succeeded in remote code execution by using the XamlReader object [32]. It is also suggested that there are other objects that can be exploited in addition to the XamlReader object.

After going through these two steps, an attacker who successfully carried out the attack can perform lateral movement and steal data by, for example, deploying a web shell. According to the report by GTSC, the open-source website management tool, AntSword, and the included web shells were found to be deployed [29].

## 5.2. Countermeasures

Based on the attacking steps discussed in the previous section, we will examine countermeasures against the vulnerability ProxyNotShell in chronological order according to the timeline in 5.1.1.

### 5.2.1. Before the vulnerability was made public

At this stage, it was difficult to detect and prevent the attack itself, but it may have been possible to prevent or detect it through design or security systems.

■ Configuration and settings that make it difficult to attack

If Exchange Server had been configured or set up in a way that would have prevented the vulnerability, the attack could have been prevented. The risk of attack could have been reduced by reducing the number of targets exposed to an attack in advance, for example, by:

- ➢ configuring the Exchange Server to not expose it directly to the outside world, such as through the use of a VPN (countermeasure to CVE-2022-41040), or
- ➢ limiting users with PowerShell execution privileges to administrators, etc. (countermeasure against CVE-2022-41082).

■ Detection of post-intrusion actions

After successfully infiltrating through a vulnerability, attackers will take actions such as deploying web shells and rewriting system files for the next attack. If these actions had been detected by configuration management tools or anti-malware software, the damage could have been minimized.

### 5.2.2. From vulnerability announcement to patch release

Along with the vulnerability announcement, Microsoft provided guidance on mitigation measures for the period until the release of a patch.

Security vendors also released updates for their security products such as IDS (Intrusion Detection System)/IPS (Intrusion Prevention System) and WAF (Web Application Firewall) within a few days of Microsoft's announcement (Table 5-3). By applying these updates, attacks could have been detected or prevented until Microsoft released the patch.

Some IDS/IPS and WAF signatures can be applied automatically. Similarly, the use of Microsoft's EEMS (Exchange Emergency Mitigation Service), included in the CU (Cumulative Update) from September 2021 onward, will automatically apply the mitigation measures. Therefore, EEMS is useful when vulnerability information cannot be collected frequently.

Table 5-3: Examples of security vendor responses

| Vendor | Information release date | Updated products/services |
|---|---|---|
| Fortinet | September 30, 2022 [34] | FortiWeb<br>FortiGate, etc. |
| Trend Micro | September 30, 2022 [35] | Cloud One<br>Deep Discovery Inspector |
| Imperva | September 30, 2022 [36] | Cloud WAF<br>WAF Gateway |
| Akamai | October 3, 2022 [37] | Kona Defender<br>App&API Protector |
| F5 | October 3, 2022 [38] | ASM<br>Advaced WAF |

### 5.2.3. After the release of the patch

On November 8, 2022, a monthly security update (KB5019758) containing a patch for this vulnerability was released [31]. The application of the patch completes the permanent fix for this vulnerability.

### 5.2.4. Possibility of intrusion

It is necessary to consider the possibility that an attacker has already gained entry through an attack that exploits this vulnerability before implementing any of the countermeasures described in 5.2.1 through 5.2.3

Before taking any countermeasures, conduct a thorough investigation to ensure that no attacker has gained entry, and if an attack is detected, eliminate its impact before taking any countermeasures.

## 5.3. Comparison with past vulnerabilities

ProxyNotShell is named after the vulnerability ProxyShell, which was discovered in 2021 by Mr. Tsai from DEVCORE. In addition to ProxyLogon and ProxyShell, which are also discussed in this report, Mr. Tsai has also discovered the vulnerabilities ProxyOracle and ProxyRelay that allow cyberattacks to be carried out by combining multiple vulnerabilities in Exchange Server [39] [40] [41] [42].

For these pre-ProxyNotShell vulnerabilities, actual cyberattacks occurred after Mr. Tsai announced them. However, with ProxyNotShell, attackers exploited this vulnerability to conduct cyberattacks before the developer Microsoft or public security agencies announced it. This indicates that attackers have acquired the ability to find complex vulnerabilities that combine multiple vulnerabilities and have begun to look for such complex vulnerabilities, and that cyberattacks targeting vulnerabilities have entered a new stage.

Mr. Tsai also suggests that there may be other vulnerabilities related to the system configuration of Exchange Server, and he expects that there will be more cases in the future where attackers conduct cyberattacks by finding complex vulnerabilities that combine multiple vulnerabilities.

## 5.4. Conclusion

The attack exploiting this vulnerability was done by someone knowledgeable about the specifications of Exchange Server and PowerShell, and until the specifics of the vulnerability were made public, it would have been difficult to detect or prevent the attack itself.

As discussed in 5.2, reviewing the Exchange Server configuration and settings and implementing other security systems will reduce the risk, but will not provide a permanent solution. There are concerns that new vulnerabilities may be discovered in Exchange Server in the future, so it is necessary to continuously collect vulnerability information to apply patches to permanently address each vulnerability.

# 6. Outlook

## Information security of the post-Covid-19 era

In May 2023, the new coronavirus infection (COVID-19) will be downgraded in the Infectious Diseases Act classification [43]. As we discussed in this report for the second quarter of 2022, under the Covid-19 pandemic, many companies established special and exceptional rules regarding the expansion of telework and the handling of confidential information [44]. However, because these special and exceptional rules prioritize ensuring business continuity, many of those companies have yet to adequately assess security risks or take security measures. In fact, data breaches have occurred during telework [45], so companies should promptly review or abolish the special or exceptional rules, or introduce additional countermeasures. However, we assume that some companies will maintain telework arrangements while accepting security risks because the benefits of telework are too great to return to office work, or because they do not have sufficient funds or know-how to implement security measures.

During the transition period to the post-Covid-19 era, easing of various regulations and voluntary restraints may cause employees to expand telework to locations such as cafes or workcation spots where it is difficult to ensure information security, leading to an increase in information security incidents such as loss or theft of terminals and storage media.

## Increased crime with Telegram

Telegram is a confidential chat application with a rich set of security features, such as deletion of posts after a certain period of time and screenshot restrictions as well as encryption, providing users with a sense of security when using it. In countries where internet censorship is implemented, it is also used as a tool to combat censorship. Meanwhile, Telegram's high level of confidentiality in terms of identity and communication content makes it a convenient app for criminals to conceal evidence of their crimes. Therefore, it is also being used for crimes such as illegal work and drug trafficking. It was also used in widely publicized large-scale robbery cases by an organizer claiming to be "Luffy" and others.

Given these circumstances, we expect that the number of people who exploit Telegram for crimes or use it with malicious intent, such as for bullying, will increase in the future. It is also a concern that there will be an increase in people using Telegram to search for information about crimes.

Telegram, however, also has its drawbacks. These include the fact that it does not encrypt end-to-end communications in its default settings and does not provide full encryption for chats of three or more people. In addition, it can be set to disclose one's phone number to the other party, which may lead to one's identity getting revealed. If you carelessly access information about illegal work or other such activities through Telegram and a record of the exchange or your information is passed on to criminals, they may exploit the information or get you involved in a crime.

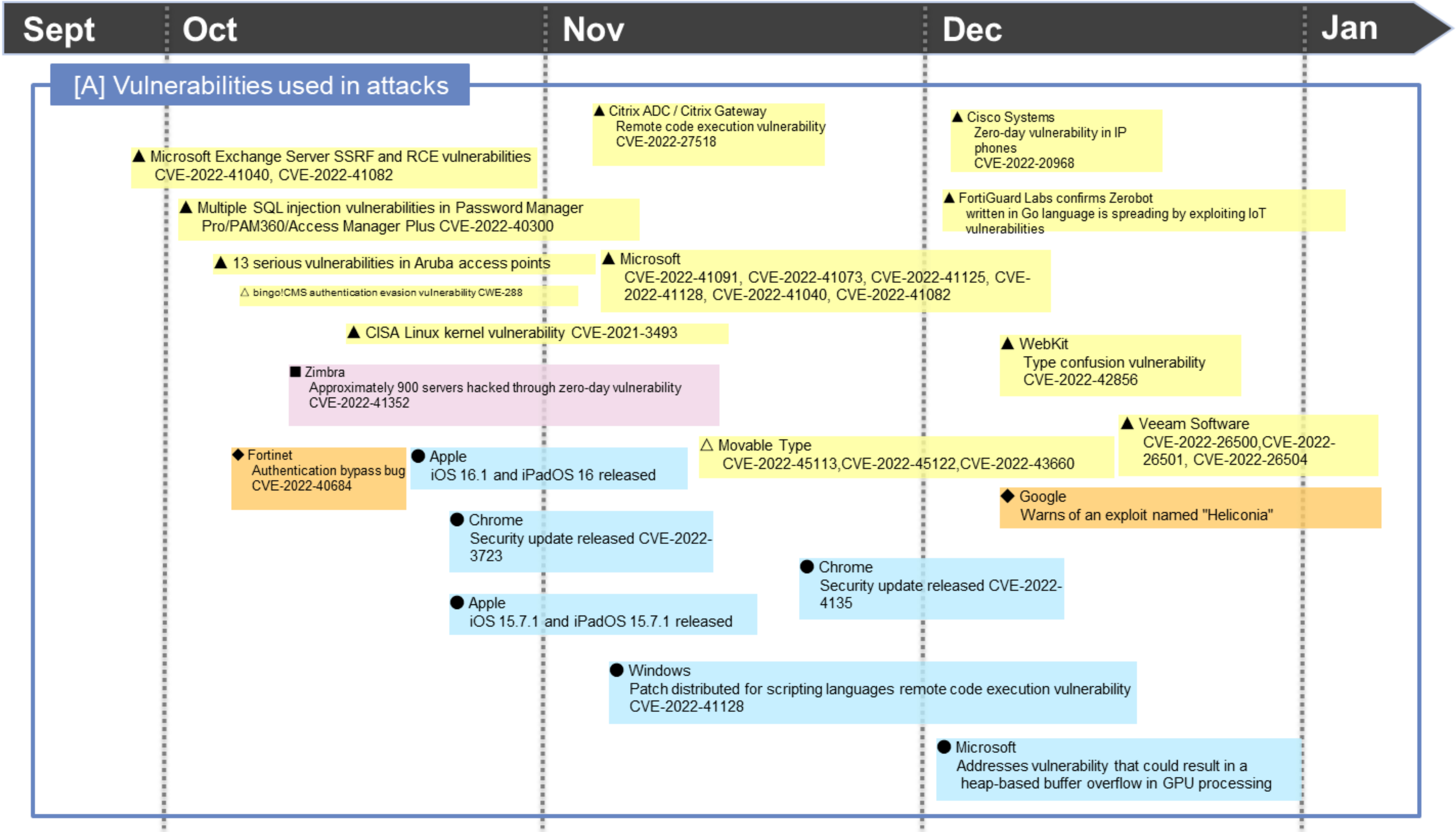
Telegram is an application that is widely used around the world, and its use itself is not a problem. However, you should not carelessly access information about crimes through Telegram, let alone use it to commit crimes.

# 7. Timeline

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

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

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



## [A] Vulnerabilities used in attacks

▲ Microsoft Exchange Server SSRF and RCE vulnerabilities
CVE-2022-41040, CVE-2022-41082

▲ Multiple SQL injection vulnerabilities in Password Manager Pro/PAM360/Access Manager Plus CVE-2022-40300

▲ 13 serious vulnerabilities in Aruba access points

△ bingo!CMS authentication evasion vulnerability CWE-288

▲ CISA Linux kernel vulnerability CVE-2021-3493

■ Zimbra
Approximately 900 servers hacked through zero-day vulnerability
CVE-2022-41352

◆ Fortinet
Authentication bypass bug
CVE-2022-40684

● Apple
iOS 16.1 and iPadOS 16 released

● Chrome
Security update released CVE-2022-3723

● Apple
iOS 15.7.1 and iPadOS 15.7.1 released

▲ Citrix ADC / Citrix Gateway
Remote code execution vulnerability
CVE-2022-27518

▲ Microsoft
CVE-2022-41091, CVE-2022-41073, CVE-2022-41125, CVE-2022-41128, CVE-2022-41040, CVE-2022-41082

△ Movable Type
CVE-2022-45113,CVE-2022-45122,CVE-2022-43660

● Chrome
Security update released CVE-2022-4135

● Windows
Patch distributed for scripting languages remote code execution vulnerability
CVE-2022-41128

▲ Cisco Systems
Zero-day vulnerability in IP phones
CVE-2022-20968

▲ FortiGuard Labs confirms Zerobot written in Go language is spreading by exploiting IoT vulnerabilities

▲ WebKit
Type confusion vulnerability
CVE-2022-42856

▲ Veeam Software
CVE-2022-26500,CVE-2022-26501, CVE-2022-26504

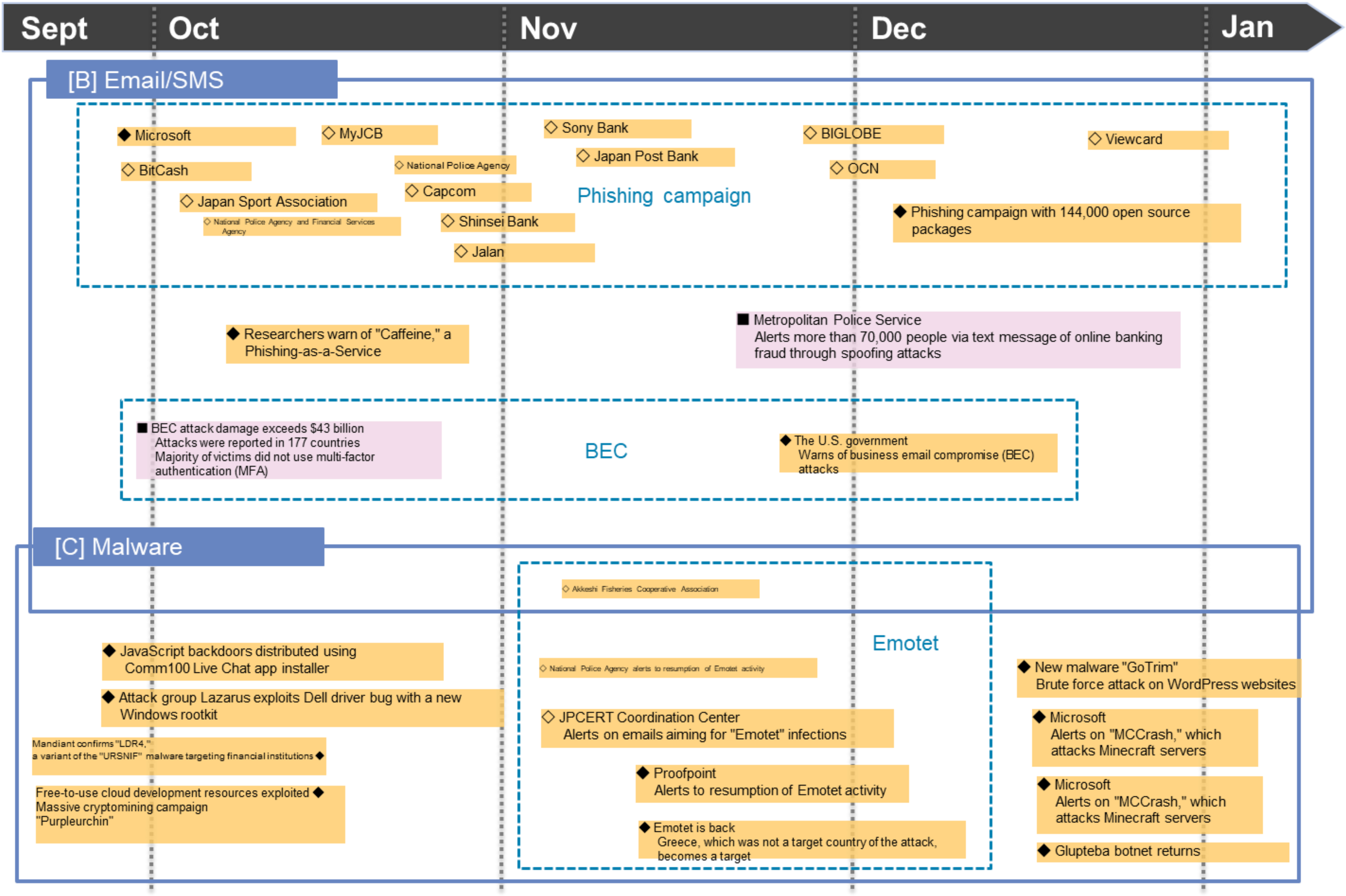
◆ Google
Warns of an exploit named "Heliconia"

● Microsoft
Addresses vulnerability that could result in a heap-based buffer overflow in GPU processing

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

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

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



Sept
Oct
Nov
Dec
Jan
[B] Email/SMS
◆ Microsoft
◇ MyJCB
◇ Sony Bank
◇ BIGLOBE
◇ Viewcard
◇ BitCash
◇ National Police Agency
◇ Japan Post Bank
◇ OCN
◇ Capcom
Phishing campaign
◇ Japan Sport Association
◇ National Police Agency and Financial Services Agency
◇ Shinsei Bank
◆ Phishing campaign with 144,000 open source packages
◇ Jalan
BEC
Emotet
[C] Malware
◇ Akkeshi Fisheries Cooperative Association
◆ New malware "GoTrim"
◇ National Police Agency alerts to resumption of Emotet activity
◆ Glupteba botnet returns

◆ Researchers warn of "Caffeine," a Phishing-as-a-Service

■ Metropolitan Police Service
Alerts more than 70,000 people via text message of online banking fraud through spoofing attacks

■ BEC attack damage exceeds $43 billion
Attacks were reported in 177 countries
Majority of victims did not use multi-factor authentication (MFA)

◆ The U.S. government
Warns of business email compromise (BEC) attacks

◆ JavaScript backdoors distributed using Comm100 Live Chat app installer

◆ Attack group Lazarus exploits Dell driver bug with a new Windows rootkit

Mandiant confirms "LDR4,"
a variant of the "URSNIF" malware targeting financial institutions ◆

Free-to-use cloud development resources exploited ◆
Massive cryptomining campaign
"Purpleurchin"

◇ JPCERT Coordination Center
Alerts on emails aiming for "Emotet" infections

◆ Proofpoint
Alerts to resumption of Emotet activity

◆ Emotet is back
Greece, which was not a target country of the attack, becomes a target

◆ New malware "GoTrim"
Brute force attack on WordPress websites

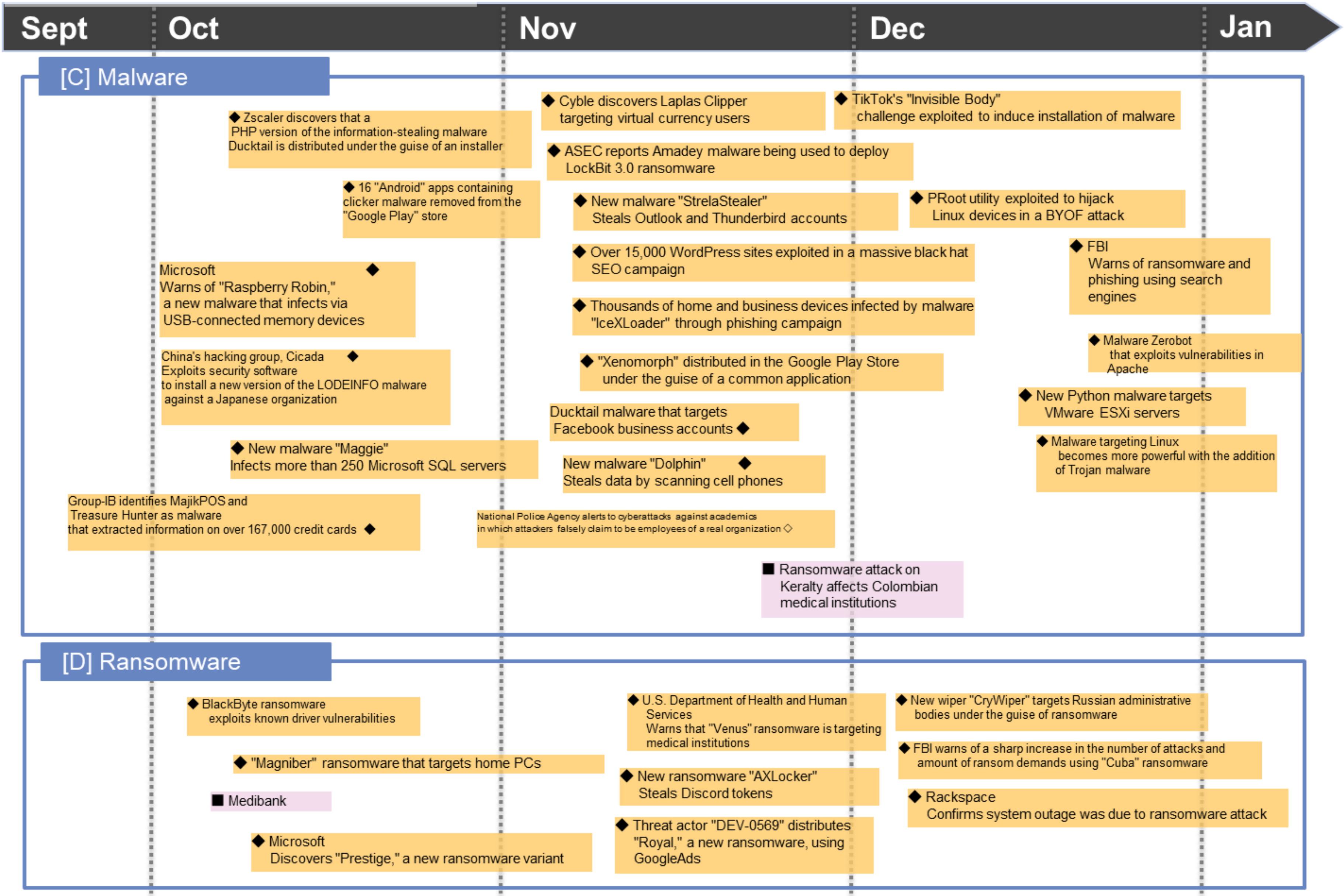
◆ Microsoft
Alerts on "MCCrash," which attacks Minecraft servers

◆ Microsoft
Alerts on "MCCrash," which attacks Minecraft servers

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

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

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



Sept | Oct | Nov | Dec | Jan

## [C] Malware

- ◆ Zscaler discovers that a PHP version of the information-stealing malware Ducktail is distributed under the guise of an installer
- ◆ 16 "Android" apps containing clicker malware removed from the "Google Play" store
- Microsoft Warns of "Raspberry Robin," a new malware that infects via USB-connected memory devices ◆
- China's hacking group, Cicada Exploits security software to install a new version of the LODEINFO malware against a Japanese organization ◆
- ◆ New malware "Maggie" Infects more than 250 Microsoft SQL servers
- Group-IB identifies MajikPOS and Treasure Hunter as malware that extracted information on over 167,000 credit cards ◆
- ◆ Cyble discovers Laplas Clipper targeting virtual currency users
- ◆ ASEC reports Amadey malware being used to deploy LockBit 3.0 ransomware
- ◆ New malware "StrelaStealer" Steals Outlook and Thunderbird accounts
- ◆ Over 15,000 WordPress sites exploited in a massive black hat SEO campaign
- ◆ Thousands of home and business devices infected by malware "IceXLoader" through phishing campaign
- ◆ "Xenomorph" distributed in the Google Play Store under the guise of a common application
- Ducktail malware that targets Facebook business accounts ◆
- New malware "Dolphin" ◆ Steals data by scanning cell phones
- National Police Agency alerts to cyberattacks against academics in which attackers falsely claim to be employees of a real organization ◇
- ■ Ransomware attack on Keralty affects Colombian medical institutions
- ◆ TikTok's "Invisible Body" challenge exploited to induce installation of malware
- ◆ PRoot utility exploited to hijack Linux devices in a BYOF attack
- ◆ FBI Warns of ransomware and phishing using search engines
- ◆ Malware Zerobot that exploits vulnerabilities in Apache
- ◆ New Python malware targets VMware ESXi servers
- ◆ Malware targeting Linux becomes more powerful with the addition of Trojan malware

## [D] Ransomware

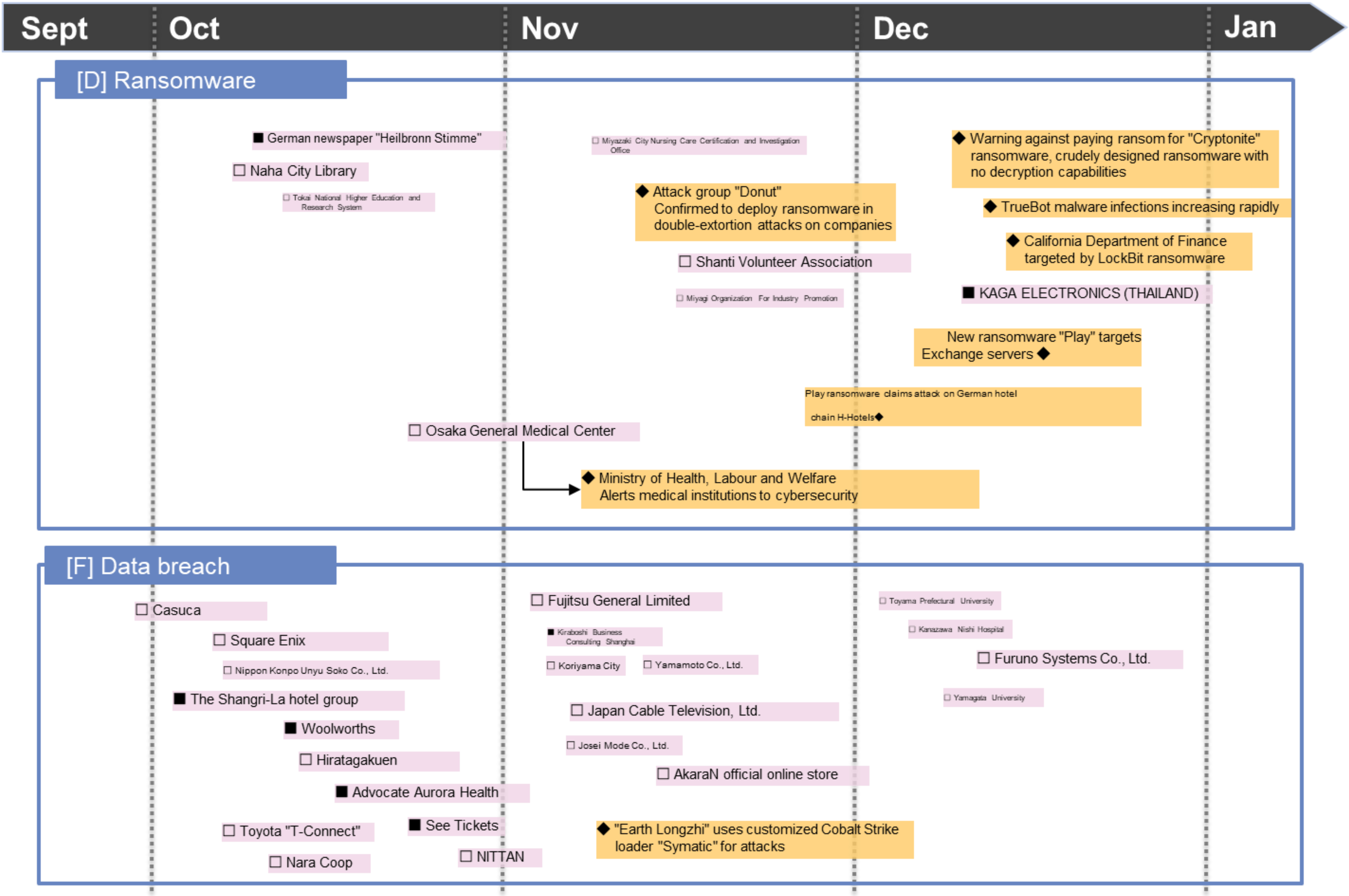
- ◆ BlackByte ransomware exploits known driver vulnerabilities
- ◆ "Magniber" ransomware that targets home PCs
- ■ Medibank
- ◆ Microsoft Discovers "Prestige," a new ransomware variant
- ◆ U.S. Department of Health and Human Services Warns that "Venus" ransomware is targeting medical institutions
- ◆ New ransomware "AXLocker" Steals Discord tokens
- ◆ Threat actor "DEV-0569" distributes "Royal," a new ransomware, using GoogleAds
- ◆ New wiper "CryWiper" targets Russian administrative bodies under the guise of ransomware
- ◆ FBI warns of a sharp increase in the number of attacks and amount of ransom demands using "Cuba" ransomware
- ◆ Rackspace Confirms system outage was due to ransomware attack

Timeline

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

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

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


Sept
Oct
Nov
Dec
Jan

[D] Ransomware

■ German newspaper "Heilbronn Stimme"

□ Naha City Library

□ Tokai National Higher Education and Research System

□ Miyazaki City Nursing Care Certification and Investigation Office

◆ Attack group "Donut"
Confirmed to deploy ransomware in double-extortion attacks on companies

□ Shanti Volunteer Association

□ Miyagi Organization For Industry Promotion

◆ Warning against paying ransom for "Cryptonite" ransomware, crudely designed ransomware with no decryption capabilities

◆ TrueBot malware infections increasing rapidly

◆ California Department of Finance targeted by LockBit ransomware

■ KAGA ELECTRONICS (THAILAND)

New ransomware "Play" targets Exchange servers ◆

Play ransomware claims attack on German hotel chain H-Hotels◆

□ Osaka General Medical Center

◆ Ministry of Health, Labour and Welfare
Alerts medical institutions to cybersecurity

[F] Data breach

□ Casuca

□ Square Enix

□ Nippon Konpo Unyu Soko Co., Ltd.

■ The Shangri-La hotel group

■ Woolworths

□ Hiratagakuen

■ Advocate Aurora Health

□ Toyota "T-Connect"

■ See Tickets

□ Nara Coop

□ NITTAN

□ Fujitsu General Limited

■ Kiraboshi Business Consulting Shanghai

□ Koriyama City

□ Yamamoto Co., Ltd.

□ Japan Cable Television, Ltd.

□ Josei Mode Co., Ltd.

□ AkaraN official online store

◆ "Earth Longzhi" uses customized Cobalt Strike loader "Symatic" for attacks

□ Toyama Prefectural University

□ Kanazawa Nishi Hospital

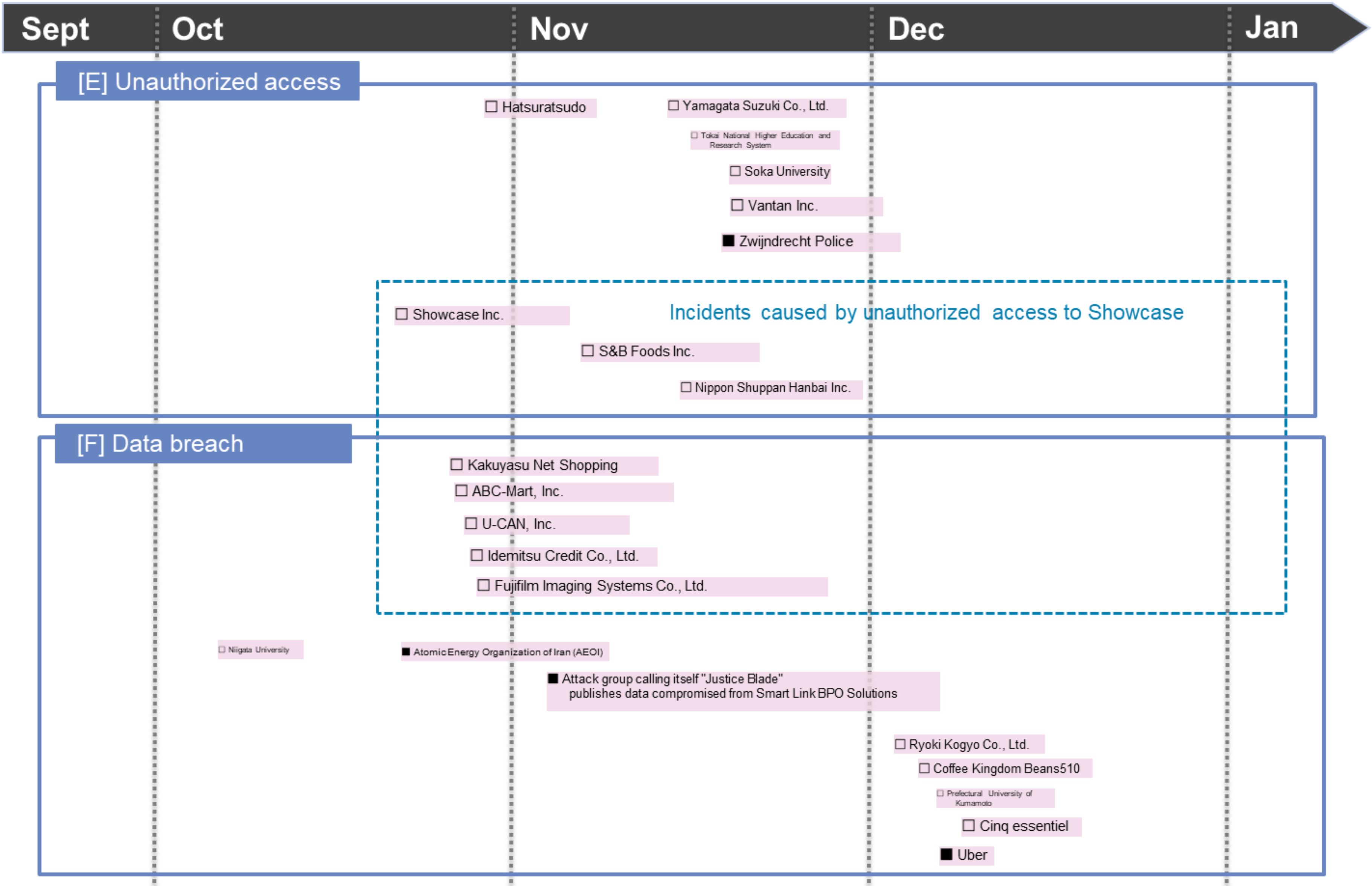
□ Furuno Systems Co., Ltd.

□ Yamagata University

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

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

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



Sept
Oct
Nov
Dec
Jan

[E] Unauthorized access

□ Hatsuratsudo
□ Yamagata Suzuki Co., Ltd.
□ Tokai National Higher Education and Research System
□ Soka University
□ Vantan Inc.
■ Zwijndrecht Police

Incidents caused by unauthorized access to Showcase

□ Showcase Inc.
□ S&B Foods Inc.
□ Nippon Shuppan Hanbai Inc.

[F] Data breach

□ Kakuyasu Net Shopping
□ ABC-Mart, Inc.
□ U-CAN, Inc.
□ Idemitsu Credit Co., Ltd.
□ Fujifilm Imaging Systems Co., Ltd.

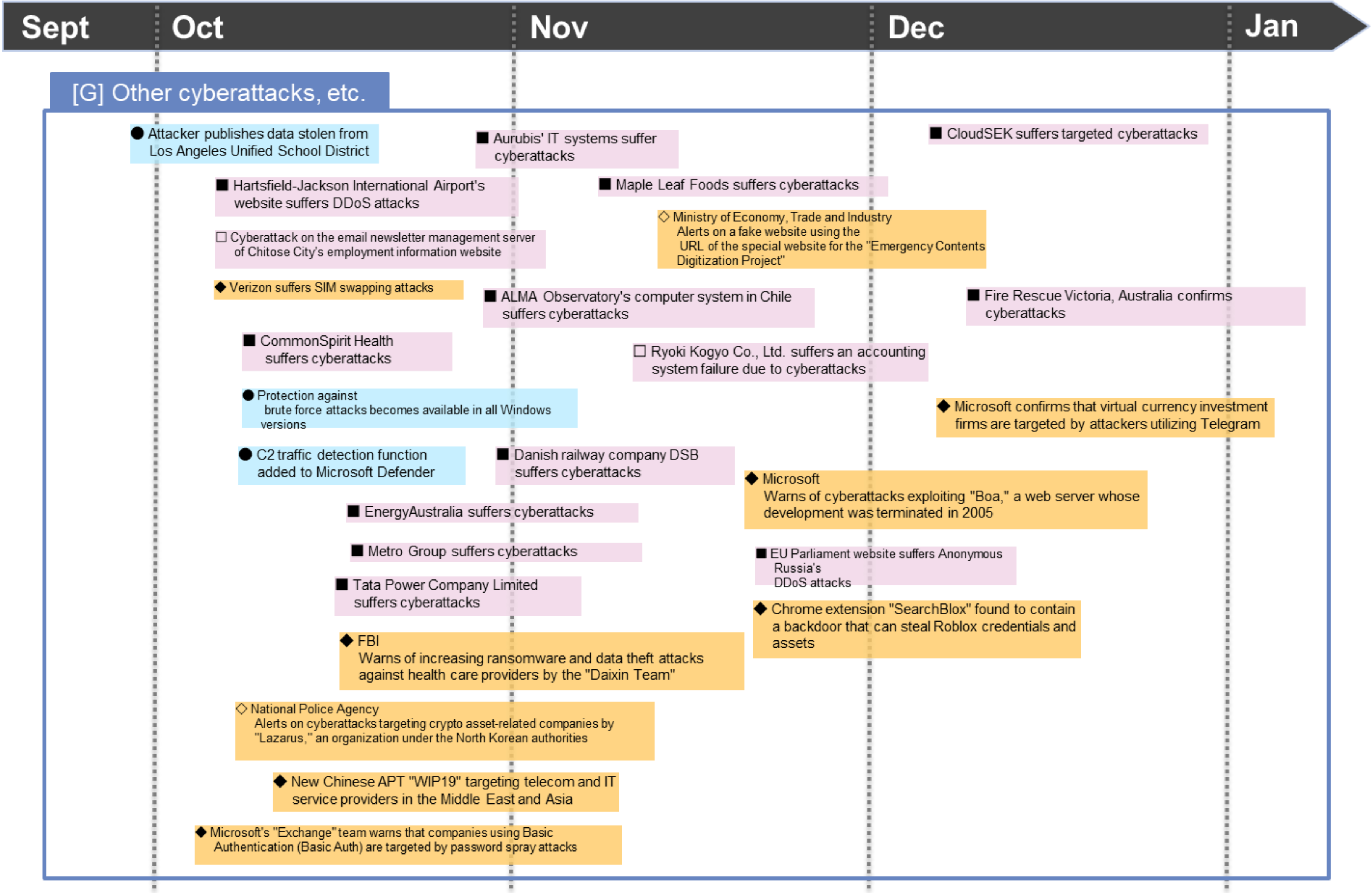
□ Niigata University
■ Atomic Energy Organization of Iran (AEOI)
■ Attack group calling itself "Justice Blade" publishes data compromised from Smart Link BPO Solutions

□ Ryoki Kogyo Co., Ltd.
□ Coffee Kingdom Beans510
□ Prefectural University of Kumamoto
□ Cinq essentiel
■ Uber

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

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

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



## [G] Other cyberattacks, etc.

● Attacker publishes data stolen from Los Angeles Unified School District

■ Hartsfield-Jackson International Airport's website suffers DDoS attacks

□ Cyberattack on the email newsletter management server of Chitose City's employment information website

◆ Verizon suffers SIM swapping attacks

■ CommonSpirit Health suffers cyberattacks

● Protection against brute force attacks becomes available in all Windows versions

● C2 traffic detection function added to Microsoft Defender

■ EnergyAustralia suffers cyberattacks

■ Metro Group suffers cyberattacks

■ Tata Power Company Limited suffers cyberattacks

◆ FBI
Warns of increasing ransomware and data theft attacks against health care providers by the "Daixin Team"

◇ National Police Agency
Alerts on cyberattacks targeting crypto asset-related companies by "Lazarus," an organization under the North Korean authorities

◆ New Chinese APT "WIP19" targeting telecom and IT service providers in the Middle East and Asia

◆ Microsoft's "Exchange" team warns that companies using Basic Authentication (Basic Auth) are targeted by password spray attacks

■ Aurubis' IT systems suffer cyberattacks

■ Maple Leaf Foods suffers cyberattacks

◇ Ministry of Economy, Trade and Industry
Alerts on a fake website using the URL of the special website for the "Emergency Contents Digitization Project"

■ ALMA Observatory's computer system in Chile suffers cyberattacks

□ Ryoki Kogyo Co., Ltd. suffers an accounting system failure due to cyberattacks

■ Danish railway company DSB suffers cyberattacks

◆ Microsoft
Warns of cyberattacks exploiting "Boa," a web server whose development was terminated in 2005

■ EU Parliament website suffers Anonymous Russia's DDoS attacks

◆ Chrome extension "SearchBlox" found to contain a backdoor that can steal Roblox credentials and assets

■ CloudSEK suffers targeted cyberattacks

■ Fire Rescue Victoria, Australia confirms cyberattacks

◆ Microsoft confirms that virtual currency investment firms are targeted by attackers utilizing Telegram

# References

[1] デジタル庁, “「ISMAP-LIU」の運用を開始しました,” 1 11 2022. [オンライン]. Available: https://www.digital.go.jp/news/76af2f66-c63c-43ef-aa2d-90ab018d5a6c/.

[2] NISC、デジタル庁、総務省、経済産業省, “ISMAP-LIUについて,” 1 11 2023. [オンライン]. Available: https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=96af45d0db21d110d2b773f4f3961995&spa=1.

[3] 内閣官房・総務省・経済産業省, “政府情報システムのためのセキュリティ評価制度（ISMAP）について,” 3 6 2022. [オンライン]. Available: https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=96af45d0db21d110d2b773f4f3961995&spa=1.

[4] ISMAP 運営委員会, “ISMAP 管理基準,” 3 6 2021. [オンライン]. Available: https://www.ismap.go.jp/csm/ja?id=kb_article_view&spa=1&sys_kb_id=e2309a581b9d301013a78665cc4bcba9&sysparm_article=KB0010028.

[5] FIDO Alliance, “Apple、Google、MicrosoftがFIDO標準のサポート拡大にコミット、パスワードレス認証の普及を促進,” 5 5 2022. [オンライン]. Available: https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins-jp/?lang=ja.

[6] FIDO Alliance, “FIDO Alliance - Open Authentication Standards More Secure than Passwords,” [オンライン]. Available: https://fidoalliance.org/.

[7] FIDO ALLIANCE, “FIDOの仕組み,” [オンライン]. Available: https://fidoalliance.org/fido%e3%81%ae%e4%bb%95%e7%b5%84%e3%81%bf/?lang=ja.

[8] FIDO ALLIANCE, “パスワードレス認証の普及を加速させる取り組み,” 17 3 2022. [オンライン]. Available: https://fidoalliance.org/charting-an-accelerated-path-forward-for-passwordless-authentication-adoption-jp/?lang=ja.

[9] FIDO Alliance, “How FIDO Addresses a Full Range of Use Cases,” 3 2022. [オンライン]. Available: https://media.fidoalliance.org/wp-content/uploads/2022/03/How-FIDO-Addresses-a-Full-Range-of-Use-Cases-March24.pdf.

[10] 板倉景子, “What are Passkeys?,” 9 12 2022. [オンライン]. Available: https://media.fidoalliance.org/wp-content/uploads/2022/12/Keiko-Itakura_What-are-Passkeys-final-as-of-Dec-12.pdf.

[11] Apple Inc., “iOS 16 のアップデートについて,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213407.

[12] Apple Inc., “macOS Ventura のアップデートの新機能,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213268.

[13] Apple Inc., “iPadOS 16 のアップデートについて,” [オンライン]. Available: https://support.apple.com/ja-jp/HT213408.

[14] D. Zavala, C. Brand, A. Naddaf , K. Buchanan, “Android と Chrome にパスキーを導入,” 4 11 2022. [オンライン]. Available: https://developers-jp.googleblog.com/2022/11/bringing-passkeys-to-android-and-chrome.html.

[15] A. Sarraf, “Chrome がパスキーに対応しました,” 15 12 2022. [オンライン]. Available: https://developers-jp.googleblog.com/2022/12/chrome.html.

[16] Google LLC, “Android と Chrome でパスキーをサポート,” 9 2 2023. [オンライン]. Available: https://developers.google.com/identity/passkeys/supported-environments?hl=ja.

[17] AgileBits, Inc., “The passwordless experience you deserve,” [オンライン]. Available: https://www.future.1password.com/passkeys/.

[18] C. Hoff, “Passwordless Is Possible: LastPass Gets You There Sooner,” 6 6 2022. [オンライン]. Available: https://blog.lastpass.com/2022/06/passwordless-is-possible-lastpass-gets-you-there-sooner/.

[19] W. Palant, “What's in a PR statement: LastPass breach explained,” 27 12 2022. [オンライン].

[20] ヤフー株式会社, “セキュリティリスクから守るパスワードレスとは？ 生体認証によるログインのメリットと設定方法,” 6 2 2023. [オンライン]. Available: https://about.yahoo.co.jp/info/blog/20230206/passwordless.html.

[21] 株式会社NTTドコモ, “dアカウントのログインにおける新たな認証手段（Web認証・パスキー）の提供を開始,” 17 10 2022. [オンライン]. Available: https://www.docomo.ne.jp/info/news_release/2022/10/17_00.html.

[22] D. Zavala, “Bringing together sign-in solutions and passkeys with Android's new Credential Manager,” 6 2 2023. [オンライン]. Available: https://android-developers.googleblog.com/2023/02/bringing-together-sign-in-solutions-and-passkeys-android-new-credential-manager.html.

[23] 株式会社ショーケース, “不正アクセスに関するお知らせとお詫び,” 25 10 2022. [オンライン]. Available: https://www.showcase-tv.com/pressrelease/202210-fa-info/.

[24] 一. 情報サービス産業協会, “ASPサービスモデル利用規約,” 3 2005. [オンライン]. Available: https://www.jisa.or.jp/Portals/0/resource/legal/download/asp_policy_model.pdf.

[25] PCISSC, “PCI DSS Version 4.0 日本語版,” 3 2022. [オンライン]. Available: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0-JA.pdf.

[26] 独立行政法人情報処理推進機構, “情報セキュリティサービス基準適合サービスリストの公開,” 5 6 2018. [オンライン]. Available: https://www.ipa.go.jp/security/it-service/service_list.html.

[27] 特定非営利活動法人日本ネットワークセキュリティ協会, “サイバーインシデント緊急対応企業一覧,” 2 2023. [オンライン]. Available: https://www.jnsa.org/emergency_response/.

[28] 一. 日本損害保険協会, “サイバー保険取り扱い会社,” 12 2022. [オンライン]. Available: https://www.sonpo.or.jp/cyber-hoken/ins/.

[29] GTSC VIETNAM TECHNOLOGY SERVICES AND COMMERCIAL JOINT STOCK COMPANY, “WARNING: NEW ATTACK CAMPAIGN UTILIZED A NEW 0-DAY RCE VULNERABILITY ON MICROSOFT EXCHANGE SERVER,” 28 9 2022. [オンライン]. Available: https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html.

[30] Microsoft Corporation, “Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server,” 30 9 2022. [オンライン]. Available: https://msrc.microsoft.com/blog/2022/09/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/.

[31] Microsoft Corporation, “Microsoft Exchange Server 2019、2016、および 2013 のセキュリティ更新プログラムについて: 2022 年 11 月 8 日 (KB5019758),” 8 11 2022. [オンライン]. Available: https://support.microsoft.com/ja-jp/topic/microsoft-exchange-server-2019-2016-%E3%81%8A%E3%82%88%E3%81%B3-2013-%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%9B%B4%E6%96%B0%E3%83%97%E3%83%AD%E3%82%B0%E3%83%A9%E3%83%A0%E3%81%AB%E3%81%A4.

[32] P. Bazydło, “CONTROL YOUR TYPES OR GET PWNED: REMOTE CODE EXECUTION IN EXCHANGE POWERSHELL BACKEND,” 16 11 2022. [オンライン]. Available: https://www.thezdi.com/blog/2022/11/14/control-your-types-or-get-pwned-remote-code-execution-in-exchange-powershell-backend.

[33] Microsoft Corporation, “Analyzing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082,” 30 9 2022. [オンライン]. Available: https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/.

[34] Fortinet, Inc., “Microsoft Exchange 0-Day Vulnerability Updates,” 30 9 2022. [オンライン]. Available: https://www.fortinet.com/blog/threat-research/microsoft-exchange-zero-day-vulnerability-updates.

[35] トレンドマイクロ株式会社, “Microsoft Exchange Serverでゼロデイ攻撃が発生,” 30 9 2022. [オンライン]. Available: https://www.trendmicro.com/ja_jp/research/22/i/ms-exchange-zero-day.html.

[36] Imperva, Inc., “Microsoft Exchange Server Vulnerabilities CVE-2022-41040 and CVE-2022-41082,” 30 9 2022. [オンライン]. Available: https://www.imperva.com/blog/microsoft-exchange-server-vulnerabilities-cve-2022-41040-and-cve-2022-41082/.

[37] Akamai Technologies, Inc., “Microsoft Exchange Server のゼロデイ脆弱性（CVE-2022-41040 および CVE-2022-41082）への Akamai の対応,” 3 10 2022. [オンライン]. Available: https://www.akamai.com/ja/blog/security-research/akamais-response-zero-day-vulnerabilities-microsoft-exchange-server.

[38] F5, Incorporated, “K54470807: Mitigating CVE-2022-41082, CVE-2022-41040 with BIG-IP ASM / Adv WAF Attack Signatures,” 3 10 2022. [オンライン]. Available: https://support.f5.com/csp/article/K54470807.

[39] O. Tsai, “A New Attack Surface on MS Exchange Part 1 - ProxyLogon!,” 6 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-1-ProxyLogon/.

[40] O. Tsai, “A New Attack Surface on MS Exchange Part 2 - ProxyOracle!,” 6 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-2-ProxyOracle/.

[41] O. Tsai, “A New Attack Surface on MS Exchange Part 3 - ProxyShell!,” 22 8 2021. [オンライン]. Available: https://devco.re/blog/2021/08/22/a-new-attack-surface-on-MS-exchange-part-3-ProxyShell/.

[42] O. Tsai, “A New Attack Surface on MS Exchange Part 4 - ProxyRelay!,” 19 10 2022. [オンライン]. Available: https://devco.re/blog/2022/10/19/a-new-attack-surface-on-MS-exchange-part-4-ProxyRelay/.

[43] 厚生労働省, “新型コロナウイルス感染症の感染症法上の位置づけの変更等に関する対応方針について,” 27 1 2023. [オンライン]. Available: https://www.mhlw.go.jp/content/001046577.pdf.

[44] NTTデータ, “グローバルセキュリティ動向四半期レポート 2022年度 第3四半期,” 2023. [オンライン].

[45] Security NEXT, “テレワーク環境でマルウェア感染、社内に拡大 - 三菱重工,” 11 8 2020. [オンライン]. Available: https://www.security-next.com/117404.

Published on May 19, 2023

Cyber Security Department, NTT DATA Corporation
Hisamichi Ohtani
Toshihiko Matsuo / Riho Miyai / Akihiro Shiota / Nobuo Idezawa / Shigeyuki Tahara
Rui Kanazawa / Chihiro Oyama / Hiroki Ogasahara
nttdata-cert@kits.nttdata.co.jp