Quarterly Report on Global Security Trends

2nd Quarter of 2024

Contents

1. Executive Summary

This is a report of investigation and analysis of the global trends in the said quarter, based on the information in relation to cyber security collected by NTTDATA-CERT during the period.

Featured Topics “Data breaches due to internal improprieties: Characteristics and required countermeasures”

Data breaches due to internal improprieties are a serious security risk for business enterprises. Its characteristics often include behaviors difficult to distinguish from normal operations and/or exploits of own privileges and competences, which are frequently committed at the time of or just before retirement. As countermeasures, employee training and thorough enforcement of rules are essential, in addition to technical countermeasures such as access limitation, privilege management and log monitoring.

For prevention of internal improprieties, approaches from both sides, i.e., technical and educational aspects are required. For business enterprises, it is important to integrate these countermeasures and to build up sustainable defense. In addition, as countermeasures depend on the characteristics of various internal improprieties, our recommendations are interference to the improprieties triangle based on 3 aspects, “opportunity”, “motive”, and “justification” for cover-up type, and implementation of access limitation and introduction of immediate interruption system for bold type. As solutions against internal improprieties, application of DLP and privilege management system, as well as UEBA are recommended.

Vulnerability “Countermeasures for vulnerability of Public API which is increasing abruptly”

In accordance with the growing use of Public APIs, vulnerability also grows bigger with the result that risks of cyber attacks increase. Particularly, improper configurations for authentication and approval occur frequently, where vulnerabilities such as Broken Object Level Authorization (BOLA) are exploited.

As countermeasures, it is essential that the Secure by Design approach is employed so that security is integrated from the initial stage of development. In concrete terms, we recommend implementation of Multi-factor authentication and/or OAuth 2.0, Runtime protection, Security tests, Security posture management, cataloging of APIs, reinforcement of API governance, and so on. In addition, as countermeasures against issues which Secure by Design is not capable to solve, application of API discovery or automated security tools, and enhancement of security education are also required.

Vulnerability “Improvement of Vulnerability triage approach using SSVC”

SSVC (Stakeholder-Specific Vulnerability Categorization) is a framework to assess the priority to response to vulnerability, and it resolves the problems of CVSS (Common Vulnerability Scoring System), the reference to assess seriousness of vulnerability. SSVC uses a decision tree to access the impact of vulnerability to indicate the priority to response to vulnerability in 4 levels, “Immediate”, “Out-of-cycle”, “Scheduled”, and “Defer”. As such, judgments for responding to vulnerability in visual and logical way are enabled.

With enhancement of AI technologies, cyber attacks aiming at vulnerability are generated in shorter cycles, as such, agile countermeasures for vulnerability are required. Important points are pre-established support and particularization for vulnerability. In particular, servers, network equipment, and software in relation to Exposure and Mission Impact, among 4 decision points of SSVC, are grouped and assessment values are prepared beforehand, then the priority for countermeasures against vulnerability is determined using SSVC. Effective countermeasures for vulnerability even by only a few members are enabled to make it possible to enhance readiness for the security of the organization.

2. Featured Topics “Data breaches due to internal improprieties: Characteristics and required countermeasures”

Shigeaki Kurimoto, Security and Network Department, NTT DATA Japan

Data breaches due to internal improprieties have been ranked within top 10 in the “10 Major Security Threats [For Organizations]” announced by the Independent administrative agency, Information-Technology Promotion Agency (IPA), Japan every year since 2016 when the IPA started announcing the results. In 2024, it was ranked third. Data breaches due to internal improprieties are a serious security risk which business enterprises must always focus on [1]. Once data breaches due to internal improprieties occur, this may result in not only the business enterprise losing its trust leading to economic loss, but it could also be developed into a legal issue.

In this article, with regard to data breaches due to internal improprieties which have been continually sophisticated year by year, we focus on common cases actually occurs, as well as their characteristics, and also comment on countermeasures, frequently applied not only as preventive measures but also as sustainable protection plan.

2.1. Example of data breaches due to internal improprieties

Data breaches due to internal improprieties can occur in a variety of cases, ranging from those caused by an individual to those involving multiple people, and can vary in the level of malicious intent. Examples of principal patterns of internal improprieties are as shown below [2] [3]:

(i) An employee planning to resign from the company lodges sensitive information/personal information illegally
(ii) A contract employee lodges sensitive information/personal information of consignor business enterprise illegally
(iii) An industrial spy lodges sensitive information/personal information illegally
(iv) 2 or more employees collude to lodge sensitive information/personal information illegally
(v) An employee brings out sensitive information for working at home on Saturday and Sunday, because she/he fails to complete to prepare the documents on time
(vi) An employee who has something against the company does harassing behavior such as destroying information or spreading false information

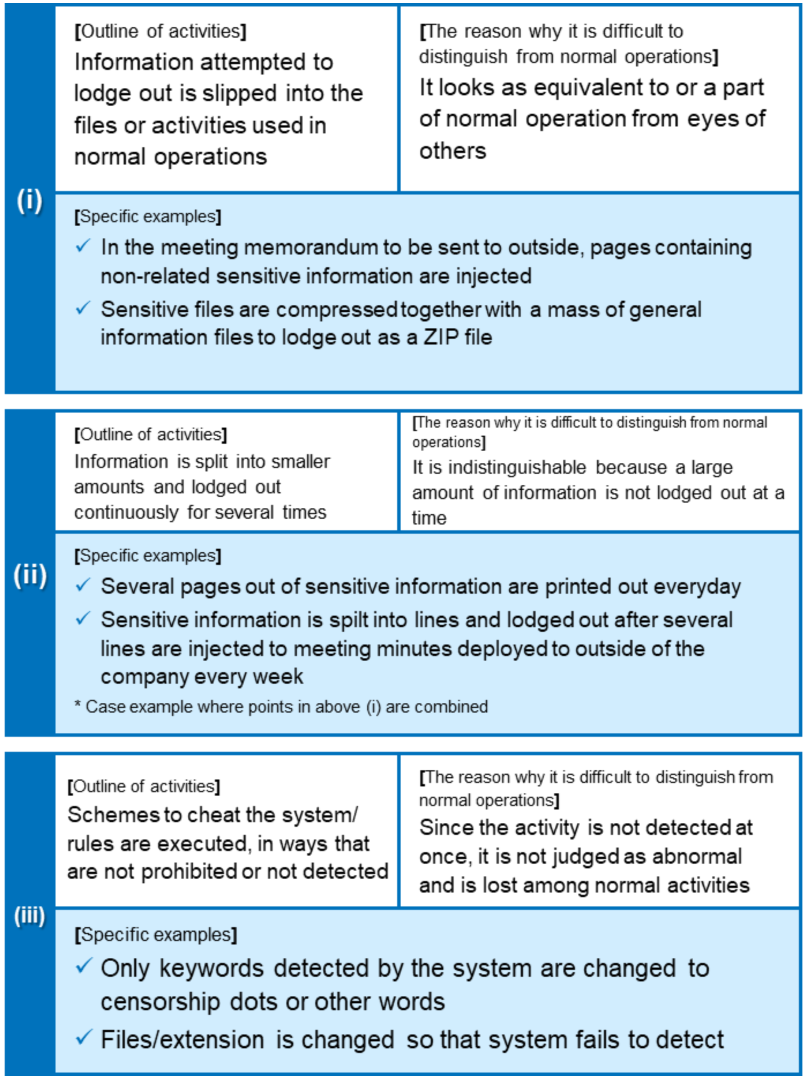
The subject or purpose of internal improprieties vary. Characteristics commonly applicable to such internal improprieties to no small extent include “Behaviors difficult to distinguish from normal operations” or “Behaviors allowed to carry out as a part of normal operation based on own privileges and competences”. Since it is not easy to judge such internal improprieties committed outrageously or intentionally from normal operation, internal improprieties could easily deceive eyes of others and slip through the supervision. In the following chapters, we explain these characteristics concretely.

2.2. Characteristics in cases of internal improprieties in recent years

For internal improprieties difficult to distinguish from normal operations, a number of sophisticated tricks are used. Examples of internal improprieties are sorted out and examples of sophisticated tricks listed below are summarized in Table 2-1.

(i) Sensitive information/personal information tried to lodge illegally is slipped into information/activities which are handled in normal operations
(ii) A large mass of information is not lodged out at a time, instead, such information is split into smaller masses and lodged out continuously for several times
(iii) Data breaches are executed by means of using loopholes of systems and rules for detection or control of internal improprieties

Table 2-1: Examples of internal impropriety activities difficult to distinguish from normal operations



	[Outline of activities]	[The reason why it is difficult to distinguish from normal operations]	[Specific examples]
(i)	Information attempted to lodge out is slipped into the files or activities used in normal operations	It looks as equivalent to or a part of normal operation from eyes of others	✓ In the meeting memorandum to be sent to outside, pages containing non-related sensitive information are injected ✓ Sensitive files are compressed together with a mass of general information files to lodge out as a ZIP file
(ii)	Information is split into smaller amounts and lodged out continuously for several times	It is indistinguishable because a large amount of information is not lodged out at a time	✓ Several pages out of sensitive information are printed out everyday ✓ Sensitive information is spilt into lines and lodged out after several lines are injected to meeting minutes deployed to outside of the company every week * Case example where points in above (i) are combined
(iii)	Schemes to cheat the system/ rules are executed, in ways that are not prohibited or not detected	Since the activity is not detected at once, it is not judged as abnormal and is lost among normal activities	✓ Only keywords detected by the system are changed to censorship dots or other words ✓ Files/extension is changed so that system fails to detect

A virtual environment is set up to simulate specific activities, then the above-mentioned points are explained.

2.2.1. Simulation for illegal lodging in a virtual organizational environment

Based on examples of internal improprieties actually occurred and relevant perceptions, a scenario of illegal lodging is described in the light of characteristics of internal Impropriety cases. First, a virtual organizational environment is established as follows (refer to Fig.2-1):

- Company A (consignor business enterprise) entrusted a new product development project (sensitive information) to Company B (consignee business enterprise).
- Mr. X of Company B participated in the project of Company A. Mr. X obtained a business account for a contract employee of Company A and accessed certain part of sensitive information to carry out his task.
- Company A and Company B used the same communication tool (Example: Microsoft Teams, etc.) and linked the tenants of the companies each other to implement information sharing.
- Nevertheless, if it is attempted to lodge sensitive information outside of company A, it is detected and blocked by the rule of the DLP (Data Loss Prevention: Security tool to prevent leakage of information) which Company A had introduced. Therefore, information exchanged between Company A and Company B does not contain sensitive information, in principle.

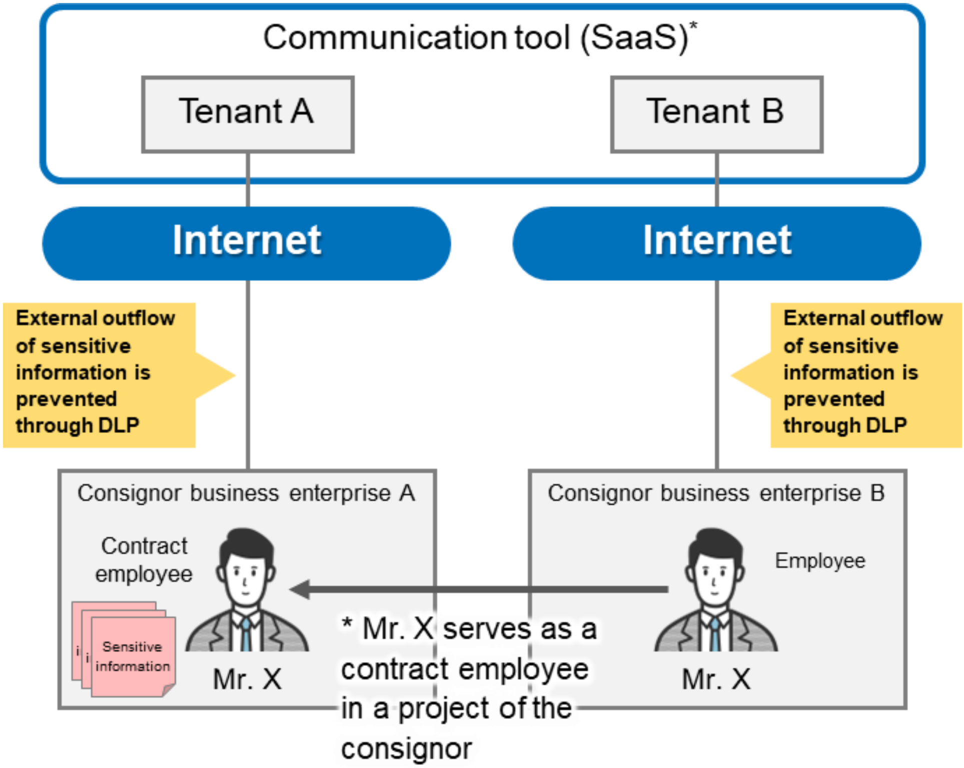

Communication tool (SaaS)*
Tenant A
Tenant B
Internet
Internet
External outflow of sensitive information is prevented through DLP
External outflow of sensitive information is prevented through DLP
Consignor business enterprise A
Contract employee
Sensitive information
Mr. X
Consignor business enterprise B
Employee
Mr. X
* Mr. X serves as a contract employee in a project of the consignor

Fig.2-1: Virtual organizational environment

2.2.2. Clues for illegal lodging

In such an environment, a case is attempted in which Mr. X lodges sensitive information of Company A (consignor business enterprise) illegally.

- During normal operations, Mr. X links information relevant to the project using a communication tool from the Company A environment to Company B environment. A number of files are linked in gross in a ZIP format.
- On one occasion, sensitive information is contained unintentionally in a ZIP file which Mr. X tried to link from the Company A environment to Company B environment, as such, the DLP detected the keyword and blocked the link.
- From this detection, Mr. X had a chance to learn the detection/blockage rule of DLP, as well as the keyword DLS uses for detection.

As in such a case, it is possible to learn certain parts of the rule of DLP during normal operations.

2.2.3. Exploit of illegal lodging

Mr. X decided to shift his job from Company B to another company, Company C, and leave the project in Company A within 3 months. In such a situation, Mr. X tried to lodge out sensitive information of Company A to make use in the Company C to which he shifts, within 3 months until he leaves the project and shifts his job. Lodging out of information through internal improprieties is often exploited at the time of or just before retirement [4]. Mr. X executed lodging out of information from the environment in consignor, Company A, using means as described below (refer to Fig.2-2).

- From the documents he tried to lodge out, Mr. X changed the keywords which the DLP detected to the words which DLP did not detect.
- Files containing sensitive information doctored as above were slipped in the ZIP file groups linked from the Company A environment to Company B environment and lodged out.
- Instead of adding a number of sensitive information files to a ZIP file to lodge out at a time, such files are added little by little to ZIP files and lodged out.
- Mr. X exploited lodging out sensitive information files continuously until he left the project after 3 months.
- After bringing in sensitive files from Company A to Company B, Mr. X printed out the files in the environment of Company B little by little, to appropriate the sensitive information for his own use.

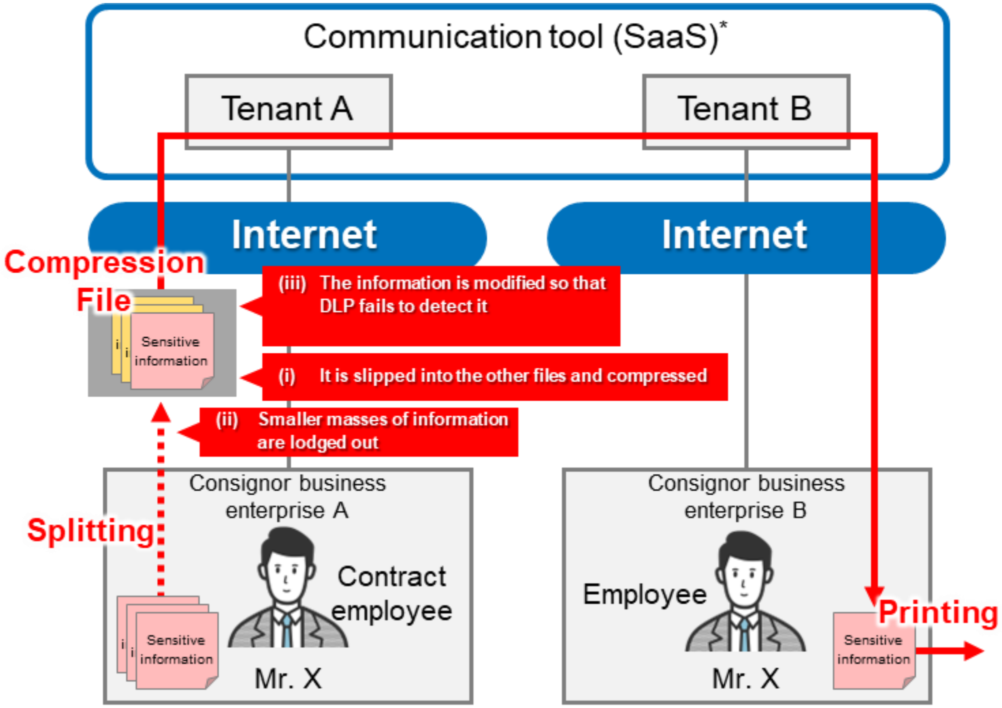

Communication tool (SaaS)*
Tenant A
Tenant B
Internet
Internet
Compression
File
Sensitive information
(iii) The information is modified so that DLP fails to detect it
(i) It is slipped into the other files and compressed
(ii) Smaller masses of information are lodged out
Consignor business enterprise A
Consignor business enterprise B
Splitting
Contract employee
Employee
Printing
Sensitive information
Sensitive information
Mr. X
Mr. X

Fig.2-2: Means for illegal lodging

This scenario of illegal lodging was schemed using illegal access methods difficult to distinguish from normal operations, i.e., (1) Sensitive information was slipped in the files used in normal operations, (2) Smaller masses of information were lodged out for several times, and (3) Sensitive information was modified to avoid detection to take advantage of loopholes in systems/rules, as mentioned above.

In addition, after lodging out the sensitive information files to the environment in his Company B, Mr. X printed out to papers to bring out to his home. During recent years, in the context of digitalization and teleworking, opportunities to print out documents on paper are decreasing. As such practices of monitoring printing process logs or implementing security measures for control of printing have been also decreasing. Such an aspect is also apt to be exploited as a loophole.

2.2.4. After exploiting of illegal lodging

As the result, Mr. X succeeded to lodge out sensitive information without being suspected by the members around since it only looked that he was carrying out normal operations despite illegality, and the DLP also failed to detect that. After that, however, the sensitive information lodged out could not be used effectively and this illegal lodging finally led to it being discovered.

- Although Mr. X attempted to make use of the sensitive information he lodged out in the new environment in Company C, further updated technologies/information in the same field as the sensitive information had been already announced publicly. As such, the information lodged out became outdated very soon and as a consequence, it was not possible to make use of it effectively in Company C.
- Furthermore, at a later date, in “Check of employees retired/left from projects (audit)” periodically conducted in Company A, a decision was made to go through procedures to check the access history to PCs/file servers of Mr. X again. During this check, it was revealed that Mr. X had “accessed sensitive information for which access could not be actually required in normal operations”. Consequently, it was considered a suspected case within Company A, then further detailed investigation was to be conducted. Finally, both the list and history of files lodged out in the past were also checked, and then it was ascertained that the files of sensitive information were lodged out though not planned in the actual operations. Consequently, fraudulence was exposed.

It is not possible for a person to openly make use of sensitive information lodged out through internal improprieties, in the competitor company she/he transitioned. Furthermore, its value is not always assured on a long-term basis. Further, when such an illegal lodging is found out, it may incur that claims for damage to Mr. X is filed by Company A or Company B, or even criminal penalties are applied such as arrestment or sending papers prosecutors, as the case may be. As such, in actuality, while it is difficult to obtain benefits using the files of sensitive information lodged out illegally, there may be cases that internal improprieties are revealed later and responsibility is pursued.

2.3. Security measures against internal improprieties per characteristics

As countermeasures against such internal improprieties, guidelines and such published by various bodies may act as useful references [5] [6]. As for internal improprieties, since activities of internal executor vary depending on the characteristics described below, security measures are difficult. We recommend the method in which the policy for the security measure is determined based on the characteristics of internal improprieties, then specific methods are studied based on those. The characteristics of internal improprieties are roughly divided to cover-up type carried out in a stealthy manner to avoid that illegality is found out, and bold type carried out on the assumption that internal improprieties are revealed. Effective security measures vary respectively.

2.3.1. Security measures against cover-up type internal improprieties

First of all, in cases of cover-up type internal improprieties, which are exploited seeking to avoid these from being revealed as much as possible, internal improprieties are exploited carefully. The cover-up types are those in which it is attempted to avoid risks such that internal improprieties are reveled to result in losing the job or incurring criminal penalties or claim for damages. As for the cover-up type, a certain prevention effect is expected when security measures are implemented which interfere with the “Improprieties triangle”, generally considered as the factors for exploit of internal improprieties [7]. Examples of security measures based on the 3 aspects of improprieties triangle, “opportunity”, “motive”, and “justification” are described below:

- “Opportunity”: Environments/means which enable internal improprieties must be seized as much as possible
  (Example) Restriction of access to sensitive information, control of privileges, and such
- “Motive”: It must be disseminated that it is difficult to exploit internal improprieties in the current situation, as well as that the return is small
  (Example) Log monitoring of terminals/security equipment for employee and thorough publicity of that
- “Justification”: Implementation of rules and training must be enforced thoroughly to build up a situation which does not allow justification and excuse for crime
  (Example) Thorough enforcement of training and rules to employees, and such

Implementation of these security measures leads to weaken the will to commit internal fraud and thus prevent it.

2.3.2. Security measures against bold type internal improprieties

On the other hand, when the committer considers it does not matter if internal improprieties are revealed, restriction through training or monitoring among the security measures in the improprieties triangle is not effective. For instance, in case of an industrial spy who considers she/he would resign the job as soon as internal improprieties are revealed, she/he lodges sensitive information out by every means and then hides her/himself once internal improprieties are revealed.

As for such bold type training and restriction are not effective, an effective countermeasure is the method in which any of significant activities are forbidden in principle. While access to any sensitive information is forbidden in principle, the administrator checks the matter every time and gives permission when it is necessary to access sensitive information. In addition, it is essential that when the sensitive information accessed is traced or any internal improprieties are detected, such activities are interrupted without delay. To implement the matters above, it is required the introduction and operation of a system which runs privilege control and access restriction, as well as a system which interrupts operation at the time it detects internal improprieties without delay.

2.4. Internal improprieties prevention solution

At the moment, for internal improprieties prevention, various solutions are available including DLP against data breach, privilege control system for permission control, and such. Using such solutions effectively, it is possible to implement cost-effective internal improprieties prevention including not only bold type but also cover-up type internal improprieties [8] [9].

In recent years, the solution considered effective for detection of internal improprieties is UEBA (User and Entity Behavior Analysis) products. UEBA consolidates and monitors logs of security equipment and each IT device, and conducts analysis by means of machine learning. As the result of machine learning, it is enabled that activities suspected as internal improprieties are immediately detected, in suspicious situations that seemingly normal operations are carried out but actually these are different from normal operations. Specific examples are as listed below [10].

- Accessing a server which is not usually accessed in operations
- Uploading files to a website which is not usually accessed in operations
- Number of mails is higher than usual number of sending mails
- A system is used in a period of time usually not used
- A system is accessed from an IP address or a site other than usual to carry out tasks

These activities are the activities not forbidden, but activities using valid permission owned, as such, they look as normal operations at first glance. However, since such activities are partially different from normal operations, internal impropriety is suspected. UEBA monitors and analyses a huge volume of logs and is capable to automatically and rapidly detect segments different from normal activities though valid permission was used.

In case of bold type internal improprieties, since restriction or training is not effective, unless otherwise the security measures forbid, restrict, or control forcibly the system, prevention is not possible. Using the result of detection by UEBA products, when SOAR products link with other products and process automatically, it is possible to prevent bold type internal improprieties also.

Methodologies and technologies of internal improprieties are continually sophisticated day by day. Business enterprises have to protect important information assets through prevention and detection of internal improprieties, by means of internal improprieties prevention solutions such as DLP, privilege control systems, and UEBA.

3. Vulnerability “Countermeasures against vulnerability of Public API which is increasing abruptly”

Tsuyoshi Itagaki, Security and Network Department, NTT DATA Japan

In recent years, use of Public API (Application Programming Interface) has been rapidly expanding along with the spread of cloud services and transition to micro service architectures, and it is one of the essential technologies which support business growth of enterprises. At the same time, however, vulnerability of Public API also has been increasing, as such, threats of cyber attacks aiming at it are increasing as well. For service providers of Public API, building up of appropriate security measures is essential. In this report, we explain the threats in relation to the fast growing use of Public API and the security measures for which service providers of Public API are required.

3.1. Cyber attacks to Public API

API itself is not necessarily a new technology, as it has been used from the early days of computer technologies. Nevertheless, along with spread of cloud services and transition to micro service architectures, the use of API, specifically the use of Public API accessible through Internet has been rapidly expanding. The use of Public API facilitates linking between systems, which offers an advantage such as speeding up of provision of services. On the other hand, cyber attacks targeting vulnerabilities of Public API are also increasing.

According to the report dated June 31, 2024 published by Akamai Technologies, Inc., cyber attacks to Public APIs and applications in the Asia-Pacific region has increased by 65% [11]. However, the awareness of business enterprises for security of Public API is still low and security measures are not yet sufficient, and a large risk is still carried. Public API involves the following risks by cyber attacks:

- **Unauthorized access:**
  Attacks by accessing Public API illegally through stealing credential data. In many cases, unauthorized accesses are achievable due to incorrect setting of access policies.
- **Brute-force attack:**
  Attacks to login illegally using trial and error to crack passwords
- **Injection attack:**
  Attacks which inject malicious code into Public API, such as SQL injection and Cross-site Scripting (XSS)
- **DDoS attack:** Attacks which send a huge number of requests to cause overload of Public API to result interruption of services
- **Layer 7 DDoS attack:**
  DDoS attacks which target the application layer Attackers send a huge number of HTTP requests or use a certain function of web application excessively to suppress processing capacity of web servers or application servers, to disrupt provision of services, and so on. It can cause severe impact even with small amount of traffics
- **API Exploit:**
  Attacks which exploit business logic of API to attempt illegal operations

In the past, data leakages have occurred in many business enterprises and organizations including Facebook and X (ex-Twitter), due to cyber attacks described below which have exploited vulnerability of Public API. According to “Cost of a Data Breach Report 2023” by IBM [12], data breach from Public API causes 10 times as much damage when compared with other data breach due to other security breach.

(1) During the period from June, 2021 to January, 2022, the attacker illegally obtained account information of X (ex-Twitter) by exploiting Zero-day vulnerability of Public API of X. The attacker entered mail address and telephone number of the target user to Public API of X and obtained ID of the user. Using the ID obtained, the attacker thieved 5.4 million of published account information (ID, name, user name, locational information, authentication status, telephone number, and mail address). The attacker sold the thieved account information in a hacking forum, then, after that disclosed them in free of charge [13].

(2) On February 15, 2024, an attacker logged into Facebook illegally due to defect of authentication of password reset process, and took over the account of user. Using Public API, the attacker requested password reset. The system in Facebook sent a 6 digits authentication code for password reset to the regular user via notice of Facebook. The system in Facebook requested to enter 6 digits authentication code for password reset but it did not specify the upper limit of number of trials. The attacker tried all the patterns from 000000 to 999999 then logged in illegally to reset the password, then took over the account. From the account taken over, personal information of the user leaked, then phishing attacks and other fraudulent practices were executed [14].

Recently, it was suspected that persons concerned of DeepSeek thieved a mass of data in relation to Generative AI from OpenAI by exploiting Public API. [15]。 As such, exploiting Public API enables thieving a mass of data over a short period of time, therefore the vulnerability of Public API is a significant threat to business enterprises.

3.2. Vulnerability of Public API

Vulnerabilities frequently seen in Public API are defects in relation to setting of authentication and approval Also as reported in OWASP API Security Top 10 [16], vulnerabilities in relation to authentication and approval are high on the list. For instance, the first ranking in the report is the vulnerability called Broken Object Level Authorization (BOLA). BOLA is vulnerability in which an attacker can run the request message illegally by faking the user identifier of own API request message to the user identifier of a regular user and sending the message, since approval setting of object level is missing when a request message is sent to API. In many data breach incidents in relation to Public API, this BOLA has been exploited.

Here, we describe cyber attacks exploiting BOLA based on Fig.3-1. Once an account is authenticated and access to Public API is approved, a normal user, Mr. YYY obtains his own profile information by sending a request message to the Public API using own message ID “YYY”. Similarly, a normal user Mr. ZZZ uses his own message ID “ZZZ” and obtains own profile information. A malicious user XXX sends a request message using the message ID of the other person, “YYY” or “ZZZ” instead of own message ID “XXX” after authenticated, and can obtain the profile information of other persons illegally.

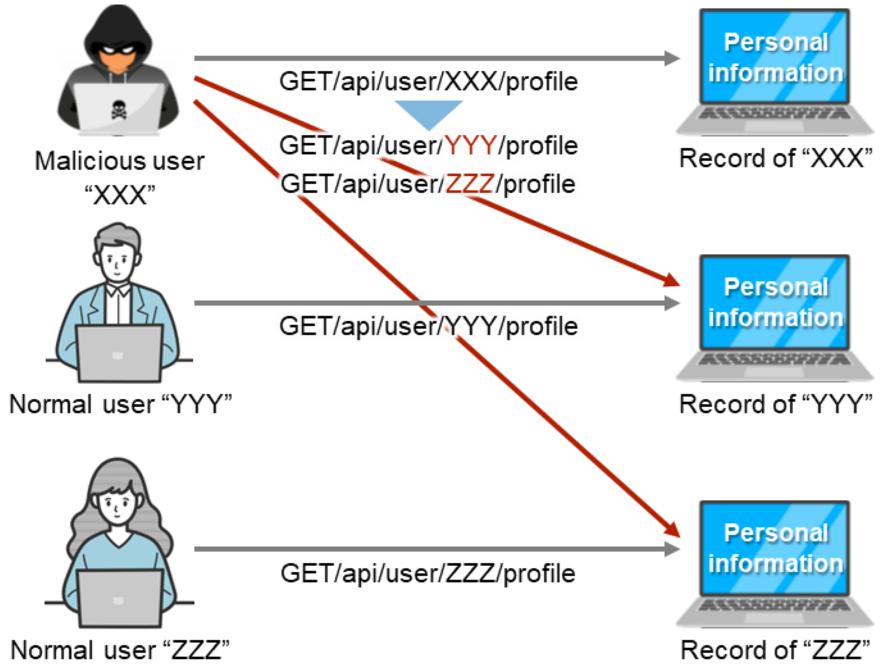


Fig.3-1: Example of cyber attack in which vulnerability of BOLA is exploited

As such, since cyber attacks exploiting vulnerability of Public API just generate request messages and send to Public API automatically using a program, they are capable of executing large numbers of cyber attacks over a short period of time. In case of a cyber attack other than cyber attacks to Public API, for instance, an attacker attacks vulnerability of VPN equipment, and once she/he obtains ID and password enabling VPN connection, she/he enters inside of the network manually via VPN. Looking into the internal network, once the attacker finds the target AD server or database server for attacking, she/he logs in the server illegally through another cyber attack to thieve sensitive information, to run ransomware, etc. When compared with such cyber attack methods, cyber attacks to Public API require less manual operation. The feature also involves occurrence of serious damage in a short period, since it is possible to thieve a mass of sensitive information with a small amount of tasks.

3.3. Security measures for Public API

Service providers of Public API take security measures so that it is avoided that vulnerability is generated within Public API during the development of the system. An approach, "Secure by Design" which considers security at the design stage of a system and an application to prevent vulnerability beforehand are security measures against generation of vulnerability We introduce strategic practices for security measures to reinforce API which system developers and organizations can adopt, as follows [17] [18]:

- **Implementation of authentication and approval:**
  When Multi-factor Authentication (MFA), OAuth 2.0, or authentication method by means of API key is used, it is necessary that respective schemes are comprehended to design and implement in a safe way. Setting must be conducted such as scope for setting authentication, detailed access permission setting based on Role-based Access Control (RBAC), and setting of valid terms for access token
- **Runtime protection:**
  A series of security measures to protect running API in real time. It verifies data received at API strictly and prevents attacks such as SQL injection and Cross-site Scripting (XSS). It conducts restriction of the number of requests to API and verification of tokens. It monitors API in real time and detects suspicious access, abnormal patterns, and abnormal behaviors and responds to them. It monitors attack patterns from attackers and blocks abnormal requests
- **Security tests:**
  Security tests are conducted in the earlier stages of a development process, to identify vulnerabilities of API and respond to it. Security tests

are integrated into CI/CD pipeline

- **Security posture management:**
  The vulnerability hidden behind the setting of Public API or its implementation should be assessed and amended
- **Cataloging of APIs and document control:**
  Inventory of all the APIs must be prepared and maintained to control APIs efficiently. Detailed API documents must be prepared and controlled
- **API governance and API security:**
  Policies of API governance and API security must be developed and the design, implementation, and deployment operation of the API must be controlled. Necessary elements for the above mentioned security measures for API must be added to the policy, including policy for design and implementation of APIs, policy for security measures, security tests, security posture management, and API catalog

Security engineers familiar with secure design and secure coding must join in the upstream process of design and development phase, to make sure of implementing the strategic practices of the above mentioned security measures, being conscious of security measures from the early stage of API development. In addition, to prevent generating vulnerability into API beforehand, Shift Left security strategy must be adopted proactively. When a vulnerability is found, the cause and timing that the vulnerability was generated must be identified, to take measures against the generation of vulnerability, in the upstream process.

Nevertheless, even using Secure by Design, it is still difficult to completely eliminate vulnerability. In the actual development sites, not only generating vulnerability by mistake, but also issues which are substantial, such as involving “Zombie API” which is no more required and must actually be deleted but forgotten and left, or “Shadow API” developed to streamline development and operation though it breaks the rule. It is not possible to solve issues such as Zombie API and Shadow API just by means of API governance and API security. Executing API discovery enables to identify APIs that the business enterprise possesses and then catalog them; thus, it is possible to identify Zombie API and Shadow API.

Another method is also available to reinforce API security by introducing advanced tools and solutions. Specifically, API gateways and API platforms. API gateway unifies management of accesses to API and executes authentication, rate limit, and record of logs of request, and so on [19]. API platform is a foundation to publish and manage APIs for business enterprises and organizations which provide APIs. It also offers security functions for protection of API, including authentication using API keys and tokens, and IP filtering. It is a useful tool that business enterprises and organizations which provide APIs can streamline publishing and management of APIs, while developers using APIs can search APIs [20].

3.4. Summary

In this article, we explained the threats associated with the growing use of Public APIs and the security measures that service providers of Public API are required. Specifically, we introduced examples in which vulnerabilities of APIs in X and Facebook were exploited in environments where cyber attacks were increasing, such as unauthorized accesses, injection attacks, DDoS attacks, and exploit of API. Particularly, in Public API, improper configurations with regard to authentication and approval occur frequently, where vulnerabilities such as Broken Object Level Authorization (BOLA) are exploited and a volume of information is leaking.

As such, we proposed to employ the Secure by Design approach so that security was integrated from the initial stage of development. Also, we recommended security measures including Implementation of authentication/approval and runtime protection, development of policies for API governance and API security, as well as proactive Shift Left security strategy.

Nevertheless, we still have issues even Secure by Design is not capable of solving. To solve such issues, introduction of API discovery, application of automated security tools, and reinforcement of security training are required. Efforts are desired to prevent generation of vulnerabilities beforehand, by reinforcing security training to developers and operation members and consciously enhancing security. When these policies are adopted and security for Public API is reinforced, it is possible to provide safer Public APIs.

4. Vulnerability "Improvement of Vulnerability triage approach using SSVC"

Naoki Murata, NTTDATA-CERT, Information Security Office, NTT DATA Group

Due to sophistication of cyber attacks and complication of system environments, vulnerability management is now a significant action assigned to ensure security of organizations. Along with increased number of published vulnerability information, organizations are required to introduce efficient and adequate vulnerability management methods. In this writing, we pick up frameworks in relation to priority assessment for response to vulnerabilities, called SSVC (Stakeholder-Specific Vulnerability Categorization). SSVC is also leveraged in the Cybersecurity and Infrastructure Security Agency (CISA) of the United States Department of Homeland Security (DHS), and will potentially be the standard of vulnerability triage in future. For members dealing with vulnerabilities of each system to which vulnerability triage approach is introduced, it may be valuable sometime in the future to deepen the understanding of SSVC from the current stage. Citing this framework as an example, we dig into the challenges we faced at the time we discussed our management policy for vulnerabilities in the internal project as well as considering them, and sort out the points to study when assessing priority of response to vulnerabilities.

4.1. Increase in the volume of vulnerability information and its impact

Recently, the number of vulnerability information disclosures has been increasing, and as a result, the study of methods to manage large amounts of vulnerability information has become an important issue. [21]. On the background of such action assignments, the system environments are getting more complex along with advancement of technologies, and cyber attack methods are becoming more diversified. Owing to an increase in number of vulnerability information published, challenges occur for persons in charge of vulnerability response for each system. If the person in charge is not an expert in the security field, or is too busy with their daily work to devote sufficient resources to vulnerability management, it may be difficult to properly determine the priority of vulnerability response, and vulnerability response may end up being put off. Such cases are not exceptional even among the projects of our company. So that projects at site can actually implement vulnerability management, the operation flow must be such that anyone even without expert knowledge can deal with it efficiently.

In this writing, we introduce an example where we introduced a method to a project, to assess priority of countermeasures based on vulnerability information, applying a framework called SSVC (Stakeholder-Specific Vulnerability Categorization). SSVC is a method which uses a decision tree to enable judgement for priority of responses to vulnerabilities mechanically. When the structure of a decision tree of SSVC is comprehended, identification of the point at which determination of priority was failed, as well as amendment of it will be easier. Leveraging this SSVC, we sorted out the steps to assess priority for responses based on vulnerability information. In the process, we faced several challenges, as such, here, we explain the way to use and the point of view of SSVC which we sorted out at those times.

4.2. Improvement of steps to assess vulnerability

4.2.1. Problems of Common Vulnerability Scoring System (CVSS)

In a project within our company, to sort out the criteria of triage for vulnerabilities, we applied a framework called SSVC (Stakeholder-Specific Vulnerability Categorization) [22] [23]. The conventional system for assessment of seriousness of vulnerability, CVSS (Common Vulnerability Scoring System) [24] contains 3 issues.

1. From the CVSS score, the method to respond to the vulnerability is not known:
   Although it is possible to output CVSS score which indicates seriousness of the vulnerability, the person in charge of responding to vulnerability cannot decide specific responding policy from these values. From CVSS score (seriousness), CVSS does not suggest any specific policy such as time limit for responding to vulnerability, or easy-to-understand countermeasures.
2. The calculation method is complicated and correction or amendment of CVSS scores is difficult:
   Since calculating the formula of CVSS is complicated, it is not possible to understand the relationship between vulnerability assessment items and CVSS scores. Consequently, correction or amendment of CVSS scores is difficult: Still, it also relates to the 1st point, for instance, when a conversion table is defined between CVSS scores and the time limit for responding to vulnerability, it is possible to determine the time limit for responding to vulnerability from the CVSS score. Using the table, it is possible to determine, “Since vulnerability assessment items AV: N and PR: N are xxxx, CVSS score is 10.0. Consequently, a response to vulnerability within is required12 hours.” However, the person in charge of vulnerability management cannot understand the structure which determines that the time limit for responding is 12 hours at the maximum, based on vulnerability assessment items, such as AV and PR. When it is considered intuitively that the result, 12 hours at the maximum, is not adequate, identifying incorrect vulnerability assessment item such as AV and PR and amending such values are no easy matters.
3. Reevaluation based on the current evaluation standards and environmental evaluation standards is difficult:
   As for CVSS scores for current assessment standards, at a change of the result of verification on the actual system for existence of damage due to vulnerability, or a change of epidemic situation of cyber attacks aiming at vulnerabilities, it is necessary to collect such information and re-calculate it. As for CVSS scores for environmental evaluation standards, when the condition of the system in relation to vulnerability changes, such as change in system environment characteristics, it is necessary to collect such information and re-calculate it. The information that must be collected to recalculate the CVSS scores for these two metrics may not be readily available or may be tedious and time-consuming.

4.2.2. Solution of problems by applying SSVC

Applying SSVC, it is possible to solve these 3 issues of CVSS. SSVC is a framework capable to determine the priority of vulnerabilities and responding policy per respective stakeholders responding to vulnerabilities such as vendors supplying patches and users applying patches. SSVC uses a decision tree (refer to Fig.4-1) to assess factors such as effect of vulnerabilities and mitigation measures, then indicates 4 grades of priority for response, i.e., “Defer (no response)”, “Scheduled (periodic response)”, “Out-of-cycle (rapid response)”, and “Immediate (emergency response)”. Fig.4-1 is the decision tree, “Deployer Tree” which is used by the organizations and system administrators conducting installation, setting, operation, and maintenance of software and systems. The person in charge of responding to the vulnerability of respective stakeholders can understand the process for determination of priority to respond to vulnerabilities visually and logically, when she/he sees the decision tree. [25], [26].

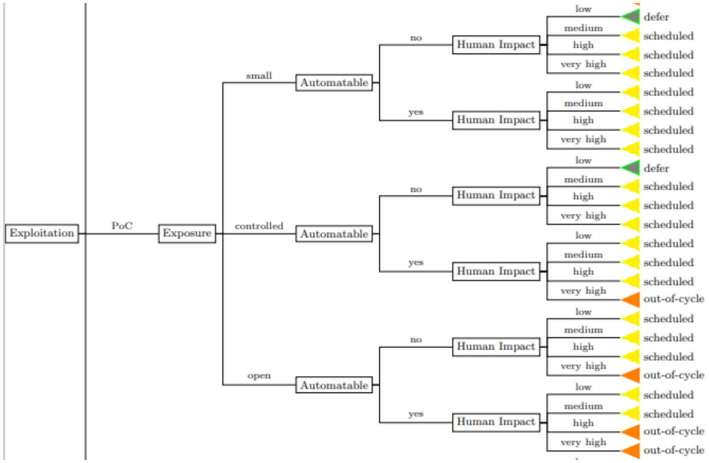


Fig.4-1: Decision tree of SSVC v2.1 Deployer Tree (only Exploitation=PoC branches are extracted) [22]

The 1st point "From the CVSS score, the method to respond to the vulnerability is not known:" is solved when SSVC is used. SSVC uses a decision tree and outputs priority to respond to vulnerabilities, but not the value of seriousness of vulnerabilities. Priority to respond to vulnerability of SSVC is in 4 grades, "Immediate", "Out-of-cycle", "Scheduled", and "Defer", from higher priority. The priority to respond to vulnerabilities in 4 grades is described below: When the person in charge of responding to vulnerabilities of each system deals with vulnerabilities based on the priority determined in SVCC, she/he can solve the issue.

Table 4-1: Priority in responding to vulnerabilities

No.	Priority in responding to vulnerabilities	Description
1	Defer	No response at this moment
2	Scheduled	Response during periodic maintenance work
3	Out-of-cycle	Mitigation measures or correction measures are applied rapidly
4	Immediate	Correction measures are applied as immediately as possible. Normal operation may be interrupted when necessary

The 2nd point "Calculation method is complicated and correction or amendment of CVSS scores is difficult": is solved thanks to the characteristics of SSVC that process of introduction of the decision tree is clearly specified. Understanding the structure of a decision tree makes it possible to check, identify and correct mistakes.

The 3rd point "Reevaluation based on the current evaluation standards and environmental evaluation standards is difficult": is solved when the decision tree is used, similarly to the 2nd point. The decision tree of SVCC contains items indicating network connection status of the system. In case that the connection status of network changes, it is possible to determine priority to respond to vulnerabilities by just revising the elements from the decision point which is the branch point for the section of the decision tree using the item, without the necessity of a complicated re-calculation.

4.2.3. Method to determine 2 decision points

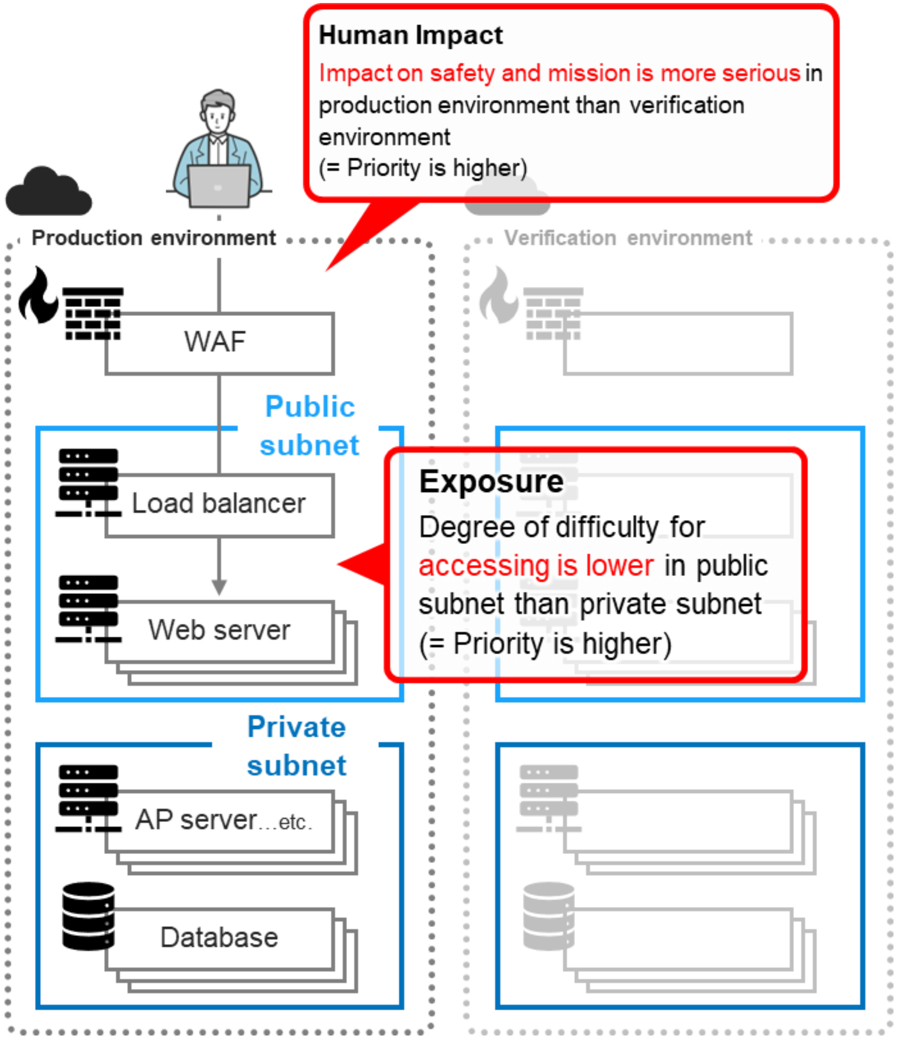
From here forward, we explain the method to determine 2 of the 4 decision points of SSVC (refer to Table4-2), Exposure and Human Impact, using specific examples.

Table4-2: Decision point of SSVC v2.1) [22]

Decision points		Description
Exploitation		Assesses situation of exploiting of vulnerabilities (or potential exploiting)
Exposure		Assesses degree of external exposure of the system
Automatable		Assesses whether automation of attacking is possible or not
Human Impact		Combines Situated Safety Impact and Mission Impact then assesses them
	Situated Safety Impact	Assesses physical safety and health risk
	Mission Impact	Assesses impact on important business processes and missions

(1) Examples of a system used for description

Examples of a system used for description here include 2 cases. Case 1 is a system built up on a public cloud as shown in Fig.4-2 which consists of 2 environments, production and verification. Case 2 is a system built up on on-premise foundation.



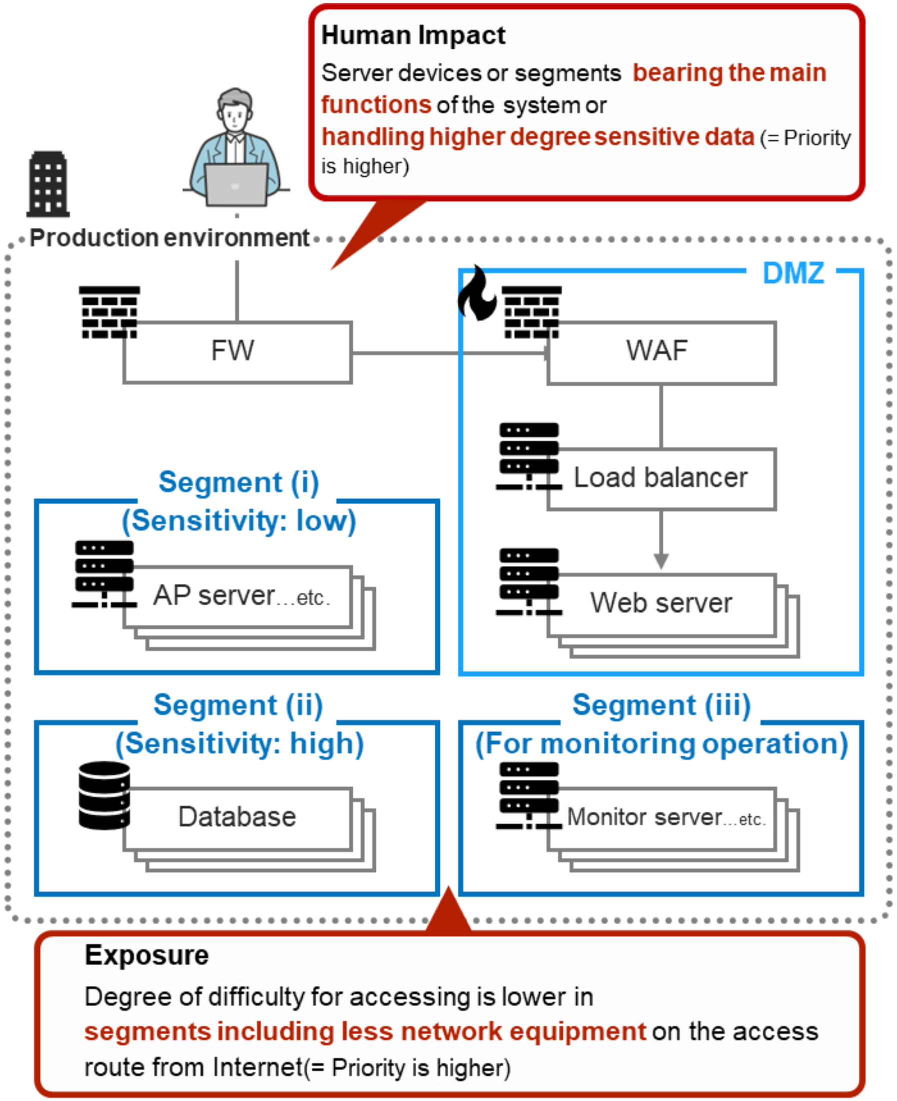
Human Impact

Impact on safety and mission is more serious in production environment than verification environment (= Priority is higher)

Exposure

Degree of difficulty for accessing is lower in public subnet than private subnet (= Priority is higher)

Fig.4-2: Case 1 System on public cloud (outline)


Production environment
FW
DMZ
WAF
Load balancer
Web server
Segment (i) (Sensitivity: low)
AP server…etc.
Segment (ii) (Sensitivity: high)
Database
Segment (iii) (For monitoring operation)
Monitor server…etc.

Human Impact

Server devices or segments **bearing the main functions** of the system or **handling higher degree sensitive data** (= Priority is higher)

Exposure

Degree of difficulty for accessing is lower in **segments including less network equipment** on the access route from Internet(= Priority is higher)

Fig.4-3: Case 2 System on on-promise foundation (outline)

(2) Method to determine Exposure of SSVC

Exposure indicates the degree of difficulty for accessing from Internet online to servers and network equipment or software involving vulnerability (refer to Table4-3). The degree includes “Open”, when direct access from Internet is allowed, “Controlled” when direct access from Internet is not allowed except when access is controlled using a firewall and such, and “Small” which exists in the closed area isolated from Internet.

In the system on public cloud as shown in Fig.4-2, load balancers and Web servers placed on the public subnets are determined as “Open”. AP servers/Web applications and database placed on private subnets are determined as “Controlled”.

In the system on on-premise foundation as shown in Fig.4-3, web servers and network equipment placed on DMZ are determined as “Open” since these are accessible directly from Internet, and other servers in internal segments are determined as “Controlled” since access control is enabled by means of a Firewall, etc. The easier the access to servers and network equipment or software involving vulnerabilities from Internet is for attackers, the higher the risk is, therefore, the priority to respond to vulnerabilities is also higher.

Table4-3: Assessment value of Exposure [22]

No.	Assessment value	Description
1	Open	Networks for which restriction or control of Internet or access is potentially disabled
2	Controlled	Networks for which access restriction or mitigation measures are implemented
3	Small	Closed area environment with no input from or output to Internet

(3) Method to determine the Human Impact of SSVC

The Human Impact is expressed as a result of multiplication of “Situated Safety Impact” which shows impact on safety when vulnerabilities are exploited, by “Mission Impact”, the impact on the mission of organization, as shown in Table4-2.

(i) Situated Safety Impact :

Situated Safety Impact assesses the impact that vulnerabilities give to 4 “Harm Categories”, i.e., “Physical Harm”, “Environment Harm”, “Psychological Harm” and “Financial Harm” in 5 grades, as shown in Table4-4. The assessment value of the largest impact among these 4 Harm Categories is applied as Situated Safety Impact. For instance, when a vulnerability lies in a life-threatening system such as for hospitals and aviation, the impact of Physical Harm is apt to be the largest, thus its assessment value of this Physical Harm is adopted in many cases. In the case of a system for basic infrastructure such as electricity or running water, the impact of the environment is large, thus the assessment value is adopted in many cases.

Table4-4: Harm categories and assessment value of Situated Safety Impact [22]

Harm categories (Harm Categories)	Description	Assessment value
Physical Harm	Physical impact on system users	1. None 2. Minor 3. Major 4. Hazardous 5. Catastrophic
Environment	Impact on the external environment including risks in relation to natural environment and public health	
Financial	Financial loss of stakeholders	

Psychological	Psychological harm to stakeholders	

(ii) Mission Impact :

Mission Impact accesses the impact of vulnerabilities on a mission of organization, as shown in Table4-5. Degree of impact that vulnerabilities give on functions necessary to achieve a mission is assessed in 4 grades as listed in Table4-5.

Table4-5: Assessment value of Mission Impact [22]

No.	Assessment value	Description
1	None, Degraded	Almost no impact. Degradation of non-mandatory functions may potentially damage essential functions eventually
2	Crippled	Activities to directly support essential functions fail to function properly
3	MEF Failure	Any of the functions indispensable for missions exceeds tolerable range and fails to function over a long period of time.
4	Mission Failure	Mandatory functions of more than one or all of the missions fail

Once the assessment values of Situated Safety Impact and Mission Impact are fixed, the assessment value of Human Impact is determined based on the combination. The determination logic to fix the assessment value of Human Impact based on combination of respective assessment values of Situated Safety Impact and Mission Impact must be prepared beforehand. For instance, in case where the Situated Safety Impact is “Major” and Mission Impact is “Mission Failure”, it must be determined that the impact which vulnerabilities have on human and environment is extremely large, thus the assessment value of the Human Impact is determined as “Very High” [27].

Table4-6: Assessment value of Human Impact [22]

No.	Situated Safety Impact	Mission Impact	Human Impact	Description
1	None/Minor	None/Degraded/ Clippled	Low	Almost no impact
2	None/Minor	MEF Failure	Medium	No impact on mission-critical tasks
	Major	None/Degraded/ Clippled		
3	Major	MEF Failure	High	A prolonged impact is given on one of the mission-critical tasks
	Hazardous	None/Degraded/Clippled/MEF Failure		
4	None/Minor/Major/ Hazardous	Mission Failure	Very High	More than one mission-critical tasks stops resulting in that mission-critical tasks are disabled to continue and unrecoverable
	Catastrophic	None/Degraded/Clippled/MEF Failure/ Mission Failure		

4.3. Optimization of vulnerability assessment procedure

4.3.1. Action assignments after the introduction of SSVC

In a particular project, when this SSVC was applied as is and the procedure to response to vulnerabilities was sorted out, action assignments described below emerged:

When compared with CVSS, the vulnerability assessment flow of SSVC is simpler and easier to understand, nevertheless, for SVCC, some indefinite part still remains in the definition of assessment standard depending on the system characteristics. If this ambiguity cannot be addressed, there is a risk that the decision points at which the decision tree branches will be judged incorrectly, resulting in incorrect priorities being determined.

Then, to determine priority to respond to vulnerabilities, the person in charge of responding to vulnerabilities has to check the status of network connection per each server, search past occurrences of cyber attacks exploiting vulnerabilities, and so on. However, in case that the number of servers is large, the person in charge of responding to vulnerabilities alone does not have enough time to check all the servers. For instance, as for the vulnerability of regreSSHion [28] occurred in the 2nd quarter of 2024, more than one server within the system were impacted.

The person in charge of responding to vulnerabilities has to search past occurrences of cyber attacks exploiting vulnerabilities. Nevertheless, there may be a case where the person in charge of responding to vulnerabilities does not know the way to collect information on the situation of exploiting of vulnerabilities.

Examples of action assignments which affect priority in responding to vulnerabilities of SSVC are as follows:

1. It was failed to define the scope and impact on business of target systems for assessment
2. The person in charge of responding to vulnerabilities has no time to check all the servers alone.
3. It is difficult to obtain external information on situations of exploiting of vulnerabilities, and such

4.3.2. Detailed examination of assessment targets and solution of action assignments

We describe the way to solve the issue of Action assignment 2, “The person in charge of responding to vulnerabilities cannot check the servers alone”, particularizing the assessment methods for Exposure and Mission Impact.

(1) Solution of the action assignments by particularizing Exposure

If the person in charge of responding to vulnerabilities cannot check all or more than one server alone, we recommend a way that more than one server, network equipment and software are grouped so that priority in responding to vulnerabilities is determined per each group.

Since SSVC is a flexible framework, it is allowed to determine the scope of application of Exposure freely. As shown in Fig.4-2 and Fig.4-3, assessment targets are grouped beforehand per degree of difficulty for accessing, depending on communication protocols from Internet online to servers and network equipment or software, etc. Preferentially, from the group that the assessment value of Exposure with higher risk for exploiting vulnerabilities is Open, priority in responding to vulnerabilities is determined using a decision tree. If it is desirable to determine priority in responding to vulnerabilities per a unit of servers and network equipment or software, priority in responding to vulnerabilities must be determined once again per unit of servers and network equipment or software using a decision tree, in the order beginning from the group with higher priority in responding to vulnerabilities.

(2) Solution of the action assignments by particularizing Mission Impact of Human Impact

The action assignment 1, “It has failed to define the scope and impact on business of target systems for assessment" can be solved by particularizing Mission Impact of Human Impact", in addition to Exposure. Mission Impact may vary depending on servers and network equipment configuring the system. For instance, the assessment values of Mission Impact are different between production environment and verification environment. The impact would be larger in the production environment, since it could lead to many of users being disabled from using the system when the service is interrupted due to vulnerability. Even as for servers and software configuring the production environment, the assessment values of Mission Impact vary between the segment applicable to implementation of the function requirement of the system and the segment applicable to the non-function requirement. For instance, log management servers and operation monitoring servers are applicable to non-functional requirement, as such direct impact on the main function of the system is nothing serious even if these are affected by vulnerability. Consequently, the assessment value of Mission Impact is None or Degraded.

When Mission Impact has been assessed beforehand per unit of servers and network equipment or unit of software and program, there is no occasion that the action assignment 1 causes a problem. Even in case where it was failed to prepare the assessment value of Mission Impact beforehand, when Mission Impact is assessed in order from the group with higher priority in responding to vulnerabilities of Exposure, it is possible to determine priority in responding to vulnerabilities in order from the segment with the higher risks.

4.4. Summary

When vulnerabilities are assessed using SSVC, it is possible to determine 4 grades priority in responding to vulnerabilities. However, there may be a case that it is not possible to carry out sufficient assessment due to lack of information on situations of exploiting vulnerabilities. Otherwise, there may be a case that it is not possible to determine priority in responding to vulnerability of all the devices because of a large number of servers and network equipment or software in the system. In such cases, it is possible to streamline the task to determine the priority if the method to assess Exposure and Mission Impact is particularized such that servers and network equipment or software are grouped depending on the condition of access control of the network, or Mission Impact is assessed individually.

Particularly, in accordance with rapidly evolving AI technologies, it is becoming more common that attack codes and attack tools exploiting vulnerability are developed in shorter cycles, once vulnerability is published. In such a situation, swiftness of response to vulnerability is more important. As such, when servers, network equipment, and software in relation to Exposure and Mission Impact are grouped and assessment values are prepared beforehand as specified in this article, and then priority for countermeasures against vulnerability is determined using SSVC, it is possible that fewer members deal with the task. Such particularization and preliminary preparation would be the key to enhance ability to respond to vulnerabilities.

5. Timeline

Yuhei Terashi, NTTDATA-CERT, Information Security Office, NTT DATA Group
Ryotaro Tanaka, NTTDATA-CERT, Information Security Office, NTT DATA Group

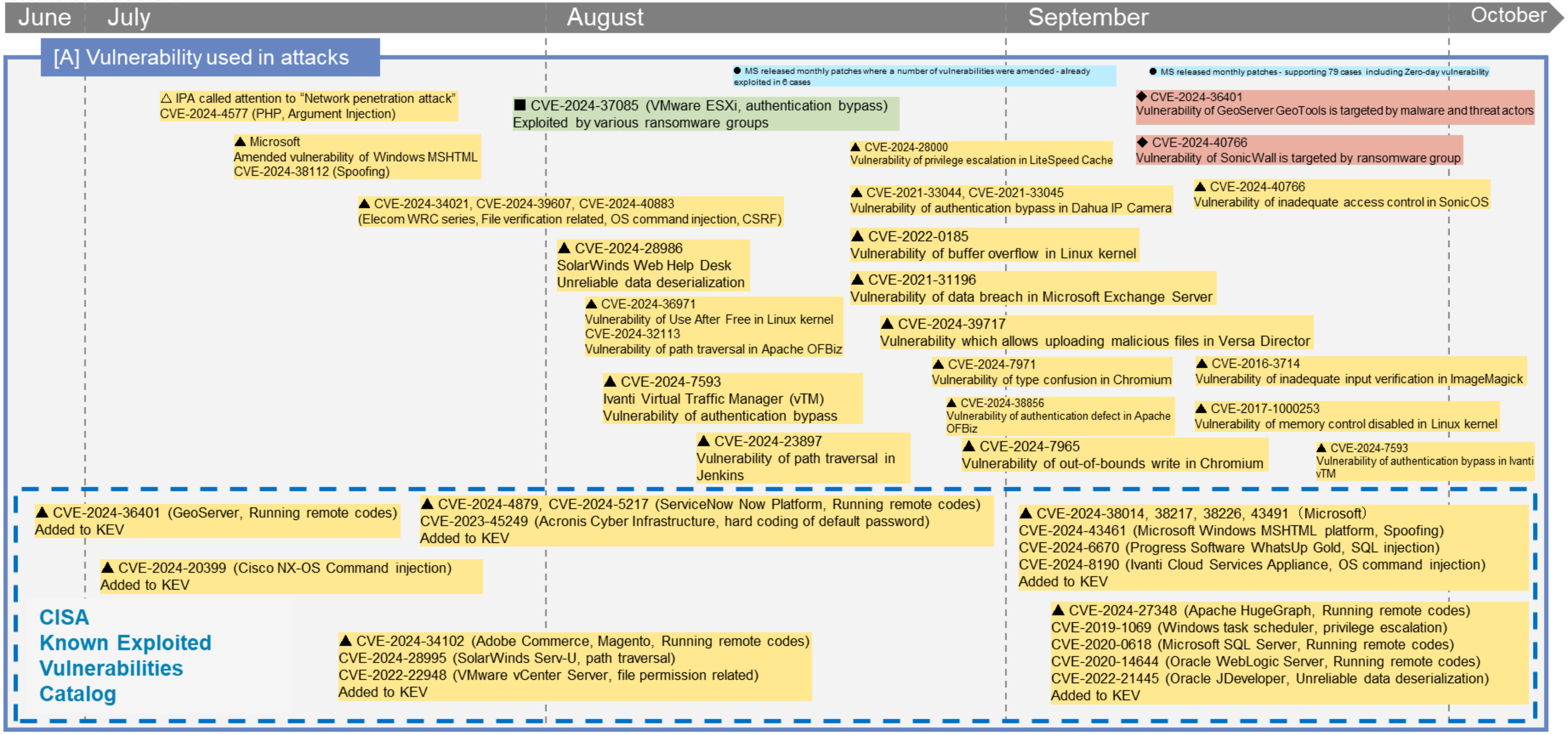
In the category of [A] Vulnerability used in attacks in the 2nd quarter of 2024, what was distinguishing was the news that a cyber attack occurred only 22 minutes after the announcement of PoC for vulnerability. Further, in categories other than vulnerability, relatively a lot of news on password list attacks were found. As for events in relation to AI also picked up in the Timeline in the 1st quarter of 2024, there was news on increase of business email compromise by means of Generative AI.

* There may be cases that the date indicated in Timeline is date as of posting but not as of occurrence of the event.

△□◇○: Domestic
▲■◆●: Common all over the world, Overseas

△▲: Vulnerability
□■: Incidents/accidents

◇◆: Threat
○●: Countermeasure



June July August September October

[A] Vulnerability used in attacks

△ IPA called attention to "Network penetration attack"
CVE-2024-4577 (PHP, Argument Injection)

▲ Microsoft
Amended vulnerability of Windows MSHTML
CVE-2024-38112 (Spoofing)

▲ CVE-2024-34021, CVE-2024-39607, CVE-2024-40883
(Elecom WRC series, File verification related, OS command injection, CSRF)

■ CVE-2024-37085 (VMware ESXi, authentication bypass)
Exploited by various ransomware groups

▲ CVE-2024-28986
SolarWinds Web Help Desk
Unreliable data deserialization

▲ CVE-2024-36971
Vulnerability of Use After Free in Linux kernel
CVE-2024-32113
Vulnerability of path traversal in Apache OFBiz

▲ CVE-2024-7593
Ivanti Virtual Traffic Manager (vTM)
Vulnerability of authentication bypass

▲ CVE-2024-23897
Vulnerability of path traversal in Jenkins

● MS released monthly patches where a number of vulnerabilities were amended - already exploited in 6 cases

▲ CVE-2024-28000
Vulnerability of privilege escalation in LiteSpeed Cache

▲ CVE-2021-33044, CVE-2021-33045
Vulnerability of authentication bypass in Dahua IP Camera

▲ CVE-2022-0185
Vulnerability of buffer overflow in Linux kernel

▲ CVE-2021-31196
Vulnerability of data breach in Microsoft Exchange Server

▲ CVE-2024-39717
Vulnerability which allows uploading malicious files in Versa Director

▲ CVE-2024-7971
Vulnerability of type confusion in Chromium

▲ CVE-2024-38856
Vulnerability of authentication defect in Apache OFBiz

▲ CVE-2024-7965
Vulnerability of out-of-bounds write in Chromium

● MS released monthly patches - supporting 79 cases including Zero-day vulnerability

◆ CVE-2024-36401
Vulnerability of GeoServer GeoTools is targeted by malware and threat actors

◆ CVE-2024-40766
Vulnerability of SonicWall is targeted by ransomware group

▲ CVE-2024-40766
Vulnerability of inadequate access control in SonicOS

▲ CVE-2016-3714
Vulnerability of inadequate input verification in ImageMagick

▲ CVE-2017-1000253
Vulnerability of memory control disabled in Linux kernel

▲ CVE-2024-7593
Vulnerability of authentication bypass in Ivanti vTM

CISA Known Exploited Vulnerabilities Catalog

▲ CVE-2024-36401 (GeoServer, Running remote codes)
Added to KEV

▲ CVE-2024-20399 (Cisco NX-OS Command injection)
Added to KEV

▲ CVE-2024-4879, CVE-2024-5217 (ServiceNow Now Platform, Running remote codes)
CVE-2023-45249 (Acronis Cyber Infrastructure, hard coding of default password)
Added to KEV

▲ CVE-2024-34102 (Adobe Commerce, Magento, Running remote codes)
CVE-2024-28995 (SolarWinds Serv-U, path traversal)
CVE-2022-22948 (VMware vCenter Server, file permission related)
Added to KEV

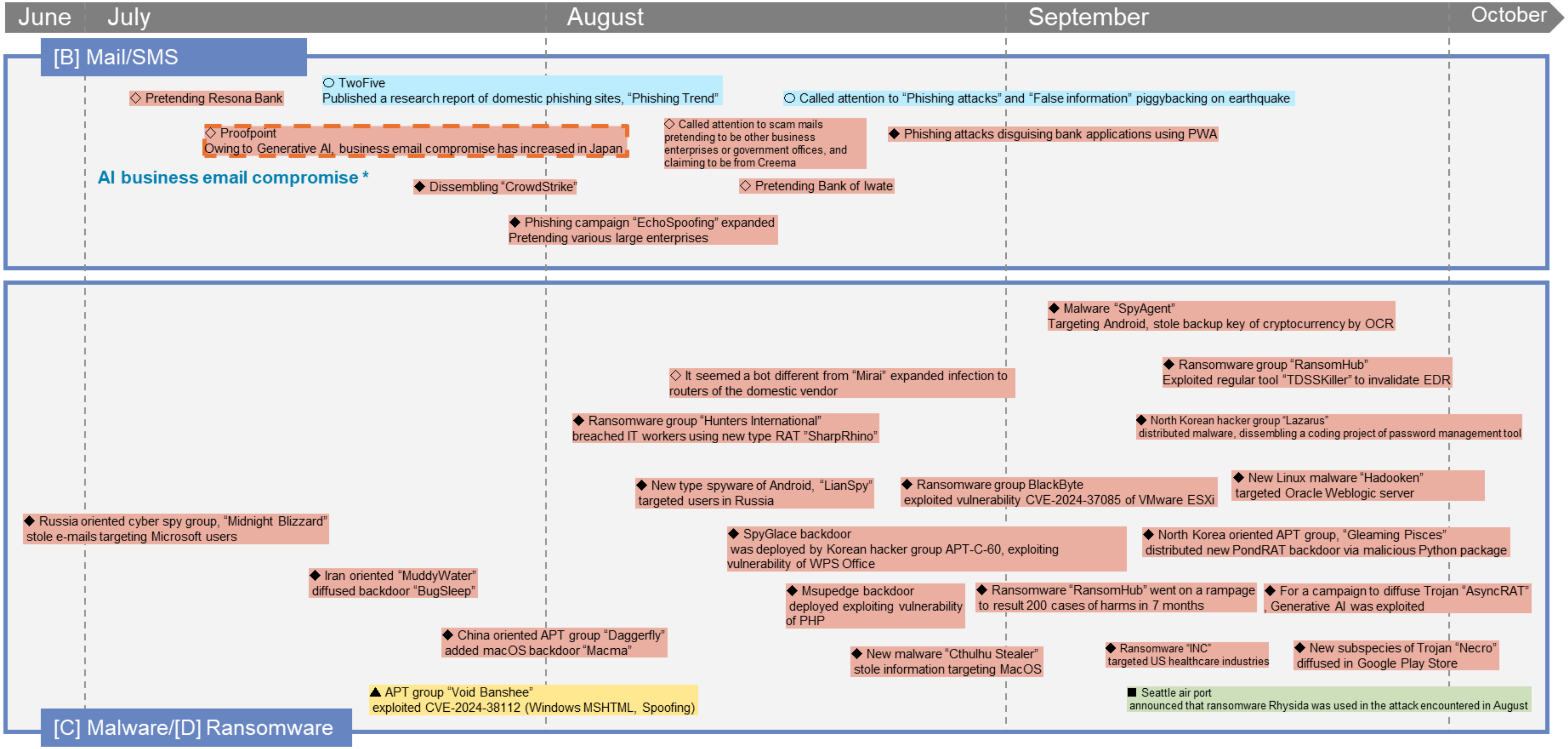
▲ CVE-2024-38014, 38217, 38226, 43491（Microsoft）
CVE-2024-43461 (Microsoft Windows MSHTML platform, Spoofing)
CVE-2024-6670 (Progress Software WhatsUp Gold, SQL injection)
CVE-2024-8190 (Ivanti Cloud Services Appliance, OS command injection)
Added to KEV

▲ CVE-2024-27348 (Apache HugeGraph, Running remote codes)
CVE-2019-1069 (Windows task scheduler, privilege escalation)
CVE-2020-0618 (Microsoft SQL Server, Running remote codes)
CVE-2020-14644 (Oracle WebLogic Server, Running remote codes)
CVE-2022-21445 (Oracle JDeveloper, Unreliable data deserialization)
Added to KEV

* There may be cases that the date indicated in Timeline is date as of posting but not as of occurrence of the event.

△□◇○: Domestic
▲■◆●: Common all over the world, Overseas

△▲: Vulnerability
□■: Incidents/accidents
◇◆: Threat
○●: Countermeasure



June July August September October

[B] Mail/SMS

◇ Pretending Resona Bank

○ TwoFive
Published a research report of domestic phishing sites, "Phishing Trend"

○ Called attention to "Phishing attacks" and "False information" piggybacking on earthquake

◇ Proofpoint
Owing to Generative AI, business email compromise has increased in Japan

AI business email compromise *

◇ Called attention to scam mails pretending to be other business enterprises or government offices, and claiming to be from Creema

◆ Phishing attacks disguising bank applications using PWA

◆ Dissembling "CrowdStrike"

◇ Pretending Bank of Iwate

◆ Phishing campaign "EchoSpoofing" expanded
Pretending various large enterprises

[C] Malware/[D] Ransomware

◆ Malware "SpyAgent"
Targeting Android, stole backup key of cryptocurrency by OCR

◆ Ransomware group "RansomHub"
Exploited regular tool "TDSSKiller" to invalidate EDR

◇ It seemed a bot different from "Mirai" expanded infection to routers of the domestic vendor

◆ Ransomware group "Hunters International"
breached IT workers using new type RAT "SharpRhino"

◆ North Korean hacker group "Lazarus"
distributed malware, dissembling a coding project of password management tool

◆ New type spyware of Android, "LianSpy"
targeted users in Russia

◆ Ransomware group BlackByte
exploited vulnerability CVE-2024-37085 of VMware ESXi

◆ New Linux malware "Hadooken"
targeted Oracle Weblogic server

◆ Russia oriented cyber spy group, "Midnight Blizzard"
stole e-mails targeting Microsoft users

◆ SpyGlace backdoor
was deployed by Korean hacker group APT-C-60, exploiting vulnerability of WPS Office

◆ North Korea oriented APT group, "Gleaming Pisces"
distributed new PondRAT backdoor via malicious Python package

◆ Iran oriented "MuddyWater"
diffused backdoor "BugSleep"

◆ Msupedge backdoor
deployed exploiting vulnerability of PHP

◆ Ransomware "RansomHub" went on a rampage
to result 200 cases of harms in 7 months

◆ For a campaign to diffuse Trojan "AsyncRAT"
, Generative AI was exploited

◆ China oriented APT group "Daggerfly"
added macOS backdoor "Macma"

◆ New malware "Cthulhu Stealer"
stole information targeting MacOS

◆ Ransomware "INC"
targeted US healthcare industries

◆ New subspecies of Trojan "Necro"
diffused in Google Play Store

▲ APT group "Void Banshee"
exploited CVE-2024-38112 (Windows MSHTML, Spoofing)

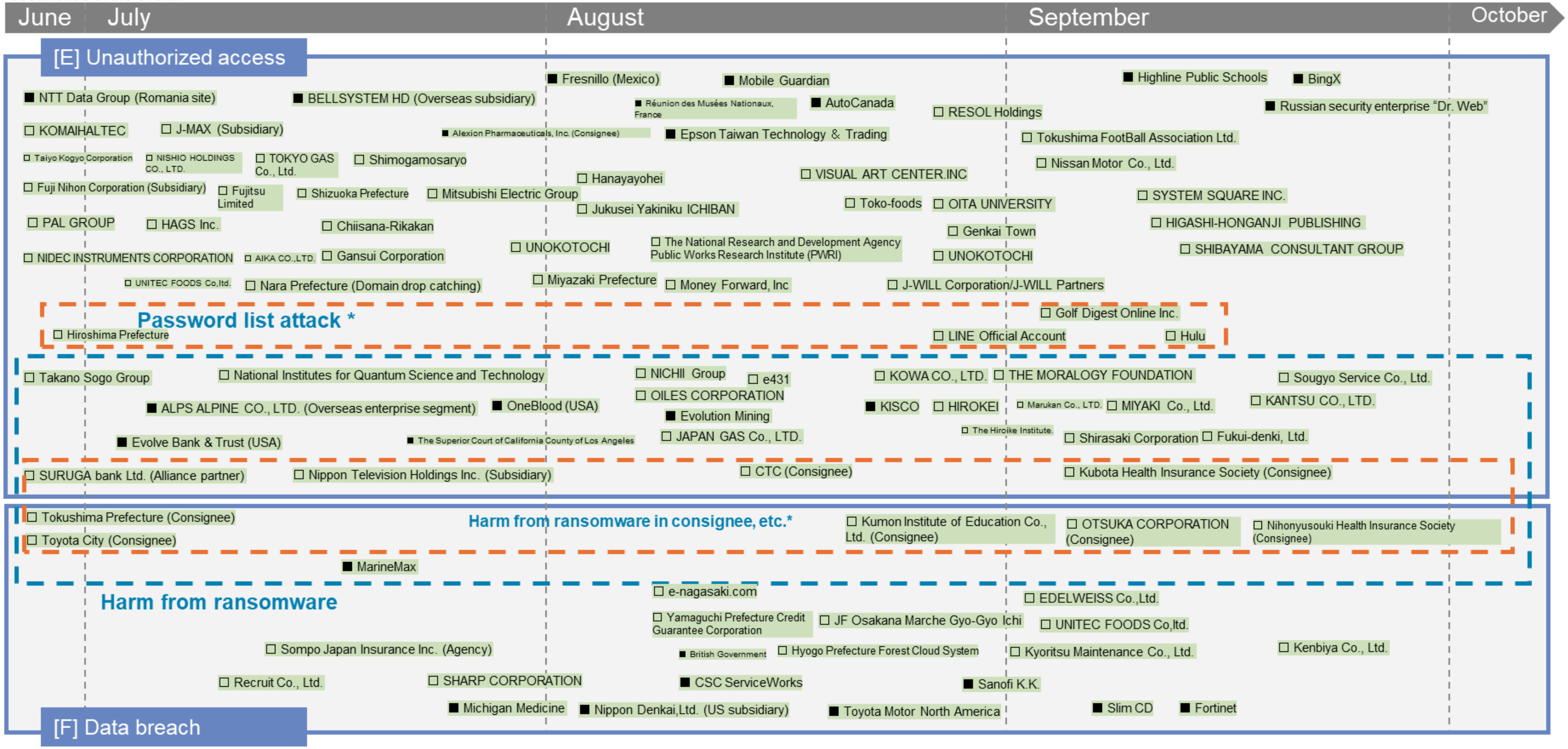
■ Seattle air port
announced that ransomware Rhysida was used in the attack encountered in August

* There may be cases that the date indicated in Timeline is date as of posting but not as of occurrence of the event.

△□◇○: Domestic
▲■◆●: Common all over the world, Overseas

△▲: Vulnerability
□■: Incidents/accidents

◇◆: Threat
○●: Countermeasure



June July August September October

[E] Unauthorized access

■ Fresnillo (Mexico) ■ Mobile Guardian ■ Highline Public Schools ■ BingX

■ NTT Data Group (Romania site) ■ BELLSYSTEM HD (Overseas subsidiary) ■ Réunion des Musées Nationaux, France ■ AutoCanada □ RESOL Holdings ■ Russian security enterprise "Dr. Web"

□ KOMAIHALTEC □ J-MAX (Subsidiary) ■ Alexion Pharmaceuticals, Inc. (Consignee) ■ Epson Taiwan Technology & Trading □ Tokushima FootBall Association Ltd.

□ Taiyo Kogyo Corporation □ NISHIO HOLDINGS CO., LTD. □ TOKYO GAS Co., Ltd. □ Shimogamosaryo □ Nissan Motor Co., Ltd.

□ Hanayayohei □ VISUAL ART CENTER.INC

□ Fuji Nihon Corporation (Subsidiary) □ Fujitsu Limited □ Shizuoka Prefecture □ Mitsubishi Electric Group □ SYSTEM SQUARE INC.

□ Jukusei Yakiniku ICHIBAN □ Toko-foods □ OITA UNIVERSITY

□ PAL GROUP □ HAGS Inc. □ Chiisana-Rikakan □ Genkai Town □ HIGASHI-HONGANJI PUBLISHING

□ NIDEC INSTRUMENTS CORPORATION □ AIKA CO.,LTD. □ Gansui Corporation □ UNOKOTOCHI □ The National Research and Development Agency Public Works Research Institute (PWRI) □ UNOKOTOCHI □ SHIBAYAMA CONSULTANT GROUP

□ UNITEC FOODS Co,ltd. □ Nara Prefecture (Domain drop catching) □ Miyazaki Prefecture □ Money Forward, Inc □ J-WILL Corporation/J-WILL Partners

Password list attack *

□ Hiroshima Prefecture □ Golf Digest Online Inc. □ LINE Official Account □ Hulu

□ Takano Sogo Group □ National Institutes for Quantum Science and Technology □ NICHII Group □ e431 □ KOWA CO., LTD. □ THE MORALOGY FOUNDATION □ Sougyo Service Co., Ltd.

□ OILES CORPORATION

■ ALPS ALPINE CO., LTD. (Overseas enterprise segment) ■ OneBlood (USA) ■ Evolution Mining ■ KISCO □ HIROKEI □ Marukan Co., LTD. □ MIYAKI Co., Ltd. □ KANTSU CO., LTD.

■ Evolve Bank & Trust (USA) ■ The Superior Court of California County of Los Angeles □ JAPAN GAS Co., LTD. □ The Hiroike Institute. □ Shirasaki Corporation □ Fukui-denki, Ltd.

□ SURUGA bank Ltd. (Alliance partner) □ Nippon Television Holdings Inc. (Subsidiary) □ CTC (Consignee) □ Kubota Health Insurance Society (Consignee)

□ Tokushima Prefecture (Consignee) Harm from ransomware in consignee, etc.* □ Kumon Institute of Education Co., Ltd. (Consignee) □ OTSUKA CORPORATION (Consignee) □ Nihonyusouki Health Insurance Society (Consignee)

□ Toyota City (Consignee)

■ MarineMax

□ e-nagasaki.com

Harm from ransomware □ EDELWEISS Co.,Ltd.

□ Yamaguchi Prefecture Credit Guarantee Corporation □ JF Osakana Marche Gyo-Gyo Ichi □ UNITEC FOODS Co,ltd.

□ Sompo Japan Insurance Inc. (Agency) ■ British Government □ Hyogo Prefecture Forest Cloud System □ Kyoritsu Maintenance Co., Ltd. □ Kenbiya Co., Ltd.

□ Recruit Co., Ltd. □ SHARP CORPORATION ■ CSC ServiceWorks ■ Sanofi K.K.

■ Michigan Medicine ■ Nippon Denkai,Ltd. (US subsidiary) ■ Toyota Motor North America ■ Slim CD ■ Fortinet

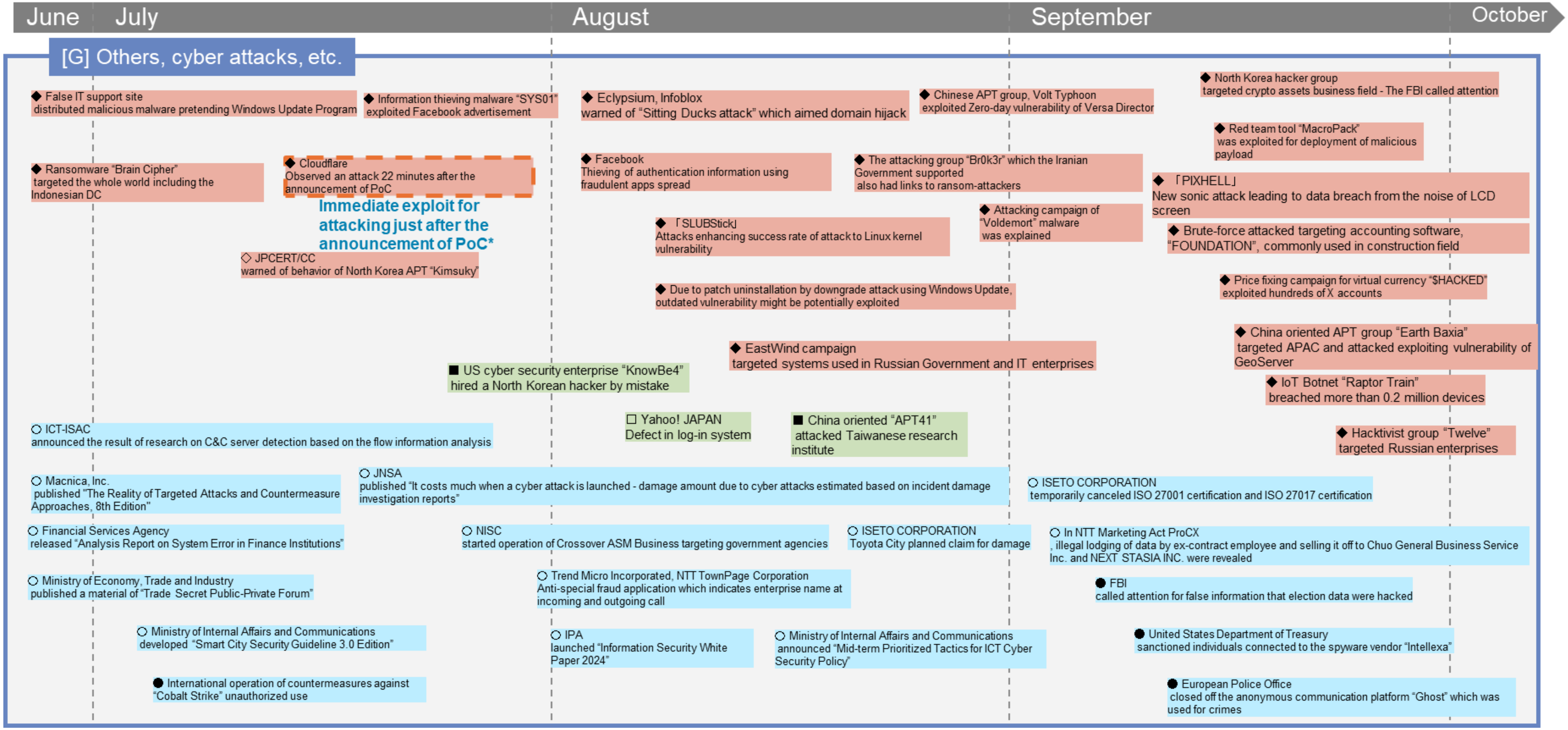
[F] Data breach

* There may be cases that the date indicated in Timeline is date as of posting but not as of occurrence of the event.

△□◇○: Domestic
▲■◆●: Common all over the world, Overseas

△▲: Vulnerability
□■: Incidents/accidents
◇◆: Threat
○●: Countermeasure

[G] Others, cyber attacks, etc.



◆ False IT support site
distributed malicious malware pretending Windows Update Program

◆ Information thieving malware "SYS01"
exploited Facebook advertisement

◆ Ransomware "Brain Cipher"
targeted the whole world including the Indonesian DC

◆ Cloudflare
Observed an attack 22 minutes after the announcement of PoC

Immediate exploit for attacking just after the announcement of PoC*

◇ JPCERT/CC
warned of behavior of North Korea APT "Kimsuky"

■ US cyber security enterprise "KnowBe4"
hired a North Korean hacker by mistake

◆ Eclypsium, Infoblox
warned of "Sitting Ducks attack" which aimed domain hijack

◆ Facebook
Thieving of authentication information using fraudulent apps spread

◆ 「SLUBStick」
Attacks enhancing success rate of attack to Linux kernel vulnerability

◆ Due to patch uninstallation by downgrade attack using Windows Update, outdated vulnerability might be potentially exploited

◆ EastWind campaign
targeted systems used in Russian Government and IT enterprises

□ Yahoo! JAPAN
Defect in log-in system

■ China oriented "APT41"
attacked Taiwanese research institute

◆ Chinese APT group, Volt Typhoon
exploited Zero-day vulnerability of Versa Director

◆ The attacking group "Br0k3r" which the Iranian Government supported
also had links to ransom-attackers

◆ Attacking campaign of "Voldemort" malware
was explained

◆ North Korea hacker group
targeted crypto assets business field - The FBI called attention

◆ Red team tool "MacroPack"
was exploited for deployment of malicious payload

◆ 「PIXHELL」
New sonic attack leading to data breach from the noise of LCD screen

◆ Brute-force attacked targeting accounting software, "FOUNDATION", commonly used in construction field

◆ Price fixing campaign for virtual currency "$HACKED"
exploited hundreds of X accounts

◆ China oriented APT group "Earth Baxia"
targeted APAC and attacked exploiting vulnerability of GeoServer

◆ IoT Botnet "Raptor Train"
breached more than 0.2 million devices

◆ Hacktivist group "Twelve"
targeted Russian enterprises

○ ICT-ISAC
announced the result of research on C&C server detection based on the flow information analysis

○ Macnica, Inc.
published "The Reality of Targeted Attacks and Countermeasure Approaches, 8th Edition"

○ Financial Services Agency
released "Analysis Report on System Error in Finance Institutions"

○ Ministry of Economy, Trade and Industry
published a material of "Trade Secret Public-Private Forum"

○ Ministry of Internal Affairs and Communications
developed "Smart City Security Guideline 3.0 Edition"

● International operation of countermeasures against "Cobalt Strike" unauthorized use

○ JNSA
published "It costs much when a cyber attack is launched - damage amount due to cyber attacks estimated based on incident damage investigation reports"

○ NISC
started operation of Crossover ASM Business targeting government agencies

○ Trend Micro Incorporated, NTT TownPage Corporation
Anti-special fraud application which indicates enterprise name at incoming and outgoing call

○ IPA
launched "Information Security White Paper 2024"

○ ISETO CORPORATION
Toyota City planned claim for damage

○ Ministry of Internal Affairs and Communications
announced "Mid-term Prioritized Tactics for ICT Cyber Security Policy"

○ ISETO CORPORATION
temporarily canceled ISO 27001 certification and ISO 27017 certification

○ In NTT Marketing Act ProCX
, illegal lodging of data by ex-contract employee and selling it off to Chuo General Business Service Inc. and NEXT STASIA INC. were revealed

● FBI
called attention for false information that election data were hacked

● United States Department of Treasury
sanctioned individuals connected to the spyware vendor "Intellexa"

● European Police Office
closed off the anonymous communication platform "Ghost" which was used for crimes

Password list attack/Brute-force attack

Topics on harms due to login spoofing and account hacking are increasing when compared to the past. In the examples of Golf Digest On-line and Hulu, introduced in [E] Unauthorized accesses, individual accounts were targeted. In the case example of FOUNDATION introduced in [G] Others, cyber attacks, etc., shared accounts used in business enterprises were targeted.

As found in the questionnaire by IPA [29], the ratio of users using less easily guessed passwords is high, 71.3% of PC users and 65.1% of smartphone users. Consequently, it is estimated that the ratio of occurrence of illegal log-in by Brute-force attack due to password setting such that it is left as default or set to easily guessed passwords is decreasing. Nevertheless, the ratio of users who avoid sharing the same password for more than one services is lower when compared with above, 58.1% of PC users and 46.6% of smartphone users. That means, many users still share the password in more than one services, thus, it is supposed that the success rate of password list attacks exploiting ID and password exposed from a certain service is high.

It is advisable that shared use of password is avoided and different passwords are set for different services. If it is troublesome to memorize passwords, it is recommended to use a password management tool. In addition, as a measure against the matter that a password is run through, use of Multi-factor authentication is effective. It is advisable that appropriate password setting is used to protect accounts from password list attacks and Brute-force attacks.

Acceleration of Zero day attack

As learned from Timeline [A] Vulnerability used in attacks, a lot of cyber attacks exploiting vulnerabilities of various products and services have occurred. In such a situation, Cloudflare has warned of increase of Zero day attack and shortened the developing time for weapons used for attacking published vulnerabilities (CVE - Common Vulnerabilities and Exposures) in its Application Security Report [30]. Especially, in the case example of JetBrains TeamCity for vulnerability of authentication bypass (CVE-2024-27198), a cyber attack was recognized 22 minutes after the announcement of the vulnerability.

This speed is faster than the speed that WAF rule is manually established or a patch is generated and deployed. That means, the speed of prevention measure manually conducted is failing to catch the speed that cyber attacks come out with.

Individual organizations are required to introduce methods capable to react to the speed of occurrence of such cyber attacks. For instance, it seems one of the measures is applying AI, just like Cloudflare is making an effort for.

Harm from ransomware in consignee

Many cases have occurred when harms from ransomware occurred in consignees and/or subsidiaries, then the consignor announced harms due to data breach. Particularly, many cases were observed when consignors suffered the impact of harms of ransomware infection occurred in ISETO CORPORATION and HIROKEI, which announced harms from personal information breach.

The Independent administrative agency, Information-Technology Promotion Agency (IPA) also raised “Attacks exploiting deficit of supply chain” as the 2nd rank of the “10 Major Security Threats [For Organizations] [1]2024”.

Even though the security measures within the own organization are strengthened, when an organization which does not take appropriate measures is joining in the supply chain system, that organization suffers ransomware attack and harm spreads from thence.

To prevent such harms, it is advisable to select consignees which have obtained international certification in relation to security measures such as ISO/IEC 27001. In addition, to be prepared for occurrence of harms due to ransomware attacks, it is also important that the extent of liability is clarified in the contract, as well as specifying the emergency contact process at the time of occurrence of incidents.

Growth of threats of business email compromise using Generative AI

In recent years, along with popularization of Generative AI tools such as ChatGPT, cyber attacks, especially business email compromise (BEC) are spreading all over the world and fraud has been rapidly sophisticated. According to Proofpoint [30], BEC in Japan marked increase of 35% from a year earlier which was the largest increase ratio in the world, with multilingualization of Generative AI as a backdrop. Using multilingualization and grammatical accuracy of Generative AI and capabilities to generate messages focusing targets, attackers succeed to generate sophisticated texts in which unnatural syntax and typos typically found in fraudulent e-mail are almost completely eliminated.

To prevent harms from BEC, it is advisable to introduce schemes to check the validity of the domain of senders' mail addresses as well as falsification of mail texts, such as SPF, DKIM, and DMAC at the minimum. However, recent sophisticated BEC executes attack mails of BEC through mails not spoofing the domain of sender's mail address to avoid from being excluded by means of mail security measures such as SPF. As such, not only schemes for mail security measures, but also periodical security education and training against BEC conventionally conducted to date are increasingly important now. The most recent patterns and tricks of BEC such as texts for instructions for urgent payment of expenses or urgent request for sensitive information should be shared so that employees can identify BEC and report that autonomously.

参考文献

[1] “情報セキュリティ10大脅威 2024,” IPA独立行政法人 情報処理推進機構, 24 1 2024. [オンライン]. Available: https://www.ipa.go.jp/security/10threats/10threats2024.html.

[2] “内部不正はなぜ起こるのか？～その発生のメカニズムを探る～,” Trend Micro, 5 12 2024. [オンライン]. Available: https://www.trendmicro.com/ja_jp/jp-security/24/l/expertview-20241205-01.html.

[3] “内部不正のプロが解説！これを読めば内部不正のすべてが分かる,” ジュピターテクノロジー株式会社, 31 5 2021. [オンライン]. Available: https://blog.jtc-i.co.jp/2021/05/ekran-5.html.

[4] “組織における内部不正防止対策,” IPA 独立行政法人 情報処理推進機構, 22 5 2015. [オンライン]. Available: https://sccs-jp.org/archives/symposium19/wp-content/uploads/sites/11/4874105411851011.pdf.

[5] “組織における内部不正防止ガイドライン,” IPA 独立行政法人 情報処理推進機構, 6 4 2022. [オンライン]. Available: https://www.ipa.go.jp/security/guide/insider.html.

[6] “秘密情報の保護ハンドブック,” 経済産業省, 2 2016. [オンライン]. Available: https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf.

[7] “不正リスクへの理解を深める ー「不正のトライアングルの活用」,” 日本システム監査人協会, 5 12 2018. [オンライン]. Available: https://www.saaj.or.jp/kenkyu/pdf/238Shiryo.pdf.

[8] “独立行政法人情報処理推進機構,” サイバーセキュリティ対策・内部不正防止対策, 20 6 2022. [オンライン]. Available: https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/forum/reiwa4_forum/06_220620_IPA.pdf.

[9] “「企業の内部不正防止体制に関する実態調査」報告書,” 情報処理推進機構, 6 4 2023. [オンライン]. Available: https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html.

[10] “従業員の不正を防ぐ！内部不正検知システムUEBA／XDR,” NTTデータ, 17 11 2021. [オンライン]. Available: https://www.nttdata.com/jp/ja/trends/data-insight/2021/1117/.

[11] A. Technologies, “Akamai 脅威レポート,” 7 8 2024. [オンライン]. Available: https://www.akamai.com/ja/newsroom/press-release/web-attacks-against-apis-and-applications-in-asia-pacific-grew-last-year.

[12] IBM, “IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs,” 24 7 2023. [オンライン]. Available: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs.

[13] Trendmicro, “HUNTING THREATS ON TWITTER - How social media can be used to gather actionable threat intelligence,” 30 July 2019. [オンライン]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter.

[14] 後藤大地, “Facebookにゼロクリックの脆弱性、アカウント乗っ取りの危険,” 2 3 2024. [オンライン]. Available: https://news.mynavi.jp/techplus/article/20240302-2896170/.

[15] 竹内薫, “DeepSeekがデータ不正利用か　OpenAIとMicrosoft調査,” 日経新聞社, 29 1 2025. [オンライン]. Available: https://www.nikkei.com/article/DGXZQOGN293P40Z20C25A1000000/.

[16] T. O. W. A. S. P. (OWASP), “OWASP API Security Top 10,” 2023. [オンライン]. Available: https://owasp.org/API-Security/editions/2023/en/0x00-header/.

[17] M. Tucci, “セキュアな設計で API の安全性を確保する（原題：Defend Your APIs: Secure by Design）,” 8 5 2024. [オンライン]. Available: https://www.xlsoft.com/jp/blog/blog/2024/05/08/smartbear-33-post-63110/.

[18] A. L. a. 2. m. Dionisio Zumerle, “Market Guide for API Protection,” Gartner, Inc., [オンライン]. Available: https://www.gartner.com/en/documents/5471595.

[19] LIBRUS株式会社, “APIセキュリティの全体像: 重要性から最新のベストプラクティスまで,” 7 3 2024. [オンライン]. Available: https://cybersecurity-jp.com/contents/librussc/202/#API-5.

[20] アスピック, “APIプラットフォームの比較14選。違いや選び方は？,” 8 1 2025. [オンライン]. Available: https://www.aspicjapan.org/asu/article/29892.

[21] S. Abbasi, “2024 Midyear Threat Landscape Review | Qualys Security Blog,” Qualys, 06 08 2024. [オンライン]. Available: https://blog.qualys.com/vulnerabilities-threat-research/2024/08/06/2024-midyear-threat-landscape-review#conclusion.

[22] Carnegie Mellon University, “GitHub - CERTCC/SSVC: Stakeholder-Specific Vulnerability Categorization,” Carnegie Mellon University, 28 09 2023. [オンライン]. Available: https://github.com/CERTCC/SSVC?tab=readme-ov-file.

[23] 菊. 美紀子, “セキュリティ脆弱性評価の新たな指標SSVCとは？ | DATA INSIGHT | NTTデータ - NTT DATA,” 株式会社NTTデータグループ, 19 01 2023. [オンライン]. Available: https://www.nttdata.com/jp/ja/trends/data-insight/2023/0119/.

[24] 独立行政法人 情報処理推進機構 セキュリティセンター, “共通脆弱性評価システムCVSS v3概説 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構,” 独立行政法人 情報処理推進機構, 05 04 2022. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/scap/cvssv3.html.

[25] NTT Communications, “CVSSを逆から読むと？脆弱性対応の意思決定に使えるSSVCについて - NTT Communications Engineers' Blog,” NTT Communications, 14 12 2024. [オンライン]. Available: https://engineers.ntt.com/entry/202412-ssvc/entry.

[26] 兼. 翼, “SSVC v2.1徹底解説：脆弱性対応フレームワークの変更点と進化 | FutureVuls Blog,” フューチャー株式会社, 21 11 2024. [オンライン]. Available: https://vuls.biz/blog/articles/20241121a/.

[27] 松. 翔. 村上 純一, “ユーザー企業におけるSSVCの導入と留意点 | PwC Japanグループ,” PwCコンサルティング合同会社, 09 03 2023. [オンライン]. Available: https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/ssvc-introduction.html.

[28] B. Jogi, “regreSSHion: Remote Unauthenticated Code Execution Vulnerability in OpenSSH server | Qualys Security Blog,” Qualys, 01 07 2024. [オンライン]. Available: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server.

[29] 独立行政法人情報処理推進機構, “2022年度 情報セキュリティの倫理と脅威に対する意識調査ー【脅威編】ー,” 2 2023. [オンライン]. Available: https://www.ipa.go.jp/security/reports/economics/hjuojm0000007fh1-att/000108321.pdf..

[30] Cloudflare, “Application Security report: 2024 update,” Cloudfr, 11 7 2024. [オンライン]. Available: https://blog.cloudflare.com/application-security-report-2024-update/.

Published on March 12, 2025

(Writers)
Shigeaki Kurimoto
Tsuyoshi Itagaki
Naoki Murata
Yuhei Terashi
Ryotaro Tanaka

(Editors)
Shinichi Oshima
Hisamichi Ohtani
Tomomi Ogushi
Rui Kanazawa
Tomoka Nakayama
Takayoshi Sawada

NTTDATA-CERT, Information Security Office, NTT DATA Group
nttdata-cert@kits.nttdata.co.jp