Report in Response to Recommendations and Request for Reports Received from PPC dated March 28, 2024 (Summary)

April 26, 2024

LINEヤフー

Introduction

On November 27, 2023, and February 14, 2024, LY Corporation reported its incident on the information leakage due to unauthorized access.

This incident was triggered by malware which infected a personal computer owned by an employee of a subcontractor used by NAVER Cloud Corporation and LY Corporation. The initial unauthorized access to our servers’ internal system began on September 14, 2023. Since NAVER Cloud and LY Corporation shared an in-house system for dealing with employee and other personnel information that is managed with a common authentication system, this allowed network access into the system of the former LINE Corporation, and thus causing unauthorized access by a third party into our system via NAVER Cloud’s system on October 9, 2023. As a result, this led to the information leakage of users, business partners, employees, and other personnel.*

We deeply recognize the gravity of this incident, which undermines the trust held in us as a platform operator with an extensive user base. We are committed to earnestly preventing such occurrences in the future.

On March 28, 2024, we have received recommendation from the Personal Information Protection Commission of Japan (“PPC”) to take prompt corrective actions for “inadequate technical safety management measures,” and “inadequate organizational safety management measures,” and have been requested to make a report on the progress of the improvement measures. Based on the recommendation and request for report, we submitted a report on April 26, 2024.

This document is a summary of the report submitted to PPC.
For more information on the response status and future schedule, please refer to the dedicated page on the incident on our corporate website.

https://www.lycorp.co.jp/en/privacy-security/recurrence-prevention/

*Employees and other personnel of LY Corporation and its group companies, NAVER Group companies, subcontractors, and temp agencies.

Table of Contents

01 Corrective Actions for Inadequate Technical Safety Management Measures

02 Corrective Actions for Inadequate Organizational Safety Management Measures

Corrective Actions for Inadequate Technical Safety Management Measures—1 (1/2)

PPC News Release No. 5-1

1 Inadequate Technical Safety Management Measures

The intrusion detection system installed and operated between the networks of NC (meaning NAVER Cloud Corporation, hereinafter the same) and LYC (meaning LY Corporation, hereinafter the same) failed to prevent and detect unauthorized access by the attacker in this case, even though the method of connection from NC’s data center to LYC’s data center by the attacker in this case was different from the connection method assumed in normal business practice. This is partly due to the fact that although LYC allowed NC to have broad access to LYC's network and internal systems, LYC did not take sufficient measures to protect the server, network and internal systems, and only blocked communications pertaining to specific ports, while other communications were widely allowed.

If LYC had understood the risks associated with such extensive network connections and had implemented measures such as a mechanism to allow only truly necessary communications from NC's system or terminal to LYC's network or system, and to disallow other access, unauthorized access could have been prevented or detected.

Corrective Actions for Inadequate Technical Safety Management Measures—1

Matters reported (Excerpt)

1 Correction of network connection between NAVER Cloud’s data center and our data center

(1) Blocking of unnecessary telecommunication

The broad network access from NAVER Cloud’s data center to the former LINE data center was the cause of the unauthorized access to our system in this incident. Considering this cause, we have configured the network access settings from NAVER Cloud’s data center to the former LINE data center and installed a firewall between the two environments. As a result, only necessary telecommunication will be allowed, and all other telecommunication will be denied. **(Completed in March 2024)**
Moving on, by June 2024, we will proceed with the formulation of a review plan on consignments and blocking of telecommunication in phases accompanying the system separation.

(2) Suspension of use of the authentication system responsible for system management conducted by NAVER Cloud and migration to our authentication system

In total, there are three common authentication systems, which are all systems related to employee accounts (authentication information of users is not included). NAVER Cloud manages the system related to these authentication systems. In light of this situation, we will stop using these systems and proceed with the migration to our own authentication system as described below.

- We will prioritize the systems managed by LY Corporation and its Group subsidiaries, as LY Corporation is able to switch authentication functions for these. In this way, we will resolve the current situation in which we share authentication systems and authentication information with NAVER. **(Scheduled to be completed in June 2024)**

- The separation of authentication system from the system managed by NAVER and NAVER Cloud will be implemented according to the following schedule.

(Scheduled to be completed at the end of March 2025 for LY Corporation, the end of March 2026 for Japanese subsidiaries and December 2026 for overseas subsidiaries)

(3) Separation from the systems of NAVER and NAVER Cloud
To eliminate the potential risks arising from the linkages of systems and networks with NAVER and NAVER Cloud, we will also implement separation from the systems managed by these companies.
(The separation for the employees’ systems[*1] is scheduled to be completed at the end of March 2025[*2] for LY Corporation, the end of March 2026 for Japanese subsidiaries and December 2026 for overseas subsidiaries)

In addition, we will continue to formulate or review plans for (1) review of outsourcing, (2) separation of authentication system, and (3) separation of systems, so that we can complete their implementation as soon as possible·

[*1] System used by the employees of LY Corporation and its Group companies, which are in NAVER or in former LINE environments provided by NAVER and NAVER Cloud.
[*2] For the accounting system, we will determine the timing of system switchover and suspension of use by November 2024.

Corrective Actions for Inadequate Technical Safety Management Measures—2

Matters reported (Excerpt)

2 Corrective action regarding access management of highly critical information systems

(1) Application of two-factor authentication for employee systems and risk assessment

Since servers and systems with two-factor authentication escaped the unauthorized access in this incident, we increased the strength of authentication and reduced the risk of unauthorized access by applying two-factor authentication to the servers and systems used by our employees to protect these servers and systems. **(Completed in March 2024)**
The application of two-factor authentication for some systems in the data centers of the former Yahoo Japan Corporation is scheduled to be implemented by the end of December 2024.

In addition, considering that the data analysis system to which unauthorized access was subjected in this incident was a critical system to which two-factor authentication should have been applied, we will define the critical systems and the safety management standards required for them, and establish a system to identify and manage risks in the risk management process utilizing ISO27001. In addition, as part of the annual risk assessment, we will establish a system to comprehensively identify and evaluate the current status of data storage, security measures in place, and associated risks for each system, and establish these as part of our regulations. To ensure the implementation of these measures, a security audit division will be established directly under the CISO to establish a system for periodic review and evaluation of risk measures. **(To be completed in June 2024, and sequentially implemented thereafter)**

(2) Reinforcement of access management of critical systems (MFA + authentication process security assessment) (Completed in March 2024)

As described in (1) on page 5, we introduced two-factor authentication. In addition, a security assessment was performed on employee systems in the former LINE data centers that are critical, by a security engineer from a division specializing in vulnerability assessment to determine if there were any attempts to bypass the authentication process or ways in which authentication factors could be exploited.

(3) Correction of Active Directory (AD) management (Completed in March 2024)

In this incident, the accounts with authority of AD manager were compromised. Therefore, we made operational changes to the accounts of AD managers. In addition, we newly introduced behavior-based detection solutions to the AD and began monitoring by SOC. Furthermore, in addition to these measures, we corrected the AD management based on the consulting received from an outside firm.

Note: We are considering moving up the completion date for measures that are currently being addressed.

Corrective Actions for Inadequate Technical Safety Management Measures—3

Matters reported (Excerpt)
）

3　Other corrective actions for the technical safety management measures

(1)　Total inspection of connection paths between outside environment and the data centers of former LINE (Scheduled to be completed at the end of July 2024)

Based on the fact that extensive network access permission from NAVER Cloud data center to the former LINE data center was the cause of the unauthorized access to former LINE data center's systems, we will inspect the adequacy of network access control and the readiness of incident response for routes connecting from outside the company to former LINE data center via leased lines, VPNs, etc. as is permitted to NAVER. This inspection will be conducted by the end of July 2024.

(2)　Formulation of plans with outside firms (Scheduled to be completed at the end of May 2024)

To ensure the adequacy, effectiveness, and objectivity of the plan for recurrence prevention measures, we received recommendations from outside firms, examined the applicability of the plan to our systems and business environment, and formulated concrete countermeasures and plans. In addition, for matters that need to be addressed in the NAVER Cloud data centers, we will examine the recommendations with NAVER Cloud and make concrete countermeasures and plans considering the corrective measures already implemented at NAVER Cloud, etc.

(3)　Verification of the effectiveness of cybersecurity measures and security monitoring, and fundamental improvements and enhancements (Scheduled to be completed at the end of August 2024)

We will develop specific plans to strengthen cybersecurity more effectively and comprehensively, and promptly and steadily take corrective measures. Specifically, we will implement the following:

Implementation of penetration tests

・July 2024	Implementation of tests, analysis of results, and reporting
・August 2024	Formulation of corrective plans based on test results

Review of mechanisms for behavior-based detection, etc. and correlation analysis rules, etc.

・July 2024	Analysis of current status and validation with external organizations
・August 2024	Formulation of corrective plans based on verification results

Note: We are considering moving up the completion date for measures that are currently being addressed.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (1/3)

PPC News Release No.5-2

⑴ Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

i) Issues related to risk management according to the relationship with NC

Although LYC is required to take security management measures in accordance with the Guidelines at its own discretion in handling personal data, LYC has continued to use the common authentication system with NC and the network configuration that allows extensive network connections with NC, which originated from the history of the former LINE Corporation. Since LYC had considered that NC was not entrusted with the handling of the personal data in question, LYC did not actually supervise NC to ensure that it took measures equivalent to its own security management measures. As a result, the system that LYC outsourced NC to build became the intrusion route and the cause of the leakage, and the personal data in question was leaked.

In other words, LYC handled a large amount of personal data, including users' personal data, without considering and understanding the responsibility and means to take necessary and appropriate measures for its security management.

Although LYC should have been aware of such risks and issues, it continued to jointly use the common authentication system and to outsource the construction and operation of critical systems to NC. Therefore, it must be said that there are problems in LYC's understanding of the state of personal data handling and in the assessment, review, and improvement of safety management measures.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (2/3)

Matters reported (Excerpt)

1 Improvement of issues related to risk management in accordance with the relationship with NAVER Cloud

(1) Corrective action on supervision methods of subcontractors

A) Review of security risk assessment criteria (Completed in March 2024)
We have established a new subcontractor checklist based on the checklist used for the outsourcing of personal information, etc. to be used more broadly for general subcontractor management.

B) Study, formulation, and implementation of supervision methods and standards to achieve effective subcontractor management (Completed formulation of standards in March 2024; to be sequentially implemented thereafter)
We will formulate internal rules for conducting a multifaceted risk assessment of security and credit aspects for new business partners and subcontractors, that is not limited to the outsourcing of personal information, etc. In the future, we will conduct multifaceted risk assessments at the start of transactions and at the time of renewal of contracts, as well as during periodic audits. Although there is a possibility that risks arising from inadequate measures taken by subcontractors may remain until the supervision under the new evaluation standards has been completed, we will conduct audits, etc. of the subcontractor that was the cause of this incident and others in advance to deal with such risks. We will also reduce risks by applying two-factor authentication when connection is made to our VPN environment and by lending PCs to accounts issued by our company.

C) Formulation of safety management measures/cybersecurity measures (Completed in January 2024)
For the subcontractors who use accounts issued by us, in principle, we have implemented measures to allow access to our network environment only after they have gone through two-factor authentication.

D) Independent ascertainment of intrusion and its extent (Scheduled to be completed at the end of September 2024)
Our policy will be to allow subcontractors who can log in or have access to our network to perform their subcontracted work only on personal computers that have been kitted by us. Although risks of malware infections, etc. of personal computers of subcontractors remain until the distribution of kitted personal computers is completed, we will mitigate the residual risks by implementing the measure described in C) above.

Note: We are considering moving up the completion date for measures that are currently being addressed.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (3/3)

Matters reported (Excerpt)

1 Improvement of issues related to risk management in accordance with the relationship with NAVER Cloud

(2) Other measures to improve the issues related to risk management in accordance with the relationship with NAVER Cloud

We conducted an on-site inspection of NAVER Cloud with a third-party company. During the inspection, we confirmed NAVER Cloud's implementation of measures to prevent a recurrence, as well as the implementation status of NAVER Cloud's various safety control measures that led to the incident, and pointed out and requested corrective actions. **(Completed in March 2024)**

In order for us to take the initiative in confirming future corrective actions, etc., we have concluded an agreement that stipulates auditing rights, etc. pertaining to NAVER Cloud and will ensure the effectiveness of the abovementioned actions in a clear manner. **(Completed in March 2024)**

Moving on, we will resolve the outsourcing of SOC-related operations (target date: end of September 2024) and will reduce the scope of outsourcing itself through termination or reduction of related outsourcing relationships, based on the plan to reduce outsourcing, which is scheduled to be formulated by June 2024 .

In addition to the above, we conducted an on-site inspection of the subcontractor company involved in this incident and also terminated the contract. **(Completed in March 2024)**

Furthermore, in addition to thorough risk management through the traditional company-wide process (ERM) to identify and manage organizational risks in each division, we will consider introducing a new mechanism to visualize and assess a wide range of risks from a more multifaceted perspective by gathering the opinions of each and every employee. **【Scheduled to complete system design in June 2024 and to be sequentially implemented thereafter.)**

Note: We are considering moving up the completion date for measures that are currently being addressed.

Corrective Actions for Inadequate Organizational Safety Management Measures—2

PPC News Release No.5-2

⑴ Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

i) Issues related to the response after the administrative guidance in 2021

In response to the administrative guidance in 2021, which required LYC to appropriately supervise the handling of personal data by its subcontractors, LYC decided to introduce two-factor authentication for logins with access privileges to highly critical personal data as one of the measures to prevent recurrence of such a situation. Nevertheless, LYC judged that the sensitivity of the user information stored in the data analysis system that received unauthorized access in this case is relatively low compared to other systems and had refrained from introducing two-factor authentication.

However, among the personal data in this case, the personal data stored in the data analysis system is personal data related to the user‘s usage history of various LINE services. These service usage histories are data related to the privacy of individuals, such as the scope of their activities, economic status, hobbies and preferences, and cannot be classified as less sensitive information from the viewpoint of protecting the rights and interests of the individuals.

In the first place, since LYC had certain peculiarities related to safety management measures in terms of (i) use of a common authentication system with NC and (ii) extensive network connection with NC, LYC should have properly assessed the risks arising from these factors and proactively decided to introduce two-factor authentication even for personal data such as user service usage history.

From the above, we find that the assessment, review, and improvement of safety management measures after the 2021 administrative guidance were not sufficient at LYC.

Matters reported (Excerpt)

2 Improvement of issues related to our response after 2021 administrative guidance

The introduction of multi-factor authentication for access to personal data, such as users' service usage history, was delayed despite the fact that there had been opportunities to review and improve it in the course of the Company's response to the 2021 administrative guidance and in the course of its consideration of the business integration (merger) conducted on October 1, 2023. On this point, we are in the process of introducing two-factor authentication for servers, systems, etc. used by our employees, and have mostly completed this process, as described in “Corrective Actions for Inadequate Technical Safety Management Measures—2.”

We believe that it is also necessary to improve the security governance system, whereby the Company's overall security management measures, which are the premise of the Company's management, are discussed and reviewed. We have established a Security Govemance Committee directly under the President to further promote measures related to this incident and to discuss the Company's overall issues, as well as a Group CISO Board to discuss overall security governance for the Company's group. (Details will be provided in “Corrective Actions for Inadequate Organizational Safety Management Measures—4.”)

Corrective Actions for Inadequate Organizational Safety Management Measures—3

PPC News Release No.5-2

(2) Development of a system in response to the information leakage incident, etc.

In order to clarify the cause of unauthorized access and the scope of the intrusion, it was necessary to investigate Company A's PCs and servers, as well as the access logs of the system that NC is commissioned to build and operate.

LYC must take safety management measures in accordance with the Guidelines at its own discretion, and should have a system in place to investigate the facts and determine the cause in the event of a leakage, etc. However, LYC is in a state in which it has to rely on NC and the NAVER Group to investigate the facts and determine the cause, and it took approximately three and a half months for LYC to grasp the full scope of this incident. Thus, LYC failed to promptly investigate the facts and determine the cause of the leakage, etc., and there were also inadequacies from the viewpoint of establishing a system to respond to incidents of leakage, etc.

Matters reported (Excerpt)

1 Establishment of a system to respond to incidents of leakage, etc., including fact-finding and investigation of the cause

We recognize that the following two factors have led to the incident, and we will work to establish a system to promptly respond to incidents when they occur.

1) Insufficient systems in place to respond to incidents of leakage, etc., at our company **(Plan formulated in May 2024 and completed external evaluation of the plan in June 2024. Being implemented sequentially thereafter)**
- We will identify areas for improvement in the process of determining the scope of investigation when an incident occurs, and develop the necessary manuals and rules. In addition, implementation of the manuals and rules will be determined after evaluation by an external organization, and periodic exercises will be conducted to ensure feasibility.
- In principle, our policy is to lend PCs to subcontractors, and to promptly collect the PCs and conduct forensic investigations when incidents occur.

2) High degree of dependence on NAVER Cloud and the NAVER Group **(Completed in March 2024)**
- We will clarify the contact point with NAVER Cloud in case of incidents.
- The logs of the NAVER Group's systems shall be kept for one year in accordance with our log retention period rules, and a separate agreement has been concluded so that the logs can be received from NAVER Cloud as needed.

2 Establishment of a system to obtain and analyze logs in-house (Establishment of an independent SOC operation system)

Based on the occurrence of this incident, we will switch the function related to SOC Tier 1 which is outsourced to NAVER Cloud to a Japanese company and will establish a structure in which we will operate SOC in cooperation with said Japanese company. **(Scheduled to be completed in October 2024)**

Note: We are considering moving up the completion date for measures that are currently being addressed.

Corrective Actions for Inadequate Organizational Safety Management Measures—4

PPC News Release No.5-2

(3) Development of organizational structures, etc.

Even after the 2021 administrative guidance issued to former LINE, despite LYC’s continued extensive network connections with other companies, it is difficult to say that its organizational structure was necessarily functioning adequately because, as mentioned above, technical safety management measures such as access control were not taken, problems were found in understanding the status of personal data handling and assessing, reviewing, and improving safety management measures, and LYC failed to promptly respond to leakage, etc. The business scale has expanded and a large amount of highly important personal data is expected to be handled in the future as a result of the business integration in October 2023. In order to ensure thorough handling of such personal data, an organizational structure should be established to ensure thorough security management measures and focus on ensuring their effective operation, led by the person in charge of handling personal data (DPO, etc.).

Matters reported (Excerpt)

(1) After the merger on October 1, 2023 among former LINE, former Yahoo Japan Corporation and other companies, the CISO is responsible for the security of all personal data handled by LYC as the company's security officer. Specifically, we define the handling levels and safety management measures for all data, including personal data, and stipulate them in our security regulations, while appointing a security officer in each division to conduct risk assessments to ensure that data is being handled appropriately.

In addition, an auditing division was established in April 2024 to monitor compliance with the regulations.

(2) When handling personal data, we have a meeting body with a specialized privacy-related organization that assesses potential privacy impacts, identifies risks and necessary actions, makes policy decisions, and escalates these decisions to our Management Committee as necessary. The DPO division also participates in this meeting body and monitors and advises on the activities of the executive side from the user‘s point of view independent from the executive side.

(3) A new organizational structure has been established to strengthen security governance and safety management measures at the management level and throughout the Group. Specifically, the Security Governance Committee, chaired by the President and CEO of the Company, was established in April 2024 to further promote measures related to this incident and to discuss the Company's issues in general. Also, from April 2024, we have established a “Group CISO Board,” constituted by the CISOs of LY Corporation and its major Group companies (including overseas companies) and the CISO of SoftBank Corp., as an observer. Through this meeting, we will conduct a fundamental review and upgrading of the Group’s overall security governance. At this Board, we will discuss and promote the formulation of uniform rules for security within our Group and ensure compliance, as well as the rearrangement of outsourcing relationships among our Group companies on the premise of such rules.

LY