Report Submitted on June 28, 2024, in Response to Request for Report and Recommendation Received from PPC dated March 28, 2024 (Summary)

June 28, 2024

LINEヤフー

Introduction

This document is an overview of the report submitted on June 28, 2024, in response to the request for report and recommendation, etc. received from Japan's Personal Information Protection Commission ("PPC") dated March 28, 2024.

This document describes the progress of the corrective actions taken to address the inadequate technical safety management measures and the inadequate organizational safety management measures.

We will make continued efforts to prevent recurrence.

Please check the dedicated webpage on our corporate website for more information on our response status and future schedule.
https://www.lycorp.co.jp/en/privacy-security/recurrence-prevention/

Previous publications

Submission of Report to the Personal Information Protection Commission of Japan (Published April 26 2024)
https://www.lycorp.co.jp/en/news/announcements/008284/

Table of Contents

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 (2/2)

Matters reported
(Excerpt)

No. 1 Correction of network connection between NAVER Cloud's data center and our data center

(1) Blocking of unnecessary telecommunication

We reviewed and changed the settings of firewall policies in accordance with the relocation to Japan*1 of servers and data of users in Japan out of our production environment servers that uses NAVER Cloud's infrastructure. In addition, we have deleted and reviewed firewall policies which were determined to be unnecessary as a result of the maintenance of firewall policy settings (conducted every three months). **[Completed in June 2024]**

In the future, we plan to gradually block communications in accordance with the review plans of consignments and system separation.

[Plan moved up with the new target completion date at the end of March 2026*2]

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

The highest priority was placed on the separation of the authentication system in the systems managed by LY Corporation and its Group subsidiaries. **[Completed in June 2024]**

Also, for the systems used by LY Corporation and managed by NAVER and NAVER Cloud, system separation and the termination of using NAVER Cloud's authentication system is scheduled to be completed by the end of March 2026. **[Scheduled to be completed by the end of March 2025 for LY Corporation and by the end of March 2026 for Japanese subsidiaries. The plan has been accelerated and the target completion date for overseas subsidiaries is now the end of March 2026.*2]**

(3) Separation from the systems of NAVER and NAVER Cloud

In order to eliminate potential risks associated with systems and network connections with NAVER and NAVER Cloud, we will also conduct separation from the systems managed by these companies. We have now completed the formulation of project plans for each target system and are currently working on the separation projects.

[Separation for the employees' systems*3 scheduled to be completed by the end of March 2025*4 for LY Corporation and by the end of March 2026 for Japanese subsidiaries. The plan has been accelerated and the target completion date for overseas subsidiaries is now the end of March 2026*2]

System separation is gradually being implemented for Japanese and overseas subsidiaries. The risks arising from the interim period will be addressed by continuously applying two-factor authentication to the systems, scrutinizing the access scope, and blocking unnecessary communications.

*1 Explanation of LINE data transfer: https://www.lycorp.co.jp/ja/news/announcements/000823/ (Japanese only)
*2 The original completion date was the end of December 2026.
*3 Systems used by employees of LY Corporation and its Group companies, which are in NAVER or in former LINE environments provided by NAVER and NAVER Cloud.
*4 For the accounting system, we will conduct the system separation in January 2025 and suspend the use by March or June 2025.

Corrective Actions for Inadequate Technical Safety Management Measures—2

Matters reported
(Excerpt)

No. 2 Corrective action regarding access management of highly critical information systems

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

We have completed the implementation of two-factor authentication on all systems, except for some systems in the data centers of former Yahoo Japan Corporation. **[Completed in March 2024]**

As an additional measure, we have distributed authentication devices that can be used in certain restricted areas where smartphones are prohibited, and have completed the additional implementation of two-factor authentication for key employee accounts that work in restricted areas. **[Completed at the end of June 2024]**

In addition, as part of the process of making some of the systems in the data centers of former Yahoo Japan Corporation compatible with two-factor authentication, we are currently working on building a new integrated Active Directory ("AD"), which is the first step in the process. We plan to start the application of two-factor authentication in August, in conjunction with the migration to our integrated AD. We are currently considering moving the plan forward for this measure. **[Target completion date: end of October 2024]**

(2) Reinforcement of access management of critical systems (MFA + authentication process security assessment) [Completed at the end of March 2024]

We have completed the security assessments for critical systems.

The establishment of the necessary security assessment mechanism, the definition and classification of the selection criteria for critical systems, and the implementation status of the standards for security measures required for these systems will be detailed on page 13.

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

Matters reported
(Excerpt)

No. 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

We will conduct a comprehensive inspection on the appropriateness of network access control and incident response preparedness for paths connecting the outside environment with the former LINE data centers. **[Scheduled to be completed by the end of July 2024]**

Our policy will be to implement appropriate network access control for outbound communications from the data center of former LINE to the data center of NAVER Cloud. A plan will be drafted for approaches, policies on specific network access control, and application of firewalls, etc., based on the results of the comprehensive inspection mentioned above**. [Plan scheduled to be drafted at the end of August 2024 and implemented based on the plan thereafter]**

(2) Formulation of plans with an outside firm

To ensure the adequacy, effectiveness, and objectivity of the plans for recurrence prevention measures, we will continue to develop countermeasures, formulate plans, and promote corrective measures based on the recommendations of an outside firm. The status of items that need to be addressed at our data centers is as follows:

- Disable management share functionality for Windows servers in the former LINE data center, except for servers that use the management share function **[Completed in June 2024]**
- Reminder and e-learning for all employees regarding prohibition of storing passwords on internal systems **[Completed at the end of April 2024]**

Additionally, we confirmed that for items that require action at NAVER Cloud‘s data centers, measures have been implemented appropriately. **[Completed at the end of May 2024]**

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

Matters reported
（Excerpt)

No. 3 Other corrective actions for the technical safety management measures

(3) Verification of the effectiveness of cybersecurity measures and security monitoring, and fundamental improvements and enhancements

We perform penetration tests to empirically understand and evaluate not only theoretical risks, but also how our systems could be attacked in practice.

- Completion of penetration testing and analysis of results **[Scheduled to be completed by the end of July 2024]**
- Development of a corrective plan based on the test results **[Scheduled to be completed by the end of August 2024]**

With an outside firm, we are reviewing the behavior-based detection systems and correlation analysis rules currently in operation at our data centers for the purpose of evaluating, verifying, and improving their resistance and effectiveness against unknown threats such as zero-day attacks, in addition to known attacks.

- Current situation analysis and effectiveness verification involving an outside firm **[Scheduled to be completed by the end of July 2024]**
- Development of a corrective plan based on the results of the verification **[Scheduled to be completed by the end of August 2024]**

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (1/5)

PPC News Release No.5-2

(1) 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 (2/5)

Matters reported
(Excerpt)

No. 4 Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

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

(1) Corrective action on supervision methods of subcontractors

(i) Review of security risk assessment criteria [New checklist completed in March 2024; to be updated sequentially]
We conduct audits using the newly established and updated security checklists.

(ii) Study of supervision methods and formulation of standards to achieve effective subcontractor management and application thereof [Completed preparation to start application in July 2024; to be gradually applied thereafter]

In preparation for the sequential implementation of audits based on the standards established to improve subcontractor management from July 2024, we have conducted audits based on the new standards since April 1, 2024, as a preliminary implementation of the new standards, and also started trial operations for some subcontractors from May 15, 2024, to test the multifaceted risk assessment based on the new standards. In the future, we will take necessary additional measures based on individual cases, etc. that occur after the start of application of the new standards, and in considering additional measures, we will seek advice from an outside firm, as we did when the standards were formulated, to further upgrade the subcontractor management model while incorporating objective outside perspectives.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (3/5)

Matters reported
(Excerpt)

No. 4 Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

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

(1) Corrective action on supervision methods of subcontractors

(iii) Independent ascertainment of intrusion and its extent

Our policy is to allow subcontractors who can access our network using accounts issued by our company to perform their subcontracted work only on personal computers that have been kitted by us. We are progressing as planned to complete the loan of personal computers both in Japan and overseas by the end of September 2024. **[Scheduled to be completed by the end of September 2024]**

Meanwhile, as an additional measure, we are planning to expand the scope of the computer loan program. Ultimately, for subcontractors who are able to have access to our network, regardless of whether they are subcontracted by us or not, we will, in principle, lend them personal computers from us or from Group companies that have been confirmed and guaranteed to have the same level of security software as LY Corporation. As part of this implementation policy, we will provide personal computers to subcontractors performing the subcontracted work of LY Corporation by the end of September 2024, and we plan to complete the provision of personal computers to other subcontractors within FY2024.

[Subcontractors that perform the subcontracted work of LY Corporation using accounts issued by Group companies: Scheduled to be completed by the end of September 2024]

[Subcontractors that can access our network other than those mentioned above: Scheduled to be completed in March 2025]

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (4/5)

Matters reported
(Excerpt)

No. 4 Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

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

(i) Actions towards NAVER Cloud

In addition to on-site inspections, audits based on the content of the outsourcing was completed by the end of April 2024[*1] and the end of June 2024.[*2] Through these audits, etc., we have confirmed that the requested corrective actions have been taken, and our outsourcing relationship with NAVER Cloud regarding SOC is scheduled to be terminated at the end of September 2024. Thereafter, we plan to conduct audits once a year. **[Audits completed at the end of April and end of June 2024; thereafter, scheduled to be conducted on a regular basis once a year]**

(ii) Relationship with NAVER Cloud

(a) Designing of new mechanism for visualizing and evaluating risks

We recognize that the risk management issue was due to the fact that awareness of the incident remained within a specific department in charge and could not be addressed as an organization-wide problem. To address this issue, we are planning to conduct a survey to all employees as part of the improvement activities to establish a system to communicate potential risks that employees perceive on a daily basis, while ensuring their psychological safety. **[Scheduled to be implemented in July and November 2024]**

[*1] Audits on suppliers of specified critical facilities and outsourcing of maintenance and management services based on the Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures.
[*2] Audits regarding outsourcing of maintenance and operation of critical systems as determined by LY Corporation.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (5/5)

Matters reported
(Excerpt)

No. 4 Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

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

(ii) Relationship with NAVER Cloud

(b) Formulation of plans to terminate/reduce outsourcing to NAVER (NAVER and its subsidiaries) and NAVER Cloud

In order to review our entire outsourcing relationship with NAVER, we have decided the termination, reduction or retention policy on all relationships that we consider to be related to the provision of ongoing services, systems, etc.

The outsourcing relationship can be broadly divided into "LY Corporation's use of NAVER's technology and systems" and "outsourcing of service planning, functions, and development to NAVER, related to LY Corporation's business," and we understand that by implementing initiatives for both the former and the latter, overall use of systems and services that NAVER provides to our company will be included.

We have drawn up specific plans for each of the outsourcing initiatives between LY Corporation and the NAVER Group (including major consignment details, specific future policies, and initial estimates of the earliest target completion date, etc.), and have begun work to terminate or scale down those that can be implemented immediately, including through discussions and negotiations with NAVER. In principle, we intend to terminate the outsourcing of system/network operation and service development/operation.

For service planning, function and development consignment, the earliest (target) completion dates for each consignment relationship are as follows.

[Outsourcing from LY Corporation to NAVER and NAVER Cloud: targeted by the end of December 2025]

[Outsourcing from LY Corporation to other NAVER Group companies: targeted by the end of March 2025]

In addition, we have decided on future policies (termination, reduction ore retention) regarding the use of commercially available SaaS, the use of general-purpose APIs, overseas businesses, the use and outsourcing of infrastructure, etc. between LY Corporation's subsidiaries and NAVER, and the relationship regarding the services and systems that LY Corporation provides to NAVER. We will implement the decided policy in the future**. [Plans formulated in June 2024 regarding technology and system usage, service planning, functions, and development consignment. Work has begun to gradually terminate and reduce operations.]**

Corrective Actions for Inadequate Organizational Safety Management Measures—2

PPC News Release No.5-2

(1) 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)

No. 4 Assessment, review, and improvement of the status regarding the handling of personal data and safety management measures

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

Although there was an opportunity to review and improve the introduction of multi-factor authentication for access to personal data after the 2021 administrative guidance, we were late in introducing the authentication. We regard that this was due to the fact that specific definitions of the applicable scope had not been established, and that there was no system in place to properly record the criteria and process for determining when two-factor authentication will not be applied. Also, there was no reevaluation process established to respond to changes in circumstances after the initial decisions.

As an effort to address these issues, we will define critical systems and the required safety management measures for them, and establish a company-wide system to identify and evaluate the current status of data storage in each system, the security measures in place, and the associated risks, with the participation of the top management. We also plan to establish these as our company regulations. **[Defined standards and established mechanisms at the end of June 2024. Establishment of internal regulations to be completed on July 1, 2024. To be regularly reviewed thereafter.]**

The following are scheduled to be implemented:

- Identification of critical systems and confirmation of their compliance with safety management measures. **[Identification scheduled to be completed early September 2024, confirmation early October 2024]**
- Risk assessment of non-compliance with safety management measures. **[Scheduled to be completed by the end of December 2024]**
- Formulation of review plans of safety management measures that meet current trends. **[Scheduled to be completed by the end of December 2024]**

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)

No. 5　Improvement in the development of a system in response to the information leakage incident

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

We will develop an improvement plan for the initial action flow when an incident occurs, the process for determining the scope of investigation, and the establishment of stakeholders and their roles and responsibilities. The plan will be evaluated by an external organization, improvements will be made, and periodic exercises will be conducted thereafter. **[Plan and its external evaluation completed at the end of June 2024, and regular exercises scheduled to be conducted in the second half of FY2024]**

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

We are currently performing an operation training with a Japanese company on the SOC Tier1 operation. After a temporary operation with a Japanese company from July 2024 to gain practical experience, we will start 24/7 operation in Japan with the Japanese company from October 1, 2024, as scheduled. **[Scheduled to begin operations from October 2024]**

Note: We are considering moving up the completion date of initiatives 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)

No. 6　Improvement in the development of organizational structures, etc. (establishment of an organizational structure to ensure that safety management measures are thoroughly implemented)

1　Establishment of an audit division to monitor compliance with security regulations

In establishing a system to identify and assess the risks of critical systems (noted in item 2 in page 13), we established a security audit division under the security division in addition to our internal audit division. This security audit division monitors the status of compliance with security regulations at the divisions in charge of systems and reports the results to the CISO. In addition, the internal audit division audits our security risk management system, including the monitoring activities by the security audit division.

2　Formation of the Security Governance Committee

The Security Governance Committee, established in April 2024, conducts various internal discussions and reviews. The status of discussions is regularly shared with our corporate officers, and we strive to ensure that awareness of preventing recurrence and improving security governance is shared throughout the company.

3　Establishment of the Group CISO Board

The Group CISO Board, established in April 2024, has made it a priority to apply the recurrence prevention measures implemented by our company to all Group companies, and has thus far discussed and deployed to each company the application of two-factor authentication and measures related to the management of subcontractors.

LINEヤフー

Unless otherwise specified, English-language documents are prepared solely for the convenience of non-Japanese speakers. If there is any inconsistency between the English-language documents and the Japanese language documents, the Japanese-language documents will prevail. In this document, the Personal Information Protection Commission of Japan is described as “PPC,” LY Corporation as “LYC,” the former LINE Corporation as “LINE,” NAVER Corporation as “NAVER,” and NAVER Cloud Corporation as “NAVER Cloud.”