Report Submitted on September 30, 2024, in Response to Request for Report and Recommendation Received from PPC dated March 28, 2024 (Summary)

September 30, 2024

LINEヤフー

Introduction

This document is an overview of the report submitted on September 30, 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/

- Submission of Report to the Personal Information Protection Commission of Japan Dated June 28, 2024 (Published June 28, 2024)
https://www.lycorp.co.jp/en/news/announcements/008729/

Table of Contents

The response/consideration status as of September 30, 2024, regarding the above matters are described from the following page onward.

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

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 (2/3)

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 are conducting continuous reviews on the firewall policies for the telecommunication between servers for the production environment of former LINE's services which use NAVER Cloud's infrastructure and the servers in the data centers of former LINE.

- We have deleted firewall policies that were judged unnecessary during configuration maintenance conducted once every three months. [Completed in September 2024]

Going forward, we will continue to block unnecessary telecommunication accompanying the completion of server relocation and termination of consignments and perform configuration maintenance on firewall policies every three months. [Target completion date: end of March 2026]

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

The deletion of some employee information, etc. that remains in the NAVER authentication system at the NAVER Cloud data center is proceeding as scheduled. [Scheduled to be completed by the end of April 2025 for LY Corporation and its domestic subsidiaries, and by the end of April 2026 for overseas subsidiaries]

As reported on June 28, 2024, for our systems managed by NAVER and NAVER Cloud, we plan to complete suspension of the use of NAVER Cloud's authentication system through completing the system separation 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 its Japanese subsidiaries. Target completion date for overseas subsidiaries: the end of March 2026]

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

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

Matters reported
(Excerpt)

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

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

As reported on June 28, 2024, 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 are currently working on the separation projects according to the project plans formulated for each target system.

[Separation for the employees' systems[*1] scheduled to be completed by the end of March 2025[*2] for LY Corporation and by the end of March 2026 for Japanese subsidiaries. The target completion date for overseas subsidiaries is the end of March 2026]

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

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

The following is being conducted to make some of the systems in the data centers of former Yahoo Japan Corporation compatible with two-factor authentication. [Target completion date: end of October 2024]

- As the first step, we released a new integrated Active Directory. [Completed in August 2024]
- We performed individual technical verification on the eligible systems and determined the migration method and schedule. [Completed in September 2024]

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

[*1] 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.
[*2] 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—3

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 conducted a comprehensive inspection on the appropriateness of network access control and and incident response preparedness for paths connecting the outside environment with the data center of former LINE.

- Regarding the appropriateness of network access control, unnecessary communication permission rules were modified and deleted for those that needed corrective action based on the inspection. [Inspection completed at the end of August 2024,[*1] correction completed at the end of September]
- Regarding the incident response preparedness, we confirmed that responses were completed without problems. [Completed at the end of July 2024]

In addition, regarding outbound communication control from the data center of former LINE to the data center of NAVER Cloud,firewall policies will be sequentially applied by the end of October 2024 based on the drafted plan. We will also inspect unnecessary communication based on the abovementioned comprehensive inspection by the end of December 2024 and perform continuous maintenance of the firewall policies thereafter. [Drafting of plans completed at the end of August 2024, inspection scheduled to be completed by the end of December, 2024]

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

Ethical hackers from an outside firm conducted penetration tests on the management and operation environment and the production environment of the former LINE environment. Through the tests, we received an evaluation on the effective disruption of the cyber kill chain, the effectiveness of the recurrence prevention measures that have been implemented so far, and the robustness of the production environment. However, we were also presented with several findings from the perspective of multilayered defense, and we have drawn up a corrective action plan to address the findings. [Completed at the end of August 2024]

Going forward, based on the corrective action plan, we will address the findingsidentified through the tests in order of priority. [Scheduled to be completed by the end of March 2025]

We also aim to achieve a cycle of maintaining and improving our security level that can respond to changing threats by conducting penetration tests once a year.

Ethical hackers from an outside firm conducted simulated attacks using the attack methods used in this incident and the attack methods frequently used in our industry, and verified the effectiveness of the behavior-based detection and the mechanism of the correlation analysis rules. [Completed at the end of August 2024]

We will sequentially take corrective actions for the simulated attack items that were not detected by this test, with the main focus on improving detection capabilities using our SIEM environment. [Correction scheduled to be completed in February 2025]

Even after the abovementioned corrections have been made, we will continue to make improvements based on the optimization ofdetection rules and the impact of damage, as part of the SOC's normal rule maintenance activities.

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

[*1] Due to the complexity of setting the policies to be inspected, it was found that the detailed investigation required more time than initially anticipated. As a result, the completion deadline was extended from the end of July to the end of August, and the task has now been completed.

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

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 (2/4)

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) Study of supervision methods and formulation of standards to achieve effective subcontractor management and application thereof

Regarding the auditing based on the standards formulated to enhance the management of subcontractors, we have started to evaluate suppliers and assess project risks from July 1, 2024, as an operation of the new standards of the Basic Policy on Management of Subcontractors and the Basic Rules on Management of Subcontractors, which came into effect on July 1, 2024. [Preparation for operation completed in July 2024, and operation began sequentially thereafter]

(ii) 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 subcortracted work only on our personal computers or personal computers of Group companies that have been confirmed and guaranteed to have the same level of security software as LY Corporation.

As individual cases, some subcontractors have undergone the approval process by our CISO to be exempted from using our loanedPCs for reasons such as restrictions on the use of loaned devices to ensure the security of the entire operations of the subcontractor.[*1] Except for these subcontractors, we have completed the lending of personal computers to (i) subcontractors that can access our network using accounts issued by us and (ii) subcontractors other than those in (i) that can access our network and are involved in our business but to which personal computers had not previously been loaned. [Completed at the end of September 2024]

As an additional measure, we decided to expand the scope of the subcontractors to whom we will lend LY Corporation's personalcomputers by including those who can access our network other than those in (i) and (ii) above, and will begin lending personal computers to these subcontractors from October 2024. [Scheduled to be completed by the end of March 2025]

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

[1]Although this is a temporary measure that has been approved by our CISO not to loan LY Corporation's personal computers, we are reviewing our response, including a review of the outsourced work.

Corrective Actions for Inadequate Organizational Safety Management Measures—1 (3/4)

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

As reported on June 28, 2024, in addition to on-site inspections, audits based on the content of the outsourcing were 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. 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 conducted a survey regarding security to all employees as part of the improvement activities to establish a system to communicate potential risks that employees normally perceive but do not necessarily materialize. **[Survey conducted in July 2024, and a survey regarding the LY Corporation Group Code of Conduct is scheduled to be implemented in November 2024]**

The response rate of the survey conducted was 98%, and approximately 1,500 comments were received in the free response section. We have shared these opinions with management and have begun implementing and considering initiatives to resolve issues.

We plan to disclose these initiatives and results to our employees.

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

*1 Audits on suppliers of specified critical facilities and subcontractors maintaining and managing such facilities based on the Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures.
*2 Audits on subcontractors maintaining and operating critical systems as determined by LY Corporation.

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

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

As reported on June 28, 2024, we have examined and formulated the basic approach and specific scope and policy for terminating or reducing the scope of the outsourcing relationship, including the use of the systems and services provided by NAVER, and have also formulated a specific plan for achieving this. Works on actually terminating or reducing the scope of the relationship have already begun and are currently being performed as planned without delay.

[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]

[Technology and system usage, service planning, functions, and development consignments: targeted by the end of March 2026]

In addition, the risk assessment for the remaining operations began in July 2024, and the assessment was completed at the end of September 2024. [Completed at the end of September 2024]

Please note that we have formulated an action plan for operations that were deemed to require additional measures based on an assessment conducted by our security division. The action plan (which outlines the content of additional measures and a completion deadline) was established in consultation with the parties involved in each operation.

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

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

ii) 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

We have added the definition of critical systems and additional safety management measures for the critical systems to the detailed rules that define the security requirements for each life cycle stage of our information systems, and the critical systems have been identified according to the definitions. [Completed the addition to the detailed rules on July 1, 2024. Identification of critical systems completed in September 2024.]

The following are scheduled to be implemented:

- Confirmation of compliance with safety management measures for the critical systems. [Scheduled to be completed by early October 2024]
- Risk assessment of non-compliance with safety management measures for the critical systems. [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]

Note: The status of implementing or considering the measures, etc. is as of September 30, 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

Based on a plan evaluated by an external organization, we are working on the initial action flow when an incident occurs, process for determining the scope of investigation, and the identification of stakeholders and their roles and responsibilities, etc. [Scheduled to be completed in October 2024]

In addition, we are preparing for the periodic exercises to secure effectiveness as scheduled. [Periodic exercises scheduled to be conducted in between October 2024 and March 2025]

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

Regarding the SOC Tier 1 monitoring, which was previously outsourced to NAVER Cloud, we have completed the necessary training to the Japanese company to which the monitoring will be switched. Temporary operation has begun from July 2024. As originally planned, 24/7 monitoring will be conducted with the Japanese company from October 1, 2024 (outsourcing to NAVER Cloud will be terminated). [Scheduled to begin operation from October 2024]

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

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 Formation of the Security Governance Committee

The Security Governance Committee, established in April 2024, has discussed the overall security governance of the Company, including reports from internal projects such as recurrence prevention, and policy decisions. From July 2024 in particular, the Committee has continued to check the progress of each project related to matters such as recurrence prevention and has provided feedback, etc. The Committee works to share awareness of recurrence prevention and improving security governance throughout the Company by measures such as regularly sharing the status of discussions, etc., with our corporate officers.

2 Establishment of the Group CISO Board

The Group CISO Board, established in April 2024, continues to discuss the common application of recurrence prevention measures implemented by our company to all Group companies as a priority agenda, and has also begun discussions on rules common to Group companies, such as the application of common security regulations. Through these efforts, we will work to standardize and raise the level of security across the Group.

Note: The status of implementing or considering the measures, etc. is as of September 30, 2024.

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.”