Report Submitted on July 1 in Response to MIC's Administrative Guidance on March 5 and April 16, 2024 (Summary)

July 1, 2024

LINEヤフー

Introduction

This document is a summary of the report submitted on July 1, 2024, in response to the administrative guidance issued by Japan's Ministry of Internal Affairs and Communications (“MIC”) on March 5, 2024, and April 16, 2024.

This document describes the progress of the fundamental review and strengthening of safety management measures and subcontractor management, as well as the essential review and reinforcement of security governance across the entire Group, including the parent company, etc.

We will make continued effort 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

Report on MIC's Administrative Guidance Dated March 5, 2024 (Summary) (Published April 1, 2024)
https://www.lycorp.co.jp/en/news/2024/20240401_appendix_ja.pdf

Table of Contents

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident"

MIC's administrative guidance dated April 16, 2024

(1) Accelerating the fundamental review and strengthening of safety management measures and subcontractor management in light of this incident

- Regarding the review of safety management measures and subcontractors for which no clear implementation plan has yet been formulated at this stage, formulate and submit a plan at an early stage and steadily proceed with the review. (In particular, promptly formulate and implement a clear plan for the separation of network that were common between your company and NAVER Corporation ("NAVER")).

- Steadily implement the measures that are planned to be implemented in the future, and where possible, implement them ahead of schedule.

- Regarding the measures that have been implemented so far and those that are scheduled to be implemented within one year (especially the separation of the authentication system and the independent operation of SoC operations), continue to verify the progress and effectiveness of these plans to ensure that they are sufficient to prevent recurrence, and take additional measures as necessary.

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 1 (1/2)

Matters reported
(Excerpt)

No. 1 Separation of private networks between NAVER Cloud Corporation ("NAVER Cloud") and LY Corporation

1. Additional measures to strengthen network access management

Regarding network access from the NAVER Cloud data center to the data center of former LINE Corporation ("LINE"), a firewall has been installed to permit only necessary communications and deny all other communications. [Completed in March 2024]

As an additional measure, 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 by the end of August 2024 and implemented based on the plan thereafter]

2. Additional measures regarding the application of two-factor authentication to employees' 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. [Considering moving up the completion to end of October 2024]

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 1 (2/2)

Matters reported (Excerpt)

No. 1 Separation of private networks between NAVER Cloud and LY Corporation

3. Separation from 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[*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 plan has been accelerated and the target completion date for overseas subsidiaries is now the end of March 2026[*3]] For details, please refer to the supplementary materials.

While sequentially separating systems for domestic and overseas subsidiaries, we will counter the risks that arise during this period by applying two-factor authentication to systems, scrutinizing the scope of access, and blocking unnecessary communications on an ongoing basis.

4. Complete separation of private networks

We have reviewed the firewall policy and changed the configuration in the course of relocating servers/data to Japan.[*4] In addition, we have deleted firewall policies that were judged unnecessary during configuration maintenance conducted once every three months. [Completed in June 2024]

Going forward, we will proceed with the plan to review our consignments and blocking of telecommunications in phases accompanying the system separation. [Planned completion date brought forward to the end of March 2026[*3]]

[*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.
[*3] The original completion date was the end of December 2026.
[*4] Explanation of LINE data transfer: https://www.lycorp.co.jp/ja/news/announcements/000823/ (Japanese only)

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 2

Matters reported (Excerpt)

No. 2 Separation of authentication system

1. Additional measures regarding the separation of authentication system in the system managed by LY Corporation

The separation of the authentication system of the systems managed by LY Corporation was completed at the end of March 2024. Based on the logs received from NAVER Cloud, we confirmed that the authentication integration settings from NAVER Cloud's authentication system to our systems had been deleted, making authentication impossible. [Completed in June 2024]

2. Deletion of employee information, etc. from NAVER's authentication system and suspension of password linkage to the authentication system of LY Corporation

As part of operational separation, we have deleted unnecessary employee information of our Group companies from the NAVER authentication system and suspended password linkage to our authentication system. [Completed in June 2024]

We will continue to delete some employee information, etc. that remains in the NAVER authentication system at the NAVER Cloud data center. [Scheduled to be completed in April 2025 for LY Corporation and its domestic subsidiaries, and April 2026 for overseas subsidiaries]

For the risks that remain for some employee information, etc., the following measures have been performed:

- Deletion of information items/authentication information out of this employee information, etc.
- Reconfirmation that there are no system at our data center that uses the authentication information possessed by NAVER's authentication system.

3. Suspension of the use of authentication system for systems managed by NAVER and NAVER Cloud

- We prioritized the separation of the authentication system for systems managed by LY Corporation and its Group subsidiaries, where authentication functions can be switched by LY Corporation, and as described on page 1, we have resolved the situation in which the authentication system and authentication information were shared with NAVER. [Completed in June 2024]
- Suspension on the use of the authentication system for systems managed by NAVER and NAVER Cloud will be implemented as follows. [Scheduled to be completed by the end of March 2025 for LY Corporation and by the end of March 2026 for its Japanese subsidiaries. The plan has been accelerated and the target completion date for overseas subsidiaries is now the end of March 2026[*1]]

[*1] The original completion date was the end of December 2026.

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 3

Matters reported (Excerpt)

No. 3 Switching SOC to a Japanese company and log acquisition

1. Independent operation of SOC

Regarding the monitoring of logs managed by NAVER Cloud, we have completed the migration to a Japanese company as planned and have already transitioned to monitoring using logs in Japan. [Completed in March 2024]

We have switched the outsourcing of our SOC Tier 1 monitoring operations, which were previously outsourced to NAVER Cloud, to a Japanese company, and intend to steadily carry out this work as originally planned, while ensuring quality and effectiveness. [Scheduled to begin operation in October 2024]

With this measure, log data, analysis systems, and Tier 1 monitoring operations will be transferred to Japan, making it possible to complete all SOC operations in Japan. We believe this will enable a more rapid response to security incidents.

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

In conjunction with the plan mentioned above, we will improve our incident response system as part of our efforts to achieve more rapid response to security incidents.

Specifically, 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 periodic exercises scheduled to be conducted in the second half of FY2024]

Status of implementation of measures described in the report dated April 1, 2024, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 4 (1/2)

Matters reported (Excerpt)

No. 4 Review of safety management measures

1. Additional measures to correct AD management

A behavior-based detection solution was introduced to AD in December 2023, and in order to verify that the solution is effective in preventing recurrence, the attack methods that were insufficiently detected in this incident was simulated and it has been confirmed that the solution can properly detect such cases. [Completed in January 2024]

2. Additional measures to reinforce access management of critical systems

As an additional measure to continue verifying the effectiveness of the measures and to sustainably improve the security level of critical systems, we have defined critical systems and the required standards of safety management measures, and established a system for company-wide understanding and evaluation of the current status of data storage in each system, security measures in place, and associated risks, with the participation of the top management. These definitions and systems have been established as our company regulation. [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]

3. 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]

Status of implementation of measures described in the April 1, 2024 report, "I. Fundamental review and strengthening of safety management measures and contractor management in light of this incident" — No. 4 (2/2)

Matters reported (Excerpt)

No. 4 Review of safety management measures

4. Implementation of penetration tests

Penetration tests will be conducted by an outside firm to verify the sufficiency and effectiveness of measures to prevent recurrence of this incident, as well as to conduct a comprehensive risk assessment, including our preparedness for unknown threats, in order to identify additional measures that are necessary and to formulate more effective security measures and improvement plans.

- 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]

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

Based on the recommendations from an outside firm in "3. Formulation of plans with an outside firm " (see page 8 of this document), we will reevaluate the behavior-based detection systems and correlation analysis rules currently in operation at our data centers.

- 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]

Status of implementation of measures described in the April 1, 2024 report, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 5 (1/2)

Matters reported (Excerpt)

No. 5 Review of subcontractor management

1. Additional measures regarding the review of security risk assessment criteria

We conduct audits using the newly established and updated security checklists. [New checklist completed in March 2024; to be updated sequentially]

2. Additional measures regarding the study of supervision methods and formulation of standards to achieve effective subcontractor management

Referring to the models used by external companies, we have formulated standards to improve the management of our subcontractors. Through the actual implementation of these standards, we will take necessary additional measures based on individual events that arise after the start of the implementation. In considering additional measures, we will seek advice from outside firms, as we did when the standards were established, and consider further upgrading the subcontractor management model while incorporating objective external perspectives. [Formulation of standards completed in March 2024; standards to be sequentially applied thereafter]

3. Status of implementing two-factor authentication when connecting to LY Corporation's data center via VPN

We have completed the implementation of two-factor authentication when logging in or accessing our network. [Completed in January 2024]

Status of implementation of measures described in the April 1, 2024 report, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 5 (2/2)

Matters reported (Excerpt)

No. 5 Review of subcontractor management

4. Management and auditing of subcontractors based on established standards

Regarding the auditing based on the standards formulated to enhance the management of subcontractors, we will gradually start implementing the new standards from July 2024. As a preliminary implementation of the new standards from April 1, we conducted audits based on the new standards. We also started trial operations targeting some of our subcontractors from May 15, and have tested multifaceted risk assessments 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 the implementation of the new standards. In considering such additional measures, we will seek advice from outside firms, as we did when the standards were established, to incorporate objective, external perspectives, and will consider further upgrading the subcontractor management model. [Preparation for operation to be completed in July 2024, with operation to commence sequentially thereafter]

5. Lending of LY Corporation's personal computers to subcontractors who can access our network using accounts issued by us

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]

Status of implementation of measures described in the April 1, 2024 report, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 6

Matters reported (Excerpt)

No. 6 LY Corporation's corrective measures on NAVER Cloud

1. Additional measures regarding audits by LY Corporation and third-parties on NAVER Cloud

We conducted an on-site inspection of NAVER Cloud with a third-party company. During the inspection, we reconfirmed NAVER Cloud's implementation of measures to prevent a recurrence, as well as confirmed 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 February 2024]

2. Status of audits by LY Corporation and third-party companies to the subcontractors involved in this case, and contract terminations

We conducted an on-site inspection and terminated the contract at the end of March 2024. [Completed at the end of March 2024]

3. Continuation of regular audits on 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]

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

Status of consideration of measures described in the report dated April 1, 2024, “II. Essential review and strengthening of security governance across the entire Group, including the parent company, etc." —No. 1

MIC’s administrative guidance dated April 16	**(2) Accelerating the essential review of security governance across the entire Group, including the parent company, etc.** • Regarding the "policy to gradually reduce and terminate the outsourcing relationship with NAVER" mentioned in the report, report on the basic approach and specific scope of the "outsourcing to NAVER" that is the subject of this policy. In particular, clarify whether the use of systems and services provided by NAVER is included in the scope of the reduction/termination. • Based on the above, formulate and report on a specific plan for realizing the "policy to gradually reduce and terminate the outsourcing relationship with NAVER" (which consignment will be reduced, terminated, or retained, and by when).
Matters reported (Excerpt)	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 details, please refer to the supplementary materials. 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.] For details, please refer to the supplementary materials.

Status of consideration of measures described in the report dated April 1, 2024, “II. Essential review and strengthening of security governance across the entire Group, including the parent company, etc." — No. 2

MIC’s administrative guidance dated April 16	**(2) Accelerating the essential review of security governance across the entire Group, including the parent company, etc.** • Promptly conduct a Group-wide review, including the parent company, etc., of the top management system for proper management and supervision of subcontractors, including a review of the relationship in which your company is subject to substantial capital control from the subcontractors, and report the results of such review in detail.
Matters reported (Excerpt)	**1. Review of capital ties** Since the administrative guidance on March 5, 2024, we have requested SoftBank Corp. and NAVER, the shareholders of LY Corporation's parent company: A Holdings Corporation, to review the capital relationship of A Holdings Corporation, as one of the measures to review the relationship in which we are subject to substantial capital control from the subcontractors. However, we have been informed that both companies recognize the difficulties associated with short-term capital movements between them at this time.Both companies have been cooperative in their response, and we intend to continue working to advance progress in the discussions. **2. Review of our top management structure** Following approval at our General Meeting of Shareholders held in June 2024, we have established a structure of six directors, four of whom are independent outside directors serving on the Audit and Supervisory Committee, as of this General Meeting of Shareholders. We believe that this will help strengthen governance. **3. Establishment of a system to ensure security governance** A steering committee consisting of the CEOs of our company and NAVER has been holding discussions since April 2024 regarding the termination of outsourcing. 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. In addition, 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.

Status of implementation of measures described in the April 1, 2024 report, ”III. Thorough customer support"

MIC’s administrative guidance dated April 16

(3) Thorough response to users through regular publication of progress reports on initiatives

- Continue to monitor the occurrence of secondary damage and provide appropriate information to users regarding this incident, and endeavor to ensure user understanding by, for example, publishing regularly updated information on the initiatives and their progress in (1) and (2) above.

Matters reported (Excerpt)

1. Responding to users through regular publication of progress reports on initiatives

On April 1, 2024, we published a dedicated webpage on our corporate website summarizing the details of this incident and the progress being made in preventing recurrence. We are providing information on the progress of our various responses to the "Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" described in the guidance document dated March 5, 2024. In addition, based on the administrative guidance dated April 16, 2024, we have published on the dedicated webpage the progress made, including "an essential review and strengthening of security governance throughout the entire Group, including the parent company," as well as plans and implementation status for terminating the outsourcing to NAVER, in conjunction with the submission of the report.

2. Response when secondary damage is discovered

As part of our efforts to recognize the occurrence and possibility of damage due to unauthorized access that we are not yet aware of, we are continuously monitoring the dark web and other such sources. Until a reasonable time has elapsed, we will strengthen such monitoring, and strive for early detection of secondary damage and prevention of its spread. In the event that information leakage is confirmed, we will promptly notify users.

Although no secondary damage has been confirmed at the time of submitting this report, we will continue to promptly investigate any reports of secondary damage received from users at our permanent customer support desk, and if we confirm the occurrence of secondary damage, we will take the necessary measures in an appropriate manner.

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, Japan’s Ministry of Communications and Information is described as “MIC,” the former LINE Corporation as “LINE,” NAVER Corporation as “NAVER,” and NAVER Cloud Corporation as “NAVER Cloud.”