Report Submitted on March 31, 2025 in Response to MIC's Administrative Guidance on March 5 and April 16, 2024 (Summary)

March 31, 2025

LINEヤフー

Introduction

This document is a summary of the report submitted on March 31, 2025, 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 efforts to prevent recurrence.
Going forward, we will continue to report to the MIC regarding the progress of our current recurrence prevention measures.

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/

Table of Contents

01 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"

02 Status of consideration of measures described in the report dated April 1, 2024, “II. Essential review and reinforcement of security governance across the entire Group, including the parent company, etc."

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

The response and consideration status as of March 31, 2025, regarding the above matters are described from the following page onward.

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

Matters reported (Excerpt)

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

1. 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. For systems used by our company, we have completed all system transitions and suspended the use of old systems as of the end of March 2025, except those required for accounting audits and tax reporting.
For systems used by our Japanese and non-Japanese subsidiaries, we are currently working on the separation projects according to the project plans formulated for each target system.
[For employee systems,*[1] the transition has been completed for LY Corporation at the end of March 2025.*[2] The transition is scheduled to be completed by the end of March 2026 for Japanese subsidiaries, and the target completion date for subsidiaries outside of Japan is the end of March 2026.]

2. Complete separation of private networks from NAVER Cloud’s data centers to former LINE’s data centers

Regarding network access from the NAVER Cloud data center to the data center of former LINE Corporation, a firewall has been installed to permit only necessary communications and deny all other communications. [Completed in March 2024]
Subsequently, we have been blocking unnecessary communications as outlined below.

- We have reviewed the firewall policy and changed the configuration in the course of relocating to Japan*[3] the servers/data related to users in Japan, among servers for the production environment of LY Corporation’s services which use NAVER Cloud’s infrastructure. [Completed in June 2024]
- Regarding the telecommunication between servers for the production environment of former LINE’s services which use NAVER Cloud’s infrastructure and servers in the data centers of former LINE, we have blocked all communications accompanying the suspension of the relevant servers. [Completed at the end of March 2025]
- Furthermore, we have blocked unnecessary communications after separating from systems that were managed by NAVER and NAVER Cloud and terminating consignments to these companies. [Completed at the end of March 2025]

Going forward, we will continue to block unnecessary communications accompanying the completion of separation of systems used by Japanese and non-Japanese subsidiaries, etc. We will also perform configuration maintenance on firewall policies every three months. [Target completion date: end of March 2026]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

*[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] Systems containing data used for accounting audits and tax reporting will be suspended in June 2025.
*[3] 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. 1

Matters reported (Excerpt)

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

3. Additional measures to strengthen network access management

We conducted a comprehensive inspection on the appropriateness of network access control and incident response preparedness for paths connecting the outside environment with the data center of former LINE Corporation, and 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, correction completed at the end of September 2024]

Regarding communication control from the data center of former LINE to the data center of NAVER Cloud, an inspection of unnecessary communication was completed at the end of December 2024 based on the abovementioned comprehensive inspection, and firewall policies that needed corrective action were modified and deleted. [Completed in February 2025]

Furthermore, we have blocked unnecessary communications from former LINE’s data centers to NAVER Cloud’s data centers after separating from systems that were managed by NAVER and NAVER Cloud and terminating consignments to these companies. [Completed at the end of March 2025]

Going forward, we will continue to review the firewall policies.

4. 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 bringing in of smartphones are not allowed, 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]

Lastly, the application of two-factor authentication was completed at the end of October 2024 for some systems in former Yahoo Japan Corporation’s data centers to which two-factor application was not applied. As a result, two-factor authentication has been applied in all internal systems used by our employees. [Completed at the end of October 2024]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

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 & No. 3

Matters reported (Excerpt)

No. 2 Separation of authentication system

2. Measures regarding the separation of authentication system in our management system

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]

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

We have deleted unnecessary employee information of our Group companies from the NAVER authentication system and suspended password linkage 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 Japanese subsidiaries, and by the end of April 2026 for subsidiaries outside of Japan]

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

For our company’s systems that were managed by NAVER and NAVER Cloud, we have suspended the use of the authentication system as a result of the system separation at the end of March 2025. The authentication system is scheduled to be suspended for systems used by our Japanese and non-Japanese subsidiaries as well after the system separation conducted by the end of March 2026. [Completed for LY Corporation at the end of March 2025, and scheduled to be completed by the end of March 2026 for Japanese subsidiaries. Target completion date for subsidiaries outside of Japan: end of March 2026]

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

1. Independent operation of SOC operations

We have established a log collection/analysis system and obtained logs at our data centers. Regarding the SOC Tier 1 monitoring that was previously outsourced to NAVER Cloud, we have started conducting 24/7 monitoring in Japan with a Japanese company (ending our consignment with NAVER Cloud) from October 1, 2024. [Operations began from October 2024]

Additionally, we have established a system and environment to collect log information from the NAVER Cloud environment, which is not currently integrated into the above-mentioned log collection/analysis system. [Completed at the end of March 2024]

2. 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 have completed the establishment of an 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. [Completed in October 2024]
Furthermore, to ensure the effective implementation of the above, we began periodic exercises in December 2024 and have conducted them multiple times by March 2025. The exercises will continue to be conducted from April 2025 onwards. [Completed conducting periodic exercises multiple times between December 2024 and March 2025]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

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

Matters reported (Excerpt)

No. 4 Review of safety management measures

1. Correction of AD management

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 in December 2023.
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]

Furthermore, in addition to these measures, we corrected the AD management based on the consulting received from an outside firm. [Completed in March 2024]

2. Reinforcing access management of critical systems

Of the systems used by our employees within the former LINE environment, we have defined critical systems as those that handle important information, including personal data, and if compromised, would increase the risk of unauthorized access to these systems.

Among the critical systems in the former LINE environment, a security assessment was performed by the end of March 2024 for those that have web interfaces to determine if there were any attempts to bypass the authentication process or ways in which authentication factors could be exploited. The identified vulnerabilities have been fixed. [Completed at the end of March 2024]

3. Additional measures to reinforce access management 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. [Establishment of internal regulations completed on July 1, 2024.]

We have confirmed the compliance status of target critical systems based on confirmation items selected from safety management measures that are stipulated in our security regulations. [Completed in October 2024]

Items that were found to be in non-compliance with safety management measures have been corrected. [Completed at the end of December 2024]

The above efforts will be conducted regularly from April 2025 onwards to improve security of our critical systems. Furthermore, as a plan for reviewing safety management measures in line with current trends, we have detailed a 12-month cycle review process for the safety management measures and have established an implementation plan. [Completed in November 2024]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

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

Matters reported (Excerpt)

No. 4 Review of safety management measures

4. Formation 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]

5. Performance of penetration tests

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]

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.

6. Additional measures based on results of implementing penetration tests

Based on an action plan established at the end of August 2024, we have undertaken corrective actions for findings identified through the tests, considered mechanisms for correction, and improved the operational process. [Completed at the end of March 2025]
We will continue to implement the established mechanism and regularly monitor the improvement status.

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

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 mechanisms for behavior-based detection and correlation analysis rules. [Completed at the end of August 2024]

8. Additional measures based on results of reviewing mechanisms for behavior-based detection, etc. and correlation analysis rules, etc.

Based on the effectiveness verification results regarding mechanisms for behavior-based detection and correlation analysis rules, all detection rules were implemented in our SIEM*[1] environment as planned. [Correction completed in February 2025]
Going forward, we will continue to review the detection rules.

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

*[1] A system for aggregating, managing, and conducting correlated analysis of various logs and is utilized for the early detection of security incidents.

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. 5

Matters reported (Excerpt)

No. 5 Review of subcontractor management

2. Review of security risk assessment criteria

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

3. Consideration 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]

4. Operational status of the application two-factor authentication when connecting to the VPN of our company’s data centers

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

5. Management and auditing of subcontractors based on established standards

As an operation of new standards from July 1 based on the Basic Policy on Management of Subcontractors and the Basic Rules on Management of Subcontractors, which came into effect on July 1, 2024, we have started evaluating suppliers and project risks and are conducting risk management based on the evaluation results. In addition, the operation has been established so that it is not possible to conclude contracts or place orders unless these supplier and project risk evaluations have been completed. Since adopting the new standards, operations have been running smoothly without any significant issues. [Operations began in July 2024]

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

We have completed lending personal computers (PCs) at the end of September 2024 for (i) subcontractors that can access our network using accounts issued by us and (ii) other subcontractors who are involved in our business but to which PCs had not previously been loaned. Regarding the additional measure of lending PCs to those beyond (i) and (ii) above who can access our network, we have completed lending PCs by the end of March 2025. With the completion of PC lending, we have also finished blocking access from PCs not loaned by LY Corporation and deleting accounts deemed unnecessary. However, in certain individual cases where the security of the contractor's overall operations necessitates restrictions on bringing in loaned devices, contractors who have undergone an approval process by our CISO and implemented risk mitigation measures are exempt from access restrictions.
[Completed lending PCs to contractors in categories (i) and (ii) at the end of September 2024 and to other contractors with access to our network at the end of March 2025]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

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. 6

Matters reported (Excerpt)

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

1. Additional measures regarding inspection of NAVER Cloud with a third-party company

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 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]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

*[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.

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 & No. 2

MIC's administrative guidance dated April 16, 2024

(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)

We have examined and formulated the basic approach, 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.
Furthermore, additional measures based on risk assessment results are also being implemented according to plan for remaining operations.
[Outsourcing from LY Corporation to NAVER and NAVER Cloud: targeted by the end of December 2025*1]
[Outsourcing from LY Corporation to other NAVER Group companies: completed at the end of March 2025]
[Technology and system usage, service planning, functions, and development consignments: targeted by the end of March 2026]

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

*1 The outsourcing from LY Corporation to NAVER and NAVER Cloud for employee systems that Japanese and non-Japanese subsidiaries will continue to use until the end of March 2026 will be terminated with the completion of the system separation at the end of March 2026.

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. 3

MIC's administrative guidance dated April 16, 2024

(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 A Holdings Corporation (LY Corporation's parent company), 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. We have continued to make this request for one year. However, we have been informed that there is no change in the recognition that short-term capital movements between the two companies remain difficult at this time. Based on the circumstances up to now, we intend to continue working to facilitate 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 continues to hold discussions regarding the termination of outsourcing.

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 is also continuously discussing 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.

In addition, 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. In particular, the Committee is continuously checking the progress of projects related to matters such as recurrence prevention and providing feedback, etc.

Note: The implementation and consideration status as of March 31, 2025.

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

MIC’s administrative guidance dated April 16, 2024

(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)

No. 1 Responding to users through regular publication of progress reports on initiatives

We continue to provide information on our efforts to prevent recurrence in the dedicated webpage on our corporate website, launched on April 1, 2024.

No. 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.

Note: The status of implementing or considering the measures, etc. is as of March 31, 2025.

Reference Materials

Past 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_en.pdf

Report Submitted on July 1 in Response to MIC’s Administrative Guidance on March 5 and April 16, 2024 (Summary)
(published July 1, 2024)
https://www.lycorp.co.jp/en/news/2024/20240701_appendix1_en.pdf

Future Policies and Plans Regarding the Outsourcing Relationship with NAVER Corporation (published July 1, 2024)
https://www.lycorp.co.jp/en/news/2024/20240701_appendix2_en.pdf

Report Submitted on September 30 in Response to MIC’s Administrative Guidance on March 5 and April 16, 2024 (Summary)
(published September 30, 2024)
https://www.lycorp.co.jp/en/news/2024/20240930_1_appendix_en.pdf

Report Submitted on December 27 in Response to MIC's Administrative Guidance on March 5 and April 16, 2024 (Summary)
(published December 27, 2024)
https://www.lycorp.co.jp/en/news/2024/20241227_1_appendix_en.pdf

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.”