# Report Submitted on December 27 in Response to MIC's Administrative Guidance on March 5 and April 16, 2024 (Summary)

December 27, 2024

LINEヤフー

# Introduction

This document is a summary of the report submitted on December 27, 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 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/

# Table of Contents



The following pages contain details on the implementation and consideration status as of December 27, 2024, for the abovementioned points.

# 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. Additional measures to strengthen network access management**

We will continue to conduct regular inspections and reviews of network access control on connection routes between the external environment and former LINE's data centers, and will work to maintain and improve it on an ongoing basis.
Regarding outbound communication control from former LINE's data centers to NAVER Cloud's data centers, firewall policies were sequentially applied based on the drafted plan, and an inspection of unnecessary communication was completed at the end of December 2024. Additionally, we have established an application process in preparation of adding new firewall policies for outbound communication. Going forward, we will perform continuous maintenance of the firewall policies.
[Application of firewall policies for outbound communication completed in October 2024, inspection completed in December 2024]

**2. Additional measures regarding the application of two-factor authentication to employees' systems**

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]

**3. Separation from systems of NAVER and NAVER Cloud**

As reported on July 1, 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] is 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 subsidiaries outside of Japan is the end of March 2026.]

**4. Complete separation of private networks**

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 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 December 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]

Note: The implementation and consideration status as of December 27, 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.

# 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**

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

As reported on July 1, 2024, 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]

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

As reported on July 1, 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. Target completion date for subsidiaries outside of Japan: the end of March 2026]

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

**1. Independent operation of SOC**

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, as originally planned. [Operations began from October 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]

Additionally, to ensure the effective implementation of the above, periodic exercises began in December 2024 and are scheduled to be conducted multiple times by March 2025. The exercises will continue to be conducted from April 2025 onwards.
[Periodic exercises scheduled to be conducted multiple times between December 2024 and March 2025]

Note: The implementation and consideration status as of December 27, 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. 4

**Matters reported (Excerpt)**

**No. 4 Review of safety management measures**

**1. Additional measures to reinforce access management of critical systems**

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]

**2. Additional measures based on results of implementing penetration tests**

Based on a corrective action plan established at the end of August 2024, we are sequentially addressing the findings identified through the tests in order of priority. [Scheduled to be completed at the end of March 2025]

**3. 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, some detection rules were implemented in our SIEM*1 environment in December 2024. Going forward, we will sequentially make corrections to improve detection capabilities using our SIEM environment. [Correction scheduled to be completed in February 2025]

Note: The implementation and consideration status as of December 27, 2024.

*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 April 1, 2024 report, "I. Fundamental review and strengthening of safety management measures and subcontractor management in light of this incident" — No. 5 & No. 6

**Matters reported (Excerpt)**

**No. 5 Review of subcontractor management**

**1. 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. [Operation started in July 2024]

**2. 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), blocked access from PCs not loaned by LY Corporation, and deleted unnecessary accounts 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 personal computers had not previously been loaned. PC lending excludes subcontractors who have undergone the approval process by our CISO for reasons such as restrictions on bringing in loaned devices to ensure the security of the entire operations of the subcontractor.*1 [Completed lending of PCs at the end of September 2024, blocked access in October 2024, and completed deletion of accounts that were deemed unnecessary thereafter]

Regarding the additional measure of expanding the scope of subcontractors and lending PCs to those beyond (i) and (ii) above who can access our network, we have identified the target companies and are currently establishing a PC lending process. [Scheduled to be completed by the end of March 2025]

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

**1. Continuation of regular audits on NAVER Cloud**

As reported on July 1, 2024, in addition to on-site inspections, audits based on the content of the outsourcing were completed by the end of April 2024*2 and the end of June 2024.*3 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 implementation and consideration status as of December 27, 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.
*2 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.
*3 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** | **(2) Accelerating the essential review of security governance across the entire Group, including the parent company, etc.**<br>• 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.<br>• 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)** | As reported on July 1, 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.<br>Furthermore, additional measures based on risk assessment results are also being implemented according to plan for remaining operations.<br>[Outsourcing from LY Corporation to NAVER and NAVER Cloud: targeted by the end of December 2025]<br>[Outsourcing from LY Corporation to other NAVER Group companies: targeted by the end of March 2025]<br>[Technology and system usage, service planning, functions, and development consignments: targeted by the end of March 2026] |

Note: The implementation and consideration status as of December 27, 2024.

# 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** | **(2) Accelerating the essential review of security governance across the entire Group, including the parent company, etc.**<br>• 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**<br>As reported on July 1, 2024, 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. However, we have been informed that both companies recognize the difficulties associated with short-term capital movements between them at this time. Based on the circumstances up to now, we intend to continue working to facilitate progress in the discussions.<br>**(2) Review of our top management structure**<br>As reported on July 1, 2024, 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.<br>**(3) Establishment of a system to ensure security governance**<br>A steering committee consisting of the CEOs of our company and NAVER continues to hold discussions regarding the termination of outsourcing.<br>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.<br>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 December 27, 2024.

# 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)**

**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 reported on July 1, 2024, 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 implementation and consideration status as of December 27, 2024.

# 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

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."