Report Submitted on September 30 in Response to MIC's Administrative Guidance on March 5 and April 16, 2024

(Summary)

September 30, 2024

LINEヤフー

Introduction

This document is a summary of the report submitted on September 30, 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 on April 1, 2024)
https://www.lycorp.co.jp/en/news/2024/20240401_appendix_ja.pdf

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

https://www.lycorp.co.jp/en/news/2024/20240701_appendix2_en.pdf

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 following pages contain details on the implementation and consideration status as of September 30, 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 (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

We conducted a comprehensive inspection on the appropriateness of network access control andand incident response preparedness for paths connecting the outside environment with the data center of former LINE Corporation ("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]

2. Additional measures regarding the application of two-factor authentication to employees' 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 implementation and consideration status 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.

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

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 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.]

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 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]

Note: The implementation and consideration status 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.

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 domestic subsidiaries, and by the end of April 2026 for overseas subsidiaries]

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 Cloudwill 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 overseas subsidiaries: 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, 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]

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 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]

Note: The implementation and consideration status as of September 30, 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 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]

2. Implementation 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]

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.

3. 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 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 implementation and consideration status as of September 30, 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 & No. 6

Matters reported (Excerpt)

No. 5 Review of subcontractor management

1. Management and auditing of subcontractors based on established standards

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]

2. 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 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 loaned PCs 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 personal computers 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]

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 was 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 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.
[*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.

- 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)

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.

[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 implementation and consideration status as of September 30, 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. 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 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.

2. Review of our top management structure

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.

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 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.

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. 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.

Note: The implementation and consideration status as of September 30, 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)

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.

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 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, 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.”