Report on MIC’s administrative guidance dated March 5, 2024 (Summary)

April 1, 2024

LINEヤフー

Introduction

On November 27, 2023, LY Corporation reported its incident on the information leakage due to unauthorized access.

This incident was triggered by malware which infected a personal computer owned by an employee of a subcontractor used by NAVER Cloud Corporation and LY Corporation. The initial unauthorized access to our servers' internal system began on September 14, 2023. Since NAVER Cloud and LY Corporation shared an in-house system for dealing with employee and other personnel information that is managed with a common authentication system, this allowed network access into the system of the former LINE Corporation, and thus causing unauthorized access by a third party into our system via NAVER Cloud's system on October 9, 2023. As a result, this led to the information leakage of users, business partners, employees, and other personnel.*

We deeply recognize the gravity of this incident, which undermines the trust held in us as a platform operator with an extensive user base. We are committed to earnestly preventing such occurrences in the future.

We have received administrative guidance from Japan's Ministry of Internal Affairs and Communications on March 5, 2024. Based on this guidance, we submitted a report on April 1, 2024.

This document is a summary of the report submitted to MIC.
For more information on the response status and future schedule, please refer to the dedicated page on the incident on our corporate website.

https://www.lycorp.co.jp/en/privacy-security/recurrence-prevention/

*Employees and other personnel of LY Corporation and its group companies, NAVER Group companies, subcontractors, and temp agencies.

Table of Contents

01 Report on the Review of Safety Management Measures, Etc.

02 Report on the Review of Subcontractor Management Measures, Etc.

03 Report on the Review of Group-Wide Security Governance, Etc.

04 Report on Thorough Customer Support

Review of Safety Management Measures, Etc. - 1

Guidance (1)-(i)(a)	There was a network connection between the former LINE environment and NAVER Cloud, which allowed NAVER Cloud to have broad access to the network and internal systems of the former LINE environment. Thus, intrusion into NAVER Cloud 's systems and terminals resulted in unauthorized access to LY Corporation's servers and systems. Considering that this was the factor leading to this incident, establish a system that allows only the truly minimum necessary access to LY Corporation's network and internal systems from NAVER's systems and terminals and otherwise does not allow any other access. Establishing such a system includes installation of firewalls, closing of unnecessary ports, elimination of internal telecommunication, and others. In addition, consider and take concrete measures to ensure the full protection of LY Corporation's servers, network, and internal systems.

Matters reported (Excerpt)

(1) Blocking of unnecessary telecommunication

The broad network access from the NAVER environment to the former LINE environment was the cause of the unauthorized access to our system in this incident. Considering this cause, as one of the measures to prevent a recurrence, we have configured the network access settings from the NAVER environment to the former LINE environment and installed a firewall between the two environments. As a result, only necessary telecommunication will be allowed, and all other telecommunication will be denied. (Completed in March 2024)

Moving on, by June 2024, we will proceed with the formulation of a review plan on consignments and blocking of telecommunication in phases accompanying the system separation.

(2) Application of two-factor authentication

Since servers and systems with two-factor authentication escaped the unauthorized access in this incident, we increased the strength of authentication and reduced the risk of unauthorized access by applying two-factor authentication to the servers and systems used by our employees to protect these servers and systems. (Completed in March 2024)

The application of two-factor authentication for some systems in the environment of the former Yahoo Japan Corporation is scheduled to be implemented by the end of December 2024.

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

To eliminate the potential risks arising from the linkages of systems and networks with NAVER and NAVER Cloud, we will also implement separation from the systems managed by these companies.

(The separation for the employees' systems*1 is scheduled to be completed at the end of March 2025*2 for LY Corporation, the end of March 2026 for Japanese subsidiaries and December 2026 for overseas subsidiaries)

*1System used by the employees of LY Corporation and its Group companies, which are in NAVER or in former LINE environments provided by NAVER and NAVER Cloud.

*2For the accounting system, we will determine the timing of system switchover and suspension of use by November 2024.

Review of Safety Management Measures, Etc. - 2

Guidance (1)-(i)(b)

LY Corporation should reevaluate the security risks associated with the common authentication system (not restricted to the authentication system on employee accounts) and system configuration that enables the synchronization of information. Then, in order to promptly and completely separate the authentication systems, etc. of NAVER Cloud and LY Corporation in terms of technology and operations from the viewpoint of ensuring the prevention of a recurrence, formulate a plan including the transfer to an authentication system, etc., managed by LY Corporation and the appropriate management after the separation, and take concrete measures by steadily implementing such a plan.

Matters reported (Excerpt)

In total, there are three common authentication systems, which are all systems related to employee accounts (authentication information of users is not included). NAVER Cloud manages the system related to these authentication systems. In light of this situation, we have determined the security management measures we can implement as a consignee are not sufficient to reduce risks. Therefore, we will stop using these systems and proceed with the migration to our own authentication system as described below to prevent unauthorized access caused by these risks.

In terms of the separation of authentication systems, we will prioritize the systems managed by LY Corporation and its Group subsidiaries, as LY Corporation is able to switch authentication functions for these. In this way, we will resolve the current situation in which we share authentication systems and authentication information with NAVER. (Scheduled to be completed in June 2024)

The separation of authentication system from the system managed by NAVER and NAVER Cloud will be implemented according to the following schedule.
(Scheduled to be completed at the end of March 2025 for LY Corporation, the end of March 2026 for Japanese subsidiaries and December 2026 for overseas subsidiaries)

Review of Safety Management Measures, Etc. - 3

Guidance (1)-(i)(c)

In relation to the cybersecurity measures for the former LINE environment, LY Corporation outsources the Security Operation Center (SOC) Tier 1 operations to NAVER Cloud. In light of the occurrence of this incident, establish at an early stage, LY Corporation’s system in Japan that can manage and operate authentication information in an independent manner, independently acquire log information of each system, etc. required for security, and independently perform SOC operations after consolidating such information. Develop a system which enables LY Corporation to ascertain the details of an incident based on the evidence held within the company, investigate the cause, and formulate your own measures to prevent recurrence, should a security incident occur in the future.

Matters reported (Excerpt)

Based on the occurrence of this incident, we will switch the function related to SOC Tier 1 which is outsourced to NAVER Cloud to a Japanese company and will establish a structure in which we will operate SOC in cooperation with said Japanese company.
(Scheduled to be completed in October 2024)

In addition, during the period leading up until when the system is separated from the system managed by NAVER Cloud, the risk remains that analysis using logs cannot be performed promptly, so a system will be established to obtain all log information necessary to understand situations and investigate causes.
(Completed in March 2024)

Review of Safety Management Measures, Etc. – 4 (1/2)

Guidance (1)-(ii)

Although strict behavior-based detection mechanisms and other measures should have been taken for Active Directory (AD) management in light of its importance, these measures were not taken and the level of security monitoring was inadequate, resulting in the failure to detect unauthorized access, etc. Furthermore, the access management level for other critical servers, etc. was also insufficient (e.g., the authentication method was a combination of an ID and password), thus failing to prevent access using illegally obtained employee accounts, etc. Based on the above, formulate a plan for the introduction of effective cybersecurity measures, including the introduction of advanced intrusion detection systems and enhanced access control (e.g., introduction of multi-factor authentication) to protect the company's servers, etc. In addition, report on the details of the plan, and promptly take concrete measures to implement them.

Matters reported (Excerpt)

(1) Correction of AD management (Completed in March 2024)
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. Furthermore, in addition to these measures, we corrected the AD management based on the consulting received from an outside firm.

(2) Reinforcement of access management of critical systems (Completed in March 2024)
As noted in Page 3 (2), we introduced two-factor authentication. In addition, a security assessment of critical employee systems in the former LINE environment was performed by a security engineer from a division specializing in vulnerability assessment to determine if there were any attempts to bypass the authentication process or ways in which authentication factors could be exploited.

(3) Formulation of plans with outside firms (Scheduled to be completed at the end of May 2024)
To ensure the adequacy, effectiveness, and objectivity of the plan for recurrence prevention measures, we received recommendations from outside firms, examined the applicability of the plan to our systems and business environment, and formulated concrete countermeasures and plans. In addition, for matters that need to be addressed in the NAVER Cloud environment, we will examine the recommendations with NAVER Cloud and make concrete countermeasures and plans considering the corrective measures already implemented at NAVER Cloud, etc.

Review of Safety Management Measures, Etc. – 4 (2/2)

Guidance (1)-(ii)

Although strict behavior-based detection mechanisms and other measures should have been taken for Active Directory (AD) management in light of its importance, these measures were not taken and the level of security monitoring was inadequate, resulting in the failure to detect unauthorized access, etc. Furthermore, the access management level for other critical servers, etc. was also insufficient (e.g., the authentication method was a combination of an ID and password), thus failing to prevent access using illegally obtained employee accounts, etc. Based on the above, formulate a plan for the introduction of effective cybersecurity measures, including the introduction of advanced intrusion detection systems and enhanced access control (e.g., introduction of multi-factor authentication) to protect the company's servers, etc. In addition, report on the details of the plan, and promptly take concrete measures to implement them.

Matters reported (Excerpt)

(4) Verification of the effectiveness of cybersecurity measures and security monitoring, and fundamental improvements and enhancements (Scheduled to be completed at the end of August 2024)

We will develop specific plans to strengthen cybersecurity more effectively and comprehensively, and promptly and steadily take corrective measures. Specifically, we will implement the following:

Implementation of penetration tests

- ・July 2024　Implementation of tests, analysis of results, and reporting
- ・August 2024　Formulation of corrective plans based on test results

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

- ・July 2024　Analysis of current status and validation with external organizations
- ・August 2024　Formulation of corrective plans based on verification results

Review of Subcontractor Management Measures, Etc. - 1

Guidance (1)-(iii)(a)

For the appropriate management of subcontractors when the handling, etc. of information that falls under the secrecy of communications is outsourced (includes cases in which the handling of information that falls under the secrecy of communications is outsourced, access is permitted to said information, and said information is accessible), review the security risk assessment criteria, and then study and formulate supervision methods and standards to achieve effective subcontractor management in accordance with the risks, and implement such methods and standards. Considering the details of this incident, with regard to the outsourcing of critical facilities, etc. (regardless of whether the handling of information is outsourced or not) standards for safety management measures, etc. should be established by the end of March 2024 to enable appropriate management and supervision of safety management measures and cybersecurity measures after identifying the subcontractors and sub-subcontractors. In addition, a monitoring and supervision method with enhanced effectiveness should be considered and established. Furthermore, review the current situation where the supervision of subcontractors relies on the results of analyses and logs submitted by the subcontractors, and where the company is unable to fully ascertain the existence and extent of intrusion unless these are obtained from subcontractors.

Matters reported (Excerpt)

(1) Review of security risk assessment criteria (Completed in March 2024)
We have established a new subcontractor checklist based on the checklist used for the outsourcing of personal information, etc. to be used more broadly for general subcontractor management.

(2) Study, formulation, and implementation of supervision methods and standards to achieve effective subcontractor management (Completed formulation of standards in March 2024; to be sequentially implemented)
We will formulate internal rules for conducting a multifaceted risk assessment of security and credit aspects for new business partners and subcontractors, that is not limited to the outsourcing of personal information, etc. In the future, we will conduct multifaceted risk assessments at the start of transactions and at the time of renewal of contracts, as well as during periodic audits. Although there is a possibility that risks arising from inadequate measures taken by subcontractors may remain until the supervision under the new evaluation standards has been completed, we will conduct audits, etc. of the subcontractor that was the cause of this incident and others in advance to deal with such risks.

(3) Formulation of safety management measures/cybersecurity measures (Completed in January 2024)
For the subcontractors who use accounts issued by us, we have implemented measures to allow access to our network environment only after they have gone through two-factor authentication.

(4) Independent ascertainment of intrusion and its extent (Scheduled to be completed at the end of September 2024)
Our policy will be to allow subcontractors who can log in or have access to our network to perform their subcontracted work only on personal computers that have been kitted by us. Although risks of malware infections, etc. of personal computers of subcontractors remain until the distribution of kitted personal computers is completed, we will mitigate the residual risks by implementing the measure described in (3).

Review of Subcontractor Management Measures, Etc. - 2

Guidance (1)-(iii)(b)

With regard to the strengthening of safety management measures at NAVER Cloud, which was the trigger of the attack in this incident, LY Corporation as the consignee should check the implementation status of the safety management measures with NAVER in a timely manner, request reinforcement of measures as necessary, and provide appropriate management and supervision to ensure that effective measures are formulated to prevent a recurrence.
In particular, according to LY Corporation’s report, NAVER Cloud was unaware of the breach until your company pointed it out, and NAVER Cloud had problems with its safety management measures such as the fact that its AD server had been compromised and had continued to be directly connected to from an external C&C server for a considerable period of time.
In light of this, LY Corporation should formulate and submit a plan to review its outsourcing and supervision practices.

Matters reported (Excerpt)

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

In order for us to take the initiative in confirming future corrective actions, etc., we have concluded an agreement that stipulates auditing rights, etc. pertaining to NAVER Cloud and will ensure the effectiveness of the abovementioned actions in a clear manner. (Completed in March 2024)

Moving on, we will resolve the outsourcing of SOC-related operations (target date: end of September 2024) and will reduce the scope of outsourcing itself through termination or reduction of related outsourcing relationships, based on the plan to reduce outsourcing, which is scheduled to be formulated by June 2024 .

In addition to the above, we conducted an on-site inspection of the subcontractor company involved in this incident and also terminated the contract. (Completed in March 2024)

Review of Group-Wide Security Governance, Etc.

Guidance (2)

In addition to implementing a fundamental review of your company’s security governance system, consider corrective measures. Furthermore, make necessary approaches to the parent companies, etc., so that the appropriate examinations will be made to review your company’s management system to ensure appropriate management and supervision of subcontractors (including review of relationships in which your company is subject to substantial capital control from the subcontractors) within the LY Corporation Group, including the parent companies themselves, and ensure the establishment of appropriate decision-making processes, etc.

Matters reported (Excerpt)

(1) We are requesting related companies to review the relationship in which we are under a substantial degree of capital control from NAVER, our subcontractor.

(2) Our Nominating and Remuneration Committee has begun discussions on the review of our management system to enable appropriate management and supervision over NAVER, our subcontractor. Necessary announcements will be made when organizational decisions, etc. are made in the future.

(3) Our policy will be to terminate/reduce outsourced service development and system use including service infrastructure between LY Corporation and NAVER. This will not be limited to the outsourcing of operations of internal system/network, etc. If there are some initiatives, etc. that are ongoing, our Governance Committee will confirm the safety management measures, etc. of said initiatives.

As of April 1, 2024, we have established a “Group CISO Board,” constituted by the CISOs of LY Corporation and its major Group companies (including overseas companies) and the CISO of SoftBank Corp., as an observer. Through this meeting, we will conduct a fundamental review and upgrading of the Group’s overall security governance.

In addition, we will establish an organization that directly reports to the President to promote various measures to prevent a recurrence and to establish Group-wide security governance.

Thorough Customer Support

Guidance (3)

In light of the fact that, at the very least, over 20,000 records of information (including estimates) that constitutes the secrecy of communications of your company’s users were leaked in this incident, information regarding this incident should continue to be appropriately provided to users from the viewpoint of user protection, and appropriate support and measures should be implemented in the event that secondary damage is discovered.

Matters reported (Excerpt)

(1) Information provision on this incident to protect users

From the viewpoint of user protection, we will continue to provide information appropriately on this incident to our users.

Specifically, on April 1, 2024, we have opened a dedicated page on our corporate website where we have summarized information such as the outline of this incident and the progress of measures to prevent a reoccurrence. In this dedicated page, we will publish information on the status of each measure. In addition, if new information that should be disclosed from the viewpoint of user protection becomes available, such information will be promptly published on this dedicated page.

(2) Response in the case that secondary damage is discovered, etc.

We will continue our efforts to recognize the occurrence or potential occurrence of damage due to unauthorized access that we are not yet aware of until a reasonable period of time has elapsed, and will work to detect secondary damage at an early stage and prevent its spread.

As of the submission of this report, we have not detected secondary damage. However, in the event that a user reports secondary damage to our customer service desk, which is permanently available, we will promptly investigate and take other necessary actions as appropriate.

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.”