Nov 12 ,2021

Notice of Submission of an Application Form for Extending the Deadline for Submission of the Quarterly Report for the First Half of FY2022

NIPPN CORPORATION (President and COO: Toshiya Maezuru; Head Office: Chiyoda-ku, Tokyo) announced that today it has decided to submit an application form for extending the deadline for submission of a quarterly report provided for in Article 17-15-2, Paragraph 1 of the Cabinet Office Order on Disclosure of Corporate Affairs to the Kanto Local Finance Bureau. Details are as follows.

1. Relevant quarterly report

Quarterly report for the first half of the fiscal year ending March 31, 2022

2. Submission deadline before extension

November 15, 2021

3. Submission deadline if extension is approved

January 31, 2022

4. Reason that the approval relating to the submission of the quarterly report is needed

(1) Overview of a cyber attack

In the early morning of July 7, 2021, a system failure occurred in the Group's information network, which is managed and operated by Nippn Business System, a subsidiary of the Company. The failure was caused by a cyber attack that encrypted all or part of the data in most of the severs and some of the terminals at the same time. Damage has been done to a large part of the network, including major critical system servers for non-consolidated financial management and sales management and file servers storing data. A sales management system (used by 11 companies) and an accounting system (used by 26 companies) for domestic group companies, systems operated in the Group's network, have also been damaged. The users include OK Food Industry Co., Ltd., a listed subsidiary. To contain the damage, the Company stopped all servers and cut off connections between the Group's network and networks outside the Group. As a result, access to all internal systems, including critical systems, and the shared file servers that store data has become impossible. The servers that are independent of the network, including

part of the production management system, have not been affected.

The Company requested outside experts to investigate the network. Their report says: in all information systems affected, all or a large part of the storage areas in the servers are encrypted as of late July, and the systems cannot be booted, no technical means that can swiftly restore the servers have been found at present, and the servers that manage data backup for the systems are in the same condition as described above, and no effective technical means that can restore data have been found. In addition, no ransomware or any other malware has been found. According to the outside experts investigating the network, the direct cause of this incident is estimated to be direct unauthorized access by the attacker itself.

Further, because this incident could result in an information leak, the Company asked outside experts to investigate the possibility of a leak. The Company received a report that the investigation found evidence of external access in some PCs, servers, etc. At present, an investigation is being conducted to check if information has leaked from these PCs, servers, etc. If evidence of a leak is found in this investigation, the Company will separately conduct an investigation into the content of the leaked information.

At the same time, to prevent a recurrence of the incident, the Company is advancing initiatives to strengthen its information security measures with advice from outside experts.

(2) BCP against system failure

On the hardware front, under the BCP against system failure, the Company has located data centers at distant places from each other in anticipation of disasters and in case of unexpected circumstances. The Company anticipated system failure at individual business sites. However, this time, a single cyber attack targeted most of the servers of the Group at the same time, and all the business sites, including the head office, were affected in the same way. The damage has been far more serious than anticipated in the Company's BCP. With regard to the security and backup system for the Company's information system, the Company has introduced an unauthorized access detection system and antivirus software to defend against cyber attacks and update them in a timely manner. It has a system where its PCs and servers are kept up to date. The Company outsources firewall operations to an outside managed service provider and has established a system where it receives advice from an expert perspective and proposals if the setting of firewalls needs to be reviewed. As for network connections with external entities, the Company has limited the use of privileged accounts and has conducted security monitoring activities, including the monitoring of exporting data to external devices. The Company stored backup data online. However, as mentioned above, backup data were also affected in the system failure.

(3) Setting up a task force

The Company's management discussed future policy. In light of the urgency of the problem and the impact on management, the Company has set up a task force and is making Group-wide efforts, also using external resources, to investigate the cause of the situation, take action to prevent secondary damage, restore the process of placing and receiving orders and accounting processes, restore the information system as soon as possible, and examine measures to prevent recurrence.

The task force discussed progress and means of restoration and has determined that restoring the main systems swiftly is difficult because it will take considerable time to review the complete network environment, rebuild the servers, and acquire the lost accounting data to restore the information system given the very large magnitude of the failure, the technical difficulty, and the prolonged period required for investigation due to the expansion of the scope of damage.

Based on these discussions, the head of the task force has mobilized the necessary labor from each division for the task force, built organizations including external experts as specialized subcommittees, and allocated a function to monitor responses to this problem to the task force as a steering committee. The subcommittees submit daily reports, to which the task force responds by summarizing their overall activities on a weekly basis.

(4) Initiatives to prevent recurrence

In response to matters concerning this incident pointed out by external experts, the task force has taken appropriate interim measures to prevent a recurrence and to enhance the Company's information security measures. Those interim measures include a firewall policy restriction and investigation to check the presence or absence of intrusions on all servers and PCs. According to opinions from external experts, the necessary interim measures have been taken to connect terminals to the information network again.

As its future initiatives, the Company will promptly implement specific action plans that were proposed to prevent a recurrence of the incident and enhance the Company's information security measures, although some have already been implemented. When a new matter that should adopted as policies is found as a result of the investigation, the Company will review the policies based on the opinions of external experts.

(5) Action to resume accounting work

At the time of the announcement of the Notice of Submission of an Application Form for Extending the Deadline for Submission of the Quarterly Report for the First Quarter of FY2022, which was made on August 16, it was unclear when the accounting system would be restored,

and the outside experts had said that the system was unlikely to be restored soon.

Based on the experts' explanation, the Company decided to implement in a different environment the accounting system used by the Company and certain group companies to complete the account closing procedures as soon as possible. This system became available for use in perfect condition in mid September. The backup data of the accounting system used by the other domestic group companies had not been damaged, and the Group ensured safety and restored the system to the state before the system failure. Accounting closing procedures was resumed in the middle of August. The Company also implemented a new consolidated accounting system and built a system to resume account closing procedures in late August.

Regarding the sales management system used by domestic group companies, the Company proceeded with restoration work, and completed the work for all companies in early October.

After the system came into operation, the account closing procedures for the first quarter was resumed promptly, and the Company announced its consolidated financial statements for the first quarter of the fiscal year ending March 31, 2022 on October 29. It will submit the quarterly report for the first quarter of the fiscal year ending March 31, 2022 on November 15.

(6) Account closing procedures for the first half

As mentioned above, the accounting system of the Company and domestic group companies and the sales management system of domestic group companies came into operation again. However, for other business systems used by the Company, the Company is restoring them under a basic policy of giving top priority to the restoration of the logistics management system and sales management system, which are used for order acceptance and placement, acceptance and delivery, inventory control, etc. in the upstream of the data, and to restore downstream systems in stages, to ensure data consistency and streamline the restoration process.

In addition, because approximately 90% of systems were affected by the cyber attack in question, the Company has completely shut down its information network, and then conducted an investigation into the causes, investigation into the intrusion, and an investigation into the leakage. It has taken security measures, spending an appropriate amount of time to prevent a secondary failure. In these circumstances, rebuilding of the critical systems needs to begin after safety is confirmed based on the results of the investigation into the causes and security measures are taken. The Company has started to rebuild them after making confirmation and taking those measures. On the other hand, for the minimum required systems for business continuity, the Company has introduced substitute systems. Among these, for the logistics management system, recording of order acceptance and shipments, acceptance and delivery, and other tasks had been done manually since the system stopped on July 7. Accordingly, the Company has introduced a substitute system with only order acceptance and placement functions as an interim measure

before system restoration. The Company put this system into operation in early September.

In the first quarter, business forms that needed to be created manually again were limited because more than half of the business forms needed for account closing procedures were those on major transactions, such as sales and rebates, which were created on upstream systems, and their backup data and printed forms had been retained.

On the other hand, in the first half, the restoration of critical systems that have stopped, including the system for operations management, which is linked to accounting data, and the one for logistics management, has not progressed beyond tentative restoration with substitute systems having only order acceptance and placement functions. Thus, restoration of major critical systems has been delayed until the last day of the third quarter or later. Under normal conditions, data on daily transactions put into each system would be automatically aggregated and created, and then converted into transfer slip data and automatically imported to the accounting system. This series of processes was replaced with manual tasks. As a result, for the time being, the business forms to be used for account closing procedures have to be created manually using Excel, etc.

Given these circumstances, in the account closing procedures for the first quarter, the accounting division mainly engaged in a simple task of re-entering data from transfer slips stored in printed form into the accounting system. In the account closing procedures for the first half, however, considerable efforts are needed to complete the creation of materials to be used for account closing. Moreover, transfer slips, which would be created automatically based on manually created business forms, need to be created from scratch, requiring longer work hours than the account closing procedures for the first quarter.

To ensure account closing procedures advance promptly, the Company uses external human resources for creating business forms at the division in charge of the tasks and has also assigned personnel from various internal divisions to support the task. Further, the accounting division also uses external human resources to speed up the task of creating transfer slips and receives advice and support from external experts concerning overall practical tasks in account closing procedures.

(7) Outlook for completion of the quarterly report for the first half

As described above, the Company is proceeding with account closing procedures for the first half by mobilizing personnel to quickly complete the manual tasks of creating business forms and entering transfer journal data. The tasks for the Company are scheduled to be completed in the middle of December and those for group companies in late November. Then, the Company plans to create the consolidated financial statements for the first half in a period of about one month from the date when the financial results of group companies will be reported.

Concerning the accounting auditor's review for the first half, the Company is facing special circumstances where a very different business process must be taken while its critical systems remain shut down. Accordingly, the necessary procedures will be newly created based on an understanding of the Company's new internal control that applies to the changed processes before the review is conducted. Therefore, the Company has been told that more time is highly likely to be required for the review than the review for the first quarter.

Specific dates and schedules are being set after consultations with external experts and the accounting auditor.

The Company thus expects that it will not complete the consolidated financial statements and the accounting auditor's review for the first half of the fiscal year ending March 31, 2022 by the deadline for the submission of the quarterly report, November 15, 2021, and has decided to apply for the extension of the deadline for the submission of the quarterly report for the first half of the fiscal year ending March 31, 2022. Considering the current status, the Company plans to complete the preparation of the consolidated financial statements for the first half of the fiscal year ending March 31, 2022 and the accounting auditor's review and submit the quarterly report for the first half by January 31, 2022, the date to which the Company will apply for extending the deadline.

The announcement of the consolidated results for the first half of the fiscal year ending March 31, 2022 will be made by January 31, 2022.

5. Outlook

If the application for extending the submission deadline is approved, the Company will disclose the approval promptly.

We offer our sincere apologies to shareholders, investors, and other stakeholders for a great deal of inconvenience and worry we have caused.

The Company is continuing normal operations and supplying food products as usual to fulfill its social responsibility to consistently provide food.

In addition, the Company has already been taking steps to restore the systems and prevent a recurrence of the incident. We kindly ask for your understanding and continued support.