Aug 16,2021

Notice of Occurrence of System Failure (continued report)

NIPPN CORPORATION (President and COO: Toshiya Maezuru; Head office: Chiyoda-ku, Tokyo)) announces regarding the system failure, etc. it announced on July 9, 2021 that the Company has recognized, as a result of subsequent investigations, that there is a possibility that some of the corporate and personal information it stores may have leaked due to unauthorized access to its server as a result of the cyberattack (hereinafter, the "Incident"). The Company sincerely apologizes for causing considerable trouble and anxiety to customers, business partners, and other stakeholders.

The facts currently identified and our measures are as follows:

Details

1. Details of the Incident and possibility of information leakage

   On July 7, 2021, as a result of an employee report, the Company recognized that a failure had occurred in multiple systems in its group network. The Company shut down the internal and external networks and asked external cyber security experts (hereinafter, the "external experts") to investigate the cause of the Incident. As a result of the initial investigation, it was found that there was a high possibility of a cyberattack on the Group's systems.

   Given the seriousness of the Incident, the Company investigated the intrusion route and damage in detail, including the possibility of an information leak, in cooperation with external experts. As a result, it was found that there was a possibility of a leak of part of the corporate and personal information managed in the Company's internal server.

   Although an information leakage has not been specifically confirmed at this moment, the Company is continuing further investigations with the assistance of the external experts to ascertain the facts. If a corporate or personal information leakage is confirmed, the Company will make an immediate announcement.

2. Actions by the Company

   Immediately after the Incident was found, the Company established a task force based on the instructions of its representative directors, and an emergency response team including external experts is taking action. In addition, the Company has already reported it to the Personal Information Protection Commission and relevant bureaus, including supervisory authorities, and is taking actions against the Incident based on guidance from the authorities.

3. Status of the Company's information network environment

   Currently, to prevent secondary damage, the Company is taking multiple security measures including a shutdown of the communication routes related to the cyberattack based on the advice of external experts. For systems that experienced a failure, the Company is restoring them sequentially from the one whose safety has been confirmed. Since the Incident occurred, no safety problems have been found.

4. Recurrence preventive measures

   The Company will further strengthen its security measures with the assistance of the external experts. It will also take recurrence preventive measures immediately after it conducts cause analysis based on the investigations by the external experts.