June 13, 2025
Nikki-Universal Co., Ltd.

Notice of Cybersecurity Incident (Update)

As previously announced on December 27, 2024 in our statement titled "Notice of Cybersecurity Incident", Nikki-Universal Co., Ltd. (“N-U”) reported that some electronic data on our servers had been encrypted and that there was a possibility of data compromised (hereinafter referred to as "the Incident").

Since confirming the Incident, N-U has been conducting an investigation including examining the extent of the Incident with the assistance of an external cybersecurity company.

N-U would like to provide an update on the Incident, including the background, the actions we have taken, and the findings of the investigation. N-U deeply regrets the significant inconvenience caused to all stakeholders.

1. Detection and action taken

On December 22, 2024 (Japan time), a system failure occurred. Upon investigation, it was confirmed that some of the servers managed by N-U had been infected with ransomware. The affected system environment was immediately disconnected from external networks, and measures were taken to prevent the escalation of the Incident.

With regard to restoring the network and system, N-U has decided to build a new system environment instead of reusing the affected environment. Such restoration has been mostly completed, and business operations are continuing as usual.

2. Cause of the Incident

According to the findings of the investigation conducted by the external cybersecurity company, it was revealed that unauthorized access to N-U's environment was gained through the internet connection point. N-U takes this situation very seriously and will implement further measures to prevent recurrence, based on advice from the aforementioned company.

3. Information Compromised

The investigation by the external cybersecurity company confirmed that information had been compromised. The compromised data included information related to business transactions and personal information (*). At this point, there have been no confirmed cases of unauthorized use involving the personal information. As a precaution, kindly remain cautious for any suspicious emails or messages.

(*) Items of personal information that were compromised or potentially compromised:

name, company name, company email address, etc.

N-U has reported the details of the Incident to the Personal Information Protection Commission.

4. Regarding this Announcement

N-U sincerely regrets the delay in providing this update since the initial announcement on December 27. To minimize confusion and inconvenience to N-U's stakeholders, N-U determined that it was essential to prepare appropriate measures before making further announcements. Therefore, N-U waited for the results of the investigation by the external cybersecurity company before disclosing the facts.

N-U deeply regrets the time it has taken to report the findings of this investigation.

5. Measures to Prevent Recurrence

N-U takes this Incident very seriously and, based on the investigation results, will strengthen N-U's system security measures and information security management framework to prevent recurrence.

6. Contact Information for Inquiries Regarding This Announcement

For inquiries regarding this matter, please contact:

General Affairs and Legal Department, Administration Division
Email: cr@n-u.co.jp
Phone: +81-3-5436-8486

N-U deeply regrets the significant inconvenience caused to all stakeholders. N-U remains committed to addressing this matter with sincerity and to implementing measures to prevent recurrence. N-U kindly asks for your understanding and cooperation as N-U moves forward.