July 19, 2024

To: The Winners of the Shareholder Benefit-based Gifts

Nidec Corporation
Nidec Instruments Corporation

Apology and Report with respect to the Recent Ransomware Infection

Thank you very much for your continued support for Nidec Corporation (hereinafter referred to as the "Company" or "we").

On May 26, 2024, an unauthorized access was made to the business operation system and other assets owned by Nidec Instruments Corporation (hereinafter referred to and as "Nidec Instruments"), encrypting the information in the system.

As the Company had consigned Nidec Instruments to handle the personal information of the shareholders who received music boxes as part of the shareholder benefit plan, those personal data had been stored in the server, file server, and other places of Nidec Instruments' internal system. Accordingly, investigations into this case revealed that we cannot deny the possibility that those personal data may have been either lost or damaged (hereinafter collectively referred to as the "information leak, etc.") in the cyberattack (hereinafter referred to as "the incident").

After the occurrence of the damage caused by the ransomware, Nidec Instruments has conducted necessary investigations in a timely manner, and has recently finished them. In this notice, we will report the results of the investigations to the shareholders of the Company whose personal data may have been subjected to the information leak, etc. from Nidec Instruments and its group companies (hereinafter referred to as the "Nidec Instruments Group") (Part of the information below overlaps with the information that has already been announced).

Even though we have conducted our investigations trying not to cause further trouble by providing our shareholders with inaccurate information, we do apologize for the amount of time we have had to spend on the investigations until now.

1. Categories and the number of sets of data that are, or may have been, subjected to the information leak, etc.:
    - Categories of the personal data: Names, addresses, and zip codes
    - Number of the shareholders: 482
    - Number of sets of personal data: 482

The shareholders whose personal information (described above) may have been leaked are those to whom the Company has given music boxes as part of its shareholder benefit plan from 2020 to 2023, and they do not include any other shareholders.

Though a link to a download site seemingly related to the incident was found on the leak site of the incident's attacker, we confirmed that the files available for download from the link do not contain any personal data of the shareholders.

2. Cause and countermeasures
    (1) Cause of the incident
    We believe that the incident occurred when its attacker somehow obtained the system administrator's ID and password improperly to obtain access to Nidec Instruments' business operation system.

    (2) Countermeasures
    After discussions with the Company, Nidec Instruments changed the passwords to all of its IDs, isolated the cyber-attacked terminals from its network, and launched other measures to prevent further expansion of the damage and to avoid damage to systems owned and retained by third parties.

    In addition, since the incident, Nidec Instruments makes sure that each employee uses, in principle, a clean

PC (a terminal not connected to its internal network) when accessing the Internet, and disconnects terminals other than clean PCs from the Internet except for those minimally required for work (*e.g.*, terminals needed for emailing and online conferences), to avoid receiving suspicious communications from the outside. Furthermore, Nidec Instruments has restricted connection sources' IP addresses for emails to prevent unintended use of those addresses by a third party. It is with comprehensive security measures including these ones above that Nidec Instruments ensures to prevent the ransomware attack's impact to the systems owned and managed by third parties.

3. Actual or possible secondary damage and its details

The ransomware-based unauthorized access was made to a Nidec Instruments-owned business operation system, and no damage was made to the Company's business operation system, which is a totally different system from Nidec Instruments'. In relation to the Company, the incident's damage is limited to the information whose management the Company had consigned to Nidec Instruments, meaning that the Company is free of any secondary damage in the incident.

If you ever receive any suspicious email, etc. from someone posing as a member of the Company's business group or as the incident's attacker, do not open the email, or access any URL, etc. in such message.

4. Recurrence prevention measures

Via discussions with the Company, Nidec Instruments has launched recurrence prevention measures. Specifically, to prevent unauthorized use of an internal account after the incident, Nidec Instruments has changed the passwords to all of its internal accounts, and deleted unnecessary accounts. In addition, to prevent unauthorized access to its business operation system, Nidec Instruments has changed its online settings to limit the number of users who can access its internal network via VPN.

5. Inquiries

For inquiries on the above matter, please contact:
Nidec Instruments Corporation's System Trouble Call Center at 0120-234430 (for use within Japan only)
(Hours of operation: 09:00 – 18:00 on Monday – Friday (Japan time). This service is not available on weekends or holidays).

6. Timeline in detail

The actions and countermeasures that the Company and the Nidec Instruments Group have executed in response to the incident are as explained below. Please be reminded that the Company and the Nidec Instruments Group have never accepted the ransom demand by the incident's attacker, and that we are constantly monitoring the leak site in collaboration with a specialized outside security organization.

- May 26: An employee who is a member of Nidec Instruments' information systems department detects an attack caused by the incident. On the same day, as part of its initial countermeasures, Nidec Instruments uses its EDR software and antimalware to remove the malware that caused the incident.

- May 27: After issuing instructions to all of the Nidec Instruments Group's employees, Nidec Instruments confirms that the malware that has caused the incident has not been activated on any of the Nidec Instruments Group's PCs. On the same day, Nidec Instruments recovers its data by using backup data, building a minimal system to continue business with the outside.

- May 28: Based on the fact that one cannot deny that possibility that the Nidec Instruments Group's information may have leaked to a third party, Nidec Instruments reports the incident to the Nagano Prefectural Police, and starts consulting with them. In addition, since then on, Nidec Instruments recovers its internal core system and peripheral system from the incident, and launches recovery and other measures in cooperation with a security product vendor.

- June 03: Nidec Instruments requests a specialized outside security organization to launch technical investigations into relevant facts on the incident. Despite the ransom demand by the incident's attacker to the Company, it has not made any such payment until now because, among other reasons,

we must never make any payment to antisocial forces.

- June 10: The Company and Nidec Instruments post the notice titled "Security Incident at a Nidec Group Company (Security Incident at Nidec Instruments Corporation)" on their respective websites. On the same day, Nidec Instruments issues a preliminary report to the Personal Information Protection Commission, while making an official notice with the same content to the two companies' employees. On the following day of June 11, Nidec Instruments Group companies other than Nidec Instruments issue their preliminary reports to the Personal Information Protection Commission.

- June 12: The Company and Nidec Instruments start consulting with an outside attorney.

- June 12: On the same day, the Company and Nidec Instruments receive a preliminary report from an outside security organization.

- June 18: A download link seemingly related to the Nidec Instruments Group is found posted on the leak site of the incident's attacker, leading us to confirm that information on the Nidec Instruments Group is available for download. However, the investigations that took place thereafter confirm that information cannot be downloaded from the link since June 19.

- June 26: Nidec Instruments' investigation report reveals that, since the personal information of the shareholders described in Section 1 above had been kept in Nidec Instruments' server, which the incident's attacker was able to access unauthorized, one cannot deny the possibility that the personal information may have been subjected to the information leak, etc.

- July 12: The investigations into the numbers of sections, items, etc. of information that may have been subjected to the information leak, etc. are completed. On the same day, the process of identifying those whose personal data may have been subjected to the information leak, etc. is completed.

- July 15: The process of building an environment that our business partners and customers can use safely and securely is completed. For more details on this environment, please see Section 2 (2), "Countermeasures," above.

- Today: The Company and Nidec Instruments plan to send a notice to inform certain people whose personal information may have been subjected to the information leak, etc., and post a release, "Apology and Report with respect to the Recent Ransomware Infection," on the Company's website for those who and others whom we cannot inform of the above information directly.

- July 24: The Company and Nidec Instruments plan to submit finalized information to the Personal Information Protection Commission.

Once again, we deeply apologize to our shareholders others concerned for the inconvenience and worry due to the aforementioned incident.