July 25, 2024
Nidec Corporation

The Security Incident at a Nidec Group Company (Third Announcement)

This is the third announcement with respect to the damage caused by the ransomware attack on Nidec Instruments Corporation (hereinafter referred to as "Nidec Instruments") – an incident reported on June 10 and 27, 2024. We deeply apologize for the inconvenience and worry that this case has caused to everyone concerned.

After experiencing damage caused by the aforementioned ransomware, Nidec Instruments has conducted investigations in a timely manner, and found out that we cannot deny the possibility that the personal data of those who have won gifts (music boxes) as part of our shareholder benefit plan – data Nidec Instruments had been managing on consignment by Nidec Corporation – may have been either lost or damaged (hereinafter collectively referred to as the "information leak, etc.") in the cyberattack.

Now, the investigations with respect to the aforementioned shareholders completed, Nidec Corporation and Nidec Instruments jointly mailed on July 19 the results of the investigations to shareholders whose personal data may have been subjected to the information leak, etc. For the content of the notice please click here (the link to the notice to the shareholder benefit plan-based gifts' winners).

For the latest announcement by Nidec Instruments on the incident, please see below.

Apology and Report with Respect to Possible Personal Information Leakage due to Unauthorized Access to Nidec Instruments' Internal System Report No. 3)

Nidec Instruments Corporation
Nidec Material Corporation
Tokyo Maruzen Industry Co., Ltd.
Nidec Instruments Akita Corporation
Sunseiki Co., Ltd.
Nidec Instruments Service Engineering Corporation
Nidec Music Box Museum Suwanone

Thank you very much for your continued support for Nidec Instruments Corporation.

As announced on the websites of Nidec Instruments and Nidec Corporation on June 10 and 27, Nidec Instruments and its group companies (hereinafter referred to as the "Nidec Instruments Group") have been a subject of a cyberattack by a malicious outside attacker (hereinafter referred to as "the ransomware incident's attacker"), who encrypted files in Nidec Instruments' multiple servers (hereinafter referred to as the "ransomware incident").

This notice once again reports the latest results of the investigations into the Nidec Instruments Group regarding the ransomware incident (Part of the information below overlaps with the information that has already been announced). Please be informed that Nidec Corporation and its group companies, both outside the Nidec Instruments Group, have not been subjected to any damage caused by the ransomware incident.

Once again, we deeply apologize for the inconvenience and worry that this ransomware incident caused to everyone.

1. Outlook of the ransomware incident
   On May 26, 2024, a ransomware-based unauthorized access to Nidec Instruments-owned business operation systems and others left information in the system encrypted.

   Our investigations revealed, as explained in the June 27, 2024 release, "Nidec Instruments Warns of Possible

Personal Information Leak Due to Recent Unauthorized Access to the Company's Information System, Makes an Apology for the Incident," issued on Nidec Instruments' website: part of the data in the internal system severs, file servers, and others of Nidec Instruments as well as those of the Nidec Instruments Group's domestic legal entities, *i.e.*, Nidec Material Corporation, Tokyo Maruzen Industry Co., Ltd., Nidec Instruments Akita Corporation, Sunseiki Co., Ltd., Nidec Instruments Service Engineering Corporation, Nidec Music Box Museum Suwanone, and part of Nidec Instruments' overseas legal entities* had been encrypted; that a link to a download site seemingly related to the ransomware incident was on the leak site of the ransomware incident's attacker; and that one cannot deny the possibility that part of the information owned by the Nidec Instruments Group may have been leaked to a third party. Follow-up investigations confirmed that those files cannot be downloaded from the download site at present.

Details of our countermeasures in response to the ransomware incident are explained later in this document.

*The following nine companies, whose network configurations are not part of the Nidec Instruments Group's, were not affected by the ransomware incident:

(1) SCD Co., Ltd.
(2) SCD (Guangzhou) Co., Ltd.
(3) SCD (Hong Kong) Co., Ltd.
(4) Nidec Instruments (America) Corporation
(5) Nidec Instruments México, S.A. de C.V.
(6) Nidec Instruments (Europe) GmbH
(7) Nidec Genmark Automation, Inc.
(8) Nidec Genmark Automation (Suzhou), Inc.
(9) Nidec Genmark Automation (Europe), Inc.

2. Categories and the number of sets of data that are, or may have been, subjected to the information leak, etc.

- Information regarding business partners and other people concerned
  - Categories of personal data:
    Names, genders, addresses, birthdates, telephone numbers, and email addresses
  - Number of the sets of personal data:
    318,151
    (This is the total number of the sets of personal data, and the actual number of the people will be less than 318,151.)

- Information regarding customers who purchased Nidec Instruments' music boxes and those who attended Nidec Instruments-hosted and other events
  - Categories of personal data:
    Names, genders, addresses, telephone numbers, and email addresses
  - Number of the sets of personal data:
    71,089
    (This is the total number of the sets of personal data, and the actual number of the people will be less than 71,089.)

- Information regarding employees, former employees, contract employees, former contract employees and their families
  - Categories of personal data:
    Names, genders, addresses, birthdates, telephone numbers, email addresses, social security and tax numbers, account information, salary information, bonus information, retirement benefit information, employment insurance certificate numbers, health insurance numbers, basic pension numbers, and passport numbers
  - Number of the sets of personal data:
    13,290
    (This is the total number of the sets of personal data, and the actual number of the people will be less than 13,290.)

3. Cause and countermeasures

(1) Cause of the ransomware incident

We believe that the ransomware 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

As an initial measure, Nidec Instruments launched temporary measures of changing the passwords to all of its IDs, and isolating the cyber-attacked terminals from its network.

In addition, since the ransomware 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.

4. Actual or possible secondary damage and its details

As explained in Section 1, "Outlook of the ransomware incident," we have confirmed that data cannot be downloaded from the leak site of the ransomware incident's attacker. In addition, as explained in Section 2, "Categories and the number of sets of data that are, or may have been, subjected to the information leak, etc.," information, such as credit card information, that could directly cause secondary economic damage, is not among the categories of the information that may have been subjected to the information leak, etc. Furthermore, Nidec Instruments has not confirmed at present any secondary damage attributable to the ransomware attack, such as the unauthorized use of information based on the aforementioned personal data.

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

5. Recurrence prevention measures

After this incident, to prevent the unauthorized use of an internal account, 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*.

In addition, after experiencing the ransomware incident, the Nidec Instruments Group has reinforced its information management system to prevent the recurrence of the ransomware incident.

*VPN, or the virtual private network, is a dedicated virtual line set on the Internet, and available for those designated only.

6. Inquiries

For inquiries on the ransomware incident, please call:
0570-004066 (a "*navi dial*" number = a nationwide unified number; for use within Japan)

7. Timeline in detail

The actions and countermeasures that Nidec Instruments and the Nidec Instruments Group have executed in response to the ransomware incident are as explained below. Please be reminded that the Nidec Instruments Group and Nidec Corporation have never accepted the ransom demand by the ransomware 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 ransomware 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 ransomware incident, and establishes a response team.

- May 27: After issuing instructions to all of the Nidec Instruments Group's employees, Nidec Instruments confirms that the malware that has caused the ransomware 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 ransomware 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 ransomware 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 ransomware incident. Despite the ransom demand by the ransomware incident's attacker to Nidec Corporation, Nidec Instruments' parent company, in parallel to the attack on Nidec Instruments, we have not made any such payment until now because, among other reasons, we must never make any payment to antisocial forces.

- June 10: Nidec Instruments 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: Nidec Instruments and Nidec Instruments start consulting with an outside attorney, and receive a preliminary report from a dedicated outside security organization

- June 18: A download link seemingly related to the Nidec Instruments Group is found posted on the leak site of the ransomware 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' investigations reveal that, since the personal information of some shareholders had been kept in Nidec Instruments' server, which the ransomware 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. Thus, Nidec Instruments informs Nidec Corporation of the possibility of 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., and 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 3 (2), "Countermeasures," above.

- July 24: Nidec Instruments submits its finalized facts to the Personal Information Protection Commission.

- July 25 and thereafter: Nidec Instruments sends a notice to inform certain people whose personal information may have been subjected to the information leak, etc., and posts today a release, “Apology and Report with respect to the Recent Ransomware Infection,” on Nidec Instruments’ website for those who and others whom we cannot inform of the above information directly.

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