



March 1, 2022

Company name: NOK CORPORATION
Representative: Masao Tsuru
Representative Director and President
Securities code: 7240
Contact person: Takashi Kaku
Department Manager
Corporate Communication Department
(TEL +81-3-5405-6372)

Notice of System Failure Due to Unauthorized Access (Final Report)

NOK Corporation announced the unauthorized access to its company on December 21, 2021 ("Notice of System Failure Due to Unauthorized Access (1st Report)") and reported the investigation results (preliminary report) on December 28 ("Notice of System Failure Due to Unauthorized Access (2nd Report)"). We would like to announce the results of the subsequent investigation by our company and the investigation company.

Once again, we deeply apologize for any inconvenience and concern this may have caused.

1. Overview of unauthorized access and investigation results

Please refer to "Notice of System Failures due to Unauthorized Access (First Report)" on December 21, 2021 and "Notice of System Failures due to Unauthorized Access (Second Report)" on December 28, 2021 for the details. Although many of our internal systems were affected, we took security measures based on the advice of the investigation company and proceeded with the restoration of the systems in order, and it did not affect the production and delivery of our products. We have also received a final report from the investigation company on this matter. As a result, it was confirmed that no data containing confidential or personal information was leaked outside the company, nor were there any traces that could lead to such suspicion.

2. Measures to prevent recurrence

The unauthorized access was caused by an intrusion into our internal network by exploiting a vulnerability in our system that was scheduled to be fixed by December last year. We have already taken measures against this vulnerability, and the same method of intrusion is no longer possible. In addition, we will take countermeasures by strengthening our detection capabilities against cyberattacks and security incidents, reinforcing our system that focuses on the three points of first response, backup data preservation and recovery, and focusing on internal education to improve the information security literacy of our employees. We take this incident very seriously and will further strengthen our security measures and monitoring system to prevent any recurrence, while continuously receiving advice from cyber security and investigation companies.

3. Impact on business performance

The impact of this matter on the business performance is minimal.

END