November 20, 2026

Company name: **Osaki Electric Co., Ltd.**
Name of representative: Yoshihide Watanabe, Chairman and CEO (Securities code: 6644; TSE Prime Market)
Inquiries: Ryuichi Ueno, Director and Senior Managing Executive Officer, Head of Group Strategy Division (Telephone: +81-3-6694-7140)

Notice Concerning Suspension of Production Due to Ransomware Cyberattack (Second Report)

Osaki Electric Co., Ltd. ("the Company") hereby announces, as reported in the "Notice Concerning Suspension of Production Due to Ransomware Cyberattack (First Report)" dated November 18, 2026, that it has confirmed that its systems were subjected to a ransomware cyberattack on November 17, 2026. The Company sincerely apologizes once again for the significant inconvenience and concern caused to its customers and all other parties concerned.

Subsequent investigations have revealed certain facts regarding the timing and route of the intrusion. The Company now provides an update on the situation as of November 20, 2026, as outlined below. Please note that the investigation is ongoing, and the information provided herein may change depending on the findings of further investigations.

1. Facts Identified (Timing and Route of Intrusion)

(1) Timing of intrusion

Based on the investigation conducted to date, unauthorized access is estimated to have occurred at approximately 1:30 a.m. on Sunday, November 15, 2026.

(2) Route of intrusion

It has been confirmed that the attacker gained access to the Company's internal network by bypassing authentication on a VPN device used to connect to the internal network from outside the Company.

The Company believes it is highly likely that the attacker gained access through repeated password attempts on an account for which multi-factor authentication had not been enabled, as some such accounts remained in use. The circumstances under which the account was created and whether the password had been compromised prior to the attack are currently under investigation.

(3) Extent of damage

Following the intrusion, some virtual servers were encrypted. All network connections, including the route used for the intrusion, have been disconnected.

(4) Timeline of major events

Date and Time	Event
November 15 (Sun.), approximately 1:30 a.m.	Unauthorized access via the VPN device is estimated to have begun.
November 17 (Tue.), around 10:35 a.m.	The Company confirmed that data on its servers had been encrypted.
November 17 (Tue.), from noon onward	Connections to external networks, including the VPN device used for the intrusion, were disconnected. Production-related systems were shut down.
November 18 (Wed.)	The Company issued its First Report.
November 19 (Thu.)	The Company became aware that information had been posted on a website believed to be operated by the attacker.
November 20 (Fri.)	The Company issued its Second Report.

2. Possibility of Other Intrusion Routes and Earlier Unauthorized Access

The Company's network is configured to provide protection at its external boundaries, and the VPN device used in this incident was the only point through which direct access to the internal network from outside the Company was possible.

Accordingly, the Company considers the possibility of intrusion through other routes to be low, and no intrusion through other routes has been identified to date.

Furthermore, the investigation conducted to date has found no evidence of unauthorized access prior to November 15, 2026.The Company will continue its investigation and verification in cooperation with external specialists.

3. Information Leakage

On November 19, 2026, the Company became aware that technical information believed to be stored in its systems had been posted on a website on the internet.

The Company is currently investigating the content and scope of the posted information, as well as whether any other information has been leaked.

If the investigation reveals that the leaked information includes information managed under confidentiality agreements with business partners, the Company will contact the relevant business partners individually.

Furthermore, if any leakage of personal information is confirmed, the Company will report the incident to the Personal Information Protection Commission and notify the affected individuals in accordance with applicable laws and regulations.

The Company continues to consult with and report the incident to the police and other relevant authorities.

4. Safety of Products and Services

This incident involved a cyberattack targeting the Company's internal systems and did not target or affect its products and services, including smart meters.

5. Recovery Status and Resumption of Operations

(1) Recovery status

The Company has confirmed that its backup data remains intact and is proceeding with system recovery.

(2) Policy for resumption of operations

Taking into account the findings of the investigation, the Company intends to resume operations in stages, beginning with those areas where safety has been confirmed.

(3) Impact on business operations

The timing of the resumption of production and shipments remains undetermined.

(4) Impact on financial results

The impact on the Company's financial results (including any estimated amount) is undetermined at this time, as it will depend on the timing of recovery.

6. Future Actions

Should any new facts requiring disclosure come to light, including progress in the investigation, the outlook for recovery, or the presence or absence of information leakage, the Company will promptly announce them through its official website and other means.

7. Requests to Customers and Other Parties Concerned

(1) If you have any questions or concerns regarding delivery schedules for existing orders or future orders, please contact your representative at the relevant business division of the Company.

(2) If you receive any suspicious emails or telephone calls purporting to be from the Company, please do not open any attachments or click on any URLs contained in such emails. Instead, please notify the relevant business division of the Company.

The Company once again sincerely apologizes for the significant inconvenience and concern caused to its customers and all other parties concerned.

[Contact for inquiries regarding this matter]

Customers and business partners:

Please contact the relevant business division or Purchasing Department of the Company.

Media inquiries:

Corporate Communications Department

pr_all@osaki.co.jp