YAMAICHI ELECTRONICS CO., LTD.
Stock listing: Tokyo Stock Exchange - Prime Market Code: 6941
President: Junichi Kameya
General Manager of General Affairs and Human Resources Group: Fusakazu Atarashi
Tel: +81-3-3734-0115

June 15, 2026

Final Report on Investigation Results and Completion of Response to Ransomware Incident at Consolidated Subsidiary in the Philippines

Further to our notices dated April 22, 2026, titled “Notice of Ransomware Incident at Consolidated Subsidiary in Philippines,” and April 30, 2026, titled “Follow-up Notice of Ransomware Incident at Consolidated Subsidiary in Philippines,” regarding the ransomware incident involving Pricon Microelectronics, Inc. (“Pricon”), our consolidated subsidiary in the Philippines, we hereby announce that the investigation conducted by external cybersecurity experts and the recovery process have been completed.

We sincerely apologize to our shareholders, investors, customers, business partners, and all other stakeholders for the significant concern and inconvenience caused by this incident.

1. Overview and Timeline of the Incident

This incident involved a ransomware attack that infected certain servers at Pricon, resulting in the encryption of a portion of its business data.

Upon confirming the incident, we immediately disconnected and isolated the affected systems from the network to prevent further damage and the spread of the infection. At the same time, we began an investigation and recovery process in cooperation with external cybersecurity experts.

The timeline of events is as follows:

- April 17, 2026: System abnormalities were detected at Pricon, and a ransomware infection was confirmed.
- April 17, 2026: The affected systems were isolated, and an investigation by external experts was initiated.
- April 22, 2026: Initial announcement of the incident.
- April 29, 2026: System recovery was completed.
- April 30, 2026: Follow-up announcement regarding the recovery and investigation status.

2. Investigation Results by External Experts

To determine the cause of the incident and confirm that no threats remained within the systems, we conducted a digital forensic investigation and log analysis with the assistance of external

cybersecurity experts.

The investigation confirmed that the incident was caused by a ransomware attack targeting certain servers at Pricon.

Although the device used as the initial point of compromise was identified, the exact intrusion route could not be fully determined because certain logs had been encrypted and deleted by the attacker.

The investigation also confirmed that there was no impact on other critical systems within the Yamaichi Electronics Group, including systems in Japan, and that the impacts of the incident were limited to certain systems at the Philippine subsidiary.

3. Confirmation of Information Leakage and Scope of Impact

A detailed investigation of the affected systems confirmed that some data loss occurred on certain devices. However, recovery operations utilizing backup data and other measures were successfully completed, and no material disruption to business continuity occurred.

In addition, log analysis conducted by external experts found no evidence of suspicious communications or abnormal data transfers indicating the external leakage of information.

Furthermore, no information leakage or secondary damage attributable to this incident has been identified as of the date of this announcement.

The affected systems contained personal information relating to customers, business partners, and employees. However, the investigation found no evidence that such information was leaked externally.

4. Recovery Status and Confirmation of System Security

In addition to restoring data, we rebuilt the affected server environment and completed recovery of the systems on April 29, 2026, after confirming their safety.
All systems are currently operating normally.

We have continued monitoring the environment following the recovery and have detected no suspicious activity or signs of further damage. We have therefore confirmed that the systems are currently operating in a secure condition.

5. Measures to Prevent Recurrence

We take this incident very seriously and are committed to further strengthening information security across the entire Yamaichi Electronics Group.

The principal measures being implemented include:

- Deployment and enhanced monitoring of EDR (Endpoint Detection and Response)
- Review of authentication credentials for all system users
- Strengthening privileged account management and access control
- Enhancement of monitoring activities in cooperation with external cybersecurity experts
- Ongoing information security training and awareness programs for employees

We will continue our efforts to improve the security level of the entire group and prevent the

recurrence of similar incidents.

6. Impact on Financial Results

Investigation expenses and system recovery costs have been incurred in connection with this incident. However, at this time, we expect the impact on our consolidated financial results to be immaterial.

Should any matters requiring disclosure arise in the future, we will promptly provide updates.