Translation

Notice: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

August 19, 2026

Company name: SAKATA SEED CORPORATION
Name of Representative: Tsutomu Kagami
President and Representative Director
President and Executive Officer
(Securities code:1377, TSE Prime Market)
Inquiries: Takenori Hoshi
Managing Executive Officer
Senior General Manager of General Administration Div.
(Telephone: +81-45-945-8800)

Notice Concerning Unauthorized Access to Our System and Its U.S. Consolidated Subsidiary's System － Final Report

SAKATA SEED CORPORATION (the "Company") has been working with external IT security specialists to fully understand the situation, identify its causes and implement measures to prevent recurrence to unauthorized intrusion into our servers by a third party which was first disclosed on November 17, 2025, as well as the unauthorized access to the servers of its consolidated subsidiary in the United States disclosed on February 13,2026 (https://corporate.sakataseed.co.jp/en/ir/library/others.html). The Company has now completed its investigation into these incidents and hereby provides a report on the final extent of the impact and the measures implemented to prevent recurrence, as outlined below.

We sincerely apologize for the concern or inconvenience this unauthorized access to the Company's system may have caused to our stakeholders. As a company entrusted with important information by our customers and stakeholders, the Company takes this incident very seriously and is committed to thoroughly implementing security measures and doing our utmost to prevent recurrence.

1. Unauthorized Access to the Company's Servers (disclosed on November 17, 2025; Second Report on December 22, 2025)

1. Overview

The Company detected unauthorized access to its servers by a third party and subsequently conducted a thorough investigation. On November 11, 2025, the Company confirmed evidence indicating that certain data may have been accessed. The Company then conducted further analysis in cooperation with external IT security specialists to investigate the route and circumstances of unauthorized access. As a result, it was determined that personal information relating to customers and business partners may have been accessed without authorization and potentially leaked externally.

To prevent the expansion of any damage and ensure security, the Company has implemented containment and remediation measures, including blocking the intrusion routes and strengthening various security tools.

2. The Status of Leakage

As of now, the types and number of potentially leaked personal information are as follows. No secondary damage resulting from this incident has been confirmed at this time. We have already reported this incident to the relevant authorities.

① Personal information related to distributors and business partners, such as business contractors and product suppliers: approximately 44,000 records Includes name, address (for certain individuals: phone number, email address).

② Personal information of applicants for our original company calendar and the "Seeds of Hope!" campaign: approximately 2,500 records Includes name, address, phone number

③ Personal information related to recruitment for research, technical, and other positions: approximately 5,000 records

④ Personal information of employees, including directors, current and former employees, contractors, and group company employees: approximately 5,000 records

⑤ Personal information related to other business partners: approximately 200 records[1]

Notes

[1] These records were additionally identified during the course of the investigation conducted following the publication of the first and second reports.

3. Cause and Recurrence Prevention Measures

① Cause and Other Detail

Our log analysis has revealed that this unauthorized access originated from a public remote access server and that there is a possibility that administrator privileges were gained. Thereafter, the Company engaged an external security specialist firm to conduct a forensic investigation to determine the cause of the unauthorized access, but no intrusion route or other new facts different from the findings identified through the Company's log analysis were confirmed.

② Recurrence Prevention Measures

Based on the actual status and causes of this unauthorized access, the Company has implemented mainly the following recurrence prevention measures.

- Reviewing the network management system and strengthening communication restrictions
- Strict operation of administrator privileges and strengthening detection of unauthorized access through a 24-hour monitoring system
- Reviewing internal related regulations and thoroughly providing information security training to all employees

4. Guidance and Response for Individuals Potentially Intruded

In accordance with the Act on the Protection of Personal Information, the Company has notified by postal mail those individuals whose personal information may have been compromised. If it is difficult to contact you individually, this public notice will serve as our official communication.

The dedicated inquiry desk for this incident was closed at the end of June 2026. For future inquiries, please contact the following.

Sakata Seed Corporation Personal Information Desk (Customer Relations office)

Phone: 0120-337-936 (toll-free)

Reception Hours: Weekdays 9:00–17:00

2. Unauthorized Access to Servers of the Consolidated Subsidiary in the United States (disclosed on February 13, 2026)

1. Overview

On January 21, 2026, we detected unauthorized access to Sakata America Holding Company, Inc.'s servers, and following our subsequent investigation, we determined that some information may have been accessed or taken by an unauthorized party and such information may have been leaked.

As previously announced, the Company recognizes that there is no direct relationship between this incident and the incident described in 1. above because of differences in intrusion pathways.

2. Investigation Results

As a result of log analysis and forensic investigation conducted by an external IT security specialists, it was determined that the intrusion into the internal network may have originated from remote access credentials.

The impact of this incident has been limited to some systems of Sakata America Holding Company, Inc., our consolidated subsidiary, and no impact on the Company or other domestic and international group companies has been confirmed.

3. Status of Secondary Damage and Recurrence Prevention Measures

At this time, no unauthorized use of the potentially affected information or any other secondary damage resulting from this incident has been confirmed. Furthermore, no significant impact on the subsidiary's operations has been confirmed, and its business continues as usual.

Based on the findings of the investigation, we have implemented recurrence prevention and security enhancement measures, including a review of our network management systems.

4. Contact for Inquiries

If you have any questions regarding both the incident at the Company and the incident at the U.S. subsidiary, please contact Corporate Communications Department.