September 10, 2026

Press release

Company name:	SAKURA internet Inc.
Listing:	Tokyo Stock Exchange
Securities code:	3778
Representative:	Kunihiro Tanaka, President and CEO
Inquiries:	Masataka Kawada, Director, CFO
Telephone:	+81-06-6476-8790

[Summary] (Progress of Disclosed Matters) Publication of Investigation Results and Measures to Prevent Recurrence Regarding Unauthorized Access to SAKURA internet Systems (Third Report)

SAKURA internet Inc. has continued its investigations, in cooperation with an external cybersecurity firm, into the intrusion route, scope of impact, and causes of the incidents described in the announcement titled "Notice Regarding Unauthorized Access to a Portion of SAKURA internet Rental Server Service Environment" published on the SAKURA internet website on August 17, 2026, and the timely disclosure titled "Notice Regarding Unauthorized Access to SAKURA internet Systems" published on August 19, 2026.

As the series of investigations has now been completed, we hereby announce the publication, on September 10, 2026, of "Investigation Results and Measures to Prevent Recurrence Regarding Unauthorized Access to SAKURA internet Systems (Third Report)," which outlines the facts confirmed to date, the final scope of impact, the causes of the incident, and measures to prevent recurrence.

We have completed containment measures regarding the unauthorized access as well as communications and credentials determined to be related to the incident. Furthermore, our investigations found no clear evidence that any data was exfiltrated. In addition, no unauthorized use of information resulting from this incident, nor any other secondary damage, has been confirmed at this time.

As a company entrusted with our customers' valuable information, we take this matter very seriously. Based on the findings of these investigations, we will steadily implement measures to prevent recurrence from technical, operational, and organizational perspectives, while continuing to treat information security as a key management priority and pursuing ongoing improvements.

Based on the investigation results disclosed in the Third Report and the response-related costs currently identified, we expect the impact of this incident on our consolidated financial results for the fiscal year ending March 31, 2027, to be limited. Accordingly, we do not currently intend to revise our earnings forecast as a result of this incident. Should any matters requiring further disclosure arise, we will promptly make an announcement.

SAKURA internet

To all media organizations

September 10, 2026
SAKURA internet Inc.

Results of Investigations into Unauthorized Access to SAKURA internet Systems and Measures to Prevent Recurrence (Third Report)

Regarding “Notice Regarding Unauthorized Access to a Portion of SAKURA internet Rental Server Service Environment” released on August 17, 2026, and “Notice Regarding Unauthorized Access to SAKURA internet Systems (Second Report)” released on August 19, 2026, SAKURA internet has conducted investigations with an external cybersecurity firm to determine the route of intrusion, the scope of impact, and the cause of the incident.

Now that the series of investigations into this incident has been completed, we would like to report on the facts we have confirmed to date, the final scope of impact, the cause of the incident, and measures to prevent recurrence.

We have completed containment measures regarding the unauthorized access and any communications and credentials determined to be related to it. Our investigations found no evidence of any data exfiltration, and no unauthorized use of information resulting from this incident, nor any other secondary damage, has been confirmed at this point in time.

We would like to sincerely apologize to our customers, business partners, partner companies, and all other stakeholders for the significant concern and inconvenience we have caused.

1. Overview of Incident

On August 9, 2026, we detected an anomaly on the maintenance servers for our SAKURA Web Hosting rental server service, and we initiated an investigation to verify the facts and determine the scope of impact.

As a result of our investigation, we have confirmed the following.

・Unauthorized access to SAKURA Web Hosting servers
・Installation of malware on a portion of those servers
・Unauthorized access to the database of the system used to manage contract information and other data of customers using our services (hereinafter “Sales Management System”)

Upon confirmation, the necessary containment measures were immediately taken, including blocking suspicious communications, isolating the affected environment, removing malware, and reviewing credentials.

Subsequently, an investigation was conducted by our internal team of specialists and an external cybersecurity firm, examining the relevant servers, various logs, and configurations to determine the route of intrusion, the attacker’s activities, and the scope of systems and information that were potentially affected.

2. Background

The main developments from the time of the discovery of this incident to the present are as follows.

Date	Details
August 9, 2026	Anomaly detected on SAKURA Web Hosting maintenance servers; investigation initiated
August 9-19, 2026	Suspicious behavior detected; measures such as disabling credentials, blocking suspicious communications, isolating the affected environment, removing malware, and other containment actions implemented
August 17, 2026	“Notice Regarding Unauthorized Access to a Portion of SAKURA internet Rental Server Service Environment” released
August 19, 2026	Investigations reveal possibility of unauthorized access to the Sales Management System and potential impact on customer information; Second Report released
August 26, 2026	Dedicated telephone hotline for this incident established; information added to Second Report
August 26, 2026 onward	Individualized support provided to potentially affected customers, ongoing investigations into related systems and consideration of measures to prevent recurrence
September 10, 2026	Results of investigations, scope of impact, and measures to prevent recurrence published in Third Report

3. Overview of Investigations

To ascertain the facts of this incident and the scope of its impact, we conducted the following investigations, focused primarily on these matters.

・Investigation of servers where unauthorized access was detected and servers that may be affected
・Investigation of logs, including connection, authentication, and operation records
・Investigation for the presence of malware, malicious files, and malicious settings
・Investigation into traces of data exfiltration
・Investigation of operations performed on the Sales Management System and information that may have been accessed
・Emergency inspection of the operating environments for services other than SAKURA Web Hosting
・Monitoring of the Internet and Dark Web to detect disclosure and unauthorized use of information related to this incident
・Confirmation and verification of internal investigation results by an external cybersecurity firm

4. Investigation Results

The results of our investigations are detailed below.
However, in the interest of security and to prevent copycat attacks, we shall refrain from disclosing any specific attack code, IP addresses, specific system and network

configurations, authentication methods, or other technical details.

(1) Results of Investigation Regarding SAKURA Web Hosting

An investigation confirmed unauthorized access to a portion of the SAKURA Web Hosting servers and the installation of malware on some servers.
As of the announcement made on August 17, 2026, 583 accounts that were potentially subject to unauthorized viewing or acquisition by third parties were identified. However, subsequent further investigation confirmed that an additional 368 accounts were also potentially subject to the same risk.
As a result, the total number of potentially affected accounts came to 951. We are contacting the potentially affected customers individually.

An investigation of the additional 368 accounts was conducted, but no clear evidence linking them to the unauthorized access to the 583 accounts announced on August 17 was found, including regarding the timing and method of the incident.
Although we were unable to confirm any connection to the initial unauthorized access, the possibility of impact cannot be completely ruled out. Therefore, we have taken the necessary measures regarding the additional 368 accounts that were identified as well.

Furthermore, during the course of our investigations, traces of suspicious activity within the SAKURA Web Hosting environment that appeared to date from July 2025 or later were identified.
Together with an external cybersecurity firm, we investigated these traces of activity to determine their connection to the incident, the methods of unauthorized access, and the scope of their impact.
The results of this investigation confirmed that these traces of activity do not indicate an ongoing breach and that there has been no unauthorized use of information or other secondary damage.

However, due to limitations in our records over time and other factors, we were unable to objectively determine whether this activity was the same as the incident in question, identify specific routes of intrusion, or confirm any impact on customer information.
For this reason, the scope of impact and number of cases covered in this report include not only matters confirmed to be related to this incident, but also matters where, although an objective link could not be confirmed, the possibility of impact on customers cannot be ruled out.

(2) Results of Investigation Regarding the Sales Management System

During the course of our investigation into SAKURA Web Hosting, we confirmed unauthorized access to the system used to manage contract information and other data of customers using our services (hereinafter “Sales Management System”).
The Sales Management System is a system used to manage contract information and other data for our various services, including SAKURA Web Hosting, yet is a separate system from the environment used to actually provide these services.
This investigation confirmed the possibility that member information and other data stored in the Sales Management System may have been viewed or acquired by a third party. The total number of member accounts potentially affected is 1,360,563.

Additionally, it was confirmed that hashed passwords associated with member IDs for 30

of these accounts may have been accessed.

Furthermore, this investigation also confirmed that unauthorized access to the Sales Management System occurred between April 2023 and March 2026.

Meanwhile, an investigation was conducted into the possible connection between the unauthorized access to SAKURA Web Hosting and the unauthorized access to the Sales Management System, but found no clear evidence linking the two was discovered.

In the interest of security and to prevent copycat attacks, we shall refrain from revealing any technical details with regard to routes of intrusion or system configurations.

*Hashed password information is data that has been processed to make it difficult to guess or recover the original password, rather than simply storing the original password as-is.

(3) Results of Investigation Regarding Password Information and Measures Taken

As detailed in our Second Report regarding information that may have been subject to unauthorized viewing or acquisition by third parties, the Sales Management System contained initial server passwords for some SAKURA Web Hosting services and some initial administrator passwords for some SAKURA VPS services.

With regard to SAKURA Web Hosting, for contracts confirmed to have server passwords potentially affected by this incident that were still in use, the server passwords were changed to protect customers' accounts and prevent unauthorized access by third parties. Affected customers are being contacted individually and asked to log in to the Member Menu and set a new password of their choosing.

Customers with SAKURA VPS contracts where this information was stored are being notified individually; those who are still using the initial password issued to them at the time of contract are being asked to change their password.
Unlike the password information for the 30 accounts listed in the previous section, these passwords are not hashed.
Please note that the Sales Management System does not store passwords that customers have changed from their initial passwords. Additionally, for passwords that have been changed from their initial passwords, those current passwords differ from the password information stored by SAKURA internet. Therefore, there is no risk of unauthorized access related to this incident.

(4) Results of Investigation Regarding Other Service Provision Environments and Internal Systems

In response to this incident, we have conducted an emergency inspection of our service provision environment and related internal systems.
The results of this inspection showed no signs of unauthorized access in any of our service provision environments, with the exception of SAKURA Web Hosting.
Additionally, investigations and strengthened monitoring of other related internal systems besides the Sales Management System are being conducted, and at this time, no signs of unauthorized access have been detected.
We are continuing to monitor and verify the situation.

5. Information That May Have Been Affected

Investigation results indicate that the information stored on some SAKURA Web Hosting servers in customers' allocated space and in the Sales Management System that may have been viewed or acquired by a third party is as follows.

Potentially Affected	No. of Accounts	Content of Information
A subset of SAKURA Web Hosting customers	951	[Information stored on SAKURA Web Hosting servers in customers' allocated space] ・User identifiers ・Information stored in customers' environments (e-mail data, website data, log information, other files stored in customers' space, etc.)
A subset of customers registered with SAKURA internet	1,360,563	[Member information and contract information stored in the Sales Management System] ・Member IDs ・Company names ・Department names ・Addresses ・Names ・Telephone numbers ・E-mail addresses ・Birthdates ・Genders ・Fax numbers ・Contracted services ・Contract periods ・Billing amounts, etc.
	30 of the above accounts	[Member information stored in the Sales Management System] ・Hashed passwords associated with member IDs

*The 1,360,563 accounts include SAKURA Web Hosting customers as listed in the first row of the table.
*The table above lists the types of information stored in the Sales Management System. It does not necessarily indicate that all of the above information pertaining to any individual customer is possessed by SAKURA internet, nor does it indicate that it has actually been viewed or acquired by a third party.
*SAKURA internet does not retain any credit card information, and no evidence of input screen tampering or similar unauthorized modifications has been identified. Accordingly, there is no risk of credit card numbers being compromised.
*The information stored in the Sales Management System includes some initial server passwords for SAKURA Web Hosting services and some initial administrator passwords for SAKURA VPS services. This information is different from the hashed passwords associated with the member IDs of the 30 accounts mentioned above. Affected customers are being contacted individually and are being asked to take the necessary measures.

6. Status of Data Exfiltration and Secondary Damage

Our investigations found no evidence of any data exfiltration, and no unauthorized use of information resulting from this incident, nor any other secondary damage, has been confirmed at this point in time. Additionally, the following facts have yet to be confirmed.

・Disclosure of any information involved in this incident on the Internet and Dark Web
・Unauthorized use of accounts resulting from this incident
・Financial losses resulting from this incident
・Instances of phishing, identity fraud, and other secondary damages resulting from the use of the information involved in this incident
・New instances of unauthorized access or the spread of damage following implementation of containment measures

Please note that, while no secondary damage has been confirmed at this point in time, extreme caution should be exercised in regard to phishing e-mails, suspicious phone calls and text messages, and attempts at identity fraud that may be exploiting this incident. SAKURA internet will continue to monitor the Internet for disclosure or unauthorized use of information.

7. Response to Customers

In addition to issuing public announcements and publishing FAQs regarding this incident, a dedicated customer support channel has been established, and response to inquiries is ongoing.

Additionally, the following customers are being contacted individually via e-mail and other means.

・Customers whose use of SAKURA Web Hosting may have been affected by this incident (including customers for whom it has been determined that their server passwords and e-mail passwords need to be changed)
・SAKURA VPS customers for whom it has been determined that their initial administrator password needs to be verified or changed
・Customers whose member information stored in the Sales Management System may have been affected

[Request to customers who have been contacted individually]
Customers who have been contacted individually are asked to review the details of the notification and take the necessary actions.

Going forward, in the event that it becomes clear that customers need to take further measures on their own, affected customers will be contacted individually and notifications will be posted on the SAKURA internet website.

Please note that for customers who cannot be contacted individually due to incomplete registration or other reasons, this announcement shall serve as their notification.

8. Measures Taken to Contain the Situation and Prevent Further Impact

After confirmation of this incident, the following key measures were implemented to prevent further spread of its impact.

・Disabling of credentials that may have been used for unauthorized access
・Blocking of suspicious communications and strengthening of source restrictions
・Isolation of affected environments
・Investigation and removal of malicious settings and malware

・Emergency inspection of related servers, systems, and networks
・Rebuilding of servers that were subject to unauthorized access
・Enhanced monitoring through measures such as expanding the scope of EDR deployment
・Direct communication with customers who may have been affected
・Reporting and sharing of information with relevant institutions
・Investigation and verification in conjunction with an external cybersecurity firm

9. Measures to Prevent Recurrence

SAKURA internet is handling this incident with the utmost importance. In addition to implementing the following measures in order to prevent recurrence, further measures will also be implemented in phases.

(1) Recurrence Prevention Measures Already Implemented
・Comprehensive review and tightening of administrator privileges and access permissions
・Review of access routes to critical systems and strengthening of communication restrictions
・Review of authentication methods and credential management practices
・Enhanced monitoring through measures such as expanding the scope of EDR deployment
・Strengthening of security settings for administrative servers

(2) Measures to Be Implemented
・Strengthening of multi-layered access controls for administration environments, internal systems, and service provision environments
・Expansion of monitoring targets and detection capabilities aimed at early detection of unauthorized access
・Review of the scope of security log collection, retention periods, and analysis capabilities
・Cleanup of all SAKURA Web Hosting servers through rebuilding
・Implementation of regular external audits and third-party evaluations
・Strengthening of continuing security education and incident response training
・Strengthening of information security governance and reporting structures, including at the executive management level

10. Actions Going Forward

SAKURA internet, as a provider of digital infrastructure services entrusted with customers' valuable information, is taking this incident very seriously.
Based on the findings of these investigations, we will steadily implement measures to prevent recurrence from technical, operational, and organizational perspectives, and remain committed to continuous improvement by treating information security as a key management priority.
Should any new facts requiring disclosure come to light going forward, we will carefully examine the details and provide notification promptly.

Once again, we offer our deepest apologies to our customers, business partners, partner companies, and all other stakeholders for the significant concern and inconvenience we have caused.

11. Related Information (in Japanese)

- Notice Regarding Unauthorized Access to a Portion of SAKURA internet Rental Server Service Environment (August 17, 2026)
  https://www.sakura.ad.jp/corporate/information/newsreleases/2026/08/17/1968225614/
- Notice Regarding Unauthorized Access to SAKURA internet Systems (Second Report) (Updated 18:40, August 19, 2026)
  https://www.sakura.ad.jp/corporate/information/newsreleases/2026/08/19/1968225633/
- Information Regarding Unauthorized Access to SAKURA internet Systems and Frequently Asked Questions (FAQ)
  https://help.sakura.ad.jp/unauth-access-faq/
- [SAKURA VPS] Request to Change Administrator (Root) Passwords
  https://vps.sakura.ad.jp/contents/info/password-change-faq/
- [SAKURA Web Hosting] [Urgent] Request to Change Server Passwords and E-Mail Passwords
  https://help.sakura.ad.jp/notification/n-2692/