October 27, 2026
IDC Frontier Inc.

IDC Frontier Reports Investigation Findings and Next Steps Regarding Unauthorized Access

IDC Frontier Inc. (“IDC Frontier”) sincerely apologizes for the serious concern and inconvenience caused to its customers and related parties due to unauthorized third-party access to its cloud service, “IDCF Cloud.”*1

IDC Frontier completed its investigation into this incident and would like to report on the facts confirmed to date, the scope of the impact, causes, and measures to prevent recurrences.

Following a detailed investigation conducted in collaboration with an external cybersecurity firm, IDC Frontier determined that a third party exploited a vulnerability in open-source software used by the “IDCF Cloud Portal” authentication system, which customers use to perform tasks such as launching virtual servers and checking billing information, to gain unauthorized access to the authentication system. Subsequently, a ransomware attack caused some customers’ virtual servers to be shut down and encrypted. However, the investigation confirmed that no data stored on customers’ virtual servers was leaked externally. Currently, all virtual servers are operational except for some of those affected by the attack in East Japan Region 1. However, the “IDCF Cloud Portal,” which contained the vulnerability, has been isolated from external access and remains unavailable. IDC Frontier plans to resume its operation once its security has been thoroughly verified.
IDC Frontier has individually contacted the 495 corporate and local government customers who were using some of the virtual servers affected by the attack in East Japan Region 1. In coordination with its parent company SoftBank Corp., IDC Frontier is mobilizing resources company-wide to help these customers restore their systems as quickly as possible, including assisting with migration to alternative environments and the retrieval of backup data.

In response to this incident, IDC Frontier established an independent organization dedicated to security management and strengthened security governance across the company.
Furthermore, based on the findings of its investigation to date, IDC Frontier will implement fundamental measures to prevent recurrences across its organization, systems, and operations, including automating software vulnerability assessments and remediation, and expanding mechanisms to detect unauthorized access early.

IDC Frontier will steadily implement measures to prevent recurrences and work to ensure the security of “IDCF Cloud” to restore trust in the service.

1. Overview of unauthorized access and service disruption

As a result of a ransomware attack on IDC Frontier’s cloud service, “IDCF Cloud,” an incident occurred at approximately 3:40 a.m. on October 7, 2026, in which some customers using East Japan Region 1 experienced virtual server shutdowns and were unable to restart their virtual servers.

■ Impact scope

495 corporate and local government customers using certain zones in East Japan Region 1 (tesla zone / henry zone / pascal zone / joule zone).

■ Event chronology

Date and time	Key events and actions taken
October 7, at approximately 3:40 a.m.	Service disruption occurred and was detected, recovery efforts initiated.
October 7, at approximately 6:20 a.m.	Initiated investigation, including the possibility of cyberattack
October 7, 6:48 a.m.	Suspended “IDCF Cloud Portal” service in East Japan Region 1
October 7, 7:00 a.m.	Disconnected storage devices in the four affected zones in East Japan Region 1
October 7, 9:00 a.m.	Established emergency response headquarters
October 7, 11:42 a.m.	Identified cause of service disruption as a ransomware attack by a third party
October 7, from 12:15 p.m. to 2:05 p.m.	● Suspended “IDCF Cloud Portal” service in other regions. ● Disconnected networks connecting “IDCF Cloud Portal” in all regions to external networks.
October 7, 4:00 p.m.	Initiated investigation in collaboration with external cybersecurity firm
October 8	● Established emergency support contact point for customers ● Began providing customers with information on alternative environments
October 10	Began providing customers with instructions for migrating to alternative environments

October 14	● Based on investigation results, determined that no data stored on customers' virtual servers had been leaked externally ● Confirmed that backup data could be retrieved for 194 customers ● Confirmed that unauthorized inquiries had been made regarding registered information on 48 corporate customers in the "IDCF Cloud Portal"
October 17	Began retrieving backup data and providing it to customers
October 18	Resumed provision of "IDCF Cloud Backup" service
October 20	Confirmed that backup data could be retrieved for 206 customers
October 27	● Confirmed that unauthorized queries were made regarding registered information on up to 71 corporate customers in the "IDCF Cloud Portal" ● Completed investigation, which included matters mentioned above.

2. About the investigation

In collaboration with an external cybersecurity firm, IDC Frontier conducted an investigation into the intrusion route, impact scope, and whether any information was leaked, including through the analysis of various logs and malicious programs.

Main investigation areas

- Attacker's intrusion route
- Various logs (access logs, authentication logs, and operation logs)
- Malicious programs installed by the attacker, as well as processes configured and executed by the attacker
- Whether there was any evidence of data exfiltration from customers' virtual servers

(1) Overview of ransomware attack

After infiltrating the authentication system of the "IDCF Cloud Portal," the attacker used the management console to gain unauthorized administrator privileges for the virtualization infrastructure, shut down customers' virtual servers, and encrypted the virtual servers.

(2) Cause

The unauthorized access by a third party occurred as a result of the exploitation of a vulnerability in open-source software used by the “IDCF Cloud Portal.”

(3) External Leakage of Data Stored on Customers’ Virtual Servers

No data stored on customers’ virtual servers was leaked externally. With regard to data stored on customers’ virtual servers in certain zones of East Japan Region 1 affected by the ransomware attack, no evidence of data exfiltration or facts substantiating such exfiltration were identified. Furthermore, currently no unauthorized use of information or other secondary damage resulting from this incident has been confirmed. IDC Frontier also conducted investigations to verify the security of zones unaffected by the service disruption and other regions, and similarly found no evidence of data exfiltration.

(4) Unauthorized inquiries regarding registered information in the “IDCF Cloud Portal”

In a previous update (issued in Japanese), IDC Frontier reported that information relating to 48 corporate customers, as well as the email addresses of two corporate customers that may contain individuals’ names, had been subject to unauthorized inquiries. Through IDC Frontier’s continued investigation, it was subsequently confirmed that unauthorized inquiries had been made to the registered information of up to 71 corporate customers in the “IDCF Cloud Portal,” which customers use to perform tasks such as launching virtual servers and checking billing information. The information subject to unauthorized inquiries included personal names and email addresses that may contain individuals’ names, involving up to 31 corporate customers (31 records). However, no evidence was found indicating that the information accessed through these unauthorized inquiries had been exfiltrated. In addition, IDC Frontier confirmed that up to four customer login passwords associated with the information subject to unauthorized inquiries had been changed without authorization. The affected passwords have already been reset, and the customers concerned have been contacted individually.

3. Measures to prevent further damage and customer support

Following this incident, IDC Frontier has worked to determine its cause while prioritizing efforts to prevent further damage and provide support to affected customers.

(1) Measures to prevent further damage

Following the service disruption, to prevent further damage, IDC Frontier suspended the externally accessible “IDCF Cloud Portal” service in East Japan Region 1, which includes the four zones affected by the attack, and disconnected the storage devices in the four affected zones. Subsequently, as a precautionary measure to verify security,

IDC Frontier also suspended the “IDCF Cloud Portal” service in all other regions and disconnected the networks connecting the “IDCF Cloud Portal” in all regions to external networks.

(2) Establishment of investigation and recovery framework
IDC Frontier established an emergency response headquarters at 9:00 a.m. on October 7, 2026, and has been responding to the incident in close coordination with its parent company, SoftBank Corp. IDC Frontier has also been reporting the incident to and consulting with relevant authorities, including Japan’s regulatory authorities and police. IDC Frontier has not had any contact with the attacker and has neither paid any ransom nor engaged in any negotiations.

(3) Support for restoring customer systems
In a previous update (issued in Japanese), IDC Frontier reported that it was expected to be difficult to restore the systems of the 495 customers in the affected zones within their existing environments, and that backup data could be retrieved for 194 customers who had been using the “Snapshot Feature.”*[2] However, through continued investigation, IDC Frontier confirmed that backup data can be retrieved for 206 customers. IDC Frontier will continue to work closely with its parent company SoftBank Corp. and make every effort to support customers in restoring their systems as quickly as possible, including by proposing specific procedures for migrating to alternative environments and retrieving backup data.

4. Measures to prevent recurrences

In light of this incident, IDC Frontier will implement the following measures to prevent recurrences.

(1) Strengthen company-wide security governance structure
- Established an independent organization dedicated to security management by bringing in external experts and assembling internal security personnel (completed).

(2) Strengthen mechanisms for early identification and remediation of software vulnerabilities
- Clearly define implementation plan and frequency of vulnerability assessments in internal policies, expand the scope of vulnerability and penetration testing to include open-source software by leveraging security solutions such as SoftBank Corp.’s “Patching as a Service (PaaS),” and conduct these assessments on an ongoing basis.

- Centralize software composition information previously managed by individual departments across the company (by creating a Software Bill of Materials (SBOM)*[3]) and automate the cross-referencing of this information against known vulnerabilities.

5. Resumption of IDCF Cloud Portal

The “IDCF Cloud Portal” is currently unavailable until its security can be assured. IDC Frontier is taking the following measures to ensure its security.

- Rebuild the “IDCF Cloud Portal” in a new environment
- Change the authentication credentials for all servers that comprise the “IDCF Cloud Portal”
- Replace the authentication system that was the cause of the intrusion with a more secure and reliable system provided by an external Identity Provider (IdP)
- Restrict access to the “IDCF Cloud Portal” to customer IP addresses and make multi-factor authentication mandatory.
- Expand the scope of vulnerability assessments and penetration testing using solutions such as SoftBank Corp.’s “Patching as a Service (PaaS)” and conduct these assessments on an ongoing basis

Furthermore, to minimize the impact on customers and safely resume the provision of the “IDCF Cloud Portal” service, we will proceed with the following three-phase approach.

Phase 1

Key functions performed by IDC Frontier on behalf of customers (currently underway)

- Starting and stopping virtual servers
- Changing security settings
- Changing network and communication settings
- Starting and stopping databases, and changing database settings

Phase 2

All functions operated by IDC Frontier on behalf of customers

- Creating and deleting virtual servers, and modifying their performance and capacity
- Adding and deleting data storage volumes, and changing their capacity
- Using the snapshot feature
- Creating databases and changing database settings

Phase 3

Resumption of the “IDCF Cloud Portal” service

- Resume provision of the “IDCF Cloud Portal” service with all functions available for customers to operate themselves

Message from Katsuhisa Suzuki, President & CEO, IDC Frontier Inc.

We sincerely apologize for the serious inconvenience and concern this incident has caused our customers and all other related parties.

We recognize that the service disruption resulting from this unauthorized access is an extremely serious incident, affecting not only customers who use our cloud services but also the business operations of their customers. The affected customers continue to bear a significant burden, including the need to rebuild their systems. We will continue to mobilize our resources across the company to provide full support to customers so they can restore their systems as quickly as possible and eliminate the impact on their business operations.

We take this incident very seriously and will thoroughly review our efforts to date, make necessary improvements, and implement measures to prevent recurrences. We will also further strengthen our security measures and governance to address increasingly sophisticated and complex cyberattacks driven by advances in AI. Recognizing the significant responsibility we bear as a provider of critical digital infrastructure that supports society, we will make every effort to restore the trust of all our stakeholders.

*1 IDCF Cloud TypeS (formerly White Cloud ASPIRE) and IDCF Private Cloud are not affected by this incident.
*2 A feature that saves the state of a virtual server’s data storage at a specific point in time.
*3 Compiling a list of information on software components, their versions, and other relevant details.

Customer inquiries
Inquiry form

Media inquiries
IDC Frontier Inc.
Email: pr@idcf.jp