June 23, 2026

＜Press Release＞

KDDI Corporation

Unauthorized Access to Email System for ISP Providers

On June 17, 2026, we confirmed that some information related to email services (hereinafter, "the email services") provided by Internet Service Providers (hereinafter, "ISP providers") may have been leaked externally from the email system (hereinafter, "the system") that we provide to ISP providers.

We sincerely apologize for the significant inconvenience and concern caused to all parties concerned, including ISP providers and their customers.

1. Timeline of Events

On June 17, 2026, we confirmed that the system we provide to ISP providers had been subjected to unauthorized access (hereinafter, "this unauthorized access"). On the same day, we modified the system to prevent further damage. We have identified the suspected points of this unauthorized access and implemented technical defensive measures.

Investigation results revealed that this unauthorized access exploited a vulnerability in third-party software used in the system, potentially leading to the leakage of customer email-related information necessary for using the email services. We are continuing our investigation to identify the scope of the impact and other details.

We are also taking necessary actions regarding this unauthorized access, including reporting to and consulting with the Personal Information Protection Commission and the Ministry of Internal Affairs and Communications, in accordance with relevant laws and regulations.

2. Affected ISP Providers

The following six ISP providers and their email services are affected:

STNet, Incorporated: Email services related to "Pikara Hikari Service," "Pikara Mobile

Service," and "Oshigoto Pikara Service"

KDDI Web Communications Inc.: Email services for the "CPI" rental server

JCOM Co., Ltd.: Email services for "J:COM NET" and cable TV providers

CHUBU TELECOMMUNICATIONS CO., INC.: Email services for Commufa Hikari and Business Commufa

NIFTY Corporation: @nifty Mail

BIGLOBE Inc.: BIGLOBE Mail

※*Listed in alphabetical order (Japanese syllabary)*

3. Potentially Leaked Email-Related Information

A maximum of 14.22 million email addresses and passwords associated with mailboxes created for these email services.

※This includes customers who have cancelled their services and inactive customers who have not used the service for a certain period.

※This includes passwords that have been hashed and/or encrypted.

※As the investigation is ongoing, this figure represents the maximum potential number.

4. Information for Affected ISP Providers

We have been contacting affected ISP providers sequentially since June 17, 2026. Concurrently, we are proceeding with discussions and implementation of countermeasures.

While technical defensive measures for the system have been implemented, there is a possibility that customers' email addresses and passwords may have been illicitly obtained by third parties due to this unauthorized access. To ensure the protection of customer data and eliminate future and potential risks, it is necessary for customers to change their email passwords. We urge customers to check the information provided by their ISP providers and take prompt action.

We will continue to cooperate with ISP providers to facilitate prompt notification to customers regarding password changes and to support related measures.

End