Press Release

Occurrence of Spam E-mail Transmission

February 4, 2026

National Institute of Health Sciences, Japan

Dear Collaborators

It has been confirmed that e-mail address of the National Institute of Health Sciences was fraudulently used by a third party to send spam e-mails to external addresses via the institute's web-mail system. The sent spam e-mails have been identified as phishing e-mails containing one or two URL links within the body text.
We sincerely apologize to those who received these e-mails.

The details of the incident are as follows:

1. Overview

Spam e-mails were sent from an e-mail address of the National Institute of Health Sciences between 22:23 on Thursday, January 8, 2026, and 04:47 on Friday, January 30, 2026 (in Japan standard time, UTC+9 hours).
The sender's e-mail address was mps-kyogikai [at] nihs.go.jp. The subject lines and body texts of the e-mails varied. Approximately 70,000 e-mails were sent, primarily targeting free e-mail addresses and other countries' addresses other than Japan. Recipients of these e-mails are requested not to click on any links.
Please note that the information handled by the institute using this e-mail account was classified as Confidentiality Level 1 (publicly available information or information that can be disclosed without any issue). No leakage of personal information or similar has been confirmed at this time.

2. Cause

Investigations indicate it is highly probable that authentication credentials were stolen by a third party after the account holder received a phishing e-mail. It is believed that the stolen credentials were then used maliciously to send spam e-mails via the National Institute of Health Sciences' web-mail system.

3. Treatment Status

After confirming the spam e-mail transmission, necessary measures were implemented, including forcing a password change and disabling the affected e-mail account, as well as blocking the IP address used for the unauthorized activity. At this time, no other accounts have been confirmed to have been compromised using similar ways.

4. Preventive Measures

In light of this incident, we called an attention for members of our institute and enhance the employee training regarding phishing e-mail countermeasures. Additionally, we will strengthen authentication functions within the web-mail system and review our monitoring systems to detect suspicious access and behavior at an early stage.