Final Report

November 1, 2013
Remote Sensing Technology Center of Japan

1. Summary

On 18 July, the CROSS-EX server[*1] that is used on the CROSS-EX system was attacked as a result of system vulnerabilities, and the homepage was found to have been tampered with. Consequently, the server was suspended and investigations were conducted. On 24 July, signs that were found on a section of this server showed that there had been unauthorized access into the server. It was confirmed that customer information registered on the server may have been leaked out as a result of this unauthorized access, and an internal emergency response headquarters was established in RESTEC. On 25 July, a notice about the unauthorized access was published on RESTEC's website.

The investigations were conducted with the cooperation of the relevant parties, obtained through submitting notification about the matter to them. These parties included the developer, Tokyo Metropolitan Police Department (TMPD), the Security Center of the Information-technology Promotion Agency, Japan (IPA), and the JPCERT Coordination Center. As a result of the investigations, we uncovered the full details about the unauthorized access into CROSS-EX, and verified that no secondary damage had been incurred by the external parties that were recipients of information from the server in question. However, we also concluded that it was not possible to identify the information that had leaked out as a result of the unauthorized access. As of the current point in time, we have not received any reports from our customers pertaining to damages arising as a result of this incident.

2. Damages

The unauthorized access took place between 01:00 and 20:40 on 18 July, and the final confirmed damages are listed as follows.

(1) Tampering with the landing page of the CROSS-EX website

(2) Uploading of programs to facilitate and cover up the unauthorized access

(3) Access to the catalogue server[*2], etc.

- There is no customer credit card information on the catalogue server.
- Registered information belonging to customers is not contained within the catalogue server.

3. Measures toward the resumption of operation

Measures were taken toward the resumption of the search service on CROSS-EX, including strengthening security for the management of passwords.

[Notes]

*1. CROSS-EX server: Web server that facilitates search and order of images and other tasks

*2. Catalogue server: Server that contains customer information, etc.