November 10, 2020

To all current students, graduates, faculty and staff members, and those who have left Keio University:

Notice and apology for leak of personal information due to unauthorized access to SFC-CNS and SFC-SFS

Vice-President for Information Infrastructure (IT) and Shonan Fujisawa Campus, Keio University
Chief Information Officer, Keio University
Jiro Kokuryo

We would like to inform you of the discovery that the IDs and passwords of 19 users (faculty and staff members) were stolen in some way from the information network system (SFC-CNS) and class support system (SFC-SFS) of Shonan Fujisawa Campus (SFC), and that the personal information of users may have been leaked from the system due to unauthorized external access using the stolen IDs and passwords and an attack aimed at a vulnerability in the Class Support System (SFC-SFS). We deeply apologize for the significant trouble and distress this has caused to all persons concerned. No secondary damage has been confirmed at this time.

As a result of our investigations, the personal information that may have been leaked is as follows.

All of this personal information that was managed by the Keio University SFC Office (some system management was outsourced to a contractor) concerns students, faculty members, staff members, etc.

a. Details of personal information that may have been leaked

a-1) Student information

- Number of cases: 5,088
- Details: Student ID numbers, personal names, account names, e-mail addresses (●●@sfc.keio.ac.jp) issued by SFC, information on affiliation (faculty, year level, class group, rules and regulations), dates of admission, number of semesters enrolled
- Applicable persons:
  - ① Students enrolled in the Faculty of Policy Management, Faculty of Environment and Information Studies, Graduate School of Media and Governance, Faculty of Nursing and Medical Care, and Graduate School of Health Management in the Fall Semester of the 2020 academic year.
  - ② Students from other campuses who attended classes or served as TA or SA in classes at the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance in the Spring Semester of the 2020 academic year.

a-2) Data of students' ID photos

- Number of cases: 18,636
- Details: data files of portrait photos submitted for Student ID card at the time of admission (file names were hashed to make it difficult to match the users)

・ Applicable persons:
  ① Students enrolled in the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance from the 2007 academic year onward (including students who have already left)
  ② Students enrolled in the Faculty of Nursing and Medical Care and Graduate School of Health Management from the 2016 academic year onward (including students who have already left)
  ③ Students from other campuses taking specific classes at the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance (including students who have already left) 29 cases

a-3) Information on course registration history (earned credits)
・ Number of cases: 4,493
・ Details: information related to credits earned for lecture courses (course names, faculty members in charge, year levels, and semesters in which credits earned)
・ Applicable persons:
  ① Students enrolled in the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance as of March 11, 2020

a-4) Faculty member information
・ Number of cases: 2,276
・ Details: ID numbers, personal names, account names, affiliations (including concurrent posts), positions
・ Applicable persons:
  ① Full-time faculty members who have been affiliated with the Faculty of Policy Management, Faculty of Environment and Information Studies, Graduate School of Media and Governance, Faculty of Nursing and Medical Care, and Graduate School of Health Management from December 2000 onward (including faculty members who have already left)
  ② Faculty members (part-time, etc.) who have taught classes at the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance from December 2000 onward (including faculty members who have taught classes in the past)

a-5) Faculty member profile data
・ Number of cases: 2,276
・ Details: e-mail addresses (●●@sfc.keio.ac.jp) issued by SFC, passwords required to log in to the syllabus system and faculty profile system (different from SFC-CNS password), birth years

・ Applicable persons:
  ① Full-time faculty members who have been affiliated with the Faculty of Policy Management, Faculty of Environment and Information Studies, Graduate School of Media and Governance, Faculty of Nursing

and Medical Care, and Graduate School of Health Management from December 2000 onward (including faculty members who have already left)

② Faculty members (part-time, etc.) who have taught classes at the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance from December 2000 onward (including faculty members who have taught classes in the past)

a-6) Data of faculty members' addresses

- Number of cases: 193
- Details: home addresses
- Applicable persons:
  - ① Full-time faculty members who were registered between December 2000 and the 2009 academic year affiliated with the Faculty of Policy Management, Faculty of Environment and Information Studies, Graduate School of Media and Governance, Faculty of Nursing and Medical Care, and Graduate School of Health Management (including faculty members who have already left)
  - ② Faculty members (part-time, etc.) who were registered between December 2000 and the 2009 academic year teaching classes at the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance and (including faculty members who have taught classes in the past)

  *193 faculty members (or former faculty members) to which the above applies have been identified, and those with contact information are being notified by the university in sequential order. The same procedures are taken for the following a-7–11 as well.

a-7) Personal e-mail data of faculty members

- Number of cases: 2 people
- Details: e-mail data owned by individual faculty members (may include the contents of a-1, 3, 4 above)
- Applicable persons: 2 people out of the 19 users confirmed to have been victims of unauthorized access

a-8) Individual e-mail data of faculty members (received between August 20 and September 16)

- Number of cases: 15 people
- Details: e-mail data owned by individual faculty members received between August 20 and September 16 (may include the contents of a-1, 3, 4 above)
- Applicable persons: 15 people out of the 19 confirmed to have been victims of unauthorized access

a-9) keio.jp e-mail data of individual faculty members

- Number of cases: 5 people
- Details: keio.jp e-mail data owned by individual faculty members (may include the contents of a-1, 3, 4 above; there is no log information to indicate all were obtained at once)

a-10) User home directory data of individual faculty and staff members

・ Number of cases: 19 people
・ Details: data placed on the user home directory owned by individual faculty and staff members (may include the contents of a-1, 3, 4 above)
・ Applicable persons: the 19 users confirmed to have been victims of unauthorized access

a-11) Information on staff members and contractors, etc.
・ Number of cases: 233
・ Details: ID numbers, personal names, account names, e-mail addresses
・ Applicable persons:
① Staff members who belong to Keio University and hold an SFC-CNS account (including those in other campuses)
② Contractors, etc., who hold an SFC-CNS account

*The possibility of other personal information existing on SFC-CNS and SFC-SFS having been leaked cannot be completely denied.

b. How the leak was discovered

Suspicious access to SFC-CNS was detected at approximately 5:45 p.m. on September 15, and an investigation of the details revealed evidence that SFC-SFS had been sporadically explored for vulnerabilities. Suspicious access to SFC-SFS was further detected on the night of September 28, and an investigation of the details on SFC-SFS, revealed the possibility of an information leak due to unauthorized access to SFC-SFS before dawn on September 29.

c. Cause of information leak

Based on our investigations to date, we believe that the main causes of the incident were the theft of user IDs and passwords for SFC-CNS accounts by some means, which were then used to break into the system, and the exploitation of a vulnerability that existed in the web service of the SFC-SFS system.

d. Response after detection of leak

The following measures have been taken after the discovery of the unauthorized access (some of the measures are continuing to be implemented):
・ All users requested to change their passwords (on September 16 and 30)
・ Continuous monitoring of all authentication points and logs (continued from September 16)
・ Log in to shared calculation server (GPGPU) from off-campus limited to public key authentication only (September 16)
・ Suspension of web services confirmed to be vulnerable and enhancement of vulnerable parts [under implementation] (from September 16 onward in sequential order; SFC-SFS has been suspended since September 29)

・ Due to the system suspension of SFC-SFS, the Faculty of Policy Management, Faculty of Environment and Information Studies, and Graduate School of Media and Governance postponed the start of the classes in the Fall Semester to one week later than the initial date, namely from October 1 to October 8.

e. Current situation

The route of the leak of SFC-CNS account IDs and passwords continues to be investigated. No specific leaks have been confirmed on the SFC-CNS system to date, and for as long as all authentication points and logs in the system have been continuously monitored, no suspicious access has been confirmed since.

Furthermore, SFC-SFS has been suspended since 10:30 p.m. on September 29 until now.

f. Measures to prevent reoccurrence

In light of this incident of unauthorized access, Keio University is urgently taking measures to prevent reoccurrence, including security checks and improvements of web applications and systems, and it will review the handling of data to protect personal information. In addition, a Computer Security Incident Response Team (CSIRT) will be set up within the university on November 1, 2020, to create an organization that can comprehensively respond to cyber security, while we will also cooperate with external specialist institutions in an effort to further strengthen security across the university.

Once again, we deeply apologize for all the trouble and distress caused by this situation. Although no secondary damage has been confirmed at this time, please get in contact using the following details if you have any questions.

(Inquiries about this matter)
Shonan Fujisawa Office Inquiry desk regarding unauthorized access
E-mail: fusei-access2020@sfc.keio.ac.jp

End of document