研究室用 Web サーバにおける不正アクセスについて

2019 年 10 月 28 日

この度、東京女子大学の研究室用 Web サーバ* において、研究者 5 名のユーザアカウントに対して不正アクセスがあり、当該アカウントから不正にファイルがアップロードされる事案が発生いたしました。

関係者の皆様にご迷惑、ご心配をおかけする事態を招いたことを深くお詫び申し上げます。

これまでに判明しました不正アクセスの詳細について、以下のとおりご報告いたします。

引き続き、必要な対応をとるとともに、全学で再発防止に取り組みます。

*東京女子大学の公式サイト（http://www.twcu.ac.jp）とは異なるサーバです。

1. 経緯

2019 年 7 月 23 日夕刻、研究室用 Web サーバ更新準備作業中に、不正アクセスを発見し、不正なファイルを 2016 年 6 月ごろからアップロードされていることが判明しました。
速やかに該当ユーザのパスワードを変更し、公開中のファイルにアクセスできないよう措置するとともに、サーバ上で実行できないよう機能を停止しました。

同時に、他のユーザについてパスワード漏洩ならびに不正アクセスの状況、上記以外のサーバ上で実行可能なプログラムについて調査し、被害状況の把握を進めてまいりました。
現在、不正アクセスのあったユーザのパスワードは、すべて変更が完了しました。
また、上記以外にサーバ上で実行可能なプログラムがなかったことを確認しました。
現在のところ、東京女子大学（以下、「本学」）以外での被害の発生は確認されておりません。

今回の件は、研究者が学外のシステムで使用していたパスワードが、不正に使用されていた可能性が高いと考えております。

2. 不正アクセスの件数

5 ユーザに対して計 52 ファイルがアップロードされていました。

3. 不正なファイルの内容

・特定の条件可で、サーバ上で動作する PHP バージョンを表示する。

・特定の条件可で、メール送信を行う。

4. 本件に関するお問い合わせ先

東京女子大学　情報処理センター

メールアドレス　cis-risk@cis.twcu.ac.jp

5. 再発防止に向けた対応

本学では、このたびの事態を厳粛に受け止め、研究室ネットワーク運営委員会ならびに情報処理センターが連携し、再発防止の強化を図ります。

すでに、全研究室用ネットワーク利用者へパスワードの適切な管理についての注意喚起を行いました。今後は、Web アプリケーションファイアーウォールの導入も検討しております。

以上