TCU ストレージにおける学外向けファイル公開機能の利用ガイドライン

2021 年 11 月
情報基盤センター

1．概要

2018 年度に導入された TCU ストレージには、TCU ストレージ上のファイルにアクセスできる URL を発行し､TCU アカウントを所有しないユーザーに対してファイルを公開する機能(以降､「学外向けファイル公開機能」と呼称）が備わっている。
この機能については、オペレーションミスや不正アクセスによって本来意図しない情報の公開を招く可能性も有るため、一定以上の機密性を有するファイルの公開について制限を設けるガイドラインを定める。

2．当ガイドラインの対象

当ガイドラインは学外向けファイル公開機能のみを対象とし、他の機能（一般的なファイル保存機能・グループによるファイル共有機能）は対象としない。学外向けファイル公開機能以外の機能については、「東京都市大学の情報システムに関する情報セキュリティポリシー」（https://www.itc.tcu.ac.jp/iss/）に則って、利用すること。

3．標準的な公開の場合

本学情報システムにおいては、一般的に公開されているセキュリティポリシーや他大学での情報システム利用ポリシーを参考に情報の機密性を 1～5 の 5 段階に評価する（別紙 1. 機密性の評価 参照)。学外向けファイル公開機能は、TCU アカウントを持たないユーザーでもアクセス可能な URL を発行する機能であるが、URL の発行にあたって一定の複雑さを持ったパスワード※を付加することが必須となっている。これにより、不正アクセスに対する必要最低限の対策がされている判断し、機密性３（公開を前提としていないもの）までのファイルを公開可能とする。
※半角大文字、半角小文字、数字または記号を３種類以上混在させた 8 文字以上の文字列をパスワードとして指定しないと、公開ができないようになっている。

4．機密４以上のファイルの公開について

機密性４（特定の職制, グループ又は部局等以外に対して機密を保持 すべきもの)、機密性５（特定の関係者以外に対し厳重に機密を保持すべきもの）のファイルについては、一般的に、パスワ

ードでのアクセス制限に加えて、追加のセキュリティ対策（追加の認証要素やネットワーク的な制限）を設けるべきであるとされている為、原則として学外向けファイル公開機能を用いて公開できないものとする。 ただし、ファイルそのものに TCU ストレージで使用した物とは異なるパスワードによる保護※を施した場合、追加の認証要素が付加されたと判断し、機密性 4 のファイルについても公開できるものとする。

※パスワード保護について

- 一旦、ファイルがダウンロードされてしまうとパスワード解析ツール等による解析が可能となるため、TCU ストレージのものと同様か、あるいはそれ以上の複雑性を持った類推されにくい文字列を用いること。
- ファイルそのものにかけたパスワードを伝達する場合、TCU ストレージのパスワードとは異なる伝達手段を用いること（TCU ストレージのパスワードをメールで伝えた場合、ファイルのパスワードは口頭で伝達する、あるいはファイルのパスワードをあらかじめ申し合わせておき、それを用いる等）。
- Microsoft Office2013、ならびにそれ以前のバージョンのパスワード保護は容易に解除できるため用いないこと。
- パスワード付き ZIP の場合、パスワードが分からなくても格納しているファイルの名称名までは確認ができるため、内容が容易に推測できるようなファイル名は避けるべきである。
- できればパスワード付き ZIP ではなく、格納するデータの暗号化を行うソフトウェア（参考：別紙 2.無償で利用可能な暗号化ソフトウェア）を用いて保護することが望ましい。

５．強制的な措置

当ガイドラインに反して、学外向けファイル公開機能にてファイルが公開されている状況が確認され、それにより、本学の利益や本学の情報セキュリティが著しく損なわれると判断された場合、情報基盤センターにて TCU ストレージにおけるファイルの公開を強制的に停止することがある。

以上

当ガイドラインは広島大学クラウドサービス利用ガイドラインならびに広島大学クラウドサービス利用ガイドラインチェックリスト（©広島大学 情報セキュリティ推進機構）を一部参考に作成している
http://www.media.hiroshima-u.ac.jp/news/cloudguide