本学教職員各位

ご利用情報端末でのセキュリティ対策のお願い

2022 年 3 月　情報システム課

情報・データ等は常に狙われています。コンピュータウィルス対策だけではなく、以下をご一読いただき、各自、教育・研究・業務で使用する PC 等について万全のセキュリティ対策をお願いいたします。

◆各ソフトウェアのアップデート

脆弱性対策として、Web ブラウザや電子メールソフト、OS、Office アプリケーション等の定期的なアップデート（修正プログラムの適用）をお願いいたします。

◆標的型攻撃メール、フィッシングメール

見慣れた件名やあて先、内容を真似て、受信側を騙そうとするメールにご注意ください。情報を盗み出すウイルスに感染し、機密情報が漏洩する事態に陥ることもあります。そのようなメールが届いても安易に添付されたファイルを開いたり、本文中のリンクをクリックしたりしないようお願いいたします。

また、ID やパスワード、カード番号を入力させようとするフィッシングメールにもご注意ください。

◆偽メッセージ

突然、ご利用端末の画面上に「危険です。至急連絡をください」といったメッセージが表示された場合、それは偽メッセージの可能性が高いです。安易に記載された電話番号に電話をしないようお願いいたします。遠隔操作をされてご利用端末の情報を抜き取られたり、その後、脅迫してくる場合もあります。

※例。Microsoft では電話番号を記載したメッセージを端末上に表示させることはありません。

◆メールの誤送信

メールを送信する際、宛先指定で「BCC」にするべきところを誤って「TO」や「CC」に指定して送信しまったために情報漏えいが起こるケースがあります。（ニュースでもよく取り上げられています）

送信前に、宛先のメールアドレスと送信欄（TO、CC、BCC）が自分の意図した通りになっているか、確認をしてから送信するようにしてください。

◆パスワード管理について

現在のパスワードが短い（8 文字以下）場合、また、類推されやすい文字列の場合、パスワードを変更するようお願いいたします。情報システム課ページより変更が可能です。

https://www.tku.ac.jp/iss/password.html

※本学ユーザ ID、TKU メール（Google Workspace）のパスワードが変更されます。

※変更後パスワードの法則は「12 文字以上、英大文字、小文字、数字が混在していること」です。

◆持ち運び可能な記憶媒体の管理（USB メモリ、外付けハードディスク等）

ファイルを保存する場合は、その記憶媒体への暗号化やパスワード保護等、情報漏えいを防止する対策をとるようお願いいたします。また、盗難や紛失には細心の注意を払うようお願いいたします。

なお、個人情報が記録された機器の盗難、紛失時、また情報漏えいの可能性がある場合は、速やかに大学へ連絡をお願いいたします。

※参考。「情報セキュリティ（IPA より）」https://www.ipa.go.jp/security/

以上