事　務　連　絡
平成２９年８月３日

各　　位

本部情報戦略課

夏季休暇中における情報セキュリティに関する注意喚起について
Attention on security during summer vacation

夏季休暇期間中及び期間後は、情報セキュリティ事案が多数発生します。
ついては、以下に利用者向けの注意事項を掲載いたしますので、遵守いただきますよう、よろしくお願いいたします。

最近、東京大学を発信元とする迷惑メールが度々発生しています。原因の一つは、アカウントが盗用されて迷惑メールの発信に悪用されるというケースです。パスワードが漏洩してしたために、アカウントを悪用されて当人の意図しない迷惑メールが多数送信されるものです。
こういった事案の発生を防ぐために、自分のアカウント管理について今一度見直しをして下さい。(休暇起案前の対応(3)、(4))

また、従前からお知らせしておりますが、標的型攻撃メールによるフィッシング行為やランサムウェア感染が増えております。学会の案内、料金請求、アカウント情報の更新などを装って、ID・パスワードの入手や、ランサムウェアへの感染を目的とした標的型攻撃メールが送られてくることがあります。このようなメールは、送信元メールアドレス、タイトル、本文、添付ファイル名などをチェックすると何らかの不自然な点がありますので、不用意に添付ファイルを開いたり、URL をクリックしたりしないようご注意下さい。((休暇期間後の対応) (4)、(5))
万一フィッシングサイトにパスワード等を入力してしまった場合や、添付ファイルを開いてしまった場合には、速やかに部局 CERT に連絡し、被害の拡大を防ぐようにして下さい。((休暇期間後の対応) (6))

【利用者向け　注意喚起事項】

(休暇期間前の対応)

(1) 情報セキュリティインシデント発生時における報告・連絡・相談先を確認して下さい。
(2) 使用しているパソコンやサーバのOS やアプリケーションソフトウェア等に最新のセキュリティ更新プログラムが適用されていることを確認して下さい。
(3) 容易に推測できる文字列（名前、生年月日、電話番号及びアカウントと同一の文字列等）や安易な文字列（12345、asdfg 及びqwerty 等）をパスワードに設定していないことを確認して下さい。
(4) IDやパスワードを他のサービスでも使い回していないか確認して下さい。もし併用している場合は前項(3)を踏まえ、パスワードの変更を行うようにして下さい。

(5) パソコンやUSBメモリ等の外部記録媒体の持ち出し・持ち込みについては、所属部局で適正な手続き（特に持ち出しに関する規程がある場合はこれを遵守）を行い、適切に管理して下さい。また、不要な情報は持ち出さないようにし、媒体に保存する情報は必要最小限にして下さい。
(6) 自身が使用するウイルス対策ソフトに最新のパターンファイルを適用してフルスキャンを行うようにして下さい。
(7) 休暇期間中に利用しないパソコンやプリンタ、ネットワークストレージ等は電源を切るようにして下さい。

（休暇期間中の対応）
(1) パソコンやUSBメモリ等の外部記録媒体による情報の不要な持ち運びは避け、必要に迫られ持ち運ぶ場合には、盗難や置き引き、紛失等に十分注意願います。

（休暇期間後の対応）
(1) 休暇明け直ちにウイルス対策ソフトを最新のパターンファイルに更新してフルスキャンを行って下さい。
(2) 休暇中にセキュリティ更新プログラムが公開されていた場合は（部局情報セキュリティ責任者の指示に従って）休暇明け速やかに更新プログラムを適用して下さい。
(3) 適正な手続きを経て休暇中に持ち出したパソコンやUSBメモリ等の外部記録媒体については、使用する前に必ずウイルス対策ソフトでフルスキャンを行ってから使用して下さい。
(4) 休暇中に受信したメールには、ウイルス付きメールや標的型攻撃メールが含まれている可能性があるので、添付ファイルは安易に開封しないようにして下さい。
(5) 覚えのない差出人（メールアドレス）など、少しでも不審を抱いたメールに記載されたURLリンクはクリックしないようにして下さい。（※差出人は、実在の人物を騙る場合もあります。）
(6) 万が一不審な電子メールの添付ファイルを開封した場合や、URLリンクをクリックした場合には、直ちにパソコンをネットワークから切断し、電源は切らずに部局CERTへ連絡を行って下さい。
(7) 業者や関係者、システム管理者等を装って利用者のパスワードや個人情報等を聞き出そうとする問合せ等が発生する可能性があるため、未確認の相手に不用意に情報を伝達しないで下さい。

※UTokyo-CERTが発行しているセキュリティ対策ガイドラインもご参照下さい。
（英文版もあります。）
2017年7月号
https://cert.u-tokyo.ac.jp/news/monthly/guideline-201707.html （日本語）
https://cert.u-tokyo.ac.jp/e/news/monthly/guideline-201707.html （English）

本件担当：本部情報戦略課セキュリティ対策チーム
内線：２２１８０、２２７０２
E-mail：jouhousecurity.adm@gs.mail.u-tokyo.ac.jp