事　務　連　絡
平成30年4月25日

各　　位

本部情報戦略課

春の大型連休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 long vacation

春の大型連休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しますので、遵守いただきますようよろしくお願いします。

従前からお知らせしておりますが、東京大学を発信元とする迷惑メールが度々発生しております。このうち、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が相当数発生しています。パスワードが漏洩してしまったために、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てしまったという事案です。
このような事案の発生を防ぐために、ご自身のアカウント管理について今一度見直しをしてください。（休暇期間前の対応(3)、(4)）

また、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引き続き報告されています。
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付され、そのメールに添付されたファイルを実行すると学外から実行形式のファイルをダウンロードして感染するものが増えています。また、フィッシングメールに記載されているURLにアクセスし、IDやパスワードを入力してしまう事案も報告されています。
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ください。（(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ください。（(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・相談先を確認してください。夜間、休日の対応についても、必要に応じて確認してください。
(2) 使用しているパソコン、スマートフォン及びサーバのOS や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ください。
(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ください。
(4) IDやパスワードを他のウェブサービスで使い回していないか確認してください。

もし併用している場合は(3)を踏まえ、パスワードを変更してください。

(5) パソコンやUSBメモリ等の外部記録媒体等の持ち出し・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、適切に管理してください。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ください。

(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ください。

(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ください。

（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は、盗難や置き引き、紛失等に十分注意してください。

（休暇期間後の対応）

(1) 休暇明けの出勤後、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ください。

(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ください。

(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等については、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た後に使用してください。不要なデータについては、速やかに削除してください。

(4) 休暇中に受信したメールの中には、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ため、添付ファイルは安易に開封しないようにしてください。

(5) 覚えのない差出人（メールアドレス）等、少しでも不審を抱いたメールの本文に記載されたURLのリンクはクリックしないようにしてください。（※差出人は、実在の人物を騙る場合もあります。）

(6) 万が一不審なメールの添付ファイルを開封したり、URLのリンクをクリックした場合や、パソコンのファイルが意図せず暗号化されている等、平常時と異なる状態にあることを確認した場合、直ちに端末をネットワークから切断し、電源は切らずに部局CERTへ連絡をしてください。

(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ください。

※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ください。

2018年3月号

https://cert.u-tokyo.ac.jp/news/monthly/guideline-201803.html （日本語）

https://cert.u-tokyo.ac.jp/e/news/monthly/guideline-201803.html （English）

2017年12月号

https://cert.u-tokyo.ac.jp/news/monthly/guideline-201712.html （日本語）

https://cert.u-tokyo.ac.jp/e/news/monthly/guideline-201712.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