ICT　第 10329 号
令和元年 11 月 28 日

本学電子メール・ネットワーク利用者各位

八景キャンパス 企画総務部
ICT 推進課長

【重要】 不審なメールにくれぐれもご注意ください（通知；注意喚起）

標記の件については従前より、利用者の皆さんにご注意いただくようお願いしていますが、昨今、いわゆる標的型攻撃メールの新たな手段として「添付ファイル付きの知人や関係者を装ったメール」による被害の急増が報じられています。

日本のセキュリティ対策機関である JPCERT コーディネーションセンターは、11 月 27 日、国内で 400 以上の組織が新種のウィルス（emotet）に感染し、拡大が続いているとの見方を明らかにしました。以下をご参照のうえ、感染防止に努めていただくよう、改めてお願いします。

１．今回のウィルス（emotet）の特徴

実在の組織や人物になりすましたメールに添付された Word 文書等ファイルに、そのパソコンの脆弱性を突くウィルス（悪質なプログラム）が仕込まれています。

この添付ファイルをメール受信者に開かせるため、**感染した端末から窃取された情報などを基に、過去のメールの送受信の相手方になりすまし、件名も「Re：」で始まる過去のやり取りを装うなど、巧妙な手段が用いられているのが大きな特徴**です。

２．ウィルス感染の影響

送信元の方の名前や、件名などだけでは一見区別が出来ない可能性が高いのは事実ですが、知人からのメールと誤解して安易に添付ファイルを開くと、このウィルスに感染する恐れがあります。

感染した場合、パソコン内の情報漏洩の恐れがあるほか、以下のような影響があります。

（１）端末や Web ブラウザに保存された、ID・パスワードなどの認証情報が窃取される。
（２）メールアカウントとパスワード、メール本文やアドレス帳などの情報が窃取される。
（３）窃取された情報が悪用され、その端末から感染を広げるメールがさらに発信される。

３．利用者の皆さんに行っていただきたい対策

別紙でご用意する「不審メールの見分け方とその対策」をご参照のうえ、Microsoft Office がインストールされている端末では事前にセキュリティ設定を確認するとともに、送信元が信頼できる場合を除き、**安易・習慣的に電子メールの添付ファイルを（ダブルクリックするなどで）開く行為だけは絶対にしないようご注意**ください。

また、不審なメールと気づかずメールそのものを誤って開いてしまった場合であっても、添付ファイルを開いていなければ被害に遭わずに済む場合もあります。不安な場合は、以下の担当までご連絡のうえ、その指示にしたがってください。

４．各所属長はじめ管理職の皆さんへのお願い

昨年のフィッシングメールによる情報流出、以前から起きている個人情報漏洩など、本学で起きたこれらの不祥事と同様の影響を生じさせないためにも、各所属・職場において、上記の注意喚起、周知・徹底を改めてよろしくお願いいたします。

※添付：別紙「不審メールの見分け方とその対策」
※参考：JPCERT の注意喚起：https://www.jpcert.or.jp/at/2019/at190044.html

【担当：お問合せ等】
八景キャンパス　ICT 推進課 ICT 推進担当
電話 045-787-2340/2341/2356
電子メール：center@yokohama-cu.ac.jp