平成 30 年 6 月 13 日

教職員各位

情報基盤センター

他大学の「なりすましメール被害事例」に伴う注意喚起

○ 某公立大学にて 6 月上旬、同大の教職員などに「Microsoft Office 365 メール管理者を騙る、なりすましメール」が届き、メールに記載された URL にアクセスして ID・パスワードを入力してしまった教職員（メールアドレス：29 件）に届いたメール 3,512 通が、不正に外部転送されていた事案が発生しました。

○ 不正に転送されていたメールには、差出人の氏名やメールアドレスなどの個人情報 計 5,794 件が含まれていたとのことです。

○ 本学も Office 365 を利用しており、本事案と同様な「なりすましメール」が今後届く場合もあることから、警戒が必要です。

○ 個人情報の入力を求めるメールの多くは不正メールです。先般から注意喚起している通り、楽天、Apple、Amazon などの企業を騙り、個人情報を窃取しようとする不正メールが横行しています。身に覚えのない内容で個人情報の入力を求めるメールのリンク先にはアクセスしないとともに、不用意に個人情報を入力しないようお願いいたします。

○ 万が一、同様なメールを受信した場合や、メール内容の真偽確認が難しい場合は、情報基盤センター（内 2289、center@fit.ac.jp）までご連絡ください。

本事案の手口
① Microsoft Office 365 メール管理者を装った不正な「なりすまし」メールが届く。 《届いたメール内容》 差出人：メール管理　Mail Delivery System <MAILER-DAEMON@messagelabs.com> 本文：以下のとおり Your Messages Has Not Been Sent Dear ***** @大学ドメイン（実際の利用者アドレス） We coherently encountered outgoing server failure …　（略）… >>Click here << to resend these mails.　…　（略）…, The Office365 team 《偽メールの主旨：和訳》 「送信サーバの障害によりメールを送信できませんでした。再送信する場合は、以下をクリックしてください。　Office365 チーム」と言うもの。 ※今回は、英文メッセージだったため、多くの利用者は迷惑メールと思い、そのまま削除された可能性もある。これが和文だった場合、さらに多くの被害が発生した可能性もある。今後、和文で配信される場合もあるため警戒が必要。
② クリック先 URL は Office 365 の公式ログインページを精巧に模した内容になっており、ID・パスワードを入力してしまうと、それら情報が窃取される。
③ その後、不正ログインされ、メール転送先に外部アドレス（gmail 等）が設定される。
④ 知らぬ間に、全ての受信メールが外部にコピー転送され、個人情報を窃取される。

以上