FDガイド第17号

知ってて、やってて、伝えてますか?

～いまどき教職員に必要な“リテラシー”としてのセキュリティ対応～

鹿児島大学 FD 委員会 FD ガイド WG

【発行／2019年3月】

釈迦に説法の域ですが、情報収集やメールのやりとり、クラウド・サービスの利用はもちろん、本学ではmanabaが導入されその利用の普及が進むなど、インターネットの利用は教育活動のインフラであり、不可欠な存在になっています。とはいえ、インターネットの活用には様々なリスクがあることも常識。教職員それぞれにセキュリティについての意識を持って、リスク対応をしていると思います。

しかし、知的情報の発展・展開を担う研究機関として、また大学という教育機関のメンバーとして、自分のことだけではなく、学生やその家族、取引先を含めたステイクホルダーに、こうしたリスク対応の必要性や対応の仕方を「伝えていくこと」も、重要なミッションです。教員であれば、自分ができるだけではなく、少なくとも研究室やゼミに所属する学生、授業の受講学生に注意を促すことができることも、いまどきの大学の教職員に必要なリテラシーなのです。

今回のFDガイドでは、こうした観点から教職員が、知ってて、やってて、「伝えなければならない」ことがらを、学術情報基盤センターのサイバー・セキュリティ戦略室の佐藤豊彦特任教授のお話を参考にまとめてみました。

伝えるべきことは3つ!

1　危険なリンクやファイルを開いてしまったらすぐ通報
2　パスワード作成の工夫で使い回しをやめる。
3　大学が許可する仕様のPCや機器をつかう。

1　危険なリンクやファイルを開いてしまったらすぐ「通報」

メールに書かれているリンクや添付ファイルを安易に開かないことは、ほとんどの教職員に知られていて、あたりまえに実践されていることと思います。

しかし、先日の「迷惑メール対応訓練」では、リンクをクリックしてしまったり、ファイルを開いてしまう人が、例外とは言えない程度いたのも事実です。さらに、必要な報告をすぐしないケースも見受けられます。

こうしたメールで使われる、ソーシャル・エンジニアリングと言われる人の心に入り込んでクリックを促す技術は、一見ちんぷで頭でわかっていても、ちょっとした状況にはまると誰でも引っかかる可能性があります。佐藤特任教授によると、「やってしまうことは誰でもあり得ることなので、恥ずかしがらず、自分の対処能力を過信せずに、速やかな通報をして欲しい」とのこと。原因の特定や対処方法が複雑な場合もあるので、問題を拡大させないためにも「通報のスピード」を重視して欲しいと言うことです。

この点、研究室やゼミの学生に使わせていたり、持ち込ませたPCで起こしたトラブルでは、通報についての意図が十分伝わっておらず、学生によってもみ消されていたり、適切な手当がなされず、被害を拡大させていることもあります。教職員として予防の実践や教育は当然として、授業を含めて指導する機会のある学生に、トラブルになったらすぐ通報することを伝える必要があります。

さらに、佐藤特任教授によれば、トラブルの原因の特定に必要なので、「万が一、**引っかかったときには、ネットワークから切断して、電源を切らないまま通報**して欲しい」ということです。

2　パスワード作成の工夫で使い回ししない

同じパスワードの使い回しをしないと言うことは、耳にたこができるほど繰り返し伝えられているところです。しかし、必ずしも十分に実践されているとは言えません。

現在、利用しなければならないがパスワードを必要とするサービスはひとつやふたつではなく、そもそも、そうしたサービスをいくつ利用しているかを覚えている人の方が珍しいのではないでしょうか。その上、パスワードの長さは安全性と相関していて、いくつかの説がありますが、現在では英数大文字小文字に記号を含めた10文字以上が推奨されています。

たくさんのサービスそれぞれに異なる複雑な10文字以上のパスワードを、すべて記憶することは不可能です。ID/PWの備忘リストを、さらにID/PW付きで暗号化したファイルで保存しておくこともできるかもしれませんが、ど忘れしたときにいちいちそれを開くのも、実際的ではありません。その上、パスワードを忘れてしまいそのサービスが利用できないと、研究も教育も学務もできないことなりかねないほど、インターネット上のサービスに依存しているのが現代社会です。

そうなると、パスワードの使い回しはやむを得ないと思いがち。それも、推測されやすいパスワードを使っても自分は大丈夫だろうと思うことに強い誘惑が生まれます。

こうした誘惑に抗するには、**パスワードそのものを決めるのではなく、様々なパスワードを作る規則性（アルゴリズム）を決めておくことが有効**です。

たとえば、佐藤特任教授がひとつの方法として紹介しているのは「６文字程度の他の人にはわからないコア・キーワードを用意して、その前後に利用するサービスから思い出せる数文字ずつを加えて10文字以上にする方法」でした。すると、覚えておくのは6文字分だけ、あとは、利用するサービスから抜き出す規則を決めておけば、それを加えて登録することで、サービスごとに異なるパスワードを利用することができます。

知ってて、やってて、伝えてますか?

そのまま真似をしないことを前提に具体的に紹介すると、たとえばmanabaを使う場合、コア・キーワードを例えばSattsunと決め英数記号を含めS@2tsunとすると、manabaを冒頭2文字とその他のふたつに割って、冒頭は大文字でMa、S@2tsunは頭の桜島の爆発で!!とつけることとして、のこりのnabaを加えて、MaS@2tsun!!nabaとする。Googleであれば、GoS@2tsun!!ogleとなります。コア・キーワードは自由ですし、文字数の割り方や選び方について自分なりの「規則性」を決めれば、かなり長くても忘れないパスワードをたくさん作ることができます。

共同研究やアクティブ・ラーニング、プロジェクト・ラーニングを進める際には、教員はもちろん、学生も、他人の個人情報を外部のクラウド・サービスなどに保存して共有し、活用することで学習効率や作業効率を高める必要があります。学生にとっては、そうしたサービスを利用することは、将来に向けて身につけるべきリテラシーでもあります。教員として学生にそれらのサービスの利用を進めたり、事実上強制することも少なくないはずです。

その際に、パスワードの使い回しをヤメなさいと言うことだけではなく、こうしたティップスを合わせて伝えることで、実効性を確保したいところです。

3　大学が許可する仕様のPCや周辺機器を使わせる

まず、現在、個々人や研究室で利用しているＰＣやタブレット、スマートフォンについては、ＯＳや使用しているアプリケーションを最新版にしておくことや、ウィルス対策ソフトを導入しパターン・ファイルを随時更新することは、みなさん実践されていると思います。現在では、そもそも機器の方で、デフォルトで自動的に対応するケースが通常といってよいでしょう。

とはいえ、現在のMicrosoftの最新OSはWindows10ですが、まだ、Windows７を利用している方や学生がたくさんいます。しかし、すでに広く知られているとおり、Windows7は2020 年 1 月 14 日 に延長されていたサポート期間も終了することになっており、学内での使用が禁止される予定です。つまり、それまでにあと１年を切っているという状況です。そのため、**Windows７を利用している教職員や学生のみなさんには、計画的にご自身のPC本体の更新やWindows10へのアップグレード作業を進めていただかねばなりません。**

Windows7登場当初に同時にMS-Officeを導入した場合には、Office2010である可能性があります。こちらは2020 年 10 月 13 日に延長サポートが終了します。Windows10であればOffice2013の可能性が高いのですが、Office10を改めてインストールしている場合は問題が生じます。これも学内で使用禁止になりますので注意が必要です。

PCを利用しての共同作業を課す先生方は当然ですが、通常の授業でmanabaを使ったり、メールでレポートの提出を課すことはPCを使うことを前提としたことである以上、このことを学生に告知して、サポート終了までに確実に大学が許可する仕様にするよう指導する必要があります。

また、見落としやすいのは、研究室内や各自の自宅で使う無線ＬＡＮのアクセスポイント、ネットワーク・ハードディスク（NAS）やネットワーク・プリンタのファームウェアといわれる内蔵プログラムを最新版にすることです。比較的最近の機材であれば、更新の通知が自動的に表示されますが、そういう機能を持たない機器もたくさん利用されています。

これらの対応も先生方が研究室で実践される際に、学生にもお伝えいただくと、研究室やゼミのメンバーのセキュリティ・リスクを小さくすることができます。

鹿児島大学のネットワーク全体を管理している学術情報基盤センターでは、外部からの危険なアクセスを遮断するとともに、迷惑メールや危険なメールを遮断する装置を導入しています。しかし、これらの対応は機械の自動的な判断に基づいた対処に依存せざるを得ず、これらをすり抜けるアプローチが絶えません。最後の砦は学内でPCを利用する教職員と学生などのみなさんです。しかし、ここでも完全な予防は難しいのも事実です。佐藤特任教授によると、「教職員、学生が上記の3つを着実に実施していただければ、事故の確率は非常に小さくなりますし、万が一事故になっても、みなさんの責任は限られた小さなものになると言える」とのことです。

これまで、PCなどのセキュリティの教育は個々の教員が担うものではないと考えられがちでしたが、この時代、そうも言えないところまで大学教育がネットワークに依存する時代になりました。教職員自身のためだけではなく、教員として学生に伝える必要をご理解いただき、この3つを「伝えることがあたりまえ」の環境作りによって、大学全体のセキュリティ・リスクを下げ、みんなで安心してネットを使える環境を確保しましょう。

【紹　介】

ネットワーク使用のリスク対応についての非常にわかりやすい解説書として、下記のふたつがあり、佐藤特任教授も推奨されています。ネット経由で無料で入手できますので、是非入手してご自身や学生などのセキュリティ対応に役立てていただければと思います。

■内閣情報セキュリティーセンター『インターネットの安全・安心ハンドブック Ver.4.00（平成 31 年 1 月 18 日）』
https://www.nisc.go.jp/security-site/handbook/index.html
■（株）LAC『情報リテラシー啓発のための羅針盤』
https://www.lac.co.jp/corporate/pdf/compass.pdf
（株）LAC『情報リテラシー啓発のための羅針盤 参考スライド集』
https://www.lac.co.jp/corporate/pdf/compass_slide.pdf

ハンドブック

LAC羅針盤

【鹿児島大学FD委員会FDガイドWG】

米田　憲市（法文学部）　木下　英二（工学部）
帆保　誠二（共同獣医学部）　渡邊　弘（共通教育センター）　出口　英樹（高等教育研究開発センター）