巻　頭　言

情報セキュリティの意識向上に向けた課題

医学部附属病院長　福田眞作

昨年，本学職員を狙ったフィッシングメールによって，個人情報漏洩（疑）事案が発生しました。私個人にもそのメールが何度か配信されており，とても巧妙なものでした。不覚にも何度目かに ID，PW を入力してしまいましたが，偶然にも入力直後に総合情報処理センターからのフィッシングメールを警告するメールを受信し，即座に PW を変更しましたので被害を防ぐことができました。立場上，情報セキュリティの意識は高いつもりでおりましたので，とても恥ずかしくもあり，ショックを受けました。フィッシングメールに騙された病院長・・ということで，私にこの原稿依頼があったのだろうと憶測しています。

企業や組織にとって，情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつです。本学でも様々な情報セキュリティ対策がとられてきましたが，今回の事案発生によって，残念ながら本学の情報管理体制がまだ不十分であることを認めざるを得ません。もし患者さんの個人情報の漏洩が発生した場合には，附属病院のイメージの失墜につながるだけでなく，賠償や訴訟などの大きな問題にまで発展することが少なくありません。

情報システムやインターネットの普及によって，記録や通信の利便性は飛躍的に向上しました。それと比例して，情報漏洩のリスクも高まっていることを私たちは忘れてはなりません。ますます手口が巧妙化する中で，如何にその利便性を損なうことなく，リスクを回避することができるのか？　本学では高額な費用負担覚悟で，Office 365 のセキュリティを強化することが検討されていますが，まずは情報セキュリティへの意識の向上が不可欠であると，騙されてみて実感しております。

本学が推奨している「Office 365 多要素認証」の設定率も職員全体の 60％程度（平成 30 年 12 月時点）と聞いています。今回の事案を紹介し，「Office 365 多要素認証の設定」を職員（とくに医師）に呼びかけていて気づいたことがあります。ほとんどの職員が，コンピューター用語をあまり理解していないように思います。PC を購入したときのことを思い出してみてください。業者さんの設定で，即座にメールができて，ワードやエクセルも使えるようになります。説明書なんか読む方は少ないのではないでしょうか。最近では説明書の同封すらありません。もちろん情報セキュリティに関する説明はほとんどありませんし，職員が情報セキュリティについて自学学習するとは到底思えません。総合情報処理センターの職員（プロ）が，情報セキュリティについて一生懸命に解説したとしても，ホームページ上で様々な情報を公開したとしても，実は前提となるコンピューター用語の意味を理解できていない（しない）職員がほとんどであるという認識に立って，セキュリティ教育を考える必要があります。「ボーっと生きてんじゃねーよ！（by チコ）」と言いたい気持ちを抑えて，粘り強い広報活動を是非とも一緒に行っていただきたいと思います。