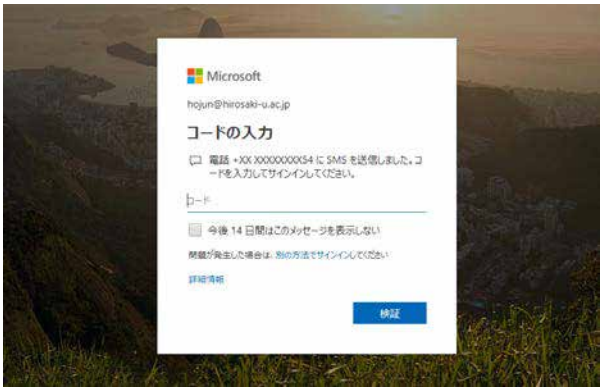
多要素認証とフィッシングメール

理工学研究科　任 皓駿
hojun@hirosaki-u.ac.jp

1 はじめに

本記事では，最近，本学でネットワークのセキュリティの強化のため始まった多要素認証とフィッシングメールについて一人のユーザーとしての意見を述べてみたいと思います。

2 多要素認証を利用して



図：携帯番号の SMS を用いて多要素認証した際のログイン画面

多要素認証は 2 種類以上の要素（知る要素，持つ要素，備える要素）[1]を用いてログインの認証を行うことですが，個人的にはウェブ上でのクレジットカードの決済以外ではあまり経験がありませんでした。昨年 11 月ごろ，本学で多要素認証の設定を始めたとき，率直にいえば馴染みのない方法で少し戸惑いました。最初，認証方法として研究室の電話番号を登録し，帰宅後，弘大メールに接続しようとすると追加認証の画面が現れ，進むことが出来なかった覚えがあります。次の日，認証方法を研究室の電話番号から自分の携帯電話番号の SMS に変更することで解決が出来ました。一方，使って行くに連れて，セキュリティがしっかりしている安心感を持つようになりました。弘大メール（Office 365）では，上記の 2 種類の方法以外でも専用のアプリケーションを利用した認証方法もあり，個人の状況に合わせて設定が出来て大変助かると思います。しかし，上記に述べた多要素認証の優れた機能にも関わらず，フィッシングメールは各職員宛に直接に来るので，被害に巻き込まれる可能性は相変わらず残っています。例えば，リンク先をクリックして思わぬ接続をしたり，個人情報などを入力したりする恐れがあります。特に，本学の機関名や職員名に成り済ましたメールは注意が必要です。不審なメールを受信した際には，弘前大学 CSIRT（csirt@ml.hirosaki-u.ac.jp）に積極的に報告するなど，各職員が高いセキュリティ認識を持つことが何より大事だと思います。

3 おわりに

短い文書ですが，最近始まった多要素認証の経験談とフィッシングメールの対策についての意見を述べました。多要素認証は一手間掛かることで少し面倒なところはありますが，セキュリティの側面から見るとその価値は十分あると思います。しかし，フィッシングメールの対策は利用者一人一人の認識が大事であり，何よりもお互いの協力が第一要素だと思います。

参考文献

[1] Wikipedia から（https://ja.wikipedia.org/wiki/多要素認証）