次期弘前大学情報基盤システムに望むこと

医学部保健学科　　陳　彦宇
h17m2326@hirosaki-u.ac.jp

1 はじめに

昨年度はフィッシングメールによる個人情報の漏洩が発生し，多大な問題が生じたことをもとに，次期弘前大学情報基盤システムに望むこと，漏洩防止の対策について考える。

2 フィッシングメールとは

フィッシングメール（Fishingmail）とは，地面上のように，エサをばら撒いて，利用者（User）を釣り上げるような意味合いである。具体的な手法としては，使用者がクリックしそうなソース（使用者が信頼する機関など）になりすまして，使用者にメールを送り，メールの開封及びリプライに誘導することで，個人情報を獲得するものがある。

3 フィッシングメール対策

弘前大学情報システムの利用者として，年間に通じて数十回の使用上では，フィッシングメールを受信することは一度もなかったが，そうした事例があったことには，予防する方策を考えなければならない。使用者側の力で被害を未然に予防するためには，フィッシングメールによる個人情報漏洩の防止としては，ソースの怪しげなメールはクリックせずに削除すること，思いの当たらないメールを受信した場合は当担当者に即座に確認すること，変に個人情報の入力を要求する旨のメールには厳重に確認をすることなどがある。それらを，習慣的に熟せることで，被害の予防に役立つと考える。

4 期望

上記 3 では使用者側の個人的なセキュリティー保護の習慣が被害の予防となることについて述べたが，学校側，情報基盤システムには，電子工学的な技術層のセキュリティーを向上させることと相まって，より被害を確実に減らすことができるのではないかと考える。