フィッシングへの注意

学術情報部情報政策グループ　山田　純一

フィッシングとは，Web サイトや電子メール等を使用した詐欺の一種である。フィッシングのために作成された Web サイトはフィッシングサイト，フィッシングサイトに誘導するためのメールはフィッシングメールと呼ばれる。本学においても，2013 年は多数のフィッシングメールが学外から届いた。

キーワード：セキュリティ，フィッシング，注意喚起

1．フィッシングとは

冒頭に Web サイトや電子メール等を使用した詐欺の一種であると記載したが，もう少し詳しく説明する。悪意のあるユーザは，実在の金融機関，有名企業等の名前をかたるフィッシングメール（図 1）をユーザに送信し，メール中にある URL から正規の Web サイトのように作成された偽 Web サイトへユーザを誘導する（図 2）。Web サイトで情報を入力させ，その情報を盗み取る詐欺行為である。このフィッシングによって盗み取ろうとしている情報は，代表的に以下のものがある。

- クレジットカードやキャッシュカード等のカード番号
- 銀行やカード等の暗証番号
- 住所，氏名，電話番号
- オークションやメール等の ID，パスワード

ここまでの流れを分かり易くすると，図 3 のようになる（図 3）。

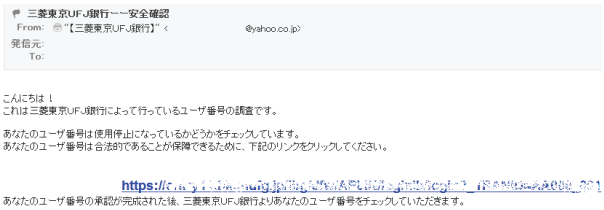

図 1　フィッシングメール

図 2　Web サイト（左側が正規の Web サイト，右側がフィッシングサイト）
※　株式会社三菱東京ＵＦＪ銀行の Web サイトから一部引用

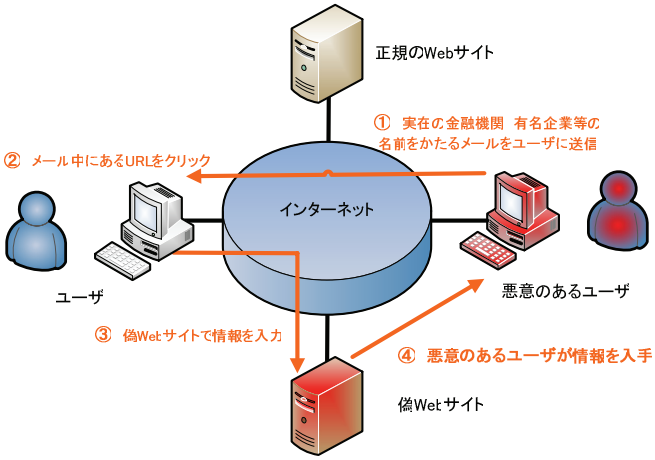

図 3　フィッシングの仕組み

本学においてもフィッシングメールはかなりの量が届いており，実際にフィッシングによる被害も発生している。本学宛に送付されてきたフィッシングメールは Webmail（Active! mail）を狙ったメールである（図 4）。この他にも文面の内容を変えたフィッシングメールが多数届いている。

差出人 Active! mail Account
件名 注意:アクティブメールユーザー
返信先
宛先

注意:アクティブメールユーザー

あなたのメールボックスのクォータは、Active便によって設定された格納域の制限を
超えている
あなたの電子メールアカウントを検証する再には、ここをクリックしてください：

http://

正しくあなたのログイン情報を提供するために、障害になることに注意してください
私達のデータベースからメールアカウントの即時閉鎖

Active! Web mail
m1998-2013 TransWARE Co. All Rights Reserved.

図 4　本学宛のフィッシングメール例 1

URL にあるフィッシングサイトは，本学の Webmail（Active! mail）のログイン画面とは全く違うもので，かなり雑に作成された Web サイトであった（図 5，図 6）。

図 5　Webmail（Active! mail）のフィッシングサイト例 1

図 6　Webmail（Active! mail）のフィッシングサイト例 2

2．フィッシングの見分け方

フィッシングに対しては，被害者にならないためにも見分け方が重要になってくる。ここでは，本学に送付されてきた Webmail（Active! mail）を例に，見分け方について解説する。

- メールの情報をしっかりと確認する。

以下のフィッシングメール（図 7）も本学に届いたフィッシングメールの一例である。まず，差出人（送信者）欄が本学のメールアドレスや Active! Mail を開発・販売している企業とは全く関係のないメールアドレスになっている。

一方，差出人が他組織等のアカウント（フィッシング被害に遭ったアカウント）となっていることもあるが，メールの内容をしっかり確認して欲しい。他組織の方が本学のアカウントを検証する，メールの容量を増やす，アカウントをロックする等ありえない話になっていることを見分けて欲し

い。

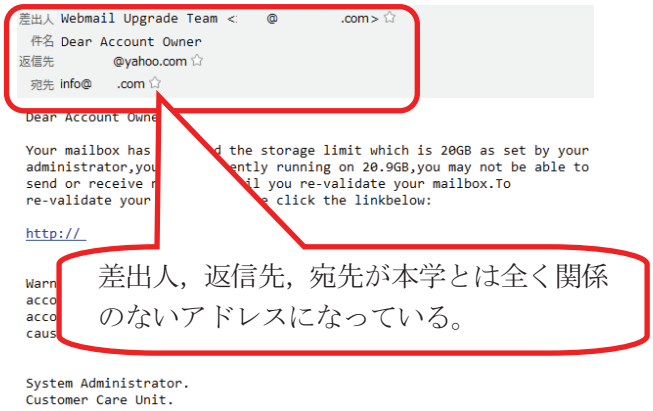

図 7　本学宛のフィッシングメール例 2

また，金融機関やクレジットカード会社がメールで口座番号やカード番号，ID，暗証番号，パスワードを確認することはないので，このような内容のメールが届いたら，フィッシングメールの可能性が高い。

- Web サイトは SSL あるいは TLS に対応しているか確認する。

もし誤って URL 先を参照してしまった場合，その Web サイトの URL が「https://～」で始まっているかを確認する（図 8）。「https://～」の場合は SSL や TLS（SSL，TLS の説明は省略）を用いて，サーバとクライアント間でやり取りするデータを暗号化している。これにより，例えば会員登録，ログイン画面等での個人情報やパスワード，クレジット番号の入力時には，これらの情報を暗号化してサーバに送信する。個人情報やパスワード，クレジット番号の入力が必須にも関わらず，URL が「http://～」で始まる場合は，フィッシングサイトである可能性が高い。

図 8　HTTPS の確認

URL の確認後は，電子証明書（電子証明書の説明は省略）を確認する。使用するブラウザによって異なるが，大抵はブラウザに鍵マークが表示されているので，その鍵マークをクリックする（図 9）。

図 9　鍵マークの確認
（Internet Explorer 10 の場合）

電子証明書の内容が表示されるので，確認する（図 10）。証明書中に本学のドメイン（u-toyama.ac.jp）が記載されていれば，本学が運用しているシステムになる。また，証明書の有効期限も問題ないか併せて確認する。証明書が本学のドメインでない場合は，フィッシングサイトの可能性が高い。

図 10　電子証明書の内容
（上から Internet Explorer 10，Safari5.1 の場合）

３．まとめ

フィッシングは，実在の金融機関や有名企業等の名前をかたってきたが，最近では大学や企業が使用しているソフトウェア，システムをかたってくるパターンになってきている。ただ，Webmail（Active! mail）のフィッシングはメールに誤字や脱字が多い日本語であり，フィッシングサイトは非常に雑な作りである。

しかし，このようなフィッシングでも被害が発生している他，今後は精巧に作成されたフィッシングが出回る可能性が非常に高い。インターネット利用者においては，フィッシングによって被害者となったり，間接的に加害者にならないためにも注意が必要である。

参考文献・資料

1) フィッシング対策協議会「フィッシングとは」
https://www.antiphishing.jp/consumer/abt_phishing.html　（2013 年 12 月現在）
2) 株式会社三菱東京ＵＦＪ銀行「インターネットバンキングのパスワード等を騙し取る不審な電子メールにご注意ください。（平成 25 年 11 月 27 日更新）」
http://www.bk.mufg.jp/info/phishing/20131118.html　（2013 年 12 月現在）
3) 株式会社三菱東京ＵＦＪ銀行「インターネットバンキング」
https://entry11.bk.mufg.jp/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001　（2013 年 12 月現在）
4) 株式会社トランスウェア「【注意喚起：パターン 1】Active! mail の利用ユーザー様を狙ったフィッシング詐欺にご注意ください！」
http://www.transware.co.jp/news/2013/10/01_1400.html　（2013 年 12 月現在）
5) 株式会社トランスウェア「【注意喚起：パターン 2】Active! mail の利用ユーザー様を狙ったフィッシング詐欺にご注意ください！」
http://www.transware.co.jp/news/2013/10/03_2030.html　（2013 年 12 月現在）
6) フィッシング対策協議会「フィッシング対策の心得」
http://www.antiphishing.jp/consumer/attention.html　（2013 年 12 月現在）