SNS サイト等におけるアカウント情報の取扱いについて

附属図書館情報基盤グループ　竹内 淑怜
s_take@hirosaki-u.ac.jp

1 はじめに

昨年 9 月、SNS サイト等へのハッキングにより、漏えいしたとみられているアカウント(認証 ID・パスワード)の中に政府機関等が使用するメールアドレス(go.jp ドメイン)が約 1.5 万件見つかった旨報道があり、先日も同様にハッキング攻撃により、ダークウェブ上に 14 億件のユーザーネームとパスワードのセットを含むデータ流出事案についても報道がありました。

9 月の報道では、職員が SNS 等の外部サービスを使用する際に、職務用のメールアドレスを認証 ID として登録していたとみられていますが、これらのメールアドレスが外部に漏えいした場合には、成りすましや標的型攻撃に悪用される恐れもあります。

2 アカウント情報の取り扱いの注意

メールアドレス等の情報の取り扱いについては、以下のリスクがあることをご理解の上、運用していただきますようお願いいたします。

- 大学内で使用しているメールアドレスとパスワードの私的利用に関する注意
  私的にウェブ上の各種サービス(SNS など)を利用する際の ID やパスワードとして、大学内において業務に使用しているメールアドレスとパスワードを利用した場合、ウェブ上の各種サービスから情報が漏えいした際に、不正アクセス等の被害を受けるといったリスクを負う可能性があります。
- 大学内情報システムで使用しているパスワードと共通のパスワードの大学外システムでの使用に関する注意
  業務上の必要性からウェブ上の各種サービスを利用するにあたり、大学内情報システムの ID を利用しない場合であっても、大学内情報システムのパスワードを大学外システムで使いまわした場合、当該外部サービスから情報が漏えいした場合には、大学内情報システムへの不正アクセスに悪用される可能性があります。

3 対応

本学が発行しているメールアドレス等アカウントについては、以下の対応を検討してください。

- 学外のサービスを利用する場合には、学内の情報システムで使用しているパスワードを設定しないようにしてください。
- 学外のサービスを私的に利用する場合には、本学が発行するメールアドレスを ID に設定しないようにしてください。
- 他者から推測されやすいパスワードの利用は避けてください。
- パスワードが漏えいするおそれがある場合は速やかにパスワードを変更してください。
- アカウントが不正に使用された場合は、弘前大学 CSIRT へ連絡してください。
  弘前大学 CSIRT:csirt@ml.hirosaki-u.ac.jp

4 パスワードの作成と管理方法

学内の情報システムと同じパスワードの設定や他者から推測されやすいパスワードの利用を避けるために、以下の例を参考にパスワードの運用について検討をお願いします。

4.1 パスワード作成方法について

(1) キーワードを分割する方法

ⅰ. 1 つ長めのキーワードを決めて、ローマ字に変換します。

ⅱ. 変換したキーワードを3つ以上に分割し、分割した先頭の文字を大文字に変換します。

ⅲ. それぞれ分割した部分の文字数を語尾に追記します。

例:「弘前大学」をキーワードに決めた場合

ⅰ. ローマ字に変換: hirosakidaigaku

ⅱ. キーワードを分割:Hirosaki Dai Gaku

ⅲ. 数字を追記: Hirosaki8Dai3Gaku4

(2) 複数のキーワードを並べる方法

ⅰ. 2 つ以上のキーワードを決めて、キーワードの最初の文字を大文字のローマ字に変換します。

ⅱ. 「あ」->「a」、「か」->「k」など各発音のはじめの文字を抜き出します。

ⅲ. 抜き出した文字の数を各キーワードの後ろに追記します。

例:「弘前」と「パスワード」をキーワードに決めた場合

ⅰ. ローマ字に変換: Hirosaki Pasuwado

ⅱ. 文字の抜き出し: Hrsk Pswd

ⅲ. 数字を追記: Hrsk4Pswd4

4.2 パスワードの管理方法について

パスワードを記憶する以外の方法として 3 つの例を紹介します。

1 つ目にはノートや手帳に記載する方法があります。これは、ネットワークから漏えいするおそれがないというメリットがありますが、紛失しないように注意する必要や他人の目に触れる場所例えば、机やパソコンのそばに放置しないよう注意が必要となります。

また、パスワードそのものを記載しない等の方法も有効です。

2 つ目に特別なツールを必要としない方法として Excel や Word ファイルの暗号化する方法があります。

Excel や Word の「ファイル」タブの「情報」から「ブックの保護」をクリックし、「パスワードを使用して暗号化」を選択します。

図 1 Excel の暗号化 1

「パスワード」及び「パスワード再入力」欄に同じパスワードを入力し、暗号化を行います。この時のパスワードを記憶しておく必要があります。

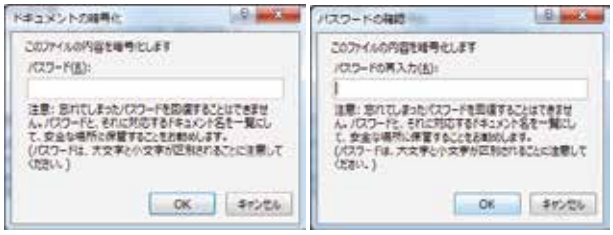

図 2 Excel の暗号化 2

3 つ目として、パスワードを管理するツールを利用する方法があります。

有料や無料のパスワード管理ソフトウェアをダウンロードして利用することができます。

- 1password (https://1password.com/)
- LastPass (https://www.lastpass.com/ja)
- KeePass (https://keepass.info/)

他に、パスワードを管理する製品も販売しています。

- ミルパス (http://www.kingjim.co.jp/sp/pw20/)

また、総合セキュリティソフトの中にはパスワード管理機能を実装しているソフトウェアもあります。

参考文献

[1] 【注意喚起】SNS サイト等におけるアカウント情報の取扱いについて (http://www.cc.hirosaki-u.ac.jp/blog/12859)

[2] 簡単パスワードでセキュリティ 10 倍！覚えやすく使い回せるおすすめのパスワードの作り方 (http://www.ochearno.net/entry/2015/11/25/091035)

[3] 安全にパスワードを管理する方法！紛失・漏えいリスクから守る (https://securitynavi.jp/596)

[4] 1password (https://1password.com/)

[5] LastPass (https://www.lastpass.com/ja)

[6] KeePass (https://keepass.info/)

[7] ミルパス (http://www.kingjim.co.jp/sp/pw20/)