

パソコンいっしょに教室新聞

ネットのサービスやスマホのアプリなど、便利なツールはたくさんあります。新聞でも様々取り上げてきました。さて、安全面はどうでしょう？

パスワードの管理

ア マゾンや楽天などのお買い物、SNS、ネットバンク、株取引など、事前登録を行いID、パスワードでログインして使用するサービスは増える一方です。またその裏側でID、パスワードの漏えいで不正に利用される事件も後を絶ちません。

パ スワードは、銀行ATMガードの「暗証番号」に当たるもので、忘れてしまうとそのサービスが使えなくなってしまう。新しいモノは手軽に作れますが、忘れたからといって再作成するのはお勧めできません。前の登録内容はそのままの残ってしまいます。それを悪用されたら…（銀行ATMカードの暗証番号を忘れたからといって新しく口座を作ることはありませんね。）
パ スワードの管理は厳重にしたいものです。

① パスワードの作成

「忘れるからから」といって簡単なパスワードはやめましょう。「英(大文字・小文字)」「数字」「記号」を組み合わせ、できるだけ長い文字がいいでしょう。(10文字程度が妥当でしょう) 複数のサービスを利用しているなら、**同じパスワードは使用せず**、サービスごとに分けることをお勧めします。(一つバレても被害は最小限にとどめよう)

② パスワードの管理

サービスごとに異なるパスワードを作成すると、覚えるのも至難の業。そこでその記録方法ですが、一番お手軽なのは「**メモに書く**」ことでしょう。これではそのメモを無くしてしまうことも考えられますし、誰かに盗み見されることもあるかもしれません。

次に手軽にできそうなのが「**ファイルに保存しておく**」方法です。ワードでもエクセルでもいいのですが、サービスとパスワードなどを入力した一覧を作成し保存すれば、紛失することもないでしょう。ただ、保存時には本人以外が開けないように「パスワード」を設定すること忘れずに。

その他、管理ソフトもありますので、探してみるのもよいでしょう。

二段階認証とは…

— **二段階認証**は、万が一IDやパスワードが漏れても、もう一つの「**認証コード(PINコード)**」が分からないとログインできない仕組みです。

いつもと異なるパソコンなどでログインしようすると「**認証コード**」の入力を求められます。あらかじめ携帯番号やメールアドレスを登録しておくと、その番号にコードが送られ、それを入力します。第三者にはログインできない仕組みです。

GoogleやFacebook、Twitter、Apple ID、Microsoftアカウントなど、その仕組みを利用できるサービスが増えてきました。

— **NE**のアカウントが乗っ取られて、友達を装った悪者から金銭をだまし取られる、なんてニュースも耳に新しいところです。

これも不正にID、パスワードがどこからか漏れたことによるものです。これも**認証コードの登録**である程度防げます。



LINE の設定画面

面倒と思いますがちなパスワードの管理。でも、被害に合わないために面倒でもキッチリ管理しておきましょう。転ばぬ先の杖です。ネットサービスは便利なものですが、悪者がいる限り防御も必要です。

教室Facebookにも書いてますが、ネットの閲覧も「プライベートブラウジング」を使えば閲覧履歴が残りません。共有しているパソコンや他人のパソコンを使用するときなど、利用するとよいでしょう。

教室のWebページもよろしくお願いします。

<http://pc-iwakura.com/>

See you next month