https://kyouikucenter.sagamihara.andteacher.jp/modules/hp_jpage14/

教育DX推進課

＼ 危ないから使わないではなく　よりよい使い方を ／

さがみはらGIGA通信
～リテラシー編～

19号

2026/10/26　発行

パスワードは「デジタルのカギ🔑」

情報が漏れても、被害を広げないために

最近、「情報漏えい」というニュースを目にすることが増えています。会社のHPや提供するアプリなどのサービスが攻撃を受けて、情報が漏れてしまうことは、利用している人だけでは防げません。でも、そのあとの被害を広げないために、自分でできることがあります。

ポイントは、パスワードを「デジタルのカギ（鍵）」として大切に使うことです。

もし、同じカギを使っていたら？

あるサービスから、IDやパスワードが漏れたとします。もし同じパスワードを、ゲーム、メール、動画サービスなどでも使っていたらどうなるでしょう。攻撃する人は、「ほかのサービスでも、このカギが使えるかも」と試すことがあります。

すると、一つのサービスからの漏えいが、別のアカウントの乗っ取りにつながることがあります。



Q. 毎月パスワードを変えれば安全？

A. いいえ

大切なのは「使い回さない」ことです

十分に長く、推測されにくいパスワードに設定し、各サービス・アプリごとに使い分けることで安全性を高めます。しかし、

・情報が漏れた可能性がある
・知らないログインがあった
・サービスから変更を求められた

こんなときは、すぐに変更しましょう。

「漏えいしました」のメールが来たら

すぐにメールのリンクを押さないことも大切です。情報漏えいに便乗した、ニセのお知らせかもしれません。

できれば、ログイン履歴も確認し、多要素認証を設定しましょう。

学校から渡されているアカウントは、自分だけで設定を変えず、学校からの指示に従ってください。情報漏えいそのものを、自分一人では止められないことがあります。

だからこそ大切なのは、「自分が悪かった」と考えることではなく、被害を次へ広げないこと。

一つ一つのアカウントに、
違う「カギ」を持つことから始めましょう。

1 公式サイトや公式アプリで確かめる
2 漏れた可能性があるパスワードを変更する
3 同じパスワードを使っているサービスも変更する

今日からできる3つ

① 貸さない・使い回さない
友達や家族であっても、IDとパスワードは自分で管理します。

② 長く、推測されにくく
名前や誕生日など、知っている人が想像しやすいものだけにしないようにします。

③ 多要素認証《たようそにんしょう》
使えるサービスでは、パスワードだけでなく、もう一つの方法でも本人確認をする設定を使いましょう。

参考になるサイト・相談先

子どもと考えたい新12の約束を公開中!!

さがみはらnetモラルサイト
https://sites.google.com/sagamihara-kng.ed.jp/moralsite/%E3%83%9B%E3%83%BC%E3%83%A0

こどもとネットのトリセツ
【安全ネットづくり促進協議会】
https://www.kodomo-safety.org/

上手にネットと付き合おう！【総務省】
https://www.soumu.go.jp/use_the_internet_wisely/

どうしよう、、、そんな時は
「相談しよう、そうしよう」

http://www-host.city.sagamihara.kanagawa.jp/kosodate/1026602/1032527.html