

パスワードの取り扱いについて

インターネット上のサービスには、アカウントを作成してから利用するものがたくさんあります。アカウントを作る際に必要となるのが、パスワードの設定。覚えやすいようにと簡易なものを設定してしまいがちなパスワードですが、そうしたパスワードを設定しているといつ危険な事態におちいらないとも限らないのです。

簡易なパスワードは推測されやすい

ではいったい、どんなパスワードが危険なのでしょうか。具体的には以下のようなものがあげられます。

危険なパスワード

- ・名前や誕生日、電話番号など個人に関するもの
- ・連番や連續の英数字（1111、123456、abcde など）
- ・6文字以下の短いもの

このようなパスワードを設定していると、他者からパスワードを推測され、アカウントの乗っ取り被害にあう可能性があります。

アカウントを乗っ取られると、自分になりますされ、詐欺目的で友人や家族にメッセージを送られたり、いたずら目的で不適切な投稿をされたりと、自分はもちろん、周りの人にまで被害が及んでしまうことがあるのです。

また、同じパスワードを複数のサービスで使いまわしていると、どこか一つのサービスで乗っ取られた場合、他のサービスで利用しているアカウントも乗っ取られてしまい、被害が大きくなってしまう可能性があります。

パスワードの適切な取扱いを。

このような被害を防ぐためには、他人にパスワードを教えないことはもちろん、複数のサービスで同一のパスワードを使いまわさないようにしたり、定期的にパスワードを変更したりすることが大切です。そのうえで、以下のようなルールに従って、他者から推測されにくいパスワードを設定する必要があります。

- ・大小の文字、数字、記号を組み合わせる
- ・8文字以上にする
- ・名前や誕生日など推測されやすいものは避ける

こうしたことを学校全体で指導し、子どもたちにパスワードの適切な取り扱い方を身につけることが大切です。

フィルタリングサービスの利用について

スマートフォンの普及などにより、インターネットは子どもたちにとってますます身近なものになっています。しかしその一方で、インターネット上でトラブルに合う子どもたちも増えています。子どもたちをトラブルから守るため、子どもたちが安全にインターネットを利用するためには、フィルタリングサービスの利用が必要です。そこで、今回はフィルタリングについてお話しします。

フィルタリングの主な機能

フィルタリングの主な機能としては、以下の三つがあげられます。

・有害サイトの閲覧制限

インターネットで有害な情報やアダルトサイトなどを閲覧できないようにします。

・書き込みの禁止

SNSや掲示板、ブログなどの書き込みを禁止することができます。

・利用時間の制限

曜日や時間帯ごとに、インターネットの利用時間を制限することができます。一日の利用は何時間までという制限を設けることも可能です。

フィルタリングサービスには、閲覧制限の対象となっているサイトや、利用制限の対象となっているアプリの中から、保護者が「これは子どもに使わせていい」と思うものを選んで、個別に閲覧・利用可能にすることができる、カスタマイズ機能がついているものがあります。このカスタマイズ機能を使えば、子どもの成長に合わせて徐々に利用範囲を広げていくことができます。

※フィルタリングサービスの中には、Wi-Fi(無線LAN)接続に対応していないものもあります。そのため、公共施設などにあるWi-Fiスポットや、友だちの家で利用しているWi-Fiなどでインターネットを使うことにより、閲覧制限をしているサイトを見たり、利用制限をしているサービスを利用したりすることができてしまうことがあるため注意が必要です。

ペアレンタルコントロールの併用でより安全に

スマートフォンやタブレット、ゲーム機などのインターネット機器の中には、ペアレンタルコントロールという機能がついているものがあります。この機能は、有害サイトの閲覧制限やインターネットの利用時間の制限、アプリのインストール制限などを機器自体にかけることができるので、フィルタリングサービスと併用することで、子どもたちがより安全にインターネットを利用する手助けをすることができます。

フィルタリングやペアレンタルコントロールは、子どもたちが安心・安全にインターネットを利用するためには必要なものです。ご家庭で話し合い、子どもの利用実態やインターネットスキルに応じた設定を心がけることが大切です。