

通信・ITネットワークの分野では、日々新しい技術が開発され、より効率的で、より安価なサービスが次々と生み出されています。知らないことは、イコール企業利益の損失です。そこで私たち大和電設工業は、情報通信やITソリューションの『知って得する最新情報』を、お世話になっている皆様に定期的にお伝えしていきます。隔月発刊のDDK通信、ぜひお楽しみください。

SNSをスマートに活用しよう

SNSが一般的に使われ始めてから20年になります。2004年に日本ではmixi、アメリカではFacebookのサービスが始まり、その後TwitterやYouTubeなど様々なSNSが開発され、それらをお使いの方も多いのではないのでしょうか？

活用方法も昔とは様変わりし、個人の情報発信としてよりも企業の宣伝や商品の案内、YouTubeに関しては、講習やマニュアルとしての活用にも利用されています。

■SNSの問題点

日本ではLINEが幅広く活用されていますが、少し前には、情報の保管サーバーの設置場所が海外だという事で問題になりました。TikTokは、中国に情報が漏洩する可能性があるということで、その使用を禁止する法案を成立させた国もあります。また、イーロン・マスク氏の買収で話題になったTwitterは、アメリカの当時の大統領のアカウントが凍結されたり、YouTubeでは偏向報道ならぬ相容れぬ思想の報道は流さないなど、情報公開の公平性が危ぶまれる場面もあり

ました。このように、色々問題のあるSNSではありますが、新聞やテレビなどに変わる新しいメディアとして広く認知され世界中で利用されています。

■SNSの今後

今後、これらSNSがどのように変化するのが気になりますが、公衆Wi-Fiの5G化が進むことで動画配信がますます活発になると思われます。これに伴い「YouTuber」という職業が認知されつつあるように、ますます新しいメディアとして発展することになるでしょう。

日本の若者が最も利用しているSNSは、LINEがほぼ9割、Instagramが6割となっています。LINEでは、LINE payの決裁アプリとしての利用が始まっています。Twitterも決裁システムを今年の1月に開発することを発表しています。また、メタバース(仮想空間)をSNSで活用することも期待されています。このように、SNSは新たな環境と技術により、廃れることなく使われ続けることになるでしょう。

SNS利用上の注意点

注意1 偽アカウント

SNSには本人確認が徹底していないサービスも存在します。著名人の名前を使った偽のアカウントも多数存在しており、それらを悪用して不正リンクの投稿などが行われることもありますので自分がかかわるアカウントの相手が本物かどうかは慎重に確認する必要があります。公式アカウントかどうかは怪しい場合、本人確認ができない場合には安易にフォローしたり友達になったりしないようにしましょう。

注意2 写真掲載による意図しない位置情報の流出

GPS機能の付いたスマホなどの機器で撮影した写真には、設定によっては撮影日時、撮影場所、カメラの機種名などの情報が含まれる場合があります。こうした写真をSNSに掲載すると、自宅や居場所が特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪被害にあうかもしれません。

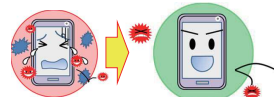
対策として、写真にどのような情報が含まれているか調べるアプリを利用する方法があります。情報を表示できるアプリや、編集・削除できるアプリもあります。むやみに写真を投稿するのではなくアプリなどを上手に使う危険な投稿を減らすように気を付けましょう。

他にも注意点は沢山あります。もちろん良い面も沢山ありますのでスマートに上手にSNSを利用することを心掛けるようにしましょう。

SNSを利用するデバイスとしてスマホを活用されている方はとても多いと思います。総務省が提供している「スマートフォン情報セキュリティ3か条」をご紹介しますのでこちらもぜひ参考になさってください。

その1 OS(基本ソフト)を更新

スマートフォンは、OSの更新(アップデート)が必要です。古いOSを使っていると、ウイルス感染の危険性が高くなります。更新の通知が来たら、インストールしましょう。



その2 ウィルス対策ソフトの利用を確約

ウイルスの混入したアプリケーションが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。



その3 アプリケーションの入手に注意

アプリケーションの事前審査を十分に行っていないアプリケーション提供サイト(アプリケーションの入手元)では、ウイルスの混入したアプリケーションが発見される例があります。OS提供事業者や携帯電話会社などが安全性の審査を行っているアプリケーション提供サイトを利用するようにしましょう。インストールの際にはアプリケーションの機能や利用条件に注意しましょう。

