生成AIにまつわるトラブル

埼玉県教育委員会

近年、「生成AI」という技術が普及し始めています。技術の進歩によりインターネットの利用環境は進化を遂げていますが、その反面、新たなトラブルや犯罪が生まれています。今回は生成AIが用いられたトラブルと危険性についてご紹介します。

生成AIとは

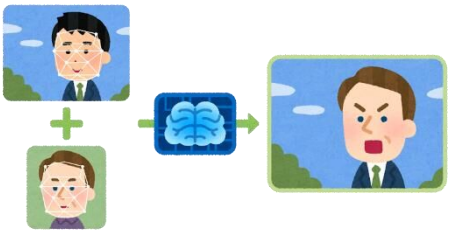
インターネット上にある膨大なデータを学習することで、指示どおりに新たな文章や画像などを生み出すことができる人工知能です。従来のAIは「学習済みのデータの中から適切な回答を探して提示する性質」を持っていましたが、生成AIは「0から1を生み出す」ことができます。

トラブル例

例1　生成AIを利用した犯罪

Aさんは生成AIを活用した自作プログラムを用いて、企業の顧客情報にアクセスしました。そこで得た顧客情報を使用して「他人を装い」商品の購入を行っていました。犯罪であると理解していながらもお金のために実行してしまいました。

例2　生成AIを利用された被害



Bさんは身に覚えのない自分の写真が知らぬ間に拡散されていました。その写真は、第三者がBさんの卒業アルバムの顔写真を生成AIによって加工し、インターネットで公開したものでした。インターネット上で拡散されたこの画像が原因で、Bさんは誹謗中傷を受けることになりました。

生成AIのリスク

利用者観点のリスクとして他者に情報が公開されるリスクがあることを認識しておく必要があります。つまり情報漏洩です。生成AIを利用するということは記録が残ります。他者が生成AIを利用した際に、その記録データが利用され、他者に情報が洩れる可能性があります。

非利用者観点のリスクとして肖像権などの権利が侵害される可能性があります。生成AIは他人の権利を侵害する可能性のある画像や文章を簡単かつ大量に作成できる能力を持っているため巻き込まれる可能性が高くなります。

生成AIを利用するにあたって・・・

生成AIを正しく活用することはわたしたちの生活を便利にする一方で、生成される情報に間違った情報が含まれていることや情報漏えいの危険性、権利侵害などさまざまなリスクや問題点があります。新しい技術が生まれたときには、新しいトラブルや犯罪の手口になる恐れがあります。

トラブルを未然に防ぐためには、興味本位での利用は控え、生成AIの特性やリスク等を十分に理解することが大切です。