

顔認証は、カメラに写った顔を事前に登録したものと照合して、同一人物かどうかを判別する技術です。空港でのセキュリティをはじめ、身近なところではスマホのロック解除など、さまざまな場面で目にするようになりました。離れた場所から非接触で本人確認できるので、感染症対策としても有効であり、今後も利用する機会が増えていくことが予想されます。東京五輪・パラリンピックでも、テロ対策・コロナ対策を目的に顔認証システムが導入される予定です。

顔認証のバイアス問題とは？

このように発展が期待されている顔認証ですが、人種差別や性差別を助長するバイアスが存在するという理由で、欧米では数年前から利用の是非が議論されています。この場合、バイアスは偏見や先入観、思考の偏りを意味しています。アメリカでは人種差別に反対する運動が広がる中、警察による顔認証システムを使用した黒人男性の誤認逮捕が相次いで起こり、顔認証の利用禁止を訴える声が高まっています。ある研究結果では、顔認証システムの性能は、白人男性を対象とした場合に最も高く、黒人女性を対象とした場合に最も低いことが示されています。このような性能の偏りはどうして生まれるのでしょうか？

顔認証システムは、データとアルゴリズム(計算方法)から構成されています。システムはデータとして与えられた数百万枚の顔画像から、顔の特徴や人を見分けるポイントなどを学習します。このとき、どのように学習するかをアルゴリズムとして設計します。データの偏りは性能を大きく左右します。つまり、白人男性のデータが多く、黒人女性のデータが少なければ、前述のような性能の偏りが生じます。データの収集は人が行うので、個人に内在する人種や性別に対するバイアスがデータに加わることとなります。アルゴリズムの設計も人が行うので、やはりそこにも個人のバイアスが存在します。

バイアスは生活する環境や文化の中で無意識に培われるものであり、人がかかわる以上、バイアスを完全に排除することは困難です。このことは顔認証だけでなく、同様にデータとアルゴリズムで構成されている人工知能(AI)全般にも言えます。システムが出す結果を客観的なものとして妄信するのではなく、人間の主観的なバイアスに起因する誤りが含まれている場合があることを正しく理解して利用する必要があります。