ディープフェイクの危険性

ディープフェイク

・AI によって作成される人物の画像合成の技術
・GAN（敵対的生成ネットワーク）を使用している
・既存と元にする画像や映像を結合することで生成
・コンピュータ上で、ファイク画像や映像が生成される

キエフ、ウクライナ -2019 年 9 月 17 日
NVIDIA の研究者によって発明された、
生成的な敵対的ネットワークによって
作成された、超現実的な AI によって
生成された人間の顔のコラージュ

AI の進化により、ディープラーニング（深層学習）とフェイク（偽物）の混成語である「ディープフェイク」という言葉が、近年話題になっています。
これは、2016 年の米国大統領選挙での、情報操作をめぐる抗議から「フェイクニュース」という言葉が流行り、政治家の加工動画などが問題になったことから、2020 年の大統領選挙には AI を駆使したディープフェイクが悪用されると予想されているからのようです。
実際、すでに有名人の多くは被害にあっており、これは技術の進歩により、スマホなどでも手軽に動画や画像の加工ができるようになったことも影響しているようですが、教師なし学習の敵対的生成ネットワークの GAN が利用されるようになって AI によってよりリアルな動画や画像加工ができるため、ファイクかどうかの見極めがしづらくなってきました。
GAN を使用することにより、元にする画像にない仕草や表情まで作成できるため、喋っていない言葉を話す様子までリアルに近い映像を作成することができます。これが、AI のオープンソースで作成できるようになると、使用者のモラルでいくらでも悪用できてしまいます。
問題は、作成される画像や映像がリアルすぎて、本物かとうかをどのように判断するかということです。AI が主流となる前の画像加工は、映画などの余程高価な映像機材を使用しないかぎり、ファイクが分かり易かったのですが、現在はその見極めがかなり難しくなってきています。それでなくても、スマホのカメラには、手軽に美しく加工したりするツールがあるため、どこからがフェイクと判定するのかも難しい問題です。こうなると、真実と信じられているものの中に、フェイクが発覚していないものも多いのではと不安になってきます。そのための、セキュリティ対策は、とても困難なものになっていくでしょう。
上司からの指示かどうかも、ファイクではないかと疑い始めたらきりがないです。テレビ会議の向こう側で会話している人が、AI が臨機応変に対応しているかもしれないということも、技術的にはあり得る時代になりました。ドッキリカメラの冗談であれば笑えますが、ネットを乗っ取られ、悪意のある行為で指示が来たとしたらとても恐ろしいことです。
今後、セキュリティ対策として、ディープファイクをどのように対応すべきなのかも、企業として本気で取り組む必要がありそうです。