2024年1月31日掲載

経済透視図 ⑩①

ウェブセキュリティー市場動向 ㊥

生成AIで模倣高度化

SMBC日興証券
プライベート・キャピタル・ソリューション室長
窪田 正吾

生成人工知能（AI）が登場したことでサイバー攻撃が高度化している。例えば、誰かに成りすましてメールを送り込むことで偽のホームページに誘導する。また、クレジットカード情報を不正に入手するフィッシング詐欺は、生成AIを活用することで特定人物のスタイルを模倣した文面を作成することが可能になっている。

現在では、会員制交流サイト（SNS）やブログなどウェブ上で個人情報や趣味嗜好、文章のくせなどを簡単に収集することが可能である。このような大量のデータとディープラーニング技術を組み合わせて大規模言語モデル（LLM）を構築することで、その人らしい自然なコミュニケーションが可能になる。

上司や知人から送られたメールは、知らない人から届いたメールと比較して開封率が高く、フィッシング詐欺の精度が大幅に向上すると考えられる。

また、生成AIは文字だけでなく音声や動画、3Dといった多様なフォーマットで活用可能で、関係者のディープフェイク映像を作り出して不正を行うよう指示を出したり、情報を入手しようとしたりする犯罪（ソーシャルエンジニアリング）の増加が懸念されている。

通常、個人情報やAIのソースコードなどの重要データは外部に開示しないように設計されているが、想定外の質問が行われた場合にAIが回答してしまい、情報が漏えいするション と呼ばれる攻撃手法は、不正アクセスを行うのではなく、正常利用に見せかけて対話型AIに対してAI開発者が意図していない質問を行うものである。

その他、生成AIが質問の正解を知らなくても無理やり回答してしまうハルシネーションという特性を悪用したサイバー攻撃も想定され、開発者やユーザー共に慎重な利用が要求される。

生成AI関連のサイバー攻撃以外に目に付くのは、ハクティビズム（ハッキングによる政治的意思表明）の増加である。ロシアによるウクライナ侵略以降にウクライナのウェブセキュリティー強化およびロシアへのサイバー攻撃目的で「ウクライナIT軍」が組織されたのは記憶に新しい。多くの人が自分の正義を信じてハクティビズムを行っているが、サイバー犯罪との線引きは非常に難しい。

次回はサイバー攻撃の高度化に併せて進化するセキュリティー対策について紹介する。

（隔週水曜日に掲載）