サイバーセキュリティ最前線

AI時代の到来にともないさらに巧妙になったサイバー攻撃を100パーセント防ぐことができるのか!?

ChatGPTをはじめとした生成AIの台頭によって、AIが急速に身近なものになってきた。では、AI時代においてはどのようなサイバー攻撃のリスクが想定され、どのような対策を講じるべきなのか。今号ではそのあたりを検証したい。

AIがサイバー攻撃を助長!?

AI（人工知能）とは「人間の知的な活動を模倣する技術」であり、コンピュータシステムによってデータを解析し、意思決定を行う能力のことを意味する。なかでも、ChatGPTなどで知られる生成AIは大量のデータを学習し、文章や音楽、画像、映像などさまざまな形式のデータを作成する機能を有している。この生成AIが世界を席巻しつつあることから、日本でもAIをめぐる議論が活発になっている。たとえば、内閣府がこの5月に公表した「AIに関する暫定的な論点整理」によると、①機密情報の漏洩や個人情報の不適正な利用のリスク②犯罪の巧妙化・容易化につながるリスク③偽情報等が社会を不安定化・混乱させるリスク④サイバー攻撃が巧妙化するリスク⑤教育現場における生成AIの扱い⑥著作権侵害のリスク⑦AIによって失業者が増えるリスクなどが指摘されている。

では、直接AIを利用しなくても影響を受ける④のサイバー攻撃が巧妙化するリスクとはどういったものなのか。ポイントのひとつは、AIは善人だけでなく、悪人の役にも立つという点だ。たとえば、よく知られる手口であるフィッシングメールや詐欺メールの内容がAIの悪用でよりリアルになり、受け取る側の判別が難しくなることが想定される。AIで作成されるディープフェイク（リアルな映像や音声）が悪用される可能性もあり、生体的認証の見直しすら必要になるかもしれない。

また、システムやソフトウェアの脆弱性（セキュリティ面での欠陥＝バグ）にも悪影響がおよびかねない。なんと米国のスタンフォード大学の研究者チームがプログラミングを行う際にAIを利用したグループと、そうでないグループとの比較テストを実施したところ、前者のほうがより多くの脆弱性を生み出してしまい、かつその被験者グループはAIの利用でより質が高いプログラミングをしていたと認識していたというのだ。かぎられた範囲のサンプルではあるが、AIの利用が慢心を生む可能性があることは否定できない。もちろん、AIによってシステムの脆弱性がより容易に発見されるおそれもあるだろう。

AI時代のソリューション

こうした状況下ではどのようなサイバーセキュリティが有効なのか。長年にわたってセキュリティシステムを手掛けてきた㈱ブロード（東京都千代田区）は真っ先に「Windowsパソコンのエンドポイント保護を実現する『HP Sure Click Enterprise（HP SCE）』を導入してほしい」と強調する。曰く、このツールは仮想化技術を生かしてPC上に別のパソコンを稼働させる仕組みになっており、仮にマルウェアが動いても本体には一切、影響が出ないという。つまり、いかにAIによって悪意のあるメールの精度が高まったとしても、マルウェアによる脅威を確実に取り除くことができるのだ。またマイクロソフトの重要な脆弱性の75パーセントは「ユーザーが管理者権限を持っていなければ、その影響が大幅に軽減される」といわれているが、その点についてはBeyondTrust社製の特権管理ソリューションがオススメだという。なんでもこのソリューションを活用すれば、標準ユーザーのままでも万全の状態で管理者権限が必要な操作を実行できるようになるそうだ。

そのほかにも多岐にわたるソリューションをラインアップしているとのことなので、AI時代に最適なセキュリティソリューションをお探しの方はブロードに相談してみてはどうだろうか。