2018 年 7 月 20 日

サービス＆セキュリティ株式会社 e-Gate センター

【コラム】 AI を悪用したサイバー攻撃

今回のコラムでは、近年注目を集めている AI 技術について情報セキュリティの観点から、今後のサイバー攻撃や対策について説明します。

1. 第 3 次 AI ブーム到来

最近、画像分析や音声認識など様々な分野で AI（人工知能）の実用化が進んでいます。AI 技術はこれまでに何度か注目されることがありましたが、最近の AI への脚光は第 3 次 AI ブームと呼ばれています。この第 3 次 AI ブームの背景には、ビッグデータや量子コンピュータの発展などの性能的な要因とニューラルネットワークのモデリングや深層学習の効率化などの手法的な要因が関係しています。

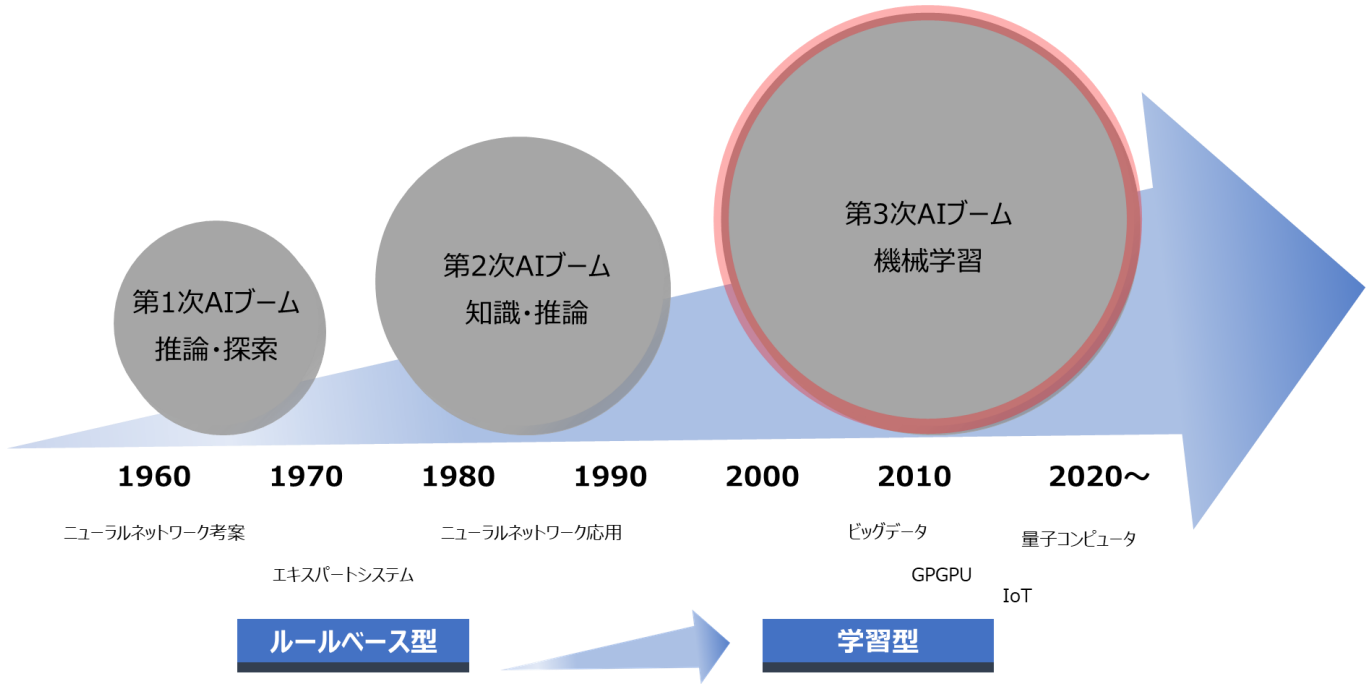

図 1 AI ブームの歴史

AI が普及することは人々の生活を豊かにしてくれる半面、それを悪用することで甚大な被害を与える可能性もあります。情報セキュリティの分野では未知の脅威の検出や対応に AI 技術を活用した製品が注目を集めています。現状はそういった製品を導入することで一定の脅威については対策が可能です。しかし AI を悪用したサイバー攻撃が発生した場合にはセキュリティ対策として不十分な状態となってしまう可能性があります。AI ブームにより AI 実装のハードルが下がってきていることから、近い将来 AI を悪用したサイバー攻撃が発生する可能性は極めて高いです。

2. AI を悪用したサイバー攻撃（AI 攻撃）

Q１．近い将来とはいつか

具体的な時期はわかりませんが、2~3 年以内には AI 攻撃が発生する可能性があります。しかし AI 攻撃の実用化にはいくつかの課題があり、その 1 つがコンピュータのリソース（処理能力）です。AI による 1 つ 1 つの処理はコンピュータの内部で膨大な演算処理が行われており、この処理は一般的な PC では処理能力が不十分です。攻撃者は AI 攻撃を実施するためにコンピュータリソースを準備する必要がありますが、準備には莫大な費用が掛かります。現状では AI 攻撃の費用対効果が低いため表立った AI 攻撃はまだ確認されていません。

近年、コインマイナーなどの被害者の PC のリソースを不正に使用するようなマルウェアが流行しています。コインマイナーは暗号通貨を発掘するための演算処理を被害者の PC で行いますが、この仕組みを攻撃者の AI の演算処理に応用することで、AI 攻撃は現実のものとなるでしょう。

＊コインマイナー：仮想通貨の発掘（マイニング）をおこなうツール。

Q２．どのような攻撃が行われるのか

① チューリングテストの突破

AI の特徴はコンピュータに人間のような動作をさせることです。AI を悪用することで、これまで人間にしかできなかったことがコンピュータでもできるようになります。すなわち、画像認証の CAPTCHA のようなチューリングテストを突破する攻撃が挙げられます。こういった認証を突破する AI アルゴリズムはすでに開発が進んでいて、人工知能ベンチャーの Vicarious 社では CAPTCHA 突破成功に関する記事が公開されています。

「Common Sense, Cortex, and CAPTCHA」- Vicarious 社 Blog
https://www.vicarious.com/2017/10/26/common-sense-cortex-and-captcha/

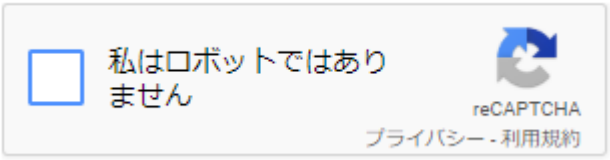

図 2 reCAPTCHA のサンプル

＊チューリングテスト アラン・チューリングによって考案された、ある機械が知的かどうか（人工知能であるかどうか）を判定するためのテスト。

② 高度なシステム探索による攻撃

企業内のネットワークに入り込んだマルウェアに様々なシステム情報を収集させて、PC の使用頻度が高い時間帯、IP アドレスの採番規則、ホスト名の命名規則などのシステムの特徴を AI により抽出してシステムの脆弱性を発見し、さらなる攻撃につなげる可能性もあります。

3. AI 攻撃から身を守るために

AI 攻撃はこれまでにない脅威になることが予測されます。しかし適切な準備を行っていれば、被害を最小限にとどめることができ、その脅威は怖くありません。

例えば、チューリングテストを突破する AI 攻撃に対しては SMS 認証や認証トークンの採用など CAPTCHA 以外の 2 要素認証を採用することで身を守ることができます。また、高度なシステム探索による攻撃についても、システムの脆弱性を取り除き、監視やフォレンジックをしっかり行っていればインシデントにつながる可能性は非常に低くなります。さらにインシデント発生時の対策方針を事前に取り決めておくことで被害範囲を最小限に限定することができます。

AI 攻撃による脅威について前述しましたが、結局のところ企業がとるべきセキュリティ対策はこれまでと同じで、セキュリティ対策の PDCA を継続的に行うことが大事です。

図 3 セキュリティ対策の PDCA

セキュリティ対策の PDCA を実施するためには CSIRT（Computer Security Incident Response Team）や SOC（Security Operation Center）などの専門組織を企業内に作る必要があるため、多くの企業がヒト・モノ・カネの面で対策が不十分となっているのが実情です。そこで、SSK（サービス＆セキュリティ株式会社）では 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッドを備えた次世代 SOC「e-Gate センター」、この 2 つを融合させることによりお客様の情報セキュリティ全体をサポートします。

4. e-Gate の活用

セキュリティ人材サービス

e-Gate センター（SOC）での実習を通じて高度な技術を身に付けたセキュリティエンジニアが、お客様のプライベート SOC、CSIRT に常駐し、円滑な運用に貢献します。お客様サイトに常駐しているセキュリティエンジニアには常に e-Gate センターからバックアップがあるため、質の高いサービスのご提供が可能です。セキュリティ運用監視サービスと併用することで、万が一のインシデント発生時にも e-Gate センターとセキュリティエンジニアの密な連携で、迅速かつ的確な対処を行います。

セキュリティ運用監視サービス

e-Gate センターがお客様のシステムに設置されたセキュリティ機器のログをリアルタイムに監視・分析。AI を使った最新のログ分析システムにより巧妙な攻撃を検知し、スピーディかつ適切な対応を可能とします。また、月次レポートの提出・説明、対面にての報告会を実施いたします。月次レポートは監視機器ごとにきめ細かな分析内容を記載しております。

セキュリティ対策支援サービス

約 40 年に渡って培った情報システム運用監視の実践的なノウハウと、e-Gate センターのセキュリティ対策技術をご提供いたします。お客様システムに潜在する脆弱性を診断し、その結果、検出されたリスクに対し対策をご提案する診断サービスや、お客様のセキュリティに対する個別ニーズへの対応や、情報システムだけでなく全社体制で取り組むべきセキュリティ対策に最適な答えを導き出します。各種診断からアドバイス、システム構築まで、あらゆる情報セキュリティニーズにワンストップで対応します。

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp