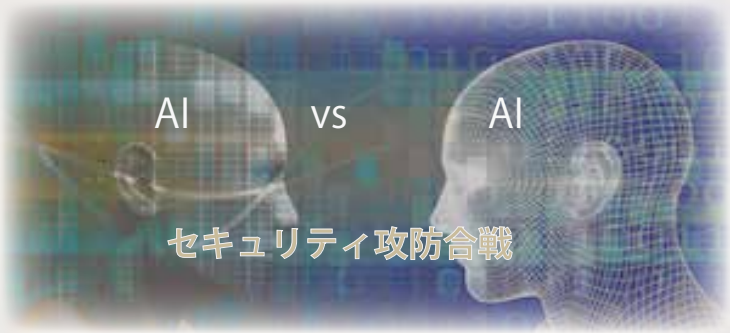
AI と AI によるセキュリティ攻防

セキュリティ対策は AI に依存する時代



パターンマッチングだけでは、マルウェア検知は無理
セキュリティ対策の AI は、犯罪者の行動パターンを学習
犯罪者は、正常な業務プロセスを真似る学習

セキュリティ対策ツールの多くに、AI による学習や分析をする技術を搭載しているプロダクトが増えてきました。
そうしたディープラーニングなどの AI 技術が必要とされている理由は、それだけサイバー攻撃が巧妙かつ大量に増加しているためです。
以前であれば、ウイルスの定義データベースの「シグネチャ」に頼っていた部分も、多種多様なマルウェアが出てきて、振る舞い検知をするようなツールも使用しないと対処しきれなくなりました。
過去のとてつもない量のマルウェアの行動パターンを学習し、瞬時にマルウェアの侵入を判断するためには機械学習による AI の技術が有効であることは間違いありません。これは、脆弱性が発見されてから修正プログラムやパッチが作成される前にその脆弱性を突いた攻撃を仕掛ける「ゼロディ攻撃」についても有効です。しかしながら、ゼロディ攻撃は、サイバー攻撃の中でも高度な標的型の ATP 攻撃と組み合わせて行われることが多いため、サイバー戦争と言われているように、セキュリティを守る人と、マルウェアで犯罪を犯すクラッカーとのネット上の対決が日々行われています。
たとえば、近年のアンチウイルスソフトウェアでは、ヒューリスティックエンジンを搭載したものが増加してきています。つまり、必ず間違いないと判断できるわけではないけれど、ある程度のレベルで正解に近い解を得ることができる方法であるため、確率的にマルウェアだという疑わしい行動について、迅速に発見することができます。
これを AI を使って更に学習量を圧倒的に増やしていったとしても、既知の脅威に対する行動なので、犯罪者は逆にセキュリティソフトに対しどのような行動をすれば、防御されてしまうかを AI で学習しています。
ネット犯罪者は、犯罪によって得たお金であらゆるセキュリティ対策ソフトを購入し、どうしたらその対策をくぐりぬけるかという研究を常に行っているといわれています。
セキュリティソフトが、犯罪を犯す特有の行動を分析しているのに対し、犯罪者は、その標的とする企業へ侵入してデータを入手、あるいは破壊という目的を達成するために、いかに正常な行動であるかのように振舞えるかを AI を使って研究しています。この攻防がいたちごっこであるため、企業が正常に行っている業務処理でさえ、セキュリティソフトによって止められてしまうリスクが生じてしまうことも気を付ける必要があります。