日刊工業新聞
年月日 18 09 28 ページ 13 NO.

ICT 世界の潮流 PART6 11

セキュリティー分野での先端技術の関わり㊦

サイバー攻撃 官軍民で備え

強国を訪問

サイバーセキュリティー分野において人工知能（AI）などの先端技術はどのように利用されているのか。現状を知るため、6月にサイバーセキュリティー強国と言われる英国とイスラエルを訪問した。

「今のところAIは、我々の味方です」。英国の国家サイバーセキュリティーセンター（NCSC）の担当者は、サイバーセキュリティー分野のAI利用について、こう語った。NCSCでは英国内から集まる膨大な情報処理にAIを利用しており、非常に役立っているという。

一方で、当面、サイバー犯罪者による悪用は既存攻撃の自動化など限定的とみる。この理由として、多くのサイバー犯罪集団は経済的な活動を営んでおり、AIよりも安価で確実な方法を持っている点を挙げた。つまり経済性を重視するサイバー犯罪者にとって、まだAIの利用価値は低い。なお、こうした考察はNCSC内の多様な分野の専門家チーム（社会経済、心理学、コンピューター等）によるもので、技術偏重になりがちな日本のロールモデルになる。

国際社会経済研究所（NECグループ）主任研究員
小林 憲司

AIの悪用

もちろんNCSCも含めて多くの専門家は、近い将来、AIの悪用は起こると予想する。その中で、AI自体がサイバー攻撃のターゲットとなる懸念が高まっている。例えば偽データによる誤動作（敵対的攻撃）や、訓練データの同定（推論攻撃）などがある。こうした悪意のある行動の研究に取り組んでいる。とても難しいテーマで、関連する学術論文はわずか3件しかないという。今の機械学習は結果説明が難しい上に、動作を保証する術がない。同教授は「現状のAIは、安全が重視される分野に利用すべきではない」と警鐘を鳴らす。AIの社会実装は、技術的な限界を十分に理解した上で、慎重に進める必要がある。

ベエルシェバのサイバーAI研究開発拠点「CyberSpark」は、機械学習が持つブラックボックスのため、検知は難しい。インペリアル・カレッジ・ロンドンのロムシオー教授は1年半前から機械学習システムの動作検証の研究に取り組んでいる。

リスク犯す

こうした高度なサイバー攻撃に備えて、サイバー強国では官軍民が一体となった研究開発が進む。イスラエルでは南部の都市ベエルシェバに国家サイバー局、国防軍の諜報部隊・IT部門、国内外のIT企業、大学が同じ敷地内に集結する。ネタニヤフ首相は、「（軍事機密の漏えいといった）国家安全保障上のリスクはあるが、リスクを犯さないとサイバー犯罪者の先には行けない」と取り組みの必要性を説く。訪問した施設では、あらゆる手段でハッキングする研究開発の説明を受けた。明らかに諜報部隊での実践経験が強みになっている。残念ながら日本にはこうした環境はない。次回はブロックチェーン（分散型台帳）の利用について紹介したい。

（金曜日に掲載）