2020 年 11 月

SoC1196

Specters of Indiscriminate Data Use

By Martin Schwirn（Send us feedback）

データ濫用の悪影響

2020 年 11 月の『SoC1192：データキャプチャーの自動化』と『SoC1194：データ利用の自動化』では、データのキャプチャー・処理・利用の自動化による潜在的メリットと使用例を論じている。こうしたデータ操作の自動化で更に多くの産業や企業に多様なデータが提供され、データが常に利用できるようになれば、サービスやオペレーション、アプリケーションの改善につながる。しかも、データ操作の自動化が標準化すれば、アプリケーションはリアルタイムの情報で継続的にサービス・機能が調整可能になる。可用性とコネクティビティが向上し、自動かつユビキタスなデータ利用システムの構造が出来上がると、大多数の商用アプリケーションがその上で機能することになると考えられる。そのメリットははかり知れない。たとえばこのシステムでは、変化する環境要因や消費者の嗜好に応じてサービス・機能を常に更新していく。セキュリティや安全性のアプリケーションでいえば、データの流れの常時監視により、新たな安心感のレベルがもたらされる。消費者側のインプットが最小限に抑えられ、企業は従業員の数を減らしてシステムやインフラの運営にあたることができる。とはいえ、データ提供・利用システムの自動化や自律性がこのように進展すると、少なからぬ問題も生じてくる。それらはデータ準備における単純なミスのことも、システム全体に不具合を連鎖させる場合もある。まぎらわしいデータ使用で最適な操作が行われない、あるいは特定の人口区分に不利益が生じることもあれば、犯罪者が接続性の向上に乗じ、自動化された操作をこっそり悪用する場合もある。

可用性とコネクティビティが向上し、自動かつユビキタスなデータ利用システムの構造が出来上がる。

『SoC1194：データ利用の自動化』が高まるエネルギー状況に対する、データ利用自動化の利点を論じた箇所がある。しかし、そうしたシステム間の相互接続や、サブシステムとインフラ全体の調整の容易化は、犯罪者があれこれと利用できる危険な経路を開くことにもなる。ジャーナリストのテッド・コッペルは 2015 年 10 月の『Lights Out: A Cyber Attack, A nation Unprepared, Surviving the Aftermath （停電：サイバー攻撃と無防備な国家 影響を切り抜ける）』で、米・電力網へのサイバー攻撃は可能かつ起こりうるが、米国はそうした事態への備えが全くできていないと主張している。この本の出版からわずか 2 か月後の 2015 年 12 月、ロシアのハッカーがウクライナの電力網を攻撃して 60 万世帯以上への電力供給を切断した可能性があり、多くの専門家は電力網に対する初の大規模サイバー攻撃と捉えている。2018 年 3 月には米・国土安全保障省（DHS）と連邦捜査局（FBI）が、米政府機関やエネルギーインフラに対する国家主導の攻撃について警告を発した。DHSとFBIは、ロシア政府が主導した行為者が複数の商業施設にスピアーフィッシングや計画的マルウェアをしかけたとしている。最終的にその攻撃者はシステムに侵入し、産業用制御システムに関するデータを入手しているので、今後の攻撃に使われるおそれがある。

デバイス間の接続性が向上し、悪意の行為者がさらに高度な攻撃をしかけられるようになっている。シンガポール National University of Singapore と New York University Abu Dhabi（アラブ首長国連邦）の研究グループは、ソーシャル

メディア・ネットワークを通じてユーザーのエネルギー消費行動が変更できると主張している。たとえば、消費者がエネルギー使用をピーク時に変えたくなるような偽のディスカウント通知を悪意の行為者がネットワークにばらまくとしよう。そうしたピークの時間帯は僅かなエネルギー使用の増加で電力網がダウンし、停電する可能性がある。また米国 Georgia Institute of Technology の研究チームは、さらに高度な攻撃を想定している。犯罪者が電力網を麻痺させる代わりにそれを利用し、エネルギー需要を変えて価格操作による金銭的利益を得るものだ。この手の攻撃では、犯罪者はボットネット（単一または複数のボットを実行する接続機器のネットワーク）を使い、電気自動車の充電器やエアコン、給湯器といった、消費電力の高いネット接続機器の使用を増大させる。そうして電力需要を変え、最終的な電気料金の差額で得をするのである。こうした攻撃は、誰かが気づくまで長期間にわたって行われないとも限らない。

それ以外の問題（たとえば一部の AI システムが特定の人口集団に偏見を持つこと）については、メディアでかなり取り沙汰されている。顔認識システムが広く報道されたおかげで、米国 Amazon.com は顔認識プラットフォーム Rekognition への警察のアクセスを一年間保留すると発表した。データ利用をめぐる問題は、はるかに分かりにくい形で広範囲に拡がり、危険を伴う可能性さえある。たとえば米国 Harvard Medical School を中心とした研究チームは先日、New England Journal of Medicine に「Hidden in Plain Sight−Reconsidering the Use of Race Correction in Clinical Algorithms（隠れているようで明白なこと 臨床アルゴリズムにおける人種修正利用を見直す）」を発表した。胸部手術、腎臓提供、帝王切開といった医療上の判断に広く用いられている複数のアルゴリズムに人種偏向があり、黒人患者の治療の質に悪影響を及ぼしていることが明らかになった。さらに米国の Harvard University と Massachusetts Institute of Technology（MIT）の研究チームは、医療の機械学習システムが敵対的攻撃に脆弱な可能性を指摘している。何者かが改ざんデータを入力するとアウトプットが大きく変更され、システムは誤った結果を出すしかなくなるという。ハッカーがこうした攻撃で誤診を引き起こすおそれもあるが、さらに懸念されるのは医師や病院、医療機関が請求書作成ソフトや保険ソフトの AI を操作し、自らの金銭的利益に利用する可能性があることだ。今後ますます多くの医療管理アプリケーションが自動で情報を引き出すようになっていくだろう。つまるところ、自動化はコスト削減につながるからだ。が、そのような自動化は悪意ある行為の温床にもなっている。システムがいっそう自律的に情報を要求するようになるにつれ、その監視を人間が行うのは不可能ではないものの、難しくなっていく。

データの要求・利用の自動化でオペレーションが加速度的に変化し、データ運用の自動化がますます一般化するなか、大きな問題となる課題がある。たとえばイタリアの University of Bologna の経済学者のグループは、2 つの自律的な強化学習型価格設定アルゴリズムを制御環境下においたところ、あっという間に結託し始めたと報告している。アルゴリズムが互いの行動への反応を学習し、個々に作動した場合よりも高く商品の価格を設定したのだ。こうしたアルゴリズムに基づく行動は、共謀法（collusion laws）の観点からで問題となる可能性がある。

SoC1196

本トピックスに関連する Signals of Change		関連する Patterns	
SoC1194	データ利用の自動化	P1388	AIが負うべき過失責任
SoC1192	データキャプチャーの自動化	P1310	デジタル化の痛み
SoC1104	ビッグデータの限界に注意	P1291	AIの論理を理解する必要はあるか?