STRATEGIC BUSINESS INSIGHTS

FORESIGHT

2022 年 6 月

SoC1308

Privacy Tech

By Rob Edmonds（Send us feedback）

プライバシー技術

デジタル技術はデータを糧として発展するが、規制当局や多くの消費者はプライバシーを求めている。現在のところ、ステークホルダーは技術の進歩とプライバシーに関する懸念のバランスを取る必要がある。高度なプライバシー技術はこの状況を変え、大規模なデータ処理と堅牢な個人のプライバシーを共存させることができるかもしれない。研究者は、準同型暗号化、連合学習、量子暗号化技術など、変革を生み出す可能性があるプライバシー技術を進展させている。プライバシー技術が飛躍的に進歩すれば、特に医学研究などのプライバシーに敏感な分野で、研究者は AI トレーニングデータにアクセスしやすくなるだろう。従って、プライバシー技術の進歩は AI や社会に大きな影響を与える可能性がある。

研究者は、準同型暗号化、連合学習、量子暗号化技術など、変革を生み出す可能性があるプライバシー技術を進展させている。

高度なプライバシー技術は、広範におよぶ商用前の個人データに関連するサイバーセキュリティ技術の一端をなす。以下に現在のプライバシー研究分野の例を示す。

- 完全準同型暗号（FHE）は、いつの日か革命的なプライバシーソリューションになる可能性がある。IBM はすでに実証試験を実施しており、Intel Corporation、Microsoft、米国国防総省の DARPA（Defense Advanced Research Projects Agency）は、FHE 処理を高速化するハードウェアを開発している。少なくとも理論的には、FHE を利用すればコンピュータは暗号化されていないデータに対してできることは何でも、暗号化されたプライベートデータに対してもできるため、このアプローチは革新的であるかもしれない。しかし、FHE のデータ処理とメモリに関わるコストは従来のコストを大きく上回るため、新しいハードウェアの登場は重要である。例えば、IBM のテストでは、FHE で暗号化された機械学習モデルは暗号化されていないモデルに比べて、同じタスクを実行するのに 40～50 倍の計算能力と 10～20 倍のメモリが必要であることが明らかになった。パフォーマンスのトレードオフにより、初期の FHE アプリケーションは、金融サービス、ヘルスケア、政府などの極めてプライバシーに敏感な業界に限定されるだろう。しかし、専用チップが登場し、FHE 技術が進化するとともにトレードオフは縮小する可能性がある。
- AI のための連合学習システムは、AI トレーニングのタスクを個別のモジュールに分割し、それをローカルデバイスに配布することでプライバシーを保護しようとするものだ。例えば、個人の電話に AI トレーニングに必要なデータが含まれている場合、モジュール化された機械学習のトレーニングシステムは、その電話自体のデータを使用することが可能でデータをクラウドにアップロードする必要がない。システムはトレーニング済みの AI モジュールのみをアップロードする。連合機械学習ソフトウェアを開発している主要企業には Google、IBM、Intel、Microsoft が名を連ねる。しかし、このアプローチはまだ不完全であり、技術者は、共有されるモデルの更新や平文での部分的なデータ集約などのソースから間接的なデータ漏洩のリスクがあると報告している。一方でますます高度な連合学習アプローチが出現している。例えば、École

Polytechnique Fédérale de Lausanne の研究者は、部分的な準同型暗号を使用して（かなり）効率的なエンドツーエンドのプライバシー保護を提供する連合学習システムを開発したと主張している。量子鍵配送（QKD）は量子力学の原理を使用して、機密性を損なうことなく暗号鍵を共有することを目的とする。暗号化された通信では、受信者はデータのロック解除に鍵を必要とするが、鍵を共有すると転送中に紛失または盗難に遭う危険性がある。量子力学に固有の不確実性は、この問題を克服できる方法を提供する。QKD によるアプローチは、英国のオックスフォード、ドイツのミュンヘン、中国の上海の研究者らによる 3 つの個別の実験で使用されたものを含むが、光子やその他の物理的特性に依存しているため、特定のハードウェア（光ファイバーなど）が必要である。

- 耐量子暗号は、新しい数学的技術およびソフトウェア技術を使用して、大規模な量子コンピュータの出現が現在の暗号化システムにもたらす脅威を克服することを目的とする。そのようなコンピュータがいつ出現するのか、そして実際に出現するかどうかさえも非常に不確実なままである。しかし、そのようなコンピュータが出現すれば、現在広く使用されている多くの暗号形式を破ることができるだろう。

高度なプライバシー技術は、今後数年以内に一部の商業市場（例えば、金融や医療研究市場）に参入する可能性が高い。高度なプライバシー技術が開発されているにもかかわらず、サイバー攻撃技術はサイバー防御技術とともに進歩しているため、おそらくいずれ完璧なデータセキュリティを達成することは不可能だと判明するだろう。しかし、状況の変化は別の結果を引き起こす可能性がある。高度なプライバシー技術開発の将来を変える可能性のある開発の例を以下に示す。

◆ プライバシー管理の自動化

高度なプライバシー技術の躍進と普及により、プライバシー問題が本質的に自動化されることは、あり得ることではあるが不確実な展開である。そのような未来において、ビッグデータはプライバシー規制や懸念に妨げられることなく、ようやくその潜在能力を発揮することができる。プライバシーの問題がデジタルトランスフォーメーションの目標を鈍らせるのを目の当たりにしてきた企業は、積極的なデジタル戦略を実装することができるだろう。

◆ AI の飛躍的進歩

連合学習や FHE 技術などの高度なプライバシー技術が急速に進歩すれば、機械学習はこれまで利用できなかった貴重なデータに幅広くアクセスでき、その結果大きな進歩が見られる可能性がある。

◆ 量子コンピュータの飛躍的進歩による暗号化の無用化

大規模な量子コンピュータは今日でも依然として理論上のものであり、そのようなコンピュータが今後 10 年で登場する可能性は非常に低い。しかし、影響が大きく不確実性の高い展開として、今日広く使用されている多くの暗号形式を破ることができる量子コンピュータの予期せぬ登場（例えば、敵対的な国から）が考えられる。高度な量子コンピュータが登場するまでに、現在の暗号形式が量子耐性に進化したとしても、官民の関係者は、量子に対して脆弱な暗号化プロトコルが保護するプライベートデータの膨大なキャッシュを、しばしば違法に取得して保存している。これらの大量のデータは、十分に強力な量子コンピュータが登場した場合、量子復号化に対して脆弱になるだろう。

SoC1308

本トピックスに関連する Signals of Change		関連する Patterns	
SoC1198	データ利用におけるプライバシーの自動化	P1746	ハッキングの未来: 悪化の一途をたどる・・・
SoC1196	データ濫用の悪影響	P1671	ランサムウェアとの闘い
SoC946	ハッキングとDDoS攻撃の拡散	P1144	セキュリティの自己満足