秘密計算でセキュリティを守る

◆物流センターの無人化を担う要素技術として実用化へ

2020年3月3日、椿本チエインは物流センターの無人化を担う要素技術として、AIを駆使した高速・高精度「AI画像認識技術」を開発したと発表した。今回の新型コロナ対策の外出自粛により、eコマース市場での物品購入が増加し、物流量増大に対応するため、人手不足解消や労働時間短縮はますます重要になる。入荷、検品、在庫管理、棚卸、梱包などの各工程における省人化・無人化ニーズが高まっており、特に倉庫内でのピッキング作業での効率化が求められている。

これらの状況に対応するため、椿本チエインはバーコードレス・ピッキング工程の無人化をターゲットに、仕分け対象商品の形状・色・模様等を画像認識し、高速・高精度で属性を認識する「AI画像認識技術」の開発を着手した。AIスタートアップ企業のEAGLYS（イーグリス）との協業により開発した「AI画像認識技術」は、商品認識において超高速（0.15秒以下）かつ高認識率（98.55%）、高正解率（99.99%）を達成している。

◆ビッグデータを活用するために重要なセキュリティ技術

EUで制定されたGDPR（一般データ保護規則）では個人データの域外移転禁止と処理に対しては安全管理措置をして保護することが要求されている。ビッグデータの活用が期待されている領域で個人データが必要なのは、車の自動運転、スマートシティ、物流、スマートファクトリーなどが考えられる。いずれも個人データが重要で、セキュリティ対策が必須であることから、ビッグデータ活用とセキュリティの両立は大きな課題となっている。たとえば、物流においては、配送物の住所、氏名等の個人データの保護が求められ、暗号化などの対策は必須となる。

情報のセキュリティを強化する方法は以前から取り組まれており、データの通信や保存時にデータを暗号化して保護するものであった。しかしながら従来の手法では、処理する直前に利用するデータを復号化して計算する必要があった（図１①）。社内ネットワークのようにセキュリティが強化されているローカルな環境で処理するケースでは、このような手法でも問題ない。

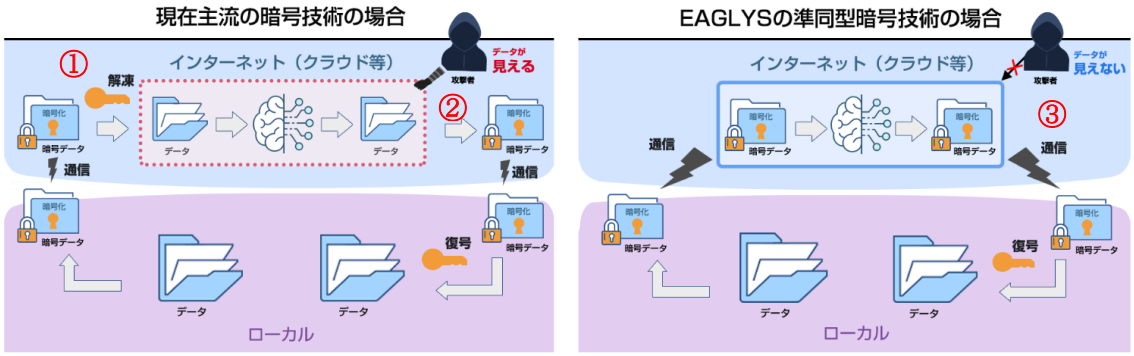

図１　秘密計算技術を用いたビッグデータ分析手法

出典：https://eaglys.co.jp/technology/

近年クラウドでのデータ処理が主流になり暗号化技術でデータを保護しても、データを処理する直前にデータを復号化するため、データ処理時に管理者権限を持っていれば、攻撃者にデータを入手されるリスクがあった（図１②）。

この問題を解決したのが、EAGLYSの秘密計算技術である。秘密計算とはデータを秘匿したまま計算する技術で、準同型暗号という特殊な暗号を使うと、暗号化したまま計算できる。EAGLYSはAIのビッグデータ分析に必要な、AIモデル、データ分析アルゴルズム、業務データベースの全てに格子暗号をベースとする準同型暗号を活用した秘密計算エンジン「CapsuleFlow(カプセルフロー)」を開発しており、データを暗号化したまま計算するので、入力データに加えデータを処理する過程やモデルのパラメータも保護することが可能となった（図１③）。

◆秘密計算技術でセキュリティが確保されビッグデータ活用が進む

従来秘密計算はメモリと計算時間で実用化が難しかったが、暗号データに関する演算処理の高速化や省メモリ化の研究成果で、実用化に目途を付けた。

全ての処理を暗号化で実行できる秘密計算は、より安全なデータ処理はもちろんのこと、今まで異なる組織が保有するさまざまな機密データ（企業の秘密情報、個人データ等）を相互に開示せずにデータを統合・分析することができる。この特長は、企業や組織の枠を超えた新しい価値創出が可能な技術であることを示す。

そのため、NTTやNECなど多くの会社で高速化に向け開発が進められている。

今後、各企業の社員の健診データと病院のレセプトデータの共有をすることによる医療と検診データの関係分析や生活者・社会データのマーケティング活用など、ビッグデータの活用で新サービスが生み出されることが期待される。　【成田誠】