CM-005

軽量 N パーティ秘匿関数計算を用いた安心・安全な次世代分散システムの構成

情報銀行，IoT，IFoT，エッジコンピューティング，ブロックチェーンの基盤

Design of Safe and Secure Next Generation Distributed System Using Lightweight N-party Secure Function Evaluation

Infrastructure for Information Bank, IoT, IFoT, Edge Computing, Block Chain

藤田　茂‡　滝 雄太郎§　白鳥則郎†　宮西洋太郎※
Shigeru Fujita　Yutaro Taki　Norio Shiratori　Youtarou Miyanishi

1. はじめに

情報システムに蓄積される情報量の増加は著しく、また利用に対する要求は増す一方である。しかし、その情報を狙った悪意ある攻撃や不注意や不作為によって、その情報が流出する、悪用される、拡散されるという問題が発生している。このため、個人情報の取得あるいは保存について、各個人が不安を感じ、自分の情報を不用意に取得されたくない、インターネット上の情報は安全でないと感じている。

一方で、Society 5.0 に代表されるように、Internet Of Things: IoT とクラウドサービスの連携により、新たな価値を創造する、スマートなサービスを実現したいという要求があり、匿名化処理によって個人に由来する情報が自由に流通する状況が到来している。

本稿では、利用者に安心・安全なサービスを提供し、円滑なサービス構築を実現する Society 5.0 のための次世代分散システムの構成を示す。

2. 背景

これまで情報の保護を実現するために、中央集権的なセキュアなサーバを構築する手法[1]が取られてきたが、個人の情報を他人に委ねたくないという要求、また高セキュアなサーバであっても内部の管理者による操作には無防備であることから、個人が管理するサーバあるいはスマートホンなどの個人が所有する装置へデータを蓄積する手法も検討されている[2]。

個人の責任において、個人が管理する装置に個人の情報を保存することに、個人の心理的な抵抗は少ない。一方で、装置に情報が蓄積されていることから、紛失や装置への不正なアクセスによって、情報が流出する恐れがある。すでに個人宅から廃棄された HEMS 装置から、無線 LAN のパスワードが流出する恐れがあることが指摘されている[3]。

情報銀行では、個人の購買履歴や位置情報を匿名化し、その情報をあたかも財のように考えて、財の流通を促進することで Society 5.0 に代表される新たな価値の創造を実現しようとしている[4]。文献[4]では技術的課題として、(1)分散型セキュアストレージ、(2)預託されているパーソナルデータの可視化と指標化、(3)データアナリシスクラウドファンクションが指摘されている。

情報処理技術への期待として、完全な安心・安全を求める利用者が存在することは容易に想像できるが、一方でハードウェアの故障あるいは、不法行為によって、情報が流出することは根絶できないとしないと実際のシステム構築やサービス提供は困難である。

文献[8]では、オペレータ等のサービス提供側の内部に不法行為を行うものがいる場合を含めて、安心・安全の定量的な評価手法を提案しており、この指標を拡張して情報システムの安心・安全度を見て、利用者がサービスの利用を決定することが可能になる。

コンテンツの販売や貸与を行うサービス事業者にとって、違法コピーの流通が大きな課題となっている。デジタル化されたコンテンツは、複製が用意であり、個人が利用できるストレージの大容量化とインターネットの広帯域化もあいまって、今後も大きな課題であると思われる。

複製と流通が容易であるというデジタル化された情報の特徴は、コンテンツサービス事業者のみならず、個人にとっても脅威となっている。例えば、不用意に SNS に掲載した写真が転載を繰り返されて、個人の意図しない範囲へ拡大することや、削除したいと思ったとしても、完全な削除は困難であることが良く知られている。

複製の検出を目的として、電子透かしが研究開発されている。電子透かし技術を使うことによって、複製されたデータの検出が行える。また情報を意図的に劣化させて、電子透かしによって埋め込まれた情報を無効化しようとする試みへの対応が研究されている。

IoT の普及によって、IoT 装置から送出されるデータは飛躍的に増加し、そのすべてのデータをクラウドへ集めることは、ネットワーク帯域の制約から困難である。この制約に対して、エッジコンピューティング[9]、フォグコンピューティング[10]、Information Flow Of Things, IFoT[11][12]が提案されている。

ビットコインに代表される仮想通貨では、ブロックチェーンにより取引記録の信頼性を担保する。ブロックチェーンは、中央サーバを置かずに取引記録の真正を保証できるので、仮想通貨のみならず、都市銀行や大学において利用実験が始まっている。

3. 情報システムに対する要求

2 章、背景で述べた事柄から、情報システムに対する安心・安全の評価を上げための要求事項を以下に列挙する。

1. 情報を個人が登録・削除・利用のコントールを行いたい
2. サーバー一か所にデータを蓄積することはしたくない
3. 1 の要求に関わらず、不法な情報を削除する方式を確保したい

‡千葉工業大学情報科学部情報工学科
§ 千葉工業大学大学院情報科学研究科
†中央大学研究開発機構
§ ISEM Inc.

4. 故障・障害に対する耐性を高くしたい
5. 秘密分散によって分散されたデータであっても削除が行えること

次章以降で、これらの要求を実現するための技術を検討する。

4. 軽量 N パーティ秘匿関数計算

情報を複数の主体（例えばサーバ）にランダムに分割したものを分散して配置し、分散したまま計算を行う、秘密分散・秘密計算の研究が行われている。我々は先行研究[5]で示された 3 パーティ秘匿関数計算の一般解を導出し、2-out-of-3 に限らず、k-out-of-n という任意の主体数を利用できることを示した[6][7]。

一般解では n が奇数の場合、$n \geq 2k-1$。n が偶数の場合、$n \geq 2k$を満たす必要がある。この結果、安心・安全性とのトレードオフで主体数を任意に設定することができる。

この軽量 N パーティ秘匿関数計算に基づいて、データを分散保存利用する分散ストレージを構成する。

5. 情報銀行

個人の購買履歴や移動履歴を保存し、匿名化処理を行った上で、そのデータを企業等へ提供し、見返りとして、企業等から、個人へポイント付与等のサービスを行う情報銀行が実証実験に入る[13]。情報銀行の法整備は 2018 年が計画されている。情報銀行は構想段階のモデル(図 1)から、検討を経て中央集権的な行政機関による中央集権的ストレージという概念から、個人のクラウドサービスあるいは、マイナンバーポータル（マイナポータル）を併用する形式もありえるという形(図 2)へ変わってきた[1][2]。

5.1 情報銀行の利用イメージ

情報銀行にはいくつかの利用シナリオが想定されている。ここでは、これまでの利用シナリオや、本稿で想定する安心・安全な、信託局を介した完全分散型パーソナルデータストア（6 章）を利用した場合のシナリオを示す。

いかなる場合でも購買情報や位置情報を提供したくないという利用者が一定数いることと、特に位置情報は日本人の 6 割が提供したくない、という調査がある。しかしながら、将来、安心・安全性の評価が定量的に行なわれるようになり、情報を提供することで得られる利点との比較が容易に行われると、この調査結果が変わることを期待している。

5.1.1 映画館でのシナリオ

映画館で映画を見ようとしている。映画館から情報の提供が、スマホ上のアプリから求められる。

「この映画をどちらで知りましたか？」「こちらにいらした交通手段を教えていただけますか？」「性別と年代を教えていただけますか？」「どなたかとご一緒ですか？」「この後、お食事をされる予定ですか？」「過去にみた映画を教えていただけますか？」「映画を見終えた後に、5 段階で評価していただけますか」

『お答え頂いた回答数に応じて入場料を最大 1000 円引きいたします』

いくつかの情報を提供した結果、入場料は 800 円引きとなった。

5.1.2 食料品購買時のシナリオ

いつものスーパーマーケットで、食料品を購入する。レジを通過した後に、ポイントの付与が行われる。いつも使うスーパーマーケットなので、質問にはあらかじめ答えている。「性別、年代」は提供する。「どのような商品を買ったのか」は提供しない。「商品購入額」は提供する。「商品購入時間」は提供する。

5.1.3 家電量販店のシナリオ

たまに行く、家電量販店でプリンタを購入する。初めて訪れた時に、情報提供範囲を決定している。「商品購入額」は提供する。「性別、年代」「商品名」「商品種別」は提供しない。

5.1.4 信託局を介した完全分散型パーソナルデータストア（1）

6 章の信託局を介した完全分散型パーソナルデータストアによるシナリオ

個人が 5.1.1-5.1.3 の履歴を破棄したいと考える。信託局に預けた鍵と対になる公開鍵を廃棄する。これにより、分散サーバ上に残ったデータを集めたとしても、データが復元できずに、5.1.1-5.1.3 の履歴データが利用できなくなる。

5.1.5 信託局を介した完全分散型パーソナルデータストア（2）

6 章の信託局を介した完全分散型パーソナルデータストアによるシナリオ

個人が著作権者によって複製が許可されてないデータを不法に分散サーバ上へアップロードする。著作権者は電子透かしや分散されたデータのハッシュ値を信託局へ預けている。この結果、データがアップロードされると、好ましくないデータとして識別され、個人に対してデータのアップロードが許可されていないことが通知される。

5.2 軽量 N パーティ秘匿関数計算による分散ストレージ

情報を一か所に集約せずに、個人クラウドやマイナポータルから得られる情報も利用可能にするという変更（図 1 から図 2 への変更）は、個人の特定につながる情報を預けたくない、情報を預ける部分を増やしたくない、という個人の意向を反映したと思われる。

しかし、ストレージの利用が一か所に固定されるのであれば、依然として一か所の脆弱性によって情報が漏洩することから、安心・安全の向上には寄与しない。そこで、文献[7]によって示した、軽量 N パーティ秘匿関数計算による分散ストレージを構成する(図 3)[7]。

この構成によって、攻撃者によって一つのストレージ（文献[7]の用語に従うと、主体）から、情報が流出したとしても、情報を復元することができず、安心・安全性の向上に寄与する。

一方で、保存されている情報の削除や、情報の有効期限を与えることは達成されていない。この対応のために、三者間公開鍵暗号を導入する。

6. 信託局を介した完全分散型パーソナルデータストア

情報を個人がコントロールし、かつ社会の要請によって流通している不法なデータを削除したいという相反する要

求を同時に満たす必要がある。このため、三者間公開鍵暗号方式を用いる。

中央集権的なストレージでなく、分散したサーバを使ってデータを保存するために、軽量 N パーティ秘匿関数計算を用いる。

各サーバ上のデータとそのデータの利用履歴の信頼性を担保するために、ブロックチェーン技術を使う。

情報に対する有効期限を設定するために、必要であれば時限暗号を用いる。

各サーバに分散されたデータは、ハッシュが付与され、信託局に鍵とペアでハッシュ値が保存される。データに対して、トレーサビリティを維持するために、電子透かしを付与する。この結果、

ハッシュ値とデータに対する公開鍵を信託局に預けることによって、個人が違法に分散ストレージに保存したデータを削除したり、他人が複製したデータを個人に無許可あるいは違法に分散ストレージに保存された場合に検出することが可能になる。

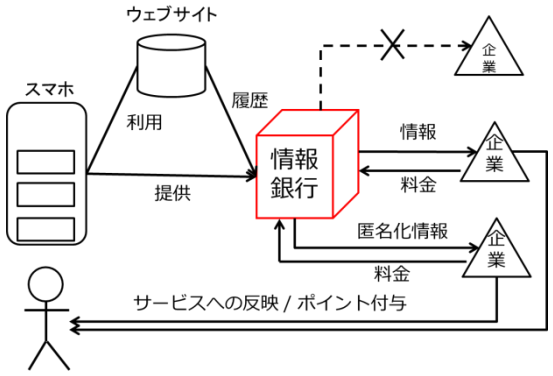

図 1 情報銀行のイメージ

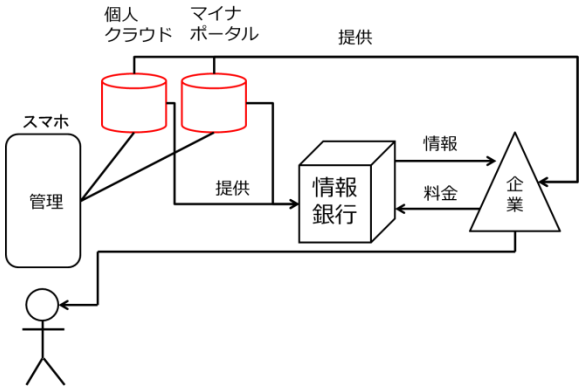

図 2 情報銀行のストレージイメージ

7. おわりに

本稿では、Society 5.0 を踏まえて、安心安全な情報システムを構成するための手法を検討した。検討した手法のなかでは、軽量 N パーティ秘匿関数計算を基盤として、ブロックチェーン、三者間公開鍵暗号、電子透かしと複数の技術を組み合わせて、ネットワーク上に展開されるデータを個人と信託局が利用を制御できるようにした。

信託局が信頼できるのか、という課題が技術的にはあるが、社会的な同意をえるためには、裁判所命令等の法的根拠をもって操作を行い、その操作記録もまた、分散ストレージ上に保存し、のちの検証に耐える記録を残すことが望ましい。

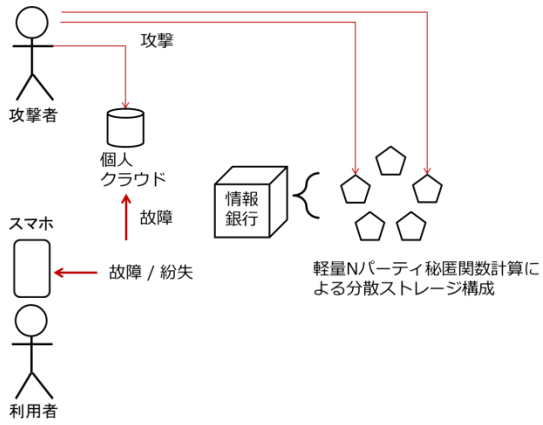

図 3 軽量 N パーティ秘匿関数計算による分散ストレージ

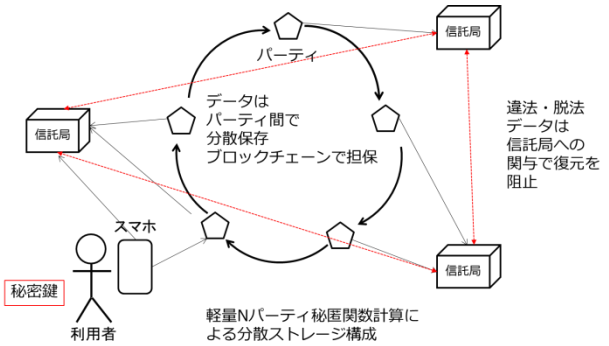

図 4 信託局を介した完全分散型パーソナルデータストア

参考文献

[1] 官邸，第 2 回 データ流通環境整備検討会 議事次第，2017 年 3 月 15 日，http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/ siryou1.pdf , p.6 (last access, 2016/05/20)

[2] http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/pdf/010_02_00.pdf, p16 (last access, 2016/05/20)

[3] HEMS のローカルデータストレージの漏洩，http://r00tapple.hatenablog.com/entry/2017/06/28/122156 (last access, 2016/06/28)

[4] 砂原秀樹、山内正人、金杉洋、柴崎亮介、「情報銀行」構想とその技術的課題、情報処理学会 DICOMO2014，pp.1024-1026,(2014)

[5] 千田浩司、五十嵐大、濱田浩気、高橋克己、エラー検出可能な軽量 3 パーティ秘匿関数計算の提案と実装評価、情報処理学会論文誌, Vol.52, No.9, pp.2674-2685, (2011)

[6] 滝雄太郎、藤田茂、宮西洋太郎、白鳥則郎、k out of n 秘密計算プロトコルの一考察、情報処理学会研究報告、マルチメディア通信と分散処理(DPS)、Vol.2016, No.5, pp.1-7 (2016)

[7] 滝雄太郎、藤田茂、宮西洋太郎、白鳥則郎, 軽量 N パーティ秘匿関数計算の一般解と情報銀行の分散型セキュアストレージサーバへの応用、情報処理学会, マルチメディア，分散，協調とモバイル(DICOMO2017)シンポジウム, pp. 779-784 (2017)

[8] 宮西洋太郎、韓嘯公、金岡晃、佐藤文明、北上眞二、浦野義頼、白鳥則郎、セキュアマルチパーティ秘密計算法におけるユーザ安心感定量化の試み～情報システムの「安信性理論」の確立を目指して～、情報処理学会、研究報告マルチメディア通信と分散処理（DPS）、No.41, pp.1-6, (2015)
[9] Arif Ahmed, Ejaz AhmedA survey on mobile edge computing, , IEEE Intelligent Systems and Control (ISCO), pp. (2016)
[10] http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf (2015), (last access 2017/06/20)
[11] Keiichi Yasumoto , Hirozumi Yamaguchi , Hiroshi Shigeno, Survey of Real-time Processing Technologies of IoT Data Streams, 情報処理学会論文誌, Vol.52, No.2, (2016)
[12] https://ubi-s13.naist.jp/ifot2016/, (last access, 2017/06/20)
[13] http://www.nikkei.com/article/DGKKASFS23H1L_T20C17A2EA1000/, (last access, 2017/06/20)
[14] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf, (last access, 2017/06/20)