BOJ Reports & Research Papers

決済システムレポート別冊シリーズ

Payment and Settlement Systems Report – Annex

プライバシー保護技術と
デジタル社会の決済・金融サービス

日　本　銀　行
決 済 機 構 局
2022 年 9 月

（決済システムレポート別冊シリーズについて）

日本銀行は、決済システムの動向を鳥瞰し、評価するとともに、決済システムの安全性・効率性の向上に向けた日本銀行および関係機関の取組みを紹介することを目的として、「決済システムレポート」を定期的に公表している。

「決済システムレポート別冊シリーズ」は、決済システムを巡る特定のテーマについて、掘り下げた調査分析を行うものである。今回は、プライバシー保護技術をテーマに考察する。本稿は、日本銀行が 2020 年 10 月に公表した「中央銀行デジタル通貨に関する日本銀行の取り組み方針」において、今後の制度設計面の検討項目のひとつとして掲げた「プライバシーの確保と利用者情報の取扱い」にかかる検討の一環として取り組んだものである。

【本レポートに関する照会先】
日本銀行決済機構局決済システム課　（post.pr@boj.or.jp）

2022 年 9 月
日 本 銀 行
決 済 機 構 局

プライバシー保護技術とデジタル社会の決済・金融サービス

■要　旨■

近年、国内外において、事業者が顧客データを収集することで多くのサービスが生まれており、決済・金融サービスの領域でもデータの利活用は事業展開の重要なモチベーションとなっている。また、近年、決済にかかる AML/CFT の重要性の認識が高まっており、国際的な議論が進められている。AML/CFT を高度化し実効性のある仕組みを整えるためにも、データを活用することが重要となってきている。こうした状況を背景として、データをビジネス創出や健全な取引の実現に用いつつ、利用者のプライバシー保護に資する技術が発展を見せている。

具体的には、個人が特定されないようにデータを変換する「匿名化」や、ノイズを加えるなどして分析結果からの識別可能性を抑制する「差分プライバシー」の考え方が挙げられる。他にも、データを秘匿した状態で分析を行う「秘密計算」や、ハードウェア技術を用いて計算処理を機密性が保たれた保護領域で実行する「TEE」などの方法もある。加えて、自組織のデータに含まれる利用者の情報を他組織に対して秘匿しながら協働して機械学習を行う「連合学習」も研究されている。関連する概念として、「自己主権型アイデンティティ」にも注目が集まっている。

こうしたプライバシー保護技術やその決済・金融サービスへの応用に関する議論は、わが国を含め各国で進められている中央銀行デジタル通貨（CBDC）に関する検討に対しても、示唆を与え得るものである。

わが国で CBDC を導入するかどうかは、内外の情勢も踏まえ今後の国民的な議論の中で決まっていくものと考えられるが、日本銀行では、決済システム全体の安定性と効率性を確保する観点から、将来の様々な環境変化に的確に対応できるよう実証実験や制度設計面の検討を計画的に進めている。今後も、制度設計面の検討の一つとして、デジタル通貨に関連するプライバシー保護に関する調査・検討を、幅広い関係者とともに進めていく。

[目　次]

１．はじめに

日本銀行では、2020 年 10 月の「中央銀行デジタル通貨（CBDC）に関する日本銀行の取り組み方針」の公表[1]以降、同方針に沿って、実証実験を実施するとともに制度設計面の検討を進めている。同方針では、今後の制度設計面の検討項目のひとつとして「プライバシーの確保と利用者情報の取扱い」を挙げており、本稿は、この検討の一環として、利用者のプライバシー保護に資する技術に焦点をあて、その概要を説明し、適用事例をみたうえで、決済領域や CBDC への含意を考察するものである。

近年、国内外において、事業者が顧客データを収集することで多くのサービスが生まれており、データの利活用は決済の領域でも事業展開の重要なモチベーションとなっている。また、近年、決済にかかるマネー・ローンダリングおよびテロ資金供与対策（AML/CFT）の重要性への認識が高まっており、国際的な議論が進められている。AML/CFT の精度を高め、実効性のある仕組みを整えるためにも、データを活用することが重要となってきている。

データ利活用の要請が高まっているなか、プライバシーに関する社会の関心も高まっている。わが国を含む多くの国では、プライバシーは人格的な権利と認識されており、データの利活用における適切なプライバシーの保護を確保するうえでは、人格的利益の保護、倫理といった視点も含む多面的な検討が行われることが重要と考えられる。サービスを運営する事業者は、個人情報保護法等の法令を遵守することはもとより、こうした点も踏まえ、どのようなデータを収集・保管するか、どのような目的でデータを利活用するか、どのような者にデータへのアクセスを認めるかなどの判断において、プライバシー保護を考慮することが求められている。そうした中にあって、「知られるべきではない相手に、知られるべきではない情報を、知られたり推測されたりすることを防ぐ」ことは、重要な要素の一つと考えられる。

こうした状況を背景として、データをビジネス創出や健全な取引の実現に用いつつ、利用者のプライバシー保護に資する技術が、近年発展を見せている。本稿では、こうした技術を「プライバシー保護技術」として、概説を試みた。まず 2 節でこうした技術の基礎を説明し、3 節で決済・金融サービスへの応用事例を紹介する。これらの技術については、社会実装を企図するときに留意すべき点があるが、各国で検討が進む CBDC の検討にも示唆を与え得るものであり、４節でこの点に触れる。なお、「プライバシー保護技術」という

[1] 日本銀行　「『中央銀行デジタル通貨に関する日本銀行の取り組み方針』の公表について」（2020 年）
https://www.boj.or.jp/announcements/release_2020/data/rel201009e1.pdf

用語は多義的であり、該当するとされる具体的な技術についても様々な考え方がある。本稿で紹介した技術やコンセプトは、あくまでその一例である。

2．プライバシー保護技術の概要

一般に、サービスを提供する過程で利用者情報を取得する主体は、利用者のプライバシーを保護するために、体制面や技術面での様々な手当てを行うことが求められる。具体的には、例えば、サービスを提供する過程で必要最低限の情報しか取得・処理・保管しないポリシーが期待される（データミニマイゼーションの考え方[2]）。また、取得したデータが含まれるデータベースを、情報セキュリティが担保されるよう体制を整備して運営する必要がある（十分な情報セキュリティ対策）。その上で、利用者の同意がある場合や、個人が特定できないくらいの粒度であると評価できる情報であれば、プライバシーを保護しつつそのデータベースに蓄積された情報を広範な主体が利活用する余地が生まれてくる。決済分野では、AML/CFT のため、法令の定めるところにより、必要な利活用が行われることもある。これらの利活用が行われる際には、「本人の意図しない利活用は行われない」ということを前提にした上で、「知られるべきではない相手に、知られるべきではない情報を、知られたり推測されたりすることを防ぐ」ことが極めて重要である。このため、分析などに用いるデータセットには、データセット自体やデータセットの分析結果から個人が特定できないよう、様々な工夫を施す必要がある。本稿では、このようなプライバシーの保護の施策に資する技術を紹介する。

まず、データセットや分析結果を取り扱う主体から個人が特定されないようにデータを「変換する」手法が挙げられる（「匿名化」2-1 節）。「ノイズを加える」ことで分析結果からの識別可能性を抑制する手法も有用とされる（「差分プライバシー」2-2 節）。また、近年、データセットの内容の変換やノイズ付加とは異なるアプローチとして、「データを秘匿した状態で分析を行う」手法が発展してきている（「秘密計算」2-3 節）。機密性が保たれた状態において意図した計算が実行されることを、ハードウェア技術を用いて保証する方法もある（「TEE」2-4 節）。さらに、機械学習に用いるデータに上記技術を活用するなどして、自組織のデータに含まれる利用者の情報を他組織に対して秘匿しながら協働して学習を行う方法も研究されている（「連合学習」2-5 節）。

---

[2] 2011 年に発行された国際標準規格「ISO/IEC29100 プライバシーフレームワーク」はデータミニマイゼーションをその 11 原則の一つに掲げているほか、EU 一般データ保護規則など各国の個人情報保護法令でもデータミニマイゼーションを原則とする例がみられる。

なお、上記で紹介した技術は必ずしも単体で用いられるものではなく、複数を組み合わせてプライバシー保護を実現する方法が提案されている。これらの技術は引き続き発展している分野であり、識者によって分類や用語法が異なることには注意が必要である。また、本稿で紹介した技術を用いることは、法的な要求を充足することを必ずしも意味しない。

2-1　データを変換する　～匿名化など～

データセットにおいて個人が特定できないようにするためには、まず「識別子（identifier）」（氏名や重要な ID 番号など、直接に個人が特定できるような情報）を削除したり変換したりする。さらに、単体では個人を特定できないような「準識別子（quasi-identifier）」（例えば郵便番号、年齢、性別など）についても、組み合わせることで個人が特定される可能性があるため、削除・変換することが重要である。このように識別子や準識別子を削除・変換して「匿名化（anonymization）」を行うなど、データの変換により個人が特定されるリスクを抑制する技法として、具体的には以下の方法がある（図表 1）。

図表 1：データ変換により個人を特定するリスクを抑制する代表的な方法

属性（列）削除	属性（氏名など）を削除すること。
仮名化	属性またはその組み合わせ（氏名・生年月日、など）を符号や番号に置換すること。
一般化	属性の値を上位の値や概念に置き換えること。例えば、「1 歳ごとの年齢」を「10 歳刻み」にする、「キャベツ」を「野菜」に変換するなど。
トップ（ボトム）コーティング	数値属性に対して、特に大きい、もしくは小さい属性値をまとめること。例えば、100 歳以上の人は「100 歳以上」と表示するなど。
ミクロアグリゲーション	元データをグループ化した後、同じグループのレコードの各属性値を、グループの代表値に置換すること。
合成データ（疑似データ）	元のデータと統計的に疑似させる人工的なデータを作成すること。
レコード（行）削除	特に大きい値など、特殊な属性を持つレコードを削除すること。例えば、120 歳以上のレコードを削除する、など。

（出所）パーソナルデータに関する検討会技術検討 WG 報告書（2013 年 12 月）などを基に作成

上記のような方法を組み合わせて個人が特定されるリスクを抑制するとき、どの程度の効果を達成できたかを評価する目的で以下のような様々な指標が考案されており、それらの指標の性質を満たすようデータの変換を行うことが提案されている。データセットの内容を闇雲に変換すると、データセット自体が価値を失ってしまう（分析結果の有用性が下がる）といったことや、適切にデータセットを変換できたと感じられたとしても実は個人が推測可能であるといったことが生じ得るため、こうした指標を用いることは重要である。

（1）k-匿名性

あるデータセットにおいて、含まれる利用者の識別子（氏名など）が削除されているとする。分析者が、当該データセットに含まれるある利用者について、その準識別子（例えば、郵便番号、年齢、性別など）をある程度知っている場合、その組み合わせで絞り込んで個人を特定し、データセットに含まれる利用者にとって知られたくない情報（本稿における「機微情報」）と個人を紐付けてしまう可能性がある。例えば、図表 2 の左表のデータセットで「病名」を機微情報とした場合に、ある利用者 X の「郵便番号：345-0060」と「年齢：59 歳」をどちらも知っている分析者は、利用者 X と「病名：E」というデータを紐付けることができてしまう。

図表 2：k-匿名性を満たすデータ

識別子を削除した元データ

No.	郵便番号	性別	年齢	病名
1	123-0001	男	45	A
2	123-0002	女	47	A
3	234-0030	男	63	B
4	234-0040	女	88	C
5	345-0005	女	59	D
6	345-0060	男	59	E
7	345-0060	女	54	F

準識別子　　機微情報

k-匿名化

2-匿名性を満たすデータ

No.	郵便番号	性別	年齢	病名	
1	123-00**	*	40-49	A	2人
2	123-00**	*	40-49	A	
3	234-00**	*	60-	B	2人
4	234-00**	*	60-	C	
5	345-00**	*	50-59	D	3人
6	345-00**	*	50-59	E	
7	345-00**	*	50-59	F	

（出所）各種資料を基に作成

こうした問題に対処する目的で、匿名性がどの程度実現できているかを示す指標「k-匿名性（k-anonymity）」が考案されている。これは、「全ての個人のデータに対して、その準識別子が全く同一の個人が少なくとも k 人以上存在する」という性質のことである。対象とする属性に含まれる人が少なくとも 5 人以上いる場合、このデータセットは「5-匿名性を持つ」と表現される。k の値は、大きいほど、個人が特定しにくいことを意味する。

この k-匿名性を実現するデータの加工技術を「k-匿名化」と呼ぶ。同じ準識別子の組み合わせをもつレコードが少なくとも k 個存在するよう、値をレンジで表現する一般化など匿名化の手法を用いて、事前に定めた k-匿名性を充足する。例えば、図表 2 の右表では、匿名化によって、前述の利用者の病名が E であることはこのデータセットからは特定できない状態になっている（D か E か F であることは分かる）。

（2）l-多様性

k-匿名性が満たされていたとしても、個人と紐付く機微情報の種類が少ない場合、その個人の機微情報が推定できてしまう可能性がある。例えば上記の図表２の右表の No.1,2 のように、特定の利用者が含まれる「準識別子を同一とする集団」の病名の種類が１種類である場合、k-匿名性が満たされていても病名がＡであると分かってしまう。

この問題を解決するため、「l-多様性（l-diversity）」という指標が提案されている。k-匿名性は準識別子に着目していたが、さらにこれに加えて機微情報に着目して匿名性を評価する指標といえる。k-匿名化によって生成された、準識別子を同一とするグループを考えたとき、l-多様性は「任意のグループについて、グループに含まれる機微情報が l 種類以上ある」という性質を意味している。これにより、ある利用者の準識別子の組み合わせを知っており、どのグループに属しているかを知っていたところで、そのグループに含まれる機微情報が l 種類あり推定が難しくなり、上記の k-匿名性が持つ限界を補完することができる。

（3）t-近接性

上記の l-多様性は、同一グループ内の機微情報の種類の数に着目している（ l 種類あればよい）が、l-多様性が満たされていたとしても、機微情報の分布の偏りがあると傾向が掴めてしまうことがあり得る。例えば、機微情報が「年収」のような連続的なデータであり、同一グループ内の年収の種類が l 種類あった場合でも、そのほとんどが一定のゾーンに含まれている場合、具体的な年収を特定できなくても相応の情報を得てしまう。

この点を改善するために、グループ分けの方法を工夫した「t-近接性（t-closeness）」という指標も提唱されている。t-近接性は「任意のグループについて、グループ内の機微情報の分布と全体の機微情報の分布の差が t 以下である」という性質を意味している。グループ内の機微情報の分布を全体の機微情報の分布と近接させるようにグループ分けをすることで、利用者の機微情報の推測を困難にできる。

2-2　分析結果にノイズを追加する　～差分プライバシーの考え方～[3]

特定の背景知識や攻撃能力を想定してプライバシー保護の強度を評価する指標を構築した場合、その指標が想定していない攻撃に対しては脆弱になってしまう。そこで、「任意の背景知識を持つ攻撃者による」、「どのようなアルゴリズムによる攻撃に対しても」

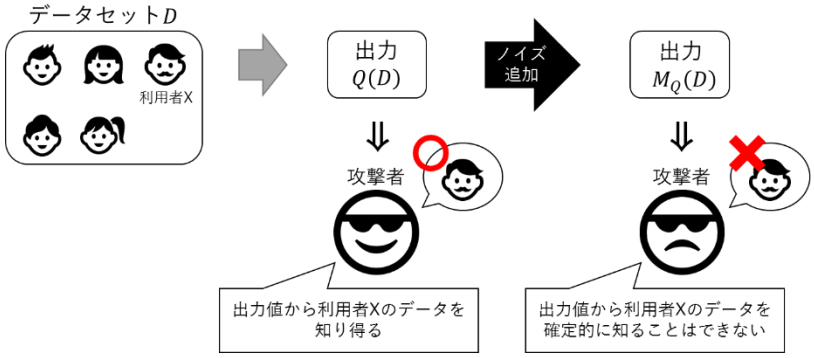
[3] この節の記述は下記文献などを参考にしている。
寺田雅之「差分プライバシーとは何か」 システム/制御/情報 63 巻 2 号 p58-63 (2019 年)

プライバシーの開示を一定以下に保証できるよう構築された指標として、差分プライバシー（differential privacy）がある。この指標を満たすようにデータセットの分析結果にノイズを加えるなどして出力をランダム化し、データセットに含まれる情報が識別されにくくする方法がある。

個人に関する情報を含むデータセット D から、何らかの情報を取り出すための問合せを行うとき、問合せの結果である出力 $Q(D)$ は、そのまま利用するとデータセット D に含まれる個人を識別し得る情報を暴露してしまう可能性がある。これについて、寺田（2019）は以下の例を挙げている。男女 20 人のクラスにおける試験の結果を記録したデータセットから、「受験者の性別」と「合否結果」を抽出する問合せを実行する。問合せの結果、「女性：合格 10 人／落第 5 人、男性：落第 5 人」という情報が得られた場合、問い合わせ結果に示された全人数を足すとクラスの人数になることから、合格者がすべて女性だったことが分かる。このため、ある男性が自らの試験結果を秘匿したいと思っていたとしても落第したことが暴露されてしまう。

そこで、$Q(D)$ に対しノイズを加えるメカニズム M_Q を考え、このときの出力値を $M_Q(D)$ とする。$M_Q(D)$ は $Q(D)$ と似ているが、ノイズが加わったことでランダム化された出力であるため、出力値から個人を識別しにくくなっている[4]（図表 3）。加えるノイズが大きいほど個人を識別しにくくなるが、分析結果が変化するためその有用性が下がる。

図表 3：出力値へのノイズの追加



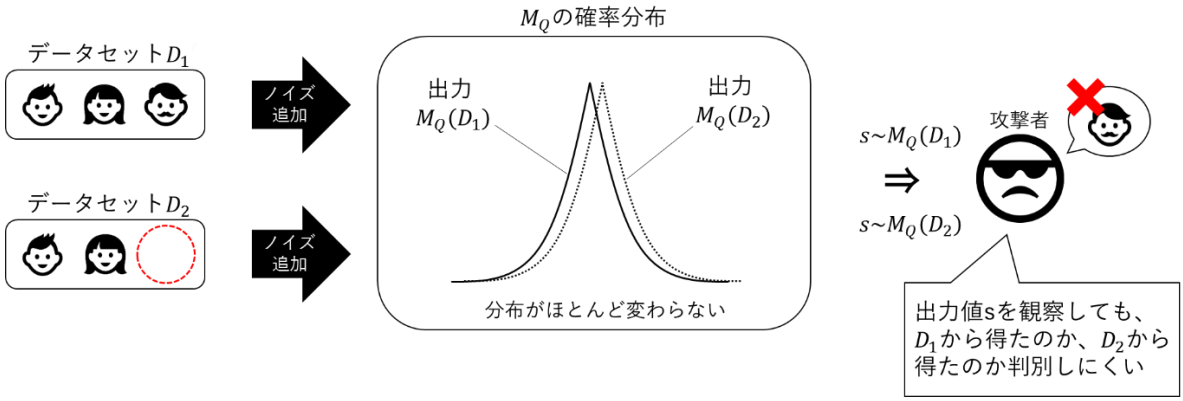
（出所）各種資料を基に作成

このとき、プライバシー保護の強度を定量的に評価する指標として、「ε-差分プライバシー」がある。ある個人 1 名分のデータが含まれているかどうかだけが異なる 2 つのデータセット $D_1 \subset D$ と $D_2 \subset D$ を考えると、ノイズ追加後の出力値 $M_Q(D_1)$ と $M_Q(D_2)$ は

[4] ノイズの加え方には様々な手法があり、代表的な方法として、ラプラス分布と呼ばれる分布に従うノイズを出力値に加算するラプラスメカニズムがある。

確率変数となる。任意の出力値 s に対して、$M_Q(D_1)$ と $M_Q(D_2)$ が s を出力する確率の比（$\Pr[M_Q(D_1)=s]$ / $\Pr[M_Q(D_2)=s]$）が e^{ε} 以下であるとき、「M_Q は ε-差分プライバシーを満たしている」という[5]。このとき、ε を小さくすれば、$M_Q(D_1)$ と $M_Q(D_2)$ の確率分布の差が小さく（区別しにくく）なり、ある出力値 s を観察しても D_1 と D_2 のどちらから出力された値か判別しにくくなる。すなわち、差分となっている個人の情報を読み取ることが難しくなる（図表 4）。任意の D_1 と D_2 の組み合わせについてこの性質が満たされるならば、ノイズ追加後の出力 M_Q からは D に含まれるどの個人についても識別が困難といえる[6]。

図表 4：ε-差分プライバシーの概要



（出所）各種資料を基に作成

2-3　データを秘匿した状態で処理する　～秘密計算を中心に～

分析用のデータセットを持つ主体が、外部の主体とデータセットを統合して分析を行ったり、高度なデータ分析のノウハウを持つ外部の専門家に分析を依頼したりといったニーズは高くなっており、それに伴い、分析用のデータセットを外部のサーバーなどに格納するようなケースも増えている。一方で、データセットに匿名化などの加工を施しているとしても、他の主体に渡す場合は、その共有先を含めてプライバシー侵害のリスクを管理す

[5] ε の詳細については下記を参照。
・宇野洋輔、園田章、別所昌樹「プライバシーの経済学入門」日本銀行ワーキングペーパーシリーズ No.21-J-10 (2021 年)
・管和聖 「望ましいプライバシー保護のあり方を巡って：差分プライバシーの有用性と限界」 日本銀行金融研究所ディスカッションペーパーシリーズ No.2022-J-5/情報技術 (2022 年)

[6] 差分プライバシーの関連技術が活用されている具体例として、米国センサス局の試みがある。米国の国勢調査では、従来、統計から回答者の情報が開示されることを回避する仕組みは存在したが、近年、コンピューターの計算能力が増大し、また照合できるデータソースに比較的安価にアクセスできるようになり、統計から再識別が可能となる危険性が高まっていることが指摘された。同局では、差分プライバシーに関係した実証研究を積み重ね、2020 年国勢調査に基づく統計データの公表に際して差分プライバシー関連技術を導入した。

る必要が生じるほか、こうした状況に対し利用者が抵抗感を覚える可能性が高い。プライバシー保護のレベルの実効的な向上と、利用者が安心できる仕組み作りが重要である。

こうした問題意識に応えるものとして、近年、データが秘匿された状態での処理を可能とする方法の研究が進められている。原データに触れることなく分析できるのであれば、データセットへのアクセスを他者に許すことなく統合したり分析したりすることで、プライバシー保護のレベルを向上させることができる。

（1）データを秘匿した状態で扱う技術

データは、暗号化されることで、そのままでは意味を読み取れない文字列（暗号文）に変換される。暗号文は、復号というプロセスにより、元の形式（平文）に戻る。この暗号化、復号のプロセスは暗号鍵を用いて行われる。この暗号鍵を持つ者のみがこれらの作業を行えるため、あるデータの内容を他人に知られたくない場合に暗号鍵を用いて暗号化を行うことや、知らせたい相手に暗号鍵を渡して復号を許す[7]といったことが可能となる。

暗号化したデータは通常は復号して平文にしない限り利用できない一方で、平文の状態ではプライバシー侵害に対して脆弱となる。こうした問題意識のもと、1980 年代以降、暗号化された状態で様々な処理を行うことを可能にする技術の研究が進められている。暗号化はデータの通信時や保存時におけるプライバシー保護の技術であり、暗号化状態での処理技術はデータの分析や操作の過程におけるプライバシーも保護する技術といえる[8]。

このような暗号化状態での処理技術を含め、複数の主体の間で一定のデータ秘匿を行いつつデータ処理を行い、分析結果を得ることを目的とする技術は「秘密計算（secure multi-party computation）」と呼ばれ、近年、その汎用性の高さから関心を集めている。

（2）秘密計算の概要と実現方法

秘密計算には主に、①秘密分散法（secret sharing scheme）を用いる方式、②準同型暗号（homomorphic encryption）を用いる方式の 2 つがある。

---

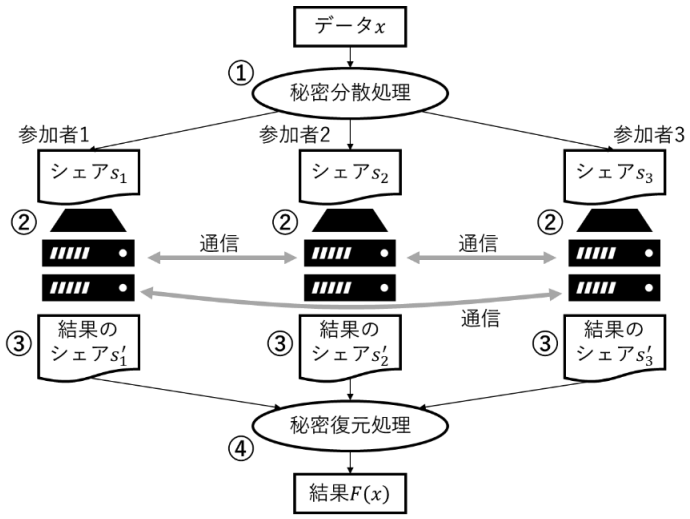
[7] こうした鍵の受け渡しでは公開鍵方式の鍵配送アルゴリズム等が用いられる。公開鍵暗号については脚注 13 を参照。

[8] 暗号化された状態で処理を行う技術の詳細については、下記を参照。
清藤武暢、四方順司 「高機能暗号を活用した情報漏えい対策『暗号化状態処理技術』の最新動向」 金融研究 第 33 巻第 4 号 p93-132 (2014 年)

① 秘密分散法を用いる方式

秘密分散法は、複数の主体で秘密を分散して管理する技術である。この方式では、データをシェアと呼ばれる複数の断片に分割する。シェアは、一定数集めることではじめてデータを復元できる。この性質により、一定数以上の参加者が結託してシェアを共有しない限り、原データに関する情報を得られない[9]。これらのシェアを複数のサーバーに割り当て、シェアの状態で計算をさせたあと、各サーバーにおける計算結果のシェアを集約して全体としての結果を導く。一連のプロセスを通じ、各サーバーは、割り当てられたシェアにしか触れないため、もともとのデータも結果も知ることはない。具体的なプロセスの一例は、以下のとおりである（図表 5）。

図表 5：秘密分散法による秘密計算



① データを提供する主体（クライアント）は、入力データ x を複数個のシェアに分割して（秘密分散処理）、参加者（サーバー）に送信し、計算を要求

② 参加者（サーバー）はシェア s_n を受け取り、計算を実行（必要に応じて他の参加者と通信を行う[10]）

③ 参加者（サーバー）は結果のシェア s'_n を得る

④ クライアントは、結果のシェアを集め復元して（秘密復元処理）、最終的な結果 $F(x)$ を得る

（出所）各種資料を基に作成

---

[9] 例えば、(k,n) 閾値法と呼ばれる秘密分散法の方式では、n 個のシェアを作成し、n 台のサーバーに割り振るとき、サーバーのうち $k-1$ 台が乗っ取られたり結託したりしても、原データの情報は復元できない。

[10] 計算は、シェアを入力として、加法や乗法などの演算がデータを復元することなく行われる。実施する計算によっては計算過程のシェアを特定の参加者と持ち合う手続きが必要とされ、そのために参加者間で通信が行われることがある。
大原一真 「秘密分散法を用いた秘密計算」 システム/制御/情報 63 巻 2 号 p71-76 (2019 年)

このように、データを提供する主体が、データをシェアに分割してデータ分析事業者に割り振り、分析結果のシェアを返してもらうケースを考えると、データ分析事業者はすべてのプロセスで自身に割り当てられたシェアにしか触れていないためデータ復元の条件を満たさず、データを提供する主体は分析事業者にデータを公開することなく分析結果を得ることができる[11]。

② 準同型暗号を用いる方式

もうひとつは、データを暗号化した状態で加法や乗法といった演算を行える、「準同型暗号」と呼ばれる暗号化方式を用いる方法である。この暗号化方式は、値の暗号文に対してある演算を実行し、その結果として得られた暗号文を復号したときに得られる平文が、元の値について演算した結果と一致する性質を持つ[12]。

準同型暗号を用いた秘密計算のモデルケースとして、例えば、データ提供者が処理者にデータを渡し、処理者が計算を実施し、その結果を利用者に提供する場面を考える（図表6）。この例では、準同型暗号の上記の性質を備えた公開鍵暗号[13]を用いて、原データを暗号化したまま処理することにより、データ提供者は他の主体（他のデータ提供者、処理者、利用者）に原データを共有することなく、処理結果のみを利用者に提供することができる。なお、暗号鍵を用いた仕組みであるため、主体間で鍵の扱いについて合意のとれた形で適切に鍵管理が行われることが重要となる。

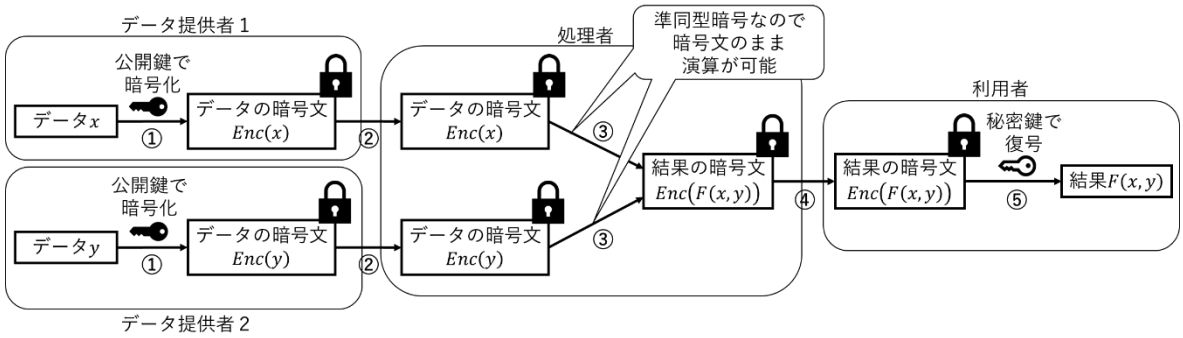
---

[11] 図表5は、単一の主体が保有しているデータを入力とし、分析を行うモデルを表しているが、他にも、異なる組織に分散して保有されているデータを入力とし、それぞれの組織が他組織からデータを秘匿した状態で協働して分析するモデルなどが存在する。

[12] 任意の平文 m_1, m_2 について、例えば加法に関して、$Enc(m_1) \oplus Enc(m_2) = Enc(m_1 + m_2)$ が成り立つような演算 $\oplus$ が存在し、暗号化したままで原データについて加法が計算できるという性質を持つ。ここで、$Enc(\cdot)$ は入力（平文）の暗号文。加法と乗法の両方の演算が可能な暗号化方式は完全準同型暗号と呼ばれる。

[13] 公開鍵暗号は、暗号化に用いる公開鍵と復号に用いる秘密鍵という、2つの異なる鍵を用いる暗号化方式である。情報の受信者が 2 つの鍵を作成して公開鍵のみを送信者に渡し、送信者が公開鍵で情報を暗号化して送信することで、秘密鍵を持つ受信者のみが情報を復号できる。

図表 6：準同型暗号による秘密計算



① データ提供者 1 とデータ提供者 2 はデータ x と y をそれぞれ公開鍵で暗号化し、暗号文 $Enc(x)$ と $Enc(y)$ を生成する
② 各データ提供者は暗号文 $Enc(x)$ と $Enc(y)$ を処理者へ送る
③ 処理者は暗号文のまま演算を行い、結果の暗号文 $Enc\big(F(x,y)\big)$を得る
④ 利用者は結果の暗号文 $Enc\big(F(x,y)\big)$ を処理者から取得する
⑤ 利用者は結果の暗号文を秘密鍵で復号して結果 $F(x,y)$ を得る

（出所）各種資料を基に作成

2-4　ハードウェアによるデータ保護のもとで計算を行う　～TEE～

プライバシーが保護された状態での計算を、ハードウェアの機能により実現する技術も発展している。TEE（Trusted Execution Environment）は、隔離された保護領域でソフトウェアを安全に実行する環境である。TEE が提供する機能や保護方式はプロセッサーによって異なるが、例えば Intel SGX（Software Guard Extensions）では、ソフトウェアはエンクレーブと呼ばれる暗号化で保護されるメモリ領域に、ロード・実行される。メモリやバス（伝送路）において、プログラムおよびデータは暗号化されており、プロセッサーの固有の鍵によってのみ復号・実行される。

これにより、OS の脆弱性やマルウェアが存在し得る環境下や、クラウド等の外部でホストされるハードウェアを利用する場合でも、外部から隔離された状態で利用者の意図したプログラムが正しく実行できる。TEE のこの特性は、プライバシーを保護した状態において複数者間でデータとロジックを共有し協働することに活用し得る。

このように TEE をシステムの一部に組み込む場合、その TEE が真に信頼できるかを外部から検証できることが必要である。この検証のために「リモートアテステーション」と呼ばれる技術が用いられ、対象が TEE に偽装されたデバイスでないことや、そこで動作するコードが利用者の意図するものと一致することが、ネットワーク経由で検証される。

なお、TEE については、ハードウェアの鍵管理や識別の仕組みなどについて、ハードウェアベンダーへの依存が大きい事柄が存在することには、留意が必要である。

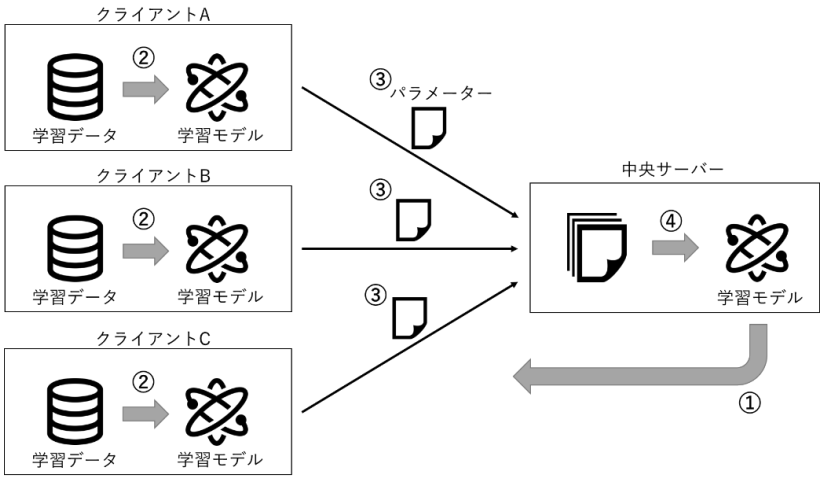
2-5　プライバシーに配慮した機械学習　～連合学習～

近年、機械学習に用いるデータに関して、プライバシーに配慮しながら学習を行う「連合学習（federated learning）」の研究が進んでいる。さらに、上記で紹介した差分プライバシーの考え方や秘密計算を活用して「プライバシーを強化した連合学習」についても検討が進んでいる。

（1）連合学習[14]

連合学習とは、データを集約せずに分散した状態で機械学習を行う方法である。クライアント・サーバー型の仕組みにおける連合学習は、一例として以下のプロセスで行われる（図表 7）。

図表 7：連合学習のプロセス



① 各クライアント（スマートフォンなど）が、中央サーバーから最新の学習モデルを取得
② 各クライアントは自らのデータに基づいた機械学習を行い、学習モデルのパラメーターを改善
③ 各クライアントは、改善されたパラメーターを中央サーバーに送信
④ 中央サーバーは集計されたパラメーターに基づいて学習モデルを更新
⑤ ①に戻る

（出所）Kairouz et al. (2021)を基に作成

[14] この項の記述は下記文献に基づいている。
Kairouz, Peter et al., "Advances and Open Problems in Federated Learning", Foundations and Trends® in Machine Learning, Vol. 14, No. 1–2, pp. 1-210, 2021.

連合学習において、原データは複数のクライアントに分散された状態のまま、各クライアントが抽出した学習モデルのパラメーターのみが中央サーバーで統合される。プライバシー保護との関係では、クライアントが保有している原データがクライアントにとどまることが、一般的な機械学習に比べたメリットである。

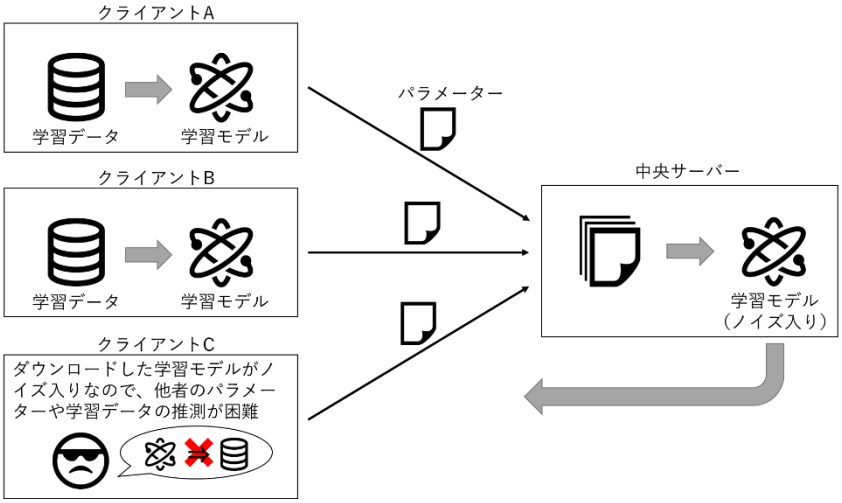
（2）プライバシーを強化した連合学習[15]

上述の連合学習では、一連のプロセスを通じて得られる情報から、クライアントや中央サーバーが元の学習データを推測するなどの懸念は残存する。こうした脅威に対し、差分プライバシーの考え方や秘密計算を用いて対策を施した「プライバシーを強化した連合学習」が提案されている。

① クライアント起点の攻撃への対策（差分プライバシーを用いた連合学習）

連合学習に参加しているクライアントや、クライアントを攻撃して情報を取得した攻撃者が、中央サーバーから提供された学習モデルから他のクライアントの学習データを推測する可能性がある。このリスクを低減するため、一例として、中央サーバーが差分プライバシーを満たす学習モデルを提供することが考えられる。すなわち、中央サーバーが、各クライアントに提供する学習モデルに差分プライバシーを満たすためのノイズを加えることで、悪意のあるクライアントやクライアントから情報を取得した攻撃者により、学習モデルから他者の学習データが推測されることを困難にできる（図表 8）。

図表 8：連合学習への差分プライバシーの適用



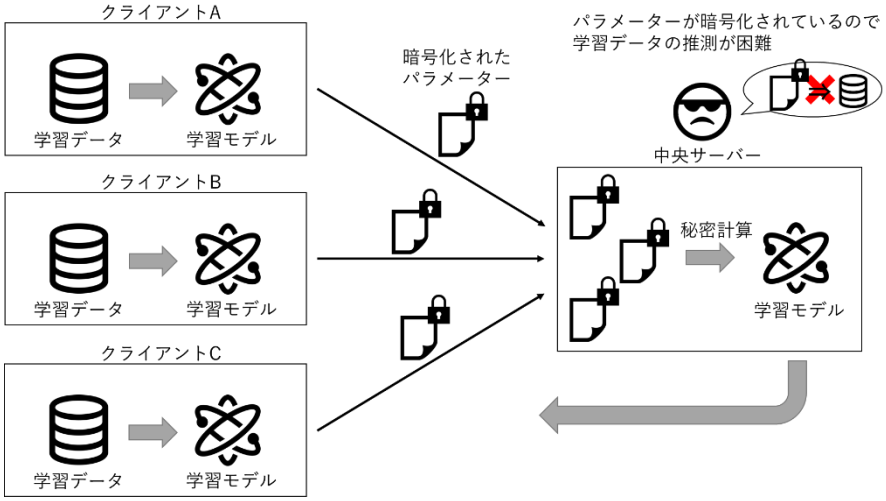
（出所）Li et al. (2020)を基に作成

[15] この項の記述は下記文献に基づいている。
Li, Tian et al., "Federated Learning: Challenges, Methods, and Future Directions", IEEE Signal Processing Magazine, Vol. 37, Issue 3, pp. 50-60, 2020.

② 中央サーバー起点の攻撃への対策（秘密計算を用いた連合学習）

連合学習に参加している中央サーバーや、中央サーバーを攻撃して情報を取得した攻撃者が、各クライアントから送信されたパラメーターから、クライアントの学習データを推測することも考え得る。このリスクを低減するため、一例として、連合学習に秘密計算を導入する手法がある。すなわち、クライアントはパラメーターを暗号化して中央サーバーに送信し、中央サーバーはそれらを暗号化したまま学習モデルの計算に用いる手法である。これにより、中央サーバーでは、暗号化されたパラメーターの平文を知ることができず、学習データを推測することが困難となる（図表 9）。

図表 9：連合学習への秘密計算の活用



(出所) Li et al. (2020)を基に作成

2-6 プライバシー保護に関連したその他の技術やコンセプト

以上で説明した技術以外にも、プライバシー保護に資する技術やコンセプトは数多く存在する。例えば、近年、デジタル領域の重要性が高まる中で、デジタルアイデンティティの管理方法への関心が高まっている。最近は、新たなアイデンティティの管理モデルとして「自己主権型アイデンティティ」が提唱されており、プライバシー保護にも関係が深いと考えられるため、BOX1 で取り上げる。

3．決済・金融サービスに関連した応用事例

本節では、２節で説明したプライバシー保護技術について、決済・金融サービスへの応用を目指して金融機関や公的機関が取り組んでいる試みを紹介する。

3-1　合成データの提供

合成データは原データをもとに生成された人工的なデータである。原データの特徴や傾向をアルゴリズムによって統計的に再現することで、原データそのものの利用を避けることができる。英国の金融行為規制機構（FCA: Financial Conduct Authority）は、TechSprints と称して、製品開発のための実験に使用できる合成データを企業に提供している[16]。TechSprints は、同機構が金融機関や企業を募って開催しているワークショップである。2019 年 7 月の回は、マネー・ローンダリングと金融犯罪の防止をテーマにして開催され[17]、外部機関の協力を得て作成した合成データを提供した。

3-2　プライバシーに配慮した機械学習と AML/CFT への活用[18]

わが国では、近年、金融機関において、AI 技術を用いた不正取引の自動検知システムの導入事例がみられる。AI による不正検知は、複数の金融機関で協力した学習をすることで、その実効性を高める効果が期待されるものの、顧客の情報を含む金融取引データを各金融機関の外部に持ち出すことには多くの課題が存在する。この問題に対応するため、情報通信研究機構（NICT）、神戸大学、エルテス、三菱 UFJ 銀行などの金融機関は、顧客情報を含むデータを外部に開示することなく機械学習を行うことを可能とする情報通信研究機構の技術を応用し、プライバシーを保護しつつ複数の金融機関が協調して不正送金等を自動検知できるシステムの実現を目指し、実証実験に取り組んでいる。

具体的には、各組織で持つデータを基に機械学習を行う際に、学習中のパラメーター（勾配情報）を暗号化して中央サーバーに送り、中央サーバーでは、暗号化したまま学習モデルのパラメーター（重み）の更新を行うことが実験されている。この更新処理は、暗号化した状態で加法が可能な準同型暗号を用いている。中央サーバーで更新された学習モデルのパラメーターは、各組織においてダウンロードされ、より精度の高い分析が可能となる。ここでは、パラメーターを複数のデータを集計した統計情報とすることで、個人を識別できない状態にできるうえ、暗号化されているため、中央サーバーがパラメーターから各組織の学習データを推測するリスクが低減されている[19]（図表 10）。

---

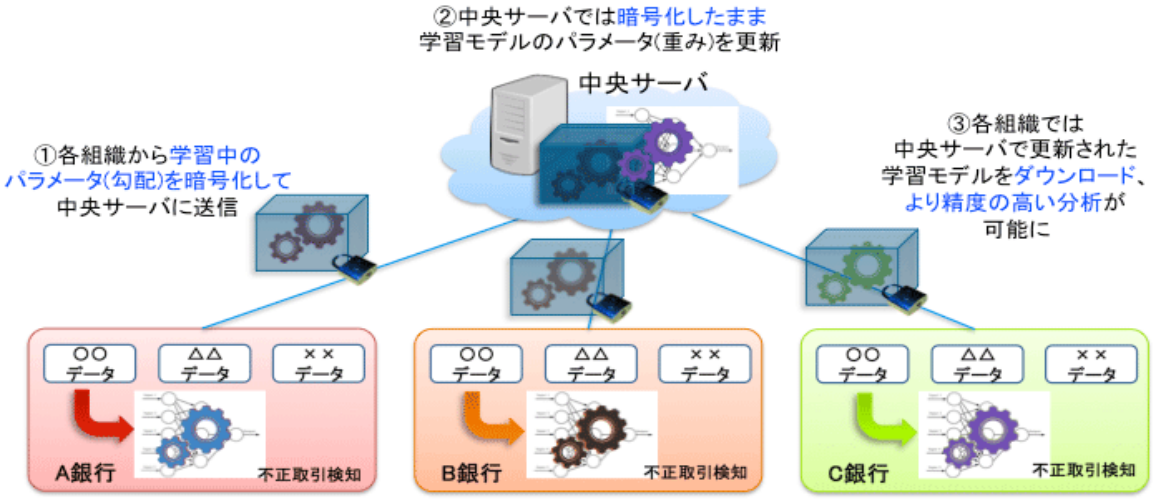
[16] FCA, "TechSprints" https://www.fca.org.uk/firms/innovation/regtech/techsprints

[17] FCA, "2019 Global AML and Financial Crime TechSprint" https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint

[18] この項の記述は、情報通信研究機構のプレスリリース、各種報道に基づいている。
情報通信研究機構 「プライバシー保護深層学習技術を活用した不正送金検知の実証実験において金融機関 5 行との連携を開始」 https://www.nict.go.jp/press/2020/05/19-1.html

[19] 詳細については、下記を参照。

図表 10：機械学習を利用した不正検知モデルの開発



（出所）情報通信研究機構プレスリリース

3-3　TEE を用いた秘密計算のマーケティングへの活用[20]

ロイヤル・バンク・オブ・カナダ（RBC）は、マイクロソフトが提供する環境（Azure confidential computing）の中に、データの秘匿性に配慮した情報共有プラットフォーム「バーチャルクリーンルーム（VCR）」を構築して、情報が分散された状態でデータを分析する実験を行っている。VCR では、ハードウェアベースの信頼できる実行環境（TEE)で計算を実行することにより、使用中のデータを保護している。

例えば、顧客が RBC のクレジットカードを使って小売店で買い物をした場合、RBC は顧客がどの小売店で購入したかを示すデータを取得するが、その小売店で何を購入したかを示すデータは持っていない。小売企業は、顧客が自社で何を購入したかを示すデータを取得するが、顧客データの秘匿の観点から外部に共有したくない。RBC は、VCR を用いることで、各小売企業が持つ個々の顧客の購買データの内容に触れることなく自社のデータと組み合わせた分析を実施し、その結果のみを取得して活用することが可能となる。

Phong, Le Trieu et al., "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption", IEEE Transactions on Information Forensics and Security, Vol. 13, Issue 5, pp. 1333-1345, 2018.

[20] この節の記述はマイクロソフトのウェブサイトに基づいている。
Microsoft, "RBC creates relevant personalized offers while protecting data privacy with Azure confidential computing" https://customers.microsoft.com/ja-jp/story/1356341973555285762-royalbankofcanada-banking-capital-markets-azure

４．おわりに　――デジタル通貨との関連で――

本稿では、プライバシー保護技術の概要と、決済・金融サービスに関連した応用事例について説明してきたが、これらの技術については将来的な社会実装を企図したときに留意すべき点がある。

まず、こうした技術の多くは現時点では実験段階にとどまっており、研究が積み重ねられている段階にある[21]。例えば、秘密計算は、秘密計算実行中の通信や暗号化状態での処理に、平文のままでの計算に比べて時間がかかることなどが課題とされる。自己主権型アイデンティティは、各団体で関連規格や仕様の検討が進んでいる段階で、実サービスの事例は少数にとどまる。しかしながら、これらの技術は、様々な領域でのビジネス機会創出につながるのみならず、デジタル社会におけるプライバシーを支える重要な基盤になり得ると考えられている。公的機関、研究機関、金融機関、サービス事業者など、幅広い主体によって研究・開発や実証実験が進められており、今後の進展が期待される。

また、将来的にプライバシー保護技術が発展し、社会実装を進め得る水準となった場合でも、技術のみですべての課題を解決することはできない。プライバシーや情報セキュリティに関する強固なポリシー、ガバナンス、運用体制など、様々な仕組みとあわせて技術を適用することが、実効性のあるプライバシー保護の仕組みにつながるという考え方が重要である。

そのうえで、デジタル社会におけるプライバシー保護技術に関する議論は、近年、わが国を含め各国で進められている中央銀行デジタル通貨（CBDC）に関する検討に対しても、示唆を与え得るものである。

一般に、決済サービスにおいて、事業者は、口座開設などのサービス利用開始時や、送金などの個々の取引時に、結果的に利用者からデータを取得することになる。CBDC でも、利用者情報の取扱いに関する様々な要請を考慮しながら、中央銀行と民間事業者の役割分担、すなわち「誰が、どの範囲のデータを、どのような条件のもとで取得し、管理するか」について検討していく必要があり、その際には、情報管理に関する配慮も必要となる。

CBDC とプライバシーに関連して、国際的な議論を概観すると、例えば、昨年 10 月公表の G7「リテール中央銀行デジタル通貨（CBDC）に関する公共政策上の原則」では、あ

---

[21] サンフランシスコ連銀スタッフの Privacy Enhancing Technology（PET）に関するサーベイペーパーでも、「これらの技術の開発と利用は初期段階にある」としている。
Asrow, Kaitlin, and Spiro Samonas, "Privacy Enhancing Technologies: Categories, Use Cases, and Considerations ", FinTech Edge Special Report, Federal Reserve Bank of San Francisco, 2021.

らゆる CBDC は信頼と信認を得るために「厳格なプライバシー基準、ユーザーデータの保護に対する説明責任、情報の保護・利用方法に関する透明性」が不可欠であるとし、加えて「犯罪を助長する利用の軽減にコミットする」必要性に言及している。また、CBDC の設計において、「取引の認証や検証を改善し得る技術進歩および革新的なソリューション」を取り入れ、不正な金融への対策に組み込むよう努めるべきとの記述もある（図表 11）。

図表 11：リテール中央銀行デジタル通貨（CBDC）に関する公共政策上の原則（抜粋）

原則 3. データプライバシー	厳格なプライバシー基準、ユーザーデータの保護に対する説明責任、情報の保護・利用方法に関する透明性は、あらゆる CBDC が信頼と信認を得るために不可欠である。 ・あらゆる CBDC エコシステムにおける公的・民間部門の主体は、個人データについて、例えば、マネー・ローンダリングやテロ資金供与のリスク削減等、明確でオープンかつ合法な目的を達成するために必要な場合にのみ、アクセス、保持、処理、共有すべきである。 ・あらゆる CBDC のユーザーは、自身の個人データの利用に関して、（できうる限りの）データの最小化と利用者のための制御に関する原則を中心に、高い透明性を与えられるべきである。必要最小限を超えた個人ユーザーのデータへのアクセスは、強固な同意の枠組みにより支えられるべきであり、それに際しては、（公的および民間の）主体が明確かつ透明性のあるかたちで、実効的かつ機能的なサービスを提供するうえで必要な追加的な要件を示さなくてはならない。
原則 6. 不正な金融	あらゆる CBDC は、犯罪を助長する利用の軽減にコミットするとともに、より速く、より多くの人々が利用可能で、安全かつ安価な決済に対するニーズを慎重に統合する必要がある。 ・CBDC とそれに伴う規制の枠組みは、犯罪を助長するような利用への対策にコミットし、マネー・ローンダリング防止、テロ資金供与対策、および大量破壊兵器の拡散防止を遵守するよう設計されるべきである。また、金融制裁の回避のリスクを軽減し、FATF による基準を遵守すべきである。 ・CBDC の設計の際、公的当局は、取引の認証や検証を改善し得る技術進歩および革新的なソリューションを取り入れることで、不正取引等の不正な金融への対策に組み込むよう努めるべきである。 ・あらゆる CBDC エコシステムにおいて、不正な金融を目的とする利用を防止するための公的当局の権限やデータの活用は、国家の法的枠組みの中で明示されるべきであり、また、こうした権限は他の目的のために用いられるべきではない。

また、中央銀行における国際的な議論の進展を、G7 各国を中心にみると、プライバシーを CBDC に関する重要事項と捉えていることを明示すると同時に、AML/CFT など他の公益とのバランスを取ることの重要性への言及が多くみられる（図表 12）。なお、ALM/CFT 以外の情報の利活用については、中央銀行として行うことへの関心はないと明示する対外発信も多い[22]。

[22] この点を踏まえ、MAS のように、自身が「不正な資金フローに対する防御を確保しつつ、既存の電子決済

図表 12：主要中央銀行の CBDC のプライバシーに関連した発信

CBDCとプライバシーに関する基本的な考え方	ユーロ圏	プライバシーはデジタルユーロの最も重要な特性。デジタル時代の決済の信認を保つ一助となるよう、利用者の個人情報保護と高水準の機密性は優先検討事項（ECB パネッタ理事（2021)[23]）。
	米国	（CBDC が導入される場合には、）消費者のプライバシー保護は重要（FRB 市中協議文書（2022)[24]）。
	英国	BOE は、プライバシーへの配慮はいかなる CBDC システムにおいても重要と認識しており、CBDC が利用者の信認を得ようとするならば、適切なプライバシーが確保されなければならない（BOE (2021)[25]）。
プライバシーと AML など他の公益との関係	ユーロ圏	プライバシーは人々の個人生活や基本権に関わる重要な権利だが、公益面での他の重要な考慮との関係で慎重に検討されなければならない。不正な活動に対抗する必要性といった他の政策・規制上の目的との様々なトレードオフに応じ、様々な水準のプライバシーを保証し得る（前掲 ECB パネッタ理事（2021））。
	米国	いかなる CBDC も消費者のプライバシー権の保護と犯罪活動を阻止するのに必要な透明性の提供との間の適切なバランスを取る必要がある（前掲 FRB 市中協議文書（2022））。
決済データの収集への中央銀行の関心	ユーロ圏	独立した公的機関として、ECB は利用者の決済データのマネタイズ、収集への関心はない（前掲 ECB パネッタ理事（2021））。
	英国	BOE は利用者のデータを収集する商業的インセンティブを有しない。…仮に CBDC を発行する場合、中銀はシステム運営と法規制上の義務に従うために必要な極めて最小限の情報のみを収集しなければならない（BOE マットン局長（2021)[26]）。
	シンガポール	公的機関として、MAS は利益を動機に、取引データまたは個人情報を収集・活用する動機を有しない（前掲 MAS(2021)）。

モデルと比べ、消費者に対しデフォルトでは高レベルのプライバシーを備えた CBDC 決済システムを提供し得る」としている中央銀行もある。
Monetary Authority of Singapore, "A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context", pp.26, 2021.

[23] Panetta, Fabio, "A digital euro to meet the expectations of Europeans, Introductory remarks by Fabio Panetta, Member of the Executive Board of the ECB, at the ECON Committee of the European Parliament, Frankfurt am Main, 14 April 2021", https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html, 2021.

[24] Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation", 2022.

[25] Bank of England, "Responses to the Bank of England's March 2020 Discussion Paper on CBDC", https://www.bankofengland.co.uk/paper/2021/responses-to-the-bank-of-englands-march-2020-discussion-paper-on-cbdc, 2021.

[26] Mutton, Tom, "Central Bank Digital Currency: An update on the Bank of England's work", https://www.bankofengland.co.uk/speech/2021/june/tom-mutton-pre-recorded-keynote-speech-the-future-of-fintech-digital-conference, 2021.

海外の中央銀行における議論には、プライバシー保護と AML/CFT の両立の実現手段として、本稿で取り上げた技術に期待する声もある。例えば、BOE は「ゼロ知識証明やデジタルアイデンティティといったプライバシー保護技術は、透明性の向上とセキュリティ・プライバシーの向上の両立の機会を与え得る」（BOE マットン局長(2021)[27]）としている[28]。もっとも、新たな技術の計算負荷の大きさと、この点が CBDC の性能に与える影響も意識されている（BOE (2020)[29]）。これらは、本稿で上述している内容と同様の認識といえよう。

以上のプライバシーに関連した議論は、わが国において CBDC を検討する過程でも非常に重要になる。そして、本稿で挙げたようなプライバシー保護に資する可能性がある技術について、その発展の動向や社会実装の試みを追うことには今後も大きな意義があると考えられる。

わが国で CBDC を導入するかどうかは、内外の情勢も踏まえ今後の国民的な議論の中で決まっていくものと考えられるが、日本銀行では、決済システム全体の安定性と効率性を確保する観点から、将来の様々な環境変化に的確に対応できるよう実証実験や制度設計面の検討を計画的に進めている。その制度設計面の検討の一つとして、今後もデジタル通貨に関連するプライバシー保護に関する調査・検討を、幅広い関係者とともに進めていく。

以　上

[27] 前掲 Mutton (2021)

[28] ゼロ知識証明については、BOX2 を参照。

[29] Bank of England, "Central Bank Digital Currency: opportunities, challenges and design", 2020.

BOX1：自身で管理するアイデンティティ　～自己主権型アイデンティティ～

決済サービスにおいては、適切な相手に適切なサービスを提供する必要があり、そのためには利用者のアイデンティティの扱いが重要である。スマートフォン端末やネットワークを介してサービスが提供されることの多い今日では、デジタルな形式で表現された利用者のアイデンティティ（デジタルアイデンティティ）をどのように扱うかが、特に重要になってきている。以下、デジタルアイデンティティの新たな管理モデルとしての「自己主権型アイデンティティ」を紹介し、この概念が利用者のプライバシー保護の観点から重要であることを示す。

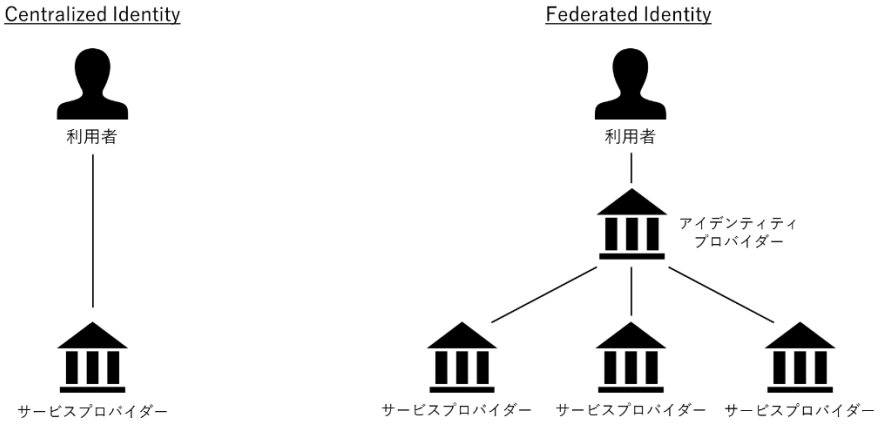
（1）既存のアイデンティティ管理モデルと自己主権型アイデンティティ

そもそもアイデンティティとは、国際標準化の推進機関である ISO/IEC のドキュメントにおける定義によれば「ある実体に関連する属性の集合」[30]である。ここで言う「属性」とは、利用者の名などの身元の情報や、資格・権利の情報などのことであり、したがってアイデンティティは「個人などに関連する身元情報・資格情報などの属性の集合」を意味すると言える。これをコンピューター上で処理できるようデジタルな形式で表現したものが、デジタルアイデンティティである。

デジタルアイデンティティの管理モデルとしては、まず、「サービスプロバイダー」が利用者のアイデンティティを直接管理する方法がある（Centralized Identity、図表 B1-1 左）。このモデルにおいては、利用者のアイデンティティはそのサービスプロバイダー以外に利用されない。デジタル化が発展し、世間に利用可能なサービスが増えるにつれ、複数のサービスにおいて横断的にアイデンティティを利用・提供する社会的ニーズが高まってきた。こうした中で、利用者が選択した「アイデンティティプロバイダー」が、利用者のアイデンティティを複数のサービスプロバイダーに連携する方法が普及した（Federated Identity、図表 B1-1 右）。実際には、あるサービスを利用する際に提供したアイデンティティがサービスプロバイダーに保管され、当該サービスプロバイダーがアイデンティティプロバイダーとして他のサービスプロバイダーに連携することが多い。このモデルでは、利用者のアイデンティティが、単一のサービスではなく幅広いサービスで用いられるようになると同時に、アイデンティティプロバイダーがハブになることで、アイデンティティが少数のアイデンティティプロバイダーに依存する状況が生じてきた。

[30] ISO/IEC 24760-1, https://www.iso.org/obp/ui/#iso:std:iso-iec:24760-1

図表 B1-1：代表的なアイデンティティ管理モデル



（出所）Reed (2018)[31]を基に作成

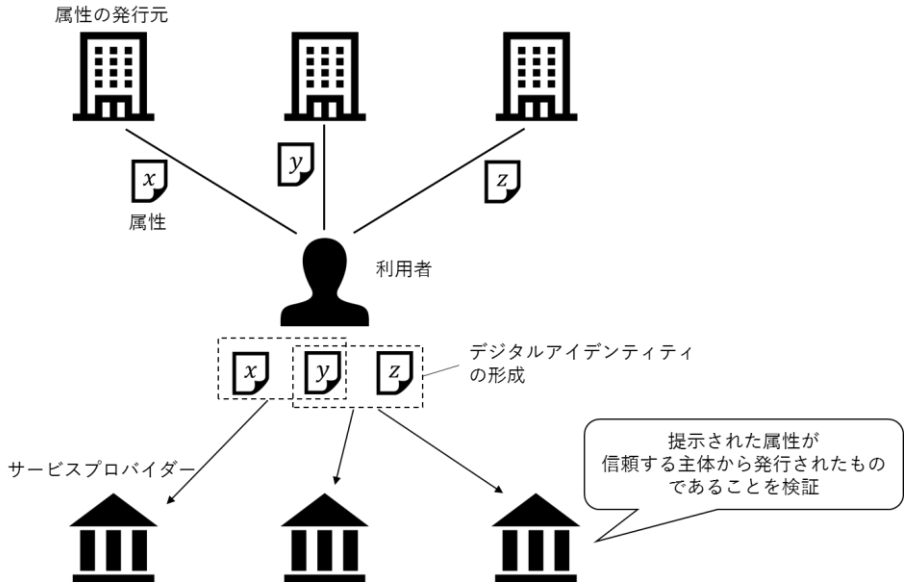
このように、デジタルアイデンティティの管理において現在主流となっている管理モデルは、アイデンティティが特定の組織に依存することを前提としており、こうしたモデルが内包するリスクとして、①特定の組織の都合や判断によりアイデンティティの提供や連携が停止されることで、サービスを利用できなくなるリスク、②過失または故意により、利用者の意に反してアイデンティティが連携されるリスク、③情報が改ざんされるリスクなどが指摘されている。

このようなリスクを軽減し得るデジタルアイデンティティ管理の考え方として「自己主権型アイデンティティ（Self-Sovereign Identity、SSI）」が注目されている。これは、管理組織が介在することなく、個人が自身のアイデンティティを自らコントロールすべきとする考え方[32]であり、例えば具体的に以下のように構成することが考えられる（図表 B1-2）。

[31] Reed, Drummond, “The Story of SSI Open Standards”, https://ssimeetup.org/story-open-ssi-standards-drummond-reed-evernym-webinar-1/, 2018

[32] Sovrin Foundation, https://sovrin.org/faq/what-is-self-sovereign-identity/

図表 B1-2：自己主権型アイデンティティの構成例



・利用者の属性（資格や身元、権利など）の発行元として、サービスプロバイダーが信頼する主体が存在する。
・利用者は、それらの主体から自身の属性の発行を受ける。属性は自身で生成した「分散型識別子」と紐付いた状態で発行される。この分散型識別子と、これに紐付けられた属性の組み合わせが、アイデンティティを構成する。
・利用者は、上記で構成したアイデンティティをサービスプロバイダーに提供する。
・サービスプロバイダーは、アイデンティティを構成する分散型識別子と属性について、①識別子が利用者本人のものであることを、利用者の公開鍵などから確認し、②その識別子が信頼する主体から発行された属性と紐づけられていることを検証する。問題がなければ、提供されたアイデンティティを構成する属性に基づいて利用者にサービスを提供する。

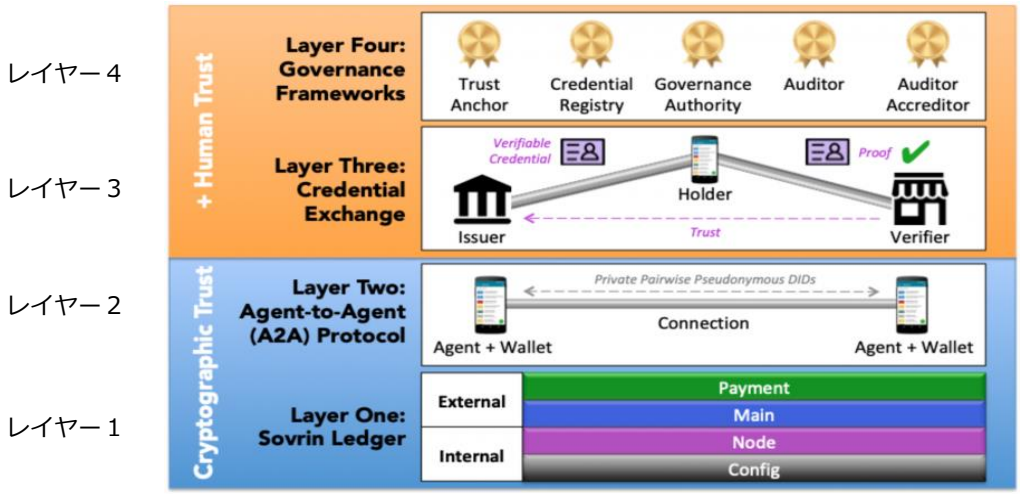
（出所）各種資料を基に作成

図表 B1-2 の例では、利用者は、自身で「分散型識別子」（Decentralized Identifiers、DIDs）を生成し、これを属性（資格や身元の情報）に紐づけた上で、属性を組み合わせてアイデンティティを構成する。分散型識別子と利用者の対応関係を集約的に管理する組織は必要とされず、利用者は特定の組織に依存することなく、自身のアイデンティティを構成したり利用したりできる。

自己主権型アイデンティティの実現を目指す非営利団体である Sovrin Foundation は、図表 B1-2 のような枠組みについて、４層のレイヤーに分けて整理している（図表 B1-3）。この整理では、自身で生成し所有できるよう設計された分散型識別子を管理する台帳が、基礎的な層として位置付けられている（レイヤー１）。この層の上に、利用者間にコネクションが確立され（レイヤー２）、検証可能な形で属性のやり取りが行

われる（レイヤー３）。そのためのデータモデルは Verifiable Credentials（VCs）と呼ばれ、分散型識別子とともに World Wide Web Consortium（W3C）により標準化されている[33]。レイヤー４は非技術層であり、資格や身元といった情報を社会で広く統一的に扱えるよう、発行者間のビジネスや法律上での合意を形成するガバナンスの層となっている。なお、レイヤー１において、システム基盤についても特定の主体に依存しない構造を実現し得るものとして、分散型台帳技術（Distributed Ledger Technology、DLT）の利用が注目されている。

図表 B1-3：Sovrin Foundation による階層図



（出所）Sovrin Foundation[34]

（2）自己主権型アイデンティティとプライバシー保護

自己主権型アイデンティティの考え方においては、利用者自身が標準化されたデータモデルを用いてサービスプロバイダーに情報を提供する。これにより、プライバシー保護の観点で、以下のような特長を持つと考えられる。

① 提供する情報の内容を制御する

自己主権型アイデンティティの考え方では、利用者自身が利用目的に応じた情報をサービスプロバイダーに提供する。このとき、サービスプロバイダーに収集される情報は必要最小限に抑えられ（データミニマイゼーション）、また、提供先であるサービ

[33] 詳細は、World Wide Web Consortium による分散型識別子の標準化関連ドキュメントを参照。https://www.w3.org/TR/did-core/

[34] Sovrin Foundation, https://sovrin.org/2020-how-ssi-went-mainstream/

スプロバイダーの名称などが属性の発行元に知られることもない。

さらに、ゼロ知識証明に関連した技術と組み合わせることで、発行済みの属性の集合の再発行を伴わずに、利用者の判断で不要な項目や情報を秘匿し、サービス利用の資格条件を満たすために必要な情報に限定して提供する方式の実現も期待される（ゼロ知識証明については、BOX2 を参照）。

② 提供先を制御する

利用者自らが属性の提供を行うため、利用者に属性提供の意思があることを前提とすることができる。少なくともサービスプロバイダーに対する一次的な属性提供については、利用者が関与しないまま行われることはない。

③ 提供先同士のデータの連結を抑止する

属性の提供先であるサービスプロバイダーごとに、どの識別子を用いて提供を行うかを利用者が選択できるため、複数の提供先が示し合わせて情報を「名寄せ」することで起こるプライバシー侵害を、ある程度抑制できる。

（3）自己主権型アイデンティティに関連する事例

カナダのブリティッシュ・コロンビア州は、デジタルガバメント推進の一環として、OrgBook BC と Verifiable Credentials for People という、デジタルアイデンティティに関わりの深い 2 つの取り組みを行っている[35]。OrgBook BC は、各種の政府機関が企業等に対して検証可能な属性として発行したビジネス上のライセンスや許可証を、Web サービス上で検索可能にした実運用中の公開登録簿であり、執筆時現在、400 万件以上の検証可能な属性が登録されている[36]。このサービスは、DIDs/VCs を扱う分散型台帳上に構築されることで、アイデンティティ管理が特定の組織に依存しない仕組みとなっている。このような分散型台帳を用いたアイデンティティ管理を、企業等でなく個人に適用する構想が Verifiable Credentials for People であり、市民が自身の属性についてのコントロールを得られるような枠組みが検討されている。

金融分野に関連する事例として、同国の Verified.Me が挙げられる。NPO の DIACC（Digital Identification and Authentication Council of Canada）が策定したフレームワークに基づき、SecureKey Technologies 社が、カナダの主要金融機関 7 社で構

[35] British Columbia, “BC Digital Trust” https://digital.gov.bc.ca/digital-trust/

[36] British Columbia, “OrgBook BC” https://www.orgbook.gov.bc.ca/search/

成されたコンソーシアムとともに、同サービスを 2019 年 5 月から提供している。ここでは、金融機関から成るコンソーシアムがアイデンティティ基盤を構成する分散型台帳を運営し、利用者は、金融機関、信用情報機関、通信事業者などの属性の発行元に指示を送ることで、自身の属性をサービスプロバイダーに提供できる。Verified.Me は、従来型のアイデンティティ（Federated Identity）と自己主権型アイデンティティを組み合わせることで双方の利点を生かすよう設計したとされている[37]。

[37] Secure Technologies, “A Primer and Action Guide to Decentralized Identity”, https://securekey.com/wp-content/uploads/2020/07/VerifiedMe_OWIWhitepaper_APrimertoDecentralizedIdentity.pdf, 2020.

BOX2：ゼロ知識証明の考え方と関連する技術

ゼロ知識証明（Zero-Knowledge Proof、ZKP）は、「ある人が、自分の主張が真であることを、それ以外の知識を明かさずに証明する（検証者に確信させる）手法」の総称である[38]。典型的には、離散対数問題など解を求めることが非常に困難とされる問題を用いて、解の情報を与えることなく、自分がその解を知っていることを検証者に確信させる形式を取る。

ゼロ知識証明は、例えばデジタル署名[39]などの暗号技術に組み込み、特定の情報を秘匿する特性を持たせることに用いられる。具体的には、グループ署名・リング署名やブラインド署名といったデジタル署名技術において、強固な匿名性の実現のためにゼロ知識証明が用いられる（図表 B2-1）。

図表 B2-1：ゼロ知識証明の考え方が具体化された例

グループ署名 リング署名	グループ署名は、予め構成したグループの任意のメンバーが、自身が署名者であることを明かすことなくグループを代表する署名を作成する技術である。グループには管理者が存在し、必要な場合には、署名者の特定やメンバーの匿名性の破棄を行うことができる。 リング署名は、このグループ署名をよりシンプルにした仕組みであり、署名者が任意の他者の公開鍵を借用し、他者の協力なくひとりで手続きを完結させる。グループ署名と異なり、グループの管理者を必要としない。借用した公開鍵に紐付く署名候補者の内、いずれかのメンバーにより署名されているということを証明しながらも、実際の署名者が自身であることを秘匿できる。
ブラインド 署名	ブラインド署名は、文書の内容を秘匿した状態で、当該文書へのデジタル署名の実施を権威等の主体（署名者）に移譲する技術である。これにより文書作成者は、文書の内容を署名者に開示することなく署名による内容の証明を受けることができ、それによって第三者による自身の特定を免れる。文書作成者と署名者との間で生じるやり取りの痕跡を何ら残さず署名されていることのみを証明することによる匿名性の強化や、署名者の協力なくして署名する手掛りを与えない偽造防止の厳密化において、ゼロ知識証明が利用され得る。

[38] ゼロ知識証明の手法は、一般に、完全性、健全性、ゼロ知識性を備えることが求められる。
・完全性：証明者の主張が真なら、真であることを検証者が分かること
・健全性：証明者の主張が偽なら、偽であることを検証者が高い確率で見抜けること
・ゼロ知識性：検証者は、証明者の主張が真であること以外の知識を得られないこと

[39] デジタル署名は、他者に伝える文書が自身によって作成されたものであることや、内容に改変がないことを保証する技術である。検証者は文書と署名の内容とを照合することによって、改変が行われていないことを確認できる。デジタル署名は文書の作成者の秘密情報にて行われるため、文書とその作成者とは署名により紐付けられる。

ゼロ知識証明の考え方は、以下のようなプライバシー保護に関連した背景もあって、近年、関心を集めている。ひとつは、データミニマイゼーションに対する関心の高まりである。利用者認証などにおいて、従来は必要とされていた情報の提示を、ゼロ知識証明を適用することにより不要にできるのではないか、という期待もある。こうした動きは、提示情報のより細やかな選択を可能にし、利用者のプライバシー強化につながる。

もうひとつは、分散型台帳技術との関係である。分散型台帳について、多くの分野で実装に向けた取り組みが進行しているが、一般に、複数の参加者が情報を共有することになるため、秘匿性の担保がハードルとなることがある。ゼロ知識証明の仕組みを導入すれば、台帳に書き込む情報のすべてを明かさずとも他者による検証を行い得るため、関心を集めている。例えば ZCash では、zk-SNARKs と呼ばれるゼロ知識証明の仕組みを利用し、送金額や送金先といった取引情報を秘匿した状態で、当該取引に不整合がないことを他者が検証できる[40]。また、Ethereum でも、zk-SNARKs を利用して秘匿性を担保したプログラム（スマートコントラクト）を実行できる。このようなゼロ知識証明の仕組みは、情報が公開されるパブリックな分散型台帳にあっても、利用者が実データを自ら管理できるという選択肢を与えている。

現時点では、必要とされる計算量の大きさなどから、ゼロ知識証明の考え方に基づいた認証技術が幅広くサービスに実装されているとはいえないが、社会の関心は高く研究の進展が期待されている。

[40] Ben-Sasson, Eli et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin", IEEE Symposium on Security and Privacy, 2014.