中央銀行デジタル通貨（CBDC）に関するレポート

2022 年 8 月

国立印刷局 CBDC 研究会

目　次

本レポートは、国立印刷局内の「中央銀行デジタル通貨に係る研究会」に関係する職員の調査・研究成果であり、今後、CBDC の検討を進める一助としての考えをまとめたものです。なお、レポート内で示された内容や意見は、執筆者個人の見解であり、国立印刷局の公式見解を示すものではありません。

1　はじめに

2019 年末に初めて確認された新型コロナウイルス感染症は、新たな変異株の発生などを繰り返しながら、現在も感染拡大が続いている。その結果、海外渡航を含む移動の制限、新たな生活様式への変化など、社会のデジタル化が製造業、小売業、流通業などあらゆる分野で進んでおり、決済に関しても同様に電子商取引やキャッシュレスによる決済が増加するなど環境の変化が見られる。

そのような中、政府は、デジタル庁を創設し、関連法令の整備、デジタル社会の実現に向けた重点計画の策定など国を挙げての取組をより具体的に進めている状況にあり、骨太の方針 2021 には、４つの原動力と基盤づくりの柱の一つとして「官民挙げたデジタル化の加速」が掲げられた。また、同方針には、中央銀行デジタル通貨（以下「ＣＢＤＣ」）に関して、政府・日銀が、2022 年度中までに行う概念実証の結果を踏まえ、制度設計の大枠を整理し、パイロット実験や発行の実現可能性・法制面の検討を進めることが記載され、デジタル社会における重要インフラとしてのＣＢＤＣの必要性が高まってきていると考えられる。

日本銀行においては、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」にて整理した機能と役割、具備すべき基本的な特性を実現するための検証として、一般利用型ＣＢＤＣの概念実証実験を 2021 年４月から開始した。また、その進捗や進め方については、中央銀行デジタル通貨に関する連絡協議会やＣＢＤＣに活用し得る技術動向を共有するフォーラムなどを通じて、民間事業者や有識者と共有しつつ知見を得ながら検討が進められている。

一方、国外に目を移すと、国民を巻き込んだ実証実験やアプリの配信など計画的な取組を進めてきた中国では、北京五輪にて海外関係者にアプリやハードウォレットを通じたデジタル人民元を提供し、利用を図り、本格的な発行に向けた準備を進めている状況にある。これに対して、主要国の動向としては、欧州中央銀行（以下「ＥＣＢ」）が 2021 年７月にＣＢＤＣ発行に向けた本格的な準備を始めると公表し、加えて、連邦準備銀行（以下「ＦＲＢ」）が 2022 年１月に初めて報告書を公表するなど各国においても検討が加速している。

このような状況下において、国立印刷局としては、これまで銀行券製造を通じて通貨制度の安定に寄与してきた視点をもって、ＣＢＤＣの設計に係る課題、その解決に必要な対応などを検討するために、2020 年度から研究を開始してきており、2021 年度は、国内外の動向を注視しつつ、ＣＢＤＣを社会実装するために必要な技術的な要素を調査し、かつ、配慮すべき事項など具体的な情報を整理したレポートとして取りまとめたことから、報告するものである。

2　環境分析

2.1　政府動向

2.1.1　政府

政府は、2021 年６月 18 日に「経済財政運営と改革の基本方針 2021」を閣議決定した。官民を挙げたデジタル化の加速に向けては、デジタル時代の官民インフラを今後５年で作り上げるものとして示す中、ＣＢＤＣについて、政府・日銀は 2022 年度中までに行う概念実証の結果を踏まえ、制度設計の大枠を整理し、パイロット実験や発行の実現可能性・法制面の検討を進めるものとしている。

その他、デジタル社会の実現に向けては、デジタル社会形成基本法をはじめとするデジタル改革関連法[1]が 2021 年５月 12 日に可決し、同年 9 月 1 日に施行されている。また、デジタル社会形成基本法第 37 条第１項に規定する重点計画として、「デジタル社会の実現に向けた重点計画」を 2021 年 12 月 24 日に閣議決定し、計画に記載された「デジタル原則」に基づき、必要となる施策等の追加・見直しの検討・整理を進めることとしており、計画内には、世界トップレベルのデジタル国家を目指し、それにふさわしいデジタル基盤を構築するための包括的なデータ戦略も定められている。

併せて、2021 年 11 月に内閣総理大臣を会長とする「デジタル臨時行政調査会[2]」を設置し、デジタル改革、規制改革、行政改革といった構造改革に係る横断的課題の一体的な検討や実行を強力に推進することとしている。

2.1.2　日本銀行

(1)実証実験

日本銀行は、ＣＢＤＣに関する技術的な実現可能性を検証するため、実証実験を段階的、計画的に進めるものとして、2021 年４月から概念実証（Proof of Concept）を開始し、そのプロセスを通じてＣＢＤＣの機能や特性が技術的に実現可能かを検証している。フェーズ１では、ＣＢＤＣの取引を記録する「ＣＢＤＣ台帳」を中心に、システム的な実験環境内において中核をなす発行、流通、還収に関する技術的な検証が進められている。

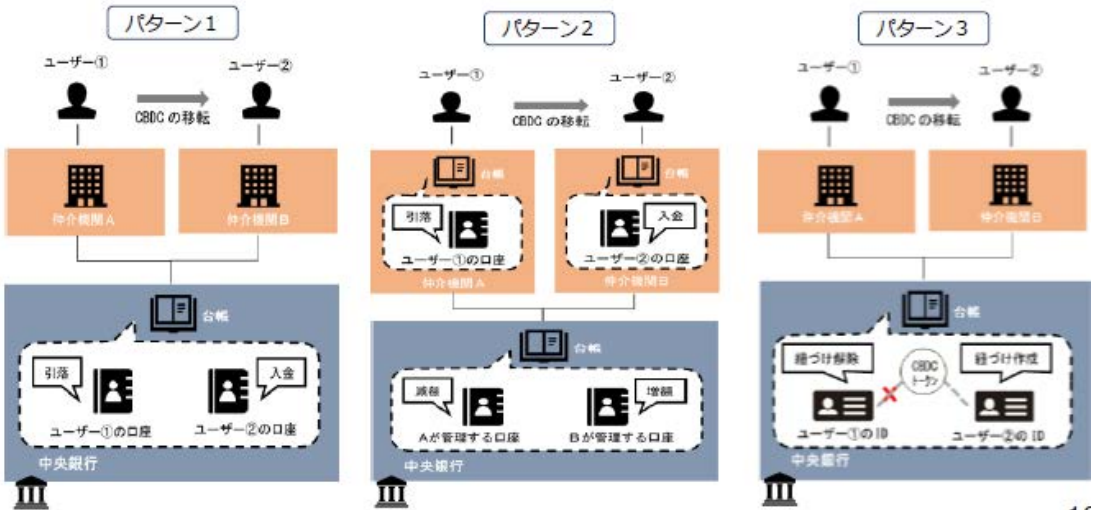
なお、検証においては、台帳の設計パターンごとに実機検証及び机上検証を行い、実機検証では、業務処理の適切性やシステムの性能を、机上検証ではシステム性能の拡張性や追加的な機能拡張の容易性などを理論的に比較・検証されており、2022 年３月までの計画に対し、予定どおり終了している[3]。

さらに、システムの性能に関する検証においては、高負荷シナリオにおけるスループット（処理件数）の低下度合や、レイテンシー（処理速度）などの数

値測定結果などから、各パターンにおける具体的な課題やボトルネックを特定している。

その後のフェーズ２は、2022 年４月から開始しており、ＣＢＤＣの「基本機能」に、ＣＢＤＣの「周辺機能」を付加して、その技術的な実現可能性や課題を検証するとされている。

	パターン1	パターン2	パターン3
台帳の管理主体	中央銀行	中央銀行・仲介機関	中央銀行
金銭データへのID の付与	付与しない（口座型）	付与しない（口座型）	付与する（トークン型）



出典：日本銀行決済機構局、2021.10.15「中央銀行デジタル通貨に関する日本銀行の取り組み」
（https://www.boj.or.jp/announcements/release_2021/rel211015c.pdf）

図 2.1　日本銀行の実証実験における台帳の設計パターン

(2) 連絡協議会

日本銀行は、2021 年３月 26 日に「中央銀行デジタル通貨に関する連絡協議会」を設置し、同年４月から開始した概念実証実験の円滑な実施に資する環境を整えている。協議会は、2021 年３月、10 月、2022 年４月に開催されており、概念実証実験の内容やその進捗状況等について、民間事業者や政府との情報共有を図るとともに、進め方についても協議されている。

なお、2021 年 10 月の協議会においては、主要国中銀共同研究グループ[4]が 2020 年 10 月から継続的に行った議論を整理し、2021 年９月末に公表した報告書の内容も踏まえて、「水平的共存」と「垂直的共存」という考えを示し、様々な決済手段や主体が関わり、ＣＢＤＣの実現を目指すことが新たに共有されている。

(3) その他

概念実証を日本銀行内で進める一方、2021 年度には、中央銀行デジタル通貨を支える技術に関して、「決済の未来フォーラム」の中で、技術面からみた将来のＣＢＤＣのあり方などについて意見交換が交わされており、これらは、フォーラムというオープンな場で共有されている。

表 2.1　決済の未来フォーラムテーマ（2021 年度分）

日程	テーマ	関連企業等
2021.6	CBDC に求められるセキュリティ	セコム㈱、日本電気㈱
	CBDC に求められるユニバーサルアクセス	㈱NTT ドコモ、App Annie Japan㈱
	デジタル通貨に関連する情報技術の標準化	日本銀行決済機構局
2021.11	決済インフラの強靭性に関する技術とノウハウ	日本電信電話㈱、ソフトバンク㈱、㈱ローソン
	決済サービスにおける迅速性の実現	㈱ジェーシービー、トヨタファイナンシャルサービス㈱
2022.1	デジタル通貨とプログラマブル性	三菱商事㈱、㈱LayerX、㈱NTTデータ
	セキュアな決済を支えるユーザーデバイス	ソニー㈱、大日本印刷㈱、㈱TRUSTDOCK

出典：日本銀行、「決済の未来フォーラムデジタル通貨分科会：中央銀行デジタル通貨を支える技術」、「決済の未来フォーラムデジタル通貨分科会：中央銀行デジタル通貨を支える技術（第2回会合）」、「決済の未来フォーラムデジタル通貨分科会：中央銀行デジタル通貨を支える技術（第3回会合）」を参考に作成
https://www.boj.or.jp/announcements/release_2021/rel210616b.htm/
https://www.boj.or.jp/announcements/release_2021/rel211130d.htm/
https://www.boj.or.jp/announcements/release_2022/rel220114c.htm/

2.1.3　民間デジタル通貨

ブロックチェーン技術の成熟を背景に、世界的にもリブラやその他のステーブルコインの発行など官民で新たな取組が始まっており、新たな決済インフラとしてのデジタル通貨の重要性が高まっていることを受け、日本国内のメガバンクや大手企業は、「デジタル通貨勉強会」を 2020 年６月に発足した。勉強会においては、現金に代わる決済手段としてのデジタル通貨の望ましい姿を検討し、現状の決済インフラの課題と解決策を議論し、同年 11 月に提言としての報告書を公表している。報告書の公表と合わせて、勉強会を「デジタル通貨フォーラム[5]」に改め、2021 年１月から様々なユースケースの概念実証を行うなど、デジタル通貨のコアとなる共通領域と、ビジネス上で活用可能なスマートコントラクトの実装に係る付加領域、それぞれの分科会で議論が進められた。その成果として、2021 年 11 月に「ＤＣＪＰＹ（仮称）ホワイトペーパー」、「デジタル通貨フォーラムプログレスレポート」を公表し、2022 年度中にデジタル通貨「ＤＣＪＰＹ」及びその運用を支えるプラットフォームの実用化を目指すこととしている。

表 2.2　ＤＣＪＰＹの特徴

項目	概要
連動通貨	円
発行主体	銀行（当面、銀行の債務（預金）と位置付けて発行）
口座管理	各銀行
付利	なし
構成	ブロックチェーン（許可型）　合意形成アルゴリズム：PBFT
秘匿性	暗号理論など活用
透明性	全てのノードの状態を検証可能

出典:デジタル通貨フォーラム、「DCJPY(仮称)ホワイトペーパー(2021年)」を参考に作成
https://www.decurret-dcp.com/.assets/forum_20211124wp.pdf

2.2　各国の動向

2.2.1　中国

(1) 中国人民銀行の取組概要

中国人民銀行は、2021 年 7 月にデジタル人民元（e-CNY）システムの背景、目的・ビジョン、設計フレームワーク、政策的検討事項を説明した白書「中国におけるデジタル人民元の調査研究の進展」[6]を公表している。

また、2022 年 2 月の北京オリンピックまでにデジタル人民元の試験的発行を目指すとして 2020 年 10 月から市民参加型の実証実験を開始した。この実証実験では、2021 年 6 月までに北京や上海、西安、蘇州などの大都市を中心に全国 23 都市にまで範囲を広げ、累計の取引回数 1 億 5,000 万回、取引額は 620 億元を超えたと言われている[7]。2022 年 2 月の北京五輪においては、海外からの入国者に対してもアプリやハードウォレットを提供することで、実際にデジタル人民元を利用させ、国際的なアピールを強めている。

併せて、中国人民銀行は、2020 年 10 月に中華人民共和国中国人民銀行法の改正草案を公表し、意見募集を行っている。公表された草案におけるデジタル人民元に関連する主な変更点は、以下の３点である。

① 人民元の定義に従来の現金通貨に加え、デジタル通貨を含める
② 組織や個人による人民元に代わるデジタル通貨の発行禁止
③ 人民元の代替となるデジタル通貨の発行行為に対する罰則

上記法改正により、今後発行されるデジタル人民元が中国国内で流通する唯一の人民元のデジタル通貨となる[8]ことを示している。

(2) デジタル人民元の設計

中国の取組は、主要国の中で最も進んでおり、その設計に関しては、2021 年 7 月公表の白書内に大枠が記載されている。その中で、デジタル人民元は、物理的な人民元が持つ支払時の決済や匿名性といった特徴と、電子決済手段が持つコストの低さ、携帯性、効率性、耐偽造性といった特徴の双方を併せ持つものとして設計していると記載されている。技術的には、集中型と分散型のハイブリッド型アーキテクチャとすることで、取引処理やデータ保存の能力が要件を満たさないと判断した分散型台帳技術について、現段階では優位とされる分野でのみ使用しつつ、技術の進化に合わせて機能追加を視野に入れている。なお、主な設計要件は、以下のとおりである。

〈設計〉

・口座型とトークン型のハイブリッド型
・少額決済は匿名、高額決済は追跡可能
・デジタル証明書、デジタル署名、暗号化技術などにより偽変造対策

・スマートコントラクトを可能とする設計
・ウォレット設計（制御可能な匿名性に向けて）

	認証情報		取引情報
	運営機関	人民銀行	運営機関
収集	四類 携帯番号 SMS認証コード	携帯番号 SMS認証コード ログインパスワードなど	取引データ・取引先の携帯番号やウォレットアドレス、決済パスワードなど
	三類 携帯番号 SMS認証コード 名前、顔認証データ、身分証明書番号など	携帯番号 SMS認証コード ログインパスワード、身分証明書番号など	
	一・二類 携帯番号 SMS認証コード 名前、顔認証データ、身分証明書番号、銀行カード番号など		
管理	運営機関	人民銀行（認証センター）	運営機関 人民銀行（登録センター）

出典：野村総合研究所 Financial Information Technology Focus 2022.1 デジタル人民元の「制御可能な匿名性」
(https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/kinyu_itf/2022/01/itf_202201_07.pdf)

図 2.3　デジタル人民元のウォレットの情報管理

〈運営〉
・二層運営
　中央銀行：発行、廃棄、機関間接続、ウォレットのエコシステム管理
　仲介機関：本人確認、顧客ウォレットの開設、e-CNY 交換
〈技術ロードマップの選択〉
長期的な進化、絶え間ない反復、ダイナミックなアップグレードが特徴
・分散型、プラットフォームベースの設計
（回復力、拡張性、取引量増加への対応）
・信頼できるコンピューティングと特殊な暗号化技術
・多層のセキュリティシステム
・集中型アーキテクチャと分散型アーキテクチャのハイブリッド
・定常状態とアジャイル状態を共存（統合的な開発）

(3) 中国人民銀行の技術開発動向

前述のとおり、中国人民銀行はデジタル人民元の設計において、長期的な進化を可能とするシステムを目指すものとしている。そこで、中国人民銀行の開発の動向、方向性を確認するために、特許出願状況を調査することとした。

なお、調査概要は表 2.3 のとおりであり、中国人民銀行が中国特許庁に出願した件数、分類等を調査している。

表 2.3　中国人民銀行特許調査概要

調査対象期間	出願日 2011 年 1 月 1 日～2021 年 7 月発行分
対象文献種別	中国特許・実用新案
検索データベース	Patent Square（中国）
対象特許分類	特許分類クラス G、H
チェックワード	Digital, electronic, crypto, cryptocurrency, virtual, stable, fiat, currency, money, bill, note, coin, cash, exchange, payment, pay, wallet, purse, finance, financial, fintech, central, bank, fund, retail, bitcoin, CNY, yuan, renminbi, RMB, DC/EP, PBOC, CBDC, anonymity, trace, interest, limit, balance, KYC

調査の結果は、図 2.4 のとおりである。2015 年以前は、偽造防止技術など銀行券に関連する特許を出願していたが、2016 年を境にＣＢＤＣやデジタル通貨に関連する特許が大半を占めるようになった。また、ブロックチェーン関係特許は、2019 年から増え始めており、中国国内において進められている実証実験の設計に使用されている技術とは別に、将来のブロックチェーン関連技術の活用を視野に入れた研究が進められていると推察できる。

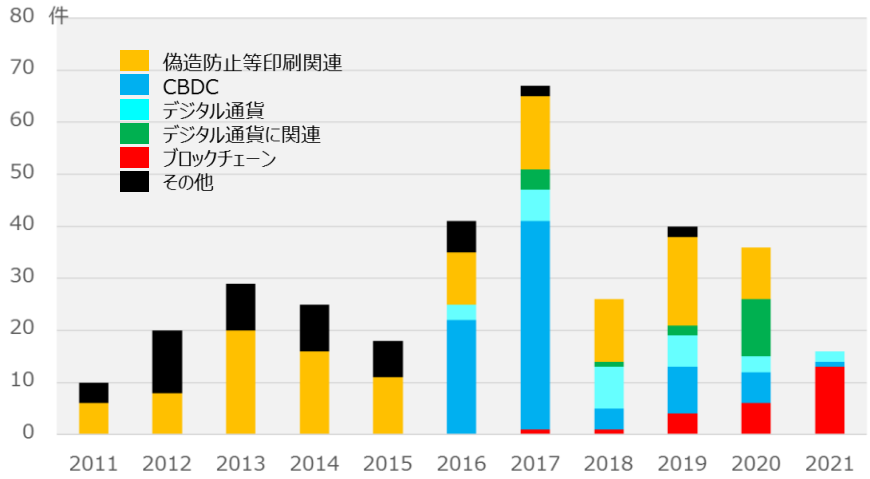


図 2.4　中国人民銀行の特許出願状況

2.2.2　連邦準備銀行

連邦準備銀行（以下「ＦＲＢ」）は、ＣＢＤＣを発行することの意味とその選択肢を探るため、数年にわたりＣＢＤＣの研究を進めてきている。2022 年 1 月には、ＤＸ時代における米ドルと称してレポートを公表[9]し、幅広い関係者から意見を聴取し、協議を行うための最初の段階に踏み入ったところである。

同レポートにおいては、研究を進めるに当たってのＣＢＤＣのあるべき姿の記載に始まり、既存通貨及び決済システムの特長と課題、新たなデジタル資産について整理した上で、ＣＢＤＣに必要な要素を整理されている。ＦＲＢは、幅広な設計オプションを継続的に検討するとしながら、現時点で米国内のニーズに応えるためには、プライバシー保護、仲介発行、資産の容易な移転、本人確認（ＡＭＬ[10]／ＣＦＴ[11]）が必要としている。そして、ＣＢＤＣが有する数ある潜在的利点に「ドルの国際的役割」を掲げ、米ドルの国際的（支配的）な役割を維持することがあるとしている。なお、ＦＲＢでは、以下の状況にあると判断した場合のみ検討を進めるとし、発行の必要性に関して慎重に判断する姿勢を示している。

① ＣＢＤＣを導入した場合のメリットと、潜在的なリスクを比較し、メリットの方が大きいと結論付けられる。
② 当該メリットを実現するためのより効果的な代替手段が存在しない。
③ 一般国民や政府・議会など横断的な広い協力を得られるような状況にある。

2.2.3 欧州中央銀行

欧州中央銀行（以下「ＥＣＢ」）は、ＣＢＤＣに関する報告書を 2020 年 10 月に公表しており、デジタル・ユーロの設計に関して、導入する上で守るべき事項と導入するとした場合の意義・要件、機能設計の可能性、技術的論点などが整理されている。その上で、予備実験を進め、機能設計の可能性や技術的な確認をすることで、関係者間で理解を深めてきた。予備実験は、4 つの作業部会にて行われ、その結果は、①デジタル・ユーロ台帳、②プライバシーとマネロン対策、③デジタル・ユーロへの制限、④最終利用者の接続といった観点で評価され、評価された設計オプションのいずれにも大きな技術的障害は特定されなかったと報告されている[12]。これら予備実験で得られた知見から、ＥＣＢ理事会[13]は 2021 年 7 月にデジタルユーロプロジェクトを立ち上げ、2021 年 10 月から 24 か月間にわたって調査段階を実施することを決定した。そして、調査の結果により、導入の意思決定がされた場合には、デジタル・ユーロの開発準備（約 3 年間[14]）に進むと言われている。

表 2.4　デジタル・ユーロに係る作業部会の主な知見

作業部会	主な知見
既存システムの拡張 既存決済システム上でのデジタル・ユーロの導入調査	①　デジタル・ユーロ台帳 作業効率・柔軟性、環境負荷などの知見
実現可能性の組合せ 中央集権と分散型を含む複数基盤の結合調査	②　プライバシーとAML 秘匿性に関する知見
新手法 ブロックチェーン及びトークンによる実現性の調査	③　デジタル・ユーロの流通制限 保有・取引制限、付利などについての知見
トークン型通貨 開発済オフライン決済手段へのデジタル・ユーロ導入調査	④　最終利用者の接続 利用者認証(本人確認)などについての知見

出典：ニッセイ基礎研究所、「デジタルユーロプロジェクト始動」2021.9.2　を参考に作成

https://www.nli-research.co.jp/files/topics/68632_ext_18_0.pdf?site=nli

2.2.4　その他

2020 年 10 月にバハマやカンボジア[15]でＣＢＤＣが発行され、2021 年 10 月にはナイジェリアにおいて「e-Naira」が発行された。ナイジェリアの現地報道によると、民間発行のステーブルコインに対する対応策とみられており[16]、ナイジェリアでは暗号資産への取締り強化の動きが強いものと思われる。新興国においては、金融包摂が発行理由の一つとしてあったが、ステーブルコイン、暗号資産、他国ＣＢＤＣへの自国通貨流出に関しても各国の強い発行動機となることが考えられる。

図 2.5　各国のＣＢＤＣ検討状況

[1] デジタル改革関連法は、(1)デジタル庁設置法、(2)デジタル社会の形成を図るための関係法律の整備に関する法律、(3)公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律、(4)預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する法律、(5)デジタル社会形成基本法案、(6)地方公共団体情報システムの標準化に関する法律から成る。

[2] 国や地方の制度・システム等の構造変革を早急に進め、個人や事業者が新たな付加価値を創出しやすい社会とすることを目的としたデジタル庁が所管する会合

[3] 中央銀行デジタル通貨に関する実証実験「概念実証フェーズ 1」結果報告書　日本銀行決済機構局 2022 年 4 月 13 日

[4] 2020 年 1 月に共同研究をスタート。7 つの先進国中銀(日、米、ユーロ、英、カナダ、スイス、スウェーデン)と国際決済銀行が参加。2020 年 10 月に、一般利用型 CBDC に求められる「基本原則①物価の安定・金融システムの安定を損なわない、②公的・民間マネーとの共存・補完、③イノベーションと効率性の促進」を公表。その後も密接に連携し、当該原則に沿ってより掘り下げた政策分析や実務的検討を継続している。

[5] 国内メガバンク、大手企業が出資し設立した、株式会社ディーカレットホールディングス、株式会社ディーカレット DCP が運営するフォーラムである。資料として「DCJPY(仮称)ホワイトペーパー」、「デジタル通貨フォーラム プログレスレポート」を作成している。

[6] Progress of Research & Development of E-CNY in China　2021.7 中国人民銀行

[7] 次世代中国　一歩先の大市場を読む「中国のデジタル人民元は「統治のツール」？操作可能な匿名性が目指すものとは」(2021.12.21)NEC　https://wisdom.nec.com/ja/series/tanaka/2021122101/index.html

[8] デジタル人民元レポートシリーズ№.2　「デジタル人民元発行に向けた歩みと最近の動向」(2021.2.16)大和総研 https://www.dir.co.jp/report/research/capital-mkt/it/20210216_022091.pdf

[9] Money and Payments:The U.S. Dollar in the Age of Digital Transformation　January 2022 https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

[10] AML は、Anti Money Laundering(マネーロンダリング対策)の略称

[11] CFT は、Countering the Financing of Terrorism(テロ資金供与対策)の略称

[12] ECB プレスリリースより　Eurosystem launches digital euro project　2021.7.14 https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

[13] 欧州中央銀行(European Central Bank)の最高意思決定機関のことで、ユーロ圏の統一的な金融政策を決定する。 6週間毎に開催され、役員会メンバー6名(総裁、副総裁、理事4名)とユーロ圏の中銀総裁 19 名の計 25 名で構成される。

[14] ECB パネッタ理事によるブログ記事(2021.7.14) https://www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog210714~6bfc156386.en.html

[15] カンボジア中央銀行は、バコンを CBDC と定義しておらず、不換紙幣(リエル、ドル)でバックアップされた決済システムであるとしている。 そのため、バコンは準 CBDC と呼ばれることもある。
JETRO「ベストプラクティスからみるバハマとカンボジアの CBDC 導入戦略」(2021 年) https://www.jetro.go.jp/biz/areareports/2021/93af43aeec2839e7.html

[16] JETRO「ビジネス短信　ジェトロの海外ニュース」(2021 年)ナイジェリア中銀、電子通貨「イーナイラ」をリリース https://www.jetro.go.jp/biznews/2021/10/64bfef366b0b9156.html

3　暗号資産、電子マネー等の事件・犯罪

3.1　概要

暗号資産、電子マネー等についての事件・犯罪を理解することは、ＣＢＤＣやデジタル通貨が普及する際のリスクを想定することにつながる。そこで、近年の傾向を改めて整理し、想定されるリスクを幅広に把握することで、ＣＢＤＣ設計の検討における一助とする。

3.2　国内の金融機関への攻撃

近年の動向として、2021 年末までの動向を整理した。その結果、国内の金融機関の利用者を標的として顧客情報を不正に取得するサイバー攻撃（フィッシングなど）が 2021 年度に入り複数発生していることがわかる。国内の金融機関の資産へ不正にアクセスし、出金するような事例は見られていないが、顧客情報のフィッシングは多く[1]、金融のデジタル化が進む場合、情報の重要性は一層高まることから、利用者保護の観点から警戒が必要となる。

表 3.1　金融機関へのサイバー攻撃事例

No.	日付	事業者名	事象概要	被害
1	2021 年 4 月 8 日	A 銀行	「●●カードから重要なお知らせ」というメールを送信し、偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象は ID、パスワード、カード番号、有効期限、口座番号、セキュリティコード、カード暗証番号等。
2	2021 年 4 月 25 日	B 証券	第三者からの不正アクセスの影響により、オンライントレードシステムに障害が発生、一部商品のオンラインでのトレードは中止し、電話のみでの顧客対応に移行。	不正アクセス時に外部への持ち出しが可能な状態であったデータ（最大値）は、以下のとおり。 ① 個人顧客情報　31,411 件 （口座、氏名、生年月日、電話番号、住所、勤務先、メールアドレス、銀行口座等） ② 法人顧客情報　2,790 件 （口座、会社名、電話番号、住所、メールアドレス、銀行口座等） 不正アクセス対象システムについては 2021 年 12 月 20 日をもって廃止、当社顧客については、吸収分割した他社に移行予定。
3	2021 年 5 月 6 日	C 銀行	「【重要なお知らせ】C 銀行 ID 必要の再アクティブ化リクエスト」というメールを送信し、偽サイトへ誘導、顧客情報を不	件数は不明。 対象は利用者 ID、ログインパスワード、アカウント指定方法、暗証番号、セキュリティカード情報（両面の情報を PDF,PNG,JPEG 形式で取

			正に取得する事象が発生（フィッシング）	得)。
4	2021 年 6 月 24 日	D 銀行	顧客申込情報を管理する外部クラウドに不正アクセスが発生、顧客情報が流出	245 件の姓名、メールアドレスが対象。 また、一部顧客については、以下の情報が漏えい。 電話番号、携帯電話番号、生年月日、性別、住所、職業、職場の名称、職場の電話番号、店舗名、店番号、口座番号。
5	2021 年 6 月 29 日	E 銀行	「E 銀行からのお知らせ」というメールを送信し、偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象はログインパスワード、店番号、口座番号、暗証番号、カード番号。
6	2021 年 7 月 5 日	F 銀行	「【F 銀行】から重要なお知らせ」というメールを送信し、偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象は店番号、口座番号、契約者番号、第一暗証、携帯電話、暗証番号、生年月日等。
7	2021 年 8 月 13 日	G 銀行	「【重要】カードご利用内容の確認のお願いのお知らせ」というメールを送信し、偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象は契約者番号、ダイレクトパスワード、店番、口座番号、名前、生年月日、暗証番号等。
8	2021 年 11 月 10 日	F 銀行	「【社名】セキュリティシステム更新通知、【F 銀行】異常振込入金のお知らせ」などのメールを送信し、偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象は店番号、口座番号、契約者番号、ログイン暗証、携帯番号、暗証番号、生年月日等。
9	2021 年 11 月 10 日	H 銀行	「H 銀行-お客さまの口座間送金管理」「H 会社から緊急のご連絡」というメールを送信し偽サイトへ誘導、顧客情報を不正に取得する事象が発生（フィッシング）	件数は不明。 対象は店番、口座番号、ログインパスワード、名前、キャッシュカード暗証番号、電話番号、生年月日、住所等。

3.3　国内外の暗号資産取引所へのサイバー攻撃等

サイバーセキュリティの専門企業（CipherTrace、Chainalysis）の調査結果[2、3]では、暗号資産取引に関する攻撃の対象が個人-個人間での取引場を提供する分散型取引所（Decentralized Exchange、以下「ＤＥＸ」）にシフトしてきており、2021 年に盗まれた 18 億 1,000 万ドルの資金の大部分が、ＤＥＸプラットフォームを標的にした攻撃であったことが報告されている。

ＤＥＸへの攻撃方法としては、2021 年度には「大量の暗号資産をフラッシュローン（単独のトランザクションで完了する場合、無担保で取引可能な融資）で借用し、システムの脆弱性を狙って相場を大きく操作し、裁定取引を実行、利益を得る」という「フラッシュローン攻撃（以下「ＦＬ攻撃」）」が連続的に発生した。

また、ＦＬ攻撃ではないが、日本国内の取引所に関係する事件として、8 月 19 日に大手暗号資産取引所のシンガポール法人がハッキングの被害を受けている。狙われたのは流動性を高めるためにネットワークに接続した状態で管理していたウォームウォレットの資産であった。

その他、攻撃の被害となった企業が存在する一方で、悪意ある業者が開発した新しいトークンを投資家にプロモーションし、価値の上昇を期待した投資家に取引を開始させた後、トークンを突如停止し、流動性プールから資金を抜き取り、行方をくらますという手口の「RugPull」詐欺が発生しており、利用者保護の観点から注視すべき事象となっている。

2021 年に発生した暗号資産取引に係る攻撃事案は、表 3.2 のとおりである。

表 3.2　暗号資産取引所における攻撃の詳細（2021 年発生分）

No.	企業名	発生時期	対象資産	被害金額（ドル）	FL 攻撃	Rug Pull	内容
1	A 社	2021/2/4	DAI, ETH, 3Crv, y3Crv	約 280 万	○		プログラムの脆弱性を悪用したスリッページ（裁定取引時に発生するレートの変動）の反復発生により、資産の流出が発生。
2	B 社	2021/2/13	sUSD, WETH, USDC, DAI, USDT	約 3,700 万			次期リリースに備えてあらかじめ作成した非公開の暗号資産プール（sUSD、流動性なし）に対して、攻撃者が連続的に借用するコマンドを実施。 複数の当事者が存在している際には発生しない脆弱性に関して、攻撃者が唯一の当事者となったことにより資産が流出。

3	C 社	2021/2/27	ETH, WBTC	約 1,400 万			攻撃者は偽のスマートコントラクトを作成し、Furucombo が新しくアプリを実装したと偽装。 結果、ユーザからの転送資産がすべて攻撃者のアドレスに転送。
4	D 社	2021/3/5	ETH 他	約 1.8 億			攻撃者はスマートコントラクトの制御に関する秘密鍵の窃取と、その鍵を使用したトークンの反復発行、償却により ETH を不正取得。
5	E 社	2021/3/6	BUSD, BNB	約 3,100 万		○	プロジェクト立ち上げから 48 時間以内の時点で、攻撃を受けて資産が流出。 一方、スマートコントラクトのハッキングがプロジェクト開始前日に E 社サービスのアカウントを使用して実施されたため、秘密鍵の窃取もしくは「Rug Pull」が発生したと考えられる。 事件後に E 社の HP やツイッターアカウントが削除されたことから、Rug Pull の疑惑が深まった。
6	F 社	2021/3/8	USDT, ETHA, WSZO, vETH, WETH	約 380 万	○		攻撃者はスマートコントラクトのバグを利用し、フラッシュローンを実行してすべてのトークンの転送、トークンの不正作成を実施。
7	G 社	2021/3/14	$WHALE, $RARE, $PICA, ETH	約 570 万			プラットフォームのセキュリティ侵害により、攻撃者がホットウォレットの秘密鍵を入手、ウォレット内のトークンを窃取。 攻撃者はプライバシー強化がなされた事業者を通じて資金の流れの匿名化を図ったとみられる。
8	H 社	2021/3/19	TTDX, BNB, ETH	約 250 万		○	DeFi プロジェクトである H 社は、専用トークンの販売開始から数日後に当該資産の流動性を低下させることにより資産を不正に移転。 もともとプロジェクトは監査を受けていたが、重要なセキュリティ問題については特定されず。 なお、資産の移転後にプロ

							ジェクトのHPやツイッターは閉鎖され、運営者は音信不通。
9	I社	2021/4/19	DAI, USDT, EASY Token	約8,000万			I社設立者兼CEOのPCに攻撃者がハッキング、DeFiスマートコントラクトのMetamaskのアカウントを乗っ取った上でMetamask内に存在する各種暗号資産を窃取。
10	J社	2021/4/22	ー	約20億		○	前日まで販売促進のキャンペーンを実施していた暗号資産交換所が突如「メンテナンス」と称して取引を停止し、経営者は預かっていた資産を持って海外へ逃亡。
11	K社	2021/4/27	BTC, ETH, DOT, ADA, USDT, u92	約5,000万		○	ローンチ後1ヶ月のプラットフォームが攻撃者によりバグを利用されハッキングを受けたと主張。運用開始直後の攻撃を踏まえると、RugPullの疑いあり。
12	L社	2021/5/2	SPARTA, WBNB	約3,000万	○		原資産を引き出すために、プール・トークンを償却する際、必要以上の原資産を引き出すというバグが発生したことに起因して大量の損失が発生。
13	M社	2021/5/8	ETH, ibETH	約1,100万	○		前出のL社と同様、プールトークンの償却による原資産の過剰引き出しバグの発生により損失が発生。
14	N社	2021/5/12	ETH, xSNXa, xBNTa	約2,500万	○		フラッシュローンを使用して原資を借り入れ、大量のxSNXaトークンを作成するとともに、xBNTaをN社のコントラクトではチェックできないという欠陥を利用し、別のトークンを使用してxBNTaトークンを不正に作成し、売却。
15	O社	2021/5/20	BUNNY, BNB	約2億	○		攻撃者はBinance Coin(BNB)についてフラッシュローンを利用し大量に借りた後、資産の価格を操作してプラットフォームのBUNNY/BNB市場に投げ売り

							した。
16	P 社	2021/6/16	USDC, IRON, TITAN	約 20 億			ステーブルコインと称していた暗号資産がバグにより価格安定に失敗、暴落を起こした結果、取り付け騒ぎが発生。
17	Q 社	2021/6/23	BUSD, USDC	約　2,200 万		○	検証時に別のスマートコントラクトを参照するソースコードを公開し、実際に稼働するスマートコントラクトに資産を流出させるようなバックドアを実装、資産を窃取。
18	R 社	2021/7/2、 2021/7/10	wBNB, DAI 等	約 80 万、 約 800 万			攻撃者は ETH-BSC 間のブロックチェーンをブリッジする際に、新しいトークンを盗み出して使用することが可能な脆弱性を利用。 各トークンは、wBNB、DAI 等に変換されたが、この際、暴落が発生。
19	S 社	2021/ 6 月下旬 2021/7/16 、 2021/7/23	USDC, SUSHI, USDT 等	14 万、 480 万、 800 万			1 ヶ月の間に 3 回立て続けにハッキングが発生。 3 回目のハッキング時においては、攻撃者が資金を預けていないにも関わらず、預託したかのようにスマートコントラクトを改変し、払戻を発生させた。 更に攻撃者は BTC、ETH、BNB 等の資産も窃取が可能である旨のメッセージを取引時に残した。
20	T 社	2021/8/10	ETH, BSC, Polygon	6 億 1,300 万			攻撃者はクロスチェーンリレー契約をエクスプロイトして 3 つの異なるチェーンから資金を引き出した。犯人は、T 社のバグを発見した際に、大金を得られる可能性をプロジェクトチームへ報告するよりも世間に公開することが問題解決につながると考えたとのこと（全額返金）。
21	U 社	2021/12/5	ETH, BSC	2 億			ホットウォレットの秘密鍵を盗難された。盗まれた仮想通貨は外部ウォレットに送金された後に、ミキシン

							グサービスである「Tornado Cash」に送金。
22	V 社	2021/12/2	ETH 等	1 億 5,000 万			侵害した cloudflare API 鍵を使って V 社アプリに不正なスクリプトを投入。スクリプトは、取引を監視し、外部のアドレスからウォレットにあるトークンの操作許可を促し、許可後に資産を盗み出した。
23	W 社	2021/5/18	BTC, ETH	1 億 4,500 万	○		攻撃者は、W 社プロトコルのガバナンストークンの価格を操作し、実勢価格を超える量の BTC と ETH を借りることに成功。ガバナンストークンの価格が下がりローンが債務不履行となったユーザの担保が清算された時点で W 社には、1 億 4,500 万ドルの債務が残った。
24	X 社	2021/10	BSC	1 億 3,900 万			管理者の秘密鍵が内部犯行（X 社の技術チームの身元不明メンバー）により漏えいした。
25	Y 社	2021/10/27	crYUSD	1 億 3,000 万	○		攻撃者は、一覧の FL 攻撃により最大 150 万ドルの crYUSD を作り出した。次に crYUSD の価値を人為的に高騰させ、FL 返済に充てた残額資産（1 億 3,000 万ドル）を流出させた。

3.4 総括

国内の金融機関への攻撃に関しては、フィッシング詐欺等による顧客情報の不正取得が大半を占め、昨年度までの動向と大きく変わりはなかった。一方、国内外の暗号資産取引においては、セキュリティの脆弱性を標的にするものだけではなく、仕組みを悪用したフラッシュローン攻撃が新たに発生している。攻撃者は、あらゆる観点から脆弱性を見つけ、攻撃をすることが想定されることから、ＣＢＤＣやＣＢＤＣを活用したスマートコントラクトなど新たな金融サービスを設計する際には幅広な検討を必要とすることに加え、モニタリングによる早期対処の仕組みも必要となることが伺える。

[1] フィッシング対策協議会、ホームページ緊急情報、https://www.antiphishing.jp/news/alert/

[2] CipherTrace、“Cryptocurrency Crime and Anti-Money Laundering Report,August 2021”、2021 年、https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/

[3] Chainalysis、“The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime”、2022 年、https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

4　現金に求められる要件とＣＢＤＣに求められる要件

4.1　概要

日本銀行券に求められる要件については、社会環境の変化に適応しつつ、その要請に応えるなかで整理してきており、製造の基本要素として局内においても活用している。そこで、ＣＢＤＣに求められる機能や要件を検討するに当たって、日本銀行券に求められる要件、内容と比較を行った。

4.2　経済的側面から見た銀行券の機能、要件

銀行券を含む通貨が持つ主な機能としては、「交換」「価値の保存」「価値の尺度」がある[1]が、ＣＢＤＣの場合も同様の機能を持つこととなると考えられる。比較表は、表 4.1 のとおりであるが、「交換手段」としてのＣＢＤＣには銀行券と同レベルの決済完了性（処理速度）が求められ、分散型台帳技術を採用する際には、その設計要件として処理速度が重要な要素となる。また、取引量増加時にも対応し得るスケーラビリティが求められる。次に、「価値保存」手段としては、データが必要な期間、完全性を保ちながら保管されることが必要であり、ＣＢＤＣが持つデータ容量が増えた場合の対応などデータ管理の在り方を十分に検討する必要がある。最後に、「価値尺度」としては、経済的な値打ちであることから銀行券と同様に通貨としての信用を保つことが求められると考えられ、当然のことながら信頼性を持った設計が必要となる。

表 4.1　経済的側面から見た銀行券の機能

	現在の銀行券		CBDCの場合
	要件	内容	内容
経済	交換手段	決済・流通手段 支払手段（即時）	決済完了性（ファイナリティ） 処理速度
	価値保存	経済的価値保存 資産の保存	データの完全性 スケーラビリティ
	価値尺度	経済的値打ち 計算単位機能	経済的値打ち 計算単位機能

4.3　市中流通において求められる機能、要件

市中流通時に求められる機能、要件についても銀行券と対比する形でまとめた。銀行券に対して、供給者である日本銀行から求められる要件のうち特に重要と考えられるのは、「安定供給性」「品質安定性」「偽変造耐性」である。

ＣＢＤＣについては、偽変造耐性がシステム上の台帳管理方法や暗号強度などの改ざん耐性となることに加え、システム上で決済が行われることからシステムの安定運用も新たな要素として必要となると考えられる。

(1) デザイン・意匠

日本銀行券には、伝統的特徴である重厚で落ち着いた色調、芸術的な図柄がふんだんに採用されており、２０２４年に発行開始が予定されている新たな様式の日本銀行券（以下「新様式券」）にも、伝統的なデザインと偽造防止技術を融合させたデザインを設計している。

加えて、誰もが使いやすい銀行券となるよう識別マークの付与など、券種識別性向上の工夫も継続的に付与しており、新様式券においては、ユニバーサルデザインとしての設計を企図したものとしている。

ＣＢＤＣのデザインにおいて、直接的に利用者が感じるデザインは、スマートフォンなどに映る画像となる。利用者が、ＣＢＤＣであると認識できるようなデザインを画面上に配置することは、日本銀行券と併存するＣＢＤＣを違和感なく利用してもらうための要素となると考えられる。また、誰もが使いやすいユニバーサルデザインという観点を含めるのであれば、音声案内や点字などの配慮も併せて検討することが好ましいと考える。

さらに、デジタル社会において意識すべきは、ユーザインターフェース（以下「ＵＩ」）、ユーザエクスペリエンス（以下「ＵＸ」）という観点であり、利用者が使いやすさを感じるような柔軟性ある設計の検討が必要となると考える。

(2) 安定供給性

決済システムの中で重要な役割を果たしている日本銀行券は、有事の際も供給し続ける必要がある。そのため、国立印刷局法においては、偽造券が増加した際など、財務大臣の命令により対応する義務が課せられているほか、国立印刷局として、事業継続計画を策定し、不測の事態が発生しても、事業を中断させない、又は中断しても可能な限り短い時間で復旧させるための方針、体制、手順等を整理している。

ＣＢＤＣについても、民間で発行されている決済サービス以上に安定供給や、関連する機関の事業継続計画も重要視しなければならないと考える。また、災害等によりシステムに障害が発生した場合にも、決済が可能なオフライン機能や、安定供給に資する情報収集の一環として、不正な作出等の有無をモニタリングするようなＣＢＤＣの総量管理機能も検討する必要があると考える。

(3) 品質安定性

日本銀行券の品質は、製品規格に基づく品質保証を行っている。時代の変遷とともに、真偽を判定させる対象が人から機械へと拡がり、偽造防止技術の高度化とともに、量産品質としてのバラツキの低減に向け、工程管理能力の強化を図ってきた歴史がある。日本銀行券製造時の継続的改善による品質安定化は、流通過程における偽造券との差別化を容易にし、人、機械による偽造券発見に寄与するものであり、安心・安全な社会インフラの構築に資するものと考えている。

ＣＢＤＣは、デジタルデータとしての品質を確保し、安定した流通環境を継続的な改善を含めて提供し続ける必要がある。データのライフサイクルを意識し、発行、流通、還収までを管理するために必要な機能、役割を検討する必要があると考えられる。

また、ＣＢＤＣに求められる品質の一つに、相互運用性があり、様々な決済手段との連携を実現するためのデータ標準、データ処理など相互運用性の確保に努めることも重要視される。

(4) 機密特性

日本銀行券の有する特性の一つに匿名性がある。現金は、決済記録、情報が残らず、その匿名性は、法的規定により生じているものではなく、通貨の歴史上自然と生じたものであると考えられる。ＣＢＤＣに匿名性を付与するかどうかは、利用者の個人情報保護を含めて検討する必要があり、個人情報保護法やプライバシー保護法などの国際的な動向を把握し、適切な対処が必要となる。具体的には、保有額や利用額に応じた設計を検討するなど、最適な設計をしつつ、平時の匿名性を確保する秘密分散、秘密計算といった匿名加工技術等を有効に活用可能な設計とする必要があると考える。

また、日本銀行券に係る秘密管理は、一国の重要なインフラである通貨を安定的に流通させるために法的に定められ、国立印刷局において、適切な秘密管理が継続的に行われてきた。ＣＢＤＣに関しても、国家安全保障上の観点から、適切に管理することも併せて必要となると考えられる。

(5) 偽変造耐性

日本銀行券の偽造は、アマチュアの偽造から組織・国家の偽造まで幅広く行使されることがある。アマチュアの偽造については、デジタル機器の普及とともに、偽造の機会が増加してきた。また、2001 年頃には、偽造券行使のターゲットが、自動販売機などの機械になるなど、対処すべき偽造防

止技術の内容も変化してきた。変わりゆく時代と銀行券流通環境の変化に対応し続けることは、ＣＢＤＣにおいても変わらず求められることとなる。

無形物であるＣＢＤＣの偽変造は、データの不正な作出、不正なアクセスによる窃取・改ざんなどが考えられるが、改ざん耐性を維持することは、通貨としての強制通用力を維持するために必須であり、取引、保管時のセキュリティを確保することが求められる。また、脅威に備えた継続的なバージョンアップ、脅威の早期発見など組織的に改ざん、偽変造に対応する必要があると考えられる。

(6) 効率性

日本銀行券の管理コストは、輸送費、管理費、ＡＴＭ維持、店頭人件費などを含めて必要なコストが積算され年間１兆円を超えると言われている[2]。その一部である、日本銀行券製造費用については、製造機関である国立印刷局において、継続的な改善による生産性向上等コスト抑制に努めてきた。

ＣＢＤＣには、システム維持費、更新費、管理・運営費など異なる要素のコストが積上げられると考えられるが、通貨としての信頼性（インテグリティ）を確保しながら、最適な管理を実施するとともに、継続的改善によるコストの効率化を全体として進めることが必要となる。

(7) 堅牢性及び安全性

日本銀行券の利用環境は、人から人への流通を基本とする時代から、機械処理を基本とする時代へと変遷してきており、堅牢性の項目に関しても、物理的な強度だけでなく、機械読取等、その機能が維持されることが求められてきた。

ＣＢＤＣに置き換えた場合は、物理的な堅牢性ではなく、台帳の完全性を維持するなどの強さ、改ざん耐性など技術的な強さ、災害時の強靭性など多くの強度が求められ、それは、仕組みの強さに置き換えられると考えられる。設計上の強さだけでなく、運用実務に係る継続性や安定性を実現するような仕組みの設計が求められると考えられる。

(8) 利便性

強制通用力を有する日本銀行券には、どこでも使える利便性に関しても時代の変化による環境変化が見られた。人から人へと流通する時代から、近年の機械処理を中心とする流通に変わり、現在では機械処理適性のしやすさ、インフラの維持などが求められている。そして、キャッシュレス決済手段が広まった背景には、個人が保有するスマートフォンの爆発的な普

及がある。ＣＢＤＣが誰でも使える通貨となるためには、あらゆる利用者が使いやすさを実感し、利用できるようにする必要があり、利用環境やＵＩの工夫など考慮に入れた設計が必要となる。

(9) 社会的受容

日本銀行券を始めとする通貨には、法的に与えられた強制通用力がある。その源には、国民の信頼があり、日本銀行券は偽造券発見枚数の少なさが信頼を支えているともいえる。また、海外からの渡航者を含め全ての利用者に使いやすい日本銀行券とするために、近年、視覚障がい者を含めた使いやすさを実現するためのユニバーサルデザインを採用するよう取り組んでいる。

ＣＢＤＣでも、利用者が信頼して使えることを重視する必要がある。信頼を得るための技術、仕組みを検討し、安心、安全に利用することができる設計を実現していく必要がある。

また、誰もが使いやすいＣＢＤＣとするために、障がい者を含む全ての利用者が利用しやすいユニバーサルデザイン、ＵＩ、ＵＸを設計時に考慮することが重要視されると考えられる。

4.4 総括

日本銀行券に求められる要件という切り口から、ＣＢＤＣに求められる要件を個別に整理することで、多くの要件を抽出することができた。共存することを前提に考えられている日本銀行券とＣＢＤＣは、社会的な信用を同じように得る必要があると考えられ、通貨として多くの要件を満たしていくことが求められる。

通貨として流通させるためには、技術的な仕様のみならず、官民相互の連携による効果的な仕組みを構築し、信頼ある社会インフラとしてのエコシステムを形成していくことが必要と考えられる。

表 4.2　市中流通において求められる要件の比較

	現在の銀行券		CBDCの場合	
	要件	**内容**	**要件**	**内容**
供給者側	デザイン・意匠	伝統的 ユニバーサルデザイン	デザイン・意匠	アプリ上の画面デザイン ユニバーサルデザイン
	安定供給性	製品管理 事業継続	**安定供給性**	可用性（台帳の消失と整合性） システム安定性、事業継続
	品質安定性	同一・均質性 量産品質	**品質安定性**	完全性(台帳、トランザクション) ソフト・通信・ネットワーク構成
	機密特性	匿名性 情報管理	情報管理	匿名性、情報管理 匿名加工技術
	偽変造耐性	耐偽造、耐複製	**耐偽変造性**	台帳記録方式（分散・集中） 強靭性、完全性 暗号強度、長期署名
	効率性	生産効率性 社会コスト(輸送コスト含む)	効率性	社会コスト(システムコスト含む) クロスボーダー取引 国民コスト（端末・通信コスト）
使用者側	**堅牢性**	流通適性、耐久性	**信頼性** **(安全性)**	強靭性、機密性、匿名性
	安全性	衛生的、環境特性		AML/CFT、環境指数　PUE
	利便性	機械処理適性 インフラ維持	利便性	オフライン利用 スループット(所用時間等)
	社会的受容	強制通用力 視覚障がい者対応 ユニバーサルデザイン	社会的受容	強制通用力 ユニバーサルアクセス UI/UX

[1] 一般社団法人全国銀行協会、「お金の機能とは？」、https://www.zenginkyo.or.jp/article/tag-g/5228/

[2] 参考文献：野村総合研究所、「平成２９年度産業経済研究委託事業　我が国における FinTech 普及に向けた環境整備に関する調査検討 経過報告　キャッシュレス化推進に向けた国内外の現状認識」、https://www.meti.go.jp/committee/kenkyukai/shoryu/credit_carddata/pdf/009_03_00.pdf

5　エコシステムの実現に向けたデジタルアイデンティティ

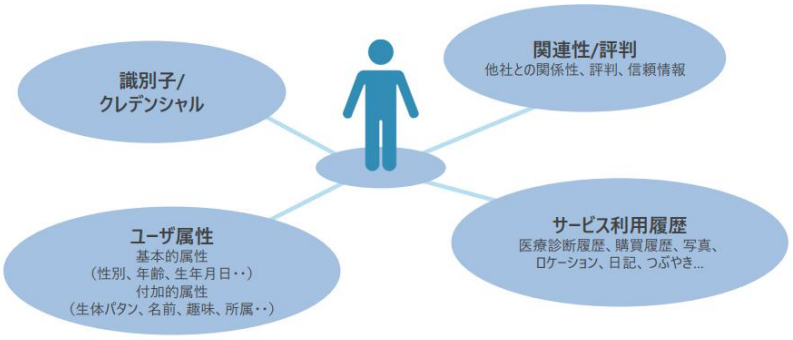
5.1　概要

現代社会においては、インターネットやスマートフォンの普及、官民のサービスのデジタル化などに伴い、リアル空間とサイバー空間でのデータ連携・利活用を行うサービスが増加し、複雑化していることから、オンライン上で本人を特定し、安全かつ簡便に取引を行うための手段として、デジタルアイデンティティ（以下「デジタルＩＤ」）が不可欠となっている。本章においては、デジタルＩＤの概要、ＩＤ管理に必要となる要素について整理し、ＣＢＤＣを社会実装する際のＩＤ管理の在り方について考えるものである。

5.2　デジタルＩＤとは

5.2.1　概要及び分類

アイデンティティとは、「ある実体（エンティティ）に関連する属性の集合」（ISO/IEC 24760）であり、エンティティは人だけでなく組織やモノも含まれる。なお、エンティティが人の場合、属性には以下のような情報が含まれると考えられている[1]。



出典：株式会社野村総合研究所及びNRIセキュアテクノロジーズ株式会社、「ブロックチェーン技術等を用いたデジタルアイデンティティの活用に関する研究報告書」、2021、https://www.fsa.go.jp/policy/bgin/ResearchPaper_NRI_ja.pdf

図 5.1　人のアイデンティティに含まれる属性例

また、アイデンティティは、サービスの利用や関係性とともに、属性も増えるため、アイデンティティは一定のものでなく、属性の増加・変更に伴い、変化・成長していく特徴を有する。こうした特徴を踏まえ、常に変化・成長するアイデンティティを管理することが重要になると考えられる。

次に、デジタルＩＤについての定義は様々あるが、「デジタル」と「アイデンティティ」をつなげたものであり、語句の主体は「アイデンティティ」にあると考えられている。実社会において、身分を証明するために運転免許証やパスポートなどをアイデンティティとして提示することがあるが、これと同様にインターネットなどのデジタル空間で、サービスやシステムを利用す

る権利、資格があることを証明するために、ＩＤやパスワード、生体認証が使われることがあり、その身分証明の方法をデジタルＩＤと考えることができる。なお、デジタルＩＤは各所で定義されており、その定義を表 5.1 に参考として示す。

表 5.1　デジタルＩＤの定義

構成要素	機能
世界銀行	個人を一意に識別する電子的に取得・保存された属性及び/又はクレデンシャルのセット。
ITU（国際電気通信連合）	一つ又は複数の主体をコンテクストのなかで十分に区別できるようにする一つ以上の属性の形式で、主体をデジタルで表現したもの。
EU （欧州連合）	電子的IDとは、自分が言っているとおりの者であることを電子的に証明する方法であり、それによってサービスへのアクセスが可能になる。IDは、主体（市民、企業、行政）を他のものと区別できる。
GSMアソシエーション[2]	電子的に取得・保存された識別属性の集合で、経歴データ（例：氏名、年齢、性別、住所）と生体データ（例：指紋、虹彩、顔写真）を含み、与えられたコンテクストの中で個人を一意的にあらわし、電子取引で使われる。
OIX[3]	主体が誰であるかを証明するために、個人を特定できるデータのセット。信頼のレベルに応じて、個人の身元確認の必要がある。通常、デジタルサービスへのアクセスには個人のIDだけでなく、属性（年齢、住所、信用格付、在留資格など）も必要。
情報処理推進機構（IPA）	デジタル情報として統一的に管理されたアイデンティティ情報（アイデンティティ情報は、エンティティ（主体：属性を管理する単位）についての属性情報の集合）。

出典：野村敦子、「デジタル時代の社会基盤『デジタル ID』」、JRI レビュー、2020、 Vol.9、No.81、p.7

表 5.2　アイデンティティの 3 要素

構成要素	機能	主な例
識別子 Identifiers	ID を識別するための情報	アカウント名、メールアドレス、保険証番号、運転免許証番号、社員番号、学生番号、電話番号など
クレデンシャル Credentials	ある情報内容の正当性を示すための情報	正当な利用者であることを示すワンタイム・パスワード、国籍を示す電子パスポート、電子証明書、印鑑、生体情報など
属性 Attributes	ID を特徴付ける情報	個人：氏名、住所、生年月日、所属、役職、信用情報、生体情報、人間関係、銀行口座番号

		企業:代表者名、所在地、ロゴ、定款、格付け情報、東証コードなど

出典:伊藤宏樹、「クラウドにおけるアイデンティティ管理の課題」、情報処理、2010、Vol.51、No.12、p.1610、https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=71625&item_no=1&page_id=13&block_id=8

5.2.2　デジタルＩＤが求められる理由

デジタルＩＤの管理が求められる理由を考えた場合、主に３つの理由が考えられる。

(1)リソースに対するアクセス制御

リソースへのアクセス制御については、過去から使われてきたものであり、出入り者を識別するための合言葉や、パスワードによる端末利用制限など身近にある制御の考え方であるが、デジタル領域で、確かに本人であることを証明するアクセス制御は、サービスの安心、安全な利用を実現するために不可欠なものとなると考えられる。

なお、リソースへのアクセスを制御するということは、「誰が」「いつ」「どこから」「何のために」「何を」「どのように」アクセスできるかを管理し、制御することであり、情報システム上では、デジタルＩＤを用いて制御されるものとなる。

(2)利用者との関係性強化

データ保護（プライバシー保護）を確実に行うとともに、利用履歴等のデータ分析による利用者ごとのカスタマイズを行い、ＵＸを高めることは利用者との関係性を強化し、サービスへの信頼、満足度を高めるものとなり得る。

(3)効率的なシステム構築

新たにシステムを構築する場合には、過去のレガシーシステムと比較をしながら検討を進めることが重要である。一般的には、すべての機能をシステム内に統合する「一枚岩の密結合な構成」のシステムは、改修、改善に適していないと言われている。将来を通じて、改修を含む安定したシステム運営を可能とするには、データ連携基盤や共通認証基盤といったような機能ごとに分割することが望ましいと考えられ、デジタルＩＤを管理する機能は、効率的なシステム構築には必要不可欠なものであると考えられる。

5.3　ＣＢＤＣにおいて必要となるデジタルＩＤ

5.3.1　金融サービスの拡がりから考える必要性

現在の社会においては、金融サービスのデジタル化が技術革新等により急速に進展しており、多様な金融サービスが様々な媒体を通じて提供されている。サービスの提供形態によらず、利用者保護を念頭に置きつつ、マネーロンダリングやテロ資金供与防止等の観点を持ってサービスを設計するには、デジタルＩＤが不可欠な要素と考えられる。そして、デジタルＩＤは適切なフレームワークにより管理されるべきものでもあり、ＣＢＤＣを設計する上でも必要不可欠な要素と考えられる。

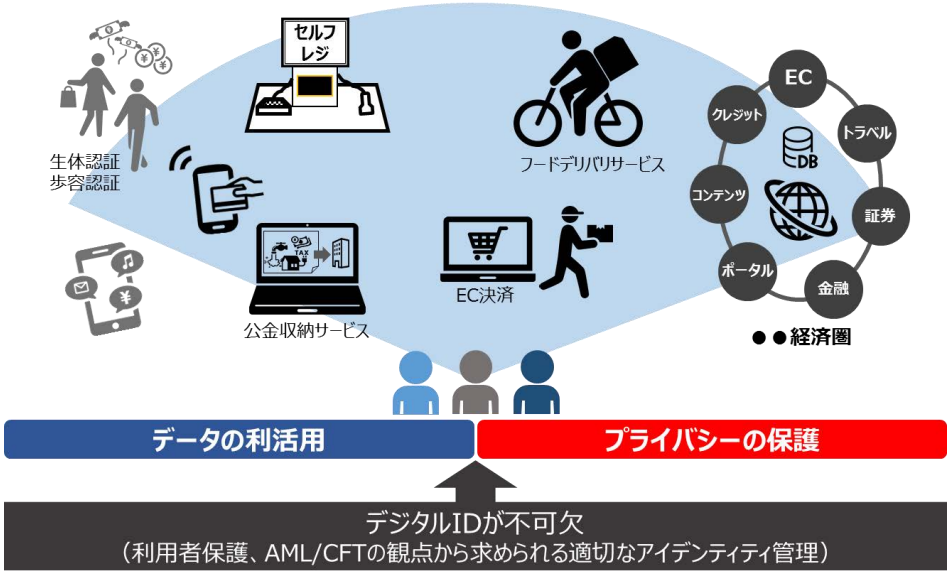


図 5.2　金融サービスの拡がり

5.3.2　ＣＢＤＣエコシステムの実現に向けての考慮事項

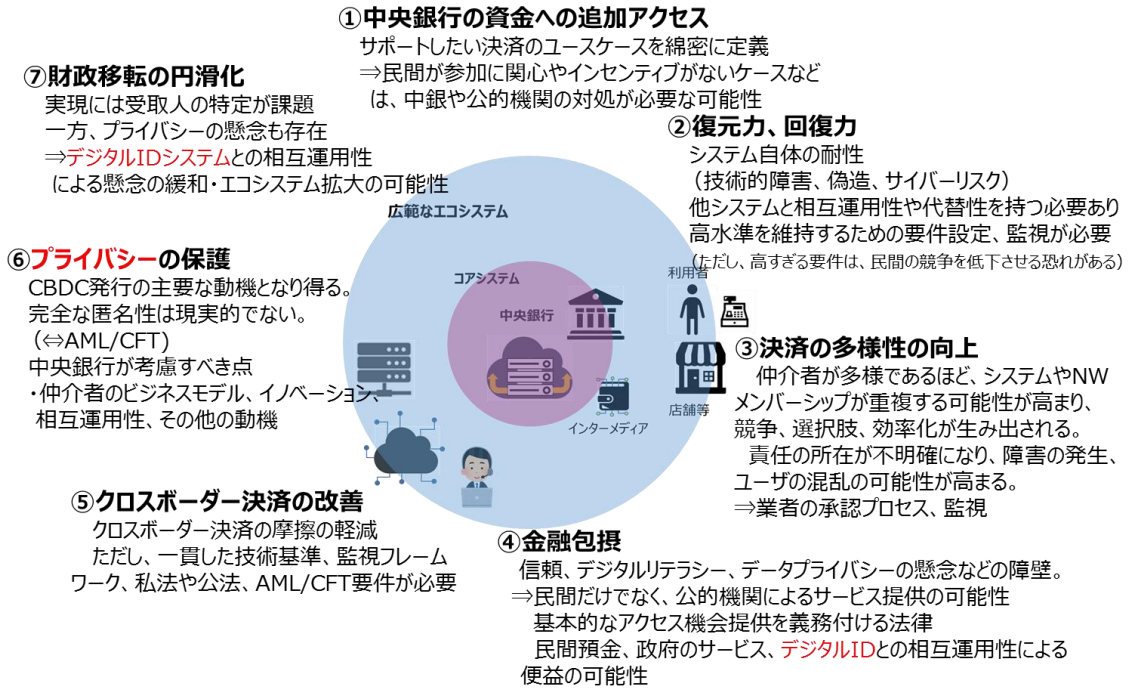
ＣＢＤＣ導入の検討に関して、日本銀行を含む７つの中央銀行と国際決済銀行（ＢＩＳ）による共同研究グループは、報告書[4]においてシステムが効果的であるには、幅広い決済システムとの相互運用性及び共存を確保するため、公的主体および民間主体の双方のバランスの取れた関与によるエコシステムを形成していく必要があるとしており、エコシステム実現に向けて、以下のとおり考慮すべき７つの事項を整理している。

① 中央銀行の資金への追加アクセス
② 復元力、回復力
③ 決済の多様性の向上
④ 金融包摂
⑤ クロスボーダー決済の改善
⑥ プライバシーの保護
⑦ 財政移転の円滑化

列挙された７つの事項のうち、財政移転の円滑化については、コロナ禍の

給付金給付などを例に挙げており、個人、法人情報との連携はデジタル社会の実現に向けた、国としての取組に関連するところがある。こうした中、利用者のアイデンティティ、口座等の情報の連携は、重要な論点になると考えられ、そのアイデンティティは、個人だけでなく、法人も視野に入れていくこと。それが、先の新型コロナウイルス感染症感染拡大に対する緊急事態宣言発令の対となる給付金給付における課題であるとも考えられる。

このように、ＣＢＤＣを社会に実装するためには、官民の役割分担の下で形成されるエコシステムを構築する必要があり、その中で、デジタルＩＤの必要性を重視すべきであると考えられる。



出典：国際決済銀行（BIS）、“Central bank digital currencies: system design and interoperability”, 2021、
(https://www.bis.org/publ/othp42_system_design.pdf)を基に作成

図 5.3　ＣＢＤＣエコシステム形成に考慮すべき事項

5.4　デジタルＩＤの管理方法

5.4.1　本人認証システム

(1) 基本的なシステム

本人認証を利用するサービスの最も基本的なシステムは、利用者とサービス事業者の２者間で認証するシステムであり、その方法は、最も古典的なパスワード認証方式が主流である。金融機関等では、複数の認証方式を組み合わせて多要素認証として実施している例がある。

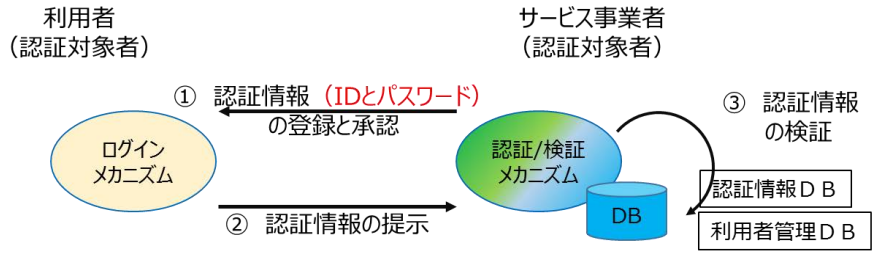


図 5.4　基本的な認証システム

(2) 第三者認証システム

利用者とサービス事業者の２者間で認証するシステムを先に述べたが、この場合、利用者はサービスごとに認証する必要があることに加え、サービス事業者も本業とは別に認証サービスを提供し続けなければならない。

そこで考えられたのが、信頼できる第三者に信頼の起点を置いた第三者認証システムである。認証機関には、技術的な信頼性と運用上の信頼性が求められるが、社会基盤としてのシステムを構築することにより、社会全体のシステムコストの低減が図られる。なお、利用者は複数のサービス事業者への登録が不要になり、ストレスを軽減できること、サービス事業者も業務に専念できることなど、社会全体としてのメリットも生じることとなる。

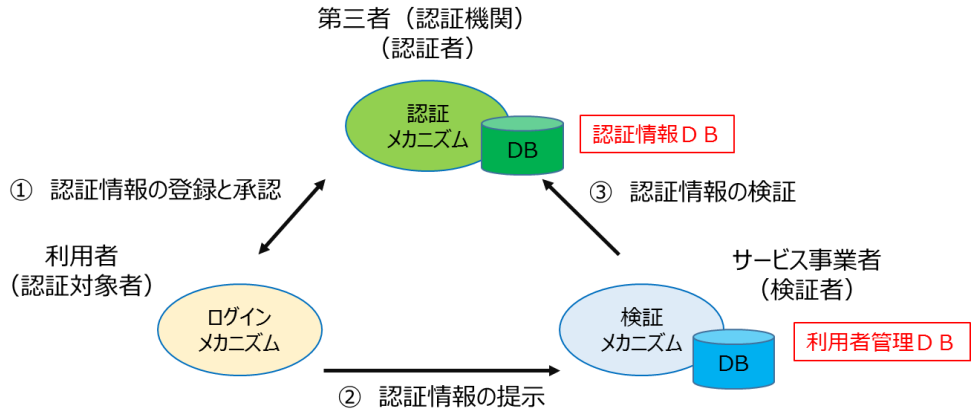


図 5.5　第三者認証による認証システム

さらに、アイデンティティ認証においては、繰り返しのサービス利用に対して、認証方法を簡略化するサービスも運用されている。初回のログイ

ン時には、認証情報としてのＩＤコード、パスワードを要求するが、２回目以降は、要求を必要としないものであり、様々なサービスにおいて利用されているものである。

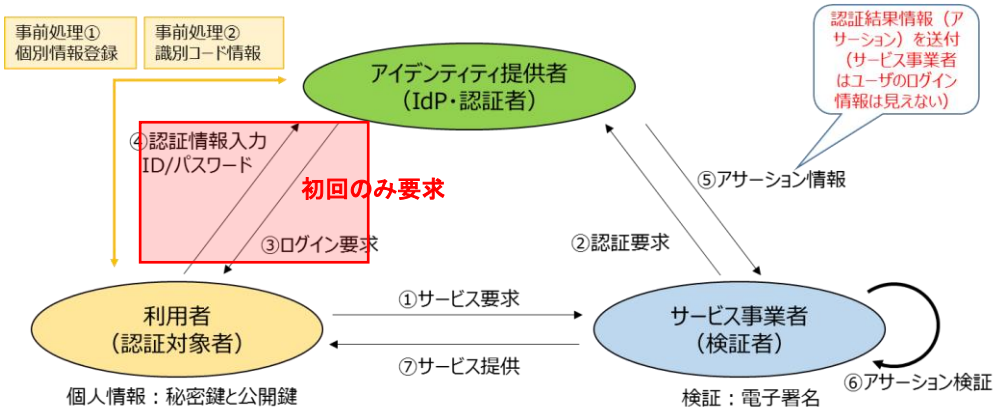
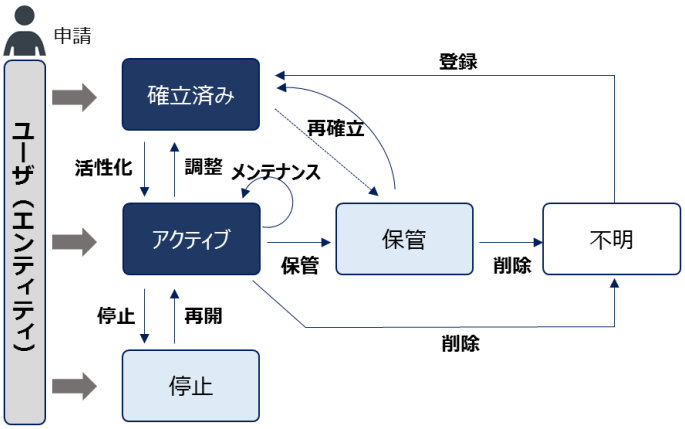


図 5.6　アイデンティティ認証における要求内容

5.4.2　アイデンティティのライフサイクル管理（狭義の管理）

アイデンティティを取り扱う認証業者は、確実な認証を行うために、保管している情報を常に最新かつ正確なものとして保つことなど、ライフサイクル管理が必要となる。アイデンティティの登録、活性化、削除に加え、利用者の状況に応じて、停止や再確立などの実務により、正しく取り扱うことなどが認証業者の業務となる。



ライフサイクルの５つの「状態」

不明	レジスタに何の情報もなく、当該エンティティを識別できない状態
確立済み	登録プロセスの中で必要な情報が確認され、対象エンティティのための識別子など、付加的な情報が生成されレジスタに登録された状態
アクティブ	アイデンティティ情報がレジスタに存在し、エンティティが対象となるリソースを利用可能な状態
停止	アイデンティティ情報はレジスタに存在するが、対応するエンティティはリソース利用を否定される状態
保管	レジスタに当該アイデンティティ情報は存在するが、通常利用ができなくなった状態。再確立プロセスでこの情報を使うことができる。

出典：崎村夏彦、「デジタルアイデンティティー　経営者が知らないサイバービジネスの核心」、日経 BP、2021 年、P.68-69　を改編して図表を作成

図 5.7　狭義のアイデンティティライフサイクル管理業務

5.5　ＩＤ管理の現状

世界の多くの国では、国民ＩＤ番号や社会保障番号など基礎的なＩＤのインフラの導入、整備が進められている。ＣＢＤＣとデジタルＩＤを連携する実例は報告されていないが、エストニア中央銀行を中心とするＥＣＢの研究実験においては、e-IDAS に準拠したデジタルＩＤについて、ブロックチェーンを利用したデジタルユーロにリンクさせ、プライバシー確保に関する検証が進められ、その結果が報告されている[5]。ＣＢＤＣとデジタルＩＤの連携を実現するには、国内のデジタルＩＤが整備されている必要があると考えられることから、諸外国のデジタルＩＤ導入事例を参考にしつつ、整理することとする。

5.5.1　日本の状況

(1)マイナンバーカード

2021 年 12 月 24 日に閣議決定された「デジタル社会の実現に向けた重点計画」においては、データの利活用による経済発展と社会的課題の解決を図ることを目的として、包括的データ戦略の推進を掲げている。包括的データ戦略では、行政機関が最大のデータ保有者であり、行政自身が国全体の最大のプラットフォームとなるべく、データの分散管理を基本として、行政機関がそのアーキテクチャを策定し、マイナンバー制度とリンクしたＩＤ体系の整備、ベース・レジストリを始めとした基盤データの整備、カタログの整備等を行うこととしている。

マイナンバー制度開始以前は、日本国内には国民に幅広く利用されるＩＤカード、ＩＤ番号が存在していなかったが、2016 年 1 月から社会保障、税、災害対策の分野など行政を効率化し国民の利便性を高めることなどを目的にマイナンバー制度が導入され、マイナンバーカードの交付が始まった。交付状況については、政府が 2019 年の消費税率引き上げに伴う需要平準化、キャッシュレス決済の推進及びマイナンバーカード普及を目的として、2020 年 9 月から実施したマイナポイント付与などの政策効果もあって、2022 年 2 月 1 日時点の交付率は 41.8%まで伸びている。

なお、政府は、2022 年度末までにマイナンバーカードがほぼ全国民に行き渡らせることを目指しての普及及び利用の推進に取り組むことを示している[6]。

表 5.3　マイナンバーカードの交付状況（2022 年 2 月 1 日時点）

区分		人口(人)	交付枚数(枚)	交付枚数率(対人口)
全国		126,654,244	52,880,461	41.8%
	特別区	9,572,763	4,420,010	46.2%
	指定都市	27,549,061	12,099,619	43.9%
	市(指定都市除く)	78,865,174	32,358,891	41.0%
	町村	10,667,246	4,001,941	37.5%

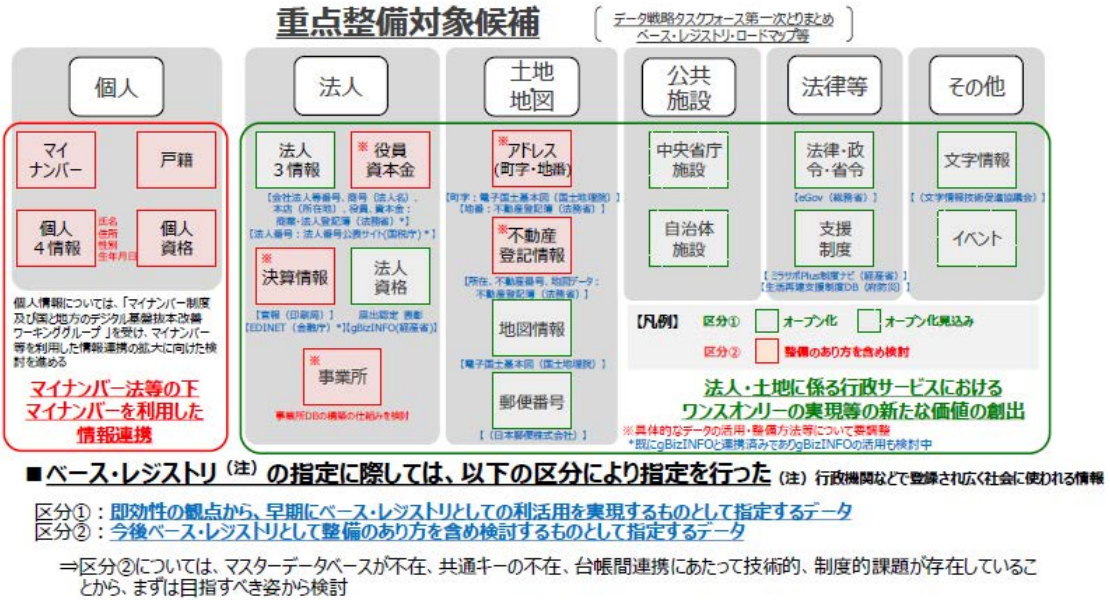
(2) 公的情報基盤（ベース・レジストリ）

データ駆動社会といわれ、あらゆる社会活動でデータが活用される中では、社会基盤としてのデータが重要となり、データの活用により人々の暮らしが豊かになり、事業活動が円滑になるようなことが期待されている。現状は、複雑化した社会の中で、様々な組織で顧客管理や住所管理が行われ、国全体で膨大な費用が情報管理に使われており、この現状を打破するために、データ管理を効率化する仕組みが必要として、そのための基礎データ整備が求められているとされている[7]。

そこで、政府は、世界トップレベルのデータ活用環境を整備し、豊かな暮らしの実現を図るとともに国際競争力の強化を図ることを目的に、データ活用環境の中核となるベース・レジストリの整備を強力に進めていくこととしている。

なお、ベース・レジストリとは、「公的機関等で登録・公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データであり、正確性や最新性が確保された社会の基盤となるデータベース」と定義されており、対象とするデータについては、2020 年 12 月に内閣官房情報通信技術（IT）総合戦略室策定のベース・レジストリ・ロードマップに記載された選定基準により、社会的ニーズ、経済効果、即効性の観点に基づき、具体のデータの抱える課題についてデータホルダーの関係省庁と調整しながら、2021 年５月に法人系、土地系、行政系のデータが指定されている。

なお、個人情報については、マイナンバー等を利用した情報連携の拡大に向けた検討を進めるものとされており、取扱いとしては、整備のあり方を含めて検討する区分とされている。



出典：閣議決定「デジタル社会の実現に向けた重点計画」、別紙「包括的データ戦略」(2021)
(https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/576be222-e4f3-494c-bf05-8a79ab17ef4d/210618_01_doc03.pdf)

図 5.8　ベース・レジストリの整備対象データ

5.5.2　デジタルＩＤ導入の海外事例

デジタルＩＤの導入が進められている国の事例を見ると、政府によるＩＤスキームを構築しているシンガポール、インド、エストニア、民間のＩＤスキームを活用するスウェーデンなどに大別される。これは、導入に至る背景が異なることに起因していると考えられるが、アプローチの方法は異なるものの、どの国もデジタルＩＤスキームを基盤として、官民協働によるサービスの効率的・効果的な提供を目指していることがわかる。

なお、表 5.4 に示す国のうち、イギリスでは基礎的なＩＤインフラが未整備である中、電子的に本人認証が行えるデジタルＩＤを提供している一例である。イギリス政府は、民間の技術を活用してデジタルＩＤを提供しつつ、民間サービスとの連携を進めることで、経済的な価値の創出を目指している。

表中に示した国以外にも、2021 年 6 月にはＥＵの欧州委員会が、デジタルＩＤを域内共通で利用するためのシステムである「デジタルウォレット」の導入案を公表しており[8]、一部加盟国が導入しているデジタルＩＤをＥＵ規模に発展させることを目指し始めている。

表 5.4　主なデジタルＩＤ導入事例

類型	国	名称	備考	国民ID番号
政府主導・中央集権型	シンガポール	NDI（National Digital Identity）	既存の認証システム等が基盤（認証SingPass/個人情報MyInfo）	NRIC(National Registration Identity Card)番号
	インド	Aadhaar Authentication	Aadhaar eKYC(個人情報照会）と連動	Aadhaar
	エストニア	e-identity	民間企業(銀行と通信会社が設立したSKID)が基盤技術開発	PIC(Personal Identification Code)
官民協調・連合型	スウェーデン	Bank ID	銀行コンソーシアムが開発、公共調達でIDプロバイダを複数選定	PIN(personnummer，Personal Identity Number)
	イギリス	Gov.UK Verify	民間IDプロバイダを複数選定	なし

注）World Bank Group et al.［2016］によれば、政府主導・中央集権型、官民協調・連合型は以下の通り分類。

政府主導・中央集権型

・個人のID属性が１つまたは複数の政府所有データベースに保存され、国発行のIDが公共部門と民間部門の全てまたはほとんどのデジタル取引の基盤として機能。

・公的IDは、銀行や携帯電話の資格情報など、他のデジタルIDを検証するための基盤として使用可能。

官民協調・連合型

・市民は複数の信頼できるIDプロバイダー（銀行、携帯電話事業者など）から自由に選択、これらの資格情報を使用して、IDハブまたはゲートウェイを介して広範な公共・民間デジタルサービスにアクセス。

・政府が身元確認の公式基盤を提供し、民間企業がデジタルIDプロバイダーとしての役割。

・公的機関も信頼できるIDプロバイダーであり、政府はIDフレームワークと承認プロバイダーの定義と規制において中心的な役割。

出典：野村敦子、「デジタル時代の社会基盤『デジタル ID』」、JRI レビュー、2020、 Vol.9、No.81、p.13

（https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/11717.pdf）

5.5.3　ＣＢＤＣへのＩＤ連携

ＣＢＤＣへのＩＤ連携に関しては、利用者のプライバシー保護の観点から慎重に検討を進める必要があるが、現時点での、国内外のＣＢＤＣ設計に関する議論においては、ＩＤ連携の要否に関する明確な言及はあまりされていない。ＢＩＳと主要中銀のレポートなどによると、ＣＢＤＣに求められるＩＤ連携に関連する機能としては、以下のような事項が考えられるが、ＣＢＤＣの社会実装に当たっては、利用者の理解が十分に得られていることが重要となり、官民の役割分担のもと、デジタル社会の基盤インフラとなるＣＢＤＣの設計を進める必要がある。

【ＩＤ連携に関連する求められる機能】

・迅速な政府施策の実現

・保有額、取引額に制限を設けるためのウォレット発行時の連携に使用

・ＡＭＬ/ＣＦＴを目的とした利用者特定　　など

なお、ＩＤ連携については、個人のみならず、持続化給付金等政府施策の実現に向けては、法人についても検討しておく必要があり、法人ＩＤを利用した情報連携や、ベース・レジストリとの連携に関する検討が、今後の課題

となると考えられ、日本国内のＩＤ管理の環境整備についても注視していく必要がある。

[1] 株式会社野村総合研究所及びＮＲＩセキュアテクノロジーズ株式会社、「ブロックチェーン技術等を用いたデジタルアイデンティティの活用に関する研究報告書」、2021、
https://www.fsa.go.jp/policy/bgin/ResearchPaper_NRI_ja.pdf
[2] GSM 方式の携帯電話システムを採用している移動体通信事業者や関連企業からなる業界団体
[3] Open Identity Exchange（OIX）は、ID 分野に関わるすべての人々がつながり、協力し、相互運用可能で信頼できる ID に必要なガイダンスを開発するためのコミュニティ
[4] BIS 報告書 2021.9.30　System design and interoperability
https://www.bis.org/publ/othp42_system_design.pdf
[5] エストニア中央銀行、”Work stream 3: A New Solution - Blockchain & eID”、2021、
https://haldus.eestipank.ee/sites/default/files/2021-07/Work%20stream%203%20-%20A%20New%20Solution%20-%20Blockchain%20and%20eID_1.pdf
[6] 閣議決定「デジタル社会の実現に向けた重点計画」（2022）
[7] 内閣官房情報通信技術（IT）総合戦略室「ベース・レジストリ・ロードマップ」（2020）
[8] 欧州委員会プレスリリース（2021 年 6 月 3 日）、
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

6　個人情報の取扱いについて

6.1　概要

近年、デジタル技術の飛躍的な進展により、ビッグデータの収集・分析等が容易かつ高度に行われるようになっている。また、新型コロナウイルス感染症への対応に伴う新しい生活様式への転換とともに、デジタル社会の実現に向けた取組が加速している状況にあり、これまで以上に多種多様なデータが生成、流通、蓄積されていくことが想定される。個人に係るデータに関しては、個人の利益のみならず、公益のために活用されることが期待される一方、個人情報保護、プライバシー保護に対する意識が強く認識されている中、これまで以上に十分な注意を払って情報を取り扱う必要性が高まっている。加えて、経済・社会活動のグローバル化に伴い、個人情報等を含むデータの越境移転も増加しており、各国・各域に対してもプライバシーやセキュリティ等への適切な対処が求められることが想定される。これらの状況を踏まえ、国内外の個人情報、プライバシー保護に関する規制の動向を比較検証した。

6.2　国内の動向

6.2.1　国内における個人情報の取扱い

個人情報は、「個人を識別できる情報」を指し、日本国内における個人情報は、個人情報保護法に、以下のとおり定義されており、氏名や生年月日など特定の個人を識別できる情報又は個人識別符号である。

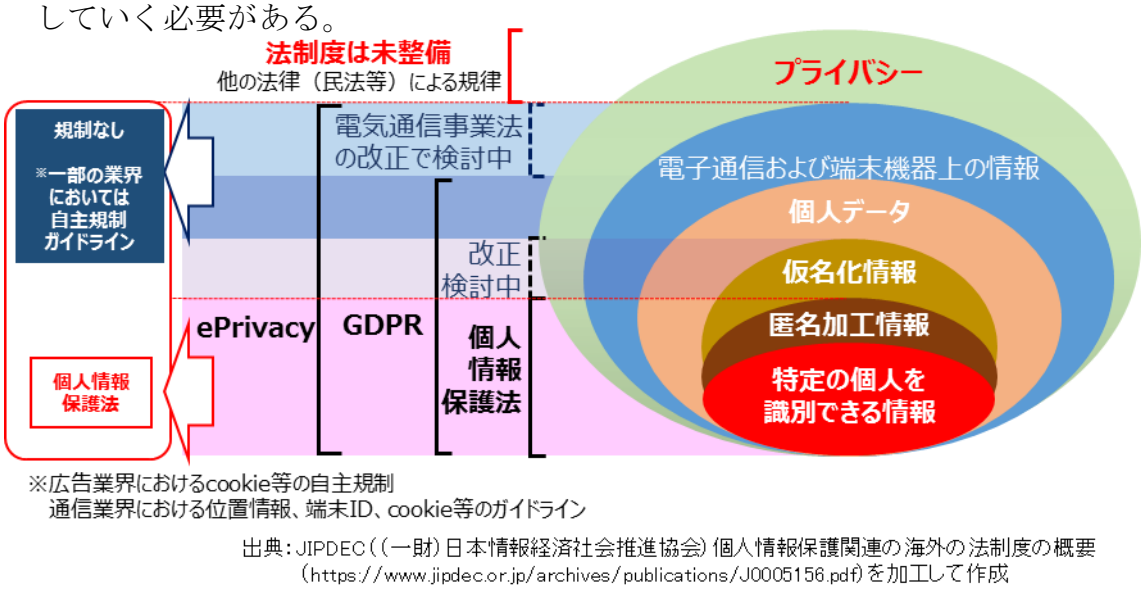
個人情報の保護に関する法律　第２条第１項に記載の「個人情報」の定義
生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）、又は個人識別符号が含まれるもの。

個人情報のうち個人識別符号は、身体的特徴を用いた個人特定が可能な符号又は運転免許証や国民健康保険の番号等である。前者の身体的特徴は、DNA の塩基配列や指紋・掌紋、歩行時の動作や虹彩の模様といったものが含まれる。その一方で、匿名化され、個人の識別が不可能となっているデータは「匿名加工情報」と呼ばれ、個人情報を含めて「パーソナルデータ」と呼称されている。

さらに、2020 年 6 月成立の改正個人情報保護法では、他の情報と照合しなければ特定の個人を識別することができないように個人情報を加工することでビッグデータの利活用に活かすことができる「仮名加工情報」も、パーソナルデータに含むものとして定められている。このように個人の識別を要しない場合に簡易な取扱いを認めることは、後述する欧州一般データ保護規則（以下

「ＧＤＰＲ」）にも採用されている。

ただし、日本国内の法制度の整備範囲に関して、ＧＤＰＲと比較すると取扱範囲が異なることから、国際的な規制との整合性に関して、今後の動向を注視していく必要がある。



出典：JIPDEC（(一財)日本情報経済社会推進協会）個人情報保護関連の海外の法制度の概要（https://www.jipdec.or.jp/archives/publications/J0005156.pdf）を加工して作成

図 6.1　法規制と取扱情報の範囲

6.2.2　今後の動向

個人情報保護委員会は、個人情報保護法の基本理念と制度について、情報を取り扱う各主体に対して、法の基本理念を踏まえたうえで、官民や地域の枠又は国境を越えた政策や事業活動等において、以下に示す考え方を基に、法の目的を実現するための個人情報の保護及び適正かつ効果的な活用の促進に取り組む必要があるとしている[1]。

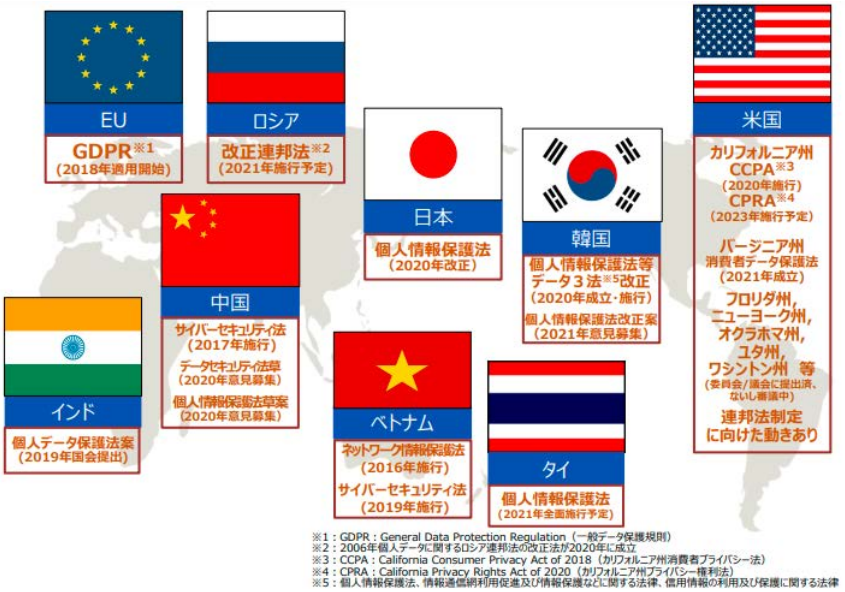
①　個人情報の保護と有用性への配慮
②　法の正しい理解を促進するための取組
③　各主体の自律的な取組と連携・協力
④　データガバナンス体制の構築
⑤　個人におけるデータリテラシーの向上

その他、国際的な制度調和と連携・協調を通じて、データが安全、円滑に越境移転できるような環境構築やデータ移転の執行協力体制の強化を進める必要があることに加え、サイバーセキュリティの確保に向け、個人情報等の漏えいリスク等を軽減させるための多層的な取組が重要とされている。

なお、個人情報保護法は、同法附則（令和２年法律第 44 号）第 10 条に基づき、国際的動向、デジタル技術の進展、それに伴う個人情報等を活用した新たな産業の創出及び発展状況等を勘案し、同法の施行の状況の検討を加えたうえで、必要とされれば所要の措置を講ずるなど３年ごとの見直し規定が定められている。

6.3　国外の動向

経済・社会活動のグローバル化に伴い、個人情報等を含むデータの越境移転が増える中、国際的に見ても法改正の動きが多く見られる（図 6.2 参照）。法制度の取扱範囲の違い、国際的な潮流などを把握するために米国、欧州、中国についての現状をそれぞれ整理する。



出典：経済産業省「第1回 生命科学・医学系研究等における個人情報の取扱い等に関する合同会議」（2021）、配布資料「個人情報保護法令和２年改正及び令和３年改正案について」（個人情報保護委員会）

図 6.2　世界の主な個人情報保護関連の立法の動き（2015 年以降）

6.3.1　米国

米国には、日本の個人情報保護法のような包括的な法律はないものの、一部の分野において個人情報の取扱いに規制を設けているケースがある。

医療情報に関するプライバシー保護について定めたＨＩＰＡＡ（医療保険の相互運用性と説明責任に関する法律）や、12 歳以下を対象とする個人情報取得について定めたＣＯＰＰＡ（児童オンラインプライバシー保護法）が代表的な例である。最新の動向としては、2020 年 1 月にＣＣＰＡ（カリフォルニア州消費者プライバシー法）が施行されており、ＣＣＰＡは、カリフォルニア州民の個人情報を収集し、カリフォルニア州で営利目的の事業を行っている企業のうち、下記条件に該当する場合を対象とする法律である[2]。

○年間総収益が 2,500 万ドルを超える

・年間 5 万以上の個人情報を購入、商業目的で受取、販売又は商業目的で共有する。

・消費者の個人情報の販売から年間収益の 50%以上を得ている。

なお、企業は、情報の開示・削除等の要求に対して 45 日以内の対応が必要

となり、ＣＣＰＡに違反すると 1 件の請求に最大 2,500 ドル（故意であれば最大 7,500 ドル）のペナルティが科せられる。

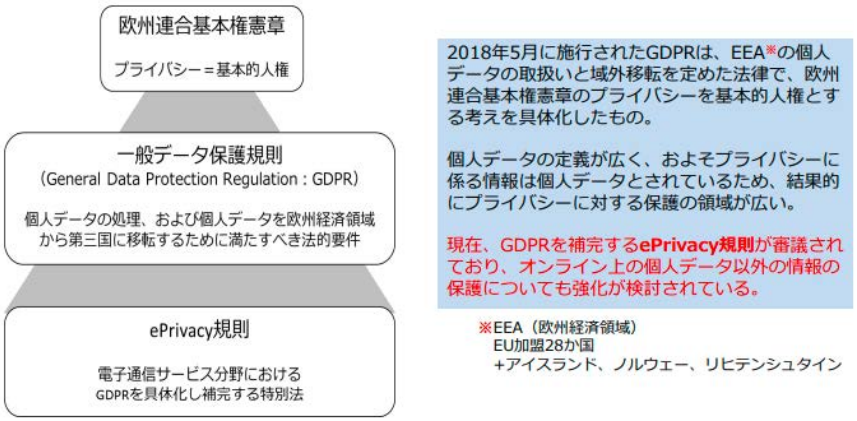
冒頭、包括的な法律はないとした連邦法に関しても、連邦プライバシー法に関する政策として、2019 年 11 月に民主党上院議員から消費者オンラインプライバシー権法（ＣＯＰＲＡ）、共和党上院議員から消費者データ保護法（ＣＤＰＡ）、米国消費者データプライバシー法（ＵＳＣＤＰＡ）が議会に提出されており、米国国民としてのプライバシー権、消費者として事業者に対し責任を追及できる権利を認めるための議論が進められている。米国は、2020 年 6 月に「プライバシーシールド[3]」を欧州が要求するデータ保護レベルに米国国内法が条件を満たさないとして、無効とされており[4]、再合意に向けた対応が進められていると考えられる。

6.3.2　欧州（ＥＵ）

ＥＵは、他国に比べて特に個人情報保護の意識が高く、2018 年には従来の法令よりも規定内容や罰則を大幅に厳格化したＧＤＰＲが施行された。

ＧＤＰＲでは、氏名や生年月日などの個人を識別できるデータだけでなく、位置データやオンライン識別子（IP アドレス、Cookie 等）も保護対象としており、プライバシーに対する保護の領域が広い。これらの情報を取得する際、取得側は個人にデータの利用目的や保管期間といった事項を明示し、そのうえで取得・利用の同意を得なければならず、規定に抵触すると判断された場合、企業の全世界年間売上高の 2%（特定のケースでは 4%）、もしくは 1,000 万ユーロ（特定のケースでは 2,000 万ユーロ）のうち高い金額が制裁金として科せられる（過去には、ＧＤＰＲに違反したとして、数百億円規模の制裁金が科せられた事例もある）。

また、ＧＤＰＲを補完する ePrivacy 規則が審議も進められており、オンライン上の個人データ以外の情報の保護についても強化が検討されている。



出典：一般財団法人日本情報経済社会推進協会ホームページ、「個人情報保護関連の海外の法制度の概要」、
https://www.jipdec.or.jp/archives/publications/J0005156.pdf

図 6.3　ＥＵの制度の構造

6.3.3　中国

(1) 関連法を含む法整備

中国では、国内外のサイバーセキュリティ問題に関して客観的かつ現実的な緊急の課題に応じるべく、2017 年に「中国サイバーセキュリティ法」が施行された。その後、2021 年６月にサイバーセキュリティ環境の変化とビッグデータ応用の漸次的な広域化に伴う、「中国データセキュリティ法」が施行、2021 年 11 月に「民法典」における人格権に対する重要な規程の制定に伴う「中国個人情報保護法」が施行されることで、デジタル化時代におけるサイバーセキュリティ、データセキュリティ及び個人情報権益の保護に向けた基礎的な制度上の保証が提供されるようになった。なお、３法の関係性は、実際には、ある程度重なっており、互いに補完し合う関係にあると考えられている[5]。

(2) 個人情報保護法

2021 年 11 月施行の個人情報保護法では、個人情報を「電子またはほかの方法を持って記録されたすでに識別されており、または識別可能である自然人に係る各種の情報をいう」と定義されている。さらに、個人機微情報として、「ひとたび漏えいし、または違法に使用されたときは、自然人の人格上の尊厳に対する侵害、または人身もしくは財産の安全性に対する脅威を容易に引き起こす個人情報をいう」と定義され、その保管に際しては、暗号化措置を講じなければならないものとされている。

その他、個人情報収集に係る同意や同意を得るための告知などを定めるなど国際標準への対応を法的に定めている一方、中国国外の組織・個人が中国の公民の個人情報権益を侵害し、又は中国国家の安全、公共の利益を脅かす個人情報取扱活動に従事した場合の懲罰的な措置の規定を設けており、セキュリティ全般に係る規定として、個人情報の保護に関してはＧＤＰＲを意識したものとなっている。

[1] 出典：閣議決定「個人情報の保護に関する基本方針の一部変更」（2022）

[2] 出典：個人情報保護委員会ホームページ、https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/

[3] EU市民の個人情報をEUの個人情報保護ルールに則った形で合法的に米国に移転するための規定（2016 年 8 月から開始）

[4] 出典：JETRO ホームページ、「EU 司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断」、https://www.jetro.go.jp/biznews/2020/07/d4dfd684421ffb4b.html

[5] 出典：日本貿易振興機構（ジェトロ）、「中国におけるサイバーセキュリティー、データセキュリティーおよび個人情報保護の法規制にかかわる対策マニュアル」（2021）

7　プライバシー保護技術の動向

7.1　はじめに

近年、金融テクノロジー（FinTech）の技術革新が目覚ましく進んでおり、中央銀行がデジタル通貨を発行する場合の技術的素地を形成するに至っている。このような技術的背景の中、世界各国の中央銀行では、将来の決済システムの効率化、金融包摂の促進の他、他国において中央銀行がデジタル通貨を導入した場合や世界的IT企業によるデジタル通貨を発行した場合の自国経済政策への影響等を想定し、様々な検討が進められている[1,2,3,4,5,6,7,8,9,10]。

このような状況に鑑み、ＣＢＤＣにおける一つの課題であるデータ利活用とプライバシー保護の観点に着目し、近年のプライバシー保護技術の研究動向について調査した。

7.2　データ利活用のためのプライバシー保護技術

7.2.1　プライバシー保護技術の目的

プライバシー保護技術とは、個人のプライバシー等に係る情報（以下「パーソナルデータ」）を各種サービスや統計解析に利用する場合や、統計情報として公開する場合などにおいて、パーソナルデータをどのように扱うべきかを考えるのに有用な技術である[11]。

プライバシー保護技術は、情報セキュリティ技術と混同されることが多いが、パーソナルデータの保管管理、データ通信網における盗聴防止（ネットワークセキュリティ）、外部の攻撃者のシステム侵入防止（システムセキュリティ）といった情報セキュリティ技術とは異なる技術である。例えば、何らかの目的でパーソナルデータを利用したいが、データ解析の過程やデータ解析結果で個人の特定に繋がるなど、プライバシー上の問題が起こらないようにするための技術がプライバシー保護技術に相当し、パーソナルデータが保管されているシステムへの侵入対策などが情報セキュリティ技術に相当することとなる。

また、プライバシー保護技術における攻撃者のモデルも異なり、情報セキュリティ技術においては、不正なアクセス者を主な攻撃者と想定する場合が多いが、プライバシー保護技術における攻撃者は、他者が有する個人情報などアクセスが認められていないデータ解析におけるデータ解析者や、データ解析結果（統計情報）を閲覧するユーザを攻撃者と想定し、それらデータ解析者やユーザが個人を特定する情報に触れないようにするための技術と言える。

プライバシー保護技術を理解するために、いくつかの過去の事例について紹介する。

一つ目の事例[11,12]としては、マサチューセッツ州のＧＩＣ（Group Insurance

Commission）の事例を紹介する。ＧＩＣは、約 135,000 人の州職員とその家族について、医療保険に関連する情報を収集しており、その情報には氏名、性別、郵便番号、生年月日に加えて、人種や医療機関の訪問日、診断結果などが含まれていた。ＧＩＣは、そのデータから氏名を取り除いたうえで、研究者への配布や民間企業への販売を行っていた。一方、マサチューセッツ州ケンブリッジの選挙人名簿は２０ドルで購入でき、選挙人の氏名、性別、郵便番号、生年月日のほか、住所や支持政党が記載されていた。そして、当時のマサチューセッツ州知事はケンブリッジ在住で、ケンブリッジの選挙人名簿によると、州知事と同じ生年月日や郵便番号を持つ人は他にいない状況であった。この状況は、個人を特定する情報が取り除かれていたはずの医療保険データが、選挙人名簿（外部情報）との照合によって再び個人が特定できる情報に復元されることを意味するものである。

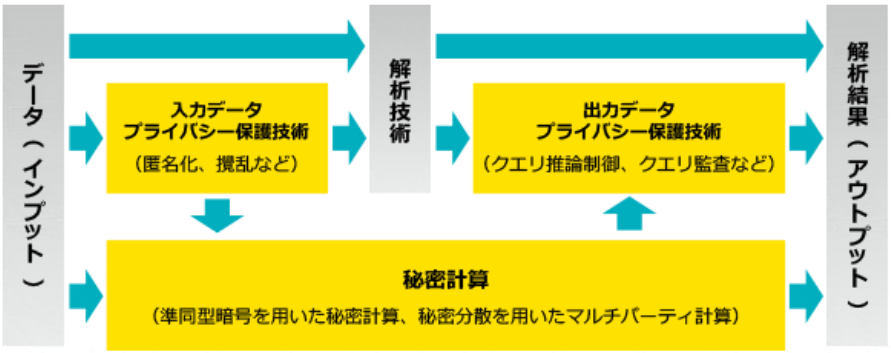
二つ目の事例[11]としては、インターネットサービス会社ＡＯＬの事例を紹介する。ＡＯＬは約 65 万人の３か月分の検索ログ（ユーザ名、検索語と遷移先の URL）を研究目的で提供していた。その際、ユーザ名はランダム番号に変換されていた。しかしながら、検索語の中には、地域や職業、同姓の複数の名前（家族など）、売家の情報などが含まれている場合もあり、電話帳などの公開データと組み合わせることで人物が特定できる情報が含まれていた。ＡＯＬはこの事件を通じて、検索ログの提供を取り止めることとなった。

これらの事例のように、データベースそのものが個人を特定する情報を含まなくても、外部のデータベースと照合したり、非定型な内容から人（又はＡＩ）が類推することで、個人の特定、引いてはプライバシーの侵害につながることとなる。このような事例は、特異的なものではなく、例えば、平均年齢や職業人口、平均年収の推移が、人口変動の少ない過疎地域では個人の年齢や収入に直結する場合となることが容易に想像できる問題である。

プライバシー保護技術は、これらの事例における問題への対策として、パーソナルデータ適切に取り扱うための手段を与える技術である。

7.2.2　プライバシー保護技術の主な分類

個人情報に関連するデータの取扱いのためのプライバシー保護技術には、主に、入力データに対する処理、データ解析時における技術、統計データの出力時（公開時）における技術がある。その全体像は、図 7.1 のとおりとなる[13]。



出典：アイティメディア㈱@IT「プライバシー保護データマイニング（PPDM）手法の種類、特徴を理解する」
https://atmarkit.itmedia.co.jp/ait/articles/1503/24/news010.html

図 7.1　データ取扱に係るプライバシー保護技術の構成図 [13]

まず、入力データに対する処理では、広く知られている技術として、仮名化・匿名化技術がある。これは、データ入力時に個人の特定に繋がる氏名やマイナンバー情報をＩＤ番号化（仮名化）したり、年齢、生年月日、住所、電話番号、職業などといった属性情報に対し、年齢であれば 20 代などに取りまとめるなど抽象化（匿名化）したりするデータ加工技術である。この処理は古くから使われている技術で、改正個人情報保護法でも仮名化情報や匿名化情報が定義されるなど、プライバシー保護の基本的処理となっている。

次に、データ解析時に使用される処理では、複数の機関が有する異なるデータベースから、データ解析者が、他の機関が有するデータや自身がアクセスを認められていないデータを閲覧することなく、統計処理などのデータ解析を行う技術がある。この技術は、秘密計算と呼ばれ、現在は、秘密分散によるマルチパーティ計算（Multi-Party Computation）と準同型暗号を用いた手法が主流となっている。

最後に、データの解析結果に曖昧さ（ノイズ）を加えることで、解析結果からパーソナルデータを決定的に類推することを不可能にする技術がある。代表的な技術としては、2006 年に Microsoft 社の研究員が開発した差分プライバシーがあり、一つの変数でプライバシー保護の度合いとデータの有用性の関係を示せることが特徴的な技術である。

そこで、データ入力時のプライバシー保護技術である仮名化・匿名化技術、データ解析時のプライバシー保護技術として秘密計算、出力時のプライバシー保護技術として差分プライバシーについて、その概要をまとめる。

7.3　仮名化・匿名化技術

不特定多数の情報を活用可能な形式で扱うためには、情報をデータベース化することが一般的になっており、データの１行１行が一人のパーソナルデータを含む表形式で表されることが広く取り入れられている。仮名化・匿名化技術は、このデータベーステーブル（及び外部のデータベース）から個人の特定等を困難にする技術のことである。そして、この技術は、データの収集や提供において最初に考慮すべき基本的な技術でもある。本節では、このようなデータベーステーブルの作成、提供に当たって、プライバシー侵害の可能性を抑制する仮名化・匿名化技術について説明する。

7.3.1　用語の定義

ここでは、仮名化・匿名化技術を説明する前段として、表形式のデータベースを用いて用語の説明を行う。

まず、「氏名」や「年齢」のように、データベース上の情報を区分するためのラベルを属性と呼び、各属性に対する個別の値を属性値と呼ぶ。例えば、図 7.2 に示す例では、職員番号 0001 番の人物のパーソナルデータ（レコード）において、「年齢」という属性に対する属性値は「54」となる。また、「職員番号」や「氏名」など単体で個人の特定可能な情報を直接識別情報と呼び、「年齢」「性別」「所属」など、単体では個人の特定に繋がらないが、複数のデータを組合せることにより個人の特定に繋がる可能性のある情報を間接識別情報と呼ぶ。また、情報の持つ特徴に応じて、プライバシー保護の観点から、主な用語は、表 7.1 のとおり定義される。

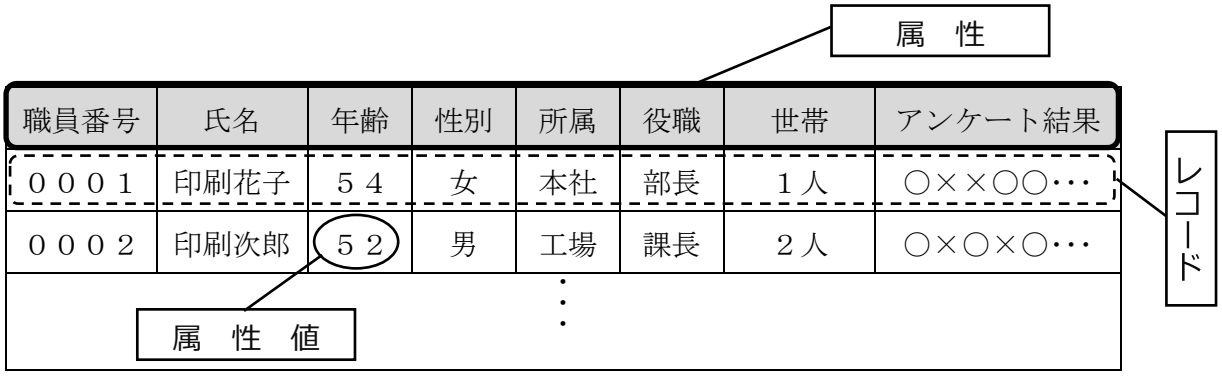


図 7.2　レコード、属性及び属性値

表 7.1　用語の定義

レコード		複数の属性の属性値を含むひとまとまりの情報
データベース		レコードの集合
	個人属性データ	一個人の情報が一つのレコードのみに含まれるデータ
	履歴データ	一個人のデータが複数のレコードに含まれる情報
属性情報		個人の出自、所属、人格、身体、生活及び行動等（属性）に関する情報
	識別情報	
	直接識別情報	単体で個人の特定を可能とする情報 時間経過によって変化することのない、個人に固有の情報であることが基本 （マイナンバー、運転免許番号、指紋データ、顔画像、遺伝子情報等）
	間接識別情報	単体では個人を識別できないが、複数を組み合わせることによって個人を識別し得る情報 時間経過によって変化することのない、個人に固有の情報であることが基本 (年齢、性別、身体的特徴)
	その他の情報	
	履歴情報	個人の活動に関わる情報。本人の意思や環境により変化する 時間経過とともに蓄積され、識別情報となる場合がある
	要配慮情報	差別的な判断、決定につながる恐れのある情報（人種、国籍、宗教、犯罪歴、病歴等） 履歴情報にも要配慮情報が含まれる恐れがある（聖書の購買履歴、刑務所への移動履歴、賭博場の利用履歴）
	連絡情報	個人に連絡することを可能にする情報（住所、電話番号、メールアドレス、SNS アカウント）
	直接被害情報	クレジットカード番号、オンラインサービスのアカウントとパスワード等

7.3.2　仮名化・匿名化技術

匿名化とは、多数の個人に関するデータベースにおいて、各レコードがどの個人に関する情報であるかを特定されることや、別のデータベースと連結されるリスクを低減するためのデータ加工処理である。代表的な匿名化手法は、以下のとおりである。

(1) 仮名化

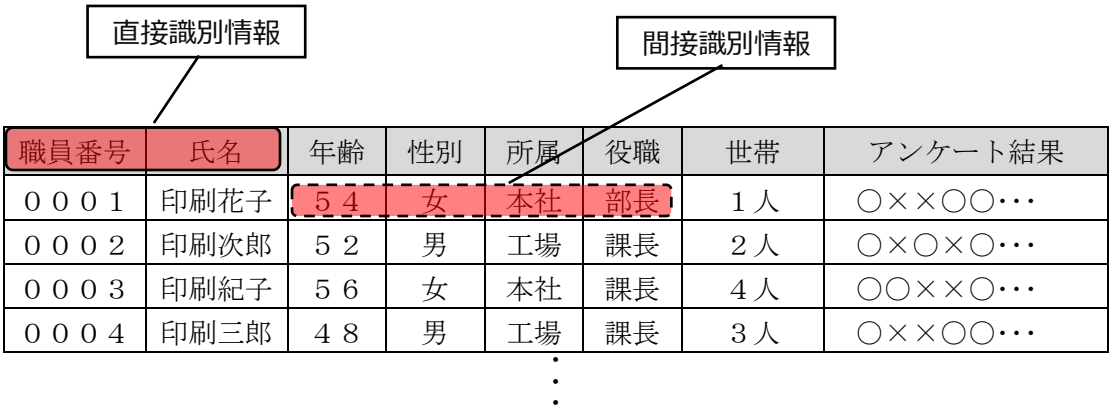
データベース上の各個人の直接識別情報（氏名やマイナンバー）を直接識別情報とは異なるＩＤ情報に置き換える処理（図 7.3 参照）。各個人に一つのＩＤ又は複数のＩＤを対応させる処理がある。一方で、一つのＩＤ情報に複数の人物を対応させることは行わない。また、一般的には、ＩＤ情報と個人を紐づけたデータベーステーブルを保有することも多い。

(2) 抑制

データベースから属性値を削除する処理である（図 7.3 参照)。

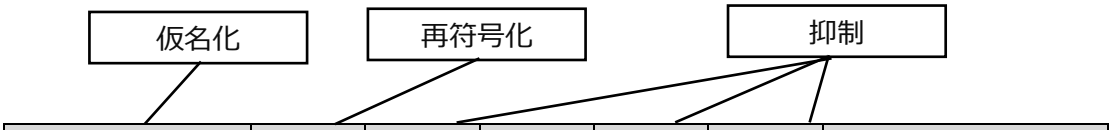
(3) 再符号化

データベース上の属性値を範囲で表現することである（図 7.3 参照)。ある属性に対して、存在し得る全ての属性値を含む範囲に再符号化すると、抑制と同じ効果となる。



職員番号	氏名	年齢	性別	所属	役職	世帯	アンケート結果
０００１	印刷花子	５４	女	本社	部長	１人	○××○○･･･
０００２	印刷次郎	５２	男	工場	課長	２人	○×○×○･･･
０００３	印刷紀子	５６	女	本社	課長	４人	○○××○･･･
０００４	印刷三郎	４８	男	工場	課長	３人	○××○○･･･

(a) 匿名化処理前のデータ



仮名ＩＤ	年齢	性別	所属	役職	世帯	アンケート結果
６８０４１３５４	５０以上	－	本社	－	－	○××○○･･･
４６８４０６３１	５０以上	－	工場	－	－	○×○×○･･･
０５６４０９６１	５０以上	－	本社	－	－	○○××○･･･
４９９８７４１３	５０未満	－	工場	－	－	○××○○･･･

(b) 匿名化処理後のデータ

図 7.3　匿名化手法

7.3.3　プライバシー侵害の類型

仮名化・匿名化技術は、プライバシー侵害のリスクを軽減することができるが、完全に排除することは困難といえる。それは、あるデータベースから不正にプライバシーを暴こうとする攻撃者は、当該のデータベースのみではなく、手に入るあらゆる情報を駆使して、データベース内の情報と個人を結び付けようとするからである。当該のデータベースだけを見るとプライバシーは十分秘匿されているように見えても、プライバシー侵害に至るケースがあるためである。

(1) 特定

直接識別情報が取り除かれた情報について、該当する個人とデータを再び結び付けることである。間接識別情報が複数個集まることで、攻撃者の知識や他のデータベースと照合可能となる場合が想定される。

(2) 連結

ある個人に関するデータを、同一人物に関する別のデータと結び付けることである。このとき個人が特定されているか、特定されていないかは問わない。異なるデータベース間で、共通の属性が複数含まれている場合に、属性値の組合せに特徴があれば、照合が可能となる。

(3) 連絡

ある個人に関するデータを保持する者が、何らかの手段でその個人に連絡することである。訪問、郵便、メール、電話等が想定される。データベースから知り得た住所によって自宅に訪問した場合、ほぼ特定にあたる。ダイレクトメール等、特定を得ない連絡もある。

(4) 直接被害

ある個人に関するデータを保持する者が、その個人に直接的な被害を与えることである。個人が特定されているか、特定されていないかは問わない。クレジットカード情報が流出した場合、個人の特定に至らなくても直接被害が発生する可能性がある。

(5) 属性推定

ある個人に関するデータの一部が抑制、あるいは再符号化されているときに、それを復元又は推定することである。個人が特定されているか、特定されていないかによらず、属性推定は起こり得る。

7.3.4　匿名化処理の評価指標

匿名化によってプライバシー侵害のリスク低減が期待できるが、闇雲に仮名化や抑制を施しても、類型に示したようなプライバシー侵害が生じ得る。ここでは匿名化後のデータについて個人特定のリスクを定量的に評価するための評価指標を説明する。

(1) k 匿名性

直接識別情報が取り除かれたデータベーステーブルから個人を特定することを想定した場合、最も重要なカギとなる情報は属性情報の属性値となる。例えば、図 7.4 に示す例では、番号 1 の個人に関しては、50 歳以上で本社所属の人が一人しかいないため、他の情報と連結することで容易に特定可能な状態にあることが分かる。一方、番号 2～5 の人物については、属性情報が同じであるため、他の情報と連結し該当者を絞り込んだとしても、どの番号がどの個人に紐付くかまでは分からない状態にあることが分かる。また、同一の属性情報が多ければ多いほど、個人の情報と紐付けることが難しくなることも容易に想像が可能である。

同じ組合せの人は一人

番号	年齢	所属	世帯
1	50 以上	本社	1 人
2	50 未満	本社	2 人
3	50 未満	本社	4 人
4	50 未満	本社	3 人
5	50 未満	本社	1 人

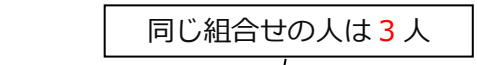
図 7.4　k＝１で個人の特定に繋がる例

k 匿名性[14]はこの属性情報の一致具合の最悪ケースを表すものであり、データベース内に同一の属性情報を持つレコードが最悪ケースで k 個存在することを表す指標である。そして、この数値 k を見ることで、とある情報に対して、最悪ケースの場合、「k 人のうちの一人」まで絞り込むことが可能であることを示す指標となっている。

(2) ℓ 多様性

データが k 匿名性を満たす場合であっても、間接識別情報の組合せが同一のレコード同士を比較して、要配慮情報の内容も同一であった場合、その間接識別情報の組み合わせに該当する個人の要配慮情報が容易に判明できる状況となる。例えば、図 7.5 の例では、このデータベースにある３名の 50 代職員

が誰であるかを知っていれば、各レコードと個人が帰属できなくても、彼らが独身であることが容易に理解可能である。



番号	年齢	所属	世帯
1	50 以上	本社	1 人
2	50 以上	本社	1 人
3	50 以上	本社	1 人
4	50 未満	本社	4 人
5	50 未満	本社	2 人

図 7.5　ℓ＝1 で要配慮情報が流出する例

そのようなことが起こらないようにするには、ある組合せの間接識別情報を含む k 個のレコードについて、各レコードが含む要配慮情報が、複数種類あればよく、その種類の数をℓとしてプライバシー侵害リスクの指標とするのがℓ多様性[15]である。なお、ℓは必然的に k 以下かつ 1 以上となる。

(3) 標本一意と母集団一意

統計学の中では一般的に使用されている用語として、「母集団」と「標本」がある[16,17,18]。

母集団とは、解析対象とする個人全体のレコードの集合のことであり、例えば、日本人の平均所得を考える場合、日本人全員分の所得を含むデータベーステーブルが母集団となる。

一方、標本とは、母集団から一部のデータをランダムに選び出した場合（ランダムサンプリング）のレコードの集合のことである。例えば、日本人の平均所得の計算において、全員分の記録を集めるのは困難であるため、ランダムに選んだ 1 万人のデータから推測する手法を考えた場合、その 1 万人分のデータベーステーブルが標本となる。

「標本一意である」とは、あるレコードが標本データ内の全体に渡って唯一である状態を指す。「母集団一意である」とは、あるレコードが母集団データの全体に渡って唯一である状態を指す。

ここで、母集団一意であるレコードが存在する場合、外部情報による特定が容易になることに注意する必要がある。例えば、日本人の最高齢の人が一人しかいないような場合には、年齢データが、即、個人の特定に繋がることになるのがその典型となる（外れ値）。

一方、標本一意であるレコードが存在する場合は、その存在のみでもって、母集団一意とは限らないこととなる。例えば、日本人全体の中からランダムに抽出した１万人分のデータの中に、100 歳の人のデータ一つだけあったとしても、日本人（母集団）の中には他にも 100 歳の人がいるため、そのデータを特定の個人と紐づけるのは困難だからである。ただし、多くの場合、手に入るのは標本データのみであるため、母集団一意性を統計により推定することが必要となる。

7.3.5　仮名化・匿名化処理のまとめ

匿名化という単語から直感的に連想するのは、いわゆる仮名化であろうと思われるが、氏名を別のＩＤ情報に置き換えることは匿名化の一手法に過ぎず、仮名化によってプライバシー侵害を防止できるというのは誤った認識である。また、匿名化処理であっても、完全なリスク排除を求めることはできないことにも注意しておく必要がある。それは、リスクを完全に排除するために再符号化や抑制を強化するほど、データが本来持っていた有用性は失われ、データ活用という目的自体が達成できなくなることや、閉じたデータベース内で匿名化処理がされていても、外部のデータベースと結び付けることによりプライバシー侵害が発生することもあるためである。

一方、プライバシーを含む情報や関連情報を活用するためには、効果的に匿名化を施すことは必要不可欠である。そして、匿名化処理によってどの程度までリスクを低減できているかについて、k 匿名性やℓ多様性といった様々な評価指標を用いて評価することが重要であることが分かる。

7.4　秘密計算

データの匿名化や後述する差分プライバシーなどの技術は、データ公開や統計量公開時に関するプライバシー保護の問題に対応する技術であり、データ収集者がデータベーステーブルや統計量など何らかの情報を公開した場合に、その情報を手にした攻撃者が、入力について何を推測できるのか、どのようにすればその推測の範囲を制限できるのかを考えることを課題とする技術である。

一方、秘密計算は、個別の機関のデータを互いに共有することなく、その秘密性を保ったまま、統計解析や機械学習などの計算を実行し結果を得るためのプライバシー保護技術である。言い換えれば、データ解析者は必ずしもパーソナルデータそのものを閲覧することなく、統計的傾向やデータ解析結果のみを取得する技術である。

秘密計算の主な方法としては、秘密分散[19]によるマルチパーティ計算[20,21,22]と準同型暗号[19,23]を用いた秘密計算方法[11,24]がある。前者の秘密分散によるマルチパーティ計算は、複数の者（パーティと呼ぶ）が秘密情報を持ち寄り、自分の秘密情報を他社に知らせることなく、対等な立場で計算を行いその計算結果のみを得る手法である。一方、後者の準同型暗号を用いた秘密計算は、データを暗号化した状態で加法や乗法の演算が可能な準同型暗号の特性を利用し、暗号化したデータに対して平均値などの計算を行い、得られた解析結果を復号することで、パーソナルデータに触れることなくデータ解析を行う手法である。ここでは上記二つの方法について概要を説明する。

7.4.1　秘密分散によるマルチパーティ計算

秘密分散によるマルチパーティ計算では、一般的に秘密分散が用いられる。そこで、まずは、秘密分散について紹介し、その後、マルチパーティ計算について紹介する。

(1) 秘密分散の概要

秘密分散とは、文字通り秘密情報を断片化し、分散する技術であり、その特徴として、所定数の断片を持ち寄れば確実に復号できることと、所定数に満たない断片からは、意味のある情報は何も得られないという特性がある。

「所定数の断片を持ち寄れば確実に復号できる」性質は、全数をそろえなくても復号可能であることを示し、つまり、一部のデータが破損しても復元可能であることを意味する（冗長性の確保）。

一方、「意味のある情報が得られない」は、専門用語で表現すると、「情報理論的識別不可能性」を持つということである。情報理論的識別不可能性[25]は、現在、広く利用されている暗号方式で、よく耳にする「スーパーコンピュータでも解読

に数千年かかる暗号解読の難しさ」といった「計算量的識別不可能性」よりも高い安全性を実現する性質のことである。

m個に分割しθ個集めると復号可能な秘密分散法を(θ, m)閾値秘密分散法と呼び、特にm個に分割しm個集めると復号可能な秘密分散法を(m, m)閾値秘密分散法と呼ぶ。(m, m)閾値秘密分散法の代表的な例として加法的シェアがあり、(θ, m)閾値秘密分散法の代表例としてシャミアらの方法[26]がある。以下、秘密分散の特性が理解しやすいシャミアらの方法について説明する。

シャミアらの方法は多項式による秘密分散法で、以下に示すアルゴリズムで実施される。

【シャミアらの方法】

整数の集合 $\mathbb{Z}$ の元を素数 q で割ったあまりの集合 $\{0, 1, 2 \cdots, q-1\}$ を $\mathbb{Z}/q\mathbb{Z}$ と表記するとき、秘密情報 $x \in \mathbb{Z}/q\mathbb{Z}$ に対して、以下の多項式を生成する

$$f(z) = x + a_1 z + a_2 z^2 + \cdots a_{\theta-1} z^{\theta-1} \mod q$$

$$(a_1, \cdots, a_n, \cdots a_{\theta-1}) \in \mathbb{Z}/q\mathbb{Z}$$

a_n ：一様ランダム

次に、秘密情報 x に対し、 i 番目のシェアu_i を以下の関数により算出

$$u_i = (i, f(i))$$

このとき、シェア u_i を θ 個集めると $f(z)$ は一意に求められ、秘密情報 x も $f(0)$ から算出可能となる

シャミアらの方法については、数式で理解することも可能であるが、幾何学的に理解することも可能である。シャミアらの方法を 1 元多項式で考えると、図 7.6 左に示すように、$f(z)$ は平面上の直線、秘密情報x はy切片 $f(0)$となる。この時、直線上の 2 点以上の点が分かれば直線は復元できるため、秘密情報xが求まることになる。一方、直線上の 1 点しか分からない場合、どのような直線になるかは不明となり、秘密情報x も復元できないことが分かる。また、この性質は 2 元多項式以降も数学上同様である。

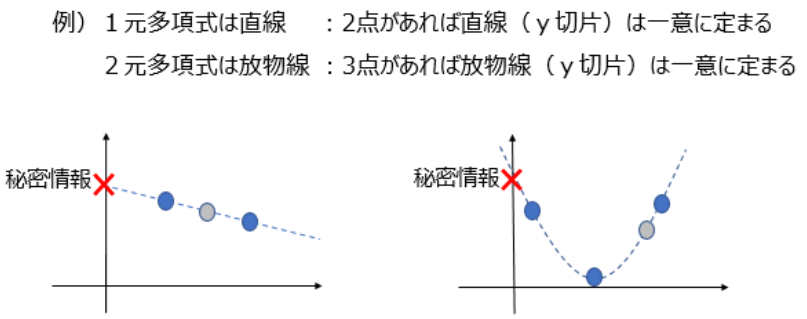


図 7.6 (θ, m)閾値秘密分散法の幾何学的解釈

(2) マルチパーティ計算

マルチパーティ計算は、その名のとおり、秘密分散によって生成されたシェアを複数の参加者がそれぞれ保有し、必要に応じて秘密情報を持ち寄って、自身の秘密情報を他の参加者に知らせることなく対等な立場で計算を行い、計算結果のみを得る手法のことである（図 7.7）。原理的には、元データを用いて実行可能なあらゆる演算結果は、秘密分散によるマルチパーティ計算によって再現可能であるとされている。一方、演算が複雑になればなるほど、参加者同士の通信回数が増大するため、通信時間がボトルネックとなり、計算速度が現実的でなくなる懸念がある。

秘密分散によるマルチパーティ計算は、1,000 万件のレコードのソートを 12.2 秒で実施するなど、すでに十分実用に耐える計算能力を実現していることが報告されている[27]。

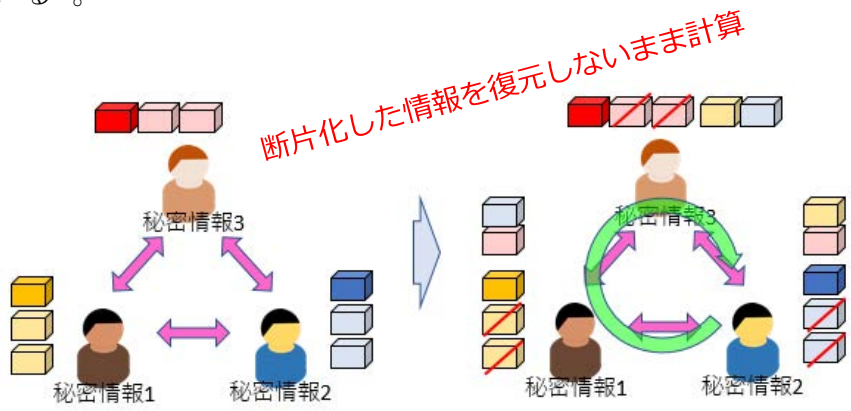


図 7.7　マルチパーティ計算のイメージ

7.4.2　準同型暗号を用いた秘密計算

(1) 準同型暗号の概要

準同型暗号とは、データ（平文）及びその暗号文が与えられたときに、平均値などの計算において、平文のデータをそのまま計算した結果と、暗号文に対して同様の計算を行った結果を復号したものが一致する特性を持つ暗号系のことである。準同型暗号の中でも、加法に準同型性を持つ暗号方式を加法準同型暗号、乗法に準同型性を持つ暗号方式を乗法準同型暗号と呼び、加法と乗法の双方に準同型性を持つ暗号方式を完全準同型暗号方式と呼ぶ。加法準同型暗号の代表例としては Paillier 暗号系や、ある種の改良を加えた ElGamal 暗号が挙げられ、乗法準同型暗号の代表例には RSA 暗号系や ElGamal 暗号系などが挙げられる[19]。

加法と乗法の双方に準同型性を持つ完全準同型暗号は、2009 年に格子問題に基づく暗号系で初めて実現可能性が示され[28]、現在も実用に向けた改良が続いて

いる状況にある[23]。

また、格子暗号は、2016 年以降、米国のＮＩＳＴが進めている次世代暗号方式（耐量子計算機暗号）[29,30,31]の有力候補（2021 年 12 月時点で 69 件の応募から７件(予備８件)まで絞られており、そのうちの５件は格子暗号系）となっている暗号方式である。格子暗号の概要や格子暗号を用いた完全準同型暗号の仕組みについては、文献 11 や文献 23 を参照願いたい。

本節では、完全準同型暗号が可能であることを前提に、どのように秘密計算が行われるのかを例を用いて説明する。

(2) 完全準同型暗号による秘密計算

完全準同型暗号を用いた秘密計算の基本は、秘密情報xを暗号化し、暗号化した秘密情報$\mathrm{Enc}(x)$のまま平均値などの統計量を算出し、最後に復号することで実施することにある。言い換えれば、情報の閲覧許可がない者は、計算過程では暗号化したデータのみを用いて秘密計算を行うことで秘密情報に触れないようにする技術である。

例として、異なる二つの機関（機関Ａ及び機関Ｂ）が異なる二つの表を有するときに、個々のデータを互いに開示することなく独立性検定を行うことを紹介する（図 7.8）。まず、独立性検定は、検定表を作成し、その検定表からχ^2検定の検定統計量を算出することで実施する。この例では、機関Ａと機関Ｂが持つ個人情報を互いに秘密にしながら検定表を作成することが課題となる。完全準同型暗号を用いた秘密計算の詳細な前提条件、実施手順についての説明は省略するが、信頼のおける第三者機関（機関 C）が機関 A 及び機関 B の双方のデータを用いないと計算できない個所を担当することで容易に計算可能となる(図 7.9)。上記例では、

- 機関Ａは、機関Ｂ及び機関Ｃから暗号化された統計量のみ受信
- 機関Ｂは、機関Ａが生成した公開鍵のみ受信
- 機関Ｃは、機関Ａ及び機関Ｂから暗号化された個々のデータを受信

とデータが移動することとなる。この時、秘密鍵を持ち、暗号化されたデータを解読できるのは機関Ａのみであることから、３機関ともに秘密情報に触れていないことが分かる（図 7.9）。

上記手順は、統計解析の一つの手法についての例となるが、本例に違わず、他の統計解析であっても、線形演算（加法・乗法の組合せ）である限りにおいて、完全準同型暗号を用いた秘密計算は可能と言える。

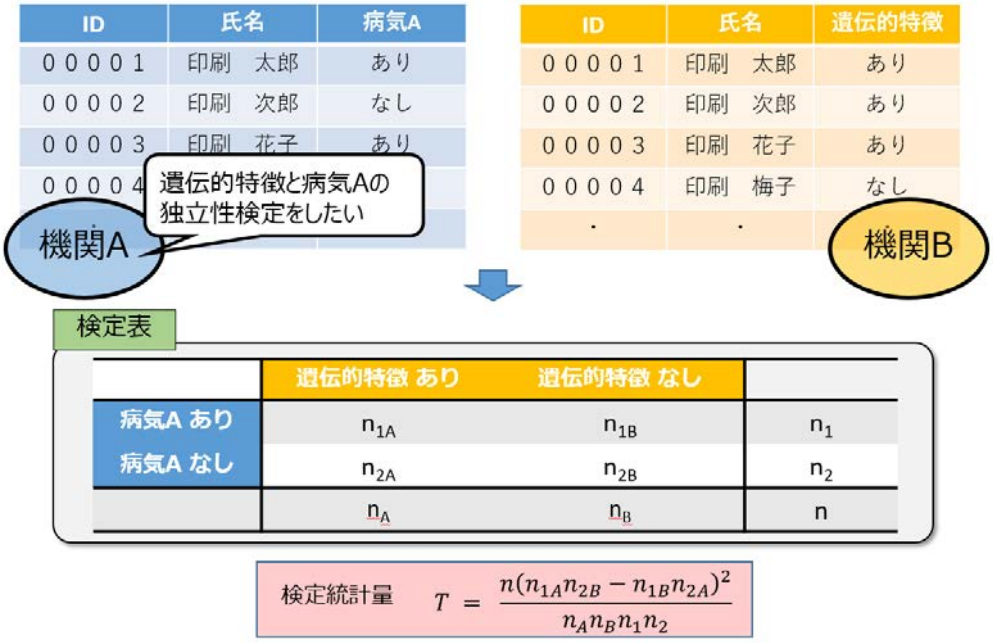


図 7.8　独立性検定の想定状況

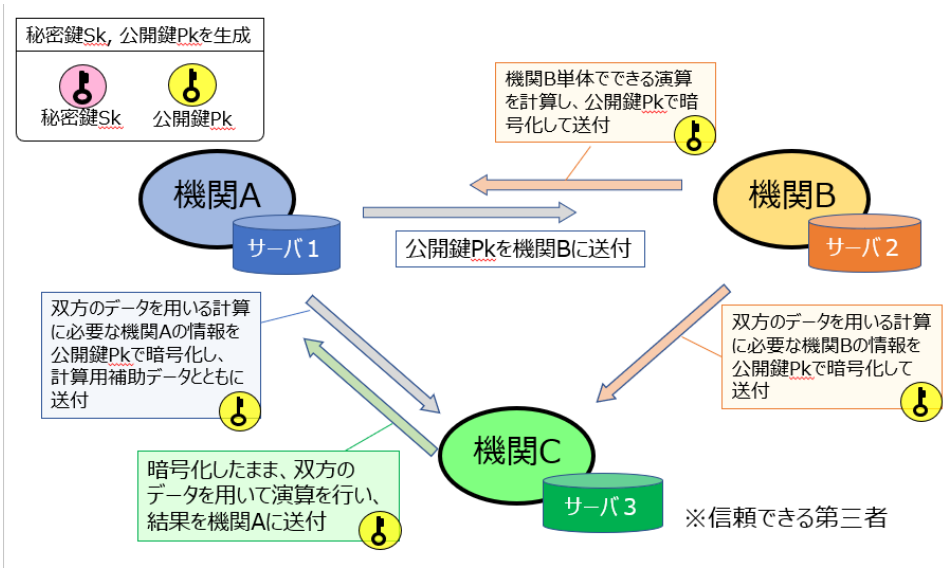


図 7.9 準同型暗号を用いた秘密計算例

7.4.3　秘密分散及び準同型暗号による秘密計算の比較

秘密分散を用いた秘密計算（MPC）と準同型暗号を用いた秘密計算は、それぞれ長所短所を持ち、処理時間やデータの通信量は異なるものとなる。一例として、20bit・100 万件のデータのソートに係る時間がある報告[32]で述べられており、秘密分散を用いた方法の通信量は複雑で示されていないが処理時間は 1.1 秒で完了するのに対して、完全準同型暗号を用いた計算の通信量は 0 とされているが

処理時間は 48,877 秒と報告されている。この結果から、現時点においては、秘密分散を用いた秘密計算では処理時間は短いが、データ通信量が多くなる傾向があり、準同型暗号を用いた秘密計算では、処理時間は長くなるが、データ通信量が小さくなる傾向があると言える。

7.4.4　秘密計算のまとめ

本節では、異なる機関が有するデータを互いに共有することなく、秘密性を保ったまま統計解析を実行する秘密計算の主な手法について述べた。これらの手法は、異なる複数の機関が有するプライバシー情報を含むパーソナルデータから全体の統計量を計算する場合に使用されるほか、一つの機関内であっても、アクセス権限を部署ごとに分散している場合にも使用可能な技術である。

つまり、パーソナルデータのデータベースへの保存方法やアクセス権限を分割することが可能な技術であり、機関に所属する職員において一人の個人が全てのパーソナルデータを閲覧できる状態（内部不正が生じやすい環境）を回避することも可能な技術と言える。また、格子暗号及びそれを利用する完全準同型暗号は、現在、開発途上であることから、今後、様々な改良が進んでいくものと考えられる。

7.5 差分プライバシー

差分プライバシーは、2006 年に Microsoft 社に関連する研究機関の研究者らが開発した、弱い秘匿性を満たすプライバシー定義の一つである[33,34]。近年、盛んに研究され、Apple 社の OS や Microsoft 社の Windows の一部に採用されている技術である[35]。

7.5.1 差分プライバシーの概要

(1) 技術の概要

差分プライバシーの概念は、様々なところで利用可能であるが、以下の前提条件を持つ統計量公開におけるモデルで説明する。

- データ収集者は、個人からデータを収集　　（データベース構築）
- データ利用者は、データ収集者に統計解析を問合せ　（クエリの発行）
- データ収集者は、問合せに応じた結果を提供　　（統計量の公開）

また、攻撃者には、無限の計算能力やデータベースに関する任意の事前分布の背景情報を持つなど、高い攻撃力を持つことを想定する。

- 攻撃者は、無制限の計算能力を持つ
- 攻撃者は、データベースについて任意の事前分布の背景情報を持つ
- 攻撃者は、ベイズ推定により入力のデータベースの事後分布を求める

このデータベースへの問合せモデルにおける統計量公開では、攻撃者は統計量から個人に関する情報がどの程度推測できるかという問題となる。この問題の極端な例としては、攻撃者による次のような二つの問合せも考えられる。

① 受験者全員の平均値
② Ａ氏を除く受験者全員の平均値

この場合、上記二つの正しい応答からＡ氏の得点は容易に推測可能であることが分かる。

差分プライバシーを直感的に表現するとデータベースに対して、平均などの何らかのクエリ（問合せ）を実行した場合、データベースはクエリに応じた統計値を算出するが、出力する際にノイズを加えることで、その統計値から個人に関わる情報を読み取れなくする技術となる。その際、ノイズの大きさは、「①一定のプライバシーが保護される大きさ（プライバシー保護）」と「②本来の統計量に近い値が出力される大きさ（データの有用性）」を考慮して設計することが重要な技術となる。

(2) 差分プライバシーの定義

表形式の二つのデータベースをD, D'とし、同一でないレコードの数（データ

ベースD, D'の距離）を$d(D, D')$と表記する。この時、$d(D, D')$が 0 の場合は、データベースD とデータベースD'は同じデータベースとなり、$d(D, D')$が 1 の場合は、任意の一つ（一人分）のレコードを除き、残りのレコードは同じことを意味する。また、データ集合Dに対する問合せqについて、ノイズを加える確率アルゴリズム（メカニズム）を$\mathrm{m}(q, D)$とする。このとき、差分プライバシーは、以下のとおり定義される。

【定義】
クエリq において、$d(D, D') = 1$ なる任意のデータベースの組 $D, D' \in \mathbb{N}^{|x|}$、及び、任意の出力range(m( )) の部分集合S について、

$$\frac{Pr[m(q, D) \in S]}{Pr[m(q, D') \in S]} \leq exp(\varepsilon)$$

$$\begin{cases} m(\ ) : \textit{確率アルゴリズム} \\ S \subseteq range(m(\ )) \\ \textbf{for all}\ \ D, D' \in \mathbb{N}^{|x|}, \textbf{such that}\ \ d(D, D') = 1 \end{cases}$$

ならば、メカニズムm( )はε差分プライバシーを満たす。

この定義の詳細について、直感的な理解は次のようになる。まず、データベースDの任意の一人分のデータを変更しても（データベースD'）、メカニズムの出力は大きく変わらず、データベースDに基づくメカニズムが出力する値の分布とデータベースD'に基づくメカニズムが出力する値の分布に大きな違いがないことになる。一方、メカニズムの出力値を受け取った攻撃者は、その出力値がデータベースDから生成されたか、データベースD'から生成されたかを高い確信度で推測することができなくなる。つまり、出力値から任意の個人のパーソナルデータを確定的に求めることが困難となる。

(3) メカニズム（確率アルゴリズム）

差分プライバシーを保証する出力関数はメカニズムと呼ばれ、メカニズムに何を用いるかが差分プライバシーの重要な要素となっている。メカニズムについては、様々なメカニズムが報告されており、ラプラス分布に従うノイズを付与するラプラスメカニズム、ガウスノイズを付与するガウシアンメカニズム、ランダムレスポンスや指数メカニズムなどがある。これらのメカニズムは、クエリの内容や使用する状況に応じて適切に設計する必要がある。

7.5.3　差分プライバシーのまとめ

差分プライバシーは、主に統計量の公開時等において使用される技術となっており、これまでのプライバシー保護技術では困難であった「プライバシー保護の度合いとデータの有用性の関係を一つの定数εで表すことができること」及び「出力値に適切なノイズを計算して加えることにより、外れ値へ対応可能なこと」に特徴を持つ技術である。

この技術は、世の中の様々なデータベースから社会の発展等に資する統計情報の公開（データの利活用）を実施する際や、ビッグデータからＡＩ等の学習を行う際に、パーソナルデータを保護するのに有用な技術となっている。

7.6　総括

近年、使用又は開発されているプライバシー保護技術の主な手法や用途について調査したが、調査結果から、プライバシー保護技術には、主として、入力データに対する処理、データ解析時における技術、統計データの出力時（公開時）における技術があり、現在のプライバシー保護への関心の高まりから、システム設計の様々な観点においてプライバシー保護への配慮がなされていることが分かる。

また、プライバシーを保護するための技術については、一方で、ＣＢＤＣでは、プライバシー保護とマネーロンダリング対策（AML/CFT）の両立という課題がある[1,6,8]。これは、単にプライバシーを保護するのみではなく、一定の条件下では犯罪捜査等が実施可能な仕組み（プライバシーを制御する仕組み）が求められていることを意味する。例えば、これまでの説明の中で、プライバシー保護の観点から外部情報との「連結」が生じないようにする処理を述べてきたが、ＣＢＤＣでは、プライバシーを保護しつつも、特殊な条件下では、限られた範囲において「連結」が生じるような仕組も検討対象となることを示唆している。

ＣＢＤＣにおいて、プライバシー等に関わる情報をどのように保管し、どのように処理し、どのような条件下で、どのような主体に、どのような情報を公開するかについては、制度設計や全体の仕組みの基本的な考え方に関わる課題である。その仕組みを検討する場合は、プライバシーバイデザイン[36,37]など高位の考え方のほか、技術面では匿名化技術やその他のプライバシー保護技術が欠かせない要素の一つになると考えられる。また、その仕組みを社会全体でスムーズに運用する際に、公開鍵暗号基盤[38,39]における認証機関と同様に、パーソナルデータを取り扱う場合も、信頼できる第三者機関の必要性が高まることが想定される。

参考文献

[1] R. Auer., G. Corelli, J. Frost., “Rise of the central bank digital currencies: drivers, approaches and technologies”,BIS Working Papers, No. 880, Aug., 2020.

[2] Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements, “Central bank digital currencies: foundational principles and core features,” Bank for International Settlements HP, 2020.

[3] Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements, “Central bank digital currencies: system design and interoperability,” Bank for International Settlements HP, 2021.

[4] Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements, “Central bank digital currencies: user needs and adoption,” Bank for International Settlements HP, 2021.

[5] Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve System, Bank for International Settlements, “Central bank digital currencies: financial stability implications,” Bank for International Settlements HP, 2021.

[6] Bank for International Settlements, “CBDCs: an opportunity for the monetary system,” Part III, BIS Annual Report 2021

[7] Federal Reserve Board, “Money and Payments: The U.S. Dollar in the Age of Digital Transformation,” Federal Reserve Board HP, 2022.

[8] U. Bindseil, F. Panetta, I. Terol, “Central Bank Digital Currency: functional scope, pricing and controls,” Occasional Paper Series, ECB HP, no. 286, Dec., 2021

[9] 日本銀行決済機構局、「第 2 回 中央銀行デジタル通貨に関する連絡協議会」(2021)、事務局説明資料「中央銀行デジタル通貨に関する日本銀行の取り組み」、
https://www.boj.or.jp/announcements/release_2022/rel220413a.pdf

[10] Gabriel Soderberg et al., “Behind the Scenes of Central Bank Digital Currency, Emerging Trends, Insights, and Policy Lessons,” FINTECH NOTES, IMF, 2022.

[11] 佐久間 淳, “データ解析におけるプライバシー保護技術“, 機械学習プロフェッショナルシリーズ, 講談社, 2016 年

[12] L. Sweeney, “k-anonymity: A model for protecting privacy,” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557-570, 2002

[13] ITMedia HP, “プライバシー保護データマイニング手法の種類、特徴を理解する”, 2015 年 3 月
https://atmarkit.itmedia.co.jp/ait/articles/1503/24/news010.html

[14] P. Samarati et al., “Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression,” Harvard Data Pricacy Lab.

[15] A. Machanavajjhala, D.Kifer, J. Gehrke, M. Venkitasubramaniam, “ℓ-diversity: Privacy beyond k-anonymity,” ACM trans. On Knowledge Discovery from Data, 1(1):3, 2007.

[16] 東京大学教養学部統計学教室, “統計学入門“, 東京大学出版会, 1991 年

[17] 東京大学教養学部統計学教室, “人文・社会科学の統計学“, 東京大学出版会, 1992 年

[18] 東京大学教養学部統計学教室, “自然科学の統計学“, 東京大学出版会, 1992 年

[19] 光成 滋生, “クラウドを支えるこれからの暗号技術“, 秀和システム, 2015 年、p.12、pp.30-38、pp.147-155

[20] NTT, 「NTT 持株会社ニュースリリース “医療統計処理における秘密計算技術を世界で初めて実証”」, 2012 年 2 月, https://group.ntt/jp/newsrelease/pdf/news2012/1202/120214a.pdf

[21] 東北大学, プレスリリース・研究成果, ”複数の研究機関が持つゲノムデータを相互に開示せず分析する解析手法を開発,” 2016 年 7 月,
https://www.tohoku.ac.jp/japanese/newimg/pressimg/tohokuuniv-press20160712_01web.pdf

[22] 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, Vol. 63, No. 2, pp.71-76, 2019.

[23] 岡本 龍明, “現代暗号の誕生と発展 ポスト量子暗号・仮想通貨・新しい暗号”, 近代科学社, 2019 年、pp.117-126、pp.205-208

[24] 林 卓也, “準同型暗号を用いた秘密計算とその応用,” システム/制御/情報, Vol. 63, No. 2, pp.64-70, 2019.

[25] C.E. Shannon, “Communication Theory of Secrecy Systems,” Bell System Technical Journal. Vol.28(4), pp656-715, Oct.1949.

[26] A. Shamir, “How to Share a Secret,” Communications of the ACM, Vol.22(11), pp.612-613, Nov. 1979.

[27] 北条 裕之, 山口 卓也, 西山 小奈未, 高橋 元, 宮島 麻美, 廣田 啓一, 西田 祥子, 橋本 順子, “秘密計算システム算師®の試用提供,” NTT 技術ジャーナル, 2019 年 2 月, pp.19-22

2019 年 2 月

[28] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” STOC '09: Proceedings of the forty-first annual ACM Symp. On Theory of Computing May, 2009, pp.169-178, 2009.

[29] NIST HP, “Post-Quantum Cryptography PQC,” http://csrc.nist.gov/groups/ST/post-quantum-crypto/, （2022 年 2 月アクセス）

[30] 宇根 正志, 菅 和聖, ”量子コンピュータ開発の進展と次世代暗号,” 日本銀行金融研究所,金融研究, 第 40 巻第 4 号, 2021 年 10 月.

[31] 高木 剛, ”耐量子計算機暗号の最新動向,” NICT サイバーセキュリティシンポジウム 2021.

[32] 菊池 亮, 五十嵐 大, ”秘密計算の発展-データを隠しつつ計算する仕組みとその発展,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 12 巻, 1 号, 2018, pp.12-20

[33] C. Dwork, F. McSherry, K. Nissim, and A. Smith, ″Calibrating noise to sensitivety in private data analysis,” In Proc. Of Theory of Crypt. Conf. 2006, pp. 265-284, Springer, 2006.

[34] C. Dwork and A. Roth, “The Algorithmic Foundations of Differential Privacy,” Foundations and Trends® in Theoretical Computer Science, Vol.9, Nos.3-4(2014)211-407.

[35] CNET Japan, ニュース・解説, “アップルのプライバシー対策--機能強化との両立を図る「Differential Privacy」,” 2016 年 6 月, https://japan.cnet.com/article/35084497/

[36] P. Hustinx “Privacy by Design: Delivering the Promises,” Springer, 2010.

[37] 総務省, 経済産業省, “DX 時代における企業のプライバシーガバナンスガイドブック ver1.2,” 経済産業省 HP, 2022 年 2 月, <https://www.meti.go.jp/policy/it-policy/privacy/guidebook12.pdf> (2022 年 2 月アクセス)

[38] 情報処理推進機構 HP, “PKI 関連技術情報,” <https://www.ipa.go.jp/security/pki/> (2022 年 2 月アクセス)

[39] 板倉 征男, 外川 政夫, “ネット社会と本人認証 原理から応用まで,” 電子情報通信学会, 2010

8　おわりに

日本を含む各国でＣＢＤＣの検討が進む背景の一つには、暗号資産、ステーブルコインなどのデジタル資産、中国などの他国が発行するＣＢＤＣなどに自国通貨が他国に流れることへの警戒、国民から海外送金を含む手数料削減要望の高まりなどへの対応があると考えられる。日本銀行をはじめ、多くの主要中銀の考え方としては、発行の計画はないが、発行に向けた準備をするというものであり、日本銀行では 2021 年４月から実証実験が計画的に進められ、その進捗は中央銀行デジタル通貨に関する連絡協議会を通じて共有されている。加えて、日本銀行の制度設計などＣＢＤＣの設計に関する議論が進められているとされており、本研究会としても、ＣＢＤＣに求められる要素や機能に着目したうえで、データ取扱いに関する知見を深めるものとして、プライバシー保護とデータの利活用、効率的な制度設計に必要となる要素を調査した。

具体的には、個人、法人など利用者のウォレット開設時の認証、取引時の認証を目的としたデジタルＩＤの活用を想定して、認証方法や認証機関の業務内容を整理することで、ＣＢＤＣエコシステムの一要素と考えられる認証機関業務についての理解を深められた。

一方、プライバシー保護とデータの利活用（ＡＭＬ／ＣＦＴ含む）というトレードオフの関係にある目的を成立させるための技術として、秘密分散、秘密計算、差分プライバシーといった技術の動向に関する整理を行った。整理を進めることで、確実にプライバシーが確保可能な匿名化方法、暗号化した状態でも統計値等の計算を可能とする技術などの理解が深まった。プライバシー保護に関しては、ＧＡＦＡ等のプラットフォーム事業者の個人情報の取扱いを巡り、国際的にも対応が求められており、国民の関心も高まってくることが想定される。利用者が納得感を持ってＣＢＤＣを使用するためには、設計上の配慮が求められることから、匿名化技術やその他プライバシー保護技術は欠かせない要素となると考えられる。なお、プライバシー保護技術等に暗号化を使用する仕組みとする場合は、公開鍵暗号基盤が必要となり、ＩＤ管理と同様に認証機関が必要となる可能性が多分にあると考えた。

今後、ＣＢＤＣエコシステム構築などの検討が進められる中で、本レポートに記載した知見を蓄積することで、その検討過程において国立印刷局の特性を踏まえ、エコシステムの中で担える領域など、引き続き調査、研究を継続していくこととしたい。