中央銀行デジタル通貨（CBDC）に関するレポート

（令和５年度）

2024 年 7 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」に関係する職員の令和6年3月末日時点の調査・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。

頭字語、略語　一覧

AML	Anti-Money Laundering
AMS	Access Management System
API	Application Programming Interface
BCP	Business Continuity Plan
BIS	Bank for International Settlements
BOE	Bank of England
CBDC	Central Bank Digital Currency
CeFi	Centralized Finance
CEO	Chief Executive Officer
CFT	Countering the Financing of Terrorism
CIO	Chief Information Officer
CSP	Credential Service Provider
DNA	Deoxyribonucleic Acid
DB	Data Base
DeFi	Decentralized Finance
DID	Decentralized Identifier
DIF	Decentralized Identity Foundation
DMA	Digital Markets Act
DoS	Denial of Service
DSA	Digital Services Act
EEA	European Economic Area
EC	Electronic Commerce
ECB	European Central Bank
e-CNY	The electronic China Yuan
ESIP	External Service Interface Provider
EU	European Union
FRB	The Federal Reserve Board
GDPR	General Data Protection Regulation
HP	Homepage
IAMS	Identity and Access Management System
ID	Identifier
IDaaS	Identity as a Service
IdP	Identity Provider
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMS	Identity Management System
ISIS	Islamic State of Iraq and Syria
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KYC	Know Your Customer
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
PArSEC	Parallelized Architecture for Scalably Executing smart Contracts
PIP	Payments Interface Provider
PSP	Payment Service Provider
RP	Relying Party
RTGS	Real-Time Gross Settlement
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SNS	Social Networking Service
SSI	Self-Sovereign Identity
SSO	Single-Sign On
TEE	Trusted Execution Environment
ToIP	Trust Over IP Foundation
UI/UX	User Interface/ User experience
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTXO	Unspent Transaction Output
VC	Verifiable Credentials
VP	Verifiable Presentation
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WG	Working Group
XML	Extensible Markup Language

1 はじめに

中央銀行デジタル通貨（CBDC）については、2019 年に当時のフェイスブック社（現メタ社）が公表したグローバルステーブルコイン構想や、中国におけるデジタル人民元の研究開発の進展等が契機となり、各国・各地域での検討が進められている。2023 年の国際決済銀行（BIS）の報告によると、2022 年には、世界の中央銀行の 93%が何らかの調査・検討を実施しているとされる[1]。

日本においても、日本銀行が 2020 年 10 月に「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」を公表し、2021 年 4 月から 2 年間実施した概念実証の結果を踏まえ、2023 年 4 月にはパイロット実験に移行する等、段階的な取組が進められている。なお、パイロット実験には、実験用システムによる検証のほかに、制度設計を適切に進める観点から、民間事業者の知見を得ながら幅広いテーマで議論・検討を行うための「CBDC フォーラム」も含められている。また、財務省は CBDC に関する制度設計の大枠の整理に向けて 2023 年 12 月に「CBDC に関する有識者会議」の議論の取りまとめを行った。そして、2024 年 1 月には政府・日本銀行として CBDC に関する制度設計の大枠を整理するため「CBDC に関する関係府省庁・日本銀行連絡会議」[2]を設置している。

国外に目を移すと、CBDC の実装に関する検討を進めている国・地域として、冒頭に記載した中国が挙げられる。その取組は、パイロット実験において、検証範囲を国内非居住者まで広げる等、検証内容や試験地域の段階的な拡大が続けられている状況にあるが、発行等に関する情報等公式な情報は少ない状況にある。その他、欧州中央銀行やイングランド銀行においては、設計に関する考え方を示した上で、国民や民間事業者の意見を聴取する市中協議等を行っている。

このように国内外で CBDC の検討が進む中、国立印刷局 CBDC 研究会は、国内外の CBDC に係る動向の整理、暗号資産・電子マネー等のデジタル資産に係る事件や攻撃事例等の分析、CBDC に必要となり得る要件や技術の考察等、調査・研究を継続的に実施している。そして、これまでに通貨に対する信頼を確保する観点から、プライバシー保護や情報通信における安全な処理方法の仕組みに焦点を当てた調査結果を報告してきたものである[3]。

本レポートにおいても、CBDC に係る国内外の動向や暗号資産・電子マネー等の事件・攻撃の整理に加えて、サイバー空間上での取引における「デジタルアイデンティティ」の取扱いに焦点を当てた調査について報告を行っている。

[1] BIS,“Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto”,2023.7.10,
（https://www.bis.org/publ/bppdf/bispap136.htm）

[2] 財務省、「CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議の設置について」、2024.1.26、
（https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/kaisai.html）

[3] 国立印刷局、「中央銀行デジタル通貨（CBDC）に関するレポート」、2022.8、2023.6、
（https://www.npb.go.jp/ja/guide/security/teikyo.html#security14）

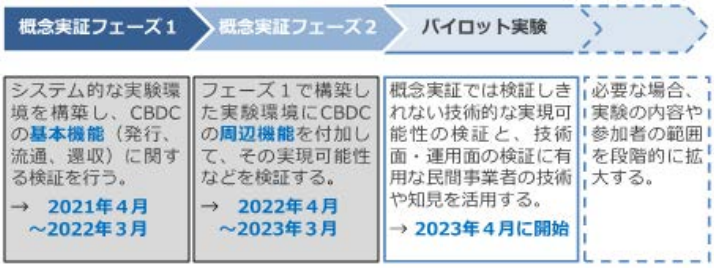
2　環境分析

2.1　国内の動向

CBDC に関しては、経済財政運営と改革の基本方針（骨太の方針）2020 に初めて記載が盛り込まれて以降、日本銀行における実証実験等の取組、財務省における有識者会議の設置など各種整理が進められている。政府は 2023 年 6 月 16 日に骨太の方針 2023 を閣議決定したが、同方針では、「CBDC について、政府・日本銀行は、年内目途の有識者の議論の取りまとめ等を踏まえ、諸外国の動向を見つつ、制度設計の大枠を整理し、発行の実現可能性や法制面の検討を進める。」としており、継続的な検討を進めることが示されている。

2.1.1　日本銀行

日本銀行は、2021 年 4 月から実証実験において概念実証を開始しており、2023 年 3 月には概念実証を終了し、2023 年 4 月からパイロット実験を開始している。

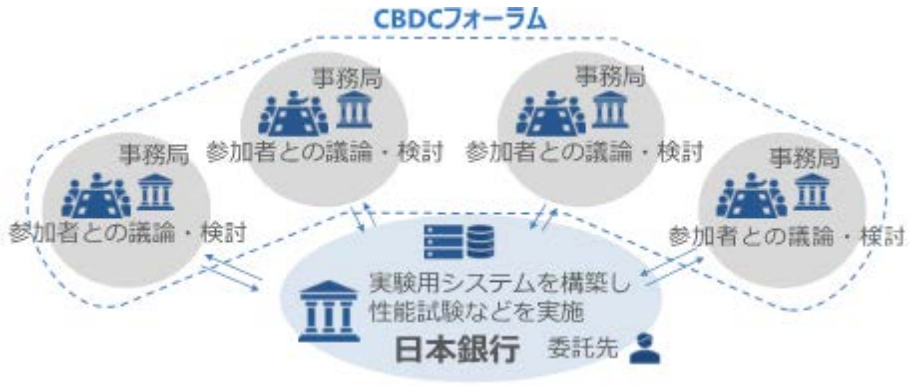


出典：日本銀行、「中央銀行デジタル通貨に関する実証実験について」、2023.2.17、（https://www.boj.or.jp/paym/digital/dig230217b.pdf）

図 2.1　日本銀行における実証実験の取組状況

パイロット実験は、検証の範囲を中央システムからエンドポイントデバイスまでを含め、技術的な実現可能性の検証を行うとともに、技術・運用の両面にわたって、CBDC を社会的に実装する場合の設計に、民間事業者の技術や知見を活用するために「CBDC フォーラム」を設置し、多岐にわたるテーマごとに関係する事業者を集めたワーキンググループ（WG）により議論が進められている。

なお、日本銀行は、CBDC の導入に関しては、現時点では決まっていないとし、今後の国民的な議論の中で決定されるべきものとしている。そして、こうした議論に資する観点からも、今後の様々な環境変化に的確に対応できるよう準備を進める方針としている。



出典：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」、2023.11.14、p.4、
（https://www.boj.or.jp/paym/digital/dig231114b.pdf）

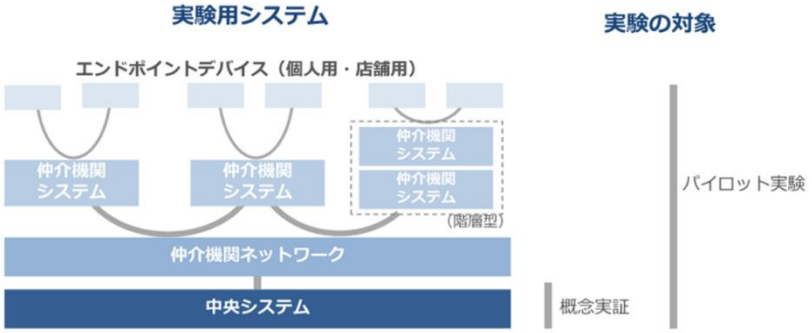
図 2.2　パイロット実験の概要

(1)　実験用システムの構築と検証

実験用システムの構築については、業務委託先の選定を行うための手続を経て、2023 年 11 月には、実験用システム構築及び各種検証作業等の業務を株式会社日立製作所[1]に、プロジェクト管理支援及び技術コンサルティング業務をデロイトトーマツコンサルティング合同会社[2]にそれぞれ委託するものとしている。以下、実験用システムの構築と検証の概要を示す。

イ　実験用システムの検証の範囲

実験用システムの検証は、2022 年度までに実施された概念実証から検証の範囲を拡大して、実験用システムを構築し、エンドツーエンドでの処理フローの確認や、外部システムとの接続に向けた課題・対応策の検討などを行うものとしている。なお、現時点では、実験用システムの検証においては、店舗や消費者が関与する実取引を行うことについて想定されていない。



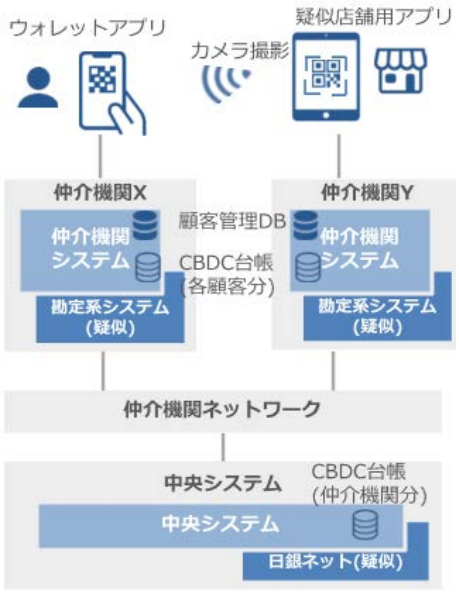
出典：日本銀行、「第 2 回 CBDC フォーラム全体会合資料」、2024.1、p.4、
（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.3　実験用システムの検証における対象範囲

ロ　システム構成と特徴

実験用システムは、エンドポイントデバイス（ウォレットアプリ）から中央システムまでの実装を含めている。また、プライバシー配慮を設計に反映し、顧客個人情報を扱う部分（データベース）と顧客の決済情報を扱う部分（台帳）を分離して構築している（図 2.4 参照）。

これら実験用システムを構築し、概念実証フェーズの知見を踏まえ、性能・事務量、更には機能・性能に関する拡張性の実現に向けた技術的な留意点や解決策の洗い出しを行うものとしている。



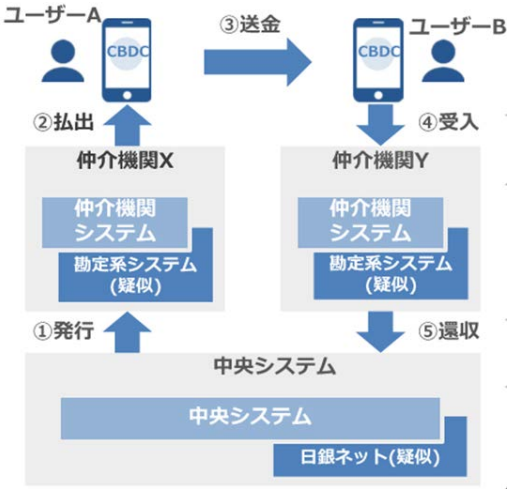
出典：日本銀行、「第2回CBDCフォーラム全体会合資料」、2024.1、p.5、（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.4　実験用システム概略

ハ　実験用システムで構築する機能

（イ）　基本機能

実験用システムには、発行・還収、払出・受入、送金の 5 つが基本機能として実装される。それぞれの機能は、図 2.5 に示すとおりであり、疑似的な日銀ネット、勘定系システムとの連携により、日銀当座預金、金融機関の預金との連携による基本機能の確認が想定されている。また、送金機能に関しては、CBDC 保有制限等を想定した機能として、ユーザの CBDC 口座に紐づく預金口座への CBDC 上限超過額の自動振替（オートスウィング）、CBDC 支払不足額の預金口座からの自動払出（オートチャージ）などの実装が想定されている。



出典：日本銀行、「第2回CBDCフォーラム全体会合資料」、2024.1、p.6、（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.5　実験用システム基本機能

（ロ）　周辺機能

実験の対象範囲をエンドポイント（ユーザ）まで拡大して検証を行うことから、周辺機能として、ユーザの求めるサービスを想定した各種機能を含めて確認することとしている。主な機能は取引指図に従い、予約送金（一括送金）及び逆引送金を行う機能や、ユーザが仲介機関システムに対して残高や過去の取引明細を照会する機能などである。

出典：日本銀行、第2回CBDCフォーラム全体会合資料、2024.1、p.7、（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.6　実験用システム周辺機能

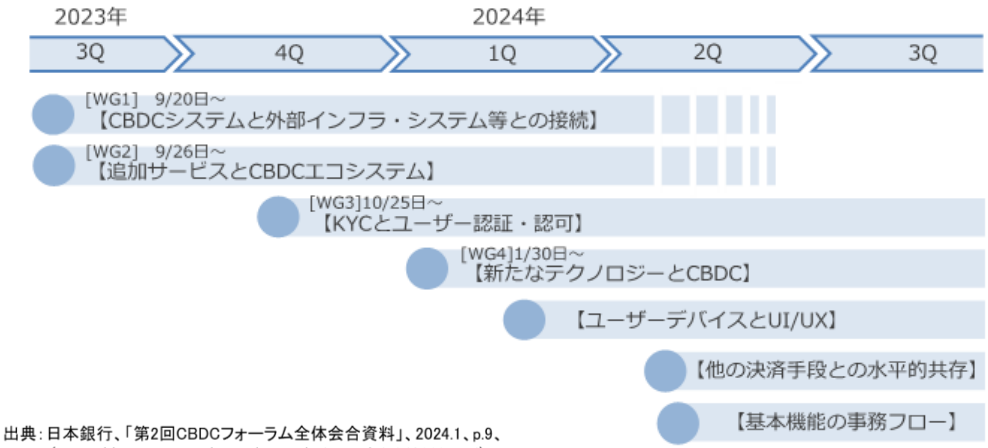
(2)　CBDC フォーラム

2024 年 1 月時点での CBDC フォーラムにおける具体的な議論・検討テーマは以下のとおり。なお、状況や議論の進捗に応じ随時追加・削除するとされており、関連する情報は、日本銀行から適宜発信されている。表 2.1 に示す WG 一覧は、2023 年 9 月時点のものであり、2024 年 1 月には WG4 として「新たなテクノロジーと CBDC」が開始されている。

表 2.1　CBDC フォーラムの WG 及び検討テーマ

WG名		検討テーマ
[WG1]	CBDCシステムと外部インフラ・システム等との接続	勘定系システムとの接続
		民間決済インフラとの接続
		既存のインターネットバンキングアプリ等との連携
[WG2]	追加サービスとCBDCエコシステム	CBDC のビジネス活用（追加サービスのあり方）
		追加サービスにかかるCBDC システムの外部連携
		CBDC エコシステムのデザイン
[WG3]	KYCとユーザー認証・認可	KYC、AML/CFT の実施
		認証・認可
	新たなテクノロジーとCBDC	代替的なデータモデルの選択肢（UTXO 等）
	他の決済手段との水平的共存	電子マネー等との交換容易性
	ユーザーデバイスとUI/UX	UI/UX、アクセシビリティ
		エンドポイントデバイス
		オフライン決済
	基本機能の事務フロー	基本的な機能にかかる事務フロー
		現金とCBDCの交換

出典：日本銀行、「【CBDCシステムと外部インフラ・システム等との接続】ワーキンググループ（WG1）について」、2023.9、p.19、（https://www.boj.or.jp/paym/digital/d_forum/dfo230920b.pdf）



出典：日本銀行、「第2回CBDCフォーラム全体会合資料」、2024.1、p.9、
（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.7　WG の進め方イメージ

2.1.2　財務省

(1)　CBDC（中央銀行デジタル通貨）に関する有識者会議

財務省は、2023 年 4 月に CBDC に関する制度設計の大枠の整理に向けて、高い識見を有する者から意見を聴取するための有識者会議を設置した。会議は、2023 年 4 月から 12 月にかけて計 8 回開催され、国内外の議論の状況を踏まえ、通貨、決済の現状、民間決済手段などの現状認識を共有しつつ、CBDC に係る論点整理を進め、12 月には取りまとめとして制度設計の大枠の整理に向けた考え方などを整理・公表している。「取りまとめ」は、CBDC 検討に至る背景、国内の決済手段としての CBDC のあり方などを念頭に置きつつ、日本において仮に CBDC を導入する場合に考えられる制度設計上の主要論点に関する基本的な考え方や選択肢等を明らかにする観点からまとめられたものである。

CBDC の検討動機は「国・地域の置かれている多種多様な環境により異なるものであり、日本の状況を踏まえた多角的な検討が必要となる」としている。また、CBDC の制度設計上の課題を考えるに当たっては、「民間デジタル決済手段と共通の課題かどうかを整理した上で検討を進めることが望ましく、これら検討の先にある我が国の CBDC は、デジタル社会にふさわしい通貨として、誰でも、いつでも、どこでも、安全・確実に利用できる、利便性の高いデジタル決済手段にしていくことが重要である」として、以下の 3 点を課題として取り上げている。

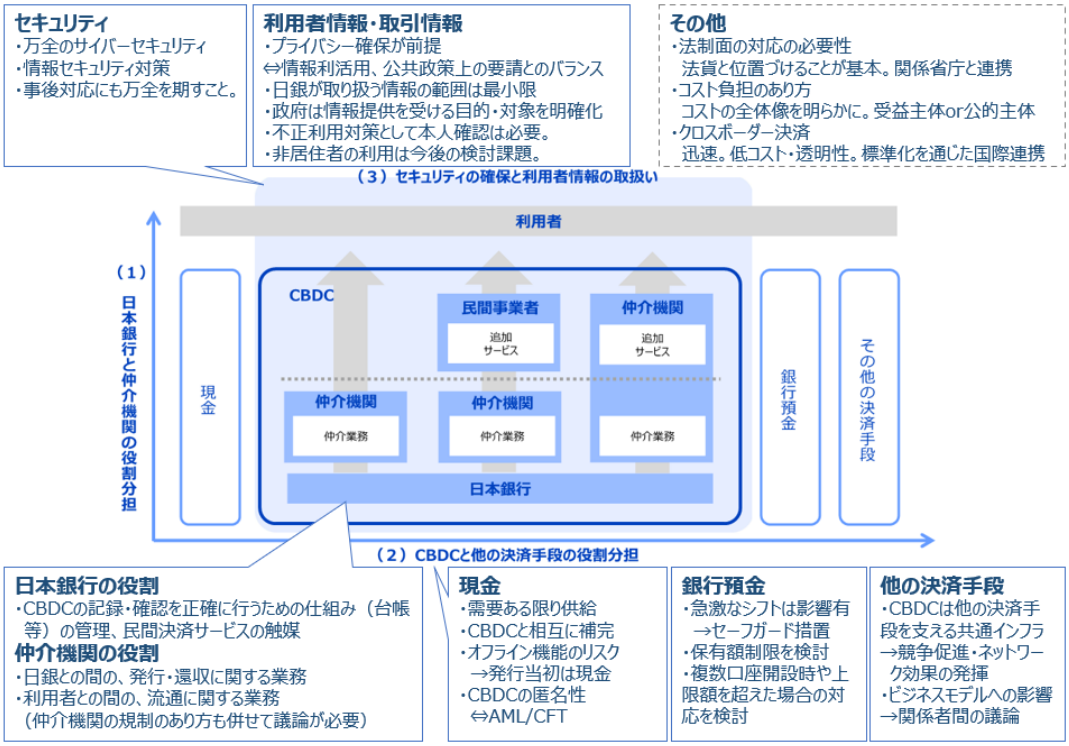
- ✓ 利用者の多様なニーズを踏まえつつ、CBDC を利便性の高い決済手段として提供していくために、日本銀行と仲介機関の役割分担をどう考えるか。

✓ 我が国では既に各種の決済手段が提供されている中で、決済システム全体としての安定性・効率性の確保を図っていくために、どのように CBDC と各種の決済手段との共存・役割分担を行うのか。

✓ いかに決済手段として常時機能させるとともに、プライバシーに対する国民の懸念に応えていくのか。

このような課題を踏まえ、制度設計の大枠の整理に向けて、以下に示す項目に関する基本的な考え方や考えられる選択肢等を整理しており、その概略は図 2.8 のとおりである（詳細は財務省 HP を参照）。

① 日本銀行と仲介機関の役割分担（垂直的共存）
② CBDC と他の決済手段の役割分担（水平的共存）
③ セキュリティの確保と利用者情報の取扱い
④ その他



出典：財務省「CBDC（中央銀行デジタル通貨）に関する有識者会議 取りまとめ（概要）」、2023.12.13、（https://www.mof.go.jp/about_mof/councils/meeting_of_cbdc/20231213torimatomegaiyou.pdf）を参考に作成

図 2.8 制度設計の大枠の整理に向けた考え方（概略）

取りまとめの結びにおいては、「通貨が経済取引の根幹を支えるものであり、そのあり方が国民生活にも広く影響を与えるものであることを示し、そのための通貨制度のあり方は、幅広い観点から、その将来のあるべき姿を見通して行く必要がある」こと、また、「欧米といった主要国・地域のほか、我が国と経済的関係が深いアジア諸国を含めた諸外国の動向、技術面

の進展等を見つつ、CBDC の設計に係る更なる具体化や必要な見直しについて、政府・日本銀行が密接に連携しながら行われることが期待されるもの」としている。

そして、「その際には、CBDC の導入によって、どのような社会課題の解決が図られるか、どのようにセキュリティやプライバシーは確保されるかなど、国民にとってわかりやすく具体的に説明を行っていくこと、更には CBDC に関する健全なエコシステムを構築していくために、関係事業者など幅広いステークホルダーの意見を踏まえて議論を積み上げていくことが重要」としている。

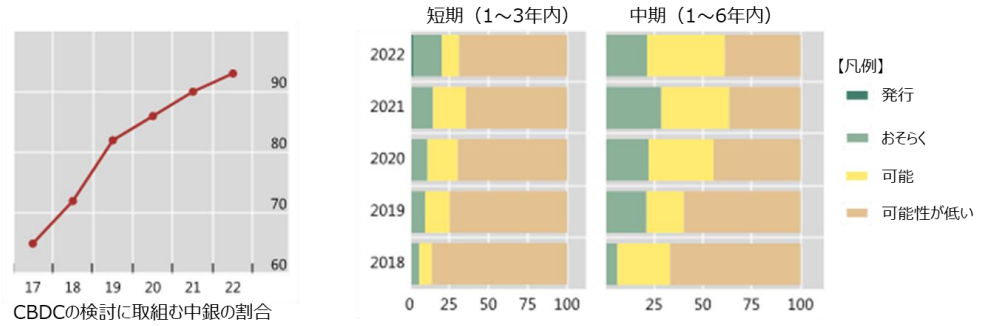
(2) CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議

政府・日本銀行として、有識者会議の取りまとめを踏まえ、制度設計の大枠を整理するために、2024 年 1 月に「CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議」を設置した[3]。会議は、財務省理財局長を議長として、内閣府、警察庁、金融庁など関係府省庁及び日本銀行の幹部で構成されている。そして、連絡会議の進め方として、仮に CBDC を導入する場合に、関係府省庁の所管行政において生じる課題の整理を行う方向で進めていくことが示されている。

2.2 各国の動向

CBDC の検討に係る状況は、国際決済銀行（BIS）が中央銀行（86 行）に対し実施した調査（2022 年 10～12 月）によると、検討中の中央銀行の割合は、前回調査の 90%から 93%に増加したとされている。加えて、半数以上の中央銀行が近い将来、リテール CBDC を発行する可能性があると回答したことを示している。

当該調査の中では、CBDC を発行している国・地域は 4 か所あり（バハマ、ジャマイカ、ナイジェリア及び東カリブ通貨連合）、金融包摂等の発行動機が高い新興国が先行している状況にある。検討の進捗については、経済取引や決済を取り巻く環境など、それぞれの置かれた環境が大きく影響するものであり、似たような環境下に置かれている国・地域の状況を中心に整理する。



出典：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、2023.11.14、p.16、（https://www.boj.or.jp/paym/digital/dig231114b.pdf）

参考：Kosse, Anneke and Ilaria Mattei, "Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto," BIS, July 2023を基に作成〈https://www.bis.org/publ/bppdf/bispap136.pdf〉

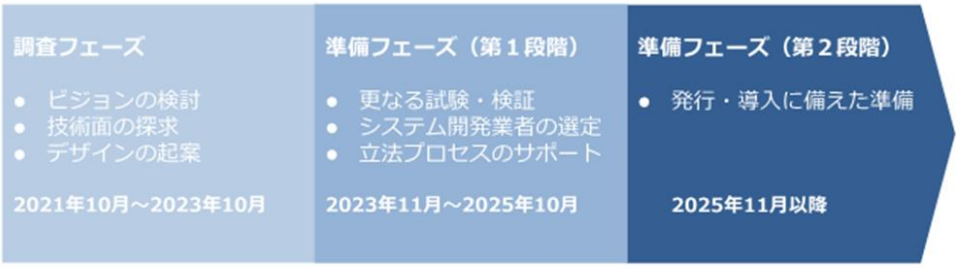
図 2.9　各国中央銀行の CBDC の検討状況及び発行の可能性

2.2.1　欧州

欧州中央銀行（ECB）は、デジタルユーロについて、2021 年 10 月から 2 年間「調査フェーズ」として検討を行い、期間終了時（2023 年 10 月）に検討結果を最終報告書として公表している。

同報告書では、ECB が 2022 年 7 月から 2023 年 2 月にかけて実施したプロトタイピング演習の結果として、革新的な機能や技術に十分な余地を残しつつ、デジタルユーロデザインの選択肢が既存の決済システムへスムーズに統合可能であること[4]と併せて、デジタルユーロの実装に係るコスト試算、要件整理を目的に、市場関係者から広くソリューションを募集した調査結果（2023 年 1 月募集、2023 年 5 月公表[5]）として、提示したデジタルユーロの各構成要素[6]に対するソリューションを開発可能なプロバイダが欧州に十分存在することが示された。

なお、ECB は最終報告書の公表を踏まえ、次の段階である「準備フェーズ」に移行しており、実装に向けた検討が進捗している状況にある。



出典：日本銀行、「第2回CBDCフォーラム全体会合資料」、2024.1、p.30、（https://www.boj.or.jp/paym/digital/d_forum/dfo240111a.pdf）

図 2.10　デジタルユーロのフェーズ展開

(1)　調査フェーズ報告書

報告書においては、欧州経済のデジタル化の進展によりデジタル決済の重要性が増しており、欧州の決済が将来にわたって安全で使いやすく、効率的な決済手段を維持することが重要として、公共財としての重要な役割を果たすデジタルユーロの必要性が示されている。

また、ユーザ視点のデジタルユーロについて、利用主体はユーロ圏居住者とし導入当初は非居住者等の利用は想定しないこと、口座開設は一人一つとし保有上限を設け、デジタルユーロに付利は行わないこと、更にはオフライン決済や現金・預金との交換を含めた利用方法などが示されている。そして、デジタルユーロ流通に係る決済サービスプロバイダ（PSP）の役割として、利用者管理、流動性管理、取引管理などの役割と、それらをサポートするユーロシステム提供のサービスなど、それぞれの利点を最大限に生かすための公的部門と民間部門の業務分担の考え方が示されている。

その他、デジタルユーロへのアクセス手段としてのスマートフォンアプリの提供に当たっては、すべての人々が包摂的に利用しやすい設計とすること[7]、現金によるウォレットへのデジタルユーロチャージ機能も想定した、物理的なカードを提供することなど、高度なデジタル金融包摂を実現する用意があることを示している。

最後に、プライバシー保護・データ保護に関しては、デジタルユーロに関する ECB と国民との対話から得られた重要な教訓であるとした上で、AML や CFT などの公共政策とのバランスを考慮したデジタルユーロ（オンライン及びオフライン）のプライバシーモデルを示しており、その中で、ユーロシステムがエンドユーザを直接特定できるようなデータにアクセスしたり、保存したりすることがないことを示している。また、エンドユーザは、自身の個人データがどのように使用されるかを完全にコントロールできるようにするなど、デジタルユーロ制度は、利用者が十分な情報を得た上で意思決定できることを保証するとしている。

(2)　準備フェーズにおけるルールブックの策定

2023 年 11 月から開始した準備フェーズにおいては、ECB は、デジタルユーロのルールブックの策定、プラットフォームやインフラの開発事業者の選定を実施することとしている。また、プライバシー保護等のユーロシステムが具備すべき要件と利用者の要望の双方を満たすデジタルユーロ開発に向けた検証も引き続き行うことを示している。

なお、ルールブックの策定の取組に関しては、調査フェーズ段階から継続的に行われており、2024 年 1 月、デジタルユーロスキームのルールブッ

ク作成グループ（消費者、小売業者、仲介業者を代表するメンバーにより構成）の取組状況に関する報告書[8]においては、以下の内容が網羅されている。

- ✓ ユースケースとサービスの機能を説明するエンドツーエンドのフローを含む機能モデルと運用モデル
- ✓ デジタルユーロのシステム構成で考慮される可能性のあるハイレベルなアーキテクチャと標準を示す技術的スキーム要件
- ✓ デジタルユーロ法案に従ってスキーム内関係者の権利と義務を定める遵守モデル

そして、このルールブック草案は、将来的な調整に対応できるような柔軟なものとし、並行して進められるデジタルユーロ立法プロセスの結果に応じて更新されるよう作成されており、今後もルールブックの最終形を目指して作業が継続される。なお、今後追加予定の要件は以下のとおり。

① ユーザ体験に関する最低要件
② ブランディング及びコミュニケーション基準
③ 認証
④ 試験及び承認手続
⑤ 内部規則
⑥ リスク管理
⑦ 相互運用性及び実装仕様

(3) 立法プロセスの開始

欧州委員会は、2023 年 6 月に欧州議会と欧州連合閣僚理事会による採択に向けた立法案（デジタルユーロ法案等）を議会に提出[9]し、立法プロセスを開始している。この状況を受け、ECB は、デジタルユーロの実際の発行が決定されてはいないものの、プロジェクト段階の進展に当たって、立法プロセスと並行するように準備フェーズの中でサポートを行うこととしている。

2.2.2 米国

米国の CBDC に係る検討状況としては、米国連邦準備制度理事会（FRB）が 2022 年 1 月に CBDC をテーマとした報告書を公表[10]し、広く一般からの意見を募集したことが挙げられる。また、2022 年 3 月にバイデン大統領がデジタルドルを含むデジタル資産の研究開発促進を指示する大統領令に署名[11]し、それに従い、2022 年 9 月に米国財務省及びホワイトハウス科学技術政策局が報告書を公表している[12,13]。加えて、ホワイトハウスは、デジタル資産

の責任ある発展に向けた初めての包括的なフレームワークであるとして、CBDC の可能性を認識した上で米国版 CBDC のための政府の優先事項を反映した政策目標を策定している。

また、ボストン連邦準備銀行とマサチューセッツ工科大学（MIT）のデジタル通貨イニシアティブが共同で研究を進めていた「プロジェクトハミルトン」は、2022 年 12 月にプロジェクトを終了している[14]。その成果は、2022 年 2 月にフェーズ 1 の報告書として公表された。また、継続して実施したフェーズ 2 の成果については、2023 年 8 月にスマートコントラクトをスケーラブルに実行するためのアーキテクチャとしての集中型プラットフォーム（PArSEC：Parallelized Architecture for Scalably Executing smart Contracts）の開発に関する報告書として、MIT により公表された[15]。

なお、ボストン連邦準備銀行と MIT は、プロジェクトハミルトンのフェーズ 1 において、デジタル通貨用の高性能な集中型トランザクションプロセッサとしての 2 つのアーキテクチャをいずれも UTXO モデルとして発表した。しかし、UTXO モデルで使用する UTXO ハッシュセットベースのシステムは、機能が限定的となり拡張性が確保しにくいことから、フェーズ 2 で開発されたプラットフォームは、汎用的なプログラミングモデルと、様々なスマートコントラクトのアプリケーションを集中環境で実行するものとして構築されている。そして、プロジェクト内で開発したコードは、「OpenCBDC」の一部として GitHub で公開され、オープンソースとして成果を共有することで、研究者や組織がこのソフトウェアに関与し、スマートコントラクト実装のユースケースとシステムセキュリティ等のトレードオフを更に探求することを望むものとされている。

上記のような検討、研究が進められる一方で、米国内においては、CBDC が政府の監視ツールとなることを危惧した反感が広範囲に広がり、CBDC の導入に対する警戒論が強まっているという見方もあり[16]、2023 年 9 月には、米下院金融委員会は、CBDC であるデジタルドルが国民監視に使用されることを阻止する法案を承認した[17]（ただし、下院で承認されたとしても、上院での可決については困難との見方がある[18]）。このような動きを受け、2023 年 10 月末の電子決済に関する会合の講演において、FRB のマイケル・バー副議長は、FRB が CBDC の発行について決定を下していないこと、政府と議会の立法承認があって初めて CBDC に関する手続を進めることを改めて強調している[19]。

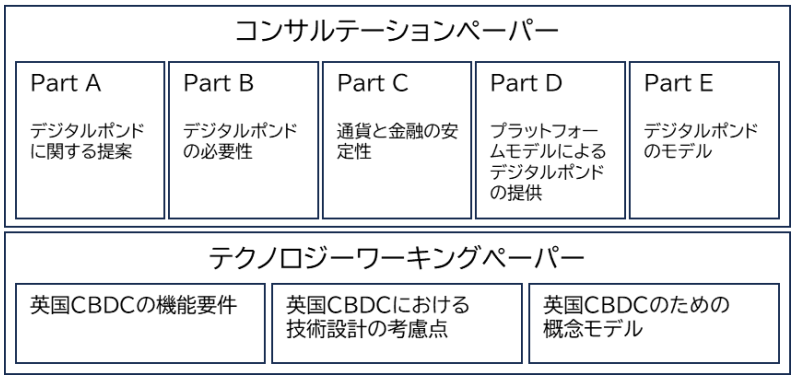
表 2.2　米国における状況

2022 年 1 月	FRB“Money and Payments: The U.S. Dollar in the Age of Digital Transformation”を公表
2022 年 3 月	バイデン大統領が大統領令に署名
2022 年 9 月	米国財務省“The Future of Money and Payments”公表
	ホワイトハウス“FACT SHEET : White House Releases First-Ever Comprehensive Framework for Development of Digital Assets”公表
2022 年 12 月	ボストン連銀と MIT の共同研究「プロジェクトハミルトン」終了
2023 年 8 月	MIT が PArSEC の開発に関する報告書を公表
2023 年 9 月	米下院金融委員会、CBDC による監視社会に反対する法案を承認

2.2.3　英国

(1)　市中協議文書の公表

イングランド銀行（BOE）と英国財務省は、2023 年 2 月にリテール CBDC（デジタルポンド）について、目的や基本的特性、構築時のシステム面の基本的考え方等を示した市中協議を目的として「コンサルテーションペーパー[20]」及び「テクノロジーワーキングペーパー[21]」を公表した[22]。



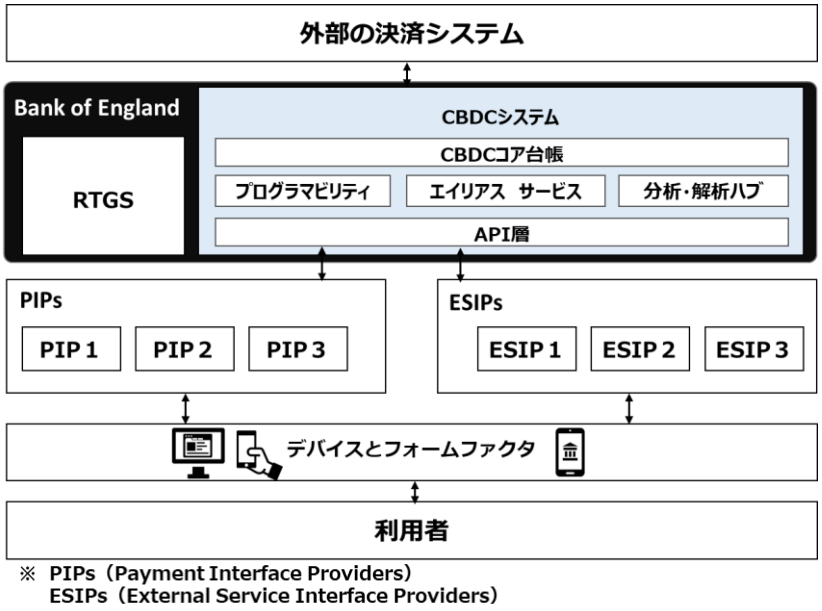
出典：イングランド銀行“The digital pound: Technology Working Paper”を基に作成
（https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf）

図 2.11　市中協議文書の構成

それぞれの文書は図 2.11 のとおり構成されており、BOE と英国財務省は、コンサルテーションペーパーにおいて、将来的にデジタルポンドが必要となる可能性が高く、そのメリットも大きいとの判断の下、通貨と金融安定性に向けた要件整理に加え、デジタルポンドの実現に向けた考え方として、中央銀行のインフラとしてのプラットフォームモデルを想定し、中央銀行と民間企業のそれぞれの役割分担により、プライバシー及びデータ保護を基本とした設計の考え方を提案している。

・現金と同じく中央銀行に対する直接的な債務として発行
・システムは、官民のパートナーシップにより実現
・アプローチとしては、以下の機能をもつプラットフォームモデルを想定
　・中央銀行はデジタルポンドの「コア台帳」を含む中央インフラを提供
　・民間企業等は、ウォレット提供など、中央銀行と利用者の間の仲介の役割
　・ウォレットの提供により利用者保有の資産は、中銀コア台帳に匿名で記録
　　※信頼と信用を支えるため、デジタルポンドはプライバシーとデータ保護に関する厳格な基準の対象となる。
・気候変動の影響を管理し、緩和させるための幅広い戦略に合致するよう設計
・付利は行わず、日常の支払に対応するものとして設計
・詐欺や偽造から保護し、金融犯罪を助長しないように設計、また、現金とは異なり保有量の制限を検討

一方、テクノロジーワーキングペーパーにおいては、現時点で考え得るデジタルポンドの機能や特徴を整理している。ただし、決済のユースケースは時間の経過とともに変化することを踏まえ、将来のニーズを満たす機能を慎重に検討する必要があるとしている。そして、技術設計上の考慮事項としては、6 つの考慮点「プライバシー」、「セキュリティ」、「レジリエンス」、「パフォーマンス」、「拡張性」及び「エネルギー使用量」を優先してアーキテクチャとソリューションの検証を進め、設計としての評価を行う基礎を固めるとしている。最後に、デジタルポンドのコンセプトモデルとして、プラットフォームモデルをベースとした概念的なモデルを今後の研究の基礎となるものとして示し、それぞれの機能について解説している。



出典：イングランド銀行“The digital pound: Technology Working Paper”を基に作成
（https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf）

図 2.12　英国 CBDC の概念モデル

(2)　市中協議の結果

BOE と英国財務省は、市中協議の結果と結果を踏まえた方針を記載した報告書を 2024 年 1 月に公表した[23]。報告書においては、デジタルポンドの発行に関する最終的な決定をしていないとの前置きをしつつ、市中協議の結果、概ね考え方が支持されたとして、設計段階で実現可能性と設計の可能性を探る作業が継続されるものとされている。

コンサルテーションペーパーに対しては、個人や団体から 5 万件を超える回答（大半は個人）が得られ、その回答は記載された設計案をおおむね支持するものであったが、同時に、デジタルポンドが現金へのアクセス、利用者のプライバシー、資産の管理等へ影響する可能性を懸念したものであった。これらの回答を踏まえ、報告書内では、デジタルポンドの導入に当たっては、改めて市中協議を行った上で議会両院の一次立法を制定し、プライバシーや現金へのアクセスの維持を保証するとしている。

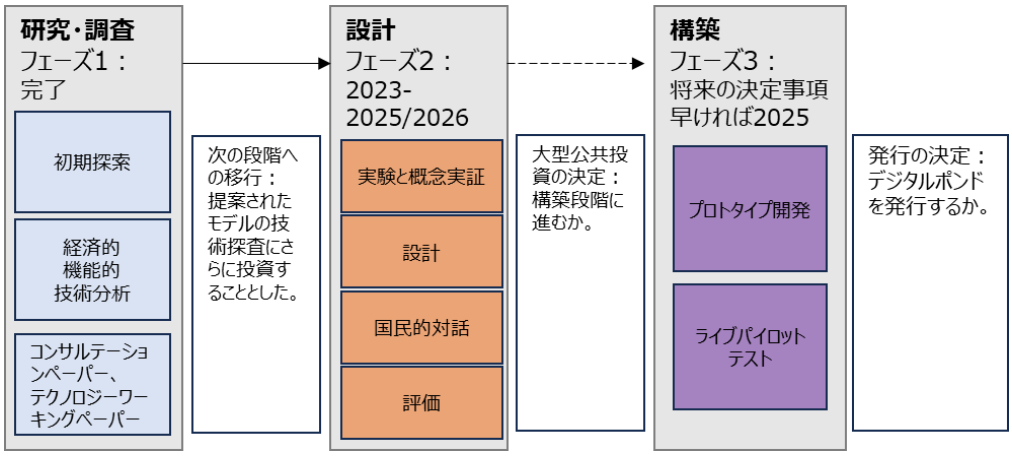
テクノロジーワーキングペーパーに対しても、個人や団体からの回答が得られ、6 つの技術設計上の考慮事項やプラットフォームモデルに基づくデジタルポンドの概念モデルについて広く支持されたと報告されている。回答の中には、その他考慮事項の提案（相互運用性、ユーザビリティ、アクセシビリティ、スケーラビリティ等）もあったとのことであり、それらを踏まえて、BOE と英国財務省は設計原則に合意し公表している。また、テクノロジーワーキングペーパー記載の活動に対しても支持されているこ

とを受け、設計段階として「設計」、「実験と概念実証」、「国民的対話」及び「評価」を相互に関係させながら取組を継続させるとしている。

表 2.3　デジタルポンドの設計原則

原則	概要
信頼性と安全性	デジタルポンドは常に利用可能であるべきで、利用者はいつでも支払ができると信頼できる。
ユーザのプライバシーと管理	中銀と政府は、中銀の基幹インフラを通じて個人データにアクセスすることはできない。 プライバシーを保護する支払オプションを有効にする。 中銀や政府によってプログラムされるものではない。
イノベーションを支援	革新的なサービスをサポートするため、公共インフラと機能を優れたパフォーマンスで提供 決済における競争を促進するため、参入障壁を低くする。
相互運用可能	利用者はデジタルポンドを他の貨幣と便利に交換可能 デジタルポンド利用者は、非利用者に便利に支払うことが可能、その逆も然り。
適応性と拡張性	優先順位の高い決済と非決済のユースケースをサポート 将来のトレンドを念頭に置いて構築 現在想定していないユースケースをサポートする適応性
包括的で魅力的	個人および企業にとって魅力的 広く受けれられるように設計 エコシステムにおいて、様々な民間のビジネスモデルを維持
エネルギー効率	ユーザの選択を損なうことなく政府のネットゼロ計画をサポート 少なくとも既存の決済インフラと同程度のエネルギー効率を持つ

出典：イングランド銀行“Response to the ditigal pound Technology Working Paper”を基に作成
（https://www.bankofengland.co.uk/paper/2024/response-to-the-digital-pound-technology-working-paper）



出典：イングランド銀行“Response to the ditigal pound Technology Working Paper”を基に作成
（https://www.bankofengland.co.uk/paper/2024/response-to-the-digital-pound-technology-working-paper）

図 2.13　デジタルポンドプロジェクトのロードマップ

2.2.4　中国

中国では、2019 年末から開始したデジタル人民元（e-CNY）のパイロット実験を、検証内容や実施地域を拡大しながら進めている。2023 年においては、公務員などの賃金のデジタル人民元による支給、国慶節の期間中にデジタル人民元アプリで利用可能な割引クーポン発行など、利用機会を増やすための施策とともに、試験運用が進められている旨の情報がある。

また、海外から中国への訪問者に向けたデジタル人民元による決済サービスを提供するために、2023 年 9 月には、デジタル人民元のアプリケーション

に海外で発行されたクレジットカードによる「プレチャージ」機能を追加している[24]。

その他クロスボーダー取引の検討に関する進捗として、国際決済銀行（BIS）イノベーションハブのクロスボーダー決済プロジェクト「mBridge」プロジェクトに中国人民銀行が 2021 年 2 月から参加している。同プロジェクトは 2024 年には実用化段階に入る予定としており、mBridge の実装によって、より高速、透明、安価かつ効率的なクロスボーダー決済が可能になるとされている[25]。なお、デジタル通貨研究所の穆長春所長は、2023 年 11 月に香港で開催されたシンポジウムにおいて、mBridge は使用するブロックチェーンと許可型のコンセンサスアルゴリズム（Dashing Consensus）などによりパフォーマンスと効率を向上させるとともに、プライバシー保護モデルを実装し、支払者と受取人の身元、取引金額、呼び出された CBDC コントラクトなどのコア取引データのプライバシー管理を実現するものであることを公表している[26]。

このように、中国人民銀行は、国内外で利用可能なデジタル人民元の検討を広く進めているが、発行に向けた取組の公式情報が少ない状況にある。そこで、取組進捗等を独自に分析するため、国立印刷局では、中国人民銀行の特許出願状況の分析を継続的に行っている。以降、参考付録として、その調査結果を示すこととする。

---

[1] 株式会社日立製作所、ニュースリリース「日本銀行が実施する中央銀行デジタル通貨に関するパイロット実験の業務委託先として契約を締結」、2023.11.20、
（https://www.hitachi.co.jp/New/cnews/month/2023/11/1120.html）

[2] デロイトトーマツコンサルティング、お知らせ「デロイト トーマツ、日本銀行が実施する中央銀行デジタル通貨に関するパイロット実験のプロジェクト管理支援・技術コンサルティング業務の委託先に選定」、2023.11.20、
（https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/news-releases/nr20231120.html）

[3] 財務省、「CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議の設置について」、2024.1.26、
（https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/kaisai.html）

[4] ECB,“Eurosystem proceeds to next phase of digital euro project”,2023.10.18,
（https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html）

[5] ECB,“Market research and prototyping exercise confirm feasibility of technical solutions and user interfaces for a digital euro”,2023.5.26,
（https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews230526.en.html）

[6] マーケットリサーチにより確認された構成要素は、決済（台帳など）、流動性管理用口座管理、オフラインソリューション、スタンドアローンアプリ、不正検知・防止など

[7] 言語についても EU 公用語に対応させ、欧州アクセシビリティ法に適合させるもの。

[8] ECB,“Second update on the work of the digital euro scheme’s Rulebook Development Group”,2024.1.3,
（https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews240103_2.en.html）

[9] European Commission,“Single Currency Package: new proposals to support the use of cash and to propose a framework for a digital euro”,2023.6.28,
（https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3501）

[10] FRB,“Money and Payments: The U.S. Dollar in the Age of Digital Transformation”,2022.1.10,
（https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm）

[11] WHITE HOUSE,“FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets”,2022.3.9,
(https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/)

[12] WHITE HOUSE,“FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets”,2022.9.16,
(https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/)

[13] U.S. Department of the Treasury,“The Future of Money and Payments”,2022.9,
(https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf)

[14] ボストン連邦準備銀行,“Boston Fed, MIT complete research project into feasibility of a central bank digital currency”,2022.12.22,
(https://www.bostonfed.org/news-and-events/news/2022/12/project-hamilton-boston-fed-mit-complete-central-bank-digital-currency-cbdc-project.aspx)

[15] MIT Media Lab,“Parallelized Architecture for Scalably Executing smart Contracts (PArSEC)”,2023.8,
(https://www.media.mit.edu/projects/parsec/overview/)

[16] MIT Technology Review、「MIT との共同研究も終了、「デジタル・ドル」構想は死んだのか？」、2023.7.26、
(https://www.technologyreview.jp/s/312985/is-the-digital-dollar-dead/)

[17] 米下院金融委員会,“Markup of H.R. 3378, H.R. 5409, H.R. 760, H.R. 5472, H.R. 5485, H.R. 5119, H.R. 5557, H.R. 5523, H.R. 5512, H.R. 5524, H.R. 3402, H.R. 5403, H.R. 3712 ”,2023.9.20,
(https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=408971)

[18] コインポスト、「CBDC による監視社会に反対する法案、米下院金融委員会で承認」、2023.9.21、
(https://coinpost.jp/?p=482974)

[19] FRB,“Opening Remarks”,2023.10.27,
(https://www.federalreserve.gov/newsevents/speech/barr20231027a.htm)

[20] BOE,“The digital pound: a new form of money for households and businesses? Consultation Paper”、2023.2.7、
(https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf)

[21] BOE,“The digital pound: Technology Working Paper”,2023.2.7,
(https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf)

[22] BOE,“HM Treasury and Bank of England consider plans for a digital pound”,2023.2.7,
(https://www.bankofengland.co.uk/news/2023/february/hm-treasury-and-boe-consider-plans-for-a-digital-pound)

[23] BOE,“Bank of England and HM Treasury respond to digital pound consultation”,2024.1.25,
(https://www.bankofengland.co.uk/news/2024/january/boe-hmt-respond-to-digital-pound-consultation)

[24] 人民網日本語版、「海外訪問者のデジタル人民元決済がより便利に プレチャージ機能がリリース」、2023.9.25、
(http://j.people.com.cn/n3/2023/0925/c94476-20076635.html)

[25] 野村総合研究所、「実用化段階に入る mBridge プロジェクト」、2024.1.7、
(https://www.nri.com/-/media/Corporate/jp/Files/PDF/knowledge/publication/kinyu_itf/2024/01/itf_202401_07.pdf)

[26] 东方财富网,“央行数研所穆长春：货币桥区块链是货币桥技术架构核心”,2023.11.2,
(https://finance.eastmoney.com/a/202311022892634719.html)

参考付録１　中国人民銀行の特許出願状況について

1　概要

中国においては、デジタル人民元の発行に向けた市民参加型の実証実験が2019 年末から継続的に行われている。デジタル人民元の設計に関しては、2021 年 7 月に公表されたデジタル人民元の調査研究の進展に関する白書[1]において、その大枠が記載されているが、その後は設計に関する情報が少ないのが現状である。実証実験の進捗の裏でも、着実に研究開発が進められており、その動向は特許出願に現れると考えられることから、特許出願状況を分析することで、デジタル人民元の設計と発行に向けた取組の状況を推察することとした。なお、同様の調査結果は令和 4 年度版レポートにおいても報告しており、出願に係る情報を更新して報告するものである。

2　調査内容

中国人民銀行を出願人又は権利保有者に含む出願特許を検索対象として、Google Patents における検索を行った。検索期間は、2012 年 1 月から 2023 年 8 月末日までとして、特許公開公報に記載の「技術領域」、「従来の技術」、「請求項 1」等から対象となる「技術分野」や「用途・課題」について分類しながら、その傾向を分析した。

【分類について】

(1)　技術分野

出願時期と出願傾向の変化を把握するために、大きくブロックチェーン、デジタル通貨、関連技術及びユースケースに分類した。さらに、デジタル通貨及び関連技術に関しては、付表 1.1 のとおり細分化した。

(2)　用途・課題

中国人民銀行が出願する特許の目的を推察するために、当該特許が使われる用途や解決したい課題について付表 1.1 のとおり分類した。用途・課題に関して、複数の内容を記載する特許出願も数多くみられるが、記載が詳細である及び／又は最初に記載されている内容に基づき分類している。

なお、項目に関しては、例えば、小分類のオフライン決済は大分類では利便性（容易）、社会性（金融包摂）ともみなせるが、多様性に区分したように一つの大分類に代表させている。

付表 1.1　技術分野、用途・課題の分類

（1）　技術分野

大分類	中分類	小分類
CBDC関連のブロックチェーン		
デジタル通貨	通貨の発行・管理	
	媒体・ウォレット	
	取引端末	
	チャージ	
	決済処理・手続	
	決済アプリ	
関連技術	データ処理	通信手段・方法
		情報の記録・管理
		情報の分散管理
		ビッグデータ解析
	情報セキュリティ	暗号技術
		認証
		鍵の管理
		不正検出・異常検知
	関連システム	インターネットバンキング
		その他の銀行システム
デジタル通貨のユースケース		
その他（関連外）		

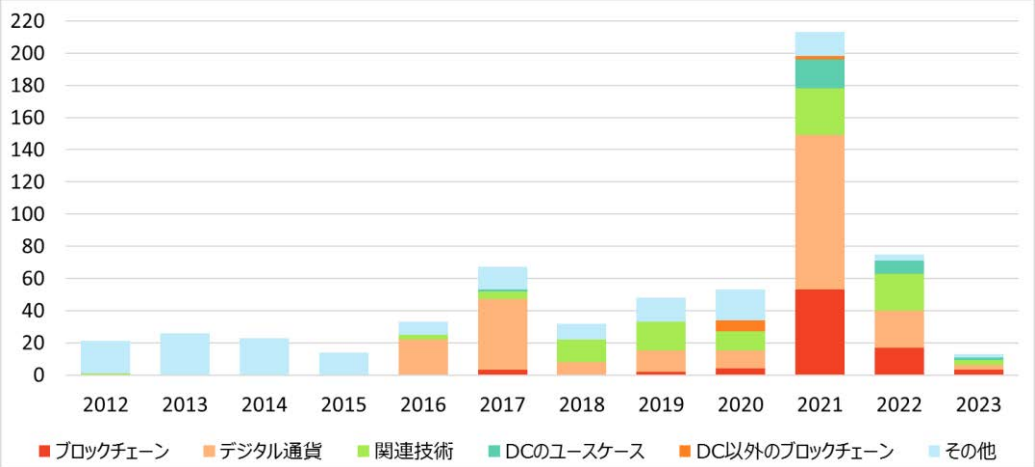
（2）　用途・課題

大分類	小分類
デジタル通貨の基本要件	
金融（通貨発行等）	
安全性の確保	不正・改ざんの防止
	情報漏洩の防止
	データ等の保守（維持）
利便性の向上	容易
	高速・効率
多様な決済手段の提供	取引相手・ソフト
	ハード
	オフライン決済
社会的な課題の解決	金融包摂
	相互運用
	省電力・電力確保
	事業継続
デジタル通貨のユースケース	

3　調査結果

調査の結果、618 件の特許が抽出された。その内訳としては、2015 年以前は、銀行券の偽造防止技術等を中心に出願されていたが、2014 年のデジタル通貨の研究開始を起点に、2016 年からデジタル通貨や関連技術に関する特許を中心に出願数が増加しており、特に 2021 年の出願数の増加が顕著である。

次に、分野別及び年代別の出願傾向から、中国人民銀行における CBDC に関する取組と現状を推察する。



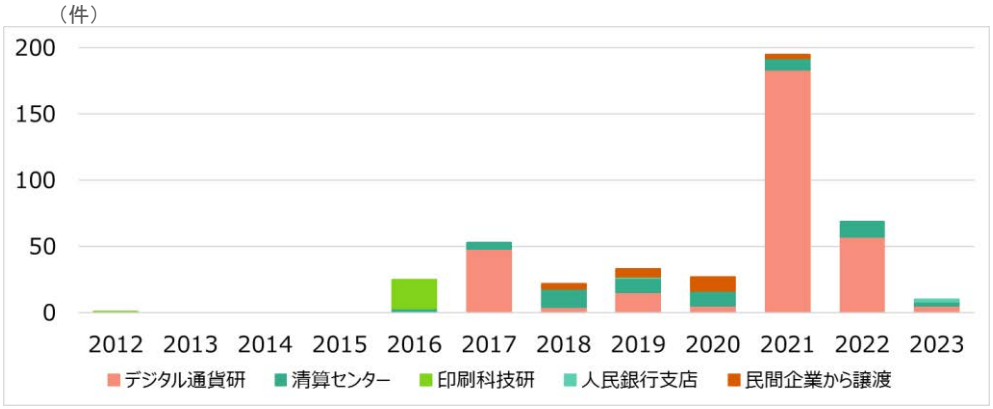
付図 1.1　中国人民銀行の特許出願（全技術分野）

3.1　出願機関

中国人民銀行において、デジタル通貨に係る特許出願を行っている機関は、主として 3 機関である。2014 年に中央銀行が発行するデジタル通貨を研究する組織を立ち上げ、2017 年にデジタル通貨研究所を設置し、2017 年以降、同機関を中心に CBDC に関連する特許出願件数を伸ばしている。また、清算センターにおいても、関連業務を想定して CBDC に係る研究組織を立ち上げ、研究及び特許出願を行っているものとみられ、複数の組織から特許が出願されている状況にある。その他、清華大学、建設銀行等との共同出願を行っているほか、アリペイ、ファーウェイ、工商銀行等から権利が譲渡されている特許出願も見られた。

付表 1.2　デジタル通貨関連特許を出願する主な機関

デジタル通貨研究所 （数字货币研究所）	2016 年に設立。設立の目的は、法定デジタル通貨の第一世代プロトタイプシステムの構築を完了させること。デジタル人民元の研究開発を主導。
清算センター （清算总中心）	1990 年に設立。決済システムの運営及び保守管理を担う。2018 年には、センター内にポスドク[2]研究ワークステーションを設立。また、2022 年には、ブロックチェーン、ビッグデータ解析等 9 つの研究の方向性を設定し、ポスドクを募集。
印刷科学技術研究所 （印制科学技术研究所）	1959 年に設立。インキ、製版、紙幣用紙、偽造防止技術及び紙幣印刷機械の設計に係る研究施設並びに製版及び紙幣印刷の実験用作業場を保有。

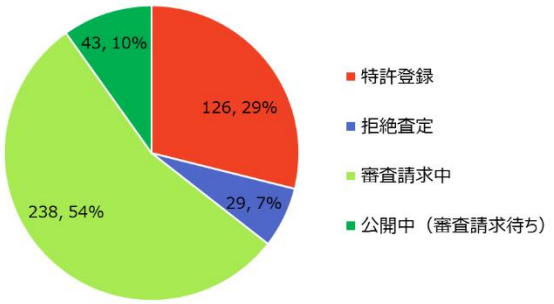


付図 2　機関別出願動向（CBDC 関連に限る）

3.2　審査の状況

中国人民銀行は、出願した CBDC 関連特許の大部分を審査請求しており、特許として登録された件数割合は、2023 年 8 月末時点で約 3 割である。また、審査が終了した特許 155 件に占める特許登録件数 126 件は、81.3%の特

許査定率となり、2021 年の中国における特許査定率（55.0%[3]）から鑑みるに、極めて高い数値となっている。



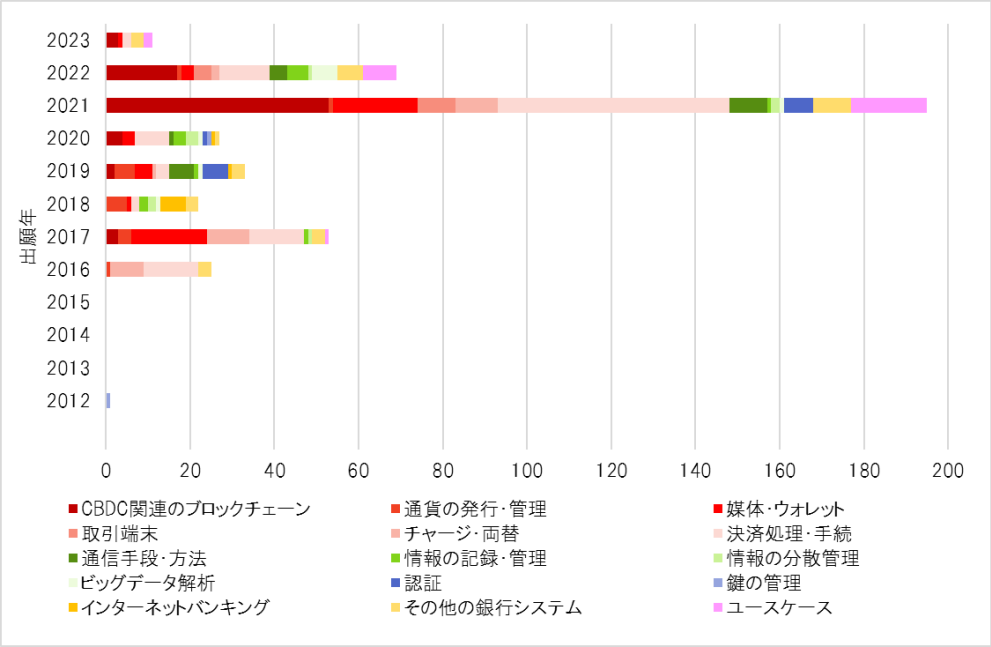
付図 1.3　特許査定の状況（CBDC 関連に限る）

3.3　出願傾向

本調査に当たっては、技術分野と用途･課題を分類し、それぞれの特許出願件数を整理した。その傾向の変化は、付図 1.4 及び付図 1.5 のとおりである。

(1)　技術分野

技術分野については、出願件数が顕著に増加した 2021 年以降パイロット実験の進捗に合わせて変化しているように思われる。具体的には、ユースケースに係る出願比率の増加を始めとして、エンドポイントに近い媒体・ウォレットに関するもの、エンドポイントとの連携を含めた決済処理・手続の比率の増加に表れている。



付図 1.4　技術分野別出願件数の推移

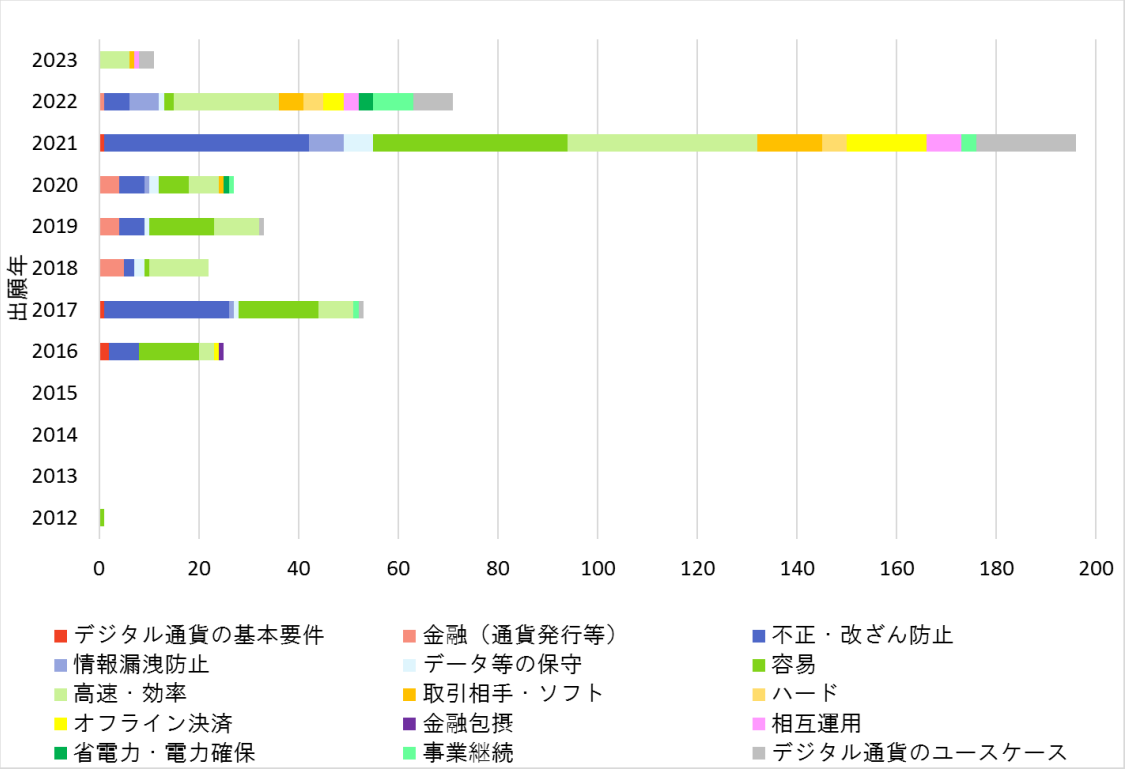
(2) 用途・課題

用途・課題について、2021 年の出願件数の大幅な増加の中では、実証実験にて課題（「不正・改ざん防止」、「高速・効率」及び「オフライン決済」）の解決を望むような特許出願の伸び率が大きくなっている。

2022 年の出願傾向からは、社会実装を意識した課題解決を目的とした出願の比率の増加がみられる。「高速・効率」の比率については、2021 年から引き続き高く、取引に使用する装置やシステム連携、更にはスマートコントラクトの実装、ブロックチェーンのアドレス抽出など幅広い領域で処理性能向上に向けた技術開発が進められていることがわかる。

その他、2022 年からは、考慮すべき事項として「省電力・電力確保」を目的とした技術開発、出願が行われていることもわかる。

技術分野における分析結果と同様、パイロット実験の進捗に応じるように解決したい課題も変化しながら幅広く検討されており、それぞれの分野の出願件数や全体に占める比率及び出願内容からの分類の傾向により、網羅的な取組が進められている。



付図 1.5　用途・課題別出願件数の推移

3.4　国際出願

国際出願は、他の国・地域において権利を主張するために出願する外国出願の前段階として、出願している事実を国際的に公表するものであり、自国

への出願後、1 年以内に行うことが原則とされている。2022 年 8 月末時点で中国人民銀行から出願された特許のうち、国際出願が行われているのは 6 件であったが、その後の一年で国際出願の件数が大幅に増加している。これは、2021 年以降、中国人民銀行の特許出願件数が大幅に増加しており、それに比例するように国際出願件数が増加したものと考えられる。国際出願が行われた特許は、30 か月以内に、国・地域を指定した外国出願が行われるため、今後の動向にも注視する必要がある。

付表 1.3　国際出願の状況

No.	国際公開番号	発明の名称	出願人	出願日（外国出願先）
1	WO2013091246A1	インクの転写と供給の方法と装置、およびその装置を有する印刷装置	印刷科技研（共同）	日、英、独、墺、瑞
2	WO2013166672A1	コンビネーション印刷機	印刷科技研（共同）	日、英、独、墺、瑞
3	WO2020119608A1	Spark shuffle ベースのリモート ダイレクト メモリ アクセス システムおよび方法	清算センター	2022/3/16（取下げ）
4	WO2022028484A1	ファイル共有方法、装置及びシステム	デジタル通貨研	2022/2/10
5	WO2022028486A1	ファイル共有方法、装置及びシステム	デジタル通貨研	2022/2/10
6	WO2022052901A1	データ保存及びアカウントチェック方法及びシステム	清算センター	2022/3/17
7	WO2022171186A1	ブロックチェーンアドレス分類方法及び装置	デジタル通貨研	2022/8/18
8	WO2022171187A1	ブロックチェーンにおけるインテリジェントコントラクトの登録及び実行方法及び装置	デジタル通貨研	2022/8/18
9	WO2022171188A1	ブロックチェーンにおけるタイミングインテリジェントコントラクトの登録及び実行方法、装置及びシステム	デジタル通貨研	2022/8/18
10	WO2022171189A1	ブロックチェーンにおけるタイミングインテリジェントコントラクトの登録及び実行方法及び装置	デジタル通貨研	2022/8/18
11	WO2022171190A1	実行順序が固定された取引方法及び装置	デジタル通貨研	2022/8/18
12	WO2022184137A1	ブロックチェーンで乱数を生成する方法とデバイス	デジタル通貨研	2022/9/9
13	WO2022206446A1	取引証明書を生成、検証、保存するための方法、装置、機器およびシステム	デジタル通貨研	2022/10/6
14	WO2022218400A1	デジタル通貨の管理方法およびシステム	デジタル通貨研	2022/10/20
15	WO2022218410A1	デジタル通貨のエクスポート方法、チャージ方法、デバイスおよびシステム	デジタル通貨研	2022/10/20
16	WO2022218417A1	取引におけるデジタル通貨の分割、検証、および管理のための方法、端末、およびシステム	デジタル通貨研	2022/10/20
17	WO2022218424A1	デジタル通貨の支払い方法、デバイス、およびシステム	デジタル通貨研	2022/10/20
18	WO2022218432A1	デジタル通貨の支払い方法、デバイス、システム セキュリティ チップおよびアプリケーション方法	デジタル通貨研	2022/10/20
19	WO2022228423A1	デジタル証明書管理方法及び装置	デジタル通貨研	2022/11/3
20	WO2022228392A1	ブロックチェーンアドレス分類方法及び装置	デジタル通貨研	2022/11/3
21	WO2022247910A1	情報検証方法及び装置	デジタル通貨研	2022/12/1
22	WO2022262527A1	デジタル通貨に基づく支払い方法、プラットフォーム、端末、および支払いシステム	デジタル通貨研	2022/12/22
23	WO2023273832A1	データ検証方法及び装置	デジタル通貨研	2023/1/5
24	WO2023020193A1	スマートコントラクトの実行方法および装置	デジタル通貨研	2023/2/23
25	WO2023050983A1	デジタルウォレット開設方法、ウォレットアプリ端末及びシステム	デジタル通貨研	2023/4/6
26	WO2023051736A1	デジタル通貨ベースの取引方法および装置	デジタル通貨研	2023/4/6
27	WO2023051737A1	車両のインターネットに基づく測位および支払い方法、装置およびシステム	デジタル通貨研	2023/4/6
28	WO2023061285A1	デジタル通貨サブウォレットベースの決済トークン化方法、装置およびシステム	デジタル通貨研	2023/4/20
29	WO2023066040A1	デジタル通貨の支払い方法および装置	デジタル通貨研	2023/4/27
30	WO2023066197A1	異常なデジタル通貨取引を検証する方法および装置	デジタル通貨研	2023/4/27
31	WO2023066215A1	デジタル通貨ウォレットの管理方法及び遠隔制御方法、装置及びシステム	デジタル通貨研	2023/4/27
32	WO2023071797A1	デジタル通貨ウォレットおよび端末・システムの更新方法	デジタル通貨研	2023/5/4
33	WO2023072115A1	デジタル通貨取引方法およびシステム、関連取引端末	デジタル通貨研	2023/5/4
34	WO2023071800A1	スマートコントラクトに基づくモノのインターネット支払いのための方法および装置	デジタル通貨研	2023/5/4
35	WO2023088467A1	デジタル通貨の支払い方法および装置	デジタル通貨研	2023/5/25
36	WO2023103760A1	通信監視方法、装置およびシステム	デジタル通貨研	2023/6/15
37	WO2023109841A1	ブロックチェーンベースの照合方法、装置およびシステム	デジタル通貨研	2023/6/22
38	WO2023124695A1	デジタル通貨取引方法、装置、電子機器、およびコンピュータ可読媒体	デジタル通貨研	2023/7/6
39	WO2023143566A1	デジタル通貨取引方法およびシステムおよびデジタル通貨カード申請装置	デジタル通貨研（共同）	2023/8/3
40	WO2023143613A1	デジタル通貨の支払い方法とデバイス	デジタル通貨研	2023/8/3
41	WO2023160667A1	デジタル通貨取引のためのセキュリティ認証方法、装置およびシステム	デジタル通貨研	2023/08/31

4　まとめ

中国人民銀行のデジタル人民元発行に向けた取組は、2014 年の研究組織立ち上げから現在の実証実験に至るまで、計画的に進められており、その成果は特許出願という形でも着実に進められていることがわかる。そして、近年では中国国内で進められているパイロット実験を進める中で判明した課題解決に向けた特許出願、さらには、社会実装に向けた特許出願へとその傾向も変移していることも明らかである。

2021 年 7 月に公表された中国人民銀行の白書[1]によると、e-CNY システムの開発は、デジタル経済の時代に国民の需要を満たす新しい人民元の形を作ることを目的としている。また、信頼性、効率性、適応性及び開放性に優れたリテール決済インフラに支えられた e-CNY システムは、デジタル経済、金融包摂を強化し、決済システムを効率化するものとされており[4]、中国人民銀行内のそれぞれの組織が将来の決済像を想定しながら、研究開発を進めていることが伺える。

令和 4 年度版レポートに引き続き行った、中国人民銀行の特許出願状況の調査により、検討状況の進捗や国際出願の状況などを把握することができたが、国際出願されている特許については、今後の各国における設計にも関わるものになると考えられる。

今後、発行が計画されているデジタル人民元について、国際出願傾向と外国出願の状況を含めて中国人民銀行の出願特許を継続的に分析することで、中国人民銀行の方向性を確かめる上で役立つと考えられる。

---

[1] 中国人民銀行,“Progress of Research & Development of E-CNY in China”,2021.7.16,
(http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/index.html)

[2] 博士号を取得したのち、大学や研究機関において任期付きで研究活動をする非正規雇用スタッフ。正式な名称はポストドクター「博士研究員」。

[3] 特許庁、「特許行政年次報告書 2023 年版　1-1-26 図 【主要特許庁の特許査定率の推移】」、2024.1.22、p.12、
(https://www.jpo.go.jp/resources/report/nenji/2023/document/index/all.pdf)

[4] 中国人民銀行,“Progress of Research & Development of E-CNY in China　§ 2.2 Objectives and visions”,
2021.7.16, p.4,
(http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/index.html)

3　暗号資産、電子マネー等の事件・攻撃等

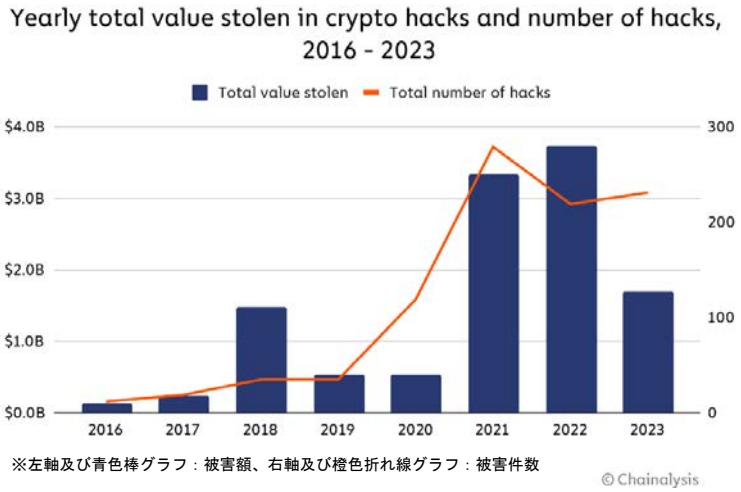
3.1　概要

暗号資産、電子マネー等についての事件・攻撃を理解することは、CBDC が将来普及する際のリスクを想定することにつながるため、近年の傾向について整理を行った。

3.2　暗号資産取引に関連するサイバー攻撃

3.2.1　2023 年における被害額について

2023 年の暗号資産取引に関するサイバー攻撃被害の世界的な動向をみると、被害額が過去最大となった 2022 年（約 37 億ドル）と比較し減少している（約 17 億ドル）。ただし、攻撃の件数は前年の 219 件から 12 件増加しており、継続的に暗号資産を標的とした攻撃が行われていることが分かる（図 3.1）[1]。



出典：Chainalysis,“Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises”,2024.1.24,(https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/)

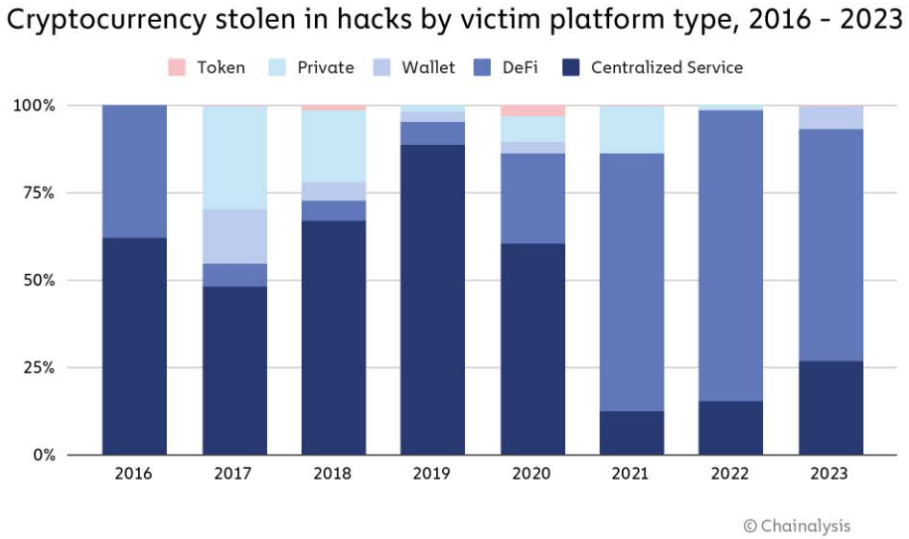
図 3.1　暗号資産取引に関するサイバー攻撃件数とその被害額（2016-2023 年）

3.2.2　サイバー攻撃の被害対象について

2023 年における暗号資産取引に関するサイバー攻撃の被害対象について、Chainalysis 社は、前年と比較して分散型金融（DeFi）に対する攻撃被害額が減少していると報告している。

ただし、サイバー攻撃の減少がセキュリティ対策によるものか、あるいはDeFi 取引の活動全体が減少したことに起因するかは明言できないとされており[1]、今後取引の活動が活発化した際における攻撃被害の変化が、今回の被害減少の要因整理につながると考えられる。

なお、同報告においては、利用者から暗号資産や秘密鍵等の情報を預かる形で暗号資産取引を行う中央集権型金融（CeFi）サービスに対する攻撃も発生しているとされており、DeFi と CeFi の両者に対する攻撃が継続的に行われていることを示していると言える（図 3.2）。



出典：Chainalysis,“Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises”,2024.1.24,(https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/)

図 3.2　暗号資産取引におけるサイバー攻撃の被害対象の推移（2016-2023 年）

3.2.3　DeFi に対するサイバー攻撃の手法について

3.2.1 で述べたとおり、2023 年の DeFi に対するサイバー攻撃被害額は減少していると Chainalysis 社は報告しているが、その手法は洗練・多様化しており、攻撃の発生や被害低減の可能性について理解するためには、その手法を分類することが重要であるとしている。

同報告では、Chainalysis 社が Halborn 社と協力し、DeFi に対する攻撃のベクトルを合計 11 種類（その他除く）に分類して分析しており、2023 年の攻撃に関する分析の結果として、①価格操作、②スマートコントラクトの悪用、③秘密鍵のぜい弱性の 3 種類の攻撃ベクトル（詳細は表 3.1 のとおり）が被害額全体の 9 割以上を占めたことを示している（図 3.3、①33.0%、②28.3%、③33.0%、合計 94.3%）。

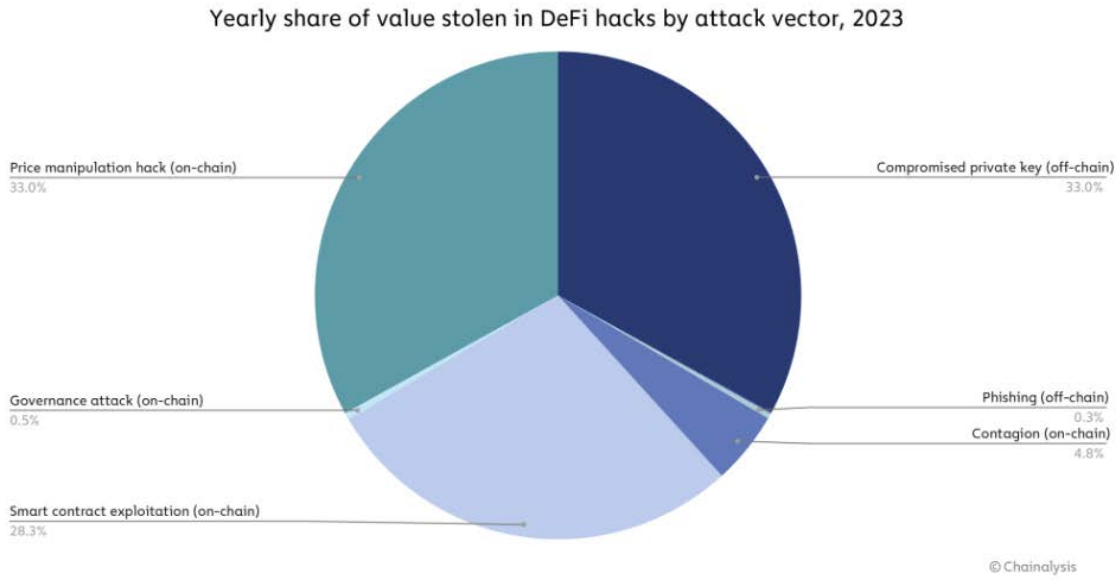
このように、2023 年においては攻撃者が特定の攻撃ベクトルを対象としてサイバー攻撃を行っている傾向がみられた。今後、環境の変化等によって対

象とする攻撃のベクトルが変わる可能性を踏まえ、攻撃手法を継続的に把握することが、サイバー攻撃のトレンドを理解する上で参考になると考えられる。

表 3.1　DeFi に対する攻撃ベクトル（代表的なもの）

攻撃のベクトル	定義
価格操作 (Price manipulation hack)	攻撃者がスマートコントラクトのぜい弱性（例：スマートコントラクトのコードの小数の処理方法に関するバグ）を悪用したり、正確な資産価格を反映しない欠陥のあるデータベース（例：データベース側の過失やデータベースの元データへの侵害）を利用したりすることで、デジタルトークンの価格操作が容易になること。
スマートコントラクトの悪用 (Smart contract exploitation)	攻撃者がスマートコントラクトのコードのぜい弱性 （例：攻撃者が損害を与えるためにバグのある関数）を悪用し、 システムの様々な制御メカニズムやトークン転送への直接アクセスが可能となること。
秘密鍵のぜい弱性 (Compromised private key)	フィッシング攻撃を使ったり、ウォレットが保存されているシステムに侵入したりすることで、攻撃者がユーザの秘密鍵にアクセスできるようになること。

Chainalysis,“Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises”,2024.1.24,(https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/)及び Halborn,“BREAKING DOWN THE TOP 50 DEFI HACKS 2016-2022 COMPREHENSIVE REPORT”,（https://www.halborn.com/reports/top-50-defi-hacks?utm_id=top50defihacksreport）を基に作成



出典：Chainalysis,“Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises”,2024.1.24,(https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/)

図 3.3　DeFi へのハッキングにおける被害額のベクトル別比較結果（2023 年）

3.3　電子マネー等の事件、攻撃事例

3.3.1　特殊詐欺の電子マネー詐取被害の傾向と犯行事例

EC サイトのギフトカード等に代表される、いわゆる「サーバ型電子マネー」は、利便性の高さから広く普及しているが、詐欺行為の支払手段としての悪用事例等の発生が続いているため、規制当局等により注意喚起がなされている[2,3]。

警察庁によると、国際電話番号を利用した特殊詐欺においても電子マネーの利用権をだまし取る事例が報告されている[4]。また、報道によると、2023 年 1 月から 11 月末までに警察庁に報告された電子マネーを用いた特殊詐欺被害の認知件数及び被害額は、統計を取りはじめた 2016 年以降最多とされている[5]。同報道では、2 月以降、特定の電子マネー被害が増加し、9 月以降の認知件数及び被害額における同電子マネーの占める割合が全体の 9 割以上であったと報じられている。

3.3.2　金融機関等へのアクセス情報窃取によるフィッシング詐欺被害の事例

暗号資産取引に関連する攻撃や電子マネー自体の詐取のほかに、金融機関等へのアクセス情報（ID、パスワード等）を窃取する手法であるフィッシング詐欺の被害が継続的に発生している。特に、インターネットバンキング利用者の ID やパスワードを窃取することにより、預金を不正に送金する事案が多発し、金融庁は 2023 年 11 月末時点の被害件数は 5,000 件超、被害額は約 80 億円と、いずれも過去最多を更新していると注意喚起をしている[6]。

なお、2022 年におけるフィッシング詐欺の標的（なりすましの対象）は、クレジットカード会社や EC サイトが 7 割以上を占めていたが、これらに加えてキャッシュレス決済サービスを騙るものも発生したと報告されている[7]。

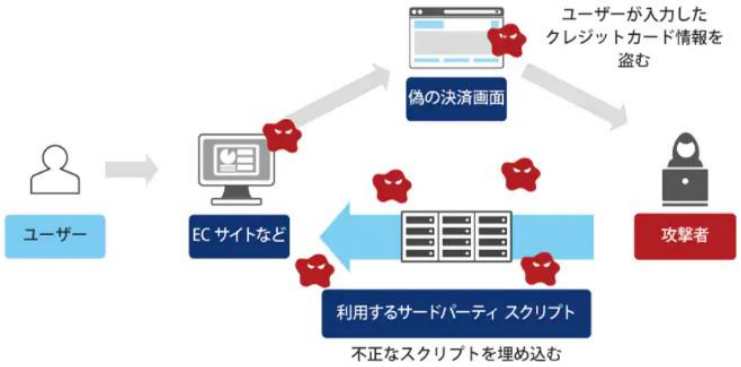
さらに、同報告では、フィッシング詐欺につながるリスクとして、法人の合併やサービスの終了等に伴い廃止したドメインの再登録・利用に関するものがあるとされている。2023 年 9 月には、2021 年に終了した電子決済サービスの公式サイト「ドコモ口座」の旧ドメイン「docomokouza.jp」がオークションサイトで競売に出品されたが、第三者の悪用を防ぐため、原取得者である㈱NTT ドコモが 400 万円以上の金額で落札している[8]。

3.3.3　ウェブスキミングによるクレジットカード情報窃取（全国初の摘発の事例）

2022 年 10 月から 11 月にかけて音楽グループのオンラインショップ公式サイトに不正なプログラムを組み込み、サイトにアクセスした利用者のクレジットカードの情報を入手したとして、犯人が逮捕された。正規のサイトに不正なプログラムを組み込み、利用者が入力した情報を盗み取る「ウェブスキ

ミング」（図 3.4）での摘発事例は全国初であった[9]。

ウェブスキミングは偽サイトを用いる「フィッシング詐欺」とは異なり、公式サイトが悪用されることから、攻撃が巧妙化している事例として注視すべきであると考えられる。

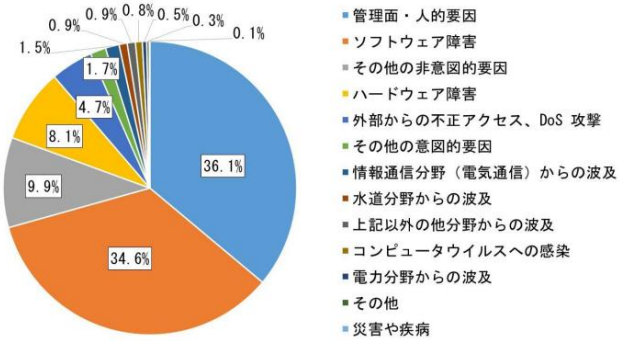


出典：NTT コミュニケーションズ株式会社、「意外と知らない？IT トレンド用語　-Web スキミングとは」、（https://www.ntt.com/bizon/glossary/e-w/web-skimming.html）

図 3.4　ウェブスキミングの一般的なモデル

3.4　国内の金融機関等におけるシステム障害事象

金融庁の報告によると、2022 年度に金融機関等から報告のあったシステム障害事象（約 1,900 件）のうち、「外部からの不正アクセス、DoS 攻撃」の割合は 4.7%であった[10]。当該報告において、「外部からの不正アクセス、DoS 攻撃」の具体的な事例として、金融機関等のランサムウェアへの感染被害の発生を報告しており、信用金庫・信用組合等において、サポート期限の切れた古いサーバが感染経路となったことを示している[11]。なお、警察庁は、感染の主な要因となる「VPN 機器のぜい弱性」について情報発信を行い、被害防止を図っている[12]。



出典：金融庁、「金融機関のシステム障害に関する分析レポート　図表 1「障害事象別割合（全業態）」」、2023.6.30、p.9、（https://www.fsa.go.jp/news/r4/sonota/20230630-2/01.pdf）

図 3.5　金融機関等のシステム障害における事象別割合

一方で、システム障害事象の大半（約 7 割）は「管理面・人的要因」と「ソフトウェア障害」が占めていた。なお、これらの具体的な事例は外部からの攻撃ではないが、デジタル資産のリスクの想定に資するものであることから、別途参考付録 2「全国銀行データ通信システムの障害事例」としてまとめることとした。

3.5　総括

暗号資産取引に関連する攻撃や電子マネー等に関する事件及び攻撃の動向を整理した結果、暗号資産取引に関するサイバー攻撃の概況からは、被害額が最大となった 2022 年と比較して被害額が減少しており、主に価格操作、スマートコントラクトの悪用、秘密鍵のぜい弱性といった特定のサイバー攻撃のベクトルが狙われていることが明らかになった。

また、電子マネー等の事件及び攻撃事例からは、前年まで主に行われていた資産自体の窃取や詐欺行為に加えて、利用者からの情報窃取によるフィッシング詐欺が増加していることが分かった。

このように、デジタル資産を標的とした攻撃手法は年々巧妙化している状況にある。今後 CBDC にどのような新たな技術を用いるかは定かではないが、攻撃や事件の事例を的確に理解し、対策を講じておくことが将来のリスク低減につながると考えられる。

その他デジタル資産に係るリスクの検討として、金融機関システムにおける障害事例に関する情報整理を行った結果、外部からの攻撃よりも内部管理やソフトウェアに起因して障害が発生していることが分かった。

[1] Chainalysis,“Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises”,2024.1.24,
(https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/)
[2] 財務省　関東財務局、「電子マネーを悪用した詐欺にご注意ください！」、
(https://lfb.mof.go.jp/kantou/rizai/pagekthp030000039.html)
[3] 一般社団法人日本資金決済業協会、「ネット上で使えるプリカ（電子マネー）を悪用した詐欺にご注意」、
(https://www.s-kessai.jp/consumer/giftcard_prica_netprica/sagi1.html)
[4] 警察庁、「特殊詐欺の電子マネー型交付形態における認知件数及び国際電話番号による既遂件数の推移について」、2023.12.25、p.1、
(https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/denshimane-ninchi-kokusaibangou.pdf)
[5] 産経新聞、「被害の9割が「アップルギフトカード」 電子マネーだまし取る特殊詐欺が過去最多」、2023.12.25、
(https://www.sankei.com/article/20231224-NUXSOVWVHRMTHL4KGFZAIBXYHA/)
[6] 金融庁、「フィッシングによるものとみられるインターネットバンキングによる預金の不正送金被害が急増しています。」、2024.1.24、
(https://www.fsa.go.jp/ordinary/internet-bank_2.html)
[7] フィッシング対策協議会、「フィッシングレポート 2023」、2023.6.1、p.6、
(https://www.antiphishing.jp/report/wg/phishing_report2023.html)
[8] 読売新聞オンライン、「ドコモが「ドコモ口座」ドメインを誤って手放す、ネット競売に…400万円で自ら落札」、2023.9.29、
(https://www.yomiuri.co.jp/economy/20230929-OYT1T50220/)
[9] 読売新聞オンライン、「「ウェブスキミング」初摘発、クレカ情報入手容疑で自称「恒心教」の男逮捕…公式サイトに不正プログラム」、2023.11.15、
(https://www.yomiuri.co.jp/national/20231115-OYT1T50086/)
[10] 金融庁、「金融機関のシステム障害に関する分析レポート」、2023.6.30、p.9、
(https://www.fsa.go.jp/news/r4/sonota/20230630-2/01.pdf)
[11] 金融庁、「金融機関のシステム障害に関する分析レポート」、2023.6.30、pp.13-14、
(https://www.fsa.go.jp/news/r4/sonota/20230630-2/01.pdf)
[12] 警察庁、「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」、2023.9.21、p.23、
(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf)

参考付録２　全国銀行データ通信システムの障害事例について

1　概要

金融庁が公表した金融機関のシステム障害に関する報告によると、「管理面・人的要因」による障害として、システム開発部門とシステム運用部門の連携が十分に機能せず、誤った認識の下で作業を行った事案等が挙げられている。また、「ソフトウェア障害」による障害として、システム設計時の考慮不足に起因して、誤った仕様の下でプログラムを作成し、ソフトウェア障害が発生した事案等が挙げられている[1]。

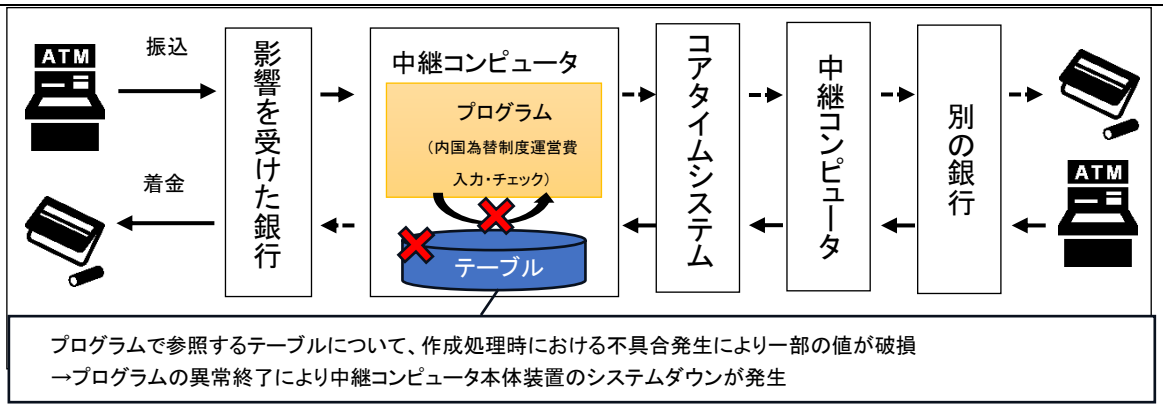
このような「管理面・人的要因」及び「ソフトウェア障害」を要因とした事象は 2023 年にも発生している。例えば、金融機関間での相互の為替取引をオンライン処理するシステムである「全国銀行データ通信システム（全銀システム)」で不具合が発生し、一部金融機関の他行宛振込みができなくなった結果、2 日間の取引停止が発生した事例が報告されている[2]。

当該事例については、その内容と対応に関する詳細な報告がなされており、障害発生から対策の立案までの流れについての理解に資するものと考え、概略を記すものである。

2　障害事例

2023 年 10 月、全国銀行資金決済ネットワークが運営する全銀システムの更新を 14 の加盟金融機関を対象に行ったところ、一部の金融機関（10 行）と全銀システムのホストコンピュータを繋ぐ「中継コンピュータ」の本体装置がシステムダウンし、10 月 10 日から 11 日にかけて他行宛振込みができなくなる事例が発生した[2]。

中継コンピュータ内のプログラムを実行する過程で不具合が発生し、参照ファイルが破損、異常終了したことがシステムダウンの原因となった。



一般社団法人全国銀行資金決済ネットワーク・株式会社 NTT データ、「全国銀行データ通信システムの障害について」、2023.12.1、（https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf）及び一般社団法人全国銀行資金決済ネットワーク、「システム障害に係る対応状況について」、2023.10.18、（https://www.zengin-net.jp/announcement/pdf/announcement_20231018_2_besshi.pdf）を基に作成

付図 2.1　2023 年 10 月全銀システム更新時における障害発生（イメージ）

10 月 7 日から 9 日の間でシステム更新を実施したが、更新後初日の営業日である 10 月 10 日の通信開始後にシステムダウンが発生した。同日中にシステムダウンの原因が判明したため、中継コンピュータに対するプログラムの修正を実施し、システム復旧に向けて対応を図ったが、翌営業日（10 月 11 日）の中継コンピュータ起動時刻までの対応が困難であったことから、顧客への影響を抑えるために対応を中断し、エラーを解消する暫定対処を行う対応に切り替えた。結果として、10 月 11 日の通信終了時点において、送信側の取引のうち、当日中に処理が完了しないものが発生した[3]。

3　システムベンダー及び運営者の課題抽出と再発防止に向けた対策について

今回の事例を受け、システムベンダーである㈱NTT データと運営者である全国銀行資金決済ネットワークは、双方で課題を抽出した上で、再発防止策を講じ対応を図る旨を報告した[4]。

システムベンダーと運営者が抽出した課題及び対策の例は以下のとおり。

【システムベンダーの課題とその対策】

・プログラム修正方針を製造関係者のみで判断し、その誤りを抽出できるプロセスになっていなかったこと

→詳細設計関係者を含めて判断するようプロセスを変更。

・プログラムの品質を最終確認する試験工程において、本番に近い（より実働に則した）環境の事例を含む試験方法が確保できていなかったこと

→より本番に近い試験方法である、実取引相当のデータを用いた疎通試験を実施。

・復旧に向けた優先順位等の考え方について、あらかじめベンダーと運営者の間で合意していなかったこと
→復旧させる業務の優先順位やバックアッププランへの切替時限についてベンダー/運営者間で合意し、障害発生時の復旧ガイドラインを策定。

【運営者の課題とその対策】

・ベンダーにおける設計のレビュー体制や試験項目の確認等、運営者側の牽制が不十分であったこと
→ベンダーにおける設計のレビュー体制及び試験内容の十分性を確認し、各工程におけるベンダーマネジメントを向上。

・所要時間、加盟金融機関ごとの練度等の把握・検証がなされず、実効的な BCP が未確立であったこと
→代行発信・受信代行運用訓練のシナリオの見直し、欠送・二重発信確認対応訓練を新規実施し、実践的な訓練を通じた実効的な BCP を確立。

・障害発生時における役割分担や障害発生時の対外告知のマニュアルに関する不備等といった、危機管理体制がぜい弱であったこと
→障害対応時の体制見直し、対外公表内容の事前整理・マニュアル化等を実施。

・運営者の蓄積している経験値、金融機関の知見等の活用が不十分であり、システム運用に関する人材・組織面にぜい弱性を抱えていること
→CIO の設置、IT・システム関連委員会の新規検討等により、所管を明確化。

4　まとめ

2023 年に発生した全銀システムにおける障害事例においては、システムベンダーと運営者の双方で再発防止策を講じ、対応が図られたことが分かった。金融機関のシステム改修・更新に当たっては、障害の発生による利用者への影響が大きくなるため、関連する多様なシステムに対応するよう、細心の注意を払って実施することが必要であると考えられる。

---

[1] 金融庁、「金融機関のシステム障害に関する分析レポート」、2023.6.30、p.9、
(https://www.fsa.go.jp/news/r4/sonota/20230630-2/01.pdf)

[2] 一般社団法人全国銀行資金決済ネットワーク・株式会社 NTT データ、
「全国銀行データ通信システムの障害について」、2023.12.1、
(https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf)

[3] 一般社団法人全国銀行資金決済ネットワーク、「システム障害に係る対応状況について」、2023.10.18、p.6、
(https://www.zengin-net.jp/announcement/pdf/announcement_20231018_2_besshi.pdf)

[4] 一般社団法人全国銀行資金決済ネットワーク・株式会社 NTT データ、
「全国銀行データ通信システムの障害について」、2023.12.1、
(https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf)

4　デジタルアイデンティティ管理技術

4.1　背景

CBDC とは、「民間銀行等が中央銀行に保有する当座預金とは異なる、新たな形態の電子的な中央銀行マネー」であると考えられており[1]、日本銀行においても、デジタル化されていること、円などの法定通貨建てであること、中央銀行の債務として発行されること、のこれら三つの要件を満たすものとされている[2]。

CBDC が従来の銀行券や貨幣といった現金通貨と大きく異なるのは、現金のような物理媒体ではなく、デジタル化され電子データによって表現されるサイバー空間上の情報媒体であることである。このため、サイバー空間上の取引相手との非対面での取引も想定される。

現実空間における対面取引においては、中央銀行から発行された法定通貨である現金通貨を利用し、取引相手のアイデンティティを証明する身分証明書による本人確認を行いながら取引することで、通貨が本物であることや、取引相手が本人であることについて担保した取引を行うことが可能であると考えられる。

サイバー空間における非対面取引においては、取引で使用される電子データが本物であり、サイバー空間上の取引相手が実在し（実在性）、また、その取引相手が本当に当人であること（真正性）を担保するためには、それを確認するための仕組みが必要になる。このため、一般には、取引相手から提示される現実空間の身分証明書と紐づけた身元確認や携帯電話を利用した当人認証といった本人確認が求められている。一方で、サイバー空間上の新たな取組として、電子データで表現されるアイデンティティ情報に基づいて本人確認を行う取組が進められている。この取組においては、電子データによる確実な本人確認が必要であるだけではなく、サイバー空間上のアイデンティティ情報の取扱いにおいて、なりすまし、漏えい、改ざん等を防止するための信頼性の高い管理の仕組みとしてトラスト[3]の確立や確認における電子データの正当性を確認し、トラストを確保する仕組みであるトラストサービスも求められる[4]。

本章では、トラストサービスにおいて不可欠な要素である、サイバー空間上のアイデンティティ、すなわちデジタルアイデンティティの考え方や、その管理の仕組みについて、技術的側面から現状を整理するとともに、最新の動向に関して調査した結果について報告する。

4.2　デジタルアイデンティティ

4.2.1　デジタルアイデンティティの考え方

用語としてのアイデンティティ（identity）については、中世ラテン語で「同じもの」を意味する「idem」を語源として、14 世紀頃にフランス語から派生し、1600 年頃に使用されるようになったと考えられている[5]。また、概念としてのアイデンティティについては、20 世紀の精神分析学者である Erik H. Erikson によって提唱された自己同一性、すなわち「自分は誰なのか」としての考え方が、心理学、社会学等において認識されている[6]。

一方、デジタルアイデンティティに関する明確な定義は存在しないものの、一般的には、アイデンティティの電子的な表現であり、情報通信システムにおいて処理可能なものとして捉えられている。

デジタルアイデンティティの考え方や性質については、米国国立標準技術研究所（NIST : National Institute of Standards and Technology）が発行した、米国政府機関向けのデジタルアイデンティティに関する技術的ガイドラインである NIST SP 800-63-3[7]において、オンライン取引に従事する対象者の固有の表現であり、デジタルサービスドメインにおいて常に一意的であるが、全てのドメインにおいて常に一意的に個人を識別するものではない、との考え方が示されている[8]。

また、情報通信システムにおけるアイデンティティ管理の考え方に関する国際標準である ISO/IEC 24760[9]では、アイデンティティとは、あるエンティティに関する属性の集合である、との考え方が示されている[10]。なお、エンティティとは、任意のドメインの運用目的に関連する媒体[11]であり、人、もの、組織等の物理媒体だけでなく、アプリ、デジタルサービス等の論理媒体も含まれる。また、属性とは、エンティティの性質を表すものであり[12]、例えば人の属性として、容姿、位置、経歴、連絡先、権利等が挙げられる。

したがって、デジタルアイデンティティとは、対象者であるユーザを含むエンティティに関する属性を電子データで表現した属性情報の集合として、任意のドメインにおいて対象者を一意的に識別可能な固有の情報である、と考えられる。

4.2.2　アイデンティティ管理

デジタルアイデンティティは、ユーザのアイデンティティを電子データで表現したアイデンティティ情報であり、不適切な利用によっては、ユーザの権利やプライバシーが侵害される恐れがあるため、適切に管理される必要がある。このようなデジタルアイデンティティ管理要件に関する著名な考え方として、Microsoft®のアイデンティティ・アーキテクトであった Kim Cameron が 2005

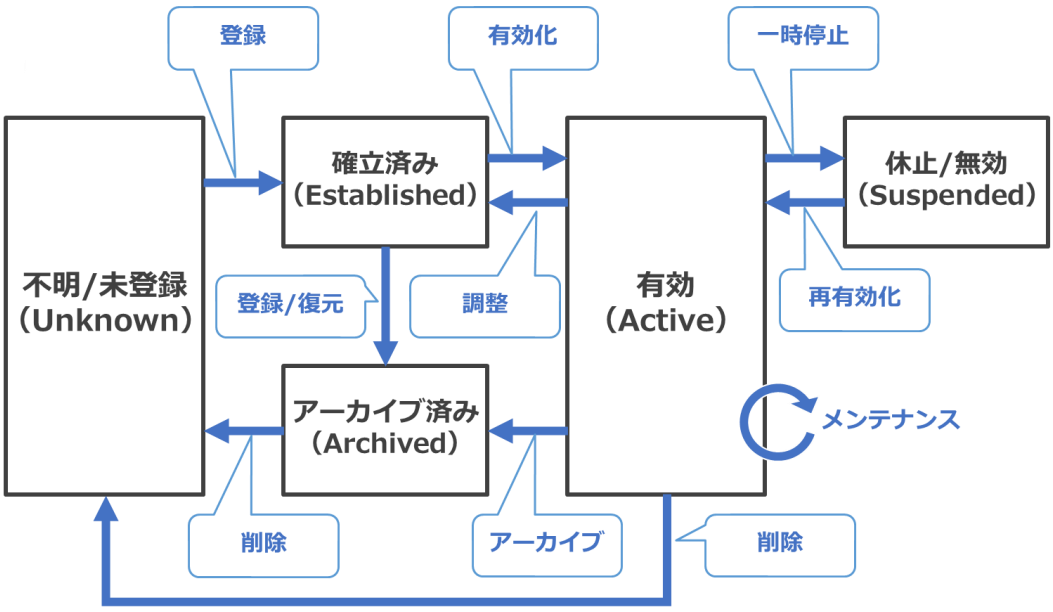
年に公表した「アイデンティティの原則」[13]が挙げられる（表 4.1 を参照）。デジタルアイデンティティの管理においては、このような原則に則ったアイデンティティ管理システム（IMS：Identity Management System）を設計し、確実に運用することが求められる。

表 4.1 アイデンティティの原則

原則	内容
ユーザによる制御と同意	ユーザの同意に基づく場合のみ、ユーザの識別に関する情報が開示される技術的なシステムでなければならない。
限定された用途での最低限の公開	最も長期的に安定的なソリューションとは、最小限のアイデンティティ情報の開示、及びその利用を最良の方法で制限するようなソリューションである。
正当と認められる関係者	特定の状況において、ユーザの識別情報を必要とする正当な立場の関係者のみに対して情報を開示するように、デジタルアイデンティティシステムを設計しなければならない。
方向づけられたアイデンティティ	識別が容易かつ、不必要な紐づけの公開を防止するため、公的用途の全方位的な識別子及び私的用途の単方位的な識別子をサポートする普遍的なシステムでなければならない。
複数の運用者及び技術の多元的共存	複数のアイデンティティプロバイダによって実行される複数のアイデンティティ技術の相互運用を実現し、相互接続を行う普遍的なシステムでなければならない。
人間の統合	確固たるマンマシンインターフェースによって結合された分散システムにおける構成要素として人間を位置付け、外部攻撃から保護する普遍的なメタシステムでなければならない。
コンテキスト全体に渡って一貫したエクスペリエンス	様々なアイデンティティプロバイダにおいてコンテキストの分離が可能かつ、シンプルで一貫性のあるエクスペリエンスを保証する統合的なメタシステムでなければならない。

“LAWS OF IDENTITY IN BRIEF”[14]を参考に筆者作成

IMS におけるアイデンティティ管理については、ISO/IEC 24760 において、特定のドメインにおいて公知である、アイデンティティに含まれる値、形式及び付帯的なメタデータ、並びにライフサイクル管理に関するプロセス及びポリシーである、との考え方が示されている[15]。なお、アイデンティティのライフサイクルとは、アイデンティティ情報の登録から確立、有効化、削除までの一連の処理プロセスのことである（図 4.1 を参照）。



役割	内容
不明/未登録 （Unknown）	識別に必要な情報が IMS に未登録で存在しないため、対象者について不明である状態
確立済み （Established）	対象者の登録申請に基づくアイデンティティ情報の検証済みで、必要な属性情報が生成され、IMS に登録された状態
有効 （Active）	IMS に登録されたアイデンティティ情報に基づき、アプリやデジタルサービス等のリソースにアクセス可能な状態
休止/無効 （Suspend）	IMS に登録された対象者のアイデンティティ情報は存在するが、対象者を認識できない状態（再利用可能）
アーカイブ済み （Archived）	対象者がドメイン内に存在する、しないに関わらず、対象者のアイデンティティ情報が存在し、保管された状態

図 4.1　アイデンティティのライフサイクル

“ISO/IEC 24760-1:2019, Figure 1 － Identity lifecycle”[16]を参考に筆者作成

また、国際電気通信連合の電気通信標準化部門（ITU-T）が策定した、アイデンティティ管理に関する勧告である ITU-T X.1252[17]においては、アイデンティティ管理の役割について、運用、保守管理、探索、関連付け、ポリシーの適用、認証及び表明といった一連の機能及び能力であり、識別子、クレデンシャル、属性等のアイデンティティ情報に関する保証、実体のアイデンティティに関する保証及びビジネスアプリやセキュリティアプリに関するサポートにおいて利用されるものである、との考え方が示されている[18]。

したがって、アイデンティティ管理とは、情報通信システムにおいて、ユー

ザのアイデンティティ情報を管理ポリシーに沿って適切に運用することによって、ユーザがリソースにアクセスするために必要となる機能をアイデンティティのライフサイクル全体にわたって提供することであり、そのための仕組みが IMS である。

IMS は、ユーザのアイデンティティ情報の管理状態に基づき、リソースへのアクセスを管理するシステムであり、適用される管理ポリシーに基づくアイデンティティ管理及びリソースへのアクセスにおけるアクセス管理を自動的に行うメカニズムとして設計される。

このうち、アクセス管理のためのアクセス管理システム（AMS：Access Management System）については、ISO/IEC 29146[19]において基本的な考え方が整理されている。ISO/IEC 29146 では、IMS と AMS との関係について、IMS において認証されたユーザからのリソースへのアクセス要求に対して、AMS において認可の判断を行うことにより、アクセス制御を行う仕組みとして示されている（図 4.2 を参照）。

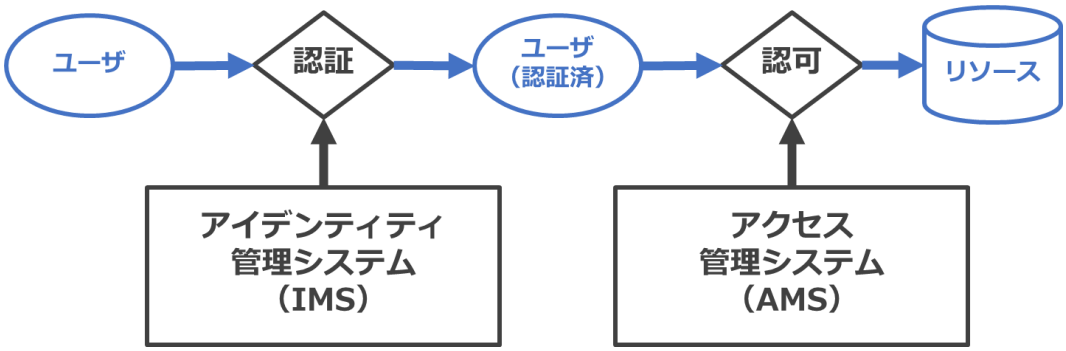


図 4.2　IMS 及び AMS の関係

“ISO/IEC 29146:2024, Figure 2 — Identity management system and access management system relationship” [20]を参考に筆者作成

なお、広義のアイデンティティ管理については、アイデンティティ管理を行う IMS とアクセス管理を行う AMS を合わせた、IAMS（Identity and Access Management System）として認識されている[21]ことから、本稿におけるアイデンティティ管理には、アクセス管理を含むものとして取り扱う。

4.3　デジタルアイデンティティの処理フロー

IAMS においては、アイデンティティのライフサイクルにおけるアイデンティティの確立、有効化及びアクセス権限の付与のための一連のプロセスとして、対象となるユーザのアイデンティティ情報の登録、識別、認証及び認可が自動的に行われる。これらの処理に関する概要は、以下のとおりである。

4.3.1 登録（enrollment）

登録については、ユーザのアイデンティティ情報をIAMSのデータベース、レジストリ等に記録する行為（registration）[22]と、ユーザのアイデンティティ情報の収集及び検証を行い、ユーザのアイデンティティを確立する行為（enrollment）[23]に区分される。本項では、後者について述べる。

登録とは、上記のとおり、アイデンティティのライフサイクルにおいて、ユーザのアイデンティティが確立済みである状態、すなわち、特定のドメインにおいてユーザが認識された状態にするためのプロセスである[24]。具体的には、ユーザの身元確認（identity proofing）[25]を行い、現実空間に実在する信頼できるユーザであることを検証するための処理が行われる。

登録においては、まず、デジタルサービス等の新規利用を要求するユーザからの登録申請に応じて、ユーザの身元確認が行われる。身元確認においては、ユーザの名前、生年月日、住所などのユーザを特定可能な属性情報及びそれらの属性情報を証明可能なエビデンスに関する検証が行われる。検証においては、ユーザから提示された属性情報及びエビデンスが IAMS の要求する仕様を満たすものであることに関する検証（validation）並びにユーザから提示された身分証明情報が間違いなくユーザに紐づいたものであることに関する検証（verification）が行われる。検証結果に問題がなければ、ユーザを一意的に識別可能な識別子等の識別情報に基づいて、ユーザのアイデンティティ情報と、ユーザが自分のアイデンティティを立証するための認証情報とを紐づけるクレデンシャル情報が発行される[26]。

4.3.2 識別（identification）

識別とは、集団の中から特定のユーザを一意的に区別するプロセスであり[27]、具体的には、任意のドメインにおける不特定多数の対象者の中から、対象のユーザが「誰か」を検索し、特定するための処理が行われる。

識別においては、ユーザの属性情報を利用した抽出が行われるが、特定のドメインにおいては、例えば、同姓同名や生年月日が同じであるなど、属性情報が重複するユーザが複数存在する可能性があり、その可能性はドメインに所属するユーザが多いほど高くなる。この場合、重複する属性情報だけでは一意的に区別できないため、重複しない属性情報を追加することによって、一意的に区別可能にする必要がある。したがって、ユーザの識別に必要となる属性情報の種類は、ドメインが大きいほど多く、小さいほど少なくなり[28]、大きなドメインにおいては、識別がより困難となる。

このような問題を解消する手段として、一般的には任意のドメインにおいてユーザを一意的に特徴づける識別情報である、識別子（identifier/ID）が利用

される。識別子とは、任意のドメインにおけるユーザのアイデンティティ情報の登録時に、当該ドメインにおいてユーザを特定可能な情報としてユーザに対して付与される属性情報である[29]。識別子の例として、学籍番号、社会保障番号、銀行口座番号、クレジットカード番号、電話番号、e メールアドレス、アカウント ID 等が挙げられる。

4.3.3 認証（authentication）

認証とは、識別されたユーザの真正性を検証し、確立するプロセスである[30]。具体的には、識別によって区別された「誰か」が、本当に「誰であるか」について検証することによって、本人確認を行うための処理が行われる。

認証時の検証では、ユーザから提示されたアイデンティティ情報が、本当にユーザに紐づいたものであることに関する検証（verification）が行われる。検証においては、ユーザから提示された認証情報がユーザの識別情報に紐づいた情報であること、信頼できる情報リソースから生成された情報であること及びドメインにおいて有効なものであることなどの確認が行われる[31]。

認証情報とは、検証において、アイデンティティ情報がユーザに紐づいていることを証明するために利用されるユーザ固有の属性情報である。ユーザが人である場合、認証要素として、生体情報、所持情報及び知識情報が利用される（表 4.2 を参照）。一般的な IAMS における認証では、これらの中から一つ以上の要素が利用されるが、高いセキュリティレベルが求められる場合は、二つ以上の要素を組み合わせる多要素認証が利用される。

表 4.2　認証情報の分類

要素	認証方法	特徴	例
生体情報	本人に固有の身体的特徴の個人差を利用	・所持・記憶不要 ・認証制度にばらつき	指紋、網膜、虹彩、静脈紋、顔、DNA 配列等
所持情報	本人しか持ちえない物理的媒体を利用	・記憶不要 ・盗用のリスク	IC カード、運転免許証、スマートフォン等
知識情報	本人しか知らない情報を利用	・所持不要 ・忘却、類推のリスク	パスワード、秘密鍵、リカバリフレーズ等

「ネット社会と本人認証 -原理から応用まで-」pp.25-31[32]を参考に筆者作成

4.3.4 認可（authorization）

認可とは、認証済みのユーザからのデジタルサービス等のリソースへのアクセス要求に対して、アクセスしてもよいか判定を行うプロセスであり[33]、具体的には、認証された「誰か」が、「何かに」アクセスするための操作を許可又は否認するための処理が行われる。

認可におけるアクセス制御においては、認証済みのユーザからのリソースへのアクセス要求に応じて、リソース管理者におけるアクセス管理ポリシーやユーザの権限に基づいたアクセスの認可又は否認が行われる[34]。

4.2.2 項に記載したとおり、認可は認証情報の検証を行う「狭義の認証」に引き続き実施されるアクセス制御のプロセスであり、付帯的な認証機能として「広義の認証」に含まれると考えられる。

認可においては、認証済みのユーザが保有する権限を把握する必要があるため、認証情報以外にユーザの権限に関する属性情報が必要であり、これらの属性情報を利用して、リソースへのアクセスに関する付帯的な認証を行うこととなる。このため、認可のことを属性認証と言うこともある[35]。

4.4　デジタルアイデンティティ管理モデル

アイデンティティ管理に係る構成要素や認証プロセスについては、NIST SP 800-63-3 においてモデル化されており（図 4.3 を参照）、米国以外の政府機関や民間サービスにおいても参照されている。

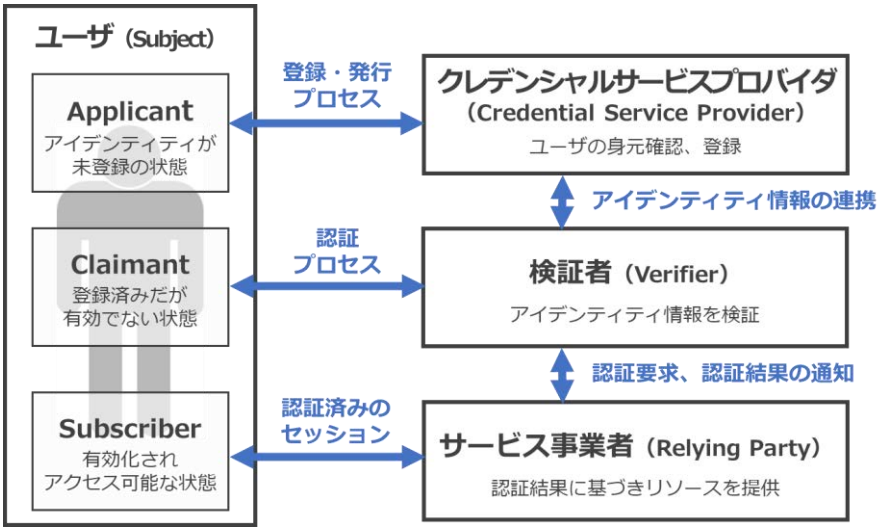


図 4.3　アイデンティティ管理モデル

“NIST Special Publication 800-63-3 Digital Identity Guidelines, Figure 4-1 Digital Identity Model ”[36]を参考に筆者作成

アイデンティティ管理モデルは、情報通信技術の発達やシステムの高度化に伴い、その構成も変化している。2023 年 3 月に公開された NIST SP 800-63-3 の変更案である NIST SP800-63-4 のドラフト版[37]では、アイデンティティ管理モデルとしてユーザのアイデンティティ管理を各ドメインにおいて個別に行う、基本的な管理モデルである集中モデル（Non-Federated model）に加え、連携する外部ドメインに自ドメインのユーザのアイデンティティ管理を委託する連携

モデル（Federated model）について、新たに示されている。各モデルの概要は、以下のとおりである。

4.4.1　集中モデル（Non-Federated model）

集中モデルとは、IAMS のすべての機能が備えられたサービス事業者のドメインにおいて、ユーザのアイデンティティ情報が一括管理され、集中的に運用される管理モデルである（図 4.4 を参照）。

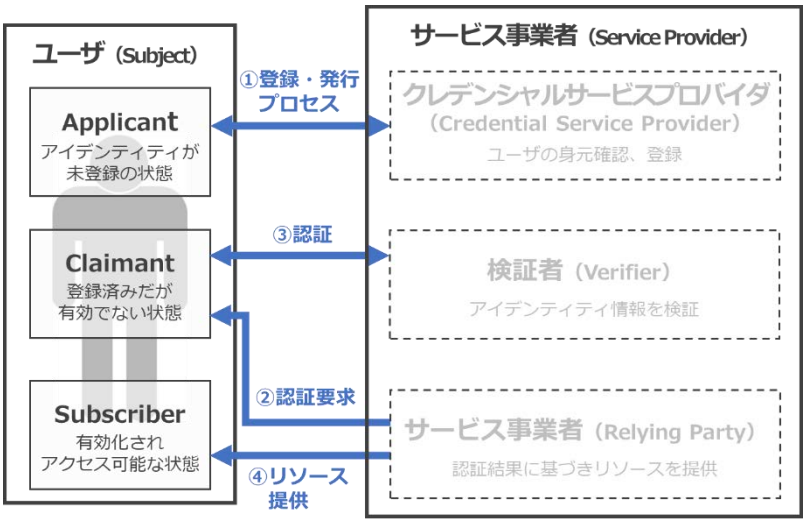


図 4.4　アイデンティティ管理モデル（集中モデル）

“NIST Special Publication 800-63-4 Digital Identity Guidelines IPD, Figure 1. Non-Federated Digital Identity Model Example”[38]を参考に筆者作成

集中モデルは、サービス事業者のドメインにおいて、ユーザとサービス事業者との二者間で情報のやり取りが完結するシンプルな構成である。ただし、各サービス事業者においては、IAMS を独自に構築し、運用する必要があるため、運用にかかるコストや労力が求められる。また、ユーザにおいても異なるサービス事業者のリソースを利用する場合、各サービス事業者のドメインで異なるクレデンシャル情報を自分で管理しなければならない。

このため、デジタルサービス等の拡充や多様化に伴い、ユーザが増加しただけでなく、一人のユーザが利用するデジタルサービス等も増加したため、ユーザ及びサービス事業者の双方において、アイデンティティ管理に係る負担が増加している。また、近年では、サービス事業者に対して、巧妙化する不正アクセス等からアイデンティティ情報を保護するための情報セキュリティ対策に加え、ユーザのプライバシーを保護するための対策も求められるようになり、アイデンティティ管理に係る負担は一層増加している。

4.4.2　連携モデル（Federated model）

連携モデルとは、ユーザとサービス事業者との間を仲介するアイデンティティプロバイダ（IdP：Identity Provider）が、第三者サービスとしてユーザのアイデンティティ情報を一括管理し、異なるドメインのサービス事業者との連携を行う管理モデルである（図 4.5 を参照）。

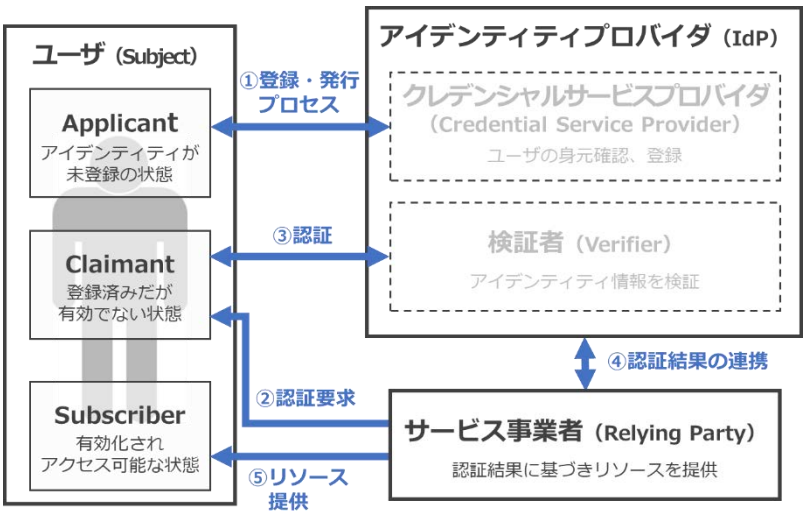


図 4.5　アイデンティティ管理モデル（連携モデル）

“NIST Special Publication 800-63-4 Digital Identity Guidelines IPD, Figure 2. Federated Digital Identity Model Example”[39]を参考に筆者作成

連携モデルは、集中モデルにおいて各サービス事業者に備わっていたクレデンシャルサービスプロバイダ（Credential Service Provider）及び検証者（Verifier）の機能をサービス事業者から切り離して IdP に集約し、IdP がアイデンティティ管理を仲介、連携する構成である。サービス事業者は IdP の Relying Party として、IdP から提供されるアイデンティティ情報や認証結果を信頼し、ユーザにデジタルサービス等のリソースを提供する。

IdP による連携は、異なるドメインのサービス事業者との連携を実現するものであり、単一の IdP を介して、複数のサービス事業者との連携が可能となる。このため、ユーザは集中モデルにおいて、IdP に登録済みのクレデンシャル情報を利用して、IdP と連携する複数のサービス事業者にアクセス可能となり（シングルサインオン）、ドメインごとに発行されていた複数のクレデンシャル情報を管理する必要がなくなるなど、利便性が向上する。また、サービス事業者においても、IdP にアイデンティティ管理を委託することによって、アイデンティティ管理に係るコストや労力が不要となり、本業に専念できる利点がある[40]。

一方、複数のドメインにおけるユーザのアイデンティティ管理を担う IdP に

は、膨大なアイデンティティ情報が集約されるため、情報セキュリティ対策やプライバシー対策も含め、より高い信頼性が求められる。

このように、連携モデルは異なるドメインのアイデンティティ連携を実現することによって、集中モデルと比較して、ユーザとサービス事業者の両方に利点がある管理モデルであることから、現在のデジタルアイデンティティ管理における主流の管理方法となっている。次節において、アイデンティティ連携において利用されている主要な技術の概要について説明する。

4.5 アイデンティティ連携技術

4.5.1 SAML（Security Assertion Markup Language）

SAML とは、XML（Extensible Markup Language）を基盤とする異なるドメインにおけるユーザの認証等に関するフレームワークの仕様である。現行仕様である SAML 2.0 は、e-ビジネスの標準化を推進する標準化団体である OASIS によって、2005 年に標準化されている[41]。

SAML 2.0 における処理プロセスの概要は図 4.6 のとおりである。

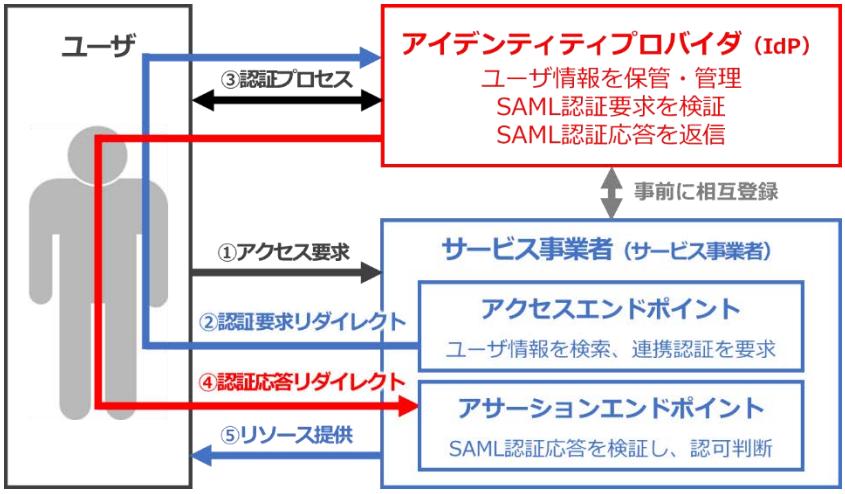


図 4.6 SAML 2.0 における処理プロセスの概要（SP-Initiated SSO）

"Security Assertion Markup Language (SAML) V2.0 Technical Overview CD, Figure 12: SP-Initiated SSO with Redirect and POST Bindings"[42]を参考に筆者作成

SAML2.0 によるアイデンティティ連携において、IdP はサービス事業者からの SAML 認証要求に基づいてユーザ認証を行い、問題がなければ、SAML 認証応答をサービス事業者に送信する。SAML 認証応答には、ユーザの認証情報、属性情報、IdP の証明書等が格納されたアサーションがトークンとして送信される。サービス事業者は、SAML 認証応答に含まれるアサーションを検証し、問題がなければユーザにリソースを提供する[43]。

SAML は、Web 技術である XML を利用することによって、特定のシステムやベンダに依存しない柔軟なアイデンティティ連携のフレームワークが構築可能である反面、データ構造が複雑かつ大容量となり、その実装や運用には高度な専門性が必要とされる。このため、企業向けクラウドサービス等、エンタープライズ用途の SaaS（Software as a Service）や IDaaS （Identity as a Service）等で利用されている。

4.5.2 OAuth

OAuth とは、異なるドメインのデジタルサービス等におけるデータ連携のためのアクセス権限の委譲に関するフレームワークの仕様である。現行仕様である OAuth 2.0 は、インターネット技術の標準化団体である IETF によって、2012 年に IETF RFC 6749 として標準化されている[44]。

OAuth 2.0 における処理プロセスの概要は図 4.7 のとおりである。

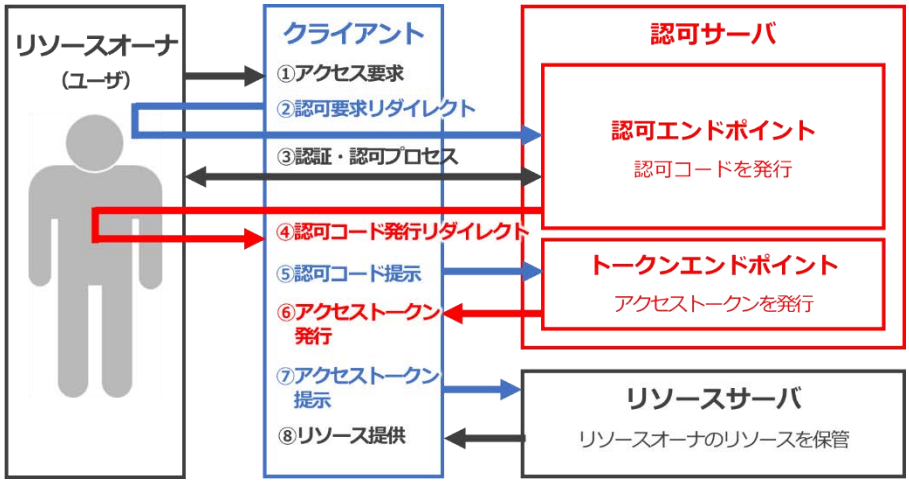


図 4.7 OAuth 2.0 の処理プロセスの概要（認可コードフロー）

“IETF RFC 6749, The OAuth 2.0 Authorization Framework, Figure 1: Abstract Protocol Flow 及び Figure 3: Authorization Code Flow”[45]を参考に筆者作成

OAuth 2.0 によるアイデンティティ連携において、認可サーバは、クライアントからのリソースサーバへのアクセス認可要求に対して、ユーザの同意に基づき、リソースサーバへのアクセスに必要なアクセストークンを発行する。クライアントは、リソースサーバにアクセストークンを提示することによって、ユーザの代理としてリソースサーバにアクセス可能となる。

このように、OAuth はユーザの代理であるクライアントがリソースサーバにアクセスするため、ユーザの権限をクライアントに移譲することを目的とした認可に関する仕様であり、認証は仕様の範囲外である。したがって、OAuth を実装する場合、別途認証用フレームワークも必要となる。

OAuth 2.0 はブラウザに加え、API(Application Programming Interface)連携によってスマートフォン等の端末上で動作するネイティブアプリにも対応可能であることから、スマートフォンの普及や利用拡大に伴い、SNS（Social Network Service）や SaaS 等、様々なデジタルサービス等において利用されている。また、日本国内では、銀行と FinTech 企業等との連携のためのオープン API における全国銀行協会の推奨プロトコルとして[46]、銀行分野において広く実装されているだけでなく、電子政府の総合窓口である「e-Gov」における電子申請 API に実装される[47]など、官民問わず幅広く利用されている。

4.5.3 OpenID Connect

OpenID Connect とは、OAuth 2.0 の仕様を拡張し、異なるドメインにおけるユーザの認証等に関するフレームワークの仕様である。OpenID Connect は、インターネットにおけるアイデンティティ管理技術の標準化団体である OpenID Foundation によって、2014 年に標準化されている[48]。

OpenID Connect における処理プロセスの概要は図 4.8 のとおりである。

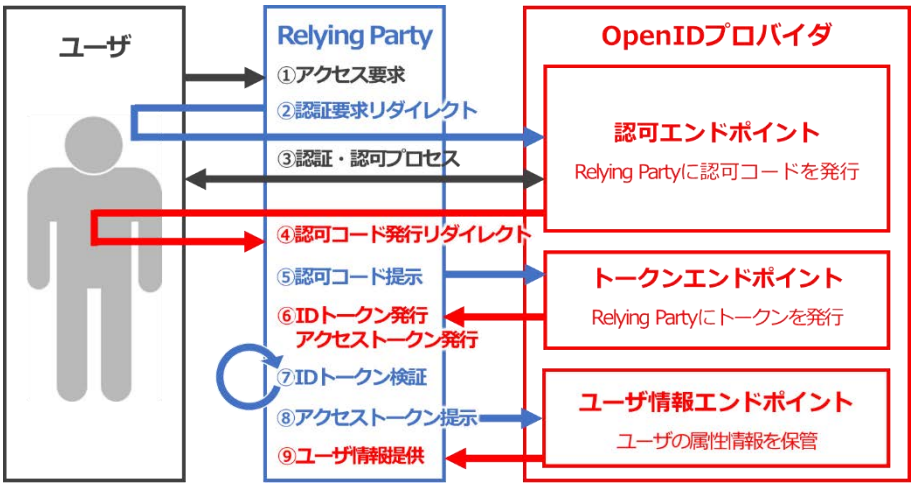


図 4.8　OpenID Connect の処理プロセスの概要（認可コードフロー）
“OpenID Connect Basic Client Implementer’s Guide 1.0 – draft 47”[49]を参考に筆者作成

OpenID Connect によるアイデンティティ連携において、OpenID プロバイダは、Relying Party であるブラウザやアプリからのユーザ情報エンドポイントへのアクセス要求に対して、ユーザの合意及び認証に基づき、ユーザのアイデンティティ情報が含まれる ID トークン及びユーザ情報エンドポイントへのアクセスに必要なアクセストークンを発行する。ブラウザやアプリは ID トークンの検証を行い、問題がなければ、ユーザ情報エンドポイントにアクセストークンを提示することで、ユーザの代理としてユーザ情報エンドポイントにア

クセス可能となり、必要なユーザの属性情報を取得する。

このように、OpenID Connect の処理プロセスは、OAuth 2.0 に ID トークンによるユーザの認証プロセスを追加したものであり、基本的なフレームワークや処理フローは OAuth 2.0 と同様である。一方、ユーザのアイデンティティ情報が含まれる ID トークンについては、JSON ウェブトークン（JWT：JSON WEB TOKEN）[50]を利用することとされており、署名や暗号化によってアイデンティティ情報を保護可能なセキュリティ性の高い仕様として、厳密に定められている。

OpenID Connect は OAuth 2.0 を拡張したアイデンティティ連携技術であり、OAuth 2.0 と同様、様々な SNS やデジタルサービス等において利用されているだけでなく、経済産業省が提供している法人・個人事業主向け共通認証システムである「G ビズ ID」の認証基盤においても利用されるなど[51]、連携モデルにおける代表的な認証方式として広く普及している。

4.6 連携モデルの課題及びその対応

4.6.1 連携モデルの課題

ユーザのアイデンティティ管理については、当初ユーザに対してデジタルサービス等を提供するサービス事業者が、各ドメインにおいて実施する集中モデルとして実施されていた。その後、アイデンティティ連携を実現可能な技術の開発や普及に伴い、それまでサービス事業者が行っていたユーザのアイデンティティ管理を IdP が一手に担う、連携モデルによるアイデンティティ管理が主流となっている。これらの集中モデル及び連携モデルはいずれも、ユーザのアイデンティティ情報がサービス事業者や IdP に集約され、一元的な管理が行われる中央集権的な管理方法である。

このような中央集権的な管理方法においては、ユーザのアイデンティティ情報の管理主体として、本来の保有者であるユーザではなくサービス事業者や IdP が担うこととなる。ユーザは、サービス事業者や IdP を信頼した上で、自分のアイデンティティ管理を委託することとなる。したがって、ユーザのアイデンティティ情報を管理するサービス事業者や IdP は、デジタルサービス等を利用するユーザに対して大きな影響力を持つこととなる。この影響力は、アイデンティティ連携によって、単一の IdP が複数のデジタルサービス等を仲介する連携モデルにおいて、より顕著となる。

特に、現在の主要な IdP は Google®、Microsoft®、Apple®、Meta®、Amazon®といった一部の大手プラットフォーム事業者による寡占状態にある。これらの大手事業者は、有力なデジタルサービス等を多数提供し、大量のユーザを自社のプラットフォームに囲い込むことによって、ネットワーク効果による競争

優位性の強化を図ってきた。その結果、今日のデジタルサービス等において不可欠な存在となり、世界規模で支配的な影響力を持つようになったため、ユーザはデジタルサービス等の利用において、これらの大手事業者に依存せざるを得ない状況となっている[52]。

このような大手事業者による寡占は、ユーザのロックイン効果を引き起こし、データ流通の不均衡や健全なデータの利活用を阻害する要因となっていることが指摘されているだけでなく、大手事業者が運営する IdP への過度な依存によって想定される以下のようなリスクが懸念されている[53]。

(1) セキュリティのリスク

大量のユーザのアイデンティティ情報を保管する IdP は、ハッキング等の外部からの攻撃の標的とされやすく、仮に外部からの攻撃を受けた場合、その被害も甚大となる。また、IdP はユーザの同意なくアイデンティティ情報を改ざんできる権限を持つため、悪意ある IdP によって、ユーザに無断でアイデンティティ情報が意図的に改ざんされる可能性がある。

(2) アクセシビリティのリスク

自然災害、インシデント、事業者の廃業等により IdP が停止した場合、ユーザは、IdP と連携している全てのデジタルサービス等が利用できなくなる。また、悪意ある IdP によって一方的にアカウントを停止された場合も、連携している全てのデジタルサービス等が利用できなくなる。

(3) プライバシーのリスク

IdP と連携しているデジタルサービス等を利用する場合、ユーザは必ず IdP を経由することとなるため、IdP はユーザのデジタルサービス等の利用履歴をすべて把握可能である。また、悪意ある IdP によってアイデンティティ情報や利用履歴が無断で流用されても、ユーザは感知できない。

4.6.2 連携モデルの課題への対応

4.6.1 項で述べたリスクへの対応策としては、大手事業者によるデジタルサービス等の寡占を解消すること及びアイデンティティ管理における IdP への依存度を下げることが挙げられる。

このうち、大手事業者によるデジタルサービス等の寡占への対応については、米国、欧州連合（EU）、日本等各国において個人データの囲い込み防止による競争の促進等の課題解決に取り組んでおり、様々な規制対策に関する検討や法整備が進められている[54]。

特に EU においては、2015 年における EU 域内調査の結果、域内のデジタル市場の約 54%が米国企業のデジタルサービス等で占められていたことが判明した[55]影響もあり、2016 年に一般データ保護規則（GDPR：General Data

Protection Regulation）[56]、2022 年にデジタル市場法（DMA：Digital Markets Act）[57]及びデジタルサービス法（DSA：Digital Services Act）[58]が立て続けに採択され、サービス事業者への適用が開始されるなど、EU 域内におけるプライバシー保護、データ流出制限、大手事業者への規制等に関する法整備が進められている（表 4.3 を参照）。

表 4.3 EU における大手事業者に対する規制

名称	概要
一般データ保護規則（GDPR：General Data Protection Regulation）	2016 年 4 月 27 日採択、2018 年 5 月 25 日適用 ・個人情報（データ）保護という基本的人権の確保が目的 ・欧州経済領域（EEA）で取得した個人情報の域外への移動を原則禁止 ・罰則規定あり（罰金）
デジタル市場法（DMA：Digital Markets Act）	2022 年 9 月 14 日採択、2022 年 11 月 1 日適用 ・大手事業者の寡占抑制及び EU の市場競争力強化が目的 ・指定「ゲートキーパー」によるサービス独占の禁止 ・罰則規定あり（罰金）
デジタルサービス法（DSA：Digital Services Act）	2022 年 10 月 4 日採択、2024 年 2 月 17 日適用 ・EU 域内のオンライン上におけるユーザの保護が目的 ・事業者に対するユーザ保護責任及び保護環境構築義務 ・罰則規定あり（罰金）

他方、アイデンティティ管理における IdP への依存度を下げる考え方として、近年、分散型アイデンティティが提唱されている。

分散型アイデンティティは、これまでサービス事業者や IdP において、中央集権的に保管及び管理されていたユーザのアイデンティティ情報を、ネットワーク上に分散して保管する仕組みである[59]。アイデンティティ情報をネットワーク上に分散して保管することによって、連携モデルのようなアイデンティティ情報を IdP に集約し、一括保管する必要がなくなるため、IdP への依存度を下げることが可能となることから、IdP への過度な依存に伴う各種リスクを解消可能と考えられている。

また、分散型アイデンティティにおいては、分散して保管されるユーザのアイデンティティ情報について、ユーザが自分で管理することも可能となる。このようなユーザが中心となって、自らアイデンティティ管理を行う「自己主権型アイデンティティ」の考え方が、近年注目されている。

4.6.3　自己主権型アイデンティティ（SSI：Self-Sovereign Identity）

自己主権型アイデンティティとは、ユーザがアイデンティティ管理の中心となって、ユーザの自律的な判断に基づき、アイデンティティ管理やアイデンティティ連携が行われるべきである、という考え方である。

アイデンティティ情報の元来の保有者であるユーザが、アイデンティティ情報に関する真の制御者であるべきである、という考え方については、2010 年頃から、様々な議論がなされてきた。インターネットセキュリティの専門家である Christopher Allen は、2016 年に、それまでのアイデンティティ主権に関する議論を踏まえ、SSI に求められる要件を整理し、SSI の 10 原則として公表した[60]。また、SSI の実現を目指す国際団体である Sovrin Foundation は、SSI に関するコミュニティ活動の成果として、デジタルアイデンティティのエコシステムに適用すべき SSI の基本原則を公表している[61]。さらに、4.2.2 項で述べた Kim Cameron も、自身の提示した「アイデンティティの原則」を更新し、SSI 時代における原則として表明している[62]。これらの SSI に関する基本原則では、アイデンティティ管理において、特定のサービス事業者にアイデンティティ情報の保管及び管理を委ねることなく、ユーザ自身によりアイデンティティ情報を保管及び管理することが可能であること、また、その実現のために十分な相互運用性が確保されるべきであることなどが共通原則として示されている。

SSI がこれらの基本原則に基づいて実現されることによって、ユーザは、サイバー空間上のデジタルアイデンティティについても、現実空間のアイデンティティと同様に取り扱うことが可能となる。また、ユーザのプライバシー保護にも有効と考えられている。このため、現在、SSI を実現するための分散型アイデンティティの実装に向けた技術開発や標準化が進められている。以下の項では、代表的な技術として、検証可能なクレデンシャル（VC：Verifiable Credential）及び分散型識別子（DID：Decentralized Identifier）について説明する。

4.7　分散型アイデンティティ関連技術

4.7.1　検証可能なクレデンシャル（Verifiable Credential）

検証可能なクレデンシャル（VC：Verifiable Credential）とは、分散型アイデンティティの実装におけるフレームワークに関する仕様である。VC は、Web 技術の標準化団体である W3C（World Wide Web Consortium）における Verifiable Credential 作業部会において、2019 年に W3C 勧告として標準化された。現行バージョンは、2022 年に標準化された “Verifiable Credentials Data Model v1.1”[63]であり、現在、v2.0 の策定に向けた検討が進められてい

る。

VC のフレームワークの概要は図 4.9 のとおりである。

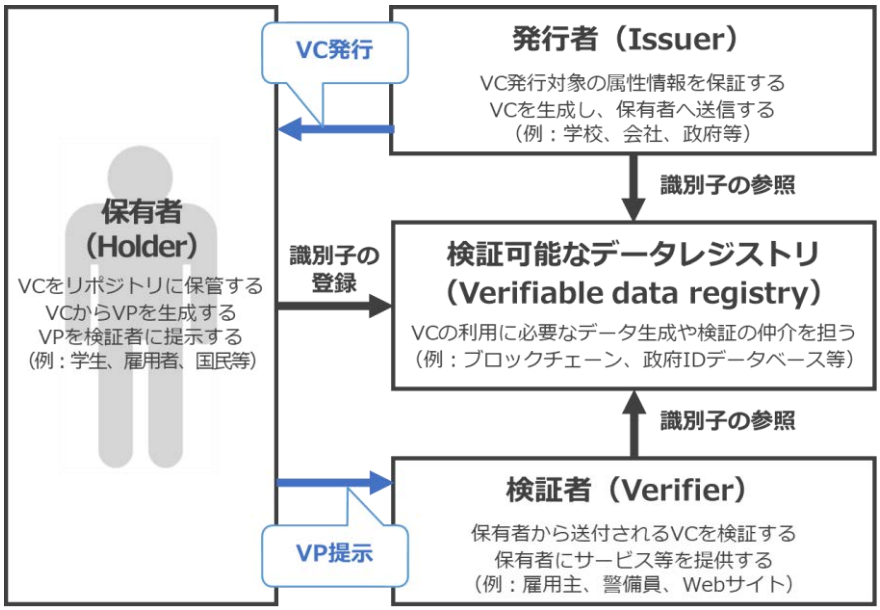


図 4.9　VC のフレームワークの概要

“Verifiable Credentials Data Model v1.1, Figure 1 The roles and information flows forming the basis for this specification.”[64]を参考に筆者作成

VC のフレームワークにおいて、保有者であるユーザは、信頼された発行者から発行された VC を、自分の管理するクラウド上や端末上のリポジトリ（格納領域）に格納するとともに、一つ以上の VC から、提示用の証明書（VP：Verifiable Presentation）を作成し、検証者に提示する。検証者は、ユーザから提示された VP の検証を行い、問題がなければ、ユーザにサービス等を提供する。検証においては、VC に記録されたユーザのアイデンティティ情報等の真正性に関する検証ではなく、VC が仕様を満たすものとして正当な発行者から正当な保有者に発行されたものであり、改ざんされていないことに関する検証が行われる[65]。なお、発行者、保有者及び検証者の間で必要となるアイデンティティ連携については、発行者、保有者及び検証者とは独立したシステムである、検証可能なデータレジストリを介して行われる。検証可能なデータレジストリとしては、政府 ID データベースのような信頼済みのデータベースに加え、分散データベース、分散型台帳システム等が想定されている[66]。

VC のフレームワークは、これまでの中央集権的な管理主体によるアイデンティティ管理と比較して、次の二点が異なる。一点目は、連携モデルにおいてアイデンティティ情報の登録・発行と保管を担っていた IdP の役割が、発行者と保有者に分離され、保有者がアイデンティティ情報を保管することである。

二点目は、サービスの利用者である保有者と、サービス等の提供者である検証者との間に、IdP の仲介が不要となることである。

このため、保有者であるユーザは、検証者に提示する VP に含まれる VC を自分の管理するリポジトリから選択可能であり、検証者に対して必要最小限の情報のみ提示する、選択的開示が可能となる。また、ユーザは、サービスを利用するための認証プロセスにおいて、VP を検証者のみに送付すればよいことから、サービスの利用履歴が発行者に知られることがないだけでなく、発行者においても、登録及び発行済みのアイデンティティ情報の保管が不要となり、アイデンティティ情報を保管するための労力から解放される。さらに、災害やサービス停止等により発行者の機能が消失しても、発行済みの VC 保有者のリポジトリ上に存在し続ける限り、ユーザはその VC を検証者に提示することで、サービスの利用を継続することが可能となる。

このように、VC を実装することによって、4.6.1 項で述べた、連携モデルにおいて懸念される各種リスクの低減や解消が期待されている。

4.7.2 分散型識別子（Decentralized Identifier）

分散型識別子（DID：Decentralized Identifier）とは、分散型アイデンティティや SSI を実装するための識別子に関する技術の仕様である。DID は、W3C の Decentralized Identifier 作業部会において、“Decentralized Identifiers (DIDs) v1.0”[67]として 2022 年に標準化されている。

DID アーキテクチャの概要については、図 4.10 のとおりである。

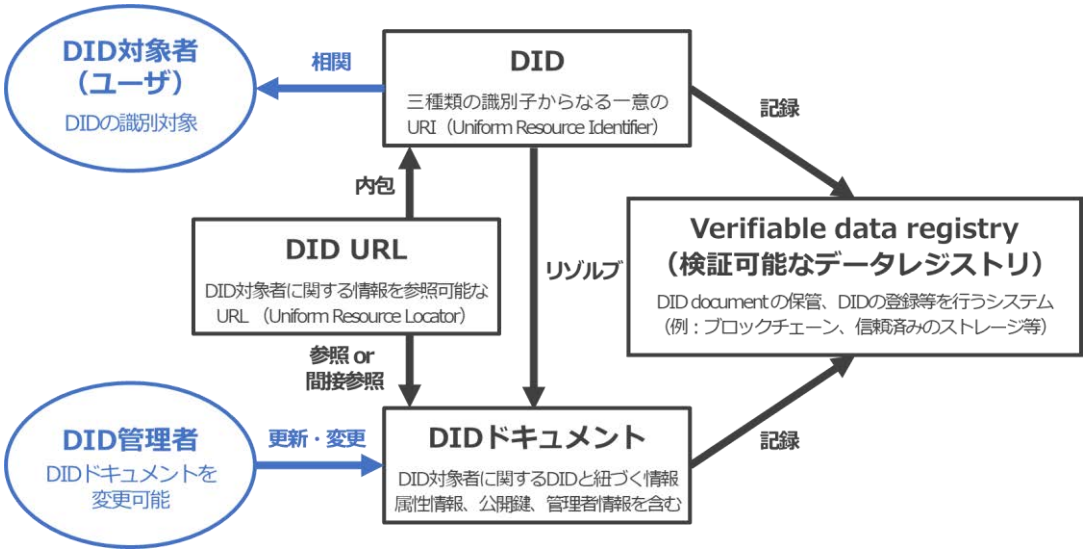


図 4.10　DID のアーキテクチャ

“Decentralized Identifiers (DIDs) v1.0, Figure 2 Overview of DID architecture and the relationship of the basic components.”[68]を参考に筆者作成

DID は、DID 対象者であるユーザ自ら識別子を生成及び登録可能な技術であり、サービス事業者や IdP のような中央集権型の管理主体による発行を必要としない識別子である。DID に紐づく DID ドキュメントには、ユーザの識別子、認証方法、検証用の公開鍵等に関する情報が含まれる[69]。DID 管理者は、DID ドキュメントの更新や変更が可能なアイデンティティ管理主体であり、ユーザも DID 管理者として設定可能である。

DID は、図 4.11 に示す構成によって表現される。

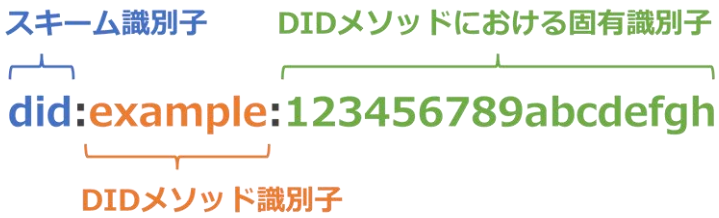


図 4.11　DID の表現例

“Decentralized Identifiers (DIDs) v1.0, Figure 1 A simple example of a decentralized identifier (DID)”[70]を参考に筆者作成

DID は、DID スキームであることを表すスキーム識別子、DID の仕様を実現する方法である DID メソッドの種類を表すメソッド識別子、及び各メソッドにおける固有情報であるメソッド固有識別子の、三つの識別子によって構成される[71]。DID メソッドは、DID を入力することによって検証可能なデータレジストリから DID ドキュメントが出力される、リゾルブに関する仕組みとして定義される。なお、W3C の仕様を満たす DID メソッドについては W3C において管理されており、2023 年 9 月時点で、180 以上の DID メソッドが登録されている[72]。

DID ドキュメントを保管するための検証可能レジストリとして、ブロックチェーンのような非中央集権的なシステムを利用する場合、中央集権的なアイデンティティ管理主体が不要となり、SSI の実現が可能となり得る。なお、DID ドキュメントには、ユーザ認証のための公開鍵など、検証に必要な情報が含まれることから、ユーザが VC を DID で署名することによって DID と紐づいたユーザが保有する VC の検証が可能となる。

4.7.3　分散型アイデンティティの課題

SSI の考え方では、アイデンティティ管理主体はユーザだが、実際の分散型アイデンティティにおけるユーザのアイデンティティ管理機能は、デジタルアイデンティティウォレット等、ユーザのアイデンティティ情報を格納するリポ

ジトリの機能として提供される。この場合、ユーザの本人確認を行うための認証プロセスが必要であるのと同様、ユーザのリポジトリが正当なものであるか確認するための認証プロセスが必要となる[73]。特に、デジタルアイデンティティウォレットの典型的なユースケースとしては、ユーザの所持するスマートフォン等の端末上のアプリによって、リポジトリの機能が実装される。この場合、ユーザのアイデンティティ管理に必要な暗号鍵等の認証情報については、端末内のセキュアエレメントや TEE（Trusted Execution Environment）等、信頼の起点（Root of Trust）となる専用のハードウェアに保管されることとなる。ただし、現状では、アプリの機能及び提供方法については、スマートフォンのサービス事業者が提供する OS、アプリストア等によって異なる[74]だけでなく、信頼の起点となるハードウェアの実装方法についても端末ベンダによって異なる[75]。このため、リポジトリの機能や提供方法次第では、特定のサービス事業者や端末ベンダに依存せざるを得ない状況が引き起こされ、利用されるサービス事業者や端末ベンダに偏りが生じるなど、現在の IdP と同様の課題が発生する可能性がある。

また、分散型アイデンティティに関する取組としては、W3C 以外にも、前述の IETF、OASIS、OpenID Foundation、Sovrin Foundation に加え、分散型アイデンティティの相互運用に関する各種仕様の検討及び開発を行う標準化団体である DIF（Decentralized Identity Foundation）、分散型アイデンティティにおけるアイデンティティ連携の信頼性向上を推進する標準化団体である ToIP（Trust Over IP Foundation）、オープンソースのブロックチェーン推進団体である Hyperledger Foundation 等、様々な標準化団体において、技術仕様の検討や標準化が進められている[76, 77]。これらの団体は、相互に連携、協働しつつ、それぞれの活動目的に沿った独自の技術仕様に関する検討及び策定に向けた取組を進めている。したがって、分散型アイデンティティがユーザにとって信頼できるだけでなく、利便性のあるものとして普及するためには、各団体で仕様が異なる技術について、柔軟な連携を実現するための技術的な相互運用性の確保が求められる。

さらに、発行者は、分散型アイデンティティのフレームワークにおいても、信頼されていることが前提となっている。このようなトラストアンカーとしての役割を果たすために発行者に求められる要件については、発行者が発行するクレデンシャル情報の性質によって異なる。例えば、現実空間において、運転免許証等の身分証明書が本人確認書類として有効なものとして認識されている理由については、公的機関により発行され、かつ、被証明者にのみ一枚だけ発行されることが十分に想定されることが挙げられている[78]。このように、分散型アイデンティティにおいても、発行者からの要請として発行するクレデン

シャル情報が、正当なユーザのみに対して一回限り発行されていることを確実に保証するための、中央集権的な発行管理が必要となる場合が想定される。したがって、分散型アイデンティティのフレームワークにおいては、従来の中央集権型のアイデンティティ管理との連携も視野に入れた相互運用性の確保に向けて、技術面だけでなく制度面においても、柔軟な連携による相互運用が可能なアイデンティティ管理基盤の構築が求められると考えられる。

以上から、分散型アイデンティティの実装においては、特定の技術や団体に依存することなく、信頼性、柔軟性及び利便性の高いアイデンティティ管理基盤をどのように構築し、ユーザに提供するかについて、技術面及び制度面の両方から、サービス事業者、標準化団体、公的機関等を交えた横断的な検討が必要であると考えられる。

4.8 まとめ

デジタルアイデンティティ管理技術は、サイバー空間におけるトラストの確保に不可欠な技術として、デジタルサービス等の普及・拡大に伴い、利便性、効率性及び信頼性の向上が図られてきたが、その結果、大手事業者による寡占化が進行し、そのことに伴うリスクが懸念されている状況にある。

このような状況に対して、分散型アイデンティティの実装や SSI の実現によって、これらのリスクを解消することが可能と考えられている。このための仕組みとして、VC、DID 等をはじめとする分散型アイデンティティや SSI の実現に向けた新たな技術開発や標準化について、広く活発に進められている。

これからのトラストサービスにおいては、安全で信頼性が高いだけでなく、ユーザが自由に選択可能かつ、柔軟な相互連携が可能な、多様性、包摂性及び公平性を兼ね備えたアイデンティティ管理基盤の構築が求められると考えられる。現状、このようなトラストサービスについては、そのあり方について技術と制度の両面から検討が進められている状況にもあり、分散型アイデンティティや SSI といった仕組みが、今後 CBDC に使われる可能性もあることから、技術動向については継続的に注視していく必要があると考えられる。

---

1 日本銀行金融研究所、「「中央銀行デジタル通貨に関する法律問題研究会」報告書」、 2022.6.22、 pp.4-5
2 日本銀行、「中央銀行デジタル通貨とは何ですか？」、2024.1.16、(https://www.boj.or.jp/about/education/oshiete/money/c28.htm)
3 国立研究開発法人科学技術振興機構研究開発戦略センター、「研究開発の俯瞰報告書 システム・情報科学技術分野(2023 年)」、 2023.5、 pp.367-368
4 総務省、「プラットフォームサービスに関する研究会 トラストサービス検討ワーキンググループ 最終取りまとめ」、2020.2.7、p.2
5 etymonline、「identity の語源」、(https://www.etymonline.com/jp/word/identity#etymonline_v_1484)
6 コトバンク、「アイデンティティ理論(アイデンティティりろん)とは？ 意味や使い方」、(https://kotobank.jp/word/%E3%82%A2%E3%82%A4%E3%83%87%E3%83%B3%E3%83%86%E3%82%A3%E3%83%86%E3%82%A3%E7%90%86%E8%AB%96-2099708#w-2165544)

7 National Institute of Standards and Technology, “NIST Special Publication 800-63-3 Digital Identity Guidelines”, 2017.6
8 National Institute of Standards and Technology, “NIST Special Publication 800-63-3 Digital Identity Guidelines”, 2017.6, p.2
9 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5
10 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.1
11 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1: Terminology and concepts”, 2019.5, p.1
12 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.2
13 Cameron, Kim, “The Laws of Identity”, 2005.5.11, (https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf)
14 Cameron, Kim, “LAWS OF IDENTITY IN BRIEF”, 2006.1.8, (https://www.identityblog.com/wp-content/images/2009/06/7_Laws_of_Identity.jpg)
15 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.5
16 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, pp.14-15
17 Telecommunication Standardization of International Telecommunication Union, “Recommendation ITU-T X.1252 Baseline identity management terms and definitions”, 2021.4
18 Telecommunication Standardization of International Telecommunication Union, “Recommendation ITU-T X.1252 Baseline identity management terms and definitions”, 2021.4, p.5
19 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 29146 Information technology Security techniques A framework for access management”, 2024.1
20 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 29146 Information technology Security techniques A framework for access management”, 2024.1, p.6
21 宮川寧夫、慶應義塾大学大学院メディアデザイン研究科、「アクセス管理の参照モデルと補償レベル要件についての研究」、2015.2.27、pp.10-11
22 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.6
23 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.5
24 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.17
25 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.5
26 National Institute of Standards and Technology, “NIST Special Publication 800-63-3 Digital Identity Guidelines”, 2017.6, pp.10-14
27 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.3
28 Telecommunication Standardization of International Telecommunication Union, “Recommendation ITU-T X.1252 Baseline identity management terms and definitions”, 2021.4, p.10

29 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.2
30 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.18
31 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 24760-1:2019 IT Security and Privacy A framework for identity management Part 1:Terminology and concepts”, 2019.5, p.16
32 板倉征男・外川政夫、社団法人電子情報通信学会、「ネット社会と本人認証 -原理から応用まで-」、2010.8.20、pp.25-31
33 宮川寧夫、慶應義塾大学大学院メディアデザイン研究科、「アクセス管理の参照モデルと補償レベル要件についての研究」、2015.2.27、p.3
34 The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 29146 Information technology Security techniques A framework for access management”, 2024.1, p.1
35 財団法人日本情報処理開発協会電子商取引推進センター・電子商取引推進協議会、「属性認証ハンドブック」、2005.2、p.29
36 National Institute of Standards and Technology, “NIST Special Publication 800-63-3 Digital Identity Guidelines”, 2017.6, p.10
37 National Institute of Standards and Technology, “NIST Special Publication 800-63-4 Digital Identity Guidelines Initial Public Draft”, 2022.12
38 National Institute of Standards and Technology, “NIST Special Publication 800-63-4 Digital Identity Guidelines Initial Public Draft”, 2022.12, p.12
39 National Institute of Standards and Technology, “NIST Special Publication 800-63-4 Digital Identity Guidelines Initial Public Draft”, 2022.12, p.13
40 National Institute of Standards and Technology, “NIST Special Publication 800-63-4 Digital Identity Guidelines Initial Public Draft”, 2022.12, p.21
41 Organization for the Advancement of Structured Information Standards, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, 2005.3.15
42 Organization for the Advancement of Structured Information Standards, “Security Assertion Markup Language (SAML) V2.0 Technical Overview Committee Draft”, 2008.3.25, p.28
43 Organization for the Advancement of Structured Information Standards, “Security Assertion Markup Language (SAML) V2.0 Technical Overview Committee Draft”, 2008.3.25, pp.28-30
44 Internet Engineering Task Force, Request for Comments: 6749, “The OAuth 2.0 Authorization Framework”, 2012.10, (https://datatracker.ietf.org/doc/html/rfc6749)
45 Internet Engineering Task Force, Request for Comments: 6749, “The OAuth 2.0 Authorization Framework”, 2012.10, (https://datatracker.ietf.org/doc/html/rfc6749)
46 全国銀行協会オープン API のあり方に関する検討会、「オープン API のあり方に関する検討会報告書 ーオープン・イノベーションの活性化に向けてー」、2017.7.13、 p.14
47 デジタル庁、「e-Gov リニューアルに伴う変更点について（電子申請関係） 第 1.0 版」、2020.10.1、pp.26-27
48 OpenID Foundation, “OpenID Connect Core 1.0”, 2014.2.25, (https://openid.net/specs/openid-connect-core-1_0-final.html)
49 OpenID Foundation, “OpenID Connect Basic Client Implementer’s Guide 1.0 - draft 47”, 2023.12.15, (https://openid.net/specs/openid-connect-basic-1_0.html)
50 Internet Engineering Task Force, Request for Comments: 7519, “JSON Web Token (JWT)”, 2015.5, (https://datatracker.ietf.org/doc/html/rfc7519)
51 デジタル庁デジタル社会共通機能グループ、「G ビズ ID 接続システム向けガイドライン 1.9 版」、2023.11.21、p.32
52 総務省、「令和 5 年版 情報通信白書」、2023.7、pp.17-20
53 PwC、「求められる次世代のデジタルアイデンティティ管理モデル SSI と実現手段としての DID」、2023.9.1、(https://www.pwc.com/jp/ja/knowledge/column/disruptive-technology-insights/disruptive-technology-insight13.html)
54 総務省、「令和 5 年版 情報通信白書」、2023.7、pp.20-29
55 European Commission, “Why we need a Digital Single Market, European Union.”, 2016.3.25, p.1

56 THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, 2016.4.27

57 THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)”, 2022.9.14

58 THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)”, 2022.9.14

59 Microsoft, “Decentralized Identity Solution | Microsoft Security”, (https://www.microsoft.com/en-us/security/business/solutions/decentralized-identity)

60 Life With Alacrity, “The Path to Self-Sovereign Identity”, 2016.4.27, (https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/)

61 Sovrin Foundation, “Principles of SSI V3”, 2022,(https://sovrin.org/principles-of-ssi/)

62 .Nat Zone HP, “The Law of Identity in SSI Era by Kim Cameron”, (https://nat.sakimura.org/2020/06/23/the-law-of-identity-in-ssi-era-by-kim-cameron/)

63 The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1”, 2022.3.3, (https://www.w3.org/TR/vc-data-model/)

64 The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1, Figure 1 The roles and information flows forming the basis for this specification.”, 2022.3.3, (https://www.w3.org/TR/vc-data-model/)

65 The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1, section 2. Terminology”, 2022.3.3, (https://www.w3.org/TR/vc-data-model/#terminology)

66 The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1, section 1.2 Ecosystem Overview”, 2022.3.3, (https://www.w3.org/TR/vc-data-model/#ecosystem-overview)

67 The World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0”, 2022.7.19, (https://www.w3.org/TR/did-core/)

68 The World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0, Figure 2 Overview of DID architecture and the relationship of the basic components.”, 2022.7.19, (https://www.w3.org/TR/did-core/)

69 The World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0, section 5. Core Properties”, 2022.7.19, (https://www.w3.org/TR/did-core/#core-properties)

70 The World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0, Figure 1 A simple example of a decentralized identifier (DID)”, 2022.7.19,(https://www.w3.org/TR/did-core/)

71 The World Wide Web Consortium, “Decentralized Identifiers (DIDs) v1.0, section 1.1 A Simple Example”, 2022.7.19, (https://www.w3.org/TR/did-core/#a-simple-example)

72 The World Wide Web Consortium, “DID Specification Registries, section 14. DID Methods”, 2023.9.11, (https://www.w3.org/TR/did-spec-registries/#did-methods)

73 株式会社野村総合研究所、「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 補足資料【公表版】」、2021.3、pp.249-250、(https://www.fsa.go.jp/policy/bgin/ResearchPaper_NRI_ja.pdf)

74 内閣官房デジタル市場競争会議、「モバイル・エコシステムに関する競争評価 最終報告書」、2023.6.16, pp.6-23、(https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai7/siryou2s.pdf)

75 国立印刷局 CBDC 研究会、「中央銀行デジタル通貨（CBDC）に関するレポート（令和 4 年度）」、2023.5、pp.38-44、(https://www.npb.go.jp/ja/guide/security/uploads/202306_cbdc.pdf)

76 株式会社野村総合研究所・NRI セキュアテクノロジーズ株式会社・株式会社ジェイシービー、「デジタルアイデンティティ ～自己主権型/分散型アイデンティティ～」、2019.11、p.8、(https://www.nri.com/-/media/Corporate/jp/Files/PDF/service/ips/technology_1.pdf)

77 株式会社 NTT データ経営研究所、「Trusted Web 共同開発支援事業に係る調査研究 報告書別紙 Trusted Web に係る国際標準化動向調査報告資料」、2023.3.23、pp.9-77、(https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/003_report_intenational_standard.pdf)

78 金融庁、「犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法に関する Q&A」、2023.6.23、(https://www.fsa.go.jp/common/law/guide/kakunin-qa.html)

5　おわりに

日本国内における CBDC に係る取組については、財務省が制度設計の大枠の整理に向けて有識者会議の議論を取りまとめたところであり、日本銀行が技術的な実現可能性の検証や民間事業者の技術や知見を活用しながらの議論を進めている等、確実に検討が進められている。

海外の取組に目を向けると、欧州や英国の中央銀行は、CBDC の基本的な考え方を示しつつ、設計の具体化に向けて、市場関係者や国民からの意見を聴取する取組等を実施している。

国内外における検討内容は共通する部分も多い。CBDC の設計においては、技術的な進展も踏まえつつ、中央銀行と仲介機関の役割分担を明確化することや誰にでも利用しやすいこと等を基本的な考え方として示し、セキュリティの確保やプライバシー保護等を具備すべき要件として挙げている。加えて、法的な課題についても検討がなされている状況にある。また、通貨は国家に対する信頼・信用に基づき利用されることから、市中協議を行うなど CBDC に関して社会に受け入れられるように利用者である国民を意識して取り組んでいると考えられる。

このような社会環境を踏まえ、国立印刷局 CBDC 研究会では、デジタル社会形成における技術的なトピックスとして、サイバー空間上の取引等において必要な本人確認に焦点を当て、「デジタルアイデンティティ管理」に関する新たな取組を整理した。

本稿では、非対面の環境下における取引相手の信頼性を担保する仕組みについて調査した。この中で、ユーザーが特定のサービス事業者に依存せずに自身の情報を管理する仕組みである「分散/自己主権型アイデンティティ」が実現することによって、取引がより安全で信頼性が高くなる可能性があることを示した。一方で、現在はその仕組みを機能させるための技術である「検証可能なクレデンシャル」や「分散型識別子」についての技術開発や標準化の検討が進められており、技術自体の信頼性の向上や、複数の異なる技術間の相互運用性の確保といった課題があることも示した。

今後、CBDC の検討が進む中で、取引時における本人確認の方法についても議論が進んでいくとみられる。現時点では、少なくともこうしたアイデンティティ管理に関連する技術の検討状況は継続的に注視する必要があると考える。

いずれにせよ、本稿で整理した内容が、CBDC に限らず今後のデジタル社会を形成する仕組みを理解するための一助となることを期待する。