中央銀行デジタル通貨（CBDC）に関するレポート

（令和６年度）

2025 年４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7年1月末日時点の調査・研究成果（3 章においては 3 月末日時点）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

AAMVA	American Association of Motor Vehicle Administrators	EAA	Electronic Attestation of Attributes
AML/CFT	Anti Money Laundering/ Countering the Financing of Terrorism	EAL	Evaluation Assurance Level
API	Application Programming Interface	ECB	European Central Bank
ARF	the Architecture and Reference Framework	eIDAS	Electronic Identification, Authentication and Trust Services
ASEAN	Association of South-Ease Asian Nations	EMV	Europay, Mastercard, and Visa
ATM	Automatic Teller Machine	EOA	Externally Owned Account
B2B	Business To Business	ERC	Ethereum Request for Comments
BIP	Bitcoin Improvement Proposals	ERPB	Euro Retail Payment Board
BIS	Bank for International Settlements	EU	European Union
BLE	Bluetooth Low Energy	EUDIW	EU Digital Identity Wallet
BOC	Bank Of Canada	EWC	EU Digital Identity Wallet Consortium
BOE	Bank of England	Expo	exposition
BTC	Bitcoin	FATF	Financial Action Task Force
CBDC	Central Bank Digital Currency	FBI	Federal Bureau of Investigation
CBOR	Concise Binary Object Representation	FRB	The Federal Reserve Board
CeFi	Centralized Finance	FSC	Financial Services Commission
CPM	Consumer-Preseted Mode	H.R.	House of Representatives
DAO	Decentralized Autonomous Organization	HCE	Host Card Emulation
DC3	Department of Defense Cyber Crime Center	HD	Hierarchical Deterministic
DeFi	Decentralized Finance	HSM	Hardware Secure Module
DESP	Digital Euro Service Platform	IB	Internet Banking
DIW	Digital Identity Wallet	ICAO	International Civil Aviation Organization
DLT	Distributed ledger technology	IdP	Identity Provider
DMA	Digital Markets Act	IEC	International Electrotechnical Commission
DS	Document Signer	IETF	Internet Engineering Task Force
DTC	Digital Travel Credential	IMF	International Monetary Fund

頭字語、略語　一覧

ISO	International Organization for Standardization	PSD2	The revised Payment Services Directive
ITU	International Telecommunication Union	PSP	Payment Service Provider
JSON	The JavaScript Object Notation	RBA	Reserve Bank of Australia
JWT	JSON Web Token	RDG	Rulebook Development Group
KYC	Know Your Customer	RoT	Root of Trust
LUK	Limited Use Key	RP	Relying Party
mDL	Mobile Driver's License	SBT	Soul-Bound Token
MIT	Massachusetts Institute of Technology	SD-JWT	Selective Disclosure JSON Web Token
MOU	Memorandum Of Understanding	SDK	Software Development Kit
MPC	Multi Party Computation	SE	Secure Element
MPM	Merchant-Presented Mode	SEP	Secure Enclave Processor
MSIT	Ministry of Science and ICT	SG	Sub-Group
MSO	Mobile Security Object	SIM	Subscriber Identity Module
NFC	Near Field Communication	SMS	Short Message Service
NFCIP	NFC Interface Protocol	SNS	Social Networking Service
NFT	Non Fungible Token	SSI	Self-Sovereign Identity
NISC	National center of Incident readiness and Strategy For Cybersecurity	TEE	Trusted Execution Environment
OWF	OpenWallet Foundation	TLP	Trusted List Provider
P2P	Peer-to-Peer	UDK	Unique Derivation Key
PArSEC	Parallelized Architecture for Scalably Executing smart Contracts	UI	User Interface
PETs	Privacy-Enhancing Technologies	UICC	Universal Integrated Circuit Card
PID	Person Identification Data	UX	User Experience
PIN	Personal Identification Number	VC	Verifiable Credentials
PIP	Payments Interface Provider	VICAL	Verified Issuer Certificate Authority List
PoC	Proof of Concept	W3C	World Wide Web Consortium
POS	Point of Sale	WG	Working Group

1　はじめに

中央銀行デジタル通貨（CBDC）については、2019 年に Facebook 社（現 Meta 社）が発表したグローバルステーブルコイン構想や、中国のデジタル人民元の進展を契機に、各国で検討が開始されており、現在では、バハマ、ナイジェリア、ジャマイカ、東カリブ通貨連合の 4 つの国・地域で CBDC が実際に発行されている。

日本では、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 年以降、実証実験を行っている。また、財務省も CBDC の「制度設計の大枠の整理」に向けて、「CBDC に関する関係府省庁・日本銀行連絡会議」を設置し、議論を行っているところである。

国立印刷局 CBDC 研究会では、これらの国内外で進む CBDC の検討動向を調査・整理するとともに、CBDC に必要となり得る技術等について継続的に調査・研究を行っている。

本レポートはこれまでの調査結果を取りまとめたものである。

本レポートの第 2 章では、まず、海外のリテール CBDC の検討動向に加え、特に令和 6 年度に進展のあった欧州や英国の取組を紹介した。

欧州では、欧州中央銀行（ECB）がデジタルユーロの導入を検討しており、2023 年 11 月から 2 年間の準備フェーズが開始され、これまでに 2 回の進捗報告書が公表された。また、デジタルユーロ決済を標準化するためのルールブックに関する報告書についても 2024 年に公表されている。準備フェーズは 2025 年 10 月末に終了する予定であり、その後は必要に応じて Next Step に進むとされている。

英国は、デジタルポンドの設計フェーズの一環として、2024 年 5 月に「POS 端末における概念実証」報告書を公表した。また、専門家等の視点から検討している「テクノロジーフォーラム」の進捗について、2024 年 8 月に公表している。加えて、2025 年 1 月には設計フェーズに関する最新の進捗報告書を公表しており、その中で英国においては、現在の設計フェーズを数年間継続することが示されている。

その他の国における動向としては、まず、中国において 2019 年よりパイロット実験が開始され、地域を拡大しながら進められている。令和 6 年度においては、ユースケースの取組やカード型ハードウォレットの販売についての報道がなされたところである。

米国では 2022 年にバイデン大統領が CBDC 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したが、2025 年 1 月にトランプ大統領がデジタル資産に関する大統領令に署名し、CBDC に関する取組が禁止された。

そのほか、オーストラリアやカナダなど一部の国ではリテール CBDC の取組に対して縮小する動きがあるほか、リテール CBDC ではなく預金をトークン化して用いる試みも見られる。

日本においては、日本銀行が 2023 年 4 月からパイロット実験における実験用システムの構築・検証や CBDC フォーラムでの検討を進めている。加えて、財務省は 2024 年より「CBDC に関する関係府省庁・日本銀行連絡会議」を設置し、同年 4 月に中間整理を行ったところである。また、同年 10 月からは連絡会議の下に幹事会を設置し、法律面やデータの取扱いに関するより実務的な議論を行っている。

本レポートの第 3 章では、これらの国内外の動向のほか、CBDC に関連する技術の一つとして、「デジタルウォレット」をターゲットとし、その機能・特徴、仕組み、利用方法について調査し、取りまとめた。

デジタルウォレットはその役割・機能面から、本人確認を行うトラストサービスとしての「デジタルアイデンティティウォレット（DIW）」、キャッシュレス決済手段としての「決済用ウォレット」、さらに暗号資産を扱う web3 サービスのインターフェースとしての「web3 ウォレット」の大きく 3 種類に分類される。本レポートでは、これらの 3 種類のウォレットについて、そのユースケースと技術的側面について解説した。

まず、トラストサービスを行う DIW については、将来のデジタルサービスの連携基盤として期待されることから、技術規格等についても詳細に解説している。現在は、デジタルサービスを提供する事業者が本人の証明書情報を確認し、サービスを提供しているが、一方で、このデジタルサービス提供者が個人情報を寡占するといった問題点もある。この DIW を利用することで、本人の資格情報等の発行者と、デジタルサービス提供者を分けることが可能となり、ユーザ主体のプライバシー保護に資するとされる。このため、この仕組みを利用したモバイル運転免許書（mDL）や欧州における EU デジタルアイデンティティウォレット（EUDIW）の取組が進められており、日本でもスマートフォンへのマイナンバーカード機能の搭載の取組が進められている。

なお、EUDIW は、デジタルユーロ規則案において、希望するユーザがデジタルユーロ決済における「本人確認」、「決済の承認」に利用できるようにすることが提唱されている。

次にキャッシュレス決済手段として一般化している決済用ウォレットについては、スマホを利用した非接触決済や QR コードを読み取る方式などの様々な

方式の特徴やメリット・デメリットを整理した。

さらに、ブロックチェーン上の暗号資産やその他のサービスを利用するための web3 ウォレットについては、「秘密鍵」の管理・保管方法について整理し解説した。

参考付録には、毎年調査対象として報告してきた「中国人民銀行の特許出願状況について」、「暗号資産等の事件・攻撃等」のほか、日本における「プライバシー保護と AML/CFT の両立に関する動向について」を掲載した。

これらのうち、「中国人民銀行の特許出願状況について」は、公表情報の少ない中国の CBDC の取組状況に対して、特許の出願状況から分析を試みたものであり、最近の出願状況を踏まえて分析結果を更新した。

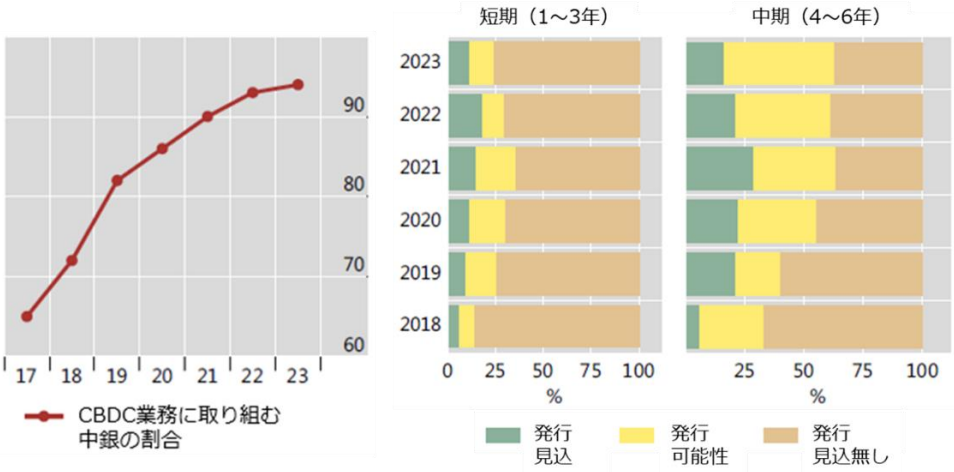
本レポートが、CBDC に関する国内外の動向や関連技術への理解の一助となれば幸いである。

2　環境分析

2.1　海外の動向

国際決済銀行（BIS）は例年、各国中央銀行に対して中央銀行デジタル通貨（CBDC: Central Bank Digital Currency）の検討状況の調査を実施している。2023 年の調査[1]（調査期間：2023 年 10 月～2024 年 1 月）では、86 行から回答を得ており、CBDC を検討中の中央銀行の割合は、2022 年の 93%から 94%に増加している。しかし、全体的な傾向として、発行時期は 2022 年の見通しよりも遅れる見込みとしている（図 2.1）。また、当該調査では、CBDC を発行している国・地域はバハマ、ジャマイカ、ナイジェリア、東カリブ通貨連合の 4 か所とされている。

BIS は、各国の置かれた経済取引や決済を取り巻く環境等が大きく影響するため、先進国と新興国に分けて発行のモチベーションに関する回答を整理している。その結果、先進国と新興国の両方が「（国内の）決済の効率化」や「決済の安全性/頑健性」を目的にしていることが示されているが、「金融包摂」については、モチベーションの一つとされるものの、特に新興国においてその重要性が高いことが示されている。



参考：Alberto Di Iorio, Anneke Kosse and Ilaria Mattei, “Embracing diversity, advancing together – results of the 2023 BIS survey on central bank digital currencies and crypto”, 2024.6, p.4 を基に作成

図 2.1　各国中央銀行のＣＢＤＣの検討状況及び発行の可能性

CBDC の活用可能性を評価するためのグループ（BIS と主要 7 中銀）は、2024 年 11 月、ワークストリームを設置して行ってきた議論をまとめた報告書「中央銀行デジタル通貨：リテール CBDC の法的側面[2]」及び「中央銀行デジタル通貨：システム設計[3]」を公表した。

法的側面の報告書では、CBDC の発行を検討する法域において、最低でも以下の 4 点を確認する必要性が示されている。

① リテール CBDC の発行とその後の利用に当たっての首尾一貫した法的枠組みの提供
② リスク管理
③ プライバシーとマネー・ローンダリング/テロ資金供与対策（AML/CFT）に関する期待と義務を果たすこと
④ クロスボーダー利用が政策目的に含まれる場合、利用促進のためにも、法制度が適切に更新されていること

システム設計の報告書では、リテール CBDC の研究と調査において考慮すべき課題の多くは、リテール CBDC 特有のものでも新規性のあるものでもないとした上で、可能であれば既存の技術、標準、事例を活用しても良いのではないかと示している。同時に、中央銀行は CBDC 設計において新たな技術や戦略を取ることも選択できるが、プライバシー強化技術（PETs）のような一部の新たな技術は、まだ利用が現実的ではない可能性があると結論付けている。

そのほかにも、国際通貨基金（IMF）は中央銀行や財務省の政策立案者・専門家向けのリファレンスガイドとして CBDC ハンドブック[4]の作成を行っており、2026 年までに約 20 章を提供するとして検討を行っている。

2.1.1 米国

米国では、米国連邦準備制度理事会（FRB）が 2022 年 1 月に CBDC に関する報告書を公表した。2022 年 3 月には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し、2022 年 9 月には米国財務省、ホワイトハウス科学技術政策局が CBDC に関する報告書を公表した。これに加えて、米国版 CBDC のための政策目標も策定している。

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「プロジェクトハミルトン」として CBDC の研究を 2020 年から開始し、2022 年 12 月にプロジェクトを終了している[5]。

これらの取組が進められてきたものの、現在、米国内では、CBDC が政府の監視ツールとなることを懸念する声が広まり、CBDC 導入に対する警戒論が強まっているとされる。そのため、CBDC が国民監視に使用されることを阻止する法案（H.R.5403 CBDC Anti-Surveillance State Act）が 2023 年 9 月に米下院金融委員会によって承認され、2024 年 5 月と 6 月には米国下院と上院でそれぞれ可決された[6]。

また、FRB のウォラー総裁も 2024 年 11 月の講演において CBDC の必要性について否定的な見解を示した[7]ほか、ドナルド・トランプ大統領が 2025 年 1 月 23 日にデジタル資産に関する大統領令[8]に署名し、その中で CBDC に関する取組を禁止した。大統領令には「米国の管轄区域内での CBDC の設立、

発行、又は促進するためのいかなる取組も禁止する」、「米国の管轄区域内の CBDC の創設に関連する機関で進行中の計画は直ちに終了する」と記載されている（表 2.1）。

表 2.1　米国における状況

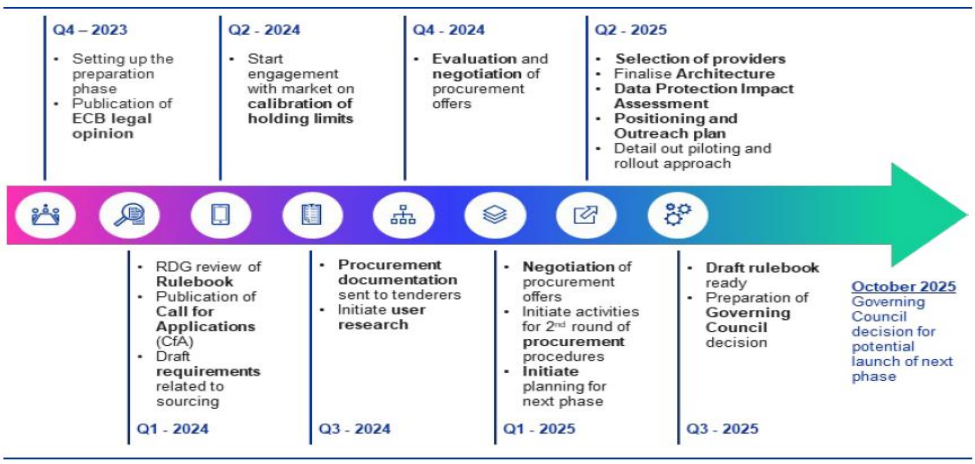
2022 年 1 月	FRB“Money and Payments: The U.S. Dollar in the Age of Digital Transformation”を公表
2022 年 3 月	バイデン大統領が大統領令に署名
2022 年 9 月	米国財務省“The Future of Money and Payments”公表
	ホワイトハウス“FACT SHEET : White House Releases First-Ever Comprehensive Framework for Development of Digital Assets”公表
2022 年 12 月	ボストン連銀と 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（Parallelized Architecture for Scalably Executing smart Contracts）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 Anti-Surveillance State Act を承認
2024 年 5 月	米下院 CBDC Anti Surveillance State Act を可決
2025 年 1 月	トランプ大統領が大統領令に署名（CBDC に関する取組の禁止）

参考：公表情報を基に作成

2.1.2　欧州

欧州中央銀行（ECB）は、2021 年 10 月からデジタルユーロに関する「調査フェーズ」を開始し、概念定義や技術的調査、設計提案の検討を実施した。2023 年 11 月からは、2 年間の「準備フェーズ」に移行し、2024 年 6 月と 12 月に進捗報告書（Progress Report）を公表した。準備フェーズでは、デジタルユーロ・スキームのルールブック（デジタルユーロのルール・基準・手順等を定めるもの）の策定も並行して進められ、2024 年 1 月、9 月にその途中経過が報告されている。

なお、準備フェーズ後に次のフェーズへ移行するかどうかは、2025 年 10 月に決定される予定である（図 2.2）。



出典：ECB, “Progress on the preparation phase of a digital euro, Second progress report”, 2024.12, p.2

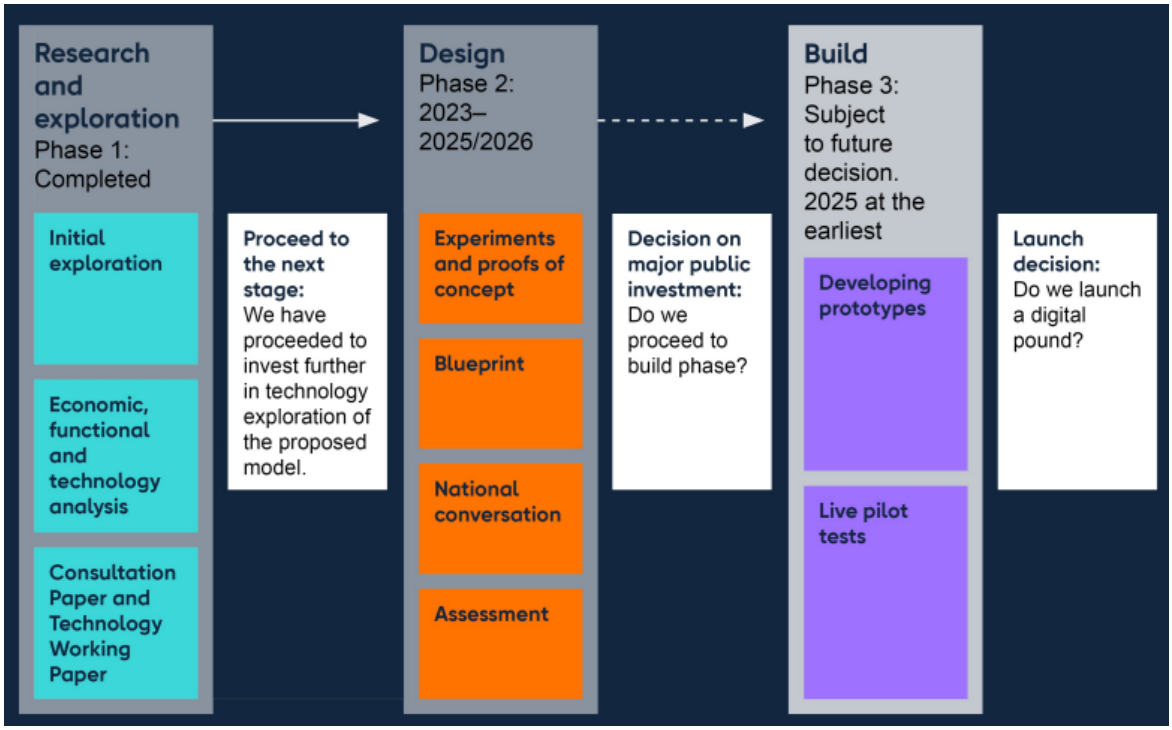
図 2.2　デジタルユーロプロジェクトのタイムライン

2.1.3　英国

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 であるデジタルポンド（digital pound）について、「コンサルテーションペーパー（The digital pound: a new form of money for household and business?）」及び「テクノロジーワーキングペーパー（The digital pound: Technology Working Paper）」を公表した。それらの文書は、市中協議を目的としたもので、デジタルポンドの目的や基本的特性、構築時のシステム面の基本的考え方等が示されている。

その後、2024 年 1 月に市中協議の結果と、結果を踏まえた方針についての報告書を公表した。当該報告書では、早ければ 2025 年に次のフェーズへ移行することが示されているが、2025 年 1 月に公表されたデジタルポンドの最新進捗情報に関する報告書（Progress Update: The digital pound and payments landscape[9]）では、設計フェーズを数年間継続する旨が示されている。

また、英国においては、BOE と英国財務省は、2021 年からデジタルポンドの技術的側面を議論する「CBDC Technology Forum」と、ユースケース等を議論する「CBDC Engagement Forum」を設置しているが、2024 年にはデジタルポンドの設計について学術的観点からの助言を得るため、「CBDC Academic Advisory Group」を設置した。



出典：BOE, “Response to the digital pound Technology Working Paper”, 2024.1.25, p.29

図 2.3　デジタルポンドプロジェクトのロードマップ

2.1.4　中国

中国は、2019 年末からデジタル人民元（e-CNY）のパイロット実験を開始し、検証内容や実施地域を拡大しながら進めている。この実験では、公務員の賃金を e-CNY で支給する施策や国慶節期間中に e-CNY アプリで利用可能な割引クーポン発行等、利用機会を増やすための施策が行われたとされている[10]。

また、2023 年 9 月には、海外から中国への訪問者に向けに、海外で発行されたクレジットカードを通じて e-CNY アプリに e-CNY をチャージする「プレチャージ」機能が追加された。2024 年 11 月には、第 18 回深圳国際金融博覧会において、タッチ決済だけでなく、ウォレット残高や QR コードの表示機能を有する小型ディスプレイを搭載したカード型のハードウォレットを公表している[11]。

そのほか、2024 年には香港金融管理局と中国人民銀行が e-CNY の越境決済の試験範囲を拡大し、香港市民が e-CNY のウォレットを利用できるようになったとの報道がある。

こうした中、中国人民銀行の幹部[12]によると、e-CNY の累計取引額は 2024 年 6 月末の時点で 7 兆元（約 155 兆円[i]）に達したとの発言があった。このように、中国人民銀行は、国内外で利用可能な e-CNY の検討を広く進めているとされるが、発行に向けた取組の公式情報が、2024 年は直近数年と比して減少している。

2.1.5　その他の国々

リテール CBDC の検討については、前述の国々以外でも進められており（表 2.2）、2024 年に特徴的な動きのあった国を紹介する。

表 2.2　各国のリテールＣＢＤＣの検討状況

国名	ＣＢＤＣ名称	進捗
ブラジル	Drex	パイロット実験フェーズ 2（2024 年 6 月～）
インド	Digital rupee	パイロット実験（2022 年 12 月～）
ロシア	Digital ruble	パイロット実験（2023 年 8 月～）
香港	e-HKD	パイロット実験フェーズ 2（2024 年 3 月～）
韓国		実証実験

参考：各国の公表情報を基に作成

[i] 2024 年 6 月 30 日時点の為替レート（約 22.12 円/元）を基に換算

ブラジルについては、2024 年 6 月にパイロット実験の第 2 フェーズの開始を公表した。ブラジルの金融機関も参加し、2025 年上半期末までにスマートコントラクトの実装の検証を行うとみられる。インドについては、2022 年末までにデジタルルピー（Digital rupee）のパイロット実験を開始しており、2024 年 8 月の時点で利用者数は 500 万人、参加銀行は 16 行とされている[13]。ロシアでは、2025 年 7 月 1 日までに大手銀行が顧客にデジタルルーブル（Digital ruble）での取引機会を提供するよう、ロシア中央銀行が 2024 年 9 月に、関連法の改正案[14]をロシア財務省へ提出している。大手銀行以外のユニバーサルライセンス[ii]を保有する銀行とそれ以外の銀行に対しては、システム調整の猶予としてそれぞれ 2026 年 7 月 1 日、2027 年 7 月 1 日までの期限を提案している。

そのほか、海外においては CBDC の検討と合わせて預金をトークン化する方法も模索されている。米国法の下においては、トークンであっても預金であれば、既存の預金の法的性質等をそのまま適用できるであろうとの指摘もあるとされるなど、既存の規制や制度と親和的である可能性がある[15]。香港では 2024 年 3 月に e-HKD のパイロットプログラムのフェーズ 2 開始を公表[16]し、プロジェクトの範囲を CBDC からトークン化された預金まで拡大している。その中で、11 の企業グループがトークン化された資産の決済、プログラマビリティ、オフライン決済等のユースケースを模索している。韓国でも、韓国中央銀行が 2024 年 11 月に、ホールセール CBDC と預金トークンを活用した実証実験に関する基本合意書（MOU）を科学技術情報通信部（MSIT）及び金融委員会（FSC）と締結した[17]。そして、このプロジェクトを推進するため、金融委員会は 7 つの国内銀行に預金トークン発行業務を許可している。

なお、CBDC の検討が進む一方で、一部の中央銀行ではリテール CBDC の研究を縮小する動きもみられる。例えば、オーストラリア準備銀行（RBA）やカナダ銀行（BOC）は、2024 年 9 月に、現時点でリテール CBDC を発行する公共政策上の根拠が無い等の理由から、研究を縮小することを公表している[18,19]。ただし、両行とも CBDC に関する検討を打ち切ったわけではなく、RBA はトークン化されたマネーと新しい決済インフラを通じて、ホールセール市場の効率性、透明性、レジリエンスを向上させることを目的とした「Project Acacia」を立ち上げている。また、BOC も、より広範な決済システムの研究と政策の検討にシフトした上で、世界的なリテール CBDC の検討状況に注視することを示している。

[ii] ユニバーサルライセンス保有銀行は、自己資本金が 10 億ルーブル以上であることを条件として、全ての銀行業務、および海外での現地法人や支店の開設が認められる。（一般財団法人ゆうちょ財団 HP より（https://www.yu-cho-f.jp/wp-content/uploads/Russia-1.pdf））

2.2　欧州の「準備フェーズ」の進捗状況等

2.2.1　準備フェーズ進捗報告書

ECB は 2023 年 11 月よりデジタルユーロの準備フェーズを開始している。このフェーズの目的は、これまでの調査フェーズの結果を基にデジタルユーロ発行の可能性に向けた基盤を構築することとして、最初の 2 年間で①ルールブックの策定、②プラットフォームインフラの開発事業者の選定、③更なる実証実験等を行うとしている。その後、次のフェーズに進むかについて判断するとしている。2024 年は、準備フェーズの進捗報告書が 6 月[20]と 12 月[21]の 2 回公表されている。

(1)　進捗報告書（6 月）

6 月の進捗報告書では、プライバシー保護の考え方、オフライン決済、立法協議に必要な技術的な専門知識等についての進捗状況が示されている。

プライバシー保護の考え方については、市中協議の結果、欧州市民はプライバシーとデータ保護がデジタルユーロにおけるもっとも重要な要素とみなしており、ユーロシステム（ユーロ非参加国中央銀行を除いた ECB 及びユーロ圏中央銀行）はプロジェクトのあらゆる段階でこれらの側面を優先してきたとしている。

このため、オンライン決済では、プライバシー保護のためデジタルユーロの発行者であり支払インフラプロバイダであるユーロシステム自体が、取引と特定の個人に直接結び付けられないように実装されるとしている。加えて、デジタルユーロへの信頼を確保するためにも、プライバシー保護を実施することで不正行為からユーザを守ることも必要であるとしている。

さらに、個人間や個人と店舗間の決済において、ユーザに現金と同程度のプライバシーを提供するオフライン決済機能を設計に含めている。オフライン決済機能とは、インターネット経由又は ATM で事前にデジタルユーロ口座へ入金しておけば、至近距離やネットワークが限られている場所、停電時等、インターネット接続がなくても支払いが可能になる機能を指す。

オフライン決済では、取引に参加する 2 つのオフライン端末間で認証されるため、端末には取引履歴が残るが、ネットワーク上で中央システムやサードパーティを介さずに相手先の端末へ送信されることから、プライバシーが保護される。このオフライン機能をスマートフォンで利用する場合、近距離無線通信（NFC: Near Field Communication）アンテナとセキュアエレメント（SE: Secure Element）へのアクセスが条件となるため、デジタルユーロへの実装については、最終的には法律によって定められる要件において、機器メーカーと電子通信サービスプロバイダが SE へのアクセスを許可す

るかどうかによるとしている。また、その他のオフラインの利用手段として、スマートカード等の利用についても調査している。

そのほか、ECB は欧州議会と欧州連合理事会に対し、立法協議に必要となる技術的な専門知識を提供している。進捗報告書では、ユーザごとに複数の口座を開設することの実現可能性と影響、報酬モデル、ユーザエクスペリエンス（UX: User Experience）の考え方について示している。複数の口座の開設に関しては、2024 年 3 月に公表した技術的な分析結果報告書[22]を示し、利用者が複数の口座を持ち、個別の保有限度額を設定することは技術的に実現可能であるが、単一口座と複数口座では、導入の容易性、プライバシーへの影響、共有デジタルユーロ口座、ポーティング[iii]等の各シナリオにおいて、可能な内容が異なっていること。また、UX や決済サービスプロバイダ（PSP: Payment Service Provider）の技術的・運用上の実装に関して、トレードオフが必要になるとしている。

(2) 進捗報告書（12 月）

12 月の進捗報告書では、主にユーザや市場参加者とのコミュニケーションに関する進捗状況が示されている。

ECB は、デジタルユーロの価値を高めるために、2024 年 9 月からユーザの嗜好調査を開始することから専門のプロバイダと契約した。この調査では、重点分野として以下の 3 点を定めており、結果の公表は、2025 年半ばに予定されている。

① 利用可能性のあるユーザ層とニーズを明確にするための一般的なセグメンテーション分析
② 保有限度額に関するユーザの嗜好
③ 社会的弱者や小規模加盟店を対象とした詳細な調査

そのほかにも、市場参加者との技術的な実験について、イノベーションパートナーシップを通じて民間企業とのエンゲージメントを促進し、潜在的な革新的ユースケースを開発することを目標としている。2024 年 10 月には、B2B（Business To Business）決済に関するオープンフォーラムを開催し、課題やニーズについて意見を集めた。この取組と並行して、ECB は条件付決済を促進するための要件について共通の理解を得るため、PSP 及び加盟店と概念と技術に関する共同実験活動を開始している。2024 年 10 月に募集要項が公表され、2024 年度末まで条件付決済やその他のテーマ、ユース

[iii] ユーザが別の PSP に変更する際、口座番号を引き継ぐ機能を指す。（ECB, “Progress on the preparation phase of a digital euro - First progress report”, p.11 より（https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.deprp202406.en.pdf））

ケースを調査するパートナーを募集するとしている。作業は 2025 年前半に実施され、結果の報告書は 2025 年 7 月の公開が予定されている。

そのほか、デジタルユーロの設計に関して、保有制限についてユーロ小売決済委員会（ERPB）の加盟協会との意見共有や、オフラインにおけるモバイルデバイスの SE に関しての技術サービスプロバイダとの技術協議の実施状況、欧州の共同立法者との意見交換状況等について示している。

ECB は次のステップとして、ERPB との議論を継続し、ユーザ調査を引き続き行うほか、2025 年にデジタルユーロ・サービスプラットフォーム（DESP: Digital Euro Service Platform）のプロバイダ候補を選定するための調達を完了させることを目指している。また、準備フェーズの次回報告書は 2025 年第 2 四半期に公表される予定である旨を示している。

2.2.2 ルールブックの策定

デジタルユーロの準備フェーズにおいては、ルールブックの策定が目的の 1 つとなっている。このルールブックは、デジタルユーロ決済を標準化し、ユーロ圏全体で利用体験と認識が同じになるように、単一のルール、基準、手続を提供するものとしている。ルールブックの策定に関しては、2023 年 1 月に、小売決済に係る団体から推薦された専門家等から構成されるデジタルユーロ・スキームのルールブック作成グループ（RDG: Rulebook Development Group）が設立され、作成が開始されている。

2024 年 1 月には、RDG の作業に関する最新情報（Update on the work of digital euro scheme's Rulebook Development Group[23]）が公表されている。

この時点でのルールブックについては、中間ドラフトであるとし、以下の内容が含まれている。また、今後、セクションが追加されるとしている。

① デジタルユーロの機能モデルと運用モデル
② デジタルユーロの高レベルアーキテクチャ及び技術スキーム要件
③ デジタルユーロ・スキームの遵守モデル

その後、RDG は 2024 年第 1 四半期に中間ドラフトのレビューを終えて、同年 9 月に RDG の作業に関する最新情報[24]として以下のことを報告している。

- ルールブックの第 1 ドラフトのレビューと、ドラフト内容の更なる改善を目的とした約 2,500 件のコメントの概要
- ルールブックの追加セクションのドラフト作成状況と既存セクションの改訂状況

なお、ルールブック作成に当たり、2024 年には新たな RDG のワークストリーム（WS）が追加され、合計で 10 の WS を設置して検討を進めており、

その進捗状況についても紹介されている。各 WS の検討内容は表 2.3 のとおりである。

また、RDG の今後の動きとしては、2025 年第 1 四半期に新たなプログレスレポートの公表が予定されている。

表 2.3　RDG の WS 一覧

WS名		検討目的
[A1]	身元確認と当人認証	エクスペリエンス及びプライバシーの最高基準を確保することを目指し、デジタルユーロのエンドユーザーの識別および認証の要件を定義
[A2]	最低限のUXに関する標準	UXに関する最低基準と要件の提案
[B1]	認証と承認のフレームワーク	適用される認証と承認のフレームワークに関しての提案
[C1]	技術スキーム要件	フロントエンドの技術的インターフェースの開発及びデジタルユーロの非機能標準及び要件の開発
[D1]	リスク管理	「エンドユーザからPSPやDESP」領域におけるリスク管理要件
[F1]	スキームの互換性	デジタルユーロスキームを既存の機能標準および仕様及び他のスキームや支払いインフラストラクチャと互換性を持たせる
[G1-3]	各種フロントエンドに関する実装仕様	デジタルユーロのルールブックの実装仕様策定の支援
[G4]	DESPとPSPのためのバックエンドに関する実装仕様	デジタルユーロのルールブックの実装仕様策定の支援

参考：ECB, “Update on the work of the digital euro scheme’s Rulebook Development Group”, 2024.9, p.15
ECB, “Update on the work of the digital euro scheme’s Rulebook Development Group”, 2024.1, p.25 を基に作成

2.2.3　デジタルユーロに関する立法プロセスの状況

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て、立法案（デジタルユーロ法案等）を提案[25]し、立法プロセスを開始している。この状況を受け、ECB は立法プロセスと並行して、準備フェーズの中で、技術的サポートとして専門知識の提供や意見交換を実施している。

2023 年 6 月の欧州議会選挙とその後の人事プロセスのため、立法案の審議が一時中断されていたが、今後、再開が見込まれている。

なお、デジタルユーロを発行するかどうかの決定は、欧州連合の立法プロセスが完了した後に、欧州連合閣僚理事会によって検討されることになるとされている。

2.3　英国の「設計フェーズ」の検討状況

2.3.1　デジタルポンドの進捗状況報告

BOE は 2025 年 1 月に、デジタルポンドの最新進捗情報に関する報告書（Progress Update: The digital pound and payments landscape [26]）を公表している。

当該報告書は、過去 1 年間の作業をまとめたものであり、2024 年 11 月に公表された「国家決済ビジョン（National Payments Vision [27]）」等に記載された決済の発展状況に関する内容も含まれている。

2024 年 7 月に公表されたディスカッションペーパー（The Bank of England's approach to innovation in money and payments [28]）では、リテール決済における以下の 4 つの政策成果が示され、デジタルポンドのような法定通貨にも適用されるとしている。

① 通貨の単一性、
② イノベーション
③ インフラと広範なエコシステムのレジリエンス
④ 効果的なガバナンスと財源

また、設計フェーズは 4 つのワークストリーム（実験と概念実証、青写真、国民との対話、評価）から構成され、それらの進捗についてもまとめている。なお、報告書内において、設計フェーズは今後数年間継続することも示されている。

本報告書と同時に、設計フェーズで検討している内容をステークホルダーへ伝えるための「デザインノート（Design note- Blueprint framework [29]）」も公開され、青写真のフレームワークの概要が示されている。BOE と英国財務省が整理している 4 つの主要な要素として、①プロダクトビジョンと戦略、②スキームと規制、③テクノロジー、④オペレーションが挙げられている。

青写真は、完成すればデジタルポンドのモデルと設計を示すものとなり、ベネフィットとコストを評価する基礎になるとしている。

2.3.2　POS 端末における概念実証

BOE はデジタルポンドの設計フェーズの一環として、実験や概念実証（PoC: Proof of Concept）を実施している。2024 年 5 月には、英国内で稼働している既存の POS 端末、モバイル POS 端末、ソフトウェア POS 端末の 3 種類の POS 端末で、デジタルポンド決済の技術的な実現可能性について評価した「POS 端末における概念実証（Point-of -sale proof of concept）[30]」報告書を公表している。

この概念実証では各端末に対して 3 つの異なる決済方法を評価している。

① パススルー（PASSTHRU）：加盟店の決済インターフェースプロバイダ（PIP: Payments Interface Provider）を経由して BoE API（Application Programming Interface）へ支払要求を行う方式
② ダイレクト（DIRECT）：加盟店の PIP をバイパスし、BoE API へ直接支払要求を行う方式
③ ピア（PEER）：ネットワークに接続されていない 2 つのデバイス間で決済する方式（オフライン決済）

結果として、パススルーとダイレクト方式は、全ての POS 端末において決済が可能であったとしている。しかし、ピア方式では、オフライン決済の実証はできたものの、ソフトウェア開発キット（SDK: Software Development Kit）へのアクセスが制限されていたため、モバイル POS 端末への実装ができなかったとし、このため、ピア方式を設計に組み込む場合には、POS 端末のソフトウェアを修正又は更新する必要があることが示されたとしている。

2.3.3 CBDC Technology Forum の進捗状況

BOE は 2021 年 9 月に、デジタルポンドに使用する可能性のある技術について、専門家や様々な視点から検討する場として CBDC テクノロジーフォーラム（CBDC Technology Forum）を設立している。このフォーラムには、公募により選出された金融機関、大学、FinTech 企業、インフラプロバイダ、テクノロジー企業等が参加している。

2024 年 8 月には、これまでの検討結果をまとめた第 11 回から第 13 回までの議事概要が公表されている。

第 11 回[31]及び第 12 回[32]では、フォーラム内に設置された 4 つのサブグループ（SG1～SG4）が検討した結果と BOE への提言が整理され、第 13 回[33]では、結果報告と提言に対して BOE からフィードバックを実施している。

SG1：プライバシーに関する技術的オプションとエイリアスサービスの設計
SG2：PIP 間のコミュニケーションモデル
SG3：コア台帳技術
SG4：イノベーションのためのプラットフォームを提供するための要件

また、BOE は各 SG からの分散型金融のユースケースや相互運用性等の実験提案を受けており、これらの提案がスマートコントラクト等の機能をサポートする新たなアーキテクチャが生まれる可能性があるとし、これらの実験を実施する意思を示している。

2.4　国内の動向

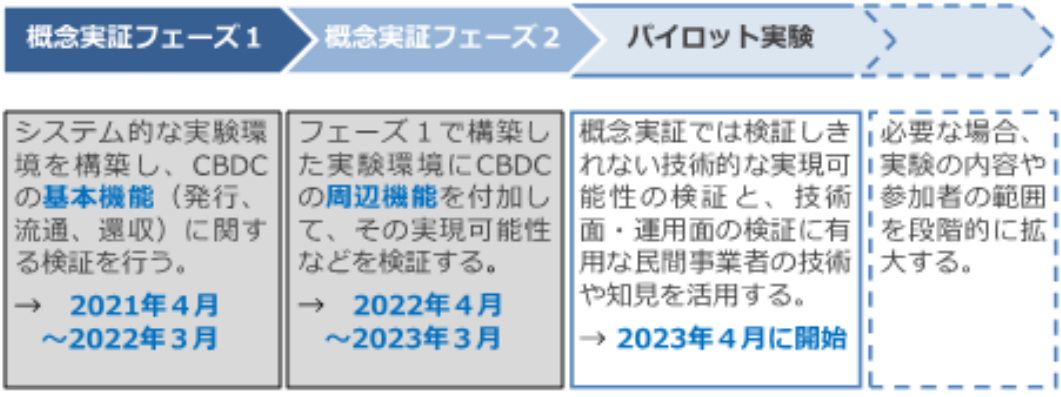
日本の CBDC に関する取組は、2020 年 7 月に閣議決定された「経済財政運営と改革の基本方針（骨太の方針）2020」に初めて記載された。それ以来、日本銀行における実証実験や、財務省における有識者会議等による議論が進められてきている。

2024 年 6 月に閣議決定された「骨太の方針 2024[34]」においても、「CBDC について、政府・日本銀行は、諸外国の動向等も踏まえ、中間整理に基づき検討を深め、制度設計の大枠の整理として、主要論点の基本的な考え方や選択肢等を明らかにする。その後、発行の実現可能性や法制面の検討を進める。」とされ、継続的に検討を進めていくことが示されている。

2.4.1　日本銀行の取組

日本銀行は 2020 年に「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」を公表した。そのなかで、「現時点では CBDC を発行する計画はないが、今後の様々な環境変化に的確に対応できるよう、しっかり準備しておくことが重要」とし、実証実験を通じて検討する方針を出している。

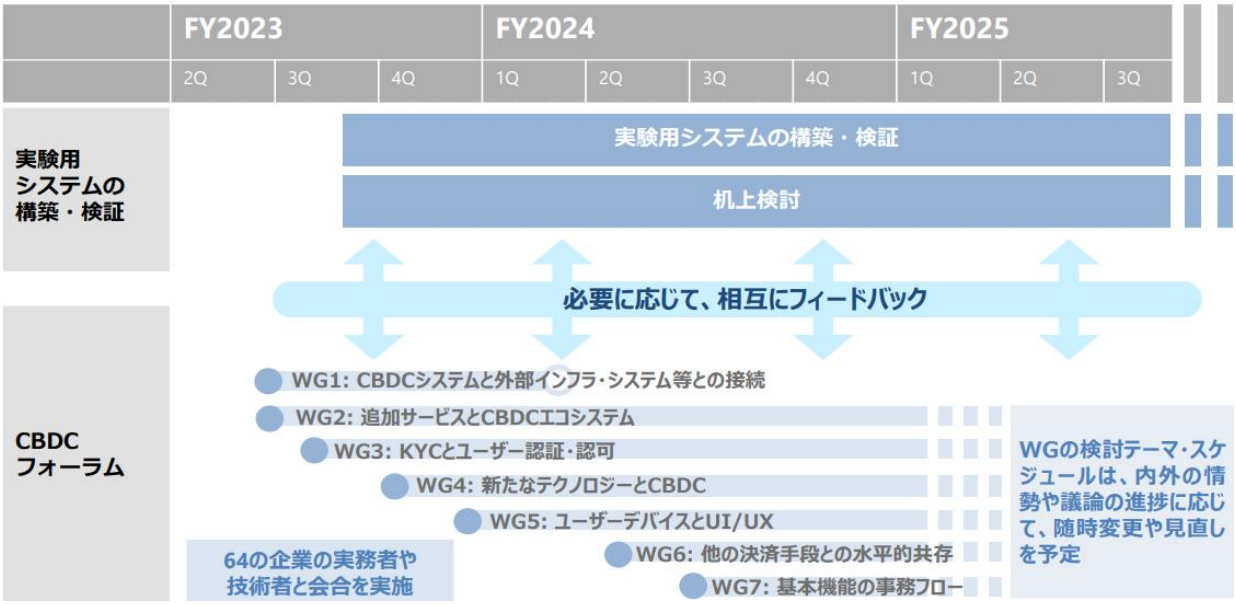
日本銀行は、2021 年より実証実験を開始し、CBDC の基本機能の検証を行う「概念実証フェーズ 1」、周辺機能の検証を行う「概念実証フェーズ 2」を実施した。さらに、2023 年 4 月からは、概念実証では検証しきれない技術的な実現可能性の検証及び民間事業者の技術や知見を活用することを目的としたパイロット実験を開始している（図 2.4）。



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

図 2.4　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、「実験用システムの構築と検証」と「CBDC フォーラム」から構成されている。前者は、日本銀行が構築する実験用システムの性能試験等を行うとされ、後者は、リテール決済に係る民間事業者の参加を得ながら、幅広いテーマについて議論・検討を行うとしている。



出典：財務省、「第 3 回 CBDC に関する関係府省庁・日本銀行連絡会議　幹事会　日本銀行資料」、2024.12、p2

図 2.5　パイロット実験の概要

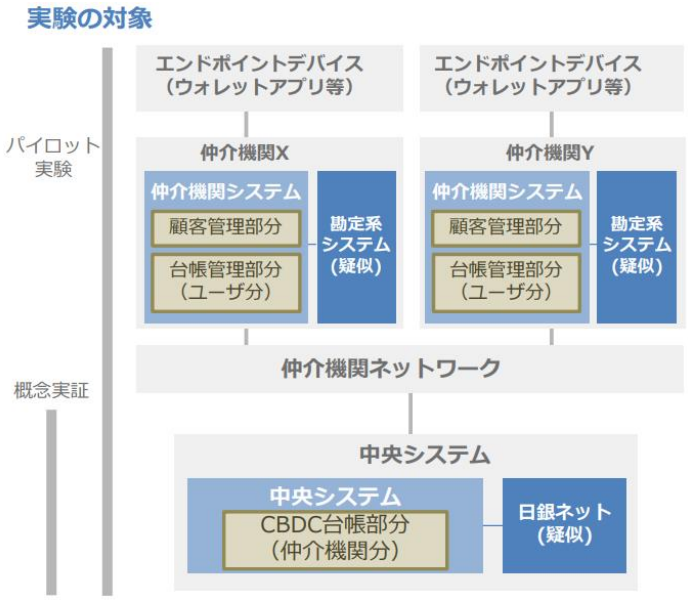
(1)　実験用システムの構築と検証

実験用システムについては、実験用システム構築と各種検証作業等の業務を株式会社日立製作所[35]に、プロジェクト管理支援と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[36]に、それぞれ委託している。図 2.5 に示すように、現在は、実験用システムの構築・検証を行い、それと並行して実験用システムで実装しない機能を中心に机上検討を実施しているとされている。

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していないとされている。

イ　実験用システムの構成及び検証

実験用システムの検証は、概念実証から検証範囲を拡大し、概念実証で検討した中央システムだけでなく、仲介機関システム、仲介機関ネットワーク（中央システムと仲介機関を結ぶネットワーク）、エンドポイントデバイス（スマートフォンやタブレットを利用したアプリ）を含めて構築し、その上でエンドツーエンドの処理フローの確認、外部システムとの接続に向けた課題・対応策の検討を実施しているとされている（図 2.6 参照）。



出典：日本銀行、「第 3 回 CBDC フォーラム全体会合資料」、2024.10、p.14

図 2.6　実験用システムの検証における対象範囲

また、実験用システムについてはプライバシーに配慮し、利用者情報や取引情報を台帳管理部分では取り扱わず、仲介機関の顧客管理部分と台帳管理部分を分離する設計とし、顧客管理部分では本人確認や認証等に必要な利用者情報・取引情報のみを管理し、台帳管理部分では口座番号や残高、取引金額といった決済に必要な情報のみ保有するとされている（表 2.4 参照）。

表 2.4　実験用システムにおけるデータの取扱いの整理

データ項目（※）				顧客管理部分	台帳管理部分
	名称		概要	保有可否	
1	口座名義人ID	利用者情報	顧客管理を行う仲介機関が顧客を一意に識別するためのID	○	×
2	利用者認証情報		氏名、住所、生年月日等	○	×
3	口座特定ID		CBDC口座を一意に識別するためのID	○	×
4	台帳管理機関ID	決済に必要な情報	台帳管理を行う仲介機関を一意に識別するためのID	○	○
5	CBDC口座番号		台帳管理を行う1つの仲介機関内で口座を一意に識別するための番号	○	○
6	残高		各シーンにおける集計単位ごとの残高	○	○
7	取引ID		取引発生の都度、付番される番号	○	○
8	取引金額		各シーンにおける集計単位ごとの送金取引の金額	○	○
9	摘要情報	取引情報	取引に関する任意のテキスト情報	○	×

※　追加サービスの提供にあたって、顧客管理を行う仲介機関または追加サービス提供事業者が収集するデータは含まない。

出典：財務省、「第2回 CBDC に関する関係府省庁・日本銀行連絡会議　幹事会　日本銀行資料「データの取扱いについて」」、2024.12、p.3

そのほか、処理性能の向上を目的に、レコード分割を可能とする仕組みを導入し、並列処理性を高める設計とする等、性能・事務量については概念実証より高負荷に対応可能なシステムの構築を目指し、更には機能や性能を拡張しやすい工夫を設計段階で組み込むことを予定するとしている。

パイロット実験では、実験用システムの構築を行った後、性能試験等の検証作業を行う予定としている。実験用システムに具備する機能としては、発行・還収、払出・受入の基本機能に加えて、送金の際のオートスウィングやオートチャージ、保有額等の制限チェックのための機能、そのほか概念実証フェーズ２で検討した一括送金を含む予約送金、逆引送金、残高・明細照会といった周辺機能も、具備することが予定されている（図2.7）。

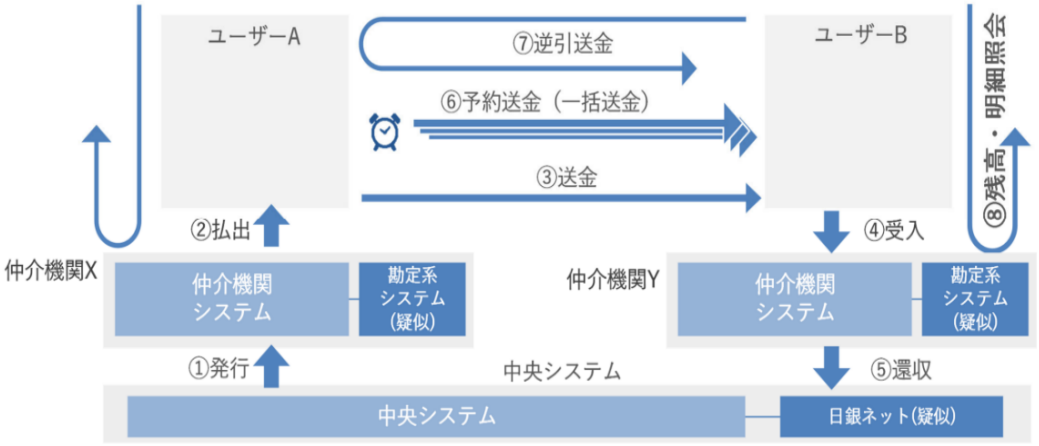


図 2.7　実験用システム基本機能

出典：財務省、「第 9 回 CBDC に関する有識者会議　日本銀行説明資料」、2024.5、p.4

ロ　ＣＢＤＣシステムの機能面や非機能面の検討

パイロット実験では実機検証と並行して、CBDC システムの機能面や非機能面を机上検討するとしている。

機能面においては、実験用システムでは実装しない各種機能のほか、外部システムとの相互運用性、オフライン決済との親和性、プライバシー保護技術等について検討するとしている。また、非機能面においては、システムの高可用性、機能・性能拡張性、セキュリティ対策に関する検討等を行うとしている。

(2) ＣＢＤＣフォーラム

CBDC フォーラムは、リテール決済に関する技術や実務に関する知見を持つ企業が参加しており、テーマごとの複数のワーキンググループ（WG）を設置し議論・検討が進められている。CBDC フォーラムにおける具体的な検討テーマは表 2.5 のとおりである。

表 2.5　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（Know Your Customer）、AML/CFTの実施状況
		認証・認可
[WG4]	新たなテクノロジーとCBDC	バックエンド（代替的な台帳データモデル等）
		フロントエンド（「ウォレット」等）
		他の決済手段や資産との共存（ステーブルコイン、アセットトークナイゼーション、DLT(Distributed ledger technology)基盤との相互運用性等）
[WG5]	ユーザーデバイスとUI/UX	UI（User Interface）/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
[WG6]	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
[WG7]	基本機能の決済フロー	基本的な機能にかかる事務フロー
		現金とCBDCの交換

参考：日本銀行、「第 9 回 CBDC（中央銀行デジタル通貨）に関する有識者会議資料」、2024.5、p.7 を基に作成

2024 年には、以下の４つの WG が立ち上げられている。

WG4：新たなテクノロジーと CBDC（1 月）

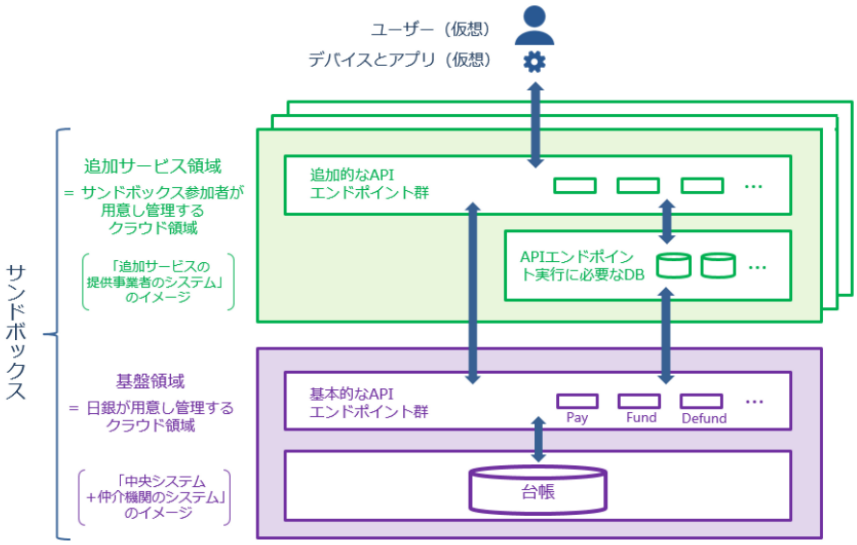
WG5：ユーザーデバイスと UI/UX（3 月）

WG6：他の決済手段との水平的共存（7 月）

WG7：基本機能の事務フロー（9 月）

また、WG1「CBDC システムと外部インフラ・システム等との接続」は、2024 年 6 月の第 11 回会合で一旦休止となり、その検討成果は実験用システムの構築に活用されるとしている[37]。

そのほか WG2「追加サービスと CBDC エコシステム」では、API サンドボックスプロジェクトが立ち上げられた。実験用システムとは別に、WG2 参加者の有志メンバーがクラウド上に共同で実験環境を用意し、送金、払出し、受入れ等の様々な API の構築を実施しているとされる（図 2.8）。



出典：日本銀行、「第 3 回 CBDC フォーラム全体会合資料」、2024.10、p.5

図 2.8　API サンドボックスの概要

2.4.2　財務省の取組

(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、高い見識を有する方々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、2024 年 10 月までに 9 回開催され、国内外の議論を踏まえながら、通貨や決済の現状、民間決済手段等についての現状認識を共有し、CBDC に係る論点整理を進めている。

なお、2023 年 12 月には、有識者会議の「取りまとめ」を公表している。これは、CBDC の検討背景や、国内における決済手段としての CBDC のあり方等を念頭に置きつつ、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、有識者会議としての議論の結果を取りまとめたものである。

(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・日本銀行は、制度設計の大枠を整理するため、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。この会議は、財務省理財局長を議長とし、内閣府、警察庁、金融庁等の関係府省庁及び日本銀行の幹部で構成されている。

2024 年 4 月に行われた第 3 回連絡会議では、有識者会議の「取りまとめ」を踏まえ、それまでの議論を整理する「中間整理[38]」を行っている。また、10 月に行われた第 4 回連絡会議では、より実務的な議論を行うため、連絡

会議の下に幹事会を開催することが決定された[39]。その中で、今後のスケジュールとして、月１回程度の幹事会を開催し、課題や論点を議論し、2025 年春を目途に第 5 回連絡会議を開催し、一定の整理を行う方向で進めていくことが示されている[40]。

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

CBDC に関する関係府省庁・日本銀行連絡会の「中間整理」に基づき、関係府省庁・日本銀行との間において、所管する業界団体の意見等にも目を配りつつ、幅広い観点から丁寧に調整することが必要となることが想定される課題・論点を中心に議論を進めて行くに当たり、より実務的な議論を行うため、連絡会議の下に幹事会が開催されることとなった[41]。幹事会は、財務省理財局国庫課長を座長として、内閣府や公正取引委員会、警察庁等関係府省庁及び日本銀行の課長級で構成されている。

イ　第１回幹事会

「私法上の整理に関する技術的な前提等」や「既存のデジタル財産等に関する整理」について議論が行われた[42]。ここでは、CBDC の帰属・移転の法律構成と CBDC 台帳で採用する技術面とは独立して検討しうること、各デジタル財産等の性質に応じて帰属・移転の取扱いやその規定に様々な違いがあることが確認された。また、民事執行の議論では各財産等の性質の違いに対応して、様々な執行の在り方が存在し、CBDC に対する執行については、仲介機関に対してどのような規律を設けるべきかの考えを深めることが重要と示された。

ロ　第２回幹事会

「データの取扱い」や「個人情報保護とデータの利活用」について議論が行われ、プライバシーに関する論点が示された[43]。

日本銀行からは実験用システムについて、プライバシーへの配慮から、利用者情報等を扱う顧客管理と決済に必要な情報のみを扱う台帳管理を分けることで、日本銀行が個人情報を持たない形で検討されていることが示された。

個人情報保護においては個人情報保護法や金融機関の具体的な対応を確認し、CBDC の仲介機関のあり方を考える上で多くの示唆があったとされた。

データの活用においては、公共政策上の要請として AML/CFT の基本的な枠組みや最新技術の活用の整理や、既存キャッシュサービスのデータ活用例が確認され、CBDC におけるデータ活用の可能性についても確認された。

ハ　第 3 回幹事会

金融庁・経済産業省より「民間事業者へのヒアリング報告」が行われ、連絡会議の中間整理で挙げられた以下の 5 つの主要論点を前提とした、民間事業者へのヒアリング報告結果が示された[44]。

① 通貨としての性質
② 共通インフラとしての可能性
③ バックアップシステムとしての可能性
④ 制限の必要性
⑤ 既存システムへの配慮について

日本銀行からは「CBDC フォーラムにおける議論の概要等」の説明がなされた。

これらを基に議論され、仮に CBDC の導入を行うこととなった場合に生じる影響について、既存事業者との関係において配慮すべき点について議論を深めたとされた。また、①CBDC が公的なシステムとして、社会におけるデジタル決済・サービスの利活用を促進するため、備えておくべき要素について理解を深めるとともに、②インフラとして異なる決済手段の相互接続等をサポートする基盤となるほか、システムやデータの形式の統一に繋がりうる可能性についても議論された。

---

[1] BIS, “Embracing diversity, advancing together – results of the 2023 BIS survey on central bank digital currencies and crypto”, 2024.6.14, (https://www.bis.org/publ/bppdf/bispap147.htm)
[2] BIS, “Central bank digital currencies: Legal aspects of retail CBDCs”, 2024.11, (https://www.bis.org/publ/othp88_legal.pdf)
[3] BIS, “Central bank digital currencies: System design”, 2024.11, (https://www.bis.org/publ/othp88_system_design.pdf)
[4] IMF, “Central Bank Digital Currency Virtual Handbook”, (https://www.imf.org/en/Topics/digital-money-and-fintech/central-bank-digital-currency/virtual-handbook)
[5] Federal Reserve Bank of Boston, “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)
[6] CONGRESS.GOV, “H.R.5403 – CBDC Anti-Surveillance State Act”, 118th Congress (2023-2024), 2024.6.3, (https://www.congress.gov/bill/118th-congress/house-bill/5403/text)
[7] PYMNTS, “Fed Governor Waller: No Need for CBDC”, 2024.11.12, (https://www.pymnts.com/cbdc/2024/fed-governor-waller-no-need-for-cbdc/)
[8] The White House, “STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY”, 2025.1.23, (https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/)
[9] BOE, “Progress update: The digital pound and the payments landscape”, 2025.1.14, (https://www.bankofengland.co.uk/report/2025/digital-pound-progress-update)
[10] 公益財団法人国際通貨研究所、「徐々に利用拡がるデジタル人民元の動向」、p.1、2023.10.17、(https://www.iima.or.jp/docs/column/2023/ei2023.23.pdf)
[11] IT 之家、「数字人民币可视硬钱包发布：可碰可扫，内置墨水屏显示余额及付款码」、2024.11.7、(https://www.ithome.com/0/808/679.htm)
[12] Central Banking, “CBDC transactions reach 7 trillion yuan, PBoC official says”, 2024.9.13,

(https://www.centralbanking.com/central-banks/currency/7962276/cbdc-transactions-hit-seven-trillion-yuan-pboc-official-says)

[13] CoinDesk JAPAN、「インド、CBDC 利用者が 500 万人に――中央銀行総裁「システム全体への展開は急がない」」、(https://www.coindeskjapan.com/247835/)

[14] Bank of Russia, "Payment infrastructure for digital ruble to become available: Bank of Russia's proposals", 2024.9.12, (https://www.cbr.ru/eng/press/event/?id=20992)

[15] 日本銀行、「海外における「預金のトークン化」の取り組みについて」、p.5、2024.6.28、(https://www.boj.or.jp/research/wps_rev/rev_2024/data/rev24j10.pdf)

[16] Hong Kong Monetary Authority , "HKMA launches Phase 2 of the e-HKD Pilot Programme", 2024.5.14, (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/03/20240314-4/)

[17] Financial Services Commission、2024.11.6、「[보도자료] 중앙은행 디지털화폐(CBDC) 활용한 새로운 디지털 금융서비스의 첫 발 내딛다」、(https://www.fsc.go.kr/no010101/83337)

[18] BIS, "Tiff Macklem: Economic growth during uncertain times", 2024.9.25, (https://www.bis.org/review/r240925a.htm)

[19] Reserve Bank of Australia, "Financial Innovation and the Future of CBDC in Australia", 2024.9.18, (http//www.rba.gov.au/speeches/2024/sp-ag-2024-09-18.html)

[20] ECB, "Progress on the preparation phase of a digital euro – First progress report", 2024.6.24, (https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202406.en.html)

[21] ECB, "Progress on the preparation phase of a digital euro Second progress report", 2024.12.2, (https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202412.en.html)

[22] ECB, "Technical note on the provision of multiple digital euro accounts to individual end users",2024.3.25, (https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.degov240325_digital_euro_multiple_accounts.en.pdf)

[23] ECB, "Update on the work of the digital euro scheme's Rulebook Development Group",2024.1.3, (https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240103_RDG_digital_euro_schemes_update.en.pdf)

[24] ECB, "Update on the work of the digital euro scheme's Rulebook Development Group",2024.9.5, (https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.derdgp240905_RDG_progress_report_September.it.pdf)

[25] 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)

[26] BOE, "Progress update: The digital pound and the payments landscape", 2025.1.14, (https://www.bankofengland.co.uk/report/2025/digital-pound-progress-update)

[27] BOE, "National Payments Vision", p.34, 2024.11.14, (https://www.gov.uk/government/publications/national-payments-vision)

[28] BOE, "The Bank of England's approach to innovation in money and payments", 2024.7.30, (https://www.bankofengland.co.uk/paper/2024/dp/the-boes-approach-to-innovation-in-money-and-payments)

[29] BOE, "Design note – Blueprint framework", 2025.1.14, (https://www.bankofengland.co.uk/report/2025/blueprint-framework-design-note)

[30] BOE, "Point-of-sale proof of concept", 2024.5.16, (https://www.bankofengland.co.uk/report/2024/point-of-sale-proof-of-concept)

[31] BOE, "Minutes of the CBDC Technology Forum – 14 May 2024", 2024.8.2, (https://www.bankofengland.co.uk/minutes/2024/may/minutes-of-cbdc-technology-forum-may-2024)

[32] BOE, "Minutes of the CBDC Technology Forum – 22 May 2024", 2024.8.2, (https://www.bankofengland.co.uk/minutes/2024/may/minutes-of-cbdc-technology-forum-22-may-2024)

[33] BOE, "Minutes of the CBDC Technology Forum – July 2024", 2024.8.2, (https://www.bankofengland.co.uk/minutes/2024/july/minutes-of-cbdc-technology-forum-july-2024)

[34] 内閣府、「経済財政運営と改革の基本方針 2024 ～賃上げと投資がけん引する成長型経済の実現～（令和6年6月 21 日閣議決定）」、p.12、2024.6.21、(https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/2024_basicpolicies_ja.pdf)

[35] 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)

[36] 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)
[37] 日本銀行、「第 3 回 CBDC フォーラム全体会合資料」、2024.10.17、p.3、
(https://www.boj.or.jp/paym/digital/d_forum/dfo241017b.pdf)
[38] 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　中間整理」、2024.4.17、
(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20240417chuukanseiri.pdf)
[39] 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」、
2024.10.3、(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241003_3_secchi.pdf)
[40] 財務省、「今後のスケジュール（イメージ）」、2024.10.3、
(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241003_5_schedule.pdf)
[41] 財務省、「CBDC（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議幹事会の開催について」、
2024.10.3、(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241003_4_kanjikai.pdf)
[42] 財務省、「第１回 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　幹事会　配布資料」、2024.10.29、(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241029haifusiryo.html)
[43] 財務省、「第２回 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　幹事会　配布資料」、2024.12.2、(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241202haifusiryo.html)
[44] 財務省、「第３回 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　幹事会　配布資料」、2024.12.19、(https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20241219haifusiryo.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

中国のデジタル人民元に関しては、2021 年 7 月に公表された白書「デジタル人民元の研究開発の進展[45]（Progress of Research & Development of E-CNY in China）」において設計の概要が示された。しかし、その後は設計に関する情報はほとんど公開されていない。一方で、2019 年末に開始されたパイロット実験は地域を拡大して継続されている状況にある。

このような状況の下、本付録では、デジタル人民元の取組の詳細については公表されていないものの、特許出願の件数や内容に反映されていると考え、特許出願状況を分析し、デジタル人民元の取組状況を推察したものである。

なお、本調査結果は、令和 5 年度版レポートの「中国人民銀行の特許出願状況について」の情報を更新するものである。

2　調査内容

Google Patents を用いて、中国人民銀行が「出願人」又は「権利保有者」として含まれる出願特許を検索対象とした。

検索期間は 2012 年 1 月～2024 年 8 月末日までとし、特許公開公報に記載されている「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」を分類し、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、特許の分類を「CBDC 関連のブロックチェーン」、「デジタル通貨」、「関連技術」及び「デジタル通貨のユースケース」の４つの大分類とした。さらに、デジタル通貨及び関連技術に関しては、付表 1.1 のとおり中分類、小分類の設定を行った。

（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、当該特許が用いられる用途や解決したい課題を付表 1.1 に示すように分類した。

特許の分析においては、複数の用途や課題が記載されている特許出願も多く見られるが、特許の概要や請求項を基に、関連度が最も高いと思われる用途に分類した。

例えば、オフライン決済は、利便性の向上（容易）、社会的な課題の解決（金融包摂）とも見なせるが、ここでは多様な決済手段の提供（オフライン決済）として分類した。このように、関連度が最も高いと思われるものに対応させ、小分類が複数の大分類に重ならないようにしている。

付表 1.1　技術分野、用途・課題の分類

（1）技術分野

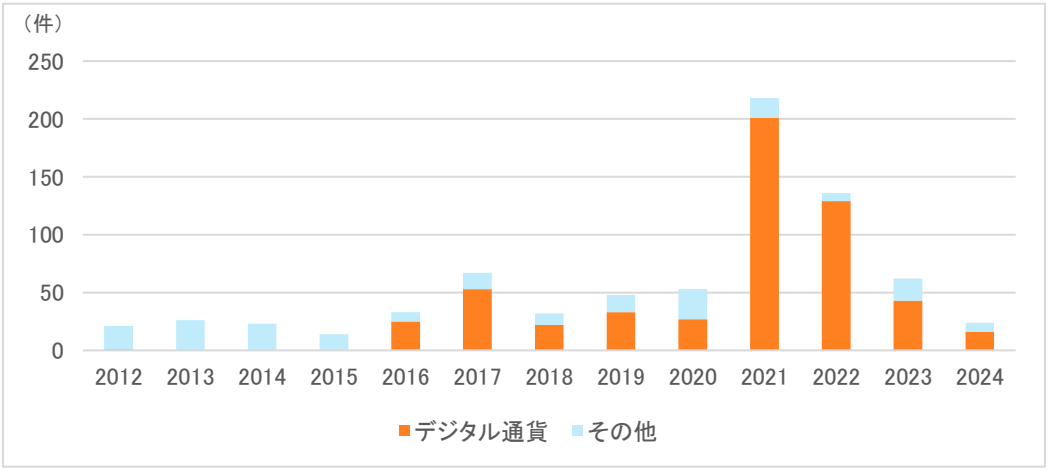
大分類	中分類	小分類
CBDC関連のブロックチェーン		
デジタル通貨	通貨の発行・管理	
	媒体・ウォレット	
	取引端末	
	チャージ	
	決済処理・手続	
	決済アプリ	
関連技術	データ処理	通信手段・方法
		情報の記録・管理
		情報の分散管理
		ビッグデータ解析
	情報セキュリティ	暗号技術
		認証
		鍵の管理
		不正検出・異常検知
	関連システム	インターネットバンキング
		その他の銀行システム
デジタル通貨のユースケース		
その他（関連外）		

（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、757 件の特許を抽出した。そのうち、デジタル技術関連の特許は 550 件である。2015 年以前は主に銀行券の偽造防止技術等に関する特許が出願されていたが、2016 年からデジタル通貨や関連技術に関する特許の出願が増加している。特に 2021 年には出願数が大幅に増加したが、その年をピークに減少傾向にある（付図 1.1）。

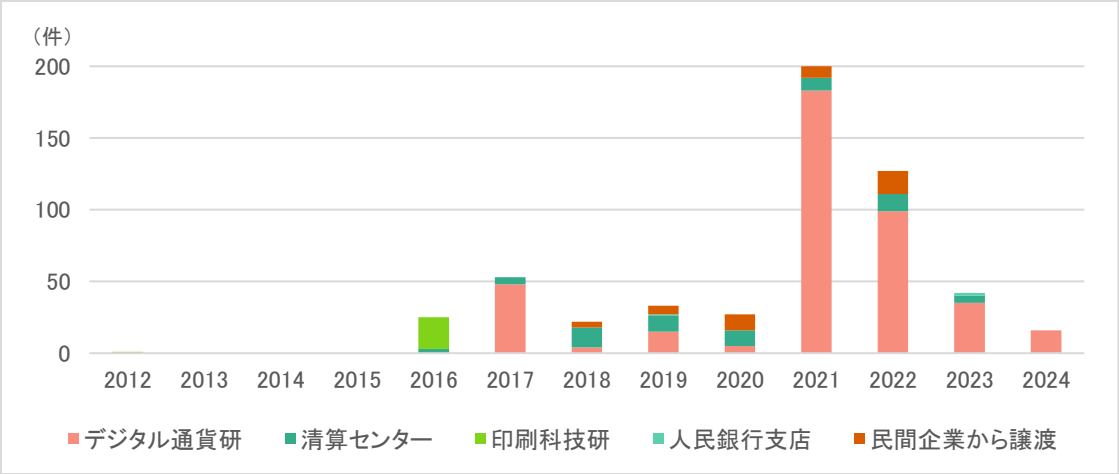


付図 1.1　中国人民銀行の特許出願（全技術分野）

3.1　出願機関

中国人民銀行には、デジタル通貨関連の特許を出願している３つの機関（印刷科学技術研究所（1959 年設立）、清算センター（1990 年設立）及びデジタル通貨研究所（2016 年設立））がある。

全体的な傾向として、2021 年以降はデジタル通貨研究所が多くの特許を出願している一方で、印刷科学技術研究所の特許出願は見られなくなっている（付図 1.2）。

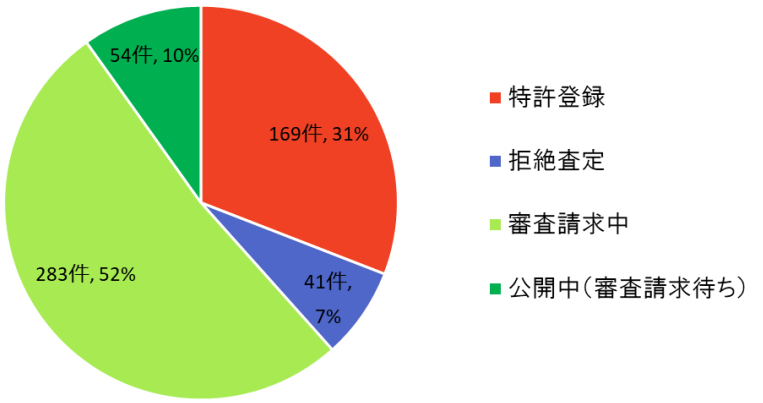


付図 1.2　機関別出願動向（CBDC 関連に限る）

3.2　審査の状況

中国人民銀行は、これまでに出願したデジタル技術関連の特許の大部分について審査請求を行い、2024 年 8 月末時点で約 3 割が実際に特許登録されている。

また、審査終了した特許は 210 件あり、そのうち 169 件が特許登録されている。これにより特許査定率は 80.5%となる。これは、2022 年の中国の特許査定率（51.1%[46]）と比べて、極めて高い数値となっている（付図 1.3）。



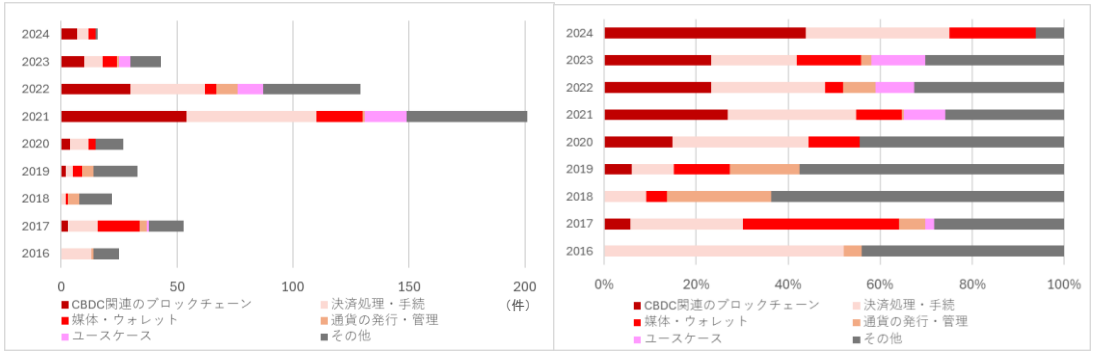
付図 1.3　デジタル技術関連特許の査定状況（審査取下げ案件等を除く 547 件）

3.3　出願傾向

特許の出願傾向を調査するために、「技術分野」と「用途・課題」を分類し、内容別にデジタル通貨関連の特許出願が本格化する 2016 年以降の特許出願件数を整理した（付図 1.4、付図 1.5）。

(1)　技術分野

技術分野の出願動向については、2016 年より決済処理・手続に関する技術出願がされるようになり、2017 年にはブロックチェーン技術、決済媒体・ウォレットに関する技術が出願され、これらの分野が現在でも多くを占めている。一方で、2021 年からはユースケースに係る技術の出願がなされている。これらの傾向は、パイロット実験の進捗に伴うものと考えられる。

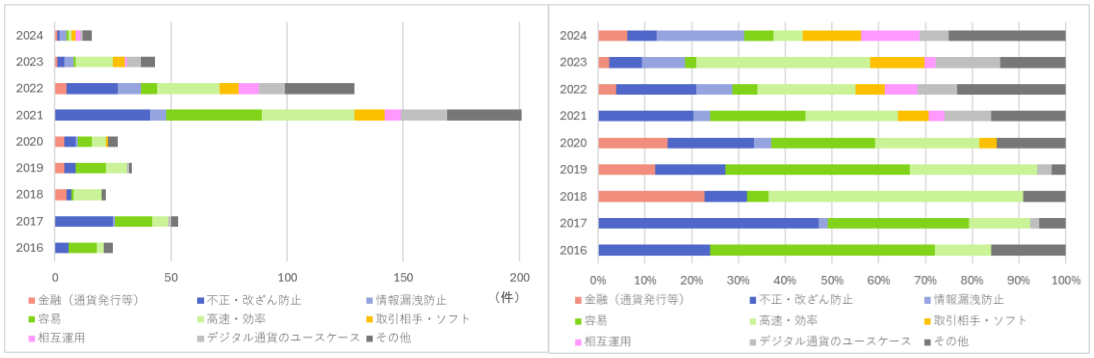


付図 1.4　技術分野別出願件数の推移

(2)　用途・課題

2016 年以降の出願特許の用途・課題については、「不正・改ざん防止」、「容易」、「高速・効率」のため課題を解決するためのものが多くを占めている。しかし、「高速・効率」以外の割合は年々減少し、「情報漏洩禁止」、「オフライン決済」、「デジタル通貨のユースケース」などの割合が増えてきている。また、「省電力・電力確保」や「事業継続」などに関する特許出願もみられる。

この傾向は、技術分野の分析結果と同様に、パイロット実験の進展に伴い、解決したい課題が変化していることに対応するものと考えられる。



付図 1.5　用途・課題別出願件数の推移

(3) 2024 年に公開された特許の一例

2024 年にはスマートコントラクトやハードウォレットに関する複数の特許が公開されていた。

スマートコントラクトに関しては、住宅購入者の住宅不動産販売者への契約条件に基づく支払（CN117455657A）、給与発行方法（CN118154179A）など、ユースケースに関する特許が公開されていた。

ハードウォレットについては、多くの特許が公開され、モバイル通信装置とウォレットの取引方法（CN118014566A）、ウォレットの残高更新（CN117974136A）、表示パネルの制御方法（CN117971095A）、非接触機能のテスト方法（CN117971573A）、アップグレードによる機能更新（CN116703393A）、ウォレットの発行装置（CN117709949A）、ウォレットの移行（CN117609179A）などがあった。

また、2024 年にはカード型のビジュアルハードウォレットが販売されており[47]、これらの特許が利用されている可能性がある（付図 1.6）。

深圳国際金融博覧会においてデジタル人民元のビジュアルハードウォレットが国内で初めて発売。

- タッチ決済
- 表示可能
  （残高、決済額、支払コードの表示）
- 厚さ１mm

付図 1.6　カード型のビジュアルハードウォレットに関する報道

3.4 国際出願

国際出願は、他の国・地域で特許の取得審査を受ける前段階として、出願の事実を国際的に公表するものであり、原則として、自国への出願後 1 年以内に行うものとされている。

2022 年以前の中国人民銀行の国際出願は全 6 件であったが、2022 年だけで 32 件の国際出願を行っている。これは 2021 年に中国人民銀行の特許出願件数が大幅に増加したことが要因と考えられる。2023 年の国際出願は 18 件となっている。国際特許の出願は、国内の特許出願から 1 年以内に出願が必要であることから、1 年遅れで同様の傾向を示すと考えられるため、2022 年をピークに次第と落ち着いていくと思われる。

4　まとめ

特許出願の傾向から推測すると、中国人民銀行のデジタル人民元の研究開発については、パイロット実験の進展に伴い、デジタル人民元のシステムに係る研究開発から、社会実装に向けたユースケースなどの課題解決にシフトし、多様な分野での研究開発が行われていると考えられる。ただし、2021 年をピークに出願件数が減少しているため、研究開発は一旦落ち着いているように見える。

また、2024 年に発売されたビジュアルハードウォレットには、2024 年に公開されたハードウォレットに関する特許が利用されている可能性が示唆される。このことから、今後も、特許出願の傾向を把握することで、デジタル人民元の開発動向が見えてくるものと思われる。

---

[45] 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)

[46] 特許庁、「特許行政年次報告書 2024 年版　1-1-26 図 【主要特許庁の特許査定率の推移】」、2025.1.9、p.12、
(https://www.jpo.go.jp/resources/report/nenji/2024/document/index/all.pdf)

[47] IT 之家、「数字人民币可视硬钱包发布：可碰可扫，内置墨水屏显示余额及付款码」、2024.11.7、
(https://www.ithome.com/0/808/679.htm)

参考付録 2　プライバシー保護と AML／CFT の動向について

1　概要

CBDC 関係府省庁・日本銀行連絡会議の中間整理において、「CBDC については、デジタル決済手段であることから、その利用者情報・取引情報の取扱いが課題となる」と記載されている。

具体的には、「個人情報保護の観点からは、プライバシーの確保が前提」としつつ、「追加サービスの提供など利便性の向上や、AML／CFT をはじめ公共政策上の要請への対応等とのバランスを図っていくことが必要である」とされている。そうした考えの下で、利用者と日本銀行の間に立つ仲介機関が利用者情報・取引情報の大部分を取り扱うことが想定されるため、その範囲や、規制のあり方について検討が進められている[48]。

こうしたことを踏まえ、我が国の現在のプライバシー保護や AML／CFT についての整理を行った。

2　プライバシー保護に関する動向について

プライバシー保護については、2005 年に「個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）」が全面施行された。この際、3 年ごとに見直されることとなり、その後もプライバシー保護とデータ利活用の観点から、個人情報の定義を明確にして健康情報などを厳しく管理する「要配慮情報」、個人を特定できないように加工しデータ活用を促す「匿名加工情報」制度、「仮名加工情報」制度が追加で規定されてきた。

また、事業者については、利用者情報の取扱いの制限[49]（表 2.1[50]）が個人情報保護法に定められているほかにも、特定分野において利用者情報を扱うための規則やガイドライン等が定められている。

付表 2.1　事業者が利用者情報を取り扱う際の制限（例）

項目	具体的な制限の内容	個人情報保護法の条番号
利用目的の特定	利用者情報の利用目的についてできる限り特定	第十七条第一項
利用目的の変更	利用目的を変更する場合、変更前の目的と関連すると合理的に認められる範囲を超えてはならない	第十七条第二項
目的外利用の制限	原則、本人同意がない利用目的を超えた情報の取扱を禁止	第十八条第一項
利用目的の通知・公表	取得した情報の利用目的や目的変更の理由を通知・公表しなければならない	第二十一条第一項及び同条第三項
第三者提供の制限	原則、本人同意がない利用者情報データの第三者提供を禁止	第二十七条第一項

3　AML／CFT に関する動向について

AML／CFT については、「一国のみが規制を強化しても、相対的に規制の緩い国で行われる傾向にある」ことから、1989 年に AML を国際的な協調を推進するための多国間の枠組みとして金融活動作業部会（FATF）が設立された。また、2001 年に米国同時多発テロ事件が発生したことを契機に、CFT についてもその任務に追加された[51]。

FATF は、AML／CFT の実効性向上のために国際的な基準として、法令等整備や法執行の有効性評価に関するガイドライン「FATF 勧告」を策定し、当該勧告に基づき各国に対して審査を実施している。

日本においては、2021 年に審査（第 4 次対日相互審査）の対象となり、法令等整備の 40 項目と有効性の 11 項目の審査が行われた。法令等整備については 11 項目が、有効性については 8 項目が、4 段階評価の下位 2 つの評価となり[52]、FATF に対して法令整備状況に関する改善状況を報告しなければならない「重点フォローアップ国」という位置づけとなった[53]。

日本政府は、この結果を受けて「マネロン・テロ資金供与・拡散金融対策に関する行動計画」を策定し[54]、法改正等の各種対応を行い実効性の向上を図った。結果として、2024 年 10 月のフォローアップ報告書では、全ての法令等整備状況について 4 段階のうち上から 2 番目までの評価に格上げされた（審査の結果と評価の変遷[55,56,57]は付表 2.2 のとおり）。

今後、第 5 次対日審査が行われる予定（2028 年頃）であり、「整備した法令が有効に執行されているか」について、検証がなされる予定である[58]。

付表 2.2　法令等整備に関する第 4 次対日相互審査結果とその評価の変遷

勧告	概要	勧告	概要	勧告	概要	勧告	概要
1	リスク評価とリスクベース・アプローチ	11	本人確認・取引記録の保存義務	21	届出者の保護義務	31	捜査関係等資料の入手義務
2	国内関係当局間の協力	12	PEPs（重要な公的地位を有する者）	22	DNFBPs（指定非金融業者及び職業専門家）における顧客管理	32	キャッシュ・クーリエ（現金運搬者）への対応
3	資金洗浄の犯罪化	13	コルレス契約	23	DNFBPs（指定非金融業者及び職業専門家）における疑わしい取引の報告義務	33	包括的統計の整備
4	犯罪収益の没収・保全措置	14	代替的送金サービス	24	法人の実質的支配者	34	ガイドラインの策定義務
5	テロ資金供与の犯罪化	15	新技術の悪用防止	25	法的取極の実質的支配者	35	義務の不履行に対する制裁措置
6	テロリストの資産凍結	16	電信送金（送金人・受取人情報の付記義務）	26	金融機関に対する監督義務	36	国連諸文書の批准
7	大量破壊兵器の拡散に関与する者への金融制裁	17	顧客管理措置の第三者依存	27	監督当局の権限の確保	37	法律上の相互援助、国際協力
8	非営利団体（NPO）の悪用防止	18	金融機関における内部管理規定の整備義務、海外支店・現地法人への勧告の適用	28	DNFBPs（指定非金融業者及び職業専門家）に対する監督義務	38	外国からの要請による資金凍結等
9	金融機関の守秘義務	19	勧告履行に問題がある国・地域への対応	29	FIUの設置義務	39	犯人引渡
10	顧客管理	20	金融機関における資金洗浄・テロ資金供与に関する疑わしい取引の届出	30	資金洗浄・テロ資金供与の捜査	40	国際協力（外国当局との情報交換）

※ 緑色ハイライト部分：第 1 回フォローアップ審査時点で合格水準と評価された項目（1 項目）
黄色ハイライト部分：第 2 回フォローアップ審査時点で合格水準と評価された項目（4 項目）
橙色ハイライト部分：第 3 回フォローアップ審査時点で合格水準と評価された項目（6 項目）

4　まとめ

日本においては、現在、プライバシー保護については個人情報保法等や各種ガイドライン等によって、利用者情報の活用とプライバシー保護のバランスが図られてきている状況にある。AML／CFT についても、FATF 勧告に基づき法令整備がなされ、対応してきている。

今後も、IT 技術の進展や海外のプライバシー保護の考え方により、国内でのプライバシー保護の考え方が変わることや、AML／CFT についてはよりその要請が高くなることが考えられる。

---

[48] 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　中間整理」、2024.4.17、pp.15-18
（https://www.mof.go.jp/about_mof/councils/meeting_of_cbdcre/20240417chuukanseiri.pdf）

[49] 個人情報保護委員会、「個人情報保護委員会事務局レポート:仮名加工情報・匿名加工情報　信頼ある個人情報の利活用に向けて―制度編―」、2022.5、pp.8-11
（https://www.ppc.go.jp/files/pdf/report_office_seido2205.pdf）

[50] e-Gov 法令検索、「個人情報の保護に関する法律（平成十五年法律第五十七号）」、
（https://laws.e-gov.go.jp/law/415AC0000000057/）

[51] 警察庁、「犯罪収益移転防止法の概要　（令和 6 年 12 月 2 日時点）」、2024.12.2、p.1
（https://www.npa.go.jp/sosikihanzai/jafic/hourei/data/hougaiyou20241202.pdf）

[52]財務省、「第４次対日相互審査報告書（令和３年８月 30 日）　仮訳」、2023.1.4、p.15
（https://www.mof.go.jp/policy/international_policy/amlcftcpf/20221228.pdf）

[53] 金融庁、「マネー・ローンダリング・テロ資金供与・拡散金融対策の現状と課題（2023 年６月）」、2023.6.30、pp.85-86
（https://www.fsa.go.jp/news/r4/20230630/2023063001.pdf）

[54] 財務省、「マネロン・テロ資金供与・拡散金融対策に関する行動計画」、2021.8
（https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20210830_2.pdf）

[55] 財務省、「対日相互審査フォローアップ報告書（第１回）（令和 4 年 9 月 13 日）　仮訳」、
（https://www.mof.go.jp/policy/international_policy/amlcftcpf/Japan-FUR-2022.pdf）

[56] 財務省、「対日相互審査フォローアップ報告書（第２回）（令和 5 年 10 月 23 日）　仮訳」、p.30
（https://www.mof.go.jp/policy/international_policy/amlcftcpf/Japan-FUR-2023.pdf）

[57] 財務省、「対日相互審査フォローアップ報告書（第３回）（令和 6 年 10 月 10 日）　仮訳」、p.18
（https://www.mof.go.jp/policy/international_policy/amlcftcpf/Japan-FUR-2024.pdf）

[58] 金融庁、「マネー・ローンダリング等対策の取組と課題（2024　年６月）」、2024.6、p.15
（https://www.fsa.go.jp/news/r5/amlcft/20240628/01.pdf）

3　デジタルウォレットの動向調査

3.1　ウォレットの概要

今後、各法域で CBDC が導入される場合、既存のキャッシュレス決済手段と同様にウォレット（Wallet）を用いることが想定される。ウォレットは、英語で「財布」を意味し、金銭を入れて持ち歩く袋や金入れに由来する[59]。一般的に財布には、現金以外にも、様々なサービスを利用するため、クレジットカード、キャッシュカード、運転免許証、学生証、会員証等の決済手段、身分証明書、資格証明書等を保管する。今日では、財布をデジタル化したものについても、ウォレットと呼ぶ。以下、本章におけるウォレットとは、「財布」の機能及び役割をデジタル化したものを示す。

3.1.1　ウォレットの役割

ウォレットは､様々なデジタルサービスを利用するために必要なキャッシュレス決済手段、デジタル身分証明書、デジタル資格証明書を保管するためのソフトウェアアプリとして提供される。

また、ウォレットは、現実空間においても、財布と同様に携帯可能なスマートフォン、タブレット等のモバイルデバイス上で動作させることで、ユーザは物理的な決済手段、身分証明書、資格証明書等を持ち運ぶことなく、デバイスを携行することで様々なサービスの利用が可能となる。

このように、ウォレットとは、サイバー空間上及び現実空間の様々なサービスを利用するために必要な情報を、デバイス上で管理可能なアプリである（図 1 参照)。ウォレットは、財布と同様、サービスの利用に必要なユーザ情報をユーザ自ら保管し、必要に応じてユーザ自ら取り出す、ユーザ主体によるユーザ情報の管理の仕組みとして、ユーザに提供される。

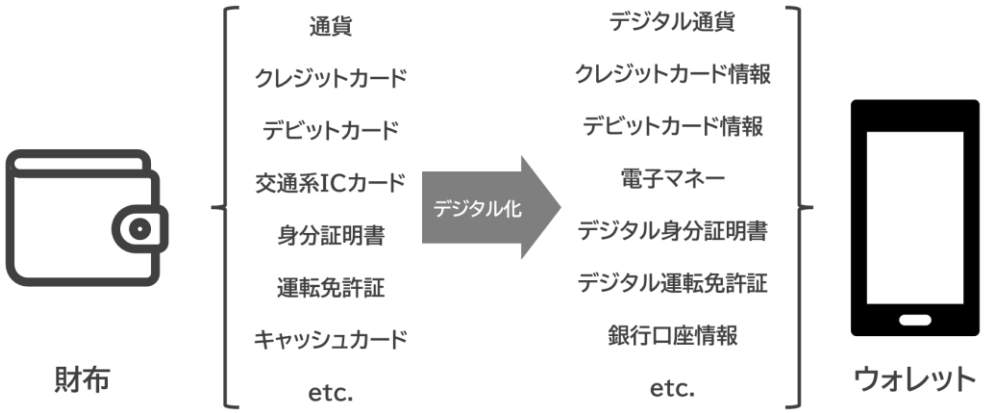


図 1　ウォレットのイメージ

3.1.2 ウォレットのユースケース

ウォレットは、これまでに様々なデジタルサービスを利用するために提供きたが、今後の新たなデジタルサービスに対応したウォレットについても開発が進められており、そのユースケースは多岐に渡る。

このうち、ウォレットの代表的なユースケースとして、以下の３つのデジタルサービスが挙げられる。

(1) トラストサービス

ウォレットにより、ユーザが自分の情報を管理し様々なサービスと柔軟に相互連携できる仕組みは、自己主権型アイデンティティ（SSI: Self-Sovereign Identity）[60]の考え方に基づいており、ユーザ自身によるアイデンティティ管理を実現可能な仕組みとして注目されている。

このようなウォレットは、デジタルアイデンティティウォレット（DIW: Digital Identity Wallet）と呼ばれ、デジタル証明書を保管することにより、サイバー空間上の身分証明や資格証明手段として、今後、様々なデジタルサービスに利用されることが想定されている。

現在、北米地域におけるモバイル運転免許証(mDL: Moblile driving license)や EU 加盟国における EU デジタルアイデンティティウォレット(EUDIW: European Union Digital Identity Wallet）など、様々な国において実装に向けた取組が進行中である[61]。また、日本においてもこれらの仕組みを基に、マイナンバーカード機能をスマートフォンに搭載する取組が進められている。

(2) 決済サービス

ウォレットは、リテール取引における主要なキャッシュレス決済手段として、近年、利用が急拡大している。この背景として、2010 年代以降のスマートフォンの世界的な普及[62]、金融機関 API の公開に伴う Fintech 事業者の拡大[63]、新型コロナウイルス感染症の影響によるキャッシュレス決済の急速な浸透等が挙げられる。

世界的なオンライン決済会社「WorldPay」の調査レポート「The Global Payment Report 2024」[64]によると、世界 40 か国における 2023 年のリテール決済額に占めるウォレットの割合は約 33%であり、決済手段として最も大きな割合を占めている。また、ウォレットによる決済は、既存のクレジットカード、デビットカード等のキャッシュレス決済手段についても置き換えつつあり、今後もその割合は増加すると見込まれている。

ウォレットによる決済は、決済サービス事業者に決済依頼を行うことで実施され、その方法として e コマース等に利用されるアカウント決済、NFC

を利用した非接触決済、QR コード等を利用したコード決済がある。また、QR コード決済には、コードの読み取り方式によっても種類が分かれる。

そして、これらの決済方法は、それぞれの特徴によってウォレットに必要な機能が異なるため、そのメリットやリスクも異なっている。

(3) web3 サービス

ウォレットによるユーザ主体のユーザ情報管理の仕組みは、ブロックチェーン技術を活用した分散型ネットワークとの親和性が高い。そのため、暗号資産、非代替性トークン（NFT: Non Fungible Token）等、ブロックチェーン技術を応用した web3 サービス[65]におけるインターフェースとして、web3 ウォレットが利用されている。

web3 ウォレットは、ブロックチェーン上の暗号資産等を管理するための秘密鍵を生成・管理する機能を持つ。そして、ウォレットは、秘密鍵の保管方法により区分され、管理方法の様々な仕組みが考案され実装されている。

非中央集権的な web3 サービスは、技術面及び制度面において、既存のサービスと馴染まない部分はあるものの、既存のデジタルサービスを技術的に補完又は代替し、イノベーションを促進する可能性があるものと考えられていることから、様々な国において、web3 サービスの開発及びユースケースの検討が進められている[66]。

これらのユースケースにおいて、ウォレットの担う役割は異なっている。したがって、デジタルサービスごとにウォレットの機能も異なるものとなっている。

現在、ウォレットの課題として、相互運用性や大規模プラットフォーマーによる寡占の課題等も存在しているが、将来的には DIW を連携基盤として様々なデジタルサービスと連携可能なウォレットが登場することで解決していく可能性がある。

以下の節では、これらのデジタルサービスにおけるウォレットの機能について、特に技術的な観点から説明する。

3.2 DIW

3.2.1 DIWの概要

DIW は、現実空間及びサイバー空間上のサービス利用におけるユーザのアインデンティティ情報を、ユーザ自身で管理するためのウォレットである。ユーザは、自分のアイデンティティを証明するための電子データであるデジタル身分証明書、デジタル資格証明書等を、自らの保有するウォレットに保管する。これらのデジタル証明書は、法制度、運用手続き等に基づき、物理的な身分証明書、資格証明書等と同等の本人確認手段及び資格証明手段として取り扱われる。

DIW によるアイデンティティ管理の仕組みは、これまでのアイデンティティ管理の仕組みとは異なる特徴を持つ。これまでは、ユーザにデジタルサービス等を提供するデジタルサービス事業者において、個々にユーザのアイデンティティ管理を行う集中モデル、又は、アイデンティティプロバイダ（IdP: Identity Provider）がユーザのアイデンティティ情報を一括管理し、様々なデジタルサービスとの連携を行う連携モデルが主流となっていた。これらはいずれも、ユーザからアイデンティティ情報の管理を委託されたデジタルサービス事業者又は IdP による、中央集権的な管理の仕組みであった。このような中央集権的な管理方法では、ユーザのアイデンティティ情報にアクセス可能なデジタルサービス事業者又は IdP において、アイデンティティ情報の漏えい、改ざん、不正利用等のリスクが存在する。また、今日のデジタルサービスにおける主要な IdP は大規模プラットフォーマーが寡占している状態にある。このため、ユーザはデジタルサービスの利用において、大規模プラットフォーマーに依存せざるを得ない状態となっており[67]、そのことによる弊害やリスクが課題となっている[68]（表 1 参照）。

一方、DIW を利用することによって、ユーザは、アイデンティティ情報をユーザ自身で管理可能となることから、これらの弊害やリスクの低減が図られる。また、ユーザの DIW を起点として、デジタルサービス事業者やプラットフォーマーの垣根を越えた柔軟なデジタルサービス連携が可能となり、デジタルサービスの相互運用性が向上するだけでなく、特定のプラットフォーマーへの過度な依存についても抑制される。

表１　大規模プラットフォーマーへの過度な依存による課題

弊害・リスク	概要
ユーザロックイン	特定のプラットフォームへの過度な依存の結果、他のプラットフォームへの移行が困難となり、データ流通の不均衡や健全なデータの利活用が阻害される。
セキュリティのリスク	大量のアイデンティティ情報を保管する IdP が外部攻撃を受けた場合、被害は甚大となる。また、悪意ある IdP が無断で、ユーザのアイデンティティ情報を改ざんする可能性がある。
アクセシビリティのリスク	災害、外部攻撃等により IdP が停止した場合、デジタルサービスが利用できなくなる。また、悪意ある IdP が、ユーザに無断で、ユーザへのデジタルサービス提供を停止する可能性がある。
プライバシーのリスク	IdP は、IdP と連携するデジタルサービスに関するユーザの利用履歴を把握可能である。また、IdP がユーザに無断でユーザの利用履歴を流用しても、ユーザからは分からない。

参考:「令和 5 年版　情報通信白書」、「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」を基に作成

3.2.2　DIW の機能

DIW に保管されるデジタル身分証明書、デジタル資格証明書等には、物理的な身分証明書等と同様のアイデンティティ情報が記録され、これらのデジタル証明書は、記録された情報が真実であることを証明するものである。これらの証明書に記録される情報には、一般的に、氏名、生年月日、顔写真、性別、住所等、ユーザ固有の特徴に関する属性情報、及び証明書の管理番号、発行年月日、有効期限、資格情報、カード IC 情報等、証明書の発行者において登録されたユーザの属性情報が、データ要素として含まれる[69,70]。

ユーザは、デジタルサービスの利用において、「発行者」から発行されたこれらのデジタル証明書を、物理的な証明書と同様に、デジタルサービス事業者に提示する。デジタルサービス事業者は「検証者」として、提示されたデジタル証明書の内容を検証する属性認証を行い、それがユーザ本人から提示されていることを確認した上で、ユーザのデジタルサービスへのアクセスを認可する。

このように、DIW に保管されるアイデンティティ情報は、デジタルサービス事業者による属性認証において、発行者により確認及び登録されたことが担保されたユーザ属性情報として取り扱われる（以下、本節において、DIW に保管されるアイデンティティ情報を、「属性証明情報」と言う。）。したがって、DIW は、デジタルサービス事業者がユーザの属性認証を行う際に必要な属性証明情報をデジタルサービス事業者に提供する、属性認証サーバとして機能する[71]。

一方、ユーザは、デジタルサービスの利用に先立ち、属性証明情報を DIW に保管する必要があるため、DIW を通じて、発行者に対して属性証明情報の発行申請を行う。この場合、DIW は、発行者に対して属性認証のための属性証明情報を要求するユーザのクライアントアプリとして機能する[72]。

したがって、DIW は、デジタルサービス事業者に対しては属性認証サーバとして機能するとともに、発行者に対しては属性認証のクライアントアプリとして機能する。

3.2.3 DIW のシステム

ウォレットを利用した属性認証システムのデータモデルについては、Web 技術の標準化団体である W3C（World Wide Web Consortium）が提唱する“Verifiable Credentials Data Model v1.1[73]（以下、「VC データモデル」と言う。）”が、W3C 勧告として標準化されている。この VC データモデルは、発行者以外の第三者による暗号的な検証が可能な属性証明情報である、検証可能な資格情報（VC: Verifiable Credential）の発行から検証に至る一連の処理プロセスをモデル化したものである。

VC データモデルに基づく属性認証システムの構成及び各構成要素の役割は、図 2 のとおりであり、その処理プロセスは、以下のとおりである[74]。

① 発行

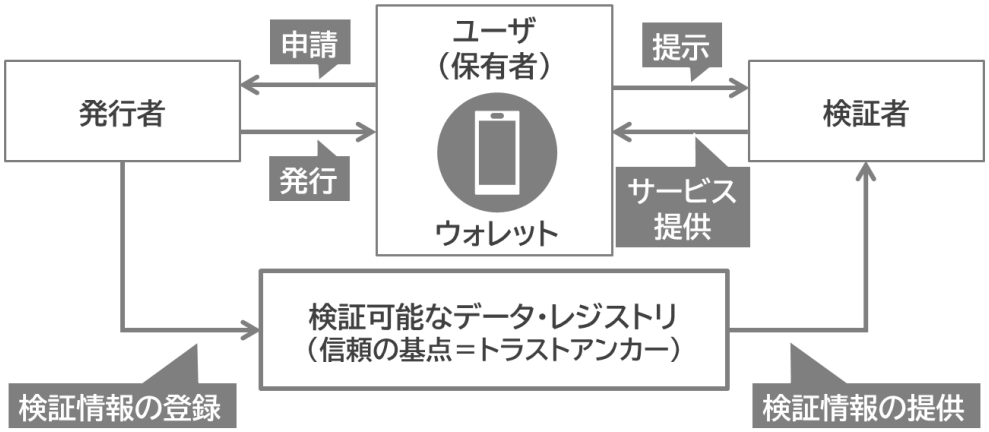
ユーザは発行者に属性証明情報の発行を申請する。発行者は、発行者の署名を付与した属性証明情報を生成し、ユーザに発行するとともに、署名の検証に必要な公開鍵証明書を検証可能なデータ・レジストリに登録する。

② 保管

ユーザは発行された属性証明情報をウォレットに保管する。ウォレットに保管された属性証明情報は、ユーザ以外に公開されず、破損、紛失等がないことについて信頼可能であることが前提となる[75]。

③ 検証

ユーザは検証者からの要求に応じて、ユーザの署名を付与した属性証明情報を検証者に提示する。検証者は、検証可能なデータ・レジストリに登録された発行者の公開鍵証明書を利用して、属性証明情報の検証を行う。



構成要素	役割
ユーザ （保有者）	ウォレットの保有者かつ大抵の場合は属性証明情報の発行対象者であり、属性証明を行うために DIW を利用する個人又は法人
発行者	ユーザからの申請に基づき、ユーザの属性証明情報を、発行者以外の第三者による暗号的な検証が可能な形式で発行する機関、組織等
検証者	ユーザにデジタルサービスを提供するデジタルサービス事業者であり、提示された属性証明情報に基づく属性認証を行う
検証可能な データ・レジストリ	ユーザの属性情報や発行者の公開鍵証明書の登録、属性証明の連携、仲介等に利用される場合がある、信頼済みのレジストリ

図 2　VC データモデルに基づく属性認証のシステム及び各構成要素の役割

参考："Verifiable Credentials Data Model v1.1, Figure 1 The roles and information flows forming the basis for this specification." を基に作成

このように、VC データモデルは、これまでのアイデンティティ管理において、デジタルサービス事業者や IdP が行っていた発行プロセスと検証プロセスの双方を分離したモデルとして示される。属性証明情報の検証は、検証可能なデータ・レジストリに登録された発行者の公開鍵証明書を利用して、ユーザと検証者の二者間で行われる。このため、発行者において、ユーザのデジタルサービス利用履歴の把握は不可能となり、ユーザのプライバシーが保護される。

上記の検証プロセスにおいて利用される発行者の公開鍵証明書は、属性証明情報が正当な発行者から発行され、改ざんされていないことを、発行者からユーザ及び検証者に対して保証するトラストアンカーとなるものである。ただし、VC データモデルは、ユーザがウォレットを保有している前提のモデルであるものの、実際には、ユーザが必ずしもウォレットを保有していない場合がある。例えば、ウォレットがインストールされたスマートフォン等のデバイスの盗難、悪用、不正アクセス等により、悪意ある第三者がユーザのウォレット、又はユーザのウォレットに発行された属性証明情報を不正に取得し、検証者に提示することによる、なりすましや不正利用が発生するリスクがある。

したがって、VC データモデルに基づいて、DIW をデバイスにインストールして運用することを想定した場合、ウォレットとユーザの同一性を確保し、ユーザの本人性を保証可能な仕組みが求められる。

3.2.4 DIW におけるユーザの本人性保証

3.2.3 項に記載したとおり、モバイルデバイスによる DIW の運用を想定した場合、図 2 におけるユーザという構成要素はさらに、ユーザとウォレットに分離できることから、ウォレットのシステム構成については、図 3 のように表すことができる。

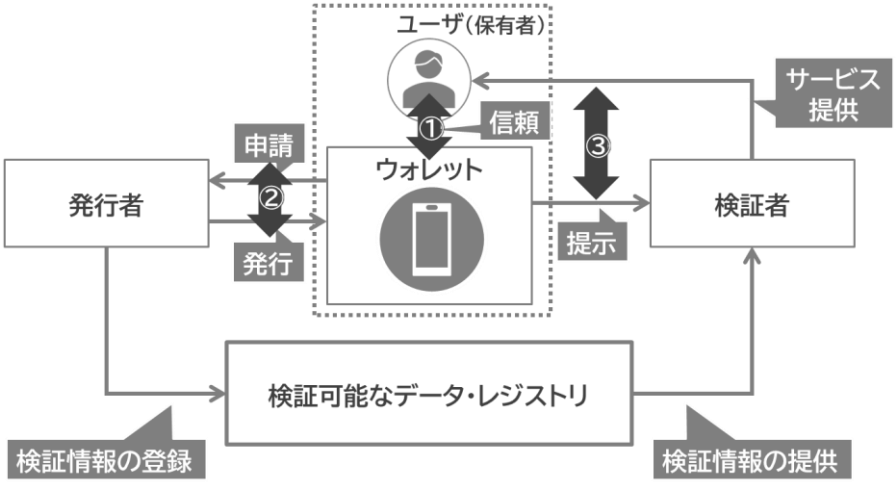


図 3 VC データモデルに基づくウォレットのシステム

参考："Verifiable Credentials Data Model v1.1, Figure 1 The roles and information flows forming the basis for this specification" を基に作成

図 3 のとおり、発行者がユーザに発行する属性証明情報は、実際にはウォレットに発行されることとなる。また、ユーザが検証者に提示する属性証明情報についても同様に、ウォレットから提示される。このため、検証プロセスにおいてウォレットとユーザの同一性を確保し、ユーザの本人性を保証するためには、検証者に対して、ウォレットから提示される属性証明情報とユーザが紐づいたものであることを保証可能な仕組みが必要となる。

このような仕組みの実装においては、以下の三つの要件を満たす必要がある。

(1) ユーザによって、ウォレットとユーザが紐づけられていること

本要件については、ウォレットがインストールされたデバイス及びウォレットアカウントへのログインにおける適切なユーザ認証によって、デバイスとユーザのウォレットアカウントを紐づけることで保証される。

ウォレットアカウントは、ウォレットの初回起動時にユーザが設定し、ウォレットの提供元であるウォレットプロバイダに登録される。ウォレットアカウントのユーザ認証に、デバイスの機能を利用した生体認証や多要素認証、

認証器等を利用することによって、より高度な保証が可能となる。

(2) 発行プロセスにおいて、ウォレットと属性証明情報が紐づけられること

本要件については、発行者において、属性証明情報をウォレットと紐づけて発行することによって保証される。具体的には、ウォレットにおいて生成される公開鍵と秘密鍵の鍵ペアを利用して、発行者において生成される属性証明情報がウォレットと紐づけられる。このような属性証明情報とウォレットの紐づけの仕組みを、キーバインディング（Key Binding）[76]と言う。

キーバインディングに係る処理プロセスは、図 4 のとおりである。

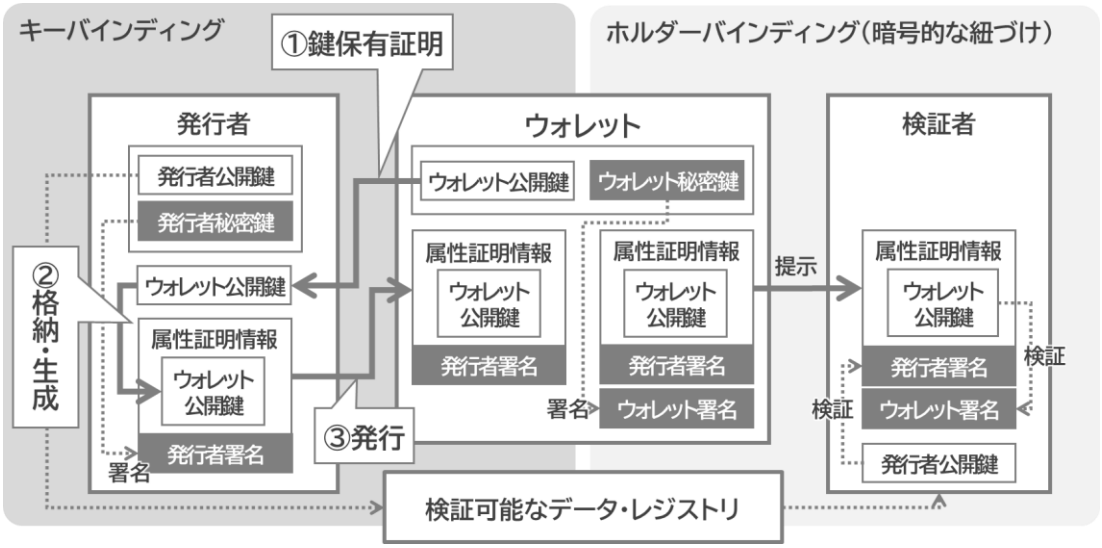


図 4　バインディングの仕組み

参考：「OpenID for Verifiable Credential Issuance 2.5.1 キーバインディング」を基に作成

キーバインディングにおいて、発行者はウォレットからの発行申請に対して、乱数チャレンジを返送する。ウォレットは、送付された乱数チャレンジに対して、ウォレットの秘密鍵による署名を生成し、当該秘密鍵のペアとなる公開鍵及びユーザの属性情報と合わせて発行者に送付する。発行者は、ウォレットから送付された情報に基づき、署名の検証を行い、ウォレットの公開鍵が有効なものであることを確認する。このようなウォレットの公開鍵の有効性を証明するプロセスを鍵保有証明（Proof-of-Possession Key）[77]と言う。発行者は、鍵保有証明によって有効性が確認されたウォレットの公開鍵を格納した属性証明情報を生成し、ウォレットに発行する。

なお、ウォレットに紐づく鍵ペアは、ウォレットがインストールされるデバイス又はウォレットプロバイダにおいて生成される[78]。

(3) 検証プロセスにおいて、ユーザと属性証明情報が紐づけられること

本要件については、上記の二つの要件が保証されていることを前提に、ウォレットから検証者に提示された属性証明情報が、ウォレットの提示者に紐づいたものであることを確認することによって保証される。このような、ウォレットの属性証明情報とウォレットの提示者の紐づけを、ホルダーバインディング（Holder Binding）[79]と言う。ホルダーバインディングは、表 2 に示す三つの方法によって紐づけが行われる。

表 2　ホルダーバインディングにおける紐づけ方法

分類	紐づけ方法
属性情報による紐づけ（Claims-based Holder Binding）	検証者において、物理的な運転免許証、身分証明書等に含まれるユーザの属性情報と、提示された属性証明情報に含まれるユーザの属性情報を照合する方法
生体情報による紐付け（Biometrics-based Holder Binding）	検証者において、ウォレット提示者の顔や指紋など、ウォレット提示者に固有の身体的特徴と、提示された属性証明情報に含まれる顔写真、生体情報等を照合する方法
暗号的な紐づけ（Cryptographic Holder Binding）	ウォレットにおいて、キーバインディングにより属性証明情報に格納されたユーザの公開鍵のペアとなるユーザの秘密鍵による署名を生成し、属性証明情報に付与する方法

参考："OpenID for Verifiable Presentations - draft 24, 2. Terminology" を基に作成

表 2 の紐づけ方法のうち、「属性情報による紐づけ」及び「生体情報による紐づけ」については、提示された属性証明情報を他のユーザ情報と比較、照合する必要がある。この場合、発行者の公開鍵証明書を利用した属性証明情報の検証後に、検証者によるホルダーバインディングが必要となる。

一方、暗号的な紐づけについては、検証者に提示される前に、ウォレットにおいてホルダーバインディングが行われる（図 4 参照）。

3.2.5 DIW のセキュリティ機能

3.2.4 項に記載したとおり、ウォレットの検証プロセスにおいてウォレットとユーザの同一性を確保し、ユーザの本人性を保証するためには、ユーザの認証情報やウォレットの秘密鍵を利用する必要がある。このため、ウォレットには、ユーザ認証情報や秘密鍵等の機密情報を確実に保管・保護するとともに、暗号化等の機密性の高い処理を安全に行うためのセキュリティ機能が求められる。

セキュリティ機能については、ウォレットはデバイス上で動作するアプリで

あり、その脆弱性に起因するハッキングや情報漏えいのリスクは大きいものとなる。このため、ウォレットがインストールされるデバイスのセキュリティ機能が利用され、その実装方法としては、デバイス内の仮想環境、又は独立したハードウェアを利用する方法がある[80]。

このうち、デバイス内の仮想環境による実装は、デバイスの CPU 上に構築される隔離環境において、デバイスの OS 機能と切り離して機密情報を処理する方法[81]である。ただし、この方法では、セキュリティ機能の実行において、OS や他のアプリの処理とデバイスの CPU やメモリを物理的に共有することとなるため、共有に伴う脆弱性を突いた外部攻撃による情報漏えいのリスクがある[82]。

一方、ハードウェアによる実装は、セキュリティ機能の実行環境として、物理的に独立した、信頼の起点（RoT: Root of Trust）[83]となるハードウェアを利用する方法[84]である。RoT ハードウェアの実装方法として、セキュアエレメント（SE: Secure Element）、UICC（Universal Integrated Circuit Card）等のセキュア IC チップをデバイスに組み込む方法、又は物理的に接続する方法[85]、さらには、クラウド上の HSM（Hardware Secure Module）にネットワーク接続して利用する方法がある[86]。ハードウェアによる実装は、RoT ハードウェアを利用した強固な暗号化処理が可能であり、アプリや OS の脆弱性から隔離されるだけでなく、物理攻撃への耐性もあることから、安全性が高い[87]。

これらのセキュリティ機能が実装されたデバイスのセキュリティ強度については、IT 製品、システム等の評価に関する国際標準規格 ISO/IEC 15408 における評価保証レベル（EAL: Evaluation Assurance Level）として、満たすべきセキュリティ機能要件及びセキュリティ保証要件が 7 段階に区分され、定められている[88]。これらの要件に基づき、デバイスには、インストールされるウォレットの機能、役割等に応じた EAL を満たすセキュリティ機能が必要となる。

ただし、利用可能なセキュリティ機能についてはウォレットによって異なるだけでなく、セキュリティ機能の具体的な実装方法についても、Apple 社製デバイスにおける SEP（Secure Enclave Processor）[89]、Google 社の Android OS 搭載デバイスにおける KeyStore システム[90]、 Samsung 社製デバイスにおける Samsung Knox[91]等、デバイスベンダやデバイスの OS プロバイダで異なっている。

3.2.6 DIW の実装技術

DIW の機能に対しては、前述のとおり、ユーザの自己主権に基づく属性証明情報の利用において、高度なセキュリティとプライバシー保護を実現可能な

技術的な仕組みが必要となる。一方、DIW には、国境を越えた様々な場面において利用が可能な仕組みとして、透明性の高い技術によって実装されることも求められる。このため、DIW の技術仕様については、公開された国際的な標準仕様に基づく設計及び開発が行われている。

DIW に関する国際的な標準仕様の技術としては、W3C 勧告である VC データモデルに加え、mDL に関する国際標準規格 ISO/IEC 18013-5[92]が挙げられる。北米地域では、ISO/IEC 18013-5 に準拠した mDL の運用がすでに開始されており[93]、日本国内においても、マイナンバーカード機能のスマートフォン搭載技術として、ISO/IEC 18013-5 に基づく技術検証、要件検討等が行われている[94]。

一方、欧州連合（EU）において発行が予定されている EUDIW は、VC データモデル及び ISO/IEC 18013-5 の両方に準拠した仕様として規定されている[95]。

以下の項では、ISO/IEC 18013-5 に準拠した mDL の技術仕様、及び EUDIW における実装が予定されている技術仕様について説明する。

3.2.7 ISO/IEC 18013-5

3.2.7.1 ISO/IEC 18013-5 の概要

ISO/IEC 18013-5 とは、mDL を実装するためのインターフェース仕様を定めた国際標準規格である。本規格は、mdoc データ[iv]の提示に関するトランザクション及びセキュリティを標準化することによって、運転免許証の利便性、相互運用性及びプライバシーの向上を図るものとして定められている。mdoc データとしては、mDL 以外に、様々な種類のモバイル資格情報等への適用も想定されている[96]。また本規格は、ユーザと検証者が近接した状態における対面型の提示及び検証プロセスを想定した仕様であり、ネットワーク上での提示及び検証については、ISO/IEC 18013-7 として 2024 年に標準化されている[97]。

なお、mDL は、モバイルデバイスに常駐可能な mdoc データとして交付され[98]、ISO/IEC 18013-1 において規定する ISO 準拠の運転免許証と同等の機能を果たすものとして定められている[99]。

3.2.7.2 ISO/IEC 18013-5 のシステム

ISO/IEC 18013-5 に準拠した mDL のシステム構成は図 5 のとおりである。

ISO/IEC 18013-5 では、検証プロセスにおいて、検証者は発行当局の認証局から、公開鍵証明書を取得する仕組みとして定められている。ただし、運転

[iv] mdoc（モバイルドキュメント）データ、スマートフォンなどのモバイルデバイスに公式な証明書や ID 情報を格納するためのデータ形式。

免許証は国や州によって異なる管理が行われ、旅券における国際民間航空機関（ICAO）のような国際的な管理組織が存在しないため、検証者は mDL の検証に対して、様々な国や州の発行当局から公開鍵証明書を取得する必要が生じることとなる。

この課題に対して ISO/IEC 18013-5 では、検証済み発行者認証局リスト（VICAL: Verified Issuer Certificate Authority List）プロバイダの役割について規定している[100]。VICAL プロバイダは、様々な発行当局の妥当性について定期的に確認を行い、発行当局の認証局から収集した公開鍵証明書をリスト化した VICAL の安全確保を行うとともに、VICAL を検証者に配布し、普及させる役割を担う。

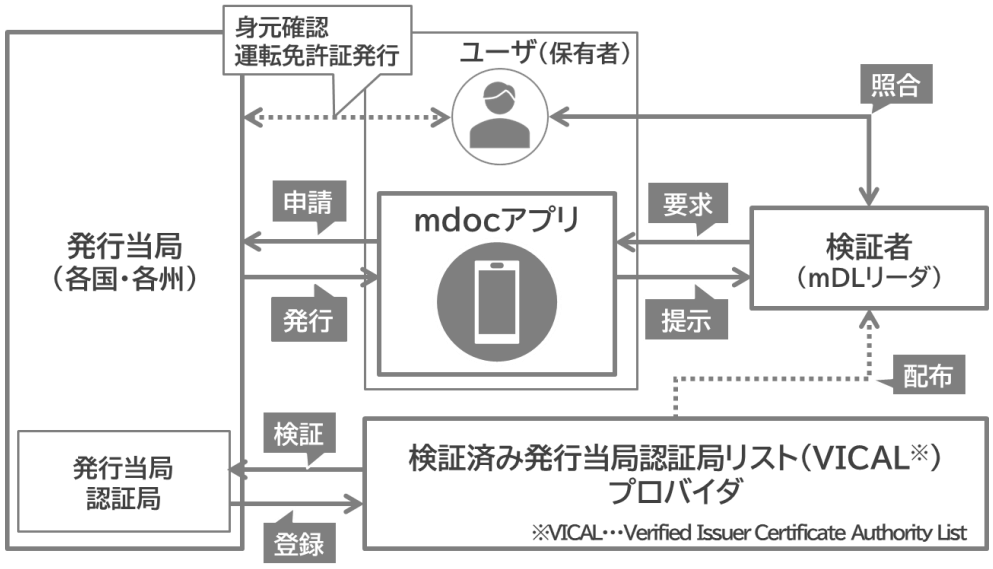


図 5　ISO/IEC 18013-5 に準拠した mDL のシステム構成

参考：“ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application “を基に作成

3.2.7.3　ISO/IEC 18013-5 における処理の流れ

ISO/IEC 18013-5 における mDL の提示及び検証プロセスは、mDL が保管されているウォレットと、検証者の mDL リーダとの間でデバイスのエンゲージメントが行われた後、mDL データの交換が行われる[101]。エンゲージメントでは、mDL データの取得方法、mDL データ取得における暗号化情報等に関する情報が交換される[102]。また、エンゲージメント情報の伝送には近距離無線通信（NFC: Near Field Communication）又は QR コードが利用される[103]。

エンゲージメント後、ウォレットと mDL リーダとの間で mDL データが交換され、mDL リーダにおいて、mDL の検証が行われる。

なお、ISO/IEC 18013-5 における mDL の検証については、発行当局の公開鍵証明書に基づいて検証が行われる必要がある。このため、ISO/IEC18013-5 に準拠した後述の米国の取組において、ユーザのモバイルデバイス上に表示された mDL を検証者が目視で検証する方法（flash pass）については、悪用リスクがあるとされ、mDL の検証方法として認められていない[104]。

ISO/IEC 18013-5 では、検証者が mDL を検証するための mDL データの取得方法として、以下の二つの方法が規定されている[105]。

① デバイス取得

ウォレットと mDL リーダとの間で mDL データの交換が行われる。mDL データの取得には、基本的にはデバイス取得によって行われる。デバイス取得における mDL データの伝送には NFC、BLE（Bluetooth Low Energy）、又はオプションとして Wi-Fi Aware が利用可能である[106]。

② サーバ取得

mDL リーダは、エンゲージメントにおいてウォレットから受信したサーバ取得トークンに基づき、発行当局サーバに対して、ネットワーク経由で mDL データの取得が行われる。mDL データの伝送には Web API 又は OpenID Connect が利用される。なお、ISO/IEC 18013-5 では、サーバ取得はオプション扱いである[107]。

このように、ISO/IEC 18013-5 では、デバイス検索によるオフライン環境下での、ウォレットと mDL リーダの二者間による検証が可能な仕組みとして規定されている。このため、ユーザの mDL はユーザデバイスに保管されている必要があることから、ユーザデバイスには、mDL を安全に保管するためのセキュリティ機能が求められ、米国での取組では SE 等のセキュリティモジュールを組み込む必要があるとされる[108]。

また、ISO/IEC 18013-5 における mDL の検証は、検証者が、mDL リーダによる mDL の真正性の検証後、mDL データに含まれる顔画像と mDL の提示者の顔を照合することによってホルダーバインディングを行い、ユーザの本人性を保証する必要がある[109]。このため、mDL データにはユーザの顔画像が含まれている必要があり[110]、顔画像の仕様については、運転免許証の機械読取技術に関する国際標準規格 ISO/IEC 18013-2 における要件を満たす必要がある[111]。

3.2.7.4　ISO/IEC 18013-5 における選択的開示

ISO/IEC 18013-5 で示されている mdoc データの構造は、構成するユーザの属性情報を、個々の属性ごとのデータ要素として格納する構造であり[112]、ユーザのプライバシー保護のためのデータ最小化及び選択的開示への対応が図

られている[113]。

このようなデータ最小化及び選択的開示のユースケースとして、店舗等における酒類の購入時に、年齢確認のための身分証明書の提示が求められた場合を例に説明する。従来の紙、カード等による運転免許証の提示では、運転免許証の券面記載情報が全て開示されるのに対して、mDL では、年齢に関する情報のみの提示が可能となる。また、年齢についても、購入可能な年齢以上か否かについて証明可能なデータ要素が含まれれば、年齢を開示しなくても、酒類の購入が可能となる。このような仕組みにより、ユーザのプライバシーが強化される。

米国で検討されている mdoc データのデータ構造は図 6 のとおりである[114]。

図 6　mdoc データのデータ構造

参考：“Docs, mdocs, Structure to Function[115]” を基に作成

mdoc データのデータ構造には、属性証明情報として個々の属性ごとのデータ要素から構成される namespace、発行機関の文書署名者（DS: Document Signer）による署名が付与された MSO（Mobile Security Object）等が含まれる。また、MSO には、namespace に含まれる個々のデータ要素のダイジェスト、ユーザデバイス公開鍵等が格納されている。

検証者はユーザに対する mDL の提示要求において、namespace に含まれるデータ要素ごとに要求を行う。ユーザは必要最小限のデータ要素のみ要求されていることを確認した上で、要求されたデータ要素だけが含まれる mDL デ

ータを提示する[115]。この場合、選択的開示によって namespace に含まれるデータ要素の一部だけ選択されても、MSO のダイジェスト及び MSO に含まれる DS 署名の値は変わらないため、mDL データの真正性は保証される。

3.2.7.5　北米地域における mDL の運用状況

米国では 2019 年から米国自動車管理者協会（AAMVA: American Association of Motor Vehicle Administrators）によって、ISO/IEC 18013-5 に準拠した mDL の試験運用が開始され、これまでに 14 の州及び地域において運用されている（2025 年 3 月時点）[116]。AAMVA は、北米地域における自動車管理に関する技術、システム等の開発やサービス提供等を行う非営利団体であり、mDL の VICAL プロバイダとして、北米地域における mDL のトラストサービスの提供も担っている[117]。

AAMVA における mDL の仕様については、AAMVA が発行する“Mobile Driver's License Implementation Guidelines[118]”に mDL の実装ガイドラインとして取りまとめられている。このガイドラインは、州ごとに異なる運転免許証の発行形態や、運転免許証が身分証明書として利用される米国内の事情を踏まえ、2025 年 5 月に施行予定の Real ID 法[119]に準拠した身分証明書としての利用も見据え、ISO/IEC 18013-5 を拡張した仕様となっている[120]。

現在、北米地域における mDL は、米国内の様々な州や地域において相互運用に向けた取組が進められているだけでなく、カナダにおいても、相互運用に向けた検討が行われている。

3.2.7.6　マイナンバーカード機能等のスマートフォン搭載

日本では、新型コロナウイルス感染症対策の経験から、緊急時における迅速かつ確実な行政サービスの提供を実現するため、マイナンバー制度に基づくデジタル基盤の抜本的改善の一環として、令和 2 年から、マイナンバーカードのスマートフォン搭載に関する検討が行われてきた[121]。

令和 5 年 5 月から、GlobalPlatform 仕様に対応した SE を搭載する Android 端末を対象に、マイナンバーカードの IC チップに記録された電子証明書をスマートフォンに搭載する、スマホ用電子証明書搭載サービスが開始された[122]。これにより、スマホ用電子証明書を搭載したスマートフォンから、マイナンバーカードで利用できる公的個人認証サービスの利用が可能となった[123]。

令和 5 年 8 月には、「マイナンバーカード機能等のスマートフォン搭載に係る実証事業（技術検証・要件検討）」[124]の公募が行われ、その実証事業において ISO/IEC 18013-5 に準拠したマイナンバーカード情報をスマートフォンに格納し、発行、管理するためのシステムの実証的な開発・検討が行われた[125]。

また、令和 6 年 5 月にマイナンバー法が改正され、マイナンバーカードの券面記載事項（氏名、生年月日、住所、性別、マイナンバー、顔写真）をスマートフォンに搭載可能となった[126]。これにより、ユーザはマイナンバーカードと同等の機能をスマートフォンに搭載し、スマートフォンによる行政手続等における本人確認ができるようになる[127]。

今後、令和 7 年春頃に、Apple 社の iPhone において、マイナンバーカード機能が搭載される予定である[128]。

3.2.8 EUDIW

3.2.8.1 EUDIW の概要

EUDIW は、EU 加盟国で発行されるデジタル ID、属性証明書、公的文書等を電子的に保管及び使用可能な DIW である。eIDAS 改正規則[129]により、各加盟国は、EUDIW の実装における機能要件等について別途定める EUDIW 実施規則の制定後、24 か月以内に EU 域内の全ての市民、居住者及び企業に対して、EUDIW を発行し、無償で提供することが義務付けられている[130]。なお、EUDIW 実施規則については、2024 年 11 月に制定されたことから[131]、EUDIW は 2026 年 11 月までに提供が開始される予定である。

EUDIW については、eIDAS 改正規則の考え方を踏まえ、ユーザによる主体的なアイデンティティ管理を基本として、柔軟な相互運用性、高度なセキュリティ、プライバシー強化等を満たすものとして設計することが求められている[132]。

このような EUDIW の機能要件については、欧州委員会の要請に基づき、各加盟国の連携により整備された「技術アーキテクチャ及び参照フレームワーク[133]（ARF: the Architecture and Reference Framework）」に EUDIW 統一規格の策定のための参照情報として取りまとめられている。

ARF に基づき、EUDIW の開発に必要なプログラムモジュールが公開され、EUDIW の参照実装等において検証が行われてきた[134]。ただし、ARF において開発が進められてきた技術には、標準化に向けた取組が進行中のものも含まれることもあり、2024 年 11 月に制定された EUDIW 実施規則において規定されている標準技術は、以下のとおりである。

・データフォーマット：W3C VC データモデル及び ISO/IEC 18013-5[135]
・検証プロトコル：ISO/IEC 18013-5 及び ISO/IEC 18013-7[136]
・仮名化技術：W3C WebAuthn[137]

なお、ARF については、検証結果等を踏まえ適宜改定されており、現時点では、2025 年 3 月に公開された ARF ver.1.6 が最新版である。以下の項では、ARF ver.1.6 の記載内容を踏まえ、EUDIW の技術仕様について説明する。

3.2.8.2 EUDIW のシステム

ARF において示されている EUDIW のシステムは図 7 のとおりである。

EUDIW は、様々な EU 加盟国の法制度に基づくデジタル ID や資格証明書、公的文書等を包括したアイデンティティ連携を実現する仕組みとして実装されることが求められている。このため、EUDIW のシステムは、技術的手段に基づく相互運用性を確保しつつ、制度や運用ポリシー等によって相互連携におけるトラストを確保する仕組みとして設計されている。

属性証明情報の発行機関である PID（Person Identification Data）プロバイダ及び各種 EAA（Electronic Attestation of Attributes）プロバイダ、並びにウォレットプロバイダは、eIDAS 規則等の法制度に基づき、各加盟国の評価機関等による認証を受ける必要がある[138]。認証済みの PID プロバイダ、EAA プロバイダ及びウォレットプロバイダについては、各加盟国における信頼済みリストの維持、管理を担う信頼済みリストプロバイダ（TLP：Trusted List Provider）によって、各組織の公開鍵証明書とともに認証済みリストに登録される[139]。また、EUDIW から提示される属性証明情報の検証を行い、検証結果に基づいてユーザにサービスを提供する RP（Relying Party）も、各加盟国の RP レジストラに登録を行い、正当な RP であることを保証するためのアクセス証明書の交付を受ける必要がある。各国の TLP に登録された発行機関及びウォレットプロバイダ、並びに RP レジストラに登録された RP の情報については、EU 域内のデジタル統一基盤から参照可能な信頼済みのリストとして、EUDIW のシステムに参加する全ての参加者に公開される[140]。このように、EUDIW のシステムの参加者は、デジタル統一基盤から信頼済みのリストを取得し、必要な証明書を取得することによって、EU 域内における連携時の相互認証が可能となる。

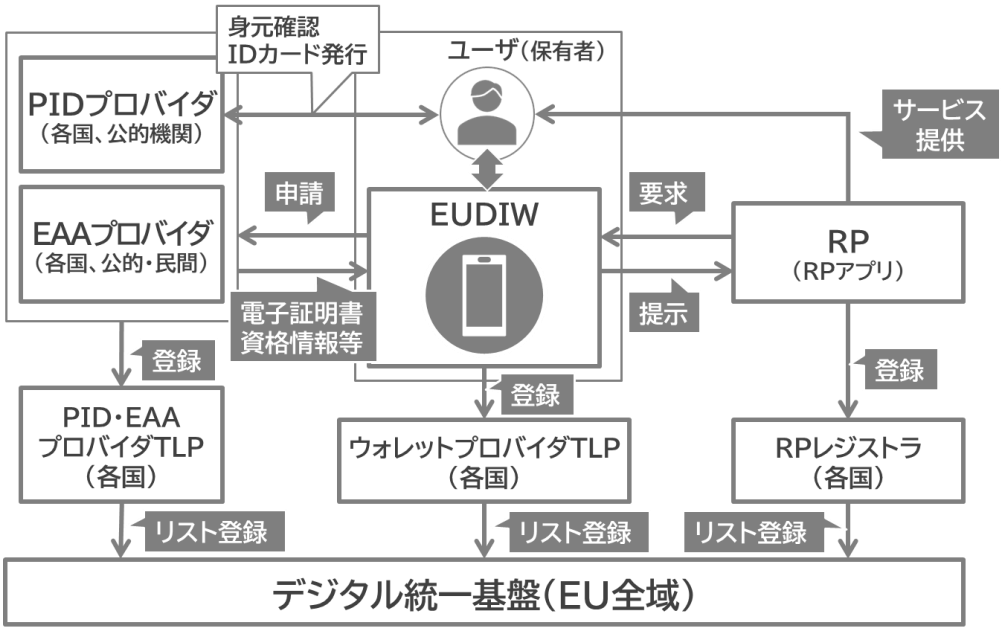


図 7　EUDIW のシステム構成

参考：“European Digital Identity Wallet Architecture and Reference Framework v1.6.0”を基に作成

3.2.8.3　EUDIW における選択的開示

EUDIW における属性証明情報のデータフォーマットについては、EUDIW 実施規則の規定に基づき、VC データモデルにおける JSON（the JavaScript Object Notation）フォーマット[141]及び ISO/IEC 18013-5 における CBOR（Concise Binary Object Representation）フォーマット[142]が利用される。このうち、EUDIW の参照実装においては、VC データモデルにおけるデータ最小化及び選択的開示の仕組みである SD-JWT（Selective Disclosure of JSON Web Token）についての検討が行われている。

SD-JWT は JWT（JSON Web Token）[143]を利用して選択的開示を実現するためのデータフォーマットであり、インターネット技術に関する標準化団体である IETF（Internet Engineering Task Force）において、現在標準化が進められている[144]。

SD-JWT のデータ構造は、図 8 のとおりである。

SD-JWT では、VC データにおける通常の JWT と異なり、VC データの本体である VC ペイロードに、ユーザの属性情報を表す個々のデータ要素から生成されたダイジェストが格納される。一方、ダイジェストの元となるデータ要素は、選択的開示可能なディスクロージャ（disclosure）として、発行機関の署名が付与された JWT（Issuer-Signed JWT）とは別に格納される[145]。このため、SD-JWT の検証において、ディスクロージャの一部だけが開示されても、Issuer-Signed JWT に含まれるダイジェスト及び発行機関の署名の値は

変わらないことから、SD-JWT の真正性は保証される。また、発行機関から発行された SD-JWT は、キーバインディングの公開鍵とペアとなる秘密鍵による署名（Key Binding JWT）を付与することによって、ユーザのウォレットにおける暗号的な紐づけによるホルダーバインディングが可能となる。

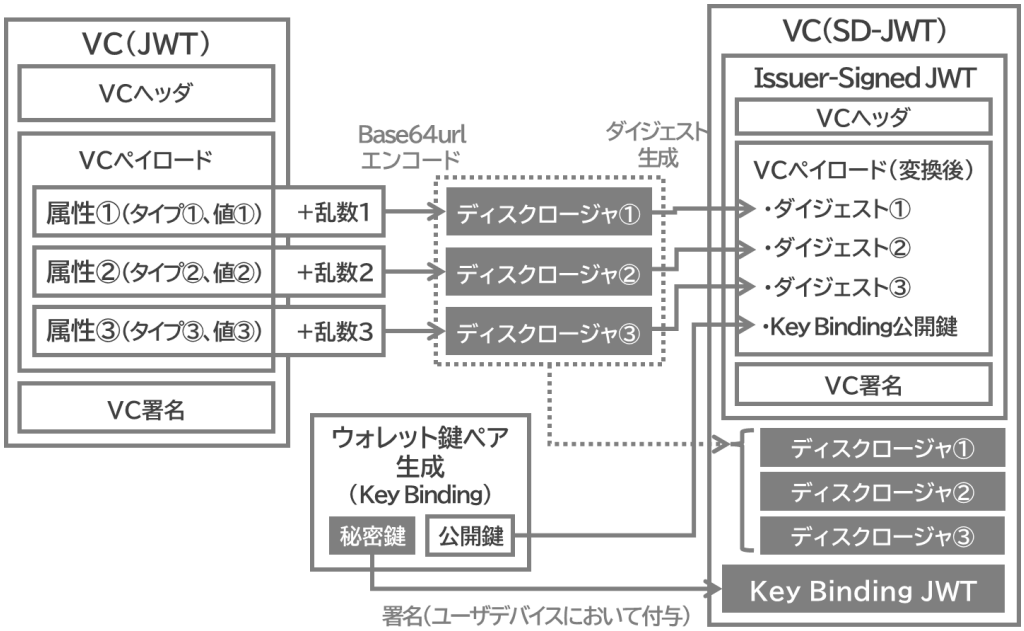


図 8　SD-JWT のデータ構造

参考："OpenID for Verifiable Credential Issuance 2.6.1. SD-JWT" を基に作成

3.2.8.4　EUDIW における仮名化技術

WebAuthn は、Web 認証における Web API の仕様に関する W3C 勧告技術であり[146]、EUDIW 実施規則における仮名化技術として規定されている。本技術は、ユーザ認証情報としてユーザの公開鍵を利用する認証方法であり、ユーザの公開鍵を利用した仮名化が行われる。具体的には、発行機関からの乱数チャレンジに対してユーザが秘密鍵で署名し、発行機関においてユーザの公開鍵を利用した署名の検証を行う、チャレンジレスポンスによるパスワードレス認証が行われる[147]。

WebAuthn で利用されるユーザの公開鍵及び秘密鍵の鍵ペアは、WebAuthn API と連携可能な認証器において生成される。認証器としては、ウォレットがインストールされたデバイスやデジタルサービス事業者が提供する認証サーバ等が利用される。認証器は、ユーザのパスワード、生体情報、認証器の PIN コード等と、認証器にあらかじめ登録された固有情報から、ユーザの公開鍵及び秘密鍵を生成する。ユーザの公開鍵は、認証器において生成される固有の識別子とともに、発行機関に登録され、ユーザの秘密鍵は認証器に保管される。

このため、認証器には強固なセキュリティ機能が求められる。EUDIW 実施規則では、認証器のセキュリティ機能について、デバイス内部の SE 等、又はクラウド上の HSM によるハードウェアとして実装することについて規定している[148]。

このように、WebAuthn は、ユーザの認証器を利用してユーザの識別子及び認証情報を管理し、認証器のトラストに基づいてユーザ認証を行う仕組みである。WebAuthn を利用することによって、ユーザ及び発行機関におけるパスワードの管理や共有が不要となり、従来のパスワード認証におけるパスワードの漏えい及び紛失リスクが解消される。また、WebAuthn における公開鍵暗号方式を利用した認証の仕組みは、中間者攻撃やフィッシング詐欺に対する耐性の高い認証方法である。さらに、ユーザの仮名化や認証情報の管理を行う認証器にはユーザ以外アクセスできないため、ユーザのプライバシー保護やセキュリティの向上が図られる。

3.2.8.5 EUDIW のユースケース

欧州委員会は、これまで、ARF において取りまとめた内容に基づき、EUDIW の開発に必要なプログラムモジュールを公開し、EUDIW の参照実装によるパイロットプロジェクトを支援してきた。パイロットプロジェクトは、金融サービス、教育、交通等、様々な分野に及ぶものであり、参照実装により得られた知見により、ARF で取りまとめられた技術仕様の検証及び改良が図られている。2023 年 5 月からは、四つの大規模パイロットプロジェクト（表 4 参照）が開始されており、2025 年まで継続される予定である[149]。これらの大規模パイロットプロジェクトには、26 の加盟国以外にノルウェー、アイスランド、ウクライナを含む、約 360 の公的機関及び民間組織が参加している。

また、EUDIW は eIDAS 改正規則以外の EU 法令に基づき、公私含む様々なデジタルサービスとの連携が行われる予定である。このうち、デジタルユーロについても、EU デジタルユーロ規則案[150]において、デジタルユーロ決済における本人確認及び決済の承認のために、希望するユーザが EUDIW を利用できるようにすることが提案されている。

表 4　EUDIW の大規模パイロットプロジェクト

プロジェクト名	プロジェクトの概要
EU Digital Identity Wallet Consortium (EWC)	EUDIW を利用した、加盟国全体で利用可能なデジタル渡航文書（DTC: Digital Travel Credential）の提供
POTENTIAL	6 つのユースケース（政府サービス、銀行口座開設、SIM（Subscriber Identity Module）契約、mDL、電子署名、電子処方箋）における EUDIW の連携
NOBID	EUDIW を利用した金融取引、支払い、送金等における欧州決済サービス指令（PSD2）に準拠した決済サービス連携等
DC4EU	EUDIW を利用した教育分野における教育資格、専門資格等及び社会保障分野における適用証明、健康保険証等の発行

参考：“What are the Large Scale Pilots”等を基に作成

3.3　決済用ウォレット

3.3.1　決済用ウォレットの概要

決済用ウォレットは、現実空間及びサイバー空間上の様々な取引におけるキャッシュレス決済手段を管理するためのアプリであり、決済サービス事業者に対して決済依頼を行うインターフェースとして機能する。

ユーザは、自身の保有する銀行口座、クレジットカード、プリペイドカード等のキャッシュレス決済手段、又は決済サービスのアカウントをウォレットに登録することにより、ウォレットによるキャッシュレス決済が可能となる[151]。

決済用ウォレットによるユーザの取引相手となる取引先は、決済端末等によって、ユーザから提示された決済用ウォレットの情報を読み取り、取引に係る決済情報と合わせて決済サービス事業者に決済依頼を行う。決済サービス事業者は、決済情報に基づく決済処理を行い、処理結果をウォレット及び取引先に通知する。このように、決済用ウォレットによる決済処理は、通常のキャッシュレス決済と同様、全て決済サービス事業者において行われる(図 9 参照[152])。

決済用ウォレットによる決済方法として、e コマース等におけるオンライン決済では、ウォレットアカウントを連携して決済を行うアカウント決済が利用されている[153]。また、対面決済では、NFC を利用した非接触決済又は QR コード等の二次元コードやバーコードを利用したコード決済が利用されている。利用可能な決済方法は、決済サービス事業者やウォレットプロバイダによって異なる。また、決済方法によって、ウォレットの機能や役割も異なる。

以下の項では、非接触決済及びコード決済について概説する。

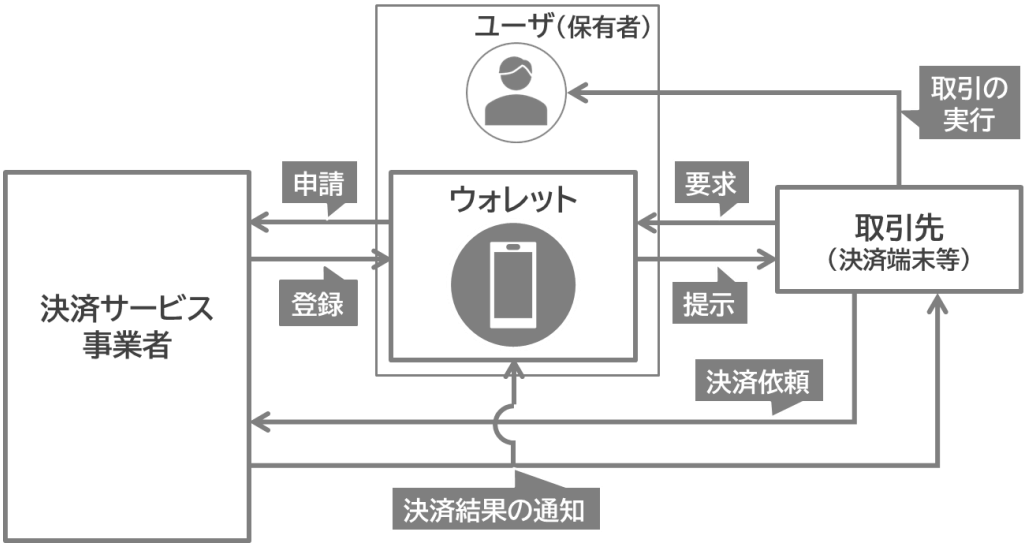


図 9　決済用ウォレットにおける処理の流れ

参考：「種類が多いスマホ決済を基礎から学ぼう」 等を基に作成

3.3.2　非接触決済

3.3.2.1　非接触決済の概要

非接触決済とは、NFC 対応の非接触 IC カードや NFC デバイス等を利用して、取引先となる店舗等の決済端末と無線通信で決済を行う方法である。このため、決済用ウォレットを利用した非接触決済を行うためには、ウォレットがインストールされるデバイスは NFC に対応している必要がある。

NFC の通信方式は、NFCIP（NFC Interface Protocol）として、国際標準規格 ISO/IEC 18092 （NFCIP-1）及び ISO/IEC 21481 （NFCIP-2）において技術仕様が定められている[154]。NFCIP は、非接触 IC カードの通信方式である NFC Type-A/B 及び Type-F に対応した通信方式である[155]。

ウォレットを利用した非接触決済では、NFC デバイス上で非接触 IC カードの動作を再現するカードエミュレーションモードが利用される。これは、NFC デバイスの相互運用に関する業界標準等の策定を行う NFC フォーラムにおいて規定された動作モードの一つである。これにより、ユーザは、カード会社から発行されたクレジットカード、デビットカード、プリペイドカード等の IC カード情報をウォレットに登録することによって、非接触 IC カードと同様に、ウォレットによる非接触決済を利用することができる。

3.3.2.2　トークナイゼーション

ウォレットに登録される IC カード情報はトークナイゼーションによって、同桁かつ別番号のトークンに置き換えられる。トークナイゼーションは、 IC カード取引に関する業界標準団体である EMVCo が定める EMV 規格技術である[156]。

トークナイゼーションの処理プロセスは、以下のとおり行われる[157]。

① ユーザは、保有する IC カードの番号をウォレットに入力し、カード発行会社にトークナイゼーションを依頼する。

② カード発行会社はユーザの本人確認を行い、EMVCo が認定するトークンサービスプロバイダに対して、①で入力されたカード番号を送信する。

③ トークンサービスプロバイダは、ランダムに生成されたトークンに基づく IC カード情報をウォレットに発行するとともに、①で入力された IC カード番号とトークンの紐づけを行う。

④ ①においてウォレットに入力したカード番号はトークンに置き換えられ、トークンサービスプロバイダから発行された IC カード情報がウォレットに登録される。

ウォレットを利用した非接触決済は、トークンサービスプロバイダから発行されたトークンに基づいて決済処理が行われる（図 10 参照）。トークンの元となるカード番号については、取引相手に提示されないだけでなく、ウォレットにも保管されないため、カード番号の漏洩リスクが低減される。加えて、日常におけるカード類の携行が不要となることから、カードの盗難、紛失リスクについても低減される。したがって、ウォレットを利用した非接触決済は、決済用 IC カード自体を利用する場合より安全性及び利便性が高い決済方法であると言える。

トークナイゼーションにおいてウォレットに登録される IC カード情報には、IC カードのオンライン認証に必要な暗号鍵情報が含まれる。オンライン認証には共通鍵暗号方式が利用され、トークンサービスプロバイダにおいて生成された暗号鍵情報が、ウォレットと共有される仕組みとなる[158]。このため、ウォレットがインストールされる NFC デバイスには、暗号鍵情報を安全に保管するためのセキュリティ機能が実装されている必要がある。NFC デバイスにおけるセキュリティ機能の実装方法については以下の 2 点が挙げられ、セキュリティ機能の実装方法によって、ウォレットに共有される暗号鍵情報は異なる。

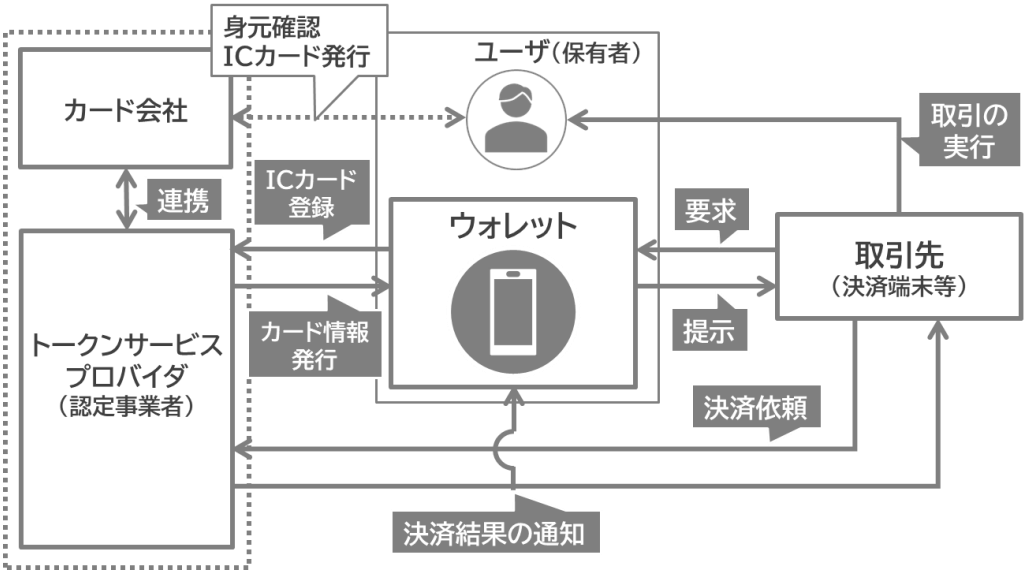


図 10　トークナイゼーションにおける処理の流れ

参考：“EMVCo Payment Tokenisation Specification Technical Framework v2.3” を基に作成

① SE 方式

SE 方式とは、ウォレットデバイスに組み込まれた SE を利用する実装方法である。IC カード情報は SE に保管され、NFC の送受信の処理は全て SE で行われる[159]。SE によって、IC カードと同等のセキュリティが保証されることから、ウォレットに共有される暗号鍵は、デバイス固有の共通鍵（UDK: Unique Derivation Key）として発行される[160]。

② HCE 方式

HCE（Host Card Emulation）方式とは、クラウド上の HSM を利用する実装方法である[161]。IC カード情報はクラウド上の HSM に保管され、NFC で送受信される情報は、デバイスの CPU 又は CPU 上の汎用 OS と隔離されたプログラム実行環境である TEE（Trusted Execution Environment）上で処理される。デバイスに SE が搭載されていない、あるいは SE を利用できない場合でも、HSM により非接触決済は可能となる[162]。ただし、IC カードと同等のセキュリティは保証されないため、共有される暗号鍵は期限付きの共通鍵（LUK: Limited Use Key）となり、定期的に更新・再発行される[163]。

3.3.3　コード決済

3.3.3.1　コード決済の概要

コード決済とは、店舗等の近接取引において、店舗等の決済端末のディスプレイや印刷物に表示される決済用コード（QR コード、バーコード等）をユー

ザのウォレットのカメラで読み取る、又はユーザのウォレットのディスプレイに表示される決済用コードを店舗等の決済端末で読み取る決済方法である。

コード決済の処理プロセスは、決済用コードを読み取った端末から決済サービス事業者に決済依頼が送信されることによって、決済処理が行われる。決済用コードの提示・読取方法については、以下の 3 つの方法がある。

(1) 静的 MPM

静的 MPM（Merchant-Presented Mode）とは、取引先が掲示する紙やステッカー等に印刷された決済用コードを、ユーザがウォレットで読み取り、ユーザのウォレットに取引金額を入力し、取引先がその金額を確認して決済依頼を行う方法である（図 11 参照）[164]。この時、決済事業者からの決済結果は、ユーザのウォレットにのみ通知されるため、取引先は、ユーザのウォレットに表示される通知を確認する必要がある。

静的 MPM に用いられる決済用コードには、決済サービス事業者に登録された取引先に関する固定情報が含まれている[165]。この決済用コードは、取引先が決済サービス事業者に加盟申請した際に、決済サービス事業者によって生成され、取引先に送付されたものである。

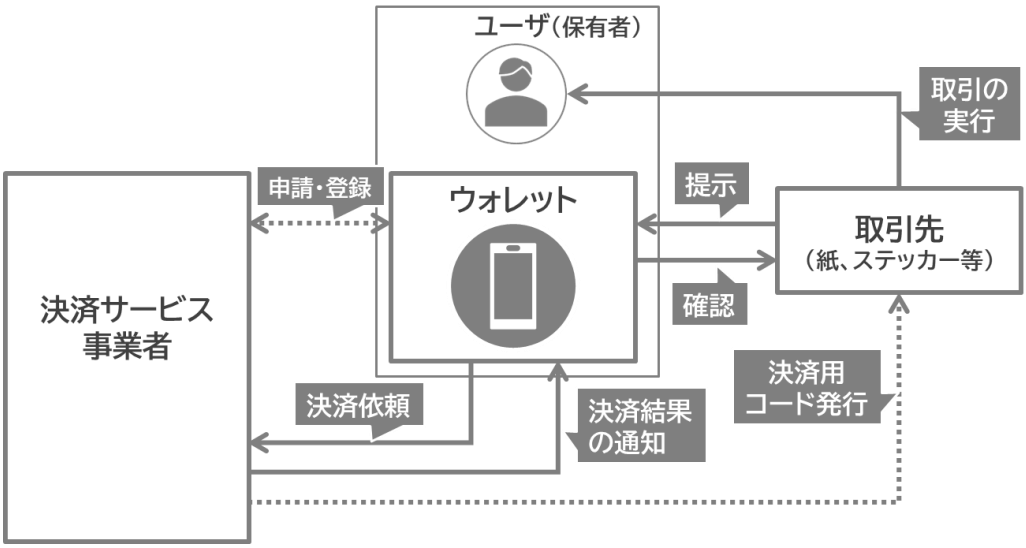


図 11　MPM 方式のコード決済における処理の流れ（図は静的 MPM）

参考：「コード決済に関する統一技術仕様ガイドライン【店舗提示型】 MPM(Merchant-Presented Mode) Ver.3.0」を基に作成

(2) 動的 MPM

動的 MPM とは、ユーザがウォレットで取引先の決済端末に表示される決済用コードを読み取り、ウォレットに表示される決済金額を確認し、決済依頼を行う方法である[166]。なお、決済結果は、ウォレット及び取引先の決済端末に通知される。

動的 MPM に用いられる決済用コードには、決済の都度、生成され、決済サービス事業者に登録された取引先に関する情報に加え、取引金額額等の動的情報が含まれる[167]。

(3) CPM

CPM（Consumer-Presented Mode）とは、ユーザのウォレットに表示される決済用コードを、取引先の決済端末から読み取り、取引先の決済端末から決済依頼を行う決済方法である（図 12 参照）[168]。

CPM に用いられる決済用コードには、決済 ID、決済サービス事業者の識別コード、ワンタイムトークン等が含まれ、決済の都度、生成される[169]。決済結果はユーザのウォレット及び取引先の決済端末に通知される。

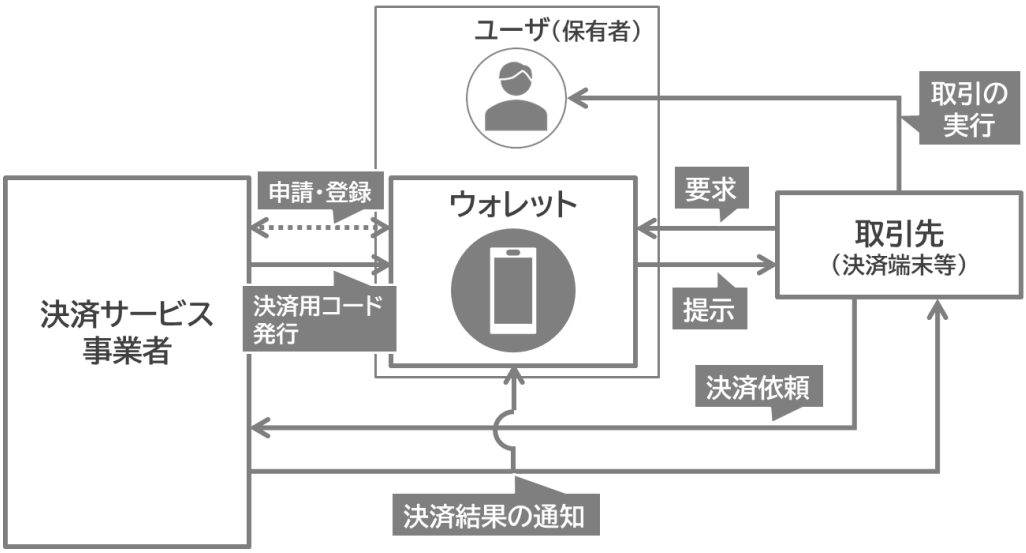


図 12　CPM 方式のコード決済における処理の流れ

参考：「コード決済に関する統一技術仕様ガイドライン【利用者提示型】 CPM(Consumer-Presented Mode) Ver.1.2」を基に作成

3.3.3.2　コード決済の特徴

コード決済は、スマートフォンを利用することを前提とした決済方法であり、従来のキャッシュレス決済と比較して、ユーザ及び取引先の双方にとって、導入が容易であることが利点として挙げられる。

MPM では、ユーザのウォレットが決済端末の役割を担うことから、取引先において決済端末の導入が不要となる。特に静的 MPM の場合、取引先には決済用コードを表示するための機器も不要となり、決済用コードを印刷・掲示するだけで、キャッシュレス決済の導入が可能となる[170]。

また、ユーザにおいても、カメラ、ディスプレイ、モバイル通信機能等を備えた一般的なスマートフォンだけでコード決済が利用可能となる。このため、

非接触決済におけるNFCやセキュリティ機能といったデバイス要件を考慮する必要がなく、幅広いデバイスで利用可能である。さらに、従来のキャッシュレス決済において不可欠であった銀行口座やクレジットカードを保有することなく、決済サービス事業者にアカウント登録を行い、アカウント口座に入金するだけで、キャッシュレス決済を利用できる[171]。

このような利点から、コード決済はスマートフォンの普及に伴い、それまで銀行口座やクレジットカードの保有率が低く、キャッシュレス決済があまり浸透していなかった中国や東南アジア諸国連合（ASEAN）地域を中心に、急速に普及している[172]。

一方、コード決済の課題として、従来のキャッシュレス決済とは異なる不正利用のリスクが挙げられる。MPMの場合、店舗等に掲示された決済用コードが異なる取引先や金額等のコードに偽装されたり、ユーザのウォレットに表示される決済完了通知が偽装されたりするリスクがある[173]。また、CPMの場合、ユーザのウォレットに表示される決済用コードの盗用、無断複製等のリスクがある[174]。したがって、コード決済においてはこれらのリスク対策が求められる。

そのほかにも、決済用コードに記録されるデータフォーマットは、決済サービス事業者によって異なるため、異なる決済サービス事業者のコード決済を利用する場合は、決済サービス事業者ごとに提供されるウォレットを利用する必要がある[175]。

このようなコード決済の相互運用性の課題に対して、決済用コードの規格を統一し、コード決済の相互運用を実現する取組が進められている。2017年、EMVCoは、EMV 仕様のコード決済技術に関する業界標準を策定した[176,177]。その後、ASEAN各国において、EMV仕様に則った決済用QRコードの規格統一が推し進められ、各国における決済サービス事業者だけでなく、ASEAN域内におけるコード決済の相互連携に向けた取組が推進されてきた[178]。日本においても、経済産業省主導の下、EMV仕様に準拠した日本国内の統一規格である「JPQR[179]」を利用して、ASEAN地域との相互運用に向けた取組が進められている[180]。

3.4 web3 ウォレット

3.4.1 web3 ウォレットの概要

web3とは、一般的には、ブロックチェーン技術を応用したアプリやインフラとして解釈されている[181]。web3の概念については、Web3 Foundationの創始者であり、ブロックチェーン基盤であるイーサリアムの共同創設者でもあるGavin Woodが2014年に提唱した、ブロックチェーンに基づく分散型エコシステムの考え方に端を発すると考えられている[182]。ただし、web3に関する明

確な定義は存在せず、その表記についても、Web3、Web 3.0 等があり、様々な表現及び解釈が混在している。以下、本節では、表記を「web3」として、「ブロックチェーン技術を応用したアプリやインフラ」を意味するものとして記載する。

web3 ウォレットは、web3 サービスにアクセスし、web3 サービスの利用に必要なブロックチェーン上の暗号資産の管理を行うためのウォレットである[183]。暗号資産の実体は、ブロックチェーン上に記録されている暗号資産の取引履歴のデータである[184]。暗号資産の所有者情報については、web3 ウォレットの秘密鍵から生成される公開鍵に基づくアドレスとして表現される[185]。

web3 サービスにおける取引とは、ブロックチェーン上のデータを更新することである。取引において、ユーザは、自身の保有する web3 ウォレットの秘密鍵によって、取引を実行するためのプログラム（トランザクション）に署名し、それをブロックチェーンに対して発行することにより、更新を行う[186]。

したがって、web3 ウォレットとは、ブロックチェーンへのアクセス及びブロックチェーン上に記録された暗号資産の管理に必要な秘密鍵を管理するためのアプリである[187]。ユーザは、web3 ウォレットの秘密鍵を管理することによって、当該の秘密鍵に紐づいたブロックチェーン上の記録を参照可能となり、自分の保有する暗号資産の管理が可能となる。

今日における web3 サービスは、暗号資産の取引だけでなく、ブロックチェーン技術の発展や利用者の拡大に伴い、スマートコントラクト、分散型金融（DeFi: Decentralized Finance）、分散型自立組織（DAO: Decentralized Autonomous Organization）等、非中央集権型の P2P（Peer-to-Peer）ネットワークにおける幅広いサービスとして提供されている[188]。このため、web3 ウォレットのシステムは、DIW 及び決済用ウォレットにおけるクライアント＝サーバ型のシステムと異なり、ユーザに属性証明情報や決済用情報を発行する発行者が存在しないシステム構成となる（図 13 参照）[189]。

このようなシステムにおいて、ユーザが web3 サービスにアクセスするための公開鍵及び秘密鍵の鍵ペアは、ユーザが保有する web3 ウォレットによって生成され、web3 ウォレットの秘密鍵だけがブロックチェーン上に記録される暗号資産とユーザを紐づける情報となる。したがって、web3 ウォレットやそれがインストールされたデバイスが破損、紛失等により、web3 ウォレットの秘密鍵が失われた場合、ユーザの暗号資産も失われることとなる。また、web3 ウォレットの秘密鍵が第三者に盗まれた場合、ユーザの暗号資産が第三者に盗まれることとなる[190]。

以上から、web3 ウォレットにおいては、秘密鍵を安全に保管する仕組みが求められることとなる。

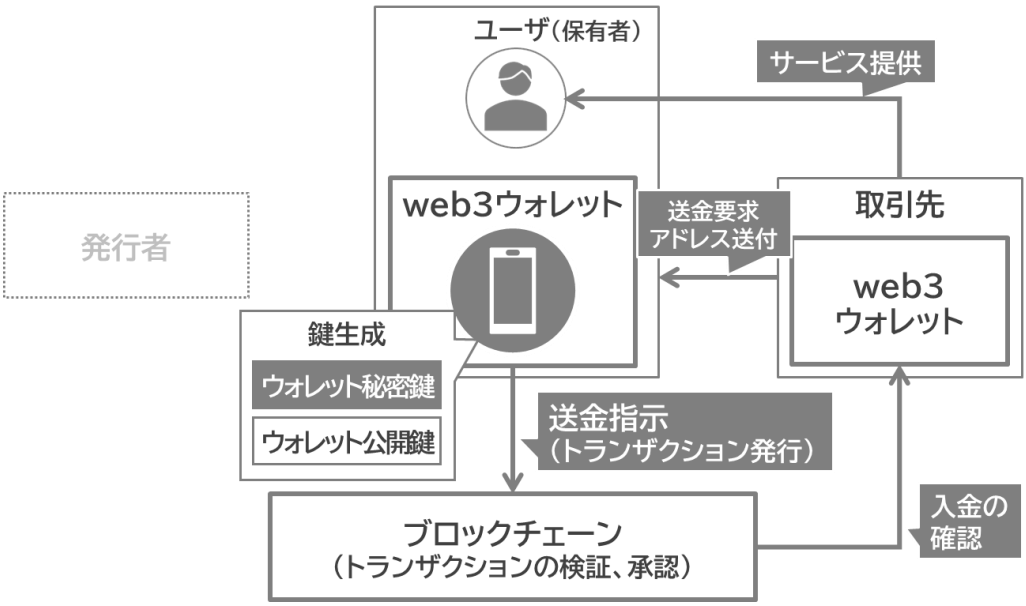


図 13　web3 ウォレットにおける基本的な処理のイメージ

参考：「ナレッジ・インサイト、用語解説、Web3」等を基に作成

3.4.2　web3 ウォレットの区分

web3 ウォレットは、秘密鍵の保管方法によってコールドウォレットとホットウォレットに大別される[191]。各ウォレットの概要は、以下のとおりである。

3.4.2.1　コールドウォレット

コールドウォレットは、秘密鍵をオフライン環境で保管するウォレットであり、通常時は、インターネット等のネットワーク環境に接続されておらず、取引時のみ、ネットワークに接続されるウォレットである。コールドウォレットの利点として、ネットワーク接続が必要な状況以外では、ネットワーク環境から隔離されており、外部攻撃によるハッキングの可能性が低く、安全性が高いことが挙げられる。ただし、ネットワークに常時接続されていないため、web3 サービスへのアクセスや暗号資産の取引の都度、ネットワーク接続を行う必要がある[192]。

コールドウォレットには、秘密鍵を印刷又は印字したペーパーウォレットや、秘密鍵を安全に保護可能なセキュア IC チップを搭載し、ネットワークデバイスと物理的に接続可能なハードウェアウォレットが利用される[193]。ユーザは、これらのウォレットを適切に管理することで、外部から秘密鍵を安全に秘匿可能である反面、ウォレット自体が物理的に盗難されるリスクや、ユーザによる物理的な紛失、破損等のリスクがある。

3.4.2.2　ホットウォレット

ホットウォレットは、オンライン環境上でユーザのウォレットや暗号資産取引所等の秘密鍵を保管するウォレットである[194]。暗号資産へのアクセスや取引を即座に行うことが可能となる利点がある。一方、オンライン上においては、常時、第三者からの攻撃やウイルス感染による秘密鍵の漏えいリスクがある[195]。このため、ホットウォレットの利用においては、ハードウェアウォレットを併用し、これらのリスクの低減を図ることが望ましいとされ、暗号資産取引所等においては、コールドウォレットによる保管が義務付けられている場合もある。

ホットウォレットは、秘密鍵の管理をユーザ自身で行うノンカストディアルウォレットと第三者に委託するカストディアルウォレットに区分される[196]。

ノンカストディアルウォレットは、ユーザ自身で秘密鍵の管理を行うことにより、web3 サービスの利用における全ての決定権限をユーザ自身で管理できる反面、ユーザが秘密鍵管理に係る責任やリスクを負う必要がある[197]。

カストディアルウォレットは、暗号資産取引所等の第三者であるカストディアンに、秘密鍵の管理を委託するウォレットである（図 14 参照）。ユーザは、暗号資産取引所等にアカウントを登録することによって、カストディアンが管理するウォレットを利用することができる。カストディアルウォレットでは、ユーザ自身による秘密鍵の管理は不要となるため、ユーザは秘密鍵管理の責任やリスクから解放されるメリットがある。一方で、暗号資産取引所のハッキングや閉鎖により、ユーザの保有する暗号資産にアクセスできなくなるリスクがあるため、信頼できるカストディアンを見分ける必要がある[198]。

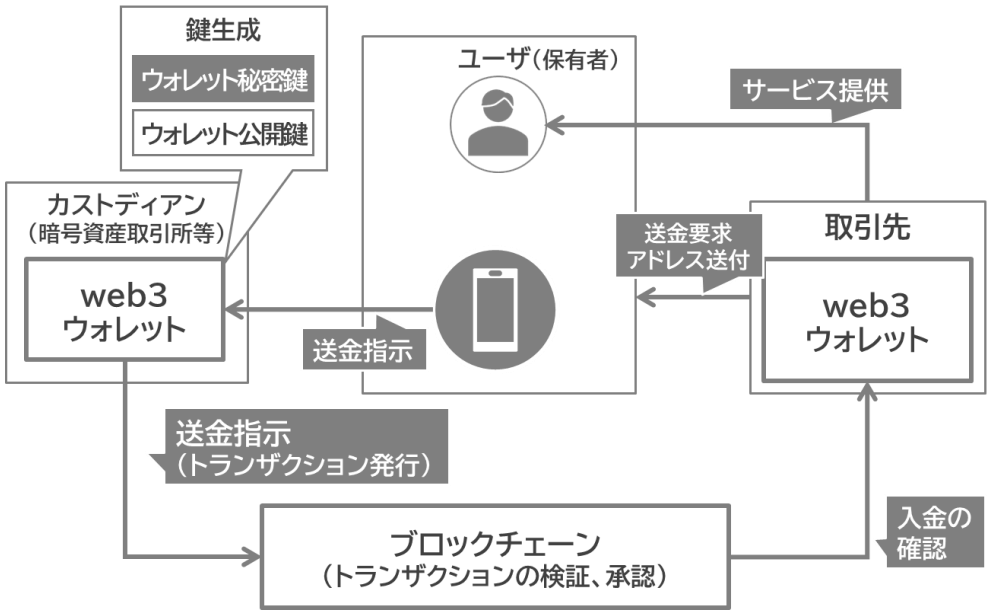


図 14　カストディアルウォレットにおける処理のイメージ

参考：「“Web3.0 におけるウォレットの基礎知識” －秘密鍵管理の重要性－」等を基に作成

3.4.3 web3 ウォレットにおける鍵管理の仕組み

3.4.2 項に記載したとおり、web3 ウォレットには、ウォレットの種類を問わず、秘密鍵の盗難、紛失、不正利用等のリスクがある。このため、秘密鍵については、紛失・破損リスクへの対応や、第三者による盗難、不正利用等への対応が可能な管理の仕組みが求められる。このような安全かつ確実な秘密鍵管理の仕組みとして、以下のような方法がこれまでに考案及び実装されている。

3.4.3.1 階層的決定性ウォレット（HD ウォレット）

階層的決定性ウォレット（Hierarchical Deterministic Wallet、以下、「HD ウォレット」という。）は、単一の乱数情報であるマスターシードから生成される暗号鍵から、複数の暗号鍵を生成可能なウォレットである[199]。このような鍵管理の仕組みは、ビットコインの改善提案である BIP（Bitcoin Improvement Proposals）32[200]において規格化され、イーサリアムの技術仕様を規定する ERC（Ethereum Request for Comments）-600[201]にも規定されるなど、現在の web3 ウォレットにおける標準的な鍵管理手法として利用されている。

HD ウォレットは、マスターシードから生成される暗号鍵（親鍵）から複数の子鍵を生成でき、さらに子鍵から複数の孫鍵を生成できるという階層的な暗号鍵の拡張が可能なウォレットである。

ユーザは、単一の HD ウォレット上で複数の暗号鍵を一括管理可能となるだけでなく、全ての暗号鍵がマスターシードから再生成可能であるため、ウォレットの復元やバックアップが可能となっている。さらに、BIP39[202]において、マスターシードを、人が覚えやすい単語（フレーズ）を組み合わせたシードフレーズに置き換える仕組みについても規定され、ウォレットの復元やバックアップに係る労力の軽減が図られている。

ただし、マスターシードやシードフレーズの取扱いには、秘密鍵と同様のリスクが伴うため、ユーザは、マスターシードやシードフレーズを安全かつ確実に保管する必要がある。

3.4.3.2 マルチシグウォレット

マルチシグウォレット（Multi Signature Wallet）は、トランザクション発行に複数の署名を必要とするウォレットである[203]。具体的には、ウォレットに複数の利用者の公開鍵及び必要な署名の数を設定し、トランザクションの発行時に複数の利用者の秘密鍵による署名が必要な仕組みとして実装される。

マルチシグウォレットにおけるトランザクションの発行には、「M-of-N」アルゴリズムが利用される。当該アルゴリズムは、ウォレットの作成時に、トラ

ンザクションの発行に必要な署名数 M（承認閾値）を設定し、署名可能な利用者の公開鍵の数を N とすることで、N 人中 M 人から署名されることでトランザクションの発行が承認される仕組みである。例えば、マルチシグウォレットに「2-of-3」を設定した場合、3 つの公開鍵のうち、公開鍵に対応する 2 つの秘密鍵による署名があれば、トランザクションの発行は承認される[204]。仮に利用者のうち 1 人の秘密鍵が盗まれたとしても、その秘密鍵だけではトランザクションの承認閾値を満たさないため、トランザクションは発行されず、不正利用を防止できる。

ただし、マルチシグウォレットでは、複数の者における秘密鍵の紛失や盗難等により、利用者全員で利用可能な秘密鍵の数が承認閾値を下回った場合、そのウォレット上で保管されている暗号資産にアクセスできなくなる。このため、マルチシグウォレットの作成時は、利用者及び承認閾値を適切に設定する必要がある。また、マルチシグウォレットにおけるトランザクションの署名は、ブロックチェーン上で行われる。このためトランザクションの発行に必要な手数料は通常のウォレットより高くなるだけでなく、承認閾値の数や署名者に関する情報を、悪意ある第三者に知られるリスクがある[205]。

3.4.3.3 MPC ウォレット

MPC ウォレットとは、秘密鍵の管理の仕組みに、マルチパーティ計算（MPC：Multi Party Computation）を利用するウォレットである[206]。MPC ウォレットにおいて、秘密鍵は複数の秘密鍵の断片（キーシェア）に分割され、トランザクションを発行する場合は、MPC によって複数のキーシェアから秘密鍵を再構築し、トランザクションに署名を行う。キーシェアの分割及び再構築には、マルチシグウォレットと同様に、「M-of-N」アルゴリズムが利用され、N 人の利用者が管理し、一部が欠損した場合であっても、承認閾値となる M 人のキーシェアから秘密鍵が再構築される。承認閾値未満のキーシェアからは、秘密鍵を再構築することが原理的に不可能であることから、秘密鍵の漏えいリスクは低減される。

MPC ウォレットは、秘密鍵の管理を複数の利用者によって行う点でマルチシグウォレットと似た仕組みであるものの、管理が必要な秘密鍵が一つである点で異なる。また、MPC ウォレットにおける秘密鍵の分割及び再構築はブロックチェーンの外部で行われるため、ウォレットの作成後も承認閾値及び利用者の数を柔軟に変更可能であるだけでなく、承認閾値の数やキーシェアの保有者に関する情報は公開されない。したがって、マルチシグウォレットと比較して、承認閾値の数や署名者に関する情報を、悪意ある第三者に知られるリスクがないことや、様々なブロックチェーンに対応可能といった利点がある[207]。

このように、MPC ウォレットは、マルチシグウォレットと比較して安全性が高く柔軟な鍵管理が可能である反面、その運用には、MPC に係る計算資源及び専門的な知識が求められる。

3.4.3.4 コントラクトウォレット

コントラクトウォレットとは、ERC-4337[208]において規定されるアカウント抽象化（Account Abstraction）の仕組みを用いたウォレットである[209]。アカウント抽象化とは、ウォレットに紐づくアカウントとして、イーサリアムの標準的なユーザアカウントである外部所有アカウント（EOA: Externally Owned Account）ではなく、コントラクトアカウントを利用可能にする技術である。

コントラクトアカウントは、ブロックチェーン上にアドレスが割り当てられる点で EOA と同様であるものの、秘密鍵が割り当てられていない点で異なっており、ブロックチェーン上の自動実行プログラムであるスマートコントラクトで制御される、トランザクションの署名及び発行ができないアカウントである。

ERC-4337 では、ユーザのコントラクトアカウントを web3 ウォレットとして利用可能な仕組みとして、EOA アカウントを持つバンドラー（Bundler）が、ユーザに代わってトランザクションの署名及び発行を行うことを規定している。バンドラーは、複数のユーザの取引内容であるユーザオペレーション（UserOperation）を格納したトランザクションを、ブロックチェーン上に記録されたスマートコントラクトであるエントリーポイントに発行する。エントリーポイントは、ユーザオペレーションの内容及び署名を検証して、実行する（図 15 参照）[210]。ユーザは、自身の署名をユーザオペレーションに記録する必要があるが、署名方法については、パスワードやデバイスの生体認証情報等、コントラクトウォレットの実装において任意に定めることが可能である[211]。

このように、コントラクトウォレットは、バンドラーがサービス連携を行う仕組みであり、ユーザは、web3 サービスの利用において、従来の web3 ウォレットのような秘密鍵の管理が不要となる。ただし、バンドラーは、これまでの連携モデルにおける IdP と同様の機能・役割を担うものであり、バンドラーが単一障害点となるリスクやバンドラーによる検閲の可能性等、これまでの連携モデルと同様の弊害やリスクについても懸念されている[212]。

コントラクトウォレットは、トランザクションの発行に必要な手数料について、暗号資産以外の任意の支払方法の設定が可能であり、ユーザは手数料のための暗号資産を保有することなく、web3 サービスを利用可能となる。新潟県長岡市山古志村では、2024 年 10 月に、マイナンバーカードを web3 ウォレッ

トとして利用する、マイナウォレットの実証実験が行われた[213]。マイナウォレットは、マイナンバーカードを活用したコントラクトウォレットである[214]。マイナウォレットは、ステーブルコイン等の暗号資産のチャージが可能であり、ユーザは、マイナンバーカードの NFC 機能を利用して、ステーブルコイン等を利用した決済が可能になる。マイナウォレットは、マイナンバーカードと連携したウォレットとして、行政サービス、地域経済等における決済やサービストークンの受領等、公的機関による web3 サービスの利活用の促進を図る可能性があるものと考えられている[215]。

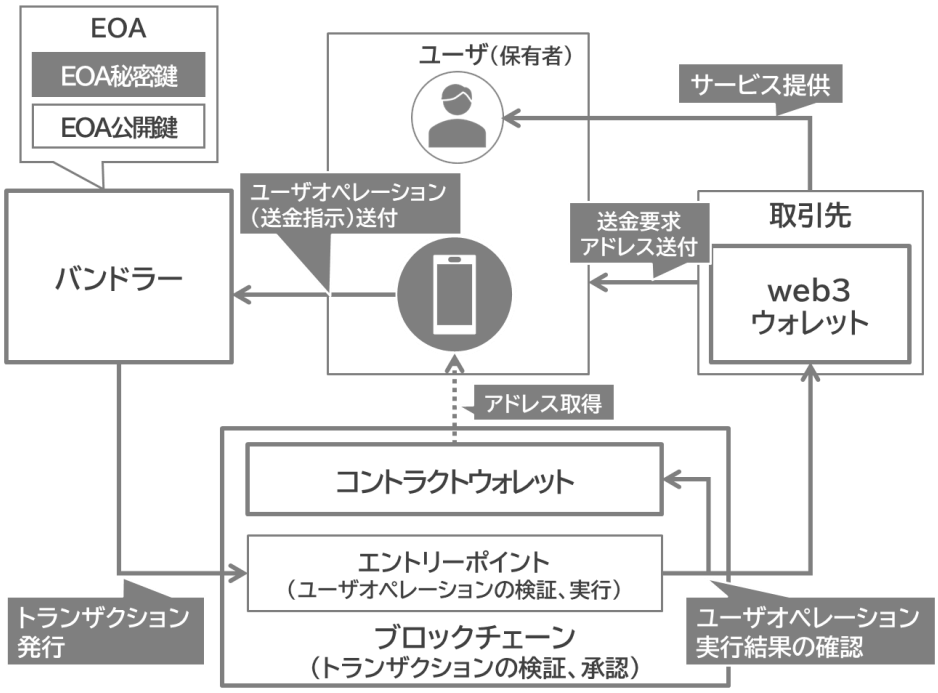


図 15　コントラクトウォレットにおける処理のイメージ

参考：「アカウントアブストラクション（アカウント抽象化）　1: 基礎知識（コラム）」等を基に作成

3.5　ウォレットの課題

ウォレットの機能・役割は、サービスの種類や形態によって異なり、様々なサービスの用途に応じたウォレットがユーザに提供されている。このため、ウォレットは、デジタルサービス事業者のデジタルサービスの一環として提供されることが多く、ユーザは自分の意思でウォレットを選択できない可能性がある。

このようなウォレットの提供方法には、以下の課題が見受けられる。

3.5.1　相互運用性の課題

ウォレットは、ユーザがデジタルサービスを利用する上での相互連携を担う

ことが期待されているが、実際には利用するサービスごとに専用のウォレットを用いる必要があり、デジタルサービス事業者によるユーザのデジタルサービスへの囲い込みやロックインに利用され、相互運用性が確保されていないことが課題となっている[216]。

2023 年 2 月、オープンソースソフトウェアに関するプロジェクトや共同開発を促進する非営利団体である The Linux Foundation は、これらの課題を解決するためのプロジェクトとして、OWF（OpenWallet Foundation）を設立した[217]。OWF は、オープンソースによるウォレットの開発を推進することによって、ウォレットの相互運用を促進するプロジェクトである。また、2024 年 5 月には、国際電気通信連合（ITU）と共同で OpenWallet Forum を創設し[218]、標準技術に基づく相互運用可能なウォレットに関する関係者間の協力と議論を促進するための作業を開始している。

3.5.2 大規模プラットフォーマーの課題

ウォレットは、スマートフォン等のデバイス上で動作するアプリとして提供されることから、ユーザは、アプリストアに登録されたアプリを入手する必要がある。ただし、アプリストアはデバイスの OS プロバイダが運営しているため、登録されるアプリについては、OS プロバイダの審査を通過する必要がある。また、3.2.5 項に記載したとおり、ウォレットのセキュリティ機能についても、OS プロバイダやデバイスによって異なる。

現在、スマートフォンの OS プロバイダは、Google 社及び Apple 社の寡占状態にあるだけでなく、これらの OS プロバイダはデバイスベンダでもある。このため、ウォレットの利用において、ユーザはこれらの OS プロバイダに依存せざるを得ない状況にある。また、これらの OS プロバイダは、自社の OS やデバイスの機能と密接に紐づいたウォレットを提供するウォレットプロバイダでもある。このため、これらの OS プロバイダの提供するウォレットと比較して、他のサードパーティが提供するウォレットの機能は、制限されている場合がある。このような状況は、大規模プラットフォーマーによるロックインや、サードパーティに対する優越性等を引き起こすものであり、特定のサービス事業者に依存しないウォレットサービスを実現する上での課題となっている。

EU では、大規模プラットフォーマーへの依存度を下げるため、2022 年にデジタル市場法（DMA）[219]が制定され、大規模プラットフォーマーによる支配的地位の乱用を防止する取組みが進められている。特に Apple 社は、自社のアプリストア以外でアプリの提供を認めていなかったことや、自社のウォレット以外にデバイスの NFC 機能を開放していなかったことについて、欧州委

員会から、DMA 違反の可能性が指摘されてきた。このため、Apple 社は、2024 年に、EU 域内における Apple 社以外の代替アプリストアの解放[220]及びサードパーティへの NFC 機能の解放[221]を発表した。ただし、代替アプリストアについては、依然として、DMA に違反しているとの予備調査の結果が示されており、2025 年 3 月に、最終的な決定が下される予定である[222]。

3.5.3 リンク可能性の課題

リンク可能性（Linkability）とは、属性証明情報の検証に必要な情報を第三者が収集し、それらを突き合わせることによって、ユーザが特定される可能性のことを指す[223]。ウォレットにおける属性証明情報の検証には、発行者の署名やユーザの識別子、アドレス、公開鍵、属性情報等が利用されるが、一般的に、検証に必要な情報が少ないほど匿名性は強くなり、情報が多いほど匿名性は弱くなる。匿名性の程度において、ユーザの特定が不可能な場合はリンク不能となりユーザのプライバシーは保護されるが、リンク可能な状態ではユーザのプライバシーが侵害されるリスクがある[224]。検証において同じ署名、識別子等が繰り返し利用される場合、第三者によるユーザと検証情報の紐づけの推測（名寄せ）が可能（リンク可能）となり、第三者によるユーザの追跡、監視等によるプライバシー侵害を引き起こす可能性がある。

リンク可能性は、複数の検証者又は発行者と検証者との結託によって引き起こされる。このうち、複数の検証者による結託に対しては、ウォレットによる開示データの最小化によってある程度の対応は可能となるが、より高度な対応として、ゼロ知識証明を用いた選択的開示の仕組みである BBS+署名[225]の実装が求められる。一方、発行者と検証者の結託において、発行者はユーザの属性証明情報に関する全ての情報を把握可能であるため、技術的手段だけで対応することは困難であり、技術的手段に加え、制度、運用方法等による対応が必要となる。技術的手段としては、発行者における署名の生成、暗号化等に HSM を利用することによって、発行に係る暗号化処理をブラックボックス化する方法が挙げられる[226]。この場合、運用方法による対応としては、発行者における署名の有効期限を適切に設定し、定期的な署名の更新や有効期限を過ぎた署名の早期削除を行うとともに、発行、更新等の履歴については長期的に保管するなどの方法が提唱されている[227]。

リンク可能性の課題は、技術的手段と運用方法を組みわせた対応が必要であり、引き続き、様々なアプローチによる検証が必要になると考えらえる。また、プライバシーとセキュリティの両立も求められることから、技術的手段や運用方法に加え、制度設計の検討も必要と考えられる[228]。

3.5.4　ビジネスモデルの課題

ウォレットの広範囲な普及及び促進を図る上で、ウォレットのビジネスモデルは重要な課題である。従来の大規模プラットフォーム事業者が提供するデジタルサービスの連携基盤に依存した連携モデルに対して、ユーザ情報をユーザ自身で管理する分散管理の仕組みを持つウォレットモデルには、新たなビジネスモデルの創出が期待されている[229]。新たなビジネスモデルについては、様々な可能性が提唱されている一方で、ビジネスモデルが多様化、複雑化し、その効率性が従来の連携モデルより劣る可能性があることも懸念されている[230]。

従来の連携モデルでは、ユーザのデジタルサービス連携を行うデジタルサービス事業者について、広告収入によるビジネスモデルが成立していた。しかしながら、発行プロセスと検証プロセスが分離しているウォレットモデルでは広告収入によるビジネスモデルの成立は困難となる。このため、デジタルサービス事業者にとって、ウォレットモデルに移行するための動機が薄れる可能性がある。

特に、DIW では、アイデンティティ情報をウォレットに発行する発行者に対するインセンティブを確保するための仕組みについて、明確なビジネスモデルが示されていない。決済用ウォレットや web3 ウォレットは取引時に手数料を徴収可能であり、DIW においても発行時にユーザから発行者に発行手数料を支払う仕組みについて検討されている。ただし、発行されたアイデンティティ情報をユーザのウォレットに保管する DIW の仕組みでは、初回発行時以外、発行手数料が発生しないことから、発行手数料の徴収によるビジネスモデルについては、持続可能性が課題となっている[231]。

ウォレットのビジネスモデルについては、今後も検証及び考察がなされてくと思われるが、その中で明確なインセンティブの訴求に加え、ウォレットによるサービスのニーズ及びコスト踏まえ、サービス事業者の役割の範囲を調整する必要がある。

3.6　ウォレットの今後

ウォレットの機能・役割は、用途やサービスによって異なり、全ての機能を備えるウォレットは存在しなかったため、ユーザは、サービスや用途に応じてウォレットを使い分ける必要があった。このため、ユーザは、ウォレットを利用するために、ウォレットプロバイダ及びデジタルサービス事業者に対して、個別に本人確認を行う必要があった。今後は、DIW を利用することによってサイバー空間上での本人確認が可能となり、様々なデジタルサービスと連携することが可能となる。例えば、EUDIW においては、様々なデジタルサービスが EUDIW 上で実装されることが予定されている（4.3.3.5 参照）。また、新潟

県長岡市山古志村におけるマイナウォレットの実証実験は、コントラクトウォレットのアドレスに、マイナンバーカード情報を利用している（4.5.3.4 参照）。

このように、DIW は、様々なデジタルサービス連携の基盤として重要な役割を担うことが想定される。また、これまで提供されてきた様々なデジタルサービスに対応したウォレットについても、将来的には DIW と連携する仕組みが実装されると考えられる。

このようなウォレットの将来像を示すものとして、2025 年 4 月から大阪で開催される関西万博の公式ウォレット「EXPO 2025 デジタルウォレット」が挙げられる[232]。このウォレットは、ウォレット ID 基盤を通じて様々なデジタルサービスと連携する仕組みとして構築されている。ユーザはウォレット上で関西万博会場における様々なキャッシュレス決済やポイントカードを利用できる。そのほかにも、ユーザには、譲渡不可能な NFT であるソウルバウンドトークン（SBT: Seoul-Bound Token）の性質を利用した SBT デジタルパスポートが割り当てられる。SBT デジタルパスポートは、ウォレット ID 基盤と連携して、関西万博に関連する各種イベント等に参加するためのデジタル身分証として機能する。ユーザはウォレット上で、関西万博に関連するイベント等において発行される NFT を保管し、他のユーザと交換するなどの web3 サービスが利用可能となる。

このように、EXPO 2025 デジタルウォレットは、web3 サービスを含む様々なデジタルサービスと連携可能な、これまでにない多機能ウォレットであり、関西万博における利用状況が注目されている。

3.7 まとめ

ウォレットは、デジタルサービスを安全かつ便利に利用するための機能をユーザに提供するだけでなく、データ連携基盤を補完する社会インフラとして、デジタル社会において重要な役割を担うものとして捉えられている。そのため、世界各国でウォレットの実装に向けた検討が行われており、実装に向けて、相互運用性やセキュリティ、プライバシー等の様々な関連技術の開発や標準化等が進められている。一方、ウォレットは、デジタルサービスにおけるシステムの一部であり、ウォレットにおいて取り扱う情報次第で、その機能や役割、ウォレットを取り巻くシステムは異なるものとなる。したがって、ウォレットの実装にあたっては、エコシステムを俯瞰し、技術・運用面を考慮した設計を行う必要がある。また、アイデンティティ情報や法定通貨等、これまで物理的な媒体によって提供されてきた公的サービスにウォレットを利用する場合、電子データとして適切に取り扱うため、並行して制度設計の検討が必要になる。

現在、多くの法域で検討が進められている CBDC においても、ウォレット

を利用することが想定される。今後のウォレットへの理解を深める上で、今回の整理がその一助となれば幸いである。

[59] Weblio 辞書、「「財布」の意味や使い方 わかりやすく解説」、(https://www.weblio.jp/content/%E8%B2%A1%E5%B8%83?dictCode=SGKDJ)

[60] Allen, Christopher, “The Path to Self-Sovereign Identity”, 2016.4.26, (https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/)

[61] 株式会社 NTT データ研究所、「令和 4 年度デジタル取引環境整備事業(Trusted Web の実現に向けた技術動向調査)調査報告書 別紙 Trusted Web に係る海外動向調査報告書」、2023.3.30, pp.120-195、(https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/001_report_international.pdf)

[62] 総務省、「平成 29 年版 情報通信白書」、2017.7、p.3、(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/29honpen.pdf)

[63] 総務省、「平成 30 年版 情報通信白書」、2018.7、pp.120-122、(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/30honpen.pdf)

[64] worldpay, “THE GLOBAL PAYMENTS REPORT 2024 9th Edition”, 2024.4※

[65] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.17、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)

[66] Web3.0 研究会, デジタル庁、「Web3.0 研究会報告書 ～Web3.0 の健全な発展に向けて～」、2022.12、pp.6-7、(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/a31d04f1-d74a-45cf-8a4d-5f76e0f1b6eb/a53d5e03/20221227_meeting_web3_report_00.pdf)

[67] 総務省、「令和 5 年版 情報通信白書」、2023.7、pp.17-20

[68] 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)

[69] デジタル庁、「マイナンバーカードとは」、2025.1.15、 (https://www.digital.go.jp/policies/mynumber/pros-and-safety)

[70] 神奈川県警察、「運転免許証について」、(https://www.police.pref.kanagawa.jp/tetsuzuki/menkyo/mes83080.html)

[71] OpenID Foundation, “OpenID for Verifiable Presentations - draft 24, 2. Terminology”, 2025.1.27, (https://openid.net/specs/openid-4-verifiable-presentations-1_0.html)

[72] OpenID Foundation, “OpenID for Verifiable Presentations - draft 24, 2. Terminology”, 2025.1.27, (https://openid.net/specs/openid-4-verifiable-presentations-1_0.html)

[73] The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1, section 5.1 Lifecycle Details”, 2022.3.3,(https://www.w3.org/TR/vc-data-model/#lifecycle-details)

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

[75] The World Wide Web Consortium, “Verifiable Credentials Data Model v1.1, section 5.2 Trust Model”, 2022.3.3, (https://www.w3.org/TR/vc-data-model/#trust-model)

[76] Internet Engineering Task Force, draft-ietf-oauth-selective-disclosure-jwt-15, “Selective Disclosure for JWTs (SD-JWT), 4.1.2. Key Binding”, 2025.1.16, (https://www.ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-15.html#name-key-binding)

[77] Internet Engineering Task Force, Request for Comments 7800, “Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs), 4.1.2. Key Binding”, 2016.4, pp.4-5、(https://www.rfc-editor.org/rfc/rfc7800.html)

[78] OpenID Foundation, “OpenID for Verifiable Credential Issuance - draft 15, Appendix D. Key Attestations”,2024.12.19, (https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html#name-key-attestations)

[79] OpenID Foundation, “OpenID for Verifiable Presentations - draft 24, 2. Terminology”, 2025.1.27, (https://openid.net/specs/openid-4-verifiable-presentations-1_0.html)

[80] 須崎有康, 「Trusted Execution Environment の実装とそれを支える技術」, IEICE Fundamentals Review Vol.14, No.2, 2020.2, pp.107-108、(https://www.jstage.jst.go.jp/article/essfr/14/2/14_107/_pdf/-char/ja)

[81] 須崎有康, 「TEE(Trusted Execution Environment)とそれに関する研究開発動向」, デジタルサービス・プラットフォーム技術特別研究専門委員会, 2021.9.27、(https://www.ieice.org/~dpf/wp-content/uploads/2021/08/DFS%E7%A0%94%E7%A9%B6%E4%BC%9A%E7%94%A3%E7%B7%8F%E7%A0%94%E9%A0%88%E5%B4%8E.pdf)

[82] 磯部光平、宇根正志、「スマートフォン等のスマート・デバイスにおけるセキュリティ:プラットフォーム化によるリ

スクの現状と展望」、金融研究 第 40 巻第 3 号、 2021.7、pp.84-85、89-90、（https://www.imes.boj.or.jp/research/papers/japanese/kk40-3-3.pdf）

[83] GlobalPlatform, “GlobalPlatform Technology Root of Trust Definitions and Requirements Version 1.1”, 2018.6, pp.21-22, （https://globalplatform.org/wp-content/uploads/2018/07/GP_RoT_Definitions_and_Requirements_v1.1_PublicRelease-2018-06-28.pdf）

[84] 須崎有康、「Trusted Execution Environment の実装とそれを支える技術」、IEICE Fundamentals Review Vol.14 No.2、2020.2、pp.107-108、（https://www.jstage.jst.go.jp/article/essfr/14/2/14_107/_pdf/-char/ja）

[85] 庭野栄一、NTT セキュアプラットフォーム研究所、「GlobalPlatform の最新標準化動向―IoT 時代のセキュアコンポーネント」、NTT 技術ジャーナル Vol.30、2018.12、pp.54-55、（https://journal.ntt.co.jp/wp-content/uploads/2020/06/JN20181253.pdf）

[86] The European Digital Identity Cooperation Group, “European Digital Identity Wallet Architecture and Reference Framework v1.6.0, 4.3.2 Components of a Wallet Unit”,2025.3.3

[87] GlobalPlatform, “GlobalPlatform Technology Root of Trust Definitions and Requirements Version 1.1”, 2018.6, p.13, （https://globalplatform.org/wp-content/uploads/2018/07/GP_RoT_Definitions_and_Requirements_v1.1_PublicRelease-2018-06-28.pdf）

[88] 独立行政法人情報処理推進機構、「セキュリティ機能と保証レベル」、2023.11、（https://www.ipa.go.jp/security/jisec/about/knowledge/about-eal.html）

[89] Apple、「Apple プラットフォームのセキュリティ」、2024.12、pp.9-15、（https://help.apple.com/pdf/security/ja_JP/apple-platform-security-guide-j.pdf）

[90] Android Developers、「Android Keystore システム」、2024.2.23、（https://developer.android.com/privacy-and-security/keystore?hl=ja）

[91] Samsung, “Samsung Knox admin guides, Knox Vault”, 2024.2.20, （https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/core-platform-security/knox-vault）

[92] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9

[93] American Association of Motor Vehicle Administrators, “Mobile Driver License”, （https://www.aamva.org/topics/mobile-driver-license）

[94] マイナンバーカードの機能のスマートフォン搭載に関する検討会、デジタル庁、「マイナンバーカードの機能のスマートフォン搭載に関する検討会（第 5 回） 資料 1 マイナンバーカード機能のスマホ搭載について」、p.8、2024.7.22、（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/fcb737a4-07b9-4abd-bdca-34af9c4f71a5/f6f1ad84/20240913_meeting_smartphone_mynumbercard_outline_01.pdf）

[95] THE EUROPEAN COMMISSION, “COMMISSION IMPLEMENTING REGULATION (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, ANNEX II, LIST OF STANDARDS REFERRED TO IN ARTICLE 8”, 2024.12.4, （https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj）

[96] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application, Introduction“, 2021.9

[97] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-7:2024 Personal identification – ISO-compliant driving license, Part 7: Mobile driving licence (mDL) add-on functions” ,2024.10

[98] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.3

[99] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9 p.3

[100] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application, Annex C “, 2021.9, p.90

[101] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.9

[102] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.10

[103] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.10

[104] American Association of Motor Vehicle Administrators, “AAMVA, Mobile Driver’s License (mDL) Implementation Guidelines Version 1.4 (November 2024)”, 2024.11, p.8

[105] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.12

[106] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.13

[107] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.13

[108] American Association of Motor Vehicle Administrators, “AAMVA, Mobile Driver’s License (mDL) Implementation Guidelines Version 1.4”, 2024.11, p.34, （https://www.aamva.org/getmedia/8d8fbb1f-1ec0-4b25-89a1-b90c36163edb/mdl-implementation-guidelines-v1-4.pdf）

[109] American Association of Motor Vehicle Administrators, “AAMVA, Mobile Driver’s License (mDL) Implementation Guidelines Version 1.4”, 2024.11, p.8、(https://www.aamva.org/getmedia/8d8fbb1f-1ec0-4b25-89a1-b90c36163edb/mdl-implementation-guidelines-v1-4.pdf)

[110] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.20

[111] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 20219, p.21

[112] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.8

[113] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application, Annex E “, 2021.9, p.140

[114] MATTR, “Docs, mdocs, Structure to Function”, 2024.12.5, （https://learn.mattr.global/docs/mdocs/structure-to-function）

[115] The International Organization for Standardization, the International Electrotechnical Commission, “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license, Part5: Mobile driving licence(mDL) application“, 2021.9, p.145

[116] American Association of Motor Vehicle Administrators, “Jurisdiction Data Maps”, （https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap）

[117] American Association of Motor Vehicle Administrators, “Mobile Driver License Digital Trust Service”, （https://www.aamva.org/identity/mobile-driver-license-digital-trust-service）

[118] American Association of Motor Vehicle Administrators, “AAMVA, Mobile Driver’s License (mDL) Implementation Guidelines Version 1.4”, 2024.11, （https://www.aamva.org/getmedia/8d8fbb1f-1ec0-4b25-89a1-b90c36163edb/mdl-implementation-guidelines-v1-4.pdf）

[119] the United States government, “About REAL ID”, 2024.5.7, （https://www.dhs.gov/real-id/about-real-id）

[120] American Association of Motor Vehicle Administrators, “AAMVA, Mobile Driver’s License (mDL) Implementation Guidelines Version 1.4”, 2024.11, p.7, （https://www.aamva.org/getmedia/8d8fbb1f-1ec0-4b25-89a1-b90c36163edb/mdl-implementation-guidelines-v1-4.pdf）

[121] マイナンバーカードの機能のスマートフォン搭載に関する検討会、総務省、「マイナンバーカードの機能のスマートフォン搭載に関する検討会（第 1 回） 資料 1 検討の方向性」、2020.11.10、（https://www.soumu.go.jp/main_content/000716654.pdf）

[122] デジタル庁、「スマホ用電子証明書搭載サービス」、2024.11.14、（https://www.digital.go.jp/policies/mynumber/smartphone-certification）

[123] デジタル庁、「スマホ用電子証明書搭載サービスリーフレット」2024.3.28、（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/29c7576b-de6c-4394-bf07-d39b78f26300/f13179e0/20240328_policies_mynumber_resources_leaflet_01.pdf）

[124] デジタル庁、「マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業（技術検証・要件検討）」、2023.8.28、（https://www.digital.go.jp/procurement/0737bb36-c494-4972-9b72-219c15b0e18a）

[125] デジタル庁、「マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業（技術検証・要件検討） 調達仕様書」、2023.8.28、p.1、（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/0737bb36-c494-4972-9b72-219c15b0e18a/92b33ddd/20230828_procurement_public_notice_outline_01.pdf）

[126] 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第 27 号）、（https://laws.e-gov.go.jp/law/425AC0000000027/20290606_506AC0000000046）

[127] マイナンバーカードの機能のスマートフォン搭載に関する検討会、デジタル庁、「マイナンバーカードの機能のスマートフォン搭載に関する検討会（第 5 回） 資料 2 マイナンバーカード機能のスマホ搭載について」、2024.7.22、（https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/fcb737a4-07b9-4abd-bdca-34af9c4f71a5/f6f1ad84/20240913_meeting_smartphone_mynumbercard_outline_01.pdf）

[128] デジタル庁、「マイナンバーカード機能の iPhone への搭載について」、2024.5.31、（https://www.digital.go.jp/news/ed0adc91-4d86-4cf6-a551-4961a07b00a2）

[129] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework”, 2024.4.30, （https://eur-lex.europa.eu/eli/reg/2024/1183/oj）

[130] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Article 5a”, 2024.4.30, （https://eur-lex.europa.eu/eli/reg/2024/1183/oj）

[131] THE EUROPEAN COMMISSION, “COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets”, 2024.12.4, （https://eur-lex.europa.eu/eli/reg_impl/2024/2977/oj）

[132] The European Digital Identity Cooperation Group, “European Digital Identity Wallet Architecture and Reference Framework v1.6.0, 4.2 Design principles”,2025.3.3

[133] The European Digital Identity Cooperation Group, “European Digital Identity Wallet Architecture and Reference Framework v1.6.0”,2025.3.3

[134] THE EUROPEAN COMMISSION, “The technical specifications behind EU Digital Identity Wallets”, （https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications）

[135] THE EUROPEAN COMMISSION, “COMMISSION IMPLEMENTING REGULATION (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, ANNEX II, LIST OF STANDARDS REFERRED TO IN ARTICLE 8”, 2024.12.4, （https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj）

[136] THE EUROPEAN COMMISSION, “COMMISSION IMPLEMENTING REGULATION (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework, ANNEX, STANDARDS REFERRED TO IN ARTICLE 5(1) AND (2)”, 2024.12.4, （https://eur-lex.europa.eu/eli/reg_impl/2024/2982/oj）

[137] THE EUROPEAN COMMISSION, “COMMISSION IMPLEMENTING REGULATION (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, ANNEX V, TECHNICAL SPECIFICATIONS FOR PSEUDONYM GENERATION REFERRED TO IN ARTICLE 14”, 2024.12.4, （https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj）

[138] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework , Article 5d”, 2024.4.30, （https://eur-lex.europa.eu/eli/reg/2024/1183/oj）

[139] The European Digital Identity Cooperation Group, “European Digital Identity Wallet Architecture and

Reference Framework v1.6.0, 3. EUDI Wallet ecosystem",2025.3.3

[140] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Article 5d

[141] Internet Engineering Task Force, Request for Comments: 8259, "The JavaScript Object Notation (JSON) Data Interchange Format", 2017.12,(https://datatracker.ietf.org/doc/html/rfc8259)

[142] Internet Engineering Task Force, Request for Comments: 8949, "Concise Binary Object Representation (CBOR)", 2020.12,(https://datatracker.ietf.org/doc/html/rfc8949)

[143] Internet Engineering Task Force, Request for Comments: 7519, "JSON Web Token (JWT)", 2015.5, (https://datatracker.ietf.org/doc/html/rfc7519)

[144] Internet Engineering Task Force, Request for Comments: 7519, "Selective Disclosure for JWTs (SD-JWT) draft-ietf-oauth-selective-disclosure-jwt-16", 2025.2.27,(https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/)

[145] Authlete,「OpenID for Verifiable Credential Issuance 2.6.1. SD-JWT」, 2024.6.28, (https://www.authlete.com/ja/developers/oid4vci/#261-sd-jwt)

[146] The World Wide Web Consortium, "Web Authentication: An API for accessing Public Key Credentials Level 2", 2021.4.8,(https://www.w3.org/TR/webauthn-2/)

[147] 工藤大樹、株式会社野村総合研究所、「次世代の認証技術　WebAuthn を紹介【前編】」、2023.1.24、(https://www.nri-digital.jp/tech/20230124-12533/)

[148] The European Digital Identity Cooperation Group, "European Digital Identity Wallet Architecture and Reference Framework v1.6.0, 4.3.2 Components of a Wallet Unit",2025.3.3

[149] THE EUROPEAN COMMISSION, "EU Digital Identity Wallet Pilot implementation", (https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation)

[150] THE EUROPEAN COMMISSION, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of the digital euro, Article 25", 2023.6.28, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369)

[151] 政府広報オンライン、「キャッシュレス決済とは？種類や活用のメリットを解説！」、2024.9.17、(https://www.gov-online.go.jp/useful/article/202309/1.html)

[152] 新関広樹、AirREGI マガジン、「種類が多いスマホ決済を基礎から学ぼう」、2020.7.30、(https://airregi.jp/magazine/guide/7051/)

[153] SB ペイメントサービス,「ID 決済（アカウント決済）とは？仕組みやメリットなどを解説」, 2025.1.31, (https://www.sbpayment.jp/support/ec/about-id-payment/)

[154] ソニー株式会社、「NFC の定義」、(https://www.sony.co.jp/Products/felica/NFC/)

[155] 株式会社トッパンインフォメディア、「NFC の基礎知識」、(https://www.toppan-im.co.jp/ic/nfc/)

[156] EMVCo, "EMVCo Payment Tokenisation Specification Technical Framework v2.3", 2021.10.19

[157] EMVCo, "EMVCo Payment Tokenisation Specification Technical Framework v2.3", 2021.10,19, pp.22-23

[158] Shana Micallef, Information Security Group, Royal Holloway University of London, "A study on the security aspects and limitations of mobile payments using Host Card Emulation (HCE) with Near Field Communication (NFC) Technical Report", 2018.4.5, p.33, (https://www.royalholloway.ac.uk/media/5618/rhul-isg-2018-6-techreport-shanamicallef.pdf)

[159] Android Developers、「ホストベースのカードエミュレーションの概要」、2024.11.24、(https://developer.android.com/develop/connectivity/nfc/hce?hl=ja)

[160] Shana Micallef, Information Security Group, Royal Holloway University of London, "A study on the security aspects and limitations of mobile payments using Host Card Emulation (HCE) with Near Field Communication (NFC) Technical Report", 2018.4.5, p.82, (https://www.royalholloway.ac.uk/media/5618/rhul-isg-2018-6-techreport-shanamicallef.pdf)

[161] Smart Card Alliance, "Host Card Emulation: An Emerging Architecture for NFC Applications", 2015.1.18, (https://www.securetechalliance.org/wp-content/uploads/HCE_Webinar_FINAL_061815.pdf)

[162] 鈴木淳也、ITmedia Mobile、「NFC＋SE は必須事項ではない―「モバイルペイメントの次」に向けて動き出した携帯業界」、2014.2.28、(https://www.itmedia.co.jp/mobile/articles/1402/28/news100.html)

[163] Shana Micallef, Information Security Group, Royal Holloway University of London, "A study on the security aspects and limitations of mobile payments using Host Card Emulation (HCE) with Near Field Communication (NFC) Technical Report", 2018.4.5, p.21, p.45, p.57, (https://www.royalholloway.ac.uk/media/5618/rhul-isg-2018-6-techreport-shanamicallef.pdf)

[164] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、p.5、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[165] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、pp.6-8、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[166] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、p.14、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[167] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、p.14-17、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[168] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【利用者提示型】CPM(Consumer-Presented Mode) Ver.1.2」、2019.10.31、p.3、(https://paymentsjapan.or.jp/wp-content/uploads/2022/02/CPM_Guideline_1.2.pdf)

[169] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【利用者提示型】CPM(Consumer-Presented Mode) Ver.1.2」、2019.10.31、p.4-7、(https://paymentsjapan.or.jp/wp-content/uploads/2022/02/CPM_Guideline_1.2.pdf)

[170] 日本経済新聞、「QR 決済、なぜ増える？　ネット企業や金融機関が注目」、2019.5.21、(https://www.nikkei.com/article/DGXZZO44773400U9A510C1000001/)

[171] SB ペイメントサービス, 「QR コード決済とは？仕組みや種類、導入メリットを解説」, 2025.1.31, (https://www.sbpayment.jp/support/ec/about-qrcode-payment/)

[172] 宮川真一、公益財団法人国際通貨研究所、「アジア諸国の QR コード決済連携の動向」、2024.4.26、pp.1-3、(https://www.iima.or.jp/docs/newsletter/2024/nl2024.15.pdf)

[173] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、pp.37-39、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[174] 一般社団法人キャッシュレス推進協議会、「コード決済に関する統一技術仕様ガイドライン【利用者提示型】CPM(Consumer-Presented Mode) Ver.1.2」、2019.10.31、pp.15-17、(https://paymentsjapan.or.jp/wp-content/uploads/2022/02/CPM_Guideline_1.2.pdf)

[175] 一般社団法人キャッシュレス推進協議会、、「コード決済に関する統一技術仕様ガイドライン【店舗提示型】MPM(Merchant-Presented Mode)　Ver.3.0」、2022.11.8、p.1、(https://paymentsjapan.or.jp/wp-content/uploads/2022/11/MPM_Guideline_3.0.pdf)

[176] EMVCo, "EMV QR Code Specification for Payment Systems: Consumer Presented Mode Version 1.0", 2017.7.13

[177] EMVCo, "EMV QR Code Specification for Payment Systems: Merchant-Presented Mode Version 1.0", 2017.7.31

[178] 三菱 UFJ リサーチ&コンサルティング株式会社, 経済産業省、「令和 4 年度第 2 次補正モバイル決済モデル統一規格・海外連携事業（統一 QR コード決済の相互運用に係る実態調査事業） 報告書」、2024.2、(https://www.meti.go.jp/meti_lib/report/2022FY/060233.pdf)

[179] 一般社団法人キャッシュレス推進協議会、「JPQR 総合情報サイト、JPQR とは」、(https://jpqr.paymentsjapan.or.jp/about/)

[180] 日本経済新聞、「QR 決済、日本と ASEAN で支払い可能　25 年度に相互利用」、2024.3.14、(https://www.nikkei.com/article/DGXZQOUA25C0Y0V21C23A2000000/)

[181] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.11、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)

[182] Gavin Wood, "ĐApps: What Web 3.0 Looks Like", 2014.4.17, (https://gavwood.com/dappsweb3.html)

[183] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.17、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)

[184] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.11.1, p.2, (https://bitcoin.org/bitcoin.pdf)

[185] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.19、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)

[186] Bitcoin.org, "Developer Guides, Wallets", (https://developer.bitcoin.org/devguide/wallets.html)

[187] Binance Academy, "Web3 ウォレットとは", 2024.1.16, (https://academy.binance.com/ja/articles/what-are-web3-wallets)

[188] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.14、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)

[189] 株式会社野村総合研究所、「用語解説、Web3」、(https://www.nri.com/jp/knowledge/glossary/web3.html)

[190] 宮川晃一、日本電気株式会社、「“Web3.0 におけるウォレットの基礎知識” －秘密鍵管理の重要性－」、2023.4.12、(https://wisdom.nec.com/ja/feature/digitalfinance/2023041201/index.html)
[191] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.17、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)
[192] 株式会社 bitFlyer、「用語集、コールドウォレット」、(https://bitflyer.com/ja-jp/s/glossary/cold-storage)
[193] Binance Academy, “Web3 ウォレットとは”, 2024.1.16, (https://academy.binance.com/ja/articles/what-are-web3-wallets)
[194] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.17、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)
[195] 株式会社 bitFlyer、「用語集、ホットウォレット」、(https://bitflyer.com/ja-jp/s/glossary/hot-wallet)
[196] 株式会社 bitFlyer Blockchain、「web3 リサーチ 2023」、2023.1.1、p.17、(https://blockchain.bitflyer.com/pdf/web3Research2023.pdf)
[197] 宮川晃一、日本電気株式会社、「“Web3.0 におけるウォレットの基礎知識” －秘密鍵管理の重要性－」、2023.4.12、(https://wisdom.nec.com/ja/feature/digitalfinance/2023041201/index.html)
[198] 宮川晃一、日本電気株式会社、「“Web3.0 におけるウォレットの基礎知識” －秘密鍵管理の重要性－」、2023.4.12、(https://wisdom.nec.com/ja/feature/digitalfinance/2023041201/index.html)
[199] LedgerAcademy、「階層型決定性ウォレット(HD)とは？」、2025.2.5、(https://www.ledger.com/ja/academy/%E9%9A%8E%E5%B1%A4%E5%9E%8B%E6%B1%BA%E5%AE%9A%E6%80%A7%E3%82%A6%E3%82%A9%E3%83%AC%E3%83%83%E3%83%88hd%E3%81%A8%E3%81%AF)
[200] bips.dev, “BIP 39: Mnemonic code for generating deterministic keys”, 2013.9.10,(https://bips.dev/39/)
[201] Ethereum Improvement Proposals, “ERC-600: Ethereum purpose allocation for Deterministic Wallets”, 2017.4.13, (https://eips.ethereum.org/EIPS/eip-600)
[202] bips.dev, “BIP 39: Mnemonic code for generating deterministic keys”, 2013.9.10,(https://bips.dev/32/)
[203] 株式会社 bitFlyer、「用語集、マルチシグ（マルチ・シグネチャーの略）」、(https://bitflyer.com/ja-jp/s/glossary/multisig)
[204] Binance Academy, “What Is a Multisig Wallet?”, 2023.9.6, (https://academy.binance.com/ja/articles/what-is-a-multisig-wallet)
[205] 株式会社レリパジャパン、「MPC ウォレット とマルチシグウォレットの比較： 徹底解説」、2024.4.26、(https://relipasoft.com/blog/mpc-wallet-vs-multi-sig-wallets/)
[206] Binance Academy, “マルチパーティ計算（MPC）ウォレットとは”, 2024.1.11, (https://academy.binance.com/ja/articles/what-are-multi-party-computation-mpc-wallets)
[207] 株式会社レリパジャパン、「MPC ウォレット とマルチシグウォレットの比較： 徹底解説」、2024.4.26、(https://relipasoft.com/blog/mpc-wallet-vs-multi-sig-wallets/)
[208] Ethereum Improvement Proposals, “ERC-4337: Account Abstraction Using Alt Mempool”, 2021.9.29, (https://eips.ethereum.org/EIPS/eip-4337)
[209] Web3 ポケットキャンパス、株式会社野村総合研究所、「アカウントアブストラクション（アカウント抽象化） 1: 基礎知識（コラム）」、2024.2.15、(https://www.pocketcampus.jp/n/n090cab622c42)
[210] Web3 ポケットキャンパス、株式会社野村総合研究所、「アカウントアブストラクション（アカウント抽象化） 2: キーコンセプト（コラム）」、2024.2.15、(https://www.pocketcampus.jp/n/n83c56ecdcce3)
[211] 株式会社日本総合研究所、「パブリックブロックチェーンの技術動向 ～企業活用に向けた技術課題と現状～」、2023.6.5、(https://www.jri.co.jp/MediaLibrary/file/advanced/advanced-technology/pdf/14491.pdf)
[212] inaridiy.eth、Zenn、「Account Abstraction の誤解と真実」、2023.3.9、(https://zenn.dev/inaridiy/articles/09429120aaba43)
[213] a42x 株式会社、「新潟県長岡市山古志地域でマイナウォレットを活用した実証実験を行いました」、2024.10.13、(https://a42x.co.jp/news/2024/10/13/mynawallet-yamakoshi-event-01/)
[214] Coinpost、「マイナンバーカードから Web3 ウォレット作成、「マイナウォレット」イーサリアム財団支援先に選出」、2023.9.8、(https://coinpost.jp/?p=481150)
[215] Coinpost、「マイナンバーカードで Web3 決済、「マイナコイン」商標出願が明らかに」、2024.12.10、(https://coinpost.jp/?p=579691)
[216] Gordon Graham, The Linux Foundation, “Why the World Needs an Open Source Digital Wallet Right Now”, 2023.2, (https://www.linuxfoundation.jp/wp-content/uploads//2023/04/OpenWallet_Why_the_World_Needs_jp.pdf)
[217] OpenWallet Foundation, “Linux Foundation Europe Announces Formation of OpenWallet Foundation 2023.2.23, (https://openwallet.foundation/2023/02/23/linux-foundation-europe-announces-formation-of-openwallet-foundation/)
[218] ITmedia、「「OpenWallet Forum」創設へ 相互運用可能なデジタルウォレットの開発と普及を目指す」、

2024.5.31、(https://atmarkit.itmedia.co.jp/ait/articles/2405/31/news053.html)

[219] 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) (Text with EEA relevance)"2022.12.10, (https://eur-lex.europa.eu/eli/reg/2022/1925/oj)

[220] Impress Watch、「アップル、EU で外部ストア開放や代替決済 リスク増大も警告」、2024.1.26、(https://www.watch.impress.co.jp/docs/news/1563994.html)

[221] Impress Watch、「アップル、iOS 18.1 からアプリ内 NFC 決済をサードパーティに開放」、2024.8.15、(https://www.watch.impress.co.jp/docs/news/1616128.html)

[222] Bloomberg、「EU がアップルに新たな警告、アップストア巡りーDMA 違反の可能性」、2024.6.24、(https://www.bloomberg.co.jp/news/articles/2024-06-24/SFKQRPDWLU6800)

[223] 富士榮尚寛、IdM 実験室、「続)リンク可能性、リンク不可能性の話」、2024.11.16、(https://idmlab.eidentity.jp/2024/11/blog-post_16.html)

[224] 折田明子、慶應義塾大学大学院 政策・メディア研究科、「CGM における匿名性レベル:リンク可能性および一覧性」、2008.5.14、(https://www.jstage.jst.go.jp/article/jasmin/2007f/0/2007f_0_15/_pdf/-char/ja)

[225] 佐古和恵、早稲田大学理工学術院教授、日本銀行金融研究所、「分散型デジタルアイデンティティとは? ～概念、仕組み、実現に資する技術と課題～ 補論 Discussion Paper No.2023-J-8」、2023.7、(https://www.imes.boj.or.jp/research/papers/japanese/23-J-08.pdf)

[226] Wayne Chang, "Provably Forgotten Signatures: Adding Privacy to Digital Identity", 2024.7.22, (https://blog.spruceid.com/provably-forgotten-signatures-adding-privacy-to-digital-identity/)

[227] American Association of Motor Vehicle Administrators, "AAMVA, Mobile Driver's License (mDL) Implementation Guidelines Version 1.4, 10.4 MDL RECORD", 2024.11, pp.50-51, (https://www.aamva.org/getmedia/8d8fbb1f-1ec0-4b25-89a1-b90c36163edb/mdl-implementation-guidelines-v1-4.pdf)

[228] 富士榮尚寛、IdM 実験室、「続々々々々々々々)リンク可能性、リンク不可能性の話」、2024.11.25、(https://idmlab.eidentity.jp/2024/11/blog-post_25.html)

[229] Web3.0 研究会, デジタル庁、「Web3.0 研究会報告書 ～Web3.0 の健全な発展に向けて～」、2022.12、pp.6-7、(https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/a31d04f1-d74a-45cf-8a4d-5f76e0f1b6eb/a53d5e03/20221227_meeting_web3_report_00.pdf)

[230] 崎村夏彦、@_Nat Zone、「VC(Verifiable Credentials, 検証可能資格情報)に未来は無いのか」、2024.11.2、(https://www.sakimura.org/2024/11/6488/)

[231] 株式会社 NTT データ研究所、「Trusted Web 共同開発支援事業に係る調査研究【報告書 別紙】(Trusted Web の実現に向けたユースケース実証 分析レポート)」、2023.3.31, p.34、(https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/2022seika/files/004_report_usecase.pdf)

[232] EXPO 2025、「デジタルウォレット」、(https://www.expo2025.or.jp/digitalwallet/)

参考付録３　暗号資産等の事件・攻撃等

1　概要

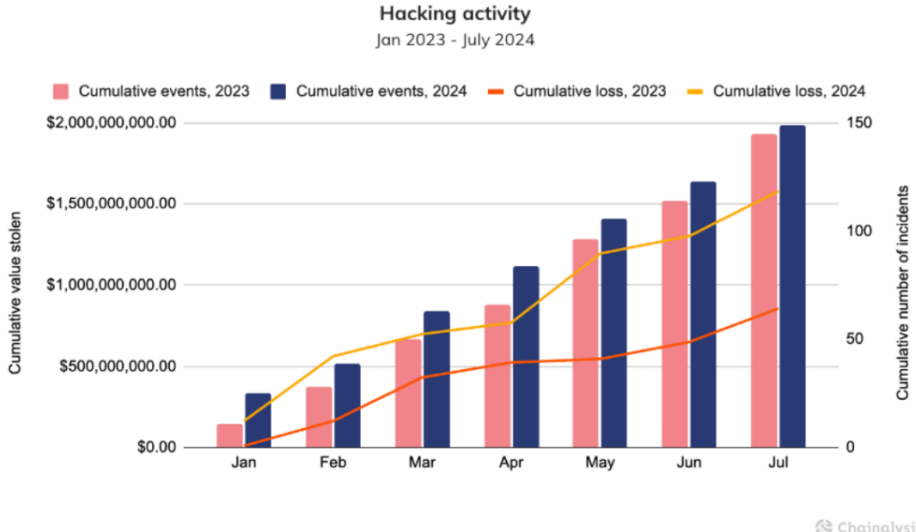
CBDC は電子的な決済手段の一種と考えられるため、暗号資産等に対する事件や攻撃等の知見が、仮に CBDC が導入された際のリスク対応に参考になる可能性があると考え、毎年その動向を整理してきた[233,234,235]。本報告書では、2024 年のサイバー攻撃による資産盗取等の動向について取りまとめた。

2　2024 年におけるサイバー攻撃による資産盗取等の動向について

暗号資産取引等における犯罪動向については、Chainalysis 社の調査によると[236]、2024 年 1 月から 7 月までの間に、合法的なサービスへの加入が増えた結果、暗号資産の違法取引額は前年同期の約 209 億米ドルから約 167 億米ドルに減少したとしている。一方で、暗号資産の盗取やランサムウェアによる不正行為は増加しているとしている。

2.1　暗号資産の盗取

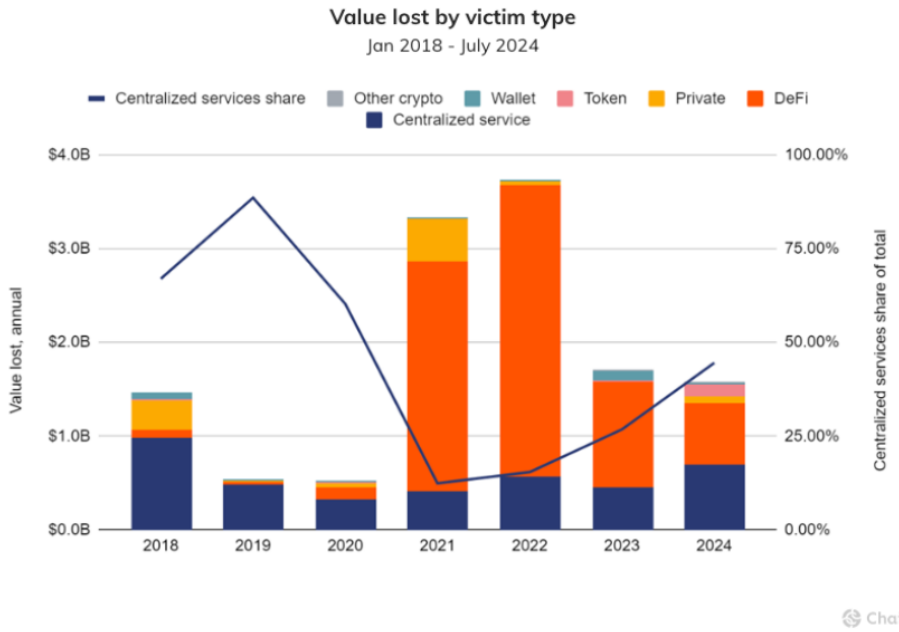
暗号資産の盗取については、被害額が前年同期比で約 84.4%増加している。被害件数は前年同期比で 2.76%の増加に対し、1 件当たりの平均被害額は 79.46%増加し、1 件あたり約 10.6 百万米ドルに達しているとされている（付図 3.1）。被害額の増加は、盗取された資産の価格上昇が要因であるとされる。特に盗取された資金とビットコイン（BTC）の取引が関係していることから、BTC 価格の上昇（前年同期比で約 130%上昇）が影響しているとしている。



出典：Chainalysis,“2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder”,2024.8.15,(https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/)

付図 3.1　暗号資産盗取の動向（2023 年と 2024 年の 1-7 月期比較）

サイバー攻撃による暗号資産の盗取の傾向については、2022 年に分散型金融[237]（DeFi）への攻撃（特にクロスチェーンブリッジ[238]攻撃）によりピークを迎えたとされる。その後、攻撃者は中央集権型金融[239]（CeFi: Centralized Finance）事業者の中でも、特に新しくぜい弱な組織を攻撃対象としていると指摘している（付図 3.2）。



出典：Chainalysis,“2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder”,2024.8.15,(https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/)

付図 3.2　暗号資産の盗取対象に関する動向（2018 年 1 月から 2024 年 7 月期の推移）

2.2 ランサムウェア

Chainalysis 社の報告によると、ランサムウェアについては、2024 年の身代金の支払い額が過去最大になると予想されている[4]。これは、2024 年に入ってからの攻撃の頻度が増え、6 月末時点で昨年の同時期の累計額 4.5 億米ドルに対し、約 4.6 億米ドルを記録しているためとされている。

ランサムウェアの攻撃の注目点として、身代金の最大額が急増している。これは、より高額の身代金を支払う可能性が高いため、大企業や重要インフラ事業者が優先的に攻撃対象となっている可能性があると記載されている。一方で、被害者の数は増えているものの、支払件数は前年より 27.29%減少しているとされている。これは、多くの企業が対策を講じてきており、支払いの必要性が無くなってきている兆候とされている。

なお、日本においても、警察庁サイバー警察局報告書「令和 6 年度上半期におけるサイバー空間を巡る脅威の情勢等について」[240]の中に、サイバー空

間の脅威として、ランサムウェアについての被害が拡大していることが報告されている。

3　ソーシャルエンジニアリングによるサイバー攻撃事例

Chainalysis 社の報告において、暗号資産の盗取は中央集権型の事業者に対して「ソーシャルエンジニアリング」という手法を使って行われるようになってきているとされる[4]。これは、人間の心理や行動の隙を突いて情報を盗み、アクセス権限を不正に取得して暗号資産を盗む方法とされる。また、警察庁は、ソーシャルエンジニアリングの手法でアクセス権限を不正に取得し、資産を窃取する事例を公表している[241]。

このように、システム自体を対象としたサイバー攻撃だけでなく、組織や個人を対象とした攻撃についても理解することが、電子的な決済手段のリスクに対応するために必要となってきているため、最近のソーシャルエンジニアリングによる攻撃事例を紹介する。

3.1　暗号資産の流出

2024 年 5 月、日本国内の暗号資産交換業者のウォレットから、約 4,500BTC（約 482 億円相当）が不正に流出するという事件が発生した[242]。

警察庁は、この不正流出が北朝鮮を背景とするサイバー攻撃グループによるものであると特定し、米国連邦捜査局（FBI）及び米国国防省サイバー犯罪センター（DC3）と合同で文書を公表した[243]。同文書では、攻撃グループの手法の特徴として、同時に同じ会社の複数の従業員に対して実施される、標的型ソーシャルエンジニアリングが挙げられるとしている。

この様な事件を受け、警察庁・内閣サイバーセキュリティセンター（NISC）・金融庁は、ソーシャルエンジニアリングの攻撃対象となり得る暗号資産に係る組織・事業者に対して、セキュリティ対策を講じるよう注意喚起を行っている[244]。

付表 3.1　暗号資産の窃取に関するサイバー攻撃の概要

日時	事象の概要
2024 年 3 月下旬	・攻撃グループは、SNS 上でリクルーターになりすまし、ウォレット管理システムに関するアクセス権を有する関連会社の従業員（攻撃対象）に接触。
	・攻撃グループは、攻撃対象に対して採用前試験を装った悪意あるプログラムコードを記載した URL を送付。 ・その後、攻撃対象が当該 URL にアクセスし、悪意あるプログラムコードを自身の作業用スペース（オンライン）にコピーした結果、侵害が発生。
2024 年 5 月中旬以降	・攻撃グループは、攻撃対象になりすますための情報を悪用し、攻撃対象の通信システムへの不正アクセスに成功。
2024 年 5 月下旬	・攻撃グループは、同アクセスを利用して、暗号資産交換業者における正規な取引を改ざんし、暗号資産を窃取。 ・当該暗号資産は攻撃グループが管理するウォレットに移動。

出典：警察庁、「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について」を基に作成
（https://www.npa.go.jp/bureau/cyber/pdf/020241224_pa.pdf）

3.2　「ＳＩＭスワップ」手法を用いた不正送金[8]

警察庁サイバー警察局報告書においては、2023 年から 2024 年にかけて発生したインターネットバンキング（IB）に係る不正送金事件について、関係都道府県警察が捜査を行い、サイバー特別操作部が情報を集約・分析した結果、同一の犯行グループが組織的に敢行している実態を解明し、犯行グループの指示役とみられる人物を特定し逮捕したとしている。このグループの被害件数及び被害額は、少なくとも 20 件、1 億 2,000 万円に上がることが明らかとなっている。

犯行グループは、情報窃取型の不正プログラムを用いて識別符号（IB の ID やパスワード）を窃取したり、ダークウェブ上で流通する識別符号を入手したりしていた可能性があるとされる。そして、そこから得た情報を利用して、不正送金対策である「SMS 認証による本人確認」機能を回避するため、「SIM スワップ」という手法を用いて攻撃対象の携帯電話番号を乗っ取り、送金時の SMS 認証コードを受け取って不正送金を実行したとされている。

なお、FBI の報告[245]ではこのような「SIM スワップ」において、識別符号を入手するための手法としてソーシャルエンジニアリングが用いられる事例もあるとされており、ソーシャルエンジニアリング手法が不正送金スキームの一部となることが明らかになっている。

4　総括

サイバー攻撃による資産盗取に関する事件・攻撃等についての動向を整理した。暗号資産の違法取引は合法的なサービスへの加入が増えた結果として減少している一方、盗取やランサムウェアによる被害が拡大している傾向がある。特に、ランサムウェアについては、大企業や重要インフラが対象となり１件当たりの被害額が大きくなっている。

こうした盗取などのサイバー攻撃事例には、ソーシャルエンジニアリングの手法が組み合わせられて用いられるなど、システムそのものを守る取組以外にも、適切なセキュリティ対策を講じることが求められるようになってきている。

---

[233] 独立行政法人国立印刷局、「中央銀行デジタル通貨(CBDC)に関するレポート」、2022.8.9、pp.12-19、(https://www.npb.go.jp/zyohoteikyo/kohyou.files/202208_cbdc.pdf)

[234] 独立行政法人国立印刷局、「中央銀行デジタル通貨(CBDC)に関するレポート(令和 4 年度)」、2023.6.1、pp.23-34、(https://www.npb.go.jp/zyohoteikyo/kohyou.files/202306_cbdc.pdf)

[235] 独立行政法人国立印刷局、「中央銀行デジタル通貨(CBDC)に関するレポート(令和 5 年度)」、2024.7.5、pp.27-33、(https://www.npb.go.jp/zyohoteikyo/kohyou.files/202407_CBDC.pdf)

[236] Chainalysis,"2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder",2024.8.15, (https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/)

[237] 明確な定義は存在しないものの、「分散台帳技術(一般的にはパブリックかつパーミッションレス型のブロックチェーン)に基づき、仲介者を必要としないことを企図した金融サービスや商品を提供するもの」と説明される。
参考:金融庁、「デジタル・分散型金融への対応のあり方等に関する研究会(第6回) 事務局説明資料」、2022.6.20、p.3、(https://www.fsa.go.jp/singi/digital/siryou/20220620/jimukyoku.pdf)、Financial Stability Board,"Assessment of Risks to Financial Stability from Crypto-assets",2022.6.16, p.15, (https://www.fsb.org/uploads/P160222.pdf)

[238] 規格・仕様の異なるブロックチェーン同士を相互に作用させ、暗号資産、トークン又はデータの転送を可能とするプロトコルのこと。
詳細は独立行政法人国立印刷局、「中央銀行デジタル通貨(CBDC)に関するレポート(令和 4 年度)」、2023.6.1、pp.25-27、(https://www.npb.go.jp/zyohoteikyo/kohyou.files/202306_cbdc.pdf)を参照。

[239] 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こと。

[240] 警察庁、「令和6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」、2024.9.19、pp.6-7、(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf)

[241] 警察庁、「令和6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」、2024.9.19、pp.26-29、(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf)

[242] DMM Bitcoin、「【重要】暗号資産の不正流出発生に関するご報告(第一報)」、2024.5.31、(https://bitcoin.dmm.com/news/20240531_01)

[243] 警察庁、「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について」、2024.12.24、(https://www.npa.go.jp/bureau/cyber/pdf/020241224_pa.pdf)

[244] 警察庁・内閣サイバーセキュリティセンター・金融庁、「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について(注意喚起)」、2024.12.24、(https://www.npa.go.jp/bureau/cyber/pdf/20241224_caution.pdf)

[245] Federal Bureau of Investigation,"Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public",2022.2.8, (https://www.ic3.gov/PSA/2022/PSA220208)

4　おわりに

リテール CBDC の国外動向を見てみると、世界各国で検討が進められており、英国や欧州等の国・地域では CBDC の発行判断はしていないものの、具体的な計画や実験が進行中である。一方で、米国、カナダ、オーストラリアのように CBDC を発行する具体的なメリットがないとして検討を縮小・中止した国もある。特に米国は、トランプ政権になり、プライバシーの懸念から CBDC の開発が大統領令で禁止され、ステーブルコインの活用が推進されている。また、世界的にも新たなデジタル通貨として預金のトークン化などの動きも出てきており、CBDC に限らない決済システムの高度化が検討され始めている。

日本においては、「制度設計の大枠」の整理に向けて、有識者会議にて「取りまとめ」を整理したのち、関係府省庁・日本銀行連絡会議での議論や、より実務的な議論をおこなうための幹事会を設置して議論が進められている。また、日本銀行では引き続きパイロット実験を通じて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議論が進められている。2024 年には API サンドボックスプロジェクトが開始され、確実に検討が進められている。

国内外の CBDC に関連する動向は、今後も変化し続けることが予想されるため、引き続き注視していく必要がある。

今回のレポートでは「ウォレット」を取り上げた。現在、キャッシュレス手段として携帯電話に搭載されたウォレットアプリが多く利用されている。これらのウォレットにより日常の買い物や送金、公共料金の支払いなど様々な用途に利用されている。そのほかにも、ウォレットは個人が自らの ID を管理する手段として、また web3 サービスにアクセスするための秘密鍵管理の手段としても利用されている。そうしたウォレットの利用方法や仕組みについて整理し、欧州連合が提案する EUDIW についても紹介した。この EUDIW はデジタル ID の統一基盤であり、デジタルユーロでも活用が検討されているものである。

国立印刷局 CBDC 研究会においては、今後も CBDC を取り巻く動向を注視しつつ、関連技術の調査を行っていくこととしたい。