Deloitte.
デロイト トーマツ

日本におけるデジタル資産・分散台帳技術の活用、事業環境整備に係る調査研究

最終報告書

2022 年 12 月

デロイト トーマツ コンサルティング合同会社

はじめに

令和 4 年 6 月 7 日に閣議決定された「デジタル社会の実現に向けた重点計画」[1] では、ブロックチェーン技術によって実現される新しいインターネットの在り方である Web3.0 の推進に向けた我が国での環境整備の必要性が謳われている。

その中で具体的な施策として

1. 有識者会議による調査研究
2. デジタル資産の発行・保有に係る課題の把握
3. 分散型アイデンティティの利用環境整備
4. スマートコントラクトと DAO の法的位置づけの整理
5. デジタル資産・分散台帳技術の活用へ向けた環境整備・人材育成

が挙げられており、デロイトトーマツコンサルティング合同会社（以下、DTC）はデジタル庁の委託を受けて、以下の業務にあたった[2]。

- 以下分野の調査
  - デジタル資産
  - 分散型アイデンティティ（DID）
  - スマートコントラクトと DAO
  - 消費者保護・法執行
- 有識者会議（Web3.0 研究会）の開催補助

本報告書は、DTC による上記関連分野の調査結果をとりまとめたものである。本報告書は全 4 章構成とし、第 1 章ではデジタル資産、第 2 章では分散型アイデンティティ（DID）、第 3 章ではスマートコントラクトと DAO、第 4 章では消費者保護・法執行をテーマに、それぞれ調査結果を整理している。

[1] https://www.digital.go.jp/policies/priority-policy-program/#document

[2] なお、業務遂行に当たっては、有限責任監査法人トーマツ、デロイトトーマツ税理士法人、アンダーソン・毛利・友常法律事務所外国法共同事業に業務の一部を再委託している

内容

1. デジタル資産

1－1. 調査の狙い・アプローチ

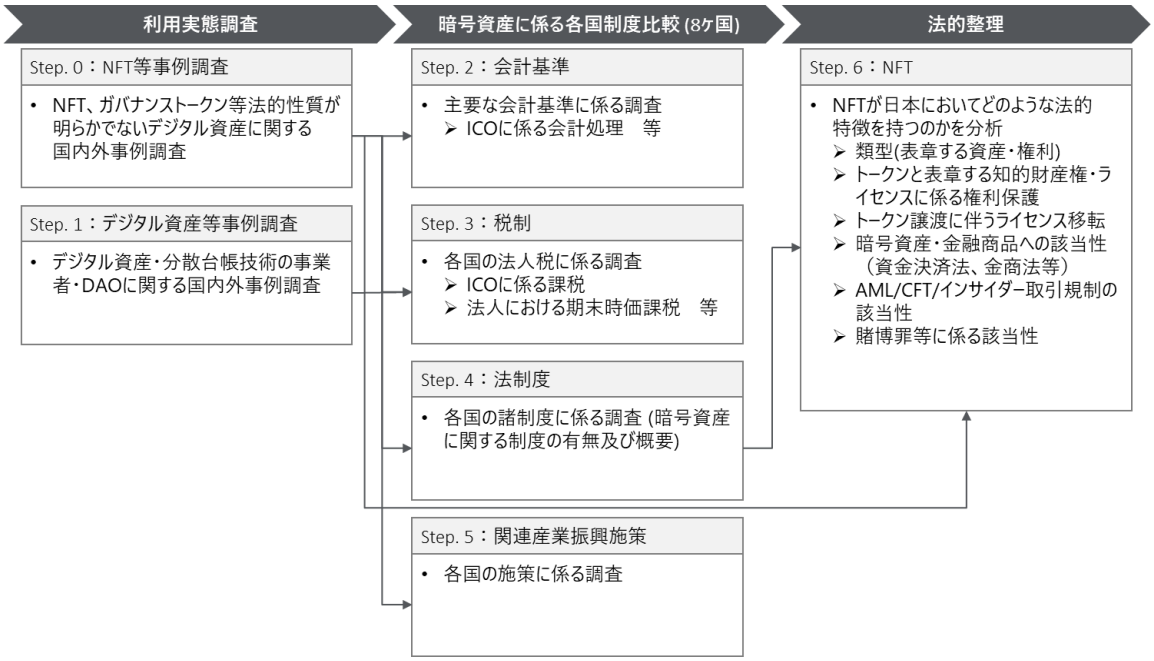
デジタル資産の市場は急速な拡大を続けると共に、NFT（非代替性トークン）やガバナンストークンをはじめとする新たなデジタル資産が登場し、多様なトークンの活用によるこれまでにない便益への期待が膨らむ一方、消費者保護や金融犯罪防止等の観点から様々な課題が指摘されている。

本調査では、日本における適切な事業環境の整備に向けた研究会での議論のインプットとすべく、以下のステップで調査を実施した。

- デジタル資産に関する国内外の利用実態を調査する
- 日本におけるデジタル資産規制の礎である暗号資産に関する諸制度について主要国でそれに相当する諸制度との国際比較を行う
- 諸制度が整備されていない NFT について、日本における法的位置づけや諸論点を整理する

以下の図表は、上記の調査アプローチの具体的な項目の関係性を図示したものである。

図表 1　調査アプローチ



1－2. 調査結果まとめ

調査・分析を踏まえて以下のように取りまとめを行った。

図表 2　調査結果まとめ表

見出し		調査サマリ
1－3. 利用実態	1－3－1. NFT、ガバナンストークン等法的性質が明らかでないデジタル資産	■ NFT のユースケースは大別して「アート」「コレクティブル」「アイテム」「証明書」の 4 つに大別され、コレクティブル、次いでアイテムが取引高の観点で最も活発なユースケースといえる ■ 代表的な NFT 活用事例として「BAYC(NFT コレクション)」「Blitmap(CC0)」、決済手段・証券該当の可能性が出てくる事例として「solv.protocol(ERC3525)」「fractiona.art(NFT 分割)」「Sand Vegas Casino Club(収益分配)」を取り上げた ■ ガバナンストークンには「支払い通貨」「投票/ガバナンス参加」「ステーキング」「バーン」の機能が複合的に付与されているケースが多く見られた ■ 代表的なガバナンストークン活用事例として「Chiliz(トークン保有者による投票)」「Nouns(NFT 保有者による投票)」「Nishikigoi NFT(Nouns と同様)」を取り上げた
	1－3－2. デジタル資産・分散台帳技術の事業者・DAO	■ 事業者: 代表的なグローバル取引所として「Binance(事業多角化・各国法規制準拠状況等)」を取り上げた ■ DAO: 法規制に抵触しうる事例として「The DAO(SEC が証券該当と指摘)」「Ooki DAO(CFTC が違法なデリバティブ取引提供と指摘)」を取り上げた
	1－3－3. 暗号資産に係る関連産業振興施策（8 ヶ国比較）	■ 産業振興施策は既存制度の影響等の個別事情により詳細は各国で異なるが、多くの国がサンドボックス制度を導入している
1－4. 暗号資産に係る会計（8 ヶ国比較）		■ 「保有」「発行」に係る会計上の取り扱いを日本基準、IFRS[3]、米国会計基準に関して調査・整理した 「保有」に関する会計基準 ■ IFRS: 会計基準は存在しないが、IASB[4]が公表するアジェンダにて「暗号通貨の保有」は他社に請求権を生じさせない場合は「棚卸資産」(投資目的では公正価値と帳簿価額の差額を純損益計上、それ以外は低価法)または「無形資産」(原価モデルか再評価モデルを用いて公正価値と取得原価を測定し、上振れを OCI[5]、下振れを純損失計上)が適用されるとしている ■ 米国: 会計基準は存在しないが公認会計士協会から実務ガイダンスが公表されており、IFRS と同様に「棚卸資産」「無形資産」のいずれかとされている

[3] IFRS: 国際財務報告基準

[4] IASB: 国際会計基準審議会

[5] OCI: その他包括利益

		■ 日本:世界に先駆けて暗号資産の会計上の取り扱いを公表した日本は、活発な市場がある暗号資産につき公正価値測定及び純損益処理としている。今後、IASB 及び FASB での会計基準開発の議論に注視しつつ、その後の暗号資産のユースケース発展を踏まえた検討が求められると考えられる 「発行」に関する会計基準 ■ IFRS & 米国: 会計基準・ガイダンスは存在しない。実務上は、ホワイトペーパーや法令を参照して発行体が ICO を通じて負う義務に着目して個別に既存の会計基準の適用を検討している状況である。発行体が配当の支払い義務を有する場合には「資本」、現金を引き渡す義務がある場合は「金融負債」、何らかのプロダクトを開発する義務がある場合は「引当金」、財務又はサービスを割安または無償で提供する義務がある場合は「収益」、何らの義務を負わない場合は「受贈益等」として認識されると考えられる ■ 日本: ASBJ[6]が論点整理の公表並びに意見募集を実施しており、現在会計基準の整備に向けた検討がなされている。また JVCEA[7]が公表する規則[8]で調達資金の目的外使用の禁止といった詳細な業規制が適用される点は我が国の特徴であり、会計基準開発においては、こうした日本特有の規制環境も考慮する必要がある
1－5. 暗号資産に係る税制（8 ヶ国比較）		■ 「期末時価評価課税」「ICO 税制」に係る法人税の各国取り扱いを調査・整理した ■ 期末時価評価課税: 日本では活発な市場がある場合期末時価評価とされており、他の調査対象国では同様の取り扱いは見られなかった(セキュリティトークンに該当する場合は金融資産として時価評価の対象となる(星)、市場公正価値が帳簿価額を下回る場合は減損(瑞)といった事例は存在する) ■ ICO 税制: スイス及びシンガポールのみ税制があり、トークンの性質により取り扱いが異なる
1－6. 法的整理	**1－6－1. 暗号資産に係る法規制（8 ヶ国比較）**	■ 暗号資産規制の有無、暗号資産の定義の有無、暗号資産取引に必要なライセンスの有無、AML/CFT 上の要請の有無の観点から、各国における規制を取り上げた ■ 暗号資産について独自の規制を設けている国・州（NY 州、星、仏)、既存の金融規制また AML/CFT の観点から暗号資産を定義付け、規制対象とする国（独、英、ドバイ（DIFC[9])、韓）とに分かれた
	1－6－2. NFT の法的位置付け整理(日本)	■ 日本法上、NFT を対象とした特有の法律等は存在しない ■ 利用規約等に基づき NFT が表章する権利内容及び権利移転の枠組みが決定される ■ 権利内容や機能等に応じて金融規制上の位置づけを個別具体的に判断する

[6] ASBJ: 企業会計基準委員会

[7] JVCEA: 日本暗号資産取引業協会

[8] 規則: 新規暗号資産の販売に関する規則

[9] Dubai International Financial Centre

		■ 現時点では NFT 取引の AML/CFT・インサイダー取引に係る法規制は存在しない（個別の NFT がその特徴により金融規制に服すべきと判断された場合のみ既存の AML/CFT 規制が適用されうる） ■ NFT の発行・販売の態様によっては刑法における賭博罪該当性等が問題となりうる

1－3. 利用実態

1－3－1. NFT、ガバナンストークン等法的性質が明らかでないデジタル資産

この節では、法的性質が明らかでないデジタル資産の利用実態を、統計及び複数の事例の概観から取り上げる。

（1） NFT の種類と利用実態

まず、NFT のユースケースは大別して「アート」「コレクティブル」「アイテム」「証明書」の 4 つに分類される。

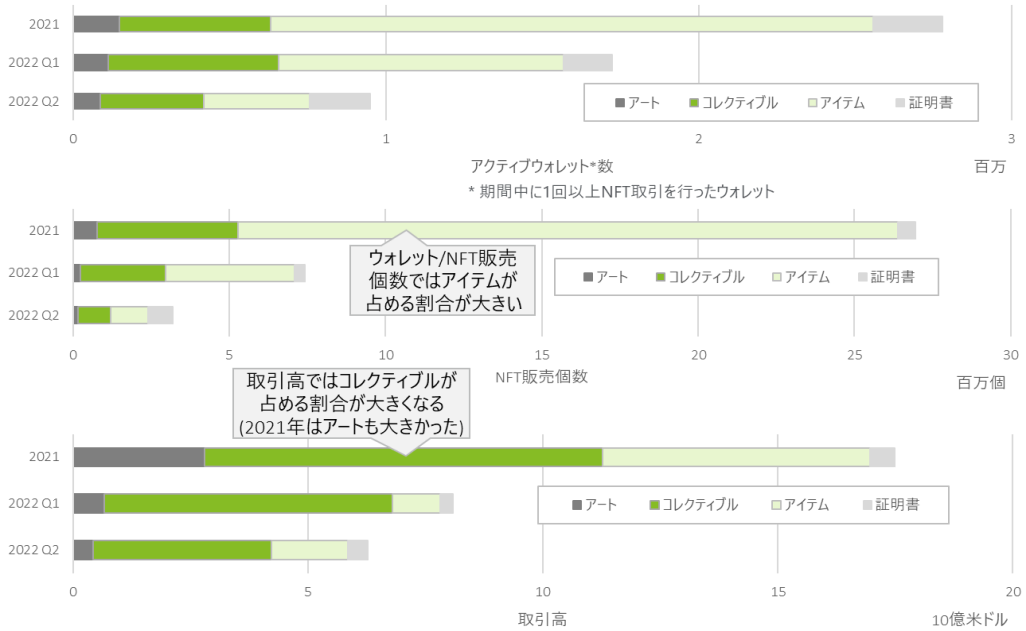
図表 3　ユースケースによる NFT の分類[10]

カテゴリ	特徴	種類	具体例
アート	保有・鑑賞して楽しむもの	デジタルアート	• Everydays – First 5000 days (Beeple)
コレクティブル	共通するテーマを持つNFTが一つのシリーズを形成するもの	コレクティブルPFP*	• Bored Ape Yacht Club (Yuga Labs)
アイテム	ゲームやメタバース等の他サービスでアイテムとして利用価値があるもの	ゲーム	• Axie Infinity (Sky Mavis)
		メタバース	• The Sandbox (Animoca Brands)
		デジタルツイン	• RTFKT (Nike)
証明書	保有者の権利・属性等を表すもの	投票権等の各種権利	• Nouns [投票権]
		チケット/参加証明	• Confirmed (Adidas)
		証書	• 保険証書NFT (IMF Financial)
		アイデンティティ	• Binance Account Bound (Binance)

上記 4 分類において取引高等の統計値の時系列推移により実態把握を試みた。以下に見られるように、NFT のユースケースは、ウォレット数・販売個数ではアイテムが 2021 年で約 7 割、2022 Q2 で約 3 割と最も大きな割合を占め、取引高の面ではコレクティブルが約 5-7 割で推移している。

[10] PFP は Profile Picture の略

図表 4　各種統計値の時系列推移[11]



（2） ガバナンストークンの種類

ガバナンストークンに付与される機能には、投票/ガバナンス参加に加えて、支払い通貨、ステーキング、バーンがある。

図表 5　ガバナンストークンに付与される典型的な機能

トークン保有の動機付け	機能	具体例
ユーティリティ	投票/ガバナンス参加	■ Curve: ステーブルコインの非常に有力な分散型取引所として独自トークン CRV によるガバナンスを通じて運営されており、流動性提供報酬が優遇される流動性プール等が CRV 保有者による投票で決定される。数多あるステーブルコインプロジェクトは Curve 上の流動性を確保する大きなインセンティブがあることから、より有利なガバナンスを行うための CRV 獲得・保持が行われることで CRV の需要と価格が上がる効果が期待される
	支払い通貨	■ Ethereum: Ethereum 上で構築されたアプリケーションの利用には独自トークンである ETH が必要であり、アプリケーションを使いたい人が増える程 ETH の需要と価格が上がる効果が期待される

[11] NonFungible.com レポート（ERC721 及び RONIN、FLOW 上の全 NFT が対象）を基にデロイト作成

リターン	**ステーキング[12]**	■ Pancake Swap: BNB チェーン上の最大手分散型取引所。流動性提供の証である LP （Liquidity Provider） トークンをステーキングすることで独自トークン CAKE が獲得できる。さらに CAKE をステーキングすることで CAKE あるいは Pancake Swap に上場しているトークンを獲得できる機能が備わっており、ユーザに CAKE の獲得・保持並びにサービスの継続利用の動機付けを与えることで、CAKE の需要と価格が上がる効果が期待される
	バーン[13]	■ STEPN: スニーカー等の NFT アイテムを購入することでプレイできる Move to Earn ゲーム。サービス運営チームが獲得した収益の一部を用いて独自トークン GMT のバーンを 2022 年に入って四半期毎に行っており、これによりトークンの流通量が減少することで、トークン価格を底上げする効果が期待できる

（3） デジタル資産の事例

法的性質が明らかでないデジタル資産の中で、コンテンツ産業育成に資する論点を含む NFT、証券該当の可能性がある NFT、ガバナンストークンといった事例を取り上げて調査を行った。特に、3～9 の事例については詳細をそれぞれ後述する。

図表 6　デジタル資産 – 事例一覧
（NFT、ガバナンストークン等法的性質が明らかでないデジタル資産）

	項目	区分	概要
1	**Sudoswap/ X2Y2**	**NFT 一般**	■ NFT の特徴の一つとされたアーティストへのロイヤリティを任意とする NFT マーケットプレイスの勃興
2	**BAYC （Yuga Labs）**	**NFT 一般**	■ 代表的な NFT コレクションである BAYC は NFT 保有者にのみ NFT の商用利用権を許諾している
3	**Blitmap**	**NFT 一般**	■ 著作権を放棄することで二次創作等、NFT 保有者コミュニティによる活動を活性化する CC0（creative commons zero）の試み
4	**ERC3525 （Solv Protocol）**	**Fractional NFT**	■ 異なる NFT を統合する技術規格を用いて、金融商品の特性を NFT により表現する試み
5	**fractional.art**	**Fractional NFT**	■ NFT を複数の ERC20/ERC1155 に変えて部分的所有権を表現する試み

[12] トークンをスマートコントラクトにロックする等して預け入れること。取引の担保とされたり、報酬の条件にされる場合がある

[13] トークンを焼却して使用不能とすること。流通量が減ることでデフレーションと同じ効果が期待できる

6	**Sand Vegas Casino Club**	**収益分配のある NFT**	■ NFT 保有者にオンラインカジノでの収益の分配を約束し、米国州当局から未登録の証券販売に該当するため証券法違反として NFT 販売停止命令を受けた
7	**Uniswap**	**ガバナンストークン**	■ サービスに係る様々な事案の決定・推進を独自トークン UNI による投票で推進
8	**Chiliz**	**ガバナンストークン**	■ トークン保有者による投票でイベント等の意思決定を行うことができるプロスポーツチームのファントークンを暗号資産として発行
9	**Nouns**	**ガバナンストークン**	■ NFT 保有者による投票で DAO トレジャリー資金使途等の意思決定を行う
10	**Nishikigoi NFT**	**ガバナンストークン**	■ NFT 保有者による投票で DAO トレジャリー資金使途等の意思決定を行う

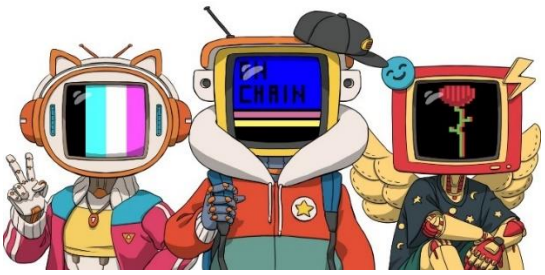
1）Blitmap

Blitmap は、コミュニティでの共創をテーマとして 2021 年 5 月にローンチされた NFT コレクションであり、CC0 （creative commons zero）を採用して二次創作等のコミュニティによる新たな創作を促進する目的で著作権を放棄している。また、NFT に係るデータが全てブロックチェーン上に記録されている。

Blitmap は、既存 NFT を組み合わせて新たな NFT をミントすることができる特徴を持ち、100 枚のピクセルアート絵をオリジナルの NFT として始まっている。オリジナル NFT の組み合わせで 1,600 枚の siblings が発行できたため、100 枚のオリジナル NFT と合計で 1,700 枚の NFT コレクションとなっている。

「Community crafted sci-fantasy universe」をテーマとし、コミュニティでのコンテンツ・ストーリー共創を奨励しているため、派生 NFT 等の二次創作が自由にでき、Blitnauts 等の取り組みが生まれている。また、Blitmap 保有者に今後関連コンテンツで利用できる NFT コレクションのエアドロップ[14]も行われており、こうした取り組みがコミュニティ起点で行われることがコンテンツ全体の盛り上げに寄与している。創業チームが大方針をロードマップとして提示し、要所でコミュニティによる投票が行われて最終決定する形で取り組みが進められている。

図表 7　代表的な派生 NFT コレクションである Blitnauts[15]



[14] 今後リリースされるゲームで使われるアイテムである Sugar といった例がある

[15] https://blitnauts.blitmap.com/

2）Solv Protocol （ERC3525）

金融商品を表章する NFT の分散型取引所を構築する Solv Protocol が提案した新たなトークン規格 ERC3525 が 2022 年 9 月に承認された。ERC3525 は ID/Value に加えて Slot という新たな変数を持つ semi-fungible token で、代表的なトークン規格と比較して以下のように異なる。

- ERC20 – Value で定義する （fungible token）
- ERC721 – ID で定義する （non-fungible token）
- ERC1155 – ID/Value で定義する （semi-fungible token）
- ERC3525 – ID/Value/Slot で定義する

これにより、例えば異なる ID を持つが同じ Slot を持つ 5 ドル紙幣と 10 ドル紙幣の統合がトークンによって表現できることとなり、例えば株式の統合・分割も同じ要領で実現することが期待される。

Solv Protocol では voucher （金券）を ERC3525 トークンで表現することを目指しており、現在以下の 3 種類が検討されている。

- Vesting Voucher （付与されたトークンの権利証書）
- Convertible Voucher （変動利付債）
- Bond Voucher （コールオプション付仕組債）

例えば、Vesting Voucher では、満期、トークンの量、ベスティング（権利確定）の方式を設定して NFT を発行する。以下に示す例では、680.4 千トークン、満期 2021 年 8 月 24 日、ベスティングは 90 日間で線形と設定されている。

図表 8　Vesting Voucher の例[16]

3）fractional.art

fractional.art では、ERC721 トークンを vault というコントラクトに保存し、任意の数の ERC20 トークンあるいは ERC1155 トークンに分割して、オリジナル NFT の一部分として取引できる。

[16] https://solv.finance/home

NFT の分割には以下のような期待と課題がある。

＜期待＞

- 小口化によりトークン単価が下がり、NFT 保有のハードルが下がる
- 多くの人がトークンを持てるようになることで、流動性が向上する

＜課題＞

- 分割により NFT の非代替性が損なわれ暗号資産や証券に該当する可能性がある
- 部分的に NFT を保有することがオリジナルの NFT に対してどの程度の法的権利を持つことになるのか、明確でない場合がある
- 分割された NFT を何らかの用途に用いるあるいは売却する際に、それぞれの部分的保有者間での協議や合意が必要となり、判断・行動に遅れが生じる

4）Sand Vegas Casino Club

キプロスに本拠地を置く Sand Vegas Casino Club の共同設立者 Martin Schwarzberger 氏、Finn Ruben Warnke 氏はメタバースにバーチャルカジノを構築する資金調達の為に NFT を販売し、購入者に対してバーチャルカジノの利益を分配することを約束した。Texas State Securities Board はこれを未登録証券の販売と認めて、販売停止を命じた[17]。その声明では、両氏が当該 NFT は証券ではないと潜在的な買い手に誤って伝えていたとされており、当該 NFT が取引されていた OpenSea では Sand Vegas Casino Club が提供する NFT コレクションの売買及び譲渡をサービス規約違反のため無効にした。

5）Uniswap

Uniswap は代表的な分散型取引所で、その開発は創業者である Hayden Adams 氏が率いる Uniswap Labs が主導する一方、運営方針等の重要事項は 2020 年 9 月に発行された独自トークン UNI（総数 10 億枚）の保有者による投票で決議している等、運営の分散化を志向・実現している。Uniswap に関する議案の提起・議決は以下のプロセスで行われる。

1．フォーラムに投稿を行い、コミュニティ内で議論を呼びかける
2．コミュニティコール、Twitter Space 等の公の場でも議論を行う
3．2-5 日の投票期間を設けて、temperature check の投票を行い、25,000UNI（0.0025%）以上の投票を集める必要がある
　※ 議案提起に 1,000 UNI（0.0001%）以上が必要
4．更に consensus check の投票を行い、50,000UNI（0.005%）以上の投票を集める
　※ 議案提起に 1,000 UNI（0.0001%）以上が必要
5．オンチェーン投票を提起し、過半数の賛同を得て提案が正式に承認される
　※ 議案提起に 2,500,000 UNI（0.25%）以上が必要

[17] https://www.ssb.texas.gov/sites/default/files/2022-04/Order_ENF_22_CDO_1860_.pdf

6）Chiliz

Chiliz は、Socios.com というプロスポーツチームがファンに向けて発行するファントークンの発行・取引プラットフォーム及びトークン購入に必要な独自トークン CHZ を提供している。同社サービスにより、パリサンジェルマン、ユベントス、AS ローマ等、世界的に有力なサッカーチームがファントークンを発行しており、メッシが 2021 年にパリサンジェルマンへ移籍した際に、その契約金 2,500～3,500 万ユーロの一部支払に使われる等、新たなインセンティブの形としても利用され始めている。

パリサンジェルマンの例では、トークン保有者の投票に従って、キャプテンバンドに記載されるメッセージを決める等、ファントークン保有者がクラブチームの活動の一部に係る意思決定に参加できることとなっており、ガバナンストークンとしての側面を有している。

その他、Socios.com 上ではサービスを通じて投票等の活動に参加するほどポイントが溜まり、ポイントの多寡に応じて VIP 席へ招待する等、ファンがクラブチームに対してより継続的・積極的な関心を寄せるような施策が用意されている。

7）Nouns

Nouns は以下の特徴を有する NFT コレクションである。

- 毎日 1 つの NFT が複数のパターンを有するパーツを組み合わせたピクセルアートとして自動的に発行され、オークションで販売されるという一連のプロセスがスマートコントラクトで自動化されている
- オークションの売り上げは 100%が DAO トレジャリーに入り、創業者・運営企業等の取り分が無い
- NFT 保有者による投票で DAO の活動が決定・推進されるため、NFT がガバナンストークンとして活用されている
- NFT はデータが全てオンチェーンで完結
- CC0 を採用

Nouns は NFT をガバナンストークンとして活用することで、NFT に新しいユーティリティを加え、コミュニティ主導の取り組み推進の一つの可能性を示すと共に、スマートコントラクトによる発行・販売プロセスの自動化、フルオンチェーン NFT、CC0 の採用、といった様々な特徴の掛け合わせから注目を集める NFT プロジェクトといえる。

１－３－２. デジタル資産・分散台帳技術の事業者・DAO

グローバルに事業展開する暗号資産交換業者の事例、DAO のスキームを利用した事業展開が既存の法令・行政の仕組みに抵触しうる事態に至った事例を取り上げた。3 については消費者保護・法執行の章においても事例として取り上げる。

図表 9　デジタル資産 – 事例一覧 （デジタル資産・分散台帳技術の事業者・DAO）

	事例	カテゴリ	概要
1	Binance	事業者	■ グローバル最大手のデジタル資産取引所。暗号資産交換業を祖業として、独自ブロックチェーン・ステーブルコイン等の収益多角化と各国法規制遵守を進めている
2	The DAO	DAO	■ 2017 年 7 月 25 日に SEC が報告書を公表、その中で The DAO が過去に販売したトークンが Howey 基準（資金の出資、収益の期待、収益獲得が他社の経営上の努力によること）に照らして有価証券であること、したがって過去の ICO が有価証券の販売に相当するため証券の登録等の所定の手続きが本来必要であったことを指摘した
3	Ooki DAO	DAO	■ 2022 年 9 月 22 日に CFTC が銀行秘密法及び商品取引法に準拠しない形で暗号資産のレバレッジ取引サービスを提供したとして bZeroX 及びその創業者 2 名に 25 万ドルの罰金を課した他、同社の事業を実質的に引き継いだとされる Ooki DAO を非法人化団体としてカリフォルニア州地裁に訴えた。Ooki DAO のガバナンストークン OOKI は 2022 年 8 月にコインベースに上場、保有者は 390 万人にのぼるとされる。

１－３－３. 暗号資産: 海外比較 （関連産業振興施策）

各国の暗号資産に関連する産業の振興施策について主要な取り組みを調査した。多くの国で Fintech に係るサンドボックスが導入されており、分散台帳技術の活用や Web3.0 を成長機会として捉える動きは各国に共通といえる。

図表 10　関連産業振興施策

	主要な出来事	サンドボックス制度
アメリカ	■ 2022 年 3 月デジタル資産の責任ある発展に関する大統領令発布 ■ 2022 年 9 月デジタル資産の責任ある発展に向けた施策を公表	■ アリゾナ、フロリダ、ネバダ、ユタ、ウェストバージニア、ワイオミング等一部の州で免許取得の免除を含むサンドボックス制度が導入されている
シンガポール	■ 2022 年 3 月 PJ Gurdian 発表（4 つの重点分野を中心とした MAS[18]によるブロックチェーン活用の取り組み） ■ 2022 年 9 月産業変革マップの更新版公表	■ 2016 年にサンドボックスを導入後、更に使いやすい形態として 2019 年にエクスプレス版を導入。デジタルアセットの取引所・カストディ等の企業が採択されている ■ 申請が認められた企業は MAS と合意した範囲内での規制緩和を受けながら金融サービスを実社会で提供できる
韓国	■ 2022 年 5 月デジタル資産基本法策定方針の公表 ■ 2022 年 6 月デジタル資産委員会設立方針の公表 ■ 2022 年 7 月暗号資産への課税を 2025 年まで延期	■ 2019 年にサンドボックスを導入し、企業は新規金融事業の適法性の確認並びに一定の条件下での免許免除を含む規制緩和を受けて金融サービスを実社会で提供できる。P2P 取引やデジタル証券等の企業が採択されている
ドバイ	■ 2016 年 10 月「Dubai Blockchain Strategy」発表 ■ 2018 年 4 月「UAE Block-chain Strategy 2021」発表 ■ 2022 年 7 月「Dubai Metaverse Strategy」発表	■ DIFC では通常の規制に比べて制約の少ない Innovation Testing License を設けて新規金融サービスを実験できる環境を提供している
イギリス	■ 2022 年 4 月イギリスを暗号資産の世界的ハブとする計画を発表 ■ 2022 年 4 月金融インフラのためのブロックチェーンサンドボックスを 2023 年に導入する計画を発表	■ 2016 年に FCA[19]が制度導入している他、ロンドン市協力の下、2021 年よりデジタル・サンドボックスを導入している。送金・決済等のブロックチェーン企業が採択されている

[18] MAS: シンガポール金融管理局

[19] FCA: 英国金融行為規制機構

		■ 申請が認められた企業は FCA と合意した範囲内で本来求められる免許等無しに金融サービスを実社会で提供できる
フランス	■ 2022 年 4 月にマクロン大統領が Web3.0 に対する積極姿勢をインタビューで明言 ■ 2022 年 10 月にルメール経済大臣がフランスを暗号資産エコシステムの欧州拠点にしたい旨の発言	■ 特になし
ドイツ	■ 2019 年 9 月「Blockchain-Strategie der Bundes-regierung」発表 ■ 2021 年 7 月「Fund Location Act」可決（特定の投資ファンドが 20%まで暗号資産に投資できるようになる） ■ 2022 年 5 月トークンに係る所得税ガイダンス発表（売却益非課税の条件緩和等）	■ 特になし
スイス	■ 1998 年より 2 年おきにデジタルスイス戦略を策定・更新 ■ 2017 年 1 月クリプトバレー協会発足 ■ 2017 年 12 月、2018 年 2 月 ICO ガイダンスを制定 ■ 2020 年 9 月にブロックチェーン法を可決、デジタル証券に既存証券と同等の法的位置づけを明確に付与	■ 利息・投資収益を生まない資金の預かりに関する規制を緩和するサンドボックス制度が存在する

1－4．会計

この節では、暗号資産に係る会計上の取り扱いに関する取り決め及び検討の動向を、日本及び米国での会計基準及び国際財務報告基準について調査した。

（1） 会計観点でのトークンの分類

会計における国際的な議論において、「トークン」が有する様々な特徴を踏まえ、一定の共通項によって区分した上で、会計上の取扱いを網羅的に整理しようとする試みが見られる。以下はEFRAG[20]が2020年7月に公表したディスカッションペーパー[21]において示したトークンの分類である。

図表 11　EFRAG のディスカッションペーパーにおけるトークンの区分[22]

主要な経済的機能	1	交換手段（支払用途）
	2	投資価値（有価証券に類似）
	3	ネットワークへの参加または、ネットワークの商品/サービスの消費による経済的便益
		8つの区分に分解
会計的な分析を行う上での基礎的区分	1	支払トークン（発行者に対する請求権のない暗号通貨含む）
	2	セキュリティトークン及びアセットトークン（投資トークン）
	3	ユーティリティトークン
	4	ハイブリッド型トークン
	5	支払トークン、セキュリティトークン、アセットトークン又はハイブリッド型トークンにも分類できるステーブルコイン
	6	電子マネートークン（英国のFCAが適用している区分）
	7	機能前トークン
	8	将来のトークンに関する単純化された契約（SAFTs）

（2） 日本における会計基準の検討状況

暗号資産の保有、電子記録移転有価証券表示権利等の発行・保有に関し、日本では実務対応報告により会計基準の整備が行われている。

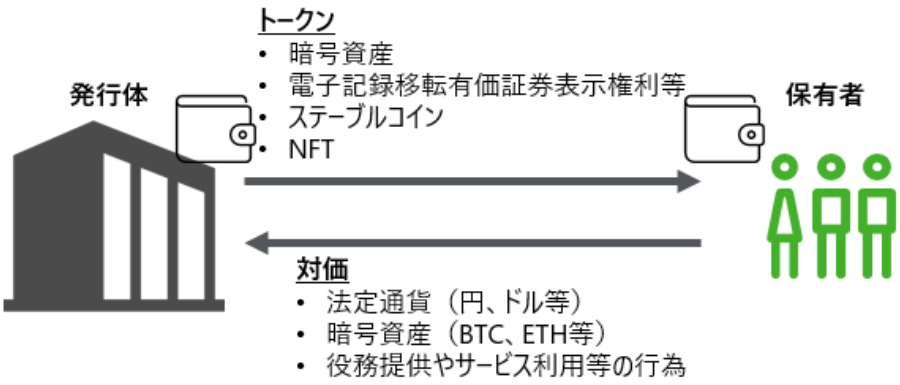
---

[20] European Financial Reporting Advisory Group（欧州財務報告諮問グループ）の略。IFRS の開発を支援する議論において欧州の関係者の十分な参加を確保するとともに、 IASB （国際会計基準審議会）の基準設定プロセスにおいて、アドバイスを行うこと等により欧州の見解を示すこと等の目的で 2001 年に設立された組織。

[21] EFRAG” Discussion Paper On Accounting For Crypto-Assets（Liabilities） ”（2020 年 7 月）

[22] SAFTs（Simple Agreement for Future Tokens）とは、ICO を計画している発行者が、公にトークン販売を行う前に、ネットワークの開発完了後にトークンの交付を受けることができる権利を相対で販売することをいう。通常、当該権利を証券規制上の証券に該当させるように設計して、関連する規制に準拠して販売される。

図表 12　トークンの発行における登場人物



1）発行者における会計論点

暗号資産の発行において、以下が発行者における主要な会計上の論点といえる。

- 資金決済法上の暗号資産の発行（以下「ICO トークンの発行」）により受け取った対価は、一時の収益とするべきか、負債に計上するべきか
- ICO トークンの発行時において自己に割り当てた ICO トークンは、資産として認識するべきか
- ICO トークンの発行後において第三者から取得した ICO トークンは関連する負債から控除するべきか、資産として計上するべきか

現在、電子記録移転有価証券表示権利等の発行に関する実務対応報告は既に公表されている一方、ステーブルコイン、NFT については特段の基準が無く、ICO トークンの発行については後述する論点整理に対して寄せられたコメントを基に現在議論されている。

2）保有者における会計論点

対して、保有者においては以下のような主要な会計上の論点がある。

- トークン取得時における資産の認識タイミングをいつとするべきか（約定日または受渡日）
- 他人のために預かったトークンを資産・負債に計上するべきか
- トークンを期末時に時価評価するべきか、また、時価評価する場合の評価差額は、純損益とするかその他の包括利益とするべきか

ステーブルコイン、NFT については特段の基準が無く、暗号資産[23]および電子記録移転有価証券表示権利等の保有に係る実務対応報告は既に公表されている（ただし、自己もしくは自己の関係者が発行した暗号資産の取得については対象外であり引き続き検討が必要）。

[23] 暗号資産については、実務対応報告第 38 号「資金決済法における暗号資産の会計処理等に関する当面の取扱い」（2018 年 3 月 14 日公表）、電子記録移転有価証券表示権利等については、実務対応報告第 43 号「電子記録移転有価証券表示権利等の発行及び保有の会計処理及び開示に関する取扱い」（2022 年 8 月 26 日公表）

3）ICO トークンの発行及び保有に係る会計処理に関する論点の整理

企業会計基準委員会（ASBJ）により、ICO トークンの発行及び保有について、現段階で基準開発に着手するべきか否かも含めて論点整理が 2022 年 3 月 15 日に公表[24]され、意見募集が行われた。

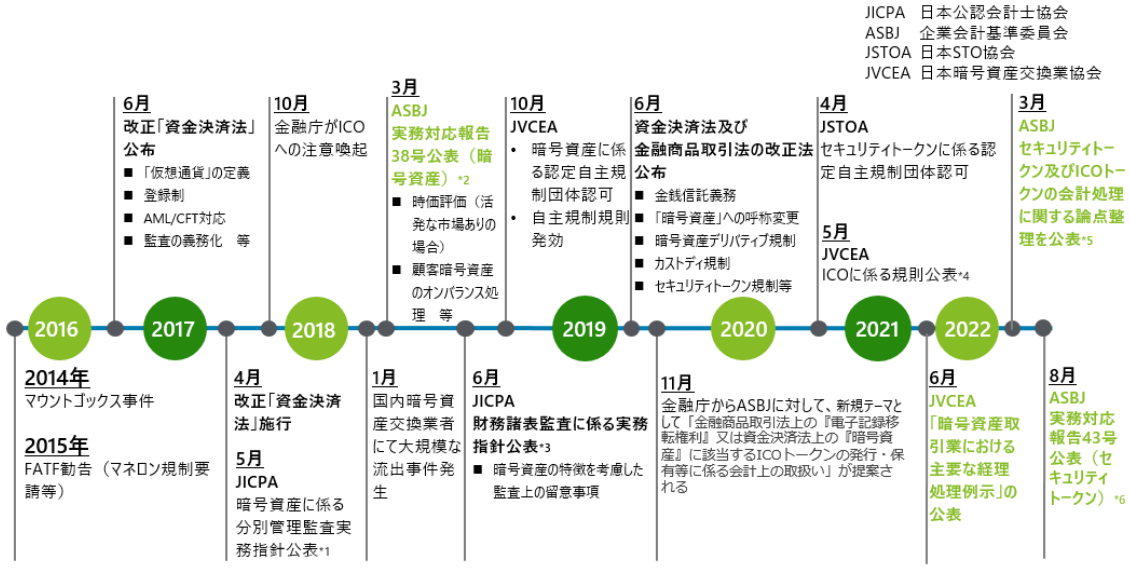
図表 13　ICO トークンに係る論点整理の概要

項目	論点
ICO トークンの発行及び保有に係る、基準開発の必要性及び緊急性、並びにその困難さ（資金決済法上の暗号資産）	■ 国際会計基準審議会（IASB）が 2021 年 3 月 30 日に公表した「情報要請：第 3 次アジェンダ協議」における潜在的プロジェクトの 1 つとして「暗号通貨及び関連取引」が含まれ、大多数の回答者が当該潜在的プロジェクトを高い優先度として評価されているという状況の中で、我が国が先行して ICO トークンの発行及び保有の基準開発を行うべきか ■ 我が国における暗号資産の私法上の取扱いが定まってから基準開発に着手する ■ 私法上の取扱いが明らかとなっているか否かにかかわらず基準開発に着手する。また、その時点で私法上の取扱いが明らかとなっていない場合、それが明らかとなった際に見直しの要否の検討を行うことを前提とした取扱いを定める
ICO トークンの発行者における発行時の会計処理（資金決済法上の暗号資産）	■ 発行者が何らかの義務を負担している ICO トークンの発行取引において、当該発行取引の実態に照らして、発行時に利益が生じ得る会計処理を定めるべきか否か ■ ICO トークンの発行取引については、発行者が何ら義務を負担しないケースのほか、 発行者が財又はサービスを提供する一定の義務を負担するとしても、その財又はサー ビスの価値が調達した資金の額に比して著しく僅少であるケースの存在も聞かれているため問題となる
自己が発行した ICO トークンを保有している場合の会計処理（資金決済法上の暗号資産）	■ ICO トークンの発行時において自己に割り当てた ICO トークンの会計処理について、第三者が介在していない内部取引として会計処理の対象としない方法 と、会計処理の対象として会計上の資産及び負債（発行者が何らかの義務を負 担している場合）を計上する方法のいずれによるべきか ■ ICO トークンの発行後において第三者から取得した ICO トークンの会計処理について、関連する負債の消滅又は控除として取り扱う方法（関連する負債の 消滅の認識を行う方法、又は関連する負債の消滅の認識は行わず ICO トークン の取得原価をもって関連する負債から控除して表示する方法）と、資産として 取り扱う方法のいずれによるべきか
電子記録移転有価証券表示権利等の発行及び保有（金商法上の電子記録移転有価証券表示権利等）	■ 株式会社以外の会社に準ずる事業体等における発行及び保有の会計処理 ■ 株式又は社債を電子記録移転有価証券表示権利等として発行する場合に財又はサービスの提供を受ける権利が付与されるときの会計処理 ■ 暗号資産建の電子記録移転有価証券表示権利等の発行の会計処理 ■ 組合等への出資のうち電子記録移転権利に該当する場合の保有の会計処理

[24] 「資金決済法上の暗号資産又は金融商品取引法上の電子記録移転権利に該当する ICO トークンの発行及び保有に係る会計処理に関する論点の整理 」（2022 年 3 月 15 日公表）

日本は、他国に先駆けて 2016 年以降暗号資産に係る法改正を実施し、2018 年以降会計基準の整備を進める中で現在は ICO トークンに係る検討が行われており、この論点整理はその重要なステップであるといえる。

図表 14　暗号資産を巡る国内の法規制及び会計基準整備の状況



*1 業種別委員会実務指針第55号「仮想通貨交換業者における利用者財産の分別管理に係る合意された手続業務に関する実務指針」
*2 実務対応報告第38号「資金決済法における仮想通貨の会計処理等に関する当面の取扱い」
*3 業種別委員会実務指針第61号「暗号資産交換業者の財務諸表監査に関する実務指針」
*4「新規暗号資産の販売に関する規則」
*5「資金決済法上の暗号資産又は金融商品取引法上の電子記録移転権利に該当するICO トークンの発行及び保有に係る会計処理に関する論点の整理」
*6 実務対応報告第43号「電子記録移転有価証券表示権利等の発行及び保有の会計処理及び開示に関する取扱い」

4）ICO トークン以外の暗号資産に係る会計基準

ICO トークン以外の暗号資産については、ASBJ が資金決済法上の暗号資産について会計上の取扱いに係る指針[25]を公表している[26]。

図表 15　暗号資産の会計上の取扱いに係る指針の概要

カテゴリ	論点	実務対応報告
認識	■ 預かった暗号資産を貸借対照表に載せるべきか ■ （暗号資産交換業者）	■ 暗号資産交換業者が顧客から預かった暗号資産は、貸借対照表に資産として計上するとともに、同額を負債に計上する
	■ 売買損益の認識タイミングはいつか ■ （保有者及び暗号資産交換業者）	■ 売買契約の成立時点で売却損益を認識する

[25] 実務対応報告第 38 号「資金決済法における仮想通貨の会計処理等に関する当面の取扱い」（2018 年 3 月 14 日公表）
[26] 資金決済法上の暗号資産に関して会計上の取扱いを定めたもので、自己（自己の関係者を含む）が発行した暗号資産については対象外

測定	■ 期末における保有暗号資産に係る評価 ■ （保有者及び暗号資産交換業者）	■ 活発な市場が存在する仮想通貨であれば、時価で評価し、評価差額は損益処理 ■ 活発な市場が存在しない場合には、取得原価評価。ただし、期末日の処分見込価額が取得原価よりも下落している場合には損失処理（切放し法）
表示	■ 暗号資産売却額を PL 上総額で表示するのか、純額で表示するのか ■ （保有者及び暗号資産交換業者）	■ 純額表示
開示	■ どのような注記を行うべきか ■ （保有者及び暗号資産交換業者）	■ 期末日に保有する暗号資産の貸借対照表価額 ■ 暗号資産交換業者が預かっている暗号資産の貸借対照表価額 ■ 暗号資産の種類ごとの保有数量及び貸借対照表価額（活発な市場があるかないかの別を含む）等

なお、次の節で詳述するが、法人税法上、期末に保有する暗号資産は活発な市場が存在する場合、時価評価が行われ含み損益が課税所得計算に参入される。

図表 16　暗号資産に係る会計上・法人税の期末評価の方法[27]

活発な市場の有無	**会計上の取扱い**		**税務上の取扱い**	
			評価	**申告調整**
有り	自己の計算において有する暗号資産	期末時価評価 損益処理	時価評価 益金・損金算入	無し
	自己以外の者の計算において有する暗号資産 （預り暗号資産）		時価評価 益金・損金算入しない	有り
無し	取得原価≦処分見込価額	取得原価	取得原価	無し
	取得原価＞処分見込価額	処分見込価額 （損失処理）	取得原価	有り

（3） 米国会計基準における動向

1）現行の取扱い

米国における会計基準設定主体である FASB（Financial Accounting Standards Bord）は暗号資産に係る会計上の取扱いを公表しておらず、米国公認会計協会のデジタル資産ワーキンググル

[27] 法人税法上、資金決済法に定義する暗号資産は「短期売買商品等」に含まれ、活発な市場が存在するものについては、期末における時価により評価した金額をもって評価額とする旨等が規定されている（法人税法 61 第 2 項、法人税法施行令 118 の 7、118 の 8、118、及び国税庁「暗号資産に関する税務上の取扱いについて」問 22 参照）。

ープが 2019 年 12 月に公表した「デジタル資産の会計及び監査上の取扱い（Practice Aid, Accounting for and auditing of digital assets)」が実務上参考にされている。その要点は以下の通りである。

- このガイドラインにおける「暗号資産」は、①交換媒体として機能し、②以下の特徴を有するものを範囲としており、a）政府等公的機関が発行するものではなく、b）保有者と他の当事者との契約が生じるものではなく、c）証券に該当しない
- 「暗号資産」は、通常無形資産の定義を満たし、企業の将来キャッシュフローに貢献されると期待される期間に制限がない限り、耐用年数の確定しない無形資産に区分される
- 耐用年数が確定しない無形資産については、年 1 回以上の頻度で減損テストを実施し、デジタル資産の公正価値が帳簿価額を下回ると判断した場合、その時点で減損損失を計上しなければならず、仮に期末時点で公正価値が回復していたとしても戻入れは禁止される
- 「暗号資産」は、有形財ではないため棚卸資産の定義を満たさないが、ブローカー・ディーラーが自己取引の中で売買し保有する暗号資産については、ブローカー・ディーラーが扱う「棚卸資産」として会計処理を行うことも考えられる
- 特殊な業界のガイダンス（例えば、トピック 946「金融サービス-投資会社」の範囲内の企業）および特定の規制ガイダンスに従う企業は、暗号資産を公正価値で測定することが要求される場合がある

2）FASB における今後の展開

FASB は、2022 年 10 月 12 日に開催したボード会議において、以下の論点に関する検討を行い、その内容を公表した。

1. 「暗号資産」の測定基準として、(a）減損を考慮した取得原価、(b）正味実現可能価額（NRV)、(c）公正価値のいずれが妥当であるか
2. 質問 1.で（C）を選択した場合、主要な測定基準は、要求事項とするべきか、オプションとするべきか
3. 市場が活発でない「暗号資産」の測定に関して、 (a） 公正価値の使用禁止、(b） 減損控除後の取得原価計上、(c） ゼロ計上する、のいずれが妥当であるか
4. 「暗号資産」の取得コストは、資産計上すべきか、それとも発生時に費用計上すべきか
5. 「暗号資産」の公正価値測定の適用に関して、追加的な適用ガイダンスを提供すべきか
6. 非公開企業の「暗号資産」の測定について、非公開企業との差異を設けるべきか

なお、ここで「暗号資産」は以下の要件を満たすものに限定されている。

- FASB 会計基準編纂書マスター用語集に定義されている無形資産の定義に合致していること
- 保有者に対して、商品、サービス又はその他の資産に対する強制力のある権利又は請求権を与えないこと
- 分散型台帳または「ブロックチェーン」上に作成される、または存在する
- 暗号技術によって保護されている
- 交換可能である

特に重要な 1 つめの論点については、各調査の結果、圧倒的多数が（c）公正価値測定を支持、すなわち、暗号資産の期末保有につき、Topic 820「公正価値測定」のガイダンスを用いて暗号資産を公正価値で測定し、公正価値の増減は各報告期間において包括利益として認識するべきであるとの見解が多数を占めたことが分かった。その場合、包括利益について、(a)「純利益」に含めるべきか、(b)「その他の包括利益」の区分に表示するべきかは、損益計算書の表示の論点として、今後のボード会議で検討される予定となっている。

（4） 国際財務報告基準（IFRS）における動向

1）現行の取扱い

IFRS では暗号資産の会計上の取扱いは規定されていないが、企業が保有する暗号資産につき現行の IFRS からどの基準をあてはめることが適切かという点につき、2019 年 6 月に開催された IFRS 解釈指針委員会でアジェンダ決定「暗号通貨の保有」が決議されている。その概要は以下図表の通りである。

図表 17　国際財務報告基準における動向

条件	適用される基準	基準内での区分	期末評価	日本基準との比較
事業の通常の過程で保有する暗号資産	IAS 第 2 号「棚卸資産」	■ コモディティブローカー・トレーダーに関する測定上の例外規定に該当する場合	■ 売却コスト控除後の公正価値で測定して、帳簿価額との差額を純損益とする（FVPL）	■ 活発な市場がある暗号資産の処理と整合的
		■ 上記以外の場合	■ 低価法により測定し、帳簿価額との差額は純損失とする	■ 活発な市場がない暗号資産の処理と整合的（但し、洗い替え法と切放し法の違いあり）
上記に該当しない暗号資産	IAS 第 38 号「無形資産」	■ －	■ 原価モデル（減損が必要な場合は、その額を純損失に計上する）	■ 日本基準では該当なし
			■ 再評価モデル（公正価値で測定し、帳簿価額を超える部分をその他の包括利益とし、下回る部分は純損失とする）	■ 日本基準では該当なし

ここでは、「発行者に対する請求権がない暗号通貨」（典型的にはビットコイン）についてのみを対象としており、何らかの請求権がある場合等についてそのまま適用する指針にはならない

「暗号通貨」の範囲は、「①分散台帳に記録され、セキュリティのために暗号を使用するデジタル又は仮想の通貨であり、②国家機関その他の者が発行するものではなく、③暗号通貨の保有は、保有者と他の者との間の契約を生じさせなるものではない」ものに限定されている

2）今後の展開

EFRAG が 2022 年 4 月に公表したレポート[28]では、現行の IFRS においてトークンの会計上の取り扱いに関して検討を要する点として以下のような指摘が示されており、今後の基準開発において参考にされるものと考えられる。

- 保有する暗号資産の期末時価評価の是非を検討するべきである
- セキュリティトークン及びアセットトークンについて、会計上の金融商品の定義にあたるか否かの判断指針を明確にするべきである
- あるトークンが複数のトークンの性質を併せ持つ場合に（ハイブリッドトークン）、どの会計基準をどのように適用するかについて明確化が必要である
- カストディアン等、他社のトークンを預かっている者についての会計処理が現在明確ではないため、この点をクリアにする必要がある

レポートの概要は以下図表の通りである。

図表 18　暗号資産等の保有者に係る会計処理の
「現行 IFRS への当てはめ」と「基準開発上の提言」

トークンの種類	経済的特性及び保有者の権利	現行 IFRS への当てはめ	今後の IFRS 開発に対する提案
発行者に請求権のない暗号資産	■ 発行者に対する請求権がない ■ 相当する財及びサービスを受け入れる相手方と交換する暗黙の権利	■ 2019 年の IFRS IC アジェンダの決定によると、IAS 38（無形資産）または IAS 2（棚卸資産）のいずれかが適用される	■ ステップ①　IAS 38 の測定要件を修正し、同基準の範囲内で暗号資産の FVPL を認める可能性を検討する。暗号資産を原価と公正価値のどちらで測定すべきか、公正価値の表示を損益と OCI のどちらで行うべきかを決定するための混合測定原則を策定する。これらの原則は、保有主体のビジネ

[28] EFRAG “Recommendations and feedback statements EFRAG Discussion Paper On Accounting For Crypto Assets（Liabilities）”（2022 年 4 月）

			スモデルと測定の不確実性を考慮すべき ■ 原価で測定された暗号資産の公正価値、およびそのリスクと経済的実質を理解するのに役立つ情報の開示を要求する
電子マネートークン-発行者に対する請求権があり、各国の定義で電子マネーに該当する暗号資産 **ステーブルコイン** **CBDC**	■ 代替可能性、売買可能性及び移転可能性がある ■ 発行者に対する請求権がある ■ 財及びサービスと等価で交換することのできる暗黙の権利がある	■ 金融商品の定義が満たされている場合はIFRS 第 9 号（金融商品）、CBDC の場合はIAS 第 7 号（金融商品：開示）のいずれかを想定 ■ ステーブルコインが現金同等物に分類される場合の明確化が必要	■ ステップ① 金融商品の定義を満たす電子マネートークン及びステーブルコインのヘッジ会計要件の適用性の明確化 ■ ステーブルコイン、電子マネートークンが現金等価物または金融商品に分類される場合の明確化 ■ 電子マネーのトークンとステーブルコインの公正価値と主要な経済的特性の開示を要求
セキュリティトークン **アセットトークン**	■ 代替可能性、売買可能性及び移転可能性がある ■ トークン発行者に対する所有持分又は支配力に係る契約上の権利 ■ 発行者又は発行者が委任した相手方に対する請求権	■ 金融商品の定義に該当するものは IFRS 第 9 号（金融商品） ■ 金融商品の定義に該当しないものについて、どの基準を適用するか不明	■ ステップ① 金融商品の定義に適合する有価証券及びアセットトークンに係るヘッジ会計の適用可能性の明確化。 セキュリティトークン及びアセットトークンの中で、IFRS の金融商品の定義を満たさなくなる可能性のある経済的特性、権利及び義務に係る開示を要求 ■ ステップ② IFRS の金融商品（金融資産）の定義を満たさない可能性のあるセキュリティトークン及びアセットトークンに係る保有者の会計処理に関する更なる調査と明確化が必要
ユーティリティトークン	■ 代替可能性、売買可能性及び移転可能性がある ■ 場合によっては NFT が含まれる可能性がある	■ IAS 第 2 号（棚卸資産）、IAS 第 38 号（無形資産）または前払資産のいずれに該当することになるのか明確化が必要	■ ステップ① 保有するユーティリティトークンの経済的特徴、権利及び義務に係る開示を要求 ■ ステップ② 保有するユーティリティトークンの

	■ 発行者又は発行者が委任した相手方に対する請求権がある場合がある		権利内容の更なる調査と適切な会計処理の明確化が必要
ハイブリッドトークン	■ ユーティリティトークン、セキュリティトークン又は支払トークンの特徴の組合せ ■ 発行者又は発行者が委任した相手方に対する請求権	■ 明確化が必要 ■ 基になっている権利の支配的な性質及び保有者の事業目的、又はさまざまな基礎となる権利の分解に応じて決まる	■ ステップ① 保有するハイブリッドトークンの経済的特性、権利及び義務に係る開示の要求 ■ ステップ② さらなる調査と明確化が必要
機能前トークン	■ 将来サービス開始の段階で他のトークンに転換することになっているトークン ■ （通常はユーティリティトークンに転換するが、そうでない場合もありうる） ■ 機能前トークンは、ブロックチェーンネットワーク上でプロトコルに従って移転可能ではあるが、サービス開始前の段階であるため、ネットワーク上のユーティリティを提供できないトークンのこと	■ 明確化が必要 ■ ユーティリティトークンと同様に、IAS 第 2 号または IAS 第 38 号の範囲内と仮定するか、または前払資産に該当する可能性もある	■ ステップ① 保有する機能前トークンの経済的特性、権利及び義務の開示の要求 ■ ステップ② ユーティリティトークンの適切な分類の原則（保有者の意図 vs 変換後トークンの性質）を含む、機能前トークンに適用される IFRS のさらなる調査と明確化が必要。またはこれらをデリバティブとみなすべきかどうかの明確化が必要
SAFT（通常、機能前トークンと一緒に発行される）	■ 将来のトークンの権利であり、有価証券とみなされる	■ IFRS 上明確化が必要。金融商品の定義を満たしている場合は、IFRS 第 9 号の適用対象に含まれると考えられる ■ 金融商品の定義に該当しないものについて、どの基準を適用するか不明	■ ステップ① SAFT 保有の経済的特徴、権利及び義務の開示の要求 ■ ステップ② 金融資産の分類を伴う IFRS 第 9 号がすべての SAFT に適用されるかについての更なる調査と明確化
他社のためにトークンを保有する者（ブローカー、カストディアン）	-	■ IFRS には、保有者が他者に代わって暗号資産を保有する場合の会計処理を行うことについての明確な要求事項がない	■ ステップ① 以下の点を含め、保有者が他者に代わって保有する場合の認識及び測定について IFRS の要件の明確化:

		■ 本人と代理人に係る会計処理の問題は、異なる IFRS 基準にまたがって発生する	• 暗号資産を経済的に支配している主体（預託者 vs 仲介者）を判断するためクライテリアの明確化 • 預託者と仲介者にそれぞれどの IFRS が適用されるかの明確化（IAS 第 2 号、IAS 第 38 号、IFRS 第 9 号）および • 預託資産の価値を測定する際に、カストディアンの信用リスクを考慮すべきかを明確化する

1－5. 税制

この節では、主要国における暗号資産に係る法人税制の調査を行った。

（1） 調査対象国の法人課税の概要

まず、以下図表に今般調査の対象国並びに法人課税の概要・課税所得・税率を一覧表として整理した。

図表 19　調査対象国の法人課税の概要・課税所得・税率

	国名	通貨	概要
1	アメリカ	USD	■ 内国法人は全世界所得に対して課税される ■ その源泉を問わず、総所得が課税所得となる（減価償却費等の項目の控除が一定程度認められる） ■ 連邦法人税率：21%、州法人税率：州によって異なる
2	フランス	EUR	■ 内国法人及び外国法人は、フランスの事業に割り当てられる利益と国内源泉所得に対して課税される ■ 帳簿上の所得に一定の税務調整（加算・減算）を加えたものが課税所得となる ■ 法人税率：原則として 25%（2022 年 1 月 1 日以降）
3	ドイツ	EUR	■ 内国法人は全世界所得に対して課税される （外国法人は国内源泉所得のみ） ■ 法人の利益が課税所得となる （課税所得計算上、事業費を控除することができる） ■ 法人税率：15%（連帯付加税を含め 15.825%）、営業税（地方税）：7~17%
4	スイス	CHF	■ 内国法人は全世界所得に対して課税される （外国法人は国内源泉所得のみ） ■ 法人の純利益が課税所得となる （課税所得計算上、事業費を控除することができる） ■ 連邦税：8.5%、州・地方自治体税：12~18%
5	シンガポール	SGD	■ 一定の例外を除き、シンガポールで発生又はシンガポールに由来するすべての所得、及び前年にシンガポールに送金又は送金されたとみなされるすべての国外所得に対して課税される（内国法人は国外源泉所得に対する課税の免除等の恩恵を受けることができる） ■ 法人税率：17%
6	韓国	KRW	■ 内国法人は全世界所得に対して課税される （外国法人は国内源泉所得のみ） ■ 会計と税務の差異を調整した帳簿上の純利益が課税所得となる ■ 法人税及び地方所得税率：11%~27.5%（超過累進税率）
7	ドバイ	AED	■ 一部の業種（外国銀行支店や石油会社等）を除いて法人課税が行われていない
8	日本	JPY	■ 内国法人は全世界所得に対して課税される （外国法人は国内源泉所得のみ） ■ 各事業年度の総収入金額（益金）から事業費（損金）を控除した金額が課税所得となる ■ 法人税率：23.2%（資本金 1 億円を超える普通法人の場合）

（2） 暗号資産に係る税制

対象国の暗号資産に係る税制を概観するために、まず OECD が取りまとめた報告書[29]の概要を以下図表に整理する。なお、OECD の報告書においては、マイニングにより取得する暗号資産の課税について議論されており、ICO に係る課税関係については詳しく言及されていない。

図表 20　OECD 報告書の概要

	取得時課税	処分時課税
取得/処分の意義	■ 取得には、マイニングによる取得や ICO による作成が含まれる（OECD の報告書においては、マイニングによる取得にフォーカスし議論がなされている） ■ 韓国は ICO が法令上禁止されている。ドバイ（UAE）については一部を除き法人税課税制度がないため、記載対象外としている	■ 処分には、法定通貨、暗号資産及び財との交換、贈与や紛失等が含まれる ■ 課税対象となる処分の範囲が国によって異なる
暗号資産のライフサイクルにおける最初の課税契機として当該課税を行う国	■ 日本、アメリカ等	■ フランス等
個別事例-スイス	■ ―	■ 仮想通貨の処分は決済手段と同様に扱われているため、取引による損益は課税対象とならない ■ ただし、取引の種類及び範囲が商業的と認められるに足りる場合には、課税対象となる
個別事例-フランス	■ ―	■ 個人所得税においては、仮想通貨を法定通貨、財、サービス、および別の仮想通貨と交換（価値の差額を法定通貨で支払う場合に限る）する場合には、課税対象となる

暗号資産のライフサイクルにおいて、最初の課税は主に取得時又は処分時に発生するが、以下に示すように、一部の国では暗号資産取引を行う者や取引自体の性質により取扱いが異なる。

[29] OECD （2020）, Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues.

図表 21　ビジネス活動か否かによって異なる取扱いをとる国々

	取扱い
スイス	■ マイニング資産により生ずる個人のキャピタルゲインは、その活動が私的資産管理として行われる場合には、課税対象とならない。しかし、マイニングが実入りの良い事業活動と見られる場合には、当該資産の処分には譲渡所得税が適用される
シンガポール	■ 仮想通貨の受け取りによるマイニング実行者の利益は、利益を得る目的で活動を行った場合、その利益または損失が本質的に取引であると評価されれば、課税対象となる ■ 通常、マイニング活動を行う企業は事業を行っているとみなされ、トークンの処分には通常の所得税規則が適用される

次に、OECD の報告書で言及されていない ICO に係る課税関係について、スイスとシンガポールでは各課税当局等が公表しているガイドラインにより詳細な確認を行った。

スイスの法人課税は、税務上の特別な規則が無い限り、会計処理に準拠することとされており、ICO によるトークン発行者の課税上の取扱いは、そのトークンの性質によって取扱いが異なる。

図表 22　トークンの区分と課税上の取扱い（スイス）[30]

	定義	トークン発行者における課税
支払いトークン（Payment tokens）	■ 一般的な意味の「仮想通貨（cryptocurrencies）」に相当し、他の機能やプロジェクトとつながりを持たないトークンをいう	■ とりわけ発行会社の目的に応じて、個別事例に即した分析により、トークン発行に係る発行者の課税上の取扱いが決定される
ユーティリティトークン（Utility tokens）	■ デジタルアプリケーションまたはサービスへのアクセスを提供するトークンをいう	■ 原則として、法人がトークンを発行した場合、その調達資金によってプロジェクトが展開される期間中は、発行者において引当金を計上することにより、課税上の利益は実現しない。ただし、引当金計上の要件として、ホワイトペーパーの公表等が必要とされる ■ 調達資金がプロジェクトの開発に使用されず、かつ、投資家に還元されない場合に限り、当該調達資金は、ホワイトペーパーに記載した当該プロジェクトの完了又は廃止事業年度における課税上の利益となる
インベストメントトークン	■ 発行者が投資の全部又は一部を返還し、若しくは利子を支払う義務を有するトークンをいう	■ 発行により調達した資金は課税利益として扱われない。また、投資

[30] AFCGE （2019）, Guide: Digital Token Generations in the Canton of Geneva. - スイス・ジュネーブ州課税当局によるガイドラインを基に作成

外国資本トークン（Foreign capital tokens）		家への利子の支払いは、費用として損金算入の対象となる
インベストメントトークン 株式/参加トークン（Equity and participation tokens）	■ 発行者が投資家に配当を支払うか否かにかかわらず、発行会社の年次利益等の指標に基づき算定される経済的利益がそれぞれの持分に応じて投資家に与えられるが、投資の全部または一部の返還請求権が投資家に与えられていないトークンをいう	■ プロジェクトの開発期間中は、課税上の利益は実現しない。調達資金がプロジェクトの開発に使用されず、かつ、投資家に還元されない場合に限り、当該調達資金は、ホワイトペーパーに記載した当該プロジェクトの完了又は廃止事業年度における課税上の利益となる
ハイブリッドトークン（Hybrid tokens）	■ 上記のトークンのいくつかの特性を持つもの	■ 該当するトークンの特性に最も適切な課税を決定するために、スイス・ジュネーブ州の課税当局 AFCGE と協力して具体的な分析を行う必要がある

シンガポールでは、ICO によるトークン発行者の課税上の取扱いは既存の所得税法の取扱いに基づくデジタルトークンの区分によって異なる。

図表 23　トークンの区分と課税上の取扱い（シンガポール）[31]

	定義	トークン発行者における課税
支払いトークン（Payment token）	■ 商品やサービスの支払手段として利用できる又は利用することを目的としたデジタルの権利をいう	■ 基本的な考え方として、支払トークンは売買目的の株式のように扱われるため、トークン発行者は ICO 時点で課税される ■ ただし、ICO による支払トークンの発行は一般的ではないため、その課税上の取扱いを決定するには、事実関係の精査が必要である
ユーティリティトークン（Utility token）	■ 商品またはサービスに対する権利を表すデジタルトークンをいう	■ トークン発行者は、投資家に対して将来的に財又はサービスを提供する義務を負う。そのため、トークン発行者は ICO 時点で課税されず、義務を履行した時点で課税対象となる
セキュリティトークン（Security token）	■ 株式や、会社の株式や債券などの原資産への投資を表すデジタルトークンをいう	■ 発行されたトークンを引き受けた投資家は出資者又は債権者と類似するものと考えられる。そのため、トークン発行者は ICO 時点で課税されない

[31] IRAS （2020）, IRAS e-Tax Guide Income Tax Treatment of Digital Tokens- シンガポール課税当局によるガイドラインを基に作成

		■ ただし、トークンに係る分配については配当又は利子に対して適用される一般的な税制の適用を受け、非居住者に対する分配の場合には源泉徴収義務が発生する

（3） 暗号資産の期末時価評価課税について

調査対象の諸外国では制度上暗号資産の時価評価を行う国は見受けられない一方で、日本では、活発な市場を有する暗号資産に限り期末時価評価課税が行われる。

1）日本を除く調査対象国の概要

米国、フランス、ドイツ、スイス、シンガポール、韓国及びドバイにおいて、法人が保有する暗号資産の期末時価評価を行う制度は見受けられず、OECD の報告書では期末時価課税に関連するポイントは以下のように取り上げられている。

- 暗号資産の作成及び処分というイベントは課税の契機となり得るものとして検討対象となるものの、暗号資産の保管は一般に課税の契機を発生させないため議論の対象にならない
- 暗号資産の時価評価課税についての言及が無く、当該報告書が世界各国の暗号資産に係る課税制度の概観を示すことを目的の一つとしていることを鑑みると、諸外国にそのような制度がないことを示唆していると考えられる

暗号資産を主な対象として想定した期末時価評価課税制度は上述の通り存在しない可能性が高い。しかしながら、調査対象国の税制を詳細に調査した場合には、一般的な金融資産の時価評価課税制度に内包される形で暗号資産が時価評価の対象とされることが発見される可能性がある点には留意されたい。

2）日本における暗号資産の期末時価評価課税

日本においては活発な市場のある暗号資産は期末時価評価課税が原則となっており、そのポイントは以下の通りである。

- 法人が事業年度終了の時において有する暗号資産（活発な市場が存在する暗号資産に限る。）については、時価法により評価した金額をもってその時における評価額とする（法人税法第 61 条第 2 項）
- また、暗号資産（活発な市場が存在する暗号資産に限る。）を自己の計算において有する場合には、上記評価額と帳簿価格との差額（評価益又は評価損）を、その事業年度の益金の額又は損金の額に算入しなければならない。また、この評価損益は翌事業年度で洗替処理をする（法人税法第 61 条第 3 項、法人税法施行令第 118 条の 9 第 1 項）

また、ここでいう「活発な市場が存在する暗号資産」は内国法人が保有する暗号資産のうち次の要件のすべてに該当するものをいう（法人税法施行令第 118 条の 7 第 1 項）。

1. 継続的に売買の価格の公表がされ、かつ、その公表がされる売買価格等がその暗号資産の売買の価格又は交換の比率の決定に重要な影響を与えているものであること
2. 継続的に 1.の売買価格等の公表がされるために十分な数量及び頻度で取引が行われていること
3. 次のいずれかの要件に該当すること
   - 1.の売買価格等の公表が当該内国法人以外の者によりされていること
   - 2.の取引が主として当該内国法人により自己の計算において行われた取引でないこと

なお、令和 5 年税制改正要望として、「法人が発行した暗号資産のうち、当該法人以外の者に割り当てられることなく、当該法人が継続して保有しているものを対象として、期末時価評価課税の対象外とする」旨の要望が金融庁、経済産業省共同で提出されており、2022 年 12 月 16 日に自民党が公表した「令和 5 年度与党税制改正大綱[32]」で自社発行暗号資産の期末時価評価課税の見直しが盛り込まれている。

3）各国における暗号資産の期末時価評価課税の状況

以下の図表に対象国各国における暗号資産の期末時価評価課税に関する取扱いの概要を取りまとめた。

図表 24　各国の暗号資産の期末時価評価の詳細[33]

	時価評価の詳細
スイス	■ 税法上の特別な規定はないため、会計上の取扱いに準拠することとなる ■ 仮想通貨について、期末時価評価は行われない。ただし、帳簿価額が公正市場価値よりも低い場合には、減損の必要がある
シンガポール	■ 会計基準において金融資産が時価評価の対象とされており、税法においても同じ扱いをすることとされている ■ セキュリティトークンはここにいう金融資産に該当する可能性があるものの、その他のトークンは一般には金融資産に該当しないと考えられる。したがって、セキュリティトークン以外のトークンの多くは、一般に時価評価の対象外となる
アメリカ[34]	■ 基本的に、暗号資産に係る期末時価評価は不要である ■ ディーラーやトレーダーが選択した場合には、評価損益を認識することもできることとされている
フランス	■ 法人が保有する NFT 以外のトークンについては、期末時価評価課税が行われる可能性がある

[32] https://storage.jimin.jp/pdf/news/information/204848_1.pdf

[33] 調査対象国のうち、ドイツと韓国は公表情報から期末時価評価課税に関する情報が得られなかったため、こうした制度が無いものと推測される。スイス、シンガポール、フランスについてはデロイトグループの各種助言実績を基に作成した

[34] Deloitte （2021）, Corporates investing in crypto: Considerations regarding allocations to digital assets.

ドバイ（UAE）	■ 一部の業種（外国銀行支店や石油会社等）を除いて法人課税が行われておらず、期末時価評価課税もなし
日本	■ 活発な市場を有する暗号資産については期末時価評価をしなければならない（法人税法 61 条 2 項）

1－6. 法的整理

1－6－1. 暗号資産に係る法規制 （海外比較）

この節では税制と同じ対象国における暗号資産の法規制の概要を以下の図表に整理した。主なポイントは以下の通りである

- 米国
  - 仮想通貨の定義は各州法でなされているところもある一方、仮想通貨該当性とは別に投資契約該当性が別途連邦法に基づいて判断される点は SEC[35]が所管するため連邦法にも留意が必要である
  - 現状、米国では投資契約の取引システム（ATS[36]）等は連邦法の定めに従い、暗号資産のサービス提供者は、NY 州の BitLicence のように各州で規制が定められている場合はその州法での定めに従う
  - 準拠すべき AML/CFT 規制が存在する
- シンガポール
  - 決済サービス法においてデジタルトークンが定義される
  - シンガポールでは DPT サービスに該当するものは規制対象となる
  - 準拠すべき AML/CFT 規制が存在する
- スイス
  - 暗号資産の法的定義、暗号資産サービス特有のライセンスは無い
  - 準拠すべき AML/CFT 規制が存在する
- ドバイ（Dubai International Financial Centre）
  - 暗号資産の法的定義、暗号資産サービス特有のライセンスは無い
  - 準拠すべき AML/CFT 規制が存在する
- 韓国
  - 日本における暗号資産に相当するものが仮想資産として定義され、仮想資産サービスプロバイダーは VASP として登録を求められる
  - 準拠すべき AML/CFT 規制が存在する
- ドイツ
  - 日本における暗号資産に相当するものの法的定義はある一方、独自のライセンスは設けられていない
  - 準拠すべき AML/CFT 規制が存在する
- フランス
  - 日本における暗号資産に相当するものの法的定義及び独自のライセンス（PACTE 法における DASP）がある
  - 準拠すべき AML/CFT 規制が存在する
- イギリス

[35] 米国証券取引委員会

[36] ATS: 私設取引システム

- 日本における暗号資産に相当するものの法的定義はある一方、独自のライセンスは設けられていない
- 準拠すべき AML/CFT 規制が存在する

図表 25　暗号資産に係る法規制

	米国[37]		シンガポール
	連邦法	州法（NY 州）	
暗号資産規制の有無	■ 仮想通貨（virtual currency）[38]特有の規制は存在しない。ただし、証券法等の規制を受ける可能性がある	■ 各州は、仮想通貨関連事業に係る規制の適用に関してさまざまなアプローチを採用しており、NY 州では仮想通貨特有の規制が存在する	■ BTC や ETH、LTC などを含む「デジタル決済トークン」（Digital payment token。以下「DPT」という。）は決済サービス法（The Payment Services Act 2019 以下「決済サービス法」又は「PSA」という。）により規制される
根拠法令	■ 証券法（The Securities Act of 1933） ■ 証券取引所法（The Securities Exchange Act of 1934） ■ 商品取引所法（The Commodities Exchange Act）	■ NY 州金融サービス法に基づく仮想通貨規制（23 NYCRR Part 200）	■ 決済サービス法
暗号資産の定義・要件	■ 仮想通貨それ自体の定義は存在しない ■ ただし、問題となっている仮想通貨が証券法及び証券取引所法上の「投資契約」（investment contract）に該当する場合、仮想通貨の発行体は登録免除要件を満たさない限り米国証券取引委員会（Securities and Exchange Commission。以下	■ 仮想通貨とは、「交換の媒体又はデジタルで貯蔵された価値の形態として使用されるあらゆる種類のデジタル単位をいい、(i) 中央集権的なレポジトリ・管理者を有するもの、(ii) 非中央集権的で中央集権的なレポジトリ・管理者を有しないもの、又は（iii）コンピューティング・製造の努力によって作成・取得さ	■ DPT は、以下の要件を満たすデジタルトークンとして定義されている ➢ 単位で表現されること ➢ いかなる通貨建てでも、また、発行者によっていかなる通貨ともペッグされていないこと ➢ 商品若しくはサービスの対価として、又は債務の弁済のために公衆又は公衆の一部によって受け入れられる交換媒体であり、またはそうなることを意図しているものであること

[37] 米国は連邦制が採用されており、その中で連邦法は州際に渡る事項を規定し、州法は州内の事項を規定する。また、連邦法が存在する領域については、連邦法は州法に優位する。

[38] 日本の資金決済法に定める「暗号資産」との混同を避けるべく、米国における“virtual currency”については「仮想通貨」との訳語を使用する。

	「SEC」という。）へ登録を行う必要がある ■ 以下の要件全て（Howey Test）を充足する場合、「投資契約」に該当する ■ 他者の努力により利益を得る合理的な期待をして共同事業に資金を出資すること ■ なお、デジタル資産の Howey Test の要件充足性について SEC がフレームワークを公表している ■ 商品先物取引員会（The Commodities Futures Trading Commission）は、商品取引所法に基づき、「商品」のデリバティブ取引及び「商品」現物に係る不公正取引規制を所轄しているところ、仮想通貨は同法における「商品」に含まれると解釈している	れるものを含む。」と定義されている	➢ 電子的に転送、保存、または取引することができること ➢ 当局が規定するその他の特性を満たしていること
暗号資産の取引に係るライセンス	■ 仮想通貨が「投資契約」に該当する場合、投資契約を含む証券について複数の買い手と売り手の注文を取りまとめる、私設取引システム（ATS）を営業する場合は規制の対象となる ■ 2022 年 3 月、SEC より証券取引所（Exchange）の定義を拡大し、通信プロトコル等も証券取引所の定義に含まれる旨の改正規則案が提出されている。これにより、仮想通貨の分散型取引所やマーケットメイキン	■ NY 州において、又は NY 州居住者に対して以下の業務を行う場合、仮想通貨事業活動（Virtual Currency Business Activity）に該当し、原則としてライセンス（以下「BitLicence」という。）を取得する必要がある ■ 送付に係る仮想通貨の受領、又は仮想通貨の送付 ■ 他人のために仮想通貨を保管、保有、管理すること ■ 顧客との事業として仮想通貨を売買すること	■ DPT の取引は、デジタル決済トークンサービス（Digital payment token service 以下「DPT サービス」という。）に該当する可能性がある。DPT サービスとは、以下のいずれかの行為をいう ➢ DPT を金銭を用いて売買又は他の DPT と交換する行為 ➢ デジタル決済トークン取引所の開設・運営を行う行為 ■ なお、2021 年 1 月に成立した改正決済サービス法によれば、DPT サービスの範囲が拡大され、以下の行為も対象となる ➢ あるアカウントから別のアカウントへの DPT の送信を容易にする行為 ➢ DPT のカストディサービス

	グプロトコルを採用するプラットフォームも規制の対象となる可能性がある	■ （仮想通貨の）取引所の業務を行うこと ■ 仮想通貨の管理または発行を行うこと ■ BitLicence を取得する者は NY 州金融サービス局（Department of Financial Services（以下「DFS」という。））の監督下におかれる	➢ サービスプロバイダが関係する貨幣または DPT を所有しない場合に、DPT の交換を促進すること ■ DPT サービスを行うには、取引高に応じて、standard payment institution license 又は major payment institution license の取得が必要とされている ■ 上記ライセンスを保有する者には、主に、以下の規制・義務が課せられる ➢ 特定の事由に係る規制当局への通知義務 ➢ 規制当局への情報提供義務 ➢ 定期的な事業報告の義務 ➢ 個人に対する信用供与などといった特定の事業の制限 ➢ 顧客から受け取った金銭の保護 ➢ 一定の資本金の維持 ➢ 顧客資産の分別管理
AML/CFT	■ 米国財務省の機関である金融犯罪執行ネットワーク（The Financial Crimes Enforcement Network（以下「FinCEN」という。））は、AML/CFT に関する規制を定める銀行秘密保護法（The Bank Secrecy Act （以下「BSA」という。））を含む連邦法を執行する ■ 仮想通貨事業者が BSA 上の Money Transmission Services（通貨又はそれに代わる価値を送金等するサービス）を行う場合は Money Transmitter に該当し、Money Services Businesses（以下「MSB」という。）を	■ BitLicence を取得して事業を行う者は主に以下の義務を負う ■ 法令リスク等の評価に基づく AML プログラムの策定・実施 ■ AML プログラムには内部統制の確立、報告書の提出、AML プログラム担当者の設置、従業員の研修等が含まれる ■ 顧客情報を含む取引記録の作成及び 1 万米ドル以上の取引発生時の DFS への報告義務 ■ DFS は、送金サービスについて定めた NY 州銀行法（Consolidated Laws of New York, Chapter 2 Banking（以下「NYB」という。））も執行する。仮想通貨を取り扱う事業者が送金に係る業務等に従事	■ 決済サービス法は DPT サービス事業者に対して、顧客デューディリジェンス、取引監視、スクリーニング、疑わしい取引の報告及び記録管理に関連する方針、手順及び管理を含む追加の AML/CFT 要件を課している ■ 2022 年 4 月に成立した金融サービス市場法（The Financial Services and Markets Act 。以下「FSMA」という。）は、DPT を含む「デジタルトークン」に係る以下のサービスを提供する事業者に対して AML/CFT の範囲と規制負担を拡大することを意図している ➢ デジタルトークンの取扱い ➢ デジタルトークンの交換の促進 ➢ デジタルトークンの譲渡または譲渡の手配のためにデジタルトークンを受け入れること（サービスプロバイダがデジタルトークンを所有しない場

	行う者として FinCEN に登録する必要がある ■ MSB を行う者は以下の AML プログラムを実施する必要がある ➢ 顧客の身元確認、報告書の提出、記録の作成と保持、法執行機関の要請への対応に関する方針、手順、内部統制の確立 ➢ AML プログラム担当者の選任 ➢ 関係者に対する AML トレーニングの実施 ➢ 疑わしい取引の検出 ➢ 適切な AML プログラム監視、維持のための独立した評価の実施	する場合は NYB 上の Money Transmitter のライセンス取得が必要になる。また、Money transmitter の義務として、AML プログラムの策定、AML プログラム担当者の選定及び従業員の教育等を行う必要がある	合も含む） ➢ デジタルトークンの販売または購入に参加するよう、または参加することを申し出るよう誘導すること、または誘導しようとすること ➢ デジタルトークンまたはデジタルトークン機器の保護または管理であって、サービスプロバイダがデジタルトークンまたはデジタルトークン機器に関連するデジタルトークンを制御する、保護または管理 ➢ デジタルトークンの提供または販売に関する助言業務
国	**スイス**	**ドバイ（DCIF[39]）**	**韓国**
暗号資産規制の有無	■ AML/CFT 上の規制を除き、暗号資産に特有の包括的な金融規制は存在しない	■ 現時点では、AML/CFT 上の規制を除き、暗号資産に対する規制は存在しない[40]	■ 仮想資産（Virtual assets）は、特定金融取引情報の報告及び利用に関する法律（Act on Reporting and Using Specified Financial Transaction Information （以下「SFIA」という。））に基づき規制される
根拠法令	■ マネー・ローンダリング防止法（Federal Act on Combating Money Laundering and Terrorist Financing （Anti-Money Laundering	■ 連邦マネー・ローンダリング防止法（Federal Decree-law No. （20） of 2018 ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF	■ 特定金融取引情報の報告及び利用に関する法律（SFIA）

[39] The United Arab Emirates （以下「UAE」という。）憲法第 121 条は、フリーゾーンの設立を許可しているところ、2004 年連邦法第 8 号は、フリーゾーンの中でも特に「金融自由区域」と呼ばれる区域を許可している。金融自由区域においてはすべての連邦民事・商事法の適用が免除されるものの、連邦マネー・ローンダリング防止法等は依然として適用される（Article 3 of Federal Law No/8 of 2004 Regarding The Financial Free Zones）。UAE には、Abu Dhabi Global Market（以下「ADGM」という。）と Dubai Internal Financial Centre （以下「DIFC」という。）の 2 つの金融自由区域が設置されており、本資料では DIFC について整理している

[40]ただし、DCIF 内の金融規制機関であるドバイ金融サービス庁（Dubai Financial Security Authority。以下「DFSA」という。）が 2022 年 3 月 8 日に公表した「CONSULTATION PAPER NO.143」（以下「CP No.143」という。）において、暗号トークン（Crypto token）に関する規制の方針が示されている

	Act（以下「AMLA」という））	TERRORISM AND FINANCING OF ILLEGAL ORGANISATIONS。以下「連邦 AML 法」という））	
暗号資産の定義・要件	■ 暗号資産の定義は規定されていない	■ 現時点では、DCIF 法上、暗号資産の定義は規定されていない ■ ただし、CP No.143 によれば、「暗号トークン（Crypto Token）とは、決済や投資の目的で使用される、又は使用されることを目的としたトークンであり、投資トークン（Investment Token）やその他の投資、除外トークン（Excluded Token）以外のものをいい、また、暗号資産に関連する権利又は持分が含まれる。」との定義が案として示されている	「仮想資産」とは、経済的価値を有し、電子的に取引または移転が可能な電子的な証票をいう。ただし、次のものは除く (i) 金銭、商品又はサービス等と交換できない電子的証票又は電子的証票に関する情報であって、発行者により使用場所及び使用目的が制限されているもの (ii) ゲーム産業振興法第 32 条第 1 項第 7 号に基づくゲーム商品の利用により得られる有形・無形の商品 (iii) 電子金融取引法第 2 条第 14 号に基づく電子前払式支払手段及び同条第 15 号に基づく電子通貨 (iv) 株式、社債等の電子登録に関する法律第 2 条 第 4 項の規定に基づく電子登録株式 (v) 電子手形の発行及び配布に関する法律第 2 条 第 2 項の規定に基づく電子手形 (vi) 商法第 862 条に基づく電子船荷証券 (vii) 取引の形態や特徴を考慮して大統領令で定める取引
暗号資産の取引に係るライセンス	■ 暗号資産が証券に該当しない限り、その販売について特段のライセンスは存在しない	■ 暗号資産取引所に関する独自の法的枠組みは存在しない ■ ただし、CP No.143 によれば、DFSA は、暗号トークンに関連して以下のサービスを提供することを認めることを意図している ➢ 自己投資を行うこと ➢ 代理人として投資を行うこと ➢ 投資のアレンジメント ➢ 資産管理 ➢ 金融商品に関する助言 ➢ 取引所の運営 ➢ カストディの提供	1. 「仮想資産サービスプロバイダ」（Virtual asset service provider。以下「VASP」という。）とは、以下のいずれかに該当する事業を営む者をいう (i) 仮想資産の販売及び購入 (ii) 仮想資産を他の仮想資産と交換する行為 (iii) 大統領令で規定されている仮想資産の譲渡 (iv) 仮想資産の保持又は管理 (v) 仮想資産の販売及び購入及び仮想資産を他の仮想資産と交換する行為に定める行為について、仲介者、媒介者又は代理人となること (vi) その他大統領令で定める行為で、仮想資産に関連するマネー・ローンダリングやテロ資金調達に利用される可能性が高い行為

		➢ カストディのアレンジ ➢ クリアリングハウスの運営 ➢ 代替取引システムの運営	2. VASP は、韓国金融情報分析院（Korea Financial Intelligence Unit 以下「FIU」という。）への報告が義務付けられるところ、ISMS 認証を取得しなければ当該報告を拒絶される可能性がある。また、VASP は、口座名義人の本人確認ができる銀行預金口座での金融取引を行わない場合は、FIU に対する報告を拒絶される可能性がある
AML/CFT	■ AMLA は金融仲介者（Financial intermediaries）に適用されるところ、支払型トークンなどの暗号通貨の発行は「金融仲介」を構成する。また、ウォレットサービス業者は、カストディアンウォレットの秘密鍵を処分する権限を持っている場合には金融仲介者に該当する ■ 金融仲介者に該当する場合、顧客/契約当事者及び保有ファンドの受益者の身元の検証を義務付けられるとともに、疑わしい取引について Money Laundering Reporting Office に報告する必要がある。また、金融仲介者は、認可された自主規制機関と提携しなければならない ■ FINMA の監督下にある金融仲介者は、ブロックチェーン取引に関するトラベルルールを遵守する必要がある。具体的には、当該金融仲介者は、トラベルルールの下、法定通貨の電信送金に必要な情報と同じ情報を送信する	■ 連邦 AML 法においては、違法な資金移動を故意に行うことを禁止しており、規制対象となる「資金（Funds)」には電子的・デジタルなものも含むとされていることから、暗号資産も「資金」に含まれると解されている ■ AML 法は、金融機関や法令により指定された非金融ビジネスを行う事業体等（以下「金融機関等」という。）に広く適用される ■ 連邦 AML 法が金融機関等に課す主な義務は以下のとおり。 ➢ リスクの特定と評価 ➢ 顧客に対するデューディリジェンス ➢ リスク管理のための体制構築 ➢ 取引記録の保存	1. 顧客が 1 回の取引で 100 万ウォン以上の仮想資産を他の VASP に譲渡する場合、VASP は取引時に送信者・受信者の名前と仮想資産のアドレスを FIU に報告する必要がある 2. VASP は、送信者の住民登録番号、パスポート番号、または外国登録番号を収集し、FIU や仮想資産を送信された VASP の要求に応じて 3 営業日以内に当該情報を提供しなければならない 3. 金融取引等に関連して受領した資産が違法であると疑う合理的な理由がある場合、マネー・ローンダリングやテロ資金供与を行っていると疑うに足りる相当な理由がある場合等は、遅滞なく FIU に当該事実を報告しなければならない 4. 金融会社は、内部報告体制を整備し、ガイドラインを作成実施し、AML/CFT のための教育・訓練を行わなければならない

	か、又は下記を行わなければならない ➢ 譲受人がスイスの金融仲介者の顧客であるかのように、スイスの AML 規則に従って譲受人を特定すること ➢ 関連するスイスの金融仲介者が定義する適切な技術的手段により、譲受人が使用しているウォレットアドレスを処分する権限を確認すること		
国	**ドイツ**	**フランス**	**イギリス**
暗号資産規制の有無	■ 暗号資産特有の規制枠組みは存在せず、暗号資産に関連するサービスは、既存の銀行法（The Banking Act 以下「KWG」という。）及び投資会社法（The German Investment Firm Act。以下「WpIG」という。）等の金融規制により規制される	■ 暗号資産・暗号通貨を含む「デジタルアセット」（digital asset）は、金融法（The Monetary and Financial Code 以下「MFC」という。）及び「企業成長と変革行動計画法」（French law n 2019-486 of 22 May 2019 以下「PACTE 法」という。）に基づき規制される	■ AML/CFT 上の規制を除き、暗号資産（Cryptoasset）に特有の金融規制は存在しない。ただし、金融サービス市場法（The Financial Services and Markets Act 2000 （以下 FSMA）という。）等の既存の金融規制の対象となる可能性がある
根拠法令	■ 銀行法（KWG） ■ 投資会社法（WpIG） ■ Anti-Money Laundering Act（以下「GwG」という）	■ 金融法（MFC） ■ PACTE 法	■ 金融サービス市場法（FSMA） ■ テロリスト資金調達及び資金移動規則 2017（Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017（以下「MLRs」という））
暗号資産の定義・要件	■ KWG 上、暗号資産（Kryptowerte）とは、「中央銀行または公的機関によって発行または保証されておらず、通貨または貨幣の法的地位を有していないが、契約または慣習によって交換または支払いの手段として、ま	■ 「デジタルアセット」とは、「中央銀行又は公的機関が発行又は保証しておらず、必ずしも法的に確立された通貨に付随しておらず、通貨又は貨幣としての法的地位を有していないが、交換手段として自然人又は法人に受け入	■ MLRs 上、BTC や ETH、LTC などを含む暗号資産（Cryptoasset）とは、「価値又は契約上の権利を暗号化して保護したデジタルな表章であり、分散型台帳技術の一形態を使用し、電子的に転送、保存、又は取引することができるもの」をいう

	たは投資目的のために自然人または法人によって受け入れられ、電子的に送信、保存および取引できる価値のデジタルな表章」と定義されている	れられ、電子的に移転、保存、取引できる価値のデジタルな表章」と定義されている	
暗号資産の取引に係るライセンス	■ 暗号資産の取引に関する特有の金融規制枠組みは存在しない ■ もっとも、暗号資産は、KWG 及び WpIG において「金融商品」に該当することから、暗号資産に関して、投資助言や取引の取次ぎ・媒介、取引プラットフォームサービス等を提供する場合、KWG 又は WpIG に基づくライセンスの取得が必要となる ■ 暗号資産カストディサービスについても、KWG 上「金融サービス」に含まれることから、当該サービスを提供する事業者についても、KWG に基づくライセンスの取得が必要となる ■ 前記「暗号資産規制の有無」記載のとおり、ドイツでは暗号資産の取引に関する特有の金融規制枠組みは存在しない。したがって、KWG 又は WpIG に基づくライセンス業者は、伝統的な金融サービスの提供事業者と同様の行為規制に服する。具体的には、資本金規制、流動性規制、リスク管理規制等の規制に服する	■ PACTE 法により、デジタルアセット提供事業者（Digital Asset Services Provider 以下「DASP」という。）に係る登録・ライセンス制度が整備されている ■ 下記のサービスを提供しようとする者は、金融市場局（Autorité des marchés financiers 以下「AMF」という。）に登録が必要（以下「AMF 登録業者」という） ➢ 第三者のためのデジタルアセットのカストディ ➢ 法定通貨とデジタルアセットの売買 ➢ デジタルアセット同士の交換 ➢ デジタルアセットの取引プラットフォームの運営 ■ AMF 登録業者は、後記の AML 規制を除いて、サービスの提供にあたって特段の規制に服するわけではない。なお、AMF 登録業者は、別途任意にライセンスを取得することができるところ、当該ライセンスを取得した業者は、賠償保険への加入（又は資本金要件の遵守）や安全な IT システムの導入、利益相反に	■ FSMA における既存の金融規制に該当しない限り、暗号資産の取引に関して金融規制上のライセンス取得は必要とされていない ■ 仮に金融規制上のライセンスを取得した場合の主な規制・義務等は以下のとおり ➢ 禁止命令により職務遂行が禁止されている者を職務遂行させないようにするための合理的な注意 ➢ 規制業務の遂行に関して管理職務を果たさないように確保することへ向けた合理的注意 ➢ 十分な資産の保持 ■ なお、FSMA の規制対象は以下のとおり ➢ 投資物件の取引（Dealing in investments） ➢ 投資物件の取引の取りまとめ（Arranging deals in investments） ➢ 預金の取扱い（Deposit taking） ➢ 資産の保管及び管理（Safekeeping and administration of assets） ➢ 投資物件の管理（Managing investments） ➢ 投資助言（Investment advice） ➢ 集団投資スキームの設立（Establishing collective investment schemes） ➢ 投資指図におけるコンピューター・ベース・システムの使用（Using computer-based systems for giving investment

		関するポリシーの作成など、一定の義務を負う	instructions） ➢ 返還請求基金の業務
AML/CFT	■ KWG に基づくライセンス保持者は、GwG に基づく規制の対象となるため、暗号資産関連のサービスについても GwG の規制に服する ■ GwG に基づき、以下のような義務が課せられる ➢ リスク分析及び内部セキュリティ対策を備えたリスク管理システムの確立 ➢ 適切な AML 担当者の任命 ➢ 顧客への KYC ➢ AML やテロ資金調達への関連を示す状況がある場合の、中央金融取引調査ユニット（The Central Financial Transaction Investigation Unit）への疑わしい取引の報告	■ AMF 登録業者は、以下の AML 規制に服する ➢ リスク評価 ➢ 顧客およびその受益者の身元確認と検証 ➢ 取引開始時および取引関係全体におけるデューディリジェンス措置 ➢ 情報処理・不正資金移転防止活動ユニット（Traitement du renseignement et action contre les circuits financiers clandestins（TRACFIN））への疑わしい取引報告書の提出義務 ➢ 内部監査と AMF への報告 ➢ 資産凍結措置の実施	■ 暗号資産交換業者（Cryptoasset exchange providers）及びカストディウォレット業者（Custodian wallet providers）は、AML/CFT に関する MLRs に基づき、金融行動監視機構（Financial Conduct Authority）への登録その他 AML/CFT 上の措置を講じることが義務付けられている ■ 暗号資産交換業者及びカストディウォレット業者は、MLRs に基づき、第 5 次マネー・ローンダリング防止指令（The fifth Anti-Money Laundering Directive（MLD5））の対象となり、例えば、以下の措置を講ずる必要がある ➢ AML リスク評価の実施 ➢ AML に関連する組織要件（システム管理、記録保持） ➢ 顧客デューディリジェンス（顧客の身元の特定など） ➢ 継続的な監視義務

１－６－２. NFT の法的位置づけ整理

この項では、日本における NFT の法的位置づけ及び関連する法規制の諸論点を整理した。ポイントは以下の通りである。

- NFT 自体は無体物であり所有権の対象ではなく、NFT 自体への著作権も発生しない
- NFT が表章するコンテンツについてはその特徴に応じて所有権・著作権が生じる可能性があり、NFT 譲渡に伴いそうした権利が移転するかは利用規約等で別に定める必要がある
- NFT は一般的に資金決済法上のいわゆる１号及び２号暗号資産には該当しないが、分割 NFT 等の事例をはじめ、その特徴によっては決済手段性が観念されることにより暗号資産に該当する可能性が生じうる
- NFT が表章する権利が金商法上の集団投資スキーム持分の要件を充足する場合は有価証券該当性の可能性が生じるところ、オンラインカジノ NFT 等に対して海外でも金融規制の観点から指摘した事例がある。AMT/CFT やインサイダー取引規制等は暗号資産・有価証券に該当しない限りにおいて特段の定めはない状態である
- NFT の販売等が刑法上の賭博罪に該当するかについては同罪の構成要件である「得喪を争う」要件が満たされるかが重要である

詳細は以下の図表に整理した。

図表 26　NFT の法的位置づけ及び諸論点

項目	整理	
類型（表章する資産・権利）	主な NFT の累計	■ ゲーム内キャラクターやアイテム等の利用等に係る権利
	ゲーム	■ デジタル上のトレーディングカード等の閲覧・視聴等に係る権利
	コレクションアイテム	■ デジタル上のアート作品等の閲覧・視聴等に係る権利
	アート	■ 仮想空間内の土地やオブジェクト（建物）等の利用等に係る権利
	メタバース（仮想空間）	■ ゲーム内キャラクターやアイテム等の利用等に係る権利
NFT が表章する知的財産権等に係る権利保護	**NFT 自体の権利保護**	
	■ 民法上、所有権の対象は「有体物」（民法 85 条）に限られ、無体物である NFT 自体は所有権の対象にならない ■ 著作権法上の「著作物」（著作権法 2 条 1 項）とは、「思想又は感情を創作的に表現したものであつて、文芸、学術、美術又は音楽の範囲に属するもの」をいうところ、NFT は単なるデータであって創作的表現ではなく、NFT 自体に著作権は発生しない	
	NFT が表章するコンテンツの権利保護	
	■ NFT が表章するコンテンは無体物であれば所有権の対象とはならない ■ NFT が表章するコンテンツは「著作物」に該当する場合、著作権法上保護の対象となる。例えば、デジタル上のアート作品に係る権利を表章した NFT では、通	

<table>
<tr><td></td><td colspan="2">常、当該アート作品は「著作物」に該当するため、当該アート作品に著作権が発生する</td></tr>
<tr><td>NFT 譲渡に伴う権利（ライセンス）移転</td><td colspan="2">■ NFT を譲渡した場合に、当該 NFT が表章するコンテンツの著作権等が当然に付随して譲渡されるものではない
■ 利用規約等において NFT が表章するコンテンツの法的性質（コンテンツ著作者から著作権の譲渡を受けるものか、著作権の利用許諾を受けるにとどまるのか等）を定めるとともに、NFT 譲渡に伴い当該コンテンツに係る著作権等も譲受人に移転するか等を定めておく必要がある</td></tr>
<tr><td rowspan="3">暗号資産/有価証券該当性</td><td colspan="2">暗号資産該当性[41]</td></tr>
<tr><td>暗号資産の要件</td><td>基本的な考え方</td></tr>
<tr><td>1 号暗号資産
■ 役務提供等の代価の弁済として不特定の者に対して使用でき、かつ、不特定の者との間で購入・売却をすることができること（要件①）
■ 電子的に記録された財産的価値であって、電子情報処理組織を用いて移転することができること（要件②）
■ 本邦通貨及び外国通貨、通貨建資産等に該当しないこと（要件③）

2 号暗号資産
■ 不特定の者との間で、1 号暗号資産と相互に交換できるものであって、要件②及び要件③を満たすもの</td><td>1 号暗号資産該当性について
■ NFT それ自体に決済手段性がない場合は、①の要件満たさないため、1 号暗号資産に該当しないと考えられる
2 号暗号資産該当性について
■ NFT それ自体に個性があり、1 号暗号資産と同等の経済的機能を有しない場合、2 号暗号資産に該当しないと考えられる [42]
■ 代替性がある場合であっても、トレーディングカードなどのように 1 号暗号資産と同等の経済的機能を有しない場合は 2 号暗号資産に該当しないとされている [43]

■ 参考事例
デジタルアート作品に係る権利を表章する NFT を複数のトークンに分割し、共同保有するプロジェクトの場合 [44]、分割され小口化されたトークンの数量・単価等に鑑み、当該分割されたトークンについて決済手段性があるものとして暗号資産に該当しないかが問題となりうる</td></tr>
<tr><td colspan="2">有価証券該当性</td></tr>
</table>

[41] NFT が暗号資産に該当する場合に、その売買や他の暗号資産との交換を行うことは暗号資産交換業に該当し、暗号資産交換業登録が必要となる（資金決済法 63 条の 2、同法 2 条 7 項）

[42] 金融庁「事務ガイドライン（第三分冊：金融会社関係）16 暗号資産交換業関係」I-1-1②によれば、2 号暗号資産該当性に関して、「不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる」ことを判断するに当たり、「1 号暗号資産を用いて購入又は売却できる商品・権利等にとどまらず、当該暗号資産と同等の経済的機能を有するか」等を考慮することとされている

[43] 令和元年 9 月 3 日付パブリックコメント No4

[44] コレクティブルアイテム等を表章する NFT を複数のトークンに小口化して複数人で保有するプロジェクトとして、fractional.art などがある

<table>
<tr><td></td><td>有価証券の要件[45]</td><td>基本的な考え方</td></tr>
<tr><td></td><td>電子記録移転権利
（いわゆるセキュリティトークン）
■ 電子記録移転権利とは、集団投資スキーム持分等の金商法 2 条 2 項の規定により有価証券とみなされる権利をブロックチェーン上のトークンに表章するものをいう（金商法 2 条 3 項）

集団投資スキーム持分
■ 他者から金銭等（暗号資産を含む）の出資又は拠出を受け、当該金銭等を充てて事業（「出資対象事業」）が行われ、当該出資対象事業から生じる収益の配当等が出資者・拠出者に対してなされるもの</td><td>■ 問題となっている NFT が表章する権利が集団投資スキーム持分の要件を充足する場合、当該 NFT は金商法 2 条 2 項の規定により有価証券とみなされる権利をブロックチェーン上のトークンに表章するものとして電子記録移転権利に該当する可能性があると考えられる

■ 参考事例
オンラインカジノを運営する NFT 発行体が、当該オンラインカジノの収益分配を受けられる権利を表章した NFT を販売する場合[46]、当該 NFT を購入するために金銭等を拠出する必要があり、NFT 発行体は当該金銭等を充ててオンラインカジノを運営し、NFT 保有者は当該オンラインカジノの収益が分配される関係にあるときは、当該 NFT が表章する権利は集団投資スキーム持分の要件を充足しうる。その場合、集団投資スキーム持分に係る権利を NFT としてトークンに表章させる場合は電子記録移転権利に該当する可能性がある</td></tr>
<tr><td>AML・CFT/
インサイダー取引規制の該当性</td><td colspan="2">■ AML・CFT
NFT が暗号資産や電子記録移転権利に該当する場合を除き、NFT の発行者や NFT 売買のプラットフォーム運営者は犯収法上の「特定事業者」（犯収法 2 条 2 項各号）には該当せず、購入者等に対して本人確認をする義務等を負わない（同法 4 条）[47]
■ インサイダー取引規制
NFT が金商法上の「特定有価証券等」（金商法 163 条）に該当しない場合には、インサイダー取引規制の対象にならない</td></tr>
<tr><td rowspan="2">景表法/
賭博罪該当性</td><td colspan="2">景品類（景表法 2 条 3 項）該当性</td></tr>
<tr><td>景品類の要件・効果</td><td>基本的な考え方</td></tr>
</table>

[45] NFT が電子記録移転権利に該当する場合、NFT の自己募集行為は、原則として第二種金融商品取引業に該当し、第二種金融商品取引業登録が必要となる（金商法 29 条、同法 28 条 2 項 1 号、同法 2 条 8 項 7 号へ）。また、勧誘対象が 50 名以上の場合は金商法上の有価証券届出書の提出等が必要になる（金商法 2 条 3 項柱書、同法 5 条）

[46] サンドベガスカジノクラブ（Sand Vegas Casino Club）は、メタバース上のオンラインカジノの開発資金を調達する目的で、当該オンラインカジノから得られる収益の分配を受ける権利を表章した NFT を販売したところ、2022 年 4 月 13 日、米国 Texas States Securities Board 及び Alabama Securities Commission より、排除措置命令の提出を受けた旨報告されている

[47] なお、一般社団法人日本暗号資産ビジネス協会 NFT 部会「NFT ビジネスに関するガイドライン 第 2 版」（以下「NFT ガイドライン」という。）6. 匿名性とプライバシーでは、「デジタルアートやゲームアイテムを始めとする一部の NFT は高額で取引されており、AML 等の観点から取り扱いにおける匿名性については注意が必要…」等とされている

<table>
<tr>
<td></td>
<td>■ 「景品類」の要件
顧客を誘引するための手段として、一定の取引を条件とするなど取引に付随して、経済上の利益等を提供すること
■ 「景品類」の提供と限度額規制
<table><tr><th></th><th>提供方法</th><th colspan="3">景品類限度額</th></tr><tr><th></th><th></th><th colspan="2">最高額</th><th>総額</th></tr><tr><td>一般懸賞</td><td>商品・サービスの利用者に対し、くじ等の偶然性、特定行為の優劣等によって景品類を提供すること（「懸賞」）</td><td>取引価額が5,000円未満</td><td>取引価額の20倍</td><td rowspan="2">売上予定総額の2%</td></tr><tr><td></td><td></td><td>取引価額が5,000円以上</td><td>10万円</td></tr><tr><td>総付景品</td><td>懸賞によらず、商品・サービスを利用したり、来店したりした人にもれなく景品類を提供すること</td><td>取引価額が1,000円未満</td><td>200円</td><td rowspan="2">－</td></tr><tr><td></td><td></td><td>取引価額が1,000円以上</td><td>取引価額の10分の2</td></tr></table></td>
<td>■ マーケティングとしてNFTを無料で配布する場合、②取引付随性が認められ、「景品類」の提供に該当しないか、個別具体的な検討が必要と考えられる</td>
</tr>
<tr>
<td></td>
<td colspan="2">賭博罪（刑法185条）該当性</td>
</tr>
<tr>
<td></td>
<td>賭博の要件</td>
<td>基本的な考え方</td>
</tr>
<tr>
<td></td>
<td>■ 偶然の勝敗により
■ 財産上の利益の
■ 得喪を争うこと</td>
<td>■ 「得喪を争う」とは、勝者が財物を得て、敗者がこれを失うことを意味し、当事者の一方がこれを失うことがない場合は、「得喪を争う」ものには該当しないとされている
■ いわゆる「ガチャ」等によるNFTの販売であっても、購入者において、その販売価格に応じたNFTを獲得していると評価できる事情があれば、購入者がNFT販売者との間で財産上の利益の得喪を争うものではなく、賭博罪に該当しないと整理しうる[48]</td>
</tr>
</table>

[48] 前掲NFTガイドライン4－2－2参照

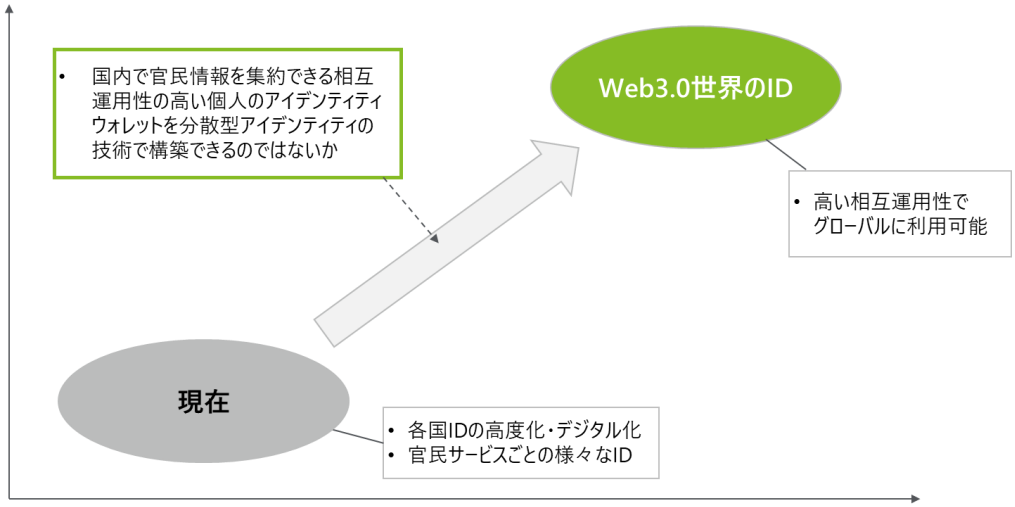
2. 分散型アイデンティティ

2－1. 調査の狙い・アプローチ

Web3.0 の将来像の一つの可能性として、高い相互運用性により国内・海外・デジタル空間の様々な場面で使用できる新たな ID サービスの実現が考えられる。

各国のデジタル ID サービス高度化や、ID 認証によって受けられる民間サービスの拡大・様々な ID サービスの台頭が起きている現在を踏まえると、将来的には自身が ID 管理を行い行政や民間事業者に対して自身の意思で属性情報を提示できる ID サービスの必要性が高まる可能性がある。またその実現に分散型アイデンティティ（DID）が活用されることが期待される。

図表 27　Web3.0 世界の ID への発展イメージ （仮説）

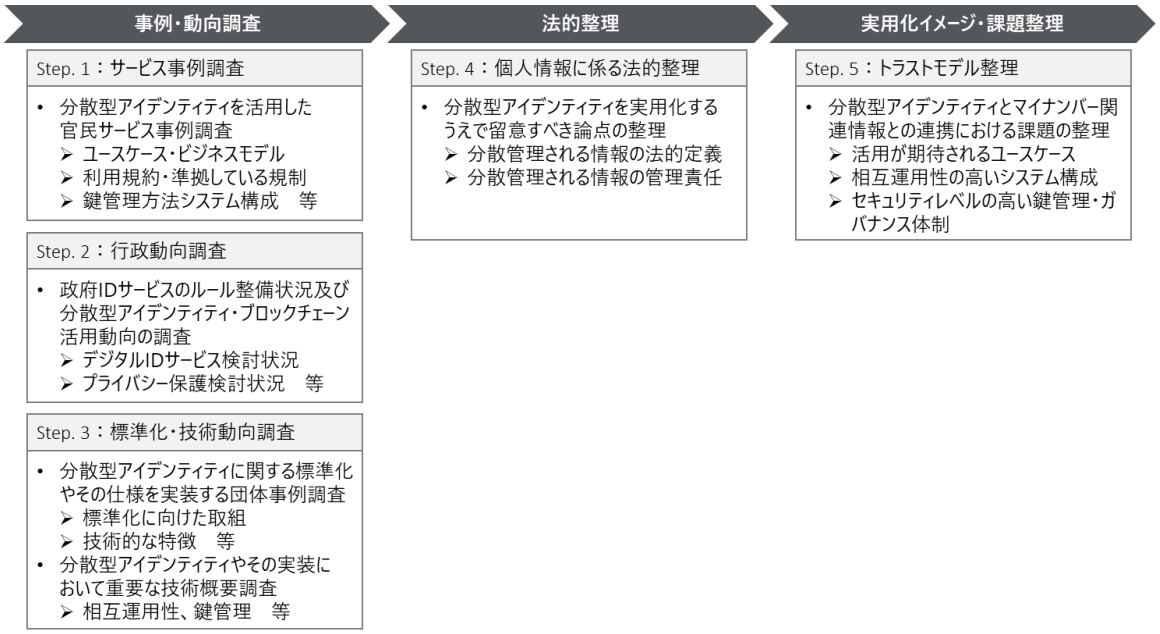


本調査では、Web3.0 世界の ID を実現し得る技術としての分散型アイデンティティに着目し、その実用性を検討するために、以下のステップで調査を実施した。

- DID の実用化事例・動向をサービス、行政、標準化・技術の 3 つの観点から調査する
- 日本において DID 活用時に留意すべき個人情報に係る法的論点を検討する
- 日本において「本人を介した官民情報の活用」に適用し得る、DID とマイナンバー関連情報を連携したデジタル ID ウォレットの実現性と課題を検討する

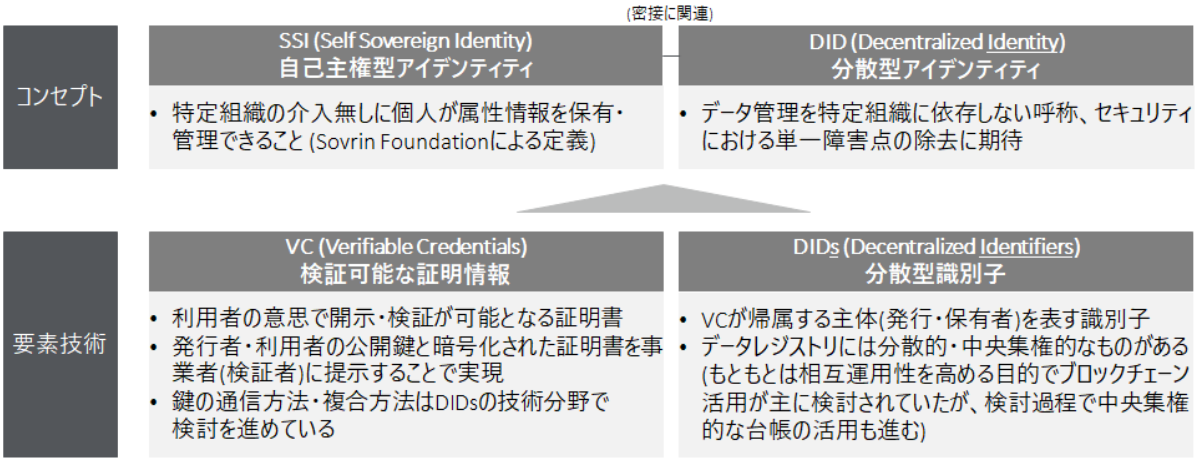
以下の図表は、上記の調査アプローチの具体的な項目の関係性を図示したものである。

図表 28　調査アプローチ



なお、本報告書では、分散型アイデンティティ（DID）は「選択的情報開示を特定事業者に依存せずに実現すること」であるものとする。DID では、VC（Verifiable Credentials）、DIDs（Decentralized Identifiers）の活用が検討されており、いずれも共に W3C（World Wide Web Consortium）によって標準化されている技術として、後に見るように既に民間事業者によるサービス実装や行政サービスでの活用検討が進んでいる。

図表 29　分散型アイデンティティ（DID）の概要



2－2. 調査まとめ

調査・分析を踏まえて以下のように取りまとめを行った。

図表 30　調査結果まとめ表

見出し		調査サマリ
2－3. サービス事例		■ 多くのユースケースで VC が個人の意思による選択的な情報開示に活用される一方、DIDs ではブロックチェーン活用を見据えた標準化とは裏腹に、ブロックチェーン上に個人情報を記録する事の懸念から、ブロックチェーン活用に濃淡が見られた ①ブロックチェーンに記録する情報を限定して詳細情報を別の方法で連携する (例:イギリス NHS、IBM) ②プライベートチェーン活用やノードの制限により公開者を限定する (例:アメリカ ニューヨーク州、カナダ Interac[49]、IBM) ③ブロックチェーンを利用しない (例: Microsoft) ■ 利用者の秘密鍵は特定組織による中央集権的な管理が主であった
2－4. 行政動向		■ 各国デジタル ID サービスに係るフレームワーク・法整備を推進、EU ではデジタルアイデンティティウォレットの実証実験を推進中、イギリス・カナダではデジタル ID サービスの要件をハイレベルに規定 ■ 要件として VC(Verifiable Credentials)の活用は想定しているが、DIDs(Decentralized Identifiers)・ブロックチェーンを活用した実装は現時点では事業者の判断に委ねられている
2－5. 標準化・技術動向	2－5－1. 標準化技術概要	■ DIDs(Decentralized Identifiers)、VC(Verifiable Credentials)等、分散型アイデンティティを構成する重要な要素は W3C が標準化を推進しており、上記事項の実装や相互運用性の確保について、「DIF」「Hyperledger Foundation」「ERC-725 Allianace」等の主要開発コミュニティで実装を進めている
	2－5－2. 課題・課題解決に向けた取り組み	■ DID メソッド[50]が乱立しており、各メソッドの安全性評価・相互運用性の確保が課題となっている。あるブロックチェーンで発行したデジタル署名を異なるブロックチェーンで解読して読み取ることに対応するために各ブロックチェーンにおける DID メソッドのライブラリ化を進めている(DIF の「Universal Resolver」等) ■ 個人の秘密鍵の管理方法や紛失時の修復方法に課題があり、鍵管理方法のシステム実装化を各種開発コミュニティで検討中、証明書・鍵暗号化に係る暗号技術の標準化も今後普及させていくにあたって課題である

[49] 銀行間ネットワークとしてデビットカードや資金決済システムを提供する企業

[50] DID メソッドは、特定のブロックチェーンにおいて DID の生成・更新・削除方法を定義したもの。詳細は W3C の「Decentralized Identifiers (DIDs) v1.0」参照。
W3C が発行しているノート「DID Specification Registries」では、2022 年 11 月 29 日現在で、136 種類の DID メソッドが登録されており、このメソッドを運用する台帳はパブリックチェーン/プライベートチェーン/非ブロックチェーンのネットワーク等各メソッドによって異なっている。中には個人情報管理を念頭に置いていないメソッドも見られる

2－6．個人情報法的整理[51]	**2－6－1．情報の性質・事業者に課すべき責任**	■ 生存する個人に関する情報(証明書情報・分散型識別子・秘密鍵・公開鍵)であって個人識別性がある場合は個人情報に該当する可能性がある ■ 上記情報を発行・保管・参照する事業者(証明書発行者/検証者・秘密鍵管理者・公開鍵/識別子ストレージ管理者)の業態が個人情報を体系的に構成されたデータベース等を事業目的に用いていると解される場合、個人情報取扱事業者にあたると考えられる
	2－6－2．個人の意思で情報提供を行う場合の留意点	■ 取り扱う情報が要配慮個人情報(機微情報)である場合、取得する際に本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示す必要がある ■ 個人が未成年または意思能力に疑義がある場合は情報取得の際に法定代理人に確認する必要がある可能性がある
2－7．トラストモデル	**2－7－1．実現案**	■ 日本国内で官民情報を集約できる相互運用性の高い個人のアイデンティティウォレットを DID の技術で構築できるのではないか ➢ 個人がスマホに様々な組織が発行する証明書を VC として格納し、必要な時にのみ意思に応じて開示できる ➢ ユーザ・VC 発行者の公開鍵を暗号化した情報が分散型識別子(DIDs)と共に台帳に記録される ➢ 標準規格を用いる事で官民情報を集約、将来的には海外政府・事業者も巻き込んだサービスを展開する
	2－7－2．実現案に向けた課題・論点	■ 調査結果、デジタル ID ウォレット構築において①マイナンバー関連情報の範囲、②識別子・公開鍵の連携方法、③秘密鍵の管理方法が主な課題として挙げられる

[51] 再委託先であるアンダーソン・毛利・友常法律事務所外国法共同事業の調べによる

2－3. サービス事例調査

VC/DIDs を活用している、あるいは、今後の活用が見込まれる事例として以下サービスの事例調査を行った。

図表 31　VC/DIDs を活用した（検討中の）サービス事例

No.	サービス名	概要
1	NHS Staff Passport	■ デジタル ID をもつことで、スタッフが国民保健サービス（NHS）の組織の間でより簡単に移動を実現 ■ Sovrin Network が提供する分散型台帳を活用
2	Microsoft Entra Verified ID	■ 様々なサービスに利用できる単一の分散型のデジタル ID を提供 ■ Web ベースの分散型識別子（DID：Web）とビットコインベースの分散型台帳を活用した分散型識別子（DID：Ion）をサービスとして用意
3	Interac Verification Service（旧 Verified.me）	■ 銀行アプリ上で他サービス利用に係る認証を実施、銀行が中央集権的にデータを管理し個人の意思を反映して情報提供を実施 ■ 現時点では VC/DIDs を活用していないが、より相互運用性を高めるために今後実装予定
4	IBM Digital Credentials	■ VC/DIDs を活用して Learinig Credential Network（学歴・専門的資格を証明するブロックチェーンに基づくプラットフォーム）や、Digital Vaccine Cards（新型コロナウイルスに関するワクチン接種済みや陰性証明のパスポート発行）のサービス提供
5	CARO / Digital Product Passports	■ Spherity 社が提供している法人向けの DIDs サービス ■ 機密性の高い会社製品情報について DIDs を活用して情報共有することでサプライチェーントレーサビリティを実現

（1） NHS Staff passport

NHS Staff Passport は、VC/DIDs を活用して医療従事者の資格証明・職歴証明を実現、個人の公開鍵・分散型識別子は台帳に書き込まず直接検証者と通信して共有している。

分散型台帳としてパーミッションド型パブリックチェーン（台帳への記載は許可性だが、誰でも情報を閲覧可能なブロックチェーン）を採用、利用者の個人情報（公開鍵・証明書）はブロックチェーンに記帳せずに Peer to Peer 通信を行うことで個人情報の保護を実現している。

1）導入背景・利用目的

NHS（国民健康保健サービス）が以下背景から 2020 年 3 月にサービスを提供開始し、医療従事者の情報（資格・身分・職歴等）を証明書情報として記録し移転先の医療機関に簡易に提供することを実現した。

- 英国では、各地域が主体で医療サービス提供しており、医療スタッフが地域を移動するごとに身分証明と医療証明を行う必要があり認証プロセスに最大 7 日を要していた
- 新型コロナウイルスの流行により、医療スタッフの地域移動が活発となり、認証プロセスの短縮化が必要だった

2）標準化・相互運用性を高める取り組み

VC/DIDs について W3C が定める基準に準拠した形でサービス設計を行っている。

3）利用・遵守する法令等

医療機関と医療従事者の間に情報利活用の契約を締結している。

4）システム構成

下記事業者がサービス提供に関わっている。

- 分散型台帳として Hyperledger Indy ベースで構築された Sovrin Network[52]を活用、ウォレットは Evernym[53]が構築
- ID 認証基盤・証明書発行・検証管理は Microsoft 及びそのパートナー企業が構築

5）ノード管理

Sovrin Foundation が管理するパーミッションド型パブリックチェーンを採用している。利用者の個人情報（公開鍵・証明書）は分散台帳に記帳せずに Peer to Peer 通信を行うことで個人情報の保護を実現している。

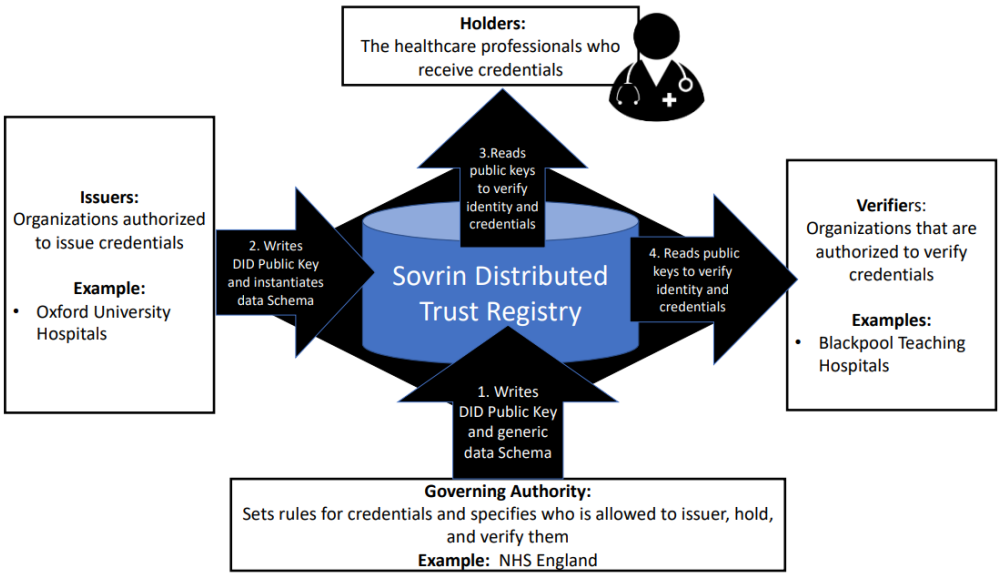
6）鍵管理

ウォレット事業者である Evernym が秘密鍵管理を行っている。

[52] Sovrin Foundation が Hyperledger Indy を活用してノード運営を実施している https://sovrin.org/overview/

[53] ウォレットアプリの開発や VC ソリューションを提供している事業者　https://www.evernym.com/

図表 32　NHS Staff Passport における分散型台帳の活用イメージ[54]



（2） Microsoft Entra Verified ID

Microsoft は、大学や政府機関向けに VC と DIDs のマネージドサービスを提供している。分散型識別子の利用はブロックチェーン・ベース（例：ION[55]）でも非ブロックチェーン・ベース（例：DID：Web[56]）でも可能となっている。ION のインフラは、Microsoft だけでなく、DIF[57]などの開発コミュニティでノード管理やプロトコル修正を行うことも可能となっている。また、鍵の管理は、自社クラウドサービスである Microsoft Azure だけでなく、他のクラウドでも実施可能である。

1）導入背景・利用目的

先行的に以下のサービス導入・実証実験等を行ったうえで「Microsoft Entra Verified ID」として 2022 年 8 月に商用化を行った。

- 職歴証明書（イギリスの NHS Staff Passport）
- 大学の卒業証明・成績証明（慶應義塾大学等）[58]
- 市民 ID サービス（ベルギーフランダース地域）

---

[54] アーカンソー州立大学「Implementing Self-Sovereign Identity （SSI） for a digital staff passport at UK NHS」 https://cpb-us-e1.wpmucdn.com/wordpressua.uark.edu/dist/5/444/files/2018/01/BCoE2022SS1FINAL.pdf

[55] Identity Overlay Network の略　Microsoft と DIF が開発したビットコイン上で実行される、分散型で許可なしのスケーラブルな分散化識別子レイヤ 2 ネットワーク　https://identity.foundation/ion/

[56] 集中型の台帳、DIDs ドキュメントは発行者 Web サーバでホストされる　https://w3c-ccg.github.io/did-method-web/

[57] Decentralized Identity Foundation の略、分散型アイデンティティに関する標準化・開発等を実施 https://identity.foundation/

[58] https://www.keio.ac.jp/ja/press-releases/files/2020/10/26/201026-1.pdf

2）標準化・相互運用性を高める取り組み

VC/DIDs について W3C に準拠している。また、学位証明において他ベンダとデータフォーマットの統一化を進めている。

3）利用規約・遵守する法令等

事業者の提供するサービスに準ずる。

4）システム構成

Microsoft ですべて構築可能となっている。他プラットフォームで発行された VC や DIDs については、「Microsoft Resolver」を活用することで読み取りを実行することが可能となっており。他プラットフォームとの相互運用性を確保している。

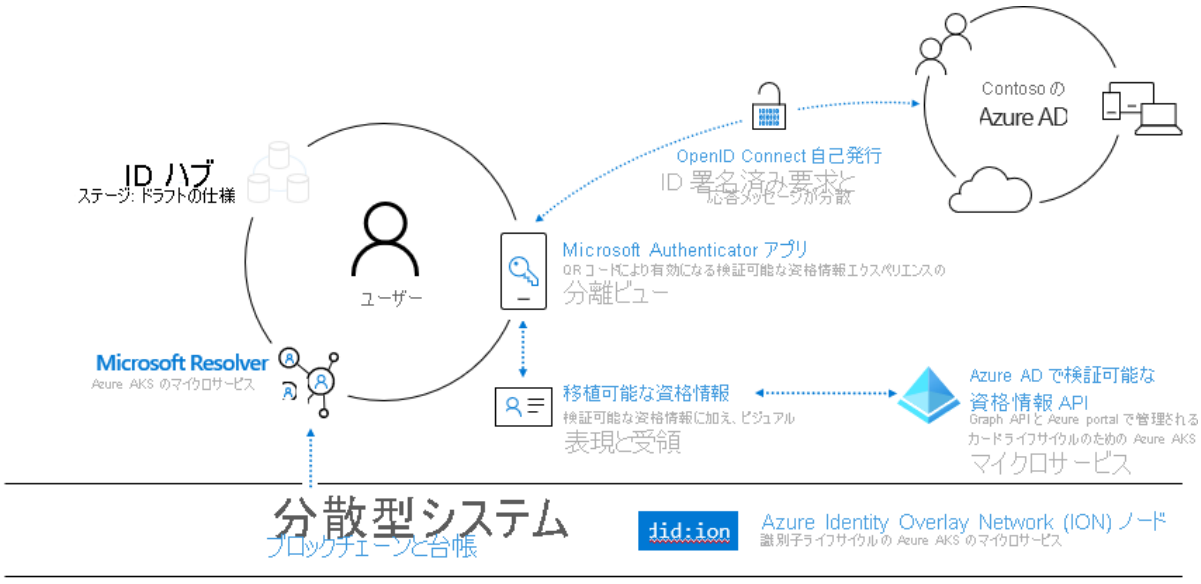
5）ノード管理

DIDs の通信方法として①ION と②WEB 通信を採用している。ION を活用する場合、DIF 等の開発コミュニティでノード管理・プロトコル修正等が可能である。

6）鍵管理

Microsoft Authenticator アプリを通じて、Microsoft Azure Key Vault（鍵などを安全に保管しアクセスできるようにするクラウドサービス）に格納される。ただし、他サービスで管理することも可能となっている。

図表 33　Microsoft Verifed ID の利用イメージ[59]



[59] Microsoft ホームページ「Microsoft Entra Verified ID の概要」
https://learn.microsoft.com/ja-jp/azure/active-directory/verifiable-credentials/decentralized-identifier-overview

（3） Interac Verification Service （旧 Verified.Me）[60]

VC/DIDs を活用していないが、個人の意思で情報提供範囲を制御している事例となっている。（相互運用性と機能を向上させるため、2023 年に VC/DIDs 導入が検討されている。）

銀行、電気通信事業者、信用情報機関が一元管理している個人情報を、本人の同意を得てサービス提供者（事業者、政府等）に提供している。

1）導入背景・利用目的

カナダの主要銀行がアンカーを務める ID と資格情報の共有ネットワークで、フェデレーションログインと検証済みデータの共有を提供している。利用可能な属性には、アイデンティティ（氏名、生年月日等）、銀行 （口座の詳細） 、通信（電話番号、SIM 情報）、信用情報機関の詳細が含まれ、民間事業者の利用手続き（銀行情報を活用して保険サービスの利用開始等）と公共サービスの利用手続き（行政サービスへの登録・受理の合理化等）の双方が可能となっている。現在、データプロバイダー（Identity＆Data Provider）/データコンシューマー（Service Providers）両方の参加者をネットワークへ追加するための継続的な取り組みが実施されている。

2）標準化・相互運用性を高める取り組み

DIACC[61]で策定されたトラストフレームワーク[62]に準拠、このフレームワークは国内・国外のサービスとの連携を念頭において策定されている。Verifiable Credential の機能を DID ネットワーク （DID:Orb[63]） に組み込むための取り組みが進行しており、2023 年中に導入を目指している（W3C に準拠）。

3）利用規約・遵守する法令等

データプロバイダーからデータコンシューマーに連携される情報は個人情報と認識され、規約・カナダ法規制で保護されている[64]。

4）システム構成

現状は、データプロバイダーが利用者の個人情報を管理し、データコンシューマーに連携している。

■ Interac は ID 認証インフラストラクチャと情報通信基盤を構築

---

[60] 2022 年 11 月末に Verified.me から Interac Verification Service に名称変更された
https://www.interac.ca/en/content/news/interac-verification-service-and-interac-document-verification-service-put-privacy-in-the-hands-of-canadians/

[61] Digital ID & Authentication Council of Canada の略、デジタル ID サービスのフレームワークを検討する官民共同の組織

[62] Pan-Canadian Trust Framework （PCTF） https://diacc.ca/trust-framework/

[63] SecureKey 社が開発する DID メソッド https://trustbloc.github.io/did-method-orb/

[64] https://verified.me/legal/

■　データプロバイダーとデータコンシューマー間の情報連携に Hyperledger Fabric を使用
（事業者のネットワーク参加をより容易にするために将来的には AWS に移行予定）

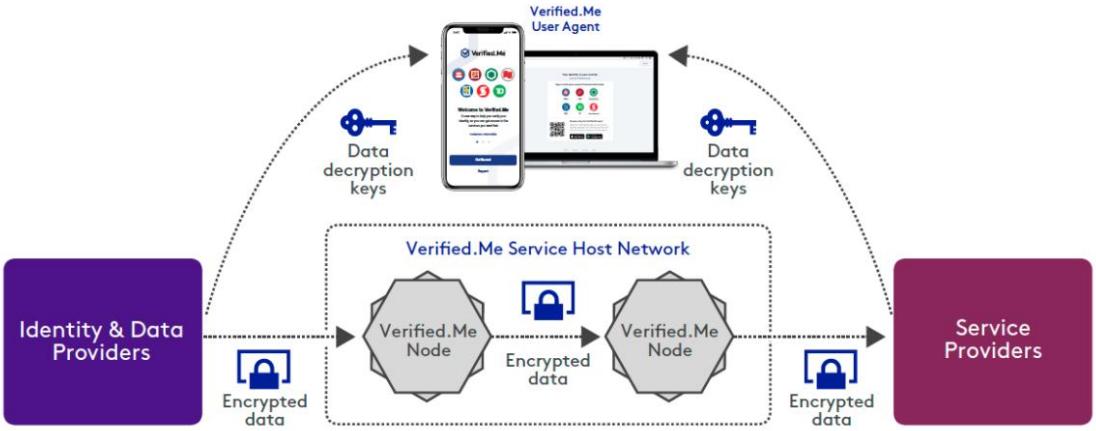
5）ノード管理

Hyperledger Fabric ノードは、データプロバイダーとデータコンシューマー（例:Interac や銀行）がネットワークノード保持・管理を行っている。Hyperledger Fabric のプライベートデータ収集機能を活用し、公開鍵と暗号化された個人情報を別々に通信することでデータの機密性を実現している。

6）鍵管理

利用者の秘密鍵・公開鍵は SecureKey 社が管理、鍵を紛失した場合は、SecureKey とデータプロバイダーのデューディリジェンスを通じて身元確認を行ったうえで復旧を行う。

図表 34　Verified.Me サービスイメージ[65]



（4） IBM Digital Credentials

IBM は公共セクターを中心に VC/DIDs を活用して Learning Credential Network（学歴・専門的資格を証明するブロックチェーンに基づくプラットフォーム）や Digital Vaccine Cards（新型コロナウイルスに関するワクチン接種済みや陰性証明のパスポート発行）のサービスを提供している。ノード・鍵は行政等の要望から中央集権的に管理されている場合が多い。例えば、米国ニューヨーク州のワクチンパスポートは、ノード・鍵管理は行政により中央集権的に行われている。

[65] https://diacc.ca/wp-content/uploads/2020/05/DIACC-Identity-Networks-Paper-Self-Assessment_SecureKey-VerifiedMe.pdf

1）導入背景・利用目的

Hyperledger Indy、Ursa、Aries や Hyperledger Fabric 等のオープンソースを活用した商用サービスを展開、公共サービスを中心にサービスを提供している。

- ワクチン接種済み証明書（Excelsior Pass Plus：米国ニューヨーク州）
- 身分証明書（ドイツ移民局）
- 大学の卒業証明・成績証明（実証実験で複数実施）

以下、米国ニューヨーク州の Excelsior Pass Plus の事例について詳述する。

2）標準化・相互運用性を高める取り組み

VC/DIDs について W3C に準拠、将来的には他地域とのワクチンパスポートとの連携を念頭において設計がされている。

3）利用規約・遵守する法令等

ニューヨーク州のプライバシーポリシーに準拠されており、個人情報のマーケティング利活用・第三者提供は禁止されている[66]。

4）システム構成

ID 認証基盤・証明書発行・検証管理は IBM が構築している。

5）ノード管理

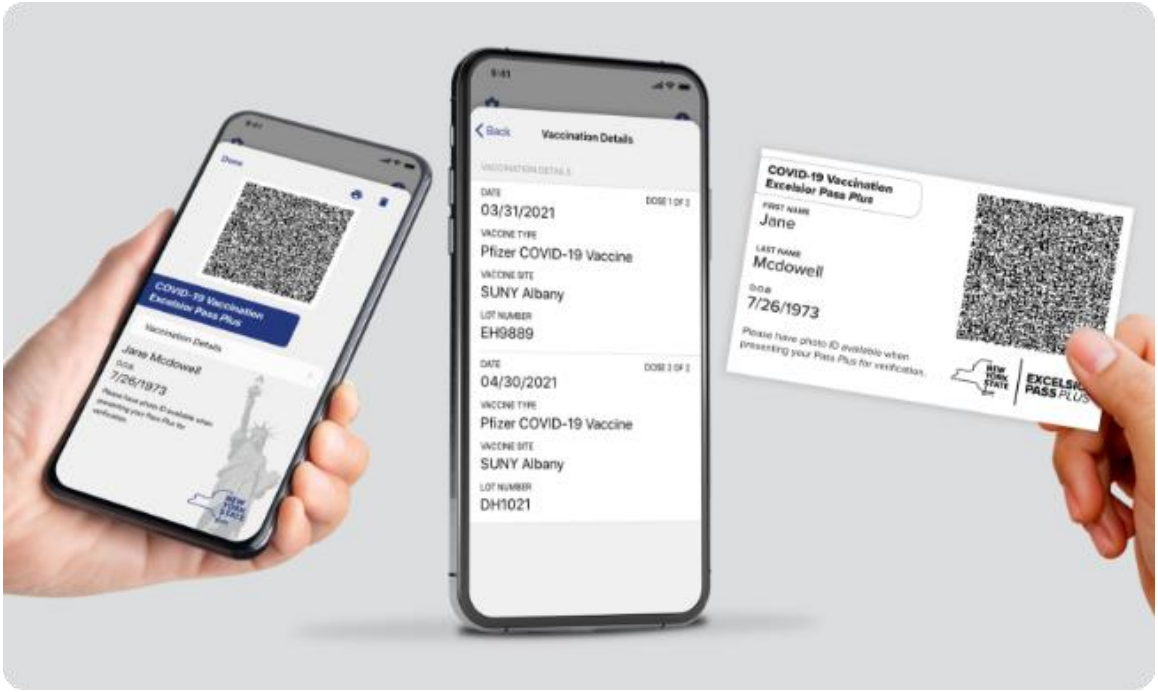
ニューヨーク州政府が鍵発行を行い、中央集権的に管理している。

6）鍵管理

ニューヨーク州政府がすべてのブロックチェーンノードを保持し、中央集権的に管理している。

[66] https://epass.ny.gov/privacy

図表 35　Excelsior Pass Plus イメージ図[67]



（5） CARO / Digital Product Passport　（Spherity 社）

規制当局が求めるサプライチェーン透明化により、自社の機密情報を安全に特定のプレイヤに提供する必要性が生じて分散型アイデンティティに関するサービスの需要が高まっている。法人の場合、個人情報保護の課題が発生しないため、ブロックチェーンの活用が進んでいる。

1）導入背景・利用目的

法人向けの ID 管理・情報共有サービスを提供している。サプライチェーンに係る規制厳格化により機密性の高い情報をサプライチェーン関係者や規制当局と共有するニーズが生じており、こうした需要に応えるため、以下サービスの提供・開発を行っている。

- CARO
  医薬品規制対応[68]のサプライチェーンに対応、ライセンスの交換ステータス資格情報としての証明書と製品情報をやり取りするプラットフォーム、今後リコール対応等サービス等を拡充予定
- Digital Product Passport
  EV バッテリー規制[69]対応のサプライチェーンに対応したプラットフォーム（開発中）

---

[67] https://epass.ny.gov/home

[68] 2023 年 11 月に施行された米国の 「医薬品サプライチェーン安全保障法」（DSCSA） では、医薬品製造プロセス情報の提出が義務付けられている

[69] EU で EV 電池規制では、EV 電池生産過程における CO_2 排出量やリチウム・コバルト等の特定鉱物のリサイクル材利用率、デューディリジェンス情報等の提出が義務付けられる予定である（2024 年以降を予定）

2）標準化・相互運用性を高める取り組み

VC/DIDs について W3C に準拠している。各種規制要件・業界標準に対応したデータフォーマットを用意している。

3）利用規約・遵守する法令等

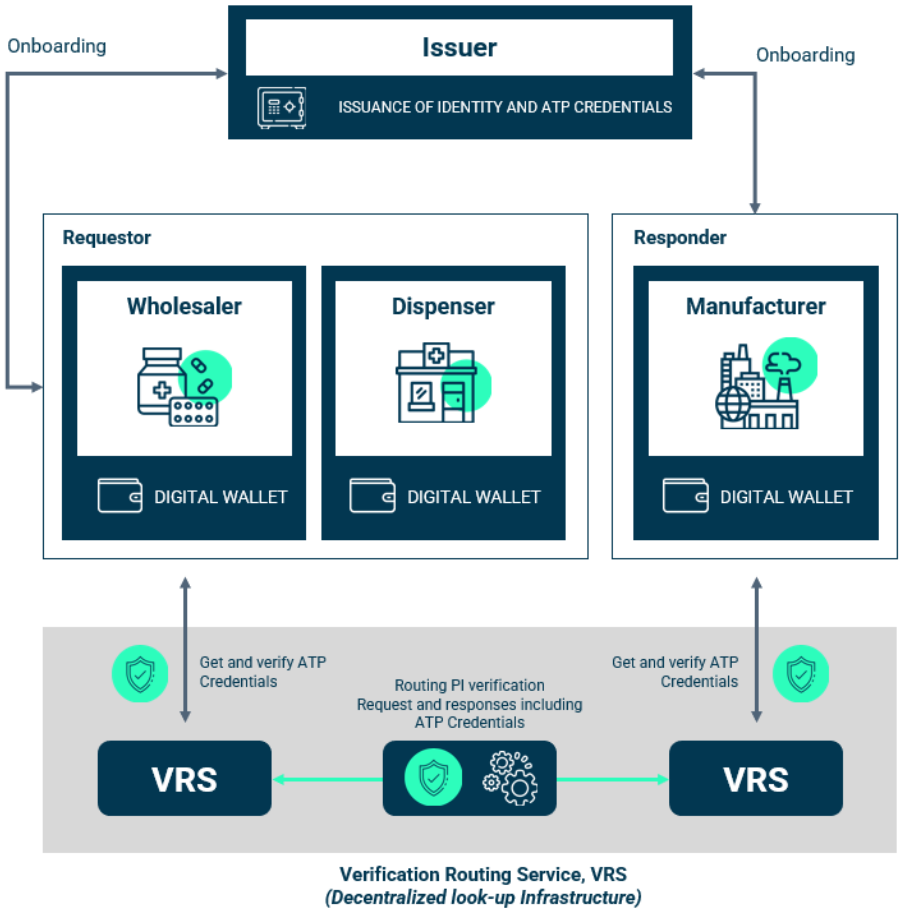
事業者の提供するサービスに準ずる。

4）システム構成

以下のような構成をとっている。

- ネットワーク：分散型台帳としてパブリックチェーン（イーサリアム）を活用
- 鍵管理：AWS Key Management Service （AWS KMS）を活用
- 証明書管理・ウォレット：Veramo wallet SDK[70]を活用

図表 36　CARO サービスイメージ[71]



[70] https://veramo.io/

[71] Spherity 社サービス紹介資料を抜粋

2－4. 行政動向調査

本調査では、ID サービスの検討が盛んな G7 の国を対象に分散型アイデンティティに関する検討状況、取り組みについて調査を行った。以下が調査対象の国と取り組み概要である。

図表 37　調査対象国と取り組み概要

No.	国名	調査対象	概要
1	EU	EU デジタル アイデンティティ ウォレット	■ 個人情報保護の強化や EU 域内のウォレット相互運用性を高めるためにデジタルアイデンティティウォレットを構想 ■ デジタル ID とウォレットのユースケースの実証を実施
2	イギリス	Gov.UK	■ より強硬な個人情報保護・シームレスな認証サービスの実現に向けて、UK digital identity and attributes trust framework（β 版）を策定
3	カナダ	DIACC	■ カナダでデジタル ID フレームワークを確立することを目的として民間や公的機関連合（DIACC）でデジタル ID の適合性基準を定めた Pan-Canadian Trust Framework （PCTF） を策定

（1） EU：EU デジタルアイデンティティウォレット

EU では、2012 年に eIDAS 規制[72]が策定され、2016 年に施行されたが ID サービスの普及率の低さや利便性の低さ等課題があり、2021 年に eIDAS 規制が改正されデジタルアイデンティティウォレットを推進することとなった。EU デジタルアイデンティティウォレットでは、各 EU 加盟国の国民 ID サービスとの連携や、データの国外移転が発生する 7 つのユースケースについて利用検討が進んでいる。ユースケースにおいては、オンライン署名や学位証明等で VC の活用が検討されている。また、2022 年 8 月から 4 つの実証実験を開始している。そのシステム基盤では、ブロックチェーンを活用する検証とされない検証が存在しており、現状どのシステム基盤を商用時に活用するかは未定の状況である。

図表 38　EU デジタルアイデンティティウォレット取り組み概要

項目	概要
実施主体	■ 欧州委員会
発足時期	■ 2021 年 6 月：サービス検討開始時期 ■ 2024 年以降サービス提供予定

[72] 正式名称は REGULATION （EU） No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

導入背景/目的	■ 2012 年に従来の強制力のない電子署名指令に代わる新たな法制度（eIDAS 規制）を策定し、2016 年 7 月から EU 加盟国全域で施行されたが、対象国サービスカバー率の低さ、利便性の低さ等の課題あり ■ 2021 年、これらの課題への対策として、「欧州デジタル ID ウォレット」の開発と提供を EU 加盟国へ義務づけることなどを規定した eIDAS 改正案を発令
ユースケース/活用データ	■ EU 加盟国の各国デジタル ID サービスと相互連携 ■ 国外移転に係る以下ユースケースを検討中 ➢ オンライン認証、電子署名 ➢ 運転免許証 ➢ 卒業証書 ➢ 電子処方箋、電子カルテ ➢ ペイメント
標準化に向けた取り組み	■ 欧州議会・理事会による提案文書を踏まえて法制度化 ■ Toolbox を活用し各ユースケースについて標準化を検討、4 つのワーキンググループを立ち上げ[73]
利用規約/準拠法	■ GDPR、eIDAS2.0 等
技術的な特徴	■ Verifiable Credentials の活用（電子署名・学位証明で活用） ■ European Blockchain Initiative （EBI）が検討している European Self Sovereign Identity Framework （ESSIF）の基盤に基づいてシステムが構築される予定（独自規格）
ガバナンス体制	■ ワーキンググループで詳細検討中

図表 39　EU デジタルアイデンティティウォレットで検討されているユースケース

	オンライン認証、電子署名	モバイル運転免許	卒業証書	電子処方箋	支払い
概要	• オンラインサービスにアクセスするための安全で信頼できるID • 契約書などの文書へのデジタル署名	• 警察の取り締まりやレンタカー予約などの用途ので、運転免許証として利用可能 • 専門能力の証明書などの他の資格情報にリンクすることが可能	• 大学や企業などの第三者との間で、教育証明書やその他のトレーニングおよび専門的な証明書をEU内で交換可能にする取組	• 現在の電子処方箋サービスをEUデジタルアイデンティティウォレットで実装 • 認証された医療機関で利用可能で	• ウォレット所有者と小売業者間の便利な支払い、個人間送金をオンラインのみで完結する取組 • WYSIWYS環境(双方が同じ支払情報を画面等で確認できる環境)での取引の署名を中心に展開
ドメイン所有者	• DG CONNECT	• DG MOVE	• DG EMPL	• DG SANTE, CNECT, eHealth Network	• DG FISMA
関連基準	• eIDAS1（2015/1502を含む） • PKI/X.509 • W3C VC	• ISO/IEC 18013-5 • ISO/IEC 18013-7（ドラフト） • ISO/IEC 23220シリーズ（ドラフト） • ISO 23220-3	• W3C VC • EMPL独自規格 • EBSI 仕様； OIDC, SIOPv2 • Europassデジタル認証情報の仕様	• ePrescription の既存サービスの規格 • EN 17269, • ISO/DIS 27269, eHealth Network Guidelines on PS	• SEPA即時信用振替制度ルールブック

[73] WG1：Provision and exchange of attributes、WG2：Functionality and security of the Wallets　WG3：Reliance on the Wallet / identity matching、WG4：Governance で構成されており、検討メンバは、欧州委員会が管理する （加盟国） eIDAS 専門家グループで構成（政府関係者のみで検討）

図表 40　実証実験概要

組織名	概要	体制	システム
EUDI Wallet Consortium（EWC）[74]	■ 旅行ユースケース向けの要素を構築 ①支払い ②組織のデジタル ID	■ EU 諸国の政府機関や民間企業を含む 65 以上の組織が参画	■ N/A
Nordic-Baltic eID Project （NOBID）Consortium[75]	■ 北欧およびバルト地域全体で国の eID ソリューションを使用できるようにすることを目的として実施 ■ 国内・国境を越えたペイメントを中心に実証	■ ノルウェー、デンマーク、ドイツ、イタリア、ラトビア、アイスランドの 6 か国の政府機関、銀行・属性情報プロバイダー等で構成	■ 銀行決済で活用している既存システムを利用
The PilOTs for EuropeaN digiTal Identity wALlet（POTENTIAL）[76]	■ 幅広い分野で実証予定（SIM カード登録・口座開設・デジタル運転免許所・行政サービスのデジタル化・電子署名・電子処方箋）	■ EU の 19 ヵ国とウクライナの 148 組織が参画	■ N/A
Digital Credentials for Europe（DC4EU）[77]	■ eID、学歴・社会保障資格の在り方を検討	■ EU の 23 ヵ国が参画	■ ブロックチェーンベースのシステムを活用見込

（2） イギリス：Gov.UK

Gov.UK は、強固な個人情報保護や、シームレスな認証サービスの実現に向けて、UK digital identity and attributes trust framework（β 版）の策定を行った。本フレームワークでは、ID 認証サービスの事業者の定義が行われており、ID 認証サービスを提供する場合に遵守すべき事項や必要な認可プロセス等の要件が記載されている。VC についても相互運用性を高めるひとつの技術要素として活用することが推奨されている（ただし必須要件ではない）。また、台帳・ネットワークにおける要件（DIDs・ブロックチェーン活用）は事業者に委ねられている。

図表 41　Gov.UK 取り組み概要

項目	概要
実施主体	■ 英国政府（デジタル・文化・メディア・スポーツ省）
発足時期	■ 2019 年 7 月：デジタルアイデンティティに関するパブコメ収集 ■ 2021 年 2 月：Trust Framework（α 版）の策定 ■ 2022 年 4 月：労働権・賃貸権・犯罪履歴に係る ID 認証サービス提供開始

[74] https://eudiwalletconsortium.org/
[75] https://www.nobidconsortium.com/
[76] https://www.digital-identity-wallet.eu/
[77] https://www.dc4eu.eu/

	■ 2022 年 6 月：Trust Framework（α 版）の改定、Trust Framework（β 版）の策定
導入背景/目的	■ 行政サービスの効率化（低コスト化・時間短縮等） ■ ユーザ体験の向上 ■ 新規認証サービスの実現 ■ セキュリティ向上（データ流失・なりすまし防止）　等
ユースケース/活用データ	■ 行政サービスや民間サービスにおける認証等幅広に想定
標準化に向けた取り組み	■ 他サービスとの運用を見据えて以下技術の活用を推奨 ➢ W3C（Verifiable Credentials Data Model v1.1） ➢ Open ID Connect ➢ データ暗号化に関する技術（NIST・ISO 等）　等
利用規約/準拠法	■ UK digital identity and attributes trust framework（β 版） ※その他英国 GDPR、Data Protection Act 2018、 ICO（Information Commissioner's Office）ガイドラインへの対応が必要
技術的な特徴	■ Verifiable Credentials の活用（W3C） ■ ID 認証技術の活用（Open ID Connect） ■ 生体認証の活用（ISO/IEC 19795-1:2021 準拠を推奨） ■ ゼロ知識証明の活用（技術活用の検討にとどまる） ※現状分散型アイデンティティ（DIDs）技術の活用は必須ではなく、ID サービスプロバイダ・属性サービスプロバイダの実装に委ねられている
ガバナンス体制	■ 暫定的にデジタル・文化・メディア・スポーツ省にガバナンス機能を集約 ■ サービスプロバイダ（ID 認証・属性提示・アグリゲータ等）の参画には UKAS（英国認証機関認定審議会）が認定した団体からの認可が必要[78]

図表 42　Trust Framework（β版）概要[79]

No.	セクション	概要
1	Ministerial foreword	■ （閣僚挨拶）
2	Feedback received and updates	■ 各種協議・コメントを踏まえてα版からの改善点の記載：以下の修正が主となる ■ 事業者役割の詳細化・Scheme owner の概念の追加 ■ Relying party（証明書利用事業者）にフローダウン条項[80]の追加 ■ ID 認証方法に生体認証活用文言追加　等
3	Introduction	■ 本フレームワークの適用範囲の説明、用語解説　等
4	What are digital identities	■ デジタルアイデンティティの概要・想定しているユースケースの説明

[78] 就労権、賃貸権、犯罪歴チェックのためのデジタル ID 認証では、2022 年 12 月現在 5 つの認定団体が存在し、17 事業者が認可を受けている
https://www.gov.uk/government/publications/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks

[79] https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version

[80] Relying party についても ID 認証サービス事業者を通じて本フレームワークを適用すること

5	**What are attributes**	■ デジタルアイデンティティで取り扱う属性情報や想定しているユースケースの説明
6	**What the UK digital identity and attributes trust framework does**	■ 本フレームワークの導入背景、規則概要
7	**What you get from adopting trust-marked digital identities and attributes**	■ デジタルアイデンティティ・属性を活用することでの利点の説明（時間・お金・労力削減、ユーザ体験向上、新規ビジネス創出、データ不正対応・データ保護の強化、各国サービスとの相互運用性確保等）
8	**Benefits for users**	■ 利用する個人ユーザのメリット （物理カード等の携帯が不要、必要最小限のデータ提示による認証が可能　等）
9	**Who runs the trust framework**	■ Trust Framework の管理者に関する記載 （暫定的な取り決めとして、政府はデジタル、文化、メディア、スポーツ省にガバナンス機能を確立）
10	**How organisations participate in the trust framework**	■ デジタルアイデンティティに携わる事業者一覧と参画方法 （サービスプロバイダは UKAS の認可が必要）
11	**Rules for identity service providers**	■ アイデンティティサービスプロバイダ特有に課される規則 ■ 検証結果の信頼性レベルの説明、検証が否認された際の理由説明等
12	**Rules for attribute service providers**	■ 属性サービスプロバイダ特有に課される規則 ■ 属性データ保護、属性データの信頼性レベルの説明等
13	**Rules for all identity and attribute service providers**	■ アイデンティティ・属性サービスプロバイダ特有に課される規則 ■ サービス停止する場合利用者への通知義務、アクセシビリティの確保　等
14	**Rules for orchestration service providers**	■ アグリゲータ特有に課される規則 （現状無し）
15	**Rules for all identity, attribute and orchestration service providers**	■ 全てのサービスプロバイダに課される規則[81]
16	**Table of standards, guidance and legislation**	■ プロバイダーが遵守すべき標準化事項・ガイドライン・法規制の一覧を記載

[81] 相互運用性に関する取り組み（データ保護要件の遵守・要件を満たす DB の保持・公開鍵基盤の活用・分散型台帳技術の活用）、ユーザ権限の確認（委任された権限の確認）、苦情や紛争への対応、スタッフとリソース配置、データ秘匿化に関する標準化対応（暗号化/DSS 標準/ハッシュ化の方法）、品質管理対応（ISO 9001:2015 への対応）、情報管理（ISO/IEC 27001:2017 への対応）、情報セキュリティ対応（ISO/IEC 27001:2017 への対応）、リスク管理（ISO / IEC 27005:2018・ISO 31000 等への対応）、不正管理、インシデント対応、製品・サービスに係るユーザへの通知、プライバシーとデータ保護の要件（ICO/GDPR 対応）、データ記録方法、その他禁止行為について記載されている

（3） カナダ：DIACC

カナダでは 2012 年に民間・公的機関の連合組織 DIACC（Digital ID & Authentication Council of Canada）を設立し、相互運用性やセキュリティを確保した公共と民間サービスのデジタル ID システム要件について検討を進めてきた。2020 年にデジタル ID の適合基準を定めたフレームワーク （PCTF） を策定し、2022 年 10 月にこのフレームワークに準拠した ID サービス事業者を認定するプログラム（Voilà Verified 認証プログラム）を開始した。

本フレームワークはハイレベルな要件を定めたもので、相互運用性を高めるために VC/DIDs 等の標準技術の活用について言及はされているが活用を強制したものではない。また、台帳としてブロックチェーンの活用要否や鍵管理方法等についても実装する事業者に委ねられている。

図表 43　DIACC 取り組み概要

項目	概要
実施主体	■ DIACC（銀行、州政府・連邦政府機関、技術プロバイダーなど）
発足時期	■ 2012 年 3 月：DIACC 設立 ■ 2020 年 9 月：Pan-Canadian Trust FrameworkTM （PCTF）導入のため、version1.0 を公開 ■ 2022 年 10 月：Voilà Verified 認証プログラム開始
導入背景/目的	■ 2010~2012 年に財務大臣が任命した決済システム見直しタスクフォースの勧告に基づき、デジタル ID と認証の利用について検討する作業部会が作られ、オンライン取引の構造のビジョンを開発 ■ DIACC は、タスクフォースの終了後も作業部会の活動を継続するために創設
ユースケース/活用データ	■ ヘルスケア ■ 政府サービス ■ 電子商取引 ■ 市民活動（選挙等） ■ 金融サービス
標準化に向けた取り組み	■ PCTF は以下の原則を反映している ➢ オープン標準に基づくプロトコルの利用 ➢ 政策面と技術面での国際的な相互運用性の維持
利用規約/準拠法	■ PCTF（公共と民間サービスのデジタル ID システム要件のベースラインを確立し、相互運用性を推進する枠組み） ■ Voilà Verified（デジタル ID サービスが PCTF に準拠しているかどうかを判断する認証プログラム）
技術的な特徴	■ PTCF は technology-agnostic なフレームワークであり、特定の技術の推進をしていない ■ 相互運用性を促進するためにオープン標準を使用することを指針としており、W3C の DIDs や Verified Credentials に関する標準を例に挙げている
ガバナンス体制	【DIACC の運営体制】 ■ DIACC メンバで構成される委員会は、DIACC のデジタル・アイデンティティ・エコシステムの原則と戦略目標に沿ったリソースを作成する ➢ トラストフレームワーク専門委員会 （TFEC） ➢ イノベーション専門委員会 （IEC） ➢ アウトリーチ専門委員会 （OEC）

	■ 各専門委員会の委員長で構成される運営評議会は、専門委員会の活動の指導と調整を支援する 【Voila Verified の運営体制】 ■ 申請者への Voilà Verified 認証の付与について、Trust Oversight board（TOB）が、DIACC が認定した審査機関の審査に基づいて意思決定をする

図表 44　PCTF 概要[82]

No.	セクション	概要
1	Overview	■ PCTF のビジョンと価値提案を定義
2	Model	■ PCTF のビジョンと価値提案を定義
3	Notice & Consent*	■ 個人情報の収集、使用、および開示に関する声明を策定し、その声明に関する同意決定を行う権限を持つ人物から得るために使用される基準を定義
4	Authentication*	■ デジタルシステムへのアクセスを有効にするために使用される基準を定義
5	Verified Organization*	■ 組織が自身または他者 （個人または組織） に関する信頼できる情報を外部と交換できるようにする基準を定義
6	Glossary	■ PCTF で特定された用語のリスト
7	Credentials（Relationships & Attributes）*	■ デジタル形式で存在するクレデンシャルの作成、発行、および管理に関連する基準を定義
8	Infrastructure（Technology & Operations）*	■ IT インフラストラクチャの信頼性に関する基準、要件、およびガイドラインを定義
9	Assurance Maturity Model	■ 保証レベルを適切に分類するための PCTF 準拠基準の使用方法に関するガイダンスを提供
10	Privacy**	■ デジタル ID 目的の個人データの処理に関する基準を定義
11	Verified Person**	■ 自然人が実在し、ユニークで、識別可能であることを確立するために使用される基準を定義
12	Digital Wallet*	■ デジタルウォレットに関する基準、要件、およびガイドラインを定義
13	Trust Registries*	■ （2022 年度の第 4 半期に公開予定）

* Voilà Verified 認証プログラムに段階的に導入予定

** Voilà Verified 認証プログラムに導入済み

[82] https://diacc.ca/trust-framework/

2－5. 標準化・技術動向調査

本項では、VC/DIDs 等分散型アイデンティティに関連する主要な標準化団体・開発コミュニティの動向や標準化状況・技術的な課題と対応方針について整理する。

本調査では主に以下団体で取り組んでいる標準化技術動向・課題について整理を行った。

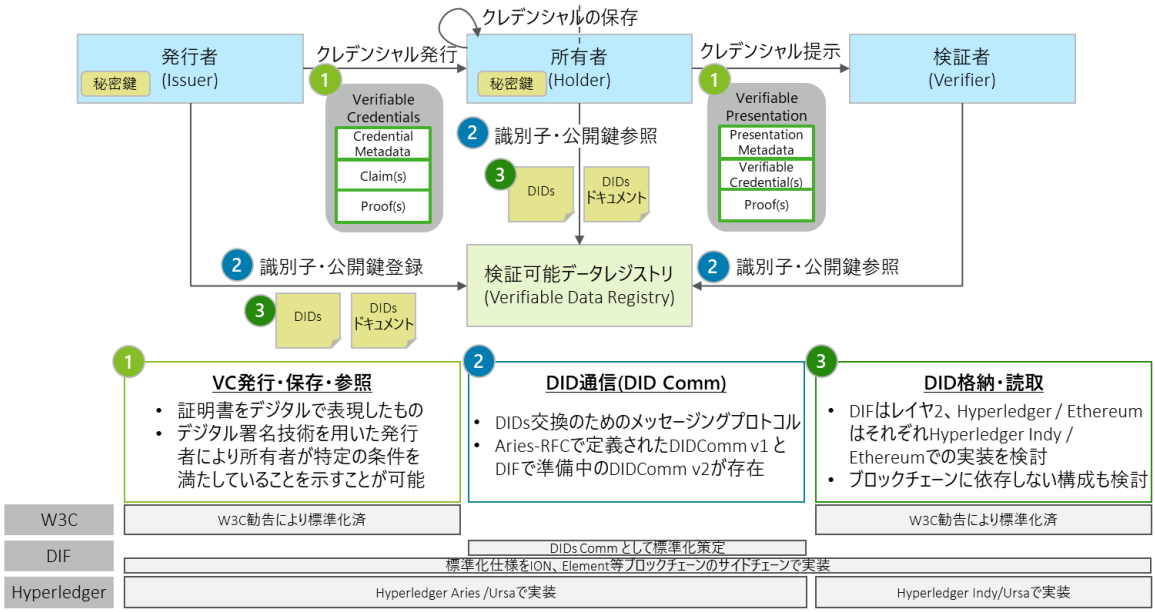
図表 45　標準化・技術動向調査団体リスト

No.	団体名	取り組み概要
1	**W3C（World Wide Web Consortium）**	■ 2021 年 11 月に「Verifiable Credentials Data Model 1.0 Recommendation」を発行、VC について標準化を実施 ■ 2022 年 7 月に「Decentralized Identifiers （DIDs） v1.0 Recommendation」を発行、DIDs について標準化を実施
2	**DIF（Decentralized Identity Foundation）**	■ DIDComm v2 の仕様策定 ■ Sidetree protocol の実装 ■ Bitcoin 及び Ethereum ブロックチェーンのレイヤ 2 を活用した実装（ION/Element） ■ DID メソッドの読み取りライブラリ（Universal Resolver）の実装
3	**Hyperledger Foundation**	■ Hyperledger Indy/Aries/Ursa の開発を実施し、分散型アイデンティティを活用した ID 認証サービス実装におけるオープンソースを提供
4	**ERC-725 Allianace**	■ ERC725 や ERC735 で自己主権型アイデンティティに関する標準化・実装を実施

２－５－１. 標準化された技術の概要

VC/DIDs 及びその通信技術については標準化及び実装が進んでいる。W3C、DIF、Hyperledger Foundation が行った標準化や技術実装について紹介する。

図表 46　分散型アイデンティティ（DID）における標準化項目



（１） VC（Verifiable Credentials） – 検証可能な資格証明書

Verifiable Credentials（VC）とは、様々な証明書と同様に、個人に関連付く属性情報をデジタル化した検証可能としたものである。VC 自体は属性情報を格納するコンテナのようなものであり、任意の情報を格納可能である。このコンテナ自体をオンラインで検証可能とすることで様々な状況に対応したデジタル証明に用いることができる。VC から状況に適した証明情報のみを取り出して表現したものが Verifiable Presentation（VP）と呼ばれる。

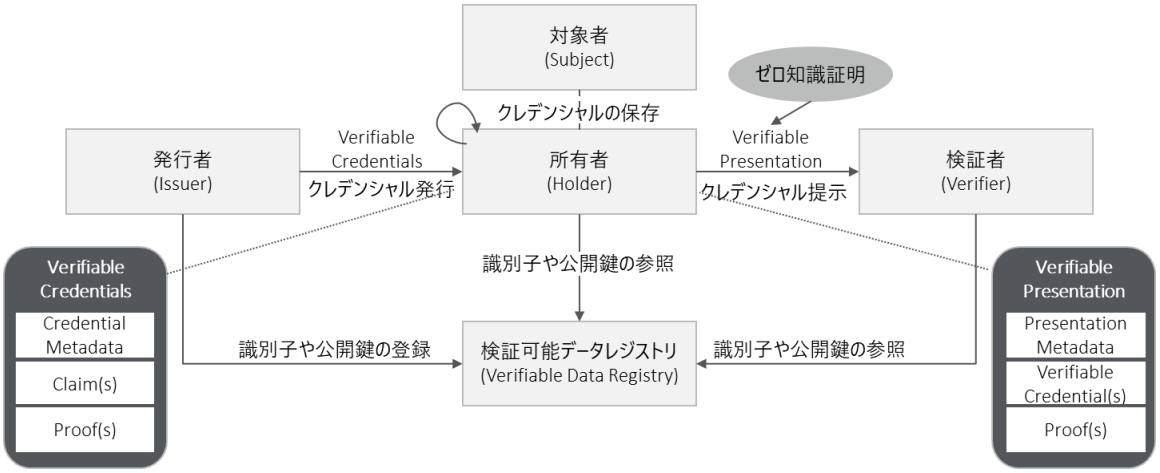
VC は W3C 勧告「Verifiable Credentials Data Model 1.0」として 2019 年 11 月 19 日に公開された。その後、2022 年 3 月 3 日に 1.1 が公開、2022 年 12 月時点で 2.0 がドラフト状態にある。

VC および VP を取り扱う場合には以下の関係者を考慮する必要がある。

- 発行者（Issuer）
  証明書を発行する自治体や企業、教育機関などであり、署名されたデジタル証明書を格納した VC を発行
- 対象者（Subject）
  VC の証明対象となる人またはモノ。VC には Subject の属性情報を記載
- 所有者（Holder）
  VC を管理する役割を持つ（多くの場合 Subject と同じ）。また、Verifier に提示する Verifiable Presentation （VP）を作成する役割も担う。発行者と検証者の間で直接のやり取りをさせずに、必ず両社の間に所有者が介在する点がフェデレーション方式と異なる

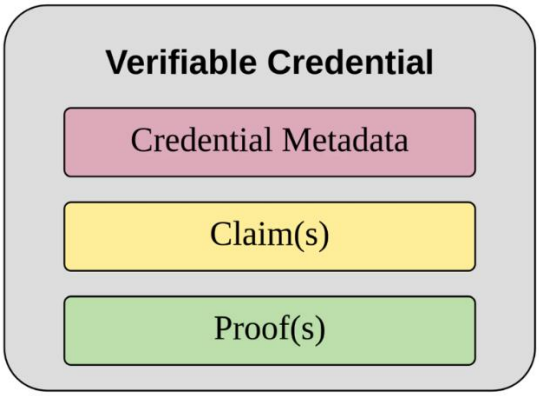
■ 検証者（Verifier）
Holder から提示された VP を検証する役割を持つ。VP 内の VC の署名検証を行い、証明書の真正性を確認

図表 47　Verifiable Credential のエコシステム



VC は下図のような構成になっており、それぞれの役割は以下となる。

図表 48　Verifiable Credential の構成[83]

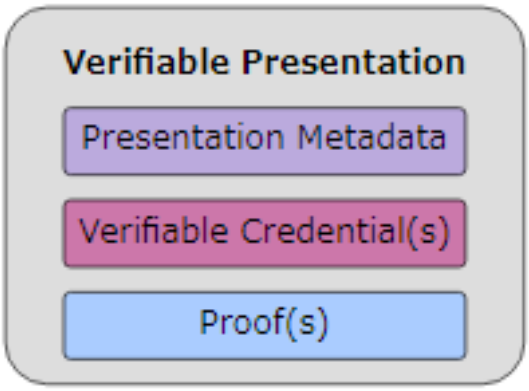


■ Credential Metadata
VC の発行者や有効期限、証明事項の属性などのデータ
■ Claim（s）
対象者の資格や状態など証明したい内容を主張するデータ。用途によって複数格納可
■ Proof（s）
VC の発行者によるデジタル署名。用途によって複数格納可。
分散型識別子（DIDs）により、デジタル署名の検証に必要な公開鍵と紐づけられる。認証局に頼らず保証される

[83] https://www.w3.org/TR/vc-data-model/

また、VP は下図のような構成となる。

図表 49　Verifiable Presentation の構成 [83]



- Presentation Metadata
  VC のメタデータから状況に適した情報を抽出したデータ
- Verifiable Credential（s）
  特定の状況に適した証明に必要とされる VC。ゼロ知識証明等を使用することで情報開示を最小化することも可能。用途によって複数格納可
- Proof（s）
  VC を検証するためのデジタル署名。用途によって複数格納可

（2） ゼロ知識証明による選択的開示の実現

検証者に VC を提示する際に、特定の状況に適した証明情報に限定して開示することで、個人情報等の重要情報の公開を最小限に抑えることができるため、VC とゼロ知識証明との組み合わせが検討されている。

前述した VP を作成する際に、ゼロ知識照明を使用することで、条件を満たす情報を持っていることのみを相手に知らせることができる。

一例として、JSON-LD ZKP with BBS+は MATTR 社から 2020 年 4 月に発表された比較的新しいゼロ知識証明の実装方式である。現在は、MATTR 社以外のメンバも加わり DIF の Crypt WG 等で仕様策定や議論が進められている。

＜特徴＞

- クレデンシャルの記述に JSON-LD を使用
- デジタル署名方式としてゼロ知識証明と相性の良い BBS+署名を用いる

JSON-LD はセマンティック Web や Search Engine Optimization（SEO）の領域で広く利用されている仕様（JWT とは異なる）で、JSON データに Linked Data の要素を取り込み、JSON の簡潔さを保ちながら、データの記述に使う用語を、URI を使って一意に特定できる。BBS 署名は BBS グループ署名を拡張したマルチメッセージ型のデジタル署名である。

楕円曲線暗号の一種として RSA 署名や ECDSA 署名とは異なり、複数のデータを並べたリストに署名を付けることができ、ゼロ知識証明と組み合わせやすい構造を備えており、署名したデータのリストから一部の要素を隠したまま署名の有効性を検証したり、一部の要素を隠したままそれがある条件を満たすことだけを証明することができる。

JSON-LD ZKP with BBS+では、JSON-LD で書かれたクレデンシャルを LD Canonicalization という方法で statement と呼ばれるデータに分解し、BBS+署名の生成や検証を行う。

BBS 署名を使って statement のリストに署名を付けることで、statement 単位で見せる/見せないの制御が可能となる（ただし、statement の中に含まれる氏名や生年月日などの情報を隠したまま、それらが特定の範囲内に収まる等の高度な証明はまだ実現できていない）。

図表 50　JSON-LD クレデンシャルの例[84]

```
{
    "@context": [                              // JSON-LD コンテキスト
        "https://www.w3.org/2018/credentials/v1",
        "https://schema.org",
        ...
    ],
    "id": "http://example.edu/creds/1234",     // クレデンシャルの識別子
    "type": "VerifiableCredential",            // クレデンシャルの種類
    "issuer": "https://example.edu/issuers/1", // クレデンシャルの発行者
    "issuanceDate": "2021-06-22T00:00:00Z",    // クレデンシャルの発行日時
    "expirationDate": "2022-06-22T00:00:00Z",  // クレデンシャルの有効期限
    "credentialSubject": {
        "id": "did:example:ebfeb1f712ebc6f1c276e12ec21", // 対象者の識別子
        "type": "Person",                      // 対象者の種類
        "birthDate": "1970-01-01",             // 対象者の生年月日
        "name": "John Smith",                  // 対象者の名前
        ...                                    // その他の属性
    },
    "proof": { ... }                           // 検証に必要な署名値など
}
```

（3） DIDs（Decentralized Identifiers v1.0）

分散型アイデンティティ（Decentralized Identity）とは中央集権的な ID 発行機関に依存することなく、人、組織、モノが、資格や経歴等の自身が持つ証明情報などを自分自身で発行・管理することができる仕組みである。個人の ID 情報や属性情報の格納にブロックチェーンなどの分散データベースを利用し、提示した ID で公開鍵認証を行う。

DIDs は「Decentralized Identifiers （DIDs） v1.0」として W3C より 2022 年 7 月 19 日に公開されている。

DIDs とは情報にアクセスするための URI（名前やインターネット上の場所を識別する文字列の書き方）の一種である。先頭の Scheme が、この文字列が DID であることを示し、次の DID Method では、DIDs がどのように実装されているか定義されている。最後の DID Method-Specific Identifier が、DID Method 内で一意となる ID になる。DIDs 経由で DID Document（JSON-LD で記述された公開鍵、エンドポイント等の情報）にアクセスできる。

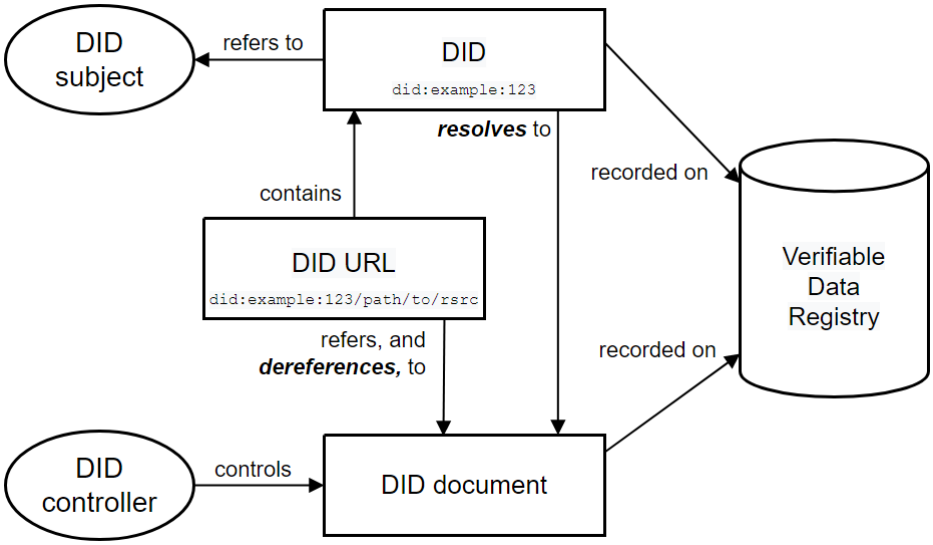
[84] https://www.iij.ad.jp/dev/report/iir/052/02.html

図表 51　DID 構文の構成[85]

DID Document は Verifiable Data Registry に格納される。Verifiable Data Registry は、ブロックチェーン・分散型ファイルシステムから、信頼できるデータストレージまで様々な種類が存在する。どのストレージにどの様な方法で格納するかは DID Method で指定する（DID Method は W3C が公開している「DID Specification Registries」で定義されている）。

DID にアクセスすることで DID Document を参照できるが、DID URL を使用することで基本的な DID の構文を拡張して、パス、クエリ、フラグメントなどの他の標準 URI コンポーネントを組み込み、DID Document 内の公開鍵、または外部のリソース参照などの情報を取得することができる。

図表 52　DID アーキテクチャイメージ図 [85]



図表 53　DID アーキテクチャ各要素の説明

要素	概要
DID Subject	■ 利用対象の人、モノ
DID Controller	■ DID を制御する主体
DID	■ 利用者の ID
DID URL	■ DID を格納した場所を示した識別子

[85] https://www.w3.org/TR/did-core/

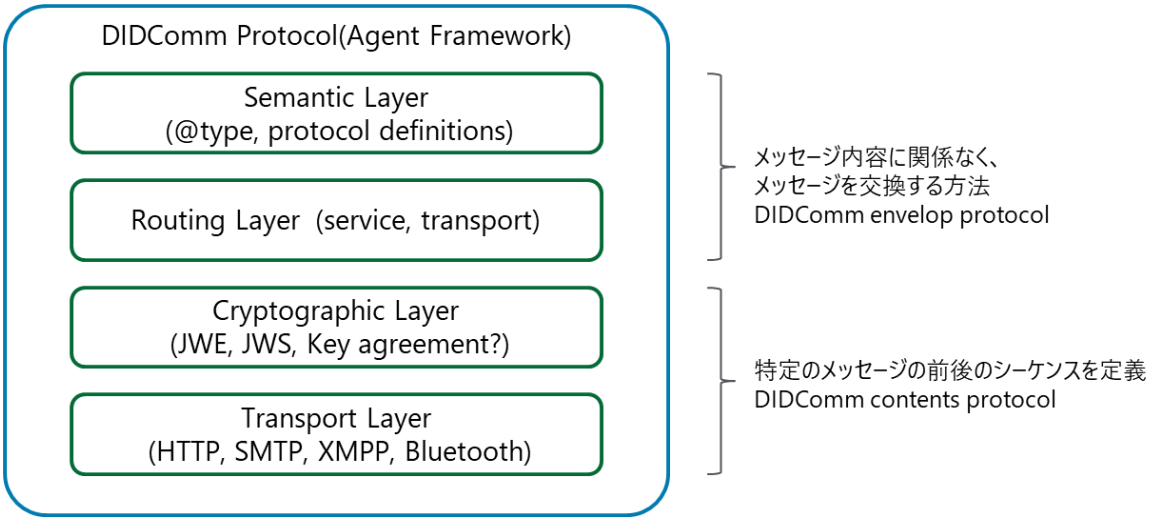
Verifiable Data Registry	■ DID および DID Document を格納するデータベース
DID Document	■ 認証に必要な公開鍵、エンドポイントなどを格納した文書

（4） DIDCommunications（DIDComm）

DIDComm は、さまざまな DID ベースのシステムから DID を制御する 2 つ以上のエンティティが相互に直接通信するためのメッセージングプロトコル（暗号化、署名、平文形式で保持するメディアタイプ、ファイルタイプを定義）である。人、組織、モノなど、これらの各エンティティによって制御されるソフトウェア間に安全な通信チャネルを構成し、任意の 2 者間で相互認証を行う方法を提供する。

Hyperledger Aries の RFC で定義された DIDComm v1 と DIF で準備中の DIDComm v2 が存在する。

図表 54　DIDComm Protocol の構成要素[86]



（5） Sidetree プロトコル[87]

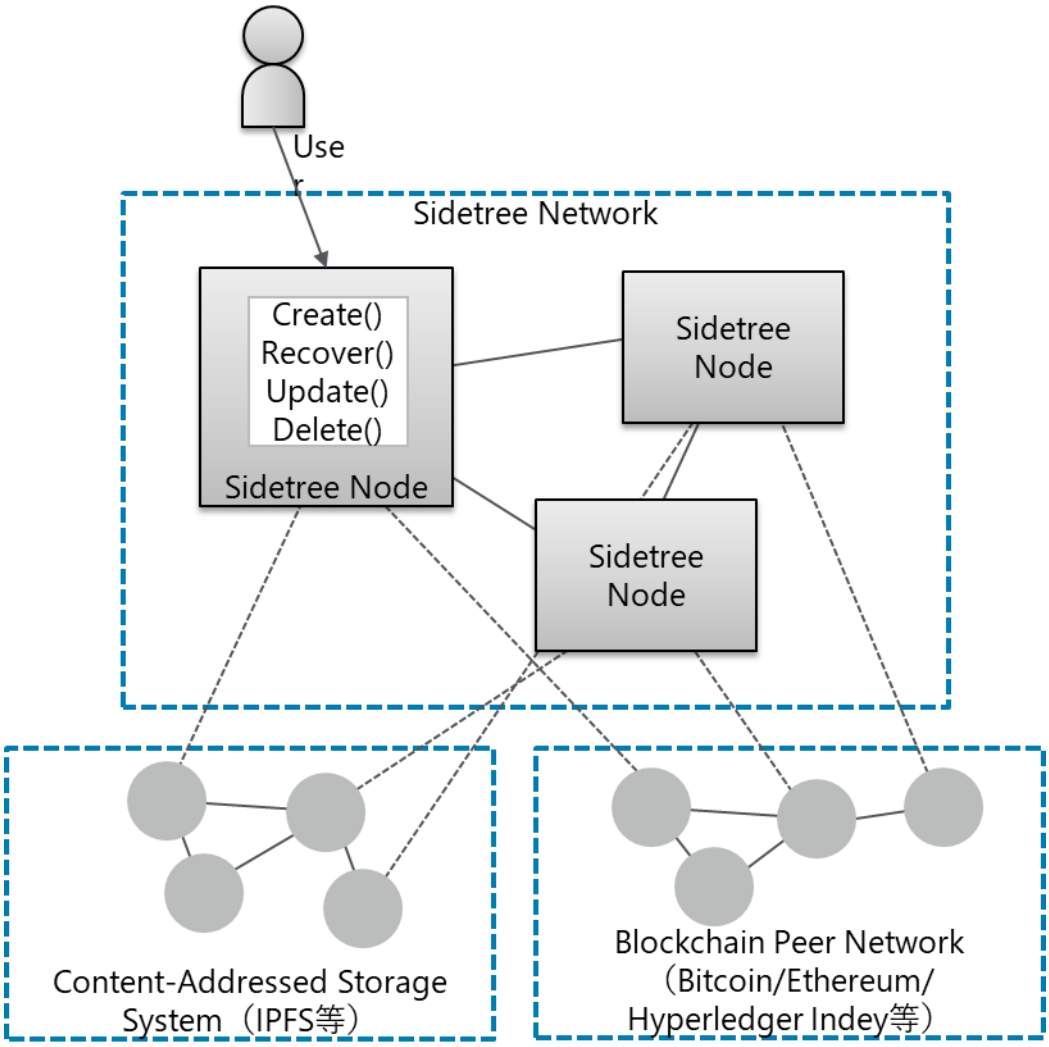
DIF のメンバ主体で策定された分散型アイデンティティを特定のブロックチェーンに依存せずに実現するプロトコル仕様で、ブロックチェーンを利用することを前提に策定されているが、スケーラビリティや秘匿化等の諸条件を充足させるために、レイヤ 2 を利用して分散型 ID をブロックチェーンにアンカリングし、DID Document に関する作成、回復、更新、非アクティブ化等の操作を行う。

アーキテクチャ的には以下の 3 つの機能から構成される。

[86] https://github.com/decentralized-identity/DIDComm-js/tree/master/docs
[87] https://identity.foundation/sidetree/spec/

- Blockchain Peer Network：
  DID や DID Document を保存するための基盤。DID Method の実行順序の制御等も担う
- Sidetree Node：
  DID Document に対してオペレーション（作成、解決、更新、削除等）を行うためのサービスのエンドポイント
- Content-Addressed Storage System：
  データとポインタをリンクして保存し、一定期間に渡りデータの更新や修正を制御するストレージ。IPFS などの分散型ストレージと連携

図表 55　Sidetree プロトコル構成イメージ [87]



Sidtree プロトコルをもとに実装されたオープンソースとして主要なものは以下が挙げられる

- ION Network：
  Blockchain Peer Network を Bitcoin、Content-Addressd Storage System を IPFS を用いて実装した Decentralized Identity 基盤

- Element：
  Blockchain Peer Network を Ethereum、 Content-Addressd Storage System を IPFS を用いて実装した Decentralized Identity 基盤
- Web5：
  Web3 に欠けていた ID レイヤを SSI を踏襲したオープンな技術で補完することを目的とし、現状では ION を採用する方向で検討されている

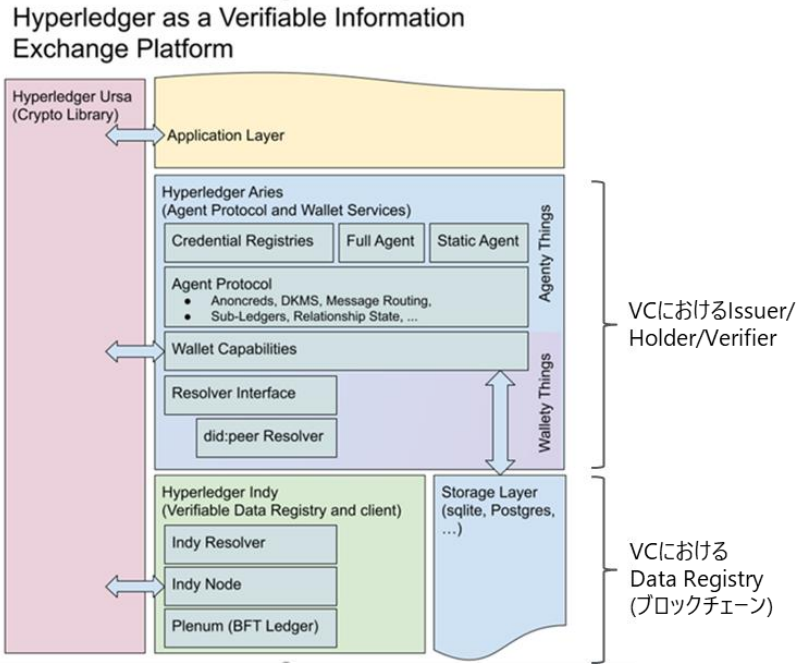
（6） Hyperledger Indy / Aries / Ursa

Hyperledger プロジェクトで ID 管理フレームワークを構成するシステム群である。Hyperledger Aries は検証可能なデジタル資格情報の作成、送信、保存に重点を置いたイニシアティブとソリューション向けに設計された、再利用可能で相互運用可能な共有ツール キットを提供する。

Hyperledger Indy は検証可能データレジストリに位置し、DID Document 等を格納するレイヤ 1 のブロックチェーン基盤となる。

Hyperledger Ursa はこれらのプロジェクトに暗号機能として秘密管理と分散鍵管理機能を提供する（ゼロ知識証明を含む）。

図表 56 Hyperledger Indy/Aries/Ursa のシステム構成[88]



[88] https://www.altoros.com/blog/hyperledger-aries-to-enable-blockchain-agnostic-self-sovereign-identity/

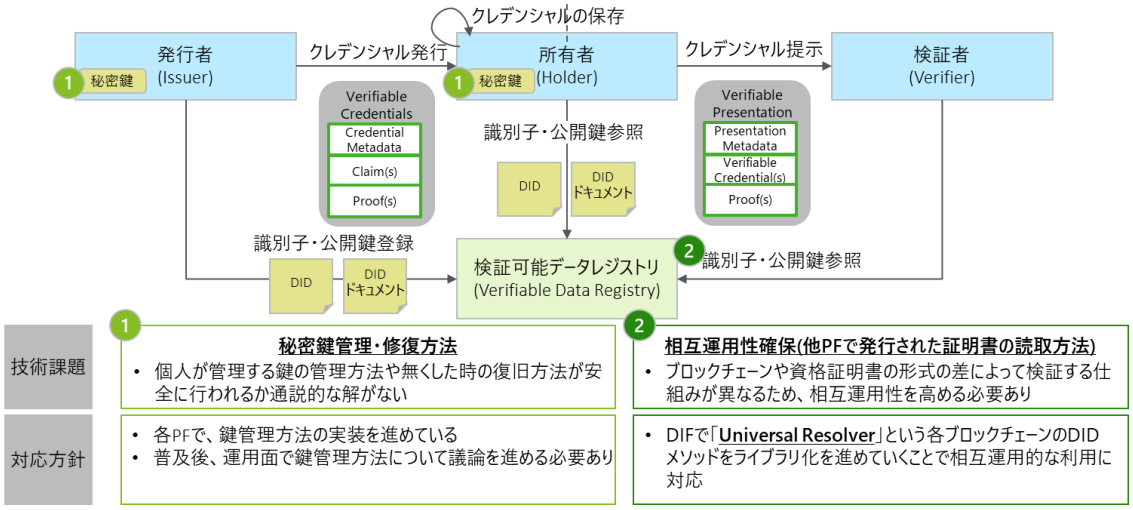
２－５－２. 課題・課題解決に向けた取り組み

VC/DIDs の実用利用においては以下のような技術的課題があり、それぞれの技術課題について以下対応を進めている。

■ 鍵管理の標準化：
安全な個人による秘密鍵の管理方法や紛失時の修復方法についての通説的な解決方法が現状ない状況である。現在各種開発コミュニティで鍵管理の標準仕様について検討中であるが、各社で実装アプローチが異なるため、今後標準的な手法の確立が期待される

■ 相互運用性の確保：
DID メソッドが乱立しており、各メソッドの相互運用性の確保が課題となっている。この課題を受けて、異なるブロックチェーンで発行したデジタル署名を別ブロックチェーンで読み取るために各ブロックチェーンの DID メソッドのライブラリ化を進められている

図表 57　分散型アイデンティティに関する技術的な課題



（１） 鍵管理に関する技術仕様

分散型アイデンティティにおいて鍵管理は重要であり、各団体において、鍵管理に関する仕様および実装が検討されている。

それぞれの仕様の違いとしては、DIF が推進している KERI はブロックチェーン依存していない鍵管理も視野に置いており、Aries-RFC は Hyperledger プロジェクトで検討されているため、Hyperledger Indy などのブロックチェーン基盤を前提とした仕様検討が中心となっている。ERC734 は Ethereum Request for Comment のひとつであり、Ethereum を前提としたスマートコントラクト上で鍵管理を行うための仕様が検討されている。

図表 58　各団体で検討されている鍵管理の仕様

仕様	検討団体	概要
Key Event Receipt Infrastructure（KERI）[89]	**DIF**	■ DIF の Identifiers & Discovery Working Group が主導 、セキュリティと相互運用性が不可欠なユースケース （サプライチェーン等）で非常に貴重であることが証明される、DID 文書の認証と解決に対するソリューションを提供 ■ KERI はキーイベントを受信・管理するインフラであり、マイクロレジャーとしての役割を持つ、キーイベントは鍵の生成、鍵のローテーション、署名などのイベントを指しており特徴としては以下が挙げられる ■ ブロックチェーンを必要とせず、暗号技術のみで証明可能な識別子を提供 ■ 証跡のため、鍵ペアを変更する都度署名付きメッセージをログに書き込む。追加証跡としてキーイベントログのコピーを他人に署名付きで保管してもらうことが可能 ■ KERI 識別子と鍵の委任により企業レベルの複雑な管理に対応が可能
Hyperledger Aries RFC（DKMS）[90]	**Hyperledger Foundation, DIF**	■ Hyperledger Aries プロジェクトを構成するコンセプトや機能で文章化されているもので、以下の仕様等を策定 ➢ Aries RFC 0023: DID Exchange Protocol ➢ Aries RFC 0036: Issue Credential Protocol ➢ Aries RFC 0037: Present Proof Protocol ➢ Aries RFC 0037: Present Proof Protocol ➢ Aries RFC 0051: DKMS （Decentralized Key Management System） Design and Architecture ■ DKMS はブロックチェーンおよび分散型台帳での使用を目的とした暗号鍵管理であり、その設計とアーキテクチャはアメリカ合衆国国土安全保障省との契約に基づいて開発[91]
ERC734[92]	**ERC-725 Alliance**[93]	■ Ethereum には Uport など ID 管理のサービスが既に存在しているが、左記に加えて標準規格として検討されている ERC725（ID インターフェース）、ERC735（クレーム管理）および ERC734（鍵管理）が存在 ■ ERC734 は ERC725 で使用することができる鍵管理の規格であり、鍵管理コントラクトは複数の鍵を管理してトランザクションやドキュメント、ログインなどに対して署名することが可能 ■ 鍵を使用する際には ERC725 へパスするインストラクションを作成し、承認（承認には複数の鍵が必要）されることで実行や ID 追加が可能

[89] https://github.com/decentralized-identity/keri

[90] https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0051-dkms/dkms-v4.md

[91] https://www.dhs.gov/science-and-technology/news/2017/07/20/news-release-dhs-st-awards-749k-evernym-decentralized-key

[92] https://github.com/ethereum/eips/issues/734

[93] https://erc725alliance.org/

（2） Universal Resolver

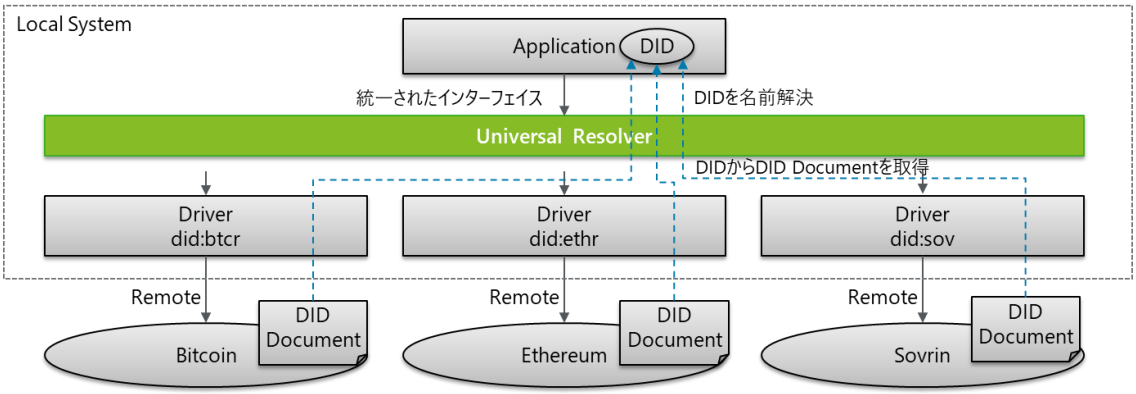
Universal Resolver は、W3C DID Core 1.0 および DID Resolution 仕様に基づき、様々な DID Method で分散型識別子（DID）を解決するため、DIF Identifiers & Discovery Working Group にて検討を行っている。

W3C で管理されている DID Method は Bitcoin、Ethereum や Sovrin, ION などプラットフォーム間で独立しており、DID を分散型アイデンティティの識別子として活用するには、プラットフォーム間で一意に特定する仕組みが必要である。

DID を利用するシステムが各プラットフォームの違いに対応させることは非常に困難であるため、この課題を解決する仕組みとして Universal Resolver が登場した。

Universal Resolver は標準仕様ではなくプログラム実装であり、DID Method で定義された各プラットフォームに対応したドライバーが存在する。DID の名前解決の仕様としては W3C で DID Resolution[94]で検討されている。このツールは DNS で URL から IP アドレスを解決するのと同様の目的を果たし、あらゆる種類の分散型アイデンティティの識別子の名前解決を可能とする統一されたインターフェースを提供しており、実質的な業界標準となっている。

図表 59　Universal Resolver のアーキテクチャ[95]



[94] DID Resolution https://w3c-ccg.github.io/did-resolution/

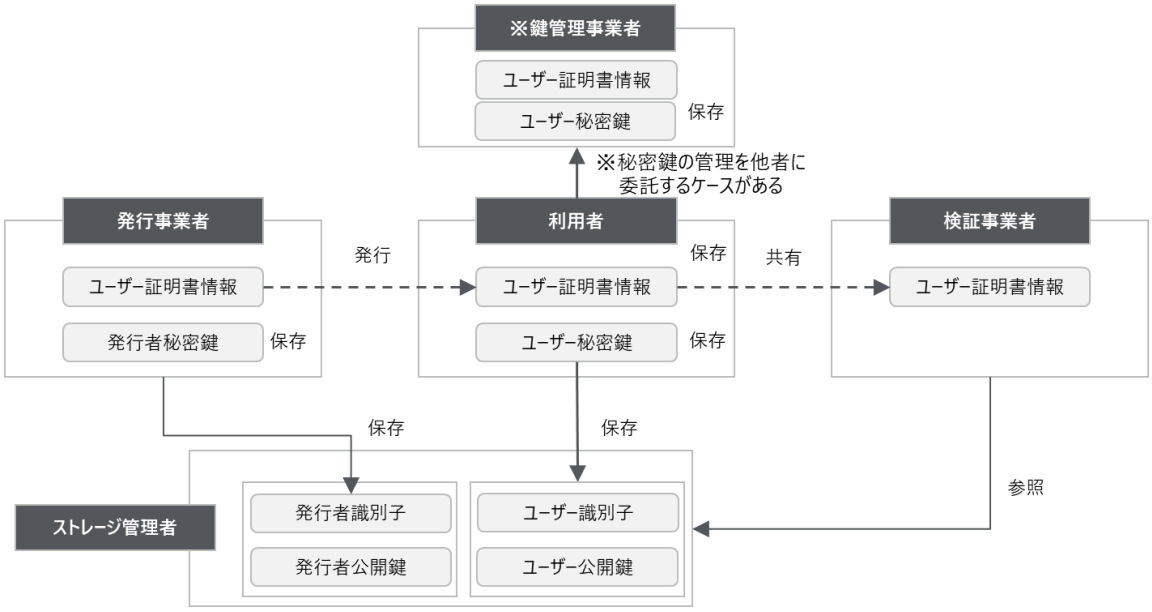
[95] https://github.com/decentralized-identity/universal-resolver 、https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c をもとに作成

2－6. 個人情報に関する法的整理

2－6－1. 分散化/暗号化された情報の性質・事業者に課すべき管理責任

本項では、分散型アイデンティティ（DID）における各種情報の個人情報該当性及び事業者に課される責任等を整理する。一般的な管理情報と事業主体は下記の図のように表すことができ、この管理構成を仮定した場合の各種情報及び事業者の管理責任について個人情報保護法をもとに整理を行った[96]。また、GDPR と ID 認証サービスについて実際に EU でアイデンティティサービスの検討を行った専門家や国内・海外民間事業者にヒアリングを行い GDPR とアイデンティティサービスの関係性についての動向を確認した。

図表 60　分散型アイデンティティにおいて一般的な事業主体と管理情報構成



（1） 国内における法的整理

主要な検討ポイントは以下の通りである。

■　ユーザ証明書情報：

「特定の個人を識別することができる」とは、社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認められる場合をいい、ユーザ証明書情報がこれにあたる場合は個人情報にあたると考えられる。

また、上記の場合でなくとも、他の情報と容易に照合することで特定の個人を識別することができる場合には個人情報にあたると考えられる

■　ユーザ識別子・ユーザ秘密鍵・ユーザ公開鍵：

ユーザ識別子/秘密鍵/公開鍵が特定の個人を識別することができる情報と結び付けられている場合、「他の情報と容易に照合することができる」といえ、個人情報にあたる可能性がある

[96] 再委託先であるアンダーソン・毛利・友常法律事務所外国法共同事業の調べにより整理を行った

■ 発行者識別子・発行者秘密鍵・発行者公開鍵：
発行者識別子や発行者公開鍵が発行者自身（法人の情報ではなく法人の担当者等）を識別することができる情報と結び付けられている場合、「他の情報と容易に照合することができる」といえ、個人情報にあたる可能性がある

■ 発行事業者・検証事業者・鍵管理事業者：
自身の取り扱うユーザ証明書情報（鍵管理事業者にあってはユーザ秘密鍵）が個人情報にあたる場合、それが体系的に構成されたデータベース等を事業の用に供する場合は個人情報取扱事業者と考えられる

■ ストレージ管理者：
ストレージに個人情報にあたる識別子・公開鍵その他ユーザの個人情報を保存し、それを体系的に構成されたデータベースにして事業の用に供している場合は個人情報取扱事業者にあたると考えられる

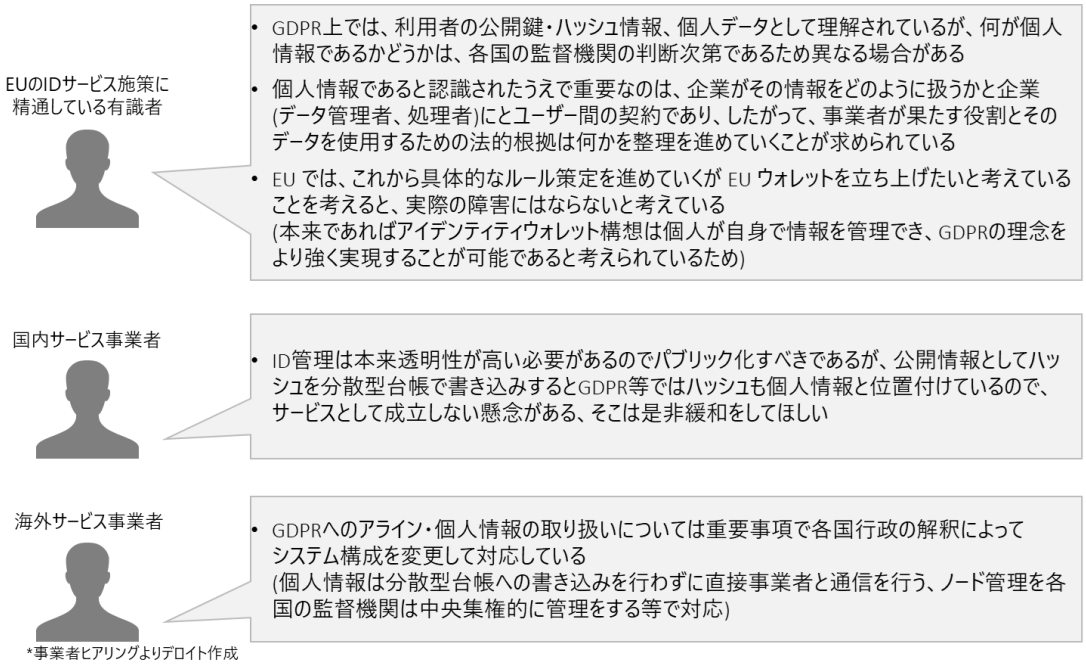
図表 61　個人情報保護法（以下「法」）上の主たる用語の定義

用語	定義
個人情報	■ 生存する個人に関する情報であって、 ① 当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む） 又は ② 個人識別符号が含まれるものをいう（法 2 条 1 項）
個人情報データベース等	① 特定の個人情報を、コンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合物をいう ② また、コンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば、五十音順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものも該当する（法 16 条 1 項、個人情報保護法ガイドライン（通則編）2-4） ※なお、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報を「個人データ」という（法 16 条 3 項）
個人情報取扱事業者	■ 個人情報データベース等を事業の用に供している者をいう（法 16 条 2 項） ■ 個人情報取扱事業者（以下「事業者」）となる場合の主な規制は以下のとおり ➢ 個人情報の利用目的のできる限りの特定及び本人への通知または公表が必要（法 17 条 1 項及び 21 条 1 項） ➢ 個人データの安全管理のために必要かつ適切な措置を講じる必要（法 23 条） ➢ 個人データの第三者提供には。原則事前に本人の同意を得る必要（法 27 条 1 項） ➢ 事業者が保有する個人データに関し、本人からの求めがあった場合には、原則その開示が必要（法 33 条 1 項、2 項） ➢ 事業者が保有する個人データの内容が事実でないという理由で本人から個人データの訂正や削除を求められた場合、訂正、追加又は削除を行う必要（法 34 条 1 項）

（2） GDPR における分散型アイデンティティ（DID）の位置づけ

参考情報として、個人情報保護の施策が進む欧州における GDPR と DID の関係性について、有識者や国内外事業者へのヒアリングを行い、そのコメントを以下図表に整理した。

図表 62　GDPR における DID の扱いに関する有識者コメント



*事業者ヒアリングよりデロイト作成

２－６－２. 個人の意思で情報提供を行う場合の留意点

取り扱う情報が要配慮個人情報（機微情報）である場合、取得する際に本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示す必要がある。

個人が未成年または意思能力に疑義がある場合は情報取得の際に法定代理人に確認しなければならない可能性がある。

図表 63　個人が自分の意思でデータ共有する場合の論点

分類		想定ケース	個人が自分の意思で情報共有する際の法的論点
データ特性	個人識別符号	• 一般的な本人確認	• (一般的な本人確認)
	要配慮個人情報 (機微情報)	• 本人が通院情報等を提供する　等	• 同意の取得に当たって、事業の規模及び性質・個人情報の取扱状況（取り扱う個人情報の性質及び量を含む。）等に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示す必要あり
共有主体属性	未成人	• 未成人の年齢確認等身元確認	• 未成人の本人確認又は法定代理人の確認を行う必要がある
	認知能力のない成人 (認知症等)	• 認知能力に疑義がある成人の銀行口座開設等にかかる身元確認	• 法定代理人が選任されている場合は、法定代理人からの確認を行うことが必要

2－7．トラストモデル

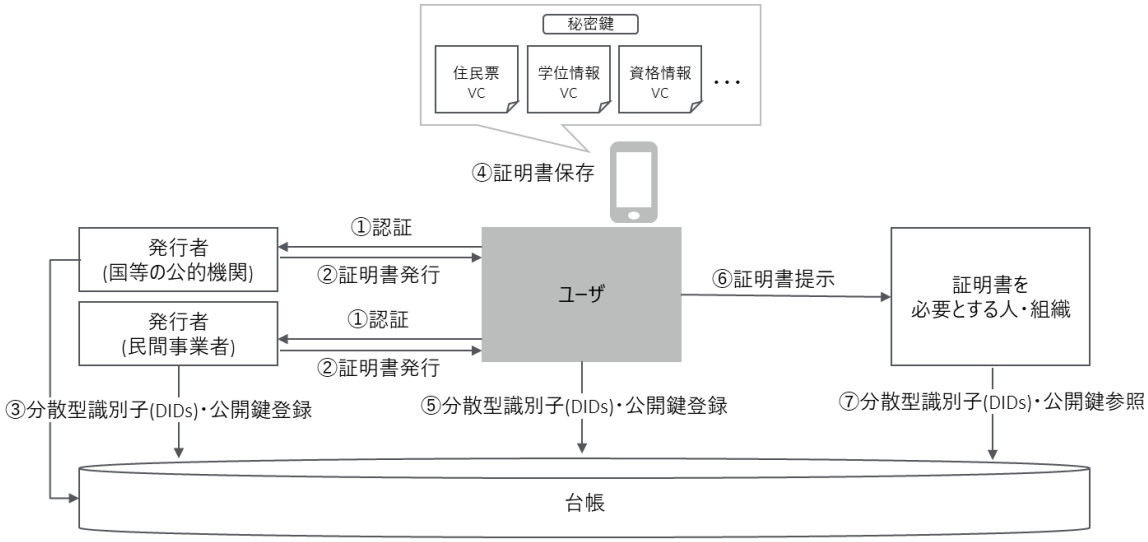
2－7－1．トラストモデル実現案

DID の技術を「本人を介した官民情報の活用」へ活用する試みの一つの方向として、様々な認証情報を個人が主体的に管理でき、将来高い相互運用性を実現しうる以下の特徴を有するデジタル ID ウォレットの構築を検討した。

- 個人がスマホに様々な組織が発行する証明書を VC として格納し、必要な時にのみ意思に応じて開示
- ユーザ・VC 発行者の公開鍵を暗号化した情報が分散型識別子（DIDs）と共に台帳に記録
- 標準規格を用いる事で官民情報を集約、将来的には海外政府・事業者も巻き込んだサービスを展開

このようなデジタル ID ウォレットにおいて、マイナンバー関連情報の連携も検討の余地があるものと考えらえる。

図表 64　DID によるデジタル ID ウォレットのイメージ



２－７－２. 実現案に向けた課題・論点

DID を活用したデジタル ID ウォレットの構築に向けては、①マイナンバー関連情報の範囲、②識別子・公開鍵の連携方法、③秘密鍵の管理方法が主な課題として挙げられる。

（1） マイナンバー関連情報の範囲

デジタル ID ウォレットに行政データを保持する際にマイナンバー関連情報と連携する必要があり、以下の点に留意する必要がある。

- マイナンバーの用途は社会保障、税、災害対策と定義されており、マイナンバーは識別子として活用不可である。
- マイナンバーカードの基本情報は公的個人認証サービス以外に取得することはできず、マイナンバーカードの情報を VC として利用することは現行法制上難しい

マイナポータルで取得できる情報を VC として発行し、個人がその証明書を管理して個人の意思で属性情報を選択的に提供するスキームは今後検討の余地がある。例えば、住基ネット等マイナポータルで個人が自身で管理できる情報をマイナポータルの自己情報取得 API で収集し、民間で保有する情報は別途手法を検討の上で同じく収集、デジタル ID ウォレットにて一元管理できると有用性の高いデジタル ID ウォレットになる可能性がある。

（2） 分散型識別子（DIDs）・公開鍵の連携方法

分散型識別子は相互運用性を確保するためブロックチェーンを活用することを念頭に W3C で標準化された。一方、識別子や公開鍵が個人情報に該当する可能性が欧州を中心に議論されており、個人情報を公開する形とならないよう、ブロックチェーンに記録する情報を限定して詳細情報を個別に連携、あるいは、ブロックチェーンではない台帳を活用したモデルを志向する動きもみられ、現状では事業者毎に異なる形を模索しているため、今後の標準化・運用方法の確立が待たれる。

また、現行の個人情報保護規制に沿った形で ID 認証サービスのルール整備も併せて行うことが効果的と思われる。EU では、EU デジタルウォレットの構築・実証実験を通じてルール作りを行っている状況であり、イギリス・カナダにおいてもルール策定を行い、ID サービス事業者を認可する形でガバナンスを整備している。

（3） 秘密鍵の管理方法

個人で秘密鍵管理を行った場合、秘密鍵が紛失または不正利用された場合の対応策が確立されていない（各開発コミュニティで秘密鍵管理に関する技術検討、標準化を進めている状況）という課題がある。

現状のサービス事例においては、AWS や Azure 等のクラウドサービスや、証明書発行者が秘密鍵を中央集権的に管理している事例が多い。鍵も個人自身で管理する場合、鍵管理・暗号化技術等の標準化を待ったうえで、秘密鍵紛失時の修復方法等の運用方法を検討していく必要がある。

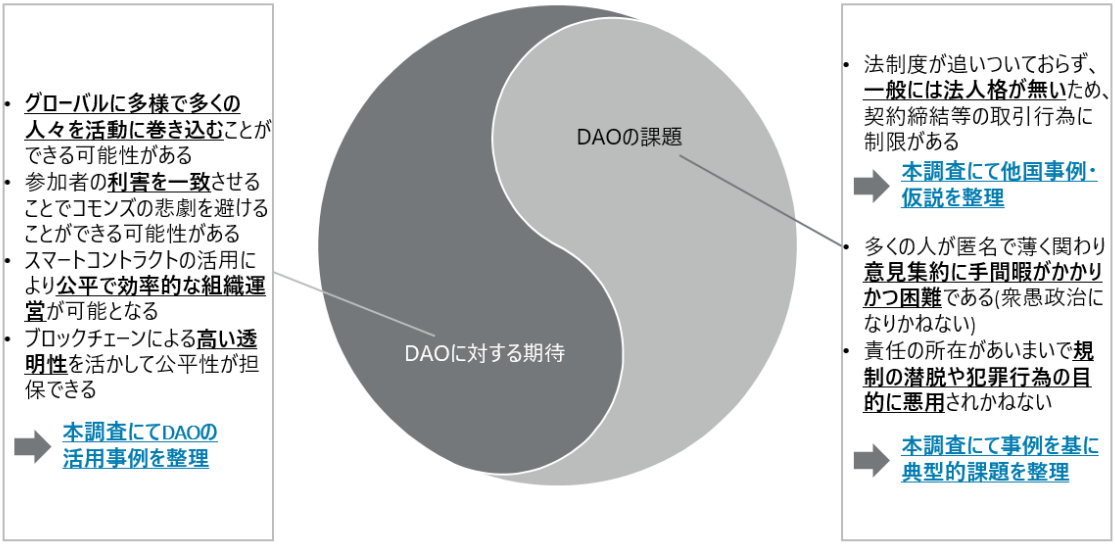
3. スマートコントラクト/DAO

3－1. 調査の狙い・アプローチ

Web3.0 では DAO が新たな組織体として活用され、そのグローバルで公平・効率的な組織活動に期待がかけられる一方、DAO と一口に言ってもその定義や活用方法が取り組みにより多種多様であり、定石がまだ確立されていないまさに黎明期の分野である。

したがって、法制度が無いことによる不透明さ等の課題が散見されると共に、米国ワイオミング州での DAO 法施行に見られるように様々な地域が DAO の可能性を最大限生かす行政上の措置を検討している。こうした状況を踏まえて、我が国においても適切な内容及びタイミングでの対応が取れる備えとして、日本の現行法における DAO の位置づけ並びに法人格の有無を含めた今後考えうる DAO の法的な定義の方向性を検討することには大きな意義があるといえる。

図表 65　DAO に対する期待と課題

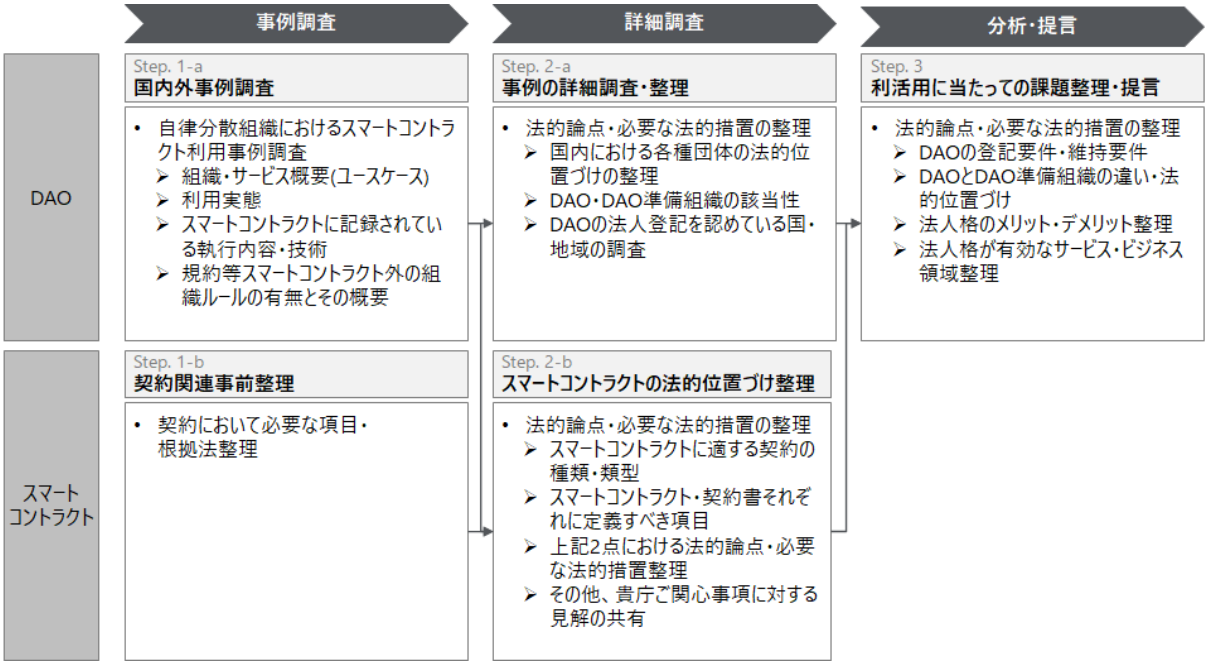


本調査では、日本における DAO に関する適切な法整備等の対応を検討するためのインプットとすべく、以下のステップで調査を実施した。

- DAO に関する国内外の利用実態を調査する
- DAO の構成要素であるスマートコントラクトの法的位置づけを整理する
- 日本において DAO に該当し得る各種団体の法的位置づけと課題を整理する
- DAO の法人登記を認めている国・地域を調査する
- DAO の活用における課題を整理し、法人格の有無を含めた日本において将来考えうる DAO の法的位置づけを検討する

以下の図表は、上記の調査アプローチの具体的な項目の関係性を図示したものである。

図表 66　調査アプローチ



3－2. 調査まとめ

調査・分析を踏まえて以下のように取りまとめを行った。

図表 67　調査結果まとめ表

見出し	調査サマリ
3－3. **DAO・スマートコントラクト事例**	■ 多様な DAO の在り方・活用シーンを念頭に「大きな経済圏を持つ DAO」「社会貢献 DAO」「訴訟等のリスクが顕在化した DAO」「ワイオミング州で登記された DAO」「日本発の DAO・関連事業者」の事例を調査した 大きな経済圏を持つ DAO ■ DAO の活用用途は数、トレジャリー規模共に DeFi 分野が圧倒的。独自トークンの時価総額の観点でも、上位 10 件のうち半数以上が DeFi である（上位 10 件 1: Uniswap、ApeCoin、Aave、BitDAO、MakerDAO、Synthetix、Dash、Curve、Lido、Decred） ■ DeFi では DAO による運営であるが故のガバナンス上の課題として、投票の定足数や投票率が低い、悪意ある提案の検証、投票参加者のスマートコントラクトへの理解度といった問題点が指摘されている ■ NFT 分野の先進的な DAO とされる Nouns DAO では、創業メンバによる拒否権が設定されており、ガバナンスの分散性と引き換えに悪意ある提案への対応を打っている 社会貢献 DAO ■ ATX DAO: テキサス州オースティンを暗号資産領域の先進地域とするべく立ち上げられたローカル DAO で、地元アーティストらとの NFT 発行、独自トークン発行の検討等、地元コミュニティを醸成・盛り上げながら様々な活動を行っている ■ Charity DAO: ウクライナへの寄付を集めており、ガバナンスの分散性・透明性は不明だが、寄付の募集・実行のスピード面でチャリティにおける DAO 活用の可能性を示している 訴訟等のリスクが顕在化した DAO ■ Ooki DAO: 暗号資産デリバティブ取引を提供する Ooki DAO のコアメンバが無免許で事業を営んでいるとして米 CFTC に訴追される一方、その根拠をガバナンストークンによる投票行為に求める事には CFTC 委員から疑義が表明される等、DAO の活用がはらむ訴訟リスクと共に適切な規制の在り方に関する議論の必要性が顕在化した ■ The DAO: ハッキング攻撃による資金流出への対応として 2016 年にイーサリアムのハードフォークが行われ、イーサリアムの分散性の在り方が議論された。また、2017 年には SEC が The DAO のガバナンストークンが証券に該当するため、当時行われた ICO が未登録証券の販売にあたるとするレポートを公表した ワイオミング州で登記された DAO

	■ ステーブルコイン Ducat を開発する「American CryptoFed DAO」等のいくつかの登記された DAO の取り組み内容を概観した ■ 有限責任、パススルー課税、土地等の資産を法人として保有するといったメリットが登記の動機ではないかと考えられる 日本発の DAO・関連事業者 ■ DAO を活用した取り組みを進める複数の非営利及び営利事業者にヒアリングを行った ➢ DAO の定義・捉え方は様々であったが、人々の新たな関わり方、コミュニティを生かした活動のスケール拡大に関心がある点は共通していた ➢ 一方、分散的な組織運営への課題意識はそれぞれが強く持っており、トークンによる動機付けが重要という指摘がある一方、投機目的の参加者を避けるためにトークン発行に慎重姿勢を取るケースもあり、取り組みの性質に応じた仕掛けが求められる ➢ DAO に法人格が無いことにより参加者が無限責任を負う可能性があるリスクは各事業者が認識しており、契約締結や財産の保有等の機能面でのメリットも考慮して、今後更に要否を検討する余地がある論点であるといえる DAO の課題と期待されるユースケース ■ 調査した事例において DAO の課題として、DAO の持続可能な活動の要素としてビジネスモデル、コミュニティ、ガバナンスに大別すると以下の通りとなった ➢ ビジネスモデル: 一部分野で高い時価総額を誇るトークンを扱う DAO が存在するがビジネスモデルは営利・非営利いずれの場合も試行錯誤の途上 ➢ コミュニティ 　➢ ガバナンス投票の参加率が限定的 　➢ 提案の内容(例: コードの一部修正)が十分に吟味されるとは限らない ➢ ガバナンス 　➢ ガバナンス投票の定足数が限定的 　➢ 悪意ある提案を検証する役割が不明確な場合がある 　➢ 規制逃れのために DAO が活用されるケースがある 　➢ 悪意ある参加者にガバナンス投票制度を悪用される恐れがある 　➢ 悪意ある参加者・提案に対して拒否権等の対抗策を取ると DAO の特徴の一つである分散性が損なわれる恐れがある 　➢ インフラであるブロックチェーン自体の分散性にも疑義が残るケースがある
3－4. **スマートコントラクトの**	■ スマートコントラクトは、通常は契約そのものではなく、事前に合意された契約内容の自動執行プロトコルと考えられる ■ DeFi 等のスマートコントラクトを活用したサービスにおいても、通常はスマートコントラクトの群が成すプロトコル自体は契約を

法的位置づけ整理[97]	構成せず、あくまで契約によって合意された内容を自動執行しているという整理になるものと考えられる ■ スマートコントラクトを使うことが難しいケースとして、故意や過失等の法的評価を伴う契約、自動で執行されると消費者保護法等の法規制や公序良俗に反してしまう契約等が挙げられる ■ 外部から誤ったデータが入力された場合に本来の意図と異なる結果が生じる可能性がある等、スマートコントラクトの実際上の留意点はまだ様々なユースケースの中で検証を要する状況である
3－5. **日本における各種団体の法的位置づけと DAO への適合度 [97]**	■ 日本においては合同会社あるいは権利能力無き社団が DAO の実態に近い既存の団体類型と考えられる ■ 一方、それぞれ DAO に適用する際には以下の課題がある ➢ 合同会社：定款等に社員の氏名・住所を記載する必要がある ➢ 権利能力無き社団：無限責任を負う民法上の組合との明確な区別の基準が確立されておらず、法人格が無いため契約締結等の法人としての活動ができない
3－6. **DAO の規制調査・法的位置づけ整理 [97]**	■ 米国ワイオミング州では 2021 年 7 月 1 日に LLC として DAO を定義した州法（以下、DAO 法）が施行された ■ DAO 法では、DAO の設立要件、登録手続、メンバの権利・義務や解散事由が定義されており、通常の LLC の特徴に加えて、定款に DAO の管理、促進、運営に直接使用されるスマートコントラクトの識別子や運営におけるアルゴリズム及び参加者が果たす役割を記載するといったブロックチェーンを基盤とする組織運営を前提とした組織設計がなされている
3－7. **日本における DAO の法人格検討**	■ 上述の通り、日本では合同会社あるいは権利能力無き社団が DAO の実態に近いと考えられる一方、それぞれに課題があった ■ 合同会社において、定款等に記載する社員の氏名・住所を KYC 済みのアドレスに置き換えることで、DAO 参加者のプライバシー・匿名性に配慮しながら、DAO に法人格を与えると共に、オンチェーンデータを生かした決算・監査対応の透明化・効率化が同時に期待できると思われる ■ 一方、アドレスの KYC 情報を別途管理する必要がある他、KYC を DAO の構成員の要件とすることが、グローバルに自由な参加を旨とする DAO の在り方を妨げないような KYC プロセスを検討する必要がある

[97] 再委託先であるアンダーソン・毛利・友常法律事務所外国法共同事業の調べによる

3－3. DAO・スマートコントラクト事例調査

様々な DAO の活用方法が考えられることから、以下のカテゴリに調査対象の事例を分けて調査を実施した。

図表 68　調査対象とした DAO の事例

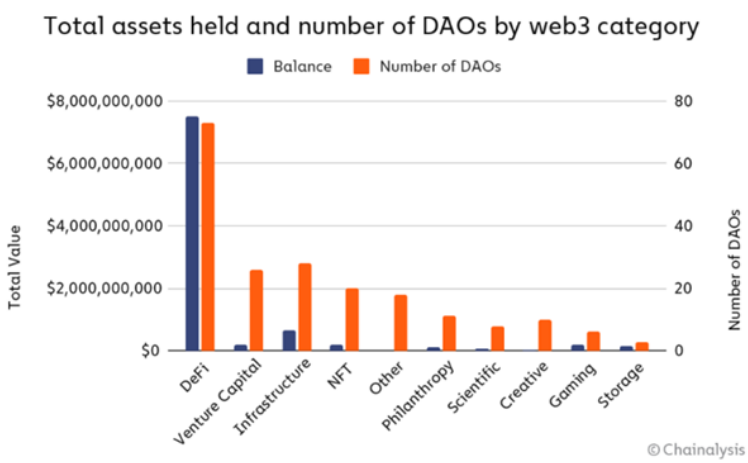
	項目	探索手法	具体例
1	大きな経済圏を持つ DAO	■ CoinMarketCap にて時価総額が高いデジタル資産に関連する DAO ■ 当該サイト上の分類で DAO と定義されているもの上位組織を選定（所謂 Protocol DAO、De-Fi 関連が多くなる）	■ Uniswap ■ Aave ■ Maker　等
2	社会貢献 DAO	■ ダウ・ジョーンズ社キュレーション（Factiva）にて過去半年の“decentralized autonomous organization”と（以下それぞれ and 条件） “charity”, “donation” を and 条件で探索後、弊社にて関連が薄いものを削除	■ ATX DAO ■ Charity DAO
3	訴訟等のリスクが顕在化した DAO	■ ダウ・ジョーンズ社キュレーション（Factiva）にて過去半年の“decentralized autonomous organization”と（以下それぞれ and 条件）“訴訟”,“lawsuit”, “sue”,”arrest”, “litigate（litigation）”, “fraud”, “indictment” を and 条件で探索後、弊社にて関連が薄いものを削除	■ Ooki DAO（bZeroX） ■ The DAO
4	ワイオミング州で登記された DAO	■ 米国ワイオミング州の DAO 法で認定された DAO	■ American CryptoFed DAO 等
5	日本発の DAO・関連事業者	■ DAO 活用のメリット・デメリット、日本の事業環境における課題等のヒアリング対象として設定	■ NPO 法人ドットジェイピー ■ Stake Technologies 株式会社 ■ Fracton Ventures 株式会社

（1） 大きな経済圏を持つ DAO

Chainalysis の分析[98]によると、以下図表が示す通り、DeFi に関連する DAO が組成数、トレジャリー（DAO が保有する資金）の残高共に最も大きい結果となった。

図表 69　類型別 DAO の数とトレジャリーの残高[99]

類型別DAOの数とトレジャリーの残高



記事詳細

- ✓ But in terms of raw numbers and treasury sizes, DeFi-related DAOs have a giant lead. The DeFi category accounts for 83% of all DAO treasury value held and 33% of all of the DAOs by count.
- ✓ There are also a large number of DAOs focused on venture capital, infrastructure, and NFTs, suggesting that DAOs are appealing to investors, developers, and artists. Their on-chain treasuries, however, are relatively tiny.
- ✓ To be fair, the lines between these categories are blurry. Gaming DAOs often engage with NFTs, venture DAOs often provide funding to DeFi, and infrastructure DAOs support all of the above categories.

実際に DAO に関連する暗号資産の時価総額に目を向けると、上位の多くが DeFi に関連している。

図表 70　DAO に関連する暗号資産の時価総額上位銘柄[100]

名称	時価総額（億円）	概要	関連会社（公開情報[101]から確認できるもの）
Uniswap	6,022	■ DEX（分散型取引所）の運営	■ Uniswap Labs（米国）：プロトコル開発・管理やコミュニティ運営への関与などを行う
ApeCoin	1,516	■ NFT プロジェクトである BAYC の運営、派生プロジェクトの管理	■ APE Foundation（ケイマン諸島）：DAO の決定を遵守し、ApeCoin の管理を行う ■ Yuga Labs（米国）：開発・デザインを担う

[98] Chainalysis 「Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated」（最終アクセス 2022 年 10 月 9 日）
[99] Chainalysis レポートより抜粋
[100] CoinMarketCap「仮想通貨時価総額上位（DAO のタグが付いたものでソート）」（最終アクセス 2022 年 11 月 9 日）
[101] Uniswap、Aave、MakerDAO は金融庁、株式会社クニエ合同研究「分散型金融システムのトラストチェーンにおける技術リスクに関する研究 研究結果報告書（概要版）」（令和 4 年 6 月）、ApeCoin については APE FOUNDATION「APECOIN IS FOR THE WEB3 ECONOMY」（最終アクセス 2022 年 11 月 9 日）、Synthetix は Defialliance「Work in Web3」、Dash は DashNews「Dash Core Group Becomes First Legally DAO-Owned Entity」（最終アクセス 2022 年 11 月 10 日）、Curve は CB Insights の情報を基に作成

Aave	1,352	■ DEX（分散型取引所）の運営	■ Aave Limited（英国）： 電子マネー業者ライセンスを取得
BitDAO	944	■ De-FI プロジェクトへの投資	-
MakerDAO	923	■ ステーブルコインである DAI に関連するプロジェクトの管理	■ DAI Foundation（デンマーク）： 知財管理等を行う ■ RWA Company LLC（ケイマン諸島）： 実世界の資産への投資管理、クライアントとの契約締結等を行う
Synthetix	855	■ DEX（分散型取引所）の運営	■ Synthetix（オーストラリア）： 不明。ただしエンジニア採用行っていることから開発機能とみられる
Dash	676	■ 仮想通貨 Dash に関連するプロジェクトの管理	■ Dash Core Group, Inc.[102]（米国）： ソースコードの作成・保守からカスタマーサポート等業務を担っている ■ The Dash DAO Irrevocable Trust（ニュージーランド）： Dash Core Group の全株式を保有している信託
Curve	538	■ DEX（分散型取引所）の運営	■ Curve Finance（スイス）：不明。 CEO は Michael Egorov となっていることから関連企業とみられる
Lido	477	■ Ethereum のリキッドステーキングサービスを構築する DAO	-
Decred	470	■ 仮想通貨 DCR に関連するプロジェクトの管理	-

金融庁と株式会社クニエの合同研究[103]ではそれぞれ代表的な DeFi サービスである Uniswap、Aave、MakerDAO のガバナンスについて、以下の課題を挙げている。

1. 悪意のあるガバナンス提案の削除
2. ガバナンス投票の定足数が低いこと
3. ガバナンスの投票率が低いこと
4. スマートコントラクトへの理解度の個人差

[102] 関連会社の中で LinkedIn の情報に基づき在職者の所在国の調査が可能と見受けられた Dash Core Group. Inc.について、2022 年 12 月 10 日時点で調査を行ったところ、当社に在籍中としていた 39 名のうち、米国に居住するメンバが 7 名と最大であり、それ以降は人数が多い順にポーランド、タイ、ロシア、ベネズエラ、中国（ここまでが複数名のメンバが居住する国で後は 1 名のみ居住する国が 10 ヶ国以上存在した）と続いた。一つのサンプルではあるが、DAO を志向する取り組みにおいては特定の国・地域に法人を設立していても、人材の採用・巻き込みはグローバルに行われることが多い事を示唆しているように思われる

[103] 金融庁、株式会社クニエ合同研究「分散型金融システムのトラストチェーンにおける技術リスクに関する研究 研究結果報告書（概要版）」（令和 4 年 6 月）

同研究によると、各サービスの DAO におけるガバナンスの実態は以下の図表が示す通りであり、代表的な DeFi サービスであってもコミュニティのガバナンス参加が大きな課題であることがわかる。

図表 71　Uniswap、MakerDAO、Aave におけるガバナンスの実態

	Uniswap	MakerDAO	Aave
ガバナンストークン	UNI（保有アドレス：27.6万）	MKR（保有アドレス：8.3万）	AAVE（保有アドレス：10.6万）
コミュニティ	Uniswapコミュニティ（DAO）	Maker DAO	Aaveコミュニティ（DAO）
悪意のあるガバナンス提案の削除	詳細不明 ・ スマートコントラクト上は管理者による提案キャンセルが可能になっているが、提案キャンセル機能および実行できる管理者は定義されていない （緊急時は開発会社やコアユニットが実施することを想定か）		ガバナンス提案をキャンセル可能 ・ 悪意のある提案が行われた場合の対策として、ガバナンス投票の待機時間内に、選ばれた権限者（Guardian）がマルチシグ承認により提案をキャンセルすることが出来る
ガバナンス提案可決率（2021年実績）	・ スナップショット投票とガバナンス投票の2段階投票 ① スナップショット投票 投票2日間、定足数0.05%、50%以上賛成 ② ガバナンス投票 投票5日間、定足数4%、50%以上の賛成	・ 提案内容によりガバナンス投票とエグゼクティブ投票のどちらかを選択 A) ガバナンス投票（金額・利率や人選などスマートコントラクトの変更以外の方針等を決定） 投票7日間、定足数1%、50%以上の賛成 B) エグゼクティブ投票（スマートコントラクトの変更部分のみを決定） 投票30日間、定足数1%、50%以上の賛成	・ スナップショット投票とガバナンス投票の2段階投票 ① スナップショット投票 投票3日間、定足数50票、50%以上賛成 ② ガバナンス投票 ・ ショートタイムロック（ガバナンスに関連しない）投票3日間、定足数2%、50.5%以上の賛成 ・ ロングタイムロック（ガバナンスに影響する提案）投票10日間、定足数20%、57.5%以上の賛成
ガバナンス投票率（2021年実績）	約5-9%	約4-9%	約2-3%
ガバナンス提案可決率（2021年実績）	スナップショット投票77%（27/35件） ガバナンス投票86%（6/7件）	ガバナンス投票90%（275/307件） エグゼクティブ投票100%（47/47件）	ショートタイムロック88%（45/51件） ロングタイムロック50%（1/2件）

悪意のあるガバナンス提案への対応について、NFT 分野で先進的な取り組みを行っているとされる Nouns DAO では、（デジタル資産の章でも確認したように）NFT の発行・販売プロセスはスマートコントラクトで自動化・自律化を大胆に進めた一方、創業メンバが拒否権を有している等、ガバナンスは分散化を現時点で徹底できているわけではない。

図表 72　Nouns DAO の概要

コミュニティ名*1	Nouns DAO	コミュニティ参加者数*1	13,756名 （Nounは10月16日時点477個生成）
トークン	Noun （NFT保有者がコミュニティの投票権を持つ）	独自トークンがある場合の時価総額	-
コミュニティの目的	**オンチェーンアバターのコミュニティを形成するための実験的な取り組み** ✓ Nouns are an experimental attempt to improve the formation of on-chain avatar communities. While projects such as Cryptopunks have attempted to **bootstrap digital community and identity**, Nouns attempt to bootstrap **identity, community, governance, and a treasury that can be used by the community.** -当該コミュニティWebサイトの説明より		
詳細	✓ 詳細 • Nouns DAOはNounとよばれるアバターをランダムに生成し、24時間ごとに一体のNounをオークションにかけるプロセスを繰り返す • オークションの収益の100％はトレジャリーに保管され、Nouns DAOで使い道を決めていく • フルオンチェーンのNFTであり、CC0であることが開設時革新的である ✓ スロースタートガバナンス • 上記の通り、参加者が当初は少ない為に、個人的な利益のためトレジャリーを不当に引き出すといった提案が悪意を持って投票権の過半を持った参加者により行われる（若しくは投票権を買収される）リスクには弱く、**初期メンバーは提案に対する拒否権を持っている** • また、Noundersと呼ばれる初期メンバーたちには最初の5年間、10個発行されるごとに新たなNounが贈呈される Nounders向けNFT  2022年10月16日生成NFT  		

出所：*1Discordの参加者（最終アクセス2022年10月17日）その他はNounsのWebサイトからDeloitteが作成

（2） 社会貢献 DAO

経済圏の規模という金銭的な指標では測れない DAO の潜在的な価値を検討するため、社会貢献の要素がある非営利活動に取り組む DAO の事例もいくつか取り上げる。

まず、米国オースティン州が Web3.0 の先進地域として認知されることを目指す ATX DAO の事例を取り上げる。ATX DAO では特定のタスク実施に対して報酬として独自トークン REP トークンの付与を検討する他、地元アーティストらとの NFT 発行、独自トークン発行の検討等、地元コミュニティを醸成・盛り上げながら様々な活動を行っている。

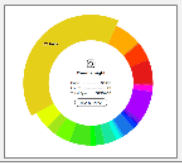
図表 73　ATX DAO の概要

コミュニティ名*1	ATX DAO	コミュニティ参加者数*1	1,545名
トークン	REP Token	独自トークンがある場合の時価総額	-
コミュニティの目的	**米国オースティン州がWeb3エコノミーをリードする都市として認知されるようにすること** ✓ ATX DAO is a **city DAO** working to build a cohesive network of crypto professionals and enthusiasts seeking **to push Austin to become a leading city in the Web3 economy.** We strive to enable artists and local businesses to participate in the crypto ecosystem and to educate the government about the benefits of Web3. -当該コミュニティWebサイトのMission Statementより		
詳細	✓ 詳細 • 米国オースティン州のWeb3エコノミーにおける立ち位置の向上を目指したCity Daoであり、暗号資産のプロフェッショナルや愛好家たちによって立ち上げられたと表記されている • タスクの実施によりREP Tokenが付与される ✓ 具体的な活動 • 2022年6月にオースティンで開催された大規模な仮想通貨カンファレンス"Consensus"にて、地元のアーティストと非営利団体とパートナーシップを組んでNFTを発行した。NFTの売り上げは、アーティスト・非営利団体・当該DAOのpublic arts fundに分配された*2 • 又、ロシアがウクライナに侵攻した当初、"♡Ukraine NFT"発行。ETHで寄付を行ったユーザーにNFTを発行した*3 		

出所：*1Discordのサーバー名と参加者（最終アクセス2022年10月9日）*2Globe News Wire「ATX DAO Partners With Artist ER, HOPE Campaign, and Native Hostel During Consensus "Keep Austin Web3" Event at Empire Control Room & Garage to Help Bring Local NFT Mural to Life」（最終アクセス2022年10月9日）
*3austonia「Texans answer Ukraine's call for crypto donations」（最終アクセス2022年10月9日）

Charity DAO の事例では、ガバナンスの分散性・透明性は不明である一方、寄付の募集・実行のスピード面でチャリティにおける DAO 活用の可能性が示されているといえる。

図表 74　Charity DAO の概要

コミュニティ名*1	DAO Charity	コミュニティ参加者数*1	-
トークン	-	独自トークンがある場合の時価総額	-
コミュニティの目的	**最新技術を使いウクライナの兵士や家族を助けること** ✓ To create an international community with one common goal: supporting displaced families across Ukraine and equipping the Armed Forces. ✓ We're global activists showing the true reality of the war and using modern tech (check out our NFTs!) for transparent, effective charity.. -当該コミュニティWebサイトのMission Statementより		
詳細	✓ 詳細 • 透明性に強くコミットしており、寄付されたすべての手段と支出内容を詳細にレポーティングしている ✓ 具体的な活動 • 最初の3か月だけで、820,000ドル以上の寄付を集め、ウクライナ軍、軍病院、ウクライナの家族への人道支援の3つの分野に分配された（これまでに1,000,000ドル以上の寄付を集めている） • 認知度の向上と寄付のさらなる募集に向けて、現在、NFT Charity を開発中。任意の寄付をすることで、ホワイトリストに加えられ、販売に関する情報を最初に知ることができる  		

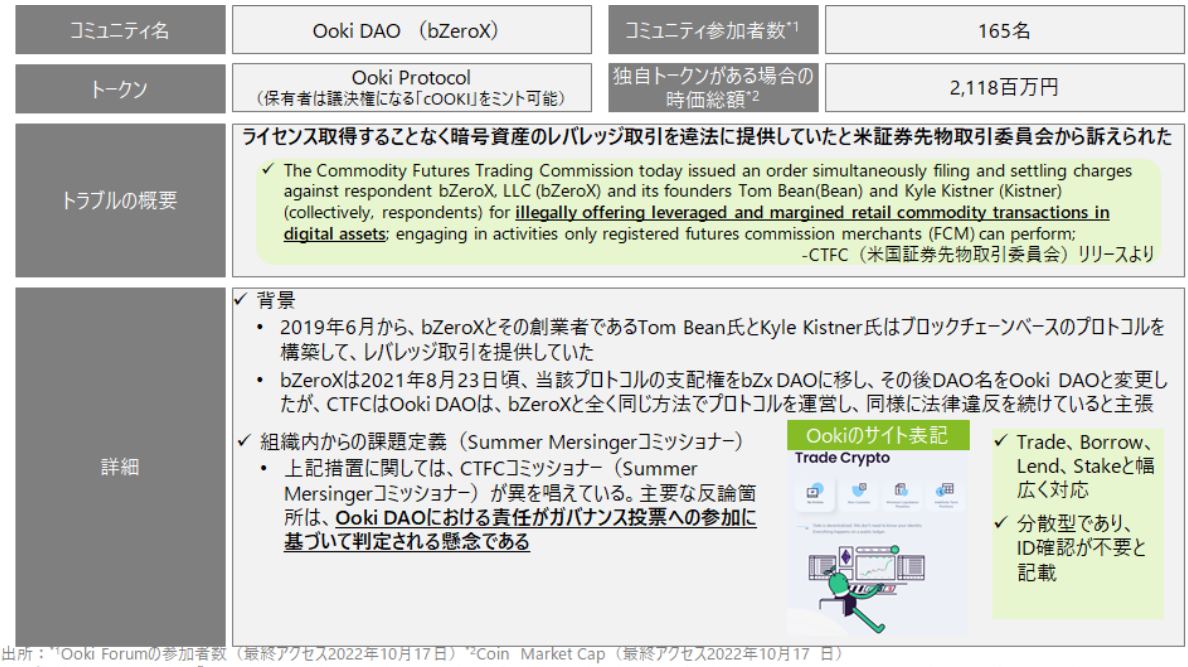
出所：Globe News Wire「DAO Charity Creating More Transparent, Effective Charity in Ukraine」（最終アクセス2022年10月9日）

（3） 訴訟等のリスクが顕在化した DAO

暗号資産デリバティブ取引サービスを開発・運営していた Ooki DAO の事例では、前身である bZeroX の創業メンバが米国 CFTC にライセンスを取得せずに事業を違法に行っていたとして訴追された他、その責がガバナンスに参加したガバナンストークンホルダーにまで求められた。後者についてはその後の CFTC 委員の声明により否定的な見解が示される等、規制当局としても統一的な方針を検討中であることが明らかとなった。

これにより、DAO が金融規制の回避に悪用される恐れがあること、DAO のガバナンス投票に参加することで参加者個人にまで DAO の活動の責任が及ぶ可能性があることが示された。

図表 75　Ooki DAO（bZeroX）の概要



出所：*1Ooki Forumの参加者数（最終アクセス2022年10月17日）*2Coin Market Cap（最終アクセス2022年10月17 日）
*3Skkaden Foundation「CFTC Settles Claims Against Founders of a Decentralized Protocol and Sues Its Successor DAO and Its Members, Pressing a Novel Theory of Liability」（最終アクセス2022年10月17 日）その他CTFC公式サイトよりDTC作成

また、The DAO の事例では、ハッキング攻撃による資金流出への対応として 2016 年にイーサリアムのハードフォークが行われ、イーサリアムの分散性の在り方が議論された。また、2017 年には SEC が The DAO のガバナンストークンが証券に該当するため、当時行われた ICO が未登録証券の販売にあたるとするレポートを公表[104]した。

資金は回収されたが、多くの DAO のメインネットであるイーサリアム自体が真に非中央集権の仕組みを構築出来ているのかという課題が提起された。

[104] https://www.sec.gov/litigation/investreport/34-81207.pdf

図表 76　The DAO の概要

コミュニティ名	The DAO
トラブルの概要	**Split機能（後述）を悪用され、ETHが盗まれるリスクに瀕した**
詳細	✓ 前提（The DAOの仕組み） • The Daoは、イーサリアムのプラットフォーム上でスマートコントラクトを利用し、分散型投資ファンドを構築することを目的としたプロジェクトであった • 具体的な投資のサイクルを簡潔にまとめると、①メンバーが投資先の提案を行う、②キュレーター（DAO保有者の中から投票により選定）が提案情報を精査し、問題なければホワイトリストに登録する、③DAO保有者が議論、投票後出資へとすすむ • The Daoに出資した資金をThe Daoの資金プールからETHに変換し移動し、28日後に引き出すことが出来る"Split機能"により投資に賛成しがたい参加者の資金を保全することを目指していた ✓ トラブルの詳細 • **The Daoのプログラムコード**の脆弱性がハッカーにより明らかになり（Split機能は資金の移動が完了する前に何度も短時間で処理を行うと資金がないのに繰り返すことができてしまうというバグがあった）、The Daoが保管する資金を別のアドレスへ移動させられてしまった（他の参加者が同じ方法で残りのDAOを別のアドレスへ避難させたため、総資金の約3分の1は保守できた） • 28日間のタイムリミットの中で対応が協議されたが、結局はイーサリアムのブロックチェーン上の記録を遡り、ハッキングされた取引自体を無効化するハードフォークという手法がとられた（イーサリアムのコミュニティ参加者のうち半数以上の賛成が条件であった） • ハッカーから資金を取り戻すことは出来たものの、**非中央集権の仕組みをアピールするイーサリアムが中央集権的にハードフォークを実行したことには、イーサリアム自体の非中央集権の仕組みに疑義が生じる結果となった**

（4） ワイオミング州で登記された DAO

米国ワイオミング州では 2021 年 7 月に新たな法律[105]を施行し、DAO を LLC（Limited Liability Company）の一種として登記できる制度を整えた。その概要については後述するが、以下図表に示すように、様々な活動を志向する DAO が同制度によりワイオミング州で登記されており、有限責任、パススルー課税、土地等の資産を法人として保有できるといったメリットを享受しているものと考えられる。

図表 77　ワイオミング州で登記された DAO の一例

#	事例	DAOの概要
1	Fries DAO	• Fries DAOファストフード店の買収が目標。当初はDAOとNFTでマクドナルドを買収するというジョークから始まったが、**実際に5.4百万ドルが集まったことから、実証を目指すことになった** • 実際の所有権ではなく、店舗購入者に対してステーブルコインを提供し、意思決定に関与しながら資金回収を行う手法を模索している模様
2	Kitchen Lands DAO ※Telos Kitchen DAO	• Telos Kitchen DAOは分散型コミュニティのグロースを企図しTelos blockchainを提供。 実際にKitchen Lands DAOを設立し、**土地を購入する等の実務を行う等自らが実証を行っている**
3	American CryptoFed DAO	• インフレ/デフレ/取引コストゼロの通貨システムをミッションとして掲げ、イオス（EOS）を基盤とした手数料なしの取引を実現するためのステーブルコイン「Ducat」を広めている
4	BLOCKS DAO	• Verified by BLOCKS (VbB、デジタル及び物理的なアセットの安全な取引、追跡、決済に利用できる)等のソリューションを提供するDAO
5	Elo DAO	• De-FI（債権）を提供し、クリプトの流動性リスクを下げることを目的としたDAO

✓ Digital asset stakeholders made it clear to us they were concerned about facing general partnership liability in the absence of a well-defined corporate structure. Our DAO LLC legislation should dispel that concern

Chris Rothfuss ワイオミング州上院議員*1

出所：THE BLOCK「Wyoming 'DAO law' to go into effect in July after receiving final approval」（最終閲覧2022年10月24）

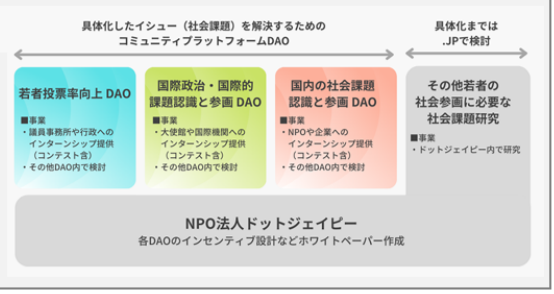
105 https://www.wyoleg.gov/Legislation/2021/SF0038

（5） 日本発の DAO・関連事業者

事例調査に加えて、日本発の DAO・関連事業者へのヒアリングを行い、日本特有の事情を踏まえた課題意識や今後求められる対応に関する意見交換を実施した。

まず、若年投票率の向上を目指す NPO 法人であるドットジェイピーによる DAO 活用の検討を取り上げる。以下の図表に示すように、人材リソースや認知度の不足を補いながら、成果が出てきている若年投票率向上の取り組みのスケールアップを狙いとした活動の DAO 化であり、事業運営に必要な経費を賄う目的で使用できるトークンの付与も検討されている。

図表 78　NPO 法人ドットジェイピーの DAO 化に向けた取り組み

コミュニティ名	特定非営利活動法人ドットジェイピー
団体概要	**若年投票率の向上を目標に活動するNPO法人** ✓ ドットジェイピーは、若年投票率の向上を目標に活動するNPO法人です。全国35拠点で約660人の大学生スタッフが中心となり、春期（2月～3月）と夏期（8月～9月）の年2回、学生を対象としたインターンシッププログラム（議員・グローバル・NPO）を提供し、また若年層向け政策コンテストを実施しています。 -当該団体のWebサイトの団体概要より
詳細	✓ 詳細 • **非営利組織をDAOへ移行**させ、組織活動を促進するためのDAO化プロジェクトを開始 • プロジェクトを支援するガイアックスニュースリリースによると、「社員だけによるPF運営」から、「ユーザーや社外の協力者も巻き込み、一体となったPF運営」という取り組みを通じて、主に**NPO法人などの非営利組織が抱える人材リソース不足**、**PRやマーケティング不足**を補いながら、社会認知を獲得し、社会課題の改善・解決のスピードを飛躍的に向上させたい意向とのこと ✓ 具体的な活動 • 22年末までに大学生スタッフ700人にトークンを発行し、組織内におけるインセンティブの仕組みを設計する予定 （トークンは事業運営に必要な書籍購入費、交通費などとして消費できるようにする想定） • 2024年3月までに外部へ公開し、具体化した社会課題を解決するためのコミュニティをオープンなDAOとして組成することを目指す 

詳細なヒアリング内容は以下の通り。

図表 79　NPO 法人ドットジェイピーのヒアリング結果

ヒアリング項目	回答
DAO 化に期待すること	【背景】 ■ 前提として、NPO 法人ドットジェイピーの最上位目標は**若年層の投票率の向上**を図ることにある ■ その事業を継続して実施する為の経済基盤を確保する為に、事業型 NPO として受け入れ先（議員事務所）や会員等から費用を頂く仕組みになっている ■ 1998 年に当初 1 人で創業した後、25 年間で 700 人の運営スタッフを抱えるまで（インターン生は年間 4,000 人程度受入）組織は右肩上がりに成長している。他方で、日本国内の若年層の投票率は横ばいに推移している。**個別単体の団体の成長の延長に社会課題の解決は無いとの仮説を持っている。**世界的に見てもこの仮説を反証する事例を見出すのは難しいと考え、現状と異なるアプローチを長らく考え続けてきた

	【DAO への期待】 ■ これまでの取り組みから、インターンを経験した学生の投票率が上がることは検証済みであり、あとはどのように参加者を増やしていくが論点であった ■ 上記の最上位目標に対するエンドゲーム（達成）のアプローチとして、所属する組織の垣根を問わず、若年層の投票率向上を目指す DAO が有用だと考えるに至った ■ NPO 自体が実行主体だけでなく、市民・国民を巻き込む仲介役・運動体としての役割も期待されていた筈である
検討のきっかけ	■ 元々保有しているリレーションから、Web3 の流行を良く聞くようになった ■ 当初は NPO への応用は想定していなかったが、理解を深めるにつれて DAO を社会的なアプローチで捉えるようになった ■ NPO やソーシャルビジネスはそもそも目標が明確であり、同一の目標に共感する個人が集っていることから、インセンティブが加わればまさに DAO だとの考えを深めるに至った
DAO 化に向けた懸念点	【懸念点】 ■ 懸念点は主に二つある ■ **権限を外部開放することに対する懸念**：本当に外部に（権限を）開放して組織が重要にしてきた文化等が失われないかを懸念している ■ **クリプトに対する世間の理解に対する懸念**：暗号資産価格の乱高下や、DeFi の不祥事に関する報道によって学生運営スタッフの親族から理解を得ることができるかも懸念している ■ 1 点目の懸念に関しては、フェーズを踏むことで解消を図りたいと考えている 1. 既存組織の DAO 化（社内の様々なパーミッションを不要としていく） 2. 既存組織の外部開放 ■ 上記フェーズを進めるにあたっても、インセンティブ設計には苦慮している。**プロフィットセンターにおけるインセンティブ設計**（例えば、インターン生の獲得と受け入れ先の獲得）**は比較的容易だが**、**コストセンター**（例えば、経理作業や事務所の清掃等）**のインセンティブ設計は非常に難しい**と考えている ■ 又、現状 NPO 法人ドッドジェイピーではチーム単位で様々な活動を行っていることから、それ（チームとしての結果）を個人のリワードにどう結び付けるかも論点だと考えている 【参考：懸念点の解消に積極的に取り組むメリット】 ■ 上記懸念点の裏返しともいえるが、積極的に解決策を考え実行していくメリットもある ■ ファーストペンギンとしてチャレンジングな取り組みを行うことで、知名度向上に役立ったこと ■ クリプトに対する目新しさもあり、運営スタッフのモチベーション向上が見込めること（但し、この状況（=目新しさ）は長くは続かないと考える）
DAO 設計の考え方	【目的の解像度】

	■ DAO が解消すべき課題は「世界平和」「若者の社会参画」のように**抽象度高く設定してしまうと熱狂を生みづらい**（=参加の必然性を減らしてしまう）為、課題を具体化したうえでパーパスごとに DAO を分けていくべきだと考えている 【DAO と NPO の関係性（仮説）】 ■ 現状、NPO 法人は二つのことを行う必要がある。例えばホームレス支援で食事の提供等を行う場合を想定する場合であれば、受益者（この場合はホームレス）に食事を提供しても金銭は得られない為、寄付を行う支援者を見つける必要がある ■ NPO 法人と DAO の関係性の仮説としては、支援者の**意思決定を株主総会のように DAO が行い**、**執行機能を NPO 法人が担う形**が現実的だと考えている。その背景には、執行機能に求められるスピード感に DAO の全員参画型の意思決定がついてこれるかという懸念が存在する。とはいえ、最終的には執行機能の DAO 化も目指していきたいところではある
行政への期待	【非営利団体としての課題】 ■ **そもそも非営利団体は資本調達手段に制限が多い**（エクイティファイナンスができない、一部を除いて社債も発行できないなど）故に、大きな助成金や寄付に頼らざるを得ない点がある ■ NPO 法人の議決権付き寄付は PST[106]に算入できない為、その点も課題になると感じている 【営利/非営利共に抱える課題】 ■ 下記の二点は非営利団体に限らず、既に多くの場所で議論がなされている理解だが、DAO の活用を目指すうえでは課題になることと認識している 1. 自社発行暗号資産が期末時価評価課税の対象となること 2. （そもそもの）暗号資産発行に当たって取引業登録が必要になること 【法人格の付与の要否】 ■ DAO を構成するトークンホルダーの無限責任問題を回避することは重要だと認識しているが、NPO 法人ドットジェイピーとして DAO への法人格付与に対する必要性は、現時点で感じていない 【その他行政によるガイダンスの要否】 ■ すべての DAO 参加者の動機が投資目的とは限らないので、主に投資家保護を目的とした行政による過度な介入、ルール策定には懐疑的であり、慎重な議論を求めたい

[106] パブリックサポートテストの略。NPO 法人の活動が広く市民からの支援を受けているかを判断する基準であり、NPO 法人へ寄付した人が税控除を受けるために必要な要件

次に、ブロックチェーン基盤である Astar Network[107]を構築する Stake Technologies Pte Ltd[108]とその雇用面での支援を行う WorkDAO[109]に対してヒアリングを行った際の内容を以下図表に整理する。特に、Astar Network に対しては自身の取り組みにおける DAO の位置づけや課題意識、WorkDAO については様々な DAO の活動をサポートしている立場から俯瞰した観点での DAO を活用することの課題意識をヒアリングした。

図表 80　Astar Network のヒアリング結果

ヒアリング項目	回答
DAO 化に期待すること	■ コア法人を解散する時に責任を負う主体の代替として DAO を法人化する必要があると考えている ■ 日本で法制度があれば何よりだし、現時点であればワイオミング州 DAO 法やスイス等でのファウンデーションが選択肢になり得る
DAO 化に向けた懸念点	■ コアメンバやトークン保有者が**無限責任を負う可能性が排除できない事はリスク**に感じる。法的なリスクに殊更懸念を抱いている人は多くないと思うが、制度が定まっていない事は共通認識であり、**グレーゾーンのやりづらさ**はあるので制度整備されると DAO を用いた取り組みがしやすくなると思う ■ 意思決定に関わる時だけトークンを入手する事ができるため、突然参加者が 2 倍にもなるような投票を根拠としてガバナンスしていく難しさがある ■ 19 ヶ国にメンバがいるため、**現地法令に沿った雇用**を検討する難しさがあった （WorkDAO がサポートしている）
DAO 設計の考え方	■ DAO は D/A/O のうち **Autonomous が肝心**。トークンによる動機づけ等で様々なメンバがオンラインで自発的に活動参加する仕組みが必要 ■ 動機にはトークンによるものと個々人のパッションがあり、現時点では多くのトークン保有者が投資目的で関わっており、実質的に意思決定をコアメンバ中心に行っている状況
行政への期待	【法人格】 ■ 個人が**無限責任を負わずに済む仕組みはマストではないがあると良い**。法人の代表が住所を公開する事はかなりのリスクを伴う（なお、シンガポールではこうした要件は無い）ため、これが KYC 済アドレスに代わるのは良いと思う ■ 法人格がある事で NFT での IP 等の**知的財産権**や大手企業との協働での**法人契約締結**等、活動の幅が広がる 【自社発行以外トークンの期末時価課税の見直し】 ■ DAO 同士でのコラボレーション（トークンの持ち合いやグラント）や DAO が日本拠点を検討する際のハードルになってしまうため、自社発行トークンと同様に早期に見直しされるのが望ましい

[107] https://astar.network/
[108] https://stake.co.jp/
[109] https://www.theworkdao.com/

図表 81　WorkDAO のヒアリング結果

ヒアリング項目	回答
DAO 化に向けた懸念点	■ DAO に法人格は不要とする向きもあるが、**メンバの雇用に法人格が必要**、**訴訟時に無限責任のリスクが生じる**、等の理由から、法人格は真剣に検討すべき論点と考える ■ bZeroX/Ooki DAO の訴追時に、司法省は投票内容如何によらず投票参加者が法令潜脱の責を負うべきとし、その後司法省の取り調べに協力すべきかというガバナンス投票に対して皆が恐れをなしたため誰も投票しなかった事例があった ■ コミュニティの中にコア法人を設けたとしても、コア法人の責任範囲を超える事象に対してコミュニティメンバの責任が問われる可能性が残る状況には変わりない ■ 規制への準拠や株主等既存の法人の構成員とトークン保有者の棲み分けの検討等、法人格を定義する事で生じる課題や論点もある
DAO 設計の考え方	■ DAO は （1） 法的枠組み （2） DAO の参加者の DAO に対する認知 の 2 つの観点があり、（1）において法人格の有無で 2 パターンに分かれるのが議論の出発点と考える ■ 米国で現在弁護士が推奨する形態は、ワイオミング州で UNA（Unincorporated Nonprofitable Association）として DAO を定義する事ではないか ■ **ワイオミング州の DAO LLC はトークン保有者の登録というハードルがあり、グローバルに自由な参加を旨とする DAO の実情には合っていない**と思うが、DAO に対する当局の前向きな姿勢は将来の制度改正に期待できるといった実益があると思う。米国では UNA でも有限責任であり、先述の懸念には対応できると思われる
行政の期待	■ 合同会社を基に定款に記載する社員情報を KYC 済アドレスで代替する事は、法人格を定義しないと無限責任のリスクが残る日本において可能性のある施策と思う ■ DAO は拡大する過程で非常に多くの国からトークンを入手して参加する人が集まるため、**KYC を要件とする事でどこまでグローバルに自由な参加を担保できるのか**は十分に検討する必要があると思う

最後に、Web3.0 分野のアクセラレータとして様々な Web3.0 事業の支援を行っている Fraction Ventures 株式会社[110]に対して、同社がサポートする DAO 及び関連事業者の事例を踏まえた俯瞰した見方からの DAO への課題意識、並びに、当社が共同で取り組む音楽系 DAO である FRIENDSHIP.DAO[111]固有の課題意識の 2 種類のヒアリングを実施した。以下の図表にそれぞれの結果を整理する。

[110] https://fracton.ventures/

[111] https://www.friendshipdao.xyz/

図表 82　Fracton Ventures のヒアリング結果（DAO 一般）

ヒアリング項目	回答
DAO 化に期待すること	■ DAO の定義は特に制限していないが、しいて言うなら**ヒト・モノ等の新たな形でのコーディネーションの仕掛け**と位置づける例が多いとみている ■ DAO は法人格を持つエンティティも関わり得るコミュニティと捉える方が自然で、特定のエンティティとしてひとまとめにして法人格の有無を検討するのが難しい存在のようにも感じる ■ ブロックチェーンにより Transparent/Programmable といった特徴がある事が本来の定義に近いが、コミュニティドリブンなものを DAO と呼ぶ向きもあり、定義にある程度揺らぎがあると思う ■ DAO が何を目指しているのか、DAO にする事で何を期待するのか、を仕分けする事が法人格の要否を検討するインプットになるのではないか ■ プロトコル収益や独自トークンといった資産を有する場合に、法人がそれを保有する主体の選択肢となりうるため、**投資 DAO はこうした議論の対象になりうるかもしれない**
DAO 化に向けた懸念点	■ 分散化が非常に難しい ■ 本当にグローバルで多様な人を巻き込む事にはハードルがある ■ 分散するほど、誰かのコントロールの範囲を超えて予期せぬ事が起こる ■ トークンを発行する事が前提あるいは出口となっているが、本当にそれで良いのか、業界として試行錯誤が必要である
行政への期待	【法人格の有無】 ■ 法人格を必要とする事例はあまり無い認識だが、投資 DAO では検討の余地がある等、DAO の用途に合わせた検討が必要である ■ 有限責任: MakerDAO では財団が解散される際に、以降はトークンを持つ個々人が無限責任を負う可能性があるのではとの指摘・議論があったが、その後は他の事例でも特に耳にしない ■ 資産の所有: 先述の通り、DAO で保有する資産の所在を考える上で法人は有力な選択肢であり、投資 DAO でニーズがあるかもしれないが、その他は特に法人格の必要性は議論されていない認識 ■ 参加のハードル （パーミッションレス性）: 真にパーミッションレスな DAO の場合は、様々な国の人が参加する DAO を特定の国の法律で定義する事にどのような意義と効果があるのか不明瞭になる。コンソーシアム的な特徴を持つより閉じたパーミッションド型の DAO の方が趣旨に沿うのかもしれない 【ワイオミング州 DAO 法について】 ■ あまり身の回りで当該制度を用いた事例は耳にしない。先述の通り、法人格を欲する DAO の類型が投資 DAO くらいに限られており、また投資に関する取り組みであれば既にデラウェア州が候補としてあった。ワイオミング州の姿勢を示すには良い一方で実益は大きくはなかったといえるのではないか 【その他の論点】

	■ Web3 VC に企業が LP 出資する時に、VC は資産を USDC やその他暗号資産で保有する等、評価額にブレが生じうるため、その損益評価や開示手続きが必要以上の負担にならない事が望ましい ■ Exit 前の起業家が持つ自社株が、必ずしも客観的な評価ができる金融資産とは言えない一方、出国税 （1 億円以上の有価証券） の対象となってしまい、現金化も難しいためグローバルな事業展開の障害となってしまう事例がある認識。何らかの措置があると良いのではないか

図表 83　FRIENDSHIP.DAO のヒアリング結果（FRIENDSHIP.DAO）

ヒアリング項目	回答
DAO 化に期待すること	■ アーディストの音楽配信を支援するサービス Friendship からの拡張として検討。元来、apple music、Spotify などのサブスクリプションへのミュージシャンの参画をサポートしているが、サービスの肝はキュレーターが介在している点。良いキュレーターをより呼び込む為に**コミュニティに対しての貢献をより還元する仕組みが必要だという考えから DAO を検討するに至った**（キュレーターに加えてイベンターやミュージシャンのジャケットを手掛ける写真家等も対象） ■ 旧来と比較して有名な（=ヒーロー視される）キュレーターが業界に少なくなってきている点に課題意識を持っており、ヒーロー視されるキュレーターを増やしたいという思いもあった
DAO 化に向けた懸念点	■ リテラシー: 関係者が Web3（DAO）を使いこなせるかという課題（そもそも、Web3 に興味がある方が対象ではなく音楽関係者が対象の為、アプリケーションのインターフェースの工夫や、勉強会実施などで対応している　※勉強会実施の前提となる対人関係はすでにある） ■ トークンの取り扱い: コミュニティへの貢献を表すものを用意したいが規制面もある為この対応を考えている ■ グローバル対応: そもそもブロックチェーンを使う 1 つの理由は、グローバルにコミュニティを広げることである。そのコミュニティ・ビルディングをどう進めていくかが課題だと考えている。キュレーターとしての活動参加には peer review による審査が必要 ■ FTX の事件もあり、Web3 やトークンといったワードがつく取り組みに対して、世の中からの第一印象が悪化していると感じている
DAO 設計の考え方	■ 動機づけのためのトークン発行は検討しておらず、メンバーシップ NFT を SBT 的に用いて貢献に対するクレジットを貯めて施設利用等のメリットを享受できる仕組みを考えている
行政への期待	■ 適切な規制や、それが難しい場合には”こういったことは行っても問題ない”といったガイドラインがあると良い ■ DAO の多様性故に、現段階で日本に於いて一律のルールを作るのは現状難しいのではないかと考える。故に、（地域行政が各々行うよりも）**中央省庁においてサンドボックス的に行政と共同で DAO を試し、ルール作りのための実験ができる場**があると良いのでは。**様々な省庁の窓口も一貫して対応頂ける体制があると良い**

（6） DAO の活用における課題

以上の事例調査において、DAO の活用における様々な課題が言及された。DAO の活動が持続可能な形で運営されるための要素を、ビジネスモデル、コミュニティ、ガバナンスと大別すると、確認された課題の分類は以下の図表のようになると考えられる。

図表 84　調査において確認された DAO 活用の課題

カテゴリ	概要	課題
ビジネスモデル	■ 持続可能な活動とするために資金等のリソースを循環させるビジネスモデルが必要である	■ (一部分野で高い時価総額を誇るトークンを扱う DAO が存在するがビジネスモデルは営利・非営利いずれの場合も試行錯誤の途上)
コミュニティ	■ 参加者の人数、モチベーション、リテラシーの観点で質の高いコミュニティを築く必要がある	■ ガバナンス投票の参加率が限定的 ■ 提案の内容(例: コードの一部修正)が十分に吟味されるとは限らない
ガバナンス	■ 意思決定やオペレーションの際どの程度分散性を保ちながら運営の質を担保できるか	■ ガバナンス投票の定足数が限定的 ■ 悪意ある提案を検証する役割が不明確な場合がある ■ 規制逃れのために DAO が活用されるケースがある ■ 悪意ある参加者にガバナンス投票制度を悪用される恐れがある ■ 悪意ある参加者・提案に対して拒否権等の対抗策を取ると DAO の特徴の一つである分散性が損なわれる恐れがある ■ インフラであるブロックチェーン自体の分散性にも疑義が残るケースがある

3－4. スマートコントラクトの法的位置づけ整理

（1） スマートコントラクトの法的位置づけ

スマートコントラクトは、「コントラクト」と呼称されているものの、法的意味における契約とは異なり、事前に合意された契約内容に従って自動的に債権債務の履行・執行するプロトコルという整理になると思われる。

他方、実際の契約における故意や過失等の評価を伴う要件についてはプロトコルで一義的に定められるものではなく、また、プロトコルの内容次第では自動で執行されると消費者保護法や公序良俗に反する結果となる場合等もあり得る。加えて、外部から誤ったデータ等が入力された場合に本来意図していない結果が出力される可能性があるなどの問題もあり、これらを踏まえるとスマートコントラクトを実際の契約に活用するには依然課題が残る。

例えば DeFi 等のサービスにおけるスマートコントラクトについても、そのプロトコル自体は契約を構成せず、あくまで契約によって合意された内容を執行するものという整理は変わらないと考えられる。

（2） DAO の構成員内で紛争が生じた場合の法的解決方法

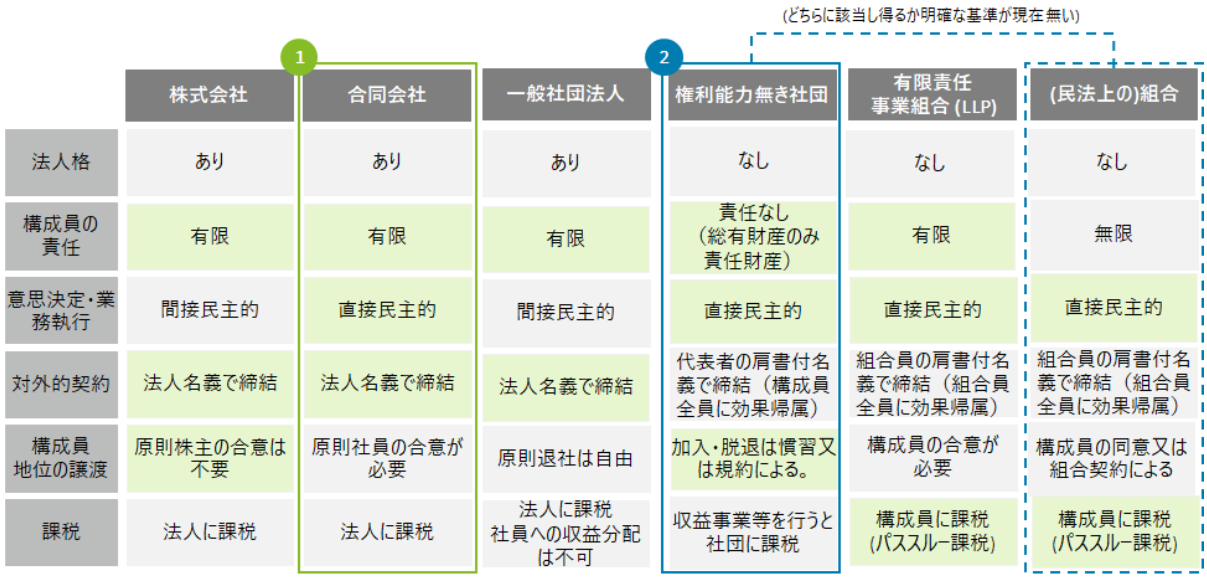
スマートコントラクトを活用した DAO 内で紛争が生じた場合の準拠法や裁判管轄についてはスマートコントラクト特有の論点ではなく、匿名の構成員が国境を跨いで散在する組織における紛争と同様の論点になると理解しており、個別具体的に判断すべきものと考えられる。

3－5. 日本における各種団体の法的位置づけと DAO への適合度

この節では、DAO に適合し得る日本における各種団体の特徴と、DAO に当てはめた際の課題について検討する。

日本においては DAO の活動は合同会社、あるいは権利能力無き社団として整理することが可能であると思われる。

図表 85　日本における各種団体の特徴



一方で、それぞれへの当てはめには以下に示すような課題がある。

図表 86　合同会社・権利能力無き社団の課題

現行制度下での団体	DAOに当てはめる際の課題
1 合同会社	• 定款等に社員の氏名・住所を明記しなければならない • 社員地位の譲渡に社員の合意が必要である(定款に定める事で合意を不要としてトークン譲渡と社員地位の譲渡を関連付ける事は一般に可能)
2 権利能力無き社団	• 構成員が無限責任を負う民法上の組合との明確な線引きが現在無い • 法人格が無いため、社団としては以下の事ができないと思われる ➢ 契約締結 ➢ 資産の所有 ➢ 銀行口座の開設 ➢ 事業免許の取得

3－6. DAO の規制調査・法的位置づけ整理

この節では、海外において DAO に適用し得る代表的な法制度を調査した。具体的には、2021年 7 月に施工されたワイオミング州 DAO 法、スイスにおける Charitable Foundation、ケイマン諸島における Foundation の概要をそれぞれ以下に示す図表に整理した。

図表 87 ワイオミング州 DAO 法の概要

項目	整理
DAO 法の位置づけ	■ いわゆる DAO 法は、ワイオミング州法第 17 編（Corporations, Partnerships and Associations）に新設された第 31 章（Decentralized Autonomous Organization Supplement）に基づく DAO に関する規律をいう ■ DAO 法において、「DAO」とは、「この章の規定に基づき設立された有限責任会社」と定義されている ■ DAO 法はワイオミング州有限責任会社法（Wyoming Limited Liability Company Act）の特則という位置づけであり、ワイオミング州有限責任会社法は、DAO 法の規定と矛盾しない範囲で DAO に適用される
DAO の設立要件	■ DAO 法に基づく DAO として設立するための要件はワイオミング州法第 17 章第 31 編 104 条以下に規定されており、例えば、定款には下記の事項を記載することが定められている （i） DAO である旨 （ii） DAO が通常の有限責任会社と異なり持分権者の信任義務や保有する権利の処分、脱退などについて一定の制限が課され得るという趣旨が記載された定型文言 （iii） DAO の管理、促進、運営に直接使用されるスマートコントラクトの識別子 （iv） DAO がどの程度までアルゴリズムに従って運営が実行されるのかを含め、参加者によってどのような運営がされるのかについての事項 （v） 参加者の権利義務や DAO の活動内容、脱退、解散前の配当、定款変更などの DAO に関連する事項 ■ DAO の名称には、「DAO」、「LAO」又は「DAO LLC」のいずれかを入れる必要がある ■ DAO の設立は、定款を州長官に提出することにより行うこととされており、組合員が 1 名であっても設立可能
DAO の登録手続き	■ DAO を法人として登録するためにはオンラインで必要な情報を入力・提出し、又は紙のフォームを提出することによって行う必要がある ■ 登録者がワイオミング州に居住している必要はないが、登録のためには、ワイオミング州に住所を有するなど一定の要件を満たした登録代理人（"registered agent"）が必要 ■ 外国の DAO を DAO 法における DAO として登録することは認められない

メンバの権利義務	■ メンバは信義誠実義務を負う一方で、信任義務（"fiduciary duty"）は負わない ■ オープンブロックチェーンにおいて公表されている限り、メンバは財務書類等の閲覧請求権を有しない
メンバの脱退	■ メンバの脱退に係る条件や手続きは定款、スマートコントラクト又は運営契約に定められる ■ これらに特段の規定がない場合、メンバが自身の持分権、議決権、又は経済的権利の元となる財産をすべて譲渡したときに脱退する
DAO の解散	■ DAO の解散事由は以下のとおり （i） DAO の存続期間が満了した場合 （ii） メンバの過半数による決議があった場合 （iii） スマートコントラクト、定款又は運営契約で規定された解散事由が生じた場合 （iv） 1 年間、DAO が何らの提案も承認せず、又は活動を行わなかった場合 （v） DAO が適法な事業目的を有しなくなった場合又は自然人のメンバが 1 名もいなくなった場合 （vi） DAO のすべてのメンバが脱退した場合

図表 88　スイスの Charitable Foundation 概要

項目	整理
根拠法令	■ スイス民法典 Swiss Civil Code （以下「 SCC」という。） ））第 3 章（第 80 条～第 89 条）
法人格	■ 法人格あり。財団の法人格は、商業登記によって付与される
財団の責任	■ 法律上、具体的に定められてはいないものの、契約の結果について責任を負う
財団の設立	■ 財団は、特定の目的のために公的証書又は遺言により資産を寄贈 することによって設立される ■ 財団の意思決定機関や運営方法については、設立趣意書（charter）により規定される。 かかる意思決定機関は、財団の代表権を有する
財団の機関	■ 財団は理事会を設置しなければならない ■ 財団は意思決定機関を設置しなければならない ■ 財団の理事会は、監督当局から免除されない限り外部監査人を任命しなければならない
財団に対する監督	■ 財団が法的に定めた所在地に所在していないこと 等が認められる場合、監督機関は以下の措置等をしなければならない ■ 財団が法的に要求される状況を回復するための期限の設定 ■ 不足している機関または管理者の任命 ■ 財団が効果的に組織できていない場合、監督機関は、財団の資産を可能な限り類似した目的を持つ他の財団に譲渡し、財団は当該譲渡等の措置に要する費用を負担する ■ 財団は財務状況に関して監督機関による監督を受ける

	■ 監督機関は財団の資産を保全し、その目的遂行の保護に緊急の必要がある場合、理事会の意見を聴取して財団の機関を変更できる
財団の解散	■ 監督機関は次の場合に申し立てによりまたはみずからの判断に基づき財団を解散させる ■ 財団の目的が達成不能となり設立趣意書を変更しても財団を維持できなくなった場合 ■ 財団の目的が違法または公序良俗違反となった場合 ■ 財団の利害関係者は財団の解散を求め、申し立てまたは訴えの提起をすることができる

図表 89　ケイマンの Foundation 概要

項目	整理
根拠法令	■ ケイマン諸島財団会社法（the Cayman Islands Foundation Companies Law, 2017）
法人格	■ 法人格あり。また有限責任となる
財団会社の主な設立要件	■ 株式又は保証によって責任が制限されていること （株式資本の有無は問わない） ■ 基本定款に以下の記載がなされていること （i）会社が財団会社である旨 （ii）一般的又は具体的な会社の目的 （iii）解散時の会社の解散時に有する余剰資産の処分につき基本定款に直接記載又は 附属定款を参照すること （iv）社員に対する配当又はその他の利益・資産の分配の禁止 ■ 附属定款を採択していること ■ 秘書役がケイマン諸島管理法の有資格者であること
財団会社の特徴	■ 財団会社の社印ではないが基本定款に基づいて財団会社の総会等に出席し、議決検討を行使できる「監査人」が存在する ■ 財団会社は基本定款に別段の定めがない限り、定款の下の義務は財団会社のみに課され、財団会社の受益者は財団会社、その経営者または資産に関する所有権または権利を有しておらず、利害関係者に該当しない ■ 基本定款において会員、取締役、役員、監督者、設立者その他の者に対して財団会社に関するいかなる権利義務を与えられる
財団会社の構成	■ 財団会社の構成員は取締役、監査人、秘書役 ■ 基本定款にその旨を記載し、一人以上の監査人を備えることで財団会社は社員を不要とする事ができる ■ 社員資格および監査人資格は当人の死亡または財団会社に対する退社の通知等で喪失することが想定されている ■ 財団法人は登録事務所に監査人の氏名および住所等を記載した登記簿を備えなければならない

3－7. 日本における DAO の法人格の検討

先に見たように、日本において DAO は合同会社あるいは権利能力無き社団が適用し得る団体として考えられるが、いずれにおいても課題があった。合同会社は定款等に社員の氏名・住所を記載する必要があり、権利能力無き社団は無限責任を負わされる民法上の組合との明確な区別の基準が無く、また法人格が無いことから契約の締結といった法人としての活動ができない。

この時、合同会社の社員の定義を一定量以上のトークンの保有等、ガバナントークンに基づく方式にした上で、定款等に記載する社員の氏名・住所の情報を、KYC 済みのアドレスに置き換えることができれば、DAO に法人格を与えつつ、DAO の主要参加者のプライバシー・匿名性に配慮しながら、DAO のコアメンバの取引状況が透明化され、オンチェーンデータを生かした決算・監査対応の効率化といったメリットが期待できると思われる。

一方、アドレスの KYC 情報を別途管理する必要がある他、KYC を DAO の構成員の要件とすることが、グローバルに自由な参加を旨とする DAO の在り方を妨げないような KYC プロセスを検討する必要がある。

図表 90　日本における DAO の法人格の一案イメージ

	株式会社	合同会社	一般社団法人	権利能力無き社団	有限責任事業組合 (LLP)	(民法上の)組合
法人格	あり	あり	あり	なし	なし	なし
構成員の責任	有限	有限	有限	責任なし（総有財産のみ責任財産）	有限	無限
意思決定・業務執行	間接民主的	直接民主的	間接民主的	直接民主的	直接民主的	直接民主的
対外的契約	法人名義で締結	法人名義で締結	法人名義で締結	代表者の肩書付名義で締結（構成員全員に効果帰属）	組合員の肩書付名義で締結（組合員全員に効果帰属）	組合員の肩書付名義で締結（組合員全員に効果帰属）
構成員地位の譲渡	原則株主の合意は不要	原則社員の合意が必要 (定款に定めることで回避可能)	原則退社は自由	加入・脱退は慣習又は規約による。	構成員の合意が必要	構成員の同意又は組合契約による
課税	法人に課税	法人に課税	法人に課税 社員への収益分配は不可	収益事業等を行うと社団に課税	構成員に課税 (パススルー課税)	構成員に課税 (パススルー課税)

現行制度の課題

- 合同会社がDAOに最も近い
- 定款等に社員の氏名・住所を明記しなければならない

対応案

- 社員の氏名・住所に代えて、KYC済アドレスを定款等に記載する
  - ➢ 社員のプライバシー・匿名性を守ることができる
  - ➢ オンチェーンデータを基に財務報告・監査を効率化できる

4. 消費者保護・法執行に関する調査

4－1. 調査の狙い・アプローチ

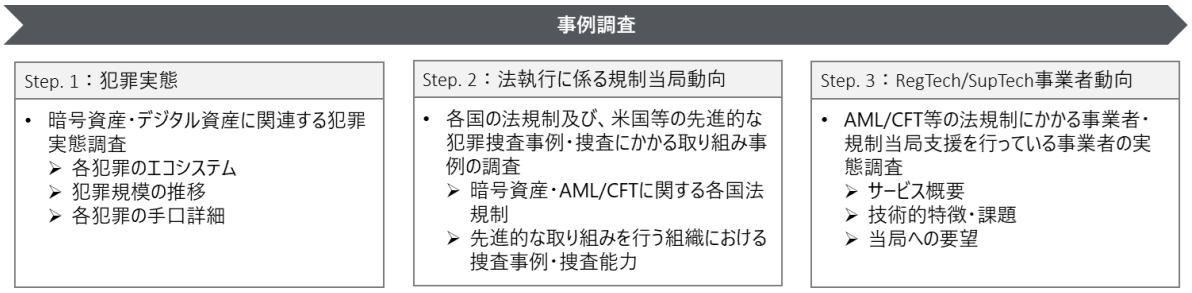
近年、NFT 等のデジタル資産、DeFi 等の分野における自律分散組織の活用により、これまでにない新たなサービスや産業の盛り上がりが期待される一方、デジタル資産や DAO に関連する越境犯罪・消費者被害の影響もまた増しており、適切な制度整備等の措置がこれまで以上に求められている。

本調査では、日本における望ましい制度・捜査執行能力等の将来的検討へのインプットとすべく、以下のステップで調査を実施した。

- 暗号資産・デジタル資産に関連する犯罪の実態を調査する
- 犯罪に対応するための国際連携の取り組みといった法執行に係る規制当局動向を調査する
- 捜査をサポートする技術を提供する RegTech/SupTech 事業者の動向を調査する

以下の図表は、上記の調査アプローチの具体的な項目の関係性を図示したものである。

図表 91　調査アプローチ



4－2. 調査まとめ

調査・分析を踏まえて以下のように取りまとめを行った。

図表 92　調査結果まとめ表

見出し	調査サマリ
4－3. 犯罪実態	全体犯罪動向 ■ Chainalysis の「2022 年暗号資産関連犯罪レポート[112]」によると 2021 年に 140 億ドルの被害が発生し、前年比約 79%の増加であった。特に被害額の大きい分野は、①詐欺(約 77 億ドル)、②盗難(約 32 億ドル) となっている 詐欺 ■ ラグプル[113]による詐取の被害額が 2020 年から 2021 年にかけて 1 億ドル未満から約 28 億ドルへ大きく増加している。また、2021 年に発生したラグプルの被害上位 15 件のうち、14 件が DeFi で発生しており、DeFi が主要な対象となっている ■ DeFi では、わざと脆弱なスマートコントラクトを実装し、開発者が資金調達後に不正に資金を引き出す事例が存在する 盗難 ■ 2021 年および 2022 年第 1 四半期における大規模な暗号資産盗難事件の上位 10 件のうち、7 件が DeFi で発生した[114] ■ DeFi の特性上、スマートコントラクトのコードが公開されているため、犯罪者が分析・ハッキングを試みやすく、スマートコントラクトの脆弱性攻撃、フラッシュローン[115]を活用した手口が多くみられる ■ また、フィッシングやソーシャルエンジニアリングによって、顧客の暗号資産の秘密鍵またはアカウント認証情報を盗み、顧客のウォレットから暗号資産を抜き取る被害が発生している その他犯罪・マネー・ローンダリング等 ■ その他犯罪として、ダークネットマーケット、ランサムウェア[116]、マルウェア[117]、北朝鮮・ロシア・イラン等の制裁対象国・地域との取引、テロ資金供与、NFT に関連する犯罪等が挙げられる ■ NFT に関する犯罪では、詐欺・盗難に加えてウォッシュトレード[118](約 850 万ドル)や、デジタルアート等の高額な NFT の購入・再販を通じたマネー・ローンダリング(約 140 万ドル)が挙げられる

[112] https://go.chainalysis.com/crypto-crime-report-2022-jp.html

[113] 顧客をだまして開発資金等を調達した後にプール資金を抜き取る手法

[114] https://blog.chainalysis.com/reports/2022-defi-hacks-japanese/

[115] 担保なしで暗号資産・トークン等を借り、その債務の処理と返済を同じ取引内(Ethereum 等の 1 つのチェーン上の取引)で解消することが可能である DeFi プロトコルの機能、
利便性が高い一方で、大量に資金を借り、その資金で資産を大量に購入することで資産価格をつり上げて、高騰した価格で売り抜けを行うことができてしまうリスクが存在する

[116] 企業等のデータを盗難し、身代金を要求する犯罪手口

[117] ウイルスソフト等を活用して、顧客のウォレットから資金を抜き取ったり顧客のデバイスから不正にマイニングを行ったりすること

[118] トレーダーが同じトレーダー ID や口座を使って、同時に買発注や売発注を行い NFT の価値を意図的につり上げること

	■ 犯罪資金の移動手法として、チェーンホッピング[119]、秘匿性の高い暗号資産[120]、ミキシングサービス[121]を活用することで、捜査による追跡を困難にしている ■ また、金融取引・暗号資産取引を行う場合は基本的に AML/CFT 規制にのっとって身元確認を行う必要があるが、AML/CFT 規制に準拠していない暗号資産取引所やノンカストディアルウォレット等を活用して取引を行うことで厳しい審査を受けずに取引を継続している事例が多くみられる
4－4. 法執行に係る規制当局動向	■ 米国では、国務省、司法省(国家安全保障課、連邦捜査局、麻薬取締局、連邦保安官等)、国土安全保障省(国土安全保障調査、米国シークレットサービス)等の法執行機関や、財務省(金融犯罪取締ネットワーク、外国資産管理室)、証券取引委員会、商品先物取引委員会等の監督機関が暗号資産に係る犯罪防止・犯罪捜査の取り組みを進めている ■ 米国司法省の報告書[122]では、①暗号資産に係る取引の匿名性が犯罪捜査を困難にすること、また、越境犯罪の場合には②規制等の理由で当事国やその国の事業者から十分な情報を収集することが困難であること、③その国の捜査当局の犯罪捜査能力が低く捜査が滞ること等が課題として挙げられており、その対処に向けた以下の取り組みが紹介されている 専門チームの創設 ■ ブロックチェーン技術に関連する専門組織を新規創設し、捜査力の高度化や部門横断的な情報共有・教育等を実施している ■ 司法省では 2021 年 10 月に NCET(National Cryptocurrency Enforcement Team)を創設し、デジタル資産の犯罪的不正使用の特定、調査、支援、捜査と起訴を行っている ■ 連邦捜査当局では、2022 年 3 月に VAU (Virtual Asset Unit)を創設し、FBI の暗号通貨の専門知識を一つの中枢に集約して高度な暗号資産に関する捜査訓練を FBI 職員に提供している 国際的な場での発信 ■ 米国ではブダペスト条約[123]の追加署名を行い、犯罪捜査における情報収集協力制度の改善を行っている。この追加署名によって自国以外のサービスプロバイダが保持するドメイン登録、インターネット加入者情報、およびトラフィックデータをより簡単に取得可能となった。また、多国間協定だけでなく、二国間による刑事共助(MLA：Mutual Legal Assistance)条約締結を推進している[124] ■ また、国際的な金融活動作業部会(FATF)、証券監督者国際機構(IOSCO)へ参加し、積極的な働きかけを行っている 各国捜査当局へのトレーニング

[119] ある暗号資産から別の暗号資産へ変換取引を複雑かつ迅速に行うこと

[120] リング署名やステルスアドレスを活用して匿名化を実施するものがある

[121] 複数の送金元・受取元からなる暗号資産取引データを混ぜ合わせることで、送金元・受取元や取引データの匿名化を行うこと

[122] 「How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets」 https://www.justice.gov/ag/page/file/1510931/download

[123] 2001 年に採択されたコンピュータ犯罪やサイバー攻撃に国際的に対応するための国際条約。2022 年 5 月 12 日にフランス・ストラスブールの欧州評議会本部において追加署名式典が行われた

[124] 2022 年 4 月の時点で 74 の国・地域・島と合意している https://www.justice.gov/criminal-oia/file/1498806/download

	■ 国務省、司法省、財務省等の各省がデジタル資産関連の調査に関する自らの専門知識を活用し、研修や事案別の連絡を通じて他国のカウンターパートとの専門知識の共有を実施している
4－5．事業者動向	取引モニタリング事業者 ■ サービス概要: 暗号資産取引の流れや、アドレスがどの組織に紐づくのかを専門的に調査・分析し、暗号資産取引が違法なものに繋がっていないかを見える化するツールを開発・提供、主要な暗号資産の取引関係者の特定に活用される。また、取引フィルタリングサービス等外部ツールと組み合わせて取引に関わったアドレスを当事者となった法人や個人の属性情報と関連付けることができるため米国において犯罪捜査等での活用が進んでいる[125] ■ 実務での課題: ミキシングサービス・DeFi を活用したマネロン等の犯罪手口の高度化が進んでおり、米国ではミキシングサービスの利用を禁止する等の取り締まりを行った事例がある[126] ■ 行政への期待: 匿名ウォレットに十分な AML/CFT 規制を課すことは難しく従来型の金融サービスと同程度の身元確認を求める必要がある。米国では民間事業者と法執行機関・規制当局との連携が進み官民情報共有システムの改善・迅速なオペレーション・人々が協力できる信頼性の高い環境が整備されている e-KYC 事業者 ■ サービス概要: 生体認証・文字読み取り技術等を活用してオンラインで KYC を行うツールを暗号資産取引所等の事業者に提供する他、身元確認時に収集した情報による当人認証サービス、顔・属性情報の使いまわし等悪質なアカウントをリスト化して提供している ■ 実務での課題: 本人確認書類を撮影する身元確認方式において、画像解析技術の限界による偽造やなりすましが少数ながら発生するリスクがあるため、本人確認書類の IC 読取りによる身元確認方式への移行を促すべく、IC 読取り技術の精度向上に取り組んでいる ■ 行政への期待: 匿名ウォレットによる犯罪の防止は難しく、匿名ウォレットを活用した犯罪を抑止するため個人が身元確認情報を保有して必要なタイミングで規制当局等に提示できる仕組みが必要である

上記を踏まえて、デジタル資産に関連した犯罪における特徴として、取引主体の匿名性が事案への対応において重要であることが改めて浮き彫りになった。

特に、①身元情報を匿名化した状態で取引できること、②取引情報を匿名化できることへの対応が犯罪の未然防止及び事後対応に大きな影響を与えると想定され、以下の図表に示す通り、身元情報収集の強化、高度な取引匿名化サービスの利用取り締まり・捜査体制の高度化等の制度的措置の検討が考えられる。

[125] 米国司法省「The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets」https://www.justice.gov/media/1245466/dl?inline=

[126] 著名なミキシングサービスであるトルネードキャッシュは 2022 年 8 月 8 日にアメリカ財務省外国資産管理局(OFAC)から利用禁止令が出され、その開発者はマネー・ローンダリングの手助けを行ったとして逮捕された

図表 93　デジタル資産関連犯罪の課題と想定される対応

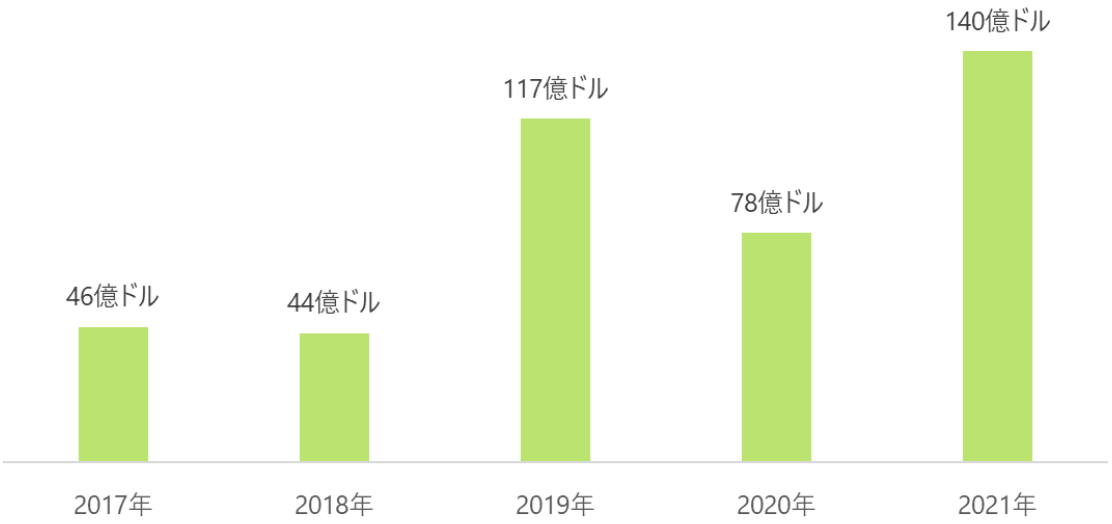
課題	概要	考えうる対応 (例)
匿名アドレスによる犯罪取引	• 以下のようなケースでは、AML/CFT規制に準拠した利用者の身元確認がなされないため、犯罪防止・捜査の難度が高まる ➢ FATFのトラベルルールやAML/CFT規制が適用されていない地域 ➢ 分散型取引所等で利用される身元確認が行われていないノンカストディアルウォレット	• FATFトラベルルール順守・サイバー条約の締結国拡大に向けた国際的な働きかけの継続・強化 • ノンカストディアルウォレットの利用者自身による身元確認対応を推進する取り組み
犯罪に係る取引の匿名化	• 取引の匿名性を高めるサービスが使われることで、捜査における取引追跡の難度が高まる	• 当該サービス利用の制限 (例：トルネードキャッシュの取り締まり) • 捜査体制の高度化 ➢ 暗号資産関連犯罪における専門組織・教育組織創設 ➢ RegTech/SupTech事業者等との連携強化

4－3. 犯罪実態調査

（1） 全体動向

Chainalysis の「2022 年暗号資産関連犯罪レポート[127]」によると 2021 年に 140 億ドルの犯罪被害が発生し、前年比約 79%の増加であった。被害額の大きい分野は、①詐欺（約 77 億ドル）、②盗難（約 32 億ドル）、③ダークネットマーケット（約 21 億ドル） となっている。

図表 94　暗号資産犯罪被害額の推移



（2） 詐欺

ラグプル による詐取の被害額が大きく、2021 年に発生したラグプルの被害上位 15 件のうち、14 件が DeFi で発生しており、DeFi が主要な対象となっている。DeFi では、わざと脆弱なスマートコントラクトを実装し、開発者が資金調達後に不正に資金を引き出す事例が存在する。

米国の消費者金融保護局（Consumer Financial Protection Bureau）の報告書[128]では、詐欺被害として、ロマンス詐欺、「Pig Butchering[129]」、インフルエンサーやカスタマーサービスを装った詐欺等、さまざまな種類の詐欺が報告されている。

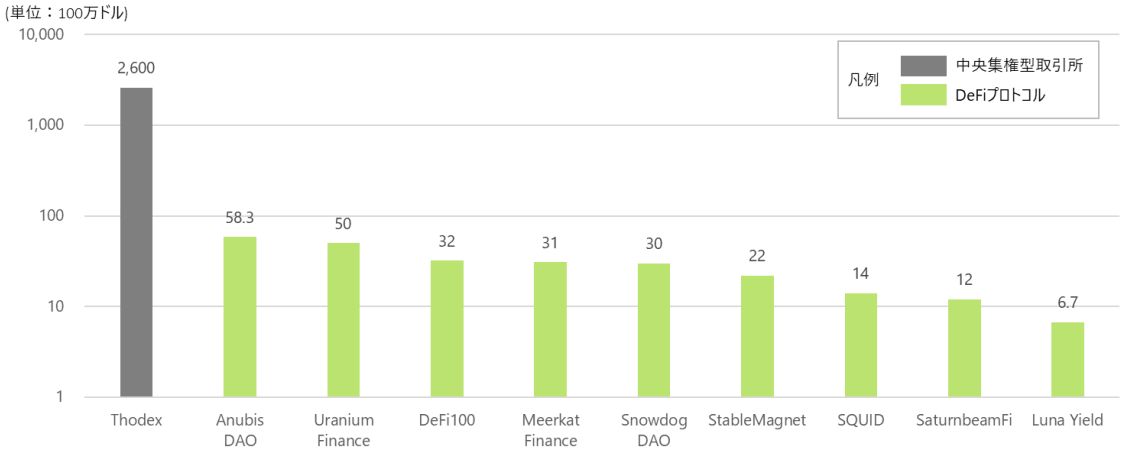
---

[127] https://go.chainalysis.com/crypto-crime-report-2022-jp.html

[128] https://files.consumerfinance.gov/f/documents/cfpb_complaint-bulletin_crypto-assets_2022-11.pdf

[129] 犯罪者が、ソーシャルメディア等を活用して被害者と信頼関係を構築し、暗号資産等の資産購入の勧誘を行い、一時的に収益を渡して安心感を与えた後に最終的に資金をだまし取ること。詐欺のプロセスを、豚を育てて殺す様子にたとえて「Pig Butchering （豚の屠殺）」と呼ばれている

図表 95　ラグプルによる暗号資産の盗難総額のトップ 10[127]（2021 年）

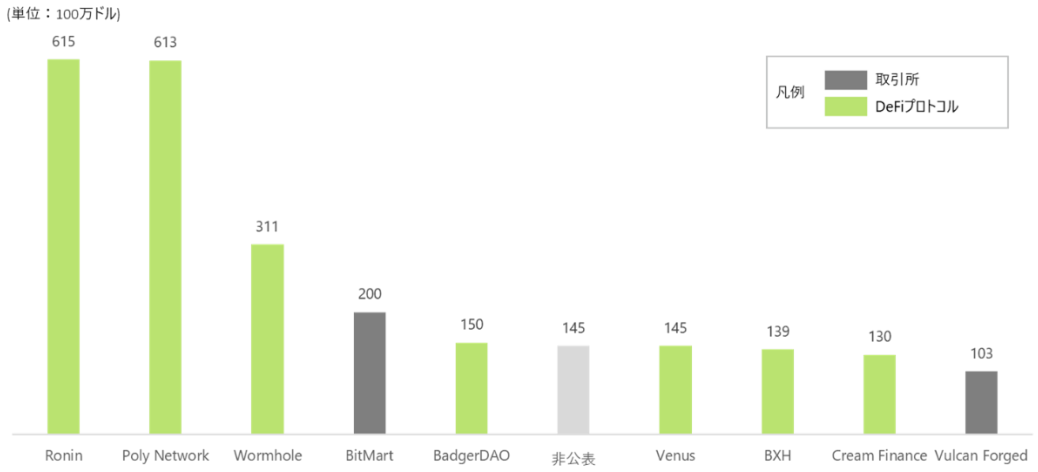


（3） 盗難

2021 年および 2022 年第 1 四半期における大規模な暗号資産盗難事件の上位 10 件のうち、7 件が DeFi で発生した。DeFi の特性上、スマートコントラクトのコードが公開されているため、犯罪者が分析・ハッキングを実施しやすく、スマートコントラクトの脆弱性攻撃、フラッシュローンを活用した手口が多く見られる。

また、「SIM スワップ[130]」ハッキング、フィッシング攻撃[131]、ソーシャルエンジニアリング[132]等によって顧客の秘密鍵やウォレットアカウントを奪い盗難を行う事例が見られる。

図表 96　盗難被害による暗号資産の盗難総額のトップ 10[133]　（2021 年-2022 年第 1 四半期）



---

[130] 通信キャリアのシステムを不正に操作し、攻撃対象の電話番号をハッカーが持つスマホの SIM カードに移転させること。ハッカーは SMS 経由で認証コードを取得し被害者のアカウントから本人になりすましてウォレット操作を行うことが可能となる

[131] 信用できると思われる送信元を装ったメールなどを不特定多数、または特定の標的に送り、ID やパスワード、クレジットカード番号や、個人情報、財産や企業秘密などを騙し取るネット詐欺

[132] パスワードやその手がかりを、それを知る本人や周辺者への接触や接近を通じて盗み取る手法の総称

[133] https://blog.chainalysis.com/reports/2022-defi-hacks-japanese/

図表 97　盗難被害概要 [133]

No.	被害サービス	犯罪手口	概要
1	Ronin Network	セキュリティ侵害	■ 攻撃者は、取引検証担当者 9 名のうち 5 名の秘密鍵を盗み出し、その大半を悪用して ETH と USDC の引き出しを承認させた
2	Poly Network	脆弱性攻撃	■ 攻撃者はクロスチェーンリレー契約の脆弱性を攻撃し、3 つの異なるチェーン、Ethereum、BSC、Polygon から、Poly Network の資金を引き出した
3	Wormhole	脆弱性攻撃	■ 攻撃者は、Wormhole の Sola ↔ Ethereum クロスチェーンブリッジを操作して、12 万 ETH が入金されたように見せかけ、Solana に同価値の whETH （Wormhole ETH） を作り出すよう仕向けた
4	BitMart	セキュリティ侵害	■ 攻撃者は秘密鍵を盗み出し、BitMart の 2 つのホットウォレットを侵害した
5	BadgerDAO	セキュリティ侵害	■ 攻撃者は侵害した cloudflare API 鍵を使って、Badger のアプリケーションに定期的に不正なスクリプトを投入していた ■ このスクリプトは取引を監視し、外部のアカウントから ERC-20 トークンの操作を許可するようユーザに促していた。許可がおりると、攻撃者はユーザのウォレットから資産を盗み出した
6	非公表	その他 （横領）	■ 企業が金融口座間で資金を移動しようとした際、従業員が資金を個人口座に移したとされている
7	Venus	脆弱性攻撃	■ 攻撃者は、Venus Protocol のガバナストークンである XVS の価格を操作し、XVS の実勢価格を超える価値の BTC と ETH を借りることに成功しました。ガバナンストークンの価格が下がり、プロトコルユーザが債務不履行となった時点で、Venus には 1 億 4,500 万ドルの債務が残された
8	BXH	その他 （秘密鍵の漏洩）	■ BXH の技術チームの身元不明のメンバが、管理者の秘密鍵を漏洩したとされている
9	Cream Finance	フラッシュローン	■ 最初に攻撃者は、一連のフラッシュローンによって、最大 150 万ドルの crYUSD を作り出した ■ 次に攻撃者は、Cream の PriceOracleProxy 機能を使って、所有す

			る crYUSD の価値を人為的に最大 30 億ドルにまで高騰させた ■ このうち 20 億ドルが、攻撃者の未払いのフラッシュローンの返済に当てられ、残りの 10 億ドルは、貸出し可能な Cream の全資産（1 億 3,000 万ドル）を流出させるために使用された
10	**Vulcan Forged**	**セキュリティ侵害**	■ 攻撃者は 96 のアドレスの秘密鍵のアクセス権を取得し、そのコンテンツをハッカーがコントロールするウォレットに送った

（4） その他犯罪・マネー・ローンダリング等

その他犯罪として、ランサムウェア、マルウェア、北朝鮮・ロシア・イラン等の制裁対象国との取引、テロ資金供与、NFT に関連する犯罪等が挙げられる。

NFT に関する犯罪では、詐欺・盗難に加えてウォッシュトレード[134]や、デジタルアート等の高額な NFT の購入・再販を通じたマネー・ローンダリングが挙げられた。犯罪資金の移動手法として、チェーンホッピング、秘匿性の高い暗号資産（AEC：Anonymity Enhanced Cryptocurrencies)、ミキシングを活用することで、捜査による追跡を困難にしている事例がある。また、金融取引・暗号資産取引を行う場合は基本的に AML/CFT 規則にのっとって身元確認を行う必要があるが、AML/CFT 規制に準拠していない暗号資産取引所やノンカストディアルウォレット等を活用して取引を行うことで厳しい審査を受けずに取引を継続している事例が多くみられる。

図表 98　その他犯罪の被害概況と手口特徴

犯罪の種類	被害概況	犯罪手口概要
ダークネットマーケット	**約 21 億ドル**	■ 危険ドラッグの販売による売上（約 18 億ドル)、盗難したログイン情報やクレジットカード情報、エクスプロイトキット[135]等の販売を仲介した違法データ販売サイトの売上（約 3 億ドル）からなる ■ 匿名通信（Tor ネットワーク）を活用して、販売サイトを立ち上げ売り上げをあげている
ランサムウェア	**約 6 億ドル**	■ 不正にデータを盗み出したり、サービスを停止させたりすることで、その復旧の見返りに身代金の要求を行うもの
NFT	**約 1,000 万ドル ※盗難は含めない**	■ NFT の価値を意図的につり上げるウォッシュトレード　（約 850 万ドル） ■ NFT（デジタルアート等の高額商品）の購入・再販を通じたマネー・ローンダリング　（約 140 万ドル）

[134] トレーダーが同じトレーダー ID や口座を使って、同時に買発注や売発注を行い NFT の価値を意図的につり上げること

[135] サイバー犯罪者が PC やデバイスの脆弱性を利用する際に用いるハッキングツール

マルウェア	**数百万ドル**	■ ウイルスソフト等を活用して、顧客のウォレットから資金を抜き取ったり顧客のデバイスから不正にマイニングを行ったりすること。以下のような手口が多い ➢ クリプトジャッキング：被害者のデバイスのコンピューティングパワーを不正に使用して、暗号資産をマイニングすること（取引匿名性の高いトークン（Monero 等）をマイニング） ➢ トロイの木馬：一見正当なプログラムを装って、被害者のコンピュータに侵入して操作を妨害し、盗難その他の危害を加えるウイルス

図表 99　制裁対象国との取引事例

国名	犯罪手口概要
北朝鮮	■ ハッキング等を活用して暗号資産を盗難 （2021 年の盗難額約 4 億ドル） ■ DeFi サービスを活用して流動性の高いトークンに変更した後、ミキシングを行い資金の出処を秘匿化したうえで資金移動を実施 （全体資産の 65%でミキシングサービスを活用）
ロシア	■ ダークネットマーケット（ロシア語圏を拠点とした Hydra[136]の売上：約 18 億ドル）やランサムウェア（約 4,000 万ドル）によって資金を獲得 ■ ロシアを拠点としている大手暗号資産取引所で資金洗浄
イラン	■ Monero 等、PoW の承認アルゴリズムをもち、かつ匿名性の高い暗号資産のマイニングによる収益を取引所で資金洗浄 （現地で容易に獲得できる石油から発電した電気等をもとにマイニング）

[136] 2022 年 4 月 5 日に、米国司法省とドイツ連邦刑事警察局が共同で取り締まりを行い、2,500 万ドル相当のビットコインと運営サーバを差し押さえ、閉鎖に追いやった

4－4. 法執行に係る規制当局動向調査

（1） 課題認識・取り組み事項

米国では、国務省、司法省（国家安全保障課、連邦捜査局、麻薬取締局、連邦保安官等）、国土安全保障省（国土安全保障調査、米国シークレットサービス）等の法執行機関や、財務省（金融犯罪取締ネットワーク、外国資産管理室）、証券取引委員会、商品先物取引委員会等の監督機関が暗号資産に係る犯罪防止・犯罪捜査の取り組みを進めている。

図表 100　米国法執行機関・規制当局における取り組み事項

組織		主な取り組み事項
国務省 (DOS)		• GLEN(Global Law Enforcement Network)で、外国の法執行機関、検察、司法パートナーにサイバー犯罪に関連する訓練および技術援助を提供 • 国連薬物犯罪事務所、米州機構、国際刑事警察機構、欧州評議会などの多国間パートナーに任意の資金を提供し、サイバー犯罪研修や技術支援プログラムを提供
司法省(DOJ)		• NCET(National Cryptocurrency Enforcement Team)を結成し、暗号資産を活用したマネーロンダリングにかかる捜査、詐欺やランサムウェアによって失われた資産追跡や回収支援を実施 • NCETや、海外検察開発援助訓練局(OPDAT)を通じて海外各国の捜査官、検察官、裁判官の能力構築や、二国間協定など国際的な協力の強化を実施
	連邦捜査局 (FBI)	• 世界各地の63のオフィス等を通じて、180を超える国、地域で世界中のデジタル資産に関連する犯罪活動の検出、捜査、および起訴の中心となる役割を担う • 専門チームVAU(Virtual Asset Unit) を結成、FBIの暗号資産の専門知識を一つの中枢に集約し、FBI職員に技術機器、ブロックチェーン分析とデジタル資産押収の訓練、その他の高度な暗号資産訓練を提供 • JCODE(Joint Criminal Opioid Darknet Enforcement)を設立し、米国郵政公社米国郵便検査局や国土安全保障省、海外捜査機関と連携して、麻薬・ダークウェブに関する捜査を実行
	麻薬取締局 (DEA)	• ダークネット市場や多国籍犯罪組織の暗号通貨の使用を含む麻薬捜査において重要な役割を担う • 69か国に設置された92の外国事務所等を通じて、暗号通貨関連を含む麻薬取締に関して、外国のパートナーと協力、暗号資産の追跡とダークネット市場調査での利用方法を指導
国土安全保障省 (DHS)	国土安全保障調査 (HSI)	• 50カ国以上の80の事務所で構成、多国籍犯罪について脅威が国境に到達する前に脅威を特定し軽減するために活動 • 暗号資産を追跡するための分析支援を金融犯罪ユニット(FCU)やサイバー犯罪センター(C3)を通じて海外各国に提供
	米国シークレットサービス (USSS)	• 国内の現地事務所と世界中の19の国際駐在事務所の両方を通じて世界の法執行機関と提携し、デジタル資産の違法な使用を含むさまざまなサイバー犯罪活動を調査 • 米国国務省の国際法執行アカデミー(ILEA)プログラムを通じて、暗号資産等多くのサイバー犯罪関連の科目で海外各国のパートナーを訓練
財務省	テロ・金融情報局 (TFI)	• FinCEN(Financial Crimes Enforcement Network)等を通じて、AML/CFT取り締まり強化に向けて法執行機関の調査活動を支援し、国内および国際的な金融犯罪に対する省庁間およびグローバルな協力を促進 (リスク評価・モニタリング・KYCを目的とした取引の分析方法・疑わしい取引の報告・不正融資動向;トランザクション分析を行うためのツール利用方法・オープンソースの調査を通じて顧客やウォレット情報収集の方法等)
	内国歳入庁-犯罪捜査 (IRS-CI)	• 内国歳入法の犯罪違反(脱税等)や、BSA違反(米国の金融機関を利用して資金の隠匿やロンダリングを行う者を防止)やマネーロンダリング禁止などの関連する金融犯罪を調査 • 世界銀行と共同で暗号資産、ダークウェブ等の犯罪捜査方法や、オープンソースの利用方法等に関するインテリジェンス共有会議を複数実施
証券取引委員会 (SEC)		• デジタル資産に関する多数の強制措置(ICOで調達した資金の凍結・トークン配布の禁止等)を実施 • 技術支援 (TA) プログラムで、外国証券および規制当局の資本市場の強化、能力構築、国際基準への準拠、ベストプラクティスの実施を支援
商品先物取引委員会 (CFTC)		• ビットコインやイーサなどのデジタル資産を原資産とするデリバティブ市場を規制 • CFTC職員と業界関係者の専門知識を活用して、世界の規制コミュニティにトレーニングとサポートを提供

米国司法省の報告書[137]では、①暗号資産に係る取引の匿名性が犯罪捜査を困難にすること、また越境犯罪の場合には更に②規制等の理由で当事国やその国の事業者から十分な情報を収集することが困難であること、③その国の捜査当局の犯罪捜査能力が低く捜査が滞ること等が課題として挙げられている。

図表 101　犯罪捜査に係る課題意識

匿名取引による特定困難	• Monero等のウォレットアドレス間の取引匿名化を目的で設計された資産の取引分析が困難なこと • ミキサー、タンブラー等のサービス(受取者に送金する前に、他の暗号資産と混合して匿名化したうえで送金すること) やチェーンホッピング(別の暗号資産同士を短期間に交換すること)を活用して、本来追跡可能な暗号資産取引の複雑化していること • 秘密鍵を受け渡しすることでブロックチェーン上に記録せずに資金取引を行うことで監視ができないこと • 管理主体が存在しないKYC未済のウォレットを使用して資金移動を行い身元の特定が困難なこと
捜査協力の取り付け	• 事業者・実質的なサービス提供者の所在地が不明または異なる場合、どこの国と協力を取り付けるべきか調整に時間を要すること • 犯罪組織・暗号資産サービスプロバイダーが法執行の協力が得られない国*で活動している場合に支援を受けることが困難であること • 捜査支援の取り付けができたとしても、その国の法規制によって必要な情報収集が困難である可能性があること、各国が規定している捜査権限すべての国が刑事訴追等以外の資産差押さえ権限を持っているわけではないため、米国の金融規制当局から要請した情報の提供への意欲が低いこと
海外パートナーの捜査能力・体制不足	• デジタル資産が新規のテーマであるため、多くの各国機関では犯罪捜査体制整備が発展途上の段階 ➢ 専門的ツール、専門知識を必要とするデジタル資産を含む複雑な捜査体制の未整備 (通常のマネーロンダリングやその他金融捜査を行うための限られたリソース体制確保に終始) ➢ ブロックチェーン分析ツール等の技術利用にかかるリテラシー・予算確保が困難 (低コスト・無料で利用可能な分析ツールに関する理解度も低い)

このような問題に対処するために以下のような取り組みを行っている。

（2） 課題への対応方針

1）専門チームの創設

ブロックチェーン技術に関連する専門組織を新規創設し、捜査の高度化や部門横断的な情報共有・教育等を実施している。司法省では 2021 年 10 月に NCET（National Cryptocurrency Enforcement Team）を創設し、デジタル資産の犯罪的不正使用の特定、調査、支援、捜査と起訴を行っている。

NCET は、デジタル資産技術に関する戦略的優先事項を設定し、デジタル資産の新たな利用に既存の法律を適用することから生じる問題に取り組み、デジタル資産の犯罪的利用を防ぐために、国内外の法執行機関、規制機関、民間企業と調整する同省の取り組みを主導しており、Hydra、Bitfinex、Helix、BitMEX 等の犯罪捜査に関わった。

また、2022 年 9 月には NCET が主導して DAC（Digital Asset Coordinator）ネットワークを創設した。DAC は、全米の連邦検事局から指名された連邦検察官と、司法省の訴訟部門で構成されている。DAC ネットワークでは、構成メンバに DeFi、スマートコントラクト、トークンベー

[137] 米国司法省「The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets」https://www.justice.gov/media/1245466/dl?inline=

スのプラットフォームなどの新たな事柄について調査分析や犯罪捜査のためのベストプラクティス獲得を行い、デジタル資産に関する専門家を増やすことを目指している。

連邦捜査当局（FBI）では、2018 年に JCODE（Joint Criminal Opioid Darknet Enforcement）チームを立ち上げ、国内・海外機関と連携をしてダークウェブに関連する犯罪捜査活動を主導している。また、2022 年 3 月に VAU （Virtual Asset Unit）を創設し、FBI の暗号通貨の専門知識を一つの中枢に集約したうえで、技術機器、ブロックチェーン分析とデジタル資産押収のトレーニング、その他の高度な暗号資産トレーニングを FBI 職員に提供している。FBI はすでにこのカリキュラムを使って、世界中の何千人もの FBI 職員やパートナーを訓練している。

図表 102　NCET が捜査協力を行った捜査概要

捜査事例	捜査概要
Helix	■ 2020 年 2 月 13 日、米司法省は、ダークネットを利用した暗号資産マネー・ローンダリングサービス 「Helix」 の管理人を起訴し、逮捕したと発表した。Helix はビットコインミキサーやタンブラーとして機能していた ■ 起訴状によると、Helix は違法な麻薬販売やその他の犯罪取引の収益となる 3 億ドル以上のビットコインをマネー・ローンダリングした容疑で起訴された。同日、Helix の管理人がアメリカ、ベリーズ司法長官省、ベリーズ国家警察部で逮捕された ■ また、FinCEN は 2020 年 10 月 19 日に Helix 社に対して 6000 万ドルの民事制裁金を科した。2021 年 8 月 18 日、この管理者は Helix 社の運営から生じたマネー・ローンダリングの共謀の罪を認めた
Bitfinex	■ 2022 年 2 月 8 日、同省は、2016 年に仮想通貨取引所 Bitfinex がハッキングされた事件で盗まれた暗号資産（逮捕時は約 45 億ドル相当）のマネー・ローンダリングの共謀容疑で、Ilya Lichtenstein と妻の Heather Morgan を逮捕したと発表した ■ これまでのところ、盗まれた暗号資産のうち 36 億ドル （押収時の価値） 以上を押収している ■ 架空の ID を使ってオンライン口座を開設したり、コンピュータープログラムを使って取引を自動化したり、盗まれた資金を異なる取引所や市場の口座に入金した後に引き出して資金の流れを分断、ビットコインを他の暗号資産 （AEC を含む） に換金して 「チェーンホッピング」の実施、米国に拠点を置くビジネス口座を使って銀行業務を合法化等、多くの高度なマネー・ローンダリング手法を用いたとされている ■ 本件は FBI（NCET）や、IRS-CI、ICE（移民関税執行局）、HSI など複数の国内法執行機関が協力した
Hydra	■ 2022 年 4 月 5 日、司法省は、当時世界最大かつ最も長く続いていたダークネット市場である Hydra Market をドイツ連邦刑事警察局と共同で押収したことを発表した ■ 2021 年、Hydra はダークネット市場に関連するすべての暗号資産取引の推定 80%を占め、2015 年から押収までの間に、市場は約 52 億ドルの暗号資産を受け取った ■ Hydra サーバの押収に加えて、約 2500 万ドル相当のビットコインを含む暗号資産ウォレットを押収した

	■ また、Hydra の閉鎖に伴い、司法省は Hydra の運営に使用されていたサーバの運用と管理に関連して、麻薬配布の共謀とマネー・ローンダリングの共謀でロシア人を刑事告発した ■ この調査は、司法省の多機関特殊作戦課と JCODE の支援と調整を受けて、DEA のマイアミ現地課、FBI、IRS-CI、米国郵便検査局、HSI が主導した ■ Hydra の閉鎖に伴い、財務省はダークネット市場と、Hydra の運営に関連する 100 以上の暗号資産アドレスが不正取引に使用されていたことを制裁した
BitMEX	■ FinCEN、CFTC は 2020 年 10 月、BitMEX がデリバティブのようなデジタル資産を米国の顧客に違法に提供していた、FCM[138]の登録を怠っていた、BSA[139]を遵守していなかったなどの容疑で民事提訴したと発表した。2021 年 8 月、同社は CFTC・FinCEN と和解し、合計 1 億ドルの罰金を支払うことで合意した ■ BitMEX は 2014 年に設立されたオンライン暗号資産デリバティブ取引所で、一時は世界最大の暗号資産デリバティブ取引所として先物などの金融商品を顧客に提供していた ■ しかし、BitMEX は BSA 準拠の AML プログラムを導入しておらず、顧客の身元を確認する手段を取らなかったため、個々の顧客は電子メールアドレスを提供するだけで取引を行うことができた ■ BitMEX は米国の顧客にサービスを提供していないという虚偽の主張をしていたが、実際には米国に拠点を置き、数千の米国の顧客にサービスを提供した。また、BitMEX はミキシングサービスを提供する既知のダークネット市場または未登録の MSB[140]と少なくとも 2 億 900 万ドル相当の取引を行っていた

図表 103　JCODE が行った捜査作戦概要

作戦名	時期	参加機関	捜査概要	成果
Operation Disarray[141]	2018 年 （4 日間）	DOJ、FBI、DEA、ATF[142]、USPIS[143]、IRS-CI、NCIS[144]、FinCEN、 HIS-ICE[145] 等	■ 薬物をオンラインで売買したことのある人に全国で 160 以上のインタビューを実施	■ 8 人逮捕

[138] Futures Commission Merchants の略であり、米国民・企業に対して先物取引商品を提供する場合に CFTC へ登録が義務付けられている

[139] 銀行秘密法（The Bank Secrecy Act） の略であり、米国の AML/CFT に関する規制を定めたもので FinCEN が法執行を行う

[140] Money Services Businesses の略であり、BSA 上の Money Transmission Services（通貨又はそれに代わる価値を送金等するサービス）を行う場合に MSB を行う者として FinCEN に登録する必要がある

[141] https://www.justice.gov/opa/pr/attorney-general-jeff-sessions-announces-results-j-code-s-first-law-enforcement-operation

[142] 司法省アルコール・タバコ・火器及び爆発物取締局（ATF：Bureau of Alcohol, Tobacco, Firearms and Explosives）

[143] 米国郵政公社米国郵便検査局（USPIS：United States Postal Inspection Service）

[144] 海軍省海軍犯罪捜査局（NCIS：Naval Criminal Investigative Service）

[145] 国土安全保障省移民・関税執行局（ICE：Immigration and Customs Enforcement）

Operation SuboTor[146]	2019 年（約 2 カ月）	DOJ、DOD[147]、FBI、DEA、HIS-ICE、HIS-CBP[148]、EU	■ 薬物購入者等に 122 回のインタビューを実施	■ 61 人逮捕 ■ 700 万ドル以上押収（うち暗号資産約 450 万ドル
Operation DisrupTor[149]	2020 年（約 9 カ月）	（米国機関に加えて）EU、オーストリア、キプロス、ドイツ、カナダ、ポルトガル、オランダ、イギリス、オーストラリアの捜査当局	■ N/A	■ 170 人以上逮捕 ■ 約 650 万ドル押収
Operation Dark HunTor[150]	2021 年（約 10 カ月）	（米国機関に加えて）EU、オーストラリア、ブルガリア、フランス、ドイツ、イタリア、オランダ、スイス、イギリスの捜査当局	■ N/A	■ 約 150 人逮捕 ■ 約 3,100 万ドルの押収

2）多国間協力・国際的な会議の場での発信

米国ではブダペスト条約[151]の追加署名を行い、犯罪捜査における情報収集協力制度の改善を行っている。これにより、自国以外のサービスプロバイダが保持するドメイン登録、インターネット加入者情報及びトラフィックデータをより簡単に取得可能となった。また、二国間による刑事共助（MLA：Mutual Legal Assistance）条約締結を推進している[152]。加えて、これらの条約締結に向けた活動だけなく国際的な金融活動作業部会（FATF）、証券監督者国際機構（IOSCO）へ参加し、積極的な働きかけを行っている。

FATF の会合には、米国財務省等が参加しており、暗号資産コンタクト・グループ（VACG）の共同議長を務めている。AML/CFT 規則、暗号資産、暗号資産サービスプロバイダ（VASP：Virtual Asset Service Provider）等の監視を強めること、また、各国に FATF 勧告を遵守するように働きかけを行うことで暗号資産に関連する犯罪の抑制に努めている。

---

[146] https://www.fbi.gov/news/press-releases/press-releases/j-code-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet

[147] 国防省（DOD：Department of Defense）

[148] 国土安全保障省税関・国境警備局（CBP：Customs and Border Protection）

[149] https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170

[150] https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-150

[151] 2001 年に採択されたコンピュータ犯罪やサイバー攻撃に国際的に対応するための国際条約。2022 年 5 月 12 日にフランス・ストラスブールの欧州評議会本部において追加署名式典が行われた

[152] 2022 年 4 月の時点で 74 の国・地域・島と合意している https://www.justice.gov/criminal-oia/file/1498806/download

IOSCO の会合には、証券取引委員会、商品先物取引委員会が参加しており、ステーブルコイン、暗号資産、DeFi、暗号資産デリバティブ商品等について、法域の裁定取引や市場の分断化のリスクを最小限に抑えるよう、法域を超えた規制提案や新たな慣行などに関する情報や経験を共有する場として機能している。

3）各国捜査当局へのトレーニング

デジタル資産関連の調査に関する自らの専門知識を活用し、研修や事案別の情報交換を通じて、外国のカウンターパートとの専門知識の共有を促進することを目的としたいくつかの主要なイニシアティブを実施している。

国務省国際麻薬法執行局（DOS/INL）が管轄をしている米国多国籍・ハイテク犯罪グローバル法執行ネットワーク[153]（GLEN：GLOBAL LAW ENFORCEMENT NETWORK）は、司法省コンピュータ犯罪・知的財産セクション（DOJ/CCIPS）、司法省海外検察開発援助訓練局（DOJ/OPDAT） と連携して外国の法執行機関、検察、および司法パートナーにトレーニングと技術支援を提供、電子証拠の収集と使用の支援を行っている。ブラジル、パナマ、ルーマニア、オランダ、クロアチア、ナイジェリア、エチオピア、香港、マレーシア、タイに人員を配置している。

また、国務省が管轄している国際法執行アカデミー[154]（ILEA：International Law Enforcement Academies）でも GLEN と同様に教育等を実施しており、アメリカニューメキシコ州、ガーナ、ハンガリー、タイ、ボツワナ、サンサルバドルにアカデミーを設置してネットワークセキュリティ対応、データ分析方法、暗号資産調査方法、麻薬捜査等、多くのサイバー犯罪関連について外国のパートナーの訓練を行っている。また、国土安全保障省米国シークレットサービス（HSI/USSS）や、司法省麻薬取締局（DOJ/DEA）等が連携してこの研修を実施している。

司法省では、NCET が、G7 ローマ/リヨン・グループ[155]の刑事・法務サブグループ、米欧暗号通貨作業部会、欧州評議会の欧州検察会議、ユーロポールの会議等、デジタル資産の起訴に関する様々な国際研修を実施してきている。また、連邦捜査局管轄の VAU では、前述したトレーニングプログラムを開発し、海外各国捜査当局に提供している。

上記（1）～（3）の米国取り組みを踏まえて、日本の法執行機関においても①暗号資産犯罪に対応できる横断的な捜査組織（NCET、JCODE 等に近しい組織）や、②捜査員教育組織 （DAC、VAU 等に近しい組織） の充実を検討する価値があると考えられる。

---

[153] https://www.justice.gov/criminal-opdat/global-cyber-and-intellectual-property-crimes

[154] https://www.state.gov/international-law-enforcement-academy-ilea/

[155] G7 の国際テロ対策の専門家で構成されるローマグループ及び国際組織犯罪対策の専門家で構成されるリヨン・グループの合同会合

4－5. RegTech/SupTech 事業者動向調査

犯罪防止・捜査において RegTech/SupTech 事業者の果たす役割は大きい。本調査においては、e-KYC 事業者（Liquid）や暗号資産取引モニタリング事業者（Chainalysis、Elliptic、NiceActimize）にサービス実態、犯罪防止・捜査に係る課題・取り組み等のヒアリングを実施した。

（1） モニタリング事業者

Chainalysis、Elliptic、NiceActimize 社等の暗号資産取引モニタリング事業者は、暗号資産取引の記録や流れ、アドレスがどの組織に紐づくのかを調査・分析し、暗号資産取引の実態を検証している。

米国司法省報告書[156]では、米国法執行機関において上記ツールを積極的に活用して、多くの主要なブロックチェーンでの取引を特定・追跡することが可能となっていると報告されている。また、取引フィルタリングサービスやオープンソース等外部ツールと組み合わせることでその取引に関わる組織や個人の属性を特定することが可能となっている。民間事業者のヒアリング結果からも米国政府は特に RegTech 事業者と緊密に連携を行っているという意見を頂いた。

ミキシングサービス・DeFi を活用したマネロン等の犯罪手口の高度化といった新たな脅威に向けて、機械学習・自動化技術等を活用して新たな技術開発が日々行われている。また、米国においてはこのような秘匿化サービスの利用を禁止する等取り締まった事例がある[157]。

（2） e-KYC 事業者

Liquid 等の e-KYC サービス事業者は、AML/CFT 規制が課される事業者（犯罪収益移転防止法の対象となる特定事業者）にオンライン身元確認サービスの提供を行っている。

特定事業者である暗号資産交換業者のサービスで利用されるウォレットについては、特定事業者による情報管理のもと、利用者の身元が明らかであるため AML/CFT 対応が十分に行われているが、DeFi 等で利用されるノンカストディアルウォレットは身元不明の状態で取引ができてしまい、犯罪防止や捜査において課題がある。将来 DeFi のように分散的に運営されるサービスでも身元確認ができるように、個人が身元確認情報を保有して必要なタイミングで規制当局に提示できる技術的・制度的基盤 が整うというシナリオがありうるのではないかといった指摘があった。

---

[156] 米国司法省「The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets」

[157] 著名なミキシングサービスであるトルネードキャッシュは 2022 年 8 月 8 日にアメリカ財務省外国資産管理局（OFAC）から利用禁止令が出され、その開発者はマネー・ローンダリングの手助けを行ったとして逮捕された

（3） 事業者ヒアリングまとめ

以下各社ヒアリング結果の取りまとめを行った。

1）Chainalysis

Chainalysis は暗号資産モニタリング事業者として以下サービスを提供している。

- Reactor / Storyline：主に政府機関が利用している、暗号資産の追跡調査ツール。ビットコインをはじめイーサリアム等のスマートコントラクトの取引追跡も可能
- Kryptos：政府機関や民間企業が利用している、各サービスのオンチェーンの動向を表示可能なダッシュボードで世界各国の取引所等の各サービスのリスクの度合いを測定可能
- KYT：暗号資産ビジネスを行う民間企業が利用している、取引モニタリングツール。取引のプリスクリーニングや継続的なモニタリングを実施し、取引内容に応じてアラート生成やその管理が可能
- Address Screening：NFT マーケットプレイス等の Web3 企業が利用している、ウォレットのリスクアセスメントツール。API ベースで接続されるウォレットのスクリーニングが可能

その他有償トレーニング、流出した資金の調査・分析サービス、捜査支援などのサービスも提供している。

課題として、ロンダリングの手法としてミキシングサービス・DeFi を利用するケースが増加し手法の高度化が挙げられる。

犯罪防止・捜査に向けた企業連携として、2014 年の創業以来連邦政府や州政府に対しツールの提供や捜査支援等、様々な領域で協業を実施している。また UAE 政府とは犯罪抑止のための人材育成を共同実施していくための覚書を締結している。

2）Elliptic

Elliptic は暗号資産モニタリング事業者として以下サービスを提供している。

- Lens（ウォレットスクリーニング）：顧客向けに取引相手のアドレスについてリスク評価を行い、暗号資産を取引するウオレットスクリーニングサービス
- Navigator（取引モニタリング）： 暗号資産取引所業者向けに、暗号資産取引のモニタリングサービス
- Discovery（リスク評価）：顧客や事業者向けに暗号資産交換業者などの暗号資産サービスプロバイダ（VASP）のリスク評価サービス
  Investigator（取引追跡）：暗号資産取引追跡サービスを提供、ウォレットアドレス間のつながりやトランザクションを可視化し、実在する事業者と紐付けることで取引を追跡

新たな脅威が常に発生するため、機械学習・自動化技術等を活用して新たなソリューション開発を行っている。特に近年顕著な DeFi やコインスワップ等を利用した犯罪に対応すべく、クロスチェーン・クロスアセットの分析に業界で初めて対応した Holistic Screening を展開している。

犯罪防止・捜査に向けた企業連携について、各国規制当局と意見を行っており、特に米国では民間事業者との連携が進んでいて、公共/民間セクター間での情報共有システムの改善、迅速なオペレーション、人々が協力できる信頼性の高い環境が整備されているという意見を頂いた。

3）Nice Actimize

Nice Actimize 社は暗号資産に加えて従来型金融商品の①マネー・ローンダリング、②詐欺行為、③コンプライアンス違反の検出・防止・調査に関するサービスを提供している。本調査では①マネー・ローンダリングサービスについてヒアリング調査を行った。マネー・ローンダリングに関するサービスとしては以下サービスを提供している。

- 取引追跡サービス：法定通貨を暗号資産・デジタル資産の相互変換、また、暗号資産同士の取引について疑わしい取引の確認・検出を行っている
- 暗号資産取引所評価サービス：上記取引追跡をもとに、暗号資産取引所がハイリスクかどうかについて情報提供銀行等事業者向けに提供している

課題として、AML とプライバシー法間での矛盾が挙げられ、この課題に金融機関等事業者が悩んでいる（例えば EMEA ではデジタル取引所に受取人の情報を提供することが禁止されている等が挙げられる）。

また、より高精度に顧客評価を行うために、暗号資産取引所から提供してもらう身元情報の項目を詳細にすることが望ましいという意見を頂いた。

加えて、ミキシング等高度な秘匿化サービスの台頭について、法執行機関でスクリーニングシステムを活用して取り締まることで犯罪リスク低減を行っていくことが重要であるという意見を頂いた。

犯罪防止・捜査に向けた企業連携について、各国の規制当局に対して、暗号資産の規制に向けた助言等のインプットを行っているという回答を頂いた。

4）Liquid

Liquid は、生体認証技術・文字読み取り技術等を活用して、AML/CFT 規制が課される事業者（犯罪収益移転防止法の対象となる特定事業者）にオンライン身元確認（e-KYC）サービスの提供を行っている。

その他、身元確認時に収集した情報をもとに当人認証サービスの提供や、顔・属性情報の使いまわし等初犯のアカウントをリスト化してフィルタリングとして記録して事業者に提供する等のサービス提供を実施している。

技術的な課題として本人確認書類を画像撮影する身元確認方式において、画像解析技術の限界によって偽造やなりすましが少数ながら発生するリスクがあり、この対策として本人確認書類の IC 読取りによる身元確認方式への移行を促すべく、IC 読取り成功率の向上に取り組んでいる。

また、また、KYC が済んでいないウォレットによる犯罪の防止は難しく、匿名ウォレットを活用した犯罪を抑止するためにも個人が身元確認情報を保有して必要なタイミングで規制当局等に提示できる仕組みが必要であるという課題認識を持っている。