データ流通部会 報告書

～次世代データエコシステムに関わる技術・動向調査

および情報サービス産業業界の協働の可能性に関わる考察～

<トラスト、アイデンティティ階層編>

令和７年５月

一般社団法人情報サービス産業協会
技術委員会 データ流通部会

・ 目 次 ・

1． トラスト、アイデンティティ階層編の目的 3

2． トラスト、アイデンティティの論議の前段として関連する論点 4

2.1 トラストの論議の前段として必要となる、事業者確認の論議について 4

2.2 事業者の当人認証について 9

2.3 Trusted Web と、データエコシステムのトラストやアイデンティティの論議との関連性 13

3． Gaia-X のトラストフレームワーク、Catena-X オンボーディングプロセス、eIDAS2.0・EUDIW トラストフレームワークとの関係 16

3.1 Gaia-X のトラストフレームワークについて 16

3.1.1 Gaia-X Trust Framework の概要 16

3.1.2 Gaia-X Digital Clearing House (GXDCH)の概要 18

3.2 Catena-X のオンボーディングプロセスにおける GXDCH の動作 22

3.2.1 登録プロセスの概要 22

3.2.2 Gaia-X Trust Framework と eIDAS の関係 25

3.2.3 Gaia-X Trust Framework と EUDIW の関係 25

3.3 EUDIW のトラストフレームワークについて 26

4． データスペースにおけるトラストやアイデンティティに関わる論議と、Trusted Web の取り組みや、事業者確認や当人認証に関わる論議の融合の期待 29

4.1 データスペースにおける事業者の認証・認可の検討の論点整理（将来課題と検討方向性） 30

4.2 データスペースにおける事業者の認証・認可の検討アプローチ仮説 35

4.3 VCおよび事業者DIWの活用の仮説 36

4.4 今後、深掘り検討が必要となる論点ポイントの仮説 43

4.5 【補足説明】仮説1：認可制御補助デバイスとしての活用のメリット 47

4.6 【補足説明】信頼できるアイデンティティ・プロバイダー（例：G ビズ ID）との ID 連携（フェデレーション）」の仮検討 50

・ 令和６年度 技術委員会 データ流通部会 委員名簿 ・

※会社名 50 音順

部会長	岡本　俊一	伊藤忠テクノソリューションズ株式会社 みらい研究所　リードスペシャリスト
副部会長	西脇　雅裕	みずほリサーチ&テクノロジーズ株式会社 デジタルコンサルティング部　政策・技術戦略チーム マネジャー　※1
委員	佐藤　久信	伊藤忠テクノソリューションズ株式会社 みらい研究所　アソシエイトプリンシパル
委員	川島　耕二郎	伊藤忠テクノソリューションズ株式会社 金融システム開発本部 金融システム開発戦略部　リードスペシャリスト
委員	藤田　健司	ＮＥＣソリューションイノベータ株式会社 社会・通信ソリューション事業部門　レジリエンス・メディア統括部　シニアディレクター
委員	坂本　久	ＮＥＣソリューションイノベータ株式会社 DX ソフトウェア開発事業部門　システム PF 開発統括部 シニアプロフェッショナル
執筆協力者	川嶋　猛	ＮＥＣソリューションイノベータ株式会社 医療ヘルスケア・スマートシティ事業部門 デジタルヘルスケア未来都市統括部　主任
委員	高橋　淳	株式会社ＮＴＴデータ 公共・社会基盤事業推進部　プロジェクト推進統括部技術戦略担当　課長
委員	正木　俊輔	ＴＩＳ株式会社 ビジネスイノベーションユニット データアナリティクスビジネス部　部長
委員	戸田　和宏	株式会社電通総研 オープンイノベーションラボ　グループマネージャ
委員	相田　洋志	株式会社野村総合研究所 デジタルトラスト基盤事業本部 ＩＤソリューション事業部 グループマネージャー
委員	和田　広之	株式会社野村総合研究所 デジタルトラスト基盤事業本部 ＩＤソリューション事

		業部 チーフエキスパート
委員	海老原　圭	三菱総研ＤＣＳ株式会社 産業・公共部門　ERP 事業本部 デジタルイノベーション部第３グループ・課長
ｱﾄﾞﾊﾞｲｻﾞ	富士榮　尚寛	伊藤忠テクノソリューションズ株式会社 みらい研究所　研究所長 一般社団法人 OpenID ファウンデーション・ジャパン代表理事
ｵﾌﾞｻﾞｰﾊﾞ	西本　靖	独立行政法人情報処理推進機構 データベース G　※1
ｵﾌﾞｻﾞｰﾊﾞ	堀越　秀朗	独立行政法人情報処理推進機構 データベース G エキスパート　※1
事務局	溝尾　元洋	一般社団法人情報サービス産業協会 事業推進本部課長
事務局	小泉　真寿	一般社団法人情報サービス産業協会 事業推進本部調査役

（令和 7 年 4 月末時点）

※1 令和 7 年 3 月末時点

1. トラスト、アイデンティティ階層編の目的

これまで、国内においては、データスペースやデータ連携基盤と、Trusted Web の取り組みは密接には絡み合っていなかった。しかし、データスペースやデータ連携基盤や Verifiable Credentials におけるガバナンスの論議の活発化を契機に、アイデンティティ、トラストという共通の接点が生まれる中で、今後の論議の融合が期待される。

データエコシステムの形成に関わる情報サービス関連企業各社を通じ、関係する検討会や団体における検討や整備の取り組みへの貢献を期待し、調査や論点整理、仮説を検討した。

- ✓ 調査や論点整理について
  「2 章 トラスト、アイデンティティの論議の前段として関連する論点」
  「3 章 データスペースに関わるトラストフレームワークの調査」
- ✓ 国内のデータスペースにおける実装の論議において、VCおよび事業者 Digital Identity Wallet（DIW）の活用の仮説について
  「4章 データスペースにおけるトラストやアイデンティティに関わる論議と、Trusted Web の取り組みや、事業者確認や当人認証に関わる論議の融合の期待」

なお、本編の記載内容には、<技術動向編>で紹介した内容が関係する箇所もある為、あわせて参照いただきたい。

2. トラスト、アイデンティティの論議の前段として関連する論点

2.1 トラストの論議の前段として必要となる、事業者確認の論議について

データの共有・利活用を、安全で信頼できる形で実現するには、データ自体およびデータやり取りの真正性やデータエコシステムに関わる様々なステークホルダーの信頼性確保のための「トラスト」の担保が、大きな鍵となる。

「データエコシステムに関わる様々なステークホルダーの信頼性担保」の論議の前段として、（法人および個人事業主を対象とした）「事業者確認」について、公的に認められた網羅性をもった定義やガイドラインが明確でない事も課題の一つと考える。共通認識の元となる定義が明確でない事から、課題に関わる論点の範囲についても曖昧となる懸念がある。

（補足）
なお、本書は、事業者確認の整理を主眼としていない為、詳細については、例えば、一般社団法人 OpenID ファウンデーション・ジャパンの KYC Working Group により、2025 年度に近々公開予定の「（仮）事業者確認に関わる現状整理と課題」等を参照されたい。当節および次節の一部の記載や図表は、KYC Working Group にて検討中の議論を参考に記載している。なお、記載内容には、当部会の独自の見解が含まれることに留意いただきたい。

自然人を対象とした本人確認は、現実の世界に実体が存在する為、信頼性の高いエビデンス（例：本人確認書類等）を軸にした Proofing をするという考え方がとりやすい事を背景に、自然人を対象としたデジタルの本人確認方法は確立されつつあり、セキュリティや利便性の向上において一層の改善が図られている状況にある。

一方、事業者確認は、後述の背景により、完全な確認（Proofing)が困難であり、複数の参考となる信頼できる情報を複合的に確認により、リスクベースで判断していく考え方が必要となる。自然人に対する確認とは異なる考え方が必要となる事も背景に、現状、事業者確認および当人認証の 2 観点において、明確なデジタルの確認方法が確立されていない。

事業者確認において、自然人に対する確認とは異なる考え方が必要となる背景としては、以下が関係する。

- ✓ 現実の世界に実態が存在しない
- ✓ 主体を構成する要素が複雑
  ※確認対象の主体が、法人格、事業者に関係する自然人、法人と自然人の関係性にまたがり、各々の主体に対する確認要素が異なる
- ✓ 第三者が法人内部情報について「完全な確認」をする事が困難
  ※例えば、内部組織や事業活動の実態有無等を外部から完全な確認は難しい

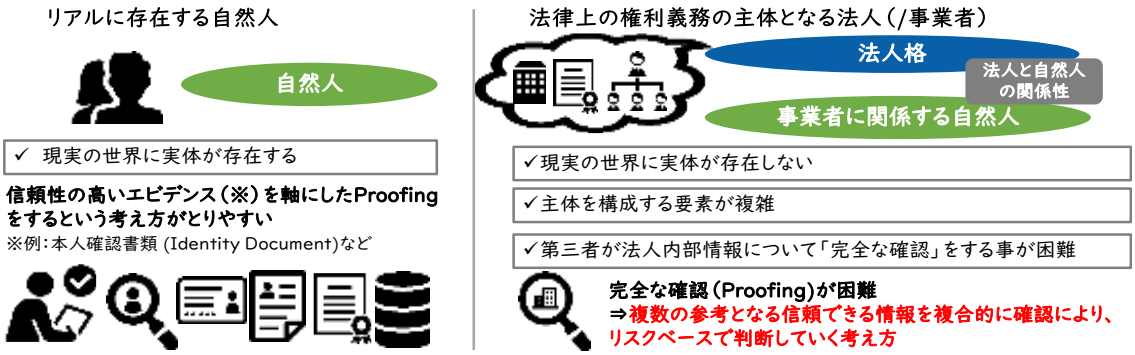


図 2-1 事業者確認の特徴

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

例えば、法人格のある事業者については、登記情報等により法的な実在性を確認するとともに、事業者や組織の所在地にオフィス等が実際に存在しているか等の物理的な実在性の確認や、部門や事業所等の内部組織の実在性の確認や、事業者としての意思表示ができる代表者等（自然人）に対する本人確認や、取引の任にあたっている担当者（自然人）の所属確認や権限確認を行うといったように、業務目的によって確認すべき範囲は様々であるが「様々な確認事項によって複合的に判断」することとなる。

また、個人事業主の実在性確認については基本的には個人に対する本人確認となるが、事業性に関わる実在性について第三者の実態確認が難しく、別途、確定申告書や納税証明等の公的情報等に基づく事業性に関わる実在性確認を行うケースも存在する。

事業者確認の大きな分類		要素
1. 事業者の身元確認（Identity Proofing）		
	1.1.法人格に対する確認	法的実在性確認、または公的情報等に基づく実在性確認
		物理的実在性確認
		法人等に属する内部組織の実在性確認
	1.2.事業者に関連する自然人に対する確認	所属確認（代表者等、従業員、代理人等）
		取引の任に当たっている事の確認（権限確認）
		（代表者等取引の任に当たっている自然人の）事業者に関連する自然人の「個人」としての本人確認
2. 意思の確認（intention）		法人格の当該行為自体に関わる意思の確認（内容確認をしている事の確認含む）
3. 顧客管理（Customer Due Diligence）		事業の内容の確認
		事業活動の実態有無の確認（当該事業者や組織の運営状態を確認）
		実質的支配者（BO）の確認
		反社確認
		資産及び収入の状況の確認
		信用情報確認

図 2-2 事業者確認の大きな分類と要素

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

事業者確認の要素が多岐に渡る事を背景に、今後の事業者確認のデジタル手法の確立にむけた検討に際して、2つの観点のハードルが存在する。

1. 様々な確認要素および様々な形態の事業者を網羅的にカバーする、官民の信頼できる情報源が存在しない
2. 様々な確認要素を一元的に円滑に確認できるデジタル手法が存在しない

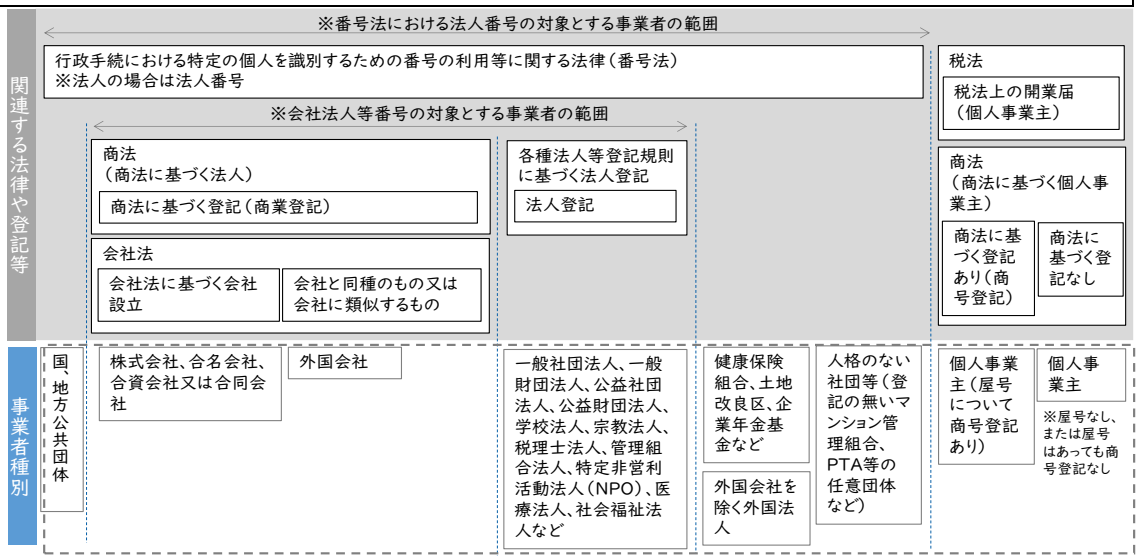


図 2-3 事業者の様々な形態

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

官民の信頼できる情報源の例として、公的なレジストリとしては、登記情報（商業登記や法人登記の登記情報）、法人番号公表サイトや、法人番号に基づく基本3情報にオープンデータを合わせた gBizINFO 等が存在し、民間のレジストリの例としては、企業信用調査会社（帝国データバンクや東京商エリサーチ等）の企業調査書（および企業情報データベース）などが存在するが、以下のような課題がある。

- ✓ 公的なレジストリに関しては、関連する法律等の目的が異なる事を背景に、対象範囲の事業者の相違や保有情報の相違が大きく、情報鮮度に関わる課題も存在する
- ✓ 企業信用調査会社の保有する情報項目とカバー率および情報鮮度は相応に高いとはいえ、網羅性があるわけではない
- ✓ 特に、個人事業主含む小規模事業者については、全体的に情報不足といえる

（なお、デジタル庁において、法人ベース・レジストリの検討整備が計画されており、将来、利用可能になると想定され課題の軽減にはつながると想定しているが、法人ベース・レジストリ単体での課題の解決は困難と想定する）

現状の事業者確認に関わるデジタル手法には以下のような例があるが、事業者確認要素の内、一部の要素のみをカバーするものとなっている。

商業登記電子証明書を用いた電子署名を用いた電子申請や取引に関わる情報の確認、
登記情報提供サービスの照会、法人番号公表サイトや gBizINFO の照会等、
企業信用調査会社（例：TBD や TSR 等）の企業情報照会サービス、
公的個人認証他、電子委任状　等

現状のデジタル手法は、各々の目的に対応するものであり、確認可能な要素の範囲は限定的である。複数の手法を使い分けする必要がある場合がある事や、確認要素の一部については、デジタル手法による確認が困難である現状がある。

- ✓ 現状、事業者確認の要素を、「一元的に円滑に確認できるデジタル手法」が存在せず、情報取得の負担が大きい

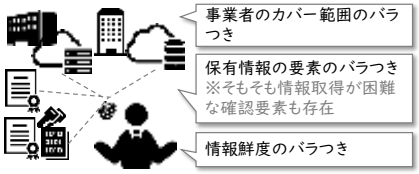
【背景】事業者確認の要素は多岐にわたっている

事業者確認の大きな分類		要素
1. 事業者の身元確認（Identity Proofing）		
	1.1.法人格に対する確認	法的実在性確認、または公的情報等に基づく実在性確認
		物理的実在性確認
		法人等に属する内部組織の実在性確認
	1.2.事業者に関連する自然人に対する確認	所属確認（代表者等、従業員、代理人等）
		取引の任に当たっている事の確認（権限確認）
		（代表者等取引の任に当たっている自然人の）事業者に関連する自然人の「個人」としての本人確認
2. 意思の確認（intention）		法人格の当該行為自体に関わる意思の確認（内容確認をしている事の確認含む）
3. 顧客管理（Customer Due Diligence）		事業の内容の確認
		事業活動の実態有無の確認（当該事業者や組織の運営状態を確認）
		実質的支配者（BO）の確認
		反社確認
		資産及び収入の状況の確認
		信用情報確認

【背景】事業者の種別や形態も様々（例：登記有無、個人事業主）

現状の課題

“官民の信頼できる情報源”において、「事業者のカバー範囲」「事業者確認の要素」「情報鮮度」の、3つの観点で確認可能な範囲のバラつきが大きい



現状、事業者確認の要素を、「一元的に円滑に確認できるデジタル手法」が存在しない

※商業登記電子証明書、登記情報提供サービス、法人番号公表サイト、gBizINFO、企業信用調査会社の企業情報照会サービス、電子委任状など

図　2-4　事業者確認の課題と背景の振り返り

（出所）一般社団法人　OpenID ファウンデーション・ジャパン　KYC Working Group　法人 KYC 分科会の議論より

以下の記載内容には、当部会の独自の見解が含まれることに留意いただきたいが、今後の論点の仮説を提示する。「データエコシステムに関わる様々なステークホルダーの信頼性担保」の論議の際には、以下の2つのポイントを意識する必要があると考える。

- ➢ 事業者確認に関わる様々な確認要素について、官民の複数の信頼できる情報源から様々な種別の参考情報を取得し、複合的に確認する事により確からしさを高める事（トラストを高める事）を、「容易にする仕組みづくり」が必要
- ➢ 今後、上記を「一元的に円滑に確認可能なデジタルインターフェースの標準的な手法」について、継続的な検討が必要

仕組みづくりに際して、テクノロジーとガバナンスの両輪の検討が必要となる。

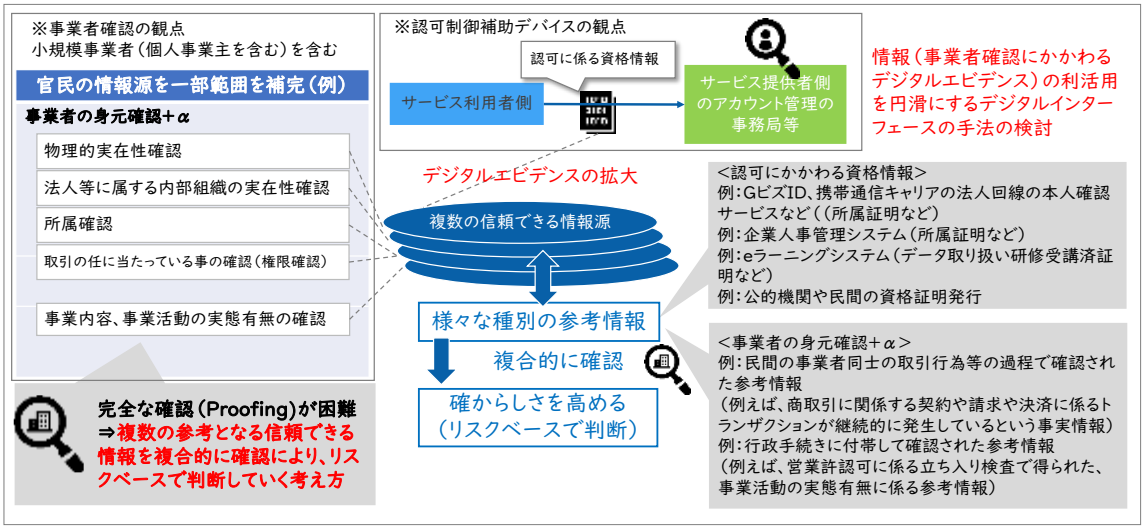


図 2-5 データエコシステムの様々なステークホルダーの信頼性担保の論議にも関わる論点

その上で、事業者確認要素の単位レベル（例：物理的実在性確認、内部組織の実在性確認、所属確認、権限確認、事業活動の実態有無の確認）での保証レベル（アシュアランスレベル）のガイドラインの検討が必要ではないだろうか？

2.2　事業者の当人認証について

事業者は法律上の権利義務の主体ではあるが現実世界の実体がない為、代表者や権限を与えられた担当者といった自然人が、実際にはオンラインのサービスを操作者として、利用することとなる。（また、今後は、操作者として、自然人だけでなく、AI 等も念頭にいれる必要性が高くなる）

データエコシステムに対するアクセス制御にも直結する事から、特に事業者の当人認証において、認証と認可を区別しながら論じる必要、および、法人と事業者に関係する自然人との関係性についても留意しながら論じる必要がある

＜補足＞

- ✓ 認証/当人認証（Authentication）は、申請者の当人性を確認し、「正しい利用者に」利用させる目的であり、対象物（リソースまたは機能）を利用しようとする者が、身元確認時に登録された者と同一の人物であることを、申請者と紐づけて登録した認証器を用いて確認し、信用を確立するプロセスのことをいう[1]。
- ✓ 認可（Authorization）は、「正しく利用させる」目的であり、対象物（リソースまたは機能）にアクセスする許可をユーザーに付与するプロセスの事をいう。

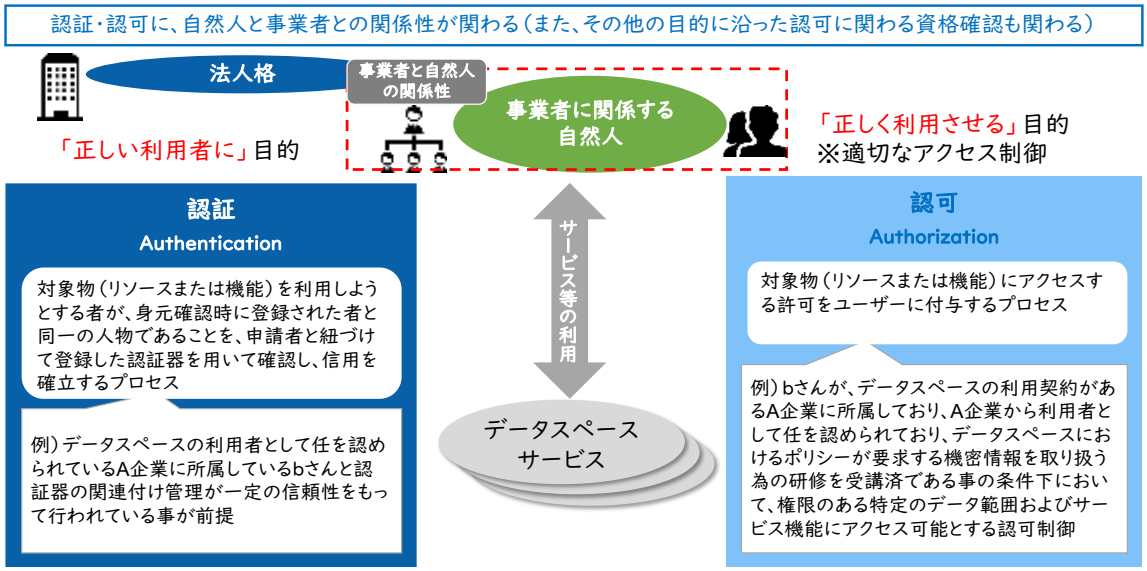


図 2-6 事業者の当人認証に関わる視点

[1] 出所：行政手続等での本人確認における デジタルアイデンティティの取扱い に関するガイドライン（案）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/058ea13e-58e4-4e77-b18f-24833a65c7b1/3c596c7a/20250304_meeting_identification-guideline-revision_outline_02.pdf
「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」2019 年（平成 31 年）2 月 25 日　各府省情報化統括責任者（ＣＩＯ）連絡会議決定
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf
なお、当該ガイドラインは上記の通り改定の検討会が存在し、今後、用語定義の改定の可能性もある為、ガイドライン（案）の用語定義に寄せて記載。

実際の事業者向けのデジタルサービスにおける、事業者の当人認証の単位や認証方式の強度、アカウント管理の業務運用の在り方の相違の背景には、認可に関わるアクセス制御で必要となる制御単位の相違や、当該サービス等のリスクと責任の範囲の相違が関係すると考えられる。

図5-5：事業者向けの当人認証の姿の相違と背景

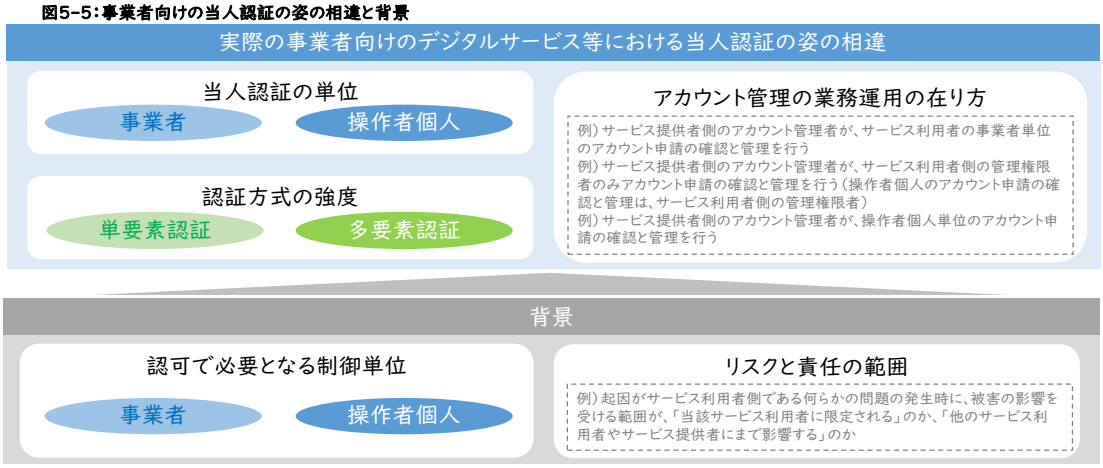


図 2-7 事業者向けのデジタルサービスにおける当人認証の姿の相違の背景

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

当人認証の単位の相違	アカウント管理の業務運用の在り方の相違（例示）	
A. 事業者単位で共通のIDによる認証情報の確認	A	✓ サービス提供者側のアカウント管理者により、事業者単位のアカウント管理を行うケース
B. 操作者個人単位のIDによる認証情報の確認	B-1	✓ サービス提供者側のアカウント管理者により、サービス利用者側の管理権限者のアカウント管理のみを行う。 ✓ その上で、サービス等を利用する事業者側の管理権限者により、サービス提供者側のアカウント管理機能を利用し、当該事業者の操作者個人単位のアカウント管理が行われるケース （≒操作者単位のアカウント管理の業務運用は、サービス利用者側の管理権限者に権限移譲） 例）請求書電子化サービス事業者や中小企業向けEDIサービス事業者の提供サービス
	B-2	✓ （契約等は事業者や組織単位であるが）サービス提供者側のアカウント管理者または機能により、サービス利用者側の操作者個人単位のアカウント管理も行うケース 例）名刺管理サービス事業者や企業向け福利厚生サービス事業者の提供サービス
	B-3	✓ 操作者個人単位で利用申請（または契約）が必要であり、サービス提供者側のアカウント管理者により、操作者個人単位のアカウント管理を行うケース 例）府省共通研究開発管理システム（e-RAD）への民間事業者に所属する民間研究員として登録と利用

図 2-8 アカウント管理の業務運用の在り方の相違

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

一方、独立行政法人情報処理推進機構の「情報セキュリティ 10 大脅威 2025」でも、“サプライチェーンの弱点を悪用した攻撃”“内部不正による情報漏えい等の被害”“標的型攻撃による機密情報の窃取”をはじめ、当人認証の強化が求められる事につながる脅威は、毎年変わらず上位にあがっている。また、データスペースの進展など社会のデジタル化の進展により、事業者向けデジタルサービス等で取り扱われる機密性の高い情報は、年々拡大しており、それに伴い事業者向けデジタルサービスの全体的なリスクも拡大する傾向がある。

データエコシステムにおける、より安全で適切な当人認証の制御の実現において、「正しく利用

させる」目的で付帯する「認可」の観点も、今後増々重要な論点となる。その上で、派生的に「アカウント管理の業務運用の負担の増大」に関わる課題の留意が必要となる。つまり、より安全かつ適切な制御と、アカウント管理の業務運用の負担の軽減の「両立」について検討する事が、今後の重要な論点となってくる。

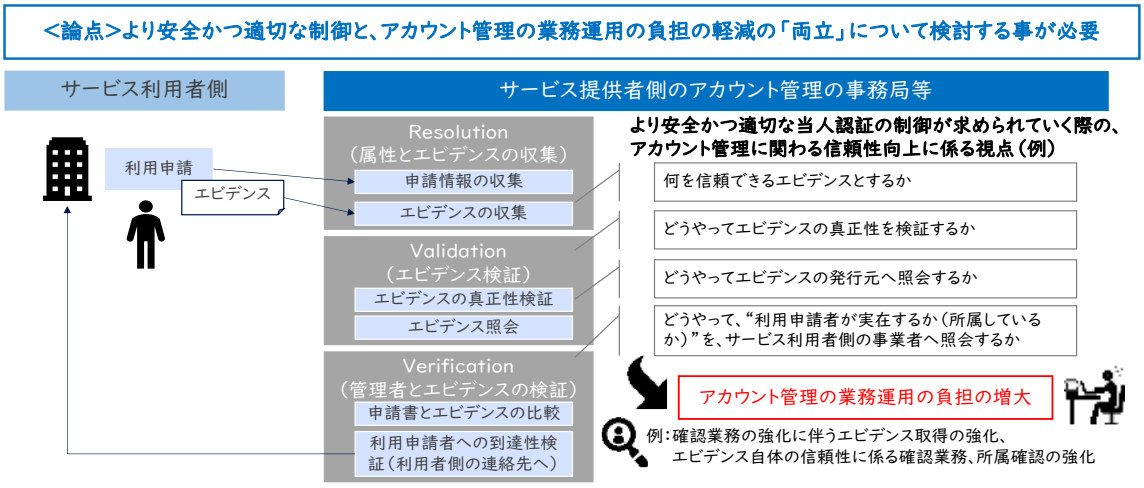


図 2-9 今後の事業者の当人認証の重要な論点

(出所)一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

以下の記載内容には、当部会の独自の見解が含まれることに留意いただきたいが、今後の論点の仮説を提示する。「データエコシステムに関わる様々なステークホルダーの信頼性担保」の論議の際、事業者の当人認証について、認証とあわせ"認可"について焦点をあてつつ、以下の観点で、継続的な検討が必要となる。

- "属性(資格情報)に応じたアクセス制御の強化の必要性の拡大" を念頭におきつつ、より安全かつ適切な認証・認可の制御と、アカウント管理の業務運用の負担の軽減を「両立」する事が可能な「事業者の当人認証および認可の標準的な手法、およびアカウント管理業務の自動化率の向上」 について、継続的な検討が必要
- その上では、様々な"認可"の目的に対し必要となる、様々な確認要素(例:所属確認、任にあたっている事の確認・権限確認、資格取得、データ取り扱いに関わる e ラーニングの受講済証明)について、アカウント管理業務の自動化率の向上の観点も踏まえながら、機械可読性と非改竄性が担保されたデータ形式で、複数の信頼できる情報源から様々な種別の参考情報を取得し、円滑かつ一元的な提示を可能にする検討が必要

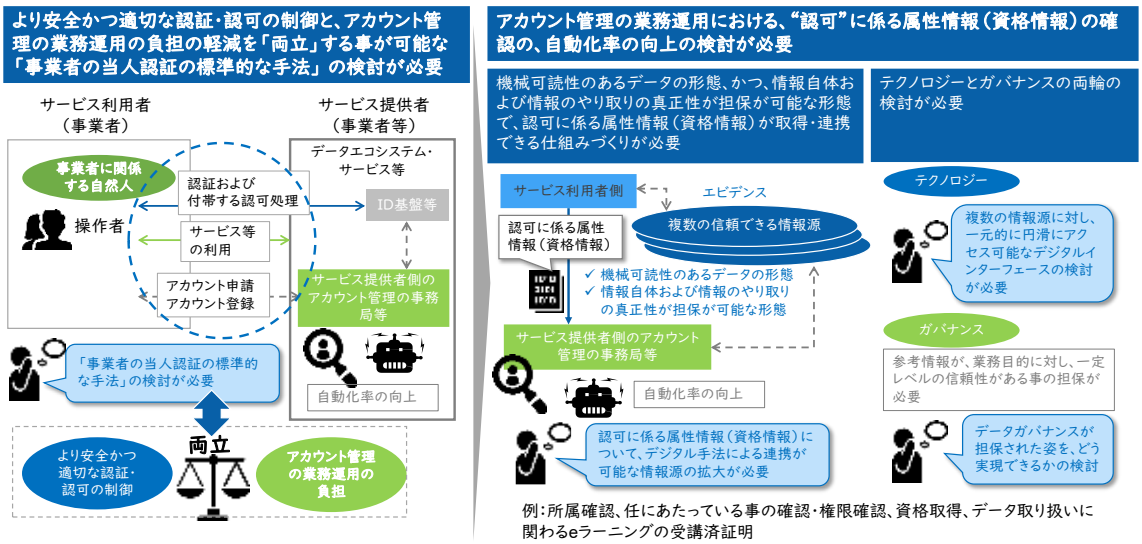


図 2-10 今後の検討ポイントの仮説提示

2.3 Trusted Web と、データエコシステムのトラストやアイデンティティの論議との関連性

データスペースやデータ連携基盤において、データそのものの真正性やデータやりとりに関わるステークホルダーの本人性の信頼性確保のためのトラストの論議がある。

その要素の一つとして、「データスペースに関わる主体の真正性・実在性に関するリスク」が存在する（産業データスペースの場合の主体は、事業者）。データスペースのサービス利用時の認証・認可の検討や、データスペースへの各ステークホルダーの新規参加（オンボーディング）や継続参画（オンゴーイング）の際の適格性の認定の検討などに関係してくる。なお、ステークホルダーの例としては、データ提供側事業者や利用側事業者（両面を兼ねる事も多い）、データスペースのマーケットプレイスにおけるアプリケーション・サービスの提供事業者などがある。

主体の真正性・実在性の検証可能性の向上には、Verifiable Identity を中心に Verifiable Data の関係が深い（なお、最終的には Verifiable Identity、Verifiable Data、Verifiable Messaging は全て関係してくる）。Verifiable Identity の実装において、VC を採用するケースも多く、同時に Verifiable Data の実装においても同様である。

構成技術要素　※定義は、内閣官房/デジタル庁 Trusted Web推進協議会 ホワイトペーパーより

国際標準化団体（例示）	W3C（World Wide Web Consortium） IETF（Internet Engineering Task Force）	OpenID Foundation	ISO（International Organization for Standardization）
代表的な規格（例示）	• Verifiable Credentials Data Model（VCDM） • Decentralized Identifiers (DIDs) • SD-JWT-VC	• OpenID for Verifiable Credential Issuance (OID4VCI) • OpenID for Verifiable Presentations(OID4VP) • Self-Issued OpenID Provider(SIOP)	• ISO 18013-5:2021（mdoc data model） • ISO 23220-1:2023

図 2-11 Trusted Web の実装に関わる技術要素の超概要

（出所）Trusted Web 推進協議会のホワイトペーパーを基に作成

「データスペースに関わる主体の真正性・実在性の検証可能性の向上」において、Verifiable Identity を VC で表現しつつ、署名検証に加え Verifiable Data として同一主体である事や実在性や適合性などの確認を、IHV モデルで実現するイメージを、図2-12、2-13で示す。

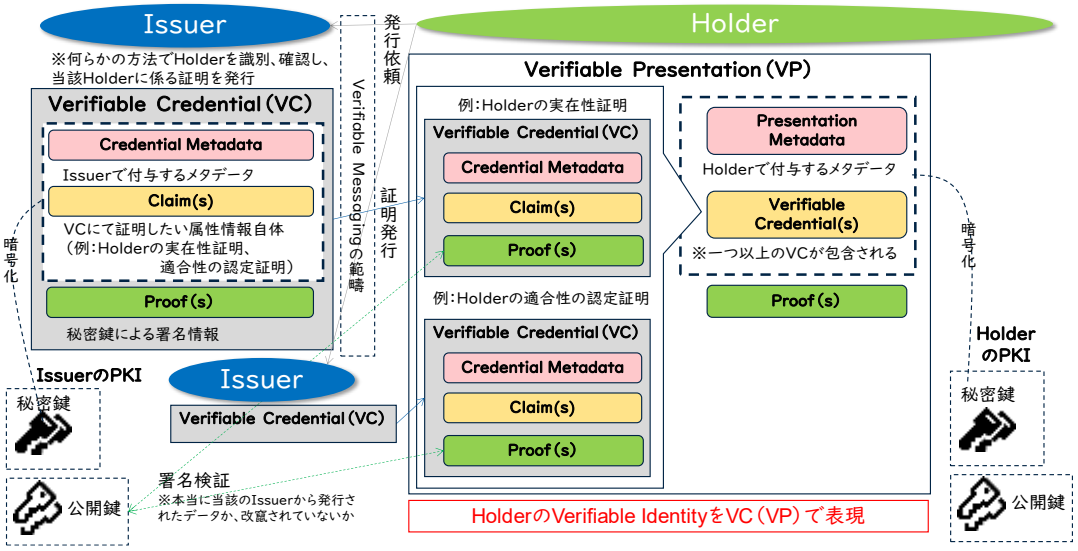


図 2-12 主体の真正性・実在性の検証可能性の向上イメージ①（Issuer⇒Holder）

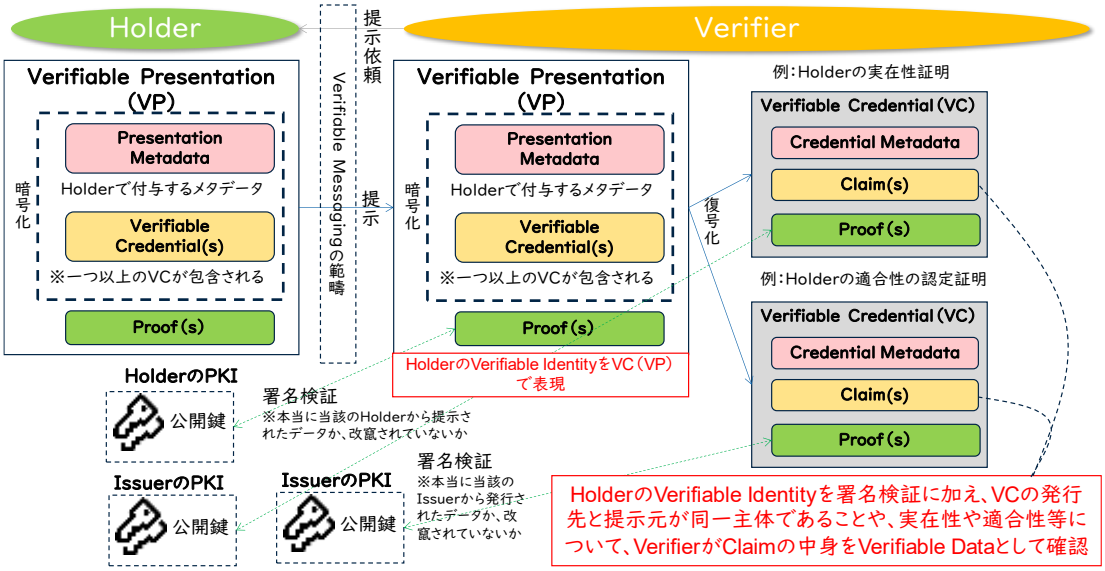


図 2-13 主体の真正性・実在性の検証可能性の向上イメージ②（Holder⇒Verifier）

また、主体の真正性・実在性は、複数の証明書の組み合わせによる総合的な確認が必要になるケースも多く、複数の証明書をまとめて提示する際に、暗号学的に情報の真正性を担保が可能なVC/Verifiable Presentation（VP）の活用は技術的選択肢として有益となる。要件によっては、選択的情報開示やゼロ知識証明（ZKP/Zero-Knowledge Proof）関連の各種技術も有益と考える。

関連仕様の例：当該目的に対し、証明書の必要範囲のみを選択的開示を可能とする IETF（Internet Engineering Task Force）の SD-JWT-VC の活用

なお、<技術動向編>2.2.3でふれたが、Verifiable Identity コミュニティ（送受信をする

主体の集合）において、信頼の起点を含む情報を一定のガバナンス下で共有できる仕組みづくり（例：Trusted Identity List）により、Verifiable Identity の信頼の確立が支援される。

Gaia-X の Trust Framework は、IHV モデルをベースにしたフレームワークであり、今後、国内のデータ連携基盤は、Gaia-X の Trust Framework と相互連携するための仕掛けが求められることが予想できる。その際に、Trusted Web で示されたガバナンスの考え方も参考にトラストフレームワークを整備し、海外データスペースとのアイデンティティとトラストに関わる相互運用性を確保するなども期待できる。

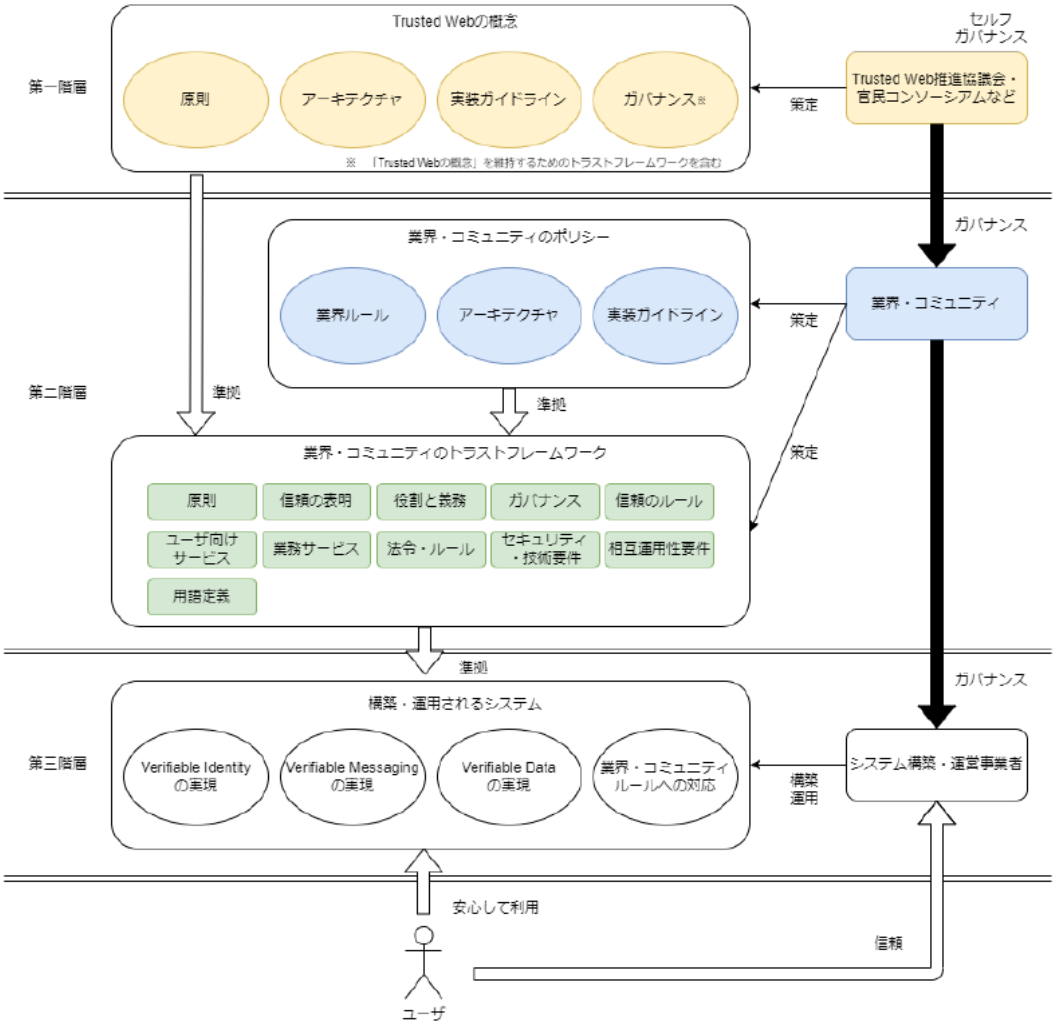


図 2-14 Trusted Web におけるガバナンスの全体像

（出所）https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb_implementation.pdf

3. Gaia-X のトラストフレームワーク、Catena-X オンボーディングプロセス、eIDAS2.0・EUDIW トラストフレームワークとの関係

3.1 Gaia-X のトラストフレームワークについて

Gaia-X は、Gaia-X エコシステムにおける「ID とトラスト」および「コンプライアンス」を実現するために Gaia-X Trust Framework を策定している。また、そのフレームワークの具体的な実装として、Gaia-X Digital Clearing House (GXDCH)という仕組みが設置されている。GAIA-X Trust Framework と GXDCH は、GAIA-X エコシステムにおける信頼性と相互運用性を確保するための重要な要素である。

Gaia-X Trust Framework と GXDCH は、Gaia-X エコシステムの信頼性と透明性を確保するために協調して機能する。Gaia-X Trust Framework は、Gaia-X エコシステム内の信頼性を確保するためのルールや要件を定めている。一方、GXDCH は、そのルールに基づき参加者やサービスの適合性を検証・認証し、エコシステム全体の信頼性を技術的に担保する。これにより、Gaia-X 内での安全なデータ共有と相互運用性を確保する。

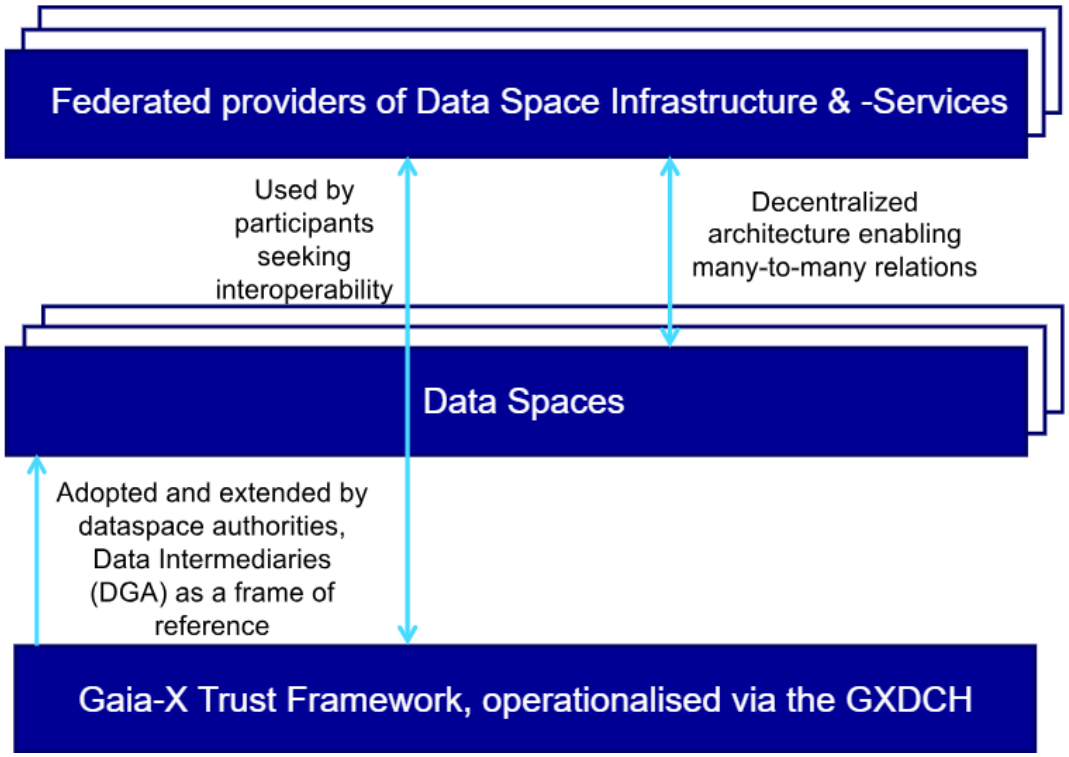


図 3-1 相互運用可能なデータ空間の基盤としての Gaia-X Trust Framework

（出所）

https://docs.gaia-x.eu/technical-committee/architecture-document/latest/gx_conceptual_model/

3.1.1 Gaia-X Trust Framework の概要

Gaia-X Trust Framework は、Gaia-X エコシステム内のすべての参加者（クラウドプロバイ

ダー、データ提供者、データ利用者など）が従うべき最小限のベースラインを定義するルールセットである。このルールセットは、Gaia-X によって定義された要件を運用するものであり、ポリシールールとラベリング文書、アーキテクチャ文書で定義されている。

ポリシールールは Gaia-X Self Description (SD: 自己記述)と呼ばれ、W3C Verifiable Credentials Data Model（VCDM）[2]に準拠した機械可読形式で記述される。

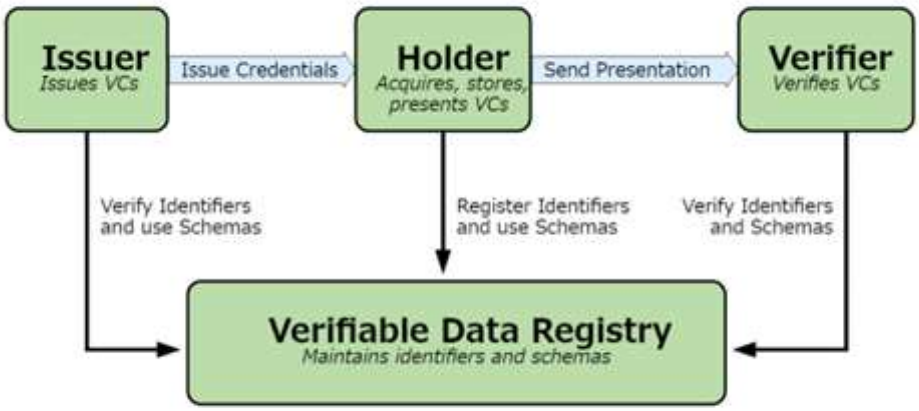


Figure 1 The roles and information flows forming the basis for this specification.

図 3-2 参考: W3C Verifiable Credentials Data Model

（出所）https://www.w3.org/TR/vc-data-model/#ecosystem-overview

(補足) Gaia-X の SD の概要

Gaia-X の SD は、Gaia-X 概念モデルのエンティティを、VCDM に準拠し記述する。これには、参加者自身の自己記述だけでなく、プロバイダーからのリソースとサービス提供も含まれる。明確に定義された SD のスキーマにより、自己記述の統一された表現が可能になる。SD により、Gaia-X 内のエンティティを検索したり比較したりすることが可能になる。

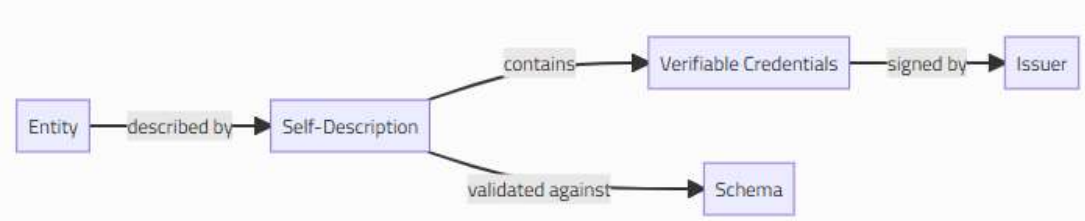


図 3-3 自己記述の構造

（出所）https://docs.gaia-x.eu/technical-committee/architecture-document/22.04/self-description/

SD は、RDF データモデルで表現されたエンティティに関するアサーションを JSON-LD 形式

[2] https://www.w3.org/TR/vc-data-model/#ecosystem-overview

で W3C 仕様に基づく VC／VP として表現する。VC と VP の両方に、信頼レベルを高めるための暗号署名が付属する。なお、SD 内の VC は、異なる信頼できる当事者によって署名される場合がある（SD 内の複数の VC の発行者が異なる場合がある）。たとえば、認証評価機関は、認証結果を VC としてアサートする場合があり、当該の SD に含めることができる。

3.1.2 Gaia-X Digital Clearing House (GXDCH)の概要

GXDCH は、Gaia-X Trust Framework の実装を技術的に支援するための仕組みである。具体的には、Gaia-X のエコシステムに参加する組織やサービスが Gaia-X Trust Framework に準拠しているかを検証し、適合性を確認する役割を果たす。Gaia-X は、安全で信頼性が高く、透明性のあるデータ交換のための一連のポリシー、ルール、仕様、検証フレームワークを通して、EU のデータスペースの標準の作成に取り組む。GXDCH は、単一の中央機関に依存しない信頼性、透明性、相互運用性の確保を目的に、Gaia-X で定義されるルール（Gaia-X Trust Framework）を基に、Gaia-X に準拠しているかを検証する仕組みを提供する。

GXDCH は、次の3つのコンポーネントで構成される。

I. Gaia-X Compliance Service
II. Gaia-X Registry Service
III. Gaia-X Notarization Service

【Ⅰ. Gaia-X Compliance Service】

Gaia-X Compliance Service は、VCDM と同様の構成で、発行者/保有者/検証者/検証可能なデータレジストリを基本構成要素として、SD を VC として検証する。

次の図で説明すると、Gaia-X Compliance Service は Verifier(検証者)であり、データスペースへの参加者は Holder(保有者)、トラストアンカーは Issuer (発行者)、Gaia-X Registry Service は Verifiable Data Registry (検証可能なデータレジストリ) にあたる。

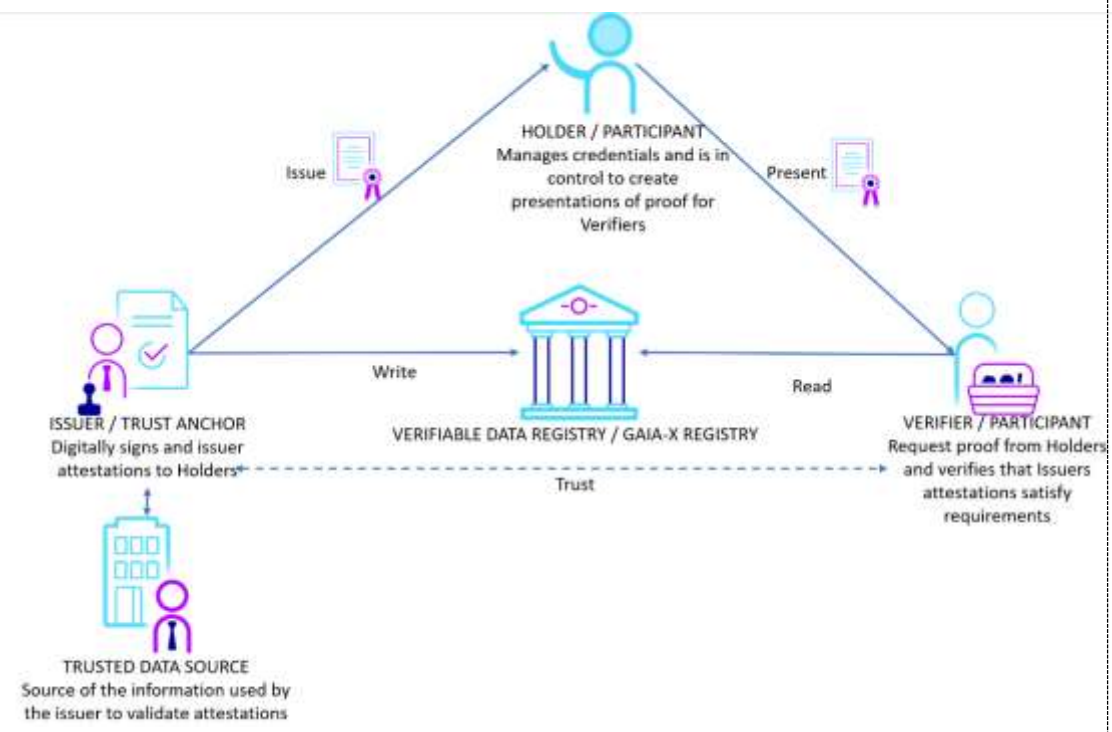


図 3-4 GXDCH における各サービスの配置と VC 検証の流れ

（出所）https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/trust_anchors/

Gaia -X Compliance Service は次の要素を検証する。

✓ 参加者から VP を受け取り、VP に含まれている VC が Gaia-X で定義された形式に準拠していること

✓ 「VC の発行者」が検証可能データレジストリ（Gaia-X Registry）に適切に登録されているこ

✓ 提供された情報が一貫していること

Gaia -X Compliance Service においては、情報の発行者とトラストアンカーは同一主体となる。トラストアンカーは、参加者によるクレーム（資格情報）を裏付けるものである。クレームが Gaia-X Trust Framework に準拠するには、クレームに署名するために使用されるすべてのキーペアの証明書チェーンに少なくとも 1つのトラストアンカーが含まれている必要がある。有効なトラストアンカーのリストは Gaia-X レジストリに保存される。

Gaia-X Trust Framework で有効なトラステッドデータソースは次のいずれである必要があり、Issuerはトラステッドデータソースに登録されている必要がある。

A) 信頼できるデータソースを直接管理するエンティティ

EORI: 欧州委員会 API

LEI Code: グローバル法人識別子 (GLEIF) API

local: OpenCorporate API

VAT ID: 欧州加盟国または北アイルランドの場合、VAT 情報交換システム API

B) Gaia-X によって認定されたエンティティ

State: 州認定の ID 発行者または EV SSL 発行者

eIDAS: eIDAS 規則 (EU) No 910/2014 で定義されている電子署名の適格証明書の発行者

EV SSL: Extended Validation (EV) Secure Sockets Layer (SSL) 証明書の発行

【Ⅱ. Gaia-X Registry Service】

Gaia-X のエコシステムにおけるガバナンスのバックボーンであり、次の情報を管理する。

- ✓ トラストアンカーのリスト（※GXDCH においては、情報の発行者と同一主体）
- ✓ トラストアンカーの検証プロセスの結果
- ✓ トラストアンカーの ID 失効
- ✓ Gaia-X における投票及び結果
- ✓ Gaia-X VC の形式とスキーマ
- ✓ Gaia-X カタログ認証情報の URL

また、次の機能を提供する。

- スマートコントラクト機能と分散ネットワークの提供
- 完全性、非拒絶、機密性を保証するメカニズム
- Gaia-X Compliance Service インスタンスへのアクセス
- 完全運用され、分散型で、簡単に検索可能なカタログの提供
- Gaia-X メンバーシップ規則に違反した参加者 ID および認証情報 URI の一覧
- エコシステムにおけるトークンの利用

【Ⅲ. Gaia-X Notarization Service】

認証評価機関は、参加者から企業データを含む自己記述を VC として受け取り、受け取った VC を Gaia-X ルールに従って検証する。検証の結果問題が無ければ、受け取った VC を検証済みの Gaia-X VC として参加者に返却する。Gaia-X Notarization Service は、利用者から Legal Registration Number（法定登録番号）を含んだ自己記述の VC を受け取り、その法定登録番号が有効であることを確認する。

なお、法定登録番号は以下のものを使用することができる。

- VAT ID： 付加価値税納税者番号（各 EU 加盟国にはその国独自の VAT ID が存在する）
- LEI Code： 取引主体識別子（国際的な識別子　LEI：Legal Entity Identifier https://www.gleif.org）
- EORI： 経済事業者登録識別番号(EU 内で国際貿易を行う企業や個人に割り当てられる固有の識別子)

3.2 Catena-X のオンボーディングプロセスにおける GXDCH の動作

Catena-X では、Gaia-X Trust Framework に準じたトラストの確保を図っており、GXDCH に則ったオンボーディングプロセスが運用されている。Catena-X で参加者になるためには、Catena-X への登録プロセスの実行が必要となる。登録プロセスは、Catena-X ネットワーク内での全ての活動に必須の要件であり、信頼を支える基礎となる。

3.2.1 登録プロセスの概要

登録プロセスは次の流れで実行される。

① 最初の連絡

Catena-X では、招待ベースの登録プロセスが基本となる。Catena-X に参加する企業（参加者）は次のいずれかの方法で Catena-X に連絡できる。

(ア) Catena-X の現会員が別の会社を候補として提案

(イ) 候補者が見本市やその他のイベントでアプローチを受ける

(ウ) 企業が Catena-X ホームページ経由で Catena-X に連絡

② 招待

オンボーディングサービスプロバイダーは、招待する会社の事前に特定された連絡先担当者に招待メールを送信する。このメールによりオンボーディングに関する登録ツールへの一時的なアクセスが許可される。

③ 企業データの収集

Catena-X は参加者から次のデータを収集する。

- 会社名
- 番地、家番号、郵便ポスト
- 郵便番号（国によって異なる）
- 市
- 国
- 法定登録番号
- 地域・州（オプション）

④ 利用規約への同意

オンボード対象の企業は次で構成されるフレームワーク契約に同意する必要がある。

- ✓ オペレーター条件
- ✓ データスペース条件

✓ CX 条件（選択した”企業の役割”によって異なる）

（補足）Catena-X ネットワーク内での”企業の役割”とは、次にあげるものである。

- Active Perticipant: データ プロバイダー、データ コンシューマー、またはアプリ ユーザーのシナリオをカバー
- App Provider: CX マーケットプレイスを通じてアプリケーション ソフトウェアを提供
- Service Provider: CX メンバーにデータスペース サービス オファリングなどのサードパーティ サービスを提供
- Onboarding Service Provider: 他の企業が Catena-X に初めて登録する際に支援

⑤ 企業データの検証

参加者は企業データと利用規約を含めた SD を作成し、Gaia-X が用意している登録用ウィザードまたは CLI によって SD を GXDCH に送付する。GXDCH は自己記述の正確性と完全性を確認するために次を検証する。

✓ 必須フィールドが全て入力されていること

✓ 法定登録番号の形式と正確性を検証

✓ 参加者（企業）の適合証明を検証

⑥ ビジネスパートナー番号の生成

検証が成功すると、参加者に Catena-X 固有のビジネスパートナー番号 (BPN) VC と Catena-X 固有のメンバーシップ VC が発行される。ビジネスパートナー番号は、データスペース内で会社の一意の識別子として機能する。

⑦ ウォレットテナントの作成と資格情報の保存

新しい参加者（企業）には、ビジネスパートナー番号が発行されると Wallet サービスでテナントが提供される。ウォレットテナントは安全にプロビジョニングされ、承認された個人のみがアクセスできるようにする必要がある。参加者は独自の分離されたウォレットテナント/インスタンスでビジネスパートナー番号やデジタル資格情報、資産を安全に保存及び管理する。

⑧ 登録承認とデータスペースへのアクセス

全てのチェックに合格した場合にのみ、Catena-X はサービスへのアクセスを提供する。一つまたは複数の検証手段に合格しなかった場合、Catena-X は登録を拒否するか、修正のために登録を延期する。

（補足）

以上が Catena-X のオンボーディングプロセスである。このオンボーディングプロセスの「⑤企業データの検証」の際に、Gaia-X Digital Clearing House（Registry/ Compliance service/ Notarization service）は次の様に動作する。

1. 参加者は、法定登録番号が含まれた企業データを自己記述の形式で作成し、Gaia-X Notarization Service に送付し、Gaia-X 形式の VC を取得する
2. 取得した VC と利用規約を含んだ VP を生成し、Gaia-X Compliance Service に送付する
3. Gaia-X Compliance Service は、送付された VP に含まれる VC を検証し、各 VC のトラストアンカーが Gaia-X Registry に登録されているかどうかを確認する

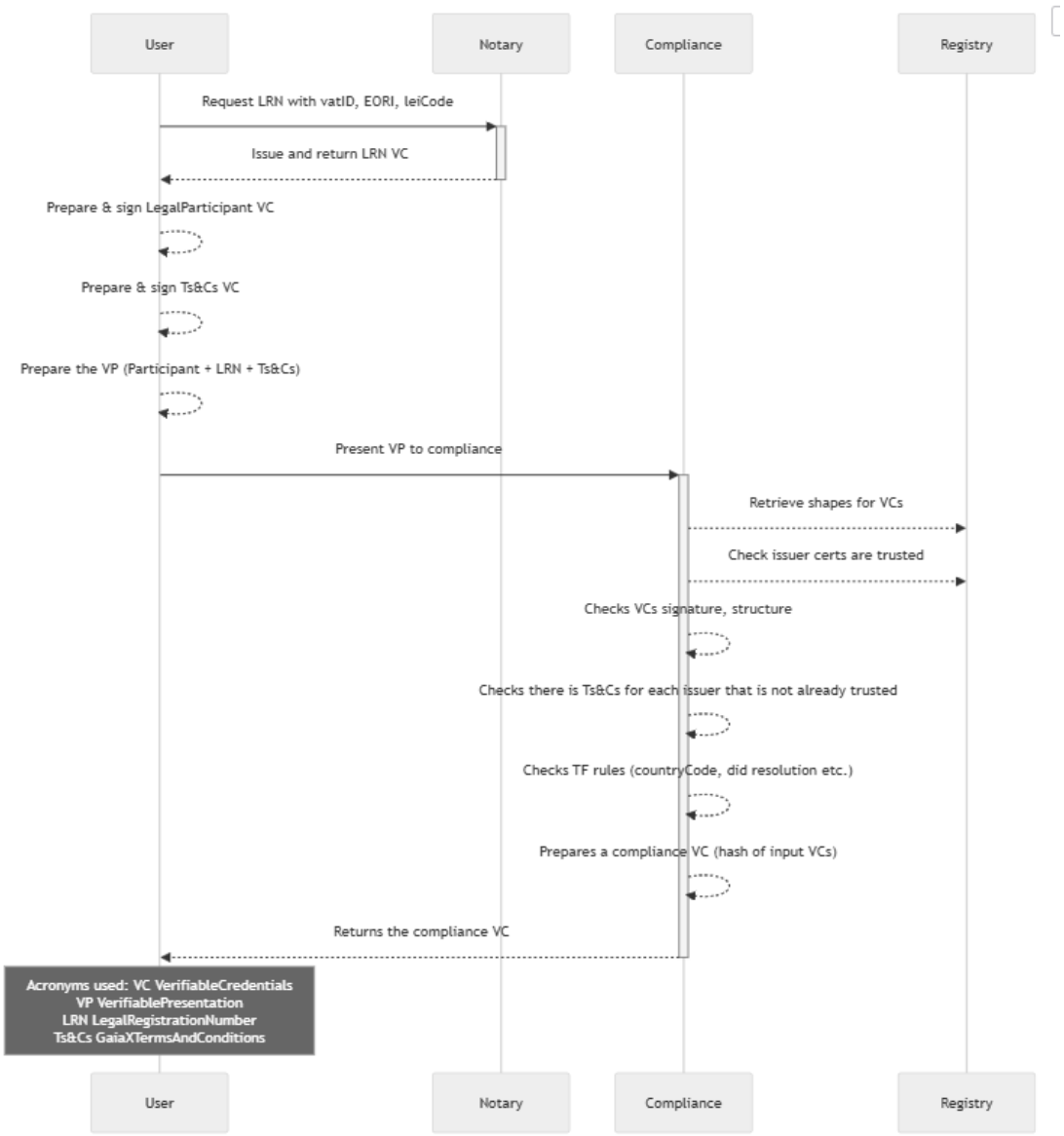


図 3-5 Catena-X オンボーディングプロセスにおける Gaia-X Digital Clearing House の動作

（出所）

/https://gitlab.com/gaia-x/lab/compliance/gx-compliance/-/blob/development/docs/api-usage.md?ref_t

ype=heads

3.2.2 Gaia-X Trust Framework と eIDAS の関係

Gaia-X Compliance Service は、自己記述を VC として検証する。Gaia-X Trust Framework に準拠して VC として検証するには、VC に含められたクレームに署名するために使用されるすべてのキーペアの証明書チェーンに少なくとも 1つの トラストアンカー（証明書の信頼を担保する基準、その情報が正しいと判断できる根拠を示す存在）が含まれている必要がある。トラストアンカーは、Gaia-X Trust Framework における「発行者」であり、それは eIDAS（electronic identification, authentication, and trust service）規則で定義されている電子署名の適格証明書の発行者である必要がある。

3.2.3 Gaia-X Trust Framework と EUDIW の関係

GXDCH は、Gaia-X Trust Framework の一部として、データの信頼性、透明性、相互運用性を確保するための分散型の仕組みを提供している。GXDCH は、ユーザーが VC を保存し、必要に応じて第三者に提示できる「ウォレットアプリケーション」を含む複数のコンポーネントで構成される。このウォレットは、ユーザーが自身の資格情報を安全に管理し、他者と共有するためのものである。しかし、現時点では、GXDCH で用いられるウォレットは必ずしも EUDIW の仕組みに準拠しているわけではない。EUDIW は、EU(欧州連合)が推進するデジタル ID の枠組みであり、ユーザーが自身のデジタル身分証明書やその他の個人情報等を安全に管理・共有するためのツールである。GXDCH のウォレットアプリケーションは、EUDIW と同様に、ユーザーが資格情報を安全に管理・共有するための機能を提供している。将来的には、これらのシステム間での相互運用性や連携が進むことが期待できる。

3.3 EUDIW のトラストフレームワークについて

EUDIW のトラストフレームワークは、The European Digital Identity Wallet Architecture and Reference Framework（ARF）にて規定されている。なお、本書の公開時点では ver1.8.1であるが、当記載は、調査時点の ver1.4.0[3]を参照しており、今後の改変により、内容に相違が出る可能性がある事、また訳語は本書における独自の解釈である事に留意いただきたい。

ARF におけるトラストフレームワークの目的は、1. 各種プロバイダー（資格証明等の発行者）、2. ユーザー（ユーザーが使用する Wallet Instance）、3. 依拠当事者（資格証明等を受け取り検証の上、各種プロバイダーの確認行為等を信頼し依拠しながら当該業務等を実行）の 3 者間のやり取りにおいて、相手の真正性（改竄、なりすまし等が無い事）や適格性（認定もしくは確認された主体である事、失効していない事等）を、相互に確認可能な仕組みを担保する事である。

トラストフレームワークを支えるエコシステムは、以下の役割で構成されている。

- EUDI ウォレットのユーザー（Users of EUDIWallets）
- EUDI ウォレットプロバイダー（EUDIWallet Providers）
- 個人識別データプロバイダー（Person Identification Data (PID) Providers）
- 信頼リストレジストラ（Trusted Lists Registrar）
- 適格電子属性証明書プロバイダー（Qualified Electronic Attestation of Attributes (QEAA) Providers）
- 公的機関の信頼できるソース電子属性証明書プロバイダー（Public Body Authentic Source Electronic Attestation of Attributes (PuB-EAA) Providers）
- （非適格）電子属性証明書プロバイダー（Electronic Attestation of Attributes (EAA) Providers）
- 遠隔電子署名作成サービスプロバイダー（Qualified Electronic signature Remote Creation Service Providers）
- 信頼できるソース（Authentic Sources）
- 依拠当事者（Relying Parties）
- 適合評価機関（Conformity Assessment Bodies (CAB)）
- 監督機関（Supervisory Bodies）
- デバイスメーカーおよび関連サブシステムプロバイダー（Device Manufacturers and Related Subsystems Providers）
- 適格および非適格電子属性証明書スキーマプロバイダー（Qualified and Non-Qualified Electronic Attestation of Attributes Schema Providers）
- 国家認定機関（National Accreditation Bodies）

[3] https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

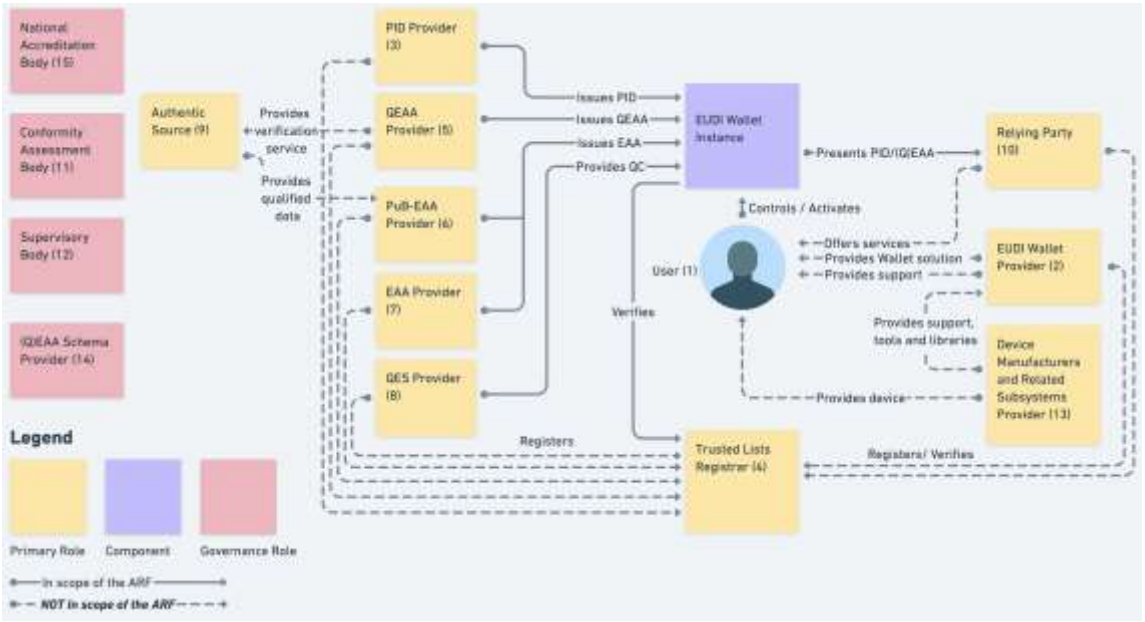


図 3-6 各役割の関係性の概念図

（出所）The European Digital Identity Wallet Architecture and Reference Framework ver1.4

各々の役割が、どのように機能しているかを全て言及する事はボリュームの関係で難しい為、例示として、ユーザーから依拠当事者への資格証明の提示の際に、ユーザーが依拠当事者の真正性や適格性をどう検証できるか、に関わるポイントを参考として記載する。

- ✓ EU Trusted List には、プロバイダーや依拠当事者の公開鍵+識別子が登録されるが、その登録に際しては、所属する加盟国の信頼リストレジストラが認定もしくは確認の上で、登録、停止、削除が行われる。
- ✓ その登録完了後に、プロバイダーや依拠当事者は、アクセス証明書認証局の電子署名されえたアクセス証明書を受け取る。（なお、アクセス証明認証局を信頼リストレジストラが兼ねるか、別認証局を立てるかは加盟国次第）
- ✓ 信頼リストレジストラは、アクセス証明認証局のトラストアンカーを含む信頼リストを作成し署名する。その上で、「信頼リストのリスト」としてURLが欧州委員会により公開される事で、すべての参加当事者がすべての信頼リストの URL を見つけることが可能となる。
- ✓ ウォレットインスタンスが、例えば個人識別情報等を安心して、依拠当事者に連携する事が出来る為には、証明書本体を連携する前に、相手先の依拠当事者の真正性や適格性を検証する事が可能である必要がある。その為には、証明書本体を連携する前に、アクセス証明書が当該の依拠当事者を指すこと、アクセス証明書自体の真正性、有効性、発行元がアクセス証明局の信頼リストにあること等が確認できる必要がある。まず、ウォレットインスタンスが依拠当事者のアクセス証明書認証局のトラストアンカーを確認可能である必要がある。依拠当事者がユーザーに対し証明書の要求をする際には、依拠当事者自体の証

明書とトラストアンカーに至る中間証明書を付与し、ウォレットインスタンスに連携する。それにより、詳細フローの説明は割愛するが、すべての証明書（依拠当事者自身の証明書、トラストアンカーおよびそれに至るトラストチェーン途上の証明書）が失効していないことを確認可能となる事で、ウォレットインスタンスから相手先の依拠当事者の真正性を検証する事が可能となる。その上で、ユーザーは、安心して依拠当事者に、証明書を提示する事が可能となる。

上記は例示であり、エコシステム内の登場する役割やフローは各々異なるが、同様に、依拠当事者によるウォレットインスタンスの真正性や適格性の検証、プロバイダーによるウォレットインスタンスの真正性や適格性の検証、ウォレットインスタンスによるプロバイダーの真正性や適格性の検証に際し、テクノロジーとガバナンスの両輪で、トラストフレームワークが成立している。

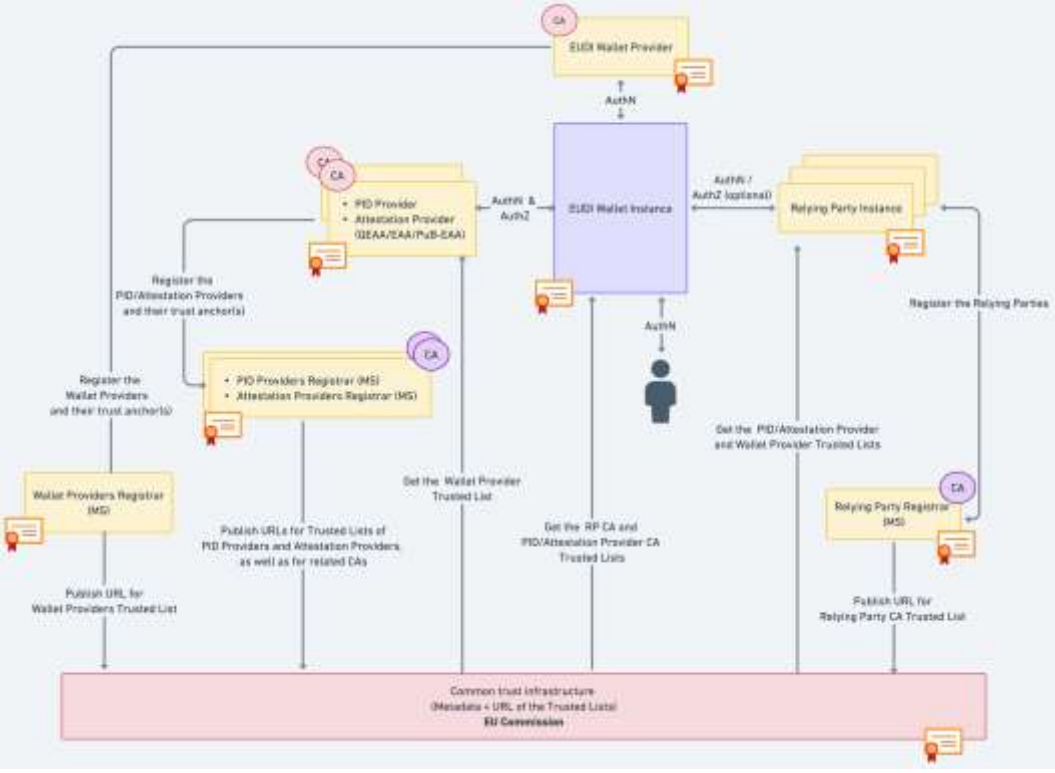


図 3-7 各役割の関係性の概念図

（出所）The European Digital Identity Wallet Architecture and Reference Framework ver1.4

社会実装において、一定レベル以上の信頼性が担保された仕組みづくりの検討が、EU で先行しており、国内における VC および DIW の社会実装の検討に際し、EU における検討内容が有益な参考情報となる。

4. データスペースにおけるトラストやアイデンティティに関わる論議と、Trusted Web の取り組みや、事業者確認や当人認証に関わる論議の融合の期待

これまで、国内においては、データスペースやデータ連携基盤と、Trusted Web の取り組みは密接には絡み合っていなかった。しかし、データスペースやデータ連携基盤や Verifiable Credentials におけるガバナンスの論議の活発化を契機に、アイデンティティ、トラストという共通の接点が生まれる中で、今後の論議の融合が期待される。

国内の、データスペースにおけるアイデンティティやトラストに関わる実装の論議において、国内環境も踏まえた上での最適なガバナンスとテクノロジーの両輪の検討が進むと想定する。
（参考：「3.Gaia-X のトラストフレームワーク、Catena-X オンボーディングプロセス、eIDAS2.0・EUDIW トラストフレームワークとの関係」「2. 3 Trusted Web と、データエコシステムのトラストやアイデンティティの論議との関係性」）

また、アイデンティティ、トラストの論議の前段として、1. 事業者確認、2. 事業者の当人認証の在り方の2つの観点について、公的に認められた網羅性をもった定義やガイドラインが明確でない事も課題の一つと考える。共通認識の元となる定義が明確でない事から、課題に関わる論点の範囲についても曖昧となる懸念があり、並行して論議が進む事を期待する。
（参考：「2.1 トラストの論議の前段として必要となる、事業者確認の論議について」「2.2 事業者当人認証とデータエコシステムのアクセス制御における認証・認可について」）

4.1　データスペースにおける事業者の認証・認可の検討の論点整理（将来課題と検討方向性）

事業者向けのデジタルサービスを取り巻く情報セキュリティリスクや、データエコシステムの進展を含む社会のデジタル化の進展により、取り扱われる機密性の高い情報は、質・量ともに年々拡大しており、それに伴い事業者向けデジタルサービスの全体的なリスクも拡大する傾向がある。言い換えると、（データスペース含む）事業者向けデジタルサービス等における事業者の当人認証および認可の制御の安全性の向上が求められるケースが拡大している。データエコシステム観点では、特に認可の制御の課題が大きい。

ゼロトラストの基本思想に沿った[4]、「セッション単位」で、リスクベースアプローチの動的ポリシーに基づく認可の実施により、アクセス目的に対し「必要最小限の権限を付与」の実現を目指す事になるが、その上で、安全性の向上と並行して、（特に認可に関わる）「アカウント管理運用の負担の拡大」の対策との両立が論点になる。

その実現の上で、アカウント運用管理として、「事前」にロールまたは権限の割り当て管理と、継続的なアカウント権限管理のメンテナンス、その為に必要となる資格情報等の業務運用の考え方には限界があるのではないだろうか？

ID 基盤や認可サーバーのシステムデザインの変化とあわせた、アカウント業務管理運用の BPR につながる検討が必要と考える。

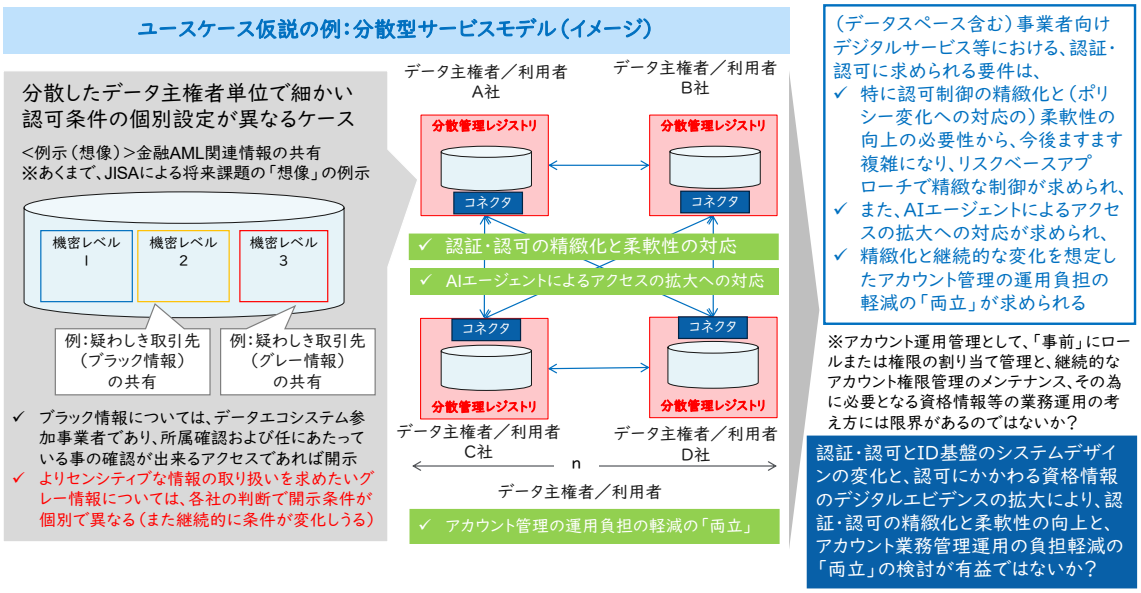


図　4-1　ユースケース仮説（想像）の例示と、将来課題と検討方向性（イメージ）

[4] ゼロトラストの「すべてのアクセスを検証し信頼しない（常に検証する）」という原則を具体的に実現するために、ユーザーの属性（役割、所属、場所、時間など）に基づいてリソースへのアクセスをセッション単位で最小限の適切な権限付与を制御する仕組みとして、PBAC (Policy Based Access Control) および ABAC (Attribute Based Access Control)の仕組みづくりが求められる。PBAC を「動的」に行うために、ABAC が必要になるが、セッション単位で都度、DIW から属性を主体的かつ自動的にに提示させることによるアカウント管理を含む複雑性の解消を検討した。

情報セキュリティ10大脅威 2025 [組織]

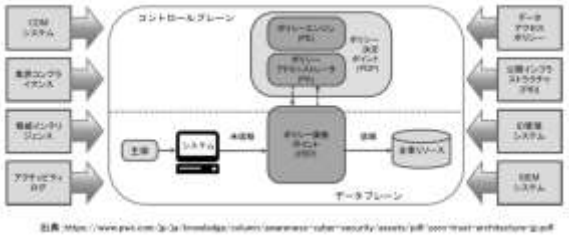
参照元･出典） 独立行政法人 情報処理推進機構 「情報セキュリティ10大脅威 2025」
情報セキュリティ10大脅威 2025 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

データエコシステムの進展を含む社会のデジタル化の進展により、事業者向けデジタルサービス等で取り扱われる機密性の高い情報は、質･量ともに年々拡大しており、それに伴い事業者向けデジタルサービスの全体的なリスクも拡大する傾向がある。

参照元･出典） 独立行政法人 情報処理推進機構 「ゼロトラスト導入指南書 」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

ゼロトラストの基本概念の論理コンポーネント（理想的なモデル）



- PDP(Policy Decision Point)：利用者（主体）からの企業リソースに対するアクセス要求を検証し、検証結果をポリシーに適用させることでアクセス許可の評価・判断を行う
- PE(Policy Engine)：アクセス要求の検証とポリシーの適用する
- PA(Policy Administrator)：PE の検証結果に基づいてアクセス許可者を PEP に連携する
- PEP(Policy Enforcement Point)：利用者からのアクセス要求を受け、PDP へ情報を流し、企業リソースへのアクセス制御を行う

図 4-2 背景となる社会環境

（出所）

https://www.ipa.go.jp/security/10threats/10threats2025.html

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf をもとに加工

<補論>

また、<ビジネス編>2. 1章でふれたように、AI 革命は産業構造に大きな変化をもたらし、情報サービス産業業界を含む全ての企業は、生存のためにソフトウェアカンパニーに、そしてデータカンパニーを目指す事になり、その上で、事業者向けデジタルサービスにおいても、AI ネイティブ[5]なアプリケーションの進展と普及が想定される。その上で、Model Context Protocol（MCP）[6]を介し、AI エージェントがユーザーの代わりにリソース等にアクセスし、情報のやり取りや API の実行などを行うという事が常態化する環境も想定される。

AI ネイティブなアプリケーションの進展と普及も念頭に、AI エージェントが、本当にユーザーの代替であることをどのように検証するのか、同意制御をどうするのか等の将来課題に対し、データスペースにおけるトラストとアイデンティティの論議と同期をあわせた、実現手法の今後の論議が重要である。

また、信頼性の高いデータソースである事のトラストの向上も重要な論議（例：データソースの主体の事業者が信頼できるか）となる。

5 従来の構造化データとビジネスロジックを中心としたソフトウェア設計から脱却し、AI モデルを核に据え、構造化データと非構造化データの双方を柔軟に活用することを前提に設計した、AI ネイティブなアプリケーション

6 OpenAI の元メンバーによって設立されたアメリカの人工知能のスタートアップ企業である公益法人の Anthropic が 2024 年 11 月に発表した、生成 AI アプリケーションと外部データソースやツールとの連携の標準化による円滑化を目指すオープンプロトコル仕様

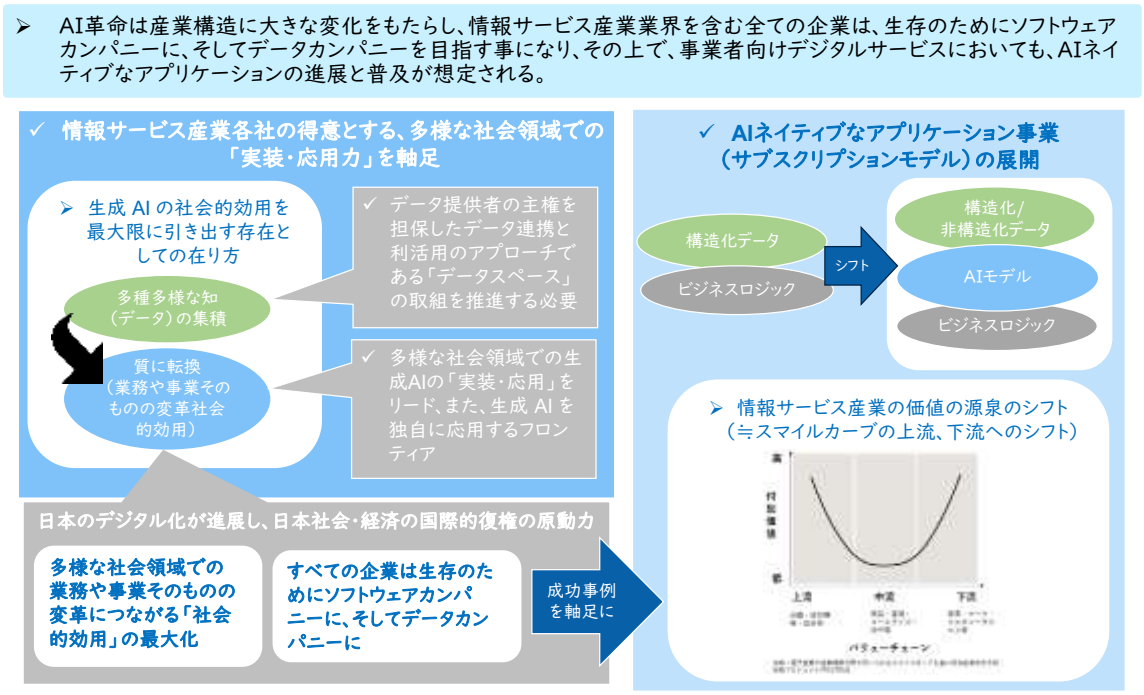


図 4-3 背景となる社会環境

（出所）

https://www.jisa.or.jp/Portals/0/resource/opnion/20241031-3.pdf

https://www.meti.go.jp/policy/it_policy/statistics/digital_economy_report/digital_economy_report.pdf を参考に作成

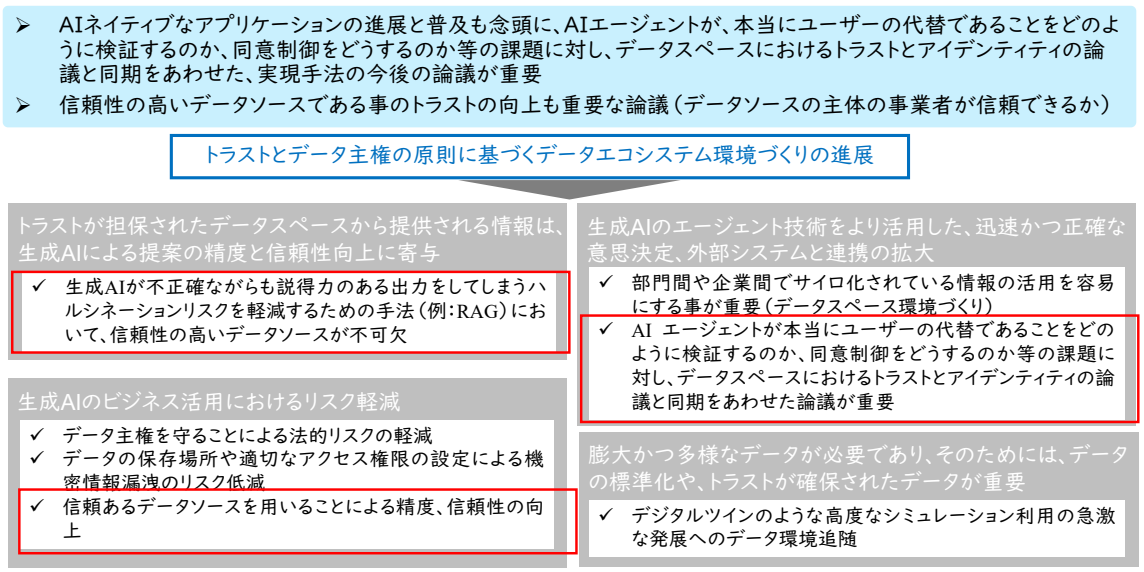


図 4-4 将来課題の背景（仮説）

前述のとおり、特に認可制御の精緻化の向上と、（アクセス制御のポリシー変化への対応の）柔軟性の向上の必要性、および AI エージェントによるアクセスの拡大への対応の必要性から、継続的な変化も想定したアカウント管理の業務運用が求められる。その際に、事業者向けデジタルサービスの運営側のアカウント管理運用の負担が拡大する事が将来課題として想定される。

より安全かつ適切な当人認証・認可の制御が求められていく際の、アカウント管理に関わる業務運用負担の軽減の「両立」が将来課題として想定される。

アカウント運用管理として、「事前」にロールまたは権限の割り当て管理と、継続的なアカウント権限管理のメンテナンス、その為に必要となる資格情報等の業務運用の考え方には限界があるのではないだろうか。

将来課題を踏まえ、認証・認可と ID 基盤のシステムデザインの変化と、認可にかかわる資格情報のデジタルエビデンスの拡大により、認可の精緻化と柔軟性の向上と、アカウント業務管理運用の負担軽減の「両立」の検討が必要ではないだろうか。

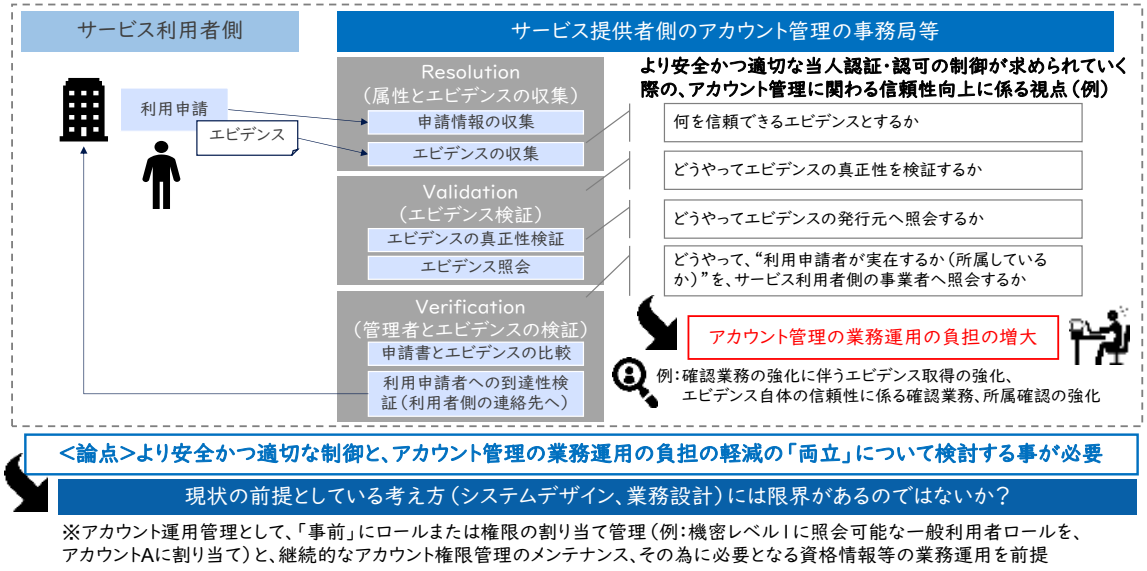


図 4-5 将来課題の背景（仮説）

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論をもとに加工

<将来課題を踏まえた検討の方向性>

✓ 認証・認可と ID 基盤のシステムデザインの変化と、

✓ 認可にかかわる資格情報のデジタルエビデンスの拡大により、

認可の精緻化と柔軟性の向上と、アカウント業務管理運用の負担軽減の「両立」の検討が有益ではないだろうか。

※「事前」のアカウント管理の業務運用ではなく、ゼロトラストの基本思想に沿って、セッション単

位で「動的」に、当該リソースのアクセスに対し必要となる資格情報（デジタルエビデンス）を自動要求・連携・検証により、アクセス目的に対し必要最小限の権限を付与への考え方への変化

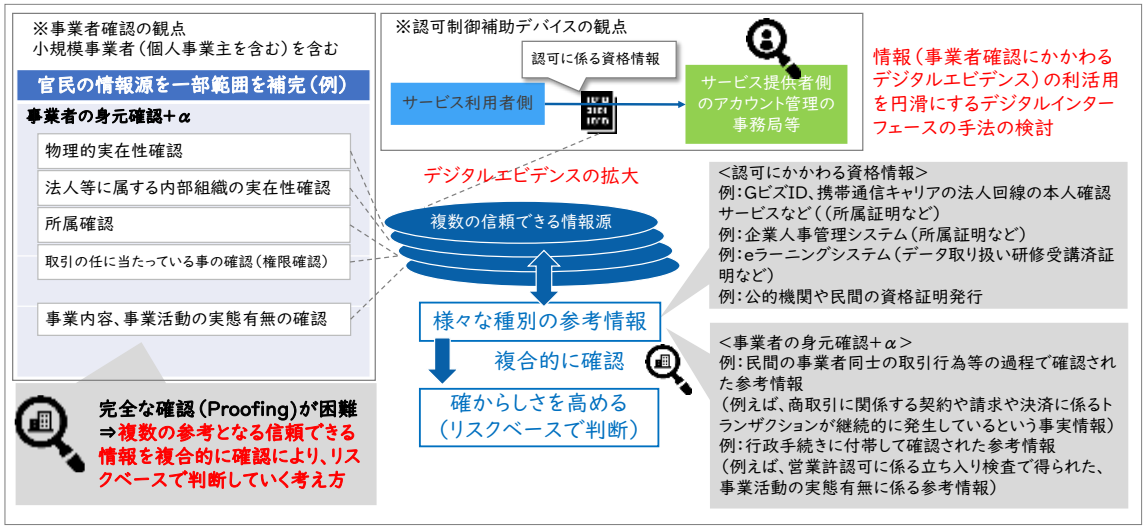


図 4-6 将来課題と検討方向性（イメージ）

4.2　データスペースにおける事業者の認証・認可の検討アプローチ仮説

前述の論点を踏まえ、(「事前」のアカウント管理による権限割り当てではなく)利用者からの「当該リソースへのアクセス要求セッション時」に、アクセス対象リソースの認可に必要となる資格情報(例:必要とされる保証レベルに応じた資格情報)を自動要求・連携・検証できる ID 基盤、認証・認可のシステムデザインの検討アプローチが有益と考える。

4.3 で、図4−6の概念イメージの、VCおよび事業者DIWの活用による実装の仮説を検討した。

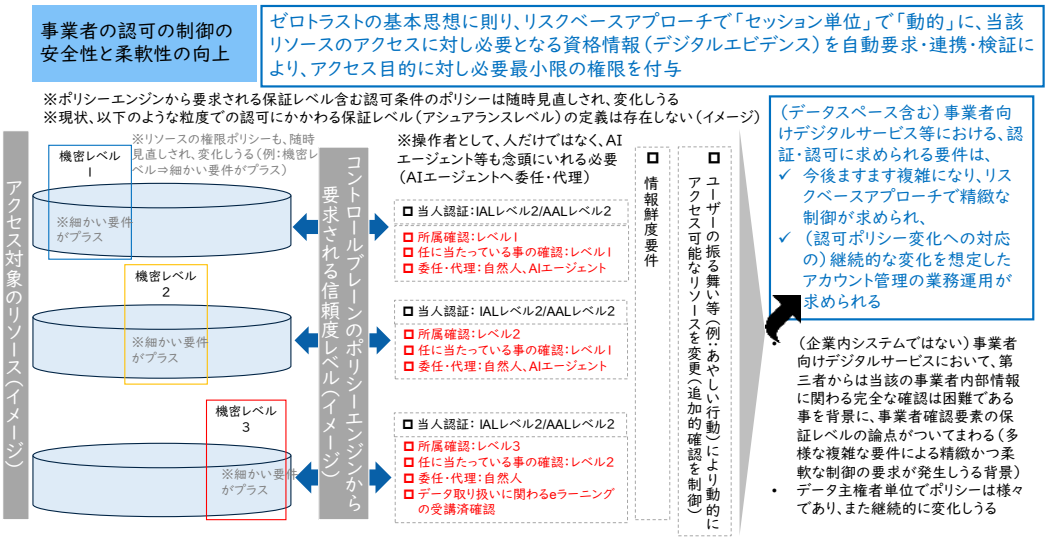


図　4-7　To Be 仮説検討の方向性

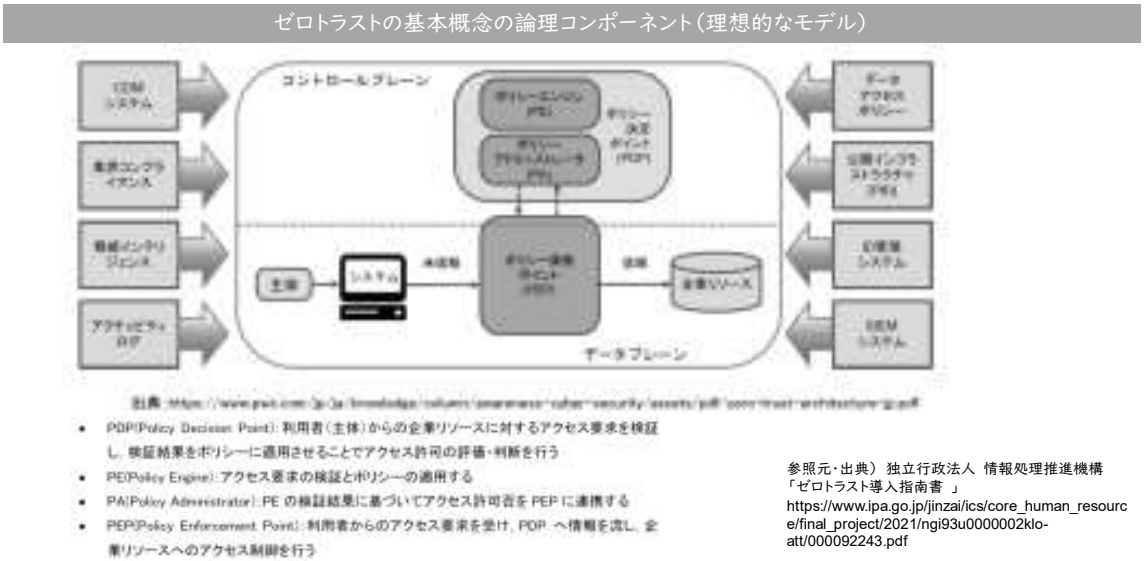


図　4-8　<参考>ゼロトラストの基本概念の論理コンポーネント(理想的なモデル)

(出所)独立行政法人 情報処理推進機構 「ゼロトラスト導入指南書 」

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

4.3 VCおよび事業者DIWの活用の仮説

4.2の検討アプローチを念頭におきつつ、国内のデータスペースにおけるアイデンティティやトラストに関わる実装の論議において、VCおよび事業者 Digital Identity Wallet（DIW）の活用について、2つの仮説を検討した。（データスペース整備の内部環境と周辺環境によって、他方式によるアプローチが最適という検討結果となる可能性もあるが、今後の論議の契機の材料となる事を期待し仮説を提示する）

なお、以下の考察内容は、あくまで当部会における見解であり、現状の Gaia-X 等のトラストフレームワークにおける整理そのものではないことに留意いただきたい。

＜仮説 I＞

- ➢ ゼロトラストの基本思想に沿った、事業者向けデジタルサービスの認証・認可における、特に認可制御の精緻化と柔軟性の向上と、アカウント管理の業務運用負担の軽減の「両立」を目指した、Verifiable Credentials(VC) および事業者 Digital Identity Wallet（DIW）を活用した「認可制御補助デバイス（仮称）」の検討

- ✓ 認証・認可と ID 基盤のシステムデザインの変化と、認可にかかわる資格情報のデジタルエビデンスの拡大をあわせた検討
- ✓ 同時に、自然人だけでなく AI エージェントによるアクセスの拡大への対応を兼ねる
- ✓ ベースとなる証明発行元の候補の一つとして、G ビズ ID の民間サービス連携への期待を含む仮説検討（※G ビズ ID の民間サービス連携に際し、G ビズ ID の API 連携で取得される結果情報を基にした、派生クレデンシャルの利活用のモデルが有益ではないかと考える。同様に、G ビズ ID 以外の一定レベルで信頼できる情報源からの派生クレデンシャルの利活用の拡大も視野にいれるが、ベースの候補の一つとして期待）
- ✓ 「社会全体のデジタル化の進展と共に、持続的に成長し続けられる事業者向けデジタルサービスの認可制御補助デバイスとなりうる可能性

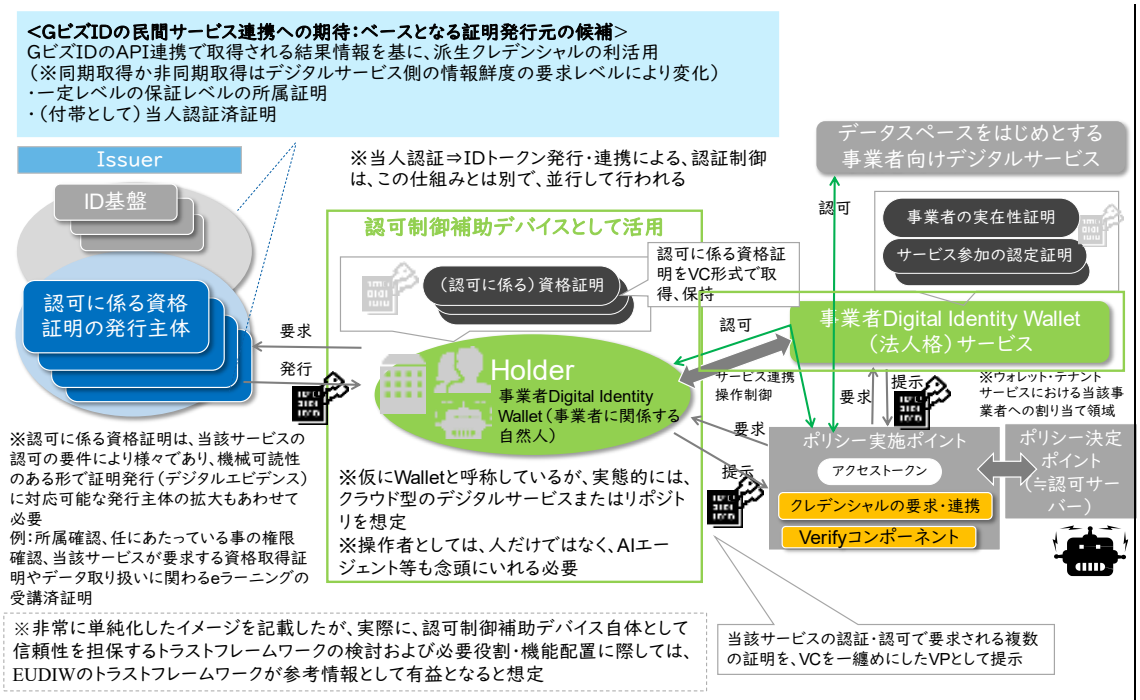


図 4-9 認可制御補助デバイスとしての活用イメージと、G ビズ ID の民間連携への期待

(「事前」のアカウント管理による権限割り当てではなく)利用者からの「当該リソースへのアクセス要求セッション時」に、アクセス対象リソースの認可に必要となる資格情報(例:必要とされる保証レベルに応じた資格情報)を、「動的」に自動要求・連携・検証により、アクセス目的に対し必要最小限の権限を付与
(※当人認証⇒IDトークン発行・連携による、認証制御は、並行して行われる)

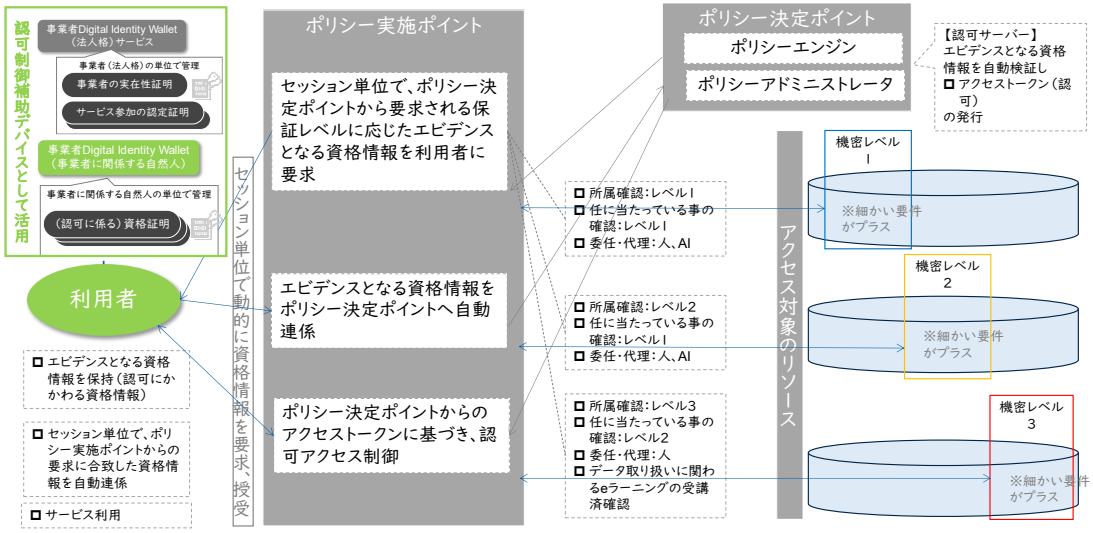


図 4-10 サービスイメージ(概念)

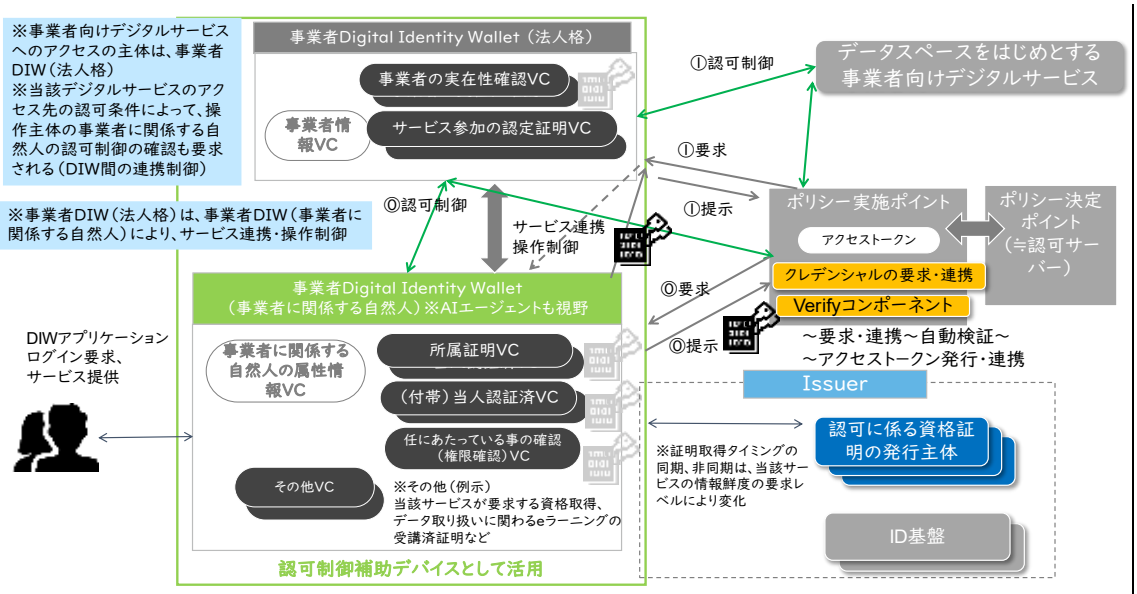


図 4-11 認可制御補助デバイスとしてのサービスイメージ

（補足1）

3.2でふれた通り、Catena-X では、参加者（企業）に対し Wallet サービスでテナントが提供され、そのウォレットテナントは、承認された個人のみがアクセスできるように制御する必要がある。

当仮説では、ウォレットテナントに相当する機能として、事業者 Digital Identity Wallet（法人格）を検討した。また、事業者 Digital Identity Wallet（事業者に関係する自然人）は、データスペースサービス等で必要となる認可にかかわる資格情報を保持するのみではなく、事業者 Digital Identity Wallet（法人格）に対し、承認された個人のみがアクセスできるように制御する役割を兼ね、両者はサービス連携される。法人格と関係する自然人の両方の事業者 DIW で保持される認可にかかわる資格情報を、データスペースサービスにおける認可制御に活用する。

（補足2）

<ニーズが想定される対象（仮説）>

1. 認可制御の精緻化と（認可ポリシーの継続的な変化への対応の）柔軟性が将来課題となる「事業者向けデジタルサービス」
2. サービス提供者側での利用者個人単位の認可のアカウント管理が必要であるが、アカウント管理運用負担を軽減したい「事業者向けデジタルサービス」
3. Model Context Protocol（MCP）を介し、AI エージェントがユーザーの代わりにリソース等にアクセスし、情報のやり取りや API の実行などを行うという事が常態化した際の、認証・認可の適切な制御と信頼性の担保が将来課題となる、機密情報や機微情報を取り扱う「事業者向けデジタルサービス」

4. AI ネイティブなアプリケーション事業として、信頼性の高いデータソースである事のトラスト（例：データソースの主体の事業者の信頼性）が求められる「事業者向けデジタルサービス」

<仮説の例示> ※令和 7 年度も継続検討、エンドユーザー企業との意見交換を予定

- ✓ 分散したデータ主権者単位で細かい認可条件の個別設定が要件となる類のデータスペース
- ✓ 金融業界の AML 関連情報の共有の検討、プログラマブルマネー等の検討
- ✓ 広く事業者向けデジタルサービスの中で該当するモデル

➢ 分散したデータ主権者単位で細かい認可条件の個別設定が異なるケース（イメージ）

※アカウント運用管理として、「事前」にロールまたは権限の割り当て管理と、継続的なアカウント権限管理のメンテナンス、その為に必要となる資格情報等の業務運用の考え方には限界があり、

認証・認可とID基盤のシステムデザインの変化と、認可にかかわる資格情報のデジタルエビデンスの拡大により、認証・認可の精緻化と柔軟性の向上と、アカウント業務管理運用の負担軽減の「両立」の検討が必要ではないか？

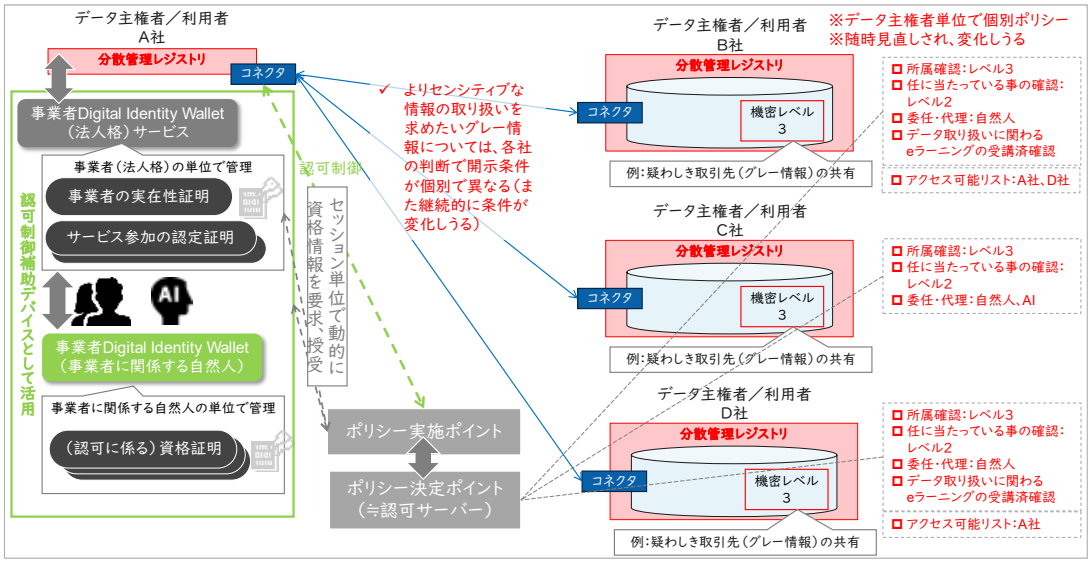


図 4-12 仮説検討の方向性（ユースケース仮説イメージ：ケース1）

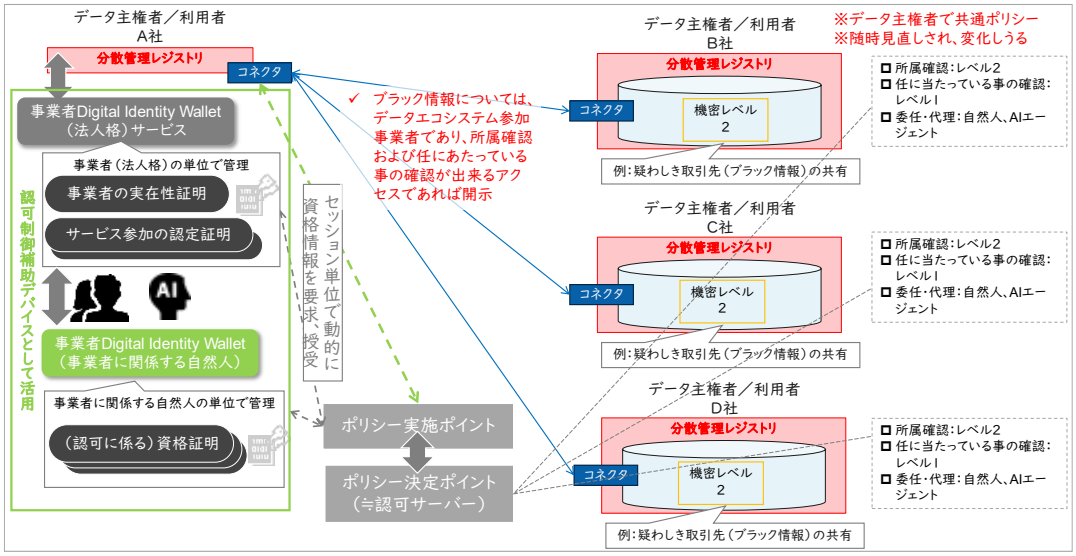


図 4-13 仮説検討の方向性（ユースケース仮説イメージ：ケース2）

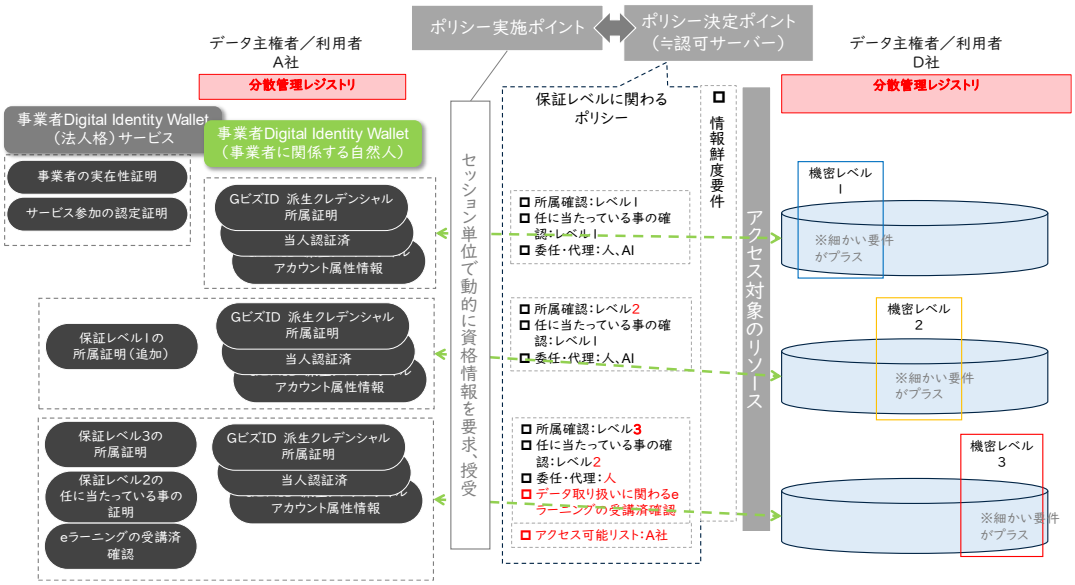


図　4-14　仮説検討の方向性（ユースケース仮説イメージ）

<仮説2>

- ➢ サービス①の事業者向けデジタルサービスの認可制御補助デバイスを、事業者確認のデジタルエビデンスの取得・連携手段として活用を検討（※事業者確認の補助デバイス）

- ✓ 事業者向けのデジタルサービスへのオンボーディング（例：参加申込）やオンゴーイング（例：更新審査・認定）時の、
  事業者確認のデジタル完結による申請者の対応負担の軽減と、
  当該デジタルサービスの事務局や認定機関等における、事業者確認のデジタルエビデンスによる信頼性の向上と、機械可読性による自動化率の向上をつうじた業務運用の負担の軽減の両立
- ✓ 発展して、事業者向けデジタルサービスに限らず、広く、事業者確認の様々な要素を「一元的に円滑に確認できるデジタル手法」の進展への検討の契機

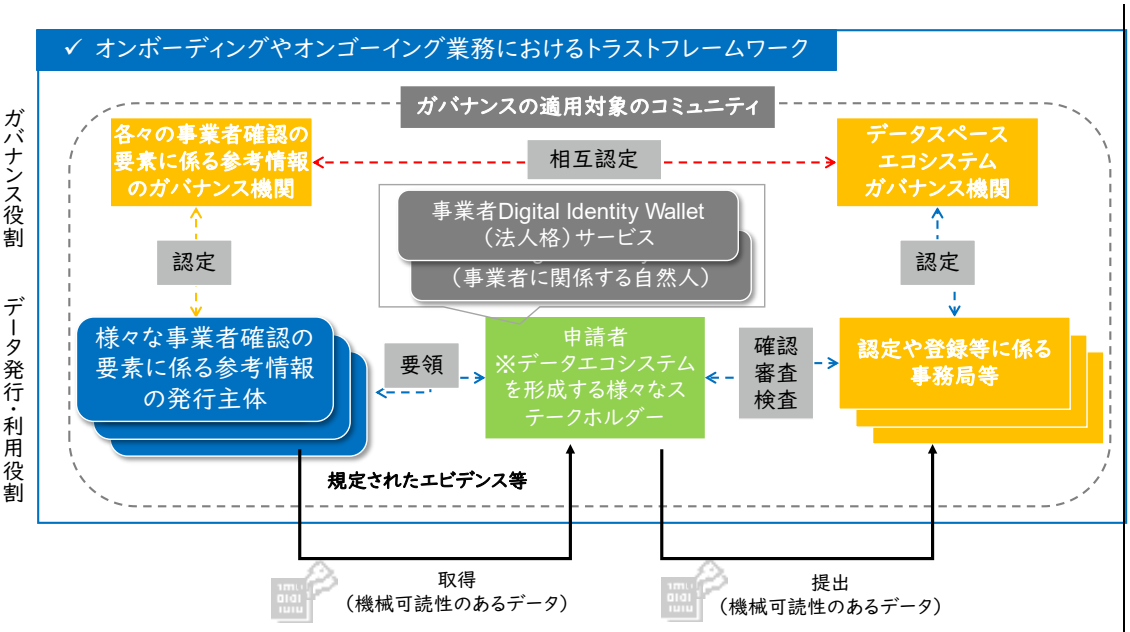


図 4-15 オンボーディング、オンゴーイング業務における活用イメージ

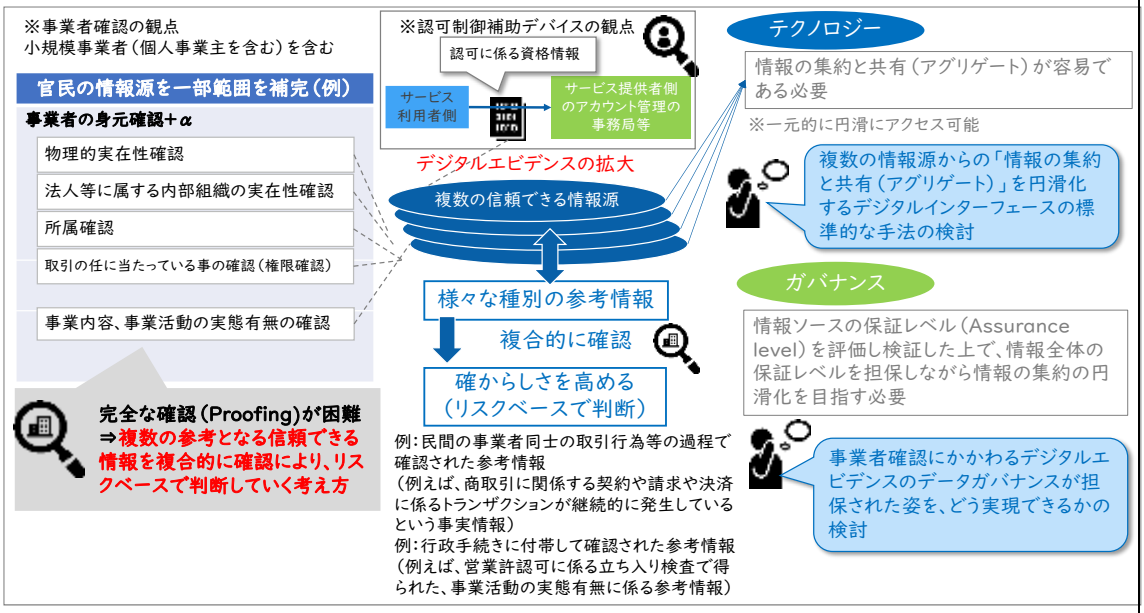


図 4-16 広く事業者確認のデジタル化の進展の契機となる期待

（補足3）

3.1、3.2 でふれた通り、現状の Gaia-X や Catena-X 準拠のデータスペースへの新規参加（オンボーディング）プロセスにおいて、以下の2つの観点での VC と検証鍵の利用がうかがえる。

1. オンボーディングの際の申込情報を、自由記述可能なデータモデルとして VCDM を活用

し、電子署名付きの電子契約書面やり取りのような利用目的で VC を利用
（言い換えると、専用 Web サイト等におけるフォーム入力の替りに VC 利用）
※参加者は、法定登録番号が含まれた企業データの自己記述（SD)を作成（Gaia-X Notarization Service に送付し、Gaia-X 形式の VC を取得）。取得した VC とあわせ、利用規約への同意を含めた申込を VC/VP として Gaia-X Compliance Service に連携

2. Gaia-X Compliance Service による検証および確認後、当該事業者に対する検証完了済証明（Gaia-X VC）として参加者へ発行により、コネクタ同士において相手先がどのような企業であるのか含め契約交渉・確認の際の、事業者適合性の証明およびデータスペース内の事業者識別として VC 利用
※Catena-X 固有のビジネスパートナー番号 (BPN) VC と Catena-X 固有のメンバーシップ VC が発行される

上記の通り、オンボーディング、オンゴーイングプロセスにおける多岐にわたる事業者確認は、欧州においても多くは業務運用確認に依存していると推測され、デジタル事業者確認の DX は実現されていないように見受けられる。各国の環境相違を踏まえる必要がある欧州よりも、日本がオンボーディング、オンゴーイングプロセスの DX において先行できる余地があるのではないだろうか。仮説 1 の“VC および事業者 DIW をデータスペース等へのアクセス時の「認可制御補助デバイス」として活用する検討“を軸足に、仮説2を通じて、社会全体のデジタル化の進展と並行し、オンボーディング、オンゴーイングプロセスの事業者確認の DX を継続的に進展させられる契機となる事に期待したい。（データスペース利用目的に閉じない形で、事業者確認のデジタル化の促進により、広くビジネス価値を生む事に繋がる可能性を期待。例えば、事業者間の電子契約の異なるサービスをまたいだ相互運用性の拡大、遠隔地の新規取引先の事業者確認の非対面・デジタルにおける信頼性の拡大）

4.4　今後、深掘り検討が必要となる論点ポイントの仮説

その上で、 今後、必要となる検討ポイントとして、以下のような論点が考えられる。

1 データスペースおよびデータスペースに閉じない他ユースケース（例：金融業界のAML等の検討 例：広く事業者向けデジタルサービス 例：AIエージェントによるアクセス拡大）の要件やモデルの整理が必要ではないだろうか？

- ✓ 検討全体としてユースケースを限定する必要はないが、議論の解像度向上や意識合わせとしてあったほうがよい
- ✓ 要件やモデルの整理をつうじ、実際のビジネス観点で想定ニーズに合致度の高いユースケースについて、JISA会員およびJISA会員の顧客のエンドユーザー企業におけるユースケース実証の機運醸成

2 （将来、長期間、公益的な社会基盤としてブラッシュアップしながら継続的に使用に耐える）汎用性と拡張性を考慮したシステムデザイン、セキュリティ要件や実運用要件を踏まえたプロトタイプ実装の取り組みが必要ではないだろうか？

- ✓ 例：事業者のソフトウェア認証デバイスとして十分な信頼性を担保する上で、最低限、クラウド環境でのHolder Binding（クレデンシャルとWallet/デバイスとのバインディング、クレデンシャルと利用者とのバインディング）を、暗号学的バインディング、属性バインディング、当人認証によるバインディングの組み合わせによる担保が必要となるが、深掘り検討が要。
  また、クラウド環境での実運用に耐えうる信頼性のおける鍵管理（バックアップ・リカバリ、同期など）の深掘り検討が要。
  あわせて、ソフトウェア認証デバイス自体としての信頼性を担保するトラストフレームワークの検討も要（The European Digital Identity Wallet Architecture and Reference Framework（ARF）もが参考情報として有益）。
- ✓ 例：複数ウォレット（最低限、法人格と所属する自然人格の2種類は存在する事を想定）に入ったクレデンシャルのバインディングの制御の深掘り検討が要。
- ✓ 例：ミクロな観点となるが、Model Context Protocol（MCP）に基づき、AI エージェントがユーザーの代わりにリソース等にアクセスし、情報のやり取りやAPIの実行などを行うという事が常態化した際に、AI エージェントが本当にユーザーの代替であることをどのように検証するのか、同意制御をどうするのか等も踏まえた汎用性と拡張性

3 （認証・認可制御にかかわる要素を優先的に）事業者確認要素の単位レベルでの保証レベル（アシュアランスレベル）のガイドラインの検討が必要ではないだろうか？

- ✓ 論議の前段となる事業者確認要素も、公的に認められた網羅性をもった定義やガイドラインが明確でない事も課題の一つと考える。共通認識の元となる定義が明確でない事から、課題に関わる論点の範囲についても曖昧となる懸念がある。
- ✓ その上で、どの視点や粒度（例：事業者確認の要素単位のレベル）での保証レベルの規定が可能か検討する必要がある。

4 （認証・認可制御にかかわるクレデンシャルについて優先的に）要件に対し必要となる保証レベルや情報鮮度の制御を可能とするデータ標準の検討が必要ではないだろうか？

- ✓ デジタルエビデンスの原本（Original）、複製（Duplicate）、派生（Derived）の観点では、事業者確認要素に関しては完全なIdentity Proofingが困難である事を背景に、参考情報となる「派生」のクレデンシャルの複数組み合わせにより、要件に対し必要なレベルの保証レベルや情報鮮度の担保をはかる事が多くなると想定され、データ標準の検討が重要となる。
  なお、単純に、派生クレデンシャルのアグリゲーションを通じ、必要となる保証レベルの担保を目指すわけではなく、情報源の保証レベルを評価し検証した上で、情報全体の保証レベルを担保しながら参考情報の集約の円滑化を目指す必要がある。
- ✓ また、「派生」の利活用が多くなる事を想定し、クレデンシャル発行の意図や想定された用途（「何」を、「どのレベル」で証明しているのか）のデジタル表現についても深掘り検討が重要となる。

5 デジタルエビデンスの実現可能性の整理（≒官民の発行元の可能性）が必要ではないだろうか？

- ✓ GビズIDや商業登記電子証明書などを情報源とする派生クレデンシャルに閉じず、事業者確認の要素単位レベルで一定レベルで信頼できる官民の情報源（民間の場合、ビジネス活動の過程で取得された参考情報も含む）の整理が必要。
  また、発行主体のメリット、インセンティブなども踏まえながら、スキーム成立の実現可能性の整理が必要。

図　4-17　今後、深掘り検討が必要となる論点ポイント（仮）

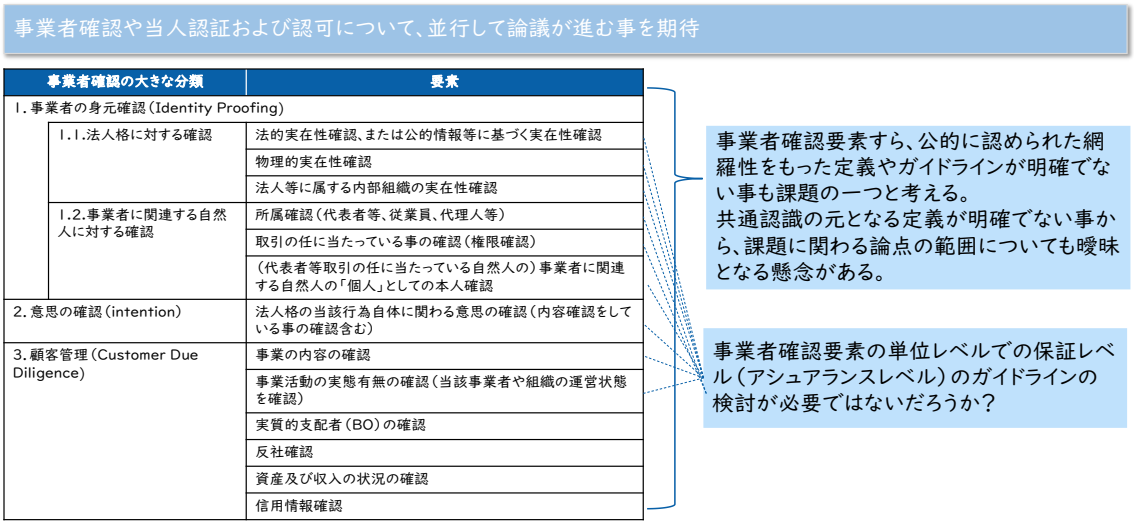


図 4-18 【補足】今後、必要となる検討ポイント（仮）

<補足：その他、必要となる検討ポイント>

また、個別論とはなるが、将来的に、G ビズ ID の API 連携で取得される結果情報を基にした、派生クレデンシャルの利活用のモデルの検討は、有益なデータ利活用となる可能性がある一方、想定外の利活用による弊害が発生しないように慎重な検討が必要と考える。

以下は、派生クレデンシャルの仮説である。

（※同期取得か非同期取得かは、デジタルサービスの情報鮮度の要求ポリシーに依存）

- 仮説①で利活用を想定する派生クレデンシャル
  - ◆一定レベルの信頼度の所属証明
  - ◆（付帯）当人認証済証明
- 仮説②で利活用を想定する派生クレデンシャル
  - ◆法的実在性確認
  - ◆一定レベルの信頼度の物理的実在性確認
  - ◆事業者属性情報

（補足）

◆ 一定レベルの信頼度の所属証明

G ビズ ID のメンバーアカウントは、当該事業者のプライムアカウントまたは第一／第二管理権限アカウントの責任の範囲内で運用されており、所属証明として一定レベルの信頼性があると認識できる。一方、信頼できる第三者である G ビズ ID 事務局による確認は経ておらず、所属証明としての信頼度としては一定レベルである事に留意が必要である。当該デジタルサービスの要求レベルによっては、リスクベースアプローチで追加的確認、つまり追加の資格証

明が補完として要求されるケースも想定される（例：同レベルの信頼度の異なるデータソースからの証明を追加要求　例：確認レベルが一段階上の証明を要求）。

また、「任にあたっている事」の派生クレデンシャルとして利活用については、行政手続きの任にあたっている事と、当該デジタルサービスの任にあたっている事で求められる条件は異なる為、派生クレデンシャルとして利活用は適切ではないと判断される（委任・代理権限も同様）。前述の通り、派生クレデンシャルは、「何を、どのレベルで証明しているのか」について、充分理解の上、活用の検討が必要となる。

データ利活用に際し、「何を、どのレベルで証明しているのか」の発行者と利用者双方の十分な理解共有が重要となる為、並行して、例えば、所属確認や、任にあたっている事の確認など、事業者確認の各要素の単位で、身元確認保証レベルや当人認証保証レベルにとどまらない保証レベルの定義を含めたガイドラインの検討が進む事を期待。

◆ （付帯の）当人認証済証明

所属証明が、「提示者に対し発行された証明である事」の信頼性を高める付帯的な証明として、G ビズ ID の当人認証済である事を、付帯的に証明発行。

また、発展的な利活用の可能性としては、当人認証の補強補助も考えうる。当人認証の「代替」としては、派生クレデンシャルである当人認証済証明は、証明の提示者と操作者の紐づけ（Binding）の信頼性の完全な担保が難しい為、「当人認証代替」の利活用は不適切と考えるが、リスクベースアプローチで、追加的認証を求められた際に、異なる ID 基盤の認証情報を提示する事は、当人認証強度を高める意味で有益なデータ利活用となる可能性があると考える。（例：当該デジタルサービスの ID 基盤またはＧビズ IDとのフェデレーションモデルによる当人認証をベースに、追加的認証を求められた際に、携帯事業者の法人回線の本人確認APIの当人認証済証明を追加で連携）

◆ 法的実在性確認

登記情報が存在する事業者については、GビズIDのプライムアカウントの申請におけるGビズIDの事務局による業務確認運用を背景に、GビズIDによる当人認証とあわせ、当該の相対する事業者について、一定レベルの法的実在性確認の円滑化が期待可能と認識。事業者サービスタスクフォースにて検討されている、Ｇビズ IDと商業登記電子証明書の一体化が整備された際には、更に有益なデータソースとなる事が期待される。一方、個人事業主をはじめとする登記が存在しない事業者について、また登記情報が存在する事業者においても共通するが、当該のデジタルサービスが必要とする事業者確認の要素として、法的実在性確認・物理的実在性確認だけでは要件を満たさない事も多く、いずれにせよデジタルエビデンスの継続的な補完・拡充につながる、社会環境全体のデジタル化の進展が必要となる。

◆ 一定レベルの信頼度の物理的実在性確認

プライムアカウントの申請における G ビズ ID の事務局による業務確認運用を踏まえると、一定レベルの物理的実在性確認の信頼性があると認識。一方、物理的実在性確認として本当

に信頼ができるかという観点では補完が必要となると想定する。
データ利活用に際し、「何を、どのレベルで証明しているのか」の発行者と利用者双方の十分な理解共有が重要となる為、並行して、例えば、事業内容の確認、事業活動の実態有無の確認など、事業者確認の各要素の単位で、身元確認保証レベルや当人認証保証レベルにとどまらない保証レベルの定義を含めたガイドラインの検討が進む事を期待。

◆ 事業者属性情報
※G ビズ ID で登録されている事業者属性情報

4.5 【補足説明】仮説 I：認可制御補助デバイスとしての活用のメリット

VC および事業者 DIW を、データスペース等へのアクセス時の「認可制御補助デバイス」として活用する検討は、以下の2つの観点で有意義と考える。

A) データスペース関連サービスと、ID 基盤や認可サーバーを疎結合にする事が可能な為、個別のデータスペース関連サービスにおける ID 基盤や認可サーバーの維持運用とアカウント管理の運用負担の軽減が期待可能な事

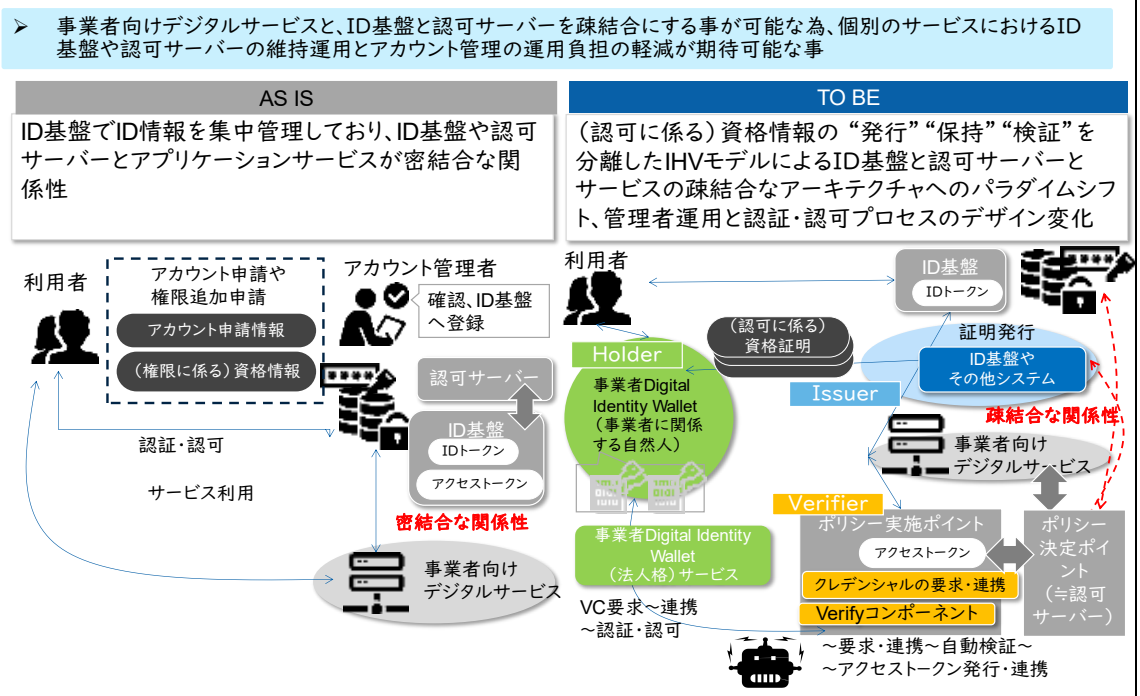


図 4-19 ID 基盤の維持運用とアカウント管理の運用負担の軽減が期待可能

（検討ポイント）

ID 基盤の機能配置および認証・認可プロセスの在り方の変更も含む、総合的な検討

✓ （認可に係る）資格情報の “発行” “保持” “検証” を分離した IHV モデルによる、ID 基盤と認可サーバーとデータスペースサービスの疎結合アーキテクチャへのパラダイムシフトによる、ID 基盤の維持運用の負担軽減

✓ 派生して、管理者運用と認証・認可プロセスのシステムデザインの変更と BPR

B) 「3.3.2 Trusted Web とデータ流通やデータエコシステムとの関連性や必要性」でふれた通り、データスペースやデータ連携基盤のアイデンティティやトラストに関わる論議において、Trusted Web の「データの送り手と受け手の検証可能性向上」「データそのものの検証可能性向上」に関わる考え方と技術が有益

（補足）

- ✓ 「データスペースに関わる主体の真正性・実在性の検証可能性の向上」において、Verifiable Identity を VC で表現しつつ、署名検証に加え Verifiable Data として同一主体である事や実在性や適合性などの確認を、IHV モデルによる実現は有益
- ✓ 主体の真正性・実在性は、複数の証明書の組み合わせによる総合的な確認が必要になるケースも多く、複数の証明書をまとめて提示する際に、暗号学的に情報の真正性を担保が可能なVC/Verifiable Presentation（VP）の活用は技術的選択肢として有益

なお、認可制御補助デバイス自体としての信頼性を担保するトラストフレームワークの検討に際しては、「3.3 EUDIW のトラストフレームワークについて」にて紹介した ARF が参考情報として有益である。

また、認可に関わる資格証明は、当該サービスの認可の要件により様々であり、機械可読性のある形で証明発行に対応可能な発行主体の拡大もあわせて必要となる為、一気に To Be の理想形には至らないが、社会全体のデジタル化の進展とともに、証明発行に対応可能な発行主体の拡大により、機能価値が向上し続ける事が期待可能である。言い換えると、「社会全体のデジタル化の進展と共に、持続的に成長し続けられる事業者向けデジタルサービスの認可制御補助デバイス」となりうる可能性がある。

<補足>

「ID 基盤や認可サーバーの機能配置および認証・認可プロセスの在り方の変更も含む、総合的な検討」と前述したが、補足する。<技術動向編>「2.2.1 データ連携に必要な観点」で紹介した“デジタル世界におけるアイデンティティのモデルの4つの段階の進化“における「フェーズ4 自己主権型」を念頭においた場合、図4−19で示したとおり、データスペースが提供するサービスと ID 基盤や認可サーバーを疎結合な関係性に変化させる事が可能となる。それにより、極論すると、個々のデータスペースにおける ID 基盤や認可サーバーの整備とアカウント管理業務運用を不要とするシステムデザイン、業務設計も視野に入る。（ID 基盤や認可サーバーの維持運用の負担軽減、ID 管理と認証・認可プロセスのデザイン変更と BPR の検討に繋がる可能性）

➢ “デジタル世界におけるアイデンティティのモデルの4つの段階の進化“における「フェーズ4 自己主権型」を念頭にきながら、事業者向けデジタルサービスが提供するサービスとID基盤や認可サーバーを疎結合な関係性に変化させる事が視野に入る

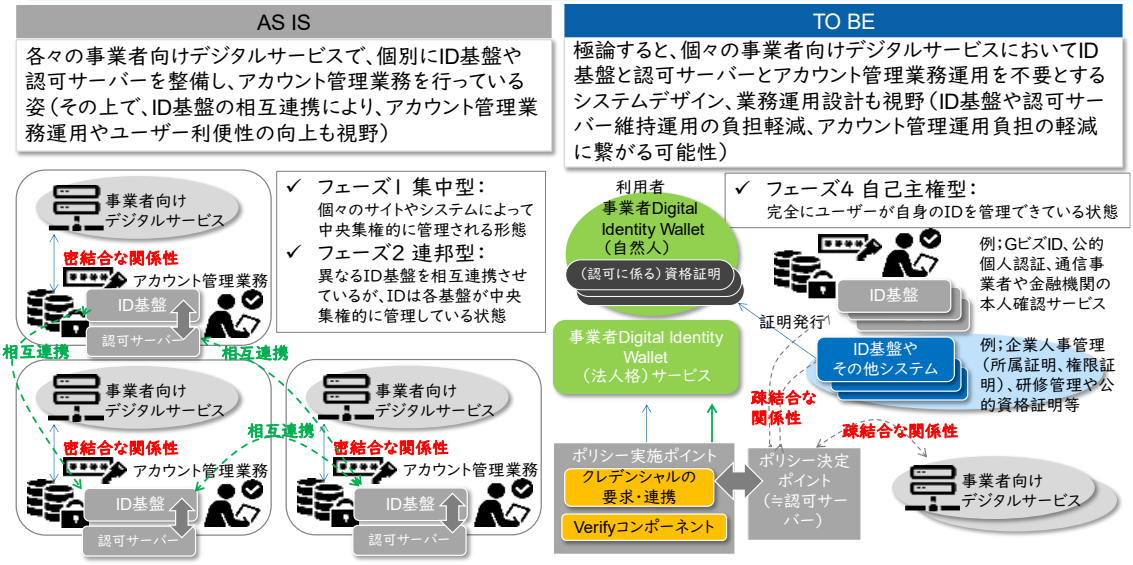


図 4-20 ID 基盤や認可サーバーの機能配置の変化の可能性

➢ アカウント管理運用の変化が期待可能な事

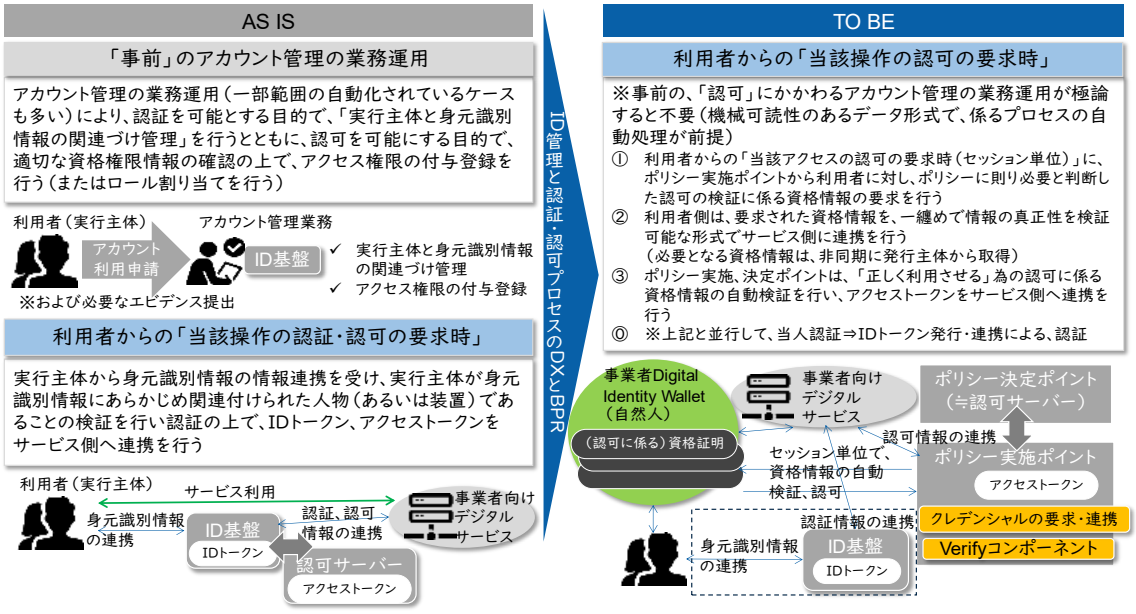


図 4-21 アカウント管理運用の変化

4.6 【補足説明】信頼できるアイデンティティ・プロバイダー（例：G ビズ ID）との ID 連携（フェデレーション）」の仮検討

仮説 I 以外の他検討として、「信頼できるアイデンティティ・プロバイダー（例：G ビズ ID）との ID 連携（フェデレーション）」の検討も有意義である。また、仮説 I の認可制御補助デバイスの検討に際し、認証については並行で検討が必要となるが、その際に、ID 連携（フェデレーション）の検討も有意義である。

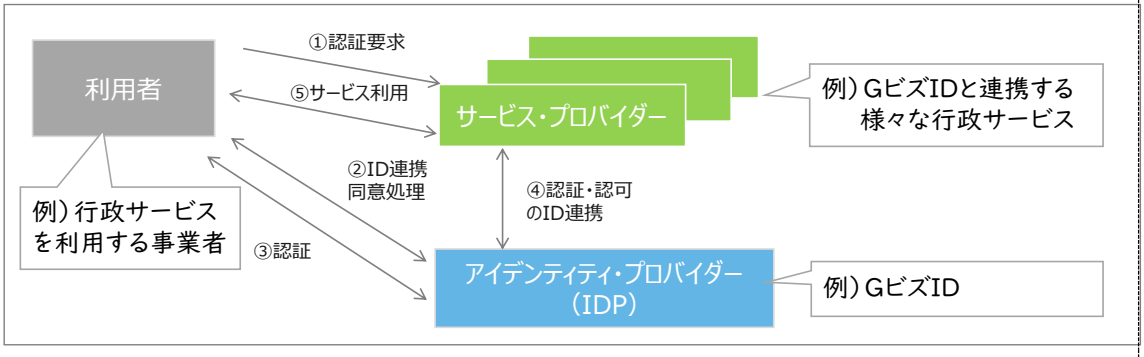


図 4-22 ID フェデレーション（ID 連携）簡略イメージ

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

しかし、“当人認証の単位”、“アカウント管理の業務運用の在り方”が様々である事や、“事業者のカバー率”等の観点から、業務目的に対し適切なアイデンティティ・プロバイダー（IDP）が存在しないケースも想定される。
上記を踏まえながら、今後の議論の継続が必要となると考える。

当人認証の単位の相違	アカウント管理の業務運用の在り方の相違（例示）	
A. 事業者単位で共通のIDによる認証情報の確認	A	✓ サービス提供者側のアカウント管理者により、事業者単位のアカウント管理を行うケース
B. 操作者個人単位のIDによる認証情報の確認	B-1	✓ サービス提供者側のアカウント管理者により、サービス利用者側の管理権限者のアカウント管理のみを行う。 ✓ その上で、サービス等を利用する事業者側の管理権限者により、サービス提供者側のアカウント管理機能を利用し、当該事業者の操作者個人単位のアカウント管理が行われるケース （≒操作者単位のアカウント管理の業務運用は、サービス利用者側の管理権限者に権限移譲） 例）請求書電子化サービス事業者や中小企業向けEDIサービス事業者の提供サービス
	B-2	✓ （契約等は事業者や組織単位であるが）サービス提供者側のアカウント管理者または機能により、サービス利用者側の操作者個人単位のアカウント管理も行うケース 例）名刺管理サービス事業者や企業向け福利厚生サービス事業者の提供サービス
	B-3	✓ 操作者個人単位で利用申請（または契約）が必要であり、サービス提供者側のアカウント管理者により、操作者個人単位のアカウント管理を行うケース 例）府省共通研究開発管理システム（e-RAD）への民間事業者に所属する民間研究員として登録と利用

GビズID側のアカウント管理者は、操作者単位（GビズIDのメンバーアカウント）では、所属確認を含む確認作業を行っていない

<思考実験>
操作者個人単位の厳密な所属確認を含む確認作業が必要になるケースにおいては、ID連携が適切ではない可能性が高いと想定

図 4-23 業務目的に対し適切な IDP が存在しないケースの例示

（出所）一般社団法人 OpenID ファウンデーション・ジャパン KYC Working Group 法人 KYC 分科会の議論より

業務目的に対し適切な IDP が既存環境で存在しない場合、新たに、様々なデータスペースの認証・認可の要件を考慮した上で、一定レベルで汎用性のある IDP の整備、運営の検討なども有意義である。

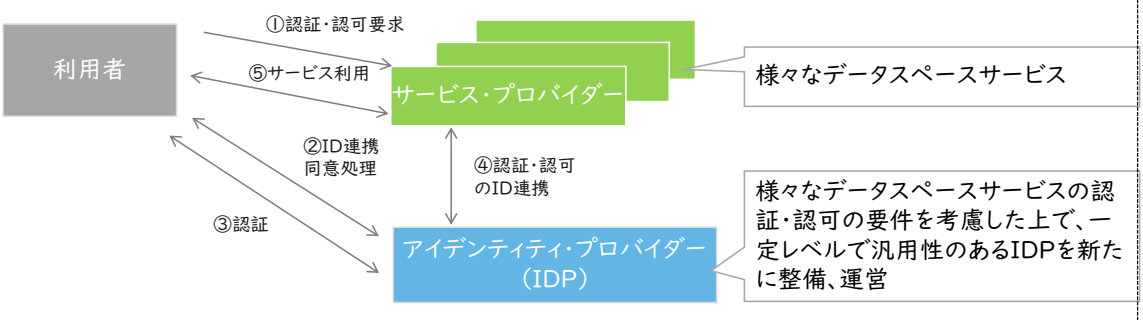


図 4-24 検討①：データスペースサービス向けに新たに IDP を整備

または、別のアプローチとして、単体の IDP では要件を満たす事が難しいケースにおいて、複数の IDP の組み合わせによる要件合致を目指す方向性も考えうる。現状は存在しないが、アイデンティティプロバイダー（IDP）に対するアグリゲーター役割（集約と共有）の検討が必要になる可能性もあると想定する。

なお、単なるアグリゲーションを目指すわけではなく、情報ソースの Assurance level（保証レベル）を評価し検証した上で、情報全体の Assurance level を担保しながら情報の集約の円滑化を目指す必要がある。その上では、現状、そもそも事業者確認要素について共通定義がない事、よって事業者確認についての Assurance level の共通定義も無い事も課題となる。

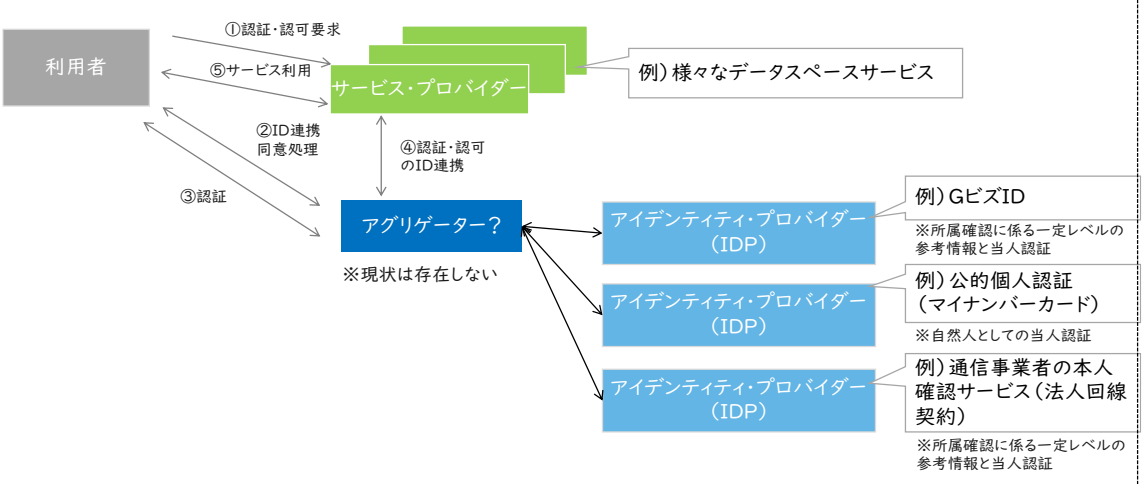


図 4-25 検討②：既存 IDP のアグリゲート機能の整備

仮説 1 の“VC および事業者 DIW をデータスペース等へのアクセス時の「認可制御補助デバイス」として活用する検討“は、上記の図4−24、4−25のような検討が難しいケースにおける複雑性の軽減の一つとして有益である。（「1. 認証および認証にかかわるアカウント管理」、「2. 認可および認可にかかわるアカウント管理」を分離し、2. の解決策とする事で、1. の検討の複雑度が軽減されると考える）

1. 将来にわたり、要件が継続的に拡大する際の対応負担の観点で有益
（「社会全体のデジタル化の進展と共に、持続的に成長し続けられる事業者向けデジタルサービスの認可制御補助デバイス」となりうる可能性）

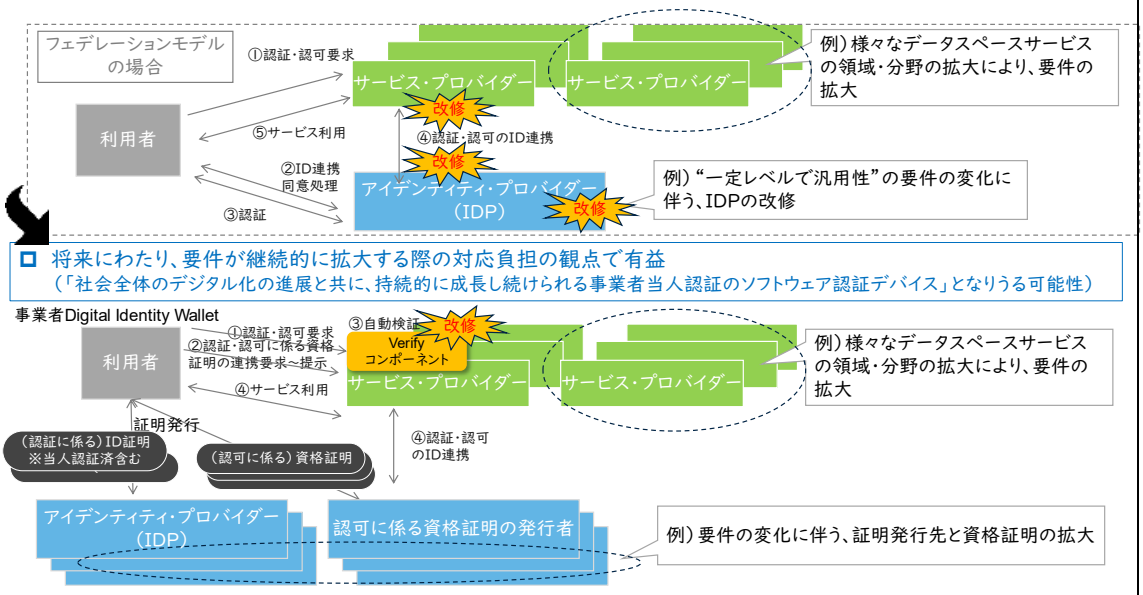


図 4-26 将来にわたり、要件が継続的に拡大する際の対応負担の軽減

2. アグリゲートを実現する実装上の観点で有益
（目的）情報ソースの Assurance level を評価し検証した上で、情報全体の Assurance level を担保しながら情報の集約の円滑化を目指す対応負担の軽減

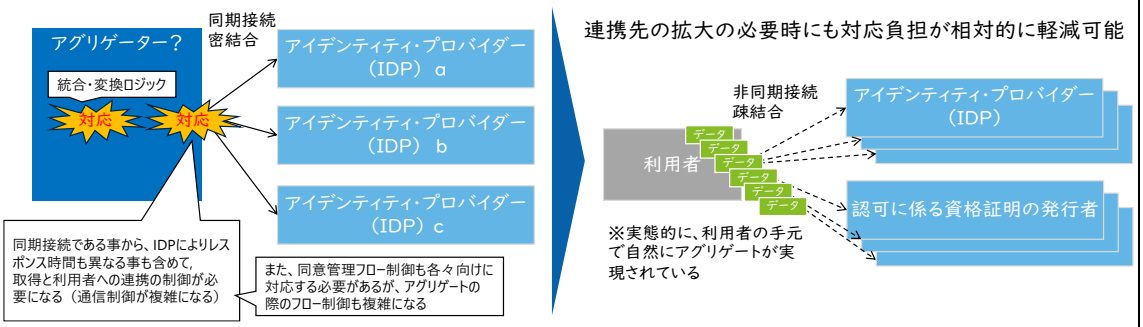


図 4-27 アグリゲートを実現する実装上の対応負担の軽減

（補足）
なお、G ビズ ID は、“VC および事業者 DIW をデータスペース等へのアクセス時の「認可制御補助デバイス」として活用する検討“の際にも、認可に関わる G ビズ ID 認証と基とした「派生クレデンシャル」の発行主体として有力な候補の一つと想定する（現時点では、デジタル庁で、民間連携も可否を含めて検討中の状況の為、不透明）。ただし、「何を、どのレベルで証明しているのか」については、充分理解の上、活用の検討が必要となる。

例えば、G ビズ ID のメンバーアカウントは、プライムアカウントと違い、G ビズ ID 事務局による本人確認とアカウント登録管理がされているわけではなく、プライムまたは第一／第二管理権限によりアカウント登録管理がされている（言い換えると、信頼できる第三者がメンバーアカウントの所属確認や任にあたっている事の確認をしているわけではなく、当該事業者の責任の範囲内で運用されている事の理解が必要）。将来、G ビズ ID の民間開放および VC 証明発行が対応されたと仮定し、データスペース等のサービスでも利用可能になった際には、リスクベースアプローチのポリシー設計が有効と考える。例えば、メンバーアカウントの所属証明（G ビズ ID 認証からの派生クレデンシャル）の保証レベルでアクセス可能なタ範囲のポリシー設定、更に機能やデータ範囲の拡大が必要になった場合は、所属や任にあたっている事の信頼度を拡充できる追加の証明が必要となる等のリスクベースアプローチのポリシー検討。

その上では、身元確認保証レベル（IAL）や当人認証保証レベル（AAL）にとどまらない保証レベルの定義を含めたガイドラインの検討が進む事を期待する。（例：所属確認レベル 1/2/3、任に当たっている事の確認レベル 1/2/3、物理的実在性確認レベル 1/2/3）

上記は、当仮説のような派生クレデンシャルの利活用モデルに限らず、通常の G ビズ ID の民間サービス連携のフェデレーションモデルにおいても、共通する課題と考える。G ビズ ID の民間サービス連携に際し、「何を、どのレベルで証明しているのか」について、データの出し元である G ビズ ID から連携される情報の、身元確認保証レベルや当人認証保証レベルにとどまらない確認レベルと、民間サービス側の業務目的で必要とする確認レベルの相違の有無を円滑に把握し、GビズID連携を適切に活用する上でも、事業者確認要素について共通定義、および事業者確認の各要素の単位で、優先度の高い可能な範囲から Assurance level の共通定義のガイドラインの検討を期待する。（GビズIDのフェデレーションをもとに、本来の業務要件に合致しない不適切な業務運用が発生する事を抑止する効果も期待できる）

認証・認可時				
	プライム	メンバー	エントリー	委任登録
IAL (Identity Assurance Level) 身元情報検証時の保証レベル	IAL レベル2 ※GビズID事務局にて、識別に用いられる属性情報を、リモート（郵送またはオンライン）で確認	IAL レベル2 ※プライムアカウントまたは第一／第二管理者権限を付与されたメンバーアカウントにより、アカウント登録管理（GビズID事務局では確認業務は行っていない）	IAL レベル1 ※自己申告で登録	※プライムアカウントと同様
AAL (Authenticator Assurance Level) 認証プロセスの保証レベル	AAL レベル2 ※2要素認証 知識(パスワード)認証 ＋ 所有物認証（スマートフォンアプリ認証またはワンタイムパスワード認証）	AALレベル2	AAL レベル1 ※単要素認証 知識(パスワード)認証	※プライムアカウントと同様

図 4-28 <参考>G ビズ ID の IAL、AAL

以上

令和 6 年度
データ流通部会　報告書
～次世代データエコシステムに関わる技術・動向調査
および情報サービス産業業界の協働の可能性に関わる考察～

令和 7 年 5 月発行
発行所：一般社団法人　情報サービス産業協会
〒101-0047　東京都千代田区内神田 2-3-4　S-GATE 大手町北 6F
TEL (03)5289-7651　　FAX (03) 5289-7653