

strategy&

Part of the PwC network

デジタル アイデンティティ その機会 と課題

通信事業者、銀行、
政府機関、そして
民間企業のための視点



著者紹介

Kağan Karamanoğlu

PwC Strategy&のパートナーでイスタンブールを拠点とする。トルコのStrategy&を統括し、通信・金融サービス業界をリードしている。欧州のStrategy&リーダーシップチームのメンバーも務める。20年以上のコンサルタント経験を有し、企業・ビジネス戦略を専門とする。また、世界各地で複数のクライアントエンゲージメントチームを率いた経験を持つ。

Samar Kallas

PwC Strategy&のパートナーでフランスを拠点とする。通信・テクノロジー業界をリードし、成長戦略、コマース、デューデリジェンス、変革プログラム、オペレーティングモデル設計などを専門とする。PwCフランスの「ケイパビリティに基づく戦略 (Capabilities Driven Strategy)」「Fit for Growth」両サービスの責任者。通信・テクノロジー分野を中心とした戦略コンサルティングに12年の経験を有する。

Mohamed-Ali Benyoucef

PwC Strategy&のマネージャーでドバイを拠点とする。通信・テクノロジー業界をリードし、通信・IT分野を中心とした、成長戦略とデューデリジェンスを専門とする。同分野をはじめとする戦略関連業務に10年以上の経験を有する。

監訳者および「はじめに」の著者紹介

樋崎 充(といざき・みつる)

mitsuru.toizaki@pwc.com

PwCコンサルティング、Strategy&のパートナー。約20年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトに数多く従事している。

大塚 悠也(おおつか・ゆうや)

yuya.otsuka@pwc.com

PwCコンサルティング、Strategy&のシニアマネージャー。IT関連企業、総合電機メーカー、金融・サービス業、官公庁に対し、事業戦略、成長戦略、新規事業の立案および実行支援などのプロジェクトに従事。近年では、量子、AI、セキュリティ、生体認証、Digital Identity (デジタルID) などのエマージングテクノロジー領域におけるコンサルティングを中心に取り組んでいる。

問い合わせ先

PwCコンサルティング合同会社 ストラテジーコンサルティング (Strategy&)

〒100-0004

東京都千代田区大手町1丁目2-1 Otemachi Oneタワー

代表Tel:03-6257-0700 Fax:03-6257-0701

email: jp_cons_strategy-info-mbx@pwc.com

http://www.strategyand.pwc.com/jp

はじめに — デジタルID

日本の現状の課題と推進の方向性

2021年の「世界デジタル競争力ランキング」(IMD)では、日本の総合順位は64カ国・地域のうち28位であった。17年に調査を始めてから最低を更新し、新型コロナウイルス感染症の対応では「デジタル敗戦」という表現も生まれた。Strategy&がグローバルで公開した本レポート「Digital identity: Opportunities and challenges A perspective for telecom operators, banks, industrial companies and government institutions」では、デジタル化の推進に伴い、注目されているデジタルアイデンティティ(デジタルID)について、諸外国の政府・民間企業の事例を基に機会と課題を論考している。残念ながら、日本については触れられていないが、デジタルIDの日本における状況についてまずはここで俯瞰したい。日本国民にとってのデジタルIDとして、まず考えられるものは、マイナンバー/マイナンバーカードであろう。しかし、マイナンバーカードの普及率は2021年5月段階では30%*程度であり、またそれを活用してさまざまな公共・民間サービスを受け入れられる状態には残念ながら至っていない。金融機関は、本人確認(KYC: Know Your Customer)を支援する形で、複数の銀行が協働して本人確認を担保できるプラットフォームの仕組みを構築し、また大手通信事業者は同様に本人確認を支援するサービスを提供しているが、諸外国のように公共のIDと金融機関・通信事業者のIDなどを統合するまでには至っていない。EコマースやSNSなどの日常生活でなじみのあるアプリのIDを活用して他のアプリにもログインできるシングルサインオン(SSO)は一定程度進んでおり、一部民間アプリケーションから公共手続きの申請が行える仕組みを整えようという動きが出始めているが、規制の問題もあり進展していない。

一方、諸外国では、政府のサービスや給付に加えて、バンキング、職場、教育、医療関連など多数のオンラインサービスの利用において、本人識別子の役割を果たすバーチャル世界でのパスポートのようなものとして普及している。Society5.0、メタバースなどのさまざまな表現はあるが、これから世界中でサイバーおよびフィジカル空間がシームレスにつながる世界が構築されていくことは間違いない。

では、日本において、今後誰がこのデジタルIDを提供し、管理していくのか。消費者の目線から見ると、信頼性・透明性・利便性をもった状態が望ましい。特に信頼性・透明性においては、単に大企業、公的機関だからといったような組織体のブランド(知名度など)や規模などによる安心感ではなくこれからの時代を見据えた実践的なセキュリティの確保が求められるのではないかと。例えば、サイバー空間における情報漏えいが全く起きないことが望ましいが、近年の情報化社会の中で、データを隠し続けることは可能だろうか。今や紙に手書きで情報を記載し引き出しの奥に隠しておくことでもしない限り、個人の情報を守る方法はない。このような中、デジタル先進国では、情報を積極的にコントロールすることこそがプライバシーを守る方法だと思いが切り替わりつつある。具体的には、①必要な情報を誰にどの程度開示するのか情報をコントロールする権利を本人が持つこと、②誰が情報にアクセスしたか見えること(アクセス履歴を追跡できること)、③本人の承諾に基づかない勝手なアクセス・盗み見には厳罰が処されること、という要件を設定し、守ろうと言う国、企業がある。処罰に関しては法の規定に依るが、①②においては民間企業や公的機関などでも技術を駆使すれば可能ではないか。

これからの日本のデジタルIDを担っていくプレーヤーは、サービス面からは積極的に仲間集めを行い、便益をエンドユーザーに提供するエコシステムを構築し、同時に、上記のような信頼性および透明性をもった仕組みを構築していくことが必要だろう。そして、そのようなプレーヤーは、仕組みによって個人々々から信頼されてさまざまなデータを集約し、結果自社にはビジネス機会をもたらしていくポジションをとることができるのではないだろうか。本レポートのデジタルID先進国の事例や示唆を、今後発展していくであろう日本市場のデジタルIDビジネスの参考にして頂ければ幸いである。

*出所：デジタル庁「マイナンバー制度」https://twitter.com/MyNumber_PR/status/1390271930528268296
2021年11月16日閲覧

1. デジタルID：確実な成長市場

公的給付の利用から銀行サービスの利用など、今や数多くのサービスがデジタル化されている。

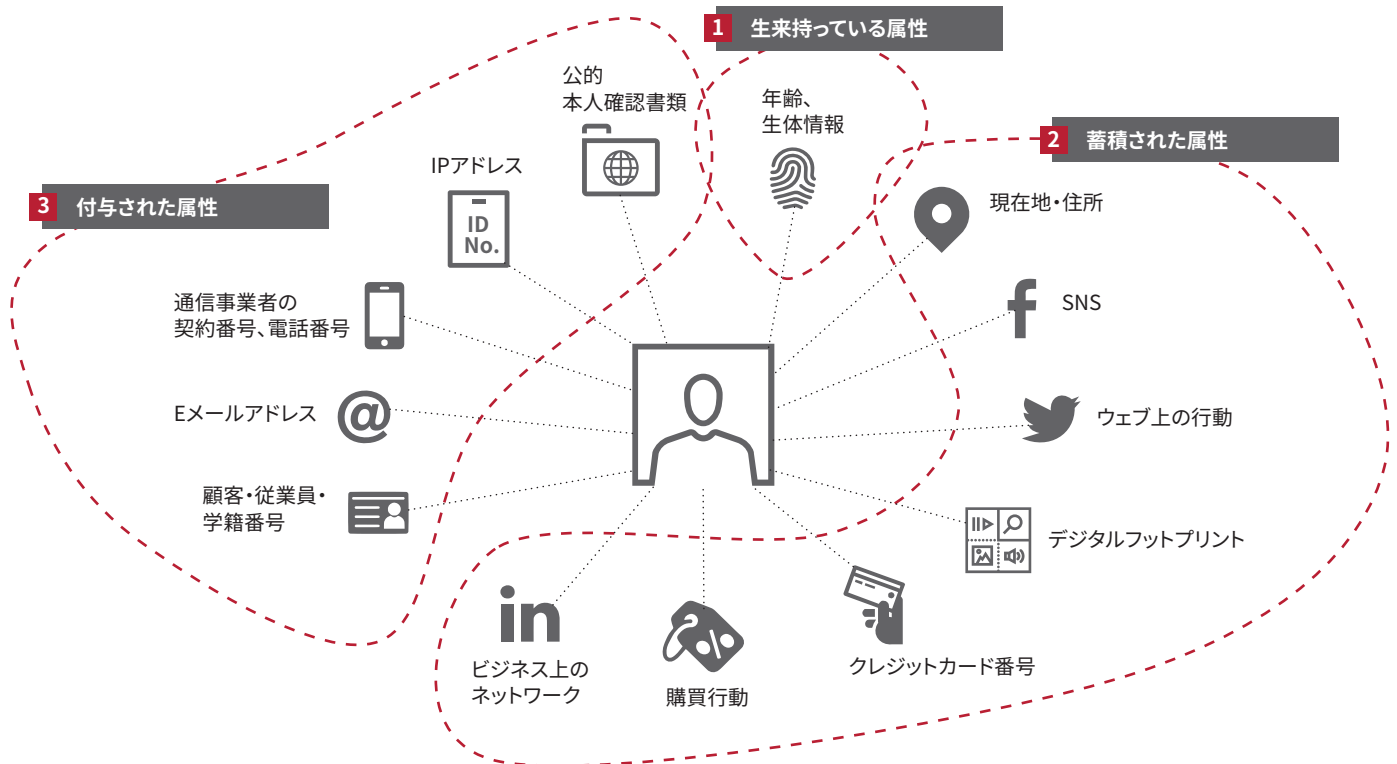
こうした動向から判断すれば、デジタルアイデンティティ(デジタルID)市場の成長は必然である。デジタルIDは、政府のサービスや給付に加えて、バンキング、職場、教育、医療関連など多数のオンラインサービスの利用において、本人識別子の役割を果たすバーチャル世界でのパスポートのようなものであるために、今後も整備が進むだろう。口座を開設するにも、取引するにも、サービスの購入契約にもデジタルIDが求められる。このように、デジタルIDは、日々の業務の効率化、時間短縮を図りながらセキュリティを維持する必要不可欠な機能を備えている。

本レポートでは、グローバルの既存事例や動向、ベストプラクティスを検証し、デジタルID業界に存在する機会に焦点を当てる。個人のアイデンティティとは、その人が生来持っている属性、過去に蓄積された属性および付与された属性が組み合わさったものである(図表1参照)。

現在、市場で主に利用されているデジタルIDは、中央集権型、サードパーティー管理型/フェデレーション型、自己主権型の3種類のIDシステムである。

デジタルIDシステムの第1号は1990年代に登場し、国が保有する従来の中央集権型IDシステムを基にしたものであった。

図表1
個人のアイデンティティを構成する属性の概要



2000年代の初めに、モバイル通信やデジタルバンキングが普及するとともにソーシャルメディアプラットフォームが登場すると、ユーザーは信頼する第三者を選んで自身のデジタルIDの管理を任せようになった(サードパーティー管理型)。デジタルIDプロバイダーの機能を持つ民間企業が登場し、一部には連携型のIDシステムも見られた(フェデレーション型)。この段階ではまだ政府も根幹的な役割を担っており、アイデンティティの枠組みを形成し管理することで上記のプロバイダーを支援した。

2010年代後半になって、顧客エクスペリエンスやデータ制御、プライバシー保護への関心が高まると、自己主権型IDシステムが誕生した。これは、ユーザーがアイデンティティの特性の所有・管理を自ら担う仕組みである(図表2参照)。

中央集権型、第三者管理型/フェデレーション型、自己主権型の3種類のシステムは全て現在でも使

用され、広く普及している。とはいえ、社会文化的規範や規制の枠組みの絶え間ない変化を受けて、システムも進化を続けている。例えば、一部の電子政府システムは、ユーザーが一定のデータを管理しコントロールすることを認めている。この場合は、ある公共主体にどのデータ(医療カルテなど)の共有を許可するかを個人が選択する。

各システムにはそれぞれ、メリットとデメリットがある。中央集権型モデルはセキュリティと信頼度が比較的高く、第三者や自己が管理する非中央集権型モデルはユーザーに比較的大きなコントロール権限を認めるために顧客エクスペリエンスが向上するというメリットがある。一方で、中央集権型モデルはシステム故障のリスクがあり、非中央集権型モデルは複雑なガバナンスが必要であり、かつアイデンティティ窃取のリスクが高まるというデメリットがある。

図表2
デジタルIDシステムの発展形態

	中央集権型IDシステム	第三者管理型/フェデレーション型IDシステム	自己主権型IDシステム
登場した年	1995	2006	2019
概要	単一プロバイダー(一般に公共主体)がユーザーのアイデンティティを確立・管理	信頼される第三者がユーザーの属性をサービスプロバイダーに送信またはチェックすることにより、同プロバイダーにユーザーが本人であることを保証	特定の管理主体に依存せず、ユーザーは自身のアイデンティティを自らで作成管理する。ただし、むやみに作成されるのではなく、信頼できる複数の第三者機関/エコシステムから保証されたものである
メリット	特に本人確認(KYC: Know Your Customer)手続きにおけるセキュリティと信頼を提供	ユーザーは効率的かつシームレスな体験を享受しながら幅広いサービスにアクセス可能	ユーザーのコントロールと信頼を強化することでユーザー体験を改善
デメリット	<ul style="list-style-type: none"> システム故障のリスク 大規模な投資が必要 寡占リスク 	複雑さ(技術面、ガバナンス面)	<ul style="list-style-type: none"> 複雑なガバナンス 開発途上の技術 ネットワーク効果発現までの期間が長い
例	e-Devlet Aadhaar Fedict エストニア共和国政府	Facebook BankID itsme® Mobile Connect GOV.UK (英国政府) Turkcell ZenKey	ICONLOOP Turkcell 韓国金融決済院

出所：世界銀行、TeleGeography、Strategy&分析

1.1. 市場の規模、主な成長要因と動向

全世界のデジタルID市場の規模は、2025年に約330億米ドルになると予測される。これは2020年の約160億米ドルから、5年間に年平均成長率（CAGR）16%で成長することを意味する（図表3参照）。この2桁成長の主な要因には、顧客エクスペリエンスや急増するサイバー犯罪、アイデンティティの窃取リスクへの重点的な取り組みと、生体認証（バイオメトリクス）の利用拡大が挙げられる。

新型コロナウイルス感染症により、Eコマースをはじめとする分野ではデジタルへの移行が加速した。その結果、Eコマース市場は2020年に最も急成長したセクターの一つとなった。顧客エクスペリエンスを高め、Eコマース事業者が組織犯罪やサイバー攻撃に遭わないようにする取り組みのなかで、Eコマースのアプリやプラットフォーム上での金融取引にデジタルIDソリューションが広く使用されるようになっている。また、世界中で電子デバイスの普

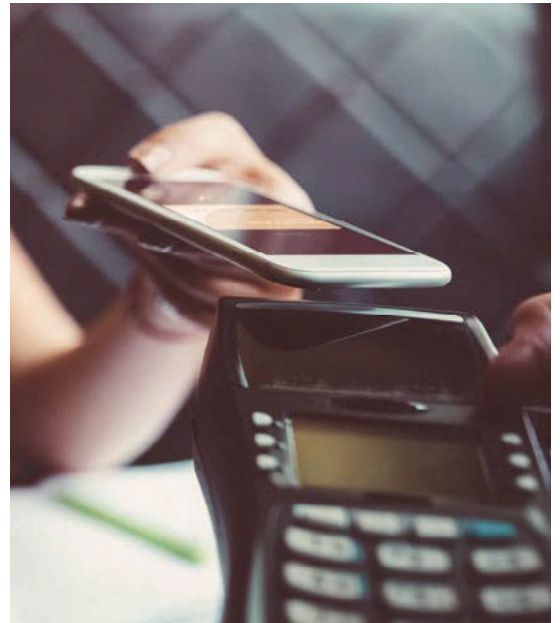
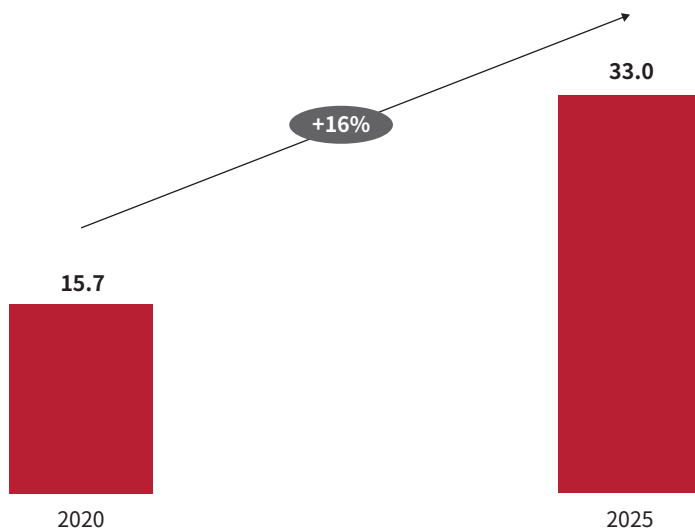
及と利用拡大が進んでいることも、市場が成長する1つの要因である。

電子政府プラットフォームの迅速な導入は、デジタルID市場の潜在性を表すものであり、市場規模の大幅な拡大を支える理想的な基盤となる。例えばトルコでは、電子政府ゲートウェイの立ち上げと電子IDの導入がデジタルIDソリューションの幅広い採用につながった結果、市場の成長が後押しされ、同ゲートウェイの利用者は5000万人を超えた。また、同市場の成長を表すもう一つの強力な指標が、電子署名である。トルコの電子署名の件数が2020年上半期末の時点で500万件に迫り、そのうち70万件がモバイル機器によるものであった。

電子政府のサービスを介した銀行のモバイルアプリへのログインも、金融サービス分野の代表的なユースケースである。ドイツやスペイン、フランス、最近ではトルコなど数多くの国で、デジタルID認証手続き（e-KYC）により銀行のオンラインサービス（口座開設など）を利用することができる。

図表3
世界のデジタルID市場規模

全世界のデジタルIDソリューション市場規模 (10億米ドル)



出所：GlobeNewswire、MarketsandMarkets、IDC、Strategy&分析

1.2. 市場セグメント

デジタルIDの活用先は、大きく2つのセグメントに分けられる。企業間 (B2B) と、企業 (対企業) 対顧客 (B2(B2)C) である。



B2B: 主として企業や政府機関が従業員を識別できるようにするサービスである。企業内のアイデンティティ管理、従業員による社内サービスの利用などがこれに含まれる。





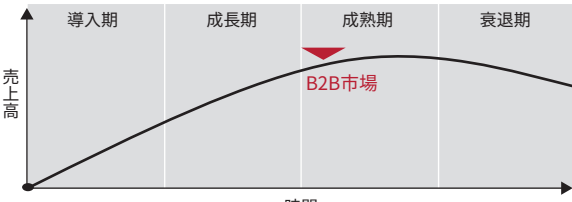
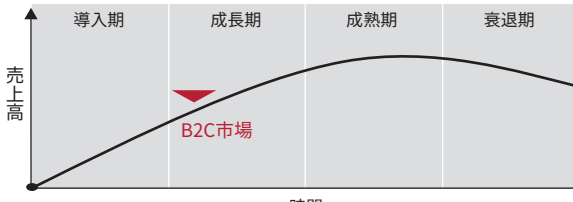
B2(B2)C: サービスプロバイダーが顧客を識別できるようにするサービスである。その内容はアカウントの作成、サブスクリプション管理、取引の認証などである。

B2B市場は高度に成熟した市場である。各種ソリューションはすでに十分確立されており、関連プレーヤーは安定的な収益モデル (SaaSやライセンスの付与による収益など) を構築済みである。一方

で、B2(B2)C市場は収益モデルが未成熟で一定の課題を抱えていることから、新興市場に分類されるかもしれない(図表4参照)。

図表4

B2B市場とB2(B2)C市場の主な特徴

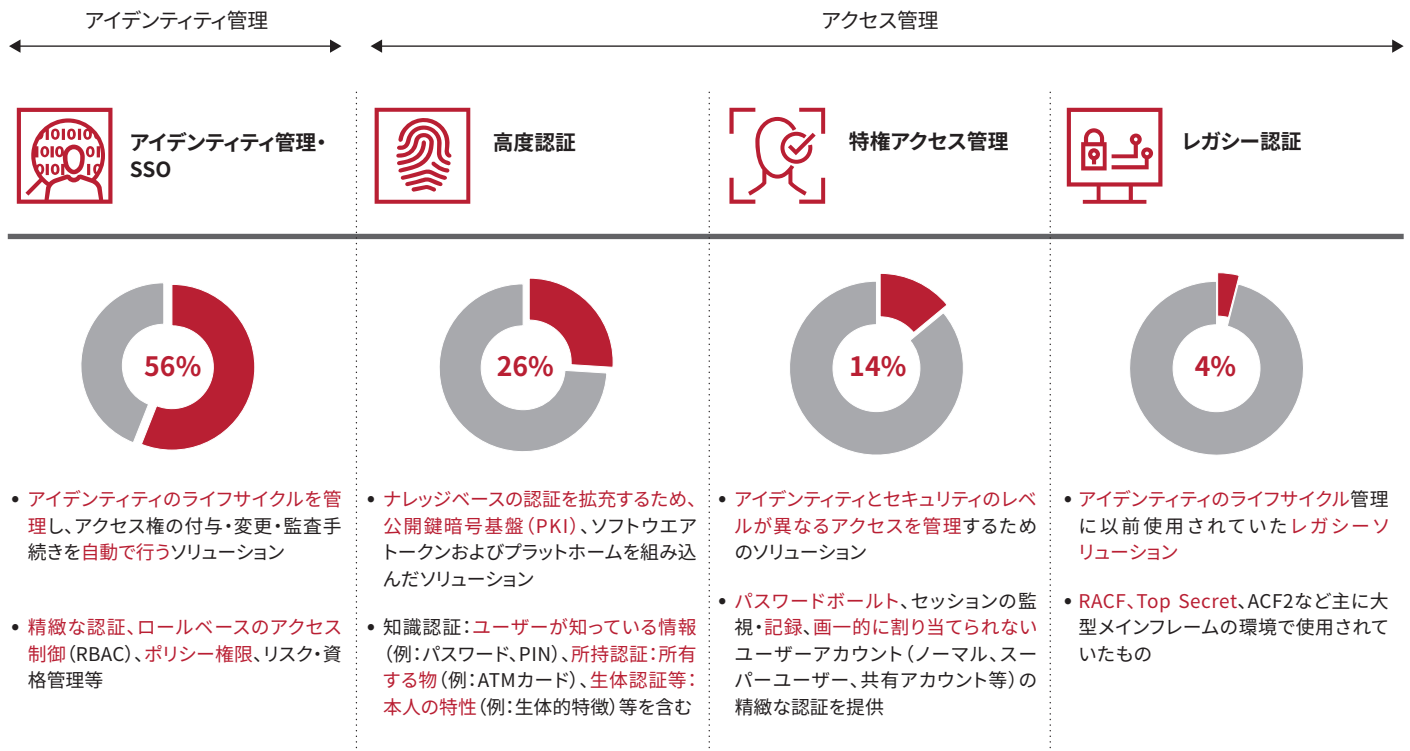
	 B2B市場	 B2C・B2B2C市場
クライアント	<ul style="list-style-type: none"> • 公的機関または民間組織 (例: 企業、政府) 	<ul style="list-style-type: none"> • エンドユーザー/サービス利用者 • サービスプロバイダー
収益モデル	<ul style="list-style-type: none"> • 有料サービス • ソフトウェアによる収益モデル (例: サブスクリプション、ライセンス付与等) 	<ul style="list-style-type: none"> • エンドユーザーは多くの場合無料 • サービスプロバイダーからの収益
提供価値	<ul style="list-style-type: none"> • 従業員やクライアントのアクセス管理・認証および本人確認を行うソリューションを組織に提供 (例: アイデンティティ管理) 	<ul style="list-style-type: none"> • 通信事業者向けに検証済みのアイデンティティやセキュアな取引を提供 (例: データベースのチェック、ドキュメントの検証、認証等)
市場の成熟度	 <p>売上高</p> <p>時間</p> <p>導入期 成長期 成熟期 衰退期</p> <p style="text-align: center;">B2B市場</p>	 <p>売上高</p> <p>時間</p> <p>導入期 成長期 成熟期 衰退期</p> <p style="text-align: center;">B2C市場</p>

出所: Strategy&分析

B2B市場は、更にアイデンティティ管理とアクセス管理の2つのセグメントに大きく分けられる。アイデンティティ管理あるいはシングルサインオン(SSO)と、アクセス管理の1要素である高度認証が市場の大半を占めている(図表5参照)。

図表5

B2BのデジタルID市場セグメント：2020年の時点で各セグメントが全世界の市場に占める支出シェア(%)



出所：IDC、Strategy&分析



B2Bのアイデンティティ市場の大半を占めるのは、アイデンティティ管理あるいはシングルサインオン(SSO)と、ユーザーの知っている情報や所有する物、本人の特性などに基づく高度認証である

B2(B2)C市場はアクセス管理を中心として構築されたモデルであり、識別と認証の両方のサービスを含む。識別では新規アカウントの作成やアプリケーションの購入が、認証ではログインサービスやトランザクション認証が主なユースケースとなる(図表6参照)。

図表6
B2(B2)CのデジタルID市場セグメント

	A 識別 (ID検証)		B ユーザー認証		
	データベースを照会し チェック	公的書類・生体認証 によるチェック	SFA (Single-Factor Authentication)	MFA (Multi-Factor Authentication)	RBA (Roll Based Authentication)
概要	サービスプロバイダーの1つ または複数のデータベース でユーザーIDを照会し、 新規 ユーザーのアイデンティティ をクロスチェック	特定の 属性がユーザーに 関連付けられている ことを チェック	登録ユーザーを単一要素で 認証	登録ユーザーを本人の選択 した多要素で認証	登録ユーザーを不正検知+ 多要素で認証
例	ユーザーIDを事業者、銀行 口座、個人信用調査機関等 のデータと突き合わせ	ユーザーは自身のIDカード をスキャンまたは読み込み、 顔の映像を撮影	ログイン名・パスワードの ペア	多要素認証要素例: ログイン名・パスワードのペ ア、WEB・端末のペア、パス ワードと生体認証等	不正検知方法例: 転送、購買行動、現在地等
代表的な ベンチマーク	AXA 保険契約 加入	Airbnb 新規アカウント 作成	Facebook サービスへの ログイン	3-D Secure 取引認証	Amazon Fnac オンライン取引での 不正取引の軽減

出所：IDC、Strategy&分析

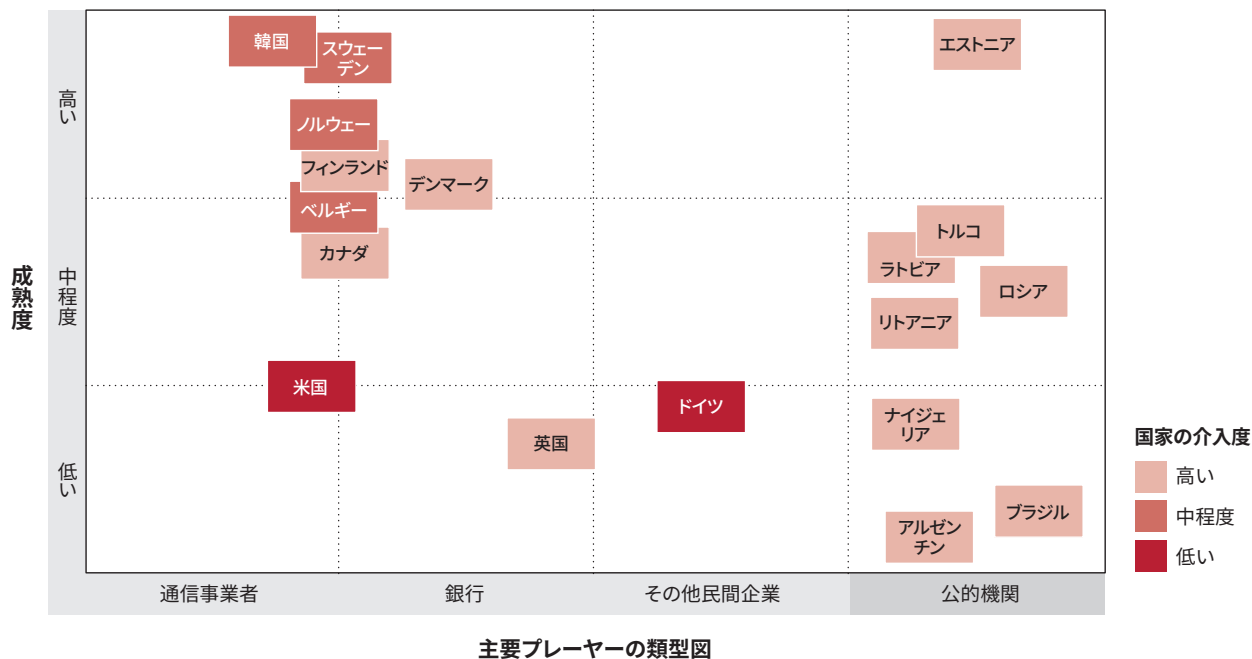


B2(B2)CのデジタルID市場は、データベースに照らしてチェックするなどの識別機能と単一要素・多要素認証などの認証機能を中心に構成されている

1.3. 主な成功要因

各国の通信事業者、銀行、企業、公的機関は、こぞってデジタルIDソリューション開発を後押ししてきた。その成熟度は国により明らかなばらつきが見られる(図表7参照)。

図表7
さまざまなデジタルIDモデルの概要



出所：Strategy&分析











成熟市場に共通した、特に重要な5つの成功要因を以下に紹介する。

1. 信頼性の確保と透明性のあるソリューション：
新規ユーザーに十分なレベルの信頼感を与えるには、ユーザーの信頼に足る透明性をもったソリューションが必要不可欠である。
2. 規制の整備(緩和/強化)：
国内の望ましい規制環境が整備されれば、デジタルIDの利用も喚起される。
3. 活用先の拡充：
ソリューションは可能な限り幅広く活用される必要がある。デジタルIDプロバイダーは、さまざまな異業種のプレーヤーと協力したりコンソーシアムを形成したりすることで、これを実現することが可能である(実践例：米国、ドイツ)。
4. ユーザービリティの確保：
ユーザーエクスペリエンスの設計は非常に重要であり、サービスとデジタルIDソリューションの各プロバイダーをシームレスに統合することが求められる。
5. エンドユーザーの無償利用
最後に、ビジネスモデルはごくシンプルなものとし、エンドユーザーには無償でソリューションを提供すべきである(図表8参照)。

図表8

デジタルIDソリューションの迅速な開発を成功に導く要諦のまとめ

	A サービスプロバイダー	B エンドユーザー
ソリューションの 適合性と透明性	 セキュリティレベルの高い頑健なアイデンティティ属性 検証を、IDプロバイダー自身の顧客に使用	 ユーザーからの信頼：データ保護、テクノロジー等 に関するコミットメント
ネットワーク効果の 得やすさ	 単一のソリューションで全対象者をカバーできる可能 性を備えた、対象範囲の広さ	 サービスプロバイダーのパートナーによるソリューショ ンの採用
シンプルで使いやすく、 障害が少ない	 サービスプロバイダーとIDソリューションプロバイダー のユーザー体験をシームレスに統合：中立的なブラン ディング、パスの単純化など	 エンドユーザーにとってのソリューションの使いやすさ
シンプルな ビジネスモデル	 従量制に基づくシンプルな価格設定モデル：サービス 単位、ユーザー単位で設定	 エンドユーザー向けの無償ソリューション

出所：Strategy&分析

1.4. 課題、リスクおよび脅威

市場やプレーヤーは数多くの課題やリスクを抱えており、セキュアで透明性が高く、かつ大規模な識別・認証プロセスの実現に成功した例は極めて少ない。現在、デジタルIDプロバイダーが直面する重要な課題は以下である。

1. 規制



規制当局は、個人データを収集、処理、共有する方法に関する透明性・安定性を備えた規則を定める必要がある。例えば韓国であらゆるEコマース取引のユーザー年齢確認を義務付けたように、デジタルIDの利用を促すような規制措置の結果、デジタルID技術の導入が進み、特定のユースケースの枠を越えて高度に発展したエコシステムが形成されるケースがある。

2. 顧客 エクスペリエンス



デジタル化によって、顧客は企業の事業運営と商品・サービスの中心となり、企業はシームレスな体験を顧客に提供する必要に迫られている。実際、そうした体験はあらゆるデジタルアプリの前提条件になっている。各プレーヤーは顧客の消費行動の動線に注意を払い、顧客第一のソリューション開発に力を入れなくてはならない。セキュリティと利便性の適正なバランスを見極めることは、デジタルIDソリューションのプロバイダーが直面する難題の最たるものである。

3. 規模と 対象範囲



成功を妨げる大きな要因の一つに、デジタルIDソリューションの導入をユーザーに対して説得するという問題がある。デジタルIDプロバイダーが効率的で信頼されるシステムを実現するためには、さまざまな客層を網羅する広範な顧客基盤を構築しなくてはならない。ところがユーザーは実績の少ないシステムを回避する傾向があるため、それが逆にサービスのさらなる成長を阻害している（鶏と卵の関係）。

4. 収益化



各プレーヤーは、エンドユーザーがデジタルIDアプリに追加料金を支払いたがらない現在のソリューションを収益につなげていかなくてはならない。ユーザーが進んで料金を支払うような事例は、欧州の先進国を中心に増えつつあるものの、その数はまだ少ない。

2. 連携と規模の拡大が必要不可欠

これまでに実施した分析と業界リーダーとの話し合いの結果、非常に多くのアプリケーションでデジタルIDが使用されていることが明らかとなった。通信事業者や銀行、その他民間企業、政府は、市場で自らを差別化し続けられる機会を精力的に模索している。これらのプレーヤーは多くの市場で、デジタルIDソリューションを協力して立ち上げたり参加したりすることが多い。こうした協業は成功を収める傾向にある(図表9参照)。

例えば、カナダのデジタルIDプラットフォーム、Verified.MeはSecureKey Technologies社の製品だが、国内の大手金融機関7社(BMO、CIBC、Desjardins、カナダ・ナショナル銀行、カナダロイヤル銀行、スコシアバンク、TD)との協力により開発された。Verified.Meの導入以後、カナダ国民はあらかじめ選択した個人情報の利用に同意することで安全かつ迅速にアイデンティティを検証できるようになり、情報の過剰な共有が緩和された。プロフィール

は信用調査機関や保険会社、健康センターなどの各種サービスと紐づけることができる。

プレーヤーが同業種・異業種をまたぐデジタルIDソリューションを提供したい場合、必要な規模のコンソーシアムを形成することは非常に重要である。米国のZenkeyがその一例だ。Zenkeyは国内のモバイルネットワーク事業者から成るジョイントベンチャー(JV)によって設立され、シームレスで優れた顧客エクスペリエンスを提供するとともに個人データへの制御を強化した結果、競合他社との差別化を実現した。Zenkeyは、デジタルIDプロバイダーとモバイル事業者をつなぐシンプルなインターフェースの役割を果たす。また、モバイル事業者の共有データベースを使用するため、アカウント作成に必要な属性はある程度簡素化される。Zenkeyは顔認証機能を使用しており、ユーザーはID認証を受けながら書類を記入することで、安全かつ迅速に登録を済ませられる。

図表9
通信事業者が単独または共同で設立したイニシアティブの例

通信事業者 1社	連携									
	主要な通信事業者との連携				銀行との連携				その他 民間企業同士の 連携	
市場シェア50%、第2位のアプリ開発事業者 2017年からOTT(「Over The Top」: 通信事業者やインターネット・サービス・プロバイダーに頼らず、インターネットを通じて提供されるメッセージや音声、動画などのコンテンツやサービスを指す)対象	10年間独立系事業として扱われていたが、2015年からソリューションが相互運用可能	2018年に主要通信事業者によるJV設立、2019年に立ち上げ	テクノロジーハブ(WSO2.Telco)を強みに、2017年にMobile Connectを中心に連携	2017年にMobile Connectを中心に連携	2007年にJV設立、2009年以降は他の通信事業者も受け入れ	2009年にJV設立、後に他の通信事業者も受け入れ	2016年にJV設立、2017年にItsme立ち上げ	2018年に通信事業者間と7つの銀行/SecureKey社がパートナーシップを結ぶ	2017年にJV設立、2018年にVerimi立ち上げ	
	1	3	4	7	4	3	3	1	4	1
	X	コンソーシアム	✓	共通テクノロジーハブ	✓	✓	✓	✓	✓	✓

出所: Strategy&分析

例えばデジタルIDを決済サービスやロイヤルティプログラムと組み合わせたオーストラリアのconnectIDのように、一部のイニシアティブは、可能な限り多くの企業を巻き込んだ全国規模のサービス提供を目指している。connectIDはオーストラリアのデジタルエコシステムを支えるマスマーケットのデジタルIDハブとして、最大手の銀行や小売企業から支援を受ける。このシステムを開発したのは、4000万件以上の銀行口座にアクセスを有する電子決済スキーム、EFTPOSである。connectIDは金融サービス、通信事業者、オンラインストア、政府省庁が行う全てのIDリクエストをオーストラリア国内のデジタルID発行者にシームレスにつなぐことができるため、企業はセキュアで機密性が高く、シンプルで信頼できるやり方で、顧客エクスペリエンスを改善することが可能である。

これらのプレーヤーの事例から、通信事業者、銀行、その他民間企業、政府が留意すべき以下の重要な教訓が得られる。

- 成功を収めるには、セキュリティと優れたユーザーエクスペリエンスが必要である。
- デジタルIDソリューションのケイパビリティ拡充、規模の実現、顧客基盤の拡大を目的とした同業種・異業種間のプレーヤー同士の連携が一般的である。
- IDソリューションを付加価値サービスと組み合わせることで、導入を拡大させることができる。
- 政府はデジタルIDイニシアティブの採用推進に向け、十分に練られた規制環境を構築する必要がある。

ある。市場が効果的に機能するために、こうした環境の整備は欠かせない。

- デジタルIDソリューションは銀行のリスク管理を改善し、本人確認(KYC)手続きを容易にするとともに、顧客エクスペリエンスと生産性を高めることができる。
- デジタルIDプロバイダーは、収益のシェアと早期導入割引を使ってサービスプロバイダーを呼び込むことができる。
- 長期的には、サブスクリプションモデルを採用したB2C収益化に大きなチャンスがあるといえる
- 通信事業者は、自社独自のソリューションよりもクロスキャリアのソリューションを採用する傾向が強い。

これとは逆に、今のところ成果を上げられず苦戦しているデジタルIDソリューションイニシアティブもある。こうした失敗例から学ぶべき重要な教訓を以下に挙げる。

- 顧客のエンゲージメントを高めるため、エンドユーザーにはデジタルIDサービスを無償で提供すべきである。
- 登録手続き、導入の手続きは、シームレスでなくてはならない。
- 政府は、関連業種間の連携を奨励すべきである。
- ソリューションは、付加価値サービスと組み合わせると成功しやすい。
- 導入を促進し消費者の信頼を得るには、十分な数のユースケースが必要不可欠である。

3. 結論：成功を収めるために

デジタルIDプロバイダーは一步引いて全体を眺め、系統立った手法をとることが肝心である。自身の分野で成果を上げ成長するためには、過去の成功例や失敗例に学びつつ、極めて重要ないくつかの

問いに答を出し、現在の市況を注意深く評価する必要がある。

デジタルIDプロバイダーが自問すべき重要な項目は以下のとおりである。

最大限の価値を創出するために最適な、自社のバリューチェーン内におけるポジションは？（例えば属性プロバイダー、デジタルIDソリューションプロバイダー、ソリューション再販業者のどれを目指すか決めておくことが重要である）



各セグメント・業種に適したプロモーションやマーケティング、市場開拓の戦略は？



直接的な価値以外に、将来的にサービスプロバイダーにとって重要な機会は何か？（金融関連IDとの接続、信用スコア、KYCデータの提供、政府とのパートナーシップ、地域レベルの拡大など）



他のデジタル企業やIT企業とのパートナーシップやコンソーシアムから、イノベーションを得られるチャンスがあるか？



市場開拓プランの大きな柱は何か？重要なマイルストーンは？成功を測定する方法は？



こうした問いへの答えを通じて、通信事業者、銀行、その他民間企業、政府組織は、デジタルアイデンティティ市場で大きな機会を見だし、オペレーションを強化することができる。

1

デジタルIDプロバイダーには、プレーヤーのひしめく市場で成功を収めるチャンスがある。セキュアで、かつシームレスな認証の発行がまだ実現していないからだ。アイデンティティは競争の激しい分野である。そのため、スピーディーな市場開拓戦略が欠かせない。

2

プレーヤーはそれぞれ異なる価値創出手段を模索することが可能である。例えばID検証サービス(IDV)、属性情報の幅広い取得、ユーザー認証、その他広告や不正分析などが挙げられる。

3

成功するための市場開拓戦略においては、市場の潜在性と関連プレーヤーの優位性を検討したうえで、業種とユースケースに優先順位を付ける必要がある。Eコマース、メディア、ヘルスケア、金融サービスなど、あらかじめ業種を決定し、的を絞った戦略を練ることができれば、他社に大きく水をあけることができるかもしれない。

4

生体認証技術などの分野で目立つ競争の激化は、デジタルIDプロバイダーへの脅威になるかもしれない。そのため各プレーヤーは、提携や買収を通じた生体認証・行動認証に関する対応力の獲得を検討すべきである。

5

KYCプロセスの合理化、より効果的な不正・リスク管理、規制順守の強化を通じてコスト削減が可能である。サービスプロバイダーはデジタルIDの恩恵を享受して、最終的にミスを減らし、オペレーションの効率性を高め、複数のコスト削減シナジーを実現することができる。

6

デジタルIDにより、サービスプロバイダーは登録手続きを合理化し、データの機密性を高められることから、顧客基盤を拡大することが可能となる。また、デジタルIDを生かしてより複雑な商品を発売することで、さらなる集客が見込める。

7

デジタルIDソリューションの普及に政府が果たすべき役割は大きい。政府は民間部門の連携を奨励し、企業によるデジタルIDソリューションの立ち上げと利用拡大を支援する必要がある。

デジタルIDプロバイダーは、バリューチェーン内の自身の戦略的ポジションを絶えず修正すべきである。最も潜在性の高い顧客セグメントに優先して取

り組み、関連するソリューションプロバイダーと連携することで、この萌芽期の市場を制するチャンスをもにすることができるだろう。

Strategy&

Strategy&は、他にはないポジションから、クライアントにとって最適な将来を実現するための支援を行う、グローバルな戦略コンサルティングチームです。そのポジションは他社にはない差別化の上に成り立っており、支援内容はクライアントのニーズに応じたテイラーメイドなものです。PwCの一員として、私たちは日々、成長の中核である、勝つための仕組みを提供しています。圧倒的な先見力と、具体性の高いノウハウ、テクノロジー、そしてグローバルな規模を融合させ、クライアントが、これまで以上に変革力に富み、即座に実行に移せる戦略を策定できるよう支援しています。

グローバルなプロフェッショナル・サービスにおいて唯一の大規模な戦略コンサルティング部門である Strategy&は、クライアントが目指すべき方向を示し、最適な方法を選択し、実現させる方法を提示すべく、戦略策定のケイパビリティを PwC の最前線のチームに提供しています。

その結果は、可能性を最大化するために強力だけでなく、効果的に実現できるような実践的アプローチであり、信頼性の高い戦略プロセスです。今日の変革が明日の成果を再定義するような戦略です。ビジョンを現実のものへと作り上げる戦略です。“It’s strategy, made real.”戦略が現実のものになるのです。

www.strategyand.pwc.com/jp

本報告書は、PwCメンバーファームが2021年に発行した『Digital identity: Opportunities and challenges A perspective for telecom operators, banks, industrial companies and government institutions』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。

<https://www.strategyand.pwc.com/jp/ja/publications/report.html>

オリジナル(英語版)はこちらからダウンロードできます。

<https://www.strategyand.pwc.com/tr/en/medya/digital-identity.html>

日本語版発刊年月：2021年12月