あずさ監査法人

Digital Identity（デジタルID）

2019年12月12日

金融取引のデジタル化が進むなか、本人確認への新技術の活用が拡大している。本稿は、①“Digital Identity”（以下「デジタルID」）についてFATFが公表した指針案と、②米国における「デジタルIDの共用可能性（portability）の実現」に向けた動きを紹介し、最後に③わが国への示唆を簡単に記す。

金融アドバイザリー部
ディレクター
水口 毅

日本銀行広島支店長等を歴任した後退職、米系大手保険会社の役員を経て、2016年から有限責任 あずさ監査法人金融アドバイザリー部ディレクター。
現在はレグテック等を担当。

日銀在職中の2000年、政府が「ミレニアムプロジェクト」で「電子政府構想」を打ち出した後に「国庫金事務の電子化について」を公表し、e-Tax実現に向けたプロジェクトを開始した経験をもつ。

本稿の目次

1. はじめに ―「本人確認」について
2. デジタルIDに関する「FATF指針案」
   (1) デジタルIDシステムの特徴と具体例
   (2) デジタルIDシステム活用の「メリット」と「リスク」
   (3) 銀行が個別のデジタルIDシステムの採用可否を決める際のプロセス
3. 米国におけるデジタルIDの「共用可能性」の実現に向けた動き
4. わが国への示唆

1．はじめに ―「本人確認」について

不正金融取引（マネーローンダリング、テロ資金供与、脱税、贈収賄、大量破壊兵器拡散金融等）の阻止に、偽名や借名の取引の排除は必要である。このため、銀行による顧客の「本人確認」は、銀行自身・社会の双方に重要な意義を持つ。

わが国の銀行が現在「本人確認」の方法は、殆どの場合「アナログ」である。しかし、仔細にみると、①「ネットで完結する本人確認」を許容する犯収法省令改正が昨年11月に実施されたほか、②それ以前から「公的個人認証サービス」が制度として確立されており、今後、実務対応としても「脱アナログ＝デジタル化」を目指すべき状況にある。

原点に戻って考えてみると、「本人確認」とは、「本人に固有の“特徴”を分析することで、対象者が『本人』であることを確かめること」と定義できる。現代は、「ユーザーIDとパスワードの確認」に加えて、「指紋」、「虹彩」、「顔」、「キーボード打鍵時の癖」、「スマートフォン（以下「スマホ」）携帯時の癖」等、さまざまな個人的属性（personal attributes）を、複数組み合わせて確認できる時代である。そして、それらによって、高い精度での「本人確認」が可能となっている。

この点、とりわけスマホの「普及」とその「技術の進歩」の貢献は大きい。

海外に目を転じると、「デジタルID」（デジタルな方法による本人確認）の利用の拡大は特に新興国で顕著である。中国では、Ant Financialによる顔認証が拡大している。インドでは、わが国の企業の生体認証技術を使ったデジタルIDシステムが、既に12.5億人を登録している。こうした展開は、これらの国々における新しい金融サービスや金融包摂の拡大に寄与している（同時に、データ・プライバシー保護の懸念も生じている）。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

2．デジタルIDに関する「FATF指針案」

10月末に、マネーローンダリング・テロ資金供与の阻止のための国際基準の策定等を使命とするFATFが、"Draft Guidance on Digital Identity"（本稿では「FATF指針案」と呼ぶ）を公表した（FATFは「同指針は2020年中に完成させる予定」としている）。

言うまでもなく、新技術には新しいリスクが伴う。「FATF指針案」は、各国で採用が広がるデジタルIDシステムの「メリット」、「リスク」を示し（→本章(2)）、さらに、銀行が個別のデジタルIDシステムのCDDへの採用可否を決める際のプロセスを論じている（→本章(3)）。

(1)　デジタルIDシステムの特徴と具体例

①　FATFは、次の4つの特徴を挙げて、議論を始めている。

a. 本人確認[1]の基礎的な情報（源）として、電子的なデータベースが存在し、活用されること。ここで、「公的機関の情報活用」が（電子的に）実行される（日本の場合、J-LIS（地方公共団体情報システム機構）のデータベースがこれに該当）。

b. 本人であることを確認するプロセスとして「モバイル端末を利用した」、あるいは「オンラインによる」、場合によっては「対面での」ものも含めて、「本人確認プロセス」が含まれており、それを踏まえて「本人であることを確認した」旨の証明（digital credential）の発行がなされること（日本の場合、「公的個人認証サービス」がこれに該当）。

c. 本人確認の目的のために、「生体認証」（目視によるものを含む）が行われること。

d. オンライン本人確認においてAPI、プラットフォームなどの技術が利用されること。

②　世界銀行のID4D（Identification for Development）によれば、世界に公的な本人確認書類を持てない人が10億人存在する。また、特に新興国において、デジタルIDシステムの新技術が急速に広がる"leapfrogging"がみられる。

——　FATF指針案はAppendix Bに各国等の18の事例を掲載。詳細に説明したものが12例あり、その中に中国の2例を含む（一方が民間主導<次表の1.>、他方が政府主導）。国名だけ挙げたものが6例。米国、日本は含まれていない。

——　次表の1.～3.は、デジタルIDシステムの例として特徴的なものを敢えて3つに絞って掲載。また、これらと比較する目的で、4.として日本のマイナンバーカード／公的個人認証の説明を加えた。なお、米国については第5章参照。

1 FATFは、FATF指針案では、銀行取引等で使える「公的な本人性」（official identity）の確認に限定して論じている。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

国・地域	具体例	説明
1.中国	Ant Financial デジタルIDentity	① 12億人のAlipayユーザーを擁するAnt Financialが構築、運営。 ② 顧客の名前とID番号は、国の公安部（Ministry of Public Security）のデータベースを使って確認（検証）。 ③ 顔認証を活用。2017年秋に杭州のKFC（ケンタッキーフライドチキン）で世界初の顔認証による支払を実現した後、年金受給、税申告、荷物受取、ホテルのチェックイン、公共交通の改札などで次々と「顔パス」を実現。 ④ 最近の報道では、11月11日（中国でネットショッピングの大キャンペーンが行われる「独身の日」）を前にブロックチェーン技術を導入済とのこと。
2.インド	Aadhaar（アドハー）	① インド政府（固有識別番号庁＜UIDAI＞）が運営。生体認証システムはわが国の企業が提供。 ② 国民一人ひとりに固有のIDを発行。指紋・顔・虹彩の認証を活用。 ③ 12月1日時点で12.5億人が登録済。 ④ インドでは、「生年月日」の公的な記録（出生証明）を持たない人が多いことなどが本人確認上の問題だったが、Aadhaarは生体認証の活用でこの問題を乗り越えている。 ⑤ 国民は、国からの社会保障関係給付等の受給、銀行口座開設などの際に使う。
3.シンガポール	SigPass、MyInfo、National Digital Identity（構築中）	① シンガポール政府は、国民が電子政府サービスを受ける際の認証システムSingPassを2003年に稼働済。 ② 同政府はまた、MyInfoという「国民各人が自らの個人情報を政府のデータベース上で管理するためのサービス」の提供を2017に稼働済。MyInfoには、個々人の選択により、政府各省庁が確認済の当該個人の個人情報や、その他データ（電話番号、メールアドレス、家計の収入月額等）、総計100項目以上を掲載できる。 ③ MyInfoは、国民にとっては、対政府や対銀行・クレジットカード会社等の手続の際に求められる個人情報を「一括して」相手先組織に提供できるメリットがある。銀行等は、顧客から個人情報を書類で提出してもらう手間が省略できる。 ④ National Digital Identyは同政府が現在構築中のシステムで、個人と法人双方を対象にし、デジタルな本人確認を可能とするシステム。2020年中に稼働予定。
4.日本	マイナンバーカード／公的個人認証	① マイナンバーカード（個人番号カード）は、2016年1月に交付が開始された。その前身は「住民基本台帳カード」（2003年に交付開始）。 ② 「行政手続における特定の個人を識別するための番号の利用等に関する法律」に基づき発行される身分証明書で、持ち主の氏名、住所、生年月日、性別、個人番号（マイナンバー）、証明写真などを券面に表示。これらを記録したICチップを内蔵（ただし、マイナンバー＜番号＞そのものはICチップへの記録対象外）。 ③ 各市町村の「住民基本台帳」をネットワーク化したものが政府のデータベースとして使われている。 ④ 電子申告（e-Tax）に使える。また、銀行の顧客受入時に「ネットで完結する本人確認」（犯収法施行規則6条1項1号のホ、ヘ、ト、ル）用の資料として使える。継続的顧客確認のためにも、「公的個人認証」（上記「ル」）の場合は、一定期間経過後に「本人特定情報が失効していないこと」を非常に低コストで確認できる。 ⑤ 交付枚数が少ないこと（人口比14.3%=1,823万枚、2019年11月初時点）が最大の問題。来年2020年に最大5,000円相当の「マイナポイント」還元策が予定されている。 ―― なお、ICカード搭載情報の読み取りにカードリーダーが必要な点も活用上のネックだったが、最近iPhoneで読取り可能となり、この点は劇的に改善した。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

(2) デジタルIDシステム活用の「メリット」と「リスク」

① メリット

1.人間によるCDDの欠点の排除	窓口担当者の経験・スキル・注意力・主観的な判断に依存する「人間によるCDD」の欠点を排除できる。
2.顧客体験の向上	FATF指針案は、「英国では金融機関のKYC手続の難しさ等を理由として、顧客の25%の取引申込を放棄している」との試算(世銀、Private Setor Economic Impacts from Identification Systems, 2018に掲載された民間の試算）を紹介している。
3.事務処理コストの節減	FATF指針案は、「顧客受入時の手続にデジタルIDの活用を組み込むことで、所用時間を数日～数週間から数分に縮減、最大で90%のコスト節減が出来る」との試算（McKinsey Global Institute, Digital Identification,2019による試算）を紹介している。
4.取引モニタリング・疑わしい取引の届出の容易化	例えば、顧客からのオンライン取引のアクセスがあった時に、そのアクセス元の「地理的な位置」、「IP address」、「アクセスに使われているIT機器の種類」等を知ることにより、「異常な（あるいは疑わしい）取引」を特定することが容易になる。
5.金融包摂	特に発展途上国において、デジタルIDの普及は①国から国民への社会保障関係を含む多くの種類の支払（G2P）の容易化・堅確化、②貧困層を含む銀行取引のすそ野の拡大等に貢献。

—— FATF指針案は、1.に該当するメリットが生じた具体例として、ナイジェリアの「幽霊公務員の撲滅」を紹介。

すなわち、同国では、「幽霊公務員」による公務員給与の不正受給の横行が疑われる中で、2015～16年に、同国中央銀行が民間銀行に対して生体認証を基盤として銀行の顧客個々人に固有番号（Bank Verification Number）を付することを求めた。これによって公務員の給与支払名簿から5万人の「幽霊公務員」を排除し、74百万米ドル相当の不正受給を無くしたとのこと。

—— 5.については、次章に示すインドの「Aadhaar」がその好例。

② リスク

デジタルIDシステムの活用は、「対面での本人確認」とは異なるリスクや問題を生じる場合がある。次に示す事項から明らかなとおり、「対面」でも起こるリスクや問題も多い。しかし、不正や攻撃が生じる頻度・反復性・発生規模等が、「サイバー空間」の場合は「対面」の場合に比べて格段に大きくなることがあり、注意が必要である。

1.顧客登録プロセスでの不正	① なりすましによる登録 他人の本人確認書類の盗取・偽造・変造等により、実在する他人になりすまして銀行口座を開設するような場合。 ② 架空の人物の登録 多くの場合、複数の他人の本人書類の盗取・偽造・変造に「合成」の手間を加えて、架空の人物の名義等を作り上げ、銀行口座を開設するような場合。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

2.顧客認証プロセスへの不正な侵入	① パスワードリスト型攻撃（Credential Stuffing） 「ユーザーアカウント情報」を盗取したり流出したものを悪用したりして、自動で多数かつ様々なサービスに不正にアクセスしようとするサイバー攻撃。多くのサービスに同じユーザーID、パスワードを「使い回し」している顧客が被害に遭いやすい。 ② フィッシング（Phishing）攻撃 偽メールや偽ウェブサイトを使って、他人のユーザー名、ユーザーID、パスワード等を入力させ、それを悪用する攻撃。 ③ man in the middle攻撃（中間者攻撃） ユーザー（例：銀行顧客）とサービス提供者（例：銀行）の間に「通信を中継する形」で勝手に割り込むことでメッセージの改ざんなどの不正を行う攻撃。 ④ キーロガー（key logging） ユーザーがPC等のキーボードに入力する内容を密かに盗取・記録し、悪用する行為。

ユーザーIDとパスワードの盗取は、ユーザーの自己防御姿勢の甘さに乗じることが多いが、時に、ユーザーの誰か、あるいはサービス提供者の内部者が、犯罪者への売却を目的にユーザーIDやパスワード等のデータを不正に扱う場合もある。顧客による口座の売却等がそれにあたる。これは対面でも非対面でも起こり得るが、デジタルIDシステムが用いられる場合には、「多数の」銀行が犯罪の場になる可能性が高い。例えば「ひとりの口座開設担当者が、多数の銀行に口座を次々と開設し、犯罪者がその者のID、パスワードを購入した上で、犯罪収益を転々と移転させて資金の洗浄を図る」ケースが挙げられる。

これらのリスクには、①多要素認証（MFA：Multi-Factor Authentication）、②生体認証、③顧客のライフサイクル（取引開始から終了までの期間）を通じた適切な顧客管理などで対応することとなるが、①～③のそれぞれにも弱点があることを理解すべきである。また、新技術の導入は④未知のリスクも伴いがちである。新技術を導入した後にその欠陥に付け入られると、その犯罪手口が明らかになるまでは、銀行等にとっては未知のリスクに晒されたままの状態が続くことになりがちである。

デジタルID Sytemの活用時には、次のような点にも留意が必要である。

1.顧客の本人確認等に「他機関への依拠」が利用される場合で、依拠元の銀行等が依拠先から取引モニタリング等に有益なデータの取得・分析をしなかったケースの問題	上記(1)メリットの4.に記したとおり、例えば、顧客からのオンライン取引のアクセスがあった時に、そのアクセス元の「地理的な位置」、「IP address」、「アクセスに使われているIT機器の種類」等を知ることにより、「異常な（あるいは疑わしい）取引」を特定することが容易になる。 しかし、顧客の本人確認・認証について、サービス提供者（銀行等）が自身でそれを行わず、委託先が運営するデジタルIDシステムに依拠するような場合に、サービス提供者が「継続的な顧客管理」や「取引モニタリング」を行う際に有益なデータを委託（依拠）先から取得しない場合には、こうしたメリットを享受し損ねるリスクがある。従って、依拠元の銀行等は、依拠先から広範囲のデータを取得し、分析するようにしなければならない。 複数の銀行等がひとつのデジタルIDシステムを共用する場合には、デジタルIDの本人確認・認証を行う組織とそれに依拠する複数の銀行等が、詐欺等の不正を行おうとする者を含む顧客からのアクセス情報を（一定の条件のもとで、コンソーシアム的に）共有することにより、不正の早期検知が可能になる可能性もある。
2.接続（connectivity）に関する問題	デジタルIDシステムは、電力供給やインターネット接続が信頼出来、スマホ等デジタル機器の普及率が非常に高い前提で使われる。そのため、それらに支障が生じた場合に問題が生じる。 デジタルIDシステムを、電力供給が停止した場合にオフラインで使えるようなバックアップ体制を構築することも検討に値する。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

3.各国に既存の公的な本人確認書類が狭い目的で多種類作られている場合の問題	FATFは、各国の本人確認書類のあり方について、特定の要請は実施していない。そうした中で、ある国では「広範囲な目的に使うことを想定して作られた本人確認の制度」がある一方、他の国では「個別具体的な（狭い）目的に使うことを想定して作られた本人確認書類が林立する状態」になっている（現状、わが国を含めて多くの国々は、後者に属すると考えられる）。後者の国では、AML/CFT規制を受ける銀行等にとって本人確認対応時のコストが高くなりがちである。 FATFは、既存の公的な本人確認書類等のあり方を、デジタルIDの時代に適合するように改善し、より効率的なものとしてきた国として、フランス、韓国、シンガポールの名を明示している。
4.データ保護、プライバシーの問題	デジタルIDは、対象となる個々人の属性情報を収集する。その中には当然「個人情報」が含まれる。このため、データ保護、プライバシー保護は、それぞれの法域で適切とされるレベルに適合したものでなければならない。各法域でこれらの保護の枠組みを決定するのは政府であり、遵守するのはデジタルIDシステムのサービス提供者である。サービス提供者は、データへの不正アクセス、データの滅紛失・破損・濫用当等が発生した場合に備えた対策も用意すべきである。 データ保護の枠組みやリスク低減措置等が劣る国は、IDの盗難やサイバー攻撃のリスクの高い国であり、信頼性の劣る国とみなされる。 各国においてAML/CFTを所管する省庁とデータ保護・プライバシー問題を所管する省庁は、互いに協力すべきである。デジタルIDシステムのサービス提供者は、自らにデータ保護に関する評価（DPIA：Data Protection Impact Assessment）を実施すべきである。新技術は、「データやプライバシーの保護」をより強固なものにする場合、より脆弱なものにする場合の両方の場合がある。
5.金融排除（financial exclusion）の可能性	①デジタルIDシステムの利用可能範囲が限られている場合、②ITリテラシーが劣る消費者がいる場合、③インターネットアクセスが可能な地域が限られている場合等は、結果的に貧困層、地方居住者、女性、難民などを「金融排除」の対象としてしまう可能性に留意すべきである。 生体認証についても、①手作業労働者についての指紋認証の失敗、②高齢者についての顔認証の失敗、③特定の人種についての生体認証上の質の低さなどが「認証不調」による「金融排除」を生む可能性があることに留意し、代替的な認証手段を用意すべきである。

FATF指針案は、このほか、デジタルIDシステムのサービス提供者が、大規模なサイバー攻撃等に屈してそのインフラに損害を蒙るリスクも指摘している。しかし、同指針案は、「（こうしたリスクへの対処は）より広いガバナンス・組織の統制の問題であり、この指針案での記載の対象にはしない」としている。

デジタルIDについては、国民の情報を政府が管理することに政治的な意味も存在し、そのことに国民側からの反対や嫌悪感も生じがちである。このことは、特に先進国で顕著で、米国におけるNSTIC（National Strategy for Trusted Identities in Cyberspace）の取組み（2011年～）に対するアメリカ自由人権協会（ACLU：American Civil Liberty Union）の反論等が挙げられる[2]。さらに、この点については、中華人民共和国香港特別行政区（SAR）で民主化を求める人々が、携帯電話の位置情報はオフに、列車の切符購入は現金にして、ソーシャルメディアでのやりとりはすぐに消去するなどの「デジタル断ち」をして、当局の監視や将来訴追される危険を回避しようとしていることが想起される[3]。

2 改めて言うまでもないが、この問題は非常に繊細な問題である。Digital Identityについての比較的新しくかつ詳細なレポートであるMcKinsey Global Instituteの Digital Identification, 2019は「The political risks and benefits of digital ID are potentially significant and deserve careful attention but are beyond the scope of this report.」としている。

3 香港では、既に11歳以上の香港特別区の住民や180日以上香港に居住する者に「ICチップを内蔵するスマートIDカードを取得し、常時携帯すること」が義務付けられている。またDigital ID Systemについても、「electronic personal identity (e-ID) system」の構築プロジェクトが稼働している。今回のFATF指針案には、香港についての言及は無い。ちなみに現在のFATFのトップ（president）は、中国人民銀行法務局長のXiangmin Liu（刘〈劉〉向民）氏である。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

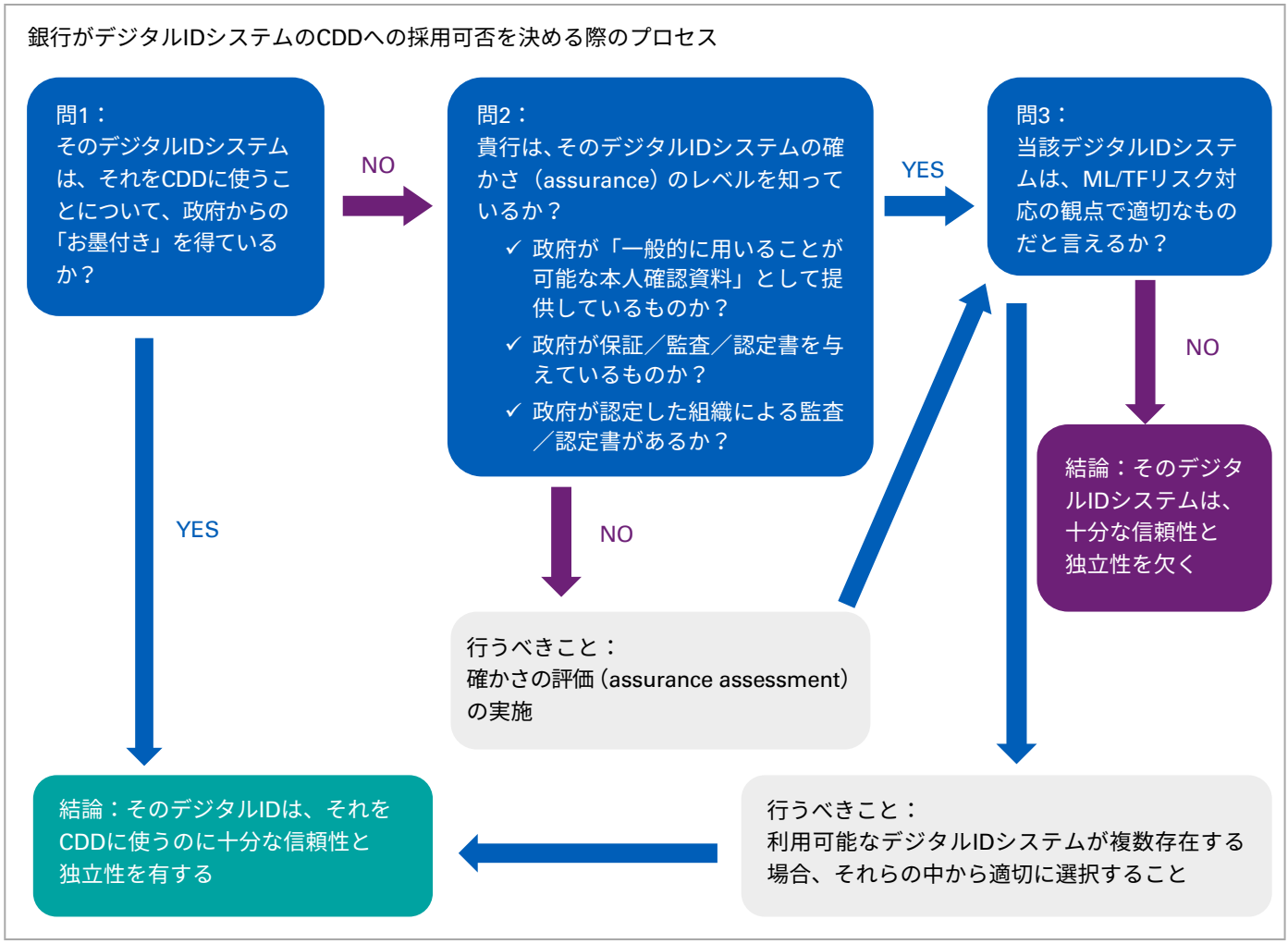
(3) 銀行が個別のデジタルIDシステムの採用可否を決める際のプロセス

① FATF指針案は、銀行など、AML/CFT規制を受ける金融機関等が、個別のデジタルIDシステムを自らのCDDに採用して良いかどうかを決める場合について、次の3つの問に答えるべきとし、それらの問を組み込んで、下に掲げる「プロセス」を提示している。

問1：そのデジタルIDシステムは、それをCDDに使うことについて、政府からの「お墨付き」を得ているか？

問2：貴行は、そのデジタルIDシステムの確かさ（assurance）のレベルを知っているか？

問3：当該デジタルIDシステムは、ML/TFリスク対応の観点で適切なものだと言えるか？



出典：FATF「Draft Guidance on Digital Identity」（https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html）34頁Figure 4を翻訳

② （2）上記の問2の関係で、銀行等は「デジタルIDシステム」について、「確かさの評価」（assurance assessment）を実施する必要に迫られるが、FATF指針は、当該評価を実施するにあたり、米国やEUの公的な機関が公表している「枠組み・基準」（digital ID assurance framework and technical standards）が役に立つと指摘している。

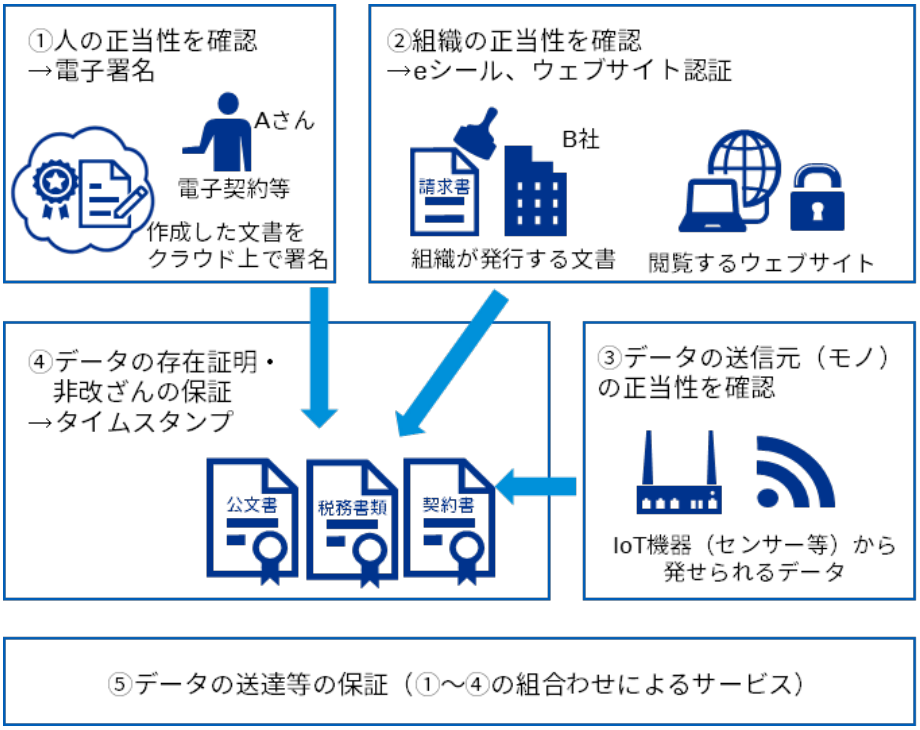
この「枠組み・基準」は、次の米欧の例に加えて、ISO等多数の国際機関が公表していることが示されている。

- 米国立標準技術研究所（NIST）の認証に関するガイドライン「Electronic Authentication Guideline（電子的認証に関するガイドライン）」第3版（NIST SP 800-63-3、JIPDEC〈一般財団法人日本情報経済社会推進協会による紹介記事参照〉）
- EUのeIDASのフレームワーク

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

なお、わが国の総務省においても、「日本版のeIDAS」策定を目指す動きがあり、本年2019年1月には「プラットフォームサービスに関する研究会」の下部組織として「トラストサービス検討ワーキンググループ」設置され、6月24日には「中間取りまとめ（案）」が公表されている。

—— この「中間取りまとめ（案）」の4頁に示された「トラストサービスのイメージ」は、次のとおり。



出典：総務省「プラットフォームサービスに関する研究会 トラストサービス検討ワーキンググループ中間取りまとめ(案)令和元年6月24日」(http://www.soumu.go.jp/main_content/000630548.pdf)の4頁をもとに加工して作成

3. 米国におけるデジタルIDの「共用可能性」の実現に向けた動き

(1) FATF指針案は、デジタルIDシステムの具体例の紹介などでは、本稿2．(1)で記したとおり米国の事例を記載していない[4]。他方、デジタルIDシステム関係の概念の整理や「確かさの評価」(assurance assessment)については、米国立標準技術研究所(NIST)の認証に関するガイドラインの記述を援用している。

そこで、本稿では、米国におけるデジタルIDについての議論の状況にも目を向けた。その結果の要点を以下に紹介する。

財務省は、報告書「経済的機会を創出する金融システム:ノンバンク、フィンテック及びイノベーション」(2018年7月、Mnuchin蔵相からTrump大統領宛の報告書)の第1章「デジタライゼーション、データ、テクノロジー」において、「Digital Legal Identity」と題する「囲み記事」(4頁に及ぶ)を掲載。骨子は次のとおり。

4 FATFは、その参加国37か国中過半数の20ヵ国が欧州（含むロシア・トルコ）であり、かつFATFは1国1票制を採用している（IMF、世銀が出資比率勘案であることと違う）。本部もパリのOECD本部内に置かれている。こうした中で、FATFにおける議論は「欧州の視線」で進むことが多いとされる。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

① グローバル経済での競争がデジタルエイジに深く突き進む中で、個人や法人の本人確認についての「信頼性」、「安全性」、「プライバシー」、「利便性」を高めるために、デジタルIDは貴重な将来性を有する。デジタルIDシステムはまた、金融サービスを提供する企業（注：銀行を含む）に、効率性の向上とコストの削減のメリットをもたらすと期待される。信頼度の高いデジタルIDシステムは、顧客口座開設時の本人確認、口座にアクセスがあった時の認証、リスク管理、不正防止対応等を高度化させる。

② 金融取引には「法的な意味での」IDが必要。「Digital Legal ID」は、電子的な手法を用いて、実在の人物の法的な本人性（identity）を明確に確認し、認証するものである。

③ この「Digital Legal ID」には、各種サービス間での「共用可能性」（portability）を持つことが望ましい。この「共用可能性」とは、ひとたび確認されたある個人のIDが、別の金融機関との取引や、政府の省庁に対する電子政府サービス受給のためのアクセスの際のIDとして、改めて自らの個人情報を提示し直すことなく使えるようになっていることを意味する。民間の第三者機関による「信頼度の高い、共用可能性をもつデジタルIDに関するサービス」が（現行の米国の法制下では民間部門に認められていないものだが）可能となれば、それに依拠する企業(注：銀行を含む）にとってCDDに要する時間・経営資源の節減が可能となる。この「Digital Legal IDの共用可能性」は、顧客には、銀行や政府からサービスを受け始めようとする都度、自らの本人確認に必要な情報を提示する手間の省略を可能とする。また、それだけではなく、個人情報を繰り返し外で使うことに伴う「IDを盗まれるリスク」を減らすことにもつながる。

④ デジタルIDシステムに必須な要素は、a.対象者の本人性を確認し（a-1）、システムに登録し（a-2）、登録済であることを示す証明を出すこと（a-3）と、b.認証すること、の大きくとらえると2つ（aとb）だが、そのIDに「共用可能性」を付加するための第3の要素として、c.協働（federation）がある。このうちa-1とa-2は、デジタル／非対面でも書面／対面でも良い。a-3とbとcは、デジタルに処理される。ひとつのデジタルIDシステムについて、複数のサービス提供者が主体となることも可能である。a-1については、政府発行の公的な本人確認書類が使われる。

⑤ 信頼度の高いデジタルIDシステムを構築するためには官民それぞれが役割を分担することになる。米国においては、イノベーティブなID プロダクツやビジネスモデルの創出は「民」の役割である。他方、「官」（連邦および州の政府）は、本人の法的なIDを確認するために最低限必要な本人確認書類の情報について役割を持つ。

(2) 米国議会下院金融サービス委員会の「AIに関するタスクフォース」の議長と委員であるBill Foster議員とBarry Loudermilk議員は、11月13日、上の(1)に記した財務省報告書中のデジタルIDに関する部分を取り上げ、次の3点をMnuchin蔵相に対して要請するレターを公表した。

① 報告書公表後の進捗状況をアップデートすること

② 「デジタルIDに関するタスクフォース」を来年2020年3月1日までに立ち上げること

③ 同6月1日までに「行動計画（Action Plan）」を作成すること

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

4．わが国への示唆

最後に以上の情報の「わが国への示唆」について、簡単に述べることとしたい。要点は、次の3点だと考えられる。

(1)　国際競争力の維持

第2章に記したとおり、デジタルID Sytemについては、新興国において新技術が急速に広がる“leapfrogging”がみられる。米国においても、デジタルIDシステムに向けた取組みが進んでいることは、第3章に記したとおりである。わが国の産業界・金融界は、政府の方針等も踏まえつつ、国際競争力の維持に努める必要がある。

(2)　マイナンバーカードの普及に向けた努力

わが国の公的な本人確認書類で、デジタルIDについて最も効果的なツールはマイナンバーカードである。その普及に向けた努力について、民間からも知恵を出していきたい。

(3)　生体認証の活用

わが国のIT企業が有する生体認証技術は、インドにおける活用や、2020年東京オリンピックでの活用（予定）などの例をみると、十分に国際競争力をもつものだと言える。本人確認や取引時の認証等に積極的に利用することが期待される。

以　上

編集・発行

有限責任 あずさ監査法人
home.kpmg/jp/regtech
regtech@jp.kpmg.com

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点及びそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2019 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.