資料6

一般社団法人電子決済等代行事業者協会

API高度化Study Groupでの検討状況等について

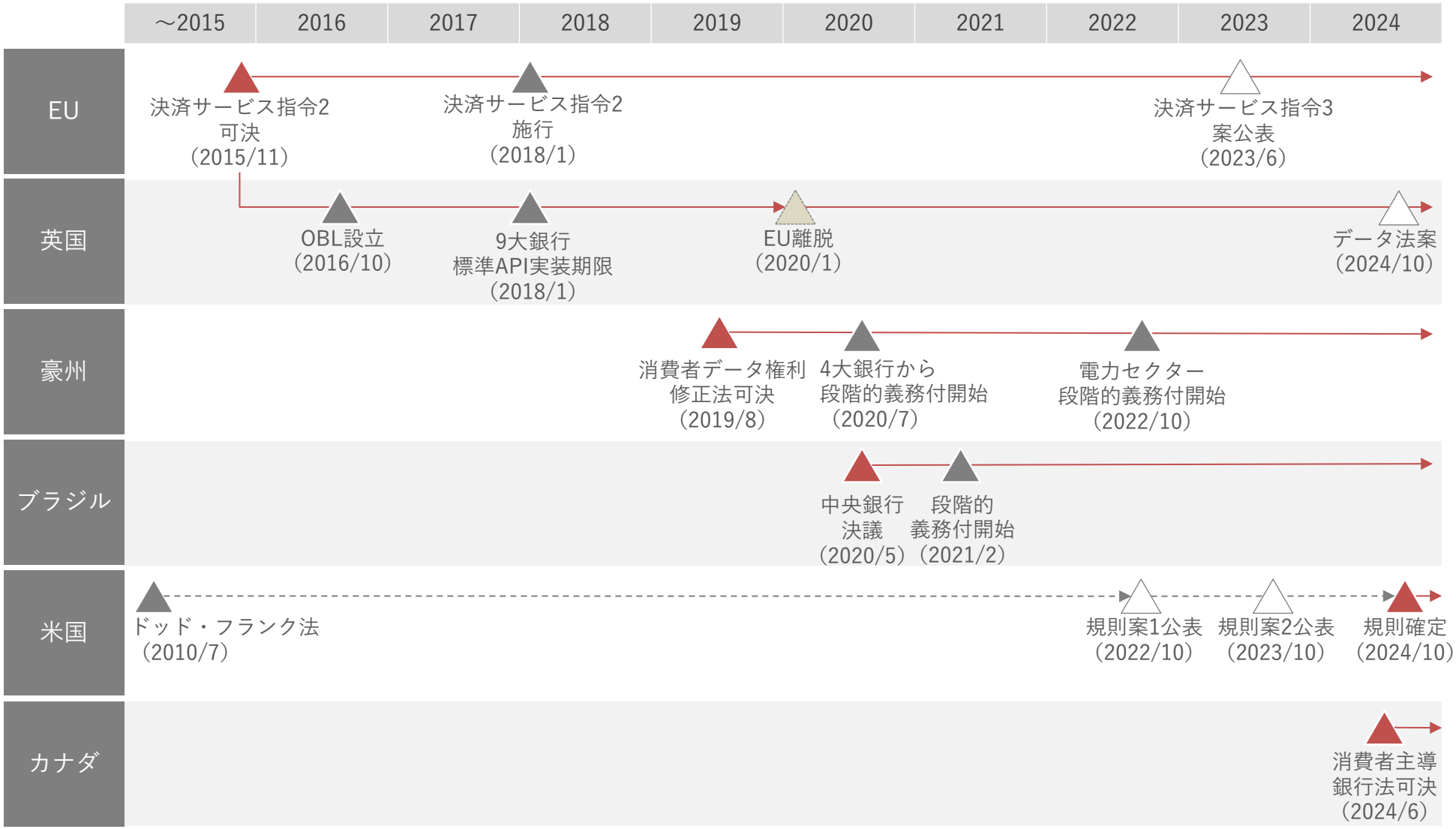
代表理事　瀧　俊雄

2025.1.30

APIアクセスを巡る海外動向

グローバルのオープンバンキングの歴史

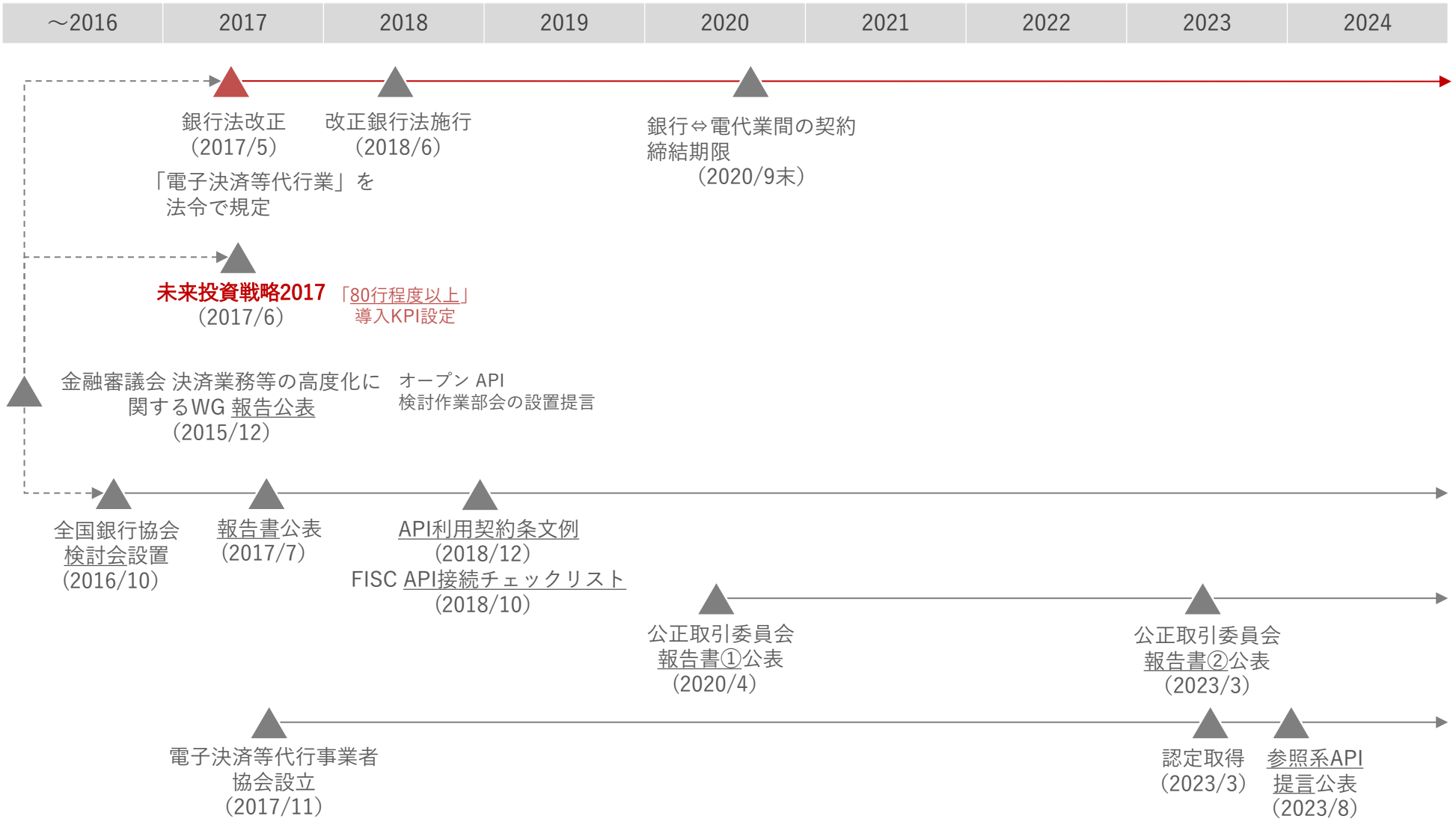
- 2015年の欧州での決済サービス指令2可決以降、各国で徐々に制度が導入されてきました



（出典）各種資料より当協会で作成

日本のオープンバンキングの歴史

- 未来投資戦略でのKPI設定も受け、法制上の義務化無しにAPI接続が実現しました



（出典）各種資料より当協会で作成

2023年頃から各国が政策の見直しを実施

- 欧州・英国・米国・カナダ等で相次いでオープンバンキング関連制度の見直し、新規法制の導入が行われています

欧州	○2022年5月10日 PSD2に関するレビュー及びオープンファイナンスに関するパブコメを開始 ●2023年6月28日　**欧州委員会がPSD3案（オープンファイナンス規則案含む）を公開** →2025年に議会通過、2026年央施行との記事あり	規制を改善 対象を拡大
英国	○2022年3月25日　合同規制監視委員会設立 （財務省、競争市場庁、金融行動監視機構、決済システム規制当局の4機関連名） ○2024年4月18日　政府（ビジネス・貿易省）が政策ペーパーとして「スマートデータロードマップ」を公開 ●2024年10月24日　政府（科学・イノベーション・技術省等）が「**データ（利用とアクセス）法案**」を議会に提出	
米国	○2010年のDodd-Frank法1033条によりOpen Bankingを義務付 CFPB （消費者金融保護局）が執行可能な規則類が整備されず、事実上「休眠状態（dormant）」 ●2024年10月22日　**CFPBが最終規則を公開**	規制を新設
カナダ	○2021年4月に助言委員会が最終報告書を提出 ●2024年6月20日「**消費者主導銀行法**」が成立 注）「予算実施法第1号」の枠内での成立。DIVISION16が該当部分。	

（出典）各種資料より当協会で作成

各国の制度導入状況（詳細）

- 自由競争に任せ切りにせず、一定程度**法的規制による関与を行う国が多数**となってきています
  - 基本的な決済データ（銀行、クレジットカード、電子マネー）については、①アクセスの義務付け＋②アクセス料金も無償化
  - アクセスの方式について　**③APIの設置を義務付ける**　とともに、**④APIのデータ形式、接続方式も標準化**

アクセス義務付対象

オープンバンキング	オープンファイナンス	スマートデータ/CDR※1
銀行データ	金融サービスデータ	電力、通信等データ

政策ポジション

※1 Consumer Data Right
「消費者データ権利」
豪州ではこの名称で制度化

※2 消費者金融保護局が規制を公表（2024年10月）
※3 「消費者主導銀行法」が成立（2024年6月）
※4 欧州委員会が決済サービス指令3（PSD3: Payment Service Directive 3）案を提示（2023年6月）
※5 「データ（利用とアクセス）法」案を英国議会で審議開始（2024年10月）

採用政策（詳細）

		日本	米国	カナダ	ブラジル	EU	英国	豪州
アクセス無償化		×	○	○（※6）	○	○（※7）	○	○
アクセス義務付対象情報								
	銀行口座	△（※8）	○	○	○	○	○	○
	クレジットカード	×	○	○	○	○	○	○
	電子マネー	×	○	○	○	○	○	○
	年金、保険等	×	×	○（※9）	○	○（※7）	△（※10）	×
	電力、通信等	△（※11）	×	×	×	×	△（※10）	○
API	API設置義務付	×	○	○	○	○（※7）	○	○
	API標準化	×	○	○	○	△（※12）	○	○

※6 「消費者主導銀行法」には規定が無く、助言委員会の報告書に「消費者承認下での対象データの「無料」共有」として記載
※7 年金・保険等へのアクセスでは①有償も認められ、②API設置も必ずしも義務ではない。
※8 アクセスは努力義務。都市銀行・地方銀行・第二地方銀行はほぼ全てAPIによるアクセスは可能となっている
※9 投資口座、住宅ローン、与信枠、貸付抵当権等
※10 審議中の法案ではアクセス義務付け対象は規則レベルで法案成立後に規定される想定
※11 電力は情報共有枠組が電気事業法の下で設定
※12 決済についてはAPI標準化を断念

（出典）各種資料より当協会で作成

（英国）API標準化等を行う独自機関

- 英国9大銀行の資金提供により標準化等を行う機構が設立されており、更新系を含めた英国のオープンバンキング施策の立役者と見なされています
- 本邦における同様の利活用推進機構の設立についても検討が必要だと考えられます

概要

【設立】2016年10月16日
【名称】Open Banking Limited（通称OBIE: Open Banking Implementation Entity）
【団体形態】保証有限責任会社（company limited by guarantee）
【運営資金提供】英国の9大銀行※1
【主な役割】API標準、セキュリティ標準の策定等（下図参照）
APIに関する統計情報の収集、公開
各種ガイドライン策定（UXガイドライン等）

※1 ロイヤルバンク・オブ・スコットランド、ロイズ銀行グループ、バークレイズ、HSBCグループ、Nationwide、サンタンデール、ダンスケ、アイルランド銀行、アライド・アイリッシュ銀行グループ

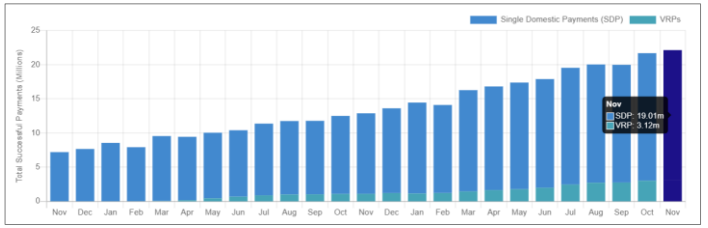
標準関連の役割

APIについては標準策定と併せて**準拠確認**（コンフォーマンステスト：接続が成功するかどうかの確認テスト）を実施

	標準策定	準拠確認
API標準	API標準の策定／バージョンアップ	API標準への準拠確認
セキュリティプロファイル標準	（FAPIを採用）	準拠確認は実施せず（OIDFの準拠確認を要請）

API統計情報の公表

可用性（％で表示）／成功したコール数／決済コール数／応答速度（ミリ秒で表示）／ユーザー数等



（出典）OBLサイトより。成功した**決済APIコール数**の月毎のグラフ

今後

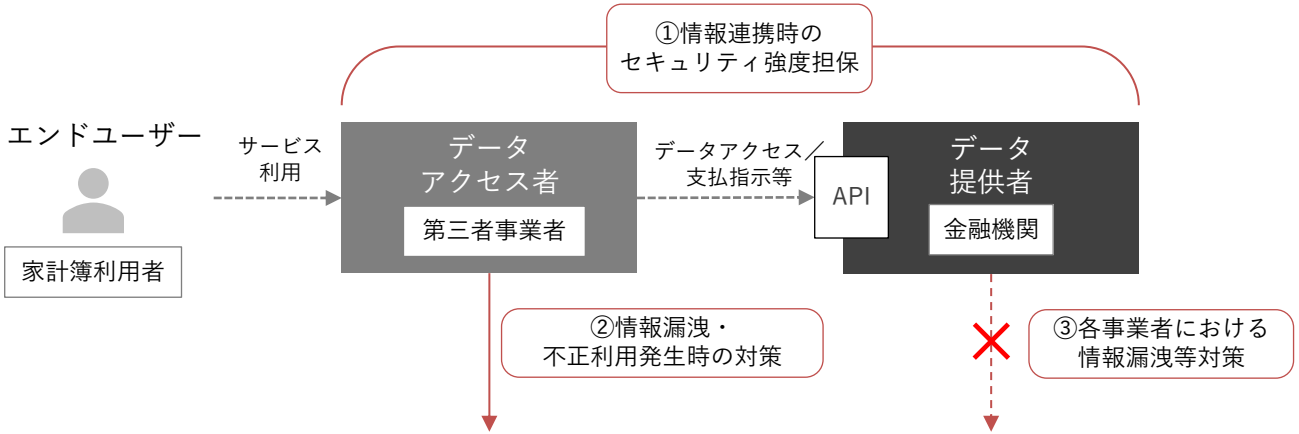
・現在のOBLとは別組織を立ち上げて、義務対象外の業務※2について実施予定
・上記別組織に、現在のOBLの業務をどこかのタイミングで移管予定
・新組織では「データ（利用及びアクセス）法案」に基づき対象となり得るオープンファイナンス関連等、**銀行以外のセクターに関するアクセス標準策定等を担当する可能性**
・運営資金については今後検討予定。データ提供者側だけでなく、第三者事業者側からも資金を募る案など、複数案が検討される見込み

※2 商業用のVRP（Variable Recurring Payment、日本の口振に相当）のユースケース検討等

（出典）各種資料より当協会で作成

APIアクセス時のセキュリティ対策

- オープンバンキング・ファイナンスにおけるAPIアクセス時のセキュリティ対策の概観は下記のとおりです



API等による情報連携時特有の対応	情報連携時のセキュリティ強度担保	①セキュリティプロファイル（Open ID Connect/FAPI等）への準拠確認
	情報漏洩・不正利用発生時の対策	②データアクセス者とデータ提供者間の契約等による責任分界点の明確化 ③法令による保険加入義務付
一般的な事業規制における対応	各事業者における情報漏洩対策	④事業者規制の中での対策義務付け ⑤Pマーク、ISMS取得（自主的対応等） ⑥業界団体による自主規制

（出典）各種資料より当協会で作成

標準・セキュリティ制度周りの課題

- 各国ではAPI標準、セキュリティプロファイルの策定団体及びそれらの準拠確認（認定）の業務を分担して実施しています
  - 日本では全国銀行協会様が電文仕様標準を策定（「銀行分野のオープンAPIに係る電文仕様標準について」）
  - セキュリティプロファイルについてはFAPI準拠を推奨（「オープンAPIのあり方に関する検討会報告書」）
  - 準拠確認（認定）については実施団体無し

※1　API認可のためのフレームワーク（OAuth2.0）を特定の条件下（例えば金融機関での活用など）で利用可能とするための設定値の一覧（仕様）

	項目	米国	英国	EU	日本
API	API標準策定団体	FDX	OBL	Berlinグループ等（複数）	全国銀行協会様
	API標準の粒度	細かい	細かい	中程度	中程度
	API標準への準拠確認（認定）	FDXが実施想定	OBLが実施中	ー	ー
セキュリティプロファイル	採用セキュリティプロファイル	FAPI（OIDF策定）	OBL独自セキュリティプロファイル※2 →FAPI（2018年8月より）	ー	FAPI（推奨レベル）
	セキュリティプロファイルへの準拠確認（認定）	FDXが実施想定	OBLが実施 →OIDFが実施 （2018年8月より）	ー	ー
UX	UXガイドライン	有り	有り	ー	ー

要検討？

実施団体無し

実施団体無し

※2 実質的にはOIDFと協力して策定

（出典）各種資料より当協会で作成

（英国）不正利用に関連する情報の共有

- 第三者事業者から金融機関に対してリスク情報を共有するための情報フィールドをOBLで標準化しています

※Payment Initiation Service Provider
（決済開始サービス提供者）

- OBLの標準APIバージョン3.1.10（2022年4月4日公開）から導入
- 採用は強制ではない
- 資金移動を行う金融機関（上図例で銀行A）は、共有された情報の内容に応じて資金移動を中止

【標準化項目（例）】

項目	情報内容（例）	規定元
受取人の口座のタイプ	個人、法人、政府等	OB_Internal_CodeSet
支払目的	送金、請求対応、払戻等	OB_External_CodeSet
第三者事業者(PISP)⇔受取人間の契約関係の有無	有／無	Data Model
マーチャント分類コード	7801（オンラインギャンブル）、7995（賭博）、5963（訪問販売）等	ISO18245
支払のコンテキスト	物品・サービス代金の支払（事前・事後）、店頭支払、第三者への送金、自身への送金	OB_Internal_CodeSet
支払目的コード	ECサイト支払、光熱通信費等支払、家賃支払、ギャンブル等	英国中央銀行発行コードリスト
（物品等の）配送先住所	国名、郵便番号、町名、番地、建物名等	Data Model

（出典）OBL「Payment Initiation API Profile v4.0 - Data Model – ORissk1」等より当協会で作成

（英国、EU）再認証の省略

●参照系では「金融機関によるユーザーの再認証」の省略が可能であり、ユーザーの離脱防止やUXの向上に繋がっています

- 一定期間毎に金融機関側の画面に移動し、金融機関側でのユーザ再認証が必要
- 期間は金融機関により、1日～10年と大きな幅がある
- 頻繁な再認証はユーザーの離脱に繋がりやすい

- 初回接続時のみ金融機関側でユーザーを認証
- 以降は一定期間毎に第三者事業者が接続継続意向をユーザに確認
- 金融機関での再認証は、不正アクセスなどの疑義が無い限りは不要

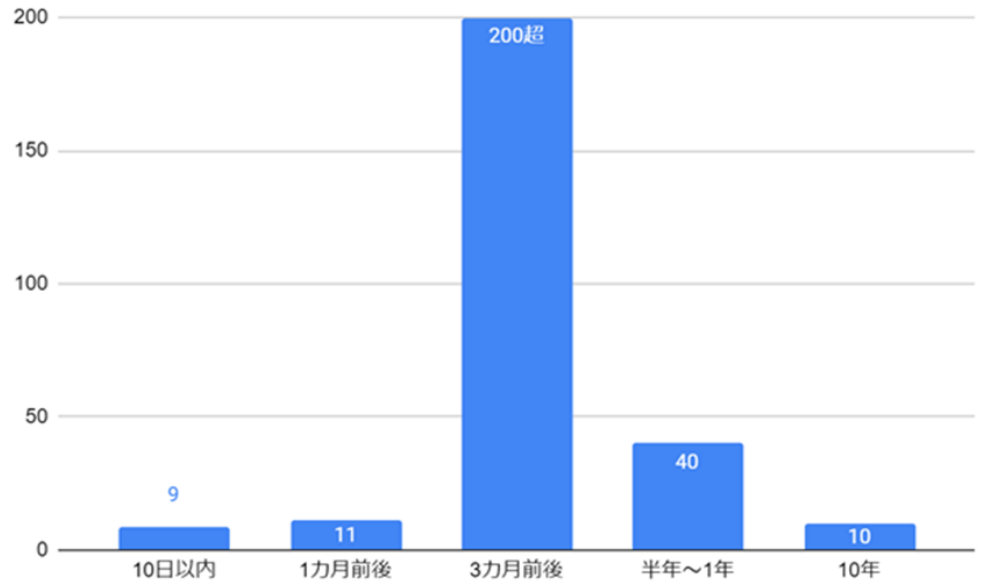
（出典）英国金融行為規制機構のPolicy Statement（PS21/19）等より当協会で作成

（参考）リフレッシュトークン有効期限の延長の課題

●2023年8月に当協会から公表した「参照系APIの技術的改善に関する提言」では、リフレッシュトークンの有効期間の差異を課題として挙げています

現状と課題

- 参照系APIにはリフレッシュトークンの有効期間が設定されており、期限が切れると、ユーザーによる再認証が必要となる
- 事務局調べによると、下表のとおり有効期間は**10日以内～10年と、金融機関によって様々**

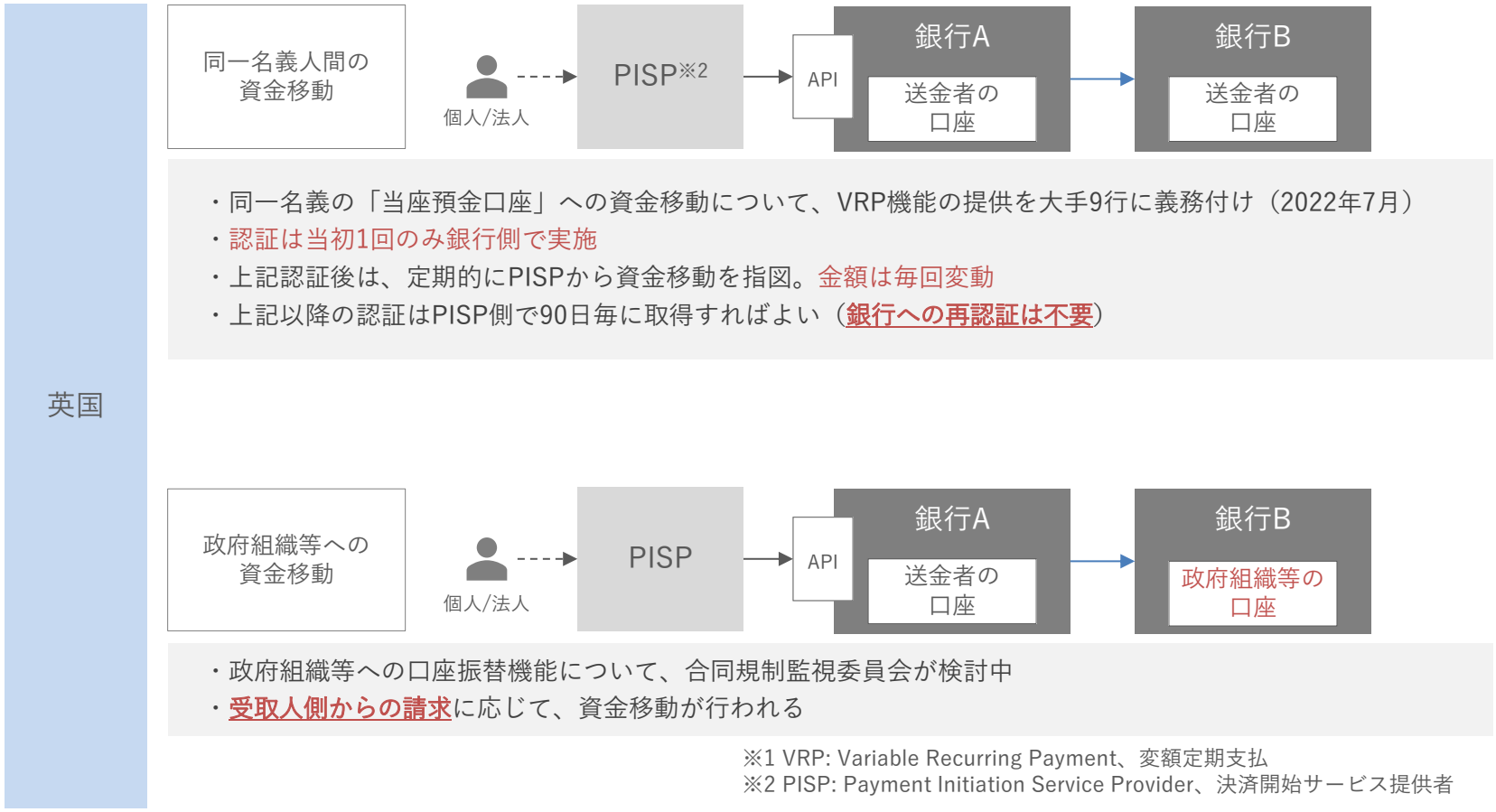


リフレッシュトークンの有効期間毎の銀行口座数（事務局調べ）

2023年12月13日「金融機関におけるAPI接続チェックリストに関する連絡会」にてご紹介

（英国）「口座振替」機能のAPIによる実現

●英国、EUでは更新系APIのビジネスユースケースとして、口座振替機能（変額定期支払：VRP※1）に注目しています。



※1 VRP: Variable Recurring Payment、変額定期支払
※2 PISP: Payment Initiation Service Provider、決済開始サービス提供者

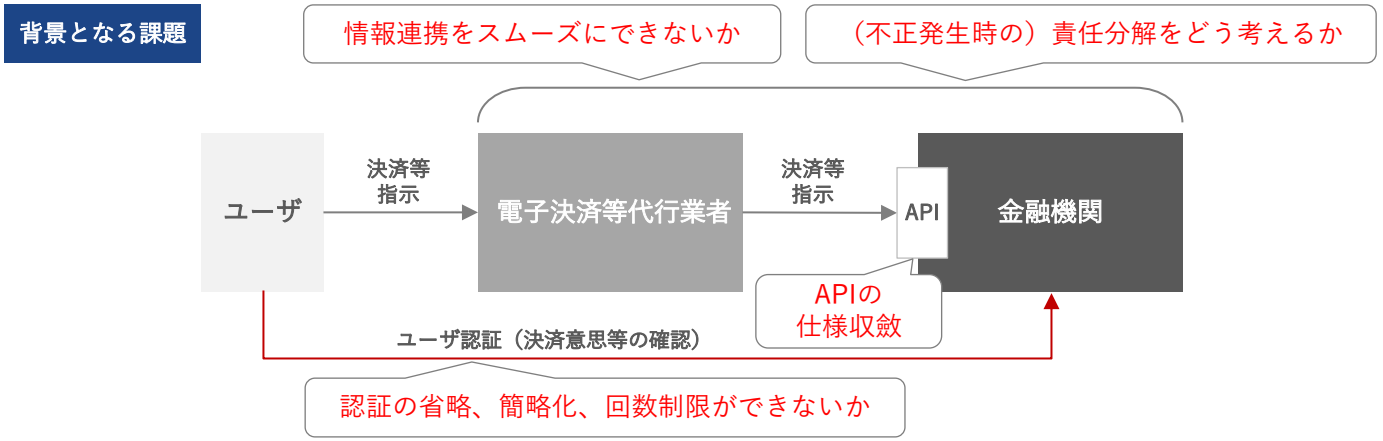
（出典）https://assets.publishing.service.gov.uk/media/610029a8d3bf7f044ee52336/Letter_to_the_Open_Banking_Implementation_Entity.pdf
Developments in Open Banking: Variable Recurring Payments and Sweeping - Bird & Bird (twobirds.com) 等より当協会で作成

API高度化に向けたStudy Group

API高度化に向けたStudy Group

● 当協会に標記Study Groupを設置し、下記の課題を検討中

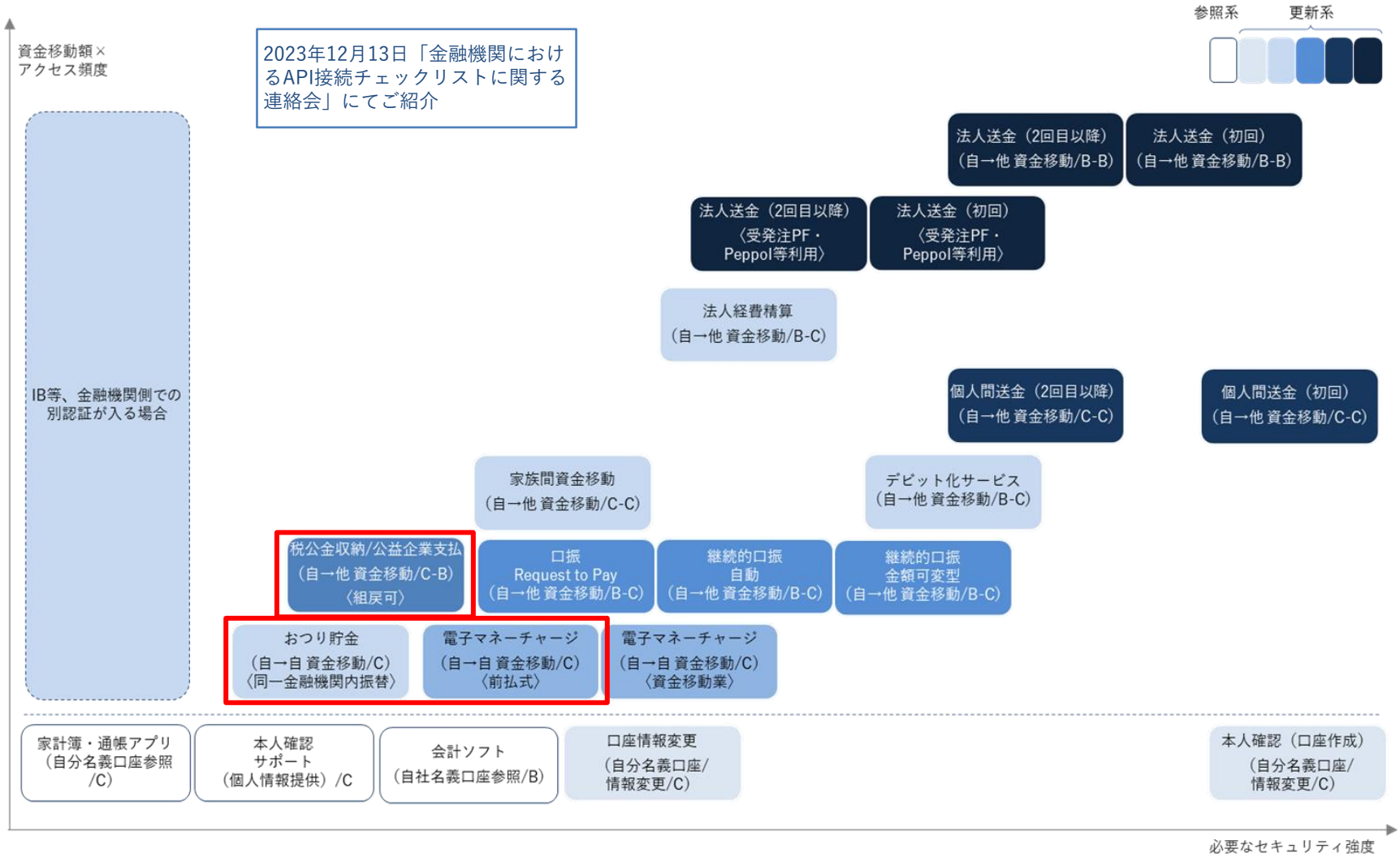
項目	内容	備考
1．認証方式の課題整理と解決方策の方向性検討	①同一人名義間、公益企業向けの振込などについて認証方式の簡素化が可能かどうかの法令面、技術面からの検討	可能であれば電子決済等代行業者サービス内での認証で完結
	②金融機関における認証方法の調査と整理	
	③海外における認証簡素化の事例を整理	①②に並行して実施
	④ UX向上に向けて、金融機関⇔電子決済等代行業間で連携すべきデータや、採用可能な認証方式についての検討【2．とも関連】	①が困難なユースケースにおいて検討
2．各国のAPI仕様の概要調査と仕様収斂に向けた課題の整理	①各国のAPI仕様の概要調査と日本のAPI仕様との比較	米国FDX、英国OBIE、欧州Berlin Group仕様　等
	②仕様収斂に向けた国内における課題の整理、分析	



（出典）当協会で作成

1-① 認証方式の簡素化の検討

●海外の事例にも倣い、同一名義人口座間、税公金等収納について認証の簡素化を検討



（出典）当協会で作成

1-② 金融機関における認証方式の調査と整理

（資料6 別紙参照）

1-③ 海外における認証簡素化の事例の整理

●EUでは決済実施時の認証要素として、下記のうち2つ以上が必須（一般的な二要素認証）。ただし、下記ユースケース時には必ずしも適用しなくてもよい

■知識（利用者だけが知っているもの）　：PWD、PIN等
■所有（利用者だけが所有しているもの）：電話番号、HDWトークン等
■内在（利用者に存在しているもの）　：指紋、顔認識等

PSR: Payment Service Regulation、現在提出中のPSD3関連法案
RTS: Regulatory Technical Standard、欧州銀行監督局が定めるハイレベル標準

条項	内容	備考
PSR案85条2.	受取人のみが開始する決済	Debit等
RTS第11条	店頭での非接触決済	50ユーロ未満等の条件付
RTS第12条	交通運賃支払、パーキングメーター支払	
RTS第13条2.	信頼できる受取人リストへの支払	リスト改訂にはユーザー認証が必要
RTS14条2.	同一の受取人への二回目以降の定期的な支払	
RTS15条	同一の決済口座サービス提供者内にある同一の自然人又は法人間の送金	いわゆる同行内振替
RTS第16条	低額取引	30ユーロ未満等の条件付
RTS第17条	専用の決済プロセス又はプロトコルによる企業決済	当局による事前の了承要（Peppol利用時等に相当すると考えられる）
RTS18条	取引監視により一定の不正率以下と見なされる場合	不正率の計算方法等は詳細に規定。監視方法等には監査が求められる
（参考）参照系		
PSR案86条3.	口座情報サービス提供者による決済口座への2回目以降のアクセス	
RTS第10条a 1.	決済口座の残高参照、90日以内の過去の決済取引の情報参照	

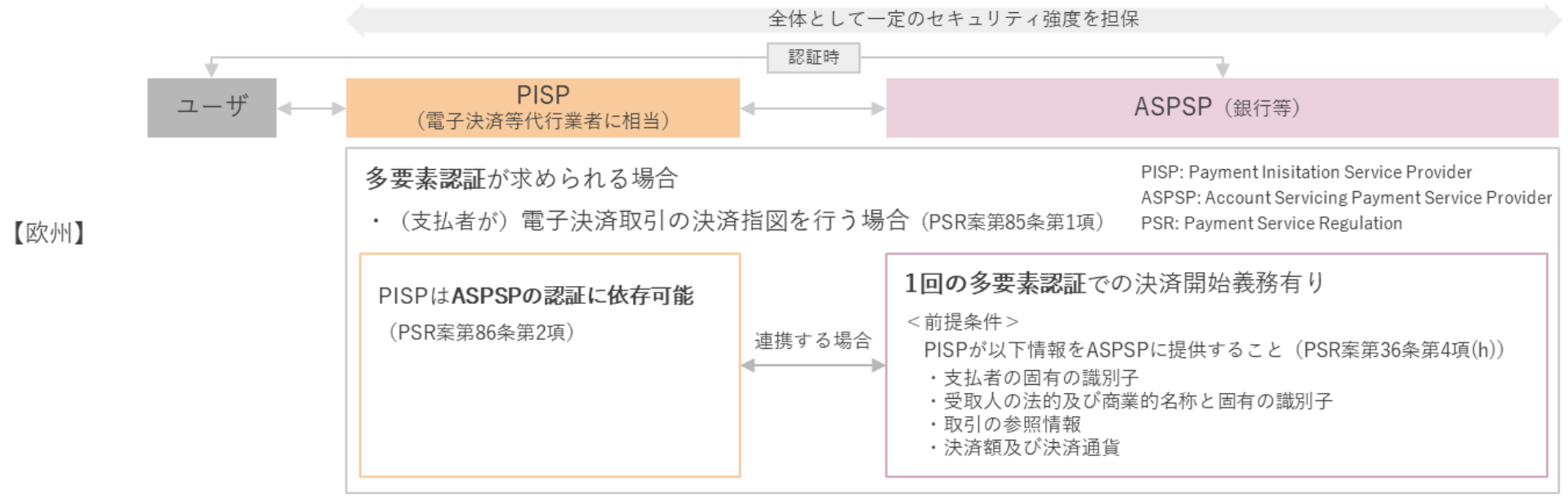
2023年12月13日「金融機関におけるAPI接続チェックリストに関する連絡会」にてご紹介

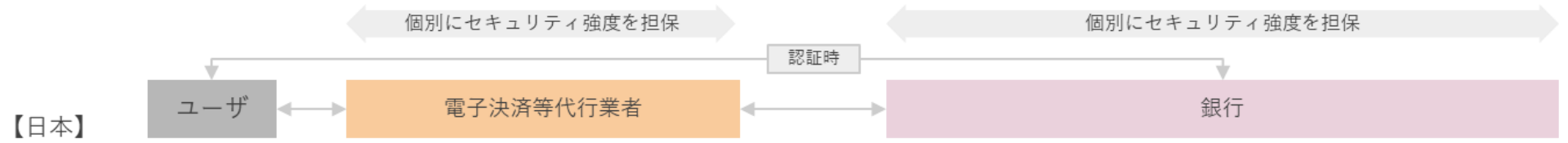
（出典）EU公開情報より当協会で作成

（参考）欧州と日本の決済時認証に関する原則の違い

●欧州では一連の決済体験全体を通して一定程度のセキュリティ強度を担保し、UXとセキュリティ対策を両立する考え方を採用している

2023年12月13日「金融機関におけるAPI接続チェックリストに関する連絡会」にてご紹介



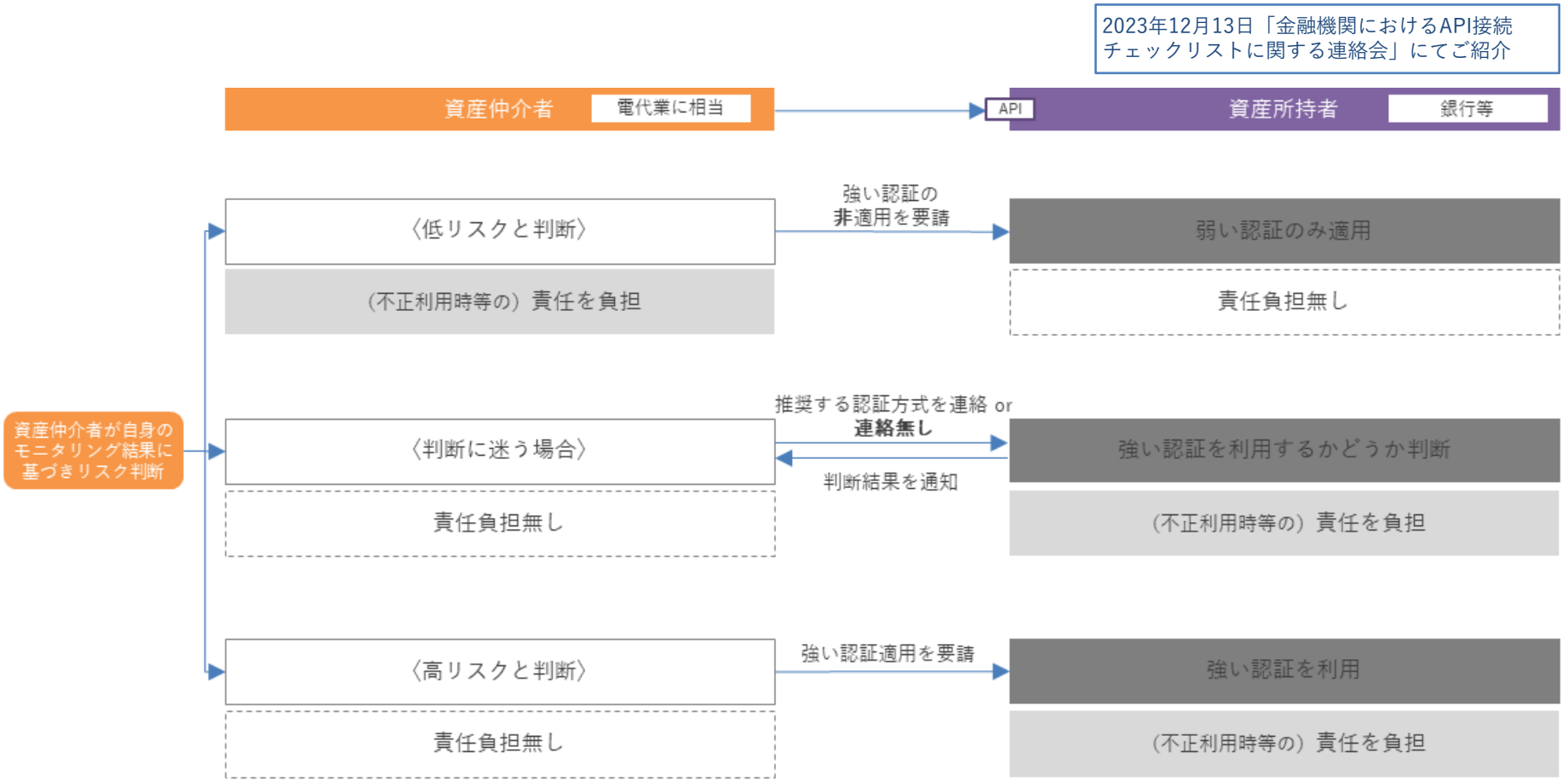


・**いずれの認証方式とも**、口座保有銀行において採用されている・・指図の認証方式と**同水準以上の強度**とすることが原則
・**API接続先**（電代業者）、**銀行の双方**において**同水準以上の強度**の認証方式を採用することが原則
（全国銀行協会「オープンAPIのあり方に関する検討会報告書」）

（出典）電子決済等代行事業者協会にて作成

（参考）欧州のTPP⇔銀行間の責任分解の考え方

- 欧州の自主規制団体では、TPP（下図の「資産仲介者」）側の認証に依拠する場合には、TPP側に責任が移動する形の柔軟な考え方も提示されている



※ SPAA（SEPA Payment Account Access）スキーム：EPCが定める決済口座アクセスに関するルール、標準、ガイドライン等の総体

※ EPC（European Payments Council）：欧州の主要な銀行等が参加する自主規制組織

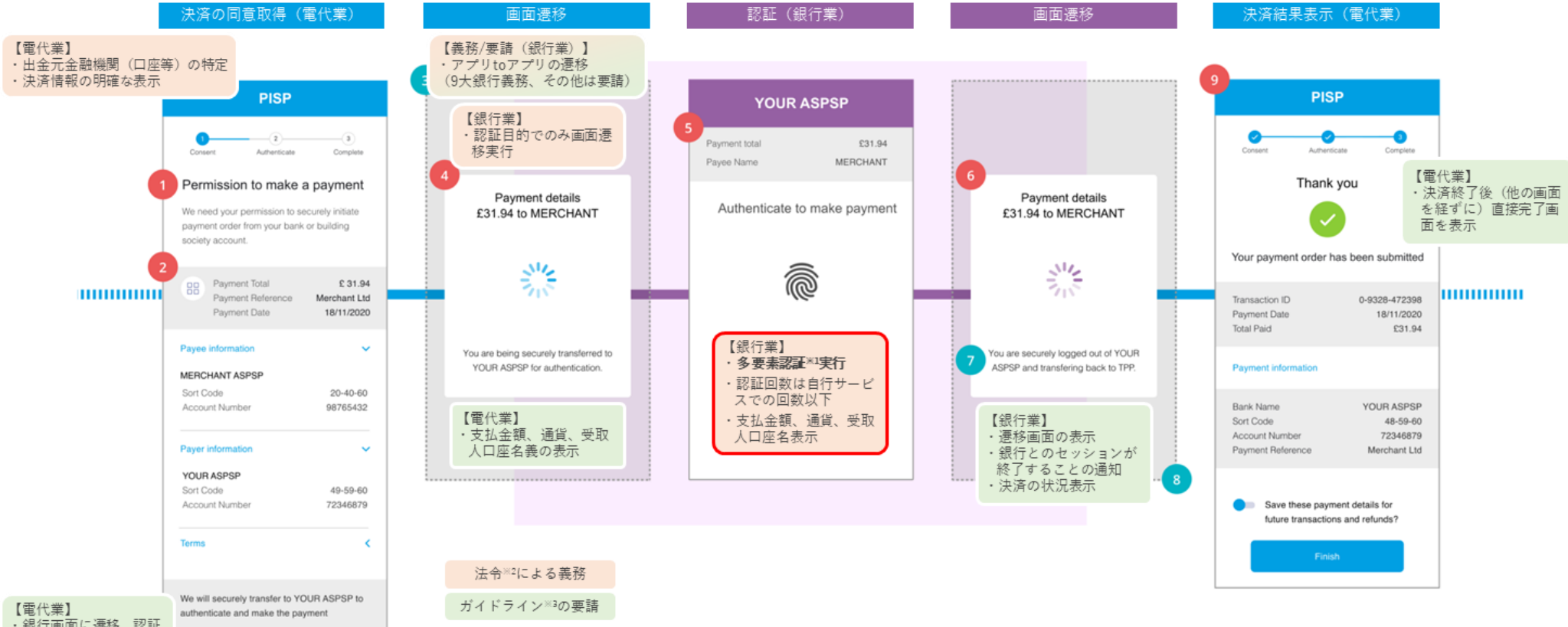
（出典） EPCサイト https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-payment-account-access-spaa-scheme-rulebook-v11 より当協会作成

1-④金融機関⇔電子決済等代行業間で連携すべきデータ　20

- 英国のOBLではガイドラインにより、TPP（下記青の画面）と銀行（下記紫の画面）で画面遷移時に引き継ぐべきデータを定め、UX向上を目指している

2023年12月13日「金融機関におけるAPI接続チェックリストに関する連絡会」にてご紹介

国内送金（一回のみ決済）のユースケース



※1 法令による義務付けである強力な顧客認証（SCA: Strong Customer Authentication、いわゆる多要素認証）
※2 英国「決済サービス規則（PSR: Payment Service Regulation）」、「規制技術標準（RTS: Regulatory Technical Standard）」等
※3 OBL「顧客体験ガイドライン」

（出典）OBL公開情報より当協会で作成

2-①各国のAPI仕様の概要調査

● （調査中）

要精査

項目	FDX（米）	OBL（英）	Berlin Group（EU）
団体の性格	・民間団体 ・政府から標準化団体として認定された	・民間団体 ・政府主導で標準化団体として設立された	・民間団体 ・政府からの認定等は無し
備考	・米国を中心にAPAC地域への拡大を企図 **・日本版作成の動きあり**	・CMA9銀行を中心に適用	・EU圏内のAPI接続の80％程度に適用
プロトコル・標準			
インターフェース	REST	REST	REST
メッセージフォーマット	JSON	JSON	JSON、XML
メッセージデータ要素		ISO20022	ISO20022
TPPの同定方式	（おそらくFDXによる登録・認証）	eIDASに類似したOBLの認証方式	eIDAS
通信暗号化	Mutual TLS（1.2以降？）	Mutual TLS 1.2	Mutual TLS 1.2
メッセージ署名	JSON web signature	JSON web signature	HTTP message signature
APIセキュリティ	FAPI	FAPI	OAuth 2.0（Optional）
APIの機能			
決済開始 Payment Initiation　手順	1. Initiate / 2. Disclose / 3. Select Data Provider / 4. Authenticate / 5. Consent / 6. Authorize / 7. Confirm	1. 事前設定　2. 認証　3. 実行	1. 事前設定　2. 認証
対象 Resources	・Bill Pay API (money movement and bill payment) ・One-time transfer / recurring payment ・Scheduling	・即時／予約／定期／一括 送金 ・国内／海外 送金	・即時／予約／定期／一括 送金 ・国内／海外 送金
口座情報取得 Account Information 手順	1. Initiate / 2. Disclose / 3. Select Data Provider / 4. Authenticate / 5. Consent / 6. Authorize / 7. Confirm	1. 事前設定　2. 認証　3. 実行	1. 事前設定　2. 認証　3. 実行
対象 Resources	Account Information / Account Statements / Account Transactions / Money Movement / Personal Information / Reward Program Categories / Reward Program Information	・口座、残高、入出金、デビット、予約決済	・口座情報、残高、入出金
（送金前の）残高チェック Confirmation of funds	1.実行（決済開始手順の中で実行）	1. 事前設定　2. 認証　3. 実行	1.実行（ユーザー同意はAPIのスコープ外）
ユーザー認証			
ユーザー認証時の挙動 SCA Integration	・銀行画面/Appに遷移 Redirect	・銀行画面に遷移 Rediret ・専用銀行アプリ利用 Decoupled	・銀行画面に遷移 Rediret ・専用銀行アプリ利用 Decoupled ・埋込型 Embedded
基本の認証方式	・二要素認証 SCA: Strong Customer Authentication ・may require a step-up authentication when scheduling a payment or transfer	・二要素認証 SCA: Srtong Customer Authentication	・二要素認証 SCA: Srtong Customer Authentication
その他			
イベント通知（Webhook？）	・サポート（Optional？）	・サポート（Optional）	・サポート無し

（出典）公開情報等より当協会で作成

今後に向けて

今後に向けて

- デジタル行財政改革会議「データ利活用制度・システム検討会」において、データ利活用に係る制度及びシステムの整備について包括的に検討が行われる予定であり、「金融」分野も対象として検討予定とうかがっております
- オープンバンキング・ファイナンスに関しては海外でも大きく制度が動いており、また当協会での検討をつうじて幾つかの課題も明確化されてきています
- 上記政府による検討などにも鑑みつつ、金融データの利活用の更なる促進に向けて、API接続チェックリストについて更改等の検討ができないかと考えます
- 具体的にはユースケースや利用状況に応じたリスクベースでの考え方を前提として、セキュリティの強度を設定していく方向性を念頭に置いています。より具体的には下記表のとおりです

通番	内容	更改等の方向性（案）
32	利用者を保護する認証機能を整備する。	・リスクが相当程度低いと考えられるユースケースについては、2段階認証を必ずしも必須としないことも許容する
41	認証の悪用リスクを可能な限り低減させる。	・トークンの有効期限設定に関して、参照系が対象ユースケースである場合には、望ましい有効期限の最低期間を例示として提示する 例）10年〈休眠預金等活用法により民間公益活動に活用可能となる休眠期間を参考〉 ・よりリスクが低いと考えられる場合には、不正アクセスなどの疑義が生じない限り、トークンの有効期限を設定しないことも許容する
42	API 接続先を含めた全体の認証強度をもって、利用者保護を図る。	・リスクベースの考え方を基軸としつつ、電子決済等代行業者が金融機関の認証に依存できるケースや、逆に電子決済等代行業者のみで認証を完結可能なケースなどを例示する

- なお、チェックリスト自体の更改は難しい場合も想定されますので、チェックリストとは別の資料にて上記許容されるケースの例示を行うなど、対外的な公表等の方法やクレジットについても、柔軟に対応させていただきたいと考えます