資料6

一般社団法人電子決済等代行事業者協会

API利活用高度化に向けて

代表理事　瀧　俊雄

2025.12.4

本日の内容

内容	スライド
1. 前回連絡会の振り返り	P2 – P3
2. 今回のご提案事項	P4 - P12
3. 委員の皆様へのヒアリング	P13 - P18
4. その他共有したい事項	P19 – P20

1. 前回連絡会の振り返り

今後に向けて

2025年1月30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」における当協会資料より

- 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

2. 今回のご提案事項

リスク関連の検討会設立について

●次スライド以降のリスクの許容度関連課題（１．）について、**下記検討会を設立した上で、ガイドライン発出等を目的として活動することをご検討いただけないでしょうか**

名称（案）	決済・金融データ流通に関する適正なリスク許容度の検討会
目的	第三者事業者（電子決済等代行業者等）が関与する、決済及び金融データ流通に関連するリスクの許容度について、安全性とユーザー体験の両立を意識した適正な条件設定の検討の実施
具体的検討項目（案）	（次スライド以降参照）

項目	スライド	スライドタイトル
多要素認証を不要とすることが可能なユースケースの検討	P6-P7	2段階認証を必須としないケースについて
リフレッシュトークンの適切な更新頻度	P8	認証トークンの更新頻度について（参照系）
電子決済等代行業者が金融機関の認証に依存可能なユースケースや、電子決済等代行業者のみで認証を完結可能なユースケースの検討	P9-P12	電代業者と銀行間の責任分界の考え方について

構成員（案）	公益財団法人　金融情報システムセンター 一般社団法人　全国銀行協会 一般社団法人　電子決済等代行事業者協会 （名称五十音順） ※ 各法人より数名程度の構成員をアサインいただき、検討実施を想定 ※ 上記以外にも必要に応じて参画法人を検討
成果物（案）	可能であれば上記検討実施後に、ガイドライン等を取り纏め公表

2段階認証を必須としないケースについて

- EUの事例を参考に、**2段階認証（多要素認証）を必ずしも必須としないケースを、例示的にガイドライン等に提示**
  - 「必ずしも必須としない」前提であり、多要素認証不要をデフォルトとする前提ではないことに留意
  - APIが整備済みの銀行へのアクセスを前提。API未整備の他の金融等業への拡大適用は企図しない
  - 後段で述べる「電代業と金融機関の責任分界」の切り分けと併せての検討が必要

考えられる例

区分	内容	要検討事項	検討優先度（電代業視点）
更新系	店頭での非接触決済	上限金額制限の必要性（EUで50ユーロ≒約1万円程度？）	
	交通運賃支払		
	信頼できる受取人リストへの支払		
	同一の受取人への二回目以降の定期的な支払		
	同一の銀行内にある同一自然人又は法人間の送金（同行内での本人口座間振替）		○
	低額の取引	上限金額制限の必要性（EUで30ユーロ≒約5千円程度？）	
	専用の決済プロセス又はプロトコルによる企業決済	**事前にオーソライズを与える枠組の必要性（当局承認等？） 具体的事例：Peppol利用での請求・支払プロセス等**	○
	取引監視により一定の不正率以下と見なされる場合	不正率の計算方法の検討	
参照系	**電子決済等代行業者による口座情報への2回目以降のアクセス**	**後段のリフレッシュトークン有効期間の議論と併せての検討**	○

（出典）当協会で作成

（参考）EU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

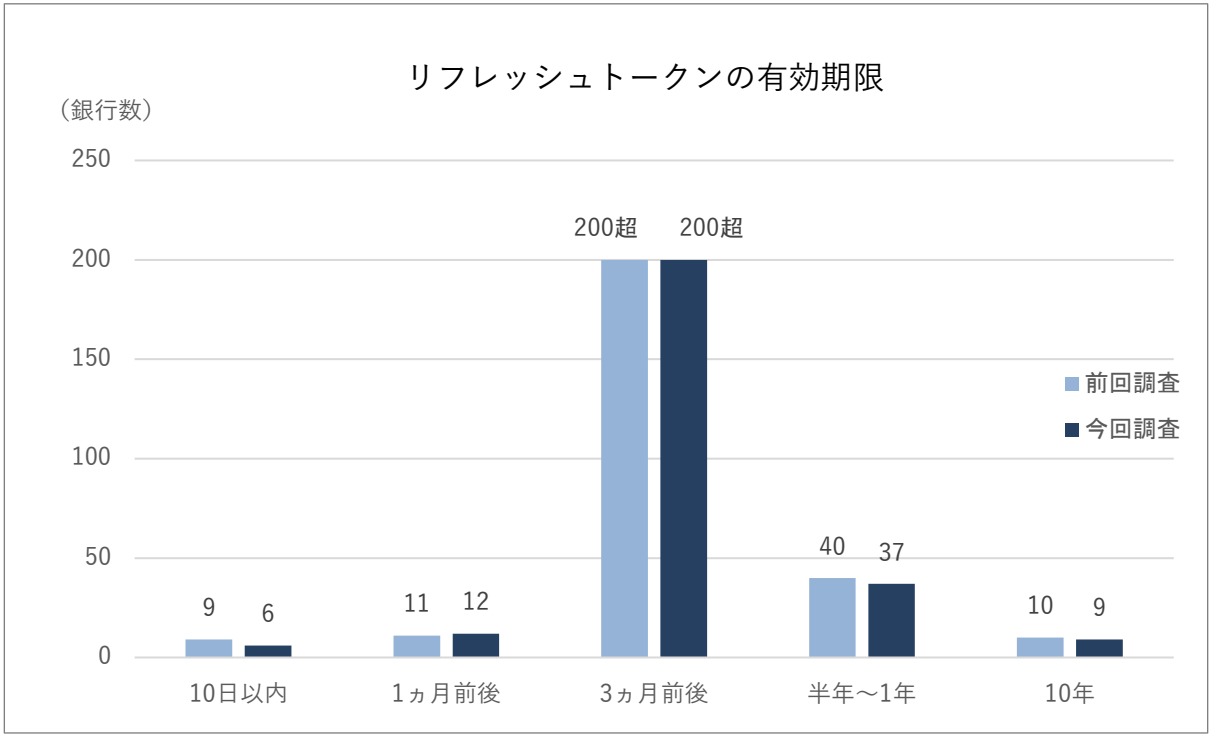
条項	内容	備考
PSR案85条2.	受取人のみが開始する決済	Debit等
RTS第11条	店頭での非接触決済	50ユーロ未満等の条件付
RTS第12条	交通運賃支払、パーキングメーター支払	
RTS第13条2.	信頼できる受取人リストへの支払	リスト改訂にはユーザー認証が必要
RTS14条2.	同一の受取人への二回目以降の定期的な支払	
RTS15条	同一の決済口座サービス提供者内にある同一の自然人又は法人間の送金	いわゆる同行内振替
RTS第16条	低額取引	30ユーロ未満等の条件付
RTS第17条	専用の決済プロセス又はプロトコルによる企業決済	当局による事前の了承要（Peppol利用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

認証トークンの更新頻度について（参照系）

- 「参照系APIの技術的改善に関する提言」で当協会が課題として提示したリフレッシュトークンの有効期間の差異について再調査結果を公開。依然として差異が残存
- 有効期間が短すぎるリフレッシュトークンの場合、銀行画面での頻繁な再認証（場合によりID/PWD入力）が必要となり、却ってフィッシングなどへの耐性が劣化
- 多くの銀行が3か月前後の有効期限を設定していることに鑑み、リフレッシュトークンの有効期限の**望ましい最低期間を3か月（仮）として、ガイドライン等に提示**

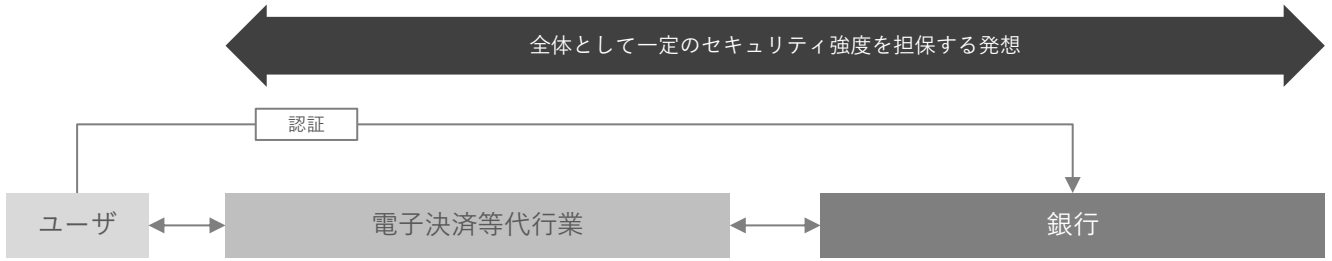


（出典）当協会「金融機関が提供する API に関する統計データの公表について（2025年7月30日付）」より

電代業者と銀行間の責任分界の考え方について

● 電子決済等代行業者と銀行との間で、認証主体＝責任主体とする原則に基づき、UX向上に向けた**ガイドライン等に考え方を提示**

原則のイメージ



- 重要な操作の認証を銀行側で実施
- 操作結果に対する対顧客責任は銀行側

- 重要な操作の認証を電代業側で実施
- 操作結果に対する対顧客責任は電代業側

重要な操作の例

■ 送金、振込、出金等のユーザー資産価値の変動を引き起こす操作
■ 上記の操作上限設定の変更
■ 金融機関に登録されている住所、メールアドレス、電話番号等の身元確認や当人認証に関係する変更

（なお、以下は重要な操作例とは見なさないこととする）
■ 送金、振込、出金等の予約のみを行う操作
　■ 上記のユーザー資産価値の変動を直接は引き起こさないもの。
　ただし、当該予約操作実施以降、別途の操作を要することなく上記ユーザー資産価値の変動が自動的に生じる場合は除く

（参考）当協会からの発出文書

● フィッシング耐性強化に向け、当協会から会員に対して周知文書を発出。電代業者側の認証のみで重要操作が行われる場合には、パスキー等の採用検討を推奨

＜更新系業務の場合＞

- ①ユーザー資産の移動等の**重要な操作**について、金融機関側の認証により実施される場合には、会員側の対策不備によるユーザー資産の棄損等に繋がる可能性は低いと考えられるため、各会員において金融機関との役割分担や、更新系の指図が可能なサービスの内容を踏まえて、受容できるリスクであるか各会員において判断を行っていただきたい。
  - ◆ **一般的に想定される重要な操作例**
    - ■ 送金、振込、出金等のユーザー資産価値の変動を引き起こす操作
    - ■ 上記の操作上限設定の変更
    - ■ 金融機関に登録されている住所、メールアドレス、電話番号等の身元確認や当人認証に関係する変更

  なお、以下は重要な操作例とは見なさないこととする
    - ■ 送金、振込、出金等の予約のみを行う操作（上記のユーザー資産価値の変動を直接は引き起こさないもの。ただし、当該予約操作実施以降、別途の操作を要することなく上記ユーザー資産価値の変動が自動的に生じる場合は除く）
- ②更新系業務について**電代業者側の認証のみにより上記の重要な操作が行われる場合**には、当該認証について**フィッシング耐性のある認証方式（パスキー等）の採用を検討していただきたい**

上記いずれの場合でも、サービス連携時及びリフレッシュトークンの有効期間経過後の再連携時には攻撃に対して脆弱性があることには留意をしていただきたい。

（参考）各操作時における認証主体

	ログイン	サービス連携	重要操作 （送金、住所変更等）	（リフレッシュトークン有効期間切れ後の） 再連携
参照系業務	電代業者	銀行	—※1	銀行
更新系業務	電代業者	銀行	銀行	銀行
	電代業者	銀行※2	電代業者	銀行

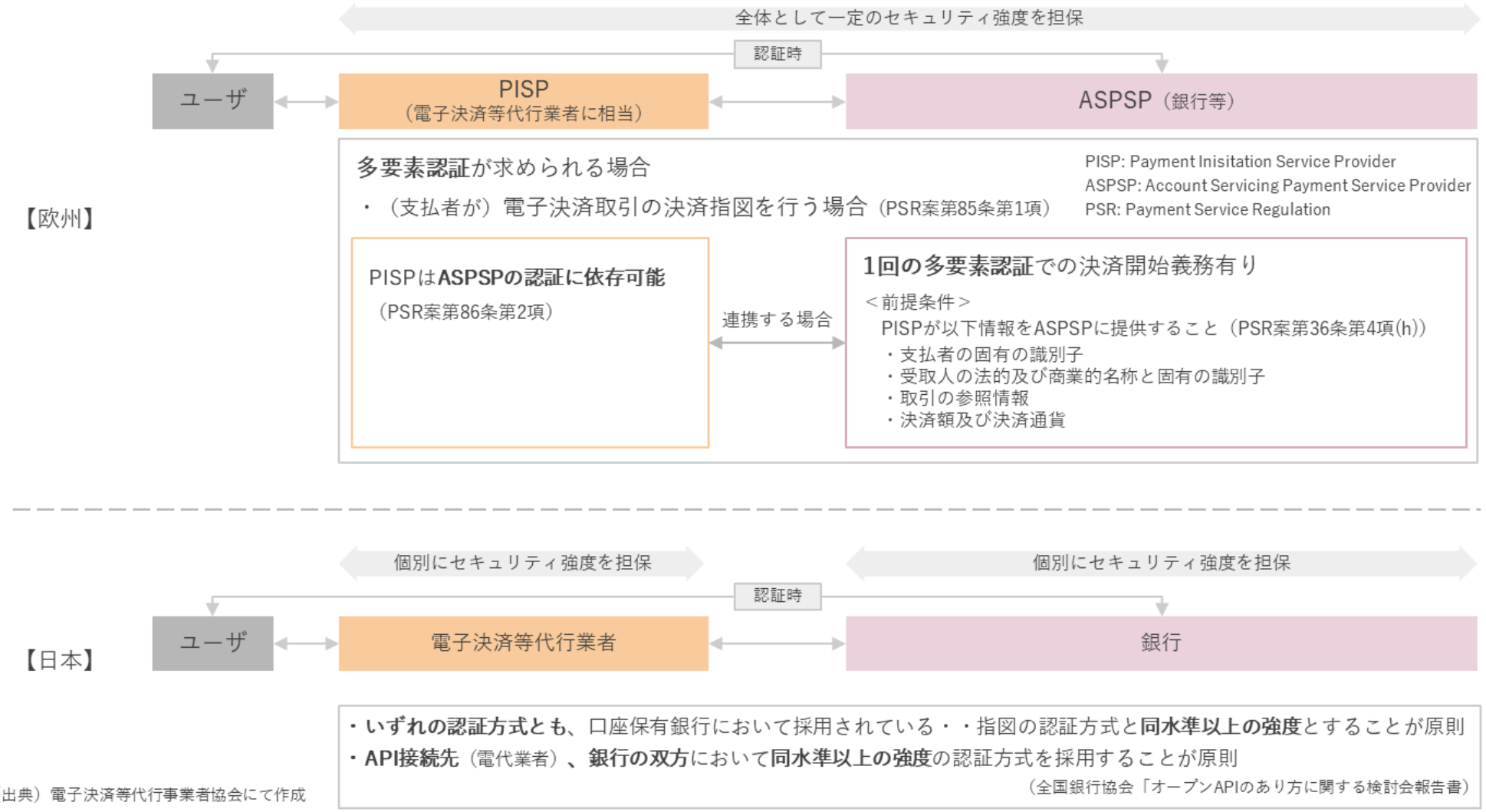
※1 重要操作は更新系を伴うため、一般的には想定されない
※2 重要操作が電代業者の認証のみによって実施される（銀行が重要操作の権限を電代業者に与える認可を行う）ことについて、銀行はサービス連携の段階で予めユーザーの承認を得る（認証を行う）

（出典）当協会発出の周知文書より（一部抜粋）

（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

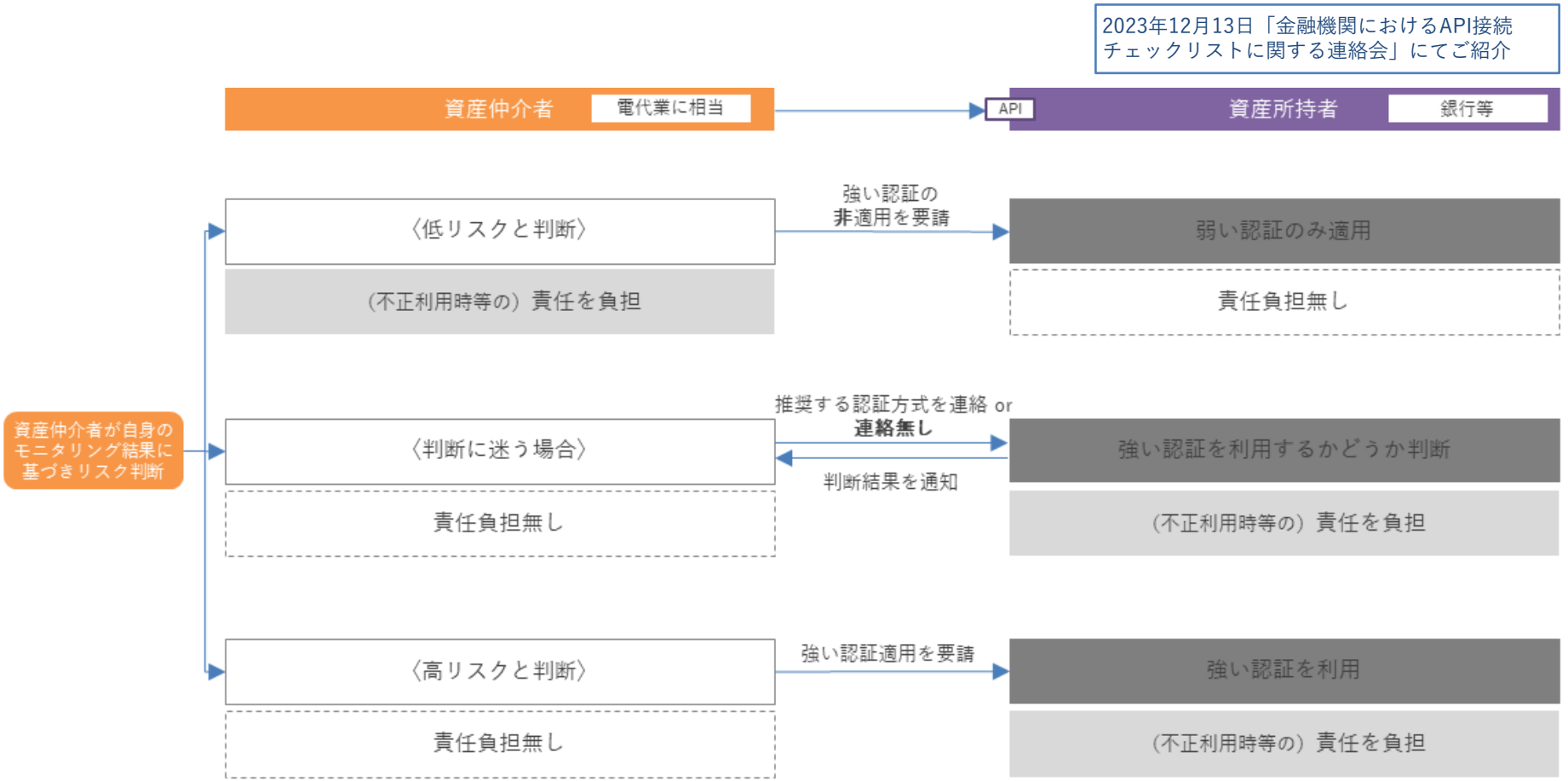
2023年12月13日「金融機関におけるAPI接続チェックリストに関する連絡会」にてご紹介



（出典）電子決済等代行事業者協会にて作成

（参考）欧州のTPP⇔銀行間の責任分界の考え方

- 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

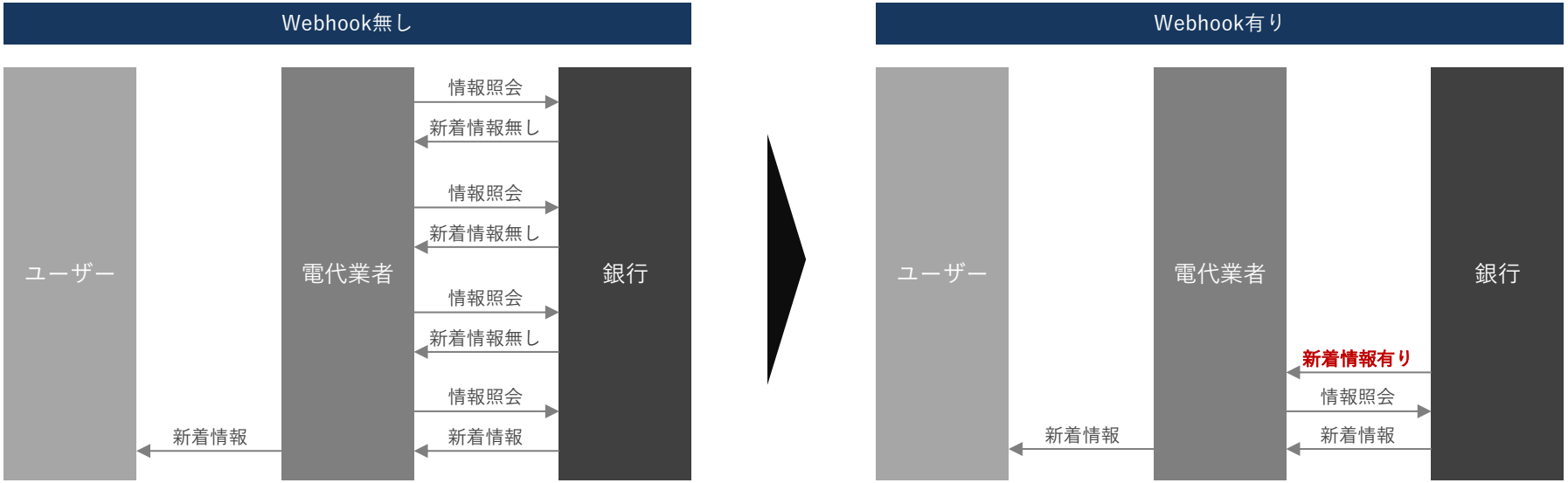
3. 委員の皆様へのヒアリング

委員の皆様へのヒアリング内容

内容	スライド
Webhookの導入について	P15-P16
セキュリティ関連の仕様標準化について	P17
その他お伺いしたい事項	P18

Webhookの導入について

●Webhookの導入は銀行、電子決済等代行業者ともにメリットのある機能であり、導入に当たっての**懸念点、課題について銀行のご意見を伺わせてください**



（出典）当協会で作成

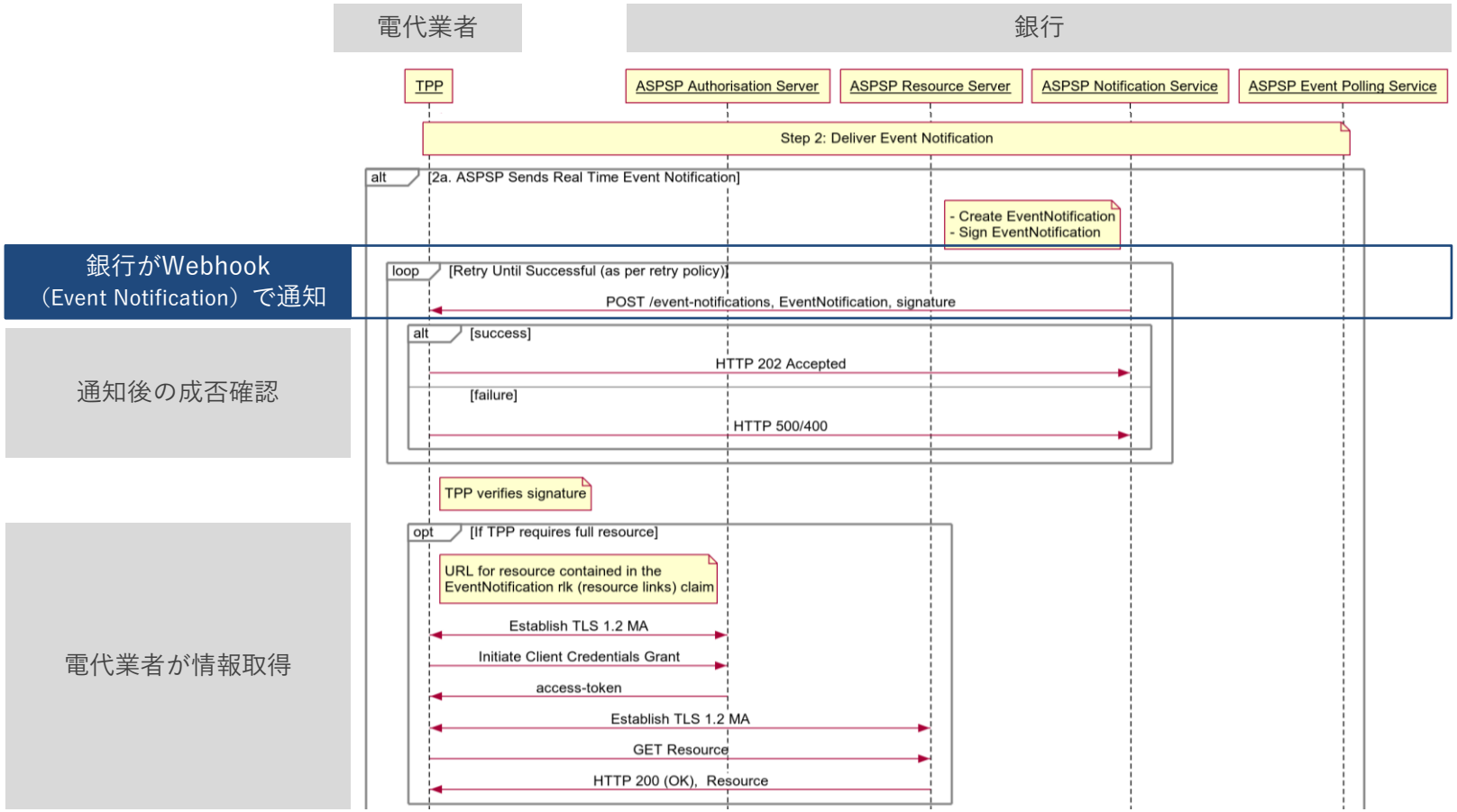
- 電代業者側のデメリットは特に無いと思料
- 通信負荷、 API接続コスト（従量制の料金の場合）の削減も期待
- 多くの銀行には入出金の都度メールを送る機能を備えているので、当該機能をAPIに準用できるのではないか
- 海外ではWebhookのAPI標準も策定（英国OBL、米国FDX等）※

※Event Notificationという名称の場合が多い

（出典）各種資料より当協会で作成

（参考）英国のWebhookの標準

●英国のOBL（API標準化団体）で定められたAPI標準におけるWebhookのシークエンス図



（出典）英国OBLのサイト掲載図表を基に当協会で作成

セキュリティ関連の仕様共通化について

- セキュリティプロファイル※1をFAPIやOpen ID Connectに仕様統一する場合に、**考えられる課題をお伺いさせてください**

※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）

- 日本では全国銀行協会様が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
  - 個別にOpen ID Foundationから認定を受けている銀行が存在
- 多くの銀行でOAuthなどは採用済みであると認識
- 金融を超えた他業態への採用拡張も見込まれる

採用状況の国際比較

項目	米国	英国	EU	日本
採用されている セキュリティプロファイル	FAPI Security Profile 2.0	FAPI 1.0 Advanced Final （2018年8月より）	―	FAPI （推奨）
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	OIDFが実施 （2018年8月より）	―	―

セキュリティプロファイル三者の関係

OAuth2.0

・第三者事業者がユーザーの許可を得て、ユーザーのデータにアクセスする「認可」のフレームワーク

Open ID Connect

・OAuth2.0をベースに認可だけでなく「認証（ユーザーの身元確認）」も可能とした拡張仕様
〈一般的なシングルサインオンはこの仕様に沿っている場合が多い〉

FAPI

・金融業界などより高いセキュリティが必要な場合の仕様

（出典）各種資料より当協会で作成

その他お伺いしたい事項

- 下記についても、ご意見を伺えますと幸いです

更新系API関係	●パスキーへの移行がAPI接続周りに及ぼす影響 ●パスキー導入にあたって、電代業者との間で課題になっている事項 ●パスキー導入の際、リフレッシュトークンの期間を短くするとフィッシング遭遇の機会を増やすことにつながりかねず、セキュリティ上の懸念があります。参照系と同様、望ましい期間を決めてみてはいかがでしょうか ●APIの整備前にパスキーが導入されることによる、スクレイピング連携の断絶を懸念しています（API連携を行っていない金融機関、証券業などが対象になるかと考えます）

4. その他共有したい事項

その他共有したい事項

- （電代業者のコメント）
  　パスキー等の導入に伴うUXの悪化は見られていないが、銀行専用アプリでの認証を利用することにより、電代業サービスを提供しているブラウザからの離脱が発生し、ユーザーにとって体験がわかりにくくなる可能性が課題と考えています
- 政府方針としてクレジットカード業界へのAPI対応が検討される予定です
- APIの海外状況、標準化等について調査を実施しています
- 資金決済システムの見直し議論が進められています

一般社団法人電子決済等代行事業者協会