2026 年 2 月 13 日
公益財団法人 金融情報システムセンター

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　議事要旨

１．開催日時

2025 年 12 月 4 日（木） 15:00～17:00 （会場開催及び Web 会議開催の併用）

２．委員・オブザーバー（敬称略・順不同）

	氏名	所属・役職
座長	住澤　整	公益財団法人金融情報システムセンター 理事長
委員	小西　健太	株式会社三菱 UFJ 銀行　リテール・デジタル企画部 新事業グループ　次長
	宇野　辰哉	株式会社横浜銀行　デジタル戦略部　決済ビジネス戦略室 決済ビジネス企画グループ　グループ長
	新居田　基彦	株式会社愛媛銀行 事務システム部　部長
	山崎　篤志	一般社団法人全国信用金庫協会 業務推進部　次長
	正木　達也	日本アイ・ビー・エム株式会社 アドバイザリー・アーキテクト　マネージャー
	松原　武司 （欠席）	アマゾン ウェブ サービス ジャパン合同会社 フィナンシャルサービスインダストリ技術本部 サービスソリューション部　部長
	畑 大作 （代理出席）	アマゾン　ウェブ　サービスジャパン合同会社 フィナンシャルサービスインダストリ技術本部 サービスソリューション部 シニアソリューションアーキテクト
	中島　悠貴	富士通株式会社　Banking&Securities 事業本部 ネットバンキング&証券事業部
	今井　博善	株式会社 NTT データ　第三金融事業本部 eービジネス事業部　部長
	瀧　俊雄	一般社団法人電子決済等代行事業者協会 代表理事
	藤川　由彦	弥生株式会社　経営企画本部 政策渉外担当　ディレクター
	茂岩　祐樹	freee 株式会社 執行役員 CISO

	氏名	所属・役職
	マーク マクダッド	マネーツリー株式会社 取締役
	小野沢　宏晋 （欠席）	GMO あおぞらネット銀行株式会社 執行役員　セールス＆マーケティンググループ長
	矢上　聡洋 （代理出席）	GMO あおぞらネット銀行株式会社 CTO
オブザーバー	今村　斎樹	金融庁　総合政策局 リスク分析総括課 ITサイバー・経済安全保障監理官室　金融証券検査官
	岸本　浩介 （欠席）	金融庁　総合政策局　リスク分析総括課 電子決済等代行業室　資金決済業調整官
	長瀬　礼明 （代理出席）	金融庁　総合政策局　リスク分析総括課 電子決済等代行業室　金融証券検査官
	佐瀬　豊	日本銀行　金融機構局　考査企画課 システム・業務継続グループ長
	寺山　大右 （欠席）	日本銀行　決済機構局　決済システム課 フィンテックセンター長
	池田　竜馬 （代理出席）	日本銀行　決済機構局　決済システム課 デジタル通貨検証グループ長

■事務局（FISC）

坂本 哲也（常務理事）、宮本 光樹（企画部長）、田村 翔（調査部長）、渡邊 暁（企画部次長）、市川 恭子（企画部主任研究員）、髙野 晴行（企画部主任研究員）、青井 良介（企画部主任研究員）、木下 雅治（企画部主任研究員）、古川 祐輔（企画部主任研究員）

３．議事内容

事務局より、【資料 3】に基づき 2025 年度金融機関アンケートについて報告し、【資料 4】に基づき Open Banking EXPO 2025 への参加報告を行った。

次に、事務局から、【資料 5】に基づき、API 接続チェックリスト見直し要否の対応方針について報告を行った。本報告を踏まえ、今年度の「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」（以下、「連絡会」という。）において、チェックリストの改訂を実施することにつき、全委員より同意を得た。

その後、一般社団法人電子決済等代行事業者協会　代表理事　瀧氏より、【資料 6】に基づき、各委員への提案、ヒアリング等が行われた。

４．API 接続チェックリスト見直し要否に関する検討結果

結論：チェックリストの改訂を行うこととする。

【資料 5】に基づき報告した事務局対応方針に対し、委員から異論はなく、今年度の連絡会において、チェックリストの改訂を行うこととした。

５．事務局からの報告に関するディスカッション（委員等から寄せられた意見等を中心に記載）

（１）2025 年度金融機関アンケート報告

特段の意見なし

（２）Open Banking EXPO 2025 参加報告

・　API の収益化モデルは日本でも課題が多く、海外でも有料化に成功した API が少ない点で悩んでいると認識している。その中で「プレミアム API」として取り上げられているものについて、具体的な機能や側面に関する情報はあるか。

・　【事務局】
具体的なものとしては「本人確認 API などのプレミアム API…」程度の言及。複数のセッションで API 収益化に関する言及はあったが、それらでも「普通の API とプレミアム API にわけて提供」という程度の表現であった。

・　「利用者の認知」や「リテラシー不足」について、どのような点が論じられていたのか、具体的な内容はあるか。

・　【事務局】
聴講した範囲では、具体的な事例の提示はなかったと記憶している。「認知が十分でない」「デジタル技術に対するリテラシーが十分でない」という程度の表現であった。

・　企業（法人全般）と消費者での認知やニーズの差異に関する情報はあるか。

・　【事務局】
小売店等では、オープンバンキングの支払手段を用いることでクレジットカード決済に比べ手数料が安価で済むため、利用を促進したい意向がある。一方で、顧客に対してはその価値が十分に伝わらず利用が進まない、あるいはそもそも存在が知られていないといった内容が述べられていた。また、加盟店向けの教育として、既存のクレジットカード決済と銀行支払と比べ構造やメリットを明らかにして、それぞれを支払いの選択肢と位置づけるべきという言及があった。また消費者に認知してもらい利用を拡大するには、慣れ親しんでいるクレジットカードと同様、銀行支払についても消費者を守り不正を防ぐという責任を果たすことがエコシステム関係者に求められると述べられていた。

（３）API 接続チェックリストの見直し要否にかかる検討

特段の意見なし

６．一般社団法人電子決済等代行事業者協会からの提案、ヒアリングについて（寄せられた意見等を中心に記載）

（１）電子決済等代行着業者協会からの提案事項

主旨	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の設立
具体的検討項目	・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 ・リフレッシュトークンの適切な更新頻度 ・電代業者と銀行間の責任分界（電代業者のみで認証完結可能なユースケースの検討）
構成員案	・電代協、全銀協、FISC より各数名の人員をアサイン、その他参画法人は必要に応じ検討
成果物案	上記３点の検討項目に関するガイドライン発出

上記提案（詳細は連絡会【資料 6】参照）に対し出席の委員間で議論が行われたが、合意は得られなかった。議論を踏まえ、座長のとりまとめにより、当日の提案については次年度に改めて議論することとなった。

各委員からの発言内容は以下のとおり。

- 構成員案に記載された各組織の賛同が得られるのであれば進められるのかもしれないが、「多要素認証を必須としないケース」について議論することに疑問を感じる。フィッシング被害が多発している昨今、金融庁がフィッシング耐性のある多要素認証の実装を求めているにもかかわらず、それに逆行するテーマを議論することになる。欧州では多要素認証を適用しなくてもよいケースが法令等で担保されているとのことだが、日本には同様の法的枠組みは存在しないため議論そのものが難しいのではないか。

- 検討会の検討項目の一部は、口座・アカウントへの不正アクセス防止の観点から、金融庁からも多要素認証の導入が推奨されている状況等を踏まえると、金融取引における認証厳格化の流れと方向性が一致しないのではないか。

- 利用者にとって頻繁な認証は不便であるため、入力が形骸化する懸念がある点には配慮が必要。

- 利用者側のニーズを踏まえて議論する必要がある。企業では IB の操作者と承認者を分けたいというニーズが少なくない。

- 全体のセキュリティ設計を考えつつガイドラインとして示すことは業界にとって有益。併せて補償の考え方についても整備が必要となるのではないか。

- セキュリティと利便性はトレードオフとなることが多いものの、生体認証等の技術でセキュリティを担保しつつ簡易化できるのであれば最良。ただしガイドラインとして定義されることで、運用や実装が縛られてしまうことに懸念を持っている。

- 本件はトレードオフの問題であるので、多要素認証を不要とすることを前提にするのではなく、幅広く検討したうえで最終的に結論が出るのであれば議論の意義がある。

- ガイドラインは「目安」として提示する前提で検討するのが良いのではないか。

- 安全性とユーザー体験の両立に向けた適切な条件の検討には賛同する。ただしイノベーション促進と同じくセキュリティは最重要事項であり、現に足元では不正取引が増加しているため、慎重に考える必要がある。議論にベンダーも参画することで技術的知見等も提供できるだろう。

- 【電代業協会】
  電代協は二段階認証、多要素認証をなくそうという提言はしていない。UX とリスクテイクのトレードオフの中で、一定の範囲でリスクを許容するのもリスク管理の一つの在り方であるという趣旨である。電代業者は銀行口座の決済サービスとしての利便性を高める役割を担っている。例えば交通系 IC カードのような少額の交通費支払いにおいて、改札で二段階認証を求められることはない。協会も自主規制機関として金融庁通達への対応を進めているが、同時に利便性の追求も行わなければならない。本日の参加各位がイノベーションに反対しているとは思っていないので、電代協の立場としてこのように伝える意味はあると考える。
  二段階認証を不要とするケースを提案している背景には、金融機関の口座振替の存在がある。口座振替は、認証・認可の度合いでいえば、強い認可権限を加盟店側、すなわち被仕向側（例：電気料金の口座振替支払でいう電力会社の立場）に付与している。口座振替の在り方を、銀行 API 時代のセキュリティ強度に耐えうるものへ見直す必要がある。口座振替の利便性が確保されない場合、海外のようにクレジットカードへの代替が進んでしまう可能性がある。銀行口座の競争力を維持するため、重要な論点と考える。
  検討会の具体的項目案として複数挙げているが、すべてをワンパッケージで議論する必要はないと考えている。リフレッシュトークンの更新期限の在り方や、電代業者と金融機関の責任分担の原則についてもご議論願いたい。

- 現行の更新頻度に対し、ユーザーが何をどこまで求めているのかについて、理解を深める必要がある。責任分界については、対象となる操作の切り分けに議論が必要。仮に電代業者側が認証責任を負う場合、銀行側に監督する役割が残るのかどうかも含めて考えていく必要がある。

- 金融庁からはフィッシング耐性のある多要素認証を求められているが、その延長で考えると今回のトークン更新についても ID・パスワード方式のままでいいのか、パスキーや生体認証を使えばユーザビリティがそこまで落ちないのではないか、という議論にもなると思う。

- 【電代業協会】
  英国では電代業者とユーザーのやり取りで、金融機関を介さずにトークンの期間延長ができる場合がある。ユーザーが常時使用していなくてもトークンが延長されデータが欠けない。通常、トークン期間が切れると最新状態に更新されなくなるが、これが例えば確定申告で必要な時に必要な情報が取得できない、といった弊害をもたらす可能性がある。

- 更新頻度がユーザビリティを損なうという考えも理解できるが、SNS のようにアカウント放置が乗っ取りにつながるケースもある。バランスが求められるのではないか。

- 責任分界については「重要な認証」の例示や区分けについて目線を揃え、定義づけを整理すること

が必要。資料の記載に「予約のみを行う操作は重要な認証に含めない」とあるが、予約後に自動実行される取引も多くある。このようなケースを含め、定義づけの整理が重要と考える。

- 利用者が意図しないままトークンが残存することは望ましくなく、長すぎる設定は慎重であるべき。責任分界については議論が尽きないのではないか。

- トークン更新頻度、責任分界のいずれもこれまで十分議論されてこなかった。トークン更新頻度については実態を踏まえて再検討することは有意義。責任分界についてはこれまで個別契約の中でのみ議論されてきたことなので、広く事業者間で議論すること自体は有益と考える。

- 【電代業協会】
  本日示したもののうち、多要素認証に関してはおおむね否定的なご意見が多かったと受け止めている。一方で、リフレッシュトークンの件については、議論として非常に建設的な示唆が得られたと感じる。業界対業界の議論になった際にも、こうした議論の進展を生む「場」を確保することが何より重要と考え、今回のご提案に至っている。また、合意しづらい論点をきちんと炙り出すこと自体にも価値があると考えており、いわば「Agree to Disagree（合意できないことを合意する)」をきちんと扱う場を持つことが重要だと考える。どこまで厳密な会議体にするかについては、今はコンセンサスがないが、年に1回「そういえばこうだった、ではまた来年」というペースでは前に進まない。開催頻度や開催方法ついては柔軟に検討しつつ、何らかの形は作っていきたいと考えている。

- 【電代業協会】
  認証・認可 API の有効期間について、利用者へ通知していない金融機関が大半であると認識している。そのため利用者は突然再認証やパスワードを求められることになり、ユーザー体験が損なわれることになる。利用者保護の観点からも認可の有効期間については金融機関から利用者へ開示することが望ましいと考える。
  議論を行うための場が今次提案の「検討会」であると考えているので、否定的な意見が多かったからこそ検討会を設けるべきなのではないかと感じた。

- 【電代業協会】
  議論ではベストプラクティスのとりまとめや、行動規範を示すといったアウトプットの仕方もあると考える。

- 【電代業協会】
  認証強度を下げる方向は皆が怖いと感じるのが前提だろうし慎重であるべきと考える。そのうえで、利便性の議論では各々が想定するユースケースが異なっているのではないかと感じた。次回以降の議論では具体的なユースケースをもとに議論できると、金融機関、ベンダー、電代業者の歩み寄りが進むと思う。継続的に議論したい。

（2）電代協から、Webhook の導入について各委員へのヒアリング事項

・銀行側で Webhook（システムでイベントが起きた瞬間に、別のシステムへ自動で通知を送る仕組み）としての通知機能を備えてもらうことで、余計なトラフィックを削減できる点がメリ

ットと考えているがどうか？
・通信負荷の低減に加え、電代協の視点では、従量制の料金体系の場合、銀行様へ API 利用料支払の削減につながる可能性があると考えるがどうか？
・多くの銀行では入出金のつどメール通知する機能がある程度整備されているので、このような既存の通知機能を API に応用可能と考えているがどうか？

- トランザクション数が少ないユーザーにとっては必ずしもニーズが高くないのではないか。一方、取引が多い口座でも、通知のニーズがどこまであるのか見極める必要がある。導入する場合はコストも発生する。その点も含め、検討が必要。

- Webhook は便利な機能である一方、現状の取引件数や利用状況を踏まえ、メリットの有無を含めて慎重に検討する必要があると考える。

- Webhook のフロー全体を考えると、電代側から「この利用者は通知希望」「この利用者は不要になった」等の情報を受け取り、銀行側で顧客管理をすることになる。銀行側の管理負荷や管理の仕組み等、検討事項は多い。

- 当社は Webhook を提供しており、UX 向上に寄与している。ただし Webhook の通知が飛ばなかった場合に誰がどのように検知・対応するかといった責任分界の整理が重要で、体制構築も容易ではない。総合的な判断が必要。

- システムの観点で話す。銀行のアーキテクチャは、古くから稼働している勘定系システムがあり、その手前に API 化のレイヤーを置いているケースが比較的多い。この構造で Webhook を実装しようとすると、手前の API レイヤーが勘定系システムへ高頻度に問い合わせ続けることになりやすく、外部向けの通信は抑制できても、銀行内部では非常に大きな通信負荷が発生する仕組みとなる可能性がある。この点は解消が難しいだろう。また、取引の都度メールを通知する機能を備えている金融機関もあるが、チャネルごと（インターネットバンキング、ATM など）に個別の仕組みで実装されていることが多く、全入出金に対して単一箇所からフックを出せるかというと、難しいと思われる。現状の一般的な構造を前提にすると、このような課題があると認識している

- メール通知の機能を備えていない金融機関も多く、導入するには新たな開発が必要になるだろう。

- 【電代業協会】
  Webhook はこの業界で最優先の要望事項の一つと考えていたが、この 2 年余りの調査、また本日の議論を通じて多くの点が明らかになった。コンセンサスに至る段階とまでは言えないが、金融機関の側に厳しい事情が存在することが理解できた。電代協側では各行の基幹系の違いなどを推測でしか把握できない部分があるので、状況を具体的に知ることができ、大変ありがたく感じている。

（3）電代協から、セキュリティ関連の仕様の共通化について各委員へヒアリング

セキュリティプロファイルの整理として、最もベーシックなものは OAuth(サードパーティアプリによる HTTP サービスへの限定的なアクセスを可能にするための認可フレームワーク)、その上で認証まで含める場合は OpenID Connect（OIDC。サービス間で利用者の同意に基づき

ID 情報を流通するための標準仕様)、さらに金融機関向けにセキュリティ強度を高めたものが FAPI（Financial-grade API の略。金融業界等の、より高い API セキュリティレベルを要求されるシステムへのガイドラインとして策定された技術仕様)。API 間のプロトコルのやり取り自体は、これらの仕様間で類似点も多い印象。

そこで伺いたいのは、仮に FAPI や OpenID Connect に仕様を厳密に統一しようとする場合、どのような課題が想定されるかという点であり、具体的にどの程度難しいのかご教示いただきたい。

- 仕様の統一・共通化という方向性には同意する。ただし、相応の開発期間が必要になると考えている。既存事業者の多くは FAPI 準拠ではない API を利用しているため、切替えにはそれなりの対応が必要になるという認識。

- 基盤寄りの領域となるので銀行の側から見通しを示すことは難しい。実務的にはベンダーと相談しながら進めるのではないか。

- FAPI に限った話ではなく OAuth などもそうだが、それらはあくまでフレームワーク。「準拠しましょう」だけでは各社それぞれの仕様となりかねないので、諸外国と同様に厳密な仕様・定義まで踏み込んで統一しないと結局乱立を招くことになる。そのうえで提供者・利用者の理解醸成、また実装においてもサンドボックスの提供等の実装支援が不可欠。難易度は高いと考える。

- シングルサインオンを念頭に置いたとき、OIDC に限定することは、過度な制約になってしまう点が懸念される。次に FAPI について。金融機関からの問い合わせは多いが、実際の実装段階でサードパーティ側から「対応が難しい」と言われることが少なくない。FAPI の採用にあたっては要件を少し緩めるなど、実装コスト面も含めた検討が必要ではないかと考える。

以　上