A COMPASS TO FIND YOUR WAY

ATSUMI & SAKAI
TOKYO | LONDON | FRANKFURT
www.aplaw.jp

更新系APIに関する取組上についての法的な視点からの留意点

渥美坂井法律事務所・外国法共同事業
プロトタイプ政策研究所所長・シニアパートナー弁護士
落合孝文

開催日: 2023年5月29日

プロフィール

落合　孝文
プロトタイプ政策研究所所長・弁護士
シニアパートナー（第二東京弁護士会所属）

takafumi.ochiai@aplaw.jp

慶應義塾大学理工学部数理科学科卒業。2005年慶應義塾大学大学院理工学研究科在学中に旧司法試験合格。2006年弁護士登録（第二東京弁護士会）。渥美坂井法律事務所・外国法共同事業シニアパートナー。医療、金融、不動産、交通、通信等の新規事業開発や規制対応、情報利活用、海外進出等に関するサポートを行う。2022年にはスマートガバナンス株式会社を設立。代表取締役共同創業者に就任し、新たな技術・ビジネスのガバナンスの社会実装を進める活動も行っている。

公的団体等
内閣府国家戦略特区WG　座長代理
内閣府規制改革推進会議　専門委員
デジタル庁デジタル臨時行政調査会作業部会委員
内閣府新技術等効果評価委員会　委員
金融庁「デジタル・分散型金融への対応のあり方等に関する研究会」オブザーバー
総務省「情報通信法学研究会」委員
経済産業省「Society5.0における新たなガバナンスモデル検討会」委員
総務省「AIネットワーク社会推進会議 AIガバナンス検討会」委員
厚生労働省「医療分野における仮名加工情報の保護と利活用に関する検討会」委員
厚生労働省、総務省、経済産業省　「健診等情報利活用ワーキンググループ　民間利活用作業班」委員
総務省・経済産業省　「情報信託スキームの情報信託機能の認定スキームの在り方に関する検討会」委員
経済産業省、公正取引員会、総務省「デジタル・プラットフォーマーを巡る取引環境整備に関する検討会 データの移転・開放等の在り方に関するワーキング・グループ」委員（終了）
福岡県国際金融都市アドバイザー他多数

民間団体等
一般社団法人日本金融サービス仲介業協会代表理事副会長
一般社団法人電子決済等代行事業者協会理事
一般社団法人データ社会推進会議　監事
一般社団法人Fintech協会常務理事
一般財団法人JCoMaaS　理事　　他多数

更新系APIの取扱いの目線

前提

全国銀行協会「銀行法に基づく API 利用契約の条文例」及びその実質的な内容を定めている全国銀行協会「オープン API のあり方に関する検討会報告書」が作成された当時、更新系APIは事例に乏しい状況であり、参照系APIについてもその後の2020年の猶予期限経過時のように広範に利用されている状況にはなかった。

↓

報告書、条文例のいずれについても、一応更新系の可能性は想定して作成していたこともあってか、その後一部進展した更新系サービス提供にあたっても、報告書、条文例、ないしFISCチェックリストのいずれも改訂はされていない。

↓

実際にこの数年間で銀行APIが使用された経験や、2023年の時点で想定される更新系APIに関する想定が反映された内容とはなっていない。

更新系APIの取扱いの目線

ポイント

① これまでの実務経験・社会環境の変化を踏まえ、議論の到着点（ゴール）を確認し、アジャイル・ガバナンスの概念（閣議決定されたデジタル原則にも含まれる後述の概念）を踏まえたルールの改善を行う。

② 現時点では、参照系APIは十分に広く利用されているが、更新系APIの推進の視点から、未解決の論点を整理していくことが重要。ここでは、更新系APIにおける為替取引における法令遵守（AML/CFTその他の法令等対応による取引審査）、セキュリティ対策、利用者保護等の視点が重要ではないか。

③ 契約上の責任分界点の整理の確認に加え、リスク管理の観点から、行為規範を整理し、更新系APIに対応したリスク管理を進める。

「アジャイル・ガバナンス」の基本的な考え方

	Society4.0以前	Society5.0
日常生活とデジタル技術の関係	フィジカル空間とサイバー空間とが分離している	フィジカル空間とサイバー空間とが一体化し、日常生活に不可欠な基盤に
信頼の対象	有体物（ヒト・モノ）	無体物（データ・アルゴリズム）
取得するデータ	限定的	大規模・広範囲・多種類
判断の主体	ヒトのみ	AI・システムの影響が拡大
システムの状態	安定的	流動的
結果の予見・統制可能性	予測・統制可能な領域が多い	予測・統制不能な領域の拡大
責任主体	特定しやすい	特定が困難
支配力の集中	集中しやすい	より集中しやすい
地理的関係性	ローカルまたはグローバル	ローカルかつグローバル

- 社会は複雑かつ急速に変化し、予想困難かつ統制困難となる。
- ガバナンスによって目指すべき「ゴール」自体も変化し続ける。

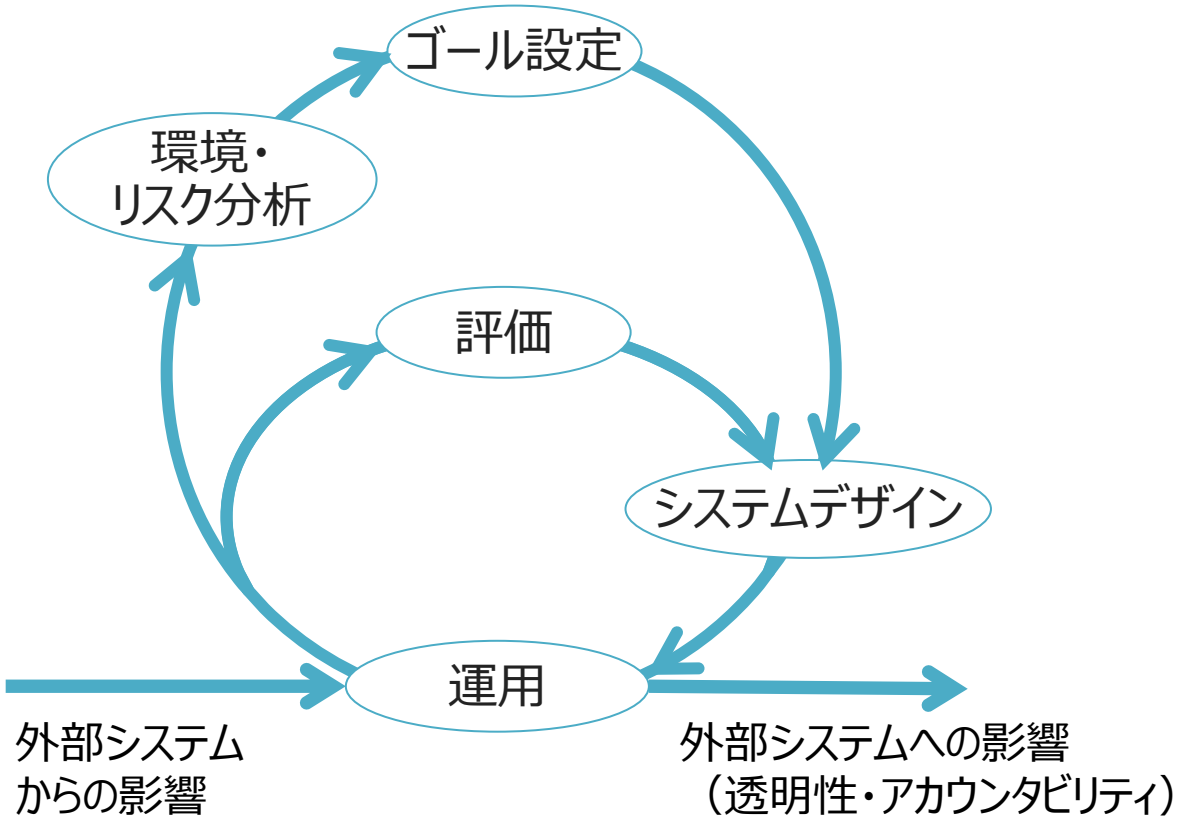
⇒ Society5.0のガバナンスモデルは、**常に変化する環境、技術とゴールを踏まえ、最適な解決策を見直し続ける**ことが必要。

出典：経済産業省GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて

アジャイル・ガバナンスについて

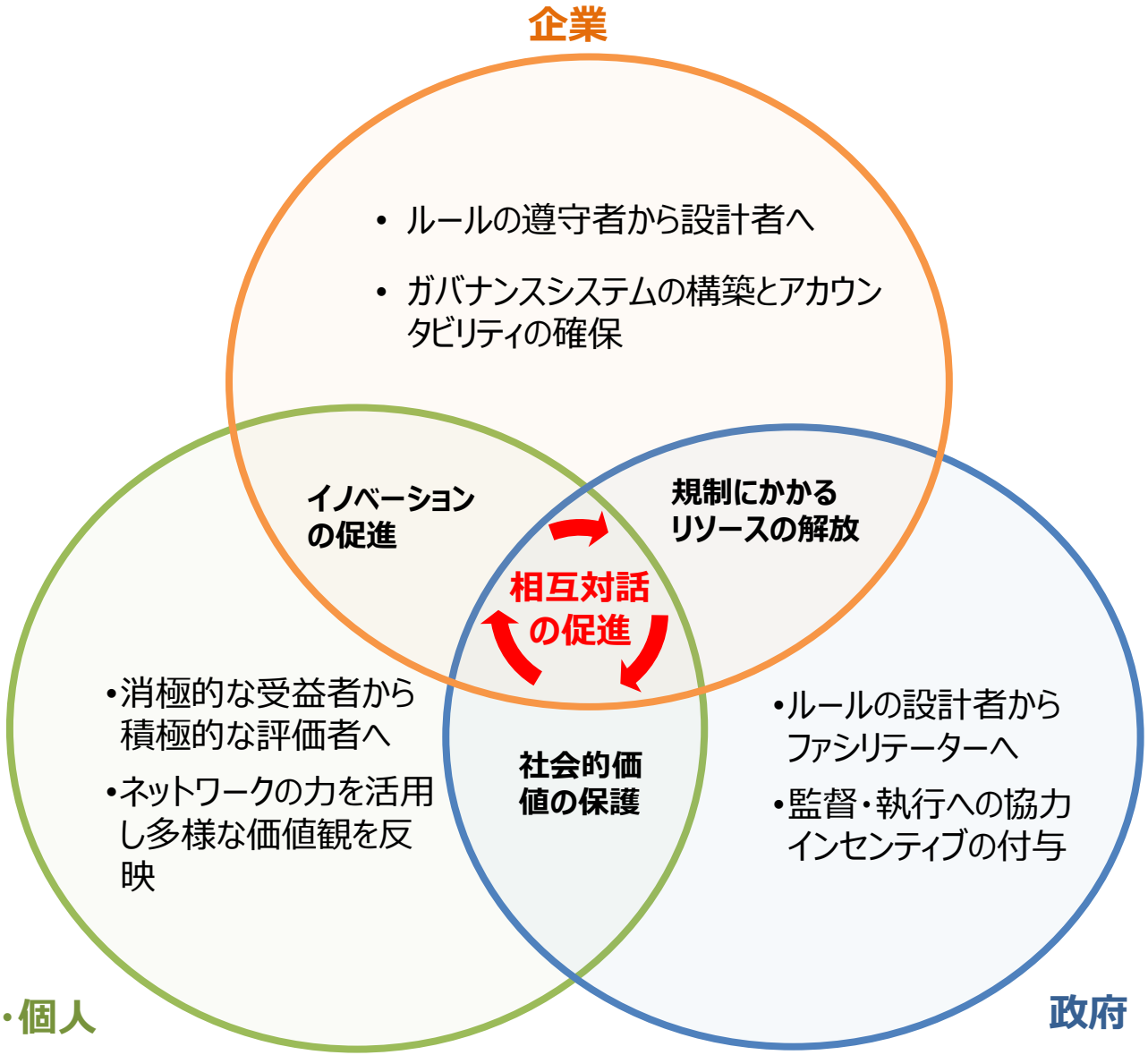
アジャイル・ガバナンスとは、

「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」「改善」といったサイクルを、**マルチステークホルダー**で**継続的かつ高速に回転**させていくガバナンスモデルをいう。



出典：経済産業省GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて

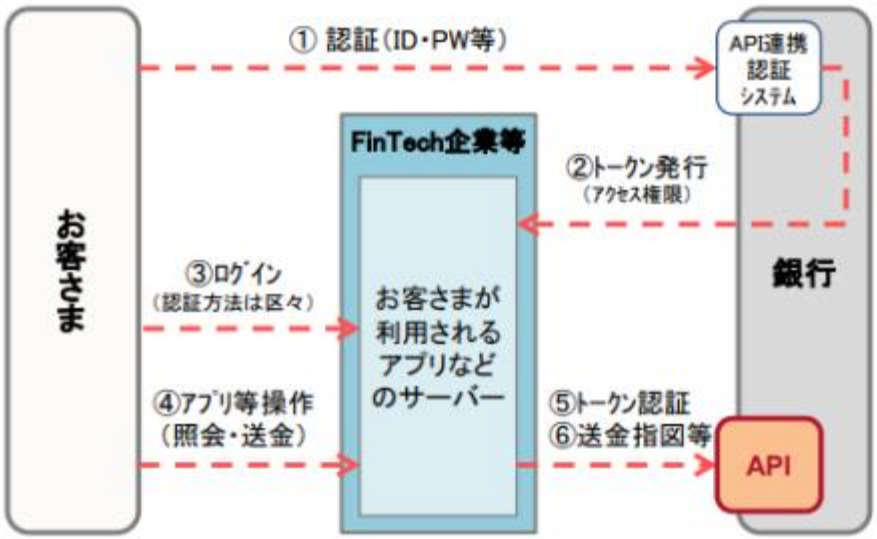
各主体の役割の変化と利益



出典：経済産業省GOVERNANCE INNOVATION Ver.2：アジャイル・ガバナンスのデザインと実装に向けて

APIの基本的な仕組み

【図表１】オープン API の基本的な仕組み（OAuth2.0）



（注１）図表は実装する通信・業務フローをごく簡略化したイメージ。
（注２）なお、データ通信はインターネット回線を通じて行われることが一般的。

- 参照系・更新系ともに、基本的には、銀行の勘定系に直接接続はされないものの、インターネットバンキング基盤にAPIが構築される。APIにおいて電子決済等代行事業者は情報取得、送金指図を行うことができるが、銀行システムを通じて情報連携・送金指図を行うことに特徴がある。
- トークンの発行、管理、抹消や、トークン認証、電子決済等代行事業者ないし利用者の権限制限、送金指図等に対する審査として銀行がどのようなことを行えるか。銀行口座開設時の本人確認等は銀行が直接行っている場合が多く、また個別の取引指図をどのようにするかは後述のように論点があるが、銀行がトークン利用の権限の付与にあたってのOAuth2.0に基づく認証・認可手続を行える。
- 一方で、利用者の面前に立つのは電子決済等代行事業者であることも多く、個別取引の指図や、利用者側への情報提供・説明等も含めて電子決済等代行事業者と役割分担を行うことも考えうる

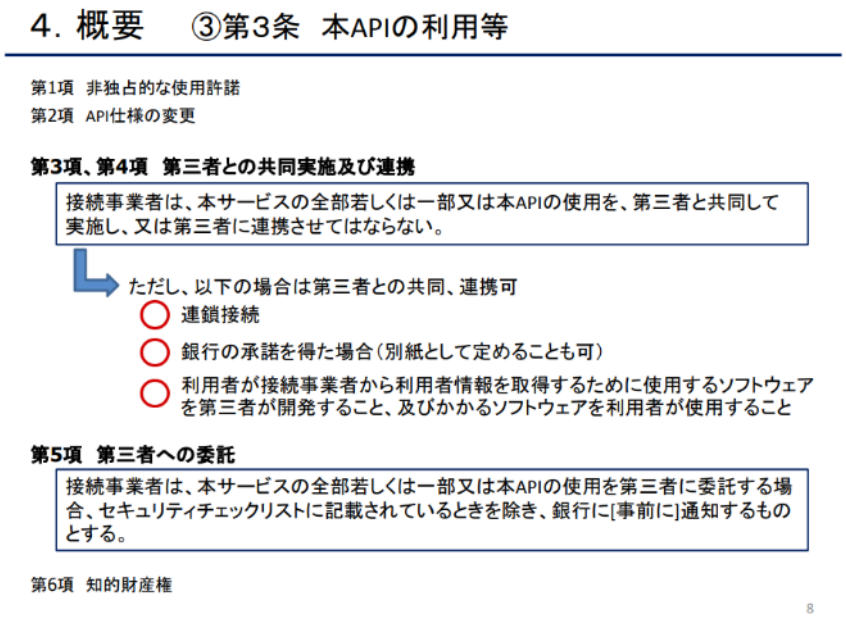
出典： 全国銀行協会「オープン API のあり方に関する検討会報告書」6頁

各論

- 法的責任について
  - API利用契約ひな形の関連条文（次項も参照）
    - ✓ 第3条（本APIの利用）
    - ✓ 第10条（利用者への補償）

  - 責任分界点がひな形で定められているものの、誰の責任であるかという点を法律で一義的に定めることは難しい部分がある。もっとも、API利用契約上文例においては、第10条の解説において以下の記載を設けており、事実上役割分担を踏まえた、責任関係をできる限り予見可能なものにしようと務めている。
    - ✓ 本サービスに関して生じた損害であるかどうかについては、例えば、本サービスが利用者の委託により送金の指図を銀行に伝達することを役務として提供するものであり、本銀行機能が当該送金の指図に基づいて送金の処理を行うことであった場合において、送金の指図の銀行への伝達は正しく行われたが、銀行が伝達された指図の内容と異なる内容の送金の処理を行ったことにより利用者に損害が生じた場合、当該損害は本サービスに関して生じたものではなく、本銀行機能に関して生じたものと考えられ、これに関して利用者に生じた損害は、接続事業者が補償するのではなく、銀行が補償することが想定される。
    - ✓ 本銀行機能に関して利用者に生じた損害について、第2項及び第3項と同様の要件を満たせば銀行が接続事業者に求償できる余地があるものとしている。但し、当然のことながら、専ら銀行の責めに帰すべき事由による損害については接続事業者に対して求償することは想定されない。運用における銀行の責めに帰すべき事由（本 API の内容及び構成の決定並び
    - ✓ 利用者に生じた損害が専ら本 API の開発過程またはに運用については、原則として銀行の責任においてなされるべきものと考えられる。）によって発生したことが、当該損害の発生時ないしその直後に明らかとなった場合には、・・・双方が合意の上で、銀行が直接利用者に対して補償または賠償を行うことが合理的であると考えられる。

APIの基本的な仕組み



4．概要　③第3条　本APIの利用等

第1項　非独占的な使用許諾

第2項　API仕様の変更

第3項、第4項　第三者との共同実施及び連携

接続事業者は、本サービスの全部若しくは一部又は本APIの使用を、第三者と共同して実施し、又は第三者に連携させてはならない。

ただし、以下の場合は第三者との共同、連携可

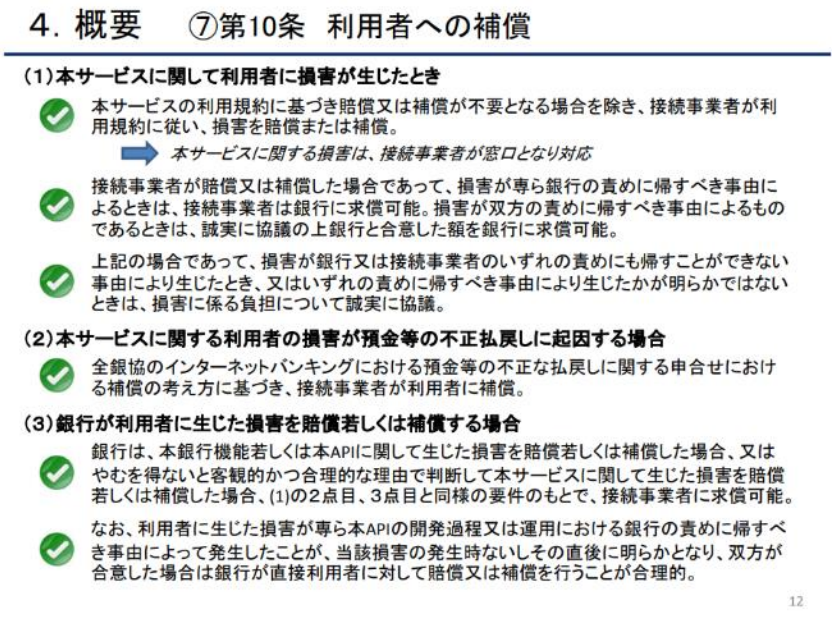
- 連鎖接続
- 銀行の承諾を得た場合（別紙として定めることも可）
- 利用者が接続事業者から利用者情報を取得するために使用するソフトウェアを第三者が開発すること、及びかかるソフトウェアを利用者が使用すること

第5項　第三者への委託

接続事業者は、本サービスの全部若しくは一部又は本APIの使用を第三者に委託する場合、セキュリティチェックリストに記載されているときを除き、銀行に[事前に]通知するものとする。

第6項　知的財産権

8



4．概要　⑦第10条　利用者への補償

(1)本サービスに関して利用者に損害が生じたとき

本サービスの利用規約に基づき賠償又は補償が不要となる場合を除き、接続事業者が利用規約に従い、損害を賠償または補償。

本サービスに関する損害は、接続事業者が窓口となり対応

接続事業者が賠償又は補償した場合であって、損害が専ら銀行の責めに帰すべき事由によるときは、接続事業者は銀行に求償可能。損害が双方の責めに帰すべき事由によるものであるときは、誠実に協議の上銀行と合意した額を銀行に求償可能。

上記の場合であって、損害が銀行又は接続事業者のいずれの責めにも帰すことができない事由により生じたとき、又はいずれの責めに帰すべき事由により生じたかが明らかではないときは、損害に係る負担について誠実に協議。

(2)本サービスに関する利用者の損害が預金等の不正払戻しに起因する場合

全銀協のインターネットバンキングにおける預金等の不正な払戻しに関する申合せにおける補償の考え方に基づき、接続事業者が利用者に補償。

(3)銀行が利用者に生じた損害を賠償若しくは補償する場合

銀行は、本銀行機能若しくは本APIに関して生じた損害を賠償若しくは補償した場合、又はやむを得ないと客観的かつ合理的な理由で判断して本サービスに関して生じた損害を賠償若しくは補償した場合、(1)の2点目、3点目と同様の要件のもとで、接続事業者に求償可能。

なお、利用者に生じた損害が専ら本APIの開発過程又は運用における銀行の責めに帰すべき事由によって発生したことが、当該損害の発生時ないしその直後に明らかとなり、双方が合意した場合は銀行が直接利用者に対して賠償又は補償を行うことが合理的。

12

- 契約の条文例においては、更新系の場合も含め、利用者の預金の不正な払戻しに至る場合も想定して整理がなされており、利用者との関係で、銀行・電子決済等代行業者が無過失の場合も想定して、契約としては一定の整備がなされているところである。
- なお、契約の条文例の考え方については、その後「資金移動業者と銀行の間の口座連携に係る覚書の条文例」も公表されている。
- また連鎖接続に限らない第三者についても、以下のAPI利用契約条文例第3条第4項により、電子決済等代行業者が責任を負担すること、第三者に対して銀行API利用契約の定めを遵守させることを求めている。
  - 接続事業者は、前項に基づく銀行の事前の書面等による承諾により、本サービスの提供の全部若しくは一部または本 API の使用を、第三者と共同して実施し、または第三者に連携させる場合には、当該第三者の行為についても本契約の定め（情報の適正な取扱い及び安全管理のための措置並びに法令等に基づき必要な事項に限る。以下本項において同じ。）による責任を負担し、当該第三者をして本契約の定めを遵守させるものとする。
- 連鎖接続先の行為の責任、連鎖接続先にもAPI利用契約の主要条項の定めを遵守させることについては、API利用契約上文例第13条第4項及び第6項に定められている。

出典：　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」6頁

更新系APIの種類について

- 為替取引に関するAPIについて、複数の種類が存在し、特に他行宛振込などは整理が難しいものと捉えられることが多い。

- 同一名義人間の口座振替　⇒　同一名義人に限らない口座振替（この中でも公金収納や、これに準じるような信頼できる取引先であるかにより異なりうる）　⇒　振込　のように実装する機能により、リスクが異なる。

- 銀行APIに接続して指図が行われることから、電子決済等代行業者が提供するサービスや機能の特性も考慮し、リスクの整理が必要。

各論

認証等について

- 実際のリスクを定義するという意味で、具体的な視点からの検証が重要。
- 検証にあたっては、OAuth2.0の利用を前提に、特に銀行APIとの接続部分（認可コード、アクセストークン、リフレッシュトークン等）についてリスク対策ができるような仕組みを構築することが重要。
- 参照系における認証認可については、現在、OAuth 2.0が主流であるが、その後の技術の進展を踏まえて、基本的なフレームワークについて留意すべき点はないか。
- さらに、更新系については追加でセキュリティ強化を要するのかという点が検討ポイント。利用者の利便性向上という更新系APIの目的も考慮しつつ、銀行側のシステム面を中心とする業務負荷と不正取引防止のバランスが重要。
- また個別為替取引において、どのように画面遷移も含めて構成を行っていくかは論点になりうる。銀行のインターネットバンクの画面において個別の指図を受け付けることが想定されているとも思われる。この場合には、主に銀行側の個別取引に関する当人認証については、通常のIB基盤と同様の対策を行っていれば足りるか。
- さらに、仮に銀行のインターネットバンク側の画面での指図を受け付けず、電子決済等代行事業者側の画面で、利用者の操作を終了する場合には、電子決済等代行業者にどのような本人確認（身元確認、当人認証）を求める必要があるか。

各論

AML/CFT等の取引審査その他の銀行と電子決済等代行業者の連携に関して役割分担、リスクヘッジについて検討しうる事項について

- コンプライアンス、リスク管理の観点から、どこまで行えば銀行が免責されるのか。契約上の責任分界点の話とは別の行為規範としてどこまで管理しなければならないのかという視点。銀行と電子決済等代行業者とのコンセンサスが取れていないという問題はある。各社が悩んでいる部分を抽出して、具体例として記載することは今後の議論では有益と思われる。

- 電子決済等代行業者は犯収法上の取引時確認義務を負わないという整理と、銀行のインターネットバンキングを基盤とした更新系APIを利用する取引であり、銀行が必要な対策を行いうる場合が多いとも想定される。

- 一方で、顧客との第一次的なインターフェイスは電子決済等代行業者が有していることや、個別取引における電子決済等代行業者のインターフェースでの取引完結を考えると、とりわけ更新系に関しては、疑わしい取引報告や継続的顧客管理という観点から、電代業者がより顧客に近い立場にあることをどのように評価するかという問題。

- なお、接続を行う電子決済等代行業者側の、利用できるAPIの種類・内容・金額等の権限範囲を限定すること等によるリスクの合理化や、API利用業務に関する報告、情報連携態勢、更新系におけるセキュリティチェックリスト等において特出しして情報提供、整理を求めるような事項があるか等について検討の余地があるのではないか。

連鎖接続について

- 連鎖接続該当性について、そもそも参照系APIの場合でも指図が連続していなければ、事実上情報連携がされていても連鎖接続には該当しないという整理がされていることが一般的。

- こういった整理がされている実態を踏まえて、リスク管理を行う必要がある。更新系APIでも、同様の情報伝達形態（必ずしも送金指図が連鎖しないケース）が想定しうるのか、想定しうるとしてどのような取引形態となるのかを踏まえたリスク整理が必要。

- 更新系API+連鎖接続というものは、現状少ないのではないか。何を行うと困るのかという部分を抽象的・暫定的に想定して議論しただけで、具体的な業務に即して検討はされていない（電子決済等代行事業者全般としてはAPIを利用しない1号事業者においては、連鎖接続は存在しうるとも思われる）。

ご清聴ありがとうございました。

お問い合わせ先

渥美坂井法律事務所・外国法共同事業
〒100-0011
東京都 千代田区 内幸町2-2-2
富国生命ビル (受付: 16階)
WEB: www.aplaw.jp

プロトタイプ政策研究所　所長
シニアパートナー弁護士 落合孝文
E-Mail: takafumi.ochiai@aplaw.jp
（第二東京弁護士会所属）

Atsumi & Sakai