オープン API のあり方に関する検討会報告書

－ オープン・イノベーションの活性化に向けて －

【中間的な整理（案）】

※ 本報告書は、2017 年３月現在の関係法令にもとづく中間的な整理（案）であり、関係法令の改正等が行われた場合には必要に応じて当該法令に準拠した改訂等を行う予定です。参照に当たっては、関係法令等の改正動向もご確認ください。

2017 年３月 16 日

オープン API のあり方に関する検討会

（　事務局：一般社団法人 全国銀行協会　）

序 文

近年、金融機関と FinTech 企業等との連携を通じた金融サービスの高度化に向けたツールとして、銀行システムへの接続仕様を他の事業者等に公開する“オープン API”への注目が高まっている。わが国銀行界においても、現在、多数の銀行がオープン API の活用可能性について検討を開始している[1]。

API（Application Programming Interface）とは、一般に「あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様等」を指し、このうち、サードパーティ（他の企業等）からアクセス可能な API が「オープン API」と呼ばれる。

金融分野におけるオープン API は、世界的にも試行錯誤フェーズにあり、考え方の整理が必要な論点が多いものの、オープン API を通じて実現される協業・連携型のイノベーションは、わが国のカルチャーとの親和性も高く、世界をリードできる分野である。

金融審議会「決済業務等の高度化に関するワーキング・グループ報告 ～決済高度化に向けた戦略的取組み～」（2015 年 12 月 22 日公表）や政府「日本再興戦略 2016 -第４次産業革命に向けて-」（2016 年６月２日閣議決定）等においても、情報セキュリティに留意しつつ銀行システムと連携した多様な金融サービスの創出を可能とする銀行システムの API（接続口）の公開について、官民連携して検討していく方針が打ち出されている。

一般社団法人全国銀行協会では、こうした状況を踏まえ、銀行界、IT 事業者、FinTech 企業、学識経験者、弁護士、消費者団体、関係当局等をメンバーとする「オープン API のあり方に関する検討会」を設置し、同検討会において、銀行分野におけるオープン API（バンキング API）のあり方について検討を行った。

報告書の取りまとめに当たっては、幅広い関係者の参加を得て、お客さま、FinTech 企業、金融機関それぞれの立場からの意見を幅広く聴取し、いずれか一方の意見に偏ることなく、わが国におけるオープン・イノベーションの活性化を目指し、イノベーションの促進と利用者保護のバランスのとれた内容とすることを追求・意識した。

本報告書は、同検討会の成果として、お客さま、FinTech 企業、金融機関の Win-Win-Win の関係の下、わが国の金融サービスの高度化、利用者利便性等の向上を実現するためのオープン API の活用促進に向けた官民連携のイニシアティブを取りまとめたものである[2]。

---

[1] 2016 年６月に実施した全銀協アンケート調査によれば、48％の銀行が活用可能性を検討中。

[2] 当検討会は、銀行以外の事業者がオープン API に取り組む場合においても、本報告書が、当該事業者の参考になることを期待する。

目次

オープンAPIのあり方に関する検討会名簿

メンバー	増田　正治	（株）三井住友銀行執行役員システム統括部長
	亀田　浩樹	（株）三菱東京ＵＦＪ銀行執行役員システム本部長兼システム企画部長
	加藤　昌彦	（株）みずほフィナンシャルグループＩＴ・システムグループ専門役員
	梅原　弘充	（株）静岡銀行理事経営企画部長
	佐々木　勉	（株）北洋銀行チャネル開発部フィンテック推進室長
	吉本　憲文	住信ＳＢＩネット銀行（株）FinTech事業企画部長
	佐畑　大輔	（株）ＮＴＴデータ　ｅ－ビジネス営業統括部長
	羽川　茂雄	日本アイ・ビー・エム（株）GBS事業本部 銀行FM金融第一インダストリーソリューション部長
	丸山　弘毅	FinTech協会代表理事／（株）インフキュリオン・グループ代表取締役
	Mark Makdad	FinTech協会理事／マネーツリー（株）営業部長
	瀧　俊雄	一般社団法人金融革新同友会FINOVATORS／ （株）マネーフォワード取締役兼Fintech研究所長
	増島　雅和	森・濱田松本法律事務所パートナー弁護士
	森下　哲朗	上智大学法科大学院教授
	小出　篤	学習院大学法学部教授
	松尾　元信	金融庁総務企画局参事官
	小林　寿太郎	金融情報システムセンター企画部長
	永沢　裕美子	Foster Forum良質な金融商品を育てる会事務局長
オブザーバー	岩下　直行	日本銀行決済機構局審議役FinTechセンター長
	鎌田　沢一郎	日本証券業協会政策本部参与
	中野　征治	日本クレジットカード協会／ユーシーカード（株）事業開発部長
事務局	一般社団法人全国銀行協会	

（敬称略）

開催概要

当検討会では、事務局説明のほか、関係者・有識者からのヒアリングを行った。各回における開催概要は以下のとおりである。なお、各会合の模様については、一般社団法人全国銀行協会のウェブサイトにおいて議事要旨を公表している。

2016 年 11 月２日 第１回検討会
- 事務局説明「検討会設置の趣旨と論点メモについて」
- 事務局説明「全銀協アンケート調査の結果について」
- 事務局説明「英国“The Open Banking Standard”の概要」
- FinTech 協会「オープン API と協働で日本の FinTech 企業及び金融機関が新しい市場を作っていく」

2016 年 12 月５日 第２回検討会
- 事務局説明「セキュリティ原則、利用者保護原則の論点骨子（案）」
- FinTech 協会「更新系 API を利用した時のリスクについての検討」
- FISC「『金融機関における FinTech に関する有識者検討会』について」
- NTT データ「PSD2 におけるセキュリティ関連ルールのご紹介」

2016 年 12 月８日 第３回検討会
- 事務局説明「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方（叩き台）」
- 日本銀行金融研究所情報技術研究センター　中村啓佑様
  「金融分野の TPPs と API のオープン化：セキュリティ上の留意点」

2016 年 12 月 16 日 第４回検討会
- 事務局説明「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方（修正案）」
- 事務局説明「前回会合におけるコメントを踏まえた修正とその考え方について」

2016 年 12 月 21 日 第５回検討会
- 事務局説明「オープン API におけるセキュリティ対策及び利用者保護に関する基本的な考え方（案）」
- ｲﾝﾌｷｭﾘｵﾝ・ｸﾞﾙｰﾌﾟ「セキュリティ原則・利用者保護原則（案）に対するコメント」
- Moneytree「セキュリティ原則・利用者保護原則（案）に対するコメント」
- マネーフォワード「セキュリティ原則・利用者保護原則（案）に対するコメント」
- freee「セキュリティ原則・利用者保護原則（案）に対するコメント」
- Zaim「セキュリティ原則・利用者保護原則（案）に対するコメント」
- W3C「W3C Web API 標準化動向」

2017 年２月２日 第６回検討会
・ NTT データ「ANSER におけるオープン API の取組みのご紹介」
・ 日本アイ・ビー・エム「銀行 API 標準についての考え方」
・ 日立製作所「オープン API の標準化に関するご検討参考資料」
・ FinTech 協会「銀行のオープン API の仕様に対する Fintech 企業の要望」

2017 年２月８日 第７回検討会
・ 事務局説明「【討議資料】API の仕様の標準化について（案）」
・ OpenID Foundation「Financial Grade OAuth & OpenID Connect」

2017 年２月 20 日 第８回検討会
・ 事務局説明「オープン API のあり方に関する検討会報告書【中間的な整理（案）】」
・ 日本アイ・ビー・エム「海外の行政での API の利用事例や検討状況について」

2017 年２月 27 日 第９回検討会
・ 事務局説明「オープン API のあり方に関する検討会報告書【中間的な整理（案）】」
・ 金融 ISAC「金融 ISAC FinTech セキュリティ WG について」

各回において、有益な示唆の提供やプレゼンテーションにご協力いただいた関係者の皆様には、この場を借りて、深く感謝申しあげる。

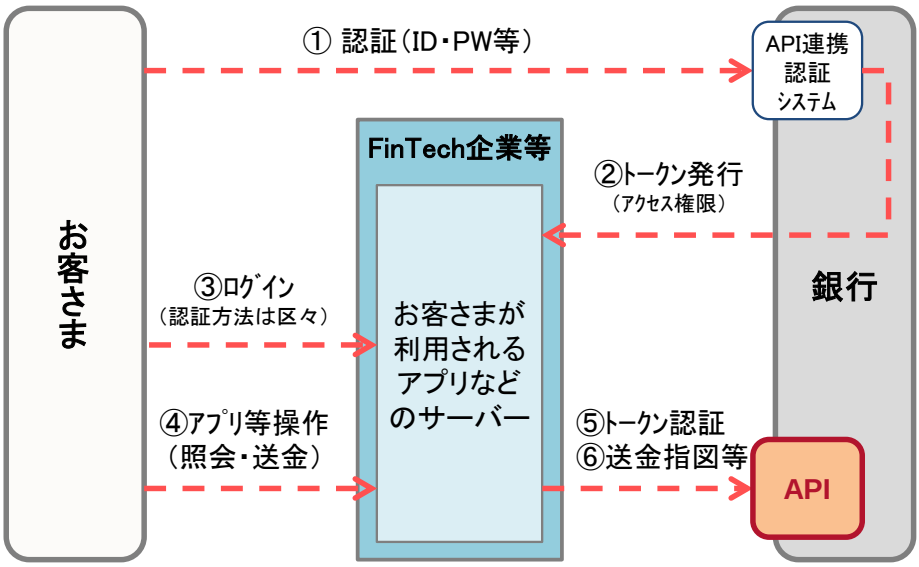
1. はじめに

1.1 本報告書の目的

・ IT の進展が金融業のあり方を大きく変容させていくことが見込まれる中で、オープン・イノベーションは、今後の金融機関における基本的な戦略の一つであると考えられる。

・ オープン API は、他の事業者等[3]とのオープンネットワーク上でのセキュアなデータ連携を可能とする技術であるが、単なるデータ連携上の意義を超えて、他の事業者等と金融機関が協働して、それぞれの保有する情報やサービスを組み合わせ、あるいはお互いに知恵を絞り、オープン・イノベーションを実現していくためのキー・テクノロジーの一つと位置づけられる。

【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。

・ 諸外国においては、英国“Open Banking Standard”をはじめ、API 仕様の標準化に関する検討、API の活用を促進していくうえでの課題への対応、利用者保護を図りつつオープン API を推進していくための法整備等について、官民連携した取組みが進展している。

・ こうした状況を踏まえ、当検討会は、わが国金融サービスの高度化、利用者利

[3] なお、オープン API を通じて銀行が協業する相手方としては、IT ベンチャー等の所謂 FinTech 企業のほか、流通小売業、サービス業等の事業会社等も考えられる（以下、FinTech 企業等）。

便の向上等を実現するためのオープン API 活用促進に向けた官民連携のイニシアティブとして、銀行分野におけるオープン API（バンキング API）のあり方について検討を行った。

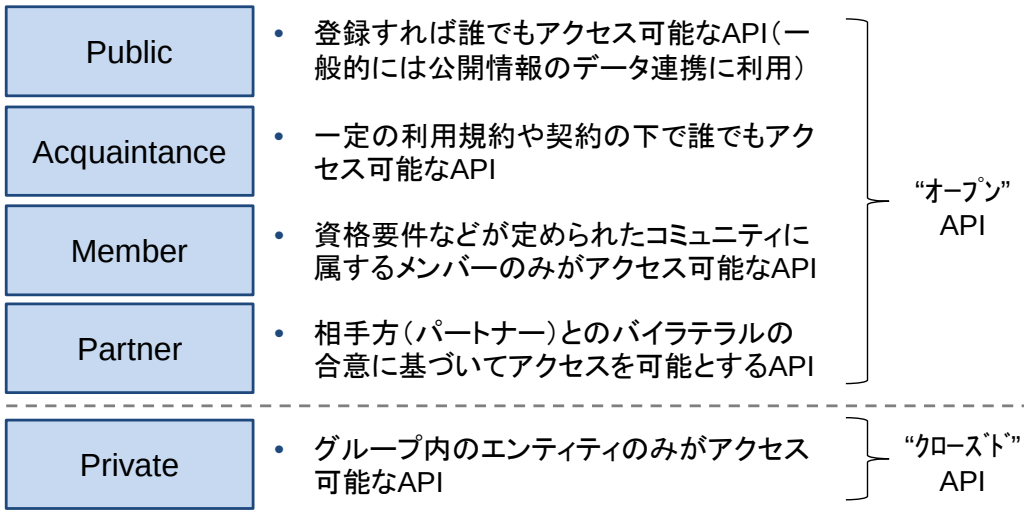
・ 本報告書は、銀行界、IT 事業者、FinTech 企業、学識経験者、弁護士、消費者団体、関係当局等の幅広い関係者をメンバーとして議論した結果としての「規範」と位置付けられるものであり、当検討会は、オープン API に取り組む関係者において本報告書が十分に尊重されることを期待する。

1.2 各提言の適用範囲

・ 本報告書は、銀行分野におけるオープン API（バンキング API）を対象とする。ただし、他業態におけるオープン API に関する取組みにおいて、本報告書を参考にすることを妨げるものではない。また、API の接続先企業等が銀行の銀行代理業者または外部委託先に該当しない場合について記載している[4]。

・ 各銀行におけるオープン API の開放度の類型（Openness）には、一般に以下四つの類型が想定されるが、本報告書における各提言はこのいずれも対象とする。

【図表２】オープン API の開放度の類型（Openness）



（資料）Euro Banking Association “Understanding the business relevance of Open APIs and Open Banking for banks”, May 2016 にもとづき作成

[4] 銀行代理業者または外部委託先に該当する場合においても、本報告書を参考にすることを妨げるものではないが、銀行代理業者または外部委託先に該当する場合、本報告書に優先して、銀行法にもとづく各種の利用者保護規定が適用されることに留意すること。

2. API 仕様の標準化について

2.1 基本的な考え方

a API の仕様は、①セキュリティ水準の確保および利用者保護を図るうえでも、②金融機関と FinTech 企業等の協働・連携を通じたオープン・イノベーションの促進を図るうえでも、重要な論点である。

- API の仕様は、本来、API での連携を目指す銀行と FinTech 企業等とが互いに協議して定められる。また、仕様の汎用性や拡張性も基本的には各銀行の戦略等にもとづいて設計される。もっとも、仕様の決定に際しては互いに技術的な優劣のない複数の選択肢の中から一つを選択する局面も多く、標準や目安のない状況下においては、銀行間で仕様が細分化していく可能性がある。

- 銀行と FinTech 企業等との N 対 N 型の接続を容易とし、オープン・イノベーションの促進を図る観点からは、仕様に関して一定の標準や目安を定め、できるだけ共通の仕様の下で接続できる環境を整備することが望ましい [5]。また、仕様の標準や目安を定めることは、各銀行の開発コストや、銀行と FinTech 企業等との間のコミュニケーションコストを低減することにも寄与する。

- セキュリティ水準の確保および利用者保護を図るうえでも、API が満たすべき基本的な仕様について定めることが必要である。

b 一方、これらの課題に対処する API の標準的な仕様を検討するうえでは、以下の点にも留意が必要である。

- API を構成するプログラムを金融機関間で共通化（標準化）した場合、当該プログラムに脆弱性が発見されると、その影響が数多くの金融機関に及ぶ可能性があるとの指摘もある [6]。

- 完全かつ詳細な API に係る仕様の標準を定めることとした場合、当該標準が定められるまでの間、関係者における API の開発が中断される可能性があるほか、各銀行の API の仕様が当該標準に収束し、わが国において実現可能な FinTech サービスの範囲が当該標準仕様の制約を受け、却ってオープン・イノベーションの実現・円滑化を妨げるおそれがある。

- 諸外国でも API 仕様の標準化に向けた動きが存在するものの [7]、現段階では

[5] 全銀協アンケート調査（2016 年 6 月～7 月、有効回答 99 行／正会員 120 行）でも、会員各行から仕様の標準化や共通規格の策定に係る要望が多数寄せられた。

[6] 日本銀行金融研究所・中村啓佑（2016）「金融分野の TPPs と API のオープン化：セキュリティ上の留意点」（11 頁）を参照。こうした点を踏まえ、同レポートでは、「標準化の対象は、データ記述言語やアーキテクチャ・スタイル、関数名やリターン値等に限定し、個別のプログラムについては、各金融機関が独自に作成、管理する方が望ましい」と指摘。

[7] 例えば、英国 Open Banking Standard(2016)では、API の仕様（7a.4 API Standards）、データの定

具体的な仕様が定まっておらず、わが国銀行と外国 FinTech 企業等との接続の円滑化等も視野に入れた標準的な API の仕様のあり方は、見定めにくい状況にある。

c　当検討会は、これらの点を踏まえ、関係者における当面の API 開発上の指針として、関係者が API を開発するに当たって留意すべき「2.2 開発原則」、推奨される API の基本的な仕様を定める「2.3 開発標準」、電文メッセージの標準的な項目やその定義等の目安を定める「2.4 電文仕様標準」、の三点（以下、指針）について取りまとめることとした[8]。

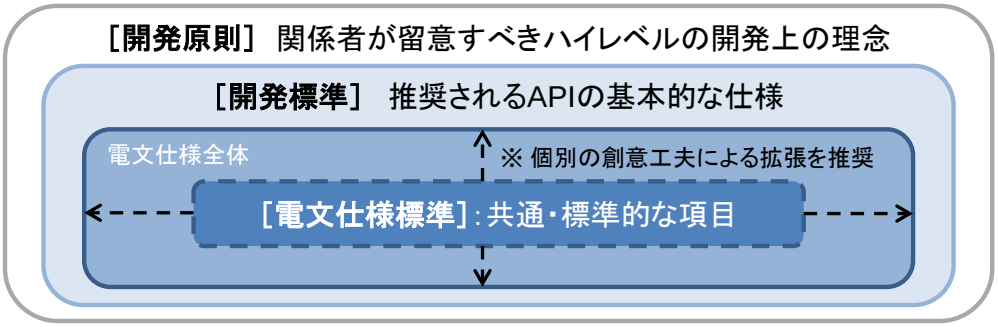
d　指針の取りまとめに当たっては、イノベーションの進展や関係者における先行的な取組みを阻害しないよう、各指針の目的、位置付けに留意するとともに（各章冒頭を参照）、関係者の判断による個別のカスタマイズや技術進歩への対応、新たな技術の採用にもできる限り柔軟に対応可能なものとすることを意識した。

e　本指針は、API 連携を目指す銀行と FinTech 企業等が個別に協議して仕様を検討することや各銀行におけるオープン API に係る戦略等を踏まえた仕様の汎用性や拡張性を確保する取組みを妨げるものではなく、むしろこれらの取組みは積極的に推奨される。

f　なお、本報告書の討議過程においては、複数の FinTech 企業から、各銀行の開発する API の詳細仕様についての期待も数多く寄せられた。これらは、各銀行が API の仕様を検討するうえで、参考になる部分も多いと考えられることから、末尾（2.5 その他）に参考として掲載している。これらの期待・要望の指針上の取扱いについては、本指針の改訂等を行う際、必要に応じて引続き検討する。

g　当検討会は、本報告書が、関係者における API 開発上の指針として参照され[9]、わが国におけるオープン・イノベーションの活性化に寄与することを期待する。

【図表３】開発原則、開発標準、電文仕様標準の関係



義や範囲（7a.8 Data Standards）の標準化に向けた方針が打ち出されているが、現段階ではアーキテクチャ・スタイルやデータ表現形式等の大枠を定めるのみとなっている。

[8] なお、アクセス権限の付与や個々の取引に係る認証方式、アクセス権限／トークンの管理、トークンの有効期限、通信方式、不正アクセス発生時の対応等に関する仕様については、「3.セキュリティ対策および利用者保護について」を参照。

[9] 銀行以外の事業者がオープン API に取り組む場合にも本指針が参考になることを期待する。

2.2 開発原則

2.2.1 開発原則の目的と位置付け

a 「開発原則」は、関係者が API を開発・仕様決定するに当たり、留意すべきハイレベルの開発上の理念を定めるものである。

b オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、様々なビジネスモデルやサービスの提供が期待される。個々の銀行と FinTech 企業等とが個別に協業・連携して検討する革新的な金融サービスを含め、その全てに対応する標準仕様を定めることは困難かつ適当ではなく、本報告書でもそれを目的としていない。

c 他方、オープン API は、銀行システムへの接続仕様等を他の事業者等に公開するものであり、基本的に自行のみがユーザーとなる銀行システムと異なり、API の種類に拘らず、ユーザーとなる他の事業者等を意識したオープンな設計思想が求められる。

d 「開発原則」は、かかる観点から、関係者が API を開発・仕様決定するに当たり、留意すべき開発上の理念を示すことで、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。

e 「開発原則」には、API を開発する関係者において既に実践されているものも含まれており、新たに API を開発しようとする関係者において参考となる有益な取組み事例については、可能な範囲で紹介している。なお、これらは 2017 年３月現在のものである。

2.2.2 開発原則

【原則１】API 利用者目線を意識した分かりやすくシンプルな設計・記述とすること

a オープン API は、他の事業者等による利用を前提とするものであり、API 利用者目線を意識したわかりやすくシンプルな設計・記述とすることが求められる [10]。かかる設計・記述は、API 利用者側でのバグの発生リスクの抑制や複数銀行と接続する FinTech サービスにおける銀行間の仕様差異の調整の容易化、銀行が他の事業者等と連携する際の API の汎用性、拡張性の確保にも資する。

b 設計・記述に当たっては、API 接続候補先等の事業者等ともよく協議・連携することが望ましい [11]。また、API の仕様決定後は、接続相手方が関係する部分の仕様について自行特有の用語や金融業界特有の略語等を使用しない平易な解説書（仕様書）を準備する等によって、API の仕様に対する接続相手方の誤解・誤認等を防止することが推奨される。

---

[10] 不必要に複雑かつ特殊な仕様とすることは原則として回避することが望ましい。一般に、API 利用者によって使い易い API とは、API の裏側にある銀行システム等の仕様等を理解しなくとも、API 利用者が API の仕様を理解し、利用可能な API とされる。

[11] ただし、接続相手方の要望を一方的に受け入れることを求めるものではない。

c　シンプルな設計・記述とすることは、実際のサービスに必要な項目のみを抽出のうえ提供する等の対応を意味し、メッセージ上の項目数の削減のみを目的に種類・性質の異なる複数の項目を結合・統合する等の対応を意味しない。一般に、統合された項目を分離して接続相手方がシステムに取り込むよりも、分離された項目を接続相手方において統合する方が、接続相手方のシステム設計がシンプルかつ汎用性の高いものとなる[12]。

d　API 利用者目線を意識した分かりやすくシンプルな設計・記述として、オープン API に先行的に取り組む関係者においては、例えば以下の取組み事例がある[13]。

（例）・ URI に API の機能が判別できる名称を設定している。URI を、可読性が高く、修正が容易な記述としている。
・ URI の表記ルールを自行内で統一し、表記内容には一般的に利用されている（意味がわかりやすい）名詞を採用している。
・ データを接続相手方から指定できる仕様としている（指定された情報以外の全ての情報を応答するような仕様としない）。
・ エラー原因を接続相手方が判別できるよう詳細情報も応答する仕様としている。

【原則２】API の種類に応じた適切なセキュリティレベルを確保すること

a　バンキング API では、銀行の保有する秘匿性の高い情報が提供されるため、API の種類に応じた適切なセキュリティレベルを確保することが必要である。認証方式、通信方式等を含めた、具体的なセキュリティ対策やその水準については、「3.セキュリティ対策および利用者保護について」を参照のこと。

b　セキュリティレベルを確保するうえでは、提供する各 API のスコープ（機能）を適切な粒度とし、接続相手方が認可された権限以上の API を使用できないようにすることが必要である[14]。

c　サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているため、API のセキュリティ対策および水準は、接続相手方とも連携のうえ、継続的な改善・見直し、高度化を図っていくことが必要である[15]。

d　API の仕様書を一般に公開する場合、セキュリティに及ぼす影響について留意することが必要である。

e　API のセキュリティ水準を確保する観点から、オープン API に先行的に取り組む関係者においては、例えば以下の取組み事例がある。

（例）・ 接続相手方と銀行間の通信経路について、BCP195 に従い TLS を使用

[12] 討議過程において、当検討会メンバーである FinTech 協会からは、「電文の粒度は細かければ細かい方が良い」との見解が示されている。
[13] 開発中の API における取組み事例を含む。以下、本章において同じ。
[14] 「3.セキュリティ対策および利用者保護について」の「アクセス権限／トークンの管理」も参照。
[15] 同上「3.3.5 セキュリティ対策の継続的な改善・見直し、高度化」も参照。

して暗号化、保護している。
・ XSS、XSRF 等の一般的なセキュリティ対策に加え、JSON ハイジャック[16]等の API 特有の脆弱性にも十分な対策を講じている。
・ API 実行回数の制限や制限値を超えた要求が行われた場合のエラー対応等の対策をとっている。
・ ユーザーが意図しない API 操作が実行された場合を想定して、トークンのリボーク（失効）機能を実装している。
・ 取引番号や接続相手方の特定番号等、取引を特定するための識別子を導入している。

【原則３】デファクトスタンダードや諸外国の API 標準、国際標準規格との整合性を意識すること

a 参照可能な国際標準規格等が存在する場合は可能な限り使用することが推奨される。例えば、日付や時刻の表現形式には RFC3339 や ISO8601/JISX0301、通貨コードの表現形式には ISO4217 といった標準がある。また、2017 年３月現在、文字コードは UTF-8 が実質的なデファクトスタンダードとなっている。

b アーキテクチャ・スタイルやデータ表現形式、認可プロトコル等の仕様については、デファクトスタンダードや諸外国の API 標準、国際標準規格等との整合性を踏まえ、「2.3 開発標準」において推奨される基本的な仕様を定めている。

c デファクトスタンダード等との整合性を意識した対応として、オープン API に先行的に取り組む関係者においては、例えば以下の取組み事例がある。

（例）・ 仕様の決定に当たっては、諸外国を含む他行の API の仕様を調査のうえ、整合性を意識した設計としている。
・ ステータスコードを含め標準化されている HTTP の仕様を最大限利用し、独自仕様の利用を最小限とするよう努めている。

【原則４】仕様変更による API 利用者への影響をコントロールすること

a API の仕様変更は、ユーザーである接続相手方でもプログラム変更等の影響が生じることから、影響を適切にコントロールすることが必要である。バンキング API は、金融・決済システムの一部として機能する可能性があるため、仕様変更によって接続相手方が突然接続不能となった場合、接続相手方のサービスを利用する多くの利用者（預金者）に影響・混乱が生じるおそれがある。

b 仕様変更による接続相手方への影響を抑制するため、API は、予めできるだけ汎用性、拡張性の高い設計とし、また、仕様変更が発生する可能性（機能追加、停止、バグ修正、データ形式の変更等）をできるだけ予め考慮した設計とすることが望ましい。これらは、各銀行における API の仕様変更コストを低減することにも資する。

c 一方的な仕様変更によって接続相手方に混乱が生じないよう、仕様変更に当た

[16] API から JSON により送られてくる情報を悪意ある第三者が盗み取る行為。

っては、原則として十分な余裕をもって事前のアナウンスを行うことが必要である。また、新バージョン移行後も新旧バージョンを一定期間並行稼働させる、旧仕様を包含した新バージョンをリリースする等の対応も推奨される。

d　パートナー型のオープン API の場合、通常、銀行側から API 連携先を特定することが可能であるため、事前アナウンス等は比較的容易であるが、公開情報等をパブリック型のオープン API を通じて提供する場合等では、銀行側から API 利用者を特定できない場合がある。また、パートナー型のオープン API であっても、銀行への通知なく API の連鎖を許容している場合は[17]、仕様変更の影響範囲を銀行側で十分把握できない場合がある。このため、仕様変更に当たっては、影響範囲を十分慎重に見極めたうえで進めることが重要である。

e　推奨される具体的なバージョン管理の方法については、「2.3 開発標準」において定めている。

f　仕様変更による API 利用者への影響をコントロールするため、オープン API に先行的に取り組む関係者においては、例えば以下の取組み事例がある。

（例）・ 開発ポータルを準備し、新バージョンリリース前に接続相手方がテストを行える環境を整備している。
・ 仕様変更を行った場合でも後方互換性をできる限り確保できるような設計を予め行っている。

2.3 開発標準

2.3.1 開発標準の目的と位置付け

a　「開発標準」は、推奨される API の基本的な仕様を定めるものである。具体的には、①アーキテクチャ・スタイル、②データ表現形式、③認可プロトコル、④バージョン管理の四点について推奨される仕様を示す。

b　「開発標準」は、関係者が API の基本的な仕様を選択する際の目安となり、仕様の乱立による社会的コストを低減し、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。

c　「開発標準」への準拠は、各銀行において検討・判断される[18]。接続相手方との協議やサービスの特性等に応じて、親和性の高い適切な仕様が選択されることが重要である[19]。

---

[17] 「3.セキュリティ対策および利用者保護について」の「API 接続先の API 接続先の取扱い」を参照。

[18] 「開発標準」は標準（Standard）であり、規則（Regulation）ではない。なお、「開発標準」に準拠しようとする銀行のうち、先行して API を開発済の銀行においては、バージョンアップやリプレイス等のタイミングで準拠を目指すといった様々な取組みが考えられる。

[19] 「開発標準」は、N 対 N 型の接続を前提として、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としており、相対型の接続（1 対 1 型）や中央管理インフラ型の接続（1 対 N）の接続を前提とする API では、その業務の特性や提供するサービスの内容

d 「開発標準」において推奨される基本的な仕様は、「2.2 開発原則」にもとづいて、2017 年３月現在、諸外国を含めた API 利用者から支持されている仕様や、諸外国における標準（例：英国 Open Banking Standard）等との整合性を踏まえて定められている。

e 当検討会は、「開発標準」が将来的な技術革新等に伴って陳腐化するリスクについても認識している。「開発標準」は、今後の技術革新の動向を踏まえ、必要に応じて見直すこととする。なお、「開発標準」の改訂は、一般社団法人全国銀行協会が事務局となって、銀行界、IT 事業者、FinTech 企業等の各関係者の意見を参考にしつつ行うものとする。

f 「開発標準」は、各銀行における、推奨された仕様以外の先進的な仕様や技術の採用を妨げるものではない。特に、セキュリティに関連する仕様については、より強固なセキュリティ水準を確保可能な最新の仕様があれば、同仕様を採用することが推奨される。

2.3.2 開発標準（2017 年３月現在）

a 「アーキテクチャ・スタイル」として、REST[20]を、「通信プロトコル」には HTTPs の使用を推奨する。REST は、Richardson Maturity Model [21] Level2（GET/POST/PUT/DELETE 等の HTTP 動詞の導入）を充足する設計とすることを推奨する [22]。これらは、2017 年３月現在、API における主流の仕様である。

b 「データ表現形式」として、JSON[23]を推奨する。REST では、JSON、XML 等の様々なデータ表現形式の利用が可能であるが、JSON は簡素かつ軽量に構造化したデータを記述可能であるため、2017 年３月現在、新たに開発される API においては JSON が主流となっている。

c 「認可プロトコル」として、OAuth2.0[24]を推奨する。なお、OAuth2.0 は、2017 年３月現在、OpenID Foundation Financial API WG(FAPI WG)において、金融分野における API のセキュリティ水準を確保する観点から、詳細仕様の標準化が検討されている。同団体で OAuth2.0 の標準仕様が定められた場合には、各銀行において同仕様への準拠や準拠に向けた方針等が検討されることが望ましい [25]。

に応じて異なる仕様を採用することも考えられる。例えば、XML 形式も技術標準として確立されている。加えて、2017 年３月現在、W3C（World Wide Web Consortium。ウェブ上で使用される各種技術の標準化を推進する非営利団体）においては、決済指図を利用者が使用するブラウザ等を用いて直接銀行に送信する仕組み（Payment Request API）も検討されている。

[20] Representational State Transfer の略。ソフトウェアがデータを連携するための設計原則の一つ。

[21] https://martinfowler.com/articles/richardsonMaturityModel.html を参照。

[22] なお、Richardson Maturity Model では、Level3（HATEOAS : hypermedia as the engine of application state）の設計レベルも定められているが、2017 年３月現在、必ずしも広く普及していないため、本開発原則の設計レベルとしては採用しない。

[23] JavaScript Object Notation の略。RFC7159 で規定される軽量なデータ記述言語。

[24] https://oauth.net/を参照。

[25] 準拠しない場合は、その合理性・許容性についての検討を含む。

d 「バージョン管理」として、セマンティック・バージョニング [26]を推奨する。仕様変更による API 利用者への影響をコントロールする観点から、メジャー、マイナー、パッチ等の区分を用いて仕様変更レベルを管理する。

2.4 電文仕様標準

2.4.1 電文仕様標準の目的と位置付け

a 「電文仕様標準」は、API のメッセージ上の標準的な項目やその定義等の目安を定めるものである [27]。

b 「電文仕様標準」のあり方には、以下、複数の選択肢が考えられる。

i. 電文の構造、項目、Value（値）、パラメータを含む、そのまま実装しても動作する完全かつ詳細な電文仕様の標準を定める方法。（例 : 全銀協 IC キャッシュカード標準仕様 [28]）

ii. API のメッセージ上の標準的な項目およびその定義等についてのみ定め、それ以外の仕様は、API での連携を目指す銀行と FinTech 企業等とが互いに協議のうえ任意に拡張して定めることを前提とする方法。（例：英国 Open Banking Standard[29]）

iii. 電文仕様の標準化は行わず、デファクトスタンダードの確立に委ねる方法。（例 : 一般事業者や FinTech 企業等が開放する Web API の仕様等もこれに相当する）

c 上記いずれの選択肢にも一長一短があるが、当検討会では、①完全かつ詳細な電文仕様を定める社会的コスト（標準の策定・維持・改訂コスト、イノベーションがむしろ阻害されるコスト、等）、②デファクトスタンダードの確立に委ねる社会的コスト（確立されるまでの間、仕様が細分化するコスト、定義に一貫性のないデータの流通によって、FinTech サービスにおいて加工、集計／統合が困難化するコスト、利用者に誤認等が生じるコスト、等）に鑑み [30]、当面の対

---

[26] http://semver.org/を参照。

[27] なお、OAuth2.0 の詳細仕様等については、2017 年 3 月現在、OpenID Foundation Financial API WG(FAPI WG)において標準化に向けた検討が行われているため、本章では、API 連携サービスに関する電文仕様についてのみ定める。

[28] なお、全銀協 IC キャッシュカード標準仕様は、セキュリティ上の観点から、利用条件を定め、一般社団法人全国銀行協会が許可した相手方に限り仕様書を提示している。

[29] 英国 Open Banking Standard(2016)では、仕様の標準化に関して、イノベーションと安定性のバランスの観点から、全ての業務分野に共通するリソースである“Core”（簡単には変更されない部分）について標準を定め、それ以外の仕様については、関係者が自由に分岐・拡張可能なアプローチが採用されている（7a.2.1 節参照）。ただし、2017 年 3 月現在、Core に関する標準は決定・公表されていない。

[30] わが国では、地域金融機関を中心として特定の IT 事業者が開発した共通システムを共同利用しているケースが多いこと、かかる共通システムでは、各 IT 事業者の努力によって共通システム単位で仕様の標準化が行われていることから、完全かつ詳細な電文仕様の標準を定めなくとも、過度な仕様の細分化が生じにくいことも考慮した。

応として、ii の方法で標準化を行うこととした。

d　「電文仕様標準」は、FinTech サービスにおいて使用される基本的な項目やデータについて、定義の一貫性を確保し、接続相手方において加工、集計／統合を容易化するとともに、利用者の誤認を防止し、もってオープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。

e　「電文仕様標準」への準拠は、「2.3 開発標準」と同様、各銀行において検討・判断される[31]。また、最終的な仕様は、電文仕様標準に機械的に準拠するのではなく、API の汎用性、拡張性も十分考慮するとともに、接続相手方との協議やサービスの特性等を踏まえて、決定されることが重要である。

f　当検討会は、「電文仕様標準」が将来的な技術革新等に伴って陳腐化するリスクについても認識している。「電文仕様標準」は、今後の技術革新等の動向を踏まえ、必要に応じて見直すこととする。なお、「電文仕様標準」の改訂は、一般社団法人全国銀行協会が事務局となって、銀行界、IT 事業者、FinTech 企業等の各関係者の意見を参考にしつつ行うものとする。

2.4.2　電文仕様標準のあり方について

a　「電文仕様標準」の策定は、一般社団法人全国銀行協会が事務局となって、銀行界、IT 事業者、FinTech 企業等の各関係者の意見も参考にしつつ進める。

b　当検討会は、「電文仕様標準」の策定に当たって、関係者に対して以下の点に留意することを要請する。

- 「電文仕様標準」を策定する対象範囲は、複数の銀行、複数の FinTech 企業等との接続を前提とする（すなわち銀行間で共通の）API とし、当面の対象としては、預金に係る、①残高照会、②入出金明細照会、③振込[32]とすること。

- 特に残高照会および入出金明細照会については、2017 年３月現在、一部の FinTech 企業等において、預金者のインターネット・バンキングのログイン ID／パスワード等の重要な認証情報を利用したスクレイピングが活用されている状況に鑑み、API への円滑なシフトを可能とする観点から、速やかに標準の策定に向けた検討を進めることが期待される。

- 「電文仕様標準」の内容は、①応答メッセージに記述する共通項目（含む項目粒度）、②当該共通項目の定義、③パラメータの記述ルール（複数許容する場合はそのパターン）を軸に検討を進めること。

- 「電文仕様標準」の策定に当たっては、「2.2 開発原則」に従うとともに、各銀行による拡張を前提とし、また関係者における API 連携に向けた先行的な

[31] 「電文仕様標準」は標準（Standard）であり、規則（Regulation）ではない。なお、「電文仕様標準」に準拠しようとする銀行のうち、先行して API を開発済の銀行においては、バージョンアップやリプレイス等のタイミングで準拠を目指すといった様々な取組みが考えられる。
[32] 同一銀行内の振替は除く。

取組みを阻害しないよう、標準の位置付け、範囲に留意すること。

- 策定した「電文仕様標準」は、関係者が広く参照し、自由に利用できるよう公表すること。
- その他の点については、銀行界、IT 事業者、FinTech 企業等の各関係者の意見を参考に進めること。

2.5 その他

a 本報告書の討議過程において、検討会メンバーである複数の FinTech 企業から、各銀行の開発する API の詳細仕様についての期待も数多く寄せられた。これらは、各銀行が API の仕様を検討するうえで、参考になる部分も多いと考えられることから、以下に示す[33]。

b これらの期待・要望の指針上の取扱いについては、本指針の改訂等を行う際、必要に応じて引続き検討する。

（参考）API の詳細仕様に対する FinTech 企業の期待（例）[34]

接続仕様について

- ✓ インターネット・バンキング契約のない顧客でも API の利用を可能とするほか、インターネット・バンキングの対象業務に限定せず広く消費者ニーズを探ることが、金融包摂や金融サービス業のパイ拡大の観点で重要であり、インターネット・バンキングを前提に API を設計しないでほしい[35]。
- ✓ 現在、日本において提供されている API の多くはインターネット・バンキング経由で提供されるため、インターネット・バンキングの契約番号およびパスワードが認証情報になっているケースが多いが、それ以外の非対面取引をする際の認証方法の採用も検討してほしい[36]。
- ✓ 参照系 API には、接続相手方が銀行の情報を「取得しに行く」フェッチ型と、銀行の API が接続先に情報を「伝えにいく」プッシュ型の２種類がある。「フェッチ型」だけでなく、「プッシュ型」の API 導入の期待も大きく、特に、法人取引については、EDI・XML の API 化伴い顧客企業の業務効率化につながることが想定される。

認可仕様とスコープ

- ✓ 認可内容は程よいスコープ定義としてほしい。あまり細かいと、利用者がスクロールして読まないことや、連携される権限の量だけで漠然と不安を感じる利用者もいると懸念される。

電文仕様について

[33] なお、各指針に反映したものは除外して掲載している。
[34] 2017 年３月現在のもの。
[35] なお、本報告書では、インターネット・バンキングを前提としない仕様についても許容している（例えば、「3.セキュリティ対策および利用者保護について」の「アクセス権限の付与に係る認証」を参照）。
[36] 同上。

- ✓ バッチやオフラインの業務も入ることによって API で取得する情報はリアルタイムではない可能性があるため、「〇〇現在」という属性情報も実装してほしい。なお、API 提供側システムの処理負荷軽減のため、差分の明細等を取得する際は検索範囲の日時指定を必須化することは支障ない（新規および変更がある明細しか返されない仕様）。
- ✓ 日本の銀行の口座番号は、7 桁の口座番号でできているため、accountNumber のようなフィールドが設定されると、7 桁の数字にする仕様となり、API 利用者として大変ありがたい（例：0 で左詰めする）。
- ✓ API でも口座情報確認機能を付与することにより、未処理取引の削減や誤入金に伴う組戻しの回避等、API 提供者および顧客にメリットがあるのではないか。
- ✓ 顧客が振込結果を確認できることにより、API 提供者への照会が不要となる、または軽減されるのではないか。
- ✓ アクセス不可の場合等のステータスコードを統一し、コードのみでエラー内容を判別可とできないか。

その他

- ✓ API を一般に広く公開する場合は、Stub/Mock 環境は簡単に公開できるため、イノベーションの観点から見て良い。
- ✓ 本番移行後も、継続的に（期間を区切る等により）テスト環境へのアクセスが認められることを希望。FinTech 企業側で自らバージョンアップする時のテストは必須（API を介し影響を排除するとの前提で、API 利用者が独自にバージョンアップすることがある）。
- ✓ 各環境では、必要なテストケースを網羅できるだけのデータが提供されることを希望。

3. セキュリティ対策および利用者保護について

3.1 基本的な考え方

a 金融分野におけるオープン API の活用は、現在、世界的にも試行錯誤フェーズにあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者保護は、オープン API を活用したサービスに対する利用者の信頼を確保し、オープン API の普及、活用促進・円滑化を図るうえで、重要な論点である。

b オープン API では、利用者からの申請・同意にもとづいて行われるとはいえ、銀行が保有する秘匿性の高い顧客情報が FinTech 企業等の他の事業者等（以下、「API 接続先」）に提供され当該 API 接続先において蓄積・保存されるほか、銀行が決済指図等を利用者ではなく API 接続先を経由して受け取ることになる。それゆえ、オープン API に取り組むに当たっては、関係者において十分なセキュリティ対策、利用者保護が図られることが必要となる。

c 他方、API 接続先に対して、銀行と同水準のセキュリティ対策、利用者保護策を徒に求めれば、API 接続先と銀行の協働・連携による利便性の高い革新的なサービスの提供や金融サービスの高度化、イノベーションに向けた取組みが阻害され、利用者がテクノロジーの進展の恩恵を受ける機会を失うおそれがある。

d こうした認識の下、当検討会では、API の機能[37]や連携するデータの種類・秘匿性等に応じたリスクベース・アプローチにもとづいて、利用者利便と利用者保護のバランスを踏まえた、銀行分野のオープン API（バンキング API）におけるセキュリティ対策および利用者保護に関する基本的な考え方を取りまとめた。

e 取りまとめに当たっては、イノベーションを阻害しないよう留意するとともに、銀行、API 接続先双方に対して対応水準の目安を示すことで、銀行による API 接続先に対する過度に保守的なセキュリティ対策の要求や、セキュリティ上の懸念から生じる銀行側のオープン API への取組みに対する躊躇といった課題を解消し、銀行と FinTech 企業等の協業・連携の円滑化に資するものとすることを意識した。

f なお、先述のとおり、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、様々なビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本報告書では、様々なビジネスモデルやサービスに共通すると思われる主なリスクに対応したセキュリティ対策および利用者保護策に焦点をあてて取りまとめている。

[37] 例えば、更新系 API において、決済指図上限が定められていない場合、不正送金によって利用者に大きな損害が生じる可能性がある。

g　具体的なセキュリティ対策および利用者保護策については、各銀行のポリシーや、個別のビジネス、各サービスのリスク、API 接続先の態様等に応じて個々に判断されるものであり、利用者保護の観点から、関係当事者において本報告書の趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本報告書では挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。

h　以下では、オープン API において想定される主なリスクを整理したうえで、セキュリティ原則および利用者保護原則を示す[38]。

3.2　オープン API の主なリスク

オープン API では、金融機関のシステムに新たな通信路を設けて他の企業等を経由した新たなサービスを利用者（預金者）に提供することになるため、当該通信路を悪用したデータの漏洩・改竄や不正取引等が生じるリスクがある。これらオープン API において想定される主なリスクを列挙すれば､以下のとおり。

3.2.1　セキュリティ上の脅威とリスク

a　API 接続先のログイン ID／パスワード等が何らかの原因で漏洩し、第三者によって、API 接続先が不正にアクセスされるリスク

b　API 接続先のシステムが第三者から攻撃を受けて、API 接続先のサービス機能の停止や、API 接続先からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

c　トークン[39]の発行を管理する銀行側の API 連携システムが第三者によって不正に認証され、トークンが不正に取得されるリスク

d　トークンの流出や偽造等により、銀行からの大規模な情報流出、情報改竄／消失、不正送金等が発生するリスク

e　ルータ等の通信経路へのハッキング、無線通信等の傍受等により、情報流出、情報改竄／消失、不正送金等が発生するリスク

f　API 接続先のプログラム不備等により、銀行のシステムがダウンするリスク

---

[38] なお、セキュリティ原則および利用者保護原則の各規定の語尾の趣旨は以下のとおり。
- 「しなければならない」： 社会規範として強く求められる対応を意味する。
- 「必要である」： 銀行および API 接続先がオープン API を活用するに当たってのベストプラクティスとして期待される対応を意味する。
- 「努めなければならない」： その状態になるよう努力が期待される対応を意味する。
- 「考えられる」： 銀行または API 接続先が任意に選択可能な対応を意味する。
- 「期待される」： 対象となる機関や団体に対する当検討会の期待を意味する。

[39] OAuth2.0 において、銀行と他の企業等のアプリケーションを連携するための認証情報を保持した「許可証」。（以下同じ）

g　銀行のオープン API の通信路に不必要に大量のデータが送信され、銀行側システムの負荷が増加し、他の銀行サービスにも影響が生じるリスク

h　内部の役職員が利用者情報を不正に利用（転売、私的利用を含む）するリスク

i　内部の役職員が、トークンを不正に使用して、口座残高情報の不正取得や不正決済指図を行うリスク

3.2.2　利用者保護上のリスク

a　API 接続先の事業内容や社会的信用に疑義があり、API を利用したサービスによって、利用者に被害や混乱が生じるリスク

b　API 接続先の利用者保護態勢、経済的信用、資力等に疑義があり、利用者が十分な保護を受けられないリスク

c　API 接続先が利用者との緊急時の連絡方法を有しておらず、十分な顧客保護対応ができないリスク

d　利用者が、誰に何の権限を与えているのか、それにどのようなリスクがあるのか、API 接続先に取得される情報の利用目的は何か等について、十分に理解しないまま、API を活用したサービスを利用するリスク

e　トラブルが発生した場合に、利用者がどこに問い合わせたら良いかわからなくなるリスク

f　十分な説明、表示を尽くしても、利用者がよく読まずに手続きを行うリスク

g　API 接続先のシステムにおいて不具合、バグ等が発生し、銀行から提供された情報が正しく表示されないリスク

h　API 接続先と銀行間の通信経路に起因する障害により、利用者・API 接続先と銀行の間に取引の齟齬が発生するリスク

3.3　セキュリティ原則

3.3.1　API 接続先の適格性

（事前審査）

a　銀行は、他の事業者等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である [40]。なお、銀行が共通システムを通じて API 接続先と接続する場合については、銀行による API 接続先の審査結果にもとづき、共通システム提供事業者が API 接続先との接続を行うものとする。

[40] 情報セキュリティ以外の適格性については、「3.4.利用者保護原則」の「3.4.1 API 接続先の適格性」を参照。

b　セキュリティに関連した適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である [41]。

- セキュリティ原則の充足状況
- 過去に発生したセキュリティ関連の不祥事案と改善状況
- 利用者の属性や取引のリスクに応じた、継続的なセキュリティ対策の高度化に向けた態勢やリソースの有無

c　適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。

d　なお、API 接続先が任意に定めたセキュリティポリシーやセキュリティ関連文書、API 接続先が取得した情報セキュリティ関連の認証（ISO27001、TRUSTe、等）は、上記の適格性の審査に当たっての参考になると考えられる。

e　複数の銀行と API 接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」（仮称）を制定することが期待される [42]。

f　なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等における審査対応負担の軽減や銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる [43]。

（モニタリング）

g　銀行は、API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的にまたは必要に応じて確認することが必要である [44]。

h　モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行のセキュリティポリシー等に応じて、個別に判断されると考えられる。

i　銀行は、API 接続に当たって、API 接続先との間でモニタリングに関する事項

---

[41] API 接続先が ASP やクラウドサービスを利用している場合には、API 接続先から必要な開示が行われる必要があることに留意する。

[42] 必須確認項目については、却って API 接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。

[43] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

[44] API 接続先が定期的な情報セキュリティ関連の外部監査を受けている場合には、それらの結果を活用すること等も考えられる。

（例：方法、深度、頻度、必要に応じた立入検査等、情報セキュリティ対策の大幅な変更を行う場合の対応、等）を予め取り決めておくことが必要である。

j　銀行は、API 接続先の情報セキュリティに関連した適格性に懸念があると判断した場合には、API 接続先に対して改善を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[45]。

k　なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる[46]。

3.3.2　外部からの不正アクセス対策

b　以下は、アクセス権限の認可に OAuth2.0[47]を実装したシステムを前提とした記載。なお、同等のまたはより強固な認可・認証が可能な他のプロトコル（新たなテクノロジーを含む）の採用を妨げるものではない[48]。

（アクセス権限の付与に係る認証）

c　銀行は、公表情報または匿名加工情報を提供する場合を除き、API 接続先に対するアクセス権限の付与（OAuth2.0 においては「認可」）を利用者の申請にもとづき行うこととし、その際、利用者の本人認証を行わなければならない。

d　認証方式は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度とすることが必要である[49]。例えば、決済指図の権限を付与する場合には、残高・入出金明細を取得する権限を付与する場合と比較してより強固な認証方式とする等が考えられる。

e　認証方式の選択に当たっては、当該銀行において採用されている他のオープンネットワークを利用した取引チャネル（例：インターネット・バンキング）の認証方式の水準が一つの目安となり得るが、以下の点にも留意が必要である。

- 個々の取引に係る認証ではなく、アクセス権限の認可に係る認証であること
- API を通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不

---

[45] ただし、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。

[46] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

[47] アクセス権限の認可を行うためのシステムフローに関する規格。一般向けに公開されており、API 開発者は誰でも参照することが可能。IETF（Internet Engineering Task Force：インターネットで利用される技術の標準化を策定する組織）が管理・運営。

[48] API 仕様の標準化については、「2. API 仕様の標準化について」を参照。

[49] 各銀行の判断にもとづき、利用者保護の観点から、強固な認証方式を一律に採用することも妨げない。

正アクセスリスクに応じた認証強度とする必要があること

f　当該銀行において採用されている他のオープンネットワークを利用した取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には（例：インターネット・バンキング契約のない利用者を対象として暗証番号認証を許容する場合等）、不正アクセスリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。例えば、店頭手続・郵送確認等を併用する、資金移動上限を少額に制限する、トークンの有効期限を短期とする、不正使用発生時の補償を予め定める、等が考えられる。

g　その他の留意点については、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-8／Ⅱ-3-5：インターネット・バンキング）や「預金等受入金融機関に係る検査マニュアル（別紙２-Ⅲ-1-(5)インターネットを利用した取引の管理）」、金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準」、一般社団法人全国銀行協会の「インターネット・バンキングにおいて留意すべき事項について」等を参考にすることが考えられる。

（アクセス権限／トークンの管理）

h　銀行は、API 接続先に付与するアクセス権限（OAuth2.0 においては「トークン」が発行される）の管理について、以下の点に留意することが必要である。

- 付与するアクセス権限は、API 接続先が提供するサービスに必要な範囲に限定すること（利用者からの申請／同意があったとしても、不必要なアクセス権限を API 接続先に付与しないこと）
- API 接続先に発行するトークンには、利用者属性やアクセス権限の内容とそのリスク、利用者の利便性等を踏まえた適切な有効期限を設定すること
- アクセス権限の内容に応じたトークンの偽造・盗用対策を講じること
- 不正アクセス等を検知、または発生した場合に速やかにアクセス権限の制限、停止、取消が可能な仕組みとすること

i　銀行は、アクセス権限やトークンを管理するシステムに堅牢なセキュリティ対策を講じなければならない。また、API 接続先に対しても、トークンの適切な管理とセキュリティ対策を求めなければならない。

（個々の取引に係る認証）

j　利用者からの個々の取引指図（残高・入出金明細取得指図、決済指図、等）は、利用者が API 接続先のシステムにアクセスする際に API 接続先において行われる認証[50]と、銀行が個々の取引指図を API 接続先から受け付ける際に銀行にお

[50] ただし、API 接続先が NFC（Near Field Communication：近距離無線通信）技術を用いた物理媒体による決済サービスを提供する場合等については、API 接続先における個々の取引に係る認証は、物理媒体の所持・使用をもって行われることがある。

いて行われる認証の、二段階の認証を経て処理される。

k　利用者保護や不正アクセス／情報流出防止の観点からは、上記いずれの認証方式とも、利用者の口座保有銀行において採用されている他のオープンネットワークを利用した取引チャネルにおける個々の取引に係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であると考えられる。

l　例えば、法人利用者の口座保有銀行のインターネット・バンキングにおいて残高・入出金明細の確認に可変式パスワードや電子証明書等の固定式のログインID/パスワードのみに頼らない認証方式が採用されている場合、API 接続先、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となる[51]。

m　他方で、強固な認証方式の中には利用者に手続負担が大きいものや API 接続先の対応に大きな投資が必要なものもあるため、原則的な考え方を一律に適用すれば、利用者利便の大幅な低下や、利便性の高いサービスのフィージビリティが確保できなくなるおそれがあると考えられる。

n　このため、他の利用者保護策や不正アクセス／情報流出対策を組み合わせることで、利用者利便を確保しつつ、個人・法人等の利用者の属性や認証する取引のリスク等に見合った利用者保護の徹底を図っていくことも考えられる。組み合わせる他の利用者保護策や不正アクセス／情報流出対策としては、例えば以下の対策が考えられる。

- 資金移動指図に係る銀行側の認証方式をトークン認証に加えて帯域外認証も組み合わせ、その都度利用者を銀行側で直接認証する
- 生体認証や端末認証、複数経路認証等、一定の認証強度を確保しつつ、利便性が確保される認証方式を採用する
- 資金移動が行われた場合には、銀行または API 接続先から利用者に対して電子メール等で通知する
- 利用者がアクセス可能な端末をセキュリティが確保された特定の端末や特定の種類の端末に限定する
- 利用者と API 接続先間または API 接続先と銀行間あるいはその両方の通信方式を閉域ネットワークとする
- トークンの有効期限を短期に設定する（例えば、１回限りとする、１か月から数か月で失効させる等）
- 提供する情報の範囲や期間を制限する
- 資金移動上限を少額に制限する（例えば、１回あたりの資金移動上限を X 円、かつ簡易な認証方式にもとづく資金移動の累積上限を Y 円とする）
- 資金移動先口座を強固な認証手続によって登録された口座に限定する
- 資金移動先口座を同一銀行内の本人口座に限定する
- サービスを利用可能な利用者の属性を制限する（例えば、一定の属性要件を満たす個人に限る、法人に限る、系列企業や従業員に限る、等）

[51] 逆に、例えば、API 接続先の認証強度がインターネット・バンキング等と比較して劣後する場合、認証強度が脆弱な API 接続先が集中的に狙われて情報流出等が発生するリスクが高まることになる。

・ 不正送金、情報漏洩が発生した場合に銀行または API 接続先が利用者に対して被害額を補償する [52]
・ 利便性が高まる半面、認証強度が低下することによるリスクについて利用者の十分な理解と同意を得たうえでサービスを提供する
・ 銀行が利用者からの決済指図を API 接続先を経由せずに直接受け付ける [53]

o なお、上記の例を組み合わせれば即座に認証強度を引き下げることが可能になるわけではなく、採用する認証方式と上記の利用者保護策を組み合わせた後においても、個人・法人等の利用者の属性や認証する取引のリスクに見合った利用者保護が十分に確保されることが必要である。

（通信方式）

p 通信方式としてオープンネットワークを使用する場合、第三者による盗取等を防止する観点から、TLS を使用して保護することが必要である。

（システムの堅牢性）

q 銀行は、顧客情報について、商慣習または信義則にもとづく私法上の義務として守秘義務を負うほか、銀行法（13 条の 3 の 2：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／II-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル（別紙２）」、FISC が定める「金融機関等コンピュータシステムの安全対策基準」、全国銀行個人情報保護協議会が定める「個人情報保護指針」・「個人データの安全管理措置等に関する指針」等にもとづき、顧客の利益が不当に害されることのないよう当該業務に関する情報を適正に管理し、かつ当該業務の実施状況を適切に監視するための体制の整備その他必要な措置を講じることが求められている。また、態勢が不十分な場合は、銀行法にもとづく業務改善命令等の対象となる。

r 銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API では、外部委託と異なり、銀行から API 接続先への情報提供は利用者からの申請／同意にもとづくものであることや高い堅牢性が求められる銀行シス

[52] ただし、資金移動上限を定めない場合、被害は補償されても、反社会的勢力等に巨額の資金が盗取される可能性がある点には留意が必要。
[53] 2017 年３月現在、W3C（World Wide Web Consortium。ウェブ上で使用される各種技術の標準化を推進する非営利団体）においては、決済指図を利用者が使用するブラウザ等を用いて直接銀行に送信する仕組み（Payment Request API）も検討されている。

テムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。

s　API 接続先が確保すべき安全管理措置の水準は、API 接続先が取得・保有する情報の内容と量、情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。

t　API 接続先が確保すべき安全管理措置の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。ただし、最低限、API 接続先においても以下の措置は必要である。

- ウィルス対策ソフトの導入
- 機密性の高い情報（例：API 接続先のログインパスワードやクライアント証明書、トークン、等）の暗号化
- ファイアーウォール等のサイバー攻撃に対する多層防御の導入
- サーバ変更監視（改竄検知）、ネットワーク監視
- 公開サーバ脆弱性対策
- API 実行ログ（ユーザー、操作、結果、等）取得、保管
- 情報喪失等に備えたバックアップ等の対策

u　なお、API 接続先に、顧客の同意を得て銀行が提供する個人情報（個人データ）の個人情報保護法上の取扱いは、個別のスキームに応じて個々に判断されるべきものではあるが、原則的には銀行は API 接続先に対して、個人情報委託先の監督義務（同法第 22 条）を負っていないと解するのが適当と考えられる。

（不正検知・監視機能）

v　不正検知・監視機能は、不正アクセス被害の発生やその拡大を未然に防止するうえで重要な機能の一つである。

w　銀行については、FISC が定める「金融機関等コンピュータシステムの安全対策基準」において、データ改竄、不正アクセス、不正な取引、異常取引の検知・監視等に関する枠組みが定められている。

x　ただし、オープン API においては、利用者の IP アドレスや認証失敗回数等の不正検知に活用される情報を銀行が直接入手できなくなるため、取引のリスクに応じて、銀行が必要とする場合には、API 接続先から銀行に不正検知に必要な情報が提供される仕組みを構築することが必要である。

y　API 接続先についても、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、情報セキュリティ関連機関において、不正検知・監視機能の要否やその水準等についての考え方や留意点の整理が行われることが期待される。

3.3.3　内部からの不正アクセス対策

a　外部からの不正アクセス対策は、内部からの不正アクセスに対して効果を発揮しない場合がある。それゆえ、銀行、API 接続先の双方において内部からの不正アクセス対策が講じられることが必要である。

（銀行における内部不正対策）

b　銀行については、銀行法（13 条の３の２：顧客の利益の保護のための体制整備、等）、「金融分野における個人情報保護に関するガイドライン」、「主要行等／中小・地域金融機関向けの総合的な監督指針」（Ⅲ-3-3-3／II-3-2-3：顧客等に関する情報管理態勢、Ⅲ-3-7／Ⅱ-3-4：システムリスク、等）や「預金等受入金融機関に係る検査マニュアル（別紙２）」、FISC が定める「金融機関等コンピュータシステムの安全対策基準」等において、内部からの不正アクセス防止に関する枠組みが定められている。また、態勢が不十分な場合は、銀行法にもとづく業務改善命令等の対象となる。

（API 接続先における内部不正対策）

c　銀行が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出（役職員による私的な閲覧・利用、転売を含む）防止の観点から、API 接続先（特に複数銀行の大量の顧客情報を蓄積している PFM 事業者）においても、銀行と同水準のセキュリティ対策が講じられることが理想的であるものの、銀行業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、銀行法、監督指針、検査マニュアル等において定められている銀行の外部委託先に対するシステムリスク管理の考え方についても、参考になるものの、オープン API は、銀行システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用できるわけではないと考えられる。

d　API 接続先が確保すべき内部不正アクセス対策の水準は、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。

e　API 接続先が確保すべき内部不正アクセス対策の目安水準については、情報セキュリティ関連機関において、考え方や留意点の整理が行われることが期待される。ただし、最低限、以下の措置については API 接続先においても必要である。

- 役職員に対するシステムアクセス権限の適切な設定・運用
- アクセスログの記録保存、定期的な査閲
- 役職員に対する教育・研修の実施

- サーバルームの監視、認証、入退出管理[54]
- 重要な機密情報・顧客情報の媒体（USB）等へのデータのコピー制限、禁止
- 重要な機密情報・顧客情報のデータの持出、削除、廃棄管理

3.3.4 不正アクセス発生時の対応

（システム設計・仕様）

a 銀行および API 接続先は、不正アクセスが判明した場合に被害発生やその拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことができるシステム設計・仕様としなければならない。

b 銀行および API 接続先は、不審な資金移動等についての利用者からの照会への対応や、不正アクセス発生時の原因調査、必要な対策の検討を行うため、適切なアクセスログの記録および保存を行わなければならない。

（情報連携、対策協議）

c 不正アクセス発生時には、速やかに銀行と API 接続先の間で情報連携を行うとともに、原因調査や必要な対策の協議等を協力して行っていくことが必要である[55]。必要な対応については、銀行と API 接続先との間で予め取り決めて明確化しておくことが必要である。

3.3.5 セキュリティ対策の継続的な改善・見直し、高度化

a サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているうえ、オープン API を活用した金融サービスの提供は世界的にみても現状、初期段階にある。そのため、銀行および API 接続先は、自社のみならず他社での不正アクセス事例等を踏まえ、セキュリティ対策の継続的な改善・見直し、高度化を図っていくことが必要である。

b セキュリティ対策の改善・見直し、高度化に向けては、銀行および API 接続先は、協力して取り組むことが重要と考えられる。

3.4 利用者保護原則

3.4.1 API 接続先の適格性

（事前審査）

a 銀行は、他の事業者等との API 接続に先立ち、利用者保護等の観点から、API

[54] クラウドサービスを利用している場合においては、FISC「金融機関等コンピュータシステムの安全対策基準」の「クラウドサービスの利用」に定めるところに拠る。
[55] その他の不正アクセス発生時の対応については、「3.4 利用者保護原則」の「3.4.4 被害発生・拡大の未然防止」を参照。

接続先の適格性を審査することが必要である[56]。なお、銀行が共通システムを通じてAPI接続先と接続する場合については、銀行によるAPI接続先の審査結果にもとづき、共通システム提供事業者がAPI接続先との接続を行うものとする。

b　適格性の審査に当たっては、少なくとも以下の点についてAPI接続先に確認することが必要である。

- グループ会社を含めた事業内容、兼業内容
- 反社会的勢力との関係の有無を含む社会的信用、組織ガバナンス
- 法令遵守態勢
- 利用者保護態勢[57]
- 利用者保護原則の充足状況
- 過去に発生した利用者保護関連の不祥事案と改善状況
- 利用者の属性や取引のリスクに応じた、継続的な利用者保護策の高度化に向けた態勢やリソースの有無

c　適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、各企業等とのAPI接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、各銀行が独自に必要と判断した事項も加えて実施する必要がある。

d　なお、API接続先が定めた社内規定等は、上記の適格性の審査に当たっての参考になると考えられる。

e　複数の銀行とAPI接続する企業等における審査対応負担を軽減する観点から、情報セキュリティ関連機関において、銀行がAPI接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API接続先チェックリスト」（仮称）を制定することが期待される[58]。

f　なお、事前審査は、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行とAPI接続する企業等における審査対応負担の軽減や銀行による事前審査水準の標準化の観点から、当該銀行の責任において他の銀行に事前審査を委ねたり、他の銀行が既に行った事前審査の結果を参考にすることも考えられる[59]。

（モニタリング）

g　銀行は、API接続先の適格性について、API接続後も定期的にまたは必要に応

---

[56] 情報セキュリティ関連の適格性については、「3.3 セキュリティ原則」の「3.3.1 API接続先の適格性」を参照。

[57] 特に顧客情報の適切な取扱い・管理態勢や、取得情報の利用目的の適切性、利用約款の適切性（過度な免責規定等、利用者保護に著しく欠ける条項の有無）について確認する。

[58] 必須確認項目については、却ってAPI接続先の対応負担が重くならないよう極力共通した内容に止めるとともに、投入人数や資本額等の形式面ではなく運用を含めた実質面に着目した確認を可能な内容とする等の留意が必要と考えられる。

[59] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

じて確認することが必要である。

h　モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各銀行の顧客保護等管理規程等に応じて、個別に判断されると考えられる。

i　銀行は、API 接続に当たって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、API 接続先に提出を求める情報、API 接続先が大幅な態勢見直しや業務停止等を行う場合の対応、等）を予め取り決めておくことが必要である。

j　銀行は、API 接続先の利用者保護態勢等に関する適格性に懸念があると判断した場合には API 接続先に対して改善を求め、利用者保護の観点から必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[60]。

k　なお、モニタリングは、各銀行がそれぞれ独立に行うことを前提としつつも、複数の銀行と API 接続する企業等におけるモニタリング対応負担の軽減や、銀行によるモニタリング水準の標準化の観点から、当該銀行の責任において他の銀行にモニタリングを委ねたり、他の銀行が既に行ったモニタリングの結果を参考にすることも考えられる[61]。

（その他の留意点）

l　API 接続先において API 接続を通じて提供する金融サービスに関して利用者保護に欠ける不祥事案等が発生した場合、銀行と API 接続先との関係、利用者からの見え方等によっては、銀行側も社会的な批判を浴びる等のレピュテーションリスクが生じる可能性に留意が必要である。

m　API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ銀行側も自行サービスの提供を取り止めて、預金者に対して API 接続先のサービスの利用を推奨する場合は、形式上、銀行と API 接続先の間に外部委託契約が締結されていなくとも、その実態において同視され、銀行法にもとづく外部委託規制の対象となる可能性があることに留意が必要である。

n　API 接続先が提供するサービスが銀行の提供するサービス（例：インターネット・バンキング）を実質的に代替するものであって、かつ利用者の大部分が当該 API 接続先のサービスの利用に依拠する場合は、API 接続先のシステム障害や業務停止等によって、利用者が金融サービスを利用できなくなり、混乱が生じるおそれがあることに留意が必要である。

o　事前の取決めにおいて、API 接続先における障害等によって銀行の業務に影響が生じるおそれがある場合には、ただちに銀行に連絡するよう定めておくこと

[60] ただし、銀行が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。

[61] 本方式を採用する場合の銀行間の取決めに係る留意点については、FISC「金融機関等のシステム監査指針」において定められている「共同監査方式」の枠組みが参考になると考えられる。

が必要である。なお、その他の障害等の報告要否やタイミングについても、予め取り決めておく必要があることに留意する。

p　API 接続先もしくは銀行の都合によるサービス停止を行う際は、一定期間の事前通知期間を設定することが必要である。

3.4.2　説明・表示、同意取得

（重要な情報の表示、同意取得）

a　インターネットを利用した取引は、基本的に画面に表示される情報にもとづいて利用者の判断・同意が行われ、また、必要な情報を表示しても、利用者が十分に確認せずに、手続きを進める可能性がある。

b　そのため、銀行および API 接続先は、利用者の判断・同意に必要な情報を単に提供・表示するに止まらず、わかりやすく画面表示するとともに、誤認・誤解を招く表現を避け、また、利用者に重要な判断・同意を求めるものについては注意喚起プロセスを設けることや、利用者のシステム操作による同意を求めること等、利用者保護に十分配慮した表示方法、画面構成とすることに努めなければならない。

c　銀行は、トークン発行に当たって、少なくとも以下の点について、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。

- アクセス権限を付与する API 接続先の名称
- API 連携するサービス等の名称
- 付与する権限の内容・範囲
- 付与する権限の有効期限[62]
- 付与した権限の削除、解除方法
- その他注意喚起が必要な事項

d　API 接続先は、サービス提供に当たって、少なくとも以下の点について、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。

- 個人情報保護法にもとづく取得情報の利用目的、共有範囲（第三者提供の有無）
- 取得した情報の削除に関する事項
- サービス利用上の制限
- その他注意喚起が必要な事項

（リスク等に関する表示）

e　API 接続先は、提供するサービスに関して生じる主なリスクの適切な表示に努めなければならない。

f　API 接続先は、サービス提供時間帯または停止時間帯、休日・休業等のサービ

[62] リフレッシュトークンを発行する場合には同トークンによって延長される最大の有効期限。

ス提供上の制約について適切な表示に努めなければならない。

（利用者の誤認防止）

g　以下の点については、特に利用者の誤認や誤解が生じるおそれがあることに留意し、適切に表示することに努めなければならない。

- API 接続先が提供するサービスは銀行が提供するサービスとは異なること
- 銀行と API 接続先の関係、それぞれの役割（特に API 接続先が銀行代理業者または銀行の外部委託先でないこと）
- 決済指図取引と他のサービスの区別
- 銀行と API 接続先の画面の区別

h　なお、銀行は、API 接続先が虚偽または意図的に誤認を招く表示を行っていることが判明した場合には、API 接続先に対して是正を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消、関係当局への通報等の必要な措置を講じなければならない。

（その他の表示）

i　銀行および API 接続先は、利用者からの相談・照会、苦情、問合せがあった場合の役割分担、業務フロー等を、予め取り決めておくことが必要である。

j　銀行および API 接続先は、上記の取決め内容を踏まえ、利用者からの相談・照会、苦情、問合せに対応するための連絡先を表示することが必要である。

k　API 接続先は、商号、代表者、住所、連絡先等について表示することが必要である。

l　API 接続先は、電磁的方法による決算公示を選択している場合、会社法にもとづく決算公告についても表示することが必要である。

3.4.3　不正アクセスの未然防止

a　API 接続先は、不正アクセスを未然に防止する観点から、例えば以下の点について、利用者に注意喚起することに努めなければならない。

- API 接続先のログインパスワード等は、銀行サービスに利用しているパスワード等と異なるものを設定すること
- API 接続先のログインパスワード等は、類推されやすいものを避けること、適切な管理に努め第三者に貸与、開示しないこと、定期的に変更すること
- ウィルス対策ソフトを導入すること

b　API 接続先は、利用者に対して、API 接続先のパスワード等の紛失、漏洩や不正アクセスの懸念がある場合には、ただちに API 接続先に対して連絡するよう求めておくことが必要である。

3.4.4　被害発生・拡大の未然防止

（初動対応）

a　銀行または API 接続先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、銀行においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことが必要である。

b　銀行と API 接続先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、一方で API に関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を銀行と API 接続先間において予め取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。

c　API 接続先が複数の銀行と接続している場合において、他の銀行においても同様の事案が発生するおそれがある場合には、API 接続先は当該他の銀行に対してもただちに連絡し、被害拡大を未然に防止することに努めなければならない。

（利用者への連絡）

d　被害が発生した利用者への連絡や、被害が広範な利用者に及ぶ可能性がある場合に利用者にただちに十分な注意喚起（例えば、ただちにパスワード等の変更を求める等）ができるよう、API 接続先は、利用者との連絡手段を予め確保しておくことが必要である。

e　利用者に届出・登録を求める連絡手段の範囲については、提供するサービスの内容や取引のリスクに応じて、個別に判断されると考えられる。

f　銀行は、API 接続先が利用者との十分な連絡手段を予め確保することができない場合、被害発生時に、銀行が API 接続先に代わって利用者に対し連絡、注意喚起する必要が生じる可能性に留意することが必要である。

3.4.5　利用者に対する責任・補償[63]

a　オープン API では、取引指図の処理・実行に API 接続先と銀行の双方が関与するため、情報流出や不正送金、システム上の不具合等により利用者に損害が発生した場合、利用者に対する責任の所在や、対応窓口・主体等が不明確になるおそれがある。

b　当事者の民事上の最終的な損害賠償責任を司法の判断に委ねた場合、速やかな

[63] 2016 年 12 月 27 日付で公表された金融審議会「金融制度ワーキング・グループ」報告書では、「金融機関は（中略）業者との間で締結する契約において顧客に生じた損失の分担を定め、公表することとする」（報告書８頁参照）とされており、当該記述を踏まえ、本節は、利用者の保護を適切に確保していくための銀行および API 接続先と顧客との間の損失分担ルールのあり方について検討したもの。

被害回復、補償等が図られず、利用者保護に欠けるおそれがある[64]。

（当事者間における事前の取決め）

c　銀行およびAPI接続先は、利用者に対して速やかな被害回復、補償等を図る観点から、不正アクセスや情報流出、不正送金、システム上の不具合等が発生した場合の対応窓口や、利用者に損害が生じた場合の補償・返金方法（含む、その主体）[65]、補償範囲について、予め取り決めておかなければならない[66]。なお、利用者に対して双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行ってはならない[67]。

d　API接続先および銀行は、予め取り決めた利用者に対する補償・返金方法とその補償範囲（免責事由も含む）について、ウェブサイト等において利用者が常時確認できるよう表示するとともに、API接続先が利用者と利用契約を締結する際にわかりやすく画面表示する等により、利用者が補償・返金を求める際の対応窓口やその方法について十分認識できるよう努めなければならない。

（補償内容・範囲に関する考え方）

e　APIを利用したサービスによる預金等の不正な払戻しについて、銀行およびAPI接続先に過失がない場合でも、利用者が個人であって利用者自身の責任によらずに被害に遭われた場合については、上記事前の取決めにもとづいて銀行またはAPI接続先から補償を行うことが必要である。なお、利用者に重大な過失または過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担にすることも含め、個別に判断されることが必要である。

f　法人の利用者については、個人の利用者と比較して、セキュリティ対策等への対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、サービス提供者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人の利用者に対する補償については、利用者が行っていたセキュリティ対策や不正利用被害の防止に関する状況、法人の属性やセキュリティ対策への対応力等の点を考慮して、個別に判断されることが必要である。

---

[64] なお、本節における記述は、API接続先および銀行が利用者保護の観点から自主的に行うことが期待される取組みであり、それぞれの利用者に対する最終的な法的責任を加重または軽減するものではない。

[65] 利用者への補償・返金後の、銀行とAPI接続先の間の内部分担（求償）についても、別途予め取り決めておくことが望ましい。

[66] 銀行およびAPI接続先が利用者に対して連帯して責任を負うこととする場合でも、利用者からみて対応窓口・主体等がわかりにくくなるおそれがあることから、任意の一次的な補償・返金方法（含む、その主体）等について、予め取り決めておくことが望ましい。

[67] その前提として、銀行は、API接続先の利用約款について、消費者契約法等を踏まえ、不相当にAPI接続先の責任を限定する条項が定められていないかを精査することが必要である。

g　銀行および API 接続先は、API を活用したサービスの形態や利用者の属性等に鑑みて、上記と異なる補償内容・範囲とすることに合理的な理由がある場合であって、かつ利用者に不測の損害が生じないよう、かかる補償内容・範囲について利用者に適切に説明または表示した場合に限り、補償内容・範囲を個別に定めることができる。

（API 接続先が補償・返金責任を負う場合の留意点）

h　銀行と API 接続先との間の取決めにもとづき API 接続先が利用者に対して補償・返金責任を負う場合、銀行は、API 接続先の利用者に対する補償・返金に係る態勢や資力等が利用者保護に欠けるおそれがないかに留意のうえ、API 接続の是非を判断するとともに、それらの状況について定期的にまたは必要に応じて確認することが必要である。

i　銀行は、API 接続先の補償・返金の態勢や資力等が利用者保護に欠けるおそれがあると判断した場合、API 接続先に対して態勢の見直しや責任財産の充実、責任保険への加入を求め、API 接続先においてそれが困難な場合は API 接続しない（あるいは接続の停止または取消を検討する）等の対応を行うことが必要である。

j　API 接続先の利用約款等において API 接続先の免責事由が過大に定められている等（例えば、過失責任も負わない等[68]）、実質的に利用者に対する補償・返金責任が果たされないおそれがある場合、消費者契約法等を踏まえ、見直しを求めることが必要である。

3.5　その他

（公表情報の取扱い）

a　店舗・ATM の所在地等、銀行のウェブサイト等においてログイン等の手続きを要さずに取得可能な公表情報（以下、「公表情報」）を API 接続先に提供する場合は、上述の記載にかかわらず、以下の取扱いとすることが考えられる。

- 銀行と API 接続先との通信経路において改竄が行われることを防止する観点から、銀行と API 接続先との通信方式は、セキュリティ原則「3.3.2 外部からの不正アクセス対策」に定める通信方式に拠るものとする。

- API 接続先は、システム上の不具合や外部または内部からの攻撃による改竄等によって、銀行に利用者からの問い合わせが行われる可能性のある事態が発生した場合には、ただちに関係銀行に対し連絡するよう努めなければならない。

[68] なお、事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項や、当該事業者、その代表者またはその使用する者の故意または重大な過失による事業者の債務不履行により消費者に生じた損害を賠償する責任の一部を免除する条項等は、消費者契約法（第８条乃至第 10 条）にもとづきそもそも無効とされる。

- 銀行は、API の利用約款等において、不具合発生時等の責任について予め定めておくことが望ましい。

- 銀行は、公表情報を提供する API のアクセス量を銀行側でコントロールできない場合には、システムキャパシティの超過が原因で不具合が発生するリスクに留意するものとする。

（「API 接続先の API 接続先」の取扱い）

b 銀行は、API 接続先との間で「API 接続先の API 接続先」（以下、「API 連鎖接続先[69]」）の取扱いについて予め取り決めておくことが必要である。

c これには、例えば、API 接続先と同様に取扱う（銀行が API 連鎖接続先と直接契約を締結）、API の連鎖接続について銀行の承諾または銀行への事前通知を条件とする、連鎖接続を許容する条件を双方協議のうえ予め定める、API 接続先の責任と管理の下で連鎖接続を許容する等、様々な方法が考えられる[70]。

d いずれの方法による場合であっても、API 連鎖接続先において、本原則の趣旨を踏まえて、十分なセキュリティ対策と利用者保護が図られていることが重要である。

e なお、API 接続先が有する自社の情報を同接続先の API を通じて他の事業者等に提供することは、API の連鎖には該当しないが、個人情報保護法等にもとづき適切な利用者保護が図られる必要があることに留意する。

（バンキング API 以外の API における本原則の活用）

f 当検討会は、銀行以外の事業者がオープン API に取り組む場合においても、本報告書で定めたセキュリティ原則・利用者保護原則が、当該事業者におけるセキュリティ対策、利用者保護態勢を整備するうえで、参考になることを期待する。

[69] 銀行に対する API 接続先からの取引指図が、API 接続先と API 接続する他の事業者等の取引指図にもとづいて行われる場合における、当該他の事業者等をいう。

[70] API 連鎖接続先の取扱いは、例えば、取引のリスクに応じて参照系 API と更新系 API との間や、API 連鎖接続先が API 接続先と同一グループに属するか否かによって異なる取扱いとすることも考えられる。

4. 今後の取組み

4.1 API 仕様の標準化に関する取組み

a 電文仕様標準の策定については、一般社団法人全国銀行協会が事務局となって、銀行界、IT 事業者、API 接続先企業等の各関係者の意見も参考にしつつ、預金に係る、①残高照会、②入出金明細照会、③振込を対象とした検討が進められる予定となっている。

b 特に残高照会および入出金明細照会については、スクレイピングから API への円滑なシフトを可能とする観点から重要な論点であり、諸外国の動向を踏まえつつ[71]、今来年度中のできるだけ早期に標準を策定することが期待される。

4.2 情報セキュリティ関連機関との連携

（API 接続先チェックリストの制定）

a 複数の銀行と API 接続する企業等における審査対応負担を軽減する観点からは、銀行が API 接続先の適格性を審査する際に使用する「API 接続先チェックリスト」（仮称）の制定が期待される[72]。

b かかる観点から、FISC においては、2017 年２月、「API 接続先チェックリスト（仮称）ワーキンググループ」が設置され、2017 年６月を目途とした API 接続先チェックリストの制定に向けた検討が開始されているところ。

c 当検討会は、FISC の取組みを歓迎する。当検討会は、同センターの取組みが、今後の API 接続先と銀行の協業・連携の円滑化やセキュリティ対策等に係る双方のコミュニケーションコストの軽減等に資することを期待する。

（業界・企業横断的なセキュリティ対策強化に向けた取組み）

d サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているうえ、オープン API は、銀行が他の事業者等に対して銀行システムとの接続口を提供する仕組みであるため、仮に API のシステムに脆弱性があった場合、システムトラブルや最悪の場合、不正送金や顧客情報の情報流出等が生じるおそれがある。

e オープン API は新たな技術であるため、技術の利用形態や技術仕様そのものが現段階では成熟していないことに鑑みれば、個別銀行レベルでの対策に加え、業界・企業横断的にも、不正アクセス事案やセキュリティ関連対策について、情報セキュリティ関連機関と連携して情報共有等を行う枠組み等を整備し、銀

[71] 英国においては、2017 年５月頃に、一部の API 仕様標準の公開が行われるとみられており、検討に当たっては、これらの動向にも留意しつつ進める。
[72] 「3.セキュリティ対策および利用者保護原則」を参照。

行、API 接続先におけるセキュリティ対策の継続的な改善、見直し、高度化を後押ししていくことが重要である。

f　かかる観点から、サイバーセキュリティに関する情報共有や分析等を行う「金融 ISAC」[73]においては、FinTech に関する業界全体のセキュリティ対策の底上げに向けた取組みとして、金融機関や API 接続先企業等が参加する「FinTech セキュリティ WG」を設置し、当面の課題として、オープン API のセキュリティに関する情報収集および情報共有に注力する方針が打ち出されている。

g　当検討会は、金融 ISAC の取組みを歓迎する。当検討会は、同団体の取組みが、わが国金融機関における安全かつ利便性の高いオープン API の取組みの後押しとなることを期待する。

4.3　銀行と FinTech 企業等の協業・連携の円滑化に向けた取組み

a　2016 年 12 月 27 日に公表された金融審議会「金融制度ワーキング・グループ（以下、金融制度 WG）報告―オープン・イノベーションに向けた制度整備について―」[74]においては、銀行と FinTech 企業等の協業・連携を促し、オープン・イノベーションを促進する観点から、金融機関は電子決済等代行業者との契約締結の可否に係る判断の基準を策定・公表することとしている。

b　一方、わが国においては、多数の銀行が存在するため[75]、FinTech 企業等が、ウェブサイト等に掲示された各銀行の判断の基準を網羅的に確認し、各銀行にコンタクトすることには負担があると考えられる。また、FinTech 企業等との積極的な協業・連携を進める銀行においても、FinTech 企業等における確認負担が大きい場合、革新的な FinTech 企業等との協業・連携機会を失する可能性がある。

c　一般社団法人全国銀行協会においては、銀行と FinTech 企業等の協業・連携を円滑にする観点から、金融制度 WG 報告書や関連法令の動向を踏まえつつ、オープン API に関する取組み実施状況（会員各行における判断の基準の公表や会員各行の照会窓口の設置等）について、当該銀行の了解を得たうえでリスト等の形で集約し、公表する等の取組みが期待される。

4.4　本報告書の改訂、継続的なコミュニケーション

（関係法令等の改正を踏まえた改訂）

a　本報告書は、2017 年 3 月現在の関係法令にもとづく中間的な整理（案）であり、関係法令の改正等が行われた場合には必要に応じて当該法令に準拠した改訂等が必要となる。

---

[73] http://www.f-isac.jp/
[74] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1.html
[75] 一般社団法人全国銀行協会正会員 120 行、準会員 71 行、特例会員 1 行。

b　事務局においては、金融制度 WG を踏まえた関連法令の動向等を踏まえつつ、本報告書の改訂要否の検討を行い、改訂を行う場合は当検討会メンバーとも連携のうえ、正式な報告書として公表することが期待される。

（銀行界と API 接続先事業者団体等との継続的な連携・コミュニケーション）

c　オープン API は世界的にみても初期段階にある取組みであり、新たに発生した様々な課題や諸問題について、銀行界と API 接続先事業者団体、IT 事業者等が継続的に連携・コミュニケーションしていくことが重要である。

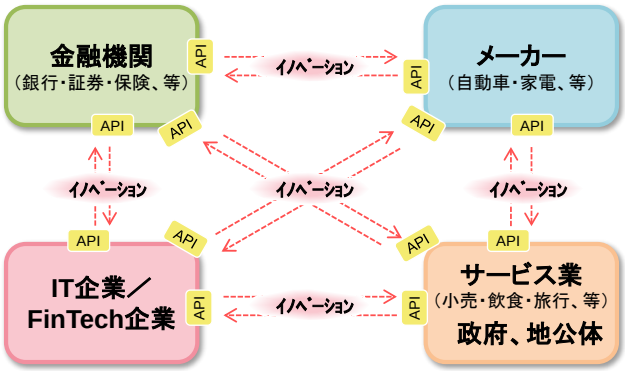
d　かかる観点から、銀行界、API 接続先等の関係する団体においては、関係団体間で協議のうえ、継続的な意見交換の場を設ける等の取組みが期待される。

（その他の改訂等）

e　事務局においては、新たな事象の発生等を踏まえて、必要に応じて本報告書の見直し・改訂等を検討していくことが期待される[76]。事務局における改訂要否の検討等の参考とするため、本報告書に対する意見提出先として、open-api@zenginkyo.or.jp を窓口として設置する。

4.5　API エコシステムの形成に向けて

a　オープン・イノベーションの活性化に向けては、銀行によるオープン API の取組みのみならず、他の事業者等においてもオープン API の取組みが進展し、金融分野に限らず、様々な事業者の間で価値のある情報が相互にやりとりされていく生態系（「API エコシステム」）が形成されていくことが重要である。



b　当検討会は、こうした API エコシステムの形成に向けて、銀行界におけるオープン API に関する取組みを契機に、銀行以外の事業者等においても、オープン API の取組みが拡がっていくことを期待する。

以　上

[76] 本報告書の改訂を行う場合の方法、枠組み等については、内容に応じてその都度、事務局において検討を行うものとする。