日銀レビュー

2018-J-3

金融分野におけるオープン API の活用

～セキュリティへの影響と対策～

金融研究所　中村啓佑

Bank of Japan Review

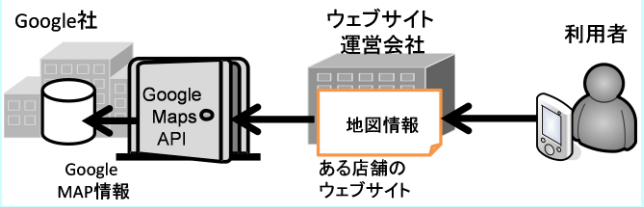
2018 年 6 月

近年、情報技術を活用した新しい金融サービスとして FinTech が注目を集めている。FinTech を推進する柱の１つといわれている API（Application Programming Interface）を公開する動きが、官民を挙げて加速している。本稿では、国内外における API の公開の動きを紹介するとともに、公開された API（オープン API）の安全な利用に向けた取組みと今後の課題を説明する。

オープン API とは

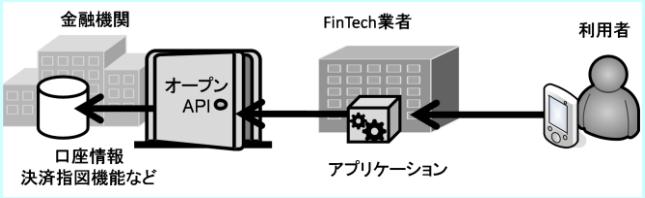
近年、情報技術を活用した新しい金融サービスとして FinTech が注目を集めている。その起爆剤の１つが API（Application Programming Interface）の公開である。API とは、「特定のプログラム」に対して、「別のプログラム」から動作させる仕様のことである。例えば、ある店舗が自店の所在地をウェブサイトで公開する際、グーグル・マップの地図で表示させるケースを想定する。この場合、グーグル社が提供している API（Google Maps API）を用いて、グーグル・マップ情報（特定のプログラムに該当）をある店舗のウェブサイト（別のプログラムに該当）から動作させることができる（図表１参照）。

【図表 1】API とは



FinTech の分野では、「API とは、銀行以外の者が銀行のシステムに接続し、その機能を利用できるようにするプログラムを指し、このうち、銀行が電子決済等代行業者（FinTech 業者）に API を提供し、利用者の同意に基づいて、銀行システムへのアクセスを許諾する形態をオープン API という」と定義される（図表２参照）[1]。

【図表２】金融分野におけるオープン API



オープン API は、金融機関が保有している情報に対して、読み取る権限のみが付与された「参照系 API」と、書き換える権限まで付与された「更新系 API」の 2 種類に大別される[2]。参照系 API を用いて提供される主なサービスは、利用者が（複数の）金融機関における自分の口座残高等のデータを集計し、確認できる口座情報サービス（Account Information Service）であり、更新系 API を用いて提供される主なサービスは、決済指図を金融機関に伝達し、その結果を確認できる決済指図伝達サービス（Payment Initiation Service）である。

金融分野におけるオープン API の活用に向けた動きは、国内外において進められている。国内においては、銀行法等の一部改正により API に関連する規定が整備されたほか、「政府・未来投資戦略 2017」では、2020 年 6 月までに 80 以上の銀行がオープン API を導入することが目標に据えられている[3]。国内の金融機関では、オープン API をすでに導入または導入予定としているところが多い[4]。海外においても、例えば、欧州連合（European Union：EU）では、第 2 次決済サービ

ス指令（Payment Services Directive 2：PSD2）において、実質的に金融機関に対してオープン API の導入を義務付けている[5]。

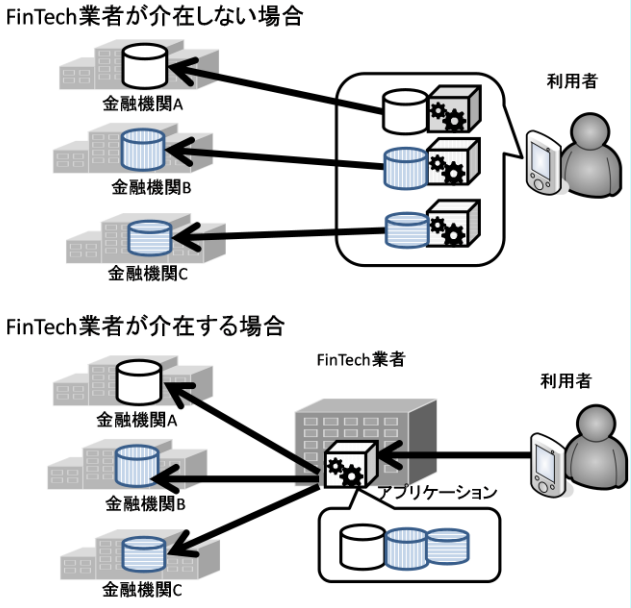
オープン API 利用のメリット：利便性及び安全性の向上

オープン API の効果として、金融分野における競争の促進等が挙げられる。すなわち、オープン API は、FinTech 業者の新規参入を促すほか、新興の金融機関にとっては新規顧客獲得の機会となり、金融機関間および FinTech 業者間の競争を高め、結果的に金融サービスの品質向上に寄与する。また、オープン API は、金融サービス利用者の利便性を高めるとともに、適切な対策および運用を行うことによりセキュリティの強化にも繋がる。

これらの点について、オープン API が利用されない場合における同様のサービス提供の態様と比較すると分かり易い。以下では、口座情報サービス（例えば預金残高照会）を例に説明する。

まず、FinTech 業者が介在しない場合（図表３上段）には、利用者は、預金口座を所持している金融機関と個々に接続、データを取得した後に自ら預金残高を集計する必要がある。この点 FinTech 業者が介在する場合（図表３下段）には、利用者は FinTech 業者から（利用者が事前に登録しておいた）複数の金融機関にかかる口座情報の自動集計結果を取得するだけですむ。

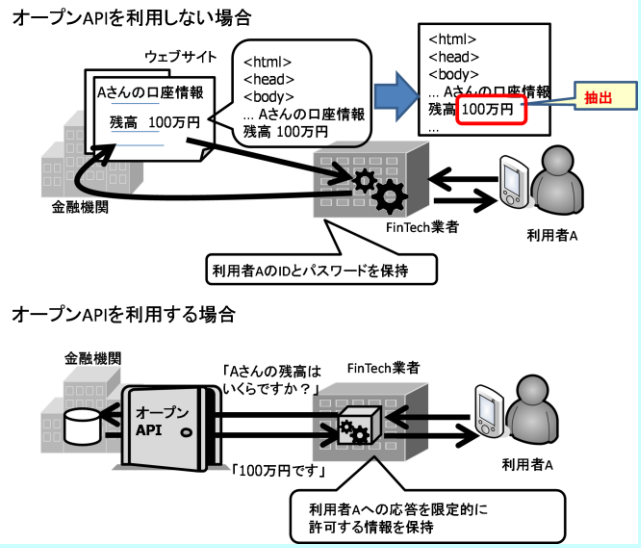
【図表３】FinTech 業者が介在する場合としない場合の比較



後者の FinTech 業者が介在する場合に関しては、オープン API を利用しないかたちでのサービス提供も考えられるが（図表４上段）、オープン API を利用することにより、より広範な FinTech サービスの提供に対応しうる仕様に変わり、利便性やセキュリティが向上する（図表４下段）。

オープン API を利用しない場合には、FinTech 業者が金融機関から情報を抽出する際、金融機関のウェブサイトのデータを用いる。具体的には、利用者の ID とパスワード情報を用いて、金融機関の利用者の口座情報が記載されたウェブサイトにアクセスし、そこから必要な情報を抽出する[6]。このため、抽出可能な情報はウェブサイトに記

【図表４】（FinTech 業者が介在する場合のうち）オープン API を利用する場合としない場合の比較



（補足）金融機関、FinTech 業者、利用者別のオープン API を利用する場合としない場合の比較

		オープンAPIを利用しない場合	オープンAPIを利用する場合
金融機関	対応負担	• 不要	• 必要 （APIを介した外部からのアクセスを可能とするように情報システムの更改が必要。）
	アクセス制御	• 不可	• 可能 （金融機関および利用者が認めたデータのみにアクセスを制御可能。）
FinTech業者	対応負担	• （オープンAPIを利用する場合に比べて）重い （ウェブサイトのレイアウト等の変更の都度、プログラム等の変更が必要。） （利用者のID、パスワード等の管理が必要。）	• （オープンAPIを利用しない場合に比べて）軽い （APIの変更の都度、プログラム等の変更が必要。ただし、変更頻度はウェブサイトよりもAPIの方が低いため、対応負担はAPIの方が軽い。） （利用者のID、パスワード等の管理が不要。）
	取得可能なデータ	• ウェブサイト上で提供されているものに限られる。	• 金融機関、利用者の同意が得られれば、ウェブサイト上で提供されないものも可能。
利用者		• アクセス制御ができないID・パスワード等をFinTech業者に提供することによる懸念が存在。	• FinTech業者がアクセス可能なデータを限定でき、IDパスワード等を提供する必要が無い。

載された情報のみとなる。金融機関は特段の対応が不要である一方で、FinTech 業者はウェブサイトから情報を抽出するためのプログラムを作成する必要があるほか、金融機関のウェブサイトのレイアウト等が変更になる都度、当該プログラムの変更を行う必要がある。さらに、セキュリティ面では、金融機関へログインする利用者の ID とパスワード情報を FinTech 業者に提供する必要があり、セキュリティ上の懸念が存在する。

これに対し、オープン API を利用する場合には、FinTech 業者はオープン API を用いて金融機関から情報を入手できる。このため、FinTech 業者が入手可能な情報は、ウェブサイト上で提供されるものに限定されず、金融機関がオープン API を介して提供するデータのうち、当該データが帰属する利用者の同意が得られたものとなる。この場合、金融機関はオープン API を構築する必要があるほか、FinTech 業者もオープン API に対応したプログラムを作成することが必要となる。さらに、オープン API の仕様が変更される都度、当該プログラムの変更を行う必要もある。もっとも、ウェブサイトの更新頻度とオープン API の変更頻度は、後者の方が少ないと考えられることから、FinTech 業者の負担はオープン API を利用しない場合に比べ、軽いと考えられる。このほか、セキュリティ面では、金融機関へログインする利用者の ID とパスワード情報を FinTech 業者に提供する必要がなく、より望ましいとされる。

オープン API と標準化

オープン API の標準化が進めば、複数の金融機関が同一のコマンドや関数等に基づいたオープン API を開発・公開可能となる。このため、金融機関は API の開発負担を、FinTech 業者はオープン API に対応したプログラムの開発負担を軽減可能となる。こうした開発負担の軽減は、FinTech 業者が新規参入する際のハードルを引き下げることに寄与する。このため、各国では、標準化に向けた動きが進展している。

英国では、2015 年 9 月、金融分野におけるオープン API のあり方や課題等にかかる検討を行うために、英国財務省の要請によりワーキング・グループ（The Open Banking Working Group[7]）が設置され、その検討結果を纏めた報告書（The Open Banking Standard[8]）が公表されている（2016 年 2 月）。同報告書では、標準化の対象とすべき事項が網羅的に整理されているほか、FinTech 業者による新しいサービスの効率的な開発を行うために、開発用コード等の公開や、サンドボックス環境の提供が重要としている。

また、ドイツでは、「Open Bank Project」という組織が、国内の銀行に対して金融サービスに活用できるオープン API の雛型を提供しており、既に、複数の銀行が同雛型を用いたオープン API の利用を検討している[9]。

金融サービスにかかる国際標準化を担当する ISO/TC68 においても、セキュリティ分科委員会（SC2）や情報交換分科委員会（SC9）の傘下に FinTech 業者やオープン API にかかるスタディ・グループやワーキング・グループが設置され、標準化に向けた検討が行われている[10]。

このほか、ID 連携の標準仕様を策定している団体である OpenID Foundation は、Financial API と呼ばれるドキュメントの作成を進めている[11]。英国は、2017 年 5 月に当該団体と共同でオープン API を推進することを公表し、2018 年 1 月から英国の大手銀行において実証実験が行われている。

オープン API で用いられる認可プロトコル OAuth2.0

オープン API を安全に活用するうえで、「認可（authorization）」が重要な概念である。認可とは、例えば、FinTech 業者 A を利用者 B の銀行 C にある口座情報にアクセスさせるために、利用者 B が当該口座情報へのアクセス権を FinTech 業者 A に事前に与えることである。認可されたことを証明するデータは「アクセス・トークン」と呼ばれる。先ほどの例では、（利用者 B が銀行 C に保有する口座情報へのアクセスを許可する）アクセス・トークンを FinTech 業者 A が用いることにより、FinTech 業者 A は銀行 C にある利用者 B の口座情報にアクセスすることができる。

金融業界では、オープン API の認可を行う仕組みを実装する際に、「OAuth2.0」と呼ばれる手順（技術用語では、プロトコルという）が推奨されることが多い[12]。OAuth2.0 は、2012 年にインターネット技術の標準化を推進する団体（IETF：The

Internet Engineering Task Force）において公表された手順である。OAuth2.0 を用いた認可の仕組みは、金融分野以外の多くの分野において既に取入れられており、認可を行う仕組みを実装する際のデファクト・スタンダードになりつつある。

OAuth2.0 はあらゆる環境に適用できるように、大枠と様々なオプションの手順のみが規定されたものであり、具体的な設定内容に関する記述は少ない。したがって、実際のシステムで実装する際に必要となる記述が少ないことから、OAuth2.0 をサービス内容や環境に応じてどう実装するかは、金融機関や FinTech 業者の判断に委ねられている。このため、適切に実装するためには、OAuth2.0 を正確に理解するとともに、個々のアプリケーションが晒される可能性のある脅威を適切に想定する必要がある[13]。

OAuth2.0 のフローについて、「利用者」、「FinTech 業者」、「金融機関」の関係を簡単に紹介する（図表 5 参照）[14]。

① 利用者が FinTech 業者アプリ（以下、FinTech 業者）を起動する。

② FinTech 業者は、利用者のスマホのブラウザを介して、金融機関にアクセス許可を要求する。

③ 金融機関は、①を起動した利用者が、金融機関に登録されている正当な利用者であることの確認（利用者認証）を行う[15]。

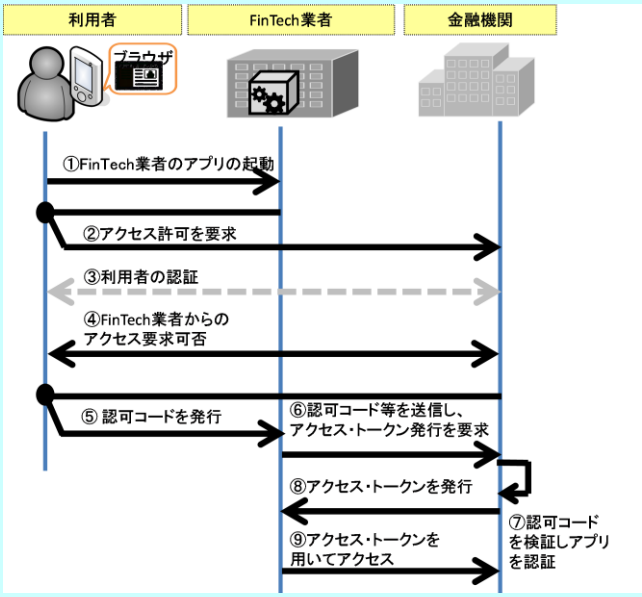
④ 上記③が成功した場合、金融機関は、②の要求を許可する、ないし拒否する。利用者は、許可する場合には、その旨を金融機関に送信する。

⑤ 金融機関は、利用者のスマホのブラウザを介して、金融機関へのアクセスを許可されたことを証明する情報（アクセス・トークン）の発行を申請できる権利が付与された情報（認可コード）を FinTech 業者に発行する。

⑥ FinTech 業者は、認可コードに加えて、当該業者のみが保有している秘密情報（正当な FinTech 業者であることを証明するための情報）を金融機関に送信し、アクセス・トークンの発行を要求する。

⑦ 金融機関は、認可コードを検証し、かつ、上記⑥の秘密情報を確認する（FinTech 業者の認証を行う）。

【図表 5】OAuth2.0 の代表的な方式のフロー



⑧上記⑦が成功した場合、金融機関は、アクセス・トークンを FinTech 業者に発行する[16]。

⑨ FinTech 業者はアクセス・トークンを用いて金融機関にアクセスする。

認可プロトコル OAuth2.0 に対する脅威と対策

前述のフローにおいて留意事項が 2 つ存在する。第 1 に、金融機関と FinTech 業者間の通信のうち、利用者を経由する通信（図表②、⑤）で認可コードが漏えいしたり、改ざんされたりする可能性がある。これは、金融機関と FinTech 業者間の通信の暗号化が、利用者のスマホで一旦復号されることによる。第 2 に、一般的なアクセス・トークンは、当該トークンの利用者に関する情報を含まない方式（持参人払式トークンと呼ばれる）であるため、攻撃者が悪用する可能性がある[17]。アクセス・トークンをファースト・フードの割引クーポンに置き換えると理解しやすい。割引クーポン券は、利用できる店（金融機関に該当）は限定されるものの、割引クーポン券を所持していれば、誰でも利用できる。

こうした留意事項も踏まえると、主な脅威として、①FinTech 業者と金融機関で発生する通信の奪取や改ざん（脅威 1）と②アクセス・トークンの奪取（脅威 2）が考えられる。

金融機関および FinTech 業者は、これらの脅威

に対する有効な対策を講じることが求められる[18]。例えば FinTech 業者において、事前に金融機関毎にアクセス・トークンの受信先を登録しておくことが考えられる。また、金融機関と FinTech 業者は、送信内容が改ざんされないように証明書を付して送信することも検討に値する。さらに、金融機関や FinTech 業者は、利用者にサービスを提供する際に、どの脅威が発生し得るかを整理したうえで、当該サービスに求められるレベルの対策を適切に講じる必要がある。例えば、参照系 API を用いたサービスと更新系 API を用いたサービスでは、求められる対策のレベルは異なりうる[19]。また、対策を講じる際は、金融機関と FinTech 業者が密に連携し、稼働開始時のみならず、定期的に確認する等、厳格な対応が求められる。

利用者の対応も重要である。例えば、端末等を第三者に盗取されることがないように適切に管理するほか、その起動時や FinTech 業者のアプリの使用時に求められる情報等（利用者の ID、パスワード、生体情報等）を適切に管理することが求められる。また、端末等の OS のパッチ適用やマルウェア対策ソフトの利用等、通常の端末等におけるセキュリティ対策も速やかに行うことなどが考えられる。

オープン API の安全な活用に向けて

今後、金融機関によるオープン API の提供が本格化するにつれて、利用者も増加することが予想される。金融機関や FinTech 業者が安全性を確保するための対応を進めることに加えて、利用者の側でも、適切な対応が一段と求められることになる。FinTech 業者においては、利用者によるセキュリティ対策や端末等の管理が適切に実施されるように、金融機関と密に連携し、サービスにかかるリスクの所在やそのインパクト、実際のサービスにおけるセキュリティの状況等について、利用者の理解を得るよう丁寧に説明していくことが求められる。その際、例えば、金融情報システムセンターや金融 ISAC の（オープン API を利用するための）チェックリスト等を活用し、十分なセキュリティが確保された状態にあることや、リスク管理上留意しなければならない事項を継続的に確認し、利用者に情報還元する体制等を整備することが考えられる。また、こうした対応の実効性を高めるために、リスクが顕在化した際の責任を関係者間でどのように分担するかについても予め明確にしておくことが有益である。

セキュリティ対策を講じる際に、それらを実施した場合に生ずる利用者の利便性の低下等についても検討する必要がある。具体的には、セキュリティ対策の実施に伴う通信のスループットの低下や、利用者に複雑な処理や過度の確認を強いることなどが考えられる。提供するサービスに求められるセキュリティを個別に判断したうえで、そのリスクに見合ったセキュリティ対策を講ずることが重要である。

このほか、API の標準化を検討する際には、セキュリティの観点から何を標準化の対象とするかに留意する必要がある。この点、API を構成するプログラムが多くの金融機関間で共有される場合、当該 API に脆弱性が発見されれば、金融システム全体の安全性に影響を及ぼすことになりかねない。こうした点を踏まえると、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考えられる。

今後、こうした検討も順次進むことが期待される。新しい対策やそれにかかる技術も活用しつつ、オープン API による革新的なサービスが、安心安全に広く利用されるようになることを期待したい。

---

[1] 金融審議会「金融制度ワーキング・グループ報告書（平成 28 年 12 月 27 日公表）」を参照。

[2] 一般的に、「更新系 API」を用いた FinTech サービスは、「参照系 API」を用いた FinTech サービスより収益機会が大きいとされ、注目されている。

[3] 内閣府「平成 29 年第 10 回経済財政諮問会議・第 10 回未来投資会議合同会議、資料 7　未来投資戦略 2017 Society 5.0 の実現に向けた改革（平成 29 年 6 月 9 日開催）」を参照。

[4] 2017 年の銀行法改正において、銀行は 2018 年 4 月 1 日までに API 接続にかかる対応方針を作成・公表することとされている。すでに公表されている対応をみると、多くの金融機関において、オープン API を提供予定としている。

[5] PSD2 において、利用者は、金融機関が保有している利用者のデータに対して、EU 加盟国により認可を受けた FinTech 業者（正規 FinTech 業者）を介してアクセスする権利を認められているほか、金融機関は正規 FinTech 業者からのアクセス要請に応じる義務（XS2A = Access to

Accounts）を課されている。さらに、EU の加盟各国に対し、これらのことを制度面から支えるための国内法制化を 2018 年 1 月までに実施することを促している。

[6] こうした技術は、ウェブ・スクレイピングと呼ばれる。

[7] Open Banking Working Group は、Open Data Institute（英国政府が設立したオープンデータを活用したビジネス開発を推進する組織）が 2015 年 9 月に英国財務省からの要請によって設置した作業部会であり、英大手行、オープンデータ推進団体、FinTech 関連団体、英国財務省などが参加している。

[8] Open Data Institute が 2016 年に公表した「The Open Banking Standard」を参照。

[9] Open Bank Project による「An Overview of the Open Bank Project」(https://openbankproject.com/)や「API EXPLORER」(https://apiexplorer.openbankproject.com/)を参照。

[10] 日本銀行金融研究の ISO/TC68 国内委員会議事録（2017 年 6 月 14 日開催分）を参照。

[11]当該団体は ISO/TC68 のリエゾン（審議団体）としての活動が認められており、金融分野で注目されている。

[12] 例えば、英国の Open Data Institute は、OAuth2.0 または OpenID Connect を推奨している。米国の FS-ISAC も OAuth2.0 を推奨している。また、わが国でも、全国銀行協会や金融情報システムセンターにおいて OAuth2.0 が推奨されている。

[13] OAuth2.0 が使用されているサービスのなかには、OAuth2.0 に起因するセキュリティ上の脆弱性を有しているものが多い。例えば、Google Play や Apple マーケット等の公式のアプリケーション配信サイトで提供されていた 149 のモバイルアプリ（OAuth2.0 が使われていたもの）を調査したところ、脆弱性を有するものが約 6 割（89 モバイルアプリ）あったとの報告もある。

[14] OAuth2.0 の手順としては、複数の方式が規定されているが、本稿では、セキュリティの観点から IETF において唯一推奨されている「認可コード方式」を前提に記述する。

[15] ③の利用者認証は、OAuth2.0 のプロトコルの対象外である。利用者認証には任意の方式が採用できるため、例えば、次世代の認証技術として注目されているファイド（FIDO ：Fast IDentity Online）を認証手段として利用することも可能である。

[16] 金融機関は、リフレッシュ・トークンと呼ばれるトークンをアクセス・トークンと併せて発行できる。リフレッシュトークンは、アクセス・トークンの有効期限が切れた際、金融機関に送信して新しい有効期限のアクセス・トークン等の発行を要求する際に用いられる。これにより、アクセス・トークンを再発行する際に、認可フローを再度行う必要がなくなり利便性が向上する。アクセス・トークンの有効期間は数分等、短い時間であることが求められる。このため、参照系 API を用いたサービスは長期間有効なリフレッシュトークンと組み合わせて利用されることが多い。これに対し、更新系 API を用いたサービスは、リフレッシュ・トークンを利用せず、都度、利用者による認証を行うことが想定されている。

[17] アクセス・トークンを記名式トークンにすると、アクセス・トークンに記名された者しか利用できなくなるため脅威 2 のリスクはなくなる。現在、この記名式トークンの標準化にかかる検討も進められている。

[18] 中村啓佑、「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」『金融研究』第 36 巻第 3 号 83～110 頁や、同、「OAuth2.0 に対する脅威と対策：金融オープン API の一段の有効活用に向けて」『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』No. 2017-J-16（著：中村啓佑）などに詳しい。

[19] 例えば、OpenID Foundation が策定しているドキュメント（Financial API）においても、参照系 API と更新系 API に分けて、必要な対策を記述している。