# オープンバンキング、オープンデータ、金融グレードAPI

世界のオープンバンキングおよびオープンデータエコシステム参加者向けホワイトペーパー

2022年3月16日

最終版1.0

編集責任者：Dave Tonge、FAPI Working Group共同議長

# 内容

本ホワイトペーパーは、世界中のオープンバンキングおよびオープンデータエコシステム参加者、さらには政府関係者、このエコシステムを設計する担当者を対象向けに作成されている。

## なぜオープンバンキングなのか？

データはデジタル経済の「新しい石油」と呼ばれることがある。データは企業がサービスを改善し、人工知能（AI）モデルを構築するために使用する強力な資産である。但し、データは時に消費者をサービスに「閉じ込める」ためも使われる。この閉じ込められた状態を打開するには、同意に基づき全ユーザーデータへアクセス可能とすることが有効だろう[1]。そうしてユーザーが様々なサービスプロバイダー間を容易に行き来できるようになれば、イノベーションの波が起きる可能性がある。また、オープンバンキングは、金融包摂を促進し、社会の周縁にいる人々に対するフォーマル経済への橋渡しとなり、より良いサービスを提供することにもつながるだろう。

APIは、同意に基づきユーザーデータへのアクセスを開放する最良の方法であり、デジタルの世界では至る所に存在する。日常生活で使用するソフトウェアの多くは、APIを通じて提供されるサービスによって動いている[2]。ナビゲーションによる道案内、オンライン注文、Eメールでのコミュニケーションなどは、APIを介してデータが提供されるケースである。しかし、これらのAPIの多くは独自開発であり、一定の国際標準に準拠しているとはいえ、特定の企業が別の企業のサービスを利用するために開発されている。このようなAPIは一般的に市場主導型であり、すべての関係者にとって開発し消費する場合、明確な商業的根拠がある。

しかし、APIには、その根拠がそれほど明快でないものもいくつかある：

- 銀行口座情報（または当座預金、普通預金、株式、債券、投資信託、保険を含むあらゆる金融口座情報）へのアクセス
- 銀行口座からの直接決済を開始
- 医療情報へのアクセス
- 通信会社や公共インフラ企業から提供される使用量や料金データへのアクセス

これらのユースケースを実現するためには、エコシステムの協力体制が必要である。なぜなら、二者間で個別にコラボレーションすることを繰り返していても、大規模に使えるものは実現できないからである。エコシステム全体の協力体制は、業界主導の取り組み（奨励金など）や参加者間の互恵関係から生まれたが、オープンデータAPIのグローバルな普及となると、いくつかの要因によって妨げられている：

1. 競争：データへのアクセスを制限することで、企業は消費者がサービスを直接比較することを困難にし、その結果、顧客が移動する可能性を低減している。

2. 管理：民間企業は、自社のサービスやデータとのやりとりが、自社が管理するインター

[1] 同意に基づくアクセスは、データポータビリティルール、監視、標準、適合性、その他本稿で取り上げた側面を含む、より広範な運用モデルの一要素である。
[2] 本稿では、APIは、第三者利用可能なHTTP APIの事である。

フェイスを通じて行われることを好む。

3. セキュリティ：APIを開放することは、新たな攻撃ベクトルを開放することだと考えられている。
4. 戦略的：多くの金融機関は、高コストでリスクの高い配管工事は行うが、エンドユーザーとの交流のない（したがって、より多くのサービスを販売する機会もない）高コストな「土管」となることを恐れている。

金融機関におけるこうした警戒やAPIの不足は、多くの市場でイノベーションを減らし、コスト増を招いている。一例として、会計ソフトや税務ソフトが挙げられる。このようなソフトは、顧客が利用するどの銀行からも情報を受信できる必要がある。オープンデータAPIにアクセスできなければ、そのようなソフトはすべての銀行やデータ保有者と独占契約を結ぶか、スクリーンスクレイピングの技術を使用してデータAPI化する高価なアグリゲーションサービスを利用しなければならない。この会計ソフトと銀行との間が分断されるような状況は、セキュリティリスクをもたらし、イノベーションを抑制し、新規参入を難しくする。そしてこのような欠陥のあるアプローチは、消費者にとっても障害となる。なぜなら、消費者は自分たちのデータが統合されることで得られるはずの効率性の恩恵を受けることができないからである。

二つ目の例は、複数の当座預金口座とクレジットカード口座を保有するユーザーである。2019 Experian Consumer Credit Review（2019年エクスペリアン社による個人の融資限度に関するレビュー）[2]によると、平均的なアメリカ人は4枚のクレジットカードを持っており、平均的なブラジル人は3.6枚[3]のクレジットカードを持っている。顧客は、取引の全体像を把握し、引き落とし口座やクレジット口座、貯蓄、投資などを横断してタイムリーな請求書支払いを促進するソリューションから最初の恩恵を受ける。フィンテックや金融機関もまた、ユーザーにすべての口座を閲覧できるようにすることで、金融商品やサービスを調整することで恩恵を受けることができる。

加盟店の決済は3つ目の例である。加盟店には、どの銀行を使っても、消費者の決済を可能な限り低コストで受け付けられるようにする明確なニーズがある。市場は、VisaやMasterCardなどのクレジットカードネットワークを通じてこの問題を解決してきた。これらの会社は、さらに付加的なサービスを提供しているが、その命題の一つは、単に加盟店、消費者、銀行間の接続を提供することである。技術的な観点からいえば、このような接続は消費者が自分の口座から加盟店に直接決済を認可できる相互運用性のあるAPIがあれば実現できる。

最後の例はオープンヘルスである。ユーザーは、医療提供者間での医療記録の共有を認可するのに苦労することがある。オープンヘルス構想は、タイムリーで安全な方法で機微データの移動を認可する方法を人々に与える方法を提供する。

この5年間、現状を変えようとする動きがあった。オープンバンキングに始まり、最近ではオープンファイナンスやオープンデータへと移行している。この動きの多くは、競争を促進し、市民に力を与え、より大きなイノベーションを可能にしようとする規制当局が推進している。

本稿では、この動きについて説明し、OpenID Foundationが作る標準が多くの市場規模の実装にお

[2] https://www.cnbc.com/select/how-many-credit-cards-does-the-average-american-have/
[3] https://www.veriskfinancialresearch.com/reports/country-reports/latin-america/brazil.html（2025年4月14日現在はリンク切れ）

いて中心的な役割を果たしていることを紹介する。

## グローバルな動き

何十年もの間、銀行データへのアクセスを中心に構築されたサービスがあった。オープンバンキングAPI以前は、これらのサービスは主にスクリーンスクレイピングやファイル交換に基づいており、特にスクリーンスクレイピングはセキュリティに関する重大な懸念要素であった。堅牢で相互運用性のあるAPIの欠如は、参入への大きな障壁となり、イノベーションを制限した。

最初の事例の一つとして挙げられるのはシンガポールである。ユーザーの同意および銀行とフィンテック間の「互恵性」という重要な原則に基づき、市場主導のアプローチで2018年から稼働している。2020年時点で1600以上のオープンAPIがあり、金融サービスや政府のユースケースに加え、タイとの提携によるP2P（個人間取引）決済にも対応している。

EUのオープンバンキングへの動きは、（数年にわたるドラフト作成と協議の末）2018年1月に法制化された第2次決済サービス指令（PSD2）から始まった。PSD2は、企業にAPIアクセスの開放を求めた最初の規制当局の取り組みの一つであった。大半は決済を対象としているが、「アカウント情報サービスプロバイダー」という新しいタイプの規制対象のエンティティが生まれた。この許可を与えられた企業は、銀行のデータAPIへのアクセスが許可される。ベルリングループは、ポーランドのPolishAPI、フランスのSTETとともに、EU内の標準化を推進してきた。

同じ頃イギリスでは、競争規制当局が小売銀行間で十分な競争が行われていないことを調査していた。銀行の反競争的行動や、顧客に高額な料金を請求していることを突き止めたが、その主な救済措置の一つは、9大銀行が共通のAPIを通じてPSD2の義務を果たすことを要求することであった。規制上の義務を果たすためにこれら9大銀行によってOpen Banking Implementation Entity (OBIE)が設立された[4]。

オーストラリアでは、2020年7月に消費者データ権が施行され、消費者は銀行データへのアクセスが可能となった。最終的には、消費者データ権は、エネルギー、電気通信、保険や投資プロバイダーなどの金融サービスなど、オーストラリア経済全体に拡大される予定である。ニュージーランドでは現在、市場主導（payment.nzが主導）のアプローチがとられているが、政府はオーストラリアと同様の規制を検討している。

米国とカナダでは、Financial Data Exchange（業界技術標準化団体）が陣頭指揮をとる市場主導のアプローチがある。この非営利団体は、「ユーザーが許可する金融データ共有のための共通の相互運用性があり、ロイヤリティ無料の技術標準を中心に、金融サービスのエコシステムを統一することに専念している。」という。[5] 現在、データプロバイダーとデータコンシューマーの両方で200以上の参加者がいる。この市場主導型アプローチは、米国でもカナダでも、ある程度の規制によって補完される可能性がある。

ブラジルは規制当局型アプローチで2021年に本稼働を開始し、多くのデータ保有者とリライング

[4] https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk
[5] https://www.financialdataexchange.org/FDX/FDX/About/About-FDX.aspx

パーティ（RP）にそのAPI標準に準拠することを義務付けている。2021年にオープンインシュアランスを開始し、オープンヘルスは初期段階にあるが、公開協議はまだ行われていない。

ラテンアメリカの他の地域では、メキシコがオープンバンキングの法案を発表し、他の国も今後数年間で同様の法案を導入する方向である。

インドには、「India Stack」の一環として、オープンバンキングに分類されるさまざまな構想がある。規制当局主導のUPI（統合決済インターフェース）は、銀行間決済のための標準との接続を提供する。データ面では、DigiSahamati財団（Sahamati）が「アカウントアグリゲーション（複数の金融機関の口座情報を一つの画面に表示するサービス）エコシステムのための自己組織化した産業主導型の提携」である[6]。特筆すべきは、インドはユーザー数が最も多く、India Stackの市場横断的な展開を目指していることである。また、インド、OIDF、その他のオープンバンキングのオピニオンリーダーの間で、世界的な相互運用性を検討する初期段階の協議が行われている。

欧州以外では、EU加盟国ではないがノルウェーがPSD2の規制下にある。しかし、スイスはそうではない。スイスでは現在もオープンバンキングに向けた動きがあるが、これは主に市場主導で、中小企業向けのユースケースから始まっている。ロシアはすでにオープンバンキングを導入しており（FAPI プロファイルを使用）、グルジアとウクライナ（現在の紛争以前）でも積極的な動きがあった。

アフリカでは、ナイジェリア、ケニア、ルワンダ、南アフリカでオープンバンキングの取り組みが初期段階にある。ナイジェリアでは、オープンバンキング・ナイジェリアが、ナイジェリア中央銀行（CBN）やその他の出資者と協力し、市場主導と規制当局主導のハイブリッド型のアプローチで取り組みを主導した。多くの標準は、中央銀行による指導をうけながら、市場によって作成された。主な目標は明らかに金融包摂で、「スマートフォン」だけでなく「フィーチャーフォン」のユーザーも利用できるようにする取り組みに表れている。これにより複数の市場に利益をもたらすことができる。ナイジェリアでの実施は2022年に開始される予定だ[7]。

日本では、早くも2015年からオープンバンキングを推進する規制当局の取り組みがあったが、APIの展開は主に市場主導で行われ、純粋に規制当局のアプローチを適用している他の国・地域に比べて遅くなっている。

中東では、サウジアラビア中央銀行（SAMA）が2020年にオープンバンキングへの取り組みを開始し、（2023年初頭に）決済および、その後に業種に特化した市場が続くが、2022年後半には本稼働を予定している。また、UAE、バーレーン、イスラエルでもオープンバンキングに関する積極的な取り組みが行われている。

オープンバンキングは、世界中に波及している動きである。

## 銀行業務以外には広がらないか？

同じ理由で、規制当局は他の金融商品やユーザーデータをより一般的に応用することを支持して

[6] https://sahamati.org.in/about/
[7] https://openbanking.ng and https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf

いる。「オープンファイナンス」は「オープンバンキング」を単純に拡大したものである。多くの銀行は、銀行口座だけでなく、投資、保険、クレジット商品も提供している。ユーザーの立場からすれば、オープンバンキング法の下で、銀行口座のデータは共有できるが投資口座のデータは共有できないというのは奇妙なことである。多くのエコシステムは、オープンバンキングからオープンファイナンス、そしてオープンデータへと移行しつつある[8]。

オーストラリアの2017年の「消費者データの権利（CDR）」法制、EUのGDPR、ブラジルの最近の規制などに、こうした傾向の明確な例を見ることができる。ユーザー、あるいは「データ主体」に、自分のデータに安全にアクセスし、好きな相手と好きなように共有する権利を与えようという動きがある。これは根本的な転換である。歴史的にみて、企業は保有するユーザーデータを自社の財産とみなしてきた。この新しい法律は、そのような価値観を変え、ユーザーの明確な権利を確立するものである。オーストラリアは、CDRによって、銀行業務以外のユーザーの要求を想定し、実質的な一歩を踏み出した。彼らのアプローチは、意図的にすべての金融口座を包含するように設計されている。また、オーストラリアは、公共インフラ事業（2022年）およびその後の通信事業への参入を目指す最初の市場でもある。

ブラジルでは、中央銀行がオープンバンキングを、民間保険監督局（SUSEP）がオープンインシュアランスを2021年に導入した。SUSEPは年金に関する権限もあり、別途、政府主導でオープンヘルスの実施を模索している。

この傾向は、投資口座、外国為替、年金、政府のデジタルIDとデジタルサービスにも拡大すると予想される。とはいえ、退職を目的とした商品、例えば年金に関しては、いくつかの違いがある。多くの国・地域では、ユーザーは複数の「年金」を持つことができるが、そのすべてがオンラインによるアクセスを提供するとは限らない。年金データへのアクセスが年金ダッシュボード・プロジェクトによって管理されているイギリスでは、これが当てはまる。このプロジェクトはオープンバンキングと同様のデータAPIを持っているが、認可と同意に関しては明確な違いがあり、ユーザーがデータプロバイダーと直接デジタルIDを確認する代わりに、中央の「同意と認可」サービスを通じて一元的に確認が行われる[9]。 この異なるアプローチは消費者にとって明確な利点があるが、既存のオープンバンキングのエコシステムとは相互運用性がない。年金をカバーするオープンファイナンスの取り組みは、国際的にはまだ初期段階にあるため、より統合された他のアプローチが登場するかもしれない。

政府のユースケースも出現している。シンガポールはAPIを通じて、政府部門と民間部門の両方のユースケースを可能にした。例えば、Singpass APIは、データとサービスが組織を越えて移動可能な信頼できるデジタルエコシステムを構築している。別の例としては、SGFinDexがある。SGFinDexは、国家デジタルアイデンティティ（Singpass）と、中央管理したオンライン同意システムを使用して、個人が異なる政府機関や金融機関にまたがる金融情報にアクセスできるようにしている。他の市場で、実装する構成要素が共通している場合、オープンデータと政府のユースケースの統合を検討することがあるかもしれない。

健康情報に関しては、アメリカやイギリスのようないくつかの市場ではすでに医療記録を共有す

[8] オープンデータはこれまでノンユーザーデータという意味だった。 例えば為替レート。しかし近年、金融データばかりでなく医療データなどすべてのユーザーデータを包含するのに使われている。
[9] https://www.pensionsdashboardsprogramme.org.uk/publications/blogs/the-central-digital-architecture

るためにOpenID Connectが使われている。データに対するユーザーによるより良い管理が、患者のケアや権限付与にどのような意味を持つのか興味深い。

また、医療および政府部門の両方がAPIベースのテクノロジースタックを採用するのが遅れていることに注意する価値がある。

しかし、COVID（検査と予防接種）による圧力や、政府の給付金詐欺という深刻な課題が、これらの部門に対してユーザー、政府、社会のニーズを満たすための技術基盤や標準を再評価する必要性を強いている。

## 市場主導か規制当局主導か

世界全体でオープンバンキングには市場主導型と規制主導型の二つの主なアプローチがある。

### 市場主導

一部の国・地域、特に米国（Financial Data Exchangeが主導）、シンガポール、ニュージーランド（patays.nzが主導）では、オープンバンキングに関しては市場が主導権を握っている。市場主導のアプローチは、実装コストが低くすむのと、規制当局が主導する場合、厳格になりすぎるなどのデメリットを回避するというようなインセンティブと適合するかもしれない。例えば、FDXは2018年以降、税金を投入することなく600万ドルを費やしている（従業員12名）。一方、イギリスのOBIEはCMA（競争・市場庁）の9銀行（従業員102名）から1億7500万ユーロを費やしており、オーストラリア政府は2021/22年[10]のサイクルで1億1100万ドルを拠出している。さらに、法律は規範的すぎる場合がある。例えば、EUの決済サービス指令（PSD2）では、ユーザーは90日ごとにデータへのアクセスを再認証しなければならないと定めている。この要件は消費者を保護するために設計されたものだが、意図しない結果を招き、一部の消費者やビジネスモデルに不釣り合いに大きな影響を与えた[11]。[12]

市場主導型の潜在的な欠点に、普及の実現に苦労する可能性があること、インセンティブが働かい場合にすべてのユーザーにサービスが行き渡らない可能性があること、市場間や特化した業種間の相互運用性が欠如している可能性があることがある。オープンデータ構想はネットワーク効果のリスクにさらされている。「市場」がユーザーやデータ保有者のクリティカルマスを達成できなければ、エコシステムは成功に必要な好循環を作ることはできない。例えば、アプリは十分なユーザーを確保したいと考え、ユーザーはプロバイダーを超えてデータにアクセスできることを望んでいる。さらに、インセンティブモデルは、サービスプロバイダーがすべてのユーザーにサービスを提供する動機をもたせるのに十分ではなく、一部ユーザーを置き去りにする可能性がある。最後に決して軽んじるべきでないことだが、適用を単一の市場主体で特化した業種にする場合、異業種への拡大やグローバルな相互運用性の障壁となるカスタムアプローチが開発される

[10] FDX分析

[11] 個人資産管理 (PFM)ソフトは、 シンセティック当座貸越（口座残高にもとづき、自動的な貸方と借り方を作ることで当座貸越をシミュレートするサービス）ほど規則に影響を受けない。さらに、複数の銀行口座をもつ消費者は、はるかに多く定期的な再認証フローを経験しなければならないため、実質的に不利であった。

リスクが高い。

## 規制当局主導

イギリス、オーストラリア、ブラジルのような多くの国・地域では、規制当局が中心となって、主要な市場参加者に明確な義務付けと期限を設け、銀行にオープンバンキングを義務付ける法律を制定している。

オープンバンキングには4つの明確な公益があり、政策や規制はこれに対処する傾向にある：

1. 競争
2. イノベーション
3. 同意に基づくデータ共有
4. 認可された企業のみがアクセス可能

### 1. 競争

市場競争を起こすことがイギリスでの推進力であった。実際、オープンバンキングは競争規制当局であるCMA（競争市場庁）によって開始した。小売銀行業務に関するCMAの調査では、イギリスの主要銀行間の競争不足が指摘されたのと、透明性を欠いた手数料や料金にエンドユーザーが悩まされていることがわかった。CMAは、銀行に利用者データへのAPIアクセスを義務付けることで、消費者が自分に最適な銀行を見つけられるよう支援する新しいサービスが可能になると判断した。

銀行が提供する金融商品の比較、銀行口座の切り替え、複数の銀行口座の運用はすべて、オープンバンキングがより簡単にすることを目指していることだ。これらのサービスは、以下のようなAPIを通じて取引データにアクセスできるようにすることで可能になる：

- アカウント・アグリゲーション・サービス　- 消費者がすべての口座を一箇所で簡単に確認できるようにすることで、消費者は単一のサービス提供者の利用に縛られることなく、異なる銀行の複数の金融商品を同時に利用することができる。
- 正確なアカウント比較　- 消費者が別の銀行の金融商品を利用した場合、銀行手数料としていくらかかるかを消費者に正確に示すことができる。
- 総合的な当座貸越　- 企業が、当座貸越と同様の機能を持つ自動的な短期信用商品を消費者に提供することができる。

イギリスが規制を導入した原動力は、"ユーザーによるデータへのアクセス "だった。EUがオープンバンキングを推進した主な要因は決済だった。銀行にAPIを公開させ決済を可能にするよう強制することで、EUの政策立案者はカードネットワークの独占を崩し、欧州全体での決済にさらなる競争を導入することを望んでいた。EUの第2次決済サービス指令の重要な条件は、銀行は決済を開始する「決済開始サービスプロバイダー」に対して手数料を請求したり、契約を要求したりしてはならないというものだった[12]。

オーストラリアでも、競争が「消費者データ権」法制化の主な原動力となった。プロジェクトの

[12] https://en.wikipedia.org/wiki/Strong_customer_authentication

概要にはこうある：

> 「CDRは、消費者のデータへのアクセスと管理を強化し、消費者が製品やサービスを比較し、切り替える能力を向上させる。CDRは、サービス提供者間の競争を促進し、顧客にとってより良い価格となるだけでなく、より革新的な製品とサービスを提供することにつながる。」[13] [14]

世界的に見ても、他国の規制当局も同様の論拠を用いている。

## 2. イノベーション

オーストラリアの CDR （消費者データ権利）導入で指摘されたように、イノベーションもオープンバンキングへの移行におけるもう一つの重要な推進力である。オーストラリアの規制当局は、API がより広範な経済におけるイノベーションを可能にすることを認識し、金融サービスにおけるイノベーションを促進することに熱心であった。

イギリスも同様である。イギリスのオープンバンキング規制のきっかけとなった2016年の報告書では、APIのイノベーションによる利点を次のように紹介している：

> 「API技術は、オンライン環境におけるデータ共有と機能性組み込みの標準として受け入れられている。API利用は広く普及しており、現在では14,000以上の公開APIが利用可能だ。最も人気のあるAPIには、フェイスブックやグーグルマップといったおなじみの名前があり、『いいね！』ボタンや地図を埋め込むためにウェブ上で広く使われている。多くのウェブサイトが他社のAPIを幅広く利用しており、その結果、イノベーションと消費者の利便性が大きく向上している。APIは、オープンバンキング標準を実現するための基本的な 要素である。」[14]

規制当局は、署名だけで、金融サービスにおけるイノベーションの足がかりを提供することができた。イギリスで規制が開始された翌年には、100[15]を超える企業（多くは新たに設立された企業）が、イギリスにおけるオープンバンキングのエコシステムへのアクセス許可を規制当局から取得した。多くの革新的な金融商品が発売され、2022年1月現在、イギリスのオープンバンキングによるサービスの実際の利用者は500万人[16]に達している。

## 3. 同意に基づくデータ共有

EUのGDPRは、EU域外でも企業のデータに対する取り組みに大きな影響を与えた。GDPRは「データ主体」の数多くの権利を成文化した。その一つが「データポータビリティの権利」であり、データ主体は「構造化され、一般的に使用され、機械で読み取り可能なフォーマット」で自分のデータにアクセスすることができ、「それらのデータを別の管理者に送信する権利を有する」ことが求められる[17]。GDPRでは、これは一般的な権利であり、データ管理者はこれを遵守するための様々な方法がある。オープンバンキングのデータアクセス面は、基本的にこの権利をより規範

[13] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0
[14] http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf
[15] https://content.11fs.com/reports/open-banking-in-the-uk-whats-happened-so-far
[16] https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2753-1-1

的に導入するものである。銀行が同一のAPIアクセスを提供し、登録された第三者サービスプロバイダーに支障なくこのアクセスを提供することを義務付けることにより、規制当局はユーザーがスムーズなデジタルでの同意プロセスを通じてデータを共有できるようにさせられるようにすることができた。

4. 認可された企業のみがアクセスできる。

ほとんどのオープンバンキング規制の特徴的な点は、参入企業の登録簿が作成され、どの企業が登録できるかを規定するルールが作成されることである。これは、通常民間企業によって管理されている他のほとんどのAPIエコシステムとの重要な違いである。対照的に、既存の金融規制当局は、どの企業がオープンデータ台帳に登録できるかを決定する役割を担い、そのルールを政策および運用上の管理を通じて実施している。

通常、当局の登録システムは、民間団体または地方自治体に対し、エコシステムを管理するための制御ポイントを提供する。このガバナンス機能については、ある政府は、民間セクターが行うのが最善であると結論付け、ある政府は政府が行うのが最善であると結論付けている。また、オープンバンキング管理団体を政府が監督するハイブリッド型モデルもある。

### 市場主導＋規制当局主導の「ハイブリッド型」

先に述べたように、ナイジェリア市場において1つの「ハイブリッド」な例が見られる。この例では、ナイジェリア中央銀行（CBN）の指導のもと、ナイジェリア市場が基準とアプローチの主導権を握った。2022年を目標とした実施計画であり、アフリカやそれ以外の他市場への導入の進捗と、またどのような知見が得られるか期待したい。

## 実装に関する考慮事項

オープンバンキングやオープンデータAPIを展開するエコシステムには、多くの重要な決定事項がある。OpenID Foundationの見解に基づく最も重要なものをいくつか紹介する。

### 機能仕様

データ交換や決済の開始に使用される実際の機能APIは、エコシステム特有のものである可能性が高い。例えば、以下のようなAPIである：

- 3ヶ月分の当座預金データを取得する
- 公共料金を支払う
- 最新の口座評価を入手する

機能仕様は通常、市場が達成しようとするユースケース、ユーザーに開放したいデータ、運用要件に依存する。このような機能仕様はまた、時間の経過とともに拡張や適応も容易となる。対照的に、セキュリティのプロファイルに変更を加えることは、費用がかかり、リスクも高い。

これは、エコシステムがセキュリティプロファイルを機能APIから分離することが重要である主な

理由である。OpenID Foundationが推奨するOAuth 2.0の設計の重要な点であり、安全に分離することができるようになっている。セキュリティプロファイルは、参加者の認証、同意、認可、安全なアクセスをカバーするべきである。それぞれの国や地域ごとの市場は、セキュリティプロファイルを分離できるグローバル標準仕様の恩恵を受けながら、機能仕様を管理することによる利点をすべて享受することもできる。

OpenID Foundationの金融グレードAPI（FAPI）ワーキンググループは初期の段階で機能APIの標準化を検討したが、その時点では実用的ではなく、市場の需要もないと結論づけた。国境を越えたユースケースをサポートすることへの関心が成熟するにつれて、これは変わるかもしれない。

## 明確な同意

明確な同意は、オープンバンキングやオープンデータの運用の基本である。ユーザーは、自分がどのようなデータや行為に同意しようとしているのか、アクセスはどのくらいの期間なのか、そのような同意を与えることの意味を正確に知る必要がある。同意を得るまでのプロセスが明確で有益なものとなるよう、顧客エクスペリエンスのガイドラインを策定することが重要である。

## セキュリティプロファイルの選択

一部のエコシステムは、「単独で」独自のセキュリティプロファイルを開発することを選択した。しかし、現在までのところ、FDX（アメリカとカナダで運営）、イギリス、オーストラリア、ブラジル、ナイジェリア、ニュージーランド、ロシアなど、ほとんどの市場がグローバルなオープン標準であるFAPIセキュリティプロファイルを選択している。FAPIを選択した市場のうち、イギリスやブラジルのような一部の市場は、エコシステム特有の要件を追加したり、実装の選択肢を減らしたりするなど、FAPI上に独自のプロファイルを追加することを望んだ。これらの市場は、OpenID Foundationと協力して「国内」FAPIプロファイルを開発し、「主要」FAPIプロファイルに可能な限り近づけるようにした。ロシアは、FAPI標準を選択したが、自国でFAPIプロファイルを開発した市場の例である。もし国内のプロファイルにふさわしい追加要件があるのであれば、開発中にそれを監視する「目」を増やし、それを維持する国内市場の費用を抑えるために、OpenID Foundation はこの作業を共同で行うことを推奨している。

FAPIを選択し、OpenID Foundationと提携する主な利点の一つは、 コンフォーマンス（仕様準拠確認）テストスイートへのアクセスができることある。これらの包括的なテストにより、国内市場はテスト開発コストを削減し、市場投入までの時間を短縮し、セキュリティおよび運用上のリスクを低減し、すべての市場参加者に利益をもたらすことができる。市場が国内プロファイルを希望する程度に応じて、OpenID Foundationは国内プロファイルのテスト開発、認証、および保守に関して国内市場と提携することもできる。

## 認証の義務化と義務化なしの比較

OpenID Foundation は、義務付けが実装を進めるのに役立つと見立てている（イギリスやブラジルなど）。もし、参加者に実装を即し、タイムリーに実装する十分な動機付けががなければ、ユーザーの取引意欲と参加者のAPI 実装意欲を高めるような規模を達成することは困難である。ブラジ

ルの中央銀行による指令は、データ保有者（銀行など）とRP（銀行、フィンテック、ユーザーによって認可された他の団体など）の両方の市場全体の認証を確保するための有用なツールであることが証明されている。OpenID Foundationは、ブラジルで行われたデータ保有者とRP（依拠当事者）に対するオープンバンキングへの対応の義務付けが、短期間（9ヶ月以内）でエコシステム参加者の認定数を有意義なレベルまで規模拡大を推進したこと見ている。しかし、義務化されていても課題はある。注目すべき点は、実運用環境のシステム認定は、相互運用が「普通に機能する」ことから受ける十分な恩恵を確保するために必要だが、開発環境の認定は、相互運用性の課題を回避するのに十分ではないことである。

## 監視

オープンデータエコシステムは、適切な監視とガバナンス機構を持つことが重要である。市場主導の国・地域では、これは通常API標準を定義する団体が対応する。しかし、規制システムにおいては様々なアプローチがある。時には規制当局がその仕事をすることもあれば（ブラジル）、独立した評価委員を持つ特定のエンティティが設立されることもある（イギリス）。エコシステムにおいて監視の役割を担う組織は、すべての参加者がエコシステムのルールやガイドラインに沿って運営されていることを確認するための十分なリソースを有していることが重要である。

ブラジルでは、監視責任を負う中央組織が存在することは注目に値する。この現在の「初期構造」は、現在のオープンバンキング業務と、数ヵ月後の「恒久的構造」への移行に責任を負っている。

## 顧客エクスペリエンスのガイドライン

APIに関する技術的なルールやアクセス要件に関する政策ルールだけでなく、顧客エクスペリエンスに関するガイドラインがあることも重要である。これにより、参加者全体で一貫した方法をとることを確保し、データプロバイダーがエンドユーザーに不必要な摩擦を与えることを防ぐことができる[18]。

## モバイルアプリ

市場にとっては、サービス開始時点からウェブベースとモバイルアプリベースの両方のジャーニーを実装に含めることが重要である。両プラットフォームを最初から想定しておかないと、セキュリティモデルを作り直すという重大な問題を引き起こす可能性がある。FAPI仕様は、モバイルアプリをサポートする二つの異なる方法をサポートしている：

1. アプリからアプリへのリダイレクト

これは、ユーザーがデータプロバイダーのモバイルアプリ内で、通常行うフローで認証することで、ユーザーが認証フローの一部としてアプリ間で途切れなくリダイレクトされるもので、多くの場合、生体認証を使用する。主なFAPI仕様はこのフローをサポートしているが、規制当局主導のオープンデータエコシステムがこのアプローチをサポートすることを義務付けることが重要である。FAPIは、強力なセキュリティ保証と相まって優れた利用者体験を提供し、イギリス市場で

[18] イギリスで例がある。: https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/

は、データへのアクセス認可に成功したエンドユーザー数が400%以上向上した[19]。

2. デカップルド認証

このフローでは、ユーザーがサービスを受けるデバイスとは別のデバイスで認証を行う。POS 端末にいるユーザーがスマートフォンで認証できるようになる。FAPIは、CIBAプロファイルを介して、この流れをサポートしている。

ナイジェリアのような一部の市場では、フィーチャーフォンのユーザーをサポートすることに熱心で、フィーチャーフォンはテキストベースのモバイルのユースケースでは、USSD標準に依存している。OpenID Foundationはナイジェリアと協力し、ナイジェリアとナイジェリア以外のフィーチャーフォンユーザーをサポートする方法を模索している。

### スクリーンスクレイピング

スクリーンスクレイピングやクレデンシャル情報の共有の必要性を排除することは、セキュリティおよびユーザー同意の課題を解決するための、オープンバンキングの目標の一つである。実装を設計する際には、既存のスクリーンスクレイピング・サービスがどのように新しいプラットフォームに移行するかを検討することが重要である。オープンバンキングは、スクリーンスクレイピングやバッチ転送によって追求されるユースケースを網羅するように設計する必要があるため、参加エンティティは、より安全なAPIと同意に基づく顧客データへのアクセス方法に移行することが奨励される。

また、オープンバンキングAPIを通じてすべての機能が利用できるようになった後、スクリーンスクレイピングが禁止されれば、実装が促進される。

## オープンデータ標準の選択

規制当局や市場イニシアティブは、オープンバンキングやオープンデータAPIに明確な根拠を持っている。しかし、これらのAPIはどのような標準に従うべきなのだろうか？

答えるべき主な質問は3つある：

1. どのデータモデルを使うか
2. どのようなデータフォーマットとトランスポートを使うか
3. APIはどのように保護され、アクセスが認可されるのか

[19] https://openid.net/guest-blog-implementing-app-to-app-authorisation-in-oauth2-openid-connect/

### データモデル

データモデルの問題は重要ではあるが、解決はそれほど難しくない。OBIEやベルリングループのようなエコシステムは、ISO20022に基づいたデータモデルを選択している。ISO規格は「残高」とは何かを定義し、様々な口座の種類を定義するのに役立つ。FDXやオーストラリアのように、独自のデータモデルを構築した市場もある。国・地域がISO20022を採用するにせよ、他の規格を選択するにせよ、明確な要件はデータモデルとスキームが明確に定義され、文書化されていることである。ロードマップの一部として、データと決済の国際的な相互運用性に関心を持っている市場は、将来の開発負担のリスクを軽減するために、ISO20022を選択することを望むかもしれない。

### データフォーマットとトランスポート

この質問も比較的簡単である。ほとんどのエコシステムはRESTful JSON APIを採用している。これは現在、より広い市場で最も頻繁にみられるアプローチだからである。特に、既存のXMLメッセージが定義されているレガシーAPIがある場合、一部のエコシステムはXMLもサポートしている。

### APIセキュリティ

これらの構想すべてに、以下の技術的要件がある：

- ユーザーが自分のデータやサービスへのアクセスを、ある企業から別の企業へ安全に許可できるようにすること

そして通常、いくつかの追加条件がある：

- 適格かつ基準に準拠した企業のみアクセス要求を許可する
- 顧客が細かくアクセス権を指定できるようにすること
- 顧客が付与したアクセス権を取り消すことができるようにすること

上記の問題は、2つの当事者間やプライベート・エコシステムのエンティティ間で使用される一般的なHTTP APIでは解決できない。すべての参加者が同じガバナンス体制もとで同じ標準を実装し、フェデレートベース（認証連携）で機能する3つ以上の当事者間の安全な相互作用が必要である。

## FAPIの開始

認証連携エコシステムの要件を満たすために最も広く使われている標準プロトコルは、OAuth 2.0である。

OAuth 2.0は2012年にIETF（インターネット技術特別調査委員会）によって発表された。第三者によるデータやサービスへのアクセスを可能にするために広く使われている認可フレームワークである。これはフレームワークであり、保護するサービスに応じてさまざまなセキュリティレベルで実装することができる。第三者によるデータやサービスへのアクセスを許可しているほとんど

の技術系企業は、すでにOAuth 2.0を使用している。

OAuth 2.0だけでは、オープンバンキングのエコシステムに求められる上記の要件を解決することはできない。そこで、OpenID Foundationの仕様の出番となる。

OpenID Connect Coreは、「OAuth 2.0プロトコル上のアイデンティティレイヤー」として2014年にOpenID Foundationによって公開された。これにより、ユーザーは「サインイン」によって「ソーシャルログイン」を行い、第三者のサービスに対してアイデンティティを確認することができるようになった。グーグル、マイクロソフト、アップルなどによって実装され、特化した業種の市場を横断したB2C、B2B、B2B2Cのユースケースで、世界中の何十億もの人々に利用されている。さらに、OpenID Connectの設計には、OAuth 2.0のセキュリティを強化するための追加のセキュリティメカニズムが組み込まれている。

2016年、金融サービスにおける安全なAPIを実現するためのセキュリティ勧告と仕様を提供することを具体的な目標としてOIDF FAPIワーキンググループが結成された。ワーキンググループはすぐに、現在FAPI 1.0 BaselineとFAPI 1.0 Advancedと呼ばれる二つのセキュリティプロファイルに焦点を当てた。この2つのプロファイルは、OAuth 2.0およびOpenID Connectの成果を基に、金融サービスでの使用に適したセキュアなOAuth 2.0プロファイルを提供するために設計されたものである

FAPIワーキンググループで開発されたプロファイルは「チェックリスト」方式で記述され、開発者が自分たちのソフトウェアがプロファイルを正しく実装しているかを検証するための自動適合性判定試験が用意されている。これらの標準は、孤立して開発されたわけではなく、当初、ワーキンググループは、英国のOBIE、ISO TC68、ブラジルの中央銀行、オーストラリアの消費者データ標準機構、FDX、FDATA等に協力を求めた。FAPI1.0標準はまた、シュトゥットガルト大学によるWIM法を用いた包括的なセキュリティ分析の主体となっている[20]。

この作業は、OBIEが最初の規制主導型オープンバンキングイニシアチブを導入し、エコシステム内の銀行および第三者にFAPI標準の使用を義務付ける道を開いた。イギリスだけでなく、FAPI標準はその後以下の国でも採用された：

- 米国およびカナダ（ファイナンシャル・データ・エクスチェンジを通じて）
- オーストラリア
- ブラジル
- ナイジェリア
- ニュージーランド
- ロシア
- ISO TC68 SC9 WG2 - WAPI[21]

実際、オープンバンキングとオープンデータに移行した市場の大半はFAPI標準を選択している。FAPI標準は、同意に基づくオープンデータ展開における最も困難な問題を解決するための基盤を

[20] Daniel Fett, Pedram Hosseyni, and Ralf Küsters, An Extensive Formal Security Analysis of the OpenID Financial-grade API. 2019 IEEE Symposium on Security and Privacy (S&P 2019). (Technical Report)
[21] https://www.iso.org/standard/74353.html

提供する。本書ではこのあと、それがどのように行われるかを説明する。

## FAPIセキュリティプロファイルを選ぶ理由

エコシステムの中には、独自のセキュリティプロファイルを開発したり、構築したりするものもあるが、OpenID Foundationが提供するFAPI標準とサービスを選択することには、大きな利点がある。

### 実証済みであること

FAPIは実証済みである。複数の国・地域で大規模に導入されている。FAPIを選択することで、運用上の失敗のリスクを減らすことができる。

### セキュア

セキュリティプロファイルの最初の決定プロセスにおいて、FAPIを採用することで、 「単独で行う」場合に比べて、実装のセキュリティリスクを軽減することができる。FAPIは安全である。多数の侵入テストに耐えただけでなく、一流の学術セキュリティ研究者による正式なセキュリティ分析も受けている。対照的に、最大規模の市場であっても「単独で」一から堅牢で安全なフレームワークを構築するには膨大な作業が必要となる。

ある政府関係者が指摘するように、これは単に初期段階だけでなく、継続的なメリットを持つ。世界中でFAPIの実装を改善する必要があるかどうか数百人の専門家の目が働いており、FAPIの継続的な品質が維持されている。例えば、FAPIワーキンググループには、いくつかのPSD2 APIに存在する「クロスブラウザ決済開始攻撃」[22]を発見し、修正を迫ったセキュリティ専門家が含まれている。独自開発の実装では、実装を監視する「目」の数が少ないため、セキュリティプロファイルを特定し、修正し、維持する人員が少なくなり、運用／セキュリティリスクと維持コストの両方が増加する可能性がある。

### コスト削減とベンダーサポート

FAPI を選択することで、規模の経済が導入され、エコシステム参加者のコストが大幅に削減される。FAPI標準はRFC群に基づいて構築されているため、「すぐに使える」ベンダーサポートが充実しており、FAPIセキュリティプロファイルはアイデンティティおよびアクセス管理業界のほとんどのベンダーによって実装されている。これは、エコシステムが FAPI を選択する場合、コストのかかるカスタマイズや特注作業が少なくて済み、ベンダーロックインや下流での切り替えコストを削減できることを意味する。標準が成熟し、広く採用されていることは、エコシステム内のデータ受信者が実装を加速するために使用できるOpenID ConnectとFAPIを実装する複数のオープンソースライブラリが存在することも意味する。最後に、実装に取り組み、知見を共有する専門家のグローバルコミュニティは、セキュリティと運用のリスクを低減するだけでなく、特注の規格を維持するための運用コストも削減する。

[22] https://bitbucket.org/openid/fapi/src/master/TR-Cross_browser_payment_initiation_attack.md

## 市場の要求に適応できる

FAPIは、OpenID Connectよりもリスクの高いユースケースに対応するように設計されている。しかし、FAPI群の仕様の中には、エコシステムのオピニオンリーダーが「プログレッシブプロファイリング」を実行できるように、baseline（基準版）やadvanced（高度版）といった多くの選択肢がある。つまり、規格そのものが、さまざまな特化した業種の市場でのユースケースや国際的相互運用性のための基盤へのオーバーレイを真剣に考慮している。これによって、あらゆる体制のセキュリティニーズとセキュリティ態勢に見合った標準が可能になり、また、法律や規制の枠組みの中で「目的に合った」モジュール化を行うことができる。

## 適合性判定試験と認証

相互運用性とセキュリティを確保するためには、標準を選ぶだけでは十分ではない。異なるソフトウェアが標準を正しく実装していることを確認する唯一の方法は、包括的な適合性テストを通じて、実装前にすべての関係者がテストされていることを確認することである。この適合性判定アプローチ（準拠確認による方法）は、一貫した利用者体験を保証し、サポートコストを大幅に削減し、データプロバイダーとデータコンシューマーが標準とエコシステムに対する義務を遵守していることを確認できる。適合性判定テストがないエコシステムでは、データプロバイダーとデータコンシューマーの双方にとって、相互運用性を阻害する問題を改善するための広範な労力を要することが多く、実装コストと運用サポートコストが高くなることが多い。これは、開発者がミスを犯したり、標準の中の条項で異なる解釈をしたりする可能性があるためである。適合性判定試験は、こうした問題を開発中に発見し修正することを確実にする。開発中に修正するのは、非常にいいタイミングである。

稼働開始前の適合性テストは、エコシステムを迅速に調整させる唯一の方法である。40人の活動的な参加者がいるエコシステムでは、参加者間に1,560の異なる接続が存在することになる（負の「ネットワーク効果」の例[23]）。1,560の接続を手作業で修正しようとしても、ただ時間がかかるだけであり、必然的にこれらの接続の一部は本番稼動せず、エンドユーザーに不利益をもたらすことになる。

本番稼働後は、すべての市場参加者の再認定の頻度に合意することも重要である。実装は、新機能、プラットフォームマイグレーション、その他の変更によって常に進化している。いかなる変更も、サービスのセキュリティや相互運用性に影響を与える可能性がある。再認定を受けることで、サービスが期待通りに運用され続けることが保証される。

OpenID Foundationは、グローバルコミュニティに対してオプションとして認定サービスを提供している。OpenID Foundationは自己証明方式を採用しており、認定を希望する、あるいは要求されるものにとっては低コストのモデルを保証している（認定価格は現在、会員一人当たりの1,000ドル、非会員5,000ドル）。またベンダーと市場参加者の双方が利用できる無料のテスト環境も用意されている。すべてのテストはオープンソースであり、標準との整合性を確保するために積極的にメンテナンスが行われている。2022年2月現在、OpenID Foundationは244のFAPIデプロイを世界的に認定しており合計739の認定があり、認定数は着実に増加している。イギリスとブラジルは参加者を登録するための適正手続きの一部としてOpenID Foundationの認定を義務付けており、これ

[23] https://en.wikipedia.org/wiki/Network_effect

はOpenID Foundationが推奨する方法である。OpenID Foundationが実施した認定はすべて公開されており、最新のFAPI認証はここからアクセスできる。https://openid.net/certification/#FAPI_OPs

OpenID Foundationはいくつかの適合性テストのパッケージソフトを管理しており、その中には特定のエコシステム向けのものもある。規制当局の中には、例えばブラジル中央銀行のように、データプロバイダーが標準への適合性を証明することを要求するものもある。ブラジルのモデル実装を担当するガバナンス体制は、OpenID Foundationの認定プログラムを選択し、データプロバイダーとRPの双方に認定を要求している。米国/カナダ（FDX）やロシアのようないくつかの市場はFAPIを選択しているが、（現時点では）OIDF認定プログラムの利用は選択していない。オーストラリアはベンダーやエコシステム参加者に OIDF 認定への参加を促しているが、その利用を義務付けてはいない。

## グローバル相互運用性

FAPIを選択することで、エコシステムはグローバルな相互運用性と国境を越えたユースケースへの道筋を保つことができる。例えば、国境を越えた医療記録、アイデンティティレコードの転送、金融口座の開設などは、共通のセキュリティプロファイルが使用されれば、すべて簡単になる。国境を越えた要件を持つユーザーや団体をサポートしたい市場参加者は、こうしたユースケースを可能にするオープンデータ標準の統合方法をすでに模索している。

## FAPIが選択されていない場合は？

オープンバンキングは本来、国内市場主導の取り組みであり、今後何年もその状況が続くであろう。一部の市場は、独自のオープンバンキング標準を開発する意欲と能力を持つと考えられる。

EUのベルリングループ、インド、シンガポールのようないくつかの先進的なエコシステムはすべて、それぞれの地域のオープンデータ要件をサポートするために標準化を追求した。インドは最大規模のオープンデータ実装を達成した点で称賛に値し、シンガポールは互恵的なアプローチで評価されている。ベルリングループの標準はEU全域で実装され、オープンファイナンスをカバーするために拡張されている。OpenID Foundationは、これらの市場の専門知識と強みを認識し、三つの市場すべてと関わり、その取り組みを統合する機会を模索している。現在グローバルな相互運用性は、高い関心を持つ領域となっている。

おそらくほとんどの市場は、独自のセキュリティプロファイルや関連する適合性テストの開発を望まず、代わりにFAPIを選択してセキュリティ要件を満たすだろう。市場は、世界的に実績のあるオープンスタンダードのセキュリティ上の利点を、コストをかけずに享受し、実装のすべての面を完全に自分たちで管理することができる。

OIDF は、FAPI を選択する市場もそうでない市場も含め、あらゆる市場のニーズをサポートするため、二者間で関与することを目指している。さらに、OIDF は「Smart Data Foundry Technical WG」ワーキンググループの「共同開催者」であり、政府、民間企業、学界を含む 20 カ国以上のオープンデータに関する代表が集まり、標準の統合について議論し、関心のある主要な学術的トピックを特定し、より広範なコミュニティとベストプラクティスを共有している。

# FAPI仕様

FAPIワーキンググループは多くの異なる仕様や文書を作成し維持している。これらはすべて、エコシステムに対して、安全で相互運用可能な金融グレードAPIの仕様を提供することを目的としている。

単にFAPIと呼ばれることが多い主な文書はOAuth 2.0のセキュリティプロファイルだが、ワーキンググループ内には4種類の文書がある：

- OAuth 2.0やその他の仕様のセキュリティプロファイル - セキュリティと相互運用性（FAPI 1.0やFAPI 2.0など）に関する具体的な実装ガイドラインを提供することを目的としている
- 新しいエンドポイントまたは操作を記述する仕様。例えばGrant Management（権限管理）など。このような文書は、FAPIセキュリティプロファイルを実装するエコシステム内でFAPI作業部会のメンバーが発見した特定の要件に基づいて作成される。
- 実装に関する助言、ガイダンス、セキュリティ勧告（例：クロスブラウザ決済開始攻撃）
- IETF OAuthワーキンググループにFAPIワーキンググループのメンバーが参加し、協力してRFCとして公開する仕様（例：RFC9126（OAuth PAR - Pushed Authorization Requests）

文書は、最終版の仕様として公表される前に、厳格な工程を経る。これには、公開レビュー期間、実装者向けのドラフト、そして多くの場合正式なセキュリティ分析が含まれる。

2022年3月現在の主要文書の概要は付録1、用語集は付録2、オープンデータの「構成要素」とFAPI 2.0のフレームワークの図は付録3にある。

# FAPIの未来

今後、OIDFがFAPIに関連して探求している3つの主要分野がある：

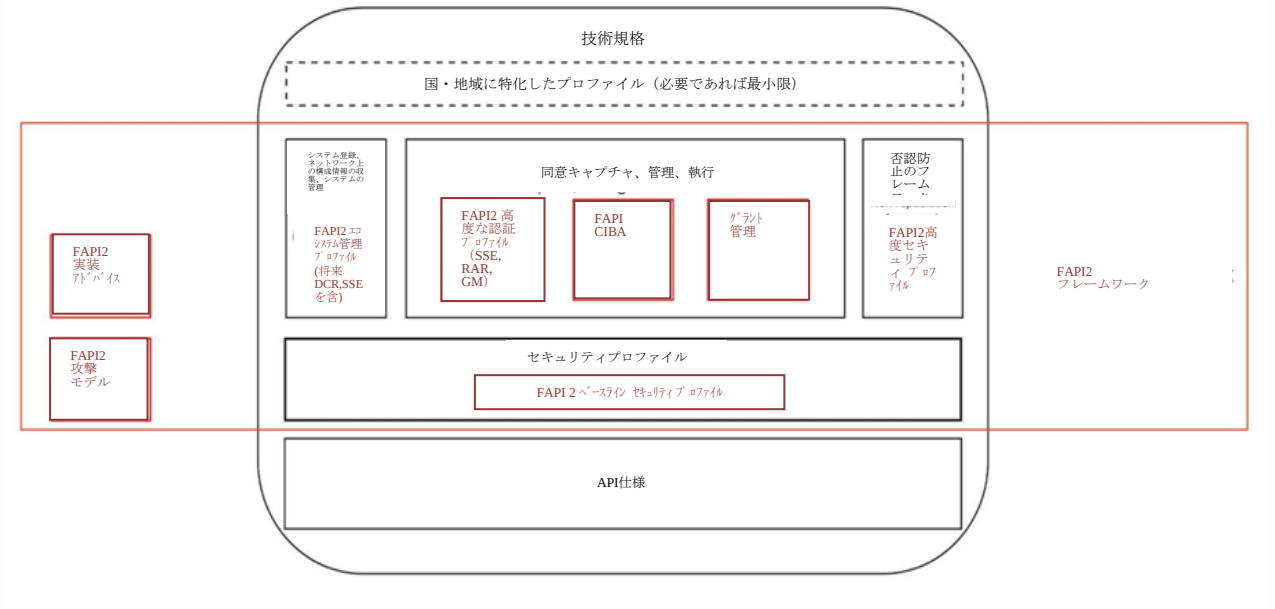
1. 市場ライフサイクル・サポート

オープンバンキングを積極的に模索または実装している20以上の市場において、OpenID Foundationはオープンバンキング、FAPIに関する知識を共有し、（FAPIを選択した場合）その実装をサポートする。

2. FAPI 2.0フレームワーク

FAPIワーキンググループは、FAPI 1.0の実装から学んだことを生かし、オープンデータエコシステムの実装に必要なすべての標準を提供するFAPI 2.0のフレームワークを構築している。これには、権限管理や動的クライアント登録などの新しい仕様や、デプロイに関するアドバイスの作業も含まれる。いくつかの市場は今年FAPI 2.0標準を採用しており、OIDFは2022年3月からFAPI 2.0 Baseline（基準版）とAdvanced（高度版）の両方でセキュリティ分析を進めている。オーストラリアは2023年にFAPI 2への移行を計画しており、他の新しいエコシステムはFAP1 2.0から始めることを検討するかもしれない。OpenID Foundationは再びシュトゥットガルト大学と協力し、FAPI 2のBaseline とAdvanced のセキュリティ分析を行い、2022年に完了する予定である。

この図は、FAPI 2フレームワークのさまざまな構成要素を示している：



## 3. グローバル相互運用性

相互接続が進む世界では、国境を越えた決済や医療データの安全な転送など、グローバルな相互運用性への欲求が高まっている。OIDF は、FAPI を選択していない組織も含め、この分野を探求するために多くの組織と協力し ている。さらに、OIDF はGlobal Assured Identity Network（GAIN）[24] に取り組んでいる。これは、保証されたアイデンティティのグローバルな相互運用性をサポートするという同様の目的を持っている。

## 4. 他業種での活用

元々FAPIワーキンググループは金融サービス内のAPIに重点をおいており、金融 API ワーキンググループと呼ばれていた。しかし、FAPIのセキュリティプロファイルが金融以外の他業種でも適しているという事実を反映するため、名称は 「金融グレード 」APIに変更された。OIDF は、金融、保険、医療、政府のユースケースを含むオープンデータのあらゆる側面に焦点を当てている。保険のようなユースケースの中には、FAPI標準（オーストラリア消費者データ標準に準ずる）を変更する必要がないものもある。このことは、市場投入のスピードを上げつつ、自国経済の多くの産業で標準化されたセキュリティフレームワークを展開しようとしている国にとって、コスト削減につながる。

より強固な医療基盤（コロナ以降）を構築できる可能性は、政府、医療コミュニティ、住民にとって魅力的である。OIDFは、FAPI（および OpenID Connect）が医療エコシステムのユースケースに適合するかを評価するために、6ヶ月間、医療セクターの調査を実施している。最初のドラフトは2022年4月に発表され、第2四半期と第3四半期に医療とアイデンティティのコミュニティにてリスニングセッションが行われ、2022年第3四半期に最終勧告が出される予定である。FAPIはノルウェーとブラジルで医療要件への対応が検討されており、OpenID Connect標準はすでに米国とイギリスで医療記録の共有に広く導入されている。

また、オープンデータと他の電子政府主導型との融合も見られる。ヨーロッパでは、eIDAS 2.0（EUデジタルウォレット）に関する新しい法律が、政府のデジタル資格情報発行のための二つの新しいグローバル標準（ISO 18013-5モバイル運転免許証、W3C検証可能な資格証明）と並行して進行している。これは、標準の統合あるいは分岐のために絶好の環境である。OpenID Foundation は政府関係者向けに2022年のホワイトペーパーを作成中で、サイバーセキュリティ、アイデンティティとアクセス管理、デジタルトランスフォーメーションに関する政府の長年の懸念と並行して、電子政府、医療、オープンデータの統合をどのように実現できるかを模索している。オープンデータをめぐる動きが市場主導型か規制当局主導型か、あるいは市場が特化業種に注目する順序に関係なく、これらの取り組みが共通の標準と「ネットワークのネットワーク」に前のめりになれば、人々は短期的にも長期的にも重大な利益を得ることができる。

[24] https://gainforum.org/

## OpenID Foundation

OpenID Foundation は非営利の技術標準化団体であり、その展望は人々がどこでも自分のアイデンティティを主張できるようにすることである。その使命は、安全で相互運用性が高く、プライバシーを保護するアイデンティティ標準の作成においてグローバルコミュニティをリードすることである。

当団体は、IETFのような純粋な標準化団体よりも広い権限を持つため、オープンデータAPIを実装する市場が目標を達成するのを支援することができ、以下を含め多くの方法でこれを行う：

- 他市場からのOIDFの学びを共有する
- 市場参加者にFAPI規格とそれが提供するものを理解してもらう
- 地方政府やオープンバンキング運営団体、オープンバンキング領域におけるグローバル団体とのパートナーシップを確立する
- FAPI規格が選択された場合、市場サポートを提供する：
    - 現地実装者に標準を説明するためのネット上のセミナー
    - ローカルセキュリティプロファイルなど、ローカル要件がFAPI標準によって満たされていることを確認する
    - 市場のプロセスや要件に沿った認定サポートを提供する
    - 問題の修復を支援する
    - アイデンティティ保証のためのOIDC、共有シグナルおよびイベントなど、将来的にローカル・ロードマップに適合する可能性のある他の標準について議論する
    - グローバルコミュニティが、グローバルな相互運用性を追求するのを支援する

この支援は、市場特有の開発作業や認証が必要な場合を除き、費用や義務を伴わずに提供される。OIDFは主に会員によって運営されている。すべての市場参加者は、OpenID Foundationの展望と使命の実現を支援するために、OpenID Foundationに加入することが積極的に推奨される。

## 結論

オープンバンキング、オープンファイナンス、オープンデータが登場し、これからも存在しつづけるであろう。エコシステムがこれらをどのように実装するかによって、コスト、イノベーション、セキュリティに多大な影響を及ぼす可能性がある。

OpenID Foundationは、この動きを可能にする開かれた相互運用性のあるセキュリティ標準を提供することに全力を傾けている。FAPI仕様を使用することで、エコシステムは実績のある厳格なセキュリティ標準を利用することができ、FAPIへの準拠を保証するために既存の認定テストパッケージソフトを活用することができる。

OIDFは、FAPI標準ファミリーを含むOpenIDのすべての標準(www.openid.net)の作業をサポートするために、OpenID Foundationへの個人、企業、組織の参加を心から歓迎する。

すべてのOIDFワーキンググループと同様、FAPIワーキンググループは透明性のある方法で運営されており、誰でも責任分担同意書（Contribution Agreement）[25]に署名するだけで参加し貢献することができる。 毎週定期的な接続があり、メーリングリストや課題管理システムがグローバルコミュニティとのつながりを保っている[26]。

FAPI ワーキンググループの詳細はこちら　https://openid.net/wg/fapi/

もしあなたがオープンファイナンスやオープンデータに取り組んでおり、OpenID Foundationについてもっと知ることを希望する場合、国内・国外で目標をサポートするので、こちらにメールして欲しい。director@oidf.org

一緒に働くのを楽しみにしている。

[25] この合意書関連では、費用はかかりません。詳細は以下のサイトに記載 https://openid.net/intellectual-property/
[26] https://openid.net/wg/fapi/ and https://bitbucket.org/openid/fapi/issues

# 付録1：FAPIの仕様[27]

以下は、FAPIワーキンググループが発表または貢献した主な仕様の要約である。

## Financial-grade API Security Profile 1.0 - Part 1: Baseline

ステータス：最終版
URL： https://openid.net/specs/openid-financial-api-part-1-1_0.html

これはOAuth 2.0のセキュリティプロファイルであり、ある操作やプロセスが持つ中程度の内在的な脆弱性やリスクを持つAPIの保護に適している。厳格なレビュー工程を経て、最終版の仕様として公開されている。

この仕様は当初「読み取り専用APIセキュリティプロファイル」と呼ばれていたが、多くのエコシステムにおいて「読み取り」APIは「書き込み」APIと同様に機密性が高いという事実を反映し、名称が変更された。

FAPI 1.0を実装しているエコシステムのほとんどは、advanced（高度版）プロファイルの使用を要求している。しかし、このプロファイルはパブリッククライアント（認証サーバーと直接コミュニケーションし、単一のクライアント識別子を共有するブラウザやモバイルアプリで実行されるソフトウェア）をサポートする唯一のFAPI仕様である。

## Financial-grade API Security Profile 1.0 - Part 2: Advanced

ステータス：最終版
URL： https://openid.net/specs/openid-financial-api-part-2-1_0.html

この仕様は、FAPI 1.0 – パート 1: Baseline（基準版）を基にしており、固有のリスクが高いAPIを保護するのに適している。この仕様も最終段階にある。

この仕様は当初「読みとり書きこみAPIセキュリティプロファイル」と呼ばれていたが、多くのエコシステムにおいて「読みとり」APIは「書き込み」APIと同様に機密性が高いという事実を反映し、名称が変更された。

これは最も広く実装されているFAPI仕様である。ほとんどの実装ではOpenID Connectの拡張として使用されているが、「vanilla OAuth 2.0」サーバーに実装することもできる。

## Financial-grade API: Client Initiated Backchannel Authentication Profile

ステータス：実装者向けドラフト
URL： https://openid.net/specs/openid-financial-api-ciba-ID1.html

欧州におけるPSD2イニシアティブとの継続的な連携の一環として、ユーザーと金融機関との間の

[27] ここでは、2025年4月10日現在の状態を記載した

以下の3種類の相互作用が特定された：

- リダイレクト - ユーザーはデータコンシューマーからデータプロバイダーにリダイレクトされ、同じデバイス上で認証を受ける（これは標準のOAuth 2.0ベースの相互作用である）。
- 分離 - データプロバイダーが別のデバイスでユーザーの認証を開始する。
- 組み込み - データコンシューマーはユーザーの「認証情報」を収集し、データプロバイダーを通して転送する

FAPI CIBAは、OpenID ConnectのCIBA仕様のプロファイルであり、Decoupled Flow（ユーザーが認証を行うデバイスとサービスを受けるデバイスが異なる場合の認証フロー）をサポートしている。例えば、FAPI APIを使ってPOS端末をサポートするなど、Decoupled Flowを必要とするユースケースは多い。

### Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

ステータス：最終版
URL：https://openid.net/specs/oauth-v2-jarm.html

この仕様は、OpenID Connectの一部として定義されたセキュリティ機能の一部をOAuth 2.0に実装するために、ワーキンググループによって作成された。FAPI 1.0 - Advancedの多くの実装では、認証レスポンスを保護するためにIDトークンをデタッチ署名として使用している。JARMは、サーバーがIDトークンを使用する必要なく認証応答に署名する方法を定義している。

### FAPI 2.0 Baseline and Attacker Model

ステータス：最終版
URL： https://openid.net/specs/fapi-attacker-model-2_0-final.html

FAPI 2.0はFAPI 1.0よりも広い範囲をカバーする。FAPI 2.0は、クライアントと認証サーバー間のインターフェイスにおける完全な相互運用性と、クライアントとリソースサーバー間のインターフェイスにおける相互運用可能なセキュリティメカニズムを目的としている。

その結果、FAPI 2.0は、認証フローのセキュリティに焦点を当てたFAPI 1.0ですでに定義されているメカニズムに加えて、APIアクセスのためのきめ細かいトランザクション認証を得るためのメカニズム、およびリプレイ検出のためのセキュリティメカニズムを提供する。

ワーキンググループはまた、様々なオープンバンキング実装の分析結果、最新のOAuthセキュリティBCPの勧告、包括的なセキュリティ脅威モデルに基づいて、開発者が使いやすいプロファイルに進化させた。

### FAPI 2.0 Advanced

ステータス：最終版
URL：https:/openid.net/specs/openid-financial-api-part-2-1_0.html

Advanced版のプロファイルは Baseline版 のプロファイルの拡張であり、リソースサーバーからの応答を含むすべての交換に対して否認防止を提供する。

### Grant Management for OAuth 2.0

ステータス：実装者向けドラフト
URL： https://openid.net/specs/oauth-v2-grant-management-ID1.html

このプロファイルは、データ主体が与える同意を表す「権限」を管理するための標準ベースのアプローチを規定している。このプロファイルは、PSD2の展開とオーストラリアにおける要求事項の経験から生まれた。

### RFC8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

状態：最終版
URL： https://www.rfc-editor.org/rfc/rfc8705.html

この仕様の認可者はFAPI ワーキンググループのメンバーであり、多くのFAPI実装の基本的な構成要素となっている。多くの金融エコシステムはすでに相互TLSを使用しており、相互TLSをOAuth 2.0とともに使用する相互運用のある方法を特定することは理にかなっていた。

### RFC9126 - OAuth 2.0 Pushed Authorization Requests (PAR)

ステータス：最終版
URL： https://www.rfc-editor.org/rfc/rfc9126.html

この仕様の初期バージョンは、FAPI 1.0の実装者向けドラフトで定義された。これは、認証リクエストパラメータを、フロントチャネルを通して渡すのではなく、サーバーに「プッシュ」する構造を提供する。これは、一つのAPI呼び出しを追加するだけで、セキュリティと簡素化をもたらす。

### OAuth 2.0 Rich Authorization Requests (RAR)

ステータス：最終版
URL： https://www.rfc-editor.org/rfc/rfc9396.html

本稿は、IETF OAuthワーキンググループの標準化過程に関するものである。これはFAPI 2.0のオプション部分であり、複雑な認証データ、例えば支払いを開始するために必要なデータタイプを提供するための相互運用性を提供する。従来のOAuth 2.0ベースのデプロイでは、ユーザーがアクセスを許可する操作（例えば 「プロファイルの読み取り」や 「タイムラインを公開」など）を示すために、粗い範囲（一般的な基準を基にアクセスを許可する広範囲の認証法）を使用している。FAPIの経験から、これでは多くのユースケースでは不十分であることが分かっている。多くのエコシステムはリッチ認証データの連絡に独自の方法を実装している。RARはこのための標準を定義している。

## OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

ステータス：最終版
URL： https://www.rfc-editor.org/rfc/rfc9449.html

本稿はIETF OAuthワーキンググループの標準化過程に関するものである。FAPI 2.0のオプション部分であり、送信者限定のアクセストークンにメカニズムを提供する。

## FAPI Developer Site

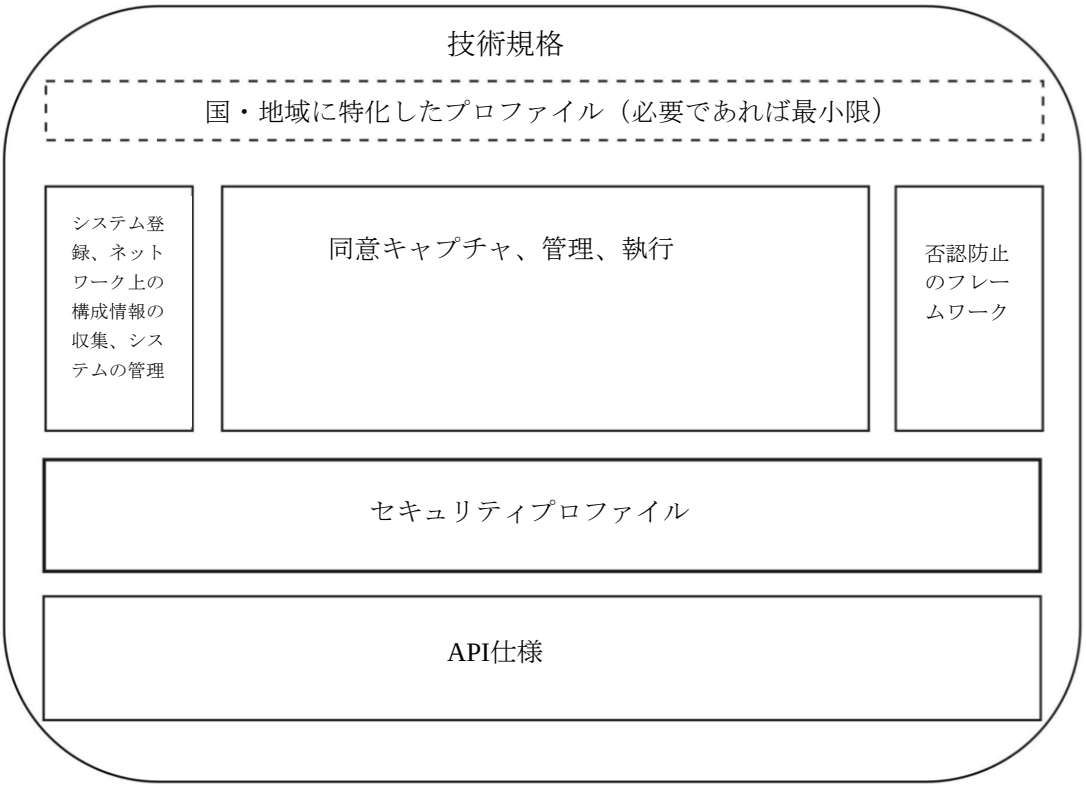
https://fapi.openid.net/

# 付録 2：用語集

| 用語 | 定義 |
|---|---|
| OAuth 2.0 | OAuth 2.0認証フレームワーク (RFC6749) |
| OIDC | OpenID Connect Core - OAuth 2.0プロトコル上のシンプルなアイデンティティレイヤー |
| 認証サーバー | サーバーは、リソース所有者を認証し認可を取得後、クライアントにアクセストークンを発行する。オープンバンキングの場合、これは銀行である。 |
| クライアント | リソース所有者に代わって、その認可のもとに保護されたリソースのリクエストを行うアプリケーション。オープンバンキングの場合、これは第三者である。 |
| リソース所有者 | 保護されたリソースへのアクセスを許可できるエンティティ。リソースの所有者が個人の場合、エンドユーザーと呼ばれる。 |
| データプロバイダー | エンドユーザーのデータを保有する企業。オープンバンキングの場合では銀行となる。 |
| データコンシューマー | エンドユーザーのためにデータプロバイダーからデータを消費するユーザーで、オープンバンキングの場合では第三者プロバイダーとなる |
| OIDF | OpenID Foundation - デジタルアイデンティティとセキュリティ標準に特化した世界的な技術標準化団体 |
| インターネット技術特別調査委員会 | Internet Engineering Task Force（インターネット技術特別調査委員会） - RFCを発行する世界的な標準化団体 |
| WG | ワーキンググループ |
| FAPI | OpenID FoundationによるOAuth2/OpenID Connectの Financial-grade APIプロファイル |
| MODRNA | Mobile Operator Discovery, Registration & Authentication (モバイル事業者の発見、登録、認証) |

# 付録3：オープンバンキングの構成要素

オープンバンキングのエコシステムを構築しようとするエコシステム参加者は、以下の構成要素を必要とする。



# 付録 4：FAPI 2 フレームワーク

FAPI 2群の仕様（赤字）は、主要な局所の区域に分かれている。これらの仕様は、下図のようにエコシステムの要求事項（黒字）の上に重なっている。