# 邦銀は英国を参考にAPIセキュリティーの共通化を急げ

## 国際的な技術仕様「FAPI（ファピ）」の標準化でコスト低減を

オーストリート
ソリューション戦略担当VP
工藤 達雄

エンドユーザーについてのデータや機能をサードパーティーに提供するオープンAPIにおける大きな論点は、「共通の標準の採用」である。オープンAPIの成否はネットワーク外部性に強く影響され、銀行は、さまざまなサードパーティーにAPIを利用してもらわない限り、利用者数・取引数は伸び悩む。その点、「FAPI（ファピ）」という国際的な技術仕様を金融業界として共通に採用し、相互接続のハードルを下げれば、コスト低減が期待できる。

### セキュリティー標準の理想と現実

エンドユーザーにかかわるデータ（例えば、口座情報・取引履歴）や機能（例えば、送金・決済）をサードパーティーに提供する「オープンAPI」では、そのユーザーの同意に基づくAPIアクセスの許可（アクセス権の付与）が重要となっていく。これを実現するためのオープン標準が「OAuth（オーオース）」である。

OAuthは当初、WEBサービス事業者が中心となり、1997年にバージョン1・0が策定された。現在は、その後継の「OAuth2・0」が広く利用されている。

OAuth2・0が2012年に策定された当初は、ソーシャルネットワークのような比較的「軽い」サービスでの利用が中心だったが、次第に従業員向けサービスや公共サービスといった領域での活用が進んだ。現在では金融サービス分野でもO

Ａｕｔｈ２・０の採用が一般的になっている。日本においても、17年に全国銀行協会の「オープンＡＰＩのあり方に関する検討会」が取りまとめた報告書で、「認可プロトコル」としてＯＡｕｔｈ２・０を推奨した。現在オープンＡＰＩに対応した国内の銀行は、基本的にＯＡｕｔｈ２・０を採用しているとみられる。

しかし、ＯＡｕｔｈ２・０の技術仕様を実際に読んでみると、ＡＰＩ提供側が決めなくてはならない項目が多いことに気付く。例えば、仕様には、ＡＰＩアクセス権の範囲・種別を表現するための「スコープ」という項目が定義されているが、そのスコープの値をどのように設計するかは記述されていない。あるいは、ＡＰＩアクセス権はアクセストークンという文字列として表現され、ＡＰＩ提供側からＡＰＩ利用側に付与されることになっているが、そのトークンの有効期限や更新期間などはＡＰＩ提供側の裁量に任されており、特に定まった値はない。

これは、ＯＡｕｔｈ２・０が、厳密な接続手順を定めた「プロトコル」ではなく、要件に応じた最適な手順を定めるための「フレームワーク」であることに起因している。ＯＡｕｔｈ２・０はＡＰＩ提供側（サーバー）と利用側（クライアント）がそれぞれ独立に実装可能なものではなく、ＡＰＩ提供側が未決項目を埋めたうえで、ＡＰＩ利用側に提示する必要があるのだ。この自由度の高さによってＯＡｕｔｈ２・０はさまざまな用途に活用される技術仕様となったが、他方、オープンＡＰＩの進展に少なからず影響を及ぼしている。

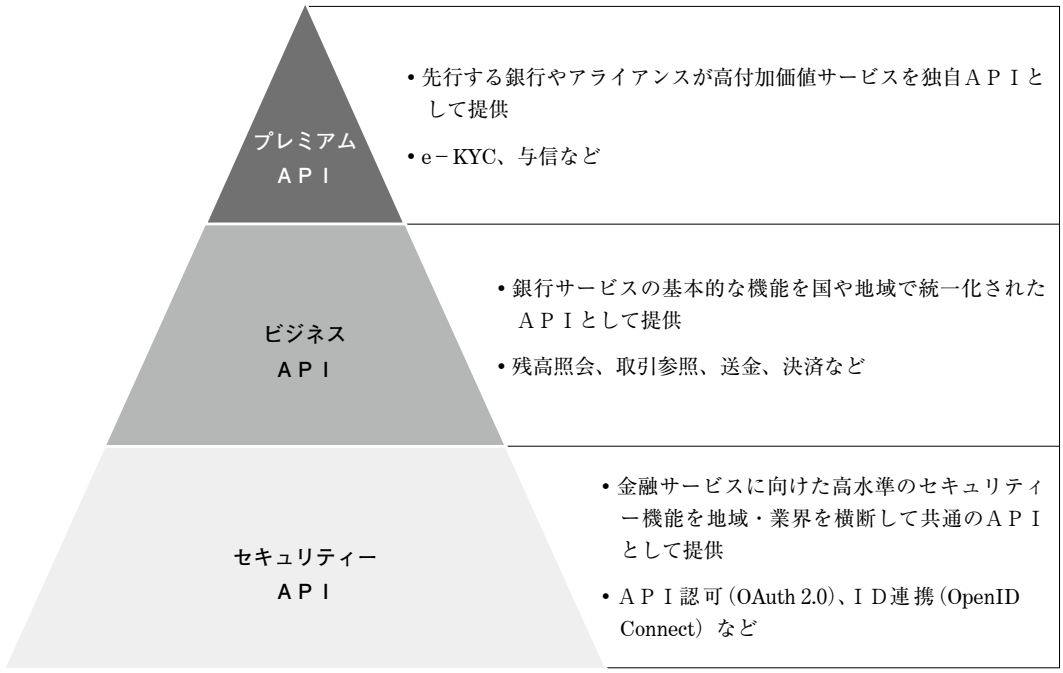
## 独自仕様でコスト負担増

具体的には二つの問題がある。第一に、オープンＡＰＩを提供する各銀行の足並みがそろわず、それぞれが独自の判断に基づきＯＡｕｔｈ２・０の詳細仕様を定義していることである。前述したスコープやトークンの扱い方はもとより、トークン授受手順のパラメーターにおける必須値や任意値などの細かな点に至るまで、大小含め、ＯＡｕｔｈ２・０詳細仕様のさまざまな点が銀行ごとにバラバラになってしまっている。その結果、ＡＰＩ利用側であるサードパーティー、とりわけスタートアップ企業が多いフィンテック事業者は、各銀行から提示されたＯＡｕｔｈ２・０詳細仕様の差異の把握・実装にコスト負担を強いられている。

第二の問題は、ＡＰＩを提供する銀行にとっての負担である。オープンＡＰＩ提供にあたっての高いセキュリティー水準の担保は当然欠かせないが、セキュリティー対策自体は直接的な収益をもたらすものではない。それにもかかわらず、自行のオープンＡＰＩにＯＡｕｔｈ２・０を適合させるために、一定のコストを費やして検討・実装する必要が生じている。

そもそも「オープンＡＰＩ」は、機能的には3層に分割して考えるべきである（図表1）。最下層は、金融サービスを取り扱うために必須の、ＯＡｕｔｈ２・０をはじめとする「セキュリティーＡＰＩ」。中間層に、顧客情報や取引履歴、基本的な送金などを担う「ビジネスＡＰＩ」。これらの層の上に各銀行が、例えばｅ－ＫＹＣのような高付加価値サービスを独自に提供する、いわば「プレミアムＡＰＩ」だ。このうち土台となるセキュリティーＡＰＩ層は、けっして競争優位の源泉となるものではない。共通化された仕様を活用することこそが、全体のコスト低減と、収益に直結する上位2層のＡＰＩの利用促進につながるのだ。

〔図表１〕　オープンＡＰＩの３階層




（出所）　筆者作成（図表２も同じ）。

## 「FAPI」でセキュリティーを共通化

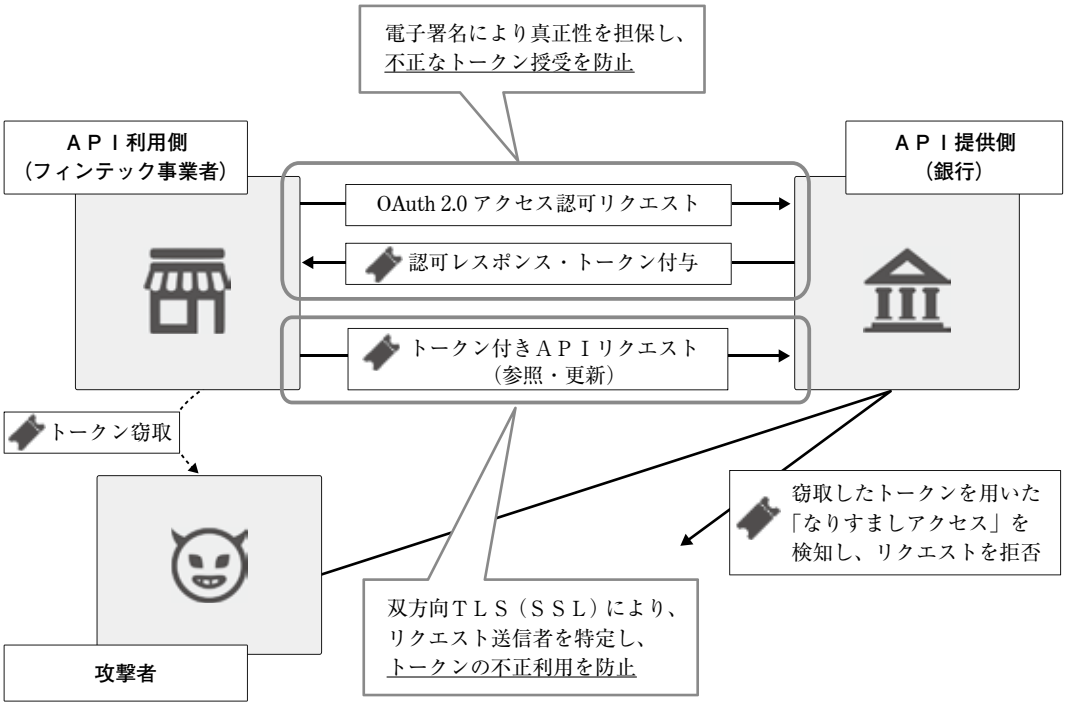
米国ＯｐｅｎＩＤ財団は16年、「Financial-grade API（当初はFinancial API）ワーキンググループ（ＦＡＰＩ ＷＧ）」を設置した。ＦＡＰＩ ＷＧでは、金融サービスＡＰＩのセキュリティーに適したＯＡｕｔｈ２・０の詳細仕様（セキュリティープロファイル）を定義し、そのうえで、ＡＰＩ仕様と実装ガイドラインの策定を目的としている。

本稿執筆時点（20年１月）では、基本的なセキュリティー対策を網羅した「パート１」と、より高度な対策を含む「パート２」の２種類のセキュリティープロファイルが、最終仕様になる前の「実装者向け草稿」として公開されている。特に後者の「パート２」では、ＯＡｕｔｈ２・０から派生したオープン仕様である「OpenID Connect（ＯＩＤＣ）」を積極的に取り込み、ＯＡｕｔｈ２・０だけでは対応できなかった範囲を含めたセキュリティー対策の標準化を図っている。

例えば、ＯＡｕｔｈ２・０では、トークン授受手順の一部（認可要求・応答）にエンドユーザーの端末（ＷＥＢブラウザーなど）を経由する箇所があり、攻撃者がそのやりとりを改竄・偽造してトークンを不正取得するリスクがある。あるいはＯＡｕｔｈ２・０で一般的に用いられている「持参型」のトークンはその利用主体を限定できないため、なんらかの方法でトークンを入手した攻撃者は、それを用いてＡＰＩへの不正アクセスが行えるようになる。

このような課題に対し、オープンＡＰＩを提供する各銀行はこれまで、それぞれが相応のコストを費やし独自拡張を加えて対策を行ってきた（あるいは、まったく対策してこなかった）。

〔図表２〕　　ＦＡＰＩによる不正なトークン授受・利用の防止




「パート２」では、認可手続きのメッセージの署名による改竄防止や、公開鍵暗号を用いたＡＰＩ利用側とトークンとの結び付けによる盗用防止の仕組みを、ＯＩＤＣ仕様に基づき定義している（図表２）。

つまり、ＦＡＰＩセキュリティープロファイルを採用した銀行は、独自仕様の設計・実装・運用に伴うコストの増大を抑えつつ、高度なセキュリティー対策を備えたＯＡｕｔｈ２・０基盤の確立が可能となるのだ。さらに各銀行のセキュリティー仕様のＦＡＰＩへの共通化は、ＡＰＩ利用側の対応工数の低減に結び付き、オープンＡＰＩの利用拡大にも貢献することとなる。

なお、ＯｐｅｎＩＤ財団では、事業者のサービスやソフトウェアベンダーの提供するコンポーネントが適切にＦＡＰＩを実装しているかどうかを検証するための「認定プログラム」の取組みも始めている。これは銀行にとって二つの側面で有用だろう。一つは、自社のオープンＡＰＩがＦＡＰＩ準拠であると認定プログラムを通じて公表し、ＡＰＩ利用側に対して自社の信頼性をアピールできるということ。もう一つは、ＯＡｕｔｈ２・０基盤の構築にあたり、認定プログラムからＦＡＰＩ準拠のソフトウェアを選定できるということである。

## 英国から広がるＡＰＩ採用の動き

英国では「オープンバンキング」を旗印に、政府主導のもと、銀行業界共通のＡＰＩ技術標準を策定し、上位９行に義務化した。またそれ以外の銀行にも、自主的な採用を促している。その結果19年11月には、ＡＰＩ提供側（銀行）68行、ＡＰＩ利用側（サードパーティー）１３０社が参加し、共通仕様に基づいてＡＰＩ提供・利用を行う環境が整備されている。

当然のように英国「オープンバンキング」仕様ではOAuth2・0を採用している。ただし、その詳細仕様については当初、FAPI仕様の初期案をベースに取捨選択を行った独自仕様だった。しかし、FAPI仕様の策定が進み、同時に英国からのフィードバックが取り込まれたこともあり、現在では独自仕様を廃止し、FAPIを改変せず、そのまま自国の標準として採用している。結果的にすべての事業者（API提供側・利用側の双方）が、グローバルに入手可能な実装とノウハウ蓄積の恩恵を受けられる段階に達している。

先行する英国の事例を参考にする動きが他国でも現われている。その筆頭であるオーストラリアでは19年に、いわゆる「消費者データ権法」が施行された。同法の目的は、サービス事業者が保有する消費者データについて、その消費者自身によるコントロールを可能とし、サービス比較・乗り換えの容易化、事業者間の競争促進、ひいてはサービスの料金適正化と価値向上にある。

実際の適用は業界単位で進められており、当初は銀行分野、続いてエネルギー分野、その後電気通信分野に広げられる予定である。実施にあたり、オーストラリアは英国オープンバンキングの仕様群を積極的に取り込み、共通仕様策定に要する期間・コストの短縮を図っている。銀行分野のみならず、将来的には他の業界にも波及する技術仕様の中核として、FAPIの役割はより重要となるだろう。

国内では、前述の「オープンAPIのあり方に関する検討会」報告書にて、「同団体（OpenID財団）でOAuth2・0適用の詳細仕様が発行された際には、各銀行において同仕様（FAPI）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」（括弧内は筆者追記）と言及されている。

最近では19年11月にふくおかフィナンシャルグループが20年度に設立予定の「みんなの銀行（仮称）」において、FAPIを実装し認定を取得したオーストリートのソリューションの導入検討を表明するなど、FAPI採用に向けた動きがある。

筆者は19年12月、英国エディンバラにて開催されたFDATAグローバルの国際会議に参加した。この会議は、「オープンファイナンス」をテーマに世界各国の関係者が一堂に会し、現状の共有と今後の方向を議論するものである。日本からも金融庁や日本銀行、筆者が所属する民間企業などから、十数名が参加していた。あるパネルディスカッションでは、オープンAPIにおけるアーキテクチャー、システム設計、セキュリティー、そして標準について討議されたが、その大きな論点は、共通の標準を採用することの重要性だった。

オープンAPIの成否はネットワーク外部性に強く影響される。銀行はさまざまなサードパーティーにAPIを利用してもらわない限り、一方のサードパーティーも多数の銀行と連携できない限り、利用者数・取引数は伸び悩み、ひいては収益拡大を望めなくなってしまう。FAPIという国際的な技術仕様を業界として共通に採用し、相互接続のハードルを下げることは、コスト低減が期待できるという意味でも合理的な施策といえるのではないか。

**くどう　たつお**
サン・マイクロシステムズ、野村総合研究所、NRIセキュアを経て18年からAthlete（オースリート）にて現職。デジタル・アイデンティティー業界において20年以上にわたり、プリセールスやコンサルティング、事業開発、エバンジェリズムを手掛けている。