# 金融APIに求められるセキュリティ ～APIDays Paris講演より

去る2016年12月に「APIDays」というカンファレンスが開催された。APIを活用したサービスがもたらす変革についての検討を目的とした会合で、欧州を中心に1,200名を超えるビジネスマンやエンジニアが会した。本稿では、同会合において筆者の講演した内容を抜粋・翻訳し紹介する。

## FinTech、API公開強制の衝撃

FinTech推進の3本柱は、「AI」、「ブロックチェーン」、「API」であると言われる。この中では、ともすればAIとブロックチェーンに目が行きがちだが、APIの重要性はこれらに引けを取らない。AIやブロックチェーンの利用には結局APIが必須になるとともに、API公開こそが新たな金融サービスの開発の鍵となるからだ。

このことは、米国やここ欧州では比較的強く認識されている。特に英国はOpen Banking Standard（OBS）として、銀行にAPI公開を強制する方向である。大陸欧州も、Payment Service Directive 2（PSD2）が採択され、2018年には第三者サービスが金融機関にアクセスして送金などが行えるよう環境整備を求めている。PSD2は法的なフレームワークであるので手段は規定していないが、APIが現実的な手段として認識されている。つまり、事実上の「API公開強制」と言えよう。

## API保護の主役、「OAuth」と「OpenID」

このような背景から各金融機関やFinTech企業はAPIの整備に着手しているわけだが、モバイル・ファーストの現在、OAuth 2.0[1)]がAPI保護のための第一選択肢であることは疑いがないだろう。実際、OBSでもOAuthとOpenID Connectを採用している。しかし、それで問題が解決したと考えるのは安易すぎる。

ガートナーのアナリストであるマーク・オニールが言うように、APIを組み立てる部品はたくさんあり、それらを「正しく」組み合わせるのが肝要で、「OAuthを使えば良い」というのは何の解決にもなっていないからだ。このことはRFC[2)]6479のタイトルが「The OAuth 2.0 Authorization Framework」となっていることからも明らかだ。OAuth 2.0はフレームワークであって、具体的なプロトコルではなく、逆にそうであることによって、多様なユースケースや環境に対応できるようになっているのだ。これは大変良いことであるが、一方では、状況に合わせて、どのオプションをどう使うか細かく定めた詳細仕様の作成をしなければならないということも表している。

たとえば、閉域網上の工場用アプリケーションのようなものであれば、セキュリティ要件の多くは環境の厳密な制御で実現し、OAuthのようなアプリケーション層での対応は最小限にすることができるだろう。あるいは、一部のソーシャルアプリにおけるデータ共有のように、環境制御はなくとも、対象となるデータへの秘匿性要求が低いということで、RFC6750に規定される持参人トークンを長期にわたって使うような簡便な実装方法の選択が正当化される場合もあるだろう。しかし、これは金融APIのように、対象となる情報リソース保護への要求が高い場合には当てはまらない。金融APIの保護にOAuthを使う場合には、それ相応の詳細仕様を用意する必要があるのだ。

## 金融向け詳細仕様への考慮点

詳細仕様を作成する場合に考慮すべき点はいくつもあるが、多くの場合これらは無視され、現状、安全でないOAuth 2.0の実装が散見される。

例えば、OAuthの最も基本的な前提条件に「クライ



野村総合研究所　金融ITナビゲーション推進部 

**NOTE**

1) APIアクセスへの認可を取得するためのフレームワーク。
2) Request For Comment。インターネットに関する技術の標準を定める団体であるIETFが正式に発行する文書。このうち「Standard Track」に含まれる文書が、いわゆるインターネット標準にあたる。「RFC」の後に番号をつけることによって、当該文書のリファレンス番号とする。
3) Transport Layer Security。電算網上の通信のセキュリティを守るための暗号プロトコル。
4) ISO（国際標準化機構）における第68技術委員会（Technical Committee）。金融サービスに関する国際標準作成のための委員会。
5) WTO（世界貿易機関）に関わる、貿易の技術的障害（Technical Barriers to Trade）に関する協定。
6) FS-ISAC（Financial Services - Information Sharing and Analysis Center）の定める継続的データAPI（Durable Data API）に関する委員会。
7) Open Financial Exchange。銀行等の口座データ等をダウンロードするための規格を定める団体。

アントは1つの認可サーバとのみ関係を持つ」というものがある。しかし、多くの実装で守られていない。

具体的な例を挙げよう。個人金融資産管理アプリは、必然的に複数の金融機関の認可サーバと関係を持つ。このような場合、リダイレクト・エンドポイントを分けることによって、クライアントの論理分割をしなければならないのだが、多くの場合ではこれを怠り、同一のリダイレクト・エンドポイントを使うことによって、サーバ混同攻撃などに対して脆弱になっている。

また、メッセージ認証処理も大きな課題だ。OAuthの認可要求は、ブラウザを経由して送られる。クライアント～ブラウザ間、ブラウザ～サーバ間はTLS[3]により暗号化されているが、ブラウザ内では平文に戻っているため、ここで情報を抜き取ったり書き換えたりすることが可能である。また、サーバ、クライアント共に、そのメッセージが当該ブラウザから来ていることはわかるが、本来の送信元がどこであるのか、送信先がどこであるのかを確認することもできない。金融APIの保護において、詳細仕様作成時には、こうした課題を解決しなければならない。

## 金融API（FAPI）ワーキング・グループ

これらの課題にこたえる「標準」を作るためにNRI、Microsoft、Intuitが中心となり組織されたのが、OpenID Foundation（OIDF）の「金融APIワーキング・グループ（FAPI WG）」である。金融系のデータ標準というと、ISO/TC68[4]が真っ先に思い浮かび、OIDFでの標準化には違和感があるかもしれない。しかし、OIDFにはOAuth関連仕様、OpenID Connect関連仕様の著者の殆どが在籍しており、参加費用が不要な上、知財管理やWTO TBT協定[5]に準拠した標準作成工程などの管理面もしっかりしているという優位性があることを考えると、ことAPIセキュリティの面に関しては、他で標準化することは考えにくい状況だ。まずは、ここでセキュリティ標準は固め、その後TC68に持ち込もうという算段だ。

## 金融業界における可能性

FAPI WGでは、現在、読み出し専用APIセキュリティの公開レビューを行っており、同時に読み書きAPIのセキュリティ仕様のドラフト作成を2017年第1四半期末完成目標に行っている。これらは、米国ではFS-ISAC DDA[6]とOFX[7]、英国ではOBSで採用されるようにリエゾン関係を結んでいる。複数の技術プロバイダから製品やサービスが提供される見込みであることから、金融機関にとっても採用しやすい技術になると思われる。

金融機関にとってAPI公開は顧客流出の元になるだけとの認識も一部にはあるようだがそれは正しくない。顧客側の帳簿類のAPIを通じた取得や、他社APIとの組合せなどによって、これまで提供できていなかったセグメントへのアクセスや新サービスの提供が可能になる。API公開に真摯に取組む企業とそうでない企業には、大きな差が生まれてくることであろう。

**Writer's Profile**
**崎村 夏彦** Natsuhiko Sakimura
デジタルビジネス開発部　上席研究員
OpenID Foundation 理事長
専門はIAM国際標準化
focus@nri.co.jp