APIエコノミーの発展を支えるAPIセキュリティ

サービス間の連携を促進するAPIの普及には、ユーザーや複数のサービス間で安全に「権限委譲」を実現する仕組み・技術の存在を忘れてはならない。オープンAPIのセキュリティの中核となる「権限委譲」があることで、企業は外部サービスとの提携・分業構造に移行するなど、多くの戦略的可能性を手に入れることが可能となる。

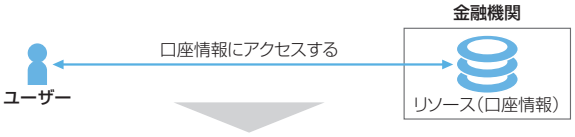
APIとは、古き良きエンジニアにとってはコンピュータプログラム間のインタフェース用語として馴染み深い。それが現代においては、「Web標準を活用したサービス連携のためのインタフェース」として意味合いが変化している。特に外部に向けて公開する「オープンAPI」の飛躍的拡大によって、デジタルビジネスの地殻変動を起こすキーワードにまで成長を遂げている。本稿では、セキュリティの専門家として「オープンAPIをセキュアに利用する仕組み・技術」という側面で紐解いていきたい。

安全な「権限委譲」の実現がAPI経済圏の骨格を作る

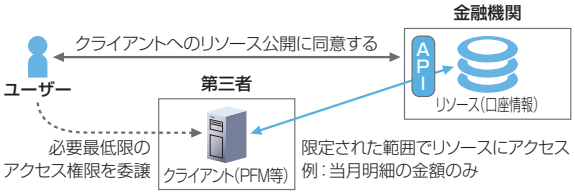
オープンAPIをセキュリティの側面から語る上で、重要なキーワードは「権限委譲」の実現である。先ず権限委譲の存在しないケースを見てみよう。例えばユーザーがWebブラウザを用いてインターネットバンキングにアクセスし自分の口座情報（リソース）を参照するケースだ。この場合、ユーザーがパスワード等でログインを行い、全アクセス権限を有して自分の口座情報に直接接続するモデルとなる（図表1）。

ではここにもう一つのアクターを介在させ、そのアクターから自分の口座情報にアクセスさせたい―例えば、自分の口座資産について外部の管理サービスを使いたい―とすると、どうなるか？この場合は、ユーザーが自分の口座情報を金融機関以外が提供する別のクライアント（スマートフォンアプリ、Bot、IoTデバイス、PFMのような第三者サービス等が該当する）にアクセス権限を委譲するモデルとなる（図表2）。ここで留意すべきは、金融機関以外が提供する別のクライアントに口座情報への全アクセス権限を委譲する必要があるか？

図表1　ユーザーがリソースに直接アクセスする



図表2　クライアントに権限を委譲して限定範囲でアクセスする



という点である。例えばPFM事業者等のクライアントに対しては、当月明細の金額参照APIのみのアクセスを認可する等、「必要最低限の権限のみを委譲したい」というニーズが想定される。ホテルのエントランスに停車した高級車の駐車をベルボーイに任せるときに預けるバレットキー（エンジン起動はできるがトランクやグローブボックスの解錠はできない等）は、実世界でこの「必要最低限の権限委譲」を実現している例と言える。

デジタル世界において、これらの第三者やモノに対して必要最低限のアクセス権限委譲を安全に実現する仕組み・技術の確立は大きな意味合いを持つ。ユーザーは安心して重要なリソースを第三者にアクセスさせ、多様なサービスを受けることが可能となる。企業は他社サービスとの提携・分業構造へトランスフォームする等、多くの戦略的可能性を手にするとともに、APIエコノミー時代の新たな競争環境への対応も必要になるだろう。

APIセキュリティの鍵は権限委譲の精緻化にあり

このようなオープンAPI提供の拡張性の確保とAPIセ

NOTE

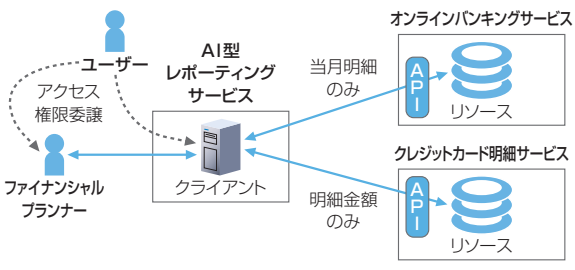
1) 標準仕様としてOAuthやOpenID Connectが広く普及している。OAuthはAPI等のサービス連携において、ユーザーの同意に基づいてクライアントに権限を委譲するための標準仕様。OpenID ConnectはOAuthの仕様範囲を包含し、ユーザーの同意に基づいてID情報を流通するための拡張要件を加えた標準仕様。
2) 最近、家庭等に設置されたIoTデバイスが乗っ取られ、大規模なサイバー攻撃に利用されている事例が発生し耳目を集めた。
3) NRIセキュアテクノロジーズでは「APIセキュリティコンサルティングサービス」の提供を開始している。(http://www.nri.com/jp/news/2016/161110_1.aspx)
4) 高度なアクセス認可仕様としてUMA(User-Managed Access)等の仕様策定が進められている。

キュリティを両立させる成功の鍵は、アクセス権限の委譲設計の精度をどこまで高めることができるか、にかかっていると筆者は考える。そのためには金融機関がどのようなビジネスでAPIを用いるのか、そのユースケースを「理解」し、それを実現する関連技術仕様を「咀嚼」した上で、ユースケースに沿った権限委譲のプロファイリングを行うことが必須となる。

前の例よりやや複雑な事例を考えよう。個人がファイナンシャル・プランナーから、銀行口座やクレジットカードの利用についてAI型サービスを用いたレポーティングサービスを受けるケースである。ここでは、ユーザーの同意のもと、ファイナンシャル・プランナーがAI型サービスを使って銀行の口座残高参照APIやクレジットカード会社の明細APIにアクセスすることになる（図表3）。

このモデルでは、ユーザーはファイナンシャル・プランナー及びAI型レポーティングサービスに対して開示可能な範囲について同意し、APIアクセス権限を委譲することになる。その際には、例えば銀行明細の開示は当月分のみ、クレジットカードの場合は明細金額のみにしたい、またそれぞれ一度限りの限定開示としたい、などのユーザーのセキュリティ意識やプライバシーを考慮したアクセス権限委譲モデルが求められるだろう。その他、アクセス権限の失効管理、ID管理との連動等、アクセス制御設計の基本をしっかり行うことも肝要である。

図表3　複雑な権限委譲モデル



これらの「権限委譲」の実現には、既にオープン標準仕様[1]が確立しており、多くのサービス事業者が採用したことでデファクトスタンダード化し、グローバルに普及している。これらの標準仕様は、①世界中の有識者に叩き上げられ日々進化を遂げており、②他サービスとの相互運用性を高め、③ビジネスモデルの「金型」として活用できる、という利点がある。こうした意味からも、権限委譲を含むAPIを用いる際は、広く浸透したオープン標準仕様の採用を第一義的に考えることを強く推奨する。

多様なクライアントからのアクセスを前提としたオープンAPI環境が、サイバー攻撃の脅威に晒されやすいのは疑いのない事実である[2]。今後は、対抗策としてAPIステルス化技術やAPIアクセスに最適化されたサイバーディフェンスサービスが続々登場してくることが予想される。自社のビジネス戦略におけるAPIの役割を検討した上で、適用分野、提供先、機能を踏まえ、適切なサイバー攻撃の防止策を検討する必要が出てくるだろう[3]。またビジネス要件によっては、さらに高度なアクセス認可仕様[4]を活用することも必要となろう。

本稿では権限委譲を中心に紹介したが、これらの例のようにビジネスユースケースを整流化するフェーズと同時並行的にAPIセキュリティを検討するアプローチこそが、革新的かつ最良なAPIサービスを生みだすための欠くことのできない要素であると考える。

Writer's Profile

石井 晋也 Shinya Ishii
NRIセキュアテクノロジーズ　サイバーコンサルティング部
ITセキュリティコンサルタント
専門はID管理・ID連携・認証・認可・APIセキュリティ
focus@nri.co.jp