Minna no Ginko

PRESS RELEASE

2024.3.15
株式会社みんなの銀行

世界トップレベルのセキュリティ規格『FAPI』に準拠した BaaSプラットフォームを最新仕様FAPI2.0に対応

株式会社みんなの銀行（取締役頭取 永吉 健一、以下「みんなの銀行」）は、外部企業へ金融機能を提供するAPI連携システム（BaaSプラットフォーム）を、国内銀行では初となる最新仕様 FAPI2.0 Security Profile/Message Signing（以下、FAPI2.0）にバージョンアップします。現在、FAPI2.0の仕様はドラフト版ですが、すでに開発を完了しており、今後最終版の仕様が確定次第、随時、外部企業への提供を開始します。

取組みの背景

非金融事業者が自社サービスに金融機能を直接取り込むためには、より安全にAPIを利活用できることが不可欠です。一般社団法人全国銀行協会が事務局となっている「オープンAPIのあり方に関する検討会」の報告書においても、金融機関によるAPIの外部提供に際しては、「OAuth2.0*1に加え、FAPIへの準拠が望ましい」とされています。

みんなの銀行は、2022年9月に日本の銀行としては初めて、FAPI1.0に準拠したAPI連携システムを開発し、現在参照系と更新系APIを7社に提供*2しています。

今回、API連携の認可方式に関して「FAPI」の仕様が最新版へバージョンアップすることを受け、当該仕様に準拠したAPI連携システムの開発を行い、ドラフト版の仕様にてOpenID Foundation*3 による認定取得を完了しました。本件に伴い「API連携に係る認可方式に関するポリシー」も定め、今後も業界に先駆けてAPI連携システムの最新仕様を取り込んでいく方針です。

「API連携に係る認可方式に関するポリシー」はこちら ▶

＊1　権限の認可（authorization）を行うための認可フレームワーク。金融機関は外部事業者へAPI連携を行う際、特にセキュリティ面で非常に重要な役割を担うことから、OAuth2.0への準拠が求められており、API提供を行う国内銀行の大半が対応しています。

＊2　みんなの銀行が提供するAPIは、参照系：口座照会（入出金明細照会）/ 本人確認済情報提供、更新系：口座振替（決済）です。
みんなの銀行がAPI提供している企業はこちらをご確認ください。（2024年3月15日現在）

＊3　OpenID FoundationはAPIアクセス管理にかかわる技術の標準化等に取り組む、2007年に米国で設立された非営利団体です。

FAPI2.0の特徴

FAPI (Financial-grade API) とは、OpenID Foundation の Financial-grade API ワーキンググループが策定した技術仕様です。OAuth2.0 と OpenID Connectを基盤として、金融業界のようにより高いセキュリティを必要とする業界への要求に対応するための技術要件を定義しています。
FAPI2.0には2つのプロファイル（Security Profile/Message Signing）があり、みんなの銀行は両方に対応し認定を取得しています。

①FAPI2.0 Security Profile

FAPI2.0は、FAPI1.0で実現している高いセキュリティ水準を維持もしくは高度化し、かつ、提携事業者が開発しやすい仕様となっています。

PAR（Pushed Authorization Request）を必須化したことで、不正アクセスの攻撃対象となりやすいWebブラウザのパブリックな通信経路ではなく、mTLSで保護されたセキュアな通信経路を介して重要な情報が含まれる口座連携の認可リクエストを提携事業者からみんなの銀行に送ることができます。（PARエンドポイントへのリクエスト）

これにより、認可リクエストへの署名、および認可コードの署名検証が不要となり、不正リスクを抑えながら提携事業者の開発難易度を軽減することができます。

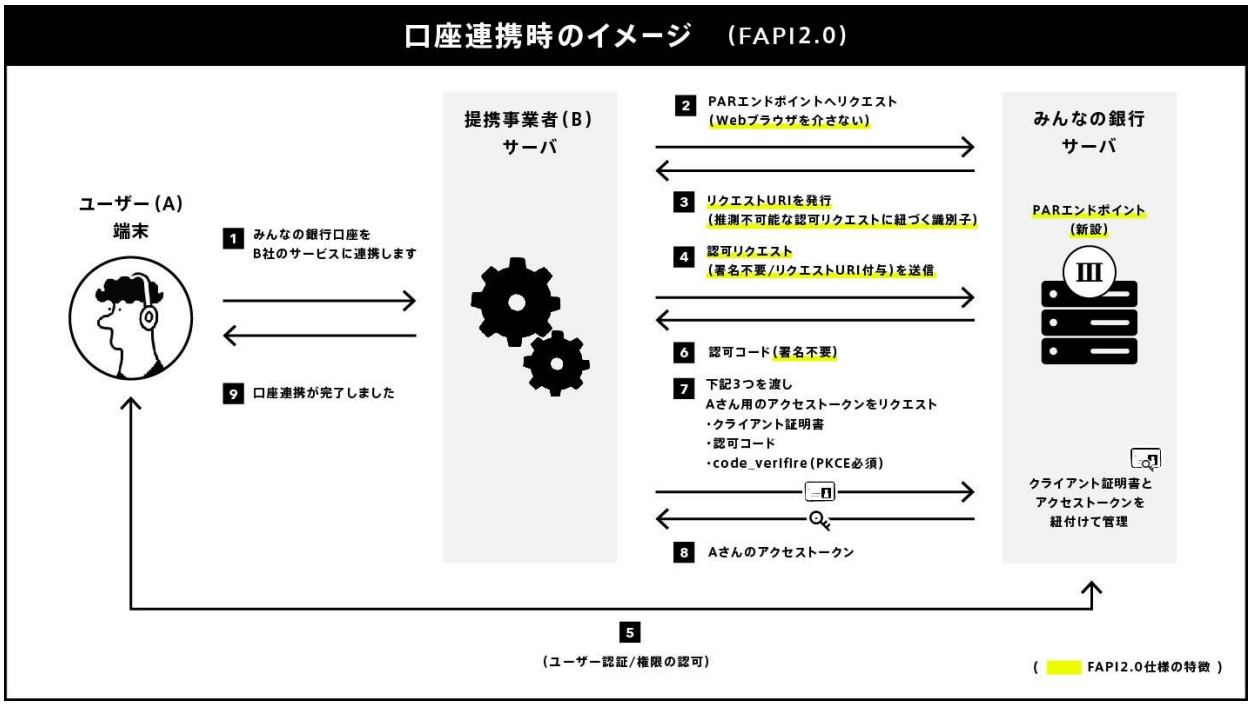
②FAPI2.0 Message Signing

FAPI2.0 では、新規API連携時には、認可リクエストへの署名、及び認可コードの署名検証が不要になりますが、既にみんなの銀行とFAPI1.0でAPI連携を開始している提携事業者が引き続き利用できるように、FAPI1.0からFAPI2.0へバージョンアップする際の互換性を確保する必要があります。

そのため、認可リクエスト及び認可レスポンスに署名を必要とするプロファイルも並行して実装しました。

下記2点はFAPI2.0の特徴ですが、みんなの銀行では現在のFAPI1.0の仕様においてもすでに実装したAPIを提供しています。

1. 口座連携に関する認可について、認可状態の確認、認可の期限延長・解除ができる『Grant Management for OAuth2 (Draft)』（FAPI2.0 において推奨）と同等の機能を実装
2. 認可コードの横取り攻撃を防ぐためにRFCで規定された推奨仕様「PKCE」の対応（FAPI2.0において必須）



本件に関するお問合せ先

株式会社みんなの銀行 広報担当: 今村・市原・中原 TEL: 092-791-9231 E-mail: pr@minna-no-ginko.com