Financial-grade API (FAPI) プロファイル

利用可能な FAPI プロファイルの比較と、セキュリティプロファイルとして FAPI の導入を検討している新規市場への推奨事項

作成者：Chris Michael, Freddi Gyara, Joseph Heenan, Torsten Lodderstedt, Dima Postnikov, Dave Tonge

バージョン: 1.0 - 2022 年 7 月 27 日

分類: 公開

1. はじめに

1.1 背景

Financial-grade API（FAPI）プロファイルは、OAuth 2.0 と OpenID Connect の上位のレイヤに位置するものであり、OAuth/OIDC が提供する選択肢を制限または強制する一連の制約（*プロファイル*と呼ばれる）を定めることで、OAuth/OpenID Connect を「強化」する。

FAPI は現在、イギリス OBIE（The Open Banking Implementation Entity）、ブラジルオープンファイナンス、オーストラリア CDR（Consumer Data Right）、バーレーンオープンバンキング、FDX（Financial Data Exchange）、サウジアラビア通貨庁（サウジアラビア王国）など、世界中のほぼすべてのオープンバンキングおよびオープンファイナンス標準の基礎として使用されている。

しかし、これらの標準のなかには（イギリス/OBIE などのように）、数年前のプロファイル/バージョンに基づいているため、後続のバージョンでの改善や強化の恩恵を受けることができないものがある。

さらに、これらの標準の（すべてではないにせよ）ほとんどは、わずかに異なるプロファイル/バージョンを使用しており、これはグローバルな相互運用性の観点からは得策ではない。

1.2 利用可能な FAPI プロファイル

以下は、複数の実装者によって使用されているか、OpenID Foundation の FAPI ワーキンググループによって精力的に開発されている FAPI プロファイルである：[1]

- FAPI 1 実装者向けドラフト 6（OBIE プロファイル）： https://openid.net/specs/openid-financial-api-part-2-wd-06.html [2]
- FAPI 1 Baseline（基準版）： https://openid.net/specs/openid-financial-api-part-1-1_0.html
- FAPI 1 Advanced（高度版）： https://openid.net/specs/openid-financial-api-part-2-1_0.html
- ブラジル・セキュリティ標準： https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID3-ptbr.html [3]
- FAPI 2： https://openid.net/specs/fapi-2_0-baseline-01.html
- FAPI 2 メッセージ署名： https://bitbucket.org/openid/fapi/src/master/FAPI_2_0_Advanced_Profile.md

1.3 本稿の目的

ここでは、FAPI をそのまま再掲するのではなく、FAPI がセキュリティを強化する以下の分野に焦点を当て、各分野に対する提言を行う：

[1] （訳注）2025 年 7 月現在、最新の状況は、次の URL で公開されている：https://openid.net/wg/fapi/specifications/
[2] （訳注）2025 年 7 月現在、UK Open Banking からは FAPI 1 Advanced（高度版）が参照されている
[3] （訳注）2025 年 7 月現在、ブラジルオープンファイナンスからは次の URL で公開されている：https://openfinancebrasil.atlassian.net/wiki/spaces/OF/pages/240649123/EN+Open+Finance+Brasil+Financial-grade+API+Security+Profile+1.0

1. 暗号アルゴリズムの選択
2. トランスポート・セキュリティ
3. クライアント認証方式
4. 認可付与のためのパラメータ渡し
5. レスポンス検証

次に、いくつかの異なる FAPI プロファイルを設定し、新規/新興のオープンバンキング/金融標準に対するそれぞれの相対的な適合性を評価する。

本稿は、特に新規/新興のオープンファイナンス標準やエコシステムに対して、どのプロファイル/バージョンの FAPI を使用すべきかについて、明確な推奨を提供することを目的としている。

2. 考察と提言

2.1 暗号アルゴリズムの選択

FAPI のすべてのバージョンにおいて、署名や暗号化が行われる場合は、非対称暗号化アルゴリズムを使用する必要がある。

特筆すべきは、安全なアルゴリズムとして RS256 が除外されていることである。当時より安全な PS256 アルゴリズムに対するライブラリのサポートが不十分であったため、OBIE 標準の初期のドラフトでのみ、これを認めていた。

安全なアルゴリズムの識別に加えて、FAPI 2 は、より包括的な RFC8725 / BCP225 - JSON Web Token Best Current Practices への参照を追加した。

推奨 1: FAPI 1 Advanced（高度版）の安全な暗号アルゴリズムの仕様を必須とすべきである。

推奨 2: RFC8725 / BCP225 - JSON Web Token Best Current Practices への準拠を推奨するが、現時点ではオプションのままとすべきである。しかし、ベンダーと実装者からの広範囲なサポートを得られた時点で必須とするべきである。

2.2 トランスポート・セキュリティ

FAPI 1 は、private-key-jwt と tls-client-auth の 2 つのクライアント認証方式を許可している。どちらの方法も、認可サーバが送信者制限付きのアクセストークン（Sender constrained access tokens）を発行し、アクセストークンが証明書に紐付けできることを確実にするため、mTLS（相互 TLS 認証：RFC 8705)を使用できるように、クライアントがトランスポート証明書を提示する必要がある。

FAPI 2 は、mTLS または DPoP（Demonstration of Proof-of-Possession）を使用する以上の、包括的なネットワーク層におけるセキュリティ対策（例：DNSSEC の要求など）を持つ。

推奨 3: 証明書紐づけアクセストークンに mTLS[RFC 8705]を使用することについて、 FAPI1 Advanced(高度版)の推奨に従うこと。[4]

[4] （訳注）FAPI1 Advanced(高度版)では、mTLS として RFC 8705 が参照されている

2.3　クライアント認証方式

OpenID Connect がプレーンな OAuth 2.0 に対して行った最大の改善点の 1 つは、OIDC クライアントが認可サーバに対して自身を認証するための拡張可能な一連の方法を提供できることである。

これは OpenID Connect 仕様のセクション 9 で取り扱っており、それぞれの具体的な方法について RFC（インターネット技術の標準仕様をまとめた文書群）を参照している。

すべての FAPI 仕様は、認証方式として tls_client_auth または private_key_jwt の使用を要求しており、クライアント認証は非対称アルゴリズムに依存すべきであるというのが一般的な原則である。

推奨 4:　FAPI 1 Advanced（高度版）および FAPI 2 の推奨に従うこと。

2.4　認可付与のためのパラメータ渡し

OAuth 2.0 の認可コード付与では（そしてハイブリッドフロー内でも）、OAuth 2.0 クライアントは、いくつかのクエリパラメータを持つ認可サーバ URL への呼び出しを構成する。

これは次に、リダイレクトしてリソースオーナーのユーザーエージェントに送られる。ユーザーエージェント（ブラウザ/モバイルアプリ）はリダイレクトを行いながら、最終的に認可サーバに到達する。

このやり取りは、安全でない「フロントチャネル」（ユーザーのブラウザを介するという意味）で行われるため、セキュリティ上の問題が数多く存在する：

- 中間者攻撃によって、クエリパラメータが変更される可能性がある。
- クライアントのふりをした攻撃者が認可サーバへの呼び出しを構成し、レスポンスの制御を奪う可能性がある。
- クエリパラメータが本質的に機密性の高いものである場合、インターネット上で暗号化されずに送信されると読み取られてしまう。

認可サーバから送信されるレスポンスは、リダイレクト URI の形をとり、エンドユーザのブラウザを経由してクライアントに送られるため、同じ問題が繰り返される。

様々なプロファイルを通して利用可能な解決策は以下の通りである：

- 署名付きリクエストオブジェクトの使用(OIDC 仕様のセクション 6.1 による)
- 参照渡しによるリクエストオブジェクトの使用(OIDC 仕様のセクション 6.3 による)
- PAR（パー）(RFC-9126)の使用(下記参照)

Pushed Authorization Requests(PAR)は、他の 2 つの方法に対して多くの利点を提供する：

- PAR は、クライアントがリクエストオブジェクトを生成するための標準化された方法を提供する。
- PAR リクエストでは、認可サーバは、クライアントが登録されているクライアント認証方式を用いてクライアントを認証し、高度なセキュリティを提供する。

- PAR は、リクエストの内容がブラウザを介して渡されることを防ぐ。このことは、プライバシー保護の点からも効果的である。
- 現在の FAPI 2 のドラフトでは、クライアント認証で PAR の使用を義務付けている。[5]

推奨 5:　認可付与のパラメータ渡しの方法として、PAR を必須とすべきである。

推奨 6: セキュリティプロファイルは、将来の FAPI 2 への移行を単純化するために、 FAPI 2 で定義された PAR に関するプロファイルルールを採用すべきである。

2.5　レスポンス検証

レスポンスにおける検証を強制する最も単純な方法は、レスポンスタイプとして code id_token の使用を強制することである。これにより、認可サーバは認可コードとともに id_token を発行することを強制される。

- id_token は認可サーバによって署名され、改ざんされないことが保証される。
- id_token は、state と code パラメータの一部のハッシュ値（s_hash と c_hash）を含んでおり、これらを検証することで、改ざんされていないことを確認できる。

JWT Secure Authorization Response Mode（JARM)は、認可サーバが認可コードに対して、署名付き JWT をレスポンスとして返却する方法である。クライアントにとってはこれで、そのレスポンスが中間者によって改ざんされていないことを保証されることになる。

JWT（JSON Web Token）は暗号化、署名、またはその両方が可能であり、認可サーバが応答する認可コードの機密確保を可能にする。

まとめると、認可レスポンスが途中で改ざんされていないことを検証する技術的なソリューションとして以下が提供されるといえる：

- id_token クレーム内のバインディングを使用
- JARM の使用

推奨 7：　FAPI 1 Advanced（高度版）の推奨に従うこと。

[5]　（訳注）2025 年 2 月に承認された FAPI 2.0 Security Profile 最終版では、必須とされている

3. プロファイル間の比較

この比較では、以下のプロファイルを除外する：

- **FAPI 1 Baseline：：** このプロファイルは、検討初期に「読み込み」と「読み書き」でプロファイルを分離したことに由来する。Baseline プロファイルは、機能性や詳細な定義に欠陥があったことで他の標準化団体や規制当局に検討されず、私たちの目的達成に至らなかった。
- **FAPI 2 メッセージ署名：** これはまだ初期のドラフトであり、現段階では検討するのに十分な成熟度に達していない。

以下の表は、残りのプロファイルの比較と、それぞれの概要、状況、影響を示している：

プロファイル	OBIE プロファイル	ブラジル・プロファイル	FAPI 1 Advanced（高度版）	FAPI 1 Advanced（高度版）PAR 付	FAPI 2
概要	FAPI 1 が最終化される前の初期のドラフトから生まれた。 当時利用可能だったいくつかの製品の機能に対するサポート不足に対処するため、多くの「リラクゼーション（要件の緩和）」が含まれている。	FAPI 1 Advanced（高度版）の派生版である。 許可された複数のバリエーションが含まれており、実装者はどれを使用するかについてかなりの柔軟性を得ることができる。	OBIE プロファイルをベースに開発された。 実装時に見られる問題に対処するための追加的な機能強化、明確化、〝要塞化〟を含む。	上述のとおり、FAPI 1 Advanced（高度版）プロファイルであるが、PAR のサポートが必須である。 ブラジル・プロファイルはこれのフルセットである。	FAPI 1 Advanced（高度版）を進化させ、プライベートキー、PAR、JARM（オプションの拡張として）のサポートを追加したものである。 実装者にとってより理解しやすく、世界的に新規/新興の標準化団体の要求に応えるように設計されている。 公式のアタッカーモデルを含む。
実装状況	当初はイギリスのプロバイダ数社が実装していたが、すべての具体例で、FAPI 1 Advanced（高度版）に移行しているはずである。 イギリス以外では広く実装されていない。	BCB（ブラジル中央銀行）がすべてのオープンファイナンスの実装を義務付けているため、ブラジルのオープンファイナンス・エコシステム全体で積極的に利用されている。 しかし、現在では複数のバリエーションが実装されており、一貫性はほとんどない。	バーレーンの全プロバイダに義務付けられている。 最新の OBIE 標準では推奨されている。	ブラジルでは、すでにいくつかのプロバイダが実装している。	いくつかのロードマップで提案されているが、他の標準化団体ではまだ正式には採用されていない。
コンフォーマンス・スイートの状況（準拠検証テスト集）	利用可能だが、積極的に保守されていない。	利用可能で積極的に維持管理されている。	利用可能で積極的に保守されている。	利用可能で積極的に保守されている。	開発中であるが、最終的な公表版としてはまだ利用できない。
新規／新興の標準への適合性	これは 5 年以上前の初期のドラフトであり、何度も置き換わっているため、もはや実装には推奨されない。	このプロファイルは原則的には目的に適合しているが，利用可能なオプションの数が多いため断片化をもたらす可能性が高く、相互運用性を低下させ，制限する。	中核的なプロファイルとして、目的に適合している。 しかし、上記の推奨 5 と 6 は、PAR の利点と要件を明確に示している。	上記の要件と推奨事項をすべて満たしている。 また、実装者が後の段階で FAPI 2 に移行するための比較的簡単なアップグレード手順や経路を提供している。	プロバイダや RP の中には、まだドラフト段階のプロファイルの実装に消極的なところもあるだろう。 最終版（最終的なコンフォーマンス・スイートを含む）がないため、規制当局が準拠を強制する能力が制限される可能性がある。

4. まとめ

FAPI 2 は、本稿では全ての推奨事項を満たしているため、オープン API（例えば、オープンバンキング/金融）標準およびエコシステムにおけるセキュリティプロファイルとすべきである。

しかし、多くのプロバイダー（例えば、銀行や金融機関）にとって、ドラフトの仕様を実装することに抵抗があるだろう。規制の厳しい分野ではなおさらである。また、いくつかの規制当局は、プロファイルおよび/またはコンフォーマンス・スイート（準拠性検証テスト集）がまだドラフト段階となると、厳格なコンフォーマンステストや認定制度を導入することに消極的姿勢を示す。

したがって、2022 年末までにオープンバンキング/金融の導入を検討しているエコシステムに対しては、以下のものを公式のセキュリティプロファイルとして採用することを推奨する：

- FAPI 1 Advanced（高度版）
- 認可グラントのパラメータ渡しの方法として、（FAPI 2 への移行を容易にするため）FAPI 1 Advanced（高度版）内の PAR オプションを必須とする。

このプロファイルは単に「PAR 付き FAPI 1 Advanced（高度版）」と記載することができるため、標準化団体やエコシステムが新しい FAPI プロファイルや派生物を作成する必要はない。

このアプローチの利点は以下の通りである：

1. プロバイダと RP は、成熟し十分に定義され、広く使用されているセキュリティプロファイルを実装することで、すべての関係者に保証を与えることができる。
2. このプロファイルをサポートするベンダーのソリューションが多数存在するため、プロバイダと RP の実装が迅速になる。
3. 堅牢で包括的なコンフォーマンス・スイート（準拠性検証テスト集）があり、どのようなエコシステムにおいても、より高いレベルの適合性を可能にする。
4. プロファイルとコンフォーマンス・スイートの両方が、OpenID Foundation によって積極的にメンテナンスされサポートされているため、他の標準化団体の作業を大幅に削減する。
5. プロバイダと RP の双方にとって、FAPI 2 への比較的シンプルなアップグレード手順があり、どのソリューションも将来性を証明し、エコシステム間の相互運用性をサポートする。

FAPI 2 とそれに対応するコンフォーマンス・スイートが確定し、OIDF が FAPI 2 認証を検証し公表できるようになり次第、標準化団体、エコシステム、実装者が FAPI 2 に移行することを推奨する。