AUTHLETE

オープン API のセキュリティ動向

OAuth2 と金融グレード API (FAPI)

工藤達雄

Authlete, Inc.

Agenda

- 「銀行 API」と OAuth2 (OAuth 2.0)
- 金融グレード API (FAPI)
- FAPI を中心とする世界の潮流
- OAuth2/FAPI 活用に向けたポイント

About Me

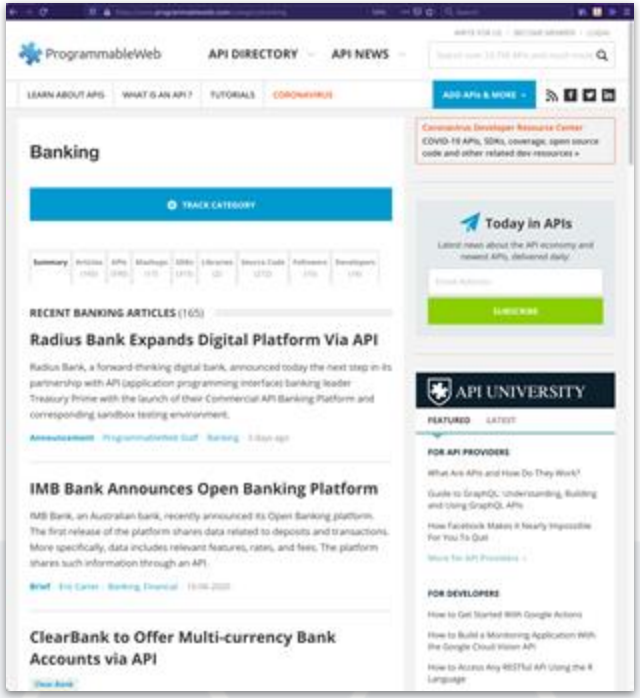
- サン・マイクロシステムズ、野村総合研究所、NRI セキュアを経て、2018年 Authlete に入社
- 20数年間、デジタルアイデンティティを中心とするプリセールス・コンサルティング・事業開発・エバンジェリズムに従事

AUTHLETE

「銀行 API」と OAuth2 (OAuth 2.0)

「銀行API」とは

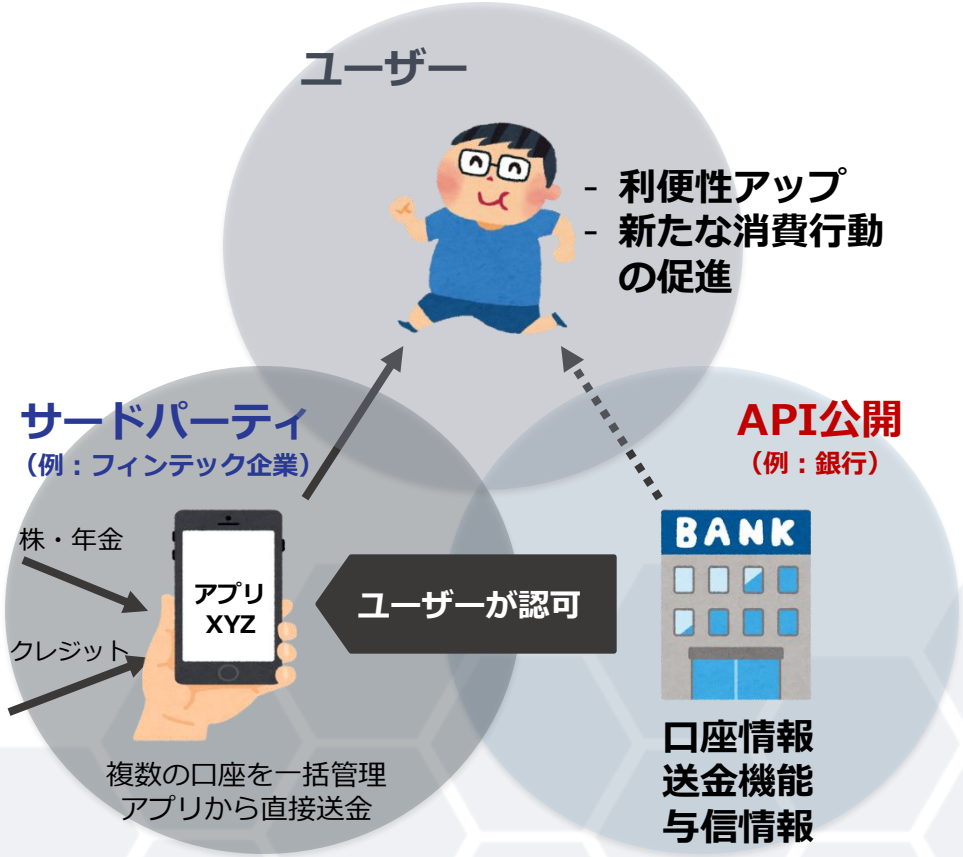
- 「オープンデータ」の提供
  - 支店の住所情報など
- コア機能のホワイトレーベル提供
  - “Bank as a Service”
- お客さまに関わるデータ・機能の提供
  - 口座情報・契約情報・取引履歴などのデータ、取引の実行機能など



約2.4万API中、Bankingカテゴリに登録されているのは590種類

Source: https://www.programmableweb.com/category/banking

API 提供をユーザーが制御するための “OAuth2”



APIアクセス認可

どのユーザーが
どのサードパーティに
どのような権限を与えるか

OAuth2

国内の銀行API におけるOAuth2 の位置づけ

- オープンAPIのあり方に関する検討会報告書
  （2017年 7 月13日） https://www.zenginkyo.or.jp/abstract/council/openapi/
  - *“「認可プロトコル」として、OAuth2.0認可フレームワーク（以下「OAuth2.0」という。）を推奨する。”*

- 金融機関とAPI接続先のためのAPI接続チェックリスト（2019年 9 月27日一部改訂） https://www.fisc.or.jp/document/fintech/004194.php
  - *“OAuth2.0の仕組みを理解しており、それに関連する項目の意味を説明することができる。”*

What Does Your OAuth2 Look Like?

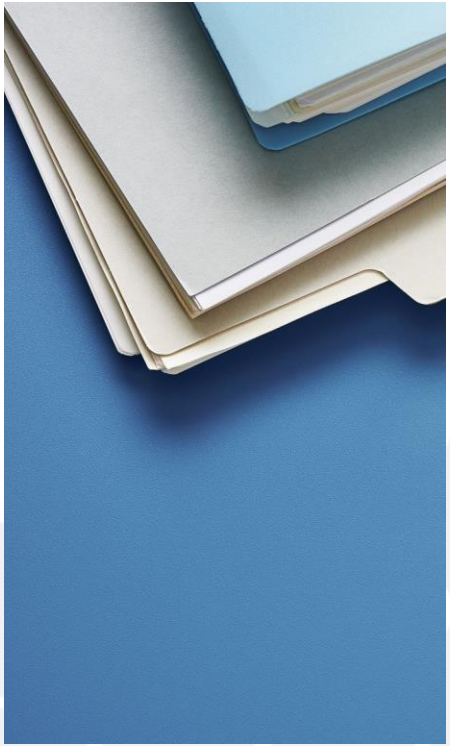
- OAuth2 は「フレームワーク」
  - 厳密な接続手順を定めた「プロトコル」ではない
- API 提供側による「詳細仕様化」が必要
  - 例: スコープ (*) の設計、アクセストークン (**) のライフサイクル管理、…
- 仕様やプラクティスが次々に追加・更新
  - 要件に応じた適切な仕様の取捨選択が必須

Source: https://tools.ietf.org/wg/oauth/, https://openid.net/wg/fapi/

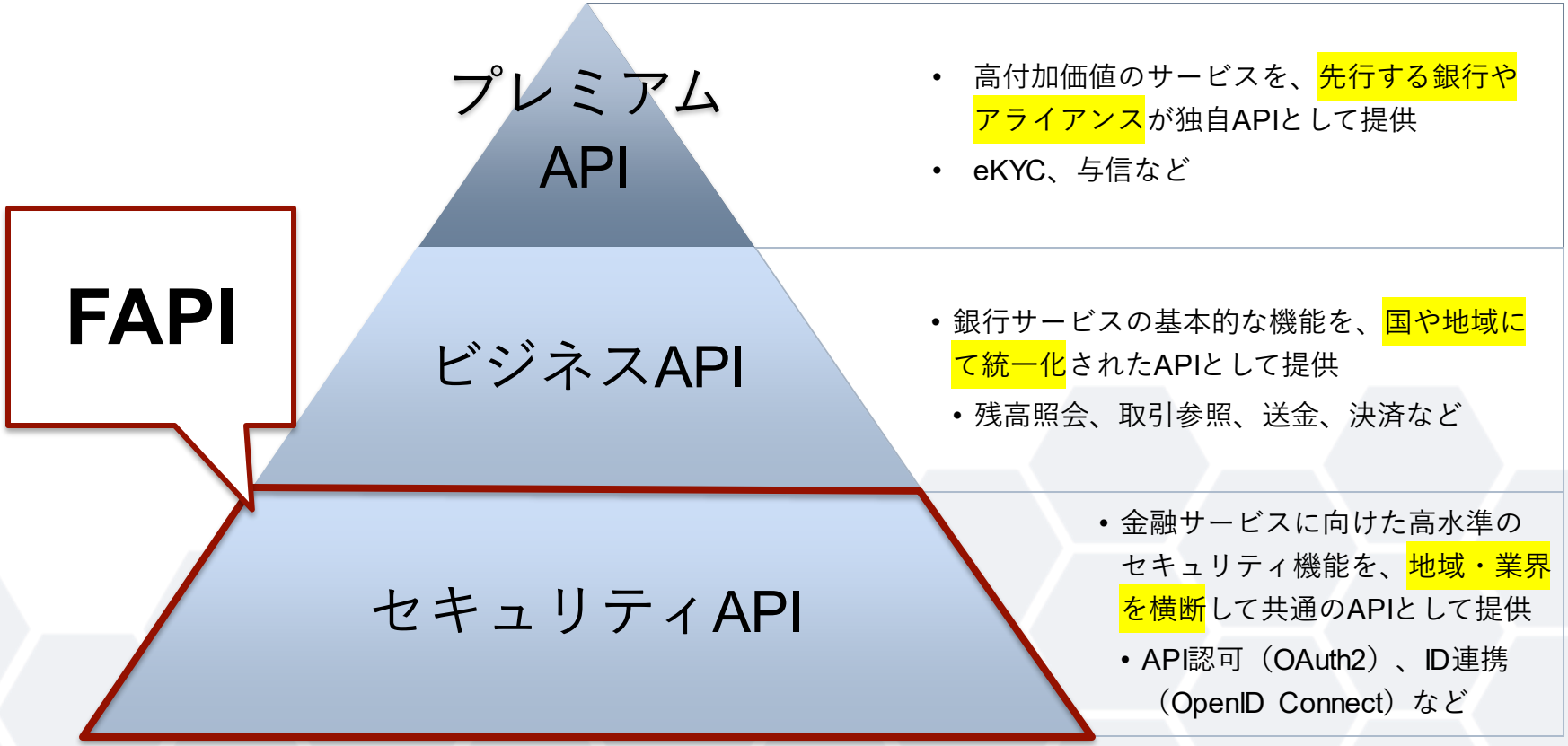
(*) APIアクセス権の範囲・種別
(**) APIアクセス権を表現する文字列

OAuth2 が銀行 API の進展を阻む（かも）

- 各行が独自に OAuth2 を詳細仕様化
  - 詳細仕様のさまざまな点が銀行ごとにバラバラ
  - 差異の把握・対応は API 利用側の負担
- 詳細仕様化のコストは各行が負担
  - オープン API 特有のセキュリティ対策は必須
  - しかし対策自体は直接的な収益に無関係



「セキュリティ API」の標準化・共通化



AUTHLETE

Financial-grade API

Financial-grade API (FAPI)

https://fapi.openid.net/

- 金融サービス API のセキュリティに適した OAuth2 の詳細仕様 (セキュリティプロファイル)
- 米国 OpenID Foundation に 2016 年設置された FAPI WG (*) にて検討
- FAPI バージョン 1 の仕様確定に向けて公開レビュー中 (**)
  - パート1 (Baseline): 基本的なセキュリティ対策
  - パート 2 (Advanced): より高度なセキュリティ対策

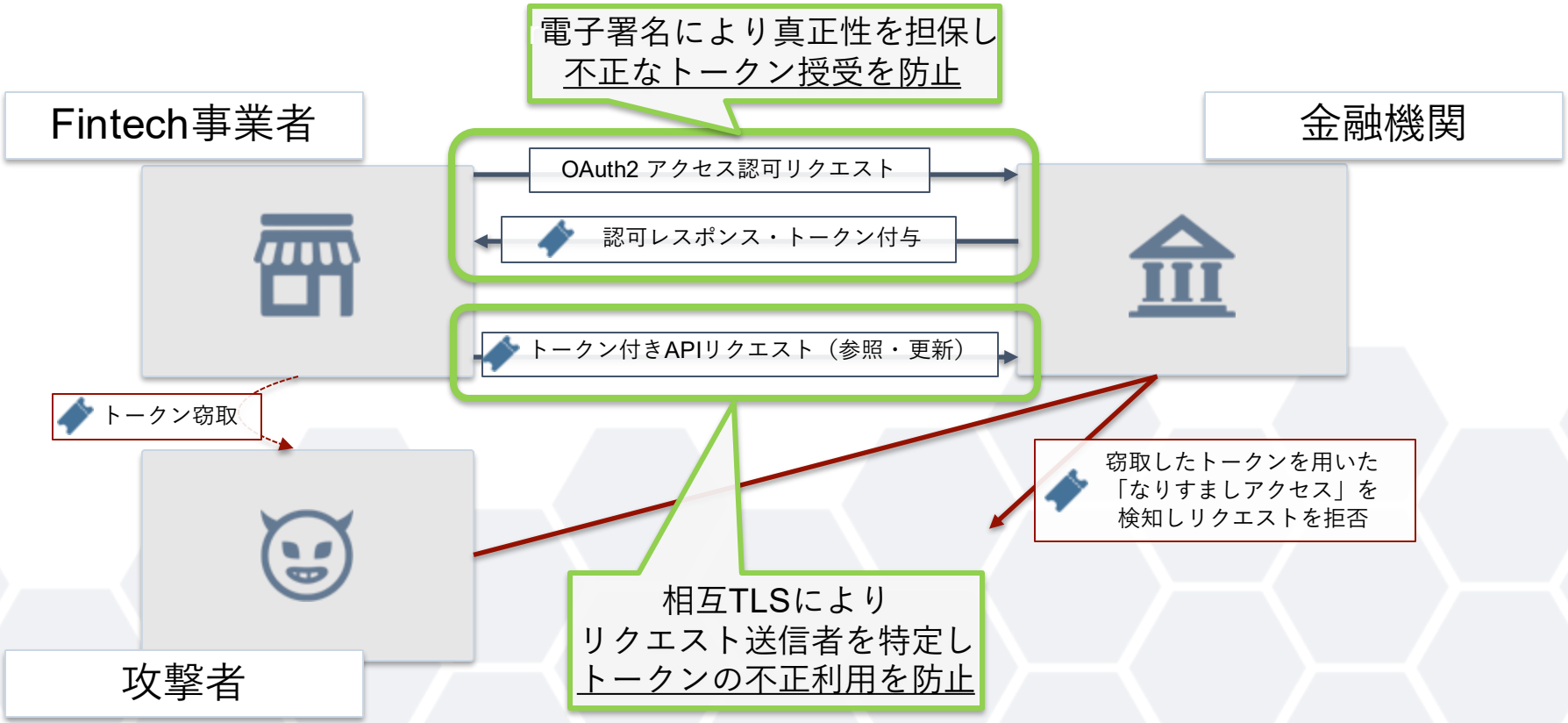
(*) Financial-grade API (*) ワーキンググループ。設立当初の名称は Financial API WG
(**) 2020 年12月現在

高度な OAuth2 セキュリティ対策の標準化

- OAuth2 の基本的な枠組みの下ではトークンの不正授受・不正使用に対処できない
  - トークンの不正授受: 攻撃者が授受手順を改ざん・偽造してトークンを不正に取得
  - トークンの不正使用: トークンを不正入手した攻撃者がそれを用いてAPIへアクセス
- FAPI Part 2 (Advanced)
  - OAuth2 をベースとする OpenID Connect (OIDC) 仕様の採用や、新たな OAuth2 拡張仕様を策定

FAPI Part 2 (Advanced)

不正なトークン授受・利用の防止



銀行における FAPI 採用の利点

- 独自詳細仕様の開発・運用に費やすコストの削減
- 高度な OAuth2 セキュリティの担保
  - “Formally verified”
- FAPI 実装の「認定プログラム」も有用
  - FAPI 準拠の有無をソフトウェア調達にて評価
  - 認定テストスイートを用いて自行の FAPI 実装を継続的にテストし、機能低下（デグレ）を防止

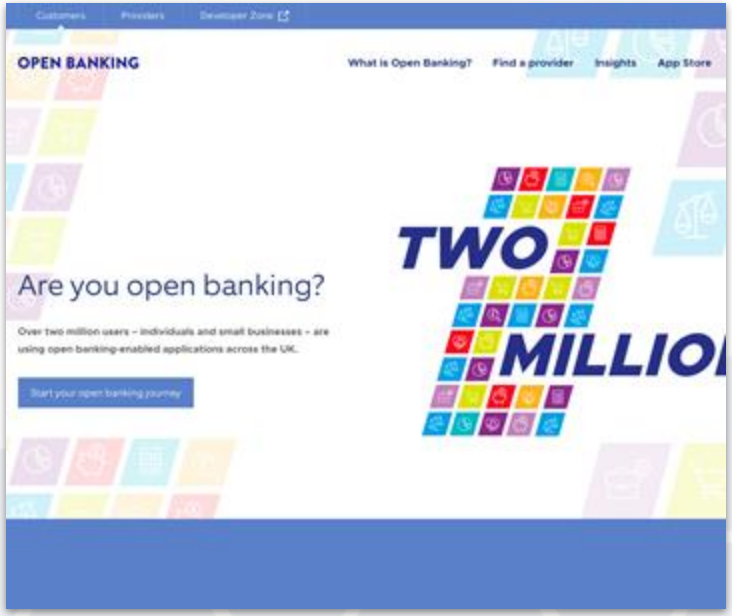
OpenID CERTIFIED

AUTHLETE

FAPI を中心とする世界の潮流

英国オープンバンキング

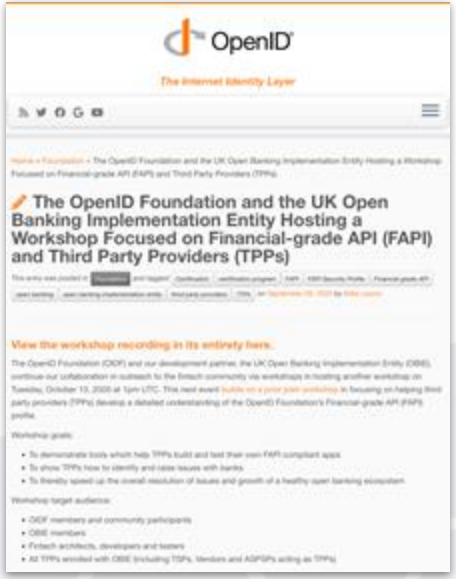
- 政府主導のもと銀行業界共通の API 技術標準を策定し上位 9 行に義務化
  - 他の銀行にも自主的な採用を促進
- 2020 年 10 月には API 提供側 (銀行) 76 行 / API 利用側 (サードパーティー) 204 社が参加



Source: https://www.openbanking.org.uk/

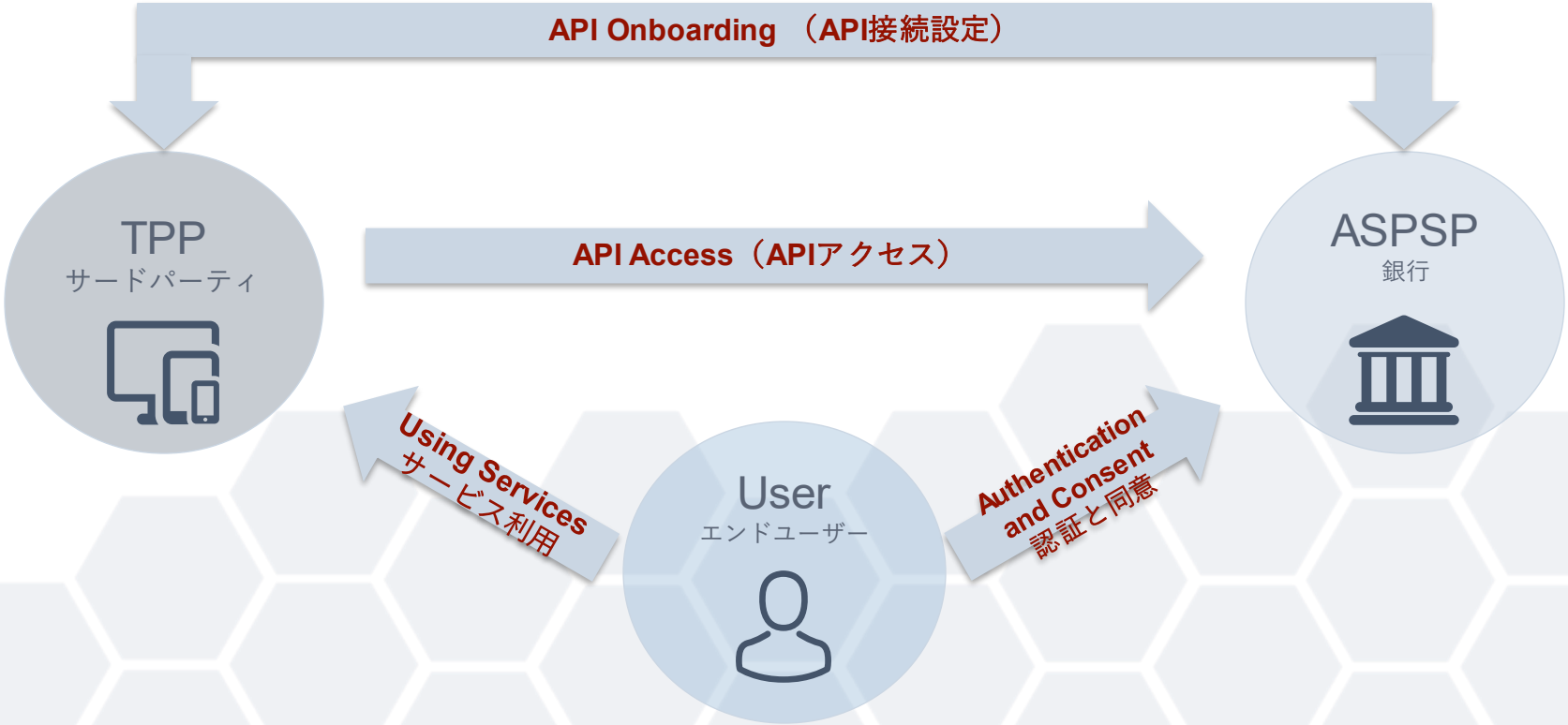
英国オープンバンキングと FAPI

- 当初（2017 年）は FAPI 仕様の初期案をベースにしつつ独自に OAuth2 を詳細仕様化
- 後に独自仕様を廃止し、FAPI をそのままのかたちで自国の OAuth2 詳細仕様として採用
  - Client Initiated Backchannel Authentication (CIBA) も採用
- 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

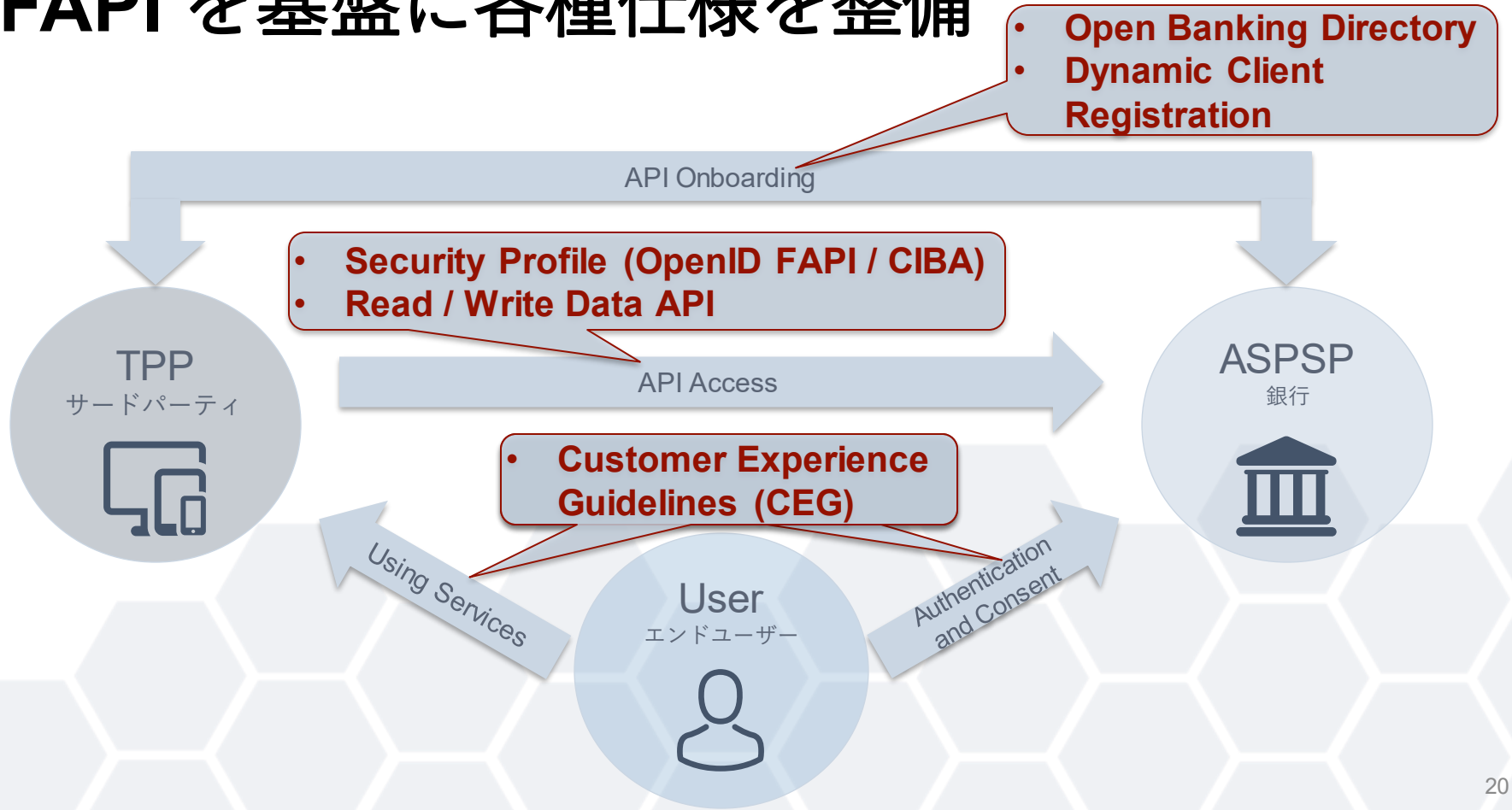


Source: https://openid.net/2020/09/29/the-openid-foundation-and-the-uk-open-banking-implementation-entity-hosting-a-workshop-focused-on-financial-grade-api-fapi-and-third-party-providers-tpps/

エンドユーザー・銀行・サードパーティの関係



FAPI を基盤に各種仕様を整備



AUTHLETE

Read/Write Data API Specification

各種 Read/Write Data API (Accounts and Transactions, Paymentsなど) のベースとなる仕様

- Overview
  - Document Structure
  - Design Principles
    - RESTful APIs
    - Standards
    - ISO 20022
    - Extensibility
    - Idempotency
    - Message Signing
    - Message Encryption
    - Agnostic to Payment Sche
    - Status Codes
    - Unique Identifiers (Id Field
    - Categorisation of Impleme
      - Mandatory
      - Conditional
      - Optional
- Basics
  - Actors
  - Character Encoding
  - Date Formats
  - Resource URI Path Stru
  - Headers
    - Request Headers
    - Response Headers
  - HTTP Status Codes
    - 400 (Bad Request) v
    - 403 (Forbidden)
    - 401 (Unauthorized)
    - 429 (Too Many Requ
  - Pre-Conditions
    - Pre-conditions for TP
    - Pre-conditions for AS
  - Idempotency
- Message Signing
  - Overview
  - Key Stores
  - Specification
  - Process for Signing a P
    - Step 1: Identify the P
    - Step 2: Form the JOS
    - Step 3: Compute the
    - Step 4: Add the JWS
  - Process for Verifying a
    - Step 1: Extract the co
    - Step 2: Validate the
    - Step 3: Verify the Sig
  - Sample JOSE Header
- Message Encryption
  - Overview
  - Message Signing and E
  - Key Stores
  - Encrypting Non-JSON
- Filtering
- Pagination
- Archiving
- Supplementary Data
- Security & Access Control
  - Scopes & Grant Types
  - Consent Authorisation
    - Error Condition
    - Token Expiry Time
    - Exemptions from Strong Customer
  - Supported Grant Types
    - Grant Types for identifying the TPP
      - Client Credentials Grant
    - Grant Types for identifying the TPP
      - Authorization Code Grant & Hybr
      - idtokenhint
    - CIBA
      - Identifying the PSU
        - Identifying the PSU Using a Us
        - Identifying the PSU Using an E
        - Identifying the PSU Using an In
        - Identifying the PSU Using a Pr
  - Changes to an Intent's Authorized Sta
    - Effect of Token Expiry on an Intent'
  - Consent Re-authentication
    - Ability to re-authenticate an Author
    - Low Friction User Experience
    - Use of Refresh Token
- Data Model
  - Enumerations
  - Common Payload Structure
    - Request Structure
      - Data
      - Risk
    - Response Structure
    - Error Response Structure
      - UML Diagram
      - Data Dictionary
    - Optional Fields
    - Links
    - Meta
- Usage Examples
  - Pagination Flows
    - Request
    - Paginated Resource Response
    - Request Next Page of Results
    - Paginated Resource Response
  - Error Flows
    - Missing or Expired Access Token
    - Incomplete or Malformed Request Payload
    - Missing or Invalid Access Token Scope
    - Sudden Burst of API Requests
    - Failed Authorisation Consent
    - JSON Error Response

Source: https://standards.openbanking.org.uk/api-specifications/red-write-specs/latest/

AUTHLETE

Security & Access Control

FAPI/CIBAをOpen Banking Standardにどう適用するか（プロファイル）の規定

- Overview
  - Document Structure
  - Design Principles
    - RESTful APIs
    - Standards
    - ISO 20022
    - Extensibility
    - Idempotency
    - Message Signing
    - Message Encryption
    - Agnostic to Payment Sche
    - Status Codes
    - Unique Identifiers (Id Field
    - Categorisation of Impleme
      - Mandatory
      - Conditional
      - Optional

- Basics
  - Actors
  - Character Encoding
  - Date Formats
  - Resource URI Path Stru
  - Headers
    - Request Headers
    - Response Headers
  - HTTP Status Codes
    - 400 (Bad Request) v
    - 403 (Forbidden)
    - 401 (Unauthorized)
    - 429 (Too Many Requ
  - Pre-Conditions
    - Pre-conditions for TP
    - Pre-conditions for AS
  - Idempotency

- Message Signing
  - Overview
  - Key Stores
  - Specification
  - Process for Signing a P
    - Step 1: Identify the P
    - Step 2: Form the JOS
    - Step 3: Compute the
    - Step 4: Add the JWS
  - Process for Verifying a
    - Step 1: Extract the co
    - Step 2: Validate the
    - Step 3: Verify the Sig
  - Sample JOSE Header
- Message Encryption
  - Overview
  - Message Signing and E
  - Key Stores
  - Encrypting Non-JSON
- Filtering
- Pagination
- Archiving
- Supplementary Data

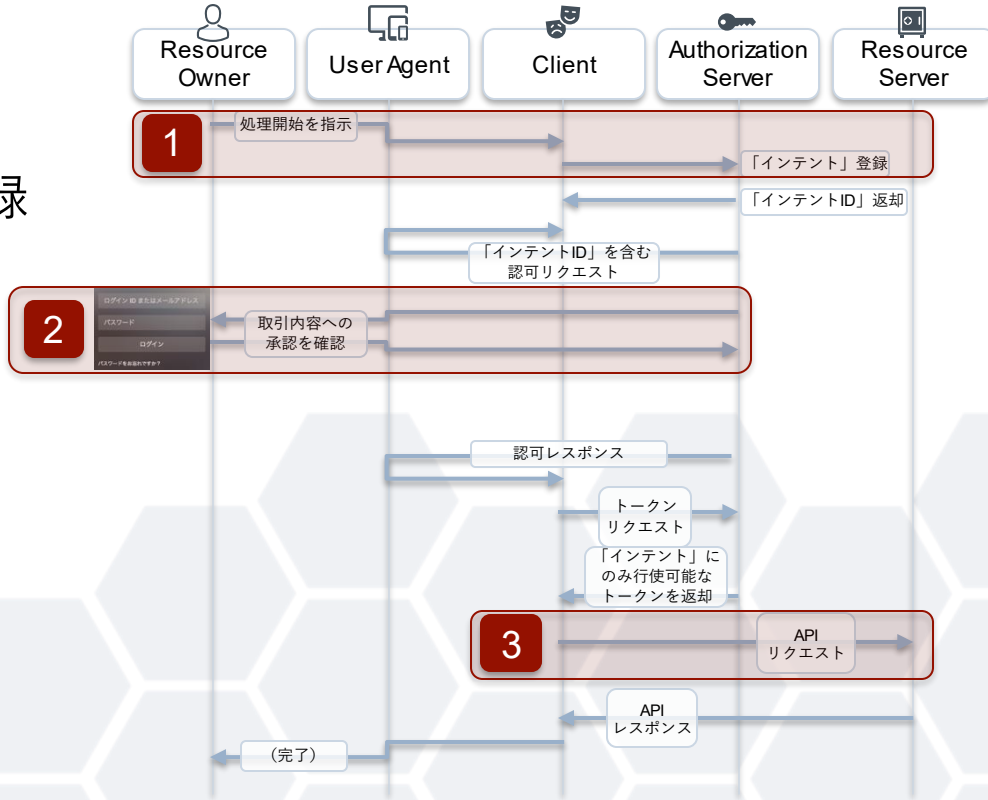
- Security & Access Control
  - Scopes & Grant Types
  - Consent Authorisation
    - Error Condition
    - Token Expiry Time
    - Exemptions from Strong Customer Authentication
  - Supported Grant Types
    - Grant Types for identifying the TPP
      - Client Credentials Grant
    - Grant Types for identifying the TPP and PSU
      - Authorization Code Grant & Hybrid Grant
      - idtokenhint
    - CIBA
      - Identifying the PSU
        - Identifying the PSU Using a User Id
        - Identifying the PSU Using an Ephemeral User Id
        - Identifying the PSU Using an Intent Id
        - Identifying the PSU Using a Previously Issued Id Token
  - Changes to an Intent's Authorized State
    - Effect of Token Expiry on an Intent's Authorized State
  - Consent Re-authentication
    - Ability to re-authenticate an Authorised consent at any point of time
    - Low Friction User Experience
    - Use of Refresh Token

- Sudden Burst of API Requests
- Failed Authorisation Consent
- JSON Error Response

Source: https://standards.openbanking.org.uk/api-specifications/red-write-specs/latest/

インテントによる「取引単位」のアクセス認可

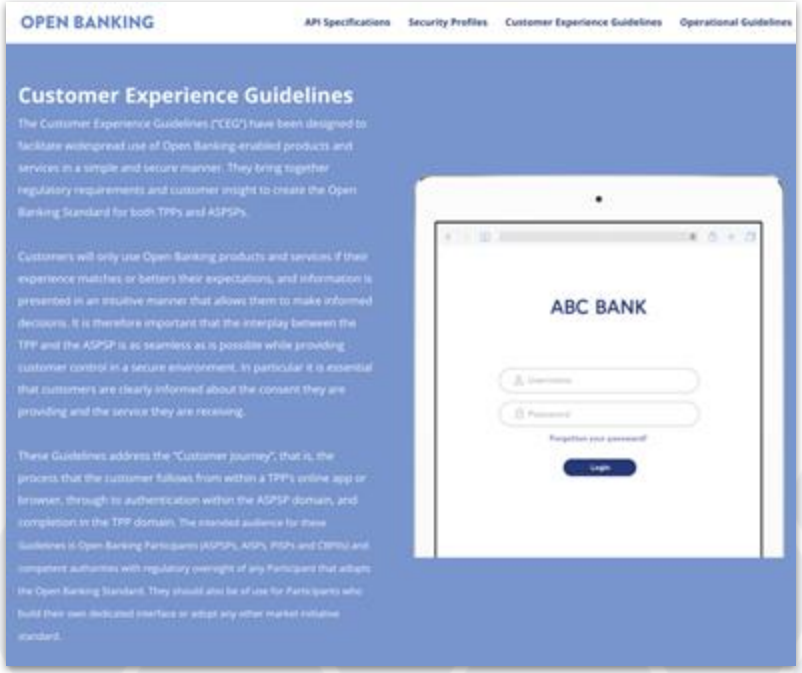
1. サードパーティが銀行の API に口座情報取得や決済指図伝達などの「インテント」を事前登録
2. 登録された内容を、利用者が銀行のWebサイトやアプリにて確認・承認
3. 承認後、サードパーティが「インテント」の内容の実行を銀行のAPIにリクエスト



Customer Experience Guidelines (CEG)

https://standards.openbanking.org.uk/customer-experience-guidelines/

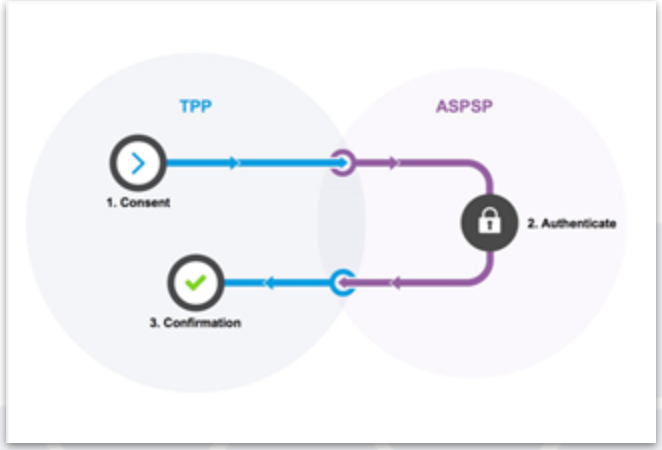
- 「カスタマージャーニー」の指針
- 各種規制（PSD2, RTS on SCA & CSC, CMA Order）への適合
- チェックリスト (CEG Checklist) を併せて提供

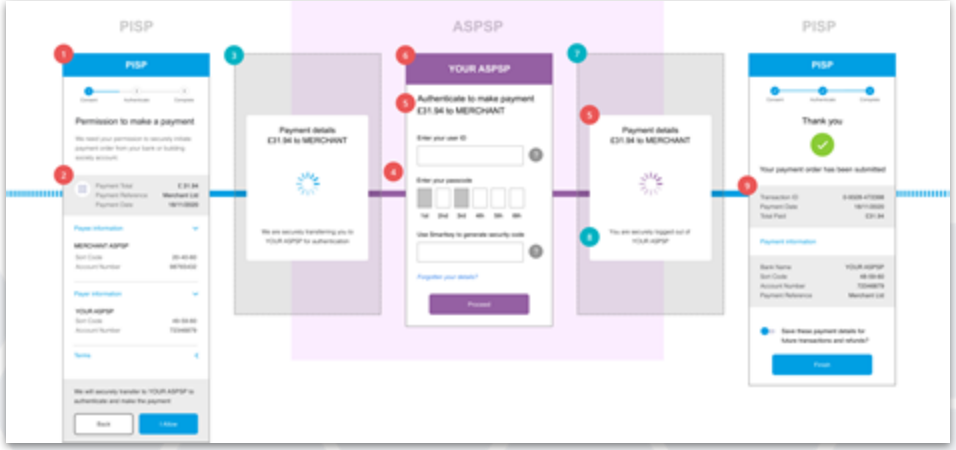


Source: https://standards.openbanking.org.uk/customer-experience-guidelines/

Open Banking カスタマージャーニー

- TPP/ASPSP間の連携プロセス
  - TPP側のアプリ/ブラウザから開始～ASPSP側でのユーザー認証～TPP側での連携完了まで
- 「TPPに共通の認証方式」と「各サービス固有の要素」を整理



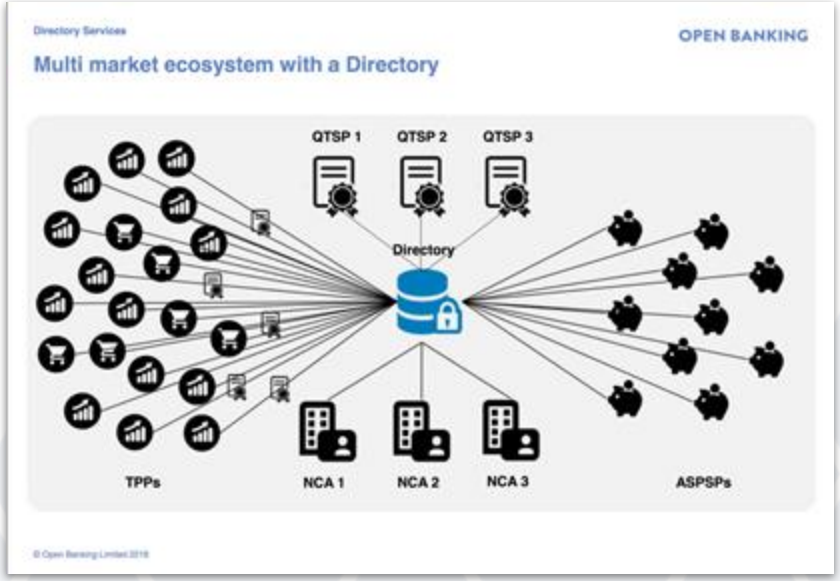


Source: https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/customer-journey/latest/, https://standards.openbanking.org.uk/customer-experience-guidelines/authentication-methods/redirection/browser-based-redirection-pis/latest/

参考: “Open Banking (OB) Directory”

- 参加する全ての事業者（銀行とサードパーティ事業者）が自組織の情報をOBディレクトリに登録
- OBディレクトリはSSA（後述）の発行や各行APIのメタデータ（接続に必要な設定情報）を管理

<u>→ サードパーティ事業者と銀行との連携にかかる設定を効率化</u>

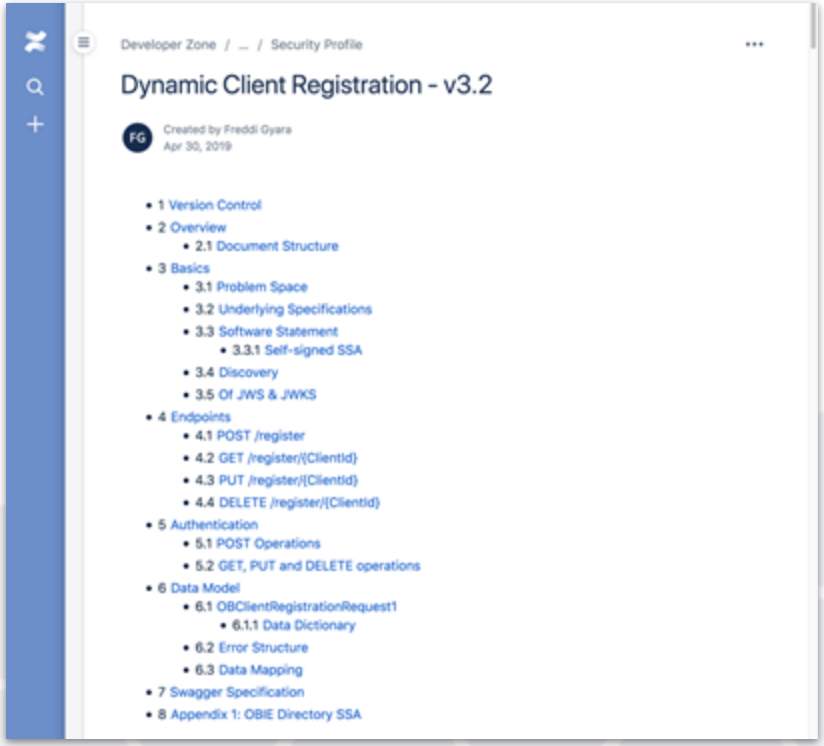


Source: https://finopolis.ru/materials-of-forum/2018/OpenBankingUpdate.pdf

参考: Dynamic Client Registration (DCR)

- Open Banking Directoryなどが TTPに “Software Statement Assertion” (SSA) を発行
  - Software Statement (SS): APIクライアントのメタデータ。署名もしくはMAC付きのJWT形式
  - SSA: 発行者（≠ TPP）によって署名されたSS
- TPPはそのSSAを用いて、ASPSPに対し、自身のAPIクライアントの動的登録を試行
- ASPSPは信頼する発行者のSSAであることを確認し、その内容を元にクライアントを登録

→ サードパーティ事業者が容易に複数行のAPIに接続可能に



Source: https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1078034771/Dynamic+Client+Registration+-+v3.2

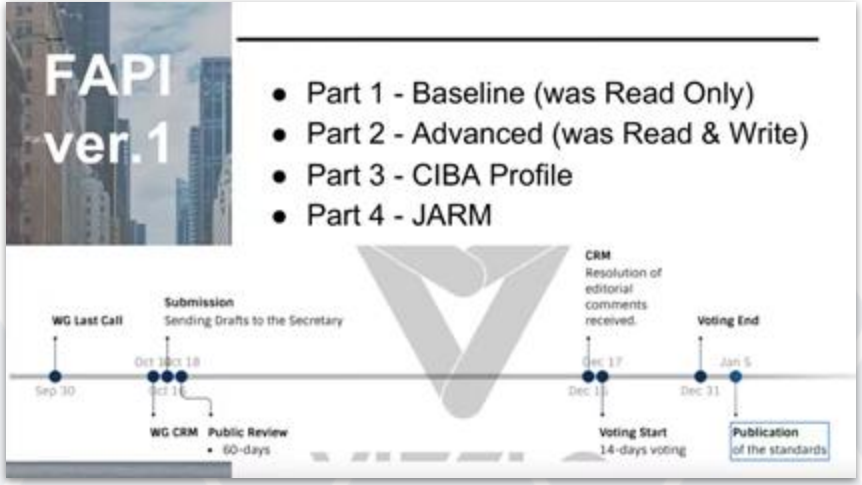
世界に波及する FAPI / OBUK プラクティス

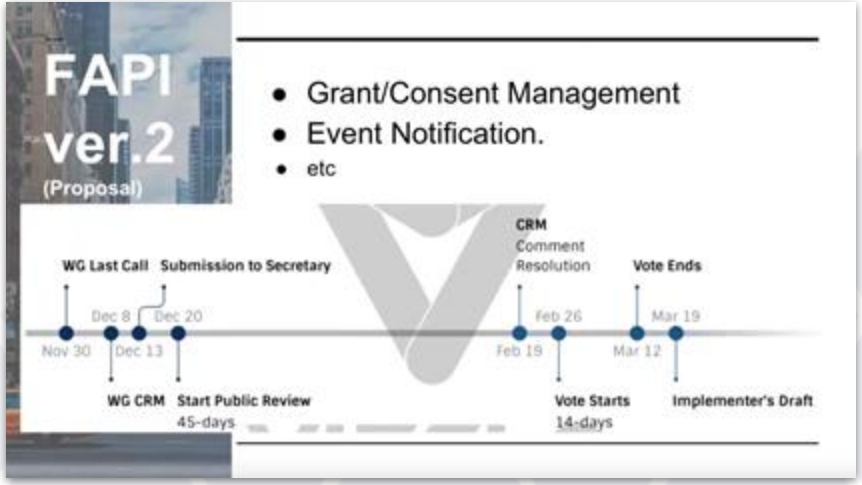
- 各国における標準のひな形として
  - オーストラリア (CDR)、ニュージーランド、米国 (FDX)、スロバキア、ナイジェリア、バーレーン、…
- 各行独自の実装として
  - 国内外の銀行および銀行向けソリューションプロバイダーからの引き合いが増えている (Authlete 社の状況)

Source: https://consumerdatastandards.gov.au/, https://paymentsdirection.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/overview, https://financialdataexchange.org/, https://www.sbaonline.sk/projekt/slovak-banking-api-standard/, https://openbanking.ng/, https://bahrainob.atlassian.net/wiki/spaces/BH/overview

FAPI の今後

- “FAPI1”
  - 2021年1月に確定の見込み
- “FAPI2”
  - リファクタリング+新機能





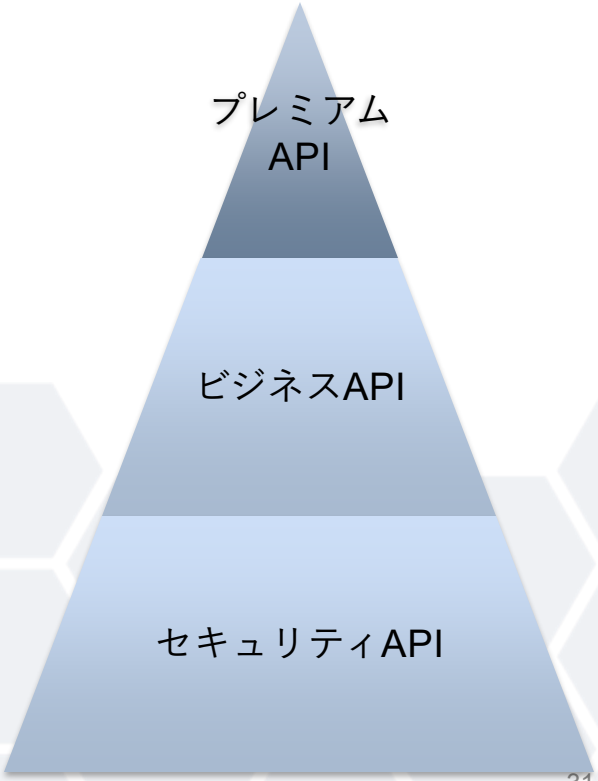
Source: https://youtu.be/LOha4RLt9eI

AUTHLETE

OAuth2/FAPI 活用に向けたポイント

FAPI が銀行 API の成否を分ける

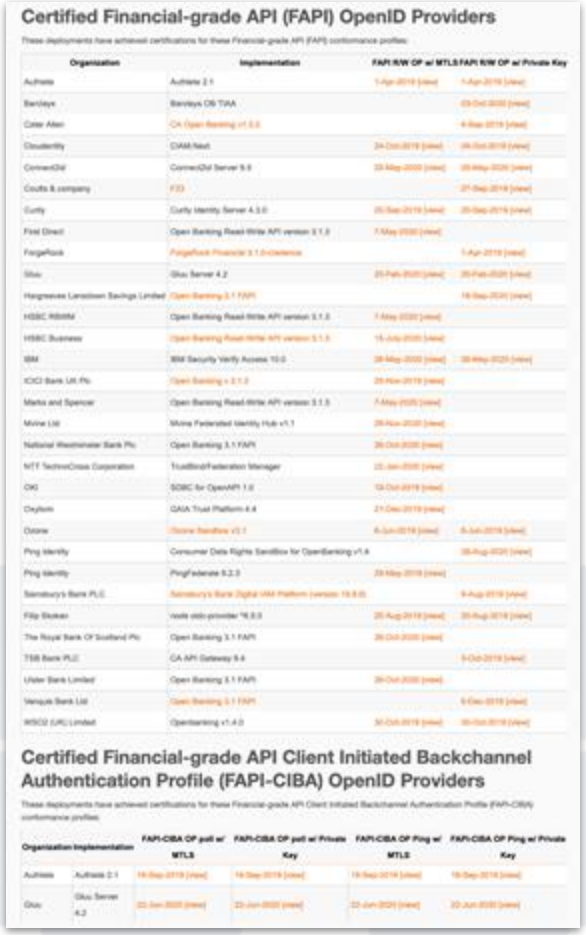
- 収益拡大のためには利用者数・取引数の増大が必須
- 業界共通のセキュリティ API として FAPI を採用し、相互接続のハードル低下と実装・運用コストの低減を目指すべきではないか



OAuth2/FAPI活用のポイント

1. 適切な実装の選定

- OAuth2/OIDC/FAPI のスタックを正しく実装するのは容易ではない
- <u>認定済のソフトウェア / サービスを利用し、コスト・期間を短縮</u>
    - FAPI OpenID Provider
    - FAPI-CIBA OpenID Provider



Certified Financial-grade API (FAPI) OpenID Providers

These deployments have achieved certifications for these Financial-grade API (FAPI) conformance profiles:

Organization	Implementation	FAPI R/W OP w/ MTLS	FAPI R/W OP w/ Private Key
Authlete	Authlete 2.1	1-Apr-2019 [view]	1-Apr-2019 [view]
Barclays	Barclays OB TAA		03-Oct-2020 [view]
Colin Allen	CA Open Banking v1.3.0		4-Sep-2019 [view]
Cloudentity	CIAM Next	24-Oct-2019 [view]	24-Oct-2019 [view]
ConnectOid	ConnectOid Server 5.0	22-May-2020 [view]	22-May-2020 [view]
Coutts & company	F33		27-Sep-2019 [view]
Curity	Curity Identity Server 4.3.0	25-Sep-2019 [view]	25-Sep-2019 [view]
First Direct	Open Banking Read-Write API version 3.1.3	7-May-2020 [view]	
ForgeRock	ForgeRock Financial 3.1.0-rc4beta		1-Apr-2019 [view]
Gluu	Gluu Server 4.2	23-Feb-2020 [view]	23-Feb-2020 [view]
Hargreaves Lansdown Savings Limited	Open Banking 3.1 FAPI		18-Sep-2020 [view]
HSBC RBWM	Open Banking Read-Write API version 3.1.3	7-May-2020 [view]	
HSBC Business	Open Banking Read-Write API version 3.1.3	15-July-2020 [view]	
IBM	IBM Security Verify Access 10.0	28-May-2020 [view]	28-May-2020 [view]
ICICI Bank UK Plc	Open Banking v 3.1.3	29-Nov-2019 [view]	
Marks and Spencer	Open Banking Read-Write API version 3.1.3	7-May-2020 [view]	
Mirine Ltd	Mirine Federated Identity Hub v1.1	29-Nov-2020 [view]	
National Westminster Bank Plc	Open Banking 3.1 FAPI	26-Oct-2020 [view]	
NTT TechnoCross Corporation	TrustBind Federation Manager	22-Jan-2020 [view]	
OKI	SOBC for OpenAPI 1.0	18-Oct-2019 [view]	
Oneform	QAIA Trust Platform 4.4	21-Dec-2019 [view]	
Ozone	Ozone Sandbox v3.1	6-Jun-2019 [view]	6-Jun-2019 [view]
Ping Identity	Consumer Data Rights Sandbox for OpenBanking v1.4		05-Aug-2020 [view]
Ping Identity	PingFederate 9.2.3	29-May-2019 [view]	
Sainsbury's Bank PLC	Sainsbury's Bank Digital IAM Platform (version 19.8.0)		8-Aug-2019 [view]
Filip Skokan	node oidc-provider *8.3.3	20-Aug-2019 [view]	20-Aug-2019 [view]
The Royal Bank Of Scotland Plc	Open Banking 3.1 FAPI	26-Oct-2020 [view]	
TSB Bank PLC	CA API Gateway 9.4		9-Oct-2019 [view]
Ulster Bank Limited	Open Banking 3.1 FAPI	26-Oct-2020 [view]	
Vanquis Bank Ltd	Open Banking 3.1 FAPI		9-Dec-2019 [view]
WSO2 (UK) Limited	Openbanking v1.4.0	30-Oct-2019 [view]	30-Oct-2019 [view]

Certified Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) OpenID Providers

These deployments have achieved certifications for these Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) conformance profiles:

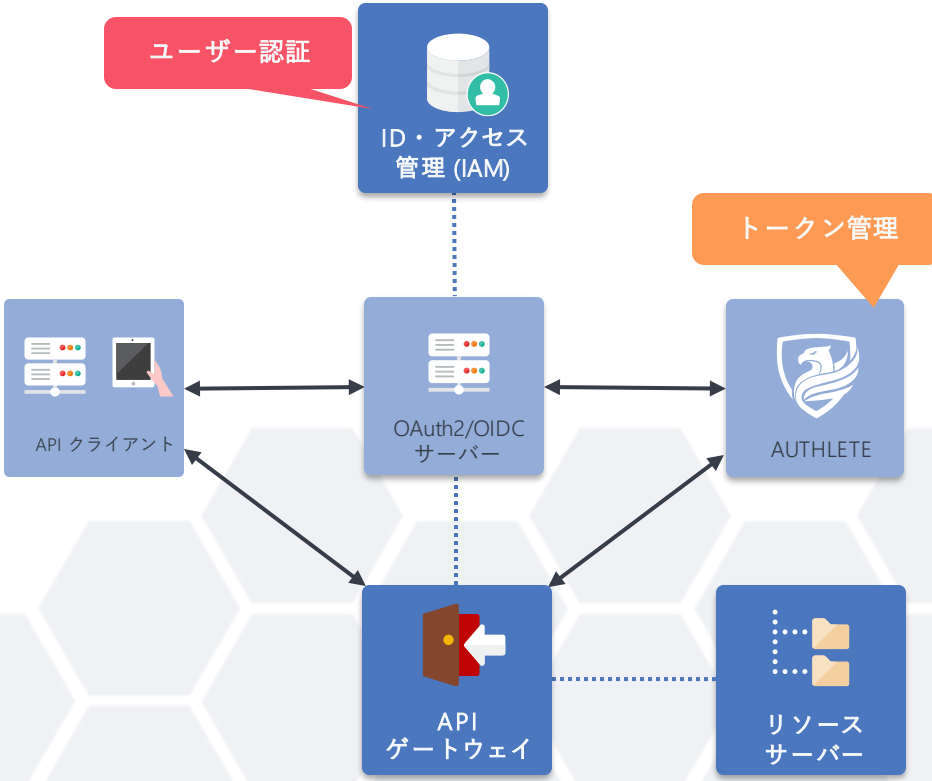
Organization	Implementation	FAPI-CIBA OP poll w/ MTLS	FAPI-CIBA OP poll w/ Private Key	FAPI-CIBA OP Ping w/ MTLS	FAPI-CIBA OP Ping w/ Private Key
Authlete	Authlete 2.1	18-Sep-2019 [view]	18-Sep-2019 [view]	18-Sep-2019 [view]	18-Sep-2019 [view]
Gluu	Gluu Server 4.2	22-Jun-2020 [view]	22-Jun-2020 [view]	22-Jun-2020 [view]	22-Jun-2020 [view]

Source: https://openid.net/certification/

OAuth2/FAPI活用のポイント

2. 既存 API 基盤の FAPI 対応

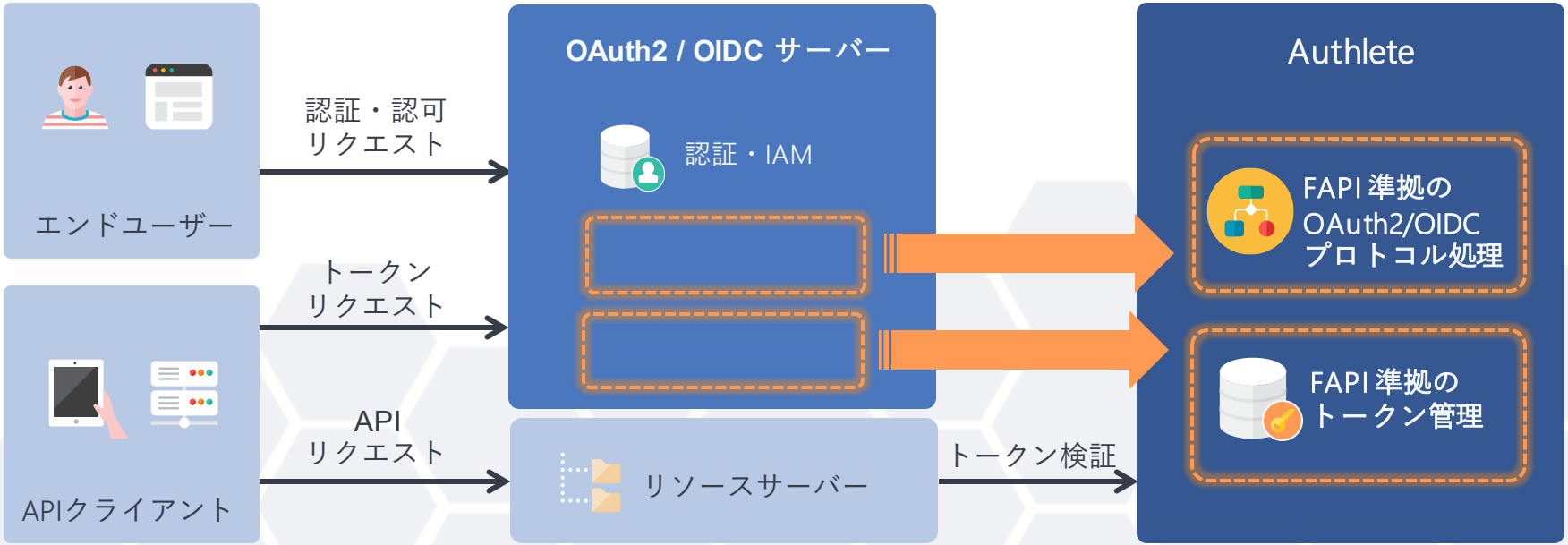
- 多くの銀行にはすでに ID・アクセス管理と API ゲートウェイ機能が存在する
- 既存 API 基盤を置き換えるのではなく、連携して FAPI に対応



OAuth2/FAPI活用のポイント

3.「FAPI対応」と「カスタマイズ性」の両立

- FAPI 対応がサービス提供の足枷になってはならない
- OAuth2/OIDC サーバーから「FAPI 対応機能」を分離



AUTHLETE

まとめ

Call to Action

自行独自の API 仕様策定は
競争優位性を創出しているか?

自行独自 API の「OAuth2 詳細仕様」は
業界標準の FAPI に勝るのか?

自行の既存 API 基盤をどうすれば
FAPI 対応にできるか?

Ask Authlete!

- OAuth2/OIDC/FAPI の専門家集団が仕様策定への貢献からソリューションとコンサルティング提供まで実施
- 独自のソリューションアーキテクチャにより既存・新規 API 基盤への容易な導入を実現
- 金融 API 分野をはじめとする国内外のさまざまな業界での豊富な経験と実績

AUTHLETE

Thank You

www.linkedin.com/in/tatsuokudo

www.authlete.com