AUTHLETE

Authlete導入事例に学ぶ オープンAPI強化のポイント

工藤達雄

Authlete, Inc.

Agenda

- 「銀行API」の強化の方向性
- FAPI: 高付加価値APIに必要なセキュリティ基準
- CIBA: モバイルによるオンライン・オフラインの融合
- Authlete活用事例

About Me

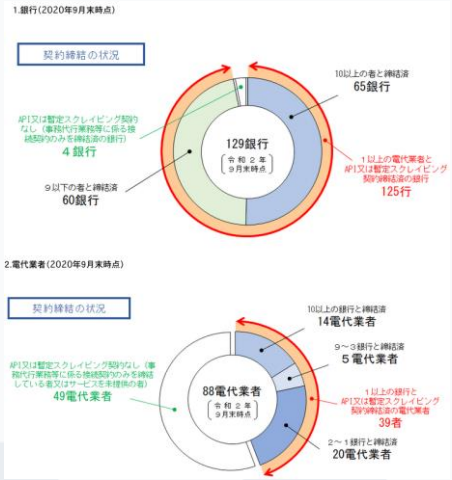
- サン・マイクロシステムズ、野村総合研究所、NRI セキュアを経て、2018年 Authlete に入社
- デジタルアイデンティティを中心とするプリセールス・コンサルティング・事業開発・エバンジェリズムに従事

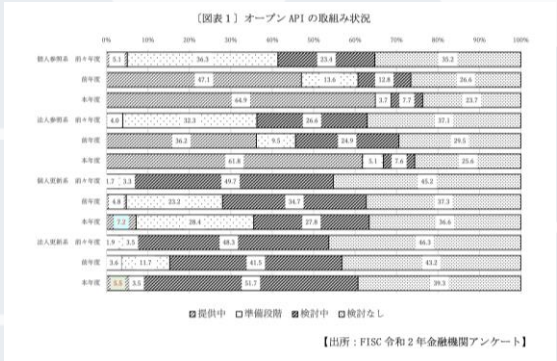
AUTHLETE

「銀行API」の強化の方向性

銀行APIの現状

- 国内のほぼすべての銀行がAPIを準備済み
  - 一方サードパーティからのAPI接続は低調
- 更新系APIの提供は限定的
  - 令和3年も微増に留まる

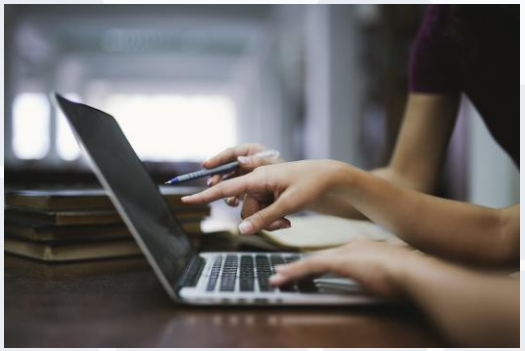




Source: 金融庁 https://www.fsa.go.jp/status/keiyakujoukyou_api/index.html,
FISC https://www.fisc.or.jp/document/fintech/file/FinTech_20210118_05.pdf

銀行APIを利用する側のニーズ

- ビジネス
  - どうすれば使えるか（契約）
  - いくらかかるか（利用料）
- テクノロジー
  - なにができるか（機能）
  - どこで使えるか（チャネル）



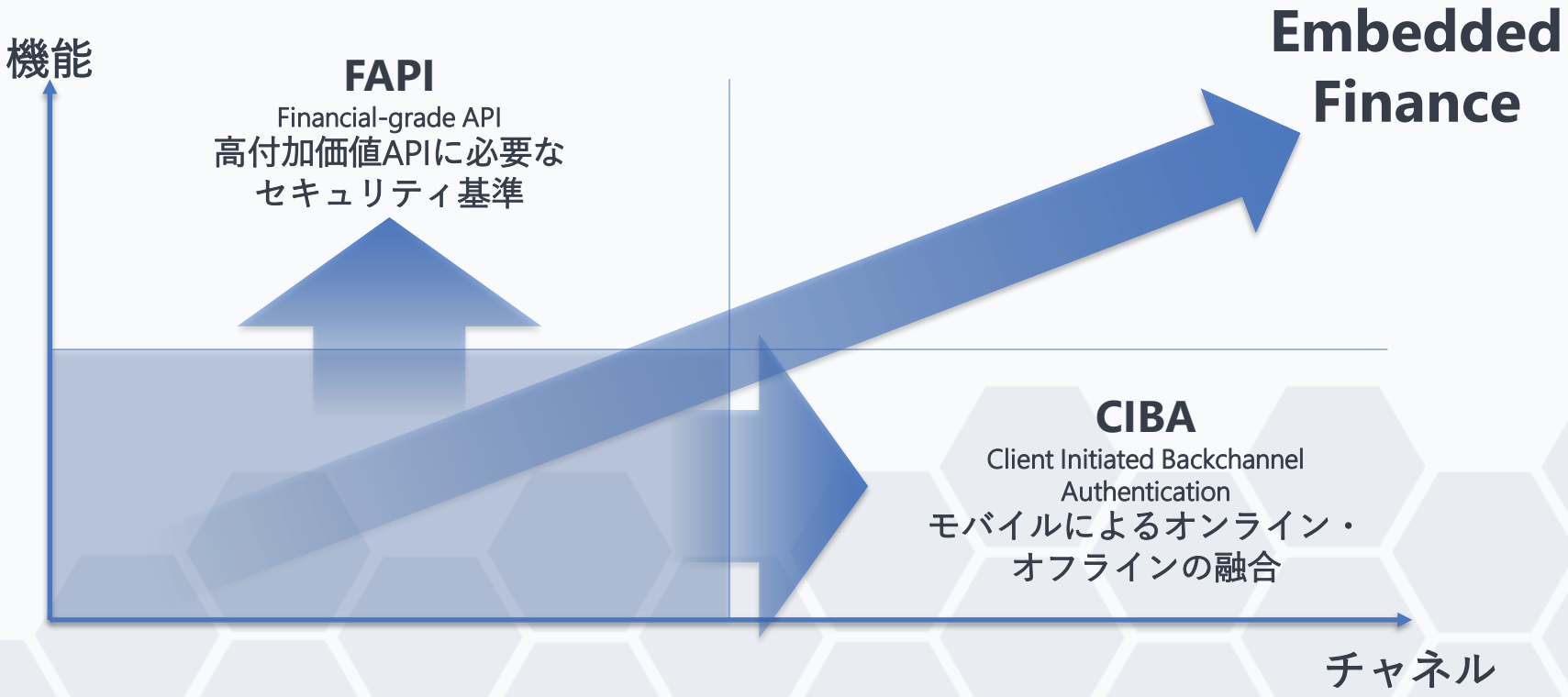
「機能」と「チャネル」

AUTHLETE

機能拡充とチャネル拡大

AUTHLETE

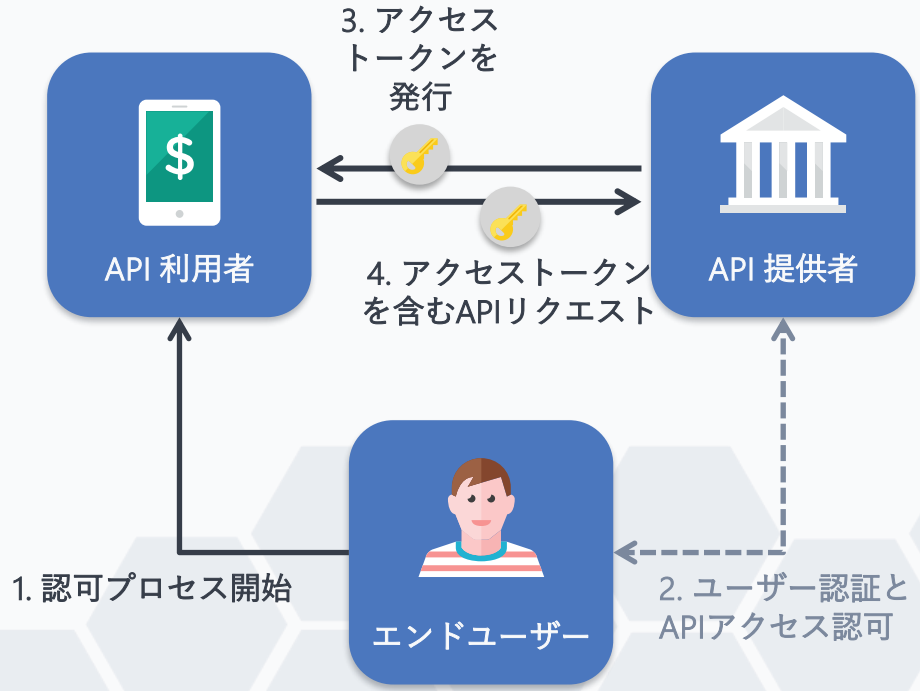
オープンAPI強化を実現する“FAPI” と “CIBA”



AUTHLETE

FAPI: 高付加価値APIに必要なセキュリティ基準

OAuth 2.0: オープン API のセキュリティの要

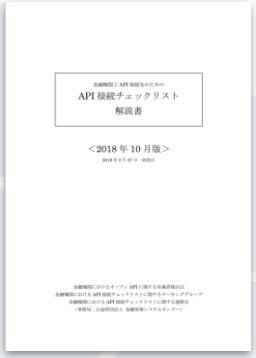


- API アクセスを
  エンドユーザーが
  認可
- “OAuth 2.0”
  - アクセストークンに
    よる API 認可
  - “OpenID Connect”
    - OAuth 2.0 の拡張

国内の銀行APIにおけるOAuth 2.0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。”



OAuth 2.0は銀行APIの認可を標準化したか?

- “金融機関は独自に具体的な対策を検討、実施”

(3). 更新系 API に関するサービスの進展状況

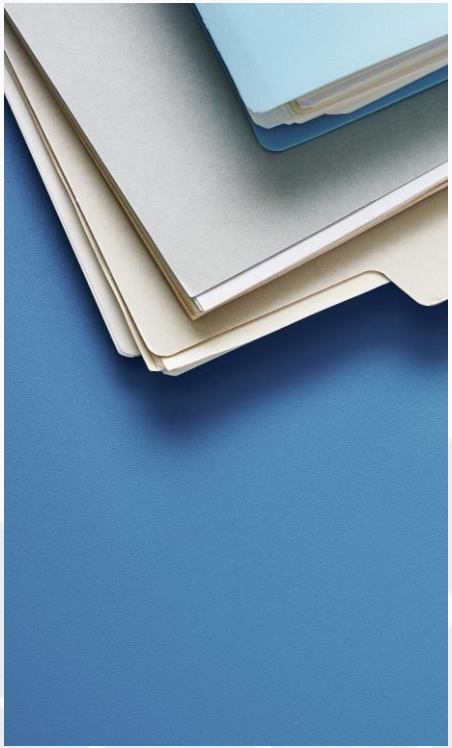
✧ 更新系 API 関連サービスを提供している電代業者、及びそのサービスを利用している金融機関に対して、更新系 API におけるチェックリストの利用状況についてヒアリングを行った。その結果の概要は次の通り。

- ➢ 更新系 API に関して、チェックリストに追加すべき確認項目はなかった。
- ➢ 更新系 API において、認証などのセキュリティは参照系 API よりも高いレベルが求められるため、金融機関は独自に具体的な対策（確認項目に対する手法例に該当するもの）を検討、実施していた。
- ➢ 更新系 API の場合、金融機関は自社システムの顧客データを更新することになるため、電代業者のシステムのセキュリティの内容について、参照系 API よりも確りと確認するようにしていた。

Source: FISC https://www.fisc.or.jp/document/fintech/file/FinTech_20210118_05.pdf

「（OAuth 2.0による）具体的な対策」の標準化

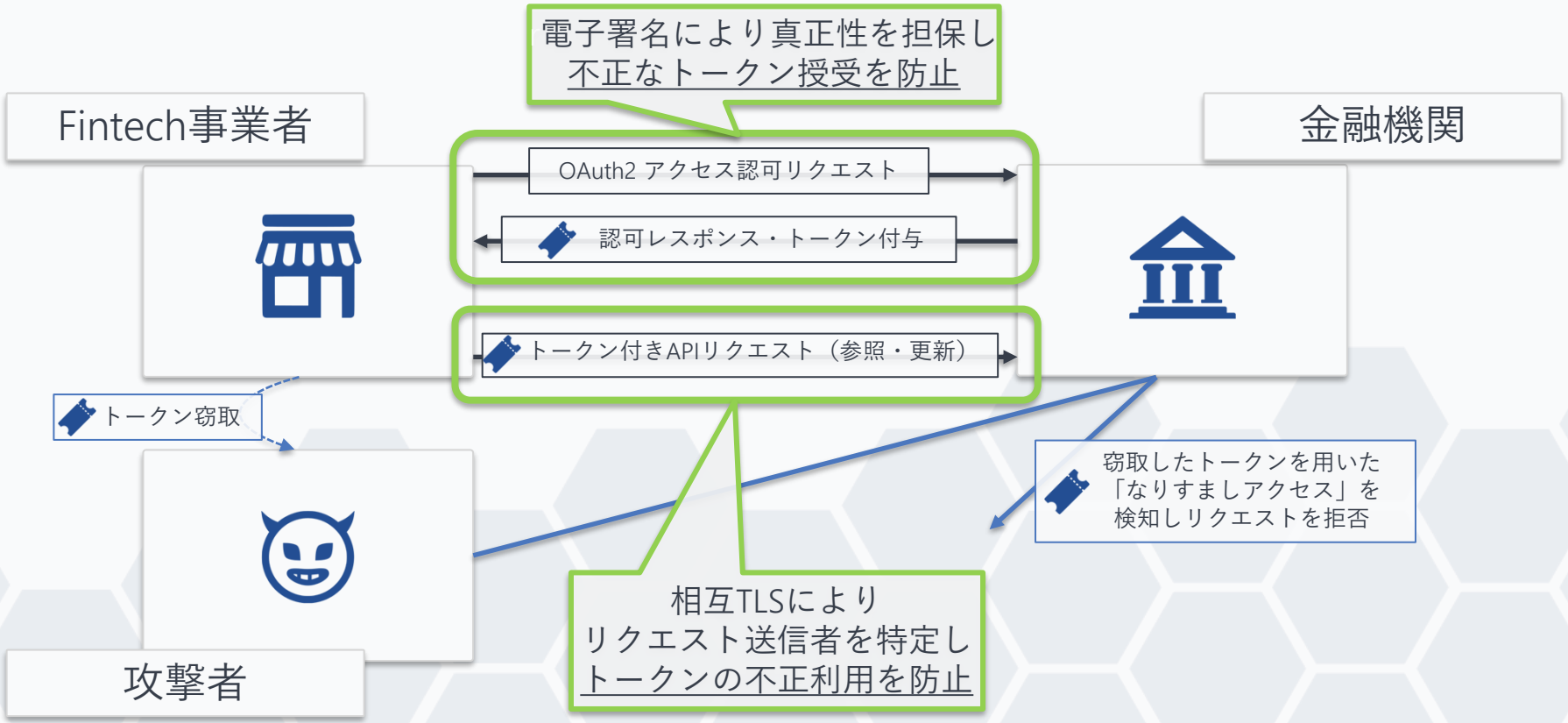
- 仕様解釈のブレや実装不備による脆弱性発生の防止
- 金融機関・事業者が個別に策定した独自仕様乱立の解消
- 過剰・冗長、あるいは逆に有意ではない「セキュリティ対策」の改善



FAPI (Financial-grade API)

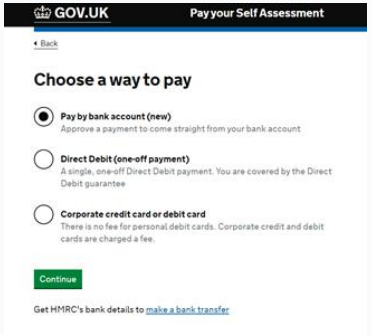
- 高いセキュリティが求められる（"金融グレード"）API向けのOAuth 2.0詳細仕様
- アクセストークンの授受・利用にかかるセキュリティ対策を標準化
- 2021年3月にFAPIバージョン1が確定

FAPI による不正なトークン授受・利用の防止



グローバルに進む FAPI 採用

- 運用中
  - 英国 (Open Banking UK)
  - オーストラリア (Consumer Data Right)
  - ブラジル (Open Banking Brasil)
- 採用表明
  - 米国 (Financial Data Exchange)
  - ロシア (FinTech Association)
- 検討開始
  - EU (Berlin Group)



Source: GOV.UK https://lifeathmrc.blog.gov.uk/2021/11/19/open-banking-payments-at-hmrc-a-team-making-history/, OneBanks https://onebanks.co.uk/cardless-cash-withdrawal/

銀行における FAPI 採用の利点

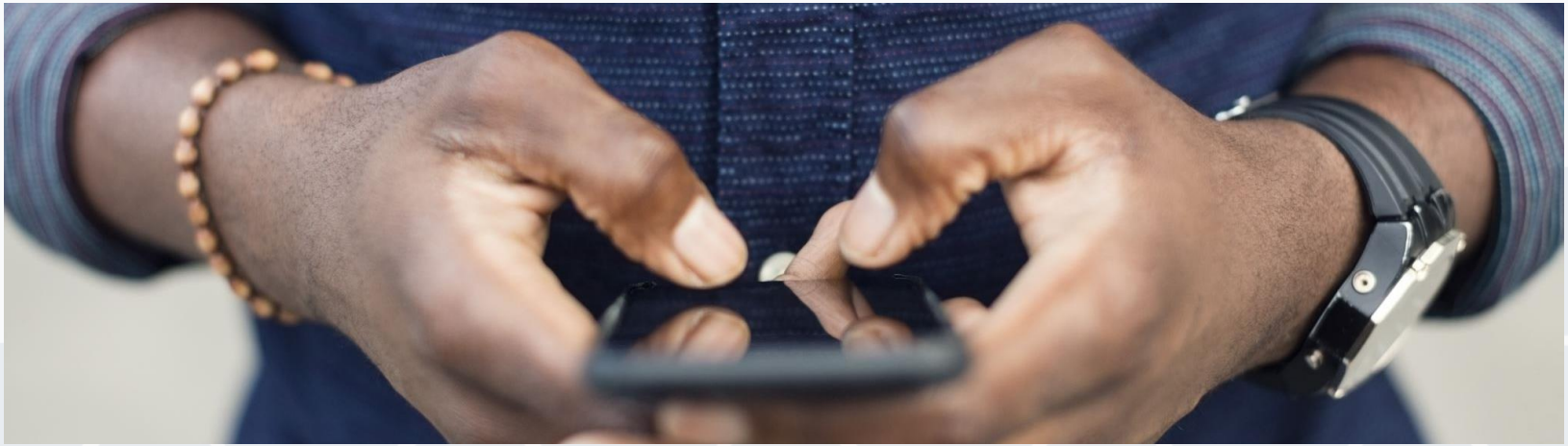
- 独自詳細仕様の開発・運用に費やすコストの削減
- 高度な OAuth 2.0 セキュリティの担保
- FAPI 実装の「認定プログラム」を活用可能
  - FAPI 準拠の有無をソフトウェア調達にて評価
  - 認定テストスイートを用いて自行の FAPI 実装を継続的にテストし、機能低下（デグレ）を防止

AUTHLETE

CIBA: モバイルによるオンライン・オフラインの融合

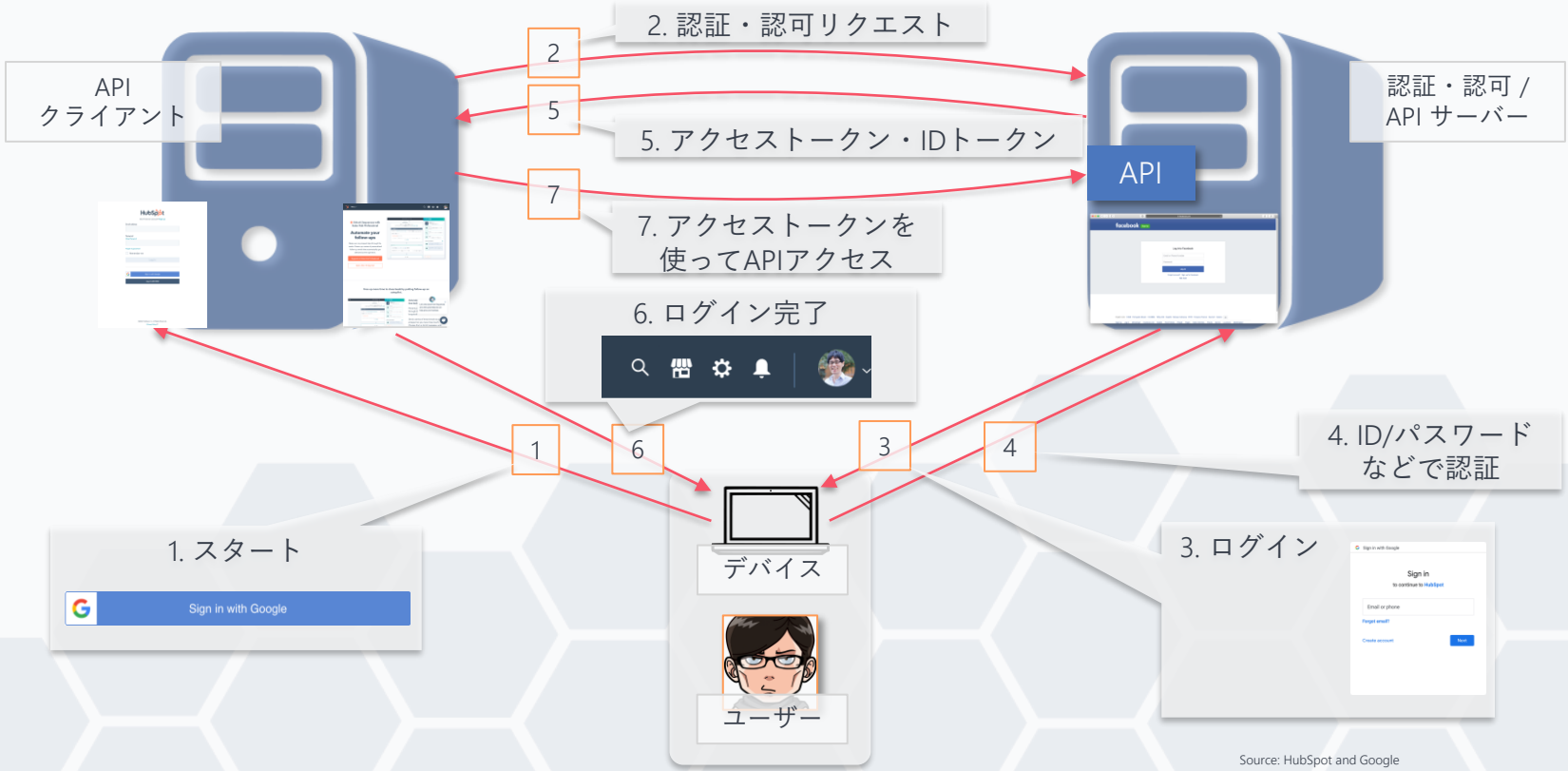
CIBAとは?（銀行の立場から）

- さまざまな局面でのユーザー認証・同意確認を「**銀行公式モバイルアプリ**」を用いて直接実施するためのサービス連携のしくみ



AUTHLETE

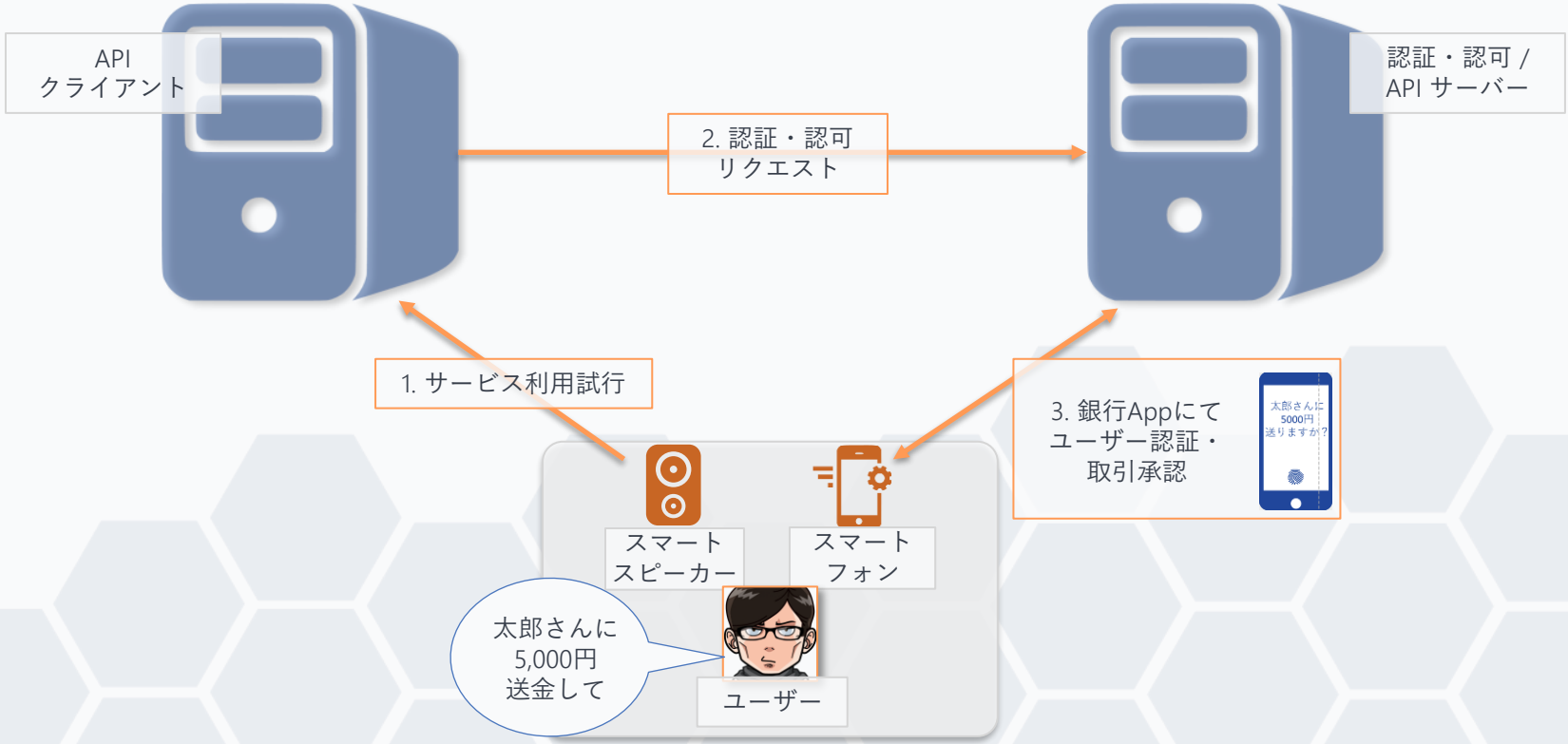
単一ユーザー/デバイスの認証・認可フロー



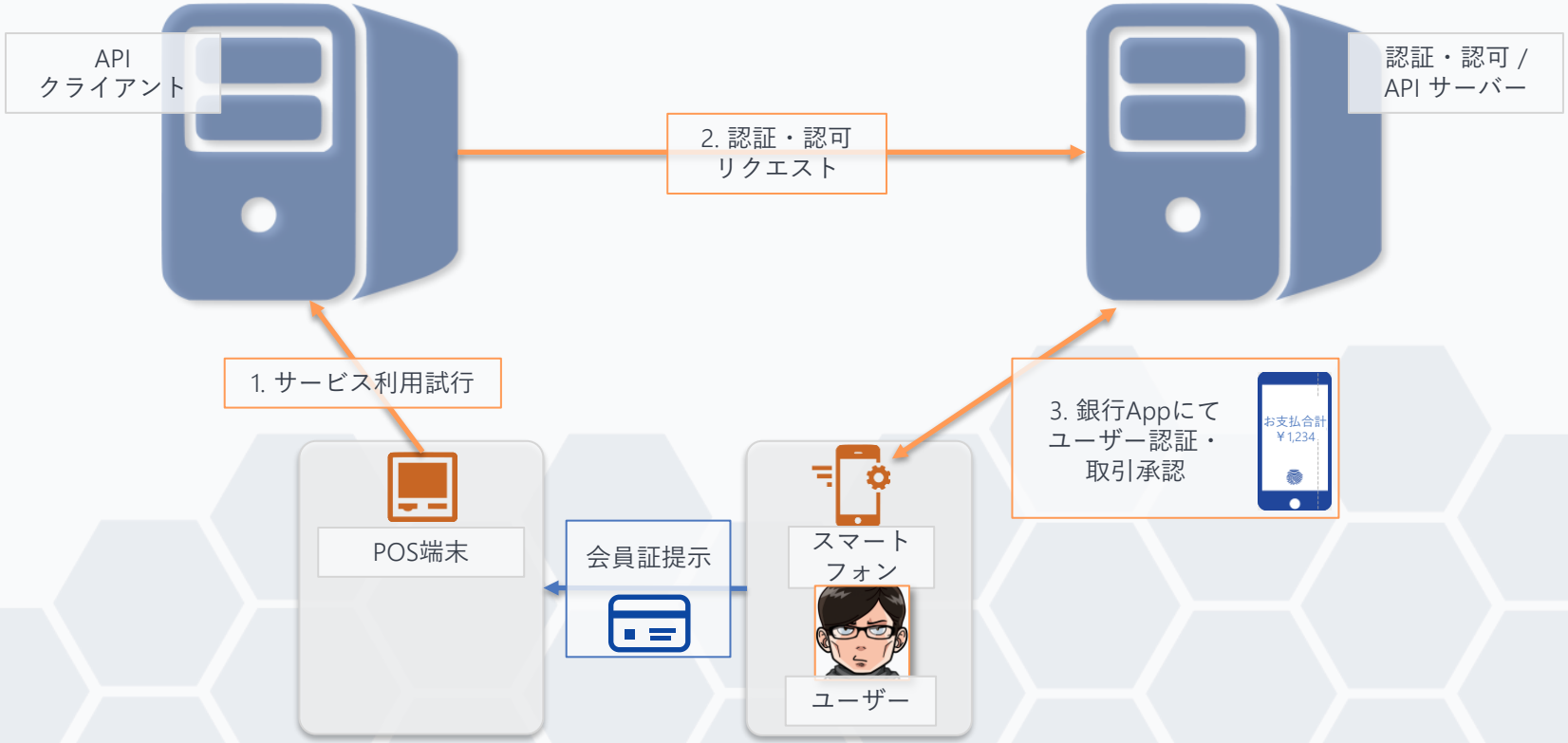
Source: HubSpot and Google

AUTHLETE

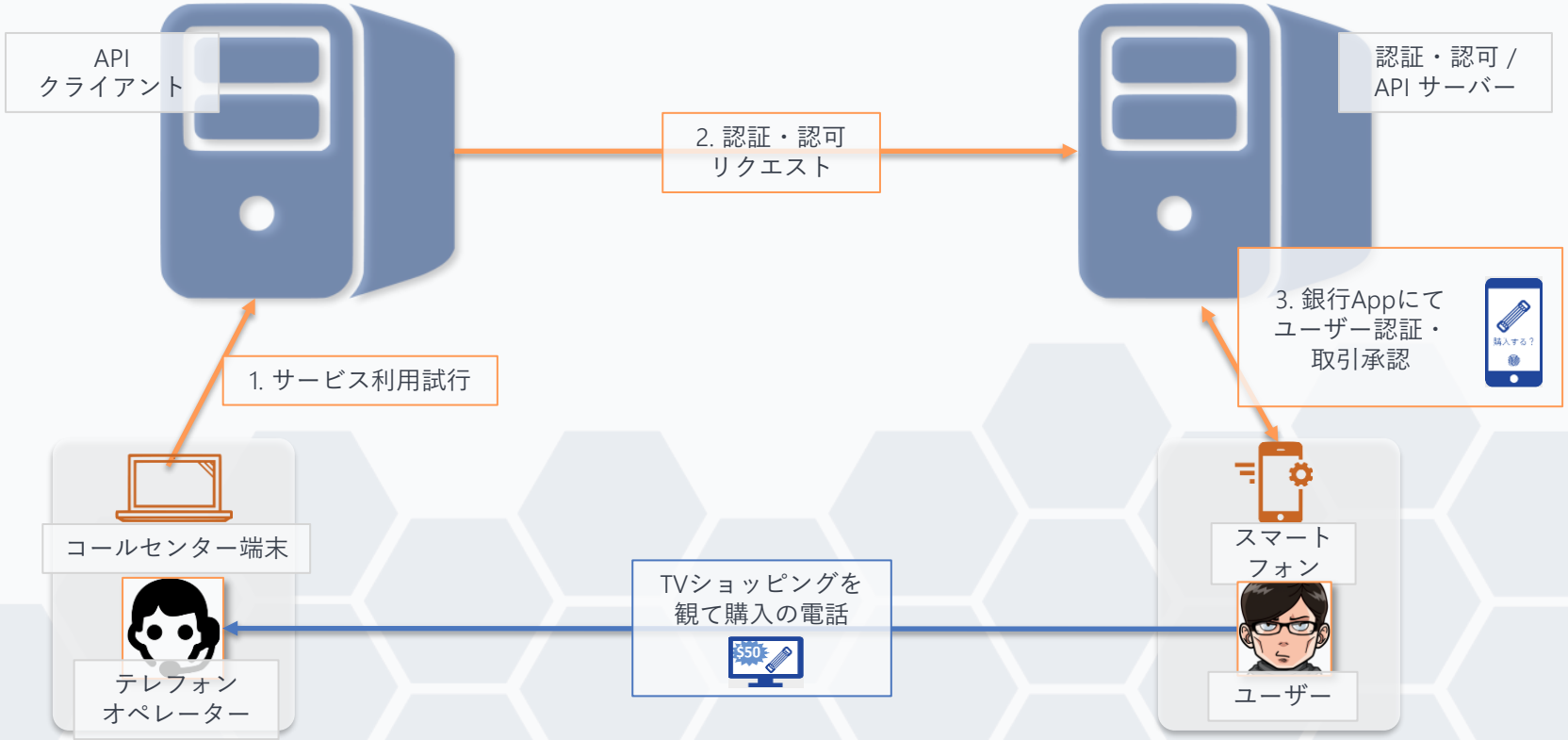
「サービス利用」と「認証・認可」の分離



ユーザーが所有しないデバイスと連携



ユーザー以外の誰かがサービスを利用

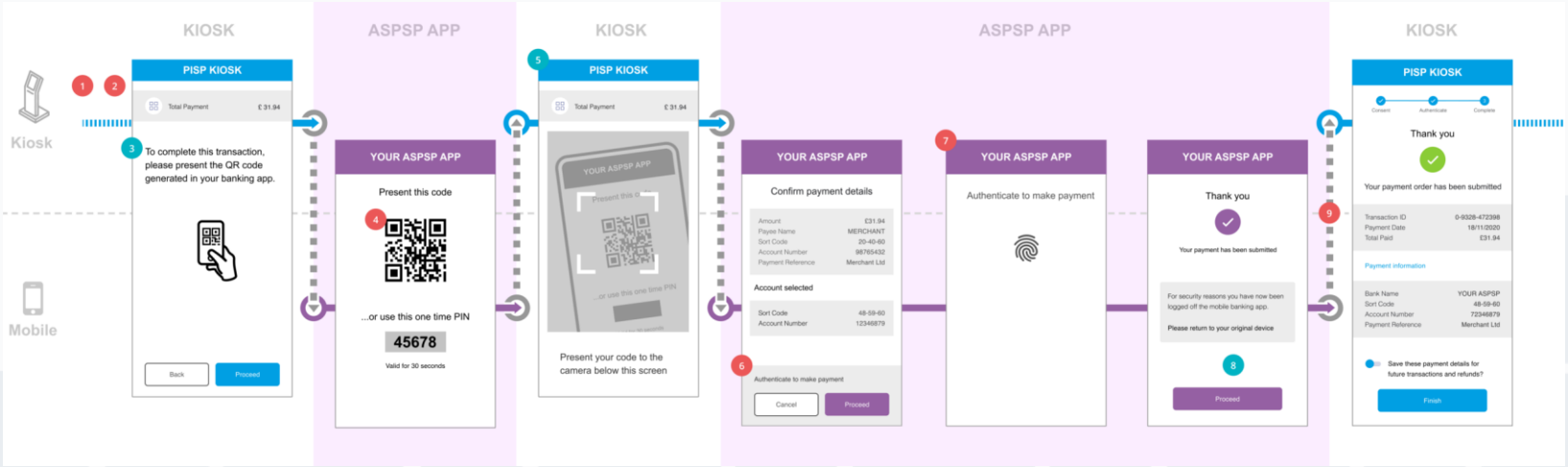


CIBA (Client Initiated Backchannel Authentication)

- 「API 利用」と「ユーザー認証・API 認可」のデバイスを分離
  - 「API 利用デバイス」がユーザーから離れていても連携できる
  - 「ユーザー認証・API 認可」は API 提供者（e.g. 金融機関）のアプリが行う

CIBAがFAPIの利用シーンを拡大

- “FAPI-CIBA プロファイル”
  https://openid.net/specs/openid-financial-api-ciba-ID1.html
  - CIBAをFAPIと組み合わせて適用するための詳細仕様
  - Open Banking UK, Open Banking BrasilなどがFAPIと併せて採用

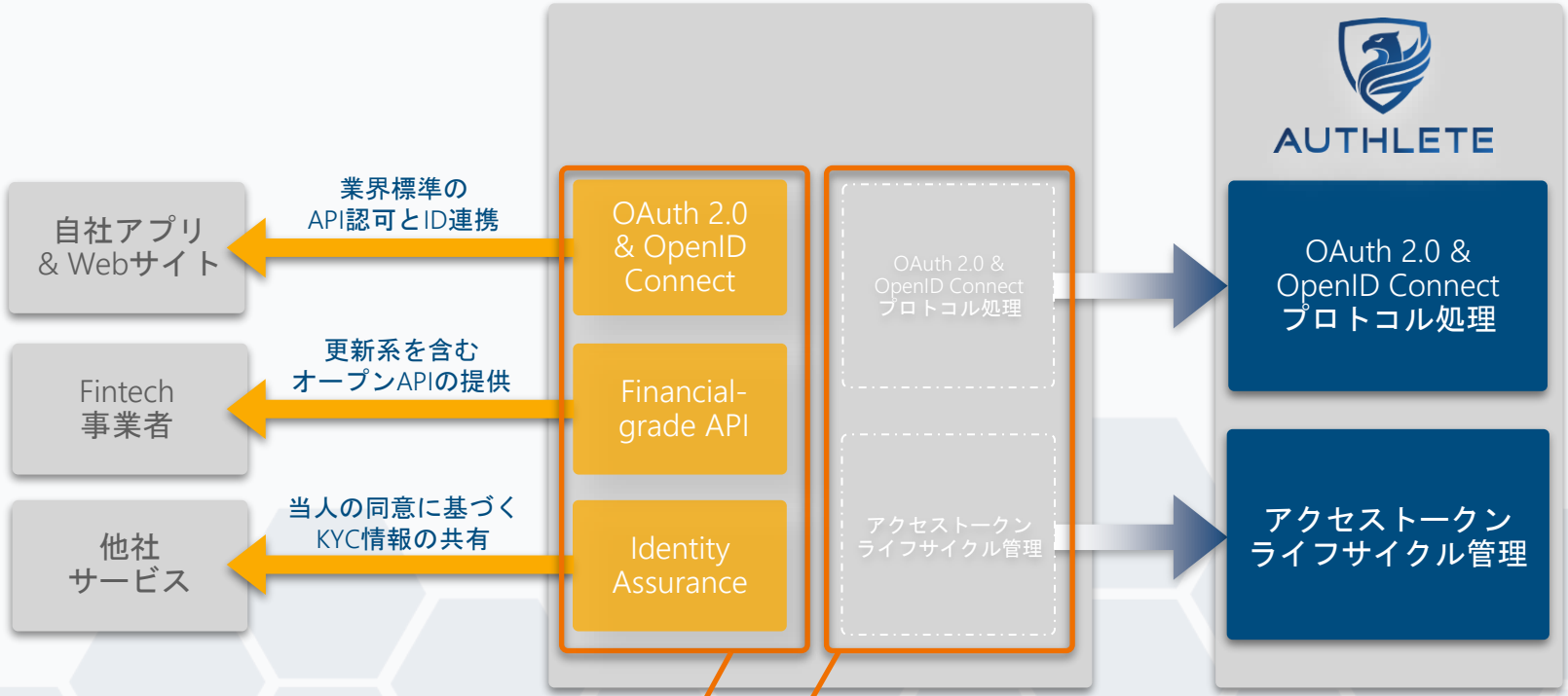


Source: Open Banking UK https://standards.openbanking.org.uk/customer-experience-guidelines/authentication-methods/decoupled/model-b-aspsp-generated-identifier/latest/

AUTHLETE

Authlete活用事例

Authlete: FAPI/CIBA準拠の「認可エンジン」



最先端の業界標準仕様に準拠したセキュアなAPI提供を実現

OAuth 2.0 & OpenID Connect に関する複雑な実装・運用を外部化
特定ソリューションに依存せず自由にUX設計が可能

金融サービスを中心に多数の採用実績

金融

SEVEN BANK
Minna no Ginko
SBI DigiTrust
楽天銀行
OneBanks
justincase
LINE Bank *1
Nubank
cora
TOYOTA FINANCE
btg pactual

システム・インテグレーション

NRI SECURE
TOPPAN
UNISYS
TIS
TIS INTEC Group
iSiD
DXC TECHNOLOGY
CTC
Challenging Tomorrow's Changes
Briscola

メディア

radiko
DPG Media
ALIS

EC

ヨドバシカメラ
www.yodobashi.com
asoview!
HOKKAIDO NIPPONHAM FIGHTERS

B2B / B2E

SmartHR
DIS
ダイフクウ情報システム株式会社

パーソナルデータ / 本人確認

MY DATA INTELLIGENCE
TRUSTDOCK

ヘルスケア

MTI Ltd.

教育

駿台 SUNDAI

IoT

NTT Docomo

音声合成

coestation

Awards

FIBC Financial Innovation Business Conference 2017
DRAPER NEXUS B2B Summit
NTT DATA OPEN INNOVATION 2020 TOKYO WINNER

*1 LINE Bank設立準備株式会社

Authlete が選ばれる理由

- ソフトウェア**内製化**との親和性
- **組込可能**な「OAuth / OIDC エンジン」
- 「**OpenID認定**」を業界最速・最多取得

In-house
Development

OAuth/OIDC
Engine

Security &
Compliance

銀行APIにおけるAuthlete導入パターン

Adapt

- 既存のインターネットバンキングサービスにAPI認可基盤を追加
  - セブン銀行・楽天銀行
  - 日本ユニシス (Resonatex)・SBIデジトラスト (Trust Idiom)

Build

- スクラッチから構築するデジタルバンキング基盤のコアにAPI認可機能を具備
  - みんなの銀行・LINE Bank*
  - Nubank・BTG Pactual

Evolve

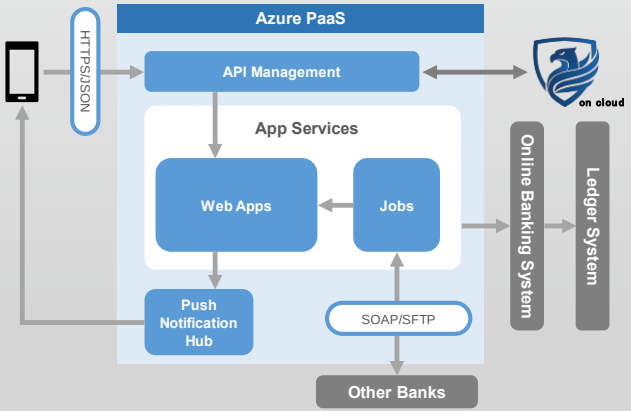
- 参照系API基盤の老朽化を契機とし、更新系APIに耐えうる基盤への刷新
  - (TBA)

* LINE Bank設立準備株式会社

セブン銀行

- AuthleteによりPaaSのAPI認可機能を置き換え3カ月で構築
- オンラインバンキングの既存認証システムをそのまま活用
- FAPI等の新しい仕様にも将来的に対応可能

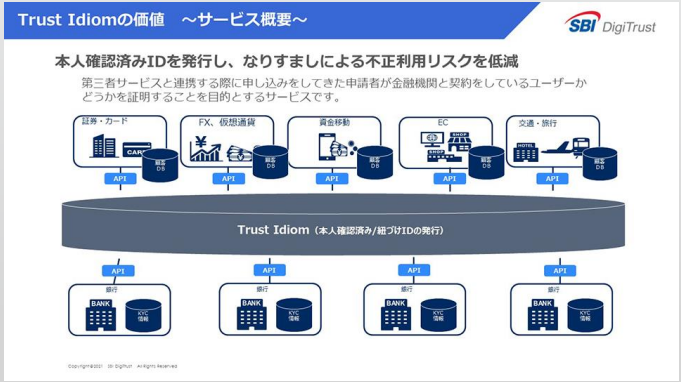
自社アプリ＆Fintech企業向け銀行API基盤を短期間に構築



SBI デジトラスト “Trust Idiom”

- 本人確認済みIDを発行する認証認可基盤サービス
- API認可基盤にAuthleteを採用しFAPI/CIBAを実装
- 高いセキュリティと優れた利便性をスピーディに実現

FAPIとCIBAに準拠した本人確認済みID発行 & 多要素認証基盤

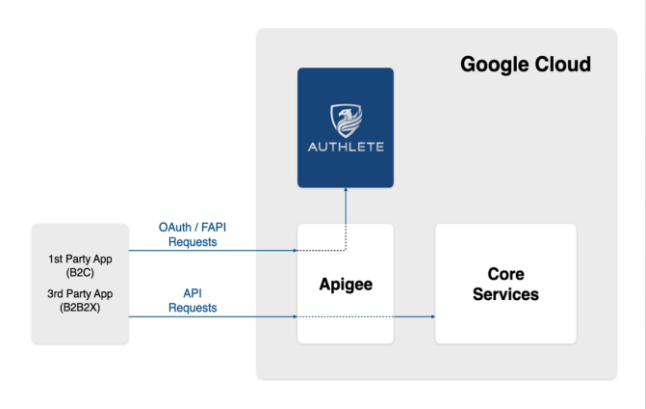


Source: NEC
https://wisdom.nec.com/ja/feature/digitalfinance/2021121001/index.html

みんなの銀行

- Google Cloud との親和性の高さからAuthleteを採用
- Authleteのマネージドサービスを利用し運用負荷低減
- OAuth/FAPIの進化に適応可能な基盤構築を迅速に実現

モバイル向けAPI認可基盤を構築。FAPI準拠のオープンAPIへ拡張予定



AUTHLETE

まとめ

まとめ

- 銀行APIの機能拡充とチャネル拡大に資する “FAPI” と “CIBA”
  - FAPI: 金融機関のセキュリティ対策に費やすコストの削減
  - CIBA: これまで銀行APIが適用できなかった領域へユースケースを拡大
- AuthleteがFAPI/CIBA対応を実現
  - Adapt, Build, Evolve の各段階をサポート

導入事例を順次公開中 https://www.authlete.com/ja/customers/

AUTHLETE

Thank You

Tatsuo Kudo
www.linkedin.com/in/tatsuokudo