デジタルバンキングに向けたAPIおよび認証・認可サービスの提供

Provision of APIs and Authentication and Authorization Services for Digital Banking

附木　孝二　　安原　正晃

あらまし

金融業界では，FinanceとTechnologyを組み合わせたFintech（フィンテック）と呼ばれる，ICTベンチャー企業を中心としたデジタル化の波が押し寄せている。銀行もこれをチャンスとして捉え，保有する機能やデータを基に自身で魅力的なサービスを作り出して顧客に直接提供するだけでなく，Fintech事業者や異業種企業のサービスとの連携を進めている。富士通では，Finplex サービス統合基盤FrontSHIP，およびそのオプションであるバンキングAPI（Application Programming Interface）認証・認可サービスを提供している。これによって，既存のインターネットバンキングの代替ではなく，ネットチャネルを全顧客・全取引レベルに開放する基盤として活用していただくことが可能となる。更に，軽量化，デジタル化が求められる伝統的な銀行の次世代店舗を支える基盤として，お客様のビジネス発展と内部効率化に寄与することを目指している。

本稿では，Fintechの黎明期からAPIが広まっていく流れ，それに対する富士通の取り組み，および今後のデジタルバンキングでますます重要となる認証・認可の対応について述べる。

Abstract

In the financial industry, digitization is surging, led by ICT ventures in Fintech (financial technology). Banks are taking this as an opportunity and working on linking with Fintech businesses and services from other industries in addition to creating attractive services for customers on their own based on the functions and data they possess. Fujitsu provides Finplex Service Integration Platform FrontSHIP together with optional features including banking application programming interfaces (APIs) and authentication and authorization services. This provides a platform that can be utilized for opening Internet channels to all customers and all transactions, not as an alternative to existing Internet banking. In addition, we intend to have this solution contribute to business development and internal efficiency improvement for customers as a platform that supports next-generation offices for traditional banks, which demands lightweight features and digitization. This paper describes how APIs have expanded since the early days of Fintech, our approach to enhancing these APIs, and how we will deal with authentication and authorization, which will see increasing importance in future digital banking.

1. まえがき

近年，金融業界ではFinanceとTechnologyを組み合わせたFintech（フィンテック）と呼ばれる，デジタル化の波が押し寄せている。このFintechという造語に，明確な定義はない。海外のICTベンチャー企業を中心として，伝統的な銀行にはない金融サービスを提供する動きが活発化している。これに対して，銀行もそれらの企業と連携して，顧客向けに価値の高いサービスを提供しようとしている。Fintechという言葉は，その状況を指している言葉と理解しても良いし，インターネットを中心としたテクノロジーと金融を組み合わせたサービス自体を表す言葉と理解しても良い。

Fintechによって，伝統的な銀行はどのような影響を受けるのであろうか。突然現れた競合企業に，市場を奪われるかもしれない。あるいは，Fintechを利用して収益を増やすチャンスかもしれない。いずれにせよ，超低金利や少子高齢化といった環境においては，テクノロジーをうまく活用することが必須である。こうした状況の中で顧客に魅力的なサービスを提供するためには，銀行が既に持っている機能やデータを銀行自身のみで活用するのでなく，Fintech事業者や異業種企業のサービスにも活用してもらうことが重要となっている。そのための重要な技術が，API（Application Programming Interface）である。

富士通では，銀行のデジタル革新を実現するFinplex サービス統合基盤FrontSHIPを提供している。更に，そのオプションとしてバンキングAPIおよび認証・認可サービスを提供している。それらを活用することで，銀行自身の新たなチャネルの創出や，Fintech事業者から銀行の既存システムとの連携が容易になり，新しい利用者接点が生み出される。また，金融サービスと異業種のサービスをマッシュアップさせる共創や，先進技術を活用した新たなサービスの創出も可能である。加えて，銀行のリアルチャネルとデジタルチャネルを容易につなぐこともできる。利用者は，銀行の窓口に出向かずに，スマートデバイス上のみで口座開設，入出金明細の照会，ローン申し込みなどを完結できる。このように，場所や時間を気にすることのない銀行サービスを提供することで，顧客満足度の向上につながる。

本稿では，銀行をとりまくAPIの状況，富士通の取り組み，今後ますます重要になる認証・認可に関連するサービスの提供について述べる。

2. APIについての前提知識

本章では，富士通の取り組みを紹介する上で必要となる知識として，APIの概要，課題，およびオープンAPI化について説明する。

2.1 APIとは

一般的にAPIとは，あるアプリケーションの機能や管理するデータなどを，ほかのアプリケーションから呼び出して利用するための接続仕様を指す。APIは大きく，クローズドAPIとオープンAPIに分類できる。クローズドAPIは，自社外に公開・提供しないAPIを意味する。一方，オープンAPIはサードパーティ（外部企業など）からアクセスできるように公開されたAPIを意味する。

Fintechの世界では，オープンAPIを介して銀行が持つ業務機能やデータにアクセスさせることで，ベンチャー企業がこれまでにない魅力的なサービスを作り出している。そのため，APIと言うとオープンAPIが注目されがちである。しかし，クローズドAPIであっても，API化することで自社サービスの開発を加速し，顧客に新たな価値を提供できる。また，オープンAPI化に向けた第一歩と考えると，クローズドAPIから整備していくことも一つの戦略である。

2.2 Fintech黎明期における課題

Fintechの黎明期には，Fintech事業者が利用者の口座残高情報などの銀行データを利用して付加価値を付けたサービスを提供したいというニーズがあった。しかし，そのデータを取得するインターフェースは，銀行から公開・提供されてはいなかった。そのため，Fintech事業者が提供するスマートフォンアプリで口座残高や入出金明細情報を表示するには，スクレイピングという手法が用いられていた（図-1）。この手法では，Fintech事業者が利用者

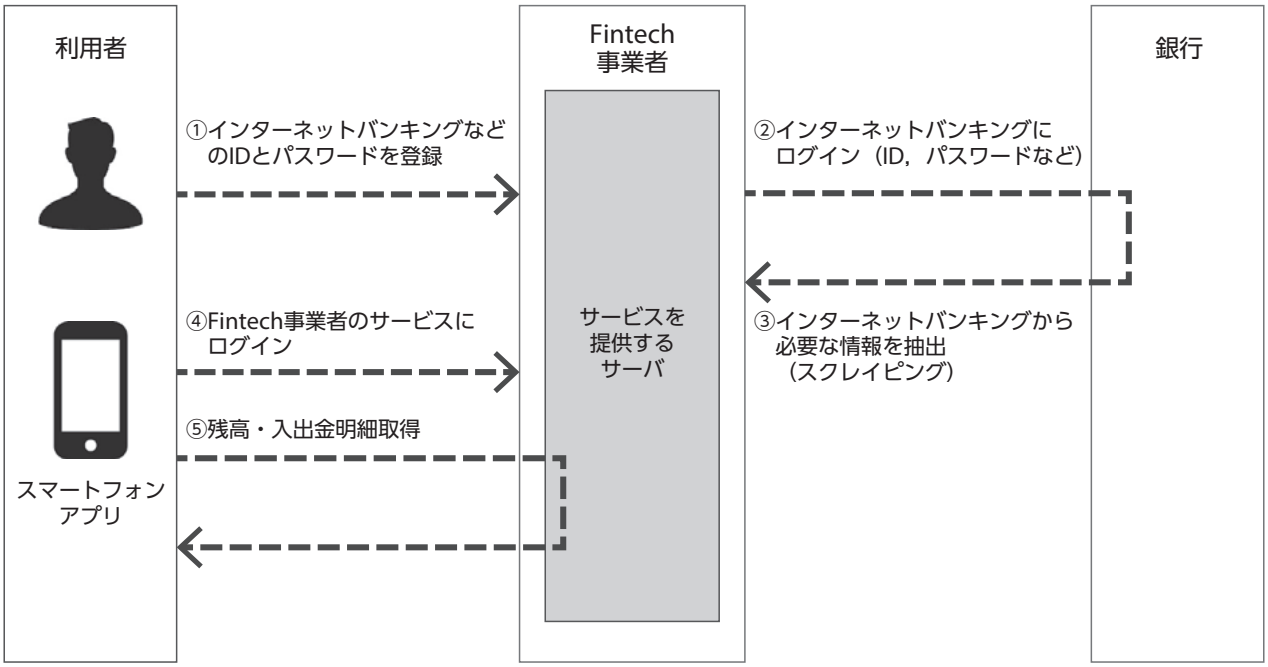

図-1　スクレイピングの処理例

の同意を得た上で，IDとパスワードを使ってインターネットバンキングに直接ログインし，情報を取得していた。つまり，Fintech事業者にインターネットバンキング用のIDとパスワードを預けなければならなかった。これは，セキュリティの面で利用者と銀行の双方にとって大きな問題であった。

また，スクレイピングを使う場合，インターネットバンキングの画面構成が変更される度に，Fintech事業者もデータ取得プログラムを変更する必要がある。Fintech事業者に対して，銀行は画面変更を事前に連絡しないため，Fintech事業者が変更に気付くまでデータが取得できなくなる。これは，Fintech事業者が提供するサービスの品質として問題となるだけでなく，システムの保守コストの面でも問題であった。[1]

2.3 オープンAPI化の加速

前節で述べた問題によって，Fintech事業者が提供する便利なサービスが急に使えなくなることは，利用者にとっても不満の種であった。そこで，IDとパスワードをFintech事業者に預けることなく，銀行のデータにアクセスさせるオープンAPIの仕組みが注目されはじめた（図-2）。

銀行業界でオープンAPI化を加速するためには，法律の整備による後押しも必要であった。日本においては，オープンバンキングを推進するために，金融庁が2017年に銀行に対してオープンAPI導入に係る努力義務を課している。これによって，2018年6月1日の施行から2年以内にオープンAPI導入に係る体制整備の努力が義務化された。2017年12月に全国銀行協会が実施した調査によると，回答した137行中14行が既にオープンAPI対応を実施しており，100行が2020年6月までにオープンAPIを提供する方向で検討していると回答した。[2]

3. FrontSHIPで提供するバンキングAPI

前章で述べた市場動向に対応するために，銀行は自身が持つデータへアクセスするAPIの仕組みの提供，およびオープンAPIに向けた法制度への対応が急務となった。その課題を解決するために，富士通ではバンキングAPIを含むFinplex サービス統合基盤FrontSHIP（図-3）を2017年5月から提供している。これは，銀行が保有するデータをAPI連携して自社サービスやFintech事業者で活用することで，利用者に新たな価値を創出するための基盤である。

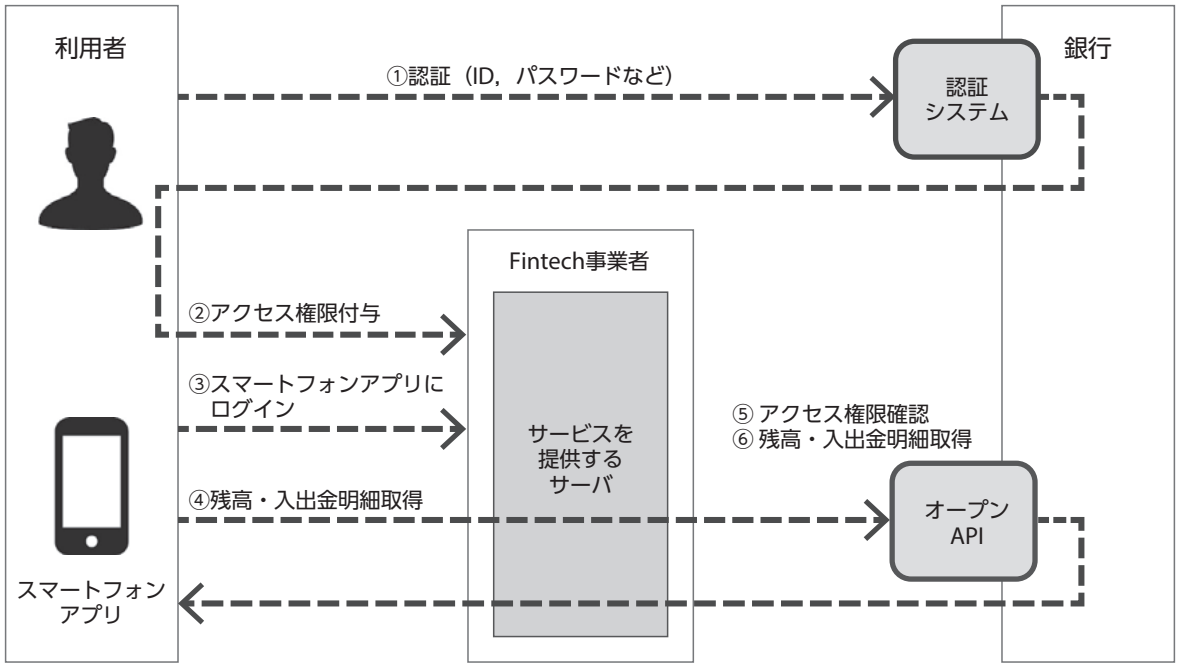

図-2　オープンAPIでの処理例

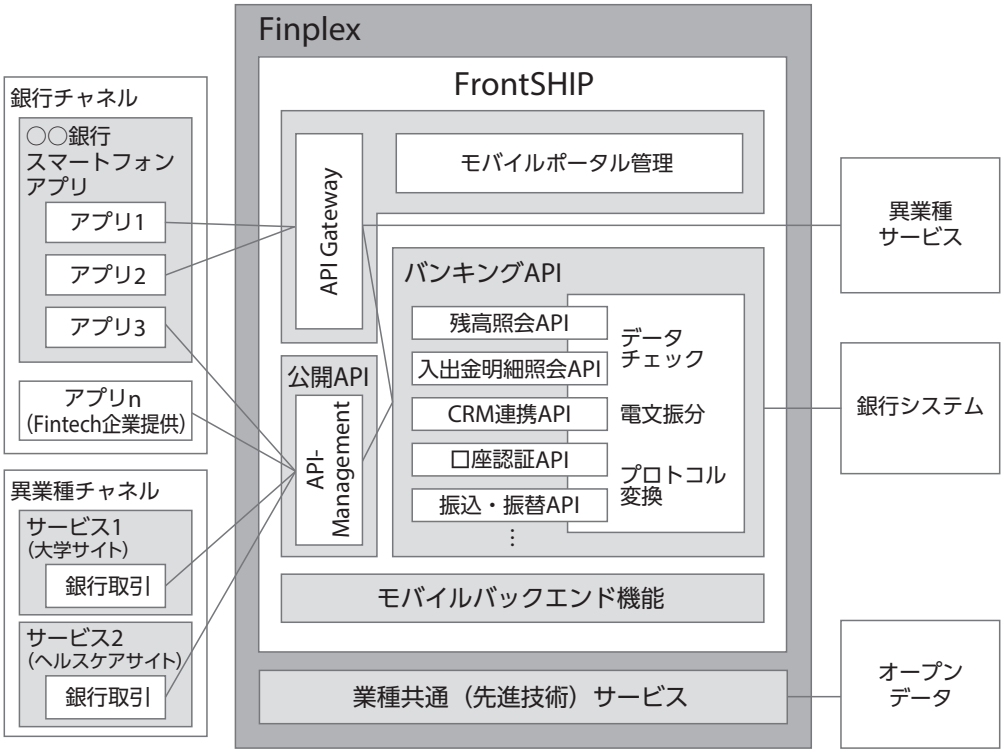

図-3　FrontSHIPの概要

現時点でFrontSHIPでは認証API，残高照会API，入出金明細照会API，CRM（顧客情報）連携APIなど，主に参照系のAPIを提供している。振替・振込APIなどの更新系のAPIも提供準備中である。今後も，既存銀行サービスを上回るサービスを可能とするAPIラインナップを準備していく。

FrontSHIPで提供するバンキングAPIについて，三つのポイントを紹介する。

(1) オープンAPIへの対応

前述したとおり，APIエコノミーにおいては銀行だけがサービスを提供するのではなく，Fintech事業者との連携が不可欠である。FrontSHIPでは，OAuth2.0プロトコルを介してFintech事業者が銀行の機能やデータを利用できる仕組みを提供している。

(2) APIインターフェースの共通化

例えば，残高照会や入出金明細照会のインターフェースと言っても，複数の口座の情報をまとめて取得するかどうか，明細を一度に取得するかどうかなど，銀行によって入出力項目が異なる場合がある。銀行やFintech事業者のサービスを早期に立ち上げるためには，同じAPIを共通的に利用でき，どの銀行でも使える標準インターフェースが必要である。

そこで，標準インターフェース策定において参考にしたシステムの一つが，富士通の営業店システムである。これは，文字どおり銀行の営業店で利用するシステムとして，銀行のバックシステムと接続してお客様の情報にアクセスするインターフェースを備えており，多くの銀行に採用されている。これに加えて，これまで富士通が長年にわたって銀行システムを構築してきたノウハウも取り入れることで，インターフェースを決定した。また，全国銀行協会でも銀行分野のオープンAPIに係る電文仕様標準について検討しており，指針となる電文仕様標準が公開されている。[(3)] 入出力仕様の共通化という観点でこの標準を継続してウォッチしており，インターフェースの改善に努めている。

(3) 従来の銀行システムと同等のセキュリティの確保

スマートフォンアプリからのアクセスにおいては，REST（Representational State Transfer）インターフェースでセキュアに銀行システムへアクセスさせることが重要である。セキュリティの確保においては，XSS（Cross Site Scripting）やSQLインジェクションをはじめとする，パラメーター操作に関するツールを利用した脆弱性対応だけでなく，ユーザー認証方式やアカウント管理ルールなど，ツールでカバーできない脆弱性も確認し，対策が施されている。運用面においても，金融情報システムセンター（FISC）の安全対策基準をクリアしている。

バンキングAPIを含むFrontSHIPを最初に採用したお客様の利用形態は，クローズドAPIであった。銀行がスマートフォンアプリを開発・提供し，そのスマートフォンアプリからAPIを呼び出すことで，手軽に口座残高や入出金明細を照会するサービスに活用されている。また，顧客情報（CRM）システムのデータにアクセスして，顧客ごとに最適な金融商品を推奨するCRM連携APIを利用しているお客様は，One-to-Oneのマーケティングに活用している。これも，クローズドAPIとしての活用例である。

従来，新しいサービスを提供したい場合であっても，Webアプリケーションとしてクライアント，サーバの双方の開発が必要であり，開発工数が大規模になりがちであった。しかし，APIを通じて既存の機能やデータを活用することができれば，スマートフォンアプリ側で魅力的なサービスを作り上げることが可能となる。オープンAPI，クローズドAPIにかかわらず，新しいサービスを創出しやすくなるということは，API化の大きなメリットと言える。

4. 認証・認可サービスの高度化の取り組み

銀行のAPIを外部から利用させるためには，認証（Authentication）と認可（Authorization）の仕組みが重要である。認証と認可はまとめて扱われることが多いが，定義は大きく異なる。認証とは，通信している相手が誰であるかを確認することである。一方認可とは，ある特定の条件に対してリソースへのアクセス権限を与えることである。

本章では，認証および認可の高度化に関する取り組みについて述べる。

4.1 認可

金融APIに対する認可の標準仕様については，国際標準化団体であるOpenID Foundationの作業部会の一つであるFinancial-grade API（FAPI）ワーキング・グループにおいて，策定作業が進められて

いる。参照系APIを使わせるための認可の仕組みとして，OAuth2.0を採用している銀行は多い。一方，OIDC（Open ID Connect）はOAuth2.0と互換性を保ちつつユーザー認証情報も送受信する仕組みである。これは，OAuth2.0と比較してセキュリティレベルを高く保つことができるため，更新系APIを使わせるための認可の仕組みとして使われている。これらの認可の仕組みは，主にオープンAPIに使われるが，考え方自体はクローズドAPIにも適用できる。

FrontSHIPでは，主に参照系取引を想定しているOAuth2.0に準拠したAPI基盤を提供している。更新系取引についても2019年度中に，FAPIの実装者向け仕様のドラフトにある「Part 2: Read & Write API Security Profile」に準拠した認可の仕組みに対応する予定である。FAPIの仕様は，銀行をはじめとした金融機関向けに高いセキュリティ要件を実現させるための認証・認可の技術仕様であり，「Part 2: Read & Write API Security Profile」では更新系APIのセキュリティを規定している。

4.2 認証

前述した認可の仕組みは，プロトコルとして標準的な手順が議論・策定されている。その手順の中には認証処理も登場するが，その手順や仕組みは明確に規定されてはいない。これは，ほとんどの既存システムは認証の仕組みを持っており，新たに認可の仕組みを取り入れる場合であっても，認証は既存の仕組みを使うことを考慮しているためと考えられる。

現在では，参照系取引においても2要素以上の多要素認証が必要と考えられている。その場合，例えばIDおよびパスワードなどの記憶情報に加えて，OTP（One Time Password）などの所有情報を採用することで多要素認証とし，セキュリティ強度を高めることができる。昨今，顔認証をはじめとした生体認証の利用も進んでいる。例えば，生体認証方式の一つであるFIDO（Fast Identity Online）を利用する場合，顔情報（生体情報），デバイス情報（所有情報）を組み合わせた多要素認証として使うことができる。FIDOのような認証方式は，セキュリティを強化しつつ，認証をスムーズにするために有効である。

FrontSHIPが提供するバンキングAPIでは，既存の銀行システムが持つ認証データを用いて認証するためのAPIを提供している。富士通ではそのほかの認証の仕組みとして，FUJITSU Cloud Service for OSSにおいてID，パスワード，OTPを含む認証サービス，Finplex オンライン認証サービス for FIDOにおいてFIDO認証を提供している。様々な認証を組み合わせてセキュリティを向上させたいお客様にとっては，個々のサービスを組み合わせる手間は大きい。FrontSHIPでは，富士通が持つこれらの認証の仕組みを互いにセキュアに連携させることで，銀行ホスト認証，ID・パスワード・OTP認証，およびFIDO認証を組み合わせた認証サービスを，2019年度中に提供予定である。

5. FrontSHIPが目指す未来

技術の進展を考えると，この先も認証方式が多様化することは容易に想像できる。例えば，海外では心拍の情報を基に認証するサービスを提供するベンダーが現れている。[4] また，日本における法制度の観点からは，犯罪収益移転防止法施行規則が2020年4月に改正される予定である。[5] これによって，オンラインで完結する本人確認方法の導入が進んでいくことが見込まれる。

今後の認証・認可で重要なことは，インターネット経由で確実な認証・認可ができることである。近年，利用者がある端末を用いて取引する中で利用者が保有する別のデバイスで認証させる方式（Decoupledフロー）や，サービス提供者が開始した処理の中で利用者に認証させるCIBA（Client Initiated Backchannel Authentication）という方式も話題となっている。[6] これは，実際にサービスの利用シーンで必要な方式と判断されているからに外ならない。

ここまで，銀行の口座保有者向けのサービスへのAPIと認証・認可サービスの導入について述べてきたが，そのほかのシーンにも応用が可能である。例えば，営業店取引機能をAPI化して，認証・認可サービスを使ってアクセスすることで，営業店の事務を改革することも可能である。具体的には，営業店窓

口に来店されたお客様の本人確認や，取引における押印の代替とするために，お客様のスマートフォンで生体認証を行うような利用シーンも考えられる。また，ある取引を担当者が処理する過程で上司の承認を得るといった，銀行内の事務処理にも活用できる。その際，上司のスマートフォンで生体認証を行うことによって，間違いなく上司が承認したことを証明することも可能である。更には，上司が事務所から外出している場合であっても，スマートフォンで承認可能となる。

このように，APIや認証・認可サービスが適用できる利用シーンは幅広い。FrontSHIPは，銀行において喫緊の課題である営業店端末の軽量化，ロケーションフリー化においても，有効な基盤となる。

6. むすび

本稿では，Fintech黎明期のAPIの課題，富士通が提供するAPI提供基盤，および今後ますます重要となる認証・認可サービスについて述べた。

Fintechという話題の中では，顧客サービス向けのオープンなAPIのみが語られる傾向にある。しかし，APIと認証・認可をうまく組み合わせることで，内部利用のためのクローズドAPIも十分にその価値を発揮できる。富士通は今後も，FrontSHIPにおいて多様な認証・認可に対応しつつ，APIのラインナップを拡充していく。これによって，既存のインターネットバンキングの代替ではないネットチャネルを，全顧客・全取引レベルに開放する基盤として活用していただくとともに，軽量化・デジタル化が求められる伝統的銀行の次世代店舗を支える基盤として，お客様のビジネス発展，内部効率化に寄与することを目指す。

参考文献

(1) 金融審議会：金融制度ワーキング・グループ報告.
https://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1/01.pdf

(2) 全国銀行協会：決済高度化に向けた全銀協の取組状況について.
https://www.fsa.go.jp/singi/kessai_kanmin/siryou/20171220/01.pdf

(3) 全国銀行協会：銀行分野のオープンAPIに係る電文仕様標準について 第2版.
https://www.zenginkyo.or.jp/fileadmin/res/news/news301227_3.pdf

(4) REUTERS：MasterCard, RBC to test if the heart is always true, for payments at least.
https://www.reuters.com/article/mastercard-rbc-bionym/mastercard-rbc-to-test-if-the-heart-is-always-true-for-payments-at-least-idUSL1N0ST11K20141103

(5) 金融庁：「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について.
https://www.fsa.go.jp/news/30/sonota/20181130/20181130.html

(6) Qiita：2019年版 世界最先端の認証認可技術、実装者による『CIBA』解説.
https://qiita.com/TakahikoKawasaki/items/9b9616b999d4ce959ba3

著者紹介

附木　孝二（つけぎ　こうじ）
富士通（株）
第一システム事業本部
デジタルビジネス事業部
金融APIおよび認証サービスの開発に従事。

安原　正晃（やすはら　まさあき）
富士通（株）
第一システム事業本部
デジタルビジネス事業部
金融APIおよび認証サービスの開発に従事。