IMES DISCUSSION PAPER SERIES

金融分野のTPPsとAPIのオープン化：
セキュリティ上の留意点

中村（なかむら） 啓佑（けいすけ）

Discussion Paper No. 2016-J-14

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
http://www.imes.boj.or.jp

IMES Discussion Paper Series 2016-J-14
2016 年 10 月

金融分野のTPPsとAPIのオープン化：セキュリティ上の留意点

中村（なかむら） 啓佑（けいすけ）*

要　　旨

近年のモバイル端末の普及に伴い、情報技術を活用した従来にない金融サービス（FinTech と呼ばれる）が利用できるようになってきた。顧客のモバイル端末にインストールされた専用のアプリケーション・ソフトウェアを使って、顧客が取引する複数の金融機関からデータを取得し、それらを集計・加工して当該顧客に提供するサービス（口座情報サービス）はその一例である。こうしたサービスを提供する主体は TPPs（Third Party Providers）と呼ばれ、各国金融当局では金融機関の API（Application Programming Interface）のオープン化を念頭においた検討を進めているほか、一部の金融機関では、TPPs の取込みに向けて、自社の API を既にオープン化している。TPPs が介在すると、金融機関が保有する顧客の取引データに、TPPs もアクセスする。また、金融機関においては、API のオープン化に伴い、新たな通信路を設けることになる。TPPs および金融機関は、新たなセキュリティ上のリスクを想定し、その対応策に関して検討する必要が生ずる。本稿では、TPPs のサービスが実現される複数のシステム形態を概説し、金融機関の API のオープン化や、その標準化に関する最近の議論を解説する。そのうえで、API を介してサービスを実施するシステムの基本的なモデルを想定し、そのリスクやセキュリティ対策について考察する。

キーワード： インターネット・バンキング、セキュリティ、モバイル端末、API、FinTech、TPPs
JEL classification: L86、L96、Z00

* 日本銀行金融研究所企画役補佐（E-mail: keisuke.nakamura@boj.or.jp）

本稿の作成に当たっては、慶應義塾大学特任准教授の杉本理氏から有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに 1
２．　TPPs サービスとデータ送受信方式 3
（１）TPPs サービスの形態 3
（２）アクセス方式と認証方式 4
イ．アクセス方式と認証方式の組合せ 4
ロ．アクセス方式 5
ハ．認証方式 7
３．金融機関における API のオープン化と標準化 10
（１）API のオープン化 10
（２）API のオープン化に関する標準化 11
４．金融機関の API を活用したサービスのリスクと対策 12
（１）想定するモデル 12
（２）セキュリティ上の脅威とリスク 13
イ．主な脅威 13
ロ．主なリスク 13
（３）主な対策と留意点 16
イ．金融機関における対策 16
ロ．通信路上における対策 19
ハ．TPPs における対策 19
ニ．利用者における対策 20
（４）リスク対策を実施するうえでの金融機関と TPPs の役割 21
５．おわりに 22
【参考文献】 23
補論．TPPs が複数の金融機関のアクセス・トークンを保存する運用の例 26

１．はじめに

近年、スマートフォンやタブレットといったモバイル端末を使って、さまざまな金融サービスが提供されるようになった。これら FinTech[1]と総称されるサービスでは、利用者が、専用のアプリケーション・ソフトウェア（以下、「専用アプリ」という）をインターネット経由でモバイル端末にインストールしたうえで、サービスを利用するケースが多い（日本銀行金融研究所［2013］）。例えば、口座情報サービス（Account Information Service）を使うと、利用者は、（複数の）金融機関における自分の口座残高等のデータを集計し、確認することができる。決済指図伝達サービス（Payment Initiation Service）を使うと、決済指図を金融機関に伝達し、その結果を確認することができる。このように、専用アプリを提供して利用者や金融機関とネットワーク経由で通信を行い、口座情報サービス等を提供する主体は、「TPPs（Third Party Providers）」と呼ばれる（European Commission [2015]）。TPPs は、利便性の高いサービスを利用者に提供するのみならず、特に欧州ではリテール金融サービス分野における金融機関間の競争促進に資するものとして注目を集めている。

また、各国金融当局の間でも、TPPs の新規参入やそれを通じた TPPs 間の競争を促進することを企図して、金融機関が保有しているデータへのアクセスや、金融機関に対する送金等の決済指図を行うための API（Application Programming Interface）をオープン化する（外部の組織に開示する）という方向で、現在、活発に議論が行われている。一般に、API とは、特定のプログラムを別のプログラムによって動作させるための技術仕様を指し、当該プログラムを動作させる際に用いる命令文（コマンドや関数）、送受信するデータの形式等を定めるものである。例えば、商店等が所在地をウェブサイトで公開する際、グーグル・マップで地図を表示させることが多いが、これは、グーグル社の API（Google Maps API）を用いて地図データ（Google Maps）を出力させることにより実現している。

European Banking Association Working Group on Electronic Alternative Payments [2016]によると、API のオープン化の形態は大きく以下の 4 つに分類できる。①個別に契約した相手に対して提供するもの（パートナーAPI）、②規範性を有する一定の取決めへの遵守が求められるコミュニティに属するメンバーに対して提供するもの（メンバーAPI）、③ある一定の資格を満たした相手に対して提供

[1] FinTech とは、金融（Finance）と技術（Technology）を掛け合わせた造語であり、主に、情報技術を活用した革新的な金融サービス事業を指す。特に、近年は、海外を中心に、ベンチャー企業が情報技術を活かして、伝統的な金融機関が提供していないサービスを提供する動きが活発化している（金融審議会［2015］）。

するもの（アクウェインタンス API）、④Google Maps API のように誰にでも提供するもの（パブリック API[2]）。TPPs が API を介して金融機関と通信できるようになれば、金融機関のウェブサイトを介した従来の方法に比べ、より効率的に金融機関のデータへアクセスすることが可能になる。

欧州連合（European Union：EU）では、2015 年 11 月に閣僚理事会で採択された第 2 次決済サービス指令（Payment Services Directive 2：PSD2）[3]において、EU 加盟国により認可を受けた口座情報サービス提供者（Account Information Service Providers）および決済指図伝達サービス提供者（Payment Initiation Service Providers）が金融機関の API（メンバーAPI を想定[4]）を利用できるよう、加盟各国は 2018 年 1 月までに国内法制化を行わなければならないとした。わが国でも、全国銀行協会から、API のオープン化のあり方を検討すべく作業部会等を設置し、2016 年度中を目途に報告を取り纏めることが表明されている（金融審議会［2015］）。2016 年 7 月に設置された金融審議会の「金融制度ワーキング・グループ」でも、口座情報サービス提供者等の「中間的業者」にかかる環境整備が、論点として挙げられている（金融庁［2016］）。

金融機関が API を TPPs に開示することは、金融機関の情報システムに新しい通信路が設けられることを意味し、当該通信路を悪用したデータの漏洩・改ざんや不正取引等、新たなリスクが生じる。また、利用者の口座情報や決済指図にかかるデータが、TPPs を経由して、漏洩・改ざん等のリスクにさらされる可能性もある。API を介したサービスを安心安全に実現するうえで、どのようなリスクが想定されるかを洗い出すとともに、各リスクへの対応策を検討することが早急に求められている。

本稿では、TPPs や金融機関の API のオープン化に関する最新の動向を踏まえ、留意すべきリスクやセキュリティ上の対策について考察する。以下、2 節では、TPPs のサービス（以下、「TPPs サービス」という）を実現するシステムの形態について、金融機関と TPPs 間の通信および金融機関の API に焦点を当てて説明する。3 節では、金融機関の API のオープン化を巡る議論の動向について説明する。4 節では、金融機関のメンバーAPI とパブリック API を想定し、TPPs サービスにかかるリスクやセキュリティ対策について考察する。

---

[2] パブリック API は、Google API、Facebook API、LinkedIn API、Salesforce API 等が該当する。

[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EU, OJ L 337, 23.12.2015, pp. 35-127.

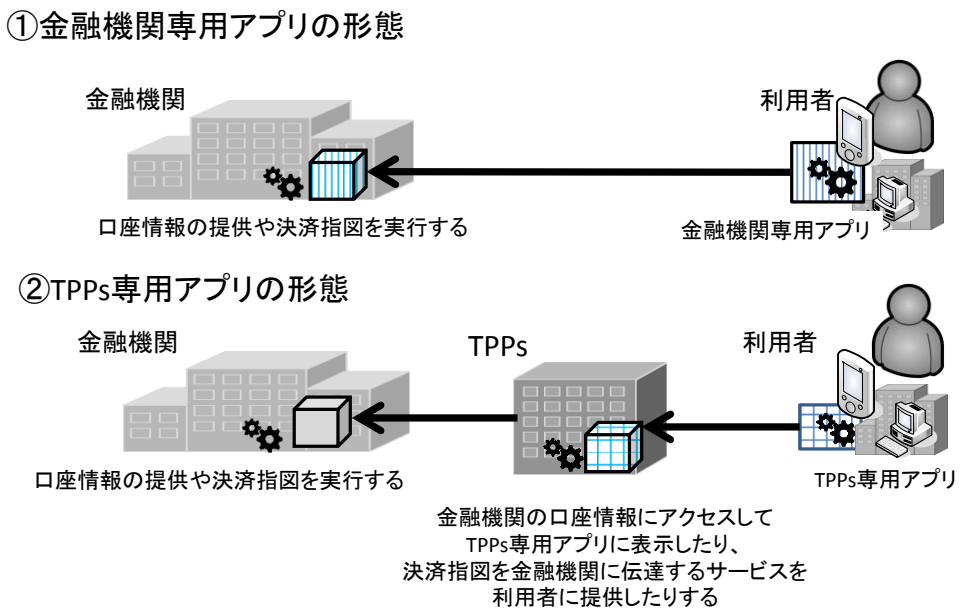
[4] European Banking Association Working Group on Electronic Alternative Payments [2016] p.8.

２． TPPs サービスとデータ送受信方式

（１） TPPs サービスの形態

いま利用者が、TPPs の専用アプリ（以下、「TPPs 専用アプリ」という）を通じて、口座情報サービスや決済指図伝達サービスを利用するケースを想定しよう。この場合の TPPs、利用者、金融機関の関係は、典型的には図表 1 のようになる。図表 1①は、金融機関が専用アプリを提供する従来からの形態を示したもので、利用者は金融機関の専用アプリ（以下、「金融機関専用アプリ」という）を用いて、インターネット経由で金融機関にアクセスし、金融機関との間で直接データを送受信する。一方、図表 1②は、TPPs が TPPs 専用アプリを提供する形態を示したもので、利用者が TPPs 専用アプリを用いて、インターネット経由で TPPs にアクセスすると、その後は TPPs と金融機関との間でデータの送受信が行われる。このとき、TPPs 専用アプリは、金融機関から受信したデータについて、必要に応じて集計等の処理を行う。

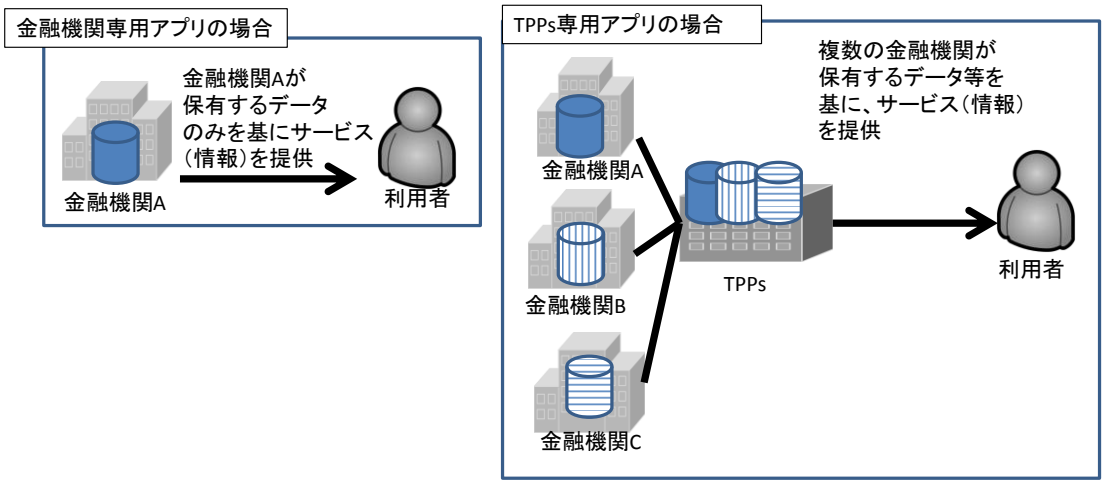
図表 1　TPPs・利用者・金融機関の関係（概念図）



図表 2 は、口座情報サービスを例に、金融機関専用アプリと TPPs 専用アプリとの差異を説明したものである。金融機関専用アプリは、当該金融機関が保有する口座残高や取引履歴等のデータしか提供しない。利用者が自分の預金残高や入出金の流れの全体を把握するためには、各金融機関専用アプリをモバイル端末にインストールした後、個々の金融機関から口座残高等のデータを別々に取得し、資産全体の管理に必要なデータを自ら生成する必要がある。一方、TPPs

の中には、複数の金融機関から口座残高等のデータを収集し、集計する機能を備えた TPPs 専用アプリを提供しているものがある。こうした複数の口座残高等のデータを集約するサービスは口座情報サービス、あるいは「アカウント・アグリゲーション」と呼ばれ、スマートフォンの普及に伴い、近年特に脚光を浴びている[5]。

図表 2　金融機関専用アプリと TPPs 専用アプリとの差異
（口座情報サービスの例）



（２） アクセス方式と認証方式

イ．アクセス方式と認証方式の組合せ

口座情報サービスでは、TPPs 専用アプリがネットワーク経由で金融機関にアクセスする方法として、主に 2 つの方式が使われている。1 つはウェブ・スクレイピング（「スクリーン・スクレイピング」とも呼ばれる）を用いた方式（以下、「ウェブ・スクレイピング方式」という）であり、もう 1 つは金融機関が公開する API を用いてアクセスする方式（以下、「API 方式」という）である[6]。一方、

---

[5] 口座情報サービスの世界最大手であるイントゥイット（Intuit）社が米国およびカナダで提供するサービス「mint.com」は、利用者数が 2,000 万人以上となっている（Prince [2016]）。また、わが国の最大手であるマネーフォワード社が提供するサービス「マネーフォワード」は、利用者数（レシートを利用した家計簿サービスのみの利用者も含む）が 350 万人に達している（マネーフォワード［2016］）。

[6] ここでは、金融機関と TPPs との間の通信に着目して分析する。なお、TPPs 専用アプリと TPPs との間の通信においても API が利用される場合があり、その場合、金融機関ではなく TPPs 等が API の開発・提供主体となる。ウェブにかかる技術仕様の標準化を進める W3C（World Wide Web Consortium）においては、TPPs が TPPs 専用アプリと通信する際に用いられる API（Payment Request API）の標準化を進めており、2016 年 4 月にファースト・ドラフトが公表された（W3C [2016a]）。こうした標準化が実現されれば、TPPs が作成する TPPs 専用アプリの送受信部分のプログラムを効率的に開発できるようになる。また、W3C において、FIDO（Fast IDentity Online）2.0（FIDO Alliance [2016]）を基とした認証にかかる API（Web Authentication API）の標準化も進

決済指図伝達サービスの場合は、API 方式により TPPs 専用アプリがネットワーク経由で金融機関に決済指図を伝達する方法が主流となっている。金融機関が利用者を認証する方式はアクセス方式に応じてほぼ決まっている。ウェブ・スクレイピング方式でアクセスする場合はレガシー認証、API 方式でアクセスする場合は OpenID Connect 等によるトークンを用いた認証（以下、「トークン認証」という）が主に利用されている（図表 3 を参照）。以下、これらのアクセス方式と認証方式について、それぞれの特徴を整理していく。

図表 3　金融機関へのアクセス方式と利用者の認証方式

TPPs サービス	アクセス方式	認証方式
口座情報サービス	ウェブ・スクレイピング方式	レガシー認証
	API 方式	トークン認証
決済指図伝達サービス	API 方式	トークン認証

ロ．アクセス方式

ウェブ・スクレイピング方式（図表 4①を参照）とは、利用者が TPPs 専用アプリを用いて、金融機関のウェブサイトにアクセスし、口座情報サービスに必要なデータを当該ウェブサイトから取得するもので、現在、広く利用されている（有吉ほか［2016］）。

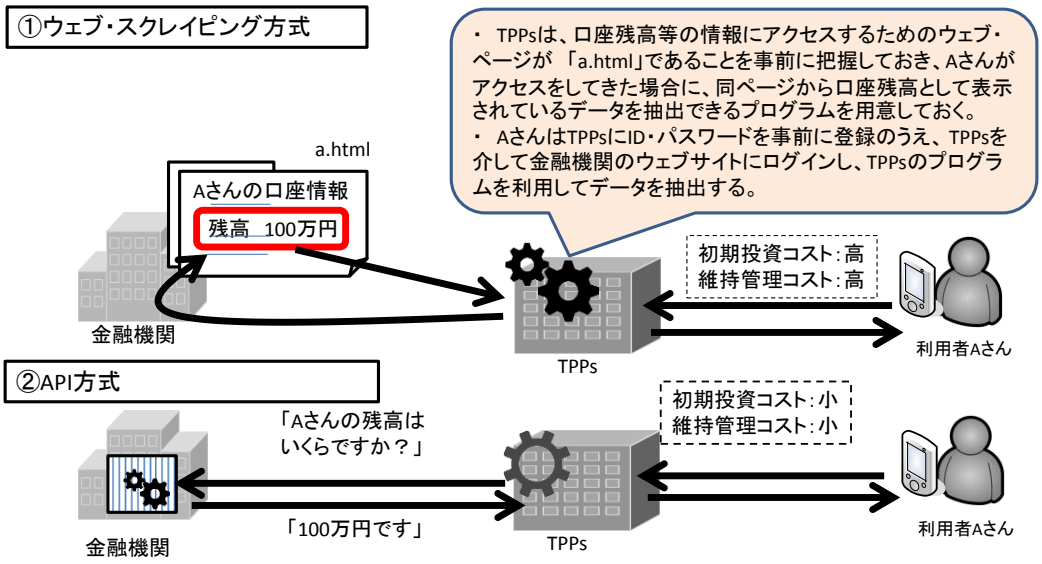
これに対し、API 方式（図表 4②を参照）とは、利用者が TPPs 専用アプリを用いて、金融機関がオープン化した API に命令文を送信することによって、金融機関の情報システムからデータを取得したり、当該システムに決済指図等に基づく処理を実行させたりするものである[7]。

これらの方式を比較すると、主に以下の 4 点において差異がみられる（日経 BP 社［2016a, b］、日本 IBM［2016］、European Banking Association Working Group on Electronic Alternative Payments [2016]、Open Data Institute [2016]）。

められており、2016 年 5 月にファースト・ドラフトが公表された（W3C [2016b]）。TPPs 専用アプリを作成する際は、これらが参考になると考えられる。

[7] 口座情報サービスや決済指図伝達サービス以外に、API を活用することによって、以下のサービスも可能となる（European Banking Association Working Group on Electronic Alternative Payments [2016]）。すなわち、TPPs は、①利用者が取引先の金融機関を変更した際、旧金融機関から新金融機関に必要な情報を TPPs 専用アプリを介して引き継ぐサービスや、②複数の金融機関が保有する利用者の口座情報や取引情報等を基に、利用者の信用格付けを行うサービスを提供可能になるほか、金融機関は、③利用者に新規の金融商品にかかる情宣を効率的に行うサービスを提供することが可能になる。開示される API の標準化が進めば、④そうした API を通じた金融機関間での情報共有が促進され、詐欺やマネーロンダリング等への対策の高度化にもつながると期待されている。

図表 4　ウェブ・スクレイピング方式と API 方式（口座情報サービスの例）



（イ）金融機関における対応負担

TPPs がウェブ・スクレイピング方式を用いる場合、金融機関は追加的な対応が不要である。一方、API 方式では、金融機関は API を介した外部からのアクセスを可能とするように情報システムを更改する必要がある。

（ロ）TPPs における対応負担

ウェブ・スクレイピング方式では、TPPs は、金融機関のウェブサイトのページを探索し、必要なデータを抽出するプログラム等を金融機関ごとに開発する必要がある。また、TPPs は、金融機関のウェブサイトの URL やページ・レイアウトが変更される都度、当該プログラム等を変更しなければならない[8]。一方、API 方式では、TPPs は、金融機関ごとに異なる API に対応できるよう、情報システムや専用アプリの開発が必要となる場合がある。ただし、その後、API が変更されない限り、当該プログラムの更新にかかる負担は限定的となる。一般に、API の変更頻度は、ウェブサイトの URL 等の変更頻度より低いと想定されるため、対応負担は、API 方式の方がウェブ・スクレイピング方式よりも軽いといえる。

[8] 例えば、ウェブサイト上の表示方法が変更となり、「マイナス 1,000 円」が「▲1,000 円」と記載されるようになった場合、「▲」の記号を「マイナス」と解釈するようにプログラムが更新されるまでの間「1,000 円」とみなされるという事象が発生しうる。こうした問題を回避するために、ウェブサイトの変更の有無の確認や迅速なプログラム更新等が必要となる。

（ハ）取得可能なデータ

ウェブ・スクレイピング方式では、利用者が TPPs 専用アプリを介して取得可能なデータは、金融機関のウェブサイト上で提供されるものに限定される。一方、API 方式では、提供対象とするデータをウェブサイト内に限定する必要がない。このため、ウェブサイト上で提供されていないデータについても、利用者は TPPs 専用アプリを介して取得することができる。この場合、金融機関が API を介して提供することを認めたデータのうち、当該データが帰属する利用者の同意が得られたものが取得可能となる。

（ニ）データの通信負荷

ウェブ・スクレイピング方式では、利用者が TPPs 専用アプリを使用する都度、金融機関のウェブサイト上の関連するページをすべて読み込む必要がある。当然、サービスの提供に必要のないデータも含まれており、TPPs と金融機関との間で、必要以上のデータ通信が行われることとなる。一方、API 方式では、サービスの提供に必要なデータのみを金融機関から入手することが可能であるため、TPPs と金融機関との間のデータ通信の負荷が軽くなる。

ハ．認証方式

（イ）レガシー認証

レガシー認証とは、利用者が金融機関のサービスを利用する際に必要となる本人確認用の ID・パスワードを TPPs に事前に登録しておき、それを用いて金融機関にアクセスするというものである。この場合、利用者の ID・パスワードを管理することに伴う負担が TPPs に発生する。

また、TPPs の内部者の一部による不正行為やマルウェア感染等により、TPPs から ID・パスワードが外部に流出する可能性がある点に注意が必要である。レガシー認証単体では、TPPs による金融機関へのアクセスの範囲を制御することは困難であり、利用者が意図していないデータを、TPPs が金融機関から不正に取得する可能性もある。

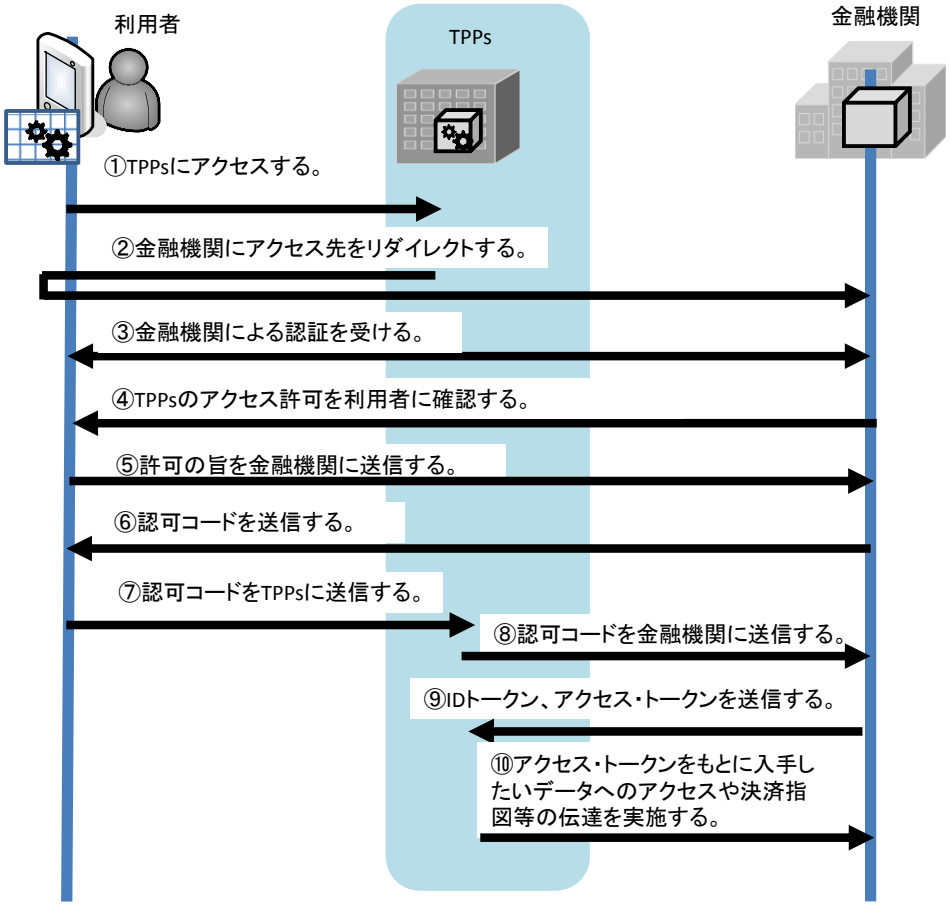
このほか、利用者は、金融機関に登録しているパスワードを変更する場合、TPPs に登録しているパスワードも同様に変更する必要がある。利用者が、金融機関に登録しているパスワードを変更したものの、TPPs に登録しているパスワードの変更を失念した場合、TPPs は金融機関にアクセスできなくなる。

（ロ）トークン認証

トークン認証とは、金融機関が利用者を認証した後、TPPs に対してアクセスするデータの範囲や利用可能なサービスの内容を示すデータ（トークン）を

生成して TPPs に送信し、それを用いて TPPs と金融機関との間でデータの送受信を行うものである。こうした認証を実現する主要なプロトコルとして、OpenID Connect が注目されている[9]。OpenID Connect を用いたトークン認証の基本的な手順は、以下のとおりである[10]（図表 5 参照）。

図表 5　トークン認証の概念図（OpenID Connect の場合）



[9] OpenID Connect は、認可（authorization）を行うプロトコルである OAuth2.0 の機能を拡張し、更に認証（authentication）を付加したプロトコルである（OpenID Foundation Japan [2014]）。ここで、認証は、アクセスを要求してきたエンティティが本人（利用者）であることを確認することであり、認可は、認証において確認されたエンティティ（利用者）が、TPPs に、金融機関が保有している利用者のデータにアクセスするなどの権限を付与することである。OpenID Connect において、認証手段は仕様の対象外であるため、例えば、次世代の認証技術として注目されている FIDO を認証手段として利用することも可能とされている（倉林［2015］）。OpenID Connect と同様、認可と認証の機能を有するプロトコルとして SAML（Security Assertion Markup Language）が存在する（OASIS [2012]）。OpenID Connect では、ウェブサイト間の信頼関係に関係なく ID 連携を実現できるのに対し、SAML では、相互に信頼関係を結んだウェブサイト間でのみ ID 連携が可能となる（総務省情報通信政策研究所［2010］）。

[10] OpenID Connect の代表的なフローである「Authorization Code Flow」を用いた場合を想定する（OpenID Foundation Japan [2014]）。

① 利用者は、TPPs 専用アプリを介して TPPs にアクセスする。
② TPPs は、利用者のアクセス先を金融機関にリダイレクトする（自動的に誘導する）。
③ 利用者は、金融機関にアクセスし、金融機関による認証（ID・パスワード等）を受ける。
④ 金融機関は、TPPs が要求するデータ（口座情報等）へのアクセスや決済指図の伝達を当該 TPPs に許可するか否か、利用者に確認する。
⑤ 利用者は、上記④の確認に対して、許可する旨を金融機関に送信する。
⑥ 金融機関は、利用者に「認可コード」[11]を送信する。
⑦ 利用者は、上記⑥で取得した認可コードを TPPs に送信する。
⑧ TPPs は上記⑦で取得した認可コードを金融機関に送信する。
⑨ 金融機関は、TPPs に「ID トークン」と「アクセス・トークン」[12]を送信する。
⑩ TPPs は、アクセス・トークンをもとに、入手したいデータへのアクセスや決済指図の伝達を実施する。

トークン認証は、レガシー認証と比べると、実装するための情報システム更改等の負担が金融機関側に生じるものの、利用者にとっては、TPPs への ID・パスワードの登録が不要になるうえに、TPPs がアクセス可能なデータの範囲を制御することが可能になるというメリットがある。なお、口座情報サービスの場合、利用者の利便性向上を目的として、複数の金融機関のアクセス・トークンを TPPs に一定期間保有させておく方式も存在する（遠藤・高橋［2016］）。この方式を用いると、TPPs 専用アプリを起動すると同時に、利用者は TPPs に保有している複数のアクセス・トークンを用いて、複数の金融機関に迅速にアクセスすることが可能となる（補論を参照）。

11 認可コードは、TPPs による金融機関へのアクセス等を当該金融機関が承認した証として、利用者に対して提供されるデータである。
12 ID トークンは､利用者の認証が正当に完了したことを示すデータであり､認証を行った時刻、トークンの有効期限等のさまざまなパラメータを含む。アクセス・トークンは、金融機関が保持している利用者情報（口座情報等）のうち、TPPs がアクセスを許可されたデータ等（「UserInfo Endpoint」と呼ばれる）を特定するデータである。OpenID Connect におけるアクセス・トークンの仕様には、OAuth2.0 が採用されている（OpenID Foundation Japan [2014]）。OAuth2.0 は Google API や Facebook API 等の多くのパブリック API で用いられている（Siriwardena [2014]）。

３．金融機関における API のオープン化と標準化

（１）API のオープン化

API のオープン化は、TPPs の新規参入を促す。特に、新興の金融機関にとっては、API のオープン化が新規顧客獲得の機会となる可能性がある。また、TPPs 間の競争を高めることを通じて、金融サービスの品質向上を促す。API のオープン化は、ドイツのフィドール・バンク（Fidor Bank）等、一部の金融機関において、既に実施されている（図表 6 を参照）。今後、欧州を中心に、API のオープン化の動きは加速していくものと予想される。

図表 6　API を公開している主な金融機関

銀行名	国	公開されている API
フィドール・バンク（Fidor Bank）[13]	独	残高照会、利用者情報照会、アカウント情報照会、送金等（Fidor Bank [2016a])
ビルバオ・ビスカヤ・アルヘンタリア・バンク（Banco Bilbao Vizcaya Argentaria）	西	残高照会、利用者情報照会、アカウント情報照会等（Banco Bilbao Vizcaya Argentaria [2016])
クレディ・アグリコル・バンク（Crédit Agricole Corporate and Investment Bank）	仏	残高照会、利用者情報照会、アカウント情報照会等（Crédit Agricole Corporate and Investment Bank [2013])
サバデル・バンク（Banco de Sabadell）	西	残高照会等（Banco de Sabadell [2016])

これに対し、EU の動向をうかがうと、2015 年 11 月、FinTech 企業等の新規参入やモバイル／オンライン決済サービスの発展の促進等を意図した PSD2 が、閣僚理事会において採択された。PSD2 では、取扱いデータを安全に管理するなど、一定の要件を満たす口座情報サービス提供業者および決済指図伝達サービス提供業者が各国当局の認可を得た場合、金融機関との間の契約関係によらず、それらのサービスを提供できるようにすることを求めている。また、欧州銀行監督機構（European Banking Authority）では、こうしたサービスを提供する際に必要なセキュリティ要件（通信データの機密性の確保や利用者等の認証）について、標準化へ向けた作業を進めている[14]（European Banking Authority [2016]）。な

[13] フィドール・バンクは 2016 年 9 月末時点で、API により提供する送金サービスの被仕向銀行を単一ユーロ決済圏（Single Euro Payments Area：SEPA）内に所在する銀行に限定しているが、同行では、今後 SEPA 外の銀行にも被仕向銀行を拡大するとしている（Fidor Bank [2016b]）。

[14] 欧州銀行監督機構は、PSD2 が目標としている 2018 年 1 月の EU 加盟各国における国内法制化が適切に行われるよう、金融機関、TPPs、利用者等の間で実施する安全な認証や通信等の技術仕様等にかかる市中協議を 2016 年 8 月 12 日から 10 月 12 日にかけて実施した（European Banking Authority [2016]）。

お、PSD2 では、オープン化する API の形態としてメンバーAPI を想定しており、2018 年度以降、EU 加盟各国の金融機関がメンバーAPI の提供を開始する見込みとなっている。

（２） API のオープン化に関する標準化

API のオープン化に関する標準化も活発化しつつある。標準化の対象としては、エンティティの範囲、関数やコマンド、データの形式、セキュリティ対策、運用方法等、さまざまな事項が想定される。標準化が進めば、複数の金融機関が同一のコマンドや関数等に基づいて API を開発・公開することが可能となり、金融機関は API の開発負担を軽減させることも可能である。TPPs 側でも、API に対応したプログラムの開発負担を大きく軽減できる。さらに、そうした開発負担の軽減は、TPPs の新規参入のハードルを押し下げ、TPPs 間の競争を促進する効果も期待される。

API に関して何を標準化するかについては、セキュリティの観点から留意が必要である。例えば、API を構成するプログラムを金融機関間で共有した場合、当該 API に脆弱性が発見されると、その影響が数多くの金融機関に及ぶ可能性がある。こうした点を踏まえると、標準化の対象は、データ記述言語やアーキテクチャ・スタイル、関数名やリターン値等に限定し、個別のプログラムについては、各金融機関が独自に作成、管理する方が望ましいと考えられる。

英国では、2015 年 9 月、金融分野における API のオープン化のあり方や課題等にかかる検討を深化させるために、ワーキング・グループ（The Open Banking Working Group）が設置された。このワーキング・グループは、金融機関、FinTech 企業、消費者団体等から構成され、2016 年 2 月には、検討結果を纏めた報告書（The Open Banking Standard）を公表している（Open Data Institute [2016]）。当該報告書は、標準化の対象とすべき事項を網羅的に整理しているほか、TPPs による新サービスの開発を効率的に行うためには、開発用のコード[15]やドキュメントを公開したり、サンドボックス環境[16]を提供したりすることが重要であるとしている。こうした取組みの背景には、EU 加盟国による PSD2 の実施に先んじて API

---

15 Open Data Institute [2016]では、金融機関が提供する API の構造に REST（REpresentational State Transfer）を採用するとともに、テキスト形式で記述されたデータ交換用フォーマットとして JSON（JavaScript Object Notation）を採用することが推奨されている。REST 以外に、API で採用される構造としては、W3C において標準化された SOAP（Simple Object Access Protocol）が挙げられるが（山本［2015］）、現在、オープン化されている主な API においては、REST が利用されている（Musser [2010]）。また、API において用いられるデータ記述形式として、主に JSON と XML が挙げられる。JSON は、XML と比べて構造化されたデータを簡潔に記述することが可能であり、人間にも理解しやすい（山本［2015］）。

16 サンドボックス環境とは、通常の情報システムを模した仮想の環境であり、通常の情報システムと隔離され、アプリケーションを開発する際の動作環境等として用いられる。

のオープン化を推進することにより、英国の金融機関や TPPs の競争力を強化したいという英国の狙いがある（Open Data Institute [2016]）。

ドイツでは、「Open Bank Project」という組織が、国内の銀行に対して金融サービスに活用できる API の雛形を提供している。既に、複数の銀行が当該 API の利用について検討を実施しているとみられる（Open Bank Project [2010, 2016]）。

また、金融サービスにかかる国際標準化を担当する ISO/TC68 においても、検討が開始された。セキュリティ分科委員会（SC2）とコア銀行業務分科委員会（SC7）のそれぞれの傘下に、TPPs にかかるスタディ・グループが設置されたほか、現在設置が検討されている分科委員会（Information Exchange Sub-Committee）においても、API の標準化が、検討項目の一候補として挙げられている（日本銀行金融研究所［2016］）。

４．金融機関の API を活用したサービスのリスクと対策

本節では、最初に、メンバーAPI またはパブリック API（以下、纏めて「オープン API」という）を前提に、口座情報および決済指図伝達のサービスを実施するための基本的なシステムのモデルを想定する[17]。そのうえで、脅威やリスク、それらに対する対応策やリスク管理上の留意点を考察する。

（１）想定するモデル

ここでは、API のオープン化にかかるリスクやセキュリティ上の対応策を検討するために、金融機関、TPPs、利用者から構成されるモデルを想定する。これらの主体は、インターネットを経由して接続されており、金融機関と利用者は、トークン認証によって、口座情報サービスに必要なデータ（口座残高、取引履歴等）へのアクセスや決済指図の伝達を TPPs に対して認めているとする。各エンティティの役割を改めて示すと、金融機関は、利用者に対して金融サービスを提供し、当該利用者の金融取引にかかるデータ（口座残高、取引履歴等）を保有する。また、決済指図が伝達された際に決済処理を行う。TPPs に対してオープン API を開示し、TPPs サービスに必要な処理を実施するほか、当該処理にか

[17] API のオープン化の形態には、これらのほかにもパートナーAPI とアクウェインタンス API が存在する。パートナーAPI については、個別に TPPs と契約を締結してオープン化するものであり、（規範性を有する一定の取決めを遵守することを約した TPPs に API をオープン化する）メンバーAPI にかかる検討結果がパートナーAPI にも適用可能であることから、ここでは検討対象外とする。アクウェインタンス API については、パブリック API とメンバーAPI の中間的な形態であり、対象となる TPPs に課される一定の資格が比較的緩い場合はパブリック API、そうでない場合はメンバーAPI に近い形態となる。これらの場合をそれぞれパブリック API とメンバーAPI に置き換えることが可能であることから、検討対象外とする。

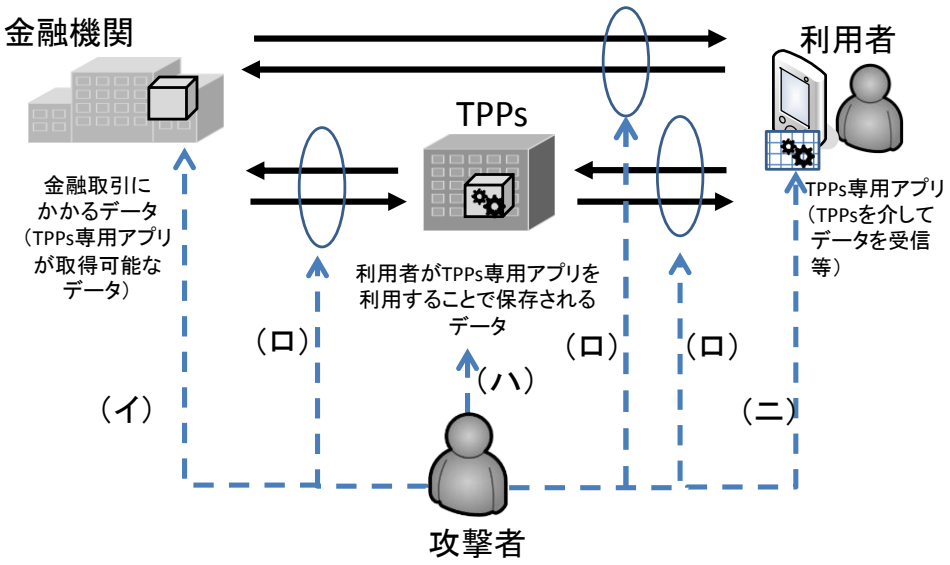
かるデータを TPPs に提供する。TPPs は、利用者からの要求に基づいて、オープン API を介して金融機関と通信した後、金融機関から受信したデータを必要に応じて加工して利用者に提供したり、金融機関に対して決済指図を伝達したりする。利用者は金融機関の顧客であり、TPPs 専用アプリをモバイル端末にインストールしたうえで、TPPs サービスを利用する[18]。

（２） セキュリティ上の脅威とリスク

イ．主な脅威

上記のモデルにおける攻撃者は、金融機関、TPPs、利用者以外のエンティティとするが、金融機関や TPPs の内部者の一部と結託する場合も想定する。主な脅威として、（イ）金融機関への攻撃、（ロ）各エンティティ間を接続する通信路上での攻撃、（ハ）TPPs への攻撃、（ニ）利用者のモバイル端末（TPPs 専用アプリ等を搭載）への攻撃の 4 つを想定する（図表 7 を参照）。

図表 7　主な脅威



ロ．主なリスク

ありうべき攻撃方法を具体的に検討しつつ、想定されるセキュリティ上のリスクを整理すると、以下のとおりである（図表 8 を参照）。

[18] TPPs 専用アプリのモバイル端末へのインストール等の準備は安全に完了しているものとする。また、TPPs 専用アプリについて、TPPs 専用アプリが本来取得するデータ以外のデータにはアクセスできない設定であることを、利用者が確認しているとする。

（イ）金融機関における主なリスク

a. データ流出・改ざんが想定されるケース

①ネットワーク機器等の脆弱性が悪用され、オープン API を介した通信路から金融機関の情報システムへの侵入をゆるし、当該システムのデータを流出させたり、改ざんしたりする。

②TPPs に保存していたトークン（補論を参照）が TPPs から漏洩し、それが悪用されてオープン API を介した通信路から金融機関の情報システムへの侵入をゆるし、当該システムのデータを流出させたり、改ざんしたりする。

b. 不正な金融取引の指図が想定されるケース

ネットワーク機器等の脆弱性が悪用され、オープン API を介した通信路から金融機関の情報システムへの侵入をゆるし、金融取引の指図が偽装され、当該指図に基づき、不正な金融取引が行われる。

c. サービス停止が想定されるケース

オープン API を介した通信路を通じて、金融機関の情報システムに対して DDoS（Distributed Denial-of-Service）攻撃が実行される。

上記 a. については、オープン API を介した通信路から侵入されて攻撃されるだけではなく、金融機関内でのマルウェア感染等によって攻撃が開始され、オープン API 等を介した通信路を経由して、データ流出が発生するケースも考えられる。また、上記 a. ～c. において、攻撃者が金融機関や TPPs の内部者の一部と結託し、TPPs から上記の各攻撃を試みるケースも想定されうる。

（ロ）通信路における主なリスク

各エンティティ間の通信路において、通信データが盗聴される、あるいは、改ざんされる（データ盗聴・改ざんのリスク）。

（ハ）TPPs における主なリスク

a. データ流出・改ざんが想定されるケース

ネットワーク機器等の脆弱性が悪用され、TPPs の情報システムへの侵入をゆるし、利用者に提供するデータ等を処理する情報システムが不正に操作され、当該システムのデータを流出させたり、改ざんしたりする[19]。

[19] TPPs がアクセス・トークンを保存しており、それらが流出するケース（本節（2）ロ.（イ）a.②のリスクにつながる）も含まれる。

図表 8　主な脅威とリスク

脅威	当該脅威にかかる主な攻撃方法	セキュリティ上の主なリスク
（イ） 金融機関（TPPs に提供するデータを処理する情報システム等）への攻撃 （金融機関や TPPs の内部者の一部と結託する場合を含む）	【オープン API を介した通信路からの侵入】 ・ネットワーク機器等の脆弱性を悪用して金融機関の情報システムに侵入。 【トークンを TPPs に保存するケース】 ・TPPs に保存していたトークンが悪意ある第三者（TPPs 内の内部者を含む）に漏洩し、トークンを悪用して侵入。 【オープン API を介した通信路以外からの侵入】 ・マルウェア（金融機関内部で感染）等により、オープン API またはそれと連携するために新しく構築された仕組みを介してデータ流出が発生。	・金融機関の情報システムで管理される（利用者の）金融取引にかかるデータが外部に流出する、あるいは、改ざんされるリスク ・金融取引の指図が偽装され、当該指図に基づき、不正な金融取引が行われるリスク
	・オープン API を介した通信路を通じて、DDoS（Distributed Denial-of-Service）攻撃を試行。	・TPPs に提供するデータを処理する情報システム等によるサービス提供が困難になるリスク
（ロ） 各エンティティ間の通信路上での攻撃	・当該通信路においてデータの盗聴や改ざんを試行。	・金融取引にかかるデータが通信路上で盗聴される、あるいは、改ざんされるリスク
（ハ） TPPs（利用者に提供するデータを処理する情報システム等）への攻撃 （金融機関や TPPs の内部者の一部と結託する場合を含む）。	・ネットワーク機器等の脆弱性を悪用して TPPs の情報システムに侵入。 ・マルウェア（TPPs 内部で感染）等により TPPs の情報システムを遠隔から操作。	・利用者に提供するデータを処理する情報システム等で管理される（利用者の）金融取引にかかるデータが外部に流出する、あるいは、改ざんされるリスク ・不正な金融取引の指図を金融機関に送信し、不正な金融取引が行われるリスク
	・DDoS 攻撃を試行。	・利用者に提供するデータを処理する情報システム等によるサービス提供が困難になるリスク
（ニ） 利用者のモバイル端末（TPPs 専用アプリ等）への攻撃 （TPPs の内部者の一部と結託する場合を含む）	・モバイル端末を盗取し、利用者へのなりすましを試行。 ・モバイル端末をマルウェアに感染させる。 ・TPPs 専用アプリの機能を改変（不正な TPPs 専用アプリの再配付等）。	・利用者の金融取引にかかるデータが外部に流出する、あるいは、改ざんされるリスク ・不正な金融取引の指図が行われる等のリスク

b. 不正な金融取引の指図が想定されるケース

TPPs の情報システムが不正に操作されて、不正な金融取引の指図が偽装され、その指図が金融機関に送信されて実行される。

c. サービス停止が想定されるケース

TPPs に対して DDoS 攻撃が試行される。

上記 a.、b. については、インターネット経由だけではなく、TPPs 内でのマルウェア感染等によって、攻撃が実行されるケースも考えられる。また、上記 a. ～c. において、攻撃者が、金融機関や TPPs の内部者の一部と結託し、上記の各攻撃を試みるケースも想定されうる。

（ニ）利用者における主なリスク

モバイル端末が不正に操作されるケースとして、①モバイル端末が盗取され、利用者へのなりすましを試行される、②モバイル端末がマルウェアに感染させられる、③TPPs 専用アプリが不正な TPPs 専用アプリの再配付等によって改変されるなどが想定される。これらが、データ流出・改ざんのリスク、および不正な金融取引の指図が行われるなどのリスクにつながる。攻撃者が、TPPs の内部者の一部と結託し、上記の各攻撃を試みるケースも想定されうる。

（３） 主な対策と留意点

ここでは、本節(2)に示したセキュリティ上の主なリスクへの基本的な対策を整理するとともに、留意すべき事項について考察する（図表 9 を参照）。

イ．金融機関における対策

（イ）データ流出・改ざんのリスクへの対策

オープン API を介して TPPs と通信する情報システムやネットワーク機器に関して、不正侵入の防止・検知、当該システムで処理されるデータの厳格な管理を実施する。主な対策の例としては、ネットワーク経由での不正侵入等に対して、①外部からのオープン API を介したアクセスに対する適切な認証の実施（OpenID Connect 等）、②ファイアウォール（レイヤー3 からレイヤー7 までを対象）、IPS（Intrusion Protection System）等の機器の適切な利用（パッチの適用、監視を含む）、③オープン API の脆弱性の有無を確認するテストの定期的な実施（脆弱性が発見された場合には、速やかに修正）が挙げられる。なお、攻撃者が、TPPs の内部者の一部だけでなく、金融機関の内部者の一部と結託する可能性にも配慮し、（金融機関内部における）TPPs に提供するデータを処理する情報システム等への厳格なアクセス制御の実施（2 名以上による特権管理、特権 ID の使用ログの監査等）についても留意することが重要である。

図表 9　主なリスクと対応策・留意点

リスク		主な対応策・留意点
所在	内容	
金融機関	データ流出・改ざん	・オープン API を介して TPPs と通信する情報システムやネットワーク機器に関して、不正侵入の防止・検知、当該システムで処理されるデータの厳格な管理を実施する。 ・TPPs にトークンを保存する場合、異常検知技術を採用するほか、トークンを速やかに失効する仕組みを構築する。 【留意点】具体的には、認証の実施、ファイアウォール等のネットワーク機器の利用、オープン API の脆弱性にかかる定期的な確認、（金融機関内部における）TPPs に提供するデータを処理する情報システム等へのアクセスの制御等が挙げられる。 ➢ メンバーAPI を提供する場合、金融機関と TPPs との間を VPN ネットワークで接続するという方法も考えられる。 トークンの失効は TPPs 経由で行う、または利用者が直接金融機関にアクセスして行うケースが考えられる。
	不正な金融取引の指図	・「データ流出・改ざんのリスク」への対応策と同様の対応策を実施する。 ・利用者の意思確認のための取引認証を実施する。 【留意点】取引認証を検討する際には、利用者の利便性に配慮しつつ、MitB（Man-in-the-Browser）攻撃等、高度な攻撃を想定することが重要であるほか、異常検知技術を活用することも考えられる。
	サービス停止	・オープン API を介した通信量を検討しつつ、DDoS 攻撃対策を実施する。 【留意点】当該通信量が、通常のインターネット・バンキングにおいて想定される通信量よりも大きい可能性がある。
通信路	盗聴・改ざん	・SSL/TLS 等を活用し、データの暗号化等を実施する。
TPPs	データ流出・改ざん	・金融機関の「データ流出・改ざんのリスク」への対応策と同様の対応策を講じる。 【留意点】TPPs は、複数の金融機関からデータを取得する場合があり、特定の利用者について金融機関よりも網羅性のある資産データを保有している可能性がある。また、TPPs が利用者のトークンを保存する場合、当該トークンを用いて当該利用者データにアクセス可能となることから、金融機関が実施している対応策と同程度以上の対応策が求められる可能性がある。
	不正な金融取引の指図	・TPPs を介して送金等のサービスの要求を処理する際には、利用者の当該取引の意思を確認するために、取引認証を実施する。 【留意点】取引認証を検討する際には、マルウェアによって TPPs 専用アプリが改変されるなどの状況も想定することが重要である。
	サービス停止	・利用者との間の通信量を検討しつつ、DDoS 攻撃対策を実施する。
利用者	データ流出・改ざん	・第三者に盗取されないよう、モバイル端末を適切に管理する。 ・モバイル端末および TPPs 専用アプリの起動時等の認証にかかる情報（パスワード、生体情報等）を適切に管理する。 ・モバイル端末の OS のパッチ適用等の通常の対応策に加え、TPPs 専用アプリのパッチ適用等を速やかに実施するほか、MitB 攻撃等の高度な攻撃に対して十分なセキュリティが確保されていることを TPPs に確認する。 【留意点】TPPs に確認すべき項目として、取引認証の機能・効果、TPPs 専用アプリの正当性の確認方法、マルウェア対策の方法・効果等が重要である。
	不正な金融取引の指図	

また、トークンを TPPs に保存する場合、トークンを盗取する攻撃を迅速に検知するために、異常検知技術[20]を導入し、不正と判断される通信を遮断するなどの対応を行うほか、トークンの漏洩が判明した際には、速やかにトークンを失効する仕組みを構築する。

（ロ）不正な金融取引の指図のリスクへの対策

TPPs からの要求に応じて処理を実行する情報システムへの不正なアクセス等を排除するために、「データ流出・改ざんのリスク」への対策と同様の対策を実施する。

また、オープン API を介して受けた送金等の金融取引の指図を処理する際には、利用者の当該取引にかかる意思を確認するために、取引認証を実施するほか、異常検知技術を導入して、不正な取引と判断されるものを検知・排除するなどの対応が考えられる。加えて、利用者に対して、取引認証の必要性を説明し、取引認証の確実な実施を促すことも重要である。なお、取引認証の方式を検討するにあたっては、MitB（Man-in-the-Browser）攻撃や偽のアプリによる攻撃[21]を想定するとともに、モバイル端末 1 台で実現できるなど、利用者にとって利便性が高い方式の採用を検討することが望ましい[22]。

（ハ）サービス停止のリスクへの対策

オープン API を介したデータの通信量を検討しつつ、DDoS 攻撃への対策を実施する。この点、現行のインターネット・バンキングでは、サービスの要求等は人間が開始・実行するという前提となっている。一方、オープン API を

---

20 異常検知技術は、データが従う規則的なパターンから逸脱した事象を効率的に検知し、それを活用する技術である。主な異常検知の手法としては、①多次元ベクトルを対象に、その確率モデルとして独立モデルを仮定し、相対的に特異なデータを検出する「外れ値検出」、②多次元時系列データを対象に、その確率モデルとして時系列モデルを仮定し、時系列上に現れる急激な変化を検出する「変化点検出」、③一連の行動データを単位とする系列を対象に、その確率モデルとして行動モデルを仮定し、相対的に異常な行動データを検出する「異常行動検出」がある（山西［2013］）。

21 MitB 攻撃は、マルウェアに感染した端末のブラウザを不正に操作し、ブラウザの表示内容やサーバとの通信内容を改ざんする攻撃の総称である。最近では、類似の攻撃として、偽のアプリケーション・ソフトウェアをインストールさせ、これを使って通信内容の盗聴や改ざんを行う攻撃（Man-in-the-App 攻撃）も知られている。

22 利用者の利便性に配慮した取引認証の実現に関して、今後の検討項目や留意点が井澤・五味［2016］において示されている。例えば、①利用者のスマートフォン内部に（マルウェアの影響を排除した）安全な実行環境を想定し、当該環境を活用した認証方式（FIDO 等）の利用を検討する、②安全な実行環境がどう実現されているかを製品レベルで確認する、③利用者と安全な実行環境との間で安全な通信路を実現する技術（Trusted User Interface 等）の動向に留意する、④異常検知技術を活用し、不審な取引を監視するとともに、必要に応じて金融機関に注意喚起する仕組みを検討するなどが挙げられている。

介したアクセスは、コンピュータによる自動かつ高負荷の処理となる可能性が高い。

また、ウェブ・スクレイピング方式と比較すると、個々の利用者がサービスを利用する際の通信量は抑制できるものの、TPPs 専用アプリが普及することに伴ってサービスの利用回数が増加し、全体としての高い負荷が発生するなかで DDoS 攻撃を受けることを想定し、従来のインターネット・バンキングにおける対応よりも高いレベルの対策の必要性に留意することが重要である。

なお、金融機関がメンバーAPI を提供している場合等は、本節(3)イ．（イ）～（ハ）の対策として、メンバーの TPPs 以外からのアクセスを、例えば VPN ネットワーク等を用いることによって遮断することが考えられる[23]。

ロ．通信路上における対策

金融機関と TPPs 間、TPPs と利用者間の通信路において、SSL（Secure Socket Layer）/TLS（Transport Layer Security）等を活用し、データの暗号化等を実施する[24]。

ハ．TPPs における対策

金融機関がメンバーAPI を提供している場合、TPPs がメンバーとして適切なセキュリティ管理等を実施していることを確認できる仕組みを構築することが必要である。なお、金融機関との間で VPN ネットワークを利用する場合においても、利用者との間のネットワークはインターネット回線を利用していることから、当該回線からの攻撃を防ぐため、以下の（イ）～（ハ）のすべての対策を行う必要がある。

（イ）データ流出・改ざんのリスクへの対策

利用者の要求に応じて処理を実行する情報システムへの侵入に対して、金融機関における「データ流出・改ざんのリスク」への対策と同様の対策を実施する[25]。

なお、TPPs は、複数の金融機関からデータを取得する場合があり、特定の

---

[23] VPN ネットワークは有料であるため、メンバー以外の先からの各種攻撃を防御するためのコストと VPN ネットワークを使用するコストを比較、検討する必要がある。

[24] 仮に VPN ネットワークを採用した場合にも、それを提供する通信会社への漏洩を防止するために、この対策は必要である。

[25] 技術的な観点では、高機能暗号の活用を検討することも有用であると考えられる。高機能暗号は、データを暗号化したままでデータを演算可能である（秘匿計算）など、高度な機能を備えた暗号の総称である（清藤・四方［2014］）。例えば、TPPs と金融機関との間でやり取りされるデータの暗号化を行う（TPPs は当該データを復号できない）と同時に、TPPs に対しては暗号化されたデータの演算のみを許可するというアイデアが挙げられる。

利用者について、金融機関よりも網羅性のある口座残高等の資産のデータを保有している可能性がある。また、利用者のトークンを TPPs 内に保存する場合[26]、当該トークンを用いると、利用者の資産をより網羅したデータにアクセス可能である。これらを踏まえると、TPPs には、金融機関が実施している対策と同程度以上のセキュリティ対策が求められる可能性がある。TPPs におけるセキュリティ管理が適切に実施されていることを、第三者による監査等によって定期的に確認するという対応も検討に値する。

（ロ）不正な金融取引の指図のリスクへの対策

利用者からの要求に応じて金融機関に金融取引の指図を伝達する際に、利用者の意思が正しく反映されていることを確認するための取引認証を実施するほか、異常検知技術[27]を導入し、不正な取引と判断されるものを検知・排除するなどの対応が考えられる。この点、今後、MitB 攻撃等の高度な攻撃に留意する必要があり、それらへの対策を検討することが考えられる[28]。例えば、利用者のモバイル端末にインストールされている TPPs 専用アプリがマルウェア等によって改変されたり、専用アプリの入出力が不正に変更されたりする状況を想定し、そうした状況を検知・回避可能な方式を検討することが求められる。

（ハ）サービス停止のリスクへの対策

金融機関と同様に、利用者との間で発生する通信量を検討しつつ、利用者からのアクセスを受け付けるために開放しているインターネット・ポートを通じて行われる DDoS 攻撃への対策を実施する。

ニ．利用者における対策

モバイル端末における「データ流出・改ざんのリスク」と「不正な金融取引等のリスク」に対しては、①第三者に盗取されることがないように、モバイル端末を管理する、②モバイル端末の起動時や TPPs 専用アプリの使用時に求められる認証にかかる情報（ID、パスワード、生体情報等）を適切に管理する、③モバイル端末の OS のパッチ適用やマルウェア対策ソフトの利用等、通常のモバイル端末におけるセキュリティ対策に加え、TPPs 専用アプリ等の脆弱性に対応

---

[26] 利用者のモバイル端末に格納されているデータと TPPs に格納されているデータの両方を組み合わせて初めてトークンを利用することができる仕組み（秘密分散技術等）を活用すれば、TPPs におけるデータの漏洩が発生した場合でも、モバイル端末が安全に管理されている限りは、トークンを利用させないことが可能となり、データ流出・改ざんのリスクを軽減できる。

[27] 脚注 20 で示した手法①～③のいずれも効果があると期待できる。それぞれが独立した検知モデルを形成しているため、並列して用いることで、より効果的な検知が可能となる。

[28] 金融機関における検討項目と同様に、異常検知技術等によって、不審な取引を監視・検知するとともに、必要に応じて利用者や金融機関に注意を喚起することも検討課題となろう。

したパッチが公開された場合には、当該パッチ適用を速やかに行うことが考えられる。また、これらに加え、例えば、MitB 攻撃等を想定した取引認証の実現方式とその効果、TPPs 専用アプリの信頼性（不正なアプリでないことの担保方法）、TPPs 専用アプリにおけるマルウェア対策の内容とその効果等、リスク軽減策の内容と効果を TPPs に確認することも重要である。

（４） リスク対策を実施するうえでの金融機関と TPPs の役割

本節(3)において示した対策を検討・実施していくうえで重要な留意点として、①TPPs におけるセキュリティ対策の適切な実施をどう担保するのか、②利用者へのセキュリティ対策の啓発をどう進めていくのか、という 2 点が挙げられる。

TPPs が安全にサービスを提供していくうえで、金融機関、TPPs、利用者がそれぞれ直面するリスクを認識し、当該リスクを軽減・回避するための対策を実施する必要がある。当然、サービス提供者である TPPs は、当該対策を確実に実施し、そのためのセキュリティ管理にかかる体制を整備・運用していくことが求められる。その際、わが国の金融機関が、金融情報システムセンターの定める「金融機関等コンピュータシステムの安全対策基準」に則ってセキュリティ対策を実施し、第三者による監査を受ける体制を整備しているように、TPPs についても、対策のための一定の基準やモニタリング体制の必要性について検討することが重要であると考えられる（Open Data Institute [2016]）。TPPs は、複数の金融機関から特定の利用者の金融取引にかかるデータを網羅的に取得するケースが多く、そうしたデータの管理には金融機関が実施している対策と同程度以上のセキュリティ対策が求められる。

もちろん、TPPs サービスにおける安全性を確保していくには、利用者の側でも適切な対応が求められることは言うまでもない。そのためにも、TPPs は、金融機関と密に連携し、当該サービスにかかるリスクの所在やそのインパクト、専用アプリにかかるセキュリティ対策等に関して、利用者に対し、正確かつ平易に説明し、その理解を得るよう努力していくことが必要である。また、こうした対応の実効性を高めるためにも、さまざまなリスクが顕在化した際の責任を、金融機関と TPPs との間でどのように分担するかについて、サービスの提供を開始する前に、予め明確にしておくことが必要である。

こうした点を踏まえると、セキュリティ上のリスクの軽減のために有効な対策を講じる観点からは、TPPs をある程度コントロール可能な範囲にとどめておけるように、API をどこまでオープン化するかについて検討することが望ましい。

５．おわりに

本稿では、金融分野における TPPs の役割と金融機関の API のオープン化について、セキュリティの観点から検討を行った。

金融機関、TPPs、利用者の 3 者間に、API を介した新たな通信路が設けられると、データの流出・改ざん、不正な金融取引、サービス停止等、新たなリスクが生み出される。本稿では、そうしたリスクを具体的に指摘するとともに、各エンティティが、そうしたリスクに対してどのように対応することが求められるかを考察した。特に、TPPs は、金融機関が保有している顧客の口座情報等を取り扱うとともに、決済指図を伝達するなどの重要な業務を担う可能性があり、そうした場合、金融機関が実施しているセキュリティ対策と同等以上の対策を実施することが求められると考えられる。

なお、本稿では、セキュリティ対策を講じたことによる副作用は分析の範囲外として特に記載をしていない。しかし、セキュリティ対策を過度に実施すると、スループットの低下や利用者に複雑な処理を強いるなど、利便性の低下が生じる。セキュリティ対策を実施する際は、利用者の利便性低下が利用者の許容範囲を超えないよう、バランスを取ることも必要となる。

中長期的な観点からは、モバイル端末に新しい機能が具備され、実現可能な機能や仕組みが増加すると、アプリケーションで実現できる機能も増加すると考えられる。同時に、セキュリティ向上に資する技術の研究・開発も進められていくと想定される。金融機関と TPPs には、こうした動きを的確に理解し、新たに採用する機能については、事前にリスクを評価し、対応策を立てていく必要がある。

これらの取組みと並行して、TPPs におけるセキュリティ対策の適切な実施を担保する仕組みをどう企画・実現するか、また、金融機関と TPPs との間でリスクが顕在化した際に責任をどう分担するかなど、セキュリティ・ガバナンスにかかる検討も必要となってくる。今後、こうした検討が進み、革新的なサービスが、安心安全に広く利用されるようになることを期待したい。

以　上

【参考文献】

有吉尚哉・本柳祐介・水島淳・谷澤進、『FinTech ビジネスと法 25 講―黎明期の今とこれから―』、商事法務、2016 年

井澤秀益・五味秀仁、「次世代認証技術を金融機関が導入する際の留意点―FIDO を中心に―」、『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』No. 2016-J-3、日本銀行金融研究所、2016 年

遠藤圭介・高橋寛、「金融分野の API エコノミー」、野村総合研究所、2016 年（https://www.nri.com/~/media/PDF/jp/opinion/teiki/it_solution/2016/ITSF1608.pdf）

金融審議会、「決済業務等の高度化に関するワーキング・グループ報告～決済高度化に向けた戦略的取組み～」、2015 年

金融庁、「金融審議会　金融制度ワーキング・グループ（第 1 回）事務局説明資料」、2016 年（http://www.fsa.go.jp/singi/singi_kinyu/financial_system/siryou/20160728/02.pdf）

倉林雅、「エンタープライズの視点から FIDO と Federation のビジネスを考える」、SlideShare、2015 年（http://www.slideshare.net/kura_lab/fidofederation）

清藤武暢・四方順司、「高機能暗号を活用した情報漏えい対策「暗号化状態処理技術」の最新動向」、『金融研究』第 33 巻第 4 号、日本銀行金融研究所、2014 年、97～132 頁

総務省情報通信政策研究所、「ID ビジネスの現状と課題に関する調査研究」、2010 年（http://www.soumu.go.jp/main_content/000061624.pdf）

日経 BP 社、『FinTech 革命』、日経 BP 社、2016 年 a

――――、『FinTech 世界年鑑 2016-1017』、日経 BP 社、2016 年 b

日本 IBM、「日本 IBM、住信 SBI ネット銀行の FinTech 対応強化を支援」、日本 IBM、2016 年（https://www-03.ibm.com/press/jp/ja/pressrelease/49405.wss）

日本銀行金融研究所、「ISO/TC68 国内委員会議事録」、2016 年（http://www.imes.boj.or.jp/iso/katsudou/kokunai/gi160601.pdf）

――――、「情報セキュリティ・シンポジウム「多様化するリテール取引の安全性：モバイル化を支える情報セキュリティ技術を中心に」の模様」、『金融研究』第 32 巻第 3 号、日本銀行金融研究所、2013 年、1～16 頁

マネーフォワード 、「自動家計簿・資産管理サービス「マネーフォワード」、利用者数 350 万人突破～継続できる家計簿、改善効果を感じる家計簿、家計簿の利用率で第 1 位に～」、マネーフォワード、2016 年（http://corp.moneyforward.com/service/20160222-pfm-3500000users/）

山西健司、『データマイニングによる異常検知』、共立出版、2013 年

山本陽平、『Web を支える技術　HTTP、URI、HTML、そして REST』、技術評論社、2015 年

Banco Bilbao Vizcaya Argentaria, “BBVA API Market, the Platform for Financial Innovators,” 2016 (https://www.bbvaapimarket.com/web/api_market/).

Banco de Sabadell, “Developers Portal,” 2016 (http://developers.bancsabadell.com/).

Crédit Agricole Corporate and Investment Bank, “API REST,” 2013 (https://www.creditagricolestore.fr/castore-data-provider/docs/V1/rest.html).

European Banking Association Working Group on Electronic Alternative Payments, “Understanding the Business Relevance of Open APIs and Open Banking for Banks,” European Banking Association, 2016.

European Banking Authority, “Consultation Paper - On the draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2,” European Banking Authority, 2016 (http://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf).

European Commission, “Payment Services Directive: frequently asked questions,” 2015 (http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en).

FIDO Alliance, “FIDO Alliance,” 2016 (https://fidoalliance.org/).

Fidor Bank, “Fidor API Reference - Fidor Bank,” Fidor Bank, 2016a (http://docs.fidor.de/).

――――, “Fidor API Reference - Global Money Transfers (coming soon),” Fidor Bank, 2016b (http://docs.fidor.de/#global-money-transfers-(coming-soon)).

Musser, John, “Open APIs: State of the Market,” SlideShare, 2010 (http://www.slideshare.net/jmusser/pw-glue-conmay2010).

OASIS, “SAML Version 2.0 Errata 05,” OASIS, 2012 (http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf).

Open Bank Project, “An overview of the Open Bank Project,” 2010 (https://openbankproject.com/).

――――, “API EXPLORER,” 2016 (https://apiexplorer.openbankproject.com/).

Open Data Institute, “The Open Banking Standard,” Open Data Institute, 2016.

OpenID Foundation Japan, “OpenID Connect Core 1.0 - draft 17,” OpenID Foundation Japan, 2014 (http://openid-foundation-japan.github.io/ openid-connect-core-1_0.ja.html).

Prince, Kim Tracy, “Mint by the Numbers: Which User Are You?” mint life, 2016 (https://blog.mint.com/credit/mint-by-the-numbers-which-user-are-you-040616/).

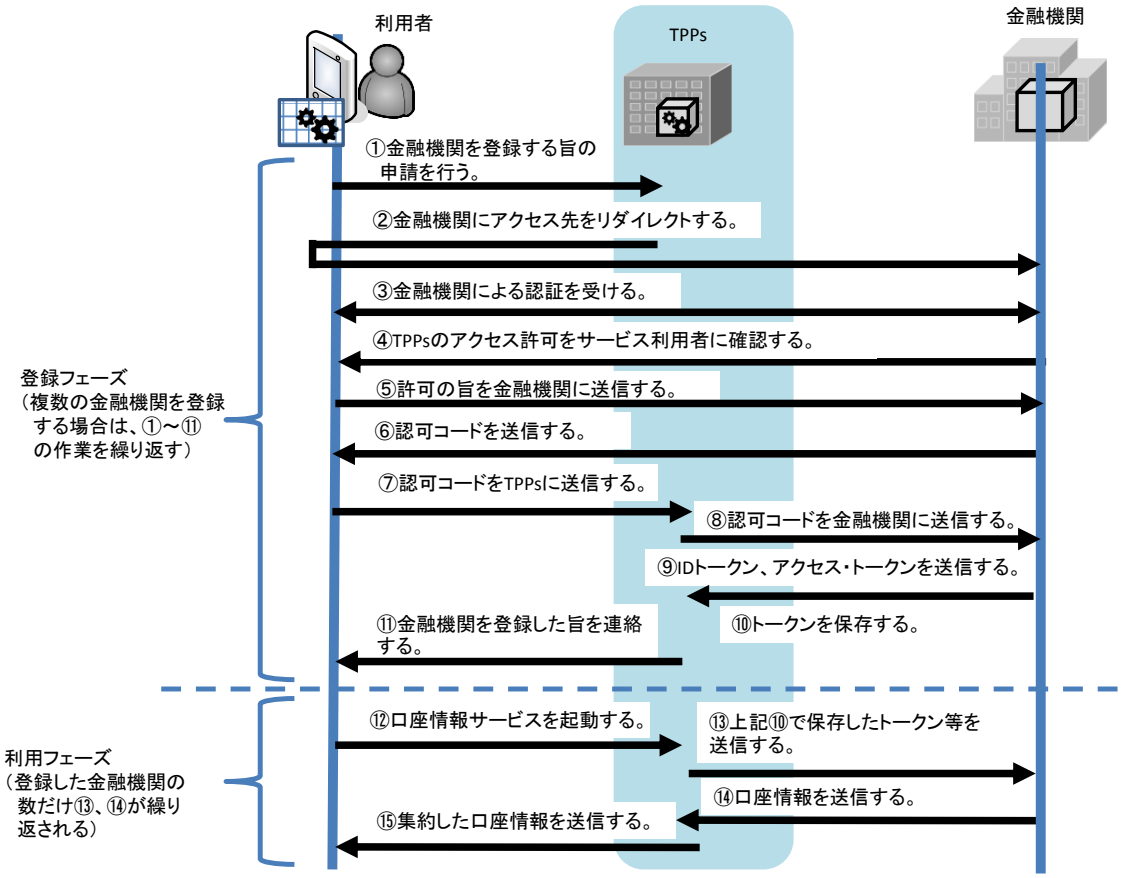
Siriwardena, Prabath, *Advanced API Security: Securing APIs with OAuth 2.0, OpenID*

Connect, JWS, and JWE, Apress, 2014.
W3C, “Payment Request API,” 2016a (http://www.w3.org/TR/payment-request/).
————, “Web Authentication Working Group,” 2016b (https://www.w3.org/Webauthn/).

補論．TPPs が複数の金融機関のアクセス・トークンを保存する運用の例

口座情報サービスにおいて、TPPs が複数の金融機関のアクセス・トークンを保存する際の運用のフローの例を以下のとおり説明する。運用フローは、登録フェーズと利用フェーズからなる。

図表 A-1　口座情報サービスを利用する際の運用フローの例



登録フェーズでは、金融機関が TPPs に登録され、アクセス・トークンが TPPs に保存される。具体的な手順は以下のとおりである。

① 利用者は、TPPs 専用アプリを起動し、集約したい口座情報を保有している金融機関を登録する旨の申請を行う。
② TPPs は、利用者が金融機関の認証を受けるように、利用者のアクセス先を金融機関にリダイレクトする（自動的に誘導する）。
③ 利用者は、金融機関にアクセスし、金融機関による認証（例えば、ID・パスワード認証）を受ける。

④　上記③の認証が成功すると、金融機関は、「TPPs が要求するデータ（口座情報等）へのアクセスを当該 TPPs に許可する」旨を利用者に確認する。
⑤　利用者は、上記④の確認に対して、許可する旨を金融機関に送信する。
⑥　金融機関は、利用者に認可コードを送信する。
⑦　利用者は、上記⑥で取得した認可コードを TPPs に送信する。
⑧　TPPs は上記⑦で取得した認可コードを金融機関に送信する。
⑨　金融機関は、TPPs に ID トークンとアクセス・トークンを送信する。
⑩　TPPs は ID トークンとアクセス・トークンを保存する。
⑪　TPPs は、金融機関の登録が完了した旨の連絡を利用者に行う。集約させる口座の数だけ、上記①～⑪を繰り返す。

利用フェーズでは、利用者は、TPPs に保存されているアクセス・トークンを用いて複数の金融機関から口座情報を入手・集約する。手順は以下のとおりである。

⑫　利用者は、TPPs 専用アプリを起動する（起動時には、TPPs にログインするための認証が必要となる）。
⑬　上記⑫の行為を受けて、TPPs は上記⑩で保存したアクセス・トークンと口座情報の提供依頼を、各トークンに対応する金融機関にそれぞれ送信する。
⑭　各金融機関は、アクセス・トークンの正当性を確認し、口座情報を TPPs に送信する。
⑮　TPPs は、上記⑭において各金融機関から受信した口座情報を集約し、その結果を利用者に送信する。

上記の場合、トークンを TPPs に保存することから、レガシー認証のケースと同様、トークンの管理にかかるセキュリティ・リスクが発生する。