資料６

クレジットカードデータ利用に係る

API ガイドライン

事務局案（2017 年 11 月版）

2017 年 11 月 20 日

資料６

目次

1　はじめに 3
1.1　本ガイドラインの目的 3
1.2　本ガイドラインの適用範囲 4
2　API 仕様の標準化 6
2.1　基本的な考え方 6
2.2　開発原則 7
2.3　開発標準 9
2.4　ステークホルダーの意見 10
2.5　その他期待される取組 10
3　セキュリティ対策及び利用者保護対策 11

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

1 はじめに

1.1 本ガイドラインの目的

クレジットカードに関連する様々な FinTech サービスが新たに生まれていくには、スクレイピングのような方法には一定の課題がある。こうした課題を解決する方法として、API によるカード会社と FinTech 企業との連携が重要な鍵を握ると考えられる。

前述のスクレイピングと比べると、API 連携は契約締結等をした者にシステムへのアクセスを許諾するため、アクセスの正当性が明確化されることによる安全面の向上の他、アクセスされる側のシステムの負荷軽減、FinTech 企業が利用者のログイン用 ID・PW を取得・保有することが不要になることによる FinTech 企業側の情報漏えいリスクの軽減という観点から優れているとの指摘がある。よりセキュアな API 連携でデータ取得を行うことは、FinTech 企業にとってもデータの同期速度が安定・迅速化する。実際、家計簿サービスにおいて、銀行口座のデータを取得する際に API 連携を行っている事例があり、その銀行を利用するユーザーの一部から、情報取得の失敗頻度が減ったといった評価を受けている。

また、新しいサービスを開発しようとする時、自社の限られたリソースによる自前主義の開発の場合は迅速性に限界があるが、カード会社が API を用意すれば、それを連携先に提供し、連携先がそれに合わせて開発することになるため、カード会社側の開発負担は削減されることとなり、開発時間も短縮化するとともに、連携先数の飛躍的増加が可能となる。

このように、API 連携はカード会社と FinTech 企業が連携を行う上で様々なメリットがある連携手段である。

また、第４次産業革命が進展し、データの処理技術や分析技術が高度化する中で、カード会社や FinTech 企業の異なる主体が保有するデータを円滑に融通できるようにし、クレジットカードデータの情報としての社会的価値を最大化することが求められる。この観点からも、カード会社と FinTech 企業による API 連携を更に促進することは重要である。

本ガイドラインは、今後、クレジットカード会社（以下、「カード会社」）と FinTech 企業を始めとする外部企業との多対多の API 連携が想定される中、API 仕様、セキュリティ及び利用者保護の対策について、規範としての方向性を示すことで、API 連携に係る事業者各位におけるサービス提供の効率化、オープン・イノベーションの促進、及び安心・安全な利用環境の創出を目指すことを目的としている。

また、本ガイドラインを策定することで、カード会社単独でサービス提供することに加え、カード会社が API 連携によって FinTech 企業等を活用することで、クレジットカードに関する今までに無かったような新しいサービスが創出され普及することにより、カード

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

サービスの利便性が一層向上するとともに、ひいては更なるキャッシュレス決済の普及に繋がっていくことを目指す。

本ガイドラインは、カード会社、FinTech 企業、小売業者、業界有識者、弁護士等の幅広い関係者による議論の結果として取りまとめられたものであり、本ガイドラインに基づいた、個別具体的なオープン・イノベーションの取組が行われることが期待される。

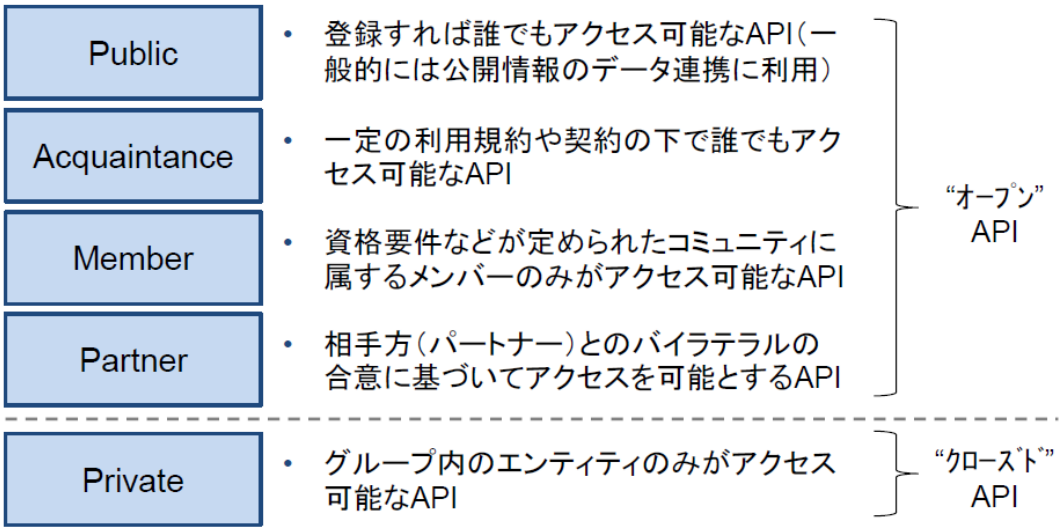
1.2 本ガイドラインの適用範囲

- オープン API の適用範囲として、本ガイドラインでは、開放性、業務、機能の３つの分類について規定する。
- 本ガイドラインは、1.1 本ガイドラインの目的 にて示したように、クレジットカード業務においてオープン API を導入する際の規範であり、必ずしもカード会社に対し、API の開放をその意に反して要求するものではない。

（１） オープン API の開放性

- オープン API の開放性には、その開放の度合いに応じて、一般的に以下の４つの類型が想定される。本ガイドラインは、この４つの類型全てについて適用対象とする。

図表 1 オープン API の開放性に関する類型



（出典）Euro Banking Association “Understanding the business relevance of Open APIs and Open Banking for banks”, May 2016 を基に NTT データ経営研究所作成

（２） 対象業務

本ガイドラインは、カード会社が提供する業務の全てを適用対象とする。

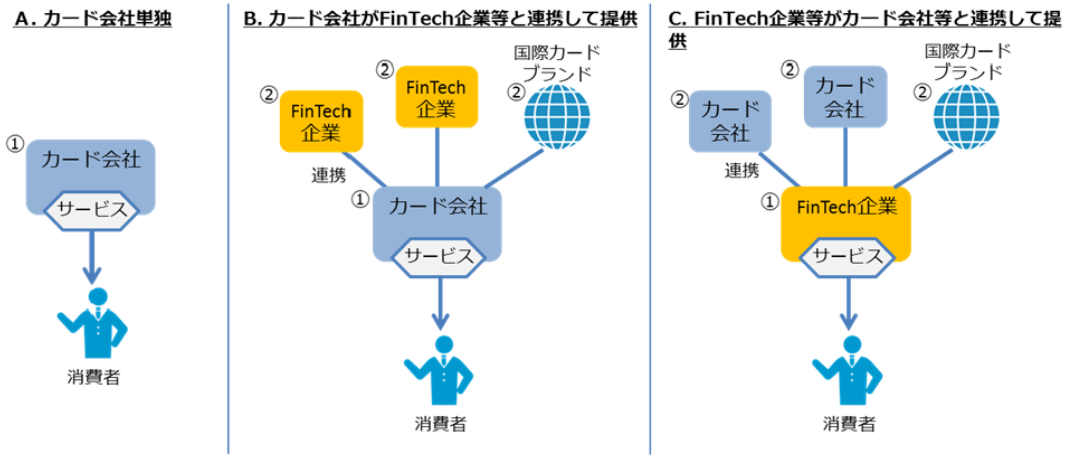
サービスが提供される上で、事業者の立ち位置として、消費者との接点を持つサービス提供者（①）と、そのサービスの実現に必要な技術や情報をサービス提供者に提供する事

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

業者（②）の２つが考えられる。具体的な事業者として、カード会社、国際カードブランド、それ以外の FinTech 企業等を想定すると、このうち国際カードブランドは、サービス提供者をサポートする立ち位置をとっている(②に相当)。

サービスの提供形態をパターン分けをすると、A.カード会社単独での提供、B.カード会社が FinTech 企業等外部企業と連携して提供する形、C.FinTech 企業等がカード会社等と連携して提供する形の 3 パターンが主に考えられる。

図表 2　クレジットカードに関するサービス提供形態



（出典）クレジットカード利用に係る API 連携に関する検討会「中間取りまとめ」（平成 29 年 6 月）

なお、本ガイドラインで言う消費者とは、個人である消費者だけでなく、例えばクラウド会計サービスを利用する法人カードを利用する法人も含まれる。

（３） 対象機能

- カード会社に係る機能は、「参照系」「更新系」「認証系」の大きく三つに分類できる。
- 「参照系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社が保有する各種データを取得し、消費者に提供する業務を指す。この場合、取得したデータを FinTech 企業等が独自の加工をし、消費者へ提供する業務も含む。
- 「更新系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社の保有するデータについて、生成、更新、削除を必要とする依頼を行う業務を指す。
- 「認証系」とは、消費者の依頼に基づき、FinTech 企業等が、カード会社が保有する、消費者を識別するための情報を取得する業務を指す。
- 本ガイドラインでは、現時点でニーズが高く、サービスの具体化が想定されるイシュアにおける「参照系」について定めるものである。なお、「更新系」「認証系」については、その利用を妨げるものではない。

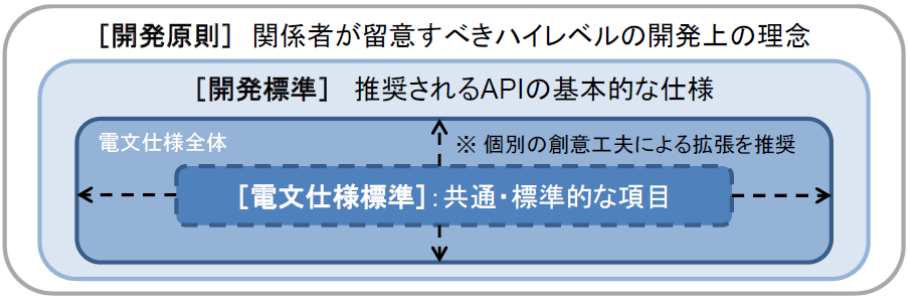
青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

2 API 仕様の標準化

2.1 基本的な考え方

- API の仕様は、セキュリティ水準の確保、利用者保護の実現、及びカード会社と FinTech 企業等の協働・連携を通じたオープン・イノベーションの促進を図るうえでも、重要な論点である。
- システム連携を行うための対応作業、特に開発面における作業において、API 仕様のガイドラインがあれば、カード会社は API を開発しやすく、API 接続を行う FinTech 企業等もカード会社の API が出来るだけ統一されていると、開発負担が軽減される。
- 金融機関における API 仕様の標準化については、前述の「オープン API のあり方に関する検討会」において、開発原則、開発標準、電文仕様標準の 3 段階で議論されてきた。電文仕様標準についても「残高照会」及び「入出金取引明細紹介」の二つの機能について定められている。

図表 3 開発原則、開発標準、電文仕様標準の関係



（出典）オープン API のあり方に関する検討会「オープン API のあり方に関する検討会報告書 ― オープン・イノベーションの活性化に向けて ―」（2017 年 7 月 13 日）

- しかしながら、金融機関の「残高照会」及び「入出金取引明細紹介」の各機能に比べ、カード会社が提供する機能に関するデータは、各カード会社独自の仕様に基づき設計されており、乖離も大きい。個々のカード会社と FinTech 企業等とが個別に協業・連携して検討する革新的なサービスを含め、その全てに対応する標準仕様を定めることは困難かつ適当ではなく、電文仕様の標準化に向けた業界内の合意形成に相当の時間を要することが想定される。
- オープン・イノベーションの実現において、スピードは重要であり、業界内の合意形成を待ってガイドラインを作成することは、かえってオープン・イノベーション

を阻害することになりかねない。

-
- 上記の判断より、現時点での電文仕様標準化は行わず、開発原則、開発標準についてのみ規定することとする。

2.2 開発原則

（１） 開発原則の目的と位置付け

- 「開発原則」は、関係者が API を開発・仕様決定するに当たり、留意すべきハイレベルの開発上の理念を定めるものである。
- オープン API は、カード会社システムへの接続仕様等を他の事業者等に公開するものであり、基本的にカード会社のみがユーザーとなる銀行システムと異なり、API の種類に拘らず、ユーザーとなる他の事業者等を意識したオープンな設計思想が求められる。
- 「開発原則」は、かかる観点から、関係者が API を開発・仕様決定するに当たり、留意すべき開発上の理念を示すことで、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。

（２） 開発原則

【原則１】API 利用者目線を意識した分かりやすくシンプルな設計・記述とすること

- オープン API は、他の事業者等による利用を前提とするものであり、API 利用者目線を意識したわかりやすくシンプルな設計・記述とすることが求められる。かかる設計・記述は、API 利用者側でのバグの発生リスクの抑制や複数銀行と接続する FinTech サービスにおけるカード会社間の仕様差異の調整の容易化、カード会社が他の事業者等と連携する際の API の汎用性、拡張性の確保にも資する。
- 設計・記述に当たっては、API 接続候補先等の事業者等ともよく協議・連携することが望ましい。また、API の仕様決定後は、接続相手方が関係する部分の仕様について自行特有の用語や金融業界特有の略語等を使用しない平易な解説書（仕様書）を準備する等によって、API の仕様に対する接続相手方の誤解・誤認等を防止することが推奨される。
- シンプルな設計・記述とすることは、実際のサービスに必要な項目のみを抽出のうえ提供する等の対応を意味し、メッセージ上の項目数の削減のみを目的に種類・性質の異なる複数の項目を結合・統合する等の対応を意味しない。一般に、統合された項目を分離して接続相手方がシステムに取り込むよりも、分離された項目を接続相手方において統合する方が、接続相手方のシステム設計がシンプルかつ汎用性の高いものとなる。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

【原則2】API の種類に応じた適切なセキュリティレベルを確保すること

- クレジットカード API では、カード会社の保有する秘匿性の高い情報が提供されるため、API の種類に応じた適切なセキュリティレベルを確保することが必要である。認証方式、通信方式等を含めた、具体的なセキュリティ対策やその水準については、「3 セキュリティ対策及び利用者保護対策」を参照のこと。
- セキュリティレベルを確保するうえでは、提供する各 API のスコープ（機能）を適切な粒度とし、接続相手方が認可された権限以上の API を使用できないようにすることが必要である。
- サイバー攻撃やサイバー犯罪の手口は年々巧妙化しているため、API のセキュリティ対策および水準は、接続相手方とも連携のうえ、継続的な改善・見直し、高度化を図っていくことが必要である。
- API の仕様書を一般に公開する場合、セキュリティに及ぼす影響について留意することが必要である。

【原則3】デファクトスタンダードや諸外国の API 標準、国際標準規格との整合性を意識すること

- 参照可能な国際標準規格等が存在する場合は可能な限り使用することが推奨される。例えば、日付や時刻の表現形式には RFC3339 や ISO8601/JISX0301、通貨コードの表現形式には ISO4217 といった標準がある。
- アーキテクチャ・スタイルやデータ表現形式、認可プロトコル等の仕様については、デファクトスタンダードや諸外国の API 標準、国際標準規格等との整合性を踏まえ、「2.3 開発標準」において推奨される基本的な仕様を定めている。

【原則4】仕様変更による API 利用者への影響をコントロールすること

- API の仕様変更は、ユーザーである接続相手方でもプログラム変更等の影響が生じることから、影響を適切にコントロールすることが必要である。クレジットカード API は、消費者の購買行動や資産管理行動の一部として機能する可能性があるため、仕様変更によって接続相手方が突然接続不能となった場合、接続相手方のサービスを利用する多くの利用者に影響・混乱が生じるおそれがある。
- 仕様変更による接続相手方への影響を抑制するため、API は、予めできるだけ汎用性、拡張性の高い設計とし、また、仕様変更が発生する可能性（機能追加、停止、バグ修正、データ形式の変更等）をできるだけ予め考慮した設計とすることが望ましい。これらは、各カード会社における API の仕様変更コストを低減することにも資する。
- 一方的な仕様変更によって接続相手方に混乱が生じないよう、仕様変更に当たっては、原則として十分な余裕をもって事前のアナウンスを行うことが必要である。また、新バージョン移行後も新旧バージョンを一定期間並行稼働させる、旧仕様を包

含した新バージョンをリリースする等の対応も推奨される。

- パートナー型のオープン API の場合、通常、銀行側から API 連携先を特定することが可能であるため、事前アナウンス等は比較的容易であるが、公開情報等をパブリック型のオープン API を通じて提供する場合等では、カード会社側から API 利用者を特定できない場合がある。また、パートナー型のオープン API であっても、カード会社への通知なく API の連鎖を許容している場合は、仕様変更の影響範囲をカード会社側で十分把握できない場合がある。このため、仕様変更に当たっては、影響範囲を十分慎重に見極めたうえで進めることが重要である。
- 推奨される具体的なバージョン管理の方法については、「2.3 開発標準」において定めている。

2.3 開発標準

（１） 開発標準の目的と位置付け

- 「開発標準」は、推奨される API の基本的な仕様を定めるものである。具体的には、①アーキテクチャ・スタイル、②データ表現形式、③認可プロトコル、④バージョン管理の四点について推奨される仕様を示す。
- 「開発標準」は、関係者が API の基本的な仕様を選択する際の目安となり、仕様の乱立による社会的コストを低減し、オープン・イノベーションが醸成されやすい環境の実現を後押しすることを目的としている。
- 「開発標準」への準拠は、各カード会社において検討・判断される。接続相手方との協議やサービスの特性等に応じて、親和性の高い適切な仕様が選択されることが重要である。
- 「開発標準」において推奨される基本的な仕様は、「2.2 開発原則」にもとづいて、諸外国を含めた API 利用者から支持されている仕様や、諸外国における標準（例：英国 Open Banking Standard）等との整合性を踏まえて定められている。
- 本ガイドラインは、「開発標準」が将来的な技術革新等に伴って陳腐化するリスクについても認識している。「開発標準」は、今後の技術革新の動向を踏まえ、必要に応じて見直すこととする。
- 「開発標準」は、各カード会社における、推奨された仕様以外の先進的な仕様や技術の採用を妨げるものではない。特に、セキュリティに関連する仕様については、より強固なセキュリティ水準を確保可能な最新の仕様があれば、同仕様を採用することが推奨される。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

（２） 開発標準

i. アーキテクチャ・スタイル

- 「アーキテクチャ・スタイル」として、REST[1]を、「通信プロトコル」には HTTPs の使用を推奨する。REST は、Richardson Maturity Model 21Level2（GET/POST/PUT/DELETE 等の HTTP 動詞の導入）を充足する設計とすることを推奨する。

ii. データ表現形式

- 「データ表現形式」として、JSON[2]を推奨する。

iii. 認可プロトコル

- 「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。

iv. バージョン管理

- 「バージョン管理」として、セマンティック・バージョニングを推奨する。仕様変更による API 利用者への影響をコントロールする観点から、メジャー、マイナー、パッチ等の区分を用いて仕様変更レベルを管理する。

2.4 ステークホルダーの意見

2.5 その他期待される取組

[1] Representational State Transfer の略。ソフトウェアがデータを連携するための設計原則の一つ。
[2] JavaScript Object Notation の略。RFC7159 で規定される軽量なデータ記述言語。

青字部分は、「中間取りまとめ」より引用
赤字部分は、全銀協「オープン API のあり方に関する検討会報告書」より引用
黒字部分は、新たに追記等を行った箇所

3　セキュリティ対策及び利用者保護対策