キャッシュレス決済データ利活用に係る
API ガイドライン

一般社団法人キャッシュレス推進協議会

Ver. 2.0

改訂履歴

版数	発行日	改訂内容	担当者
第 1 版	2018 年 4 月 11 日	・制定	経済産業省 商務・サービスグループ 消費・流通政策課
第 2 版	2019 年 10 月 30 日	・改訂	キャッシュレス推進協議会 「API ガイドラインの整備」 プロジェクト

目次

1 はじめに

1.1 本ガイドラインの目的

FinTech 企業等を通じて、クレジットカードを始めとする顧客利便性の高い新たなキャッシュレス決済サービス（以下、「決済サービス[1]」）を実現していくためには、顧客の ID やパスワードを FinTech 企業等が保管することにより実現する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、クレジットカード会社等のキャッシュレス決済事業者（以下、「決済事業者[2]」）と FinTech 企業等との API による連携が重要な鍵を握ると考えられる。

本ガイドラインは、前述のスクレイピングのようなセキュリティやシステム負荷、社会コストに課題を残す方法から、情報漏えい等のリスクを軽減し、安全性が高く、API 提供側および利用側双方のシステム負荷を軽減することができ、かつ、データの同期速度を安定・迅速化することができると考えられる API を活用した外部連携へと社会全体が移行していくべきであると考えている。実際、我が国においても、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顧客の一部から、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。

加えて、決済事業者が新たな決済サービスを開発しようとするとき、自社の限られたリソースによる自前主義の開発では迅速性に限界があるが、決済事業者が API を提供することで、FinTech 企業等の API を活用しサービスを提供する連携先（以下、「API 接続先」）を通じて、多様な決済関連サービスを提供することが可能となる。API 接続先においても安定的かつセキュアであり、仕様が明確となっている API を活用することができるようになることで、開発負荷の軽減につながり、より安価で高品質な決済関連サービスを顧客に提供することができるようになる。

このように、API は決済事業者と FinTech 企業等が連携を行う上で、双方にとってメリットがある手段といえる。

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、決済事業者や FinTech 企業等の異なる主体が保有するデータを円滑に融通することができるよう

---

[1] 本ガイドラインでは、表現上「キャッシュレス決済サービス（以下、決済サービス）」と呼称するが、当該サービスにはクレジットカードだけにとどまらずコード決済等を含む。また、単に支払サービスだけに留まらず、データ利活用や新たな与信サービスといった、幅広いサービスを想定している。

[2] 本ガイドラインでは、決済サービスを提供するクレジットカード会社や、クレジットカードに類するコード決済事業者等を総称してキャッシュレス決済事業者（以下、決済事業者）と定義する。また、ブランド型を中心としたプリペイドサービスの事業者等も本ガイドラインを参考にすることが期待される。

にし、決済データの情報としての社会的価値を最大化し、顧客に還元することができるような仕組みを構築することが重要であると考える。この観点からも、決済事業者と FinTech 企業等による API 連携を更に促進することは重要である。

このように API の重要性は、本ガイドラインの制定を待たずとも意識されているところであり、今後、さらなる API の利活用が進むものと考えられる。

本ガイドラインは、今後、決済事業者と FinTech 企業等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、セキュリティおよ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決済サービス提供の効率化、オープン・イノベーションの促進、および安心・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、決済事業者単独で決済サービスを提供することに加え、決済事業者が API 連携によって FinTech 企業等を活用することで、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、決済サービスの利便性を一層向上させ、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、決済事業者、FinTech 企業等、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第１版に、キャッシュレス決済の進展状況を踏まえキャッシュレス推進協議会分科会が改訂を加えたものである。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。

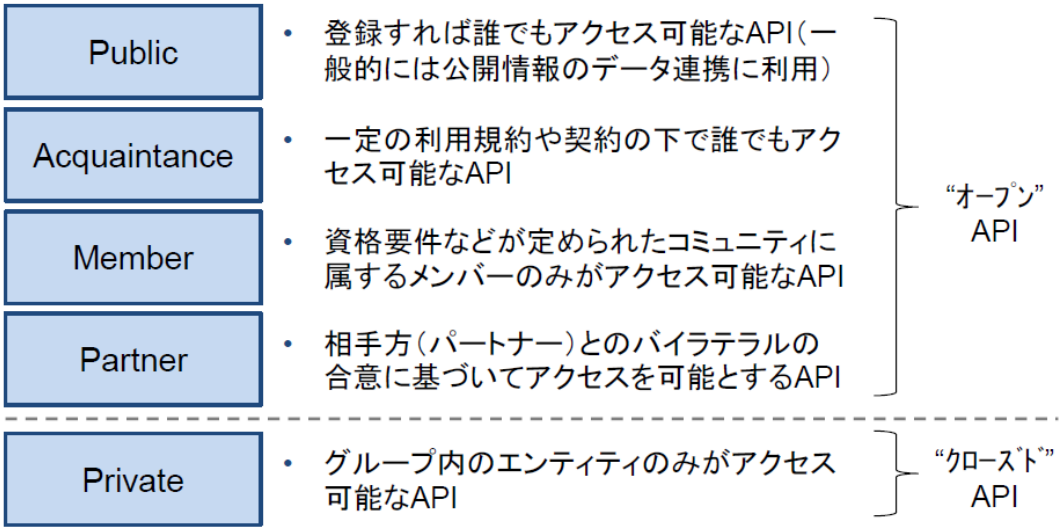
1.2　本ガイドラインの適用範囲

- 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、決済サービスにおいてオープン API を導入する際の規範であり、本ガイドラインに基づく決済事業者における API 導入が促進されることを期待するものの、必ずしも決済事業者に対し、API の開放をその意に反して要求するものではない。
- また、決済事業者と API 接続先の双方において合意がなされている場合においては、本ガイドラインの各規定に形式上準拠していないケースであっても、本ガイドラインの趣旨を逸脱しない範囲であれば、当該 API 連携を妨げるものではない。

（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



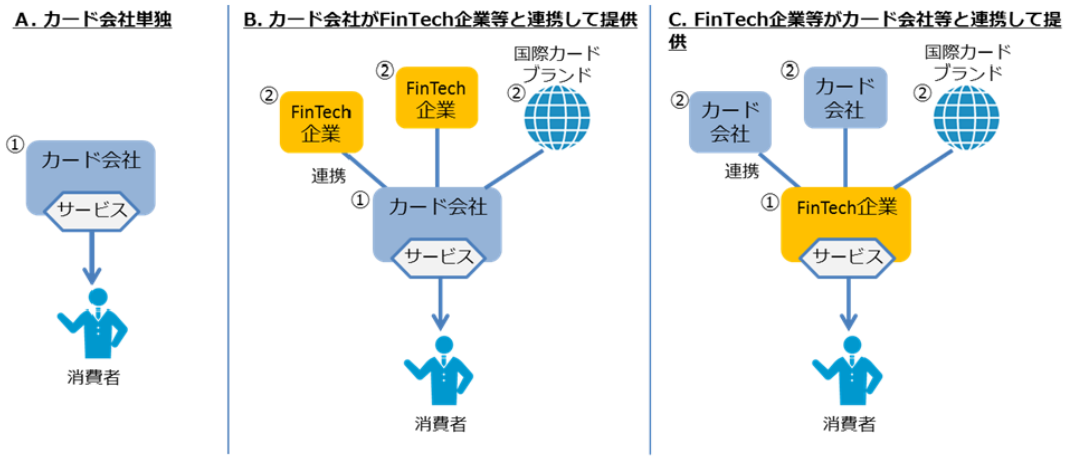
（出典）Euro Banking Association “Understanding the business relevance of Open APIs and Open Banking for banks”, May 2016 を基に NTT データ経営研究所作成

（２） 対象業務

i. API 関連事業者の立ち位置

- 決済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についてパターン分けをすると、A. 決済事業者単独での提供、B. 決済事業者が FinTech 企業等外部企業と連携して提供する形、C. FinTech 企業等が決済事業者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　クレジットカードを例にしたサービス提供形態



（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利用者とは、個人である消費者だけでなく、例えば法人クレジットカードを利用する個人事業主を含む法人（以下、「法人顧客」）も含まれる。

ii.　PAN 情報および ID/パスワードの API 不通過

- 決済サービスの中で、カードサービスでは、PAN（Primary Account Number）と呼ばれる、クレジットカードを一意に特定する番号が用いられる。この PAN 情報が漏えいすると、クレジットカードの不正利用に繋がることが容易に想定される。そのため、クレジットカード業界では PCI DSS[3]等の非常に高度なセキュリティ体制を敷いている。
- 決済サービスに関連する API の活用において、この PAN 情報が取り扱われる場合、API 接続先も PCI DSS に準拠する必要が生じる。
- また、決済事業者が提供している Web サービス等で利用される ID およびパスワードについては、利用者および決済事業者のみが把握すべきものであり、API 接続先であったとしても不必要な保持は望ましくない。
- そのため、本ガイドラインで定める API に関する各規約は、PAN 情報および ID/パスワードを取り扱わない前提として記載する。

（３）　対象機能

- 決済事業者の提供する機能は、「参照系」「更新系」「認証系」の大きく三つに分類することができる。
- 「参照系」とは、API 接続先が、利用者の依頼に基づき、利用者の求めるデータを提供するため、決済事業者が保有する各種データを取得するためのデータ提供機能を指

[3] Payment Card Industry Data Security Standard の略。クレジットカードの主要なブランド 5 社により設立された PCI SSC (Payment Card Industry Security Standards Council) が制定するクレジットカードに関するセキュリティ基準。

す。

- 「更新系」とは、API 接続先が、利用者の依頼に基づき、決済事業者の保有するデータについて、生成、更新、削除を行うことを可能にする機能を指す。
- 「認証系」とは、API 接続先が、利用者の依頼に基づき、決済事業者が保有する利用者を識別するための情報を取得する機能を指す。
- 本ガイドラインの第１版は、決済事業者における「参照系」（特に、PFM サービスや会計ソフト等における利用明細の照会）を対象に作成されたが、コード決済における利用の拡大等も踏まえた「更新系」および事業者からの要望のあった「認証系」についても本ガイドラインの対象範囲とする[4]。

[4] ガイドラインの範囲は、API の開発原則やセキュリティ・利用者保護に関する内容であり、電文標準および決済事業者と API 接続先との契約などについては、参照系を参考にしつつも別途定めることが望ましい。

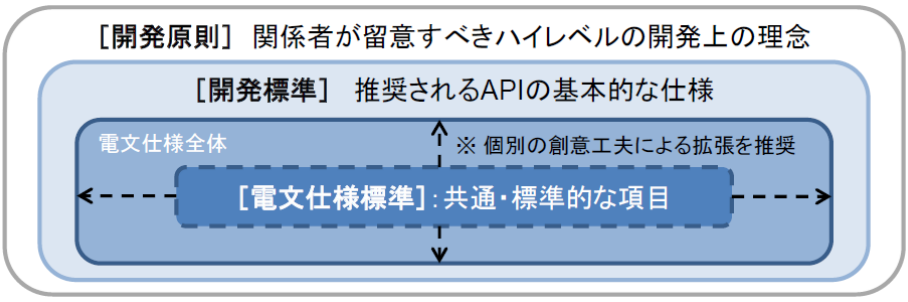
また、更新系・認証系を実現するにあたり、API を利用する事業者は、決済事業者に係る割賦販売法、貸金業法その他の法令を遵守することが求められている。（個別の条文に記載がない事項、例えば貸金業の媒介業務を貸金業法に基づく登録を経ないで行わないことなどの法令遵守は、当然に求められるものであり対応が必要である。）この点に留意した上で、決済事業者・関連当局・関連自主規制団体などと協議することが求められる。

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、および決済事業者と 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上でも、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、決済事業者は API を開発しやすく、API 接続先においても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、全国銀行協会公表の「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」および「入出金取引明細照会」の二つの業務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」および「入出金取引明細照会」の各業務に比べ、決済事業者の業務に関するデータは、各決済事業者独自の設計思想に基づき仕様が策定されており、個社毎の乖離も大きい。個々の決済事業者と 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ため、電文仕様の標準化に対しては慎重な対応が必要である。
- 上記の判断に基づき、本ガイドラインでは開発原則、開発標準の規定を先行して進め

てきた。しかしながら、クレジットカード決済の参照系 API の標準電文が制定されたことに加えて、コード決済に参入する決済事業者が近年急増したことを背景として、コード決済用の標準電文が制定されるなど電文仕様の標準化も進展している。

- 電文仕様の標準化は、上述の通り開発負担の軽減やデータ利活用への利便性向上が期待されるところである。そのため、電文仕様の標準化が可能となるような各社の取組みが期待される。

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、決済事業者の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、基本的に決済事業者のみがユーザーとなる既存の決済事業者システムと異なり、API の種類に拘らず、API 接続先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、API 提供者および API 接続先（以下、「API 関係者」）の双方が 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 接続先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、API 接続先による利用を前提とするものであり、API 接続先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 接続先側でのバグの発生リスクの抑制や複数決済事業者と接続する FinTech サービスにおける決済事業者間の仕様差異の調整の容易化、決済事業者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。
- 決済事業者における設計・記述に当たっては、API 接続を行うことを検討している FinTech 企業等ともよく協議・連携することが望ましい。また、API の仕様決定後は、API 接続先が関係する部分の仕様について自社特有の用語や決済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 API 接続先の誤解・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 API 接続先がシステムに取り込むよりも、分離された項目を API 接続先において統合する方が、API 接続先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。

【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

- 決済サービスの API（以下、「決済 API」）では、決済事業者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 セキュリティ対策および利用者保護対策」を参照のこと。
- セキュリティレベルを確保する上では、提供する各 API のスコープ（機能）を適切な粒度とし、API 接続先が認可された権限以上の API を使用することが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、API 接続先とも連携のうえ、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 接続先への影響をコントロールすること

- API の仕様変更は、API 接続先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。決済 API は、利用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 API 接続先が突然接続不能となった場合、API 接続先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 API 接続先への影響を抑制するため、決済 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、各決済事業者における 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 API 接続先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、決済事業者側から API 接続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、決済事業者側から API 接続先を特定することが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、決済事業者への通知なく API の連鎖[5]を許容している場合は、仕様変更の影響範囲を決済事業者側で十分把握することが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上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。

【原則5】サービス提供までに十分な確認を行うこと

- 仕様書に十分な記載が行われていたとしても、システムを稼動させることで発覚する課題等があることも想定される。そのため、実際にサービス提供を開始するまでに、決済事業者、API 接続先の双方が参加する事前の確認を十分に行う必要がある。
- 上記の確認を行うための環境（テスト環境やテストデータ等）については、決済事業者側にて準備されることが望ましい。

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４点について推奨される仕様を示す。
- 「開発標準」は、API 提供者が 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、各決済事業者において検討・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」に基づいて、諸外国を含めた API 接続先から支持されている仕様や、諸外国における標準[6]等との整合

[5] API の連鎖については「3.5（２） 「API 接続先の API 接続先」の取扱い」を参照。
[6] 例えば、シンガポール通貨監督庁（MAS）の策定した「Open API Playbook」、英国競争・市場庁（CMA）主導で策定されている「Open Banking」、汎欧州の取組みである「Berlin

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が必要である。
- 「開発標準」は、各決済事業者における、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。

（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[7]を、「通信プロトコル」にはHTTPsの使用を推奨する。RESTは、Richardson Maturity Model[8] Level2（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[9]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（RFC 6749）認可フレームワーク（以下「OAuth2.0」）を基本とする。また、より安全なトークンの授受を実現するため、PKCE（Proof Key for Code Exchange）（RFC 7636）の活用を推奨する[10]。
- ただし、APIの開放がパートナー型など、API接続先を特定することができ、かつ、相手方のセキュリティ対策等が容易に把握することができる場合等においては、PKCEの活用までを求めなくてもよい。

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接続先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。

Group」などが挙げられる。

[7] 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。

[8] https://martinfowler.com/articles/richardsonMaturityModel.html を参照。

[9] JavaScript Object Notationの略。RFC7159で規定される軽量なデータ記述言語。

[10] なお、金融分野におけるAPIへのOAuth2.0の適用に関する詳細仕様は、2018年2月現在、OpenID Foundation Financial API WG（FAPI WG)において標準化作業が進められている。

2.4　電文仕様標準

（１）　電文仕様標準の目的と位置付け

- 「電文仕様標準」は、API 提供者が API の基本的な仕様を策定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。
- 「電文仕様標準」は、API のメッセージ上の標準的な項目やその定義等の目安を定めることが望ましい。
  例えば、クレジットカードでの参照系 API においては、項目の規定に際し、以下 3 区分を定義している。

  標準項目：各項目の定義が明確であり、かつ最低限必要と考えられるもの。
  推奨項目：各クレジットカード会社で実現可否や仕様が異なるものの、
  　　対応することが望ましいもの。
  任意項目：各クレジットカード会社で実現可否や仕様が異なるものの、
  　　可能な場合は対応が望まれるもの。

- 「電文仕様標準」への準拠は、各決済事業者において検討・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。
- 電文種別毎の、具体的な項目、コードの定義等については、個別に関連するステークホルダーによる検討が必要であり、本ガイドラインとは別に定めるものとする。

（２）　電文仕様標準

既に定まっている具体的な仕様については、以下を参照とされたい。

i.　クレジットカードにおける参照系 API
　「クレジットカード分野のオープン API に係る電文仕様標準について」[11]

ii.　コード決済における決済 API
　「コード決済に関する統一技術仕様ガイドライン」[12]

[11] キャッシュレス推進協議会【PJ18-6】として 2019 年 3 月に制定
[12] キャッシュレス推進協議会【PJ18-1】として 2019 年 3 月に制定

3 セキュリティ対策および利用者保護対策

3.1 基本的な考え方

- 決済 API の活用は、現在、世界的にも試行錯誤の状況にあり、考え方の整理が必要な論点が多い。とりわけ、セキュリティ対策、利用者保護は、オープン API を活用したサービスに対する利用者の信頼を確保し、オープン API の普及、活用促進・円滑化を図る上で、重要な論点である。
- オープン API では、利用者からの申請・同意に基づいて行われるとはいえ、決済事業者が保有する秘匿性の高い顧客情報が API 接続先に提供され当該 API 接続先において蓄積・保存されることになる。それゆえ、オープン API に取り組むに当たっては、API 関係者において十分なセキュリティ対策、利用者保護が図られることが必要となる。
- 他方、API 接続先に対して、決済事業者と同水準のセキュリティ対策、利用者保護策を徒に求めれば、API 接続先において対応負荷が増すこととなり、決済事業者と API 接続先の協働・連携による利便性の高い革新的なサービスの提供やサービスの高度化、イノベーションに向けた取組みが阻害され、消費者がテクノロジーの進展の恩恵を受ける機会を失うおそれがある。
- こうした認識の下、本ガイドラインでは、API の機能や連携するデータの種類・秘匿性等に応じたリスクベース・アプローチに基づいて、利用者利便と利用者保護のバランスを踏まえた、決済 API におけるセキュリティ対策および利用者保護に関する基本的な考え方を取りまとめた。
- 取りまとめに当たっては、イノベーションを阻害しないよう留意するとともに、決済事業者、API 接続先双方に対して対応水準の目安を示すことで、決済事業者による API 接続先に対する過度に保守的なセキュリティ対策の要求や、セキュリティ上の懸念から生じる決済事業者側のオープン API への取組みに対する躊躇といった課題を解消するとともに、API 接続先に対しても一定程度のセキュリティ対策、利用者保護対策を求めることで、決済事業者と FinTech 企業等の協業・連携の円滑化に資するものとすることを意識した。
- なお、先述のとおり、オープン API は、オープン・イノベーションを実現していくためのキー・テクノロジーの一つであり、今後、本技術を活用して、様々なビジネスモデルやサービスが提供されることが期待される。それゆえ、ビジネスモデルやサービスによって異なるリスクと対策の全てを網羅的に検討することは困難であり、本ガイドラインでは、様々なビジネスモデルやサービスに共通すると思われる主なリスクに対応したセキュリティ対策および利用者保護策に焦点をあてて取りまとめている。
- 具体的なセキュリティ対策および利用者保護策については、各決済事業者のポリシー

や、個別のビジネス、各サービスのリスク、API 接続先の態様等に応じて個々に判断されるものであり、利用者保護の観点から、関係当事者において本ガイドラインの趣旨を十分に踏まえつつ、検討されることを期待する。例えば、リスクの内容等を勘案して本ガイドラインでは挙げていない追加的な対策を講じることも考えられる。他方で、リスクが小さいと考えられるビジネスやサービス等についてはセキュリティ対策を軽減することも考えられる。

- 以下では、オープン API において想定される主なリスクを整理した上で、セキュリティ原則および利用者保護原則を示す。

3.2 オープン API の主なリスク

- オープン API では、決済事業者のシステムに新たな通信路を設けて API 接続先を経由した新たなサービスを利用者に提供することになるため、当該通信路を悪用したデータの漏洩等が生じるリスクがある。
- 他方、決済事業者や FinTech 企業等では、取扱うデータの重要性に鑑み、これまでもセキュリティ対策や利用者保護対策を行ってきているのも事実である。
- そこで、本章ではオープン API に関するリスクを包括的に概観した後、オープン API の利用に伴い、新たに生じることが想定されるリスクに着目し、整理を行う。

（1） セキュリティ上のリスク

- オープン API に関連するセキュリティリスクを、以下の観点から分類した。実際に発生するリスクの発現は、これら観点に基づく要素の組合せによると言える。

i. リスクの発生要素に関する分類

a） 発生場所

- 発生場所は、「内部環境」と「外部環境」に分類することができる。
- 内部環境とは、API 関係者のそれぞれにおいて直接的に管理下に置くことのできる環境を指す（直接的に管理下に置くような契約がない限り、API 接続を行う相手先は含まない）。具体例として、API 関係者の拠点、システム、ネットワーク、契約上管理下に置くことのできる外部システム、ネットワークを指す。
- 外部環境とは、API 関係者の管理下にはない場所を指す。具体的には、公衆ネットワーク、スマートフォン等の利用者の有する環境、利用者等の生活環境、委託先の拠点、システム、ネットワークを指す。

b） 発生者

- 発生者は、「内部者」と「外部者」に分類することができる。
- 内部者とは、上記の内部環境に直接的にアクセスすることができる者を指す。具体的には、API 関係者の役職員や外部委託先の役職員を指す。

- 外部者とは、内部環境に直接的にアクセスすることができない者を指す。利用者や無関係の第三者が想定される。

c） 動機

- 動機は、「故意的」か「偶発的」かに分類することができる。

d） 対象資産

- リスク発生時に対象となる資産は、「資金」「データ」および「その他有形/無形」資産に分類することができる。
- 資金には、顧客資金だけではなく、API 関係者の資金も含む。
- データとは、API 関係者の企業情報や利用者の個人情報に加え、システム上の設定値等が含まれる。

ii. API 利用に特有のリスク

- API の利用に伴うセキュリティリスクは、上述の通り、多様な要素の掛け合わせとなるため、多種多様であると言える。
- しかしながら、決済事業者や FinTech 企業等では、従前よりリスク対策を行ってきていることも事実である。そのため、徒にリスクを指摘することは、既存の対策と重複した、さらなるセキュリティ対策コストを要求することとなり、かえってイノベーションを阻害する要因となりかねない。
- そのため、本ガイドラインでは、上記分類から導出される多様なセキュリティリスクの内、API に特有のリスクについてのみ記載を行うこととする。当然ながら、他のリスクについても十分な対策が既にとられていることが前提となる。

a） API 基盤に関するセキュリティリスク

- API 基盤とは、API 接続を実現するためのシステム基盤を指す。当該基盤が独立して存在するか、他のシステムに内包されているかは問わない。また、当該基盤の構築、保守、運営を外部に委託しているとしても、委託元企業は、自身のシステムと同等に管理を行わなくてはならない。
- API 基盤は、システムを管理する企業の外部へのゲートウェイとしての役割を担っており、不特定多数のアクセスが発生することが想定される。そのため、不特定多数のアクセスが発生することを想定したセキュリティ対応が求められる。システムへの侵入だけでなく、DDoS 攻撃等の大量データ送信による攻撃リスクも想定される。
- また、API 基盤における影響が、内部システムへ波及することによるリスクも想定される。

b） 公衆ネットワークにおける API 通信に関するセキュリティリスク

- API 通信は、インターネット等の公衆ネットワークを介して行われることが想定される。そのため、悪意のある第三者により、通信内容の傍受、改ざん、消去等が行われ

るリスクが内在する。

- この公衆ネットワークの利用は、利用者－API 接続先間、および API 接続先－決済事業者間の 2 経路があり、双方におけるリスクを考慮する必要がある。

c） トークン管理に関するセキュリティリスク

- 「2.3 開発標準」において記載したとおり、認可プロトコルでは OAuth2.0 の利用が推奨される。本プロトコルはトークンを利用した認可処理が行われる。そのため、トークンを発行する決済事業者、トークンを利用する API 接続先の双方において、トークンの管理に対するセキュリティ対策が重要である。
- API 関係者において、トークンの流出、偽造のリスクを考慮する必要がある。

（２） 利用者保護上のリスク

- API 利用サービスは、その技術的特性から、以下の特徴が挙げられる。
  ① 不特定多数の利用者が利用する
  ② サービス提供の基礎となる API を始めとする技術要件が消費者にとって高度かつ複雑であり、十分な理解を得ることが困難である
  ③ スマートフォンのアプリ等によるサービス提供が中心となり、対面でのサービス提供が行われないケースが多い
  ④ 本来のサービス提供者（決済事業者）と、直接のサービス提供者（API 接続先）が異なる
- 上記の特徴から、利用者がサービス提供主体、提供内容等を十分に理解しないままサービスを利用するというリスクが内在する。
- また、責任の所在が不明確な場合、利用者に発生した損害に対する補償が十分に得られないというリスクも存在する。

3.3 セキュリティ原則

（１） API 接続先の適格性

i. 事前審査

- 決済事業者は、FinTech 企業等との API 接続に先立ち、セキュリティ等の観点から、API 接続先の適格性を審査することが必要である[13]。
- セキュリティに関連した適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である[14]。
  ① セキュリティ原則の充足状況

[13] 情報セキュリティ以外の適格性については、「3.4 利用者保護原則」を参照。
[14] API 接続先が ASP やクラウドサービスを利用している場合には、API 接続先から必要な開示が行われる必要があることに留意する

② 過去に発生したセキュリティ関連の不祥事案と改善状況
③ 利用者の属性や取引のリスクに応じた、継続的なセキュリティ対策の高度化に向けた態勢やリソースの有無

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、API 接続によって目指すビジネスモデルやその固有リスク、各決済事業者のセキュリティポリシー等に応じて、各決済事業者が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が任意に定めたセキュリティポリシーやセキュリティ関連文書、API 接続先が取得した情報セキュリティ関連の認証（ISO27001、TRUSTe、等）、決済事業者との API 接続状況、銀行等を含めた他の金融機関との API 接続状況等は、上記の適格性の審査に当たっての参考になると考えられる。
- 複数の決済事業者と API 接続する FinTech 企業等における審査対応負担を軽減する観点から、キャッシュレス推進協議会において、決済事業者が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」を制定しており、決済事業者はこれを利用することを求められる。
- なお、事前審査は、各決済事業者がそれぞれ独立に行うことを前提としつつも、複数の決済事業者と API 接続先における審査対応負担の軽減や決済事業者による事前審査水準の標準化の観点から、当該決済事業者の責任において他の決済事業者に事前審査を委ねたり、他の決済事業者が既に行った事前審査の結果を参考にしたりすることも考えられる[15]。

ii. モニタリング

- 決済事業者は、API 接続先の情報セキュリティに関連した適格性について、API 接続後も定期的にまたは必要に応じて確認することが必要である[16]。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各決済事業者のセキュリティポリシー等に応じて、個別に判断されると考えられる。
- 決済事業者は、API 接続に当たって、API 接続先との間でモニタリングに関する事項（例：方法、深度、頻度、必要に応じた立入検査等、情報セキュリティ対策の大幅な変更を行う場合の対応、等）を予め取り決めておくことが必要である。
- 決済事業者は、API 接続先の情報セキュリティに関連した適格性に懸念があると判断した場合には、API 接続先に対して改善を求め、利用者保護の観点から、必要な場合

[15] 本方式を採用する場合の決済事業者間の取決めに係る留意点については、銀行界で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。
[16] API 接続先が定期的な情報セキュリティ関連の外部監査を受けている場合には、それらの結果を活用すること等も考えられる。

にはAPI接続先のアクセス権限の制限、停止、取消等を行わなければならない[17]。

- なお、モニタリングは、各決済事業者がそれぞれ独立に行うことを前提としつつも、複数の決済事業者と API 接続先におけるモニタリング対応負担の軽減や、決済事業者によるモニタリング水準の標準化の観点から、当該決済事業者の責任において他の決済事業者にモニタリングを委ねたり、他の決済事業者が既に行ったモニタリングの結果を参考にしたりすることも考えられる[18]。

（２） 外部からの不正アクセス対策

- 以下は、アクセス権限の認可にOAuth2.0を実装したシステムを前提とした記載としている。なお、同等の、またはより強固な認可・認証が可能な他のプロトコル（新たなテクノロジーを含む）の採用を妨げるものではない。

i. アクセス権限の付与に係る認証

- 決済事業者は、公表情報または匿名加工情報を提供する場合を除き、API接続先に対するアクセス権限の付与（OAuth2.0においては「認可」）を利用者の申請に基づき行うこととし、その際、利用者の本人認証を行わなければならない。
- 認証方式は、利用者の属性や付与するアクセス権限の内容とそのリスクに応じた強度とすることが必要である[19]。
- 認証方式の選択に当たっては、当該決済事業者において採用されている他のオープンネットワークを利用した取引チャネル（例：Web サービス）の認証方式の水準が一つの目安となり得るが、以下の点にも留意が必要である。
  ① 個々の取引に係る認証ではなく、アクセス権限の認可に係る認証であること
  ② API を通じて指図を受ける個々の取引に係る認証方式も勘案した全体の不正アクセスリスクに応じた認証強度とする必要があること
- 当該決済事業者において採用されている他のオープンネットワークを利用した取引チャネルの認証方式と比較して、強度の劣後する認証方式を採用する場合には、不正アクセスリスクが高まることを踏まえた利用者保護上の別途の対策が必要となる。例えば、店頭手続・郵送確認等を併用する、参照可能範囲を制限する、トークンの有効期限を短期とする、不正利用発生時の補償を予め定める、等が考えられる。

ii. アクセス権限／トークンの管理

- 決済事業者は、API接続先に付与するアクセス権限（OAuth2.0においては「トーク

---

17 ただし、決済事業者が恣意的な判断によりアクセスを制限してAPI接続先の事業に影響を与えることのないよう留意する。

18 本方式を採用する場合の決済事業者間の取決めに係る留意点については、銀行界で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。

19 各決済事業者の判断に基づき、利用者保護の観点から、強固な認証方式を一律に採用することも妨げない。

ン」が発行される）の管理について、以下の点に留意することが必要である。

① 付与するアクセス権限は、API 接続先が提供するサービスに必要な範囲に限定すること（利用者からの申請／同意があったとしても、不必要なアクセス権限を API 接続先に付与しないこと）

② API 接続先に発行するトークンには、利用者属性やアクセス権限の内容とそのリスク、利用者の利便性等を踏まえた適切な有効期限を設定すること

③ アクセス権限の内容に応じたトークンの偽造・盗用対策を講じること

④ 不正アクセス等を検知、または発生した場合に速やかにアクセス権限の制限、停止、取消が可能な仕組みとすること

- 決済事業者は、アクセス権限やトークンを管理するシステムに対し、必要なセキュリティ対策を講じなければならない。また、API 接続先に対しても、トークンの適切な管理とセキュリティ対策を求めなければならない。

iii. 通信方式

- 通信方式としてオープンネットワークを使用する場合、第三者による盗取等を防止する観点から、TLS を使用して保護することが必要である。

iv. システムの堅牢性

- 決済事業者は、顧客情報について、商慣習または信義則に基づく私法上の義務として守秘義務を負うほか、国際ブランドルール、日本クレジット協会（JCA）の「カード情報の保護対策の計画」やクレジット取引セキュリティ対策協議会の「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」等を参考に、利用者の利益が不当に害されることのないよう当該業務に関する情報を適正に管理し、かつ当該業務の実施状況を適切に監視するための態勢の整備その他必要な措置を講じることが求められる。
- 決済事業者が保有する顧客情報の秘匿性を踏まえれば、利用者保護や不正アクセス／情報流出防止の観点から、API 接続先（特に複数決済事業者の大量の顧客情報を蓄積している PFM 事業者）においても、決済事業者と同水準のセキュリティ対策が講じられることが理想的であるものの、決済事業を前提とした上記安全管理措置を一律に API 接続先に適用することは必ずしも適当ではないと考えられる。また、決済事業者が行っている外部委託先に対するシステムリスク管理の考え方についても参考になるものの、オープン API では、外部委託と異なり、決済事業者から API 接続先への情報提供は利用者からの申請／同意に基づくものであることや高い堅牢性が求められる決済事業者システムの一部を外部委託するものではないことから、外部委託先管理の枠組みを一律に適用することができるわけではないと考えられる。
- API 接続先が確保すべき安全管理措置の水準は、API 接続先が取得・保有する情報の内容と量、情報が万一流出した場合に想定される利用者への影響や被害、API 接続先

に対する利用者の情報管理に関する期待の程度等を踏まえて、第一義的には API 接続先が自らリスクベースで個別に判断することが必要である。

- API 接続先が確保すべき安全管理措置の目安水準については、最低限、API 接続先においても以下の措置は必要である。
  ① ウィルス対策ソフトの導入
  ② 機密性の高い情報（例：API 接続先の ID/PW やクライアント証明書、トークン、等）の暗号化
  ③ ファイアーウォール等のサイバー攻撃に対する多層防御の導入
  ④ サーバ変更監視（改竄検知）、ネットワーク監視
  ⑤ 公開サーバ脆弱性対策
  ⑥ API 実行ログ（ユーザー、操作、結果、等）取得、保管
  ⑦ 情報喪失等に備えたバックアップ等の対策
- なお、API 接続先に、顧客の同意を得て決済事業者が提供する個人情報（個人データ）の個人情報保護法上の取扱いは、個別のスキームに応じて個々に判断されるべきものではあるが、原則的に決済事業者は API 接続先に対して、個人情報委託先の監督義務（同法第 22 条）を負っていないと解するのが適当と考えられる。

v. 不正検知・監視機能

- 不正検知・監視機能は、不正アクセス被害の発生やその拡大を未然に防止する上で重要な機能の一つである。
- オープン API においては、利用者の IP アドレスや認証失敗回数等の不正検知に活用される情報を決済事業者が直接入手することができなくなるため、取引のリスクに応じて、決済事業者が必要とする場合には、API 接続先から決済事業者に不正検知に必要な情報が提供される仕組みを構築することが必要である。
- API 接続先についても、API 接続先が取得・保有する情報の内容と量、当該情報が万一流出した場合に想定される利用者への影響や被害、API 接続先に対する利用者の情報管理に関する期待の程度等を踏まえて、情報セキュリティ関連機関において、不正検知・監視機能の要否やその水準等についての考え方や留意点の整理が行われることが期待される。

（３） 不正アクセス発生時の対応

i. システム設計・仕様

- API 関係者は、不正アクセスが判明した場合に被害発生やその拡大を未然に防止する観点から、速やかに、決済事業者においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことができるシステム設計・仕様としなければならない。
- API 関係者は、不審なアクセス等についての利用者からの照会への対応や、不正アク

セス発生時の原因調査、必要な対策の検討を行うため、適切なアクセスログの記録および保存を行わなければならない。

ii. 情報連携、対策協議

- 不正アクセス発生時には、速やかに決済事業者と API 接続先の間で情報連携を行うとともに、原因調査や必要な対策の協議等を協力して行っていくことが必要である。必要な対応については、決済事業者と API 接続先との間で予め取り決めて明確化しておくことが必要である。

（４） セキュリティ対策の継続的な改善・見直し、高度化

- 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上、オープン API を活用したサービス提供は世界的にみても現状、初期段階にある。そのため、API 関係者は、自社のみならず他社での不正アクセス事例等を踏まえ、セキュリティ対策の継続的な改善・見直し、高度化を図っていくことが必要である。
- セキュリティ対策の改善・見直し、高度化に向けては、API 関係者は、協力して取り組むことが重要と考えられる。

3.4 利用者保護原則

（１） API 接続先の適格性

i. 事前審査

- 決済事業者は、他の事業者等との API 接続に先立ち、利用者保護等の観点から、API 接続先の適格性を審査することが必要である[20]。なお、決済事業者が共通システムを通じて API 接続先と接続する場合については、決済事業者による API 接続先の審査結果に基づき、共通システム提供事業者が API 接続先との接続を行うものとする。
- 適格性の審査に当たっては、少なくとも以下の点について API 接続先に確認することが必要である。
  ① グループ会社を含めた事業内容、兼業内容
  ② 反社会的勢力との関係の有無を含む社会的信用、組織ガバナンス
  ③ 法令遵守態勢
  ④ 利用者保護態勢[21]
  ⑤ 利用者保護原則の充足状況
  ⑥ 過去に発生した利用者保護関連の不祥事案と改善状況

[20] 情報セキュリティ関連の適格性については、「3.3 セキュリティ原則」の「3.3（１）API 接続先の適格性」を参照。
[21] 特に顧客情報の適切な取扱い・管理態勢や、取得情報の利用目的の適切性、利用約款の適切性（過度な免責規定等、利用者保護に著しく欠ける条項の有無）について確認する。

⑦ 利用者の属性や取引のリスクに応じた、継続的な利用者保護策の高度化に向けた態勢やリソースの有無

- 適格性の審査は、画一的・機械的に行うものではなく、また、上記に限らず、API 接続によって目指すビジネスモデルやその固有リスク、各決済事業者の顧客保護等管理規程等に応じて、各決済事業者が独自に必要と判断した事項も加えて実施する必要がある。
- なお、API 接続先が定めた社内規定や銀行等を含めた他の金融機関との API 接続状況等は、上記の適格性の審査に当たっての参考になると考えられる。
- 複数の決済事業者と API 接続する企業等における審査対応負担を軽減する観点から、キャッシュレス推進協議会において、決済事業者が API 接続先の適格性を審査する際に使用する、必須確認項目と独自確認項目からなる「API 接続先チェックリスト」を制定しており、決済事業者はこれを利用することが求められる。
- なお、事前審査は、各決済事業者がそれぞれ独立に行うことを前提としつつも、複数の決済事業者と API 接続先における審査対応負担の軽減や決済事業者による事前審査水準の標準化の観点から、当該決済事業者の責任において他の決済事業者に事前審査を委ねたり、他の決済事業者が既に行った事前審査の結果を参考にしたりすることも考えられる[22]。

ii. モニタリング

- 決済事業者は、API 接続先の適格性について、API 接続後も定期的にまたは必要に応じて確認することが必要である。
- モニタリングの方法、深度、頻度等については、利用者の属性や取引のリスク、各企業等との API 接続によって目指すビジネスモデルやその固有リスク、各決済事業者の顧客保護等管理規程等に応じて、個別に判断されると考えられる。
- 決済事業者は、API 接続に当たって、API 接続先との間でモニタリングに関する事項（例えば、方法、深度、頻度、API 接続先に提出を求める情報、API 接続先が大幅な態勢見直しや業務停止等を行う場合の対応、等）を予め取り決めておくことが必要である。
- 決済事業者は、API 接続先の利用者保護態勢等に関する適格性に懸念があると判断した場合には API 接続先に対して改善を求め、利用者保護の観点から必要な場合には API 接続先のアクセス権限の制限、停止、取消等を行わなければならない[23]。
- なお、モニタリングは、各決済事業者がそれぞれ独立に行うことを前提としつつも、複数の決済事業者と API 接続先におけるモニタリング対応負担の軽減や、決済事業

[22] 本方式を採用する場合の決済事業者間の取決めに係る留意点については、銀行界で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。
[23] ただし、決済事業者が恣意的な判断によりアクセスを制限して API 接続先の事業に影響を与えることのないよう留意する。

者によるモニタリング水準の標準化の観点から、当該決済事業者の責任において他の決済事業者にモニタリングを委ねたり、他の決済事業者が既に行ったモニタリングの結果を参考にしたりすることも考えられる[24]。

iii. その他の留意点

- API 接続先において API 接続を通じて提供するサービスに関して利用者保護に欠ける不祥事案等が発生した場合、決済事業者と API 接続先との関係、利用者からの見え方等によっては、決済事業者側も社会的な批判を浴びる等のレピュテーションリスクが生じる可能性に留意が必要である。
- API 接続先が提供するサービスが決済事業者の提供するサービス（例：Web サービス）を実質的に代替するものであって、かつ決済事業者側も自社サービスの提供を取り止めて、利用者に対して API 接続先のサービスの利用を推奨する場合は、形式上、決済事業者と API 接続先の間に外部委託契約が締結されていなくとも、その実態において同視される可能性があることに留意が必要である。
- API 接続先が提供するサービスが決済事業者の提供するサービス（例：Web サービス）を実質的に代替するものであって、かつ利用者の大部分が当該 API 接続先のサービスの利用に依拠する場合は、API 接続先のシステム障害や業務停止等によって、利用者がサービスを利用することができなくなり、混乱が生じるおそれがあることに留意が必要である。
- 事前の取決めにおいて、API 接続先における障害等によって決済事業者の業務に影響が生じるおそれがある場合には、ただちに決済事業者に連絡するよう定めておくことが必要である。なお、その他の障害等の報告要否やタイミングについても、予め取り決めておく必要があることに留意する。
- API 接続先または決済事業者の都合によるサービス停止を行う際は、一定の事前通知期間を設定することが必要である。

（２） 説明・表示、同意取得

i. 重要な情報の表示、同意取得

- インターネットを利用した取引は、基本的に画面に表示される情報に基づいて利用者の判断・同意が行われ、また、必要な情報を表示しても、利用者が十分に確認せずに、手続きを進める可能性がある。
- そのため、API 関係者は、利用者の判断・同意に必要な情報を単に提供・表示するに留まらず、わかりやすく画面表示するとともに、誤認・誤解を招く表現を避け、また、利用者に重要な判断・同意を求めるものについては注意喚起プロセスを設けることや、

[24] 本方式を採用する場合の決済事業者間の取決めに係る留意点については、銀行界で検討が行われている「共同監査方式」の枠組みが参考になると考えられる。

利用者のシステム操作による同意を求めること等、利用者保護に十分配慮した表示方法、画面構成とすることに努めなければならない。

- 決済事業者は、トークン発行に当たって、少なくとも以下の点について、「インフォームド・コンセント」の考え方に基づき、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。
  ① アクセス権限を付与する API 接続先の名称
  ② 付与する権限に基づいて提供される API 接続先のサービス等の名称
  ③ 付与する権限の内容・範囲
  ④ 付与する権限の有効期限[25]
  ⑤ 付与した権限の削除、解除方法
  ⑥ その他注意喚起が必要な事項

ii. （リスク等に関する表示）

- API 接続先は、提供するサービスに関して生じる主なリスクの適切な表示に努めなければならない。
- API 接続先は、サービス提供時間帯または停止時間帯、休日・休業等のサービス提供上の制約について適切な表示に努めなければならない。

iii. 利用者の誤認防止

- 以下の点については、特に利用者の誤認や誤解が生じるおそれがあることに留意し、適切に表示することに努めなければならない。
  ① API 接続先が提供するサービスは決済事業者が提供するサービスとは異なること
  ② 決済事業者と API 接続先の関係、それぞれの役割
  ③ 決済事業者と API 接続先の画面の区別
- なお、決済事業者は、API 接続先が虚偽または意図的に誤認を招く表示を行っていることが判明した場合には、API 接続先に対して是正を求め、利用者保護の観点から、必要な場合には API 接続先のアクセス権限の制限、停止、取消、関係当局への通報等の必要な措置を講じなければならない。

iv. その他の表示

- API 関係者は、利用者からの相談・照会、苦情、問合せがあった場合の役割分担、業務フロー等を、予め取り決めておくことが必要である。
- API 関係者は、上記の取決め内容を踏まえ、利用者からの相談・照会、苦情、問合せに対応するための連絡先を表示することが必要である。
- API 接続先は、商号、代表者、住所、連絡先等について表示することが必要である。

[25] リフレッシュトークンを発行する場合には同トークンによって延長される最大の有効期限。

- API 接続先は、電磁的方法による決算公示を選択している場合、会社法に基づく決算公告についても表示することが必要である。

（３） 不正アクセスの未然防止

- API 接続先は、不正アクセスを未然に防止する観点から、例えば以下の点について、利用者に注意喚起することに努めなければならない。
  ① API 接続先のログインパスワード等は、決済サービスに利用しているパスワード等と異なるものを設定すること
  ② API 接続先のログインパスワード等は、類推されやすいものを避けること、適切な管理に努め、第三者に貸与、開示しないこと[26]
  ③ ウィルス対策ソフトを導入すること
- API 接続先は、利用者に対して、API 接続先のパスワード等の紛失、漏洩や不正アクセスの懸念がある場合には、ただちに API 接続先に対して連絡するよう求めておくことが必要である。

（４） 被害発生・拡大の未然防止

i. 初動対応

- 決済事業者または API 接続先において不正アクセス等が判明した場合、被害発生・拡大を未然に防止する観点から、速やかに、決済事業者においてはアクセス権限の制限、停止、取消を、API 接続先においてはサービス利用の制限、停止を行うことが必要である。
- 決済事業者と API 接続先双方において速やかに機能制限、停止、その他必要な措置を行う観点から、一方で API に関連した不正アクセス、情報流出・漏洩が判明した場合にはただちに他方に連絡することとし、その場合の連絡先や連絡方法等を決済事業者と API 接続先間において予め取り決めておく等、被害拡大防止に向けた必要な態勢を整備しておくことが必要である。
- API 接続先が複数の決済事業者と接続している場合において、他の決済事業者においても同様の事案が発生するおそれがある場合には、API 接続先は当該他の決済事業者に対してもただちに連絡し、被害拡大を未然に防止することに努めなければならない。

ii. 利用者への連絡

- 被害が発生した利用者への連絡や、被害が広範な利用者に及ぶ可能性がある場合に、

---

[26] パスワードの定期的な更新も方策の一つとして考えられるが、米国国立標準技術研究所（National Institute of Standards and Technology）において、セキュリティ対策のライフサイクルが研究されおり、その中で定期的なパスワードの変更がかえってセキュリティレベルを下げることが指摘されている。変わりに 64 文字以上のパスフレーズの利用が提案されており（https://pages.nist.gov/800-63-3/sp800-63b.html）、利用者利便とセキュリティレベルの確保とのバランスにおいて検討されることが期待される。

関係する全ての利用者にただちに十分な注意喚起（例えば、ただちにパスワード等の変更を求める等）ができるよう、API 接続先は、利用者との連絡手段を予め確保しておくことが必要である。

- 利用者に届出・登録を求める連絡手段の範囲については、提供するサービスの内容や取引のリスクに応じて、個別に判断されると考えられる。
- 決済事業者は、API 接続先が利用者との十分な連絡手段を予め確保することができない場合、被害発生時に、決済事業者が API 接続先に代わって利用者に対し連絡、注意喚起する必要が生じる可能性に留意することが必要である。

（５） 利用者に対する責任・補償

- オープン API では、API 接続先と決済事業者の双方が関与するため、情報流出やシステム上の不具合等により利用者に損害が発生した場合、利用者に対する責任の所在や、対応窓口・主体等が不明確になるおそれがある。
- 当事者の民事上の最終的な損害賠償責任を司法の判断に委ねた場合、速やかな被害回復、補償等が図られず、利用者保護に欠けるおそれがある[27]。

i. 当事者間における事前の取決め

- API 関係者は、利用者に対して速やかな被害回復、補償等を図る観点から、不正アクセスや情報流出、不正利用、システム上の不具合等が発生した場合の対応窓口や、利用者に損害が生じた場合の補償方法（含む、その主体）[28]、補償範囲について、予め取り決めておかなければならない[29]。なお、利用者に対して双方とも責任を負わない等の利用者保護に著しく欠ける取決めは、行ってはならない。
- API 関係者は、予め取り決めた、利用者に損害が発生した場合の対応窓口や問合せ方法について、ウェブサイト等において利用者が常時確認することができるよう表示するとともに、API 接続先が利用者と利用契約を締結する際にわかりやすく画面表示する等により、利用者が十分認識することができるよう努めなければならない。
- 法人顧客については、消費者と比較して、セキュリティ対策等への対応力が相対的に高いと考えられる。利用者の利用環境やセキュリティレベルを原因として不正利用される可能性がある中では、API 関係者側のセキュリティ対策に加え、利用者においてもセキュリティ対策を講じ、不正利用被害の防止に努めていくことが重要であると考えられる。こうした点を踏まえ、法人顧客に対する補償については、利用者が行って

---

[27] なお、本節における記述は、API 関係者が利用者保護の観点から自主的に行うことが期待される取組みであり、それぞれの利用者に対する最終的な法的責任を加重または軽減するものではない。

[28] 利用者への補償後の、決済事業者と API 接続先の間の内部分担（求償）についても、別途予め取り決めておくことが望ましい。

[29] API 関係者が利用者に対して連帯して責任を負うこととする場合でも、利用者から見て対応窓口・主体等がわかりにくくなるおそれがあることから、任意の一次的な補償方法（含む、その主体）等について、予め取り決めておくことが望ましい。

いたセキュリティ対策や不正利用被害の防止に関する状況、法人顧客の属性やセキュリティ対策への対応力、個別の利用契約等の点を考慮して、個別に判断されることが必要である。

ii. 補償内容・範囲に関する考え方

- API 接続先の提供サービスによる利用者の金銭的損害について、API 関係者に過失がない場合でも、利用者が個人であって利用者自身の責任によらずに被害に遭った場合については、上記事前の取決めに基づいて決済事業者または API 接続先から補償を行うことが必要である。なお、利用者に重大な過失または過失がある場合については、被害に遭った利用者の態様やその状況等を加味して、全額あるいは一部を利用者負担にすることも含め、個別に判断されることが必要である。
- API 関係者は、サービスの形態や利用者の属性等に鑑みて、上記と異なる補償内容・範囲とすることに合理的な理由がある場合であって、かつ利用者に不測の損害が生じないよう、かかる補償内容・範囲について利用者に適切に説明または表示した場合に限り、補償内容・範囲を個別に定めることができる。

iii. API 接続先が補償責任を負う場合の留意点

- 決済事業者と API 接続先との間の取決めに基づき API 接続先が利用者に対して補償責任を負う場合、決済事業者は、API 接続先の利用者に対する補償に係る態勢や資力等が利用者保護に欠けるおそれがないかに留意の上、API 接続の是非を判断するとともに、それらの状況について定期的にまたは必要に応じて確認することが必要である。
- 決済事業者は、API 接続先の補償に係る態勢や資力等が利用者保護に欠けるおそれがあると判断した場合、API 接続先に対して態勢の見直しや責任財産の充実、責任保険への加入を求め、API 接続先においてそれが困難な場合は API 接続しない（あるいは接続の停止または取消を検討する）等の対応を行うことが必要である。
- API 接続先の利用約款等において API 接続先の免責事由が過大に定められている等（例えば、過失責任も負わない等[30]）、実質的に利用者に対する補償責任が果たされないおそれがある場合、消費者契約法等を踏まえ、見直しを求めることが必要である。

3.5 その他

（１） 公表情報の取扱い

- 店舗や提供する決済サービスの種類等、決済事業者のウェブサイト等においてログイ

[30] なお、事業者の債務不履行により消費者に生じた損害を賠償する責任の全部を免除する条項や、当該事業者、その代表者またはその使用する者の故意または重大な過失による事業者の債務不履行により消費者に生じた損害を賠償する責任の一部を免除する条項等は、消費者契約法（第８条乃至第 10 条）に基づきそもそも無効とされる。

ン等の手続きを要さずに取得可能な公表情報（以下「公表情報」）を API 接続先に提供する場合は、上述の記載にかかわらず、以下の取扱いとすることが考えられる。

① 決済事業者と API 接続先との通信経路において改竄が行われることを防止する観点から、決済事業者と API 接続先との通信方式は、セキュリティ原則「3.3（２）外部からの不正アクセス対策」に定める通信方式に拠るものとする

② API 接続先は、システム上の不具合や外部または内部からの攻撃による改竄等によって、決済事業者に利用者からの問い合わせが行われる可能性のある事態が発生した場合には、ただちに関係決済事業者に対し連絡するよう努めなければならない

③ 決済事業者は、API の利用約款等において、不具合発生時等の責任について予め定めておくことが望ましい

④ 決済事業者は、公表情報を提供する API のアクセス量を決済事業者側でコントロールすることができない場合には、システムキャパシティの超過が原因で不具合が発生するリスクに留意するものとする

（２） 「API 接続先の API 接続先」の取扱い

- API 接続先は、利用者が認める範囲において、API 接続で決済事業者から取得した利用者のデータを API 経由で他のサービス提供者、「API 接続先の接続先」（以下「API 連鎖接続先[31]」）へ提供する場合がある。決済事業者は、API 接続先との間で API 連鎖接続先の取扱いについて予め取り決めておくことが必要である。
- これには、例えば、API 接続先と同様に取扱う（決済事業者が API 連鎖接続先と直接契約を締結）、API の連鎖接続について決済事業者の承諾または決済事業者への事前通知を条件とする、連鎖接続を許容する条件を双方協議のうえ予め定める、API 接続先の責任と管理の下で連鎖接続を許容する等、様々な方法が考えられる[32]。
- いずれの方法による場合であっても、API 連鎖接続先において、本原則の趣旨を踏まえて、十分なセキュリティ対策と利用者保護が図られていることが重要である。
- なお、API 接続先が有する自社の情報を同接続先の API を通じて他の事業者等に提供することは、API の連鎖には該当しないが、個人情報保護法等に基づき適切な利用者保護が図られる必要があることに留意する。

[31] API 接続先が決済事業者から取得した情報を、API 接続先と API 接続する他の事業者等が参照する場合における、当該他の事業者等をいう。

[32] API 連鎖接続先の取扱いは、例えば、API 連鎖接続先が API 接続先と同一グループに属するか否かによって異なる取扱いとすることも考えられる。

4 関係法規制、ガイドライン等との関係性

4.1 既存法規制との関係性

（１） 割賦販売法との関係性

i. オープン API の導入に関する強制力

- 銀行業界では、銀行法の改正により、オープン API 導入に関する努力義務が課せられている。このように、法規制の改正によるオープン API の社会的普及を図ることも、採りうる方策であると考えられる。
- クレジットカード取引等を規制する割賦販売法においては、現時点でオープン API の導入に関する法改正等は予定されていない。そのため、決済事業者におけるオープン API の導入は、各決済事業者の個別戦略に基づく判断に委ねることとなる。

ii. 自主規制団体の必要性

- 割賦販売法では、日本クレジット協会が認定割賦販売協会として認定され、当該協会が自主規制団体としての機能を有し、適正なクレジットカード取引の実現を目指している。
- 他方、API 接続先においては、銀行法が定める認定電子決済等代行業者協会と類似の団体は存在しない。この点において、API 提供側、利用側双方における対等な関係性や業界間の効率的な環境整備の観点から、同様に適正な API 接続の実現を目指す観点から、FinTech 企業等の API 接続先側において業界の意見をとりまとめる仕組みの検討が望ましい。現在は、キャッシュレス推進協議会が当該役割を果たしているが、自主規制団体の位置づけにはなっていないため、継続的に枠組みの検討が必要である。

（２） その他の法規制との関係性

- オープン API の普及により、企業における情報の利活用が促進されることが想定される。そのため、個人情報保護法が定める規制および法の目的に沿った対応が求められる。他方、個人情報の利活用によるビジネスは未だ発展途上にあり、かつオープン API を活用したサービスやその利用者、決済事業者、API 接続先等の関係当事者間の適用関係や法的責任については、サービスの態様等に応じて個々に判断されるものであるため、本ガイドラインでは個人情報保護法の適合を保証するものではなく、関係各団体における個別の検討が求められる。
- また、景品表示法、消費者契約法等のその他の法令および関連するガイドラインについても、個別の提供サービスに応じた、決済事業者、API 接続先双方の対話による適切な対応が求められる。

4.2　既存ガイドラインとの関係性

（１） 銀行業界におけるガイドライン

- 本ガイドラインは、銀行業界におけるガイドラインと言える、全国銀行協会公表の「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－」を参考にしつつ策定している。
- API 接続先においては、決済業界のみならず、銀行業界とも API 接続を行うケースが容易に想定され、本ガイドラインへの対策と同時に銀行業界のガイドラインへの適合も求められるところである。
- そのため、本ガイドラインの改訂においても、銀行業界における検討、ガイドライン改訂に十分配慮して行った。引き続き、我が国として銀行業界のガイドラインの方向性、考え方と足並みを揃えてガイドラインをメンテナンスすることが必要と考える。

（２） セキュリティ、利用者保護に関するガイドライン

- 本ガイドラインで定める API に関する各規約は、クレジットカードの PAN 情報および ID/パスワードを取り扱わない前提としているため、日本クレジット協会が事務局を務める「クレジット取引セキュリティ対策協議会」による「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」には該当しないが、PAN 情報および ID/パスワードを取り扱う場合には、本実行計画を参考とすべきである。
- また、今後の本ガイドラインの改訂において、クレジットカード業界と共通の対策が求められると判断された場合は、クレジット取引セキュリティ対策協議会が求める対策が本ガイドラインに盛り込まれることが期待される。

5 今後の取組み

5.1 API 仕様の標準化に関する取組み

（1） 電文の標準化

- 諸外国における事例を見ても、さらなるオープン API の利活用に向けて、電文の標準化は整備が必要な事項の一つであると考えられる。
- 我が国の現状においては決済事業者間の管理するデータ内容、使用している電文等の乖離もあることから、統一的な電文の制定には時間を要すると想定し、電文仕様に関しては、段階的に進めることを目指すとしてきた。
- これを受け、キャッシュレス推進協議会における 2018 年度のプロジェクトを通じ、クレジットカードに関する参照系 API の標準電文およびコード決済用 API の標準電文が制定された。
- 本ガイドライン第 1 版においてはクレジットカードの参照系のみを対象としていたが、既にコード決済を中心に広まりつつある更新系や、事業者からの要望があった認証系についても、今般規定したものである。このため、コード決済以外の更新系や認証系 API に関しても、既に制定されたクレジットカードの参照系 API の標準電文や、コード決済用 API の標準電文を参考にして、実現を目指す必要があると考える。
- また、このような検討に際しては、我が国の現状だけに着目するのではなく、API 連携が国内企業とのみに留まらず海外企業との連携が行われる可能性もあること、また、我が国の仕組みを海外に展開していくことも考慮し、グローバルな視点に立って、検討されることが望まれる。

（2） その他の仕様の標準化

- 現時点では API 関係者として、イシュアである決済事業者と FinTech 企業等が想定されているが、銀行等の金融機関、事業会社による API の利活用も、相応のニーズがあるものと考えられる。
- そのため、今後の検討においては、利用主体の拡大に向けた議論や、まだ実例が出てきていない新たな分野における積極的な検討が期待される。
- このような新しい分野の検討に際しては、利用者ニーズへの対応が重要なことは言うまでもないが、利用者ニーズの存在を待っていては、必要なタイミングでサービスを提供できなくなる可能性も存在する。そのため、将来的なニーズへの対応、業界によるニーズの喚起という点にも着目し、できるだけ早期に検討を進める必要がある。
- また、各社間の API 連携をより円滑に実施するために、クレジットカードの参照系については、決済事業者と API 接続先の標準的な契約雛形も、キャッシュレス推進協議会のプロジェクトを通じて、契約の参考案が提示された。今後、参照系以外について

も、関係業界全体で検討されることが望ましい。

- さらに、このような検討に際しては、電文の標準化と同様、グローバルな視点での検討が行われることを期待する。

5.2 セキュリティ対策、利用者保護対策に関する取組み

- セキュリティ、利用者保護等については、一定程度の自由裁量を認めつつも、業界として合意することができる範囲で、より具体的な内容の検討や時代に応じた検討が求められる。また、技術の進展や消費者意識の変化に応じた、タイムリーな対応も併せて求められる。
- 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上、オープン API は、決済事業者が他の事業者等に対して自社システムとの接続口を提供する仕組みであるため、仮に API のシステムに脆弱性があった場合、システムトラブルや最悪の場合、不正利用や顧客情報の情報流出等が生じるおそれがある。
- オープン API に関連する技術は、技術的進展や利用者ニーズに応じ変化していくことに鑑みれば、個別の決済事業者での対策に加え、業界・企業横断的にも、不正アクセス事案やセキュリティ関連対策について、情報セキュリティ関連機関と連携して情報共有等を行う枠組み等を整備し、決済事業者、API 接続先におけるセキュリティ対策の継続的な改善、見直し、高度化を後押ししていくことが重要である。
- かかる観点から、FISC や金融 ISAC、FinTech 協会等において業界全体のセキュリティ対策の底上げに向けた検討がなされているところであり、このような活動が、我が国決済業界における安全かつ利便性の高いオープン API の取組みの後押しとなることを期待する。
- また、このような検討に際しては、我が国の現状だけに着目するのではなく、API 連携が国内企業とのみに留まらず海外企業との連携が行われる可能性もあること、また、我が国の仕組みを海外に展開していくことも考慮し、グローバルな視点に立って、検討されることが望まれる。

5.3 業界間の協業・連携にむけた取組み

- 本ガイドラインの改訂にあたっては、キャッシュレス推進協議会の参加メンバーを中心に、決済事業者やクレジットカード業界、FinTech 業界等の決済 API に関連する多くの業界関係者の協力を頂いている。策定の過程において、各業界が対等な立場で意見交換できたことは、単にオープン API の導入だけではなく、我が国におけるキャッシュレス社会の実現に向けて有益であったと言える。
- さらに、決済業界において、利用者利便に資する API 活用サービスに向け、利活用しやすいデータの流通を目指した、継続的な検討が期待される。

- 我が国におけるキャッシュレス社会の実現、促進に向けた推進母体として、キャッシュレス推進協議会が発足しており、今後は、キャッシュレス推進協議会において、各業界が対等な立場で意見交換を行い、社会全体として、オープン API　の発展、キャッシュレス社会の実現に向けた検討が進むことが望まれる。
- キャッシュレス推進協議会においては、銀行業界やその他のオープン API に対する取組み、海外における同様の取組みとの調和も意識した検討が必要とされる。

5.4　本ガイドラインの改訂方針

- 本ガイドラインは、時代のニーズや技術の進展、関係法令等の改正に応じた、恒常的な改訂が必要である。関係各業界の貢献を期待しつつ、キャッシュレス推進協議会において、継続的な改訂を行うものとする。
- 改訂に際しては、内容が陳腐化しないよう、最低でも 1 年に 1 度は改訂の検討が行われることが望ましい[33]。

5.5　継続的なコミュニケーション、エコシステムの形成に向けて

- 本ガイドラインが与える影響は、単に決済事業者や FinTech 企業等に閉じず、加盟店や一般事業会社、データ利活用企業、さらには一般消費者等、多岐に及ぶ。そのためキャッシュレス推進母体においては、広く意見を集約することができる機能の具備が必要であると考える。
- オープン・イノベーションの活性化に向けては、決済事業者によるオープン API の取組みのみならず、他の事業者等においてもオープン API の取組みが進展し、決済分野に限らず、様々な事業者の間で価値のある情報が相互にやりとりされていく生態系（API エコシステム）が形成されていくことが重要である。
- キャッシュレス推進協議会においては、API エコシステムの形成に向けて、オープン API の利用状況を定期的に把握するとともに、技術の進展や社会情勢、利用者や API 関係者のニーズに応じ、本ガイドラインに基づく決済 API のさらなる普及に向けた必要な対応が検討されることが望まれる。
- 決済業界や銀行業界等の取組みを契機に、他の金融以外の分野も含めたオープン・イノベーションの議論に発展することを期待する。また、本ガイドラインの定める API の活用が、我が国における安心・安全なキャッシュレス化の一助になれば幸いである

[33] 2019 年度については、特に要望の多かった認証系について、銀行業界などとも足並みを揃えながら早期に検討を開始することが望まれる。例えば、新年度開始後 6 ヶ月程度で、検討是非を確認することが考えられる。