資料2

NTT DATA
Global IT Innovator

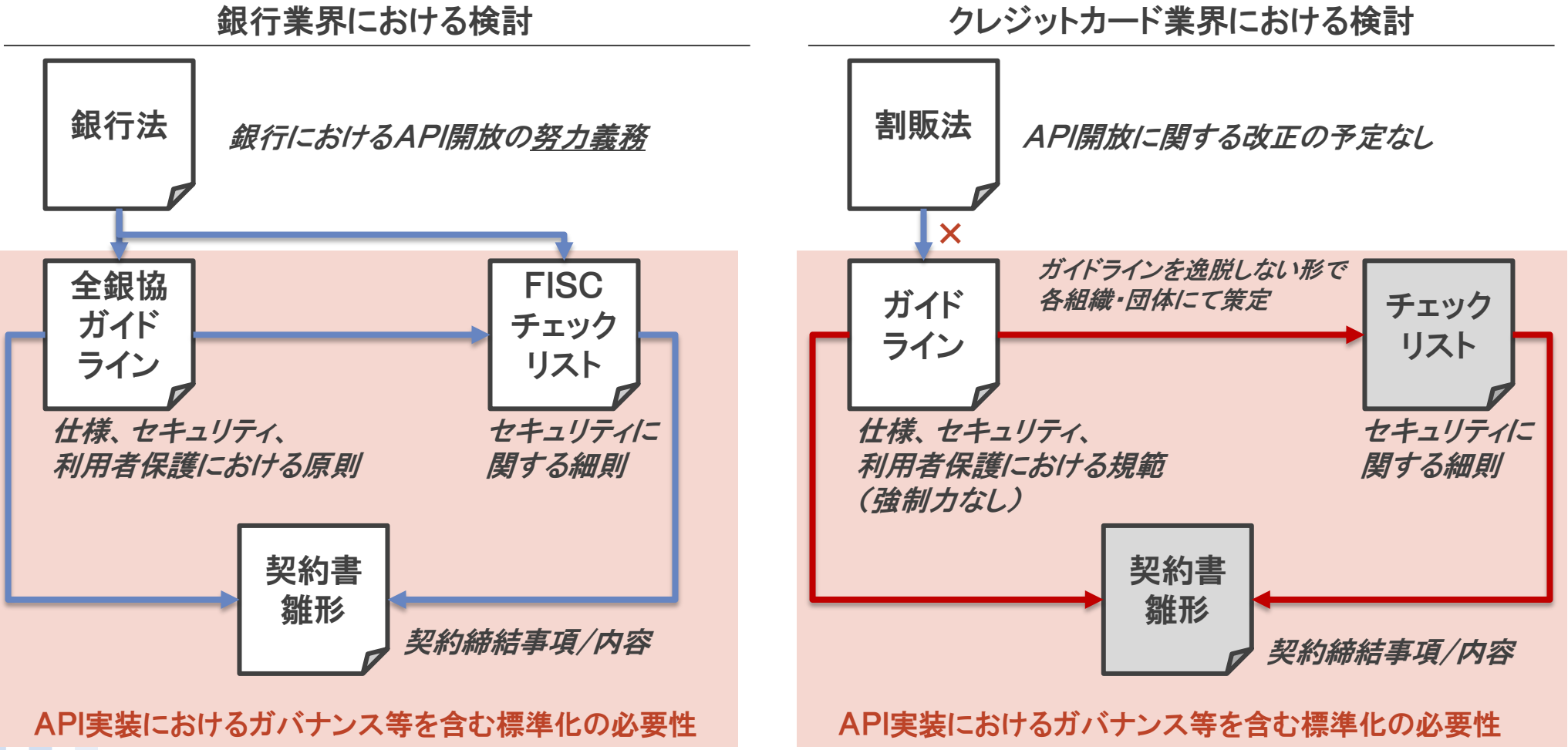
第七回　クレジットカードデータ利用に係るAPI連携に関する検討会
API連携検討資料（APIガイドライン）

2017年12月11日

株式会社NTTデータ経営研究所
グローバル金融ビジネスユニット

ガイドラインの前提

本ガイドラインは、クレジットカード会社におけるAPI開放を強制付けるものではなく、クレジットカード会社が個社の判断においてAPIを開放する場合に、規範となる事項を取りまとめるものである。



今年度の射程（案）

事務局として、今年度作成するガイドラインについては、射程範囲を下記のように分類して考える。
API-SWGでは、API利用者側でPAN情報及びID/PWを扱わない前提での策定が検討された。

分類	射程内	射程外
適用範囲	• 参照系API • PAN情報、ID/PWを扱わない業務 • 外部との連携を行うすべてのAPI • イシュアが開放するAPI	• 更新系等、その他のAPI • PAN情報、ID/PWを扱う業務 • 機関の内部に利用が閉じたAPI • アクワイアラ、加盟店、FinTechが開放するAPI
仕様標準化	• 開発原則 • 通信プロトコル、表現形式等のすでに一定程度の標準がデファクトとして存在する事項	• メッセージフォーマット、メッセージ内容 （ただし、今後の標準化に向けた期待は示す）
セキュリティ対策	• 接続先審査の必要性及び観点 • リスクの提示、及び対応方針 • OAuth2.0/OpenID Connect、TLS等 一定程度の標準がデファクトとして存在する事項	• 接続先審査の具体的項目 • リスクに対する具体的な対応手法 • 認証、暗号化、PCI-DSS等のセキュリティ対策 （今後の検討で整理）
利用者保護対策	• 接続先審査の必要性及び観点 • 顧客への説明事項 • リスクの提示、及び対応方針	• 接続先審査の具体的項目 • 顧客被害への対応、当事者間の負担割合 （関係者の合意が得られる部分は射程内） • リスクに対する具体的な対応手法
その他	• 継続的なガイドラインの更新方針	• コスト、手数料等の金銭に関する事項

セキュリティ対策において想定されるリスク

関係企業：
クレジットカード会社及び当該クレジットカード会社とAPI接続を行っているFinTech企業等

発生者	• 外部者（内部環境にアクセスできない者） ✓ 利用顧客 ✓ 第三者	• 内部者（内部環境にアクセスできる者） ✓ クレジットカード会社役職員 ✓ FinTech企業等役職員 ✓ 外部委託先役職員
発生場所	• 外部環境（関係企業の管理下にない場所） ✓ 公衆ネットワーク（API通信時） ✓ 利用者顧客端末（API利用アプリ使用時） ✓ 外部者の生活拠点 ✓ 委託先の拠点/システム/ネットワーク	• 内部環境（関係企業の直接的な管理下にある場所） ✓ 関係企業の拠点 ✓ 関係企業のシステム（API基盤等） ✓ 関係企業のネットワーク ✓ 契約上管理下にあるシステム/ネットワーク（API基盤等）
動機	• 故意的 ✓ 営利目的 ✓ 営業妨害 ✓ その他意図	• 偶発的 ✓ オペレーションミス ✓ うっかり ✓ 失念
対象資産	• 資金 ✓ 顧客資金 ✓ 関係企業資金	• データ ✓ 企業情報 ✓ 個人情報 ✓ システム関連情報（トークン等） • その他有形/無形資産 ✓ 固定資産（サーバー等） ✓ 紙媒体の文書

赤字は、クレジットカード会社にとって、API公開により新たに発生するリスク要因

利用者保護対策において求められるルール

個人情報保護法、景品表示法、消費者契約法等の既存法規制については触れない

API活用サービスの特徴	• 不特定多数の利用者が活用用する • サービス提供の基礎となるAPIを始めとする技術要件が一般利用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 • 対面でのサービス提供が行われない • 本来のサービス提供者（クレジットカード会社）と、直接のサービス提供者（FinTech企業等）が異なる
サービス提供に向けた説明義務	• 高齢者、未成年者、障がい者、スマートフォンアプリに未習熟な利用者等、利用者の理解度に応じた説明が必要 • サービス提供に向け、電話相談等、必要に応じた対面相当での説明機会を用意 • トークンの発効においては、当該トークンによる提供情報、FinTech事業者等が実施できる業務範囲を明示 • サービス提供者が誰（クレジットカード会社、FinTech企業等）であるのかが容易かつ継続的に把握できる必要 • 書面交付は求めないが、利用者の承諾、提供を受けるサービス内容が事後も確認できる必要 • 利用者の承諾時における、自由な意思の確保
契約関係からの離脱	• 関係企業の都合によりサービスが終了する場合において、事前通知、必要な対応方法が示される必要 • 法人と個人とでは、契約やサービス内容に対する習熟度に違いがあることから、一定程度の異なる対応も認める • 利用者が本来のサービス（クレジットカード会社の提供サービス）契約から離脱することで、付随するサービス（FinTech企業等が提供するサービス）への対応が必要か • 利用者保護上の問題が生じた場合に、本来のサービス提供者（クレジットカード会社）が採りうる措置は何か
販売勧誘活動	• 誤認防止に向けた対応が必要
苦情・相談体制	• 利用者における苦情・相談は、直接のサービス提供者が担う必要 • 関係企業の一方のみで解決できない苦情・相談がある可能性も含め、関係企業間における役割分担、情報連携のあり方を事前に取り決めておく必要 • 利用者に財産的損失が発生する可能性も含め、利用者への補償、相手方関係企業に対する求償のあり方を事前に取り決めておく必要

その他のステークホルダーのご意見

- ビジネスの実現に向けて、実際の契約をイメージした内容とした方がよいのではないか。
  → クレジットカード会社の多様性を考慮しつつ、関係者間で合意できる範囲内で、できるだけ具体的な記載とする

- 電子決済等代行業者（銀行API利用者）であればセキュリティ等の対応が満たされていると考えられるので、クレジットカードAPIの利用においても、同様に理解され、簡易な事前審査等とできないか。
  → 銀行APIのチェック事項を参考にしつつ、共通化できる部分は極力共通化することで、社会全体の効率化を図ることとしたい。ただし、クレジットカード業務独特の確認事項がある場合は、その限りではない

- クレジットカード会社（イシュア）が保有する情報は、加盟店のデータを反映しているということをご理解いただきたい

- 基本的に、クレジットカード会社がWebサービスとして利用者に提供している情報はAPIを介して提供可能と考える
  → 一方、クレジットカード会社のWebサービスの整備状況は区々であり、一律的な要求や対応は困難と考える

【参考】ガイドラインの目次案

ガイドラインの目次案

今後の取組に向けた記載方針（案）

銀行APIでは、認定電子決済等代行事業者協会と全国銀行協会等の銀行業界団体との連携によるガイドライン等のメンテナンス、状況の把握が行われることが想定される。
クレジットカード業界ではどのように対応すべきか。

API仕様の標準化に関する取組	電文及び電文内容の標準化の必要性は共通理解として存在する。 現状の課題及び解決の方向性を示すことで、今後のシステム更改時の参考としていただく。
セキュリティ対策、利用者保護対策に関する取組	技術や社会の進展により、セキュリティ対策や利用者保護対策も変化していくと考えられる。 継続的な求められるセキュリティ対策や利用者保護対策の把握が必要。
業界間の協業・連携にむけた取組	キャッシュレスに向け、民間の各業界団体等が、定期的かつ継続的に対話できる環境を整える
本ガイドラインの改訂方針	上記環境の下、本ガイドラインの知的財産権の管理を移転し、当該環境下での継続的なメンテナンスを行う
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	将来的に、対話の環境を拡げ、銀行系、電子マネー系、テクノロジー系も含めた、我が国におけるキャッシュレス推進母体とすることが望ましいのではないか

今後の進め方

ガイドラインの検討は、次回検討会にてファイナルドラフトのご確認をいただきます。
そのため、1月上旬にAPI-SWG #2の開催を検討いたします。

検討会	検討内容
第五回	• ガイドラインの作成方針検討 ✓ ガイドラインの位置付け ✓ 「参照系」「更新系」の分類、及び「参照系」の先行着手に関する是非 ✓ 目次案に関する是非
第六回 (11/20)	• 第1章、第2章の案提示、検討 • 第3章策定に向けた、想定リスクの提示、検討
本日 第七回 (12/11)	• FinTech企業、カード会社において求められる措置・体制の提示、検討 • 第2章、第3章における、ステークホルダーの意見集約 • 第4章、第5章の記載ポイントの提示、検討
第八回 (1/23)	• ファイナルドラフトの提示、検討 • 今後の進め方の確認

ガイドラインに関する
案及び意見集約
（API-SW #1）

事務局案に対する
詳細検討
（API-SW #2）

NTT DATA

Global IT Innovator