「非対面クレジットカード取引のセキュリティ向上に向けた取り組み」

～本人認証技術の非対面取引への普及促進にむけて～

調査報告書「公表版」

2021 年 3 月

日本クレジットカード協会

＜受託会社＞

株式会社エヌ・ティ・ティ・データ経営研究所

目次

1. はじめに

日本のクレジットカード利用環境は、割賦販売法の改正を経て、情報漏洩件数の減少、偽造カードによる不正使用被害額の減少等、一定の効果が現れているが、非対面取引の不正使用は増加が続き、2019 年の被害額は 222 億円、総被害額は 273 億円で高止まりとなっている。

割賦販売法の実務上の指針であるクレジットカード取引セキュリティ対策協議会のセキュリティ・ガイドラインでは、本人認証、券面認証、属性・行動分析、配送先情報の 4 方策による不正使用対策が実施、推進されているが、残念ながら被害は高止まりしたままである。

日本クレジットカード協会では、このような状況を踏まえて足元の 3D Secure や Tokenization の活用などの不正使用防止策検討と並行し、国内外の取組事例、先端技術の活用事例等の調査を行い、中長期的な視点に立った将来的な不正使用防止策の普及促進策を検討する必要があると考え、本調査及び研究を実施した。(足元の不正使用防止対策は認識したうえで、本報告書上では将来的な不正使用防止策を前提に整理したもの)

具体的には、今後取りうる非対面取引での不正使用防止のための対策手法を概観するため、カード会員の負担や抵抗感が少ない汎用的な本人認証の仕組みをはじめとする国内・海外での先端的取組事例等を調査し、中長期的な不正使用対策への活用を展望した日本での実装・普及に向けた課題の抽出、及び解決策を検討した。

なお本報告書は、今後カード会社各社や業界が不正使用被害の対策を検討するにあたり、その取り組みの方向性等を考えていく際の参考情報として活用される事を想定したものである。

本調査では、今後非対面取引の不正使用被害防止に効果が期待できる方策として、「非対面取引におけるスマートフォンの生体認証機能の活用」、「SMS やプッシュ通知等によるカード利用時の利用確認」、「イシュア等の提供情報による加盟店での対策」の 3 方策を選定し、分野を問わない国内外の本人認証活用事例調査も加えた計 4 方策の調査を行った。

(1) テーマ①：非対面取引におけるスマートフォンの生体認証機能の活用

・非対面取引での不正使用は、偽画面への誘導によりカード会員本人による ID、PW、セキュリティコードの漏洩などもあり、これまで通りの会員の記憶に基づく本人認証だけでは不正使用の防止効果が期待できなくなっている。

・このような環境のなか、既にスマートフォンに標準搭載されておりカード会員にとっても馴染みがあると考えられる生体認証機能を汎用的な認証の仕組みとして導入することで、カード会員の負担や抵抗がなく不正使用防止を期待するもの。

(2) テーマ②：SMS やプッシュ通知等によるカード利用時の利用確認

・現在一部のイシュアで導入されている「利用後の通知」では不正使用発生を完全に抑えることが困難であることから、「利用時の通知」に「本人認証プラス本人が承認する仕組み」を作ることで不正使用防止効果を期待するもの。

(3) テーマ③：イシュア等の提供情報による加盟店での対策

・国内においては、一部のイシュアによる非対面取引での「不正配送先情報」のデータベースが、一部の加盟店に提供されている。

・しかし、イシュアが限られていることや、加盟店の使い勝手の問題等の理由により十分な効果が得られるとは言い切れない状況である。

・そのため、不正取引情報をより多くのイシュアから集約・分析を行ったうえで、不正なカード取引をシステム的に検知して、オーソリへの反映や加盟店との迅速な情報共有による不正使用防止効果を期待するもの。

(4) テーマ④：その他、本人認証等についての国内外成功事例

・決済分野に限定せず、広い分野での非対面本人認証技術を調査し、それらの活用可能性を検討するもの。

なお本報告書を閲覧頂く際には、以下の点にご留意願いたい。

① 情報の時点

内容は調査時点（2020 年 6 月～8 月）のものとなること。

② 情報の正確性

事業者への直接ヒアリングはしていないこと（公開情報が中心となる）。

③ 各検討内容のカード会社への適応性

各検討内容の適応性は、カード会社個社の仕組みによって異なること。

2. テーマ①：非対面取引におけるスマートフォンの生体認証機能の活用

本テーマでは、現在本人認証の主流となっている ID・PW の課題を解決し、非対面取引でカード会員の負担が少ない生体認証を利用する方策の調査を行った。

(1) 生体認証の特徴

本人の認証方法には、「記憶」「所有」「生体」によるものがある。

クレジットカード決済では、主に「記憶」（パスワードなど）によるものが中心であり、「忘れてしまう」「騙されて教えてしまう」といった課題があったが、「生体」では「記憶する必要がない」「騙されても教えようがない」に加え「本人固有のもの」という特徴がある。近年、生体認証はスマートフォンでも使われており一般に使い慣れたものとなっていることから、（セキュリティ強度の向上だけでなくカード会員の使い勝手を含め）カード決済時の本人認証方法として期待できるものと考えられる。

(2) カード決済時の本人認証に適した生体認証

現在、一般的に生体認証の方法には以下の 13 種類が存在する。クレジットカード取引での本人認証では、「認識精度」「永続性」などが優れ、スマートフォンに既に実装されており、新たな認証装置が不要な「指紋」「静脈」「虹彩」「顔」の 4 種類が適している。

（13 種類の生体認証）[1]

身体的特徴：指紋、静脈、虹彩、顔、掌形、音声、耳形、体臭、瞬き

行動的特徴：歩行、筆跡、キーストローク、リップムーブ

(3) スマートフォンを使った生体認証の方法

「カード会員の利便性」「各カード会社の導入負荷」「早期かつ広範な普及」の観点から、パスワードレス認証の国際的な標準化団体である FIDO Alliance（ファイド・アライアンス）が作成したスマートフォン等での生体認証の方法を定めた FIDO・FIDO2 という仕様[2]の活用を検討した。本仕様を活用することで、新たな認証方法を開発することなく効率的に実装が可能である。

なお、FIDO には FIDO/FIDO2 という 2 つの規格があり、それぞれネイティブアプリと Web ブラウザ向けの仕様[3]が策定されている。非対面取引では、①端末のロック解除、②サービスへのログイン、③サービス内での利用承認のうち②と③で使用する。

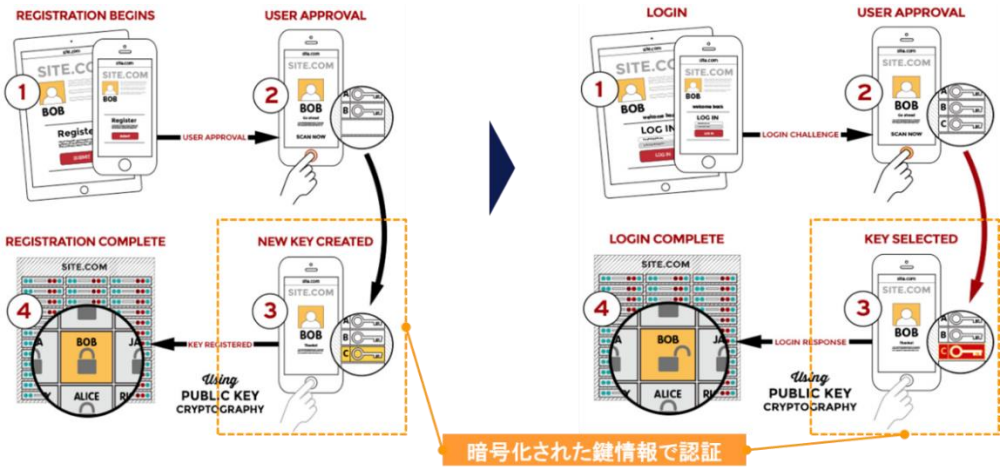
---

[1] 既にスマートフォンに実装されている生体認証機能を導入することで、カード会員の負担や抵抗がなく収集、活用することができる。

[2] FIDO Alliance は、2012 年に Paypal や Lenovo など 6 社が中心になって、パスワードに拠らないより安全な認証技術の標準を策定するために設立され、現在はクレジットカード国際ブランドを始め、日本でも金融機関やカード会社・通信事業会社を始め、多くの企業が参加している。

[3] ネイティブアプリは、各 OS 開発企業が提供するアプリストア等を通じて入手し、スマートフォンにダウンロードする利用方式であるのに比べ、Web ブラウザ（Web アプリ）はダウンロードなしに利用することができる。一般には、ネイティブアプリは Web ブラウザ比でスマートフォン搭載機能との連携がより優れていると言われている。

図 1：FIDO の利用イメージ（FIDO Alliance の HP よりイメージ抜粋）



(4) FIDO・FIDO2 の基本的内容と 2 つのプロセス

FIDO・FIDO2 の認証は、次の 2 つのプロセス（「事前準備」と「認証判定」）により構成されている。なお、ここで記載する 2 つのプロセスは、後述するカード決済に実装するためのいくつかのパターンにおいて必須かつ共通のものになる。

① 基本的原理

A. スマートフォンで生体を読み取る

B. スマートフォンに登録されている生体情報[4]と照合

C. 生体情報自体はスマートフォンの外には出ない

② プロセス

A. 事前準備（カード会社での生体認証確認情報の登録）

a. カード利用者が生体認証[5]で真正本人であるかを確認するために、カード会社がカード会員の生体認証確認情報の登録[6]を行う。

b. 方法として、予めカード会員が自身のスマートフォンから、スマートフォンアプリや Web アプリを通じて「カード番号」と「生体認証確認情報[7]」をカード会社に送り、これをカード会社が登録・保存する。

B. 「カード番号」と「生体認証確認情報」の登録に必要な機能

a. 登録チャネルとして、スマートフォンアプリ・Web アプリの構築。

b. 「カード番号」と「生体認証確認情報」を、スマートフォンアプリ・Web アプリからカード会社へ送るための IF の構築。

c. 送られてきた情報を、カード会社で登録・保存する機能の構築。

---

[4] 指紋や静脈など、生体認証に用いられる（個人に由来する生体）情報の事を指す。

[5] 指紋、顔等に代表される「生体情報」を用いた本人認証方法のことを指す。

[6] カード会員の生体情報は、スマートフォンの機能を用いて登録及び保管が行われ、カード会社では保管しない。

[7] カード会社は生体情報を自社で登録・保存しない代わりに、スマートフォンが発行する「生体認証確認情報（生体情報に紐づく暗号鍵）」を登録・保存する。

図 2：「カード番号」と「生体認証確認情報」の登録イメージ

(5) カード決済時の生体認証情報の利用方法

生体認証の実現方法として、「A オーソリ電文に生体認証結果[8]を付加する方法」「B スマートフォンアプリから生体認証結果をカード会社に送る方法」「C スマートフォンからカード会社サービスに生体認証結果を送る方法」の 3 つを想定した。

① パターン A. オーソリ電文に生体認証結果を付加する方法

現存するカード決済の認証方法を踏まえた方法として、加盟店サイトでカード決済の際に、パスワードの代わりにスマートフォンの生体認証機能を使用するもので、よりカード会員に負荷がかからない方法である。

A. メリット・デメリット

a. メリット

・ 完全新規で機能構築する場合に比べ、規格化された仕組みや既存の仕組み等を流用する分、全体の実装負荷が軽減できる可能性がある。

b. デメリット

・ 国際ブランド・カード会社・加盟店のそれぞれでオーソリ電文仕様等の改修が必要。
・ スマートフォンアプリや Web アプリ等、新規構築する機能について個社単体もしくは業界標準として検討していくのかで費用負担が大きく変わる。

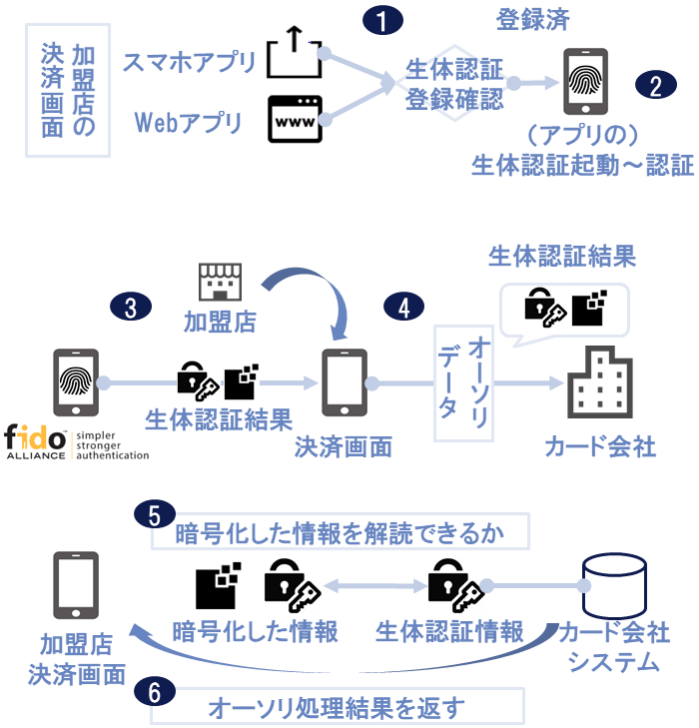
[8] ここでは「正しく生体認証が行われた結果」を示す何かしらのフラグや項目のことを指す。

B.　実装イメージ

a. カード会員は加盟店の決済画面で生体認証を行い、加盟店はオーソリ電文に生体認証結果を付加しカード会社へ送る。

b.カード会社は、予め登録した情報で生体認証結果が解読できたらオーソリ処理し、加盟店に結果を返す。

図 3：実現イメージ



② パターン B. スマートフォンアプリから生体認証結果をカード会社に送る方法

スマートフォンから直接カード会社に生体認証結果（＋オーソリに必要な情報）を送り、その結果を加盟店に通知する方法で、イシュアダイレクトの仕組みとなり、取引情報や承認結果をイシュアから加盟店に連絡する方法である。

A. メリット・デメリット

a. メリット

・ 完全新規で機能構築する場合に比べ、規格化された仕組みや既存の仕組み等を流用している分、全体の実装負荷が軽減できる可能性がある。

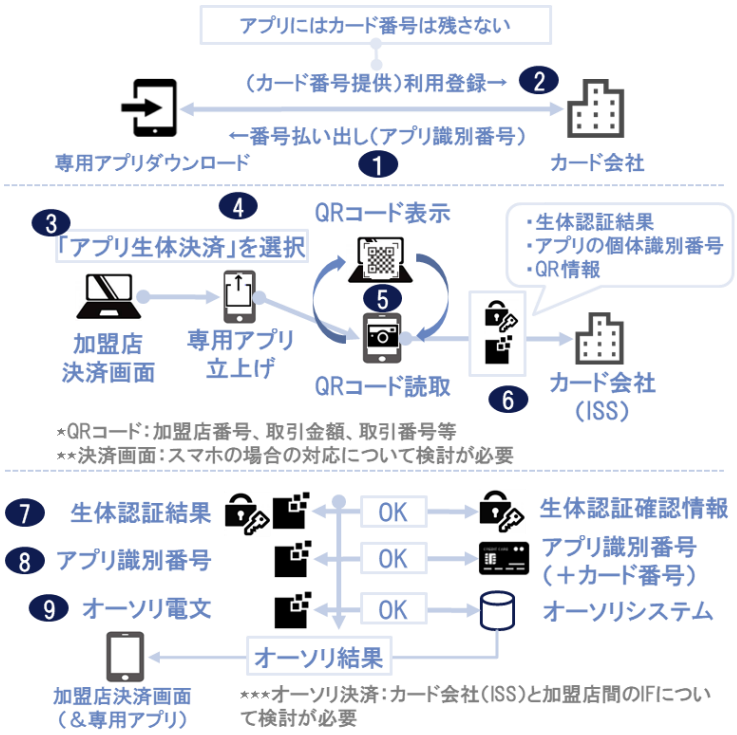
b. デメリット

・ 加盟店でカード会社の専用アプリとの IF、オーソリ結果の受取、QR の表示等、新規構築が必要。

・ スマートフォンアプリや Web アプリ等、新規構築する機能について個社単体もしくは業界標準として検討していくのかで費用負担が大きく変わる。

B. 実装イメージ

図 4：実現イメージ



③　パターン C. スマートフォンからカード会社サービスに生体認証結果を送る方法

カード会社の自社サービス（会員ポータル等）にログインし、そこから EC 加盟店へアクセス～決済する場合、自社サイトへログイン出来たことを以て、真正本人であることを確認（認証）する。

この認証結果を加盟店にも連携し、加盟店はオーソリ電文に認証済であることを付加してカード会社に送ることで、本人利用を確認する方法。

A.　メリット・デメリット

a.　メリット

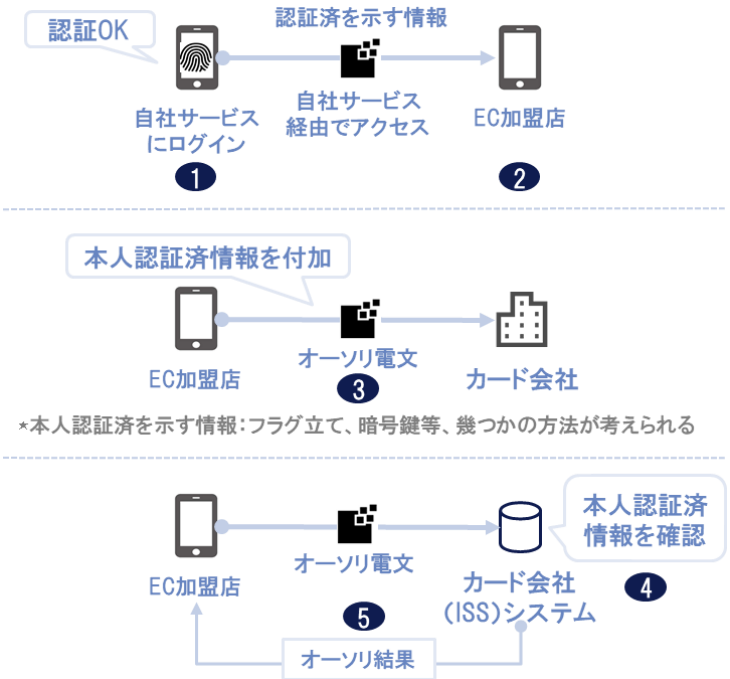
- 完全新規で機能構築する場合に比べ、規格化された仕組みや既存の仕組み等を流用している分、全体の実装負荷が軽減出来る可能性がある。
- 会員認証及び送客機能があるポイント優待サイト等を流用することで、パターン AB 比でより費用負担を軽減できる可能性がある。

b.　デメリット

- 加盟店側で、認証済情報の読み込みとその情報をオーソリ電文にセットする改修が必要。

B.　実装イメージ

図 5：実現イメージ



④　各手法の評価、課題、解決の方法

	A オーソリ電文に生体認証結果を付加する方法	B スマートフォンアプリから生体認証結果をカード会社に送る方法	C スマートフォンからカード会社サービスに生体認証結果を送る方法
期待効果	普及すればパスワードに頼らない一意の認証として一定の効果が期待できる。	同左	同左
カード会社負荷	生体認証確認情報の収集・保存方法の構築等、相応の開発が必要。	左記に加え、アプリ開発等が必要。	会員ポータル等への誘導。
加盟店負荷	オーソリシステムの改修が必要。	カード会社の専用アプリとの IF、オーソリ結果の受取、QR の表示等、新規構築が必要。	認証済情報の読み込みと、その情報をオーソリ電文にセットする改修が必要。
会員負荷	決済時にパスワード入力の代え生体認証を行うのみで簡単。	専用アプリのダウンロードや、決済時の QR コード読み取りが必要。	カード会社のポータルサイトを経由するステップが必要。
想定課題	オーソリ電文の改修等、国際ブランド・加盟店・ネットワークセンター等での開発が必要。	・会員のアプリのダウンロードが進まない。 ・イシュアダイレクトの仕組みとなるため、利用結果をイシュアから加盟店に回答するスキーム構築が必要。	・カード会員がカード会社ポータルサイトを経由しないと効果がない。 ・ポータル経由先の EC 加盟店の充実。
解決方法	国際ブランド含め、関連プレーヤの理解。	同左	カード会社ポータル経由時のインセンティブ提供。

(6) 《参考資料 1》各生体認証の特徴及び導入事例

調査した 13 の生体認証方法について、その特徴と導入事例について整理した。

図 6：各生体認証の特徴及び導入事例

【A】決済分野、【B】決済以外、【C】国内事例、【D】海外事例

認証手段			個社事例
1	身体的特徴	指紋	＜特徴＞ ✓ 生体認証としては歴史が長いと言われており、国内外・決済/決済以外で幅広く活用されている。 ＜事例＞ ✓ 【ABCD】各種「スマートフォン」への搭載（iOS、Android 等） ✓ 【 BC 】成田、羽田、中部、関西空港の「出入国における自動化ゲート（セキュリティ強化、手続き簡素化）」
2		静脈	＜特徴＞ ✓ 指紋認証と組み合わせて利用されることが多く、より精度が高いとされており、主に国内外の金融機関 ATM や公的機関等、より高セキュリティの求められる分野で導入されている。また近年は、従来型の接触型に加えカメラ画像による非接触型が出始めており、一部スマートフォンへの搭載が始まっている。 ＜事例＞ ✓ 【ABCD】韓国 LG 製スマートフォン G8 ThinQ に搭載された Hand ID ✓ 【 BC 】みずほ銀行「金融機関 ATM（セキュリティ強化、認証簡素化）」 ✓ 【 B D】英 Barclays PLC「コーレポートバンキング、ビジネスバンキング向け認証端末（認証簡素化）」 ✓ 【 BC 】横浜市立大学附属病院「医療情報システムのポータルでの個人認証（ID に応じた情報アクセス）」
3		掌形	＜特徴＞ ✓ 掌の形、指の長さ・太さといった外形に加え、静脈と組み合わせて利用することが多く、指紋よりも心理的障壁が低いとされている。静脈と同様高セキュリティの求められる空港や自治体等で導入されている。 ＜事例＞ ✓ 【 BC 】住基ネット「操作者認証装置（セキュリティ強化、認証簡素化）」 ✓ 【 B D】米主要空港「無人入国審査機械：INSPASS）」

4		虹彩	＜特徴＞ ✓ 瞼や角膜に保護されていることから指紋よりも経年劣化がなく、かつ顔と比べると形状が一定している他、非接触での認証が行えることで指紋等に比べて心理的障壁が低いとされている。比較的新しい技術であり精度も高いものの、導入には法改正が必要となるケース（入国審査等）がある。 ＜事例＞ ✓ 【ABCD】スマートフォンへの搭載（セキュリティ強化、認証簡素化）例：NTT ドコモ ✓ 【 B D】シンガポールの空港の一部で虹彩×顔認証による非接触型入国審査システムの試験運用を開始（シンガポール出入国管理庁：ICA が主導） ✓ 【 B D】国際民間航空機関 （ICAO）による生体認証パスポートの規格策定 （現在は顔画像が必須、指紋及び虹彩画像の搭載が各国家の任意事項）
5		顔	＜特徴＞ ✓ メガネや帽子、ひげ、表情、加齢といった要素で認証精度に影響を受けるが、虹彩と同様に非接触で認証を行える、人間の目でも判断ができる、といった特徴がある。指紋・静脈・虹彩等とは異なり一般的なカメラでも認識ができるため、特別な読取装置がなくても実装することができる。 ✓ スマートフォンや PC への搭載から、空港や自治体、企業の各出入口、最近では無人店舗での認証等、複数のセキュリティ手段と組み合わせつつ様々な分野で活用されている。 ＜事例＞ ✓ 【ABCD】スマートフォンへの搭載（セキュリティ強化、認証簡素化）例：NTT ドコモ ✓ 【ABC 】日本_レジ無しデジタル店舗での顔認証（セキュリティ強化、購買体験の向上）例：NTT データ 【 BC 】日本_防犯カメラ映像からの顔照合による不審者の特定（セキュリティ強化）例：NTT コミュニケーション ✓ 【 BC 】日本_スマートフォンの顔認証による二次産業の入退管理（セキュリティ強化、認証簡素化） 例：NTT ドコモ
6		音声	＜特徴＞ ✓ 音声認証は近年発達した比較的新しい技術であり、人間の発声器官（口、鼻、喉等）から発せされる声から固有特徴を抽出し、発話者を特定する。 ✓ 固定電話、スマートフォン、タブレット等に付属している汎用的なマイクが活用できる他、発する言語・内容に依存しないのが特徴となる。 ＜事例＞ ✓ 【 B D】香港_HSBC のテレホンバンキングにおける声紋認証（セキュリティ強化、認証簡素化） ✓ 【 B D】米_Google 製スマートスピーカー（Google Home）への搭載（セキュリティ強化、認証簡素化）

7		耳形	＜特徴＞ ✓ 音声認証と同様近年発達した比較的新しい技術であり、人間の耳に非可聴音を当てその反射から耳形を特定する。耳形は指紋と同様に、個人単位でその特徴が現れる。 ✓ 応用としては、近年普及し始めたスマートイヤホンへの搭載が見込まれている。高セキュリティ、ハンズフリー、自然な認証動作といった特徴から、移動や他作業と同時並行や求められる産業（建築、医療機関、インフラ保守等）での導入が予想されている。 ＜事例＞ ✓ 事例未確認
8		体臭	＜特徴＞ ✓ 人の臭気に含まれる化学物質を基に個人認証を行う技術だが、他技術と比べて発展途上にあり、犯罪捜査等によく使われる他技術と比べて、生体情報の当特に対して心理的障壁が低いとされている。 ＜事例＞ ✓ 事例未確認
9	行動的特徴	瞬き	＜特徴＞ ✓ 近年発達した比較的新しい技術であり、カメラを用いて瞬きによる黒目領域の変化量を測定する技術となり、顔や虹彩認証、瞬きの有無で生体か否かの判断も期待されている。 ＜事例＞ ✓ 事例未確認
10		歩行	＜特徴＞ ✓ 近年発達した比較的新しい技術であり、監視カメラ等の映像・マット・スキャナーに加え、スマートフォンやウェラブルデバイスに搭載されている各種センサから得られる運動量（加速度、角度、電磁場）を組み合わせることで精度向上を見込んでいる。 ✓ 大量の人が行きかう公の場所（空港、医療機関、自治体、企業オフィス等での）応用が検討されている。 ＜事例＞ ✓ 【 B D】米_国防分野に強みを持つ Blink Identity による歩行認証ソリューションの公表
11		筆跡	＜特徴＞ ✓ 近年発達した比較的新しい技術であり、人が文章を書く際の速度・筆圧の癖を利用する技術になる。一般に混同されがちですが、字体認証とは異なることに留意する必要がある。 ✓ 近年では精度向上のために専用のペンとタブレットを用意し、サインの形状・筆圧・速度・書き順・ペンの動きを見ることができます ＜事例＞ ✓ 【 B D】日本_ペンタスネットの①端末ロック、②クラウド認証等向け筆跡認証ソリューション

12		キーストローク	＜特徴＞ ✓ 従来からある技術だが、近年はスマートフォンへの応用が検討されている。パソコンのキーボードの打鍵、スマートフォンの入力の癖を特徴として抽出する。 ＜事例＞ ✓ 【B　D】日本_北里大学及び明治大学の e ラーニング向け認証（セキュリティ強化、認証簡素化）NTT コミュニケーション
13		リップムーブ	＜特徴＞ ✓ 発話時の唇の動きの癖を特徴として抽出する技術となる。監視カメラの映像（顔や歩行等）と組み合わせて活用されることがある。 ＜事例＞ ✓ 事例未確認（治安維持等）

(7) 《参考資料 2》本人認証スキームの調査結果

① 認証技術としての生体認証

A. 一般に認証技術は「知識認証」「所有物認証」「生体認証」に大別され、それぞれの特徴に応じた認証手段が研究・開発されてきている。

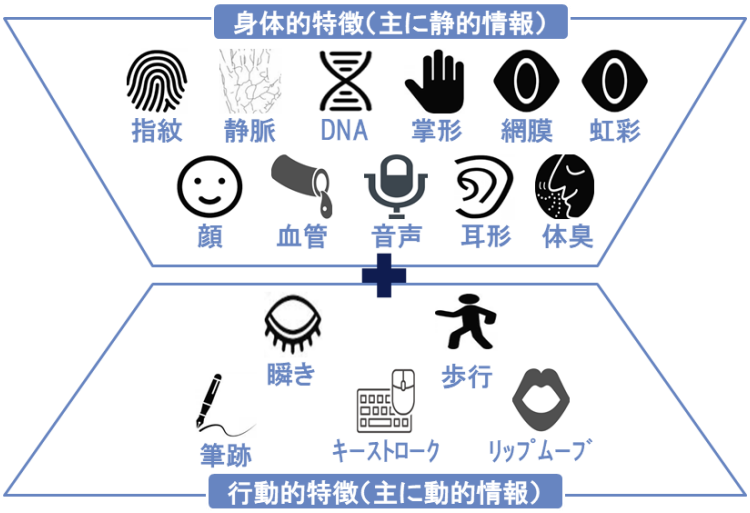
B. なお、近年では公共・民間の両領域においてサイバーセキュリティの脅威が増していることから、認証要素を単独ではなく「多要素」「多段階」で運用するケースが増えてきている。また、生体認証は、どの認証方法が一番性能が良いというものではなく、使われる装置や利用目的によって最適な認証方法を検討していく必要がある。

図 7：認証の 3 要素の整理

② 生体認証に利用される生体情報

生体認証はどの認証方法が一番性能が良いというものではなく、使われる装置や利用目的によって最適な認証方法が異なる。

図 8：生体認証に利用される生体情報の例

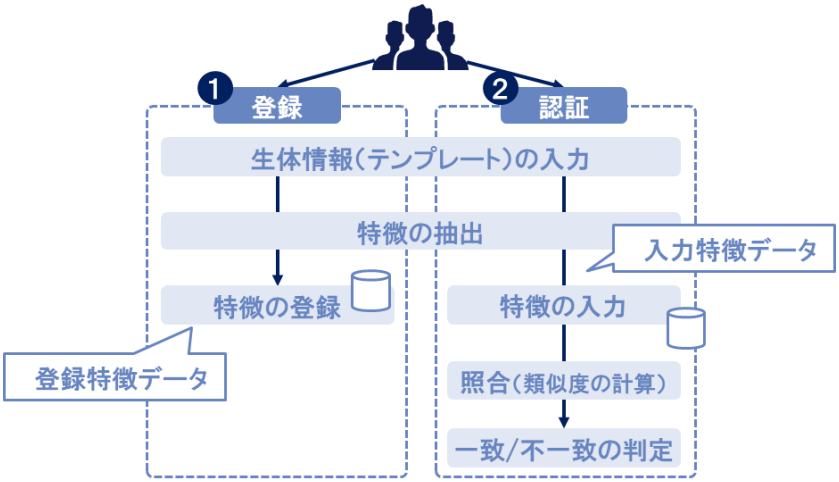


③ 生体情報の登録～認証の仕組み

A. 生体認証の活用には通常「テンプレート」と呼ばれる情報を事前に登録し、認証時に装置（センサ等）で取得した情報と比較することで認証を行う。[9]

B. 認証の際は「入力特徴データ」と「登録特徴データ」を照合してスコアを算出し、類似度が高い場合に本人と一致と判定するが、入力特徴データは湿度や気温等環境条件により変化する。

図 9：生体認証の仕組み



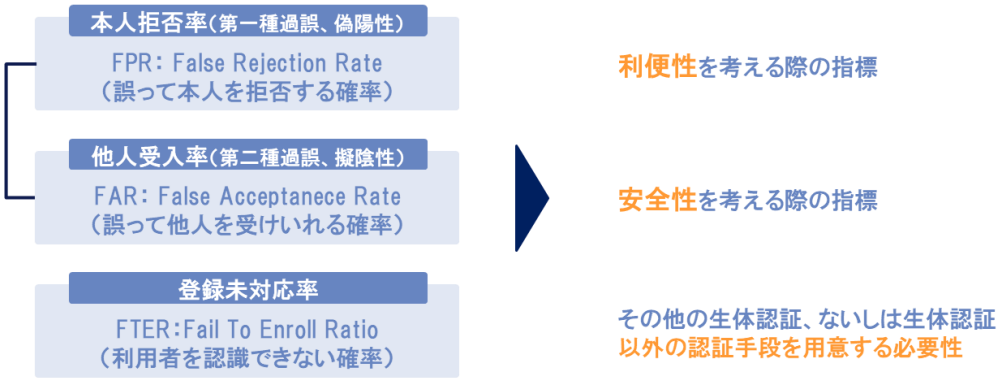
[9] （指紋認証のパターンマッチング等を除き）登録されるデータはあくまで指紋や虹彩を始めとした生体の「特徴量」であり、画像そのものではないことに留意する必要がある。

④　生体認証の性能指標

A.　生体認証は（DNA 等を除き）入力特徴データと登録特徴データは完全に一致することはなく、類似度のスコア計算結果と予め設定した閾値（判定値）が比較され、本人との一致/不一致が判定される。

B.　生体認証は、認証の目的に応じてセキュリティと利便性の兼ね合いで適切な閾値の設定を行う必要がある他、どのように閾値を定めても（DNA 認証を除き）、誤って他人を受け入れる可能性をなくし、かつ誤って本人を拒否する可能性を無くすことはできないことに留意する必要がある。

図 10：性能指標としての閾値、本人拒否率及び他人受入れ率の考え方

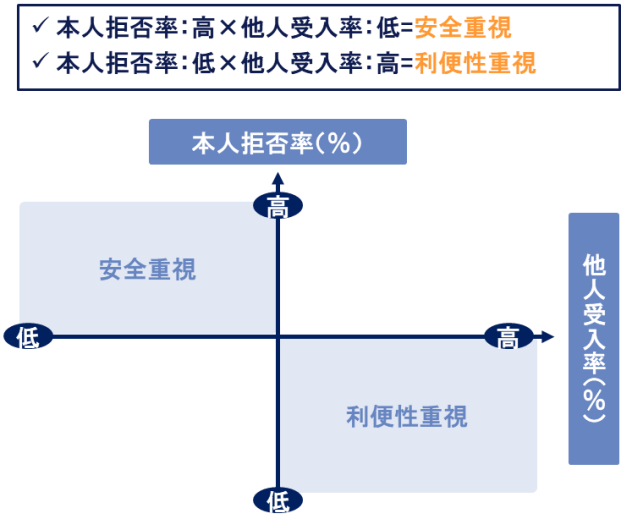


⑤　利便性と安全性のトレードオフ関係

A.　生体認証では、入力特徴データと登録特徴データの照合を厳密にするほど「本人拒否率」が高くなり、逆に緩くするほど「他人受入率」が高くなるという特徴がある。

B.　このことから、生体認証方法を導入する際は、アルゴリズム等でこれらの値をどのように 0 に近づけるのかがポイントの 1 つとなる。

図 11：生体認証のアルゴリズムの大まかな傾向



⑥　シングルモーダルとマルチモーダル

A.　単一の生体認証方法（シングルモータル）に対して、2 つ以上の生体認証方法を組み合わせて認証を行うことをマルチモーダル認証という。

B.　マルチモーダルの組み合わせの数やパターンは、ユーザにとっての使いやすさや認証強度・導入コスト等を勘案して検討する必要がある一方、判定アルゴリズムの選択肢拡大による精度向上の他、多様なユーザへの配慮も可能となる利点がある。

⑦　マルチモーダルの特徴

A.　判定アルゴリズムの選択肢の拡大

　単一の生体認証よりも、多様かつ複雑な組み合わせが可能となることで、認証に係るアルゴリズム調整の幅が広がるという利点がある。

⑧　判定方法の選択肢の拡大

　直接型、並列型、類似型等、総合的な照合判定を行うことで、本人拒否率や他人受け入れ率の減少、認証速度の向上に繋がるという利点がある。

・直列型：認証 A で合致した後に、認証 B の判定を行う。
・並列型：認証 A 及び B 同時に判定を行う。
・類似型：認証 A 及び B（両方の）判定を行い総合的に判定する。

3. テーマ②：SMS やプッシュ通知等によるカード利用時の利用確認

本テーマでは、ショートメッセージサービス（SMS）や、スマートフォンのアプリ等から自動的に通知する機能（プッシュ通知）等を非対面取引で活用する方策を検討する。

SMS、プッシュ通知は一部のイシュアで既に導入済であるものの、現行サービスは利用後に「利用確認通知」が届くものであるため、不正使用の早期発見には繋がるものの、不正使用の防止策とはなってないという課題がある。

こうした課題解決のため、本テーマでは「利用前」に「利用確認」として SMS、プッシュ通知等を活用するスキームの構築を目指し、方策の調査を行った。

(1) 可変化したセキュリティコードの利用確認時での活用

利用確認通知時の情報として、可変化したセキュリティコードを活用する事が有効と考えた。

これは、可変化したセキュリティコードを会員のみが確認できる環境で通知するスキームが構築できれば、カード会員本人はよりセキュリティ強度の高い決済情報を用いた利用承認が可能となり、非対面不正使用対策につながるためである。

なお、利用承認のタイミングは、決済時ではなく決済前が望ましいと考えられる。

これは、決済時にカード会員へ通知し対応を求めるような方法をとる場合、決済プロセスの複雑化やカード会員が通知に気が付かないことによる加盟店でのタイムアウト（=販売機会損失）等の課題が残ってしまうためである。上記の課題を解決するためには、加盟店がカード会員ではなくカード会社に照会を行う事が想定されるが、その場合、加盟店側での実装が必要であり、導入、普及のしやすさの面で実現可能性が低い。

(2) 可変化したセキュリティコードの使用環境

① 可変化したセキュリティコードの組込先

組込先としては、現行の固定セキュリティコードが表示されているクレジットカードの券面と、新たにスマートフォンが考えられる。

スマートフォンについてはアプリへの組込であり、会員ポータルのような既存の自社サービスの他、新たに専用のワンタイムパスワード（OTP）アプリを想定する。

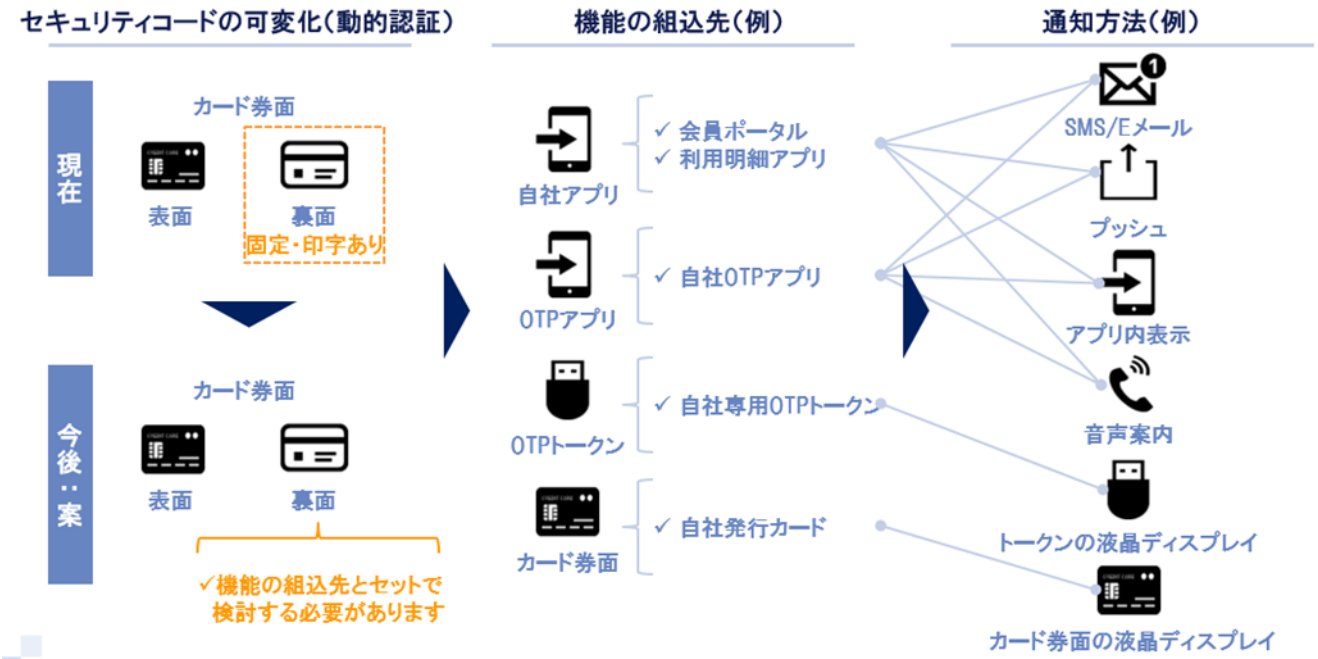
なお組込先としては OTP トークンも想定されるが、カード会員にとってはクレジットカードとスマートフォンに続く第 3 の認証媒体となる事から、以下の観点を勘案したうえで検討対象から除外した。

・カード会員にとっての使い勝手
・各カード会社の導入負荷
・早期かつ広範な普及

② 可変化したセキュリティコードの通知方法

通知方法としては、クレジットカード券面の他、SMS/E メール、プッシュ、アプリ内表示が挙げられる。なお音声案内や OTP トークンの液晶ディスプレイへの通知も想定されるものの、日本での馴染みの薄さや追加デバイスの必要を考慮し、項番 3(2)①の 3 つの観点からも検討対象から除外した。

図 12：セキュリティコードの可変化に伴う「機能の組込先」と「通知方法」の例



(3) 非対面取引における考察と検討

スマートフォンへの実装（パターン A)、カード券面への実装（パターン B）の 2 パターンでの実装検討結果を説明する。

① パターン A ：スマートフォンへの実装

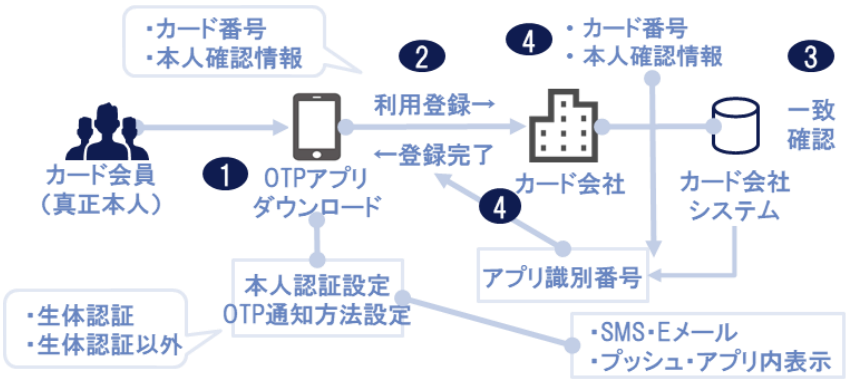
予め、真正本人が、動的セキュリティコードを発行する OTP アプリをダウンロードし、本人認証と利用登録を行う。

決済時は、OTP アプリに通知される同コードで決済し、カード会社はその内容で真正本人かどうか一致確認を行う。

A. OTP アプリの利用登録

予め、真正本人が動的セキュリティコードを発行する「OTP アプリ」をダウンロードし、（本人認証と）利用登録を行う。

図 13：実現イメージ



B. OTP アプリの利用

決済時は通知される同コードで決済し、カード会社はその内容で真正本人かどうか一致確認を行う。

図 14：実現イメージ

② パターン B：カード券面への実装

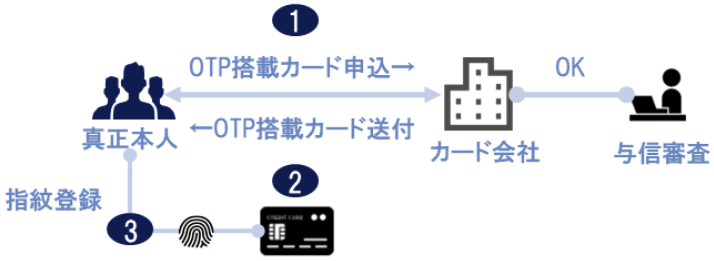
予め真正本人が、可変セキュリティコード搭載カードを申込、カード会社が会員に当該カードを送付する。

決済時は、真正本人がカード券面上で指紋認証を行い、認証結果 OK の場合に表示される OTP で決済する。カード会社は、オーソリ電文（＋認証結果）等で、真正本人かどうか一致確認を行う。

A. OTP 搭載カードの申込

予め、真正本人が、OTP（可変セキュリティコード）搭載カードを申込み、カード会社が会員に当該カードを送付する。

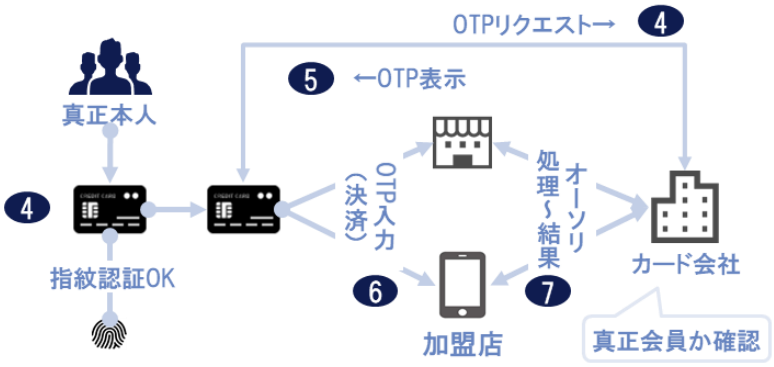
図 15：実現イメージ



B. OTP 搭載カードの利用

決済時は、真正本人がカード券面上で指紋認証を行い、認証結果 OK の場合に表示される OTP で決済する。カード会社は、オーソリ電文（＋認証結果）等で、真正本人かどうか一致確認を行う。

図 16：実現イメージ



③　セキュリティ強度の向上方法

カード券面及びスマートフォンの共通仕様として、可変セキュリティコードの起動（利用）に認証を必須とすれば、更なるセキュリティ強度の向上が想定できる。

また、国際ブランドやその認定ベンダーのソリューションによって国際標準化され、一部国内外で試験運用が行われているソリューションを使用することでカード会社の実装負荷の軽減が想定できる。その例としては、国際ブランドの認定ベンダーである、IDEMIA（アイデミア）、Zwipe（ズワイプ）、THALES（タレス）の 3 社のソリューションがある。[10]

IDEMIA（アイデミア）　・・・フランス[11]

・指紋認証搭載カード、動的セキュリティコードのソリューションがある。

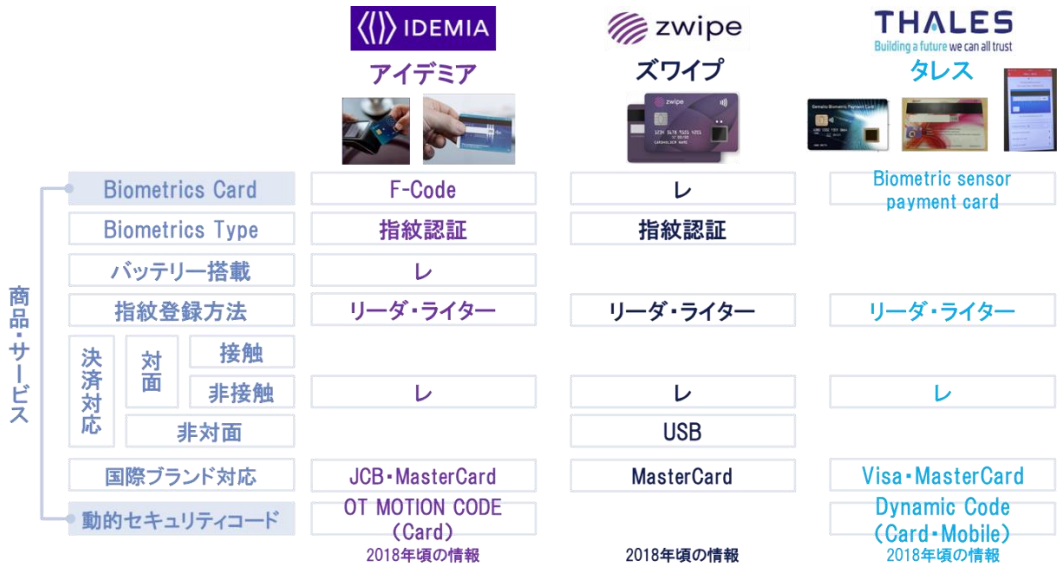
Zwipe（ズワイプ）　・・・ノルウェー[12]

・指紋認証カードのソリューションがある。

THALES（タレス）　・・・フランス[13]

・指紋認証搭載カード、動的セキュリティコードのソリューションがある。
（指紋認証搭載カードに動的セキュリティコードを搭載する計画あり）

図 17：国際ブランドやその認定ベンダーのソリューション例（各社 HP イメージ抜粋の上再構成）



[10] 現時点では、指紋認証搭載カードと動的セキュリティコードのソリューションは別々に構築されており、一体化されていない。

[11] IDEMIA は 2017 年にセキュリティ製品を手がける Morpho と Oberthur Technologies の 2 社が合併して誕生した企業だが、もともと航空防衛産業を手がける Safran グループの一部として製品を提供してきた経緯がある。

[12] 2009 年創業。指紋センサを搭載した非接触決済カード技術を提供しており、2018 年に Gemalto と提携し、キプロス銀行の決済カード開発にも携わることになった。

[13] タレスは航空宇宙防衛分野における欧州の中心企業の一つとして、装備品の技術提供等により、日本内外の安全保障ソリューションを提供している。

④　各手法の評価、課題、解決の方法

	A スマートフォンに可変セキュリティコード及び生体認証を搭載する	B カードに可変セキュリティコード及び生体認証を搭載する
期待効果	普及すればパスワードに頼らない一意の認証として一定の効果が期待できる。	同左
カード会社負荷	生体認証確認情報の収集･保存方法の構築等、相応の開発が必要。	左記に加え、OTP 搭載カード等の調達が必要。
加盟店負荷	セキュリティコードを用いた決済に対応済みであれば､基本的に加盟店での実装は不要。	同左
会員負荷	右記に加え､専用ないしは何かしらのアプリのダウンロードが必要。	決済時にセキュリティコードを起動するため認証を要するが動作は簡単。
想定課題	セキュリティコードが使えないタイミングが発生しないよう、OS 等アップデート対応が必要。	OTP 搭載カードは、これまでのカード券面よりも高単価になる。
解決方法	関連プレーヤの理解に加え､カード会社各社でのアプリ開発・運用状況の調整。	業界全体での取り組みによる共同調達の実施や、国際ブランドへの働きかけ。

4. テーマ③：イシュア等の提供情報による加盟店での対策

本テーマでは、イシュア等から不正使用の取引情報を利用した加盟店での不正使用防止対策について、内外の事例を調査し、更に効果を高める方策について考察を行った。

(1) 国内事例調査

現状、国内においては一部イシュア間で不正配送先情報を集約し、加盟店に情報提供することにより不審な売上を未然に察知できるためのスキームが実装されている。

「fdec」は国内カード会社 6 社が運営しているスキームである。このスキームは加盟店に対してこれらイシュアの「不正配送先情報」を提供し、加盟店が利用者の申し込んだ配送先情報と突合することで、不正使用懸念の取引に対して配送を停止したり、カード会社に本人利用確認を依頼する等の対応を行っている。

しかしながら、提供情報が 6 社に限定されていることや、配送停止等の判断は加盟店に依存している他、加盟店の使い勝手の問題等の理由により十分な効果が得られるとは言い切れない状況である。

(2) 海外事例調査

一方、海外においても同様のスキームが存在している。「ethoca（エソカ）」[14]は 2019 年に MasterCard が買収計画を発表している企業であるが、この企業には、不正利用されたカード番号をリアルタイム連携する「ETHOCA　ALERTS」と、Web ポータル経由で加盟店に利用内容照会ができる「ETHOCA LIMINATOR」が存在しており、ここではこれらのスキームの詳細を一部紹介する。

①　ETHOCA　ALERTS

イシュアが不正利用されたカード番号を、ethoca 経由で加盟店にリアルタイムで連携するサービスである。アクワイアラは介在せず、加盟店は配送停止、カード会員への返金等の対応状況を 24 時間以内にイシュアに回答する義務がある。

②　ETHOCA ELIMINATOR

カード会員からの問い合わせを受けたイシュアが ethoca の Web ポータルを使用し加盟店に利用内容照会ができるサービスである。イシュアが自社のオンライン明細に詳細を確認するためのクリックボタンを設置し、カード会員がボタンをクリックした際、加盟店の利用明細を API で呼び出し表示することができる。

---

[14] 同社の持つネットワークは、2019 年時点で（グローバルにおいて）5,000 以上の加盟店、4,000 以上の金融機関と接続されている他、北米の e コマースブランド上位 10 社のうち 8 社、北米のカード発行会社上位 20 社のうち 14 社、英国のカード発行会社上位 10 社のうち 6 社が、ethoca ソリューションとそれらを支えるネットワークを活用している。

(3) 他業界事例調査

他業界においても同様のスキームが存在する。ここでは、旅行業界における「JIRSTA[15]」の事例を紹介する。

JIRSTA（Japan Internet Reservation Standard for Travel Agency）は、2007 年に旅行会社が合同で立ち上げたコンソーシアムであり、インターネットによる海外航空券や国内宿泊の不正購入に対応するための活動を行っている。

① 設立のきっかけ

インターネット上だけで取引を行う旅行会社（OTA）での旅行サービスの不正取得が国内でも顕在化している。これまでは、旅行業は換金性が低いと考えられていたため、不正利用の対象となることは稀であったが、数年前から悪徳事業者が旅行サービスを不正取得し、転売するというモデルが確立され、国内旅行会社が被害に遭うケースが散見されるようになった。そのため、同業者間でカードの不正利用を検知・防止する目的で事例を蓄積して加盟会社間で情報共有している。

② 具体的な運用

利用者のカードを承認する前に、予約データや利用した端末情報のデータなどを送信する。システムは予め設定したルールに基づいて不正利用の可能性を点数制で採点し、その結果を加盟各社にリアルタイムで送信する。

(4) 非対面取引での活用方法の検討

前述での調査により、不正取引情報等の集約により、不正利用防止に一定の効果があることがわかったが、現在国内で実装しているスキームである fdec においても以下のような課題があるため、これらを解決していくことが重要であると言える。

① サービス品質の向上、加盟店の負荷軽減

fdec は加盟店に対して不正配送情報を提供することでそのサービスが成立するが、その課題としては、まず情報提供者であるイシュアが 6 社に限定されていることから情報量が少ないことが挙げられる。

また、加盟店は不正配送情報を目視により確認し自らのデータベースと突合するが、非常に手間がかかるだけでなく精度にも影響があると考えられる。これらの課題を解決するためには、情報提供元の拡大、登録データの項目追加、外部サービスの取込みを行うことでサービス品質の向上を図ることが望ましいと考えられる。

加えて、自動化・オンライン化といった手段も負荷軽減に効果があると考えられる。fdec は現在無料で加盟店に提供しているが、サービス品質の向上・加盟店の負荷軽減はシステムの追加開発と運用が前提となるため、引き続き加盟店に無料かつ簡易な形式で提供できるかどうかという観点も必要となる。

[15] ジャパンシステム株式会社がシステムを運用している。

図 18：各課題に対する BPR の方向性（案）

	現状の課題	BPR の方向性（案）
①	1. fdec に 1 件づつ情報を手入力して検索するのに体力がかかる。 2. バッチ DL（ダウンロード）をしても、加盟店が自ら照合する仕組みを構築しなければ十分に効果を発揮できない。 3. バッチ DL の最新性を維持するには適宜 DL を繰り返す必要がある。	根本的にはオンライン照合システムの構築～提供が望ましいが、システム構築には提供主体であるカード会社の費用負担が発生するため、現在の無償提供が難しくなる懸念がある。
②	1. 現在疑わしい取引の情報が各関係者から ISS に入ってくると、ISS 担当者はカード会員へ（電話で）利用確認をする等、相応の体力を要している。 2. しかしながら、fdec への情報登録には不正利用の確定が必要である。 3. 「疑わしい取引の発生～fdec への情報登録」の時間差が、fdec の効果を減退させてしまう。	より簡素かつ迅速にカード会員への連絡～確認できる双方向機能を検討する。具体的には、既存のカード会社アプリへ（カード会員への）の確認機能の追加、その他カード会社での登録情報（携帯電話番号、E メールアドレス等）を用いた自動発信等が考えられる。
③	1. ISS が不正利用を特定後、ACQ が加盟店とやり取りをして fdec に登録するまでのプロセスに相応の体力を要している。 2. このことが、ACQ の負担になっていると共に、fdec への情報登録までのリードタイムとなってしまっている。	ACQ⇔加盟店間のやり取りを自動化・オンライン化等することで、人的体力の削減と共に fdec への情報登録までの時間を短縮することが期待できる。

(5) fdec の精度向上に向けた取り組み

以下はこれらの課題解決のためのアプローチ方法である。

	①他サービスの取込 ・fdec と他サービスの連携 ・fdec に他サービスと同等機能を構築 ・fdec と他サービスを統合	②機能性向上 ・情報提供先の拡大 ・追加項目の検討	③BPR（自動化） ・ethoca の取込みによる業務負荷軽減及びサービス品質の強化
期待効果	不正使用検知率の向上により、に一定の不正使用防止効果が期待できる。	同左。	運用負荷軽減による業務効率化や迅速化によるサービス品質の向上、新たに参加カード会社を募る上で一定の訴求ポイントとなることが期待できる。
カード会社負荷	システム開発会社との要件整理に始まり、開発内容の管理が必要。	同左。	同左。
加盟店負荷	・新サービスの運用構築が必要。 ・新サービスの提供方式によっては、システム開発が必要。	同左。	同左。
会員負荷	カード会社と連絡を取るために専用ないしは何かしらのアプリを構築する場合、予めダウンロードが必要。	同左。	同左。
想定課題	・他アプローチとの組み合わせを考慮し、システム開発会社との要件整理が必要。 ・新たなシステム開発により、加盟店へ無料でサービス提供が困難となる可能性がある。	左記に加え、予め期待効果のある項目の検討及び選定に加え、情報提供先（候補）との交渉・調整が必要。	左記に加え、ethoca を取り込むのか、同等機能を fdec に構築するのか等の検討が必要。
解決方法	・システム開発会社と協業し、各アプローチの組み合わせに応じた要件整理や見積もり取得等を行う。	左記に加え、情報提供先との事前協議を通じて実現性を確認する。	左記に加え、ethoca は MasterCard 経由で、fdec への同等機能の構築はシステム開発会社へ打診の上、費用等を確認する。

5. テーマ④：その他、本人認証等についての国内外成功事例等

テーマ①からテーマ③までは、それぞれの限定された範囲の対策を説明してきたが、ここではその他の国内外事例について説明する。

また、更に、これまで説明してきた方策を組み合わせるなどして、本検討の中から発想を得た対策手法についても併せて紹介する。

(1) その他の国内外事例

① カード会員自身によるカード機能コントロール

従来、カードの機能（例、利用限度額など）は、もっぱらカード発行会社がコントロールするものだったが、近年、カード会員自身が自身のカードの利用できる範囲など（例えば、対面取引でしか使わない、海外では使わないなど）を適宜設定できるサービスが登場しており、既に国内の一部カード会社で採用されている。

カード会員が、「非対面取引での買い物をしない」と設定しておけば、不正使用者がネット加盟店で悪用しようとしても利用できなくなり、不正使用の防止効果に期待がもてる（カード会員自身がネット加盟店で利用したい時は容易に設定を変更できる）。このようなサービスの具体例を以下に紹介する。

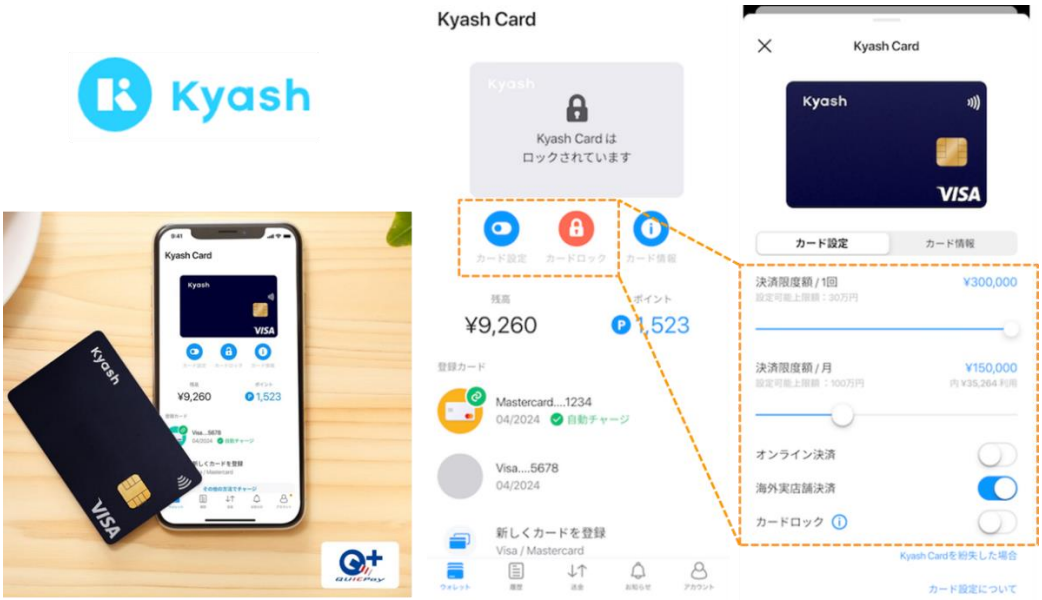
A. Kyash

同社は同社の発行するクレジットカードまたはデビットカードの利用範囲をカード会員が選択し登録できる機能を提供している。また、他社から要請があれば同様の機能を提供することができる。

なお同社の提供しているカード会員が設定できる機能は以下の通りである。

決済限度額（回）
決済限度額（月）
オンライン決済（可否）
海外実店舗決済（可否）
カードロック（利用可否）

図 19：Kyash サービス利用イメージ（同社 HP 及び Blog より抜粋の上再構成）



B. Ondot

同社は決済事業者（ISS、ACQ)向けに様々なサービスを提供しており、そのサービスの1つとしてカード管理機能（カードコントロール、セルフサービス）を提供している。これらのサービスは、他社の提供する同様のサービスに比べてより詳細な設定ができるのが特徴である。

同社の提供する機能としては、次のようなものがある。

カード利用可否（オンオフ）

・カードの利用可否を設定。

モバイルロケーション

・モバイルの位置情報と合致する場所のみカード利用が可能。

ロケーション

・予め地図上で指定した場所でのみカード利用が可能。

近傍

・登録したスマートフォンと取引場所が離れている場合取引拒否

利用制限（取引）

・一取引あたりの上限金額の設定。

利用制限（月）

・一ヶ月のカード利用制限の設定。

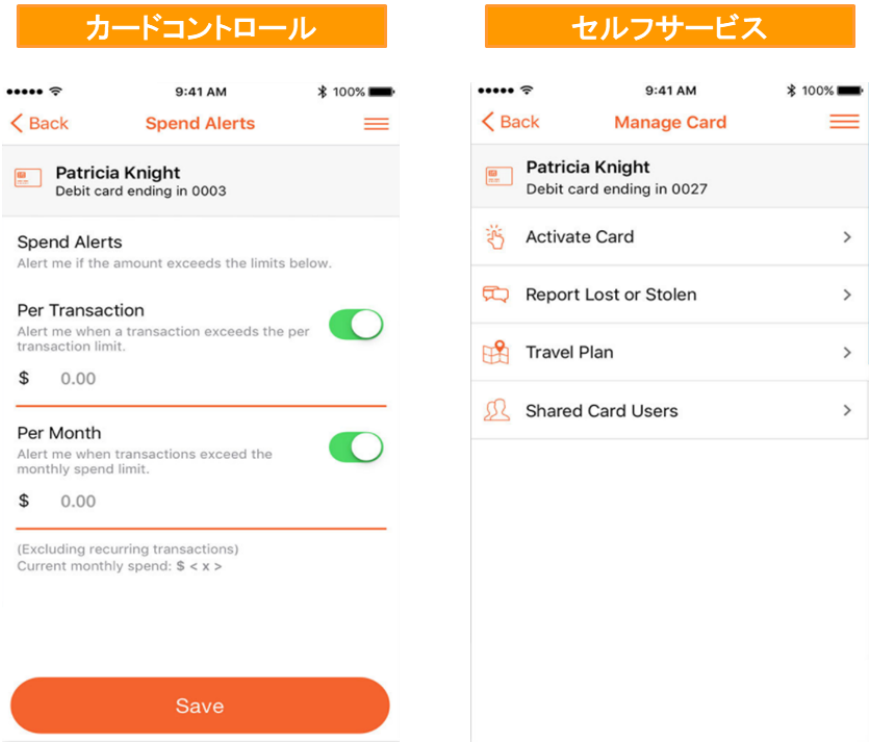
決済カテゴリ

・公共料金、食商品、銀行、デパート等、利用可能な加盟店業種の設定。

取引タイプ

・オンライン、店舗、ATM 等、利用可能な取引の設定。

図 20：Ondot サービス利用イメージ（同社 HP よりイメージ抜粋の上再構成）



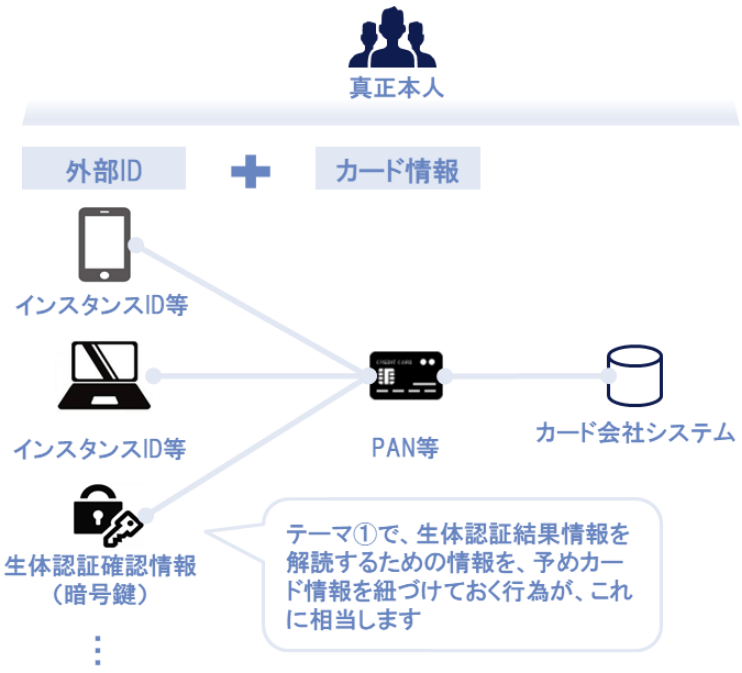
② スマートフォン等 ID・カード情報の紐付け[16]

この手法は、非対面取引に使うスマートフォンや PC などの ID（例、インスタンス ID[17]等）と、その機器の持ち主が使うクレジットカード番号等とを組み合わせたデータをカード会社が取得し登録しておき、非対面取引が発生した際には使用しているスマートフォン等と利用されるクレジットカード番号との組み合わせが、予め取得していた組み合わせと一致するかを判定し不正か否かを判定しようとするものである。

なお、現在のスマートフォン等は、操作開始前に生体認証などにより真正な持ち主の操作であることを確認していることから、テーマ①で取り上げた生体認証が間接的に行われていると言え、非対面取引時の本人識別判定の信頼度は高いと考えられる。

また、この手法では、どのように予めスマートフォン等とカード番号の紐づけを多くの会員から集めるかが課題となるが、「会員のサービス利用登録時」等の際に収集することも考えられる他、簡易的に「カード会社の会員向けサービス」において（利用許諾の上で）Cookie を取得する等が考えられる。不正使用で利用された各種 ID は、ブラックリスト照合として以後のオーソリ時にも利用できる。

図 21：「外部 ID・カード情報の紐付け」の実現イメージ



[16] コード決済に関する統一技術仕様ガイドライン（JPQR）では、本人認証要件の 1 つとして、サービス利用登録時等に利用者のモバイルデバイスとコード決済アプリを紐付け管理することが記載されており、実際に複数サービスに導入されている。

[17] 現在、SSAID（Android ID）や IMETI（携帯電話の製造番号）、MAC アドレス等は、情報の取得に際してユーザから特権情報へのアクセス承認取得が必要である他、生体情報と同じく変更ができない情報であることから、OS 開発企業からはアプリがインストールされている間のみ有効である「インスタンス ID 等」が推奨されている。

(2) 本検討過程で想起された対策手法

① 高機能アプリ

非対面取引での不正利用被害防止のためには、先に説明してきた事例からもわかる通り、カード会員とカード発行会社の連携が重要である。

これにはカード会員とカード会社のコミュニケーションをいかに負担なく簡単に行えるかがカギとなるが、その実現にあたってはセキュリティ面もさることながら営業サービス面で重要なのは論を待たないところである。そこで、営業サービス面の機能をベースに、セキュリティ面の各種の機能も備えたカード会員向けのアプリ（高機能アプリと呼ぶ）を作成し普及させることが必要だと考えられる。

ここでは、セキュリティ面でどのような機能をアプリに持たせるかについて、これまで説明してきた各対策を組み合わせて説明する。なお、各機能は全てを備える必要はなく、採用する不正使用対策に応じて取捨選択されるものと考える。

A. 可変セキュリティコードの表示機能

非対面取引時に使用するもの。カード発行会社側システムで都度生成したものを表示する機能。アプリ側負担を軽減（テーマ②関連）

B. 本人利用確認問合せ機能

カード発行会社側で、不審な取引を検知した場合、自動的に問合せをする機能。（事後確認とはなるものの、カード会社側の人的体力の削減、早期の回答入手が期待できる）（テーマ③関連）

C. 使用端末の ID 取得機能

アプリダウンロード時に「普段利用する端末」として何かしらの ID を取得しカード番号との紐づけを可能にする。（テーマ④関連）

D. 生体認証必要情報の取得機能

アプリで生成した生体認証に必要な公開鍵をカード発行会社に登録する機能（テーマ①関連）

E. カード会員自身がカード利用範囲を制限できる機能

容易に設定内容をコントロールできるようにする。（テーマ④関連）

② タッチ決済機能付きクレジットカードのスマートフォンでの読取り

昨今、タッチ決済機能付きクレジットカードの普及が世界的に進みつつあり、国内においても普及の方向にあると考えられる。このカードには、NFC という近距離無線通信機能が組み込まれている（既にマイナンバーカード、運転免許証にも組み込まれている[18]）。

NFC を読み取れる機能は、既に多くのスマートフォンに搭載されている。こうした状況の中で、米国 Mobeewave 社（2020 年 8 月に Apple 社が買収）は、NFC カード（国際ブランド付き）をスマートフォンにかざすことによって決済処理ができる技術を開発しており、今後、NFC クレジットカードをスマートフォンにかざすだけで非対面取引ができるようになる可能性があると考えられるため、現時点で実用化事例はまだないが、あえて紹介するものである。

特にクレジットカードでの NFC 取引では、カードが本物であることを瞬時に確認できる技術（EMV）が使われており、また、カード上で指紋による生体認証機能を有するカード（実用化済み）を採用すれば[19]、「真正なカードが真正な本人により利用された」ことが確認出来ることとなり、極めて安全性の高い取引が実現できることから、非対面取引での不正使用防止効果は極めて大きいものになると考えられる。

NFC カードの利用分野は、現在は、対面取引だけであるが、スマートフォンの NFC 読取り機能を活用し非対面取引でも利用できれば、カード会員の利便性・安心感が格段に増し、カード会社が投資する意義も増すものと考える。

図 22：Mobeewave サービスの利用イメージ（同社 HP よりイメージ抜粋の上再構成）

[18] マイナンバーカードの IC 情報は、公的個人認証サービスポータルサイトに掲載されている「マイナンバーカード対応 NFC スマートフォン」であれば、NFC で読み取ることができる。IC 免許証の IC 情報は、NFC 読取機能が組み込まれている Android スマートフォンで読み取ることができる。iPhone は①iOS13 以降、②Felica 読取に対応した iPhone7 以降の端末、③2020 年 1 月時点ではサードパーティ製アプリを DL、の条件を満たす場合に読取が可能。

[19] NFC 取引（対面取引）で本人認証不要とする取引限度額を超える場合、どのように本人認証を行うかが課題となっているが、その一つの対応方法がカード自体で生体認証を行うものである。

(3) 各手法の評価、課題、解決の方向性

上記の 4 つの手法について、期待効果、負荷（カード会社、カード会員、加盟店)、課題及び解決の方向性について、下表にまとめた。それぞれ大まか内容とはなっているが、今後さらに検討を進めて行くうえでの参考としてご覧願いたい。

	カード会員自身によるカード機能コントロール	スマホ等ID・カード番号の紐付け	高機能アプリ	タッチ決済機能付きクレジットカードのスマートホンでの読取り
期待効果	普及し会員が使えば相応の効果が期待できる。	紐づけデータが十分蓄積できれば効果期待できる。	普及し会員が使えば相応の効果が期待できる。	普及できればほとんどの不正を排除できる。
カード会社負荷	カード会社（自社）だけで対応できるの点から実装しやすい。	紐付けられた情報の蓄積、オーソリ時照合のシステム対応が必要	カード会社（自社）だけで基本的には対応できるの点から実装しやすい。	・（生体認証機能付きの）NFCカードへの切り替え ・スマホアプリ開発
加盟店負荷	加盟店の対応不要	スマホ等ID・カード番号の収集、一部の加盟店の協力が必要。 カード会社側で作成したものを利用することで加盟店負荷は限定的。	加盟店の対応不要	非対面取引でのNFC決済のための加盟店側手当てがあり得る。
会員負担	操作は簡単。	・会員からの申告を求める場合は、若干手間。 ・カード会社側で取集なら、負担なし。	操作は簡単。	極めて便利。 スマホにかざすだけ。
想定課題	コントロールに紐づくオーソリシステムの改修が必要。	スマホIDが異なるオーソリ時の対応方法。	・アプリのダウンロードが進まない。 ・各機能に紐づく本体システムの改修が想定される。	物理的なNFCカードへの差し替え体力が大きい。（不正対策施策というより利便性向上施策）
解決方法	国際ブランドがこの機能を提供している場合はこれを利用することも選択肢	他のモニタリング指標で総合判断。 事後本人利用か自動照会	・アプリダウンロードへの大幅なインセンティブ ・業界内で共同して利用できる部分を洗い出しコストセーブを目指す	スマホ搭載型NFCカードとすること、スマホ生体認証機能の利用で、物理的カードの差し替えコストのセーブを検討する。

6. 今後の検討に向けて

非対面取引の不正使用は、業界の懸命の努力にも拘わらず被害額が増加し続けている。

本報告書では、新たな視点に立った中長期的な対策の手がかりとなるべく調査、検討を行った結果を述べてきた。ここでは、これまで掲げてきた方策に限らず、今後業界として不正使用対策を進めて行く上での、共通的な考え方について触れておきたい。

(1) 許容できるコスト

当然のことながら、不正使用対策を実施していくためにはコストが必要となるが、どの程度のコストが適当かという問題が付いて回る。様々な要素があり容易に答えが得られるものではないが、一つの考え方として、次のように考えられるのではないか。不正使用対策は、その効果の大きさ（不正使用防止額、顧客満足度）とコストとのバランスの問題である。

例えば、業界の被害額（2019 年番号盗用被害額 222 億円）が今後 5 年間継続すると想定した場合（被害累計額 1110 億円)、被害額防止効果 50%の対策なら 5 年で 555 億円のコストも 5 年間で回収可能との計算になる。業界として被害の大きさを改めて認識し、相応のコストを許容することも必要である。

(2) コストセーブの方向性

上記の考え方は極論ではあるが、いかにコストセーブを図るかは課題である。不正使用防止は、業界の共通利益につながるものと考え、カード会社が個々に同様の対応をするのではなく、可能な範囲で共同して対応することも検討すべきではないか。

(3) 普及の方策

カード会員、加盟店などに協力を求める必要のある対策については、業界が一丸となって働きかけることが必要である。

(4) 加盟店負担の軽減

加盟店側の対応が必要な対策では、負担を減らせるようカード業界側で汎用的なシステムモジュールを構築・提供し、システム開発負荷を減らすなどの対応が普及を早めるものと考えられる。

不正使用による被害は、単にカード会社が損失を被っているだけではなく、毎年巨額の資金が犯罪者の手にわたっている事実を真摯に受け止め、クレジットカード業界として、有効な不正使用対策を行っていく必要がある。

検討課題が多く実現が容易ではなさそうな対策であっても、確実に一歩一歩今から検討に着手することが必要である。

本報告が、今後の非対面取引の不正使用被害対策を検討する上での参考となり、不正使用防止に少しでも役立てれば幸いである。

以上