コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン

一般社団法人キャッシュレス推進協議会

Ver. 1.0

2020 年 9 月 18 日

【履歴】
2020 年 9 月 18 日　新規制定(Ver. 1.0)

目次

【用語集】 I
1 はじめに 1
1.1 本ガイドラインの目的 1
1.2 本ガイドラインの適用範囲・注意事項 2
2 コード決済に係る不正 4
3 銀行口座の不正紐づけと検知のタイミング 4
4 アカウント作成時 6
4.1 総論 6
4.2 コード決済事業者による対策 7
(1) 総論 7
(2) アカウント作成時における利用者からの情報収集 7
(3) コード決済事業者が保有する周辺情報の活用 8
(4) モニタリング結果の活用 8
(5) 利用者又はモバイルデバイスを一意に特定できる手段での認証 9
(6) 不正利用の傾向に合わせたアカウント作成の制御 9
5 銀行口座紐づけ時 9
5.1 総論 9
5.2 コード決済事業者による対策 10
(1) 総論 10
(2) 金融機関が保有する属性情報との突合 10
(3) 1つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止 10
(4) 1つの銀行口座を紐づけられるアカウント数の制限 11
(5) モニタリング結果の活用 11
6 チャージ時 11
6.1 総論 11
6.2 コード決済事業者による対策 11
(1) チャージ額の制限 11
(2) モニタリング結果の活用 12
7 決済時 12
7.1 総論 12
7.2 コード決済事業者による対策 12
(1) 総論 12

(2)　決済時における制限の設定 13
(3)　モニタリング結果の活用 13
8　常時行うべき対策 13
8.1　総論 13
8.2　コード決済事業者による対策 13
(1)　総論 13
(2)　不正に対するモニタリング体制の構築 14
(3)　不正検知をした場合の対応体制の整備 14
9　今後について 15
9.1　本ガイドラインの改訂方針 15
9.2　コード決済の発展に向けて 15

【用語集】

本ガイドラインにおける用語は以下の通りの意味を有する。

用語	定義
アカウント	利用者がコード決済サービスを利用することのできる権利であり、コード決済サービスを利用するにあたり、利用者ごとに作成されるもの
アカウントの乗っ取り	何らかの不正な方法により、正当な権限のない者に自己のアカウントを使用される状態
関連事業者	コード決済事業者、金融機関、契約店等、銀行口座を紐づけたコード決済に関係する事業者のほか、コード決済関連事業者を含む幅広い事業者
協議会	一般社団法人キャッシュレス推進協議会
金融機関	顧客の口座内で顧客から預金を預かる業を営む銀行、信用金庫、信用組合等の事業者
契約店	コード決済事業者やコード決済アクワイアラ等との契約に基づき、自己の商品・サービス等の対価を利用者からコード決済にて支払を受ける者
ゲートウェイ事業者	契約店とコード決済事業者の間で、契約店からのコード決済情報をコード決済事業者へと仕向けを行う事業者
コード決済	バーコード又はQRコード®[1]を用いたキャッシュレス決済
コード決済アクワイアラ	契約店と契約を締結の上、契約店がコード決済を取り扱えるようにする事業者
コード決済アプリ	コード決済を行うことを目的とした、利用者又契約店用アプリケーション
コード決済関連事業者	コード決済事業者、コード決済アプリ開発者、コード決済アクワイアラ、契約店への処理端末提供者、ゲートウェイ事業者等コード決済に関係する幅広い事業者
コード決済事業者	コード決済を利用者及び契約店に提供する事業者
属性・行動分析	利用者が入力する情報や、利用者のモバイルデバイスに関する情報、利用履歴等、コード決済事業者が収集できる情報に基づいて、不正か否かを判定する手法
店舗提示型ガイドライン	協議会「コード決済に関する統一技術仕様ガイドライン

[1] QRコード®は、株式会社デンソーウェーブの登録商標である。

	【店舗提示型】 MPM(Merchant-Presented Mode)」（Ver. 2.0、2020 年 4 月 27 日）
当人認証	認証要素を照合することにより、作業をしている者が登録を行った利用者本人であることを確認すること
バーコード	コード決済用の一次元コード
身元確認	利用者の住所、氏名、生年月日等の情報が当該利用者の正しい情報であることを確認すること
モバイルデバイス	キャッシュレス決済手段を利用するための端末であり、一般的にはスマートフォンなどの携帯端末
利用者	コード決済事業者の提供する利用規約等にあらかじめ同意した上で、自己が契約店から受けた商品・サービス等の対価をコード決済によって支払おうとする者
利用者提示型ガイドライン	協議会「コード決済に関する統一技術仕様ガイドライン【利用者提示型】 CPM(Consumer-Presented Mode)」（Ver. 1.2、2019 年 10 月 31 日）
QR コード	コード決済用の二次元コード

1　はじめに

1.1　本ガイドラインの目的

キャッシュレスの推進に向けて、スマートフォン等のモバイルデバイスとバーコード又は QR コードを活用したコード決済サービスが利用者にとって利便性のある決済サービスの方法としてその活用が期待されているが、一方でコード決済において不正利用が発生している。コード決済の普及のためには、安心かつ安全な決済手段であることは必要不可欠な条件であることから、協議会ではコード決済における不正利用対策についての検討を随時行っており、2019 年 4 月 16 日には不正流出したクレジットカード番号等を用いた不正利用対策について、「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」を公表している。

本ガイドラインは、コード決済における不正利用対策のうち、銀行口座紐づけに関する不正利用対策に関するものである。コード決済サービスの中には、銀行口座を当該コード決済サービスに紐づけることによって、当該銀行口座の残高を用いてコード決済サービスにチャージを行ったり、当該コード決済サービスで決済を行った場合に当該銀行口座の残高から直接決済金額が差し引かれたりするサービスを提供するものがある。こういったサービスにおいて、他人の銀行口座が不正に紐づけされてしまうと、当該銀行口座の名義人の残高が不正に利用されることになってしまう。本ガイドラインはこういった不正に対する対策を記載している。なお、銀行口座紐づけに関する不正利用対策としては、大きく分けてコード決済事業者等コード決済サービスを提供する側が行う不正利用対策と紐づけられる金融機関側が行う不正利用対策とが考えられる。本ガイドラインは、速やかにコード決済事業者として守るべきセキュリティ水準を定めることの重要性に鑑みて、まずはコード決済事業者側で行う不正利用対策について定めている。ただし、協議会としては、今後、金融機関側が行う不正利用対策についても検討を進める予定である。

コード決済の不正に対する対策が十分になされていない場合、コード決済サービスの利用者のみならず、不正利用された銀行口座の名義人等、コード決済に係る不正に巻き込まれた者に対して損害が発生する事態をも招来し、さらにはコード決済サービスに対する社会的信用を害することにもなりかねない。コード決済の更なる普及に向けては、コード決済によって生ずる不正を防止すべく、想定される不正を洗い出した上、これらの不正が発生するリスクに見合ったセキュリティ水準の向上等の対策を講ずることが重要である。

本ガイドラインは、上記の通り、銀行口座紐づけに関する不正利用防止対策について記載するものであるが、かかる不正利用防止対策の中には、銀行口座紐づけの不正利用事案以外の不正についても参考とできる点が含まれている。本ガイドライン

は、これらの対策を通してコード決済の不正利用を防止し、利用者及び契約店にとって安心かつ完全なキャッシュレス決済手段としてのコード決済の健全な発展を図ることを目的としている。一方で、コード決済事業者が直面するコード決済の不正利用のリスクに応じて対策を選択することを可能とし、コード決済サービスの安全性を向上させるとともに、各コード決済事業者のサービス展開やその利便性を不必要に阻害しないよう、留意している。

なお、本ガイドラインは、本ガイドライン記載の不正利用防止対策を行ったことにより、不正利用が完全に防げることを保証するものではなく、また、考えられる不正利用防止対策を網羅的に記載したものでもない。さらに、新たな手口の不正が生じた場合、現在考えられている不正利用防止対策の実効性は損なわれる可能性がある。コード決済関連事業者においては、本ガイドライン記載の対策のみにとらわれることなく、新たな不正の可能性を常に見据えながら、現在講じている不正利用防止対策の実効性を絶えず検証し、これら新たな不正が発生するリスクに見合った対策を適時適切に講ずることが重要である。なお、本ガイドラインに記載されるセキュリティ対策以外にも、協議会、関係省庁、関係団体等がセキュリティ対策に関する指針やガイドラインを策定している場合があり、関連事業者はこれらも参照されたい。

本ガイドラインは、コード決済事業者、金融機関、その他決済事業者、関係団体、専門家等の幅広い関係者にご参加いただいた協議会における検討会の結果を踏まえて作成されたものであり、本ガイドラインに基づいた不正利用防止対策の実行により、さらなるコード決済の普及及び活用を期待するものである。

1.2 本ガイドラインの適用範囲・注意事項

- 本ガイドラインに記載される不正利用防止対策は、コード決済に係る不正のうち、銀行口座の不正紐づけに係る対策を念頭においているものの、その他の不正に係る対策においても、参考となるべき事項が含まれる。
- 本ガイドラインは、コード決済事業者による対策を中心とするものである。ただし、金融機関においても、コード決済サービスにおけるセキュリティ対策の考え方を把握するために、本ガイドラインを参考にしてもらいたい。
- 本ガイドラインは、コード決済を念頭に記載されているが、コード決済だけではなく、EC 等での使用やオンラインでの送金が可能なウォレットサービス等の決済サービスにおいても参考になる部分がある。
- 本ガイドラインでは、考えられる不正対策を、「必須である」「推奨される」「考えられる」事項に区別して記載している。
- 銀行口座が不正に紐づけられるリスクや当該リスクに対する具体的な対策は、不正利用者による手法及び事業者による対策の高度化や、各事業者が提供す

るサービスの内容等によっても変化し得るものである。各事業者においては、自らが直面する銀行口座紐づけによる不正利用のリスクを把握し、事業者ごとにこれに見合った対策を講じて銀行口座不正紐づけを可能な限り防止していくことが不可欠である。本ガイドラインでは、各事業者がリスクに見合った対策を講ずることが求められる事項や、本ガイドライン制定に至る検討に参加した事業者の対応状況等を参考に、各事業者が最低限実施することが求められる具体的な事項につき、「必須である」事項として記載している。

- 他方、各事業者が全てを実施することまでは必ずしも求められないが、各事業者がリスクに見合った対策として選択して実施することが望まれる事項や、各事業者及び事業者間相互で継続的に検討することが望まれる事項につき、「推奨される」事項として記載している。
- この他、対応することも一案である事項や、本ガイドライン制定に至る検討の過程で挙がった事項のうち参考となる事項等につき、「考えられる」事項として記載している。
- 本ガイドラインは強制力を持つものではないが、上記 1.1 に記載のとおり、本ガイドラインは不正利用防止を通じたコード決済の発展のために、コード決済に関係する幅広い関係者による検討を踏まえて作成されたものであり、本ガイドラインの目的達成のためにも、コード決済事業者及び金融機関は、本ガイドラインで記載されている不正利用防止対策のみならず、新たな不正の可能性等も考慮しながら、常に積極的に不正利用防止対策を講じられたい。
- 本ガイドラインは、関連事業者が協調できる領域について共通事項を定めるものであり、協調領域以外の領域における自由な競争を否定するものではない。
- **本ガイドラインは、不正な銀行口座紐づけに係る対策に関連する事項を記載するものであり、本ガイドラインの遵守により、決済事業に適用のある関連法令の適合性を保証するものではない。関連事業者は、自己の責任と負担において関連法令を調査し、これらを遵守しなければならない。また、本ガイドラインの遵守により安全かつ欠陥のない決済システムを構築できることを保証するものでもない。**
- **協議会は、本ガイドラインに含まれるすべての事項につき、明示的であれ非明示的であれ、いかなる表明も保証も行わない。本ガイドラインを利用する者は、自己の責任と負担において本ガイドラインを利用するものとし、協議会は本ガイドラインの利用により関連事業者、利用者、その他第三者に生じた損害・損失・負担等の一切の結果についていかなる責任も負わず、本ガイドラインを利用する者は協議会に対していかなる責任の追及も行わないものとする。**

2　コード決済に係る不正

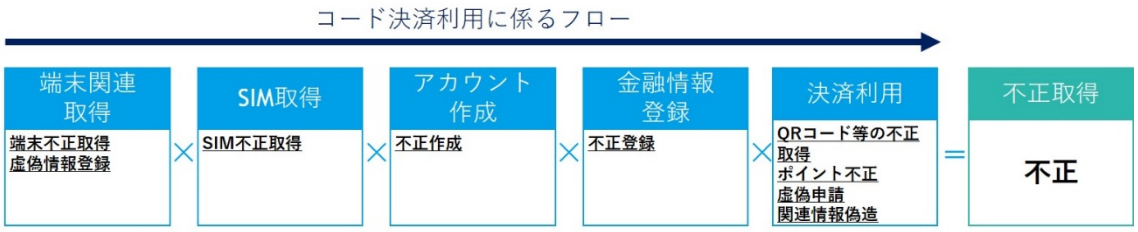
コード決済においては、モバイルデバイスを利用した決済のフローの各時点において、不正の可能性がある。関連事業者は、各時点において生じ得る不正の可能性を意識しながら、適時適切な不正利用防止対策を講ずることが重要である。

もっとも、コード決済に係る不正の手法は、技術の高度化等に伴って常に変化している。関連事業者としては、以下の図 2 に記載する不正利用のケースにとどまらず、今後発生する新たな不正にも留意することが重要である。

なお、本ガイドラインに記載する不正利用防止対策は、銀行口座の紐づけによる不正利用への防止対策を念頭に置いている。もっとも、これらの中には、コード決済に係るその他の不正に対しても実効性を有するものが含まれているため、関連事業者においては、以下の記載を参考としながら、コード決済に係る不正の性質に応じて、これに見合った対策を講ずることが重要である。

なお、これらの不正利用防止対策は、協議会が制定した利用者提示型ガイドラインや店舗提示型ガイドライン等、本ガイドライン以外の協議会、関係省庁、関係団体等が策定した指針やガイドライン等にも記載されているものがある。関連事業者においては、こうした関連する指針やガイドライン等も参照しながら、コード決済に係る不正全般に対する堅牢な対策を講ずることが重要である。

また、コード決済に係る不正には、関連事業者以外にも、コード決済の利用者や不正に登録された銀行口座の名義人等が幅広く関係する。コード決済に係る不正に対しては、これらコード決済に関わる全ての者の役割や関連性等も意識しながら、不正が起きないようにするための防止策や、既に発生している不正の分析・対応等の措置を講ずることが重要である。



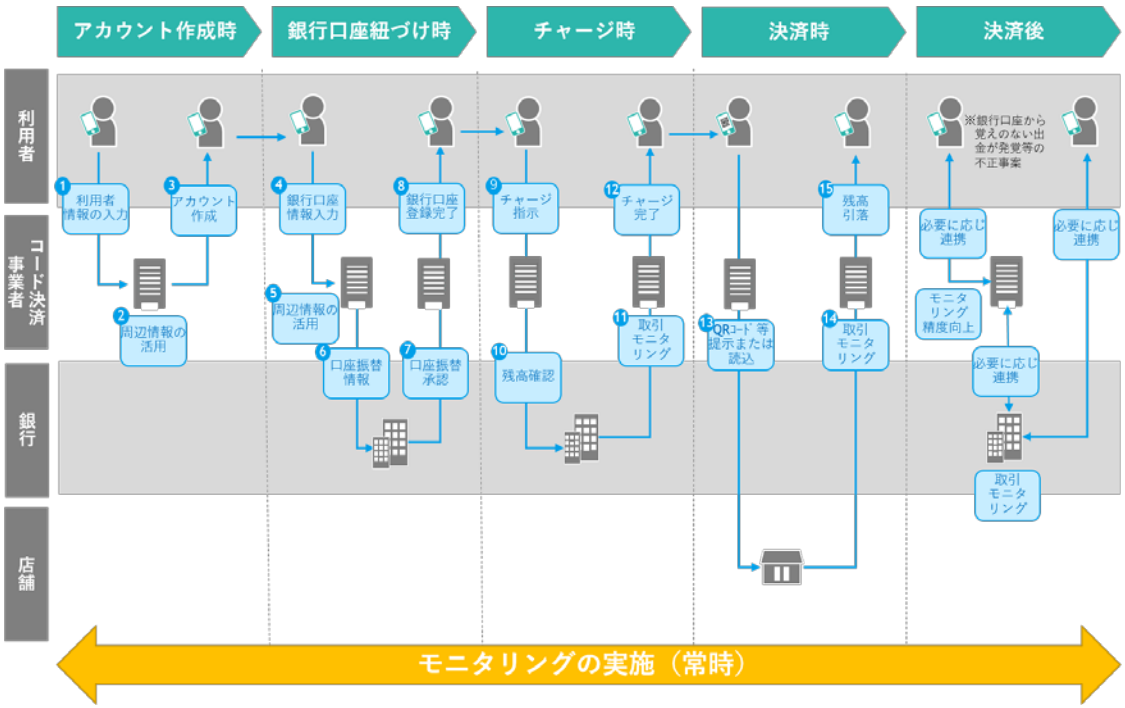
【図 2　コード決済に係る不正（イメージ）】

3　銀行口座の不正紐づけと検知のタイミング

コード決済に係る不正利用防止対策及び不正検知の可能性を検討するに当たっては、コード決済の利用に係るフロー及びフローごとにコード決済に関わる者の役割

や関連性等を検討していくアプローチが有用と考えられる（図 3 参照）。特に、不正な銀行口座の紐づけによる不正利用を防止するためには、コード決済アプリに銀行口座を紐づける時点において、当該不正な紐づけを行わせないための対策をコード決済事業者及び金融機関において講ずることが最も重要な対策の一つとなる（ただし、上記 1.1 記載のとおり、本ガイドラインは、まずはコード決済事業者において行うべき不正利用対策について定めており、金融機関において行うべき不正利用対策については追って検討される予定である。）。一方で、不正な銀行口座のコード決済アプリへの紐づけを完全に防止することは困難であるため、コード決済利用に係る各時点において、不正に銀行口座紐づけがなされてしまったケースであっても事後に早期検知する枠組みを構築すること等により、被害の拡大を防止していくことが重要である。そのためには、コード決済サービスの利用開始に伴うアカウント作成時から決済時までの各時点及びコード決済サービス全体において、コード決済に関わる全ての者が講ずることのできる対策を網羅的に検討していくことが重要である。そこで 4 以降では、上記対策を A アカウント作成時、B 銀行口座紐づけ時、C チャージ時、D 決済時の 4 つの時点と E 常時行うべき対策の 5 つに分類した上で、関係する当事者が講ずることのできる対策を検討している。

以下では、対策の具体例を記載しているが、対策の内容や実効性は、コード決済事業者が提供するコード決済サービスの内容等によっても異なるものであり、以下に記載するものが唯一の方法ではなく、対策の全部又は一部を講じただけで直ちに全ての不正利用を防止できるものでもない。また、新たな不正手段が登場した場合には、以下の対策の実効性が失われることも想定される。さらに、不正利用防止対策はコード決済事業者が提供するサービス全体を通して実現されるものであり、コード決済事業者は特定の時点における不正利用防止対策のみにとらわれることなく、利用者や契約店における利便性も考慮しながら、サービス全体を通してコード決済の安全性を高めるための継続的な取組みを行っていくことが重要である。コード決済事業者においては、以下の具体的な対策も参考としながらも、これのみに固執することなく、不正利用を捕捉するのに活用できる情報の内容や信頼性等も考慮し、自らが直面する銀行口座の不正紐づけのリスクを正確に把握して、これに見合った複数の不正利用防止対策を適切に組み合わせて実施していくことが重要である。



※　一例であり、様々なパターンが考えられる

【図 3　コード決済サービスにおける全体のフローの例】

4　アカウント作成時

4.1　総論

銀行口座紐づけを利用したコード決済において、コード決済アプリに銀行口座を紐づけようとしている利用者が、当該銀行口座の利用に関し正当な権限を有していれば（多くの場合、銀行口座の名義人とコード決済の利用者が同一であれば）、アカウントの乗っ取りや利用者のモバイルデバイスの盗難等といった場合を除き、当該紐づけられた銀行口座の残高が不正に利用される事態は基本的には想定されない。コード決済事業者は、コード決済に係るアカウント作成時から銀行口座紐づけ時に至るまで、当該銀行口座の利用に係る正当な権限の有無を判断するのに必要な情報を可能な限り収集し、これを銀行口座紐づけ時に活用するなどの方法により、正当な権限のない者が不正に銀行口座を紐づける事態を防止していくことが重要である。アカウント作成時にコード決済事業者が取得する情報は、それのみで正当な権限のない者による銀行口座の紐づけと判断できるわけでは必ずしもないが、銀行口座紐づけ時までに取得する他の情報と併せて活用することで、不正検知の一助となり得る。し

たがって、コード決済事業者は、コード決済事業者が利用者と最初に接点を有し、コード決済サービスの提供を開始する「入口」時点であるアカウント作成時における情報収集が、後の銀行口座紐づけ時や決済時等において正当な権限のない者による銀行口座の利用と判断する一助となる可能性も踏まえ、各事業者の判断でアカウント作成時における情報収集を行っていくことが重要である。なお、ここでいうアカウント作成時とは、利用者がコード決済の利用を開始しようとする時点を意味し、例えば、複数のサービス（コード決済サービスに限らず、また、コード決済事業者自身のサービスに限らない。）で共通のアカウントを使用している場合には、コード決済サービス以外の目的で当該共通のアカウントが作成される段階ではなく、コード決済サービスの利用を開始するための手続きを利用者が開始する時点を意味することになる。

4.2 コード決済事業者による対策

(1) 総論

本ガイドラインでは、アカウント作成時における具体的な不正利用防止対策として、以下(2)から(6)にコード決済事業者において導入可能な対策を示している。他方、3 に記載のとおり、コード決済における不正利用の防止は、コード決済サービス全体（特にアカウント作成時から決済時まで）を通して実現されるものである。コード決済事業者は、正当な権限のない者が銀行口座を不正利用するリスクや、利用者の利便性、各事業者が展開するコード決済サービスの内容等も考慮しながら、自己のコード決済サービス全体を通していかに不正利用を防止するかを検討し、複数の不正利用防止対策を組み合わせて実施することが重要である。

(2) アカウント作成時における利用者からの情報収集

コード決済事業者は、後のコード決済の利用において、コード決済を行おうとする者がアカウントの作成を行った者と同一であることを確認できるようにするため（すなわち、当人認証を可能とするため）に、アカウント作成時に当人認証を行うために必要な情報を収集することが重要である。コード決済事業者は、アカウント作成の過程で利用者に特定の情報の入力を求めること等により、利用者から情報収集を行うことができる。もし、アカウント作成時に誤った情報が当人認証のための情報として登録されてしまうと、後の当人認証を有効に実行することができなくなるため、こういった誤登録を防ぐ必要がある。また、資金移動業登録を取得しているコード決済事業者による犯罪による収益の移転防止に関する法律に基づく取引時確認等、関連法令において、特定の時点や条件下において、利用者の氏名等特定の項目の確認（身元確認）がコード決済事業者に義務付けられている場合もある。

しかしながら、アカウント作成時における情報収集は上記のとおり、後のコード決

済の利用において、当人認証を可能とする目的で行われるものであり、これ自体でコード決済に紐づけられた銀行口座等の支払手段の利用に関し正当な権限を有する者である点まで確認できるものではない。

また、上記 3 で述べたとおり、コード決済における不正利用防止対策はコード決済サービス全体を通して実現されるものであり、コード決済サービスの内容によってはアカウント作成時には特別な情報の入力を求めない（すなわち、利用者に情報を入力してもらう形での当人認証に向けた情報収集を行わない）ことも否定されるものではない。アカウント作成時においてコード決済事業者が利用者から収集する情報の内容及び収集の方法については、コード決済サービスの利便性等も考慮しながらコード決済事業者が自ら検討すべきものである。

コード決済事業者においては、アカウント作成の際に収集する情報が正当な権限のない者による銀行口座の利用と判断する一助となる可能性や、利用者の利便性、利用者に係る個人情報保護その他の制約等も考慮しながら、アカウント作成時に取得する情報の内容やその内容を基礎付ける資料の確認方法等を検討・判断することが必須である。

⑶ コード決済事業者が保有する周辺情報の活用

アカウント作成時にコード決済事業者が入手できる情報は、利用者に情報を入力してもらうことにより利用者から直接収集するものに限られるわけではない。コード決済事業者は、利用者がアカウントを作成する際にモバイルデバイスに関する情報等の周辺情報を入手することが可能である。

コード決済事業者としては、これらアカウント作成時に取得可能な周辺情報が正当な権限のない者による銀行口座の利用と判断する一助となる可能性や、利用者の利便性、利用者に係る個人情報保護その他の制約等も考慮しながら、これらアカウント作成時に取得可能な周辺情報の活用を検討・判断することが必須である。

⑷ モニタリング結果の活用

後記 8.2(2)のとおり、コード決済における不正抑制のためには、常時モニタリングを行うことが非常に重要であり、コード決済事業者はモニタリング体制を構築することが必須であるが、当該モニタリングの結果をアカウント作成時において活用することが考えられる。なお、モニタリング結果をどの時点でどのように活用するかはコード決済事業者の判断によるが、アカウント作成時においては、過去に不正が行われたアカウントに関する情報を蓄積してブラックリスト化し、アカウント作成時にブラックリストと突合の上、一致する場合には当該アカウントの作成を拒絶することは必須である。ブラックリストに記載する項目については各コード決済事業者が自己のコード決済サービスの内容やモニタリングシステムの設計等を考慮して適切に設定すべきである。

なお、ブラックリストとの突合による新規アカウント作成の拒絶を行うにあたっては、過去になりすまし等の被害にあってしまったがためにブラックリストに掲載されているが、真正な本人が行うアカウント作成である可能性もあることに念頭に、かかる真正な本人によるアカウント作成及びコード決済の利用を阻害しないように留意する必要がある。

⑸ 利用者又はモバイルデバイスを一意に特定できる手段での認証

後記 5.2⑵のとおり、銀行口座の不正な紐づけを防止する手段の１つとして、金融機関が保有する銀行口座に関連する情報とアカウントに登録されている利用者の情報の一致を確認したり、アカウント情報の変更に制限をかけたりすることがあげられるが、不正利用者が複数のアカウントを大量に作成することが可能な場合、不正利用者は不正に取得した口座情報の数だけアカウントを作成して、それぞれに紐づけることができてしまう可能性がある。したがって、コード決済事業者としては、かかる不正利用者によるアカウントの大量作成を防止する必要があり、そのために、アカウント作成時点において、利用者又はモバイルデバイスを一意に特定できる手段での認証を行うことが必須である。これにより、同一人物又は同一モバイルデバイスからの大量のアカウントの作成を阻止することができるようになる。なお、当該「利用者又はモバイルデバイスを一意に特定できる手段」については、各コード決済事業者が自己の判断で決定するものとする。

⑹ 不正利用の傾向に合わせたアカウント作成の制御

上記⑷のほかにも、アカウント作成にあたっては不正利用の傾向に合わせたアカウント作成の制御を行うことが考えられる。ただし、かかるアカウント作成の制御にあたっては、正当なアカウント作成が不必要に阻害されることのないように注意する必要がある。

5 銀行口座紐づけ時

5.1 総論

銀行口座の不正紐づけによる不正利用を防止するには、コード決済アプリに銀行口座を紐づける時点において、不正な紐づけをさせないための対策を講ずることが最も重要である。銀行口座紐づけ時における対策としては、パスワードや属性情報等、利用者を特定するために必要な情報の入力を追加で求める方法や、5.2⑶及び⑷で記載する銀行口座の紐づけ制限といった方法のほか、銀行口座紐づけ時までに収

集した情報を正当な権限のない銀行口座の紐づけのリスクの判断に活用する等の方法が想定される。コード決済事業者としては、各コード決済事業者が提供するコード決済サービスの内容やその利便性等も考慮しながら、正当な権限のない者による銀行口座紐づけのリスクを低減するための手法を各コード決済事業者の判断で選択して講ずることが重要である。

5.2 コード決済事業者による対策

⑴ 総論

本ガイドラインでは、銀行口座登録時における具体的な不正利用防止対策として、以下⑵から⑸までにコード決済事業者において導入可能な対策を示している。他方、3 に記載のとおり、コード決済における不正利用の防止は、コード決済サービス全体（特にアカウント作成時から決済時まで）を通して実現されるものである。コード決済事業者は、正当な権限のない者が銀行口座の残高を不正利用するリスクや、利用者の利便性、各事業者が展開するコード決済サービスの内容等も考慮しながら、自己のコード決済サービス全体を通していかに不正利用を防止するかを検討し、複数の不正利用防止対策を組み合わせて実施することが重要である。

⑵ 金融機関が保有する属性情報との突合

銀行口座の不正紐づけの防止にあたっては、紐づけられようとしている銀行口座について、利用者がその利用について正当な権限を有していることを確認することが重要である。利用者が紐づけようとしている銀行口座について正当な権限を有することを確認する手段として、コード決済事業者は、利用者がコード決済事業者に提供した利用者に関する情報のうち金融機関から求められる情報を金融機関に提供し、金融機関が保有する紐づけようとされている銀行口座についての情報と一致するとの回答を金融機関から得た場合にのみ当該銀行口座の紐づけを認めることが必須である。

⑶ 1つのアカウントに複数名義の不正な銀行口座が紐づけられることの防止

前記 5.2⑵に記載される金融機関が保有する属性情報との突合を行ったとしても、コード決済アプリ側の利用者に関する情報を簡単に変更できてしまうと、不正者は1つの紐づけを行った後、コード決済アプリ側の利用者情報を次々に紐づけようと思っている銀行口座の情報に書き換えることにより、容易に次々と不正な銀行口座紐づけが行えてしまう。したがって、コード決済事業者は、1つのアカウントに複数の不正な銀行口座紐づけが行われないように対策をすることが必須である。対策の具体的内容は、各コード決済事業者が自己のサービス内容や他の不正対策等を考慮して決

定するものとする。

⑷ 1つの銀行口座を紐づけられるアカウント数の制限

不正な銀行口座紐づけを防止するには、上記 5.2⑶に記載されるような制限をするだけでなく、1つの銀行口座を複数のアカウントに紐づけることを制限することも有効であり、推奨される。可能であるならば、1つの銀行口座は1つのアカウントにしか紐づけられないとすることが望ましい。これにより、既に正規の口座の保有者が当該銀行口座を紐づけてコード決済サービスを利用している場合には、後から不正利用者が銀行口座を不正利用者のアカウントに紐づけようとしても紐づけることができなくなる。

⑸ モニタリング結果の活用

後記 8.2⑵のとおり、コード決済における不正抑制のためには、常時モニタリングを行うことが非常に重要であり、コード決済事業者はモニタリング体制を構築することが必須であるが、当該モニタリングの結果を銀行口座紐づけ時において活用することが考えられる。なお、モニタリング結果をどの時点でどのように活用するかはコード決済事業者の判断による。

6 チャージ時

6.1 総論

銀行口座の不正紐づけが防げなかったとしても、チャージ時点で不正対策を行うことにより、不正利用により利用される額を減らすことができる。不正利用防止においては、不正自体の発生を防止することはもちろんであるが、不正利用が発生してしまった場合に、その被害金額をなるべく低く抑えることも大切である。したがって、コード決済事業者はチャージ時の対策も怠るべきではない。

6.2 コード決済事業者による対策

⑴ チャージ額の制限

銀行口座の不正紐づけは、前記 5.2 に記載するような対策を行ったとしても、完璧に防ぎきることができない場合もある。万が一、不正に銀行口座が紐づけられた場合、銀行口座の残高のすべてが使用されてしまうと、利用者が非常に大きな被害にあう可能性がある。このような事態を回避するために、コード決済事業者はアカウント単

位又は銀行口座単位でチャージできる金額を制限することが重要である。もっとも、かかる制限は、必ずしもチャージ金額において設定されなければならないものではない。チャージというお金の入口ではなく、決済というお金の出口で制限をかけることによって、被害拡大を防止することも可能である場合がある。例えば、チャージ経路が銀行口座からのチャージしかないのであれば、特定の期間におけるチャージ金額又は決済金額のいずれかの制限だけで、自動的に被害金額の最大値も制御できることになる。したがって、コード決済事業者は、自己のコード決済サービスの内容等を考慮しながら、チャージ金額又は決済金額について、何らかの形で上限額を設定することが必須である。なお、具体的にどのような条件で制限するかは各コード決済事業者の判断にゆだねられる。

⑵ モニタリング結果の活用

後記 8.2⑵のとおり、コード決済における不正抑制のためには、常時モニタリングを行うことが非常に重要であり、コード決済事業者はモニタリング体制を構築することが必須であるが、当該モニタリングの結果をチャージ時において活用することが考えられる。なお、モニタリング結果をどの時点でどのように活用するかはコード決済事業者の判断による。

7 決済時

7.1 総論

正当な権限のない者による不正な銀行口座の利用を防止するためには、銀行口座紐づけ時においてコード決済事業者が講ずる上記 5.2 の対策が最も重要である。もっとも、銀行口座の不正利用の未然防止や、不正に紐づけられた銀行口座が使用されることによる被害の拡大防止のためには、コード決済事業者による利用金額・回数の上限設定等、決済時における対策を行うことも重要である。

7.2 コード決済事業者による対策

⑴ 総論

本ガイドラインでは、決済時における具体的な不正利用防止対策として、以下⑵及び⑶にコード決済事業者において導入可能な対策を示している。他方、3 に記載のとおり、コード決済における不正利用の防止は、コード決済サービス全体（特にアカウント作成時から決済時まで）を通して実現されるものである。コード決済事業者は、正当

な権限のない者が銀行口座を不正利用するリスクや、利用者の利便性、各事業者が展開するコード決済サービスの内容等も考慮しながら、自己のコード決済サービス全体を通していかに不正利用を防止するかを検討し、複数の不正利用防止対策を組み合わせて実施することが重要である。

(2) 決済時における制限の設定

一定の条件で利用時の制限を設定する対策は、不正利用の被害拡大を防止する効果があるほか、利用上限が設定されていることにより、不正を行うインセンティブを減ずる効果も期待できる。なお、かかる制限については、必ずしも入金手段ごとに設ける必要はない。また、6.2(1)記載のとおり、コード決済サービスによっては、チャージというお金の入口か決済というお金の出口のいずれかで制限をかけることによって、被害拡大を防止することも可能である。したがって、コード決済事業者は、自己のコード決済サービスの内容等を考慮しながら、チャージ金額又は決済金額について、何らかの形で上限額を設定することが必須である。

(3) モニタリング結果の活用

後記 8.2(2)のとおり、コード決済における不正抑制のためには、常時モニタリングを行うことが非常に重要であり、コード決済事業者はモニタリング体制を構築することが必須であるが、当該モニタリングの結果を決済時において活用することが考えられる。なお、モニタリング結果をどの時点でどのように活用するかはコード決済事業者の判断による。

8 常時行うべき対策

8.1 総論

コード決済における不正利用事案の発生及び被害の拡大を可能な限り防止するためには、上記 4 から 7 に記載する、アカウント作成から決済に至るまでの各段階における対策だけでなく、不正に対応する体制づくりをしっかりとコード決済事業者の内部で行い、常時、不正利用事案に対応し、対策できるようにしておくことが重要である。

8.2 コード決済事業者による対策

(1) 総論

本ガイドラインでは、常時行うべき不正利用防止対策として、以下(2)及び(3)にコー

ド決済事業者において導入可能な対策を示している。他方、3 に記載のとおり、コード決済における不正利用の防止は、コード決済サービス全体（特にアカウント作成時から決済時まで）を通して実現されるものである。コード決済事業者は、正当な権限のない者が銀行口座を不正利用するリスクや、利用者の利便性、各事業者が展開するコード決済サービスの内容等も考慮しながら、自己のコード決済サービス全体を通していかに不正利用を防止するかを検討し、複数の不正利用防止対策を組み合わせて実施することが重要である。

⑵ 不正に対するモニタリング体制の構築

上記 4.2(4)、5.2(5)、6.2(2)及び 7.2(3)で記載したとおり、アカウント作成から決済までの間においてモニタリングを前提としたモニタリング結果の活用は不正利用の防止において重要な役割を果たす。したがって、コード決済事業者は、不正検知のためのモニタリング体制を構築することが必須である。そして、コード決済事業者としては、自らが提供するコード決済サービスの内容や、利用者の利便性等も踏まえながら、正当な権限のない者による決済のリスクに見合った取引モニタリングを実施し、その精度向上・強化に努めていくことも必須である。

⑶ 不正検知をした場合の対応体制の整備

コード決済事業者が取引モニタリング等で不正な銀行口座紐づけや不正な決済を検知した場合、これに迅速に対応していくことが被害拡大の防止にとって重要となる。したがって、コード決済事業者は、不正の対応体制（インシデントレスポンス体制）を整備することが必須である。なお、不正事案の対応にあたっては、コード決済事業者自身が行うものだけでなく、金融機関、契約店、利用者、口座名義人等への調査依頼や連携等を通じて行うものもあり、これらが不正利用の被害拡大を防止することに役立つ可能性がある。不正の対応体制の整備にいては、以下の点にも留意しながら、自己のコード決済サービスにとって必要かつ十分な体制を構築することが必須である。また、不正の対応においては、現在発生している不正に起因する被害拡大防止だけではなく、事後的に当該不正事案の不正態様や対応内容を検証することで、再発防止や将来の新たな不正の防止に役立てていくことも必須である。

- ✧ 金融機関との関係では、個人情報保護法制等、情報を共有・連携することに伴う課題が生ずる可能性があること。
- ✧ 契約店との関係では、不正検知時は必要に応じて利用を一時的に止める等の措置を講じたうえ、調査への協力を依頼するとともに、契約店による行為が不正の原因となっているような場合には、加盟店規約等に基づき契約店に対して指導・解約等を含む適切な対応を講ずること。
- ✧ 利用者・銀行口座名義人との関係では、不正利用の検知は、取引モニタリン

グ等によるもののほか、窓口への問合せ等から発覚することもあるため、この点にも留意しながら問合せ窓口を適切に設置する必要があること。また、不正利用等に関する問合せ窓口の設置や寄せられた問合せへの対応等の措置を適切に講ずること。

9 今後について

9.1 本ガイドラインの改訂方針

本ガイドラインは、コード決済を巡る環境の変化や技術の発展等に応じ改訂が必要である。協議会は適時、本ガイドラインの改訂についての検討を行うものとする。

9.2 コード決済の発展に向けて

コード決済は、キャッシュレスの推進において今後重要な意味を持つと思われる。コード決済事業者及び金融機関のみならず、契約店や他の分野の事業者との連携も大切にしながら、関連事業者及び利用者の双方がともに利益を享受できるようなキャッシュレスの在り方を今後も引き続き模索していきたい。本ガイドラインがコード決済、ひいては日本のキャッシュレス社会の発展の一助になれば幸いである。

以上

PAYMENTS JAPAN