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

一般社団法人キャッシュレス推進協議会

Ver. 1.0

2019 年 4 月 16 日

【履歴】
2019 年 4 月 16 日　新規制定(Ver. 1.0)

目次

【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
オーソリゼーション	クレジットカード名義人のクレジットカード取引について、その販売承認を取引ごとにクレジットカード事業者が承認、判定する処理
オーソリモニタリング	契約店（コード決済事業者を含む）から送信されるコード決済に係るオーソリゼーション電文で得られる情報等を用いて、正当な権限のない者による不正な取引か否かを判定するために行われるモニタリング
関連事業者	コード決済事業者、クレジットカード事業者、契約店等、クレジットカードに紐づい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
クレジットカード事業者	本ガイドラインでは、特に断りのない限り、クレジットカードを発行する会社（イシュア）を指す
クレジットカード番号等	クレジットカード番号、有効期限及びセキュリティコード
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

[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。

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
セキュリティコード	クレジットカード裏面又は表面に記載された 3 桁又は 4 桁の番号で、EC サイト等で取引を行う際にクレジットカード名義人に入力等を求めてクレジットカードを実際に手元に所持していることを確認するもの
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
端末識別番号	クレジットカード決済においてオーソリゼーションの送信等を行う決済端末を識別するため、当該端末ごとに付番される番号
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【店舗提示型】 MPM(Merchant-Presented Mode)」（Ver. 1.0、2019 年 3 月 29 日）
電文	一定の形式に従って記述された、システム間で送受信されるひとまとまりのデータ
バーコード	コード決済用の一次元コード
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. 1.1、2019 年 3 月 29 日）
EC サイト	インターネット上で商品・サービスを提供するウェブサイト
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、今般、当該コード決済サービスにおいて、クレジットカード番号等が不正利用される事案が発生した。

EC サイトにおける商品等の購買のようにクレジットカードを対面で提示しないケースにおける不正利用防止対策の１つとして、クレジットカード番号とは別にセキュリティコードを入力させる方法が広く一般的に行われてきた。また、コード決済において、あらかじめ登録しておいたクレジットカードでの支払を選択する場合、商品の購入自体は対面で行われるものの、クレジットカード自体は対面で契約店に提示しないため、不正利用防止対策として、EC サイト等における利用と同様にクレジットカード番号や有効期限等の名義人に関するデータをコード決済アプリに登録する際にはセキュリティコードの入力を求めることが一般的である。さらに、クレジットカード登録時において、不正利用者の総当たり攻撃によるセキュリティコード入力の突破を防止するために、セキュリティコードの入力回数に制限を設けていることも多い。しかし、今般判明した不正利用においては、不正利用者がクレジットカード番号、有効期限のみならず、セキュリティコードをも不正に入手した上でコード決済サービスを利用しているケースが多数であったことが判明しており、クレジットカード登録時におけるセキュリティコードの入力回数制限のみでは対策として十分でなく、セキュリティコードが流出している実態を踏まえた不正利用防止対策が必要であることが明らかとなった。

スマートフォンの普及に伴い、コード決済は、従来のクレジットカード、デビットカード、プリペイドカード等に加えて、新しいキャッシュレス決済手段としてその活用及び発展が期待されるところである。一方で、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、不正利用されたクレジットカードの名義人等、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、まずはコード決済サービスに関して想定される不正について幅広く洗い出し、その上で近時発生した上記の不正利用事案に対する早急な対応の必要性から、その対策についてはクレジットカード番号等の不正利用を中心に検討している。その中で、コード決済事業者及びクレジットカード事業者が、コード決済に係る

クレジットカード番号等の不正利用を防止するために参照すべき水準を定めている。もっとも、かかる不正利用防止対策の中には、クレジットカード番号等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当に阻害しないよう、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、コード決済事業者やクレジットカード事業者が講ずる不正利用防止対策では不十分な新たな不正が生じた場合、当該不正利用防止対策の実効性は損なわれる。コード決済事業者及びクレジットカード事業者においては、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

- 本ガイドラインでは、コード決済において想定される不正については、クレジットカード番号等の不正利用に限らず、広く記載している。
- 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、クレジットカード番号等の不正利用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、コード決済事業者及びクレジットカード事業者が行う必要のある対策を中心とするものである。
- 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クレジットカード事業者は、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、コード決済に係る不正について考えられる不正のケースを列挙するとともに、クレジットカード番号等の不正利用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

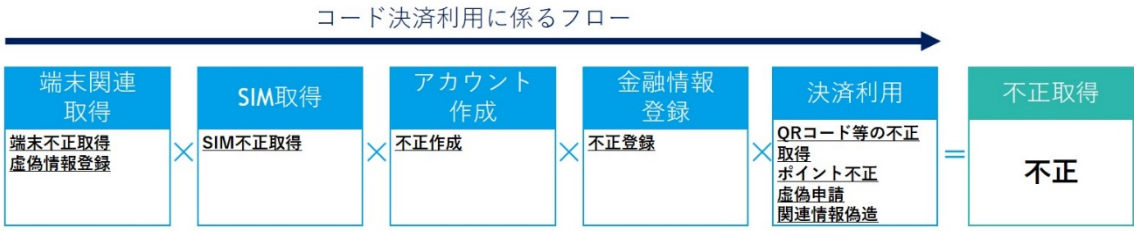
コード決済においては、モバイルデバイスを利用した決済のフローの各時点において、不正の可能性がある。関連事業者は、各時点において生じ得る不正の可能性を意識しながら、適時適切な不正利用防止対策を講ずることが重要である。

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、近時発生したクレジットカードの不正利用事案に対する早急な対応の必要性等から、流出したクレジットカード番号等の不正利用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クレジットカード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　　クレジットカード番号等の不正利用と検知のタイミング

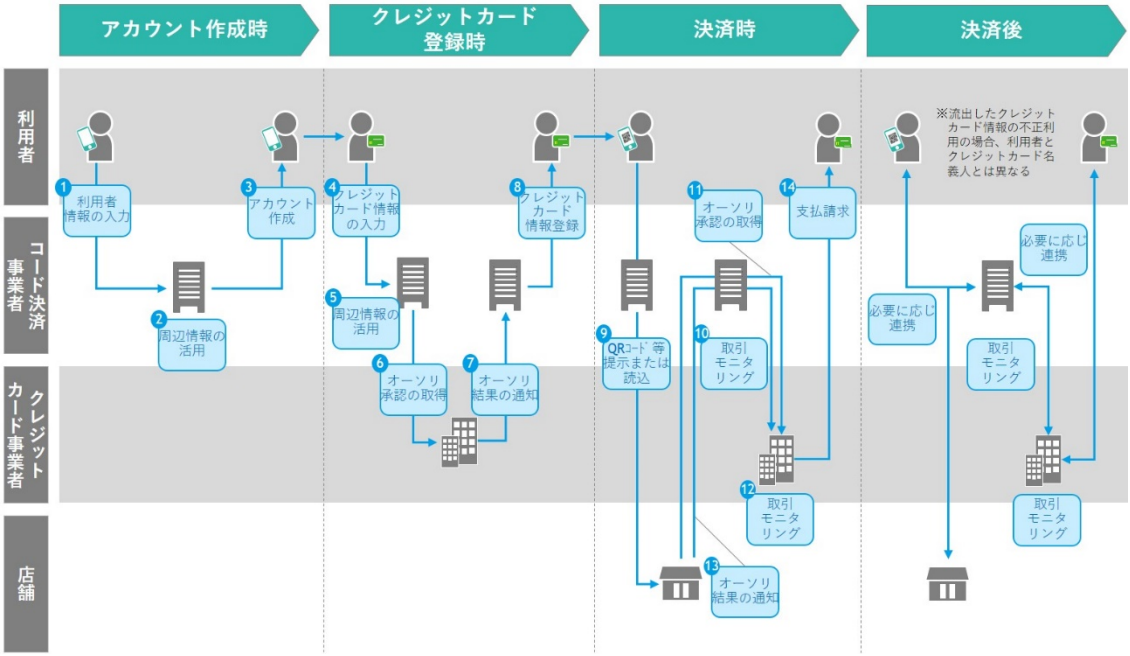
コード決済に係る不正利用防止対策及び不正検知の可能性を検討するに当たっては、コード決済の利用に係るフロー及びフローごとにコード決済に関わる者の役割や関連性等を検討していくアプローチが有用と考えられる（図 3 参照）。特に、流出したクレジットカード番号等の不正利用を防止するためには、コード決済アプリにクレジットカードを登録する時点において、当該不正流出したクレジットカード番号等を登録させないための対策をコード決済事業者、クレジットカード事業者において講ずることが最も重要な対策の一つとなる。一方で、不正流出したクレジットカード番号等の登録を完全に防止することは困難であるため、コード決済利用に係る各時点において、不正流出したクレジットカード番号等の登録の事前防止のみならず、仮に登録され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後までの各時点において、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。

4 以降では、上記対策を講ずることができる時点を、A アカウント作成時、B クレジットカード登録時、C 決済時、D 決済後の 4 つの時点に分類した上で、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、対策の一部を講じただけで直ちに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。コード決済事業者及びクレジットカード事業者においては、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、自らが直面するクレジットカード番号等の不正利用のリスクを正確に把握して、不正利用防止対策を実施していくことが重要である。

なお、コード決済サービス全体を通して 3D セキュアの導入又はこれと同等／相当のセキュリティ確保が可能である他の不正利用対策の実施が必須である。



※　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

クレジットカードを利用したコード決済において、コード決済アプリにクレジットカー

ドを登録しようとしている利用者が、当該クレジットカードの利用に関し正当な権限を有していれば（多くの場合、クレジットカード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、当該クレジットカードの名義人に対して身に覚えのない請求がな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クレジットカード登録時に至るまで、クレジットカード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、これをクレジットカード登録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クレジットカード番号等を登録する事態を防止していくことが重要である。

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)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クレジットカード番号等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、コード決済を行おうとする者が当該決済を行う権限がある者であることを担保するために、本人認証を行うことが重要である。コード決済事業者は、本人認証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。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、利用者の氏名等特定の項目の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。

アカウント作成時における本人認証の主な目的は、アカウント作成の際に情報を入力する者が、当該入力につき正当な権限があること（多くは、利用者の属性に関する情報が、アカウント作成の際に入力される情報と一致すること）を確認する点にあり、コード決済に紐づけられたクレジットカード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。しかしながら、かかるアカウント作成時に収集された情報がその後のクレジットカード登録時、決済時、決済後における不

正対策に役立てることができる可能性がある。

コード決済事業者においては、アカウント作成時における本人認証の際に収集する情報が正当な権限のない者によるクレジットカード番号等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、利用者の入力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クレジットカード番号等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。

5 クレジットカード登録時

5.1 総論

クレジットカード番号等の不正利用を防止するには、コード決済アプリにクレジットカードを登録する時点において、不正流出したクレジットカード番号等を登録させないための対策を講ずることが最も重要である。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クレジットカード番号等の登録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。

クレジットカード事業者においても、クレジットカード登録時において、登録を行おうとする者が登録に関して正当な権限を有していないリスクを踏まえた本人認証を行っていくことが重要である。こうしたリスクを踏まえた本人認証その他の対策を講ずるに当たっては、コード決済事業者・クレジットカード事業者相互で情報を連携する方法が一つの有用な方法となり得るが、これらの手法については、5.4 で述べる通り、システム開発の負荷や、個人情報保護との関係等、その実現可能性も含めて課題が認められる。

5.2　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、クレジットカード登録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(5)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クレジットカード番号等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) クレジットカードに係る「券面認証」（入力回数制限を含む）

セキュリティコードによる認証（券面認証）は、使用するクレジットカード番号が真正であることをクレジットカード事業者が確認できるのみならず、クレジットカードを物理的に保有していない者が、クレジットカード番号と有効期限のみでコード決済アプリに登録することを防止する効果を有している。

しかしながら、セキュリティコードの入力回数に制限がない場合、クレジットカード番号・有効期限のみを不正に取得した者が、任意のセキュリティコードの入力を繰り返し行うことにより、正当な権限を有することなくコード決済アプリにクレジットカードを登録し、当該クレジットカードによる決済が可能となる。こうした事態を防止するためには、クレジットカード事業者と同様、コード決済事業者においても、クレジットカード登録時において、セキュリティコードによる認証を利用者に対して求めるとともに、その入力回数を制限することが必須である。

もっとも、この対策は、クレジットカード番号・有効期限とともにセキュリティコードも流出している場合には実効性がない。そのため、コード決済事業者においては、セキュリティコードの入力回数制限のみでは根本的な不正利用防止対策とはならないことを前提とした上で、その他の有効な手法の導入と併せて対策を講ずることが必須である。

(3) クレジットカードに係る「本人認証」の活用

クレジットカード事業者が提供する本人認証の手法としては、EC サイトにおけるなりすまし不正利用防止のための本人認証の具体的手法として、クレジットカード名義人のみが知るクレジットカード事業者へ事前に登録したパスワード等を、当該クレジットカード事業者が照合することにより、クレジットカード名義人がクレジットカードを使

用していることを確認する「3D セキュア」等がある。

コード決済事業者は、正当な権限のない者がクレジットカード番号等を不正に登録するリスクや、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、リスクに見合った本人認証の方法を選択することが必須である。

また、本人認証の方法については、コード決済事業者が採用するのみでは十分でなく、利用者がクレジットカード番号等の不正利用のリスクを理解した上で積極的に採用することが必要となる。コード決済事業者としては、クレジットカード事業者とも連携しながら、クレジットカード番号等の不正利用のリスク、各コード決済事業者が講ずる上記の 3D セキュア等による本人認証の意義等につき、利用者に対して周知し、その採用を働きかけていくことが推奨される。

⑷ クレジットカード登録時までに収集した情報の活用

不正に取得されたクレジットカード番号等の登録を防止するには、コード決済事業者がクレジットカード登録時までに収集した情報を活用し、コード決済アプリへのクレジットカードの登録についての属性・行動分析を行うことが有効である。

なお、かかる情報の利用可能性は、コード決済サービス等に係る利用規約・プライバシーポリシー等によって異なるものであり、入手可能な情報の内容も、コード決済事業者のサービスの内容等によっても異なるものである。

コード決済事業者は、クレジットカード登録時までに収集した情報が正当な権限のない者によるクレジットカード番号等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、これらクレジットカード登録時までに収集した情報の活用を検討・判断することが必須である。

また、コード決済事業者が収集した上記の情報をクレジットカード事業者と連携し、クレジットカード事業者によるコード決済へのクレジットカードの登録の可否の判断に活用していくといった方法も考えられる。その前提として、コード決済事業者は、クレジットカードの登録にかかるオーソリゼーション電文をクレジットカード事業者に対して送信し、承認を取得することが必須である。

⑸ その他の手法

不正利用防止対策の一環として、①同一クレジットカードの複数アカウントへの登録制限、②同一アカウントへのクレジットカードの登録数の制限といった措置を講じている例もみられる。①については、不正に入手した1つのクレジットカード番号等の複数のアカウントへの登録、②については、不正に入手した多数のクレジットカード番号等の同一アカウントへの登録を防止し、いずれも安易なクレジットカード番号等の不正利用を抑止する事実上の効果が認められる。しかしながら、①②だけで実効的な不正利用防止対策となるものではない。

本手法を導入する際の留意点として、正当な権限のない者がクレジットカード番号等を不正に登録するリスクや、正当な権限に基づき許容される利用と不正利用との区別、不正利用防止対策としての実効性等も考慮しながら、正当な権限のない者によるクレジットカード番号等の登録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必須である。なお、この際、具体策として、モバイルデバイスまたはアカウントに登録できるクレジットカードの枚数の上限を各コード決済事業者の判断に応じた枚数で設定することは必須である。

5.3 クレジットカード事業者による対策

(1) クレジットカードの登録に係る本人認証及び有効性確認の実施

クレジットカード登録時における利用者による 3D セキュアのパスワードの入力、またクレジットカード事業者によるそれら情報の照合等については、利用者の理解と協力が必要であることから、クレジットカード事業者においては、クレジットカード名義人に対し、不正利用防止対策やパスワードの登録等について啓発を行うことが必須である。

また、コード決済事業者がクレジットカード登録時にクレジットカードの有効性確認をクレジットカード事業者に求める場合（1円オーソリなどと呼ばれる）において、クレジットカード事業者は、オーソリゼーション情報を活用したオーソリモニタリングにより、正当な権限を有しない者にクレジットカード番号等を登録させないよう、必要に応じてコード決済事業者と連携し、不正検知に努めることが必須である。

なお、上記に加え、コード決済事業者がクレジットカード登録時までに収集した情報等も活用していくことが有効であるが、その実現可能性や課題等については、5.4にて後述する。

(2) クレジットカードが登録された事実のクレジットカード名義人への通知

クレジットカードが登録された事実がクレジットカード名義人に通知される等の方法により、クレジットカード名義人の了解なくコード決済アプリに自己のクレジットカードが登録された事実を把握できれば、クレジットカード名義人自らが不正利用の被害を防止するための対策を講ずることが可能となる。

もっとも、メール受信に関するクレジットカード名義人の同意が必要であることや、クレジットカード事業者においてクレジットカード名義人のメールアドレスの登録・更新が必要となる等の課題があり、全てのクレジットカード名義人に対してメールによる通知ができるわけではない。

このような状況において、コード決済アプリにクレジットカードが登録された事実をクレジットカード名義人に通知する枠組みを新たに構築するには、その実現可能性や

費用対効果が課題として挙げられる。

5.4 クレジットカード登録時における、コード決済事業者・クレジットカード事業者間の情報連携

コード決済サービスの利用者がコード決済アプリにクレジットカードを登録する際に、正当な権限を有していることを確認するためには、コード決済事業者とクレジットカード事業者が有している情報を相互に連携することが、一つの有用な対策となり得る。

もっとも、かかる情報連携をするには、既存のシステムの変更や新たなシステムの構築が必要となることが想定される。加えて、個人情報保護法制等、情報を保有・連携することによって生ずる課題もある。

コード決済事業者・クレジットカード事業者（コード決済アクワイアラを含む。）においては、こうした課題を踏まえ、情報連携の枠組みの構築に向けて、引き続き検討していくことが推奨される。

6 決済時

6.1 総論

正当な権限のない者による不正なクレジットカード番号等の利用を防止するためには、クレジットカード登録時においてコード決済事業者及びクレジットカード事業者が講ずる上記 5 の対策が重要である。もっとも、クレジットカード番号等の不正利用の未然防止や、不正に登録されたクレジットカード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・回数の上限設定や、コード決済事業者・クレジットカード事業者による取引モニタリング等、決済時における対策を行うことも重要である。

6.2 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、決済時における具体的な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クレジットカード番号等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の上、実施することが重要である。

⑵ 利用者の決済時における金額や利用回数等の上限設定

コード決済事業者の中には、決済に係る金額や利用回数の上限値を設けている例もある。こうした対策は、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。

コード決済事業者は、正当な権限のない者がクレジットカード番号等を不正に用いて決済するリスクや、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、上限設定の要否を検討し、上限設定をする場合には、対象となる利用者、上限設定の単位（アカウント単位とするか端末単位とするか等）、決済時の金額・利用回数等の上限値設定を実施することが必須である。

⑶ 取引モニタリング結果の決済への活用

コード決済事業者は、正当な権限のない者がクレジットカード番号等を不正に用いて決済するリスクや、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つつ、コード決済に係る取引モニタリングを実施し、その結果に基づき正当な権限のない者による決済のリスクに見合った金額・利用回数の上限設定や追加の本人認証を実施する等の措置を講ずることが必須である。

なお、コード決済事業者とクレジットカード事業者とが連携してクレジットカード事業者によるコード決済に係るオーソリモニタリングの精度を向上するためには、コード決済事業者は、コード決済の都度オーソリゼーション電文をクレジットカード事業者に送信し、その承認を取得することが必須である。

6.3 クレジットカード事業者による対策

⑴ コード決済に係る不正検知の精度向上・強化

クレジットカード事業者では、モニタリングの精度向上・強化に努めていくことが必須である。

クレジットカード事業者による不正検知の精度向上・強化に当たっては、クレジットカード事業者が保有する情報のみならず、コード決済事業者が保有するコード決済に係る情報も併せて活用し、正当な権限のない者によるクレジットカード決済の不正検

知の精度を向上・強化していくことが推奨される。

6.4 決済時における、コード決済事業者・クレジットカード事業者間の情報連携

クレジットカード事業者がコード決済に係るオーソリモニタリングの精度を向上・強化させるためには、オーソリゼーション電文を通じてコード決済事業者から提供される情報がより細分化・精緻化されることが重要である。コード決済事業者・クレジットカード事業者（コード決済アクワイアラを含む。）において、その細分化・精緻化を含む適切な情報連携の枠組みを継続的に検討していくことが推奨される。

7 決済後

7.1 総論

コード決済に紐づいたクレジットカード番号等の不正利用による被害の拡大を可能な限り防止するためには、正当な権限のない者による決済に対し、コード決済に関わる全ての者が速やかに当該不正を検知し、適切に対応できる環境づくりが重要である。

7.2 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、決済後における具体的な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クレジットカード番号等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、不正利用防止対策を実施することが重要である。

(2) 不正検知の精度向上・強化

上記 6 で記載した不正検知の枠組みは、決済時における金額・回数等の上限設

定や追加の本人認証の実施等、正当な権限のない者による不正な決済の未然防止に資するのみならず、決済後の不正検知においても有効なものとなる。

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が必須である。

(3) 決済後の対応

コード決済事業者が取引モニタリング等で正当な権限のない者による決済を検知した場合、クレジットカード事業者、契約店、利用者、クレジットカード名義人等への調査依頼や連携等を通じて、不正利用の被害拡大を可及的に防止するとともに、以下の点にも留意しながら、原因究明・再発防止を図っていくことが必須である。

- ✧ クレジットカード事業者との関係では、共有・連携する情報の内容及び範囲により、上記 5.4、6.4 で述べたのと同様、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・クレジットカード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。

7.3 クレジットカード事業者による対策

(1) コード決済に係る不正検知の精度向上・強化

上記 6.3 で述べた決済時の場合と同様、クレジットカード事業者は、決済後においても、コード決済に係る不正検知の精度向上・強化に努めることが必須である。

コード決済事業者・クレジットカード事業者間で共有する際には、上記 6.4 で記載した内容と同様の課題が想定される。

(2) 決済後の対応

流出したクレジットカード番号等を用いてコード決済が不正に行われた事実は、クレジットカード名義人からクレジットカード事業者への連絡等により発覚することも想定される。こうした場合、クレジットカード事業者としては、不正がコード決済によるも

のであるか等の事実を調査した上、コード決済事業者・クレジットカード名義人等への調査依頼や連携等を通じて、不正利用の被害拡大を可及的に防止するとともに、以下の点にも留意しながら、原因究明・再発防止を図っていくことが必須である。

- ✧ コード決済事業者と共有・連携する情報の内容及び範囲により、上記 5.4、6.4 で述べたのと同様、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。
- ✧ クレジットカード名義人との関係では、名義人による利用履歴の確認やクレジットカード事業者からの連絡への対応等、不正検知や原因究明・再発防止には名義人の協力が必要となるため、この点に関して名義人への周知や理解を得ることが重要であること。

7.4 決済後における、コード決済事業者・クレジットカード事業者間の情報連携

決済後においても、コード決済事業者・クレジットカード事業者双方において適切な情報連携の枠組みを継続的に検討していくことが推奨される。

8 コード決済事業者・クレジットカード事業者間の情報連携

不正流出したクレジットカード番号等がコード決済に用いられる場合、利用者とクレジットカード名義人が同一人でないため、不正利用防止や決済後の対応等においては、コード決済事業者とクレジットカード事業者とで、利用者・クレジットカード名義人に関して保有する情報や、決済の情報等を相互に連携することが有効となり得る。

一方で、これまで述べてきたとおり、上記の情報等を相互に連携するには、既存のオーソリゼーションの枠組みの変更や、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ことが想定される。

コード決済事業者・クレジットカード事業者においては、例えば既存のオーソリゼーションの枠組みの中でも対応可能と思われる情報の連携、細分化・精緻化等をはじめとして、上記諸点につき、継続的に検討していくことが推奨される。

その他、不正利用の未然予防という見地からは、コード決済事業者・クレジットカード事業者双方において、過去に経験した不正利用の事案やその対処方法、その他不正の手法や対策、関連事情に関する最新の動向等につき、協議会等の場において情報共有する枠組みを構築することも有用と考えられる。

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クレジットカード事業者のみならず、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