資金決済業者等とクレジットカードとの連携に係る本人認証等セキュリティガイドライン

（2021 年 3 月 24 日制定）

一般社団法人
日本クレジット協会

１．はじめに

- 今般、悪意のある第三者が不正に入手した預金者の口座情報等をもとに当該預金者の名義で資金移動業者のアカウントを開設し、銀行口座と連携したうえで、銀行口座から資金移動業者のアカウントへ資金を口座引落しすることにより不正な出金を行う事象が複数発生した。
- キャッシュレス化において決済手段の連携が進むなか、今後も上記のような他の決済手段との連携の仕組みを悪用した犯罪による被害の発生が懸念される。
- 資金決済業者と連携しているクレジットカード取引に関しても、クレジットカード番号等の不正利用等により同様の事象が発生する可能性があるところ、本ガイドラインはクレジットカード会社が取組むべき不正防止策を中心に取りまとめた。
- 当協会の会員であるクレジットカード会社においては、本ガイドラインの趣旨を踏まえ、自らの提供するサービスを改めて検証し、本ガイドラインに沿った対応を実施することで不正防止に取組むことが求められる。

１．１　ガイドラインの適用範囲

- 本ガイドラインでは、当協会会員であるクレジットカード会社がコード決済サービス等[1]を提供する資金決済業者(以下「資金決済業者」という。)と連携する場合において、クレジットカード会社が取組む必要のある措置を中心に記載している。
- 連携先である資金決済業者が行う取組みについては、クレジットカード業界の横断的な取組みとして、クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」において連携先に求める対策のほか、関係省庁、関係団体等のセキュリティ対策に関する指針やガイドラインの遵守を前提に、連携先の取組みについて確認するべき事項、及び相互に協力すべき事項を中心に記載している。
- また、なりすましによる不正防止の観点から、オンラインでのクレジットカード申込受付における本人確認等の対応についても記載している。

[1] クレジットカードに 2 次元バーコード、QR コード等の決済用情報を紐づけて行う決済、及びチャージ。

１．２　ガイドラインの位置づけ

- 本ガイドラインは、資金決済業者と連携する場合において、当協会の会員であるクレジットカード会社における不正防止のための取組み及び具体的事例等を示すものである。
- クレジットカード会社は、本ガイドラインに示す取組みの実施にあたっては、自社の取組みに加え、資金決済業者等をはじめ関係各社の業界団体等による指針やガイドライン等も参照のうえ、連携する資金決済業者の不正防止策の取組み状況を踏まえた取引の真正性を確認するなど、的確な対応が求められる。
- なお、本ガイドラインに記載されている取組みが「クレジットカード・セキュリティガイドライン」に規定される取組みである場合には、割賦販売法第 35 条の 16、第 35 条の 17 の 8、第 35 条の 17 の 15 の運用指針として位置づけられているものである。

２．資金決済業者との連携における不正防止

クレジットカードを、資金決済業者が提供するコード決済サービス等と連携する取引において、不正な手段で入手したクレジットカード番号等を連携された場合、反復的に不正なチャージが行われるなど高額な不正利用被害が発生する蓋然性が高いことから、コード決済サービス等の連携、決済の各プロセスにおいて、以下の対策を講じることとする。

２．１　資金決済業者とのコード決済サービス等利用に関する契約締結前

２．１．１　リスク評価等

資金決済業者と連携することにより生ずるリスクを含め、サービス全体のリスクを評価する。

その際、資金決済業者による本人確認、実在性の確認、クレジットカードとの連携、チャージ、決済等の一連のプロセスにおいて脆弱性がないか確認し、問題があると認められた場合には、本人認証等の内容、方法の変更等、対策を講じたうえで資金決済業者との連携を行う。

２．１．２　クレジットカード会社が確認すべき連携先である資金決済業者の不正防止策

連携先である資金決済業者の不正防止策について、クレジットカード会社が確認すべき事項は以下のとおり。

・２．１．１のリスク評価を踏まえ、コード決済サービス等とクレジットカードの連携時において、資金決済業者における認証手段及び方式がリスクに見合った実効的な不正防止策となっているか。[2]

・連携先の資金決済業者において、認証に用いる情報の登録・変更手続きに堅牢な認証を求めているか。

２．２　コード決済サービス等がクレジットカードと紐づけられる時

２．２．１　不正防止策の実施（本人認証等）

連携先の資金決済業者との連携時における各プロセスにおいて、下記の複数の対策を組み合わせることにより、多面的・重層的なセキュリティ対策を講じる。

・オーソリゼーションによるモニタリング

・セキュリティコードの照合及び入力回数の制限

・3-D セキュアにおけるパスワード照合及びリスクベース認証、等

「3-D セキュア」については、現行バージョン 1.0 より精度が向上した EMV 3-D セキュアを早期に導入することとし、併せてリスクベース認証を実施する。また、EMV 3-D セキュアに移行するまでの間 1.0 で対応する場合にはリスクベース認証を導入する。

EMV 3-D セキュアでは、加盟店である資金決済業者がクレジットカード会員の同意を取得したうえで、資金決済業者が取得したクレジットカード会員に関する情報等をクレジットカード会社に提供し、クレジットカード会社が提供されたクレジットカード会員情報を利用し本人認証を行う。クレジットカード会社において本人認証のリスクが高いと判断した場合は、当該取引の拒否、クレジットカード利用者本人だけが知りうる情報による追加認証、又はクレジットカード利用者本人に対しての連携の事実を確認するための通知を行う。

クレジットカード会社及び資金決済業者は、コード決済サービス等の利用者

---

[2] 前払式支払手段のリスク・特性に応じて、例えば、チャージ金額が多額である場合には、認証の要素を追加するなどの措置が考えられる。

に対し、3-D セキュア等による本人認証の必要性、利用方法やパスワードの登録等について啓発を行う。

２．３　コード決済サービス等の利用時

２．３．１　不正検知のモニタリング

クレジットカード会社は、不正検知のモニタリングにより、コード決済サービス等に係るクレジットカード取引において不正利用が行われていないかモニタリングを行う。

モニタリングでは、コード決済サービス等のリスク・特性に応じ、取引の頻度や金額等に関して、適切なシナリオ・閾値を設ける。

早期に不正の疑いのある取引を検知できるよう過去の不正利用、詐欺被害、捜査機関等からの照会事例を分析し、その結果を不正検知モニタリングに反映させるなど、モニタリングの精度向上・強化に努める。

不正な取引のおそれがある場合、或いは不正な取引が認められた場合には、契約のある連携先の資金決済業者と情報を共有する。また、これらの不正な取引に関する情報の提供を受けた資金決済業者が、必要に応じてコード決済サービス等の一時的な利用停止等を実施すること、十分な調査を実施すること、コード決済サービス等の利用者に通知することを適切に実行するための態勢を整備する。

２．３．２　連携先の資金決済業者との契約等における必要な対応

クレジットカード会社におけるモニタリング態勢整備等のため、クレジットカード会社は、連携する資金決済業者との間の契約等において、認証方法、モニタリング態勢や不正が検知された場合の対応等について、あらかじめ具体的に定めておく。

その際、連携する資金決済業者との役割分担や責任を明確化する。

２．４　コード決済サービス等の利用後

２．４．１　利用者への相談対応・情報提供

クレジットカード会社は、今後コード決済サービス等あらゆる金融サービスとの連携の促進が見込まれることから、サービスの利用者からの相談、問合せ対応に関する連携する資金決済業者との協力体制、責任関係の明確化等により、複数の決済手段の連携によって消費者に混乱が生じないよう十分留

意する。

相談窓口については、消費者が安心してアクセスできるように、メールや電話等、一般にアクセス可能な方法を確保するとともに、広く周知する。

連携先の資金決済業者と相互に相手方への相談を促すこと（たらい回し）などの不適切な対応を行っていないか検証し、不適切な対応が認められる場合には、連携先の資金決済業者とともに、発生原因の究明、改善措置、再発防止策を的確に講じる。

不正発生後、不正検知や原因究明・再発防止にはクレジットカード利用者の協力が必要となる点に関して、クレジットカード利用者への周知や理解を得ることが重要であることに留意しながら原因究明・再発防止を図る。

３.不正利用が発生した場合の対応態勢等

不正利用が発生した際、クレジットカード会社は迅速な対応を行うために、あらかじめ緊急連絡ルートや指揮命令系統の構築、連携先の資金決済業者との連絡態勢、コード決済サービス等の停止の手続等について定めておく。

クレジットカード会社がコード決済サービス等の取引において不正利用の疑いがある場合、対象の契約のある連携先の資金決済業者に通知のうえ、被害の拡大防止に向けた対応を行う。

クレジットカード会社が複数の連携先である資金決済業者と連携している場合において、他の連携先である資金決済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、被害拡大防止のため、当該他の連携先である資金決済業者に対しても連絡し、必要な対応を実施する。

利用者の不安や混乱を回避するため、クレジットカード会社及び連携先である資金決済業者は適時・適切な情報発信・対外公表を行うよう努める。

クレジットカード会社は、連携先である資金決済業者の関係者と連携のうえ、事実関係を調査し、被害の対象となったクレジットカード利用者への通知や相談対応を行う。

連携先の資金決済業者が提供するコード決済サービス等の利用者が、自身の責任によらず被害に遭われた場合、クレジットカード会社は当該利用者の負担とするなどの不利益が生じることのないよう、適切に対応するとともに、あらかじめ連携先である資金決済業者との間で、利用者保護を最優先とした支払いに関する方針について合意しておく。

４.その他、オンラインでのクレジットカード申込受付時におけるなりすましによる不正防止

オンラインでのクレジットカード申込は、漏えいした個人情報等を利用した、なりすましによる不正なクレジットカード申込、受領が発生する可能性がある。

「犯罪による収益の移転防止に関する法律（以下「犯罪収益移転防止法」という。)」に基づく取引時確認として、犯罪収益移転防止法施行規則第６条第１項第１号による、本人確認義務履行のためのｅKYC[3]による方法や本人確認資料の写し２点の徴求による方法、また犯罪収益移転防止法施行規則第13条第１項第１号による銀行での取引時確認済みの確認(銀行依拠)による方法等が行われているが、これらに加え、クレジットカード会社ではクレジットカード等の転送不要かつ簡易書留、又は本人限定郵便での送付や、宅配業者が提供する受取確認サービス等による配送等により、なりすましによる不正の防止を行う。また、その後の使用状況等について継続的にモニタリングを実施する。

クレジットカードの券面を発行しない契約(バーチャルカード)の場合には、申込者本人へのメール、SMS、アプリ等による通知、確認書類の転送不要での郵送等により、なりすましによる不正の防止を行う。

また、オンラインでのクレジットカード申込受付の際に、銀行依拠による取引時確認を実施する場合は、提携先の銀行における取引時確認の実効性を確認、その後なりすましによるクレジットカードの不正利用の早期発見のための不正検知モニタリングを行う。

[3] 「electronic Know Your Customer」の略称で、 オンラインで本人確認が行える技術のことを指す。犯罪収益移転防止法施行規則において、第６条第１項第１号にてその手法が規定されており、第６条第１項第１号ホ「顧客等から、特定事業者が提供するソフトウェアを使用して、本人確認用画像情報の送信を受ける方法」や、第６条第１項第１号チ「非対面取引において、特定事業者が提供するソフトウェアを使用して、本人確認用画像情報の送信を受けるとともに、顧客等の住居に宛てて、転送不要郵便等を送付」する方法などがある。

５. 当協会の対応

当協会は、本ガイドラインを協会会員に周知するとともに、適時に本ガイドラインの適切性を評価し、必要に応じ改定を行う。

以上