クレジットカード取引における セキュリティ対策

ークレジットカード不正利用被害防止に向けた取組みについてー

一般社団法人 日本クレジット協会

クレジットカード市場と不正利用被害の発生状況

わが国では、政府が成長戦略の一環としてキャッシュレス決済の推進を図っています。具体的には大阪万博が開催される2025年6月までにキャッシュレス決済比率40%をめざすことにしています。このため政府はこれまで、2019年10月～2020年6月にかけて、消費税率引上げに伴う需要平準化の対策として、中・小規模事業者を対象とした「キャッシュレス・ポイント還元事業」を実施するなどの後押しをしてきました。

また社会的にも、2020年以降新型コロナウイルスの流行による巣ごもり消費などにより、インターネットによる通信販売(EC取引)が、2021年には20.7兆円(前年比7.35%増)と大きく伸びていますが、このようなEC取引の決済方法として、キャッシュレス決済が利用されることが多く、キャッシュレス決済にとっては追い風となっています。さらに、コロナ禍では、対面での取引においても人と接触する機会をなるべく少なくしたいという衛生面の観点から、キャッシュレス決済を利用するという消費者の方が増えています[*1]。

このような動きもあり、2022年のわが国のキャッシュレス決済は111兆円、比率としては36.0%に達しています。もちろん、これらのすべてがクレジットカード(カード)によるものではありません。電子マネーやコード決済も含まれており、これらの決済方法も順調に推移していますが、カードによる決済はそのうち93.8兆円、比率で30.4%と圧倒的なウェイトを占めています[*2]。

しかし、このようにキャッシュレスの市場が拡大することにより、残念ながらそのしくみを悪用する不正利用被害も増大しています。2022年のカード不正利用による被害額は436.7億円に上ります。そのうち、EC取引など「非対面取引」で不正に利用される「番号盗用」という手段による被害額が411.7億円と全体の94.3%を占めています。一方で、約300億円まで被害額が拡大していた2002年当時は、「偽造カード」による不正利用被害額は165億円、全体の56.6%を占めていましたが、カードのIC化対応により2022年には1.7億円、0.4%まで減少しています[*3]。

カード取引における不正利用防止対策

カード取引における不正利用の防止対策については、これまでもカード会社や加盟店を中心に取り組んできたところですが、カード取引に携わるプレーヤーの多様化や不正利用手口の巧妙化等に対応していくため、2015年からはカード取引にかかわる幅広い事業者や業界・消費者

＊1 経済産業省「電子商取引に関する市場調査の結果を取りまとめました」https://www.meti.go.jp/press/2022/08/20220812005/20220812005.html
＊2 経済産業省「2022年のキャッシュレス決済比率を算出しました」https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html
＊3 (一社)日本クレジット協会「クレジット関連統計」四半期調査：クレジットカード不正利用被害額調査
https://www.j-credit.or.jp/information/statistics/index.html

団体、行政等から成る「クレジット取引セキュリティ対策協議会」（以下、協議会）を設置し、取組みを強化しています。

協議会では、2016年以降「カード情報保護対策」や「対面取引、非対面取引における不正利用防止対策」を実行計画として取りまとめ、推進しています。2020年4月からはカード取引に関係する事業者が実施する具体的なセキュリティ対策を示す「クレジットカード・セキュリティガイドライン」を策定し、安全・安心なカード利用環境の整備に取り組んでいます。特に、昨今のカードの不正利用被害のほとんどが、既に述べたように、番号盗用による「非対面取引」によるものであることから、協議会では、特に「非対面取引におけるセキュリティ対策」に力を入れて取り組んでいます。

（1）最近のカードの不正利用を目的とした、カード情報等盗用の主な手口と対策

①サイバー攻撃等不正アクセスによるカード情報等の漏えい防止対策

不正利用者は、カード情報等を不正に詐取するため、カード決済に関係する事業者に対して、サイバー攻撃などによる不正アクセスやマルウェアを用いたシステムの改ざんなどを行ってきます。このためカード情報を取り扱う事業者は、VISA（ビザ）やMastercard（マスターカード）、JCBといった国際ブランドが共同で策定した国際的なデータセキュリティ基準である「PCI DSS（Payment Card Industry Data Security Standard）[*4]」に準拠することにより防御することが求められています。これに加え、多くの加盟店はカード情報等の漏えいをしないよう、そもそもカード情報を持たない「非保持化」という方法でも対応しています。

②フィッシングによるカード情報漏えい防止対策

「フィッシング」とは、カード会員等にカード会社や宅配便業者、ショッピングサイトなど実在する企業を装った電子メールを送り、企業のホームページと酷似した偽物のウェブサイトに誘い込み、カード番号、アカウント情報（ユーザID、パスワード等）、暗証番号等を入力させて詐取し、当該カード会員本人になりすましてネット通販などで買い回りや、サービスの不正受領を行う“不正行為”です。

このようなフィッシングに対して、カード会社では、第三者がカード会社のドメイン名に「なりすまし」て消費者に送信するメールを検出することができる送信ドメイン認証技術（DMARC等）の導入を進めています。このしくみを導入することにより、メール受信者に表示される送信者アドレスの詐称によるなりすまし送信を検出し、なりすましメールを受信拒否するなどの対応を行っています。

③カード決済時の不正利用防止対策

このように不正アクセスやフィッシングなどに対して防止対策を講じていますが、それでも防ぎ切れずにカード情報等が漏えいしてしまった場合、カード決済時の不正利用を防止する対策を講じています。

カードが利用者の手元にあるかどうか確認するためのセキュリティコードや、利用者が真正なカード会員本人かを認証するサービスである3-Dセキュアなどを活用しています。

現在は、さらにセキュリティレベルを上げるため、3-Dセキュアの後継でより精度の高い“EMV 3-Dセキュア”の導入に取り組んでいます。EMV 3-Dセキュアは、カード決済時に、カード会員本人かどうかを利用者の属性情報やデバイス情報などを活用することによりリスク判定し、一定以上のリスクが認められた場合に、カード会員がカード会社に事前に登録しているID・パスワードの入力や、事前に登録している携帯電

＊4　安全なネットワークの構築やカード会員データの保護など、12の要件に基づいて約400の要求事項から構成されている

話番号やメールアドレスにワンタイムパスワードを受信して入力することにより、カード会員本人であることを確認したうえで決済が行われるようにするというものです。

カード会員が取り組むセキュリティ対策の重要性

前述のとおりカードの不正利用に対してさまざまな防止措置を講じていますが、これらの対策の多くはカード会員の方々の協力がないとその効果が限定的になる、あるいは、そもそも対策自体が成り立たないというものになります。

不正利用の被害にあわないためには、カード会員ご自身も、カード決済システムの一員であることをご理解いただき、セキュリティ対策に取り組んでいただくことが重要になります。

(1)「フィッシング」被害にあわないための対策

フィッシングメールにより、偽サイトに誘導され、不正利用に必要な各種情報を詐取されてしまうと、真正なカード会員の情報でのアクセスが可能になり、不正利用を防ぐことが難しくなってしまいます。メールやメールに記載されたリンク先で、カード番号、アカウント情報(ユーザID、パスワード等)、暗証番号等についての問い合わせや、回答を求められた場合には、そのまますぐに情報の入力や回答をせず、改めて当該事業者等の公式ホームページや問い合わせ窓口からアクセスし直すなど、情報を詐取されないよう注意する必要があります。

なお、複数のウェブサイト(オンラインサービス)等で同じIDやパスワードを利用すると、フィッシング等によりユーザIDやパスワードが詐取された場合、ほかのウェブサイト(オンラインサービス)等にもアクセスされ、不正利用被害にあうリスクが高くなります。IDやパスワードの使い回しはせず、ウェブサイトごとにどのような情報が登録されているかをしっかり把握しておくことが必要です。

(2)番号盗用による「なりすまし」被害にあわないための対策

EC取引において第三者のなりすましによる不正利用がなされないために、カード会社や加盟店で取り組んでいるEMV 3-Dセキュアにおいては、カード決済をしようとしている人が、カード会員本人であることを証明するためにあらかじめカード会社に手続きをしておく必要があります。

具体的には、各カード会社に対してカード会員本人しか知らないID・パスワードを登録しておく、あるいはワンタイムパスワードを受け取るために携帯電話番号やメールアドレスを登録しておく、または、ワンタイムパスワードを組成するためのアプリケーションをダウンロードしておくなどの方法があります。このような登録等がなされていないと、EC取引等のカード決済で、本人を確認する必要が生じた場合に、カード会員本人を証明する術(すべ)がないため、カードの決済が利用できない可能性もありますので、この点からも注意が必要です。

経済産業省の審議会においても、2025年4月以降、原則としてすべてのEC加盟店においてEMV 3-Dセキュアの導入を義務づけることについての提言がなされています[*5]。カード会員の方々には、それまでに各カード会社が求めるID・パスワードや、携帯電話、メールアドレス等の登録手続きを完了していただく必要があります。そのため、カード業界では、業界のセキュリティ対策の取組状況とカード会員の方々の協力を得るための周知・啓発活動を継続的に実施しています。

＊5 経済産業省「クレジットカード決済システムのセキュリティ対策強化検討会 報告書」
https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/20230120_1.pdf