クレジットカード取引における**セキュリティ対策**

最終回

インターネット決済におけるセキュリティ対策(2)

山本 正行 Yamamoto Masayuki **山本国際コンサルタンツ代表**
関東学院大学経済学部経営学科講師、決済サービス事業の企画、戦略立案を専門とするコンサルタント。消費生活相談員を対象とした研修も実施。講演、執筆多数。

今回は、インターネット決済を取り扱う事業者が行うべきセキュリティ対策の内容を解説します。消費者からは見えにくい部分ですが、クレジットカードのシステムを理解するうえで重要な要素です。

カード情報漏えい防止と不正使用対策の義務づけ

2018年に予定される改正割賦販売法の施行に伴い、クレジットカードでインターネット販売を行う事業者(EC事業者)などに、①カード情報の漏えい防止対策 ②インターネット決済における不正使用対策―が義務づけられます。対策の目標、各主体の役割などは「実行計画2017」*1に記されています。以下、「実行計画2017」の内容に従って解説します。

カード情報の漏えい対策

カード情報の漏えい対策として、EC事業者などに対し、①カード情報の非保持化(カード情報を保持しない) ②保持する場合はPCI DSS*2に準拠―の2つのうちいずれかの対策が義務づけられます。

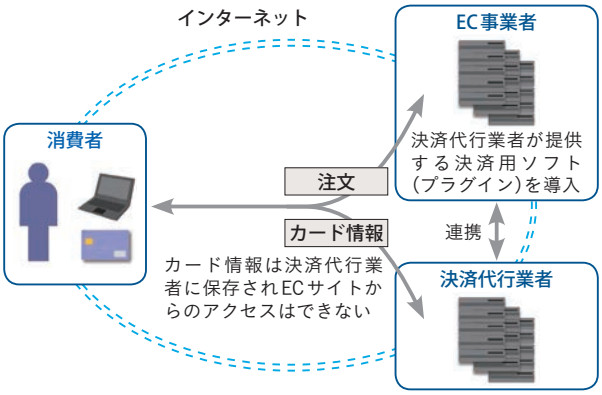
①カード情報の非保持化

カード情報の非保持化は、クレジットカードを取り扱う事業者がシステム上にカード情報を保存しないばかりか、一時的にも保持せず、処理もしないことを意味します。カード情報の漏えいを防ぐにはカード情報を持たないことが最善というわけですが、カード情報を保持も処理もせずクレジットカード決済ができるのでしょうか。

通常、利用者がパソコンやスマホから打ち込んだカード情報は、EC事業者のサーバにいったん保存されます。しかし、EC事業者が決済代行業者のシステムを利用することで、カード情報を持たずにインターネット決済に対応することもできるのです。この方式は、クレジットカード決済に必要なオーソリゼーションや売上処理のすべてを決済代行業者が行い、EC事業者は決済代行業者とプラグインなどと呼ばれるソフトウェアで連携し、カード情報を含まない処理結果を受け取ります(図1)。

現在、既にこの方式のEC事業者は多数あり、

図1 EC事業者がカード情報を保持しない方法



*1 ウェブ版「国民生活」2017年10月号「クレジットカード取引におけるセキュリティ対策」第5回「ICカードのセキュリティ対策(2)」
http://www.kokusen.go.jp/wko/pdf/wko-201710_11.pdf

*2 Payment Card Industry Data Security Standardの略。

今後はこれが主流になっていくものと考えられます。決済代行業者が重要な役割を担う一例です。

さらに今後は決済代行業者ばかりでなく、アクワイアラー（主にクレジットカード会社）や決済サービスを提供するシステム会社などにも同様のサービスが増えるでしょう。

②PCI DSSとは

EC事業者の中には運用上カード情報を保持せざるを得ない事業者も少なくありません。アマゾン、楽天市場などの大手EC事業者、アップル、グーグルなどのスマホのプラットフォーム事業者などは、利用者のアカウントにカード情報も登録し、ショッピングや有料サービスを利用する際に登録されたカード情報を用いて決済処理を行っています。

また、EC事業者がカード情報の非保持化を行っても、それをサポートする決済代行業者、クレジットカード会社（以下、カード会社）などはカード情報を直接処理するため、サーバ上にカード情報を保持せざるを得ません。結局誰かがカード情報を保持しなければならないわけです。「実行計画2017」はカード情報を保持する事業者にカード情報の厳格な取り扱い方法を求めるPCI DSSに準拠することを義務づけています。

PCI DSSはクレジットカードを含む国際カードを取り扱う事業者のセキュリティ対策基準を定めた国際的な標準規格で、ビザ、マスターカードなどの国際決済ブランドが共同で策定しました。表に示す6つの目標を掲げ、そのすべてを実現するための要件（12要件）を事業者に義務づけています。なお、先述の大手EC事業者、プラットフォーム事業者を含む多くの事業者が既にPCI DSSに準拠ずみですが、中小事業者などには準拠していないところが残ります。

表 PCI DSSの目標

- 安全なネットワークの構築と維持
- カード会員データの保護
- 脆弱性を管理するプログラムの整備
- 強固なアクセス制御手法の導入
- 定期的なネットワークの監視およびテスト
- 情報セキュリティポリシーの整備

PCI DSSに準拠していない事業者が新たに準拠する際、多くの場合システム改修を伴い、さらにカード情報取扱いに関する運用ルール（業務）も変更しなければなりません。その後、PCI国際協議会によって認定された審査機関による訪問調査（オンサイトレビュー）を受けるか、自ら所定の自己問診を行うことで準拠ずみであることを確認します。ビザ、マスターカードなどの国際決済ブランドは、年間売上件数が一定以上の大手事業者にオンサイトレビューの実施を義務づけています。日本では一般社団法人日本クレジット協会が国内における運用ルールを定め、年間売上件数が少なく国際決済ブランドの基準に当てはまらない事業者にも自己問診によるPCI DSS準拠を義務づけました。

対応期限は2018年3月末

インターネット決済を行う事業者は、カード情報の漏えい対策を2018年3月末までに終わらせなければなりません。カード情報の漏えい対策は喫緊の課題であり、改正割賦販売法の施行（遅くとも2018年6月）まで待ってはいられないということです。なお、対面販売の加盟店の対応期限は2020年3月末です。対面販売の加盟店の場合は、カード情報の漏えい対策に加えてIC化対応も行う必要があり、その対応がより困難である点などを考慮した結果です。

不正使用対策の現状

不当に入手したカード情報を悪用する「なりすまし」の被害の発生を抑制するために、カード情報の漏えい対策に加えて、ECにおける不正使用対策も早急な対応が求められます。

インターネット決済を行う場合、カード番号に加え有効期限、利用者名、セキュリティコードなどを入力して認証を行うことが一般的です。それに加えてカード会社（イシュアー）による3Dセキュア方式に対応する事業者も増えています。3Dセキュアは、インターネット決済の際に、事

前にイシュアーに登録したID、パスワードなどで追加の本人確認を行う認証方式です。3Dセキュアに対応したECサイトなどでインターネット決済を行うと、決済時にウェブサイトのドメインがECサイトからイシュアーに一時的に切り替わります。そこでイシュアーのウェブサイトにログインするためのID、パスワードなどを入力して認証します。この方式はイシュアーが直接利用者を認証するため、第三者がなりすましてクレジットカードを悪用する被害を食い止める効果があります。

こうして多くのEC事業者やイシュアーが、さまざまな方法で取引を認証し、不正取引を排除しようと心がけています。しかし、今でも「カード番号＋有効期限」のみなど十分とはいえない認証方式のままクレジットカード決済を行う事業者が存在し、危険な状態が残ります。対応の足並みがそろわない点も問題であり、対応が遅れる事業者には早急な対応が求められます。事業者によって認証方式が異なり一貫性がない点も課題です。

さらに最近は不正使用の手口が巧妙になり、セキュリティコードや3Dセキュアなどのイシュアーによる対策だけでは十分とはいえない状況が指摘されます。EC事業者などによる協力も不可欠になってきています。

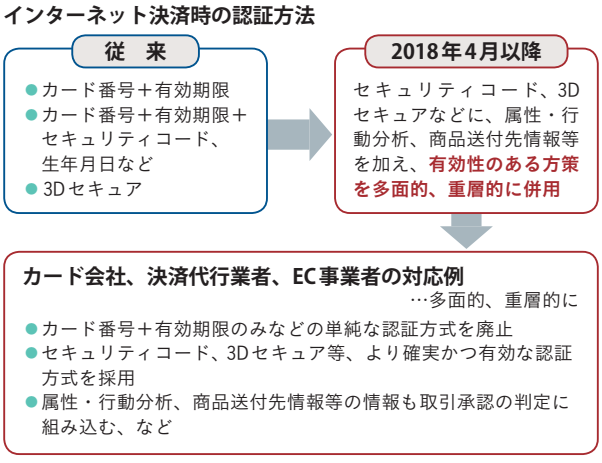
新たに義務づけられた不正使用対策

カード会社、決済代行業者に加えEC事業者などインターネット決済を行う事業者には、カード情報の漏えい対策と同じ2018年3月を期限に「多面的・重層的な不正使用対策の導入」が義務づけられました。少し分かりにくい表現ですが、これはセキュリティコードや3Dセキュアなどのイシュアーによる従来の認証方式に加え、EC事業者が行う利用者の「属性・行動分析」*3、それに商品送付先情報なども加味して、より高度な認証に対応せよ、という意味です。例えば、大手EC事業者などにはクレジットカード決済の認証とは別に、取引を常時監視し、利用者の行動パターンや商品送付先に不審な点が認められる取引を保留にする、などの不正検知システムを運用するところがあります。今後はこうしたEC事業者による不正検知も含め、さまざまな手段を組み合わせ、多面的、重層的に不正使用を検知し対処していくことが義務づけられたのです（図2）。しかし、特定の方式を義務づけてはおらず、方式の選択は事業者の任意となっています。そのため、事業者にとって具体的な対策方法が分かりにくい点も否めません。

消費者が注意すべきこと

消費者には事業者が対策を施したかどうかが分かりにくいという問題があります。特にカード情報の非保持あるいはPCI DSSに準拠しているかどうかの判別は、消費者には困難です。最近は「PCI DSS準拠」などの表記を行うウェブサイトも増えていますので、注意してみることも大切です。不正使用対策に関しては、これまで3Dセキュアに対応していなかったECサイトで対応が進む可能性もあります。そのような場合は、インターネット決済の際にイシュアーのウェブサイトにID、パスワードの入力が必要となりますので、自分のID、パスワードを登録していない人はこの機会に登録しましょう。

図2 インターネット決済における多面的・重層的な不正使用対策



＊3　通信時のIPアドレス等のデバイス情報や、過去の取引情報、取引頻度等に基づいたリスク評価を行い、不正な取引であるか判定する手法。