

クレジットカードを 取り扱う加盟店の皆様へ

割賦販売法改正に伴うセキュリティ対策の取組みについてのお知らせ

日頃は、クレジットカードによる取引に関してご理解とご協力を賜り、厚くお礼申し上げます。

さて、平成28年12月9日に「割賦販売法の一部を改正する法律」（「改正割賦販売法」）が公布され、クレジットカードを取り扱う加盟店において、カード番号等の適切な管理や不正使用対策を講じることが義務づけられることになりました。改正割賦販売法の施行は、平成30年5月～6月の予定とされております。

これに関連して、同法を所管する経済産業省より、カード会社との間で契約を締結している加盟店に対して、後述の内容を周知するよう要請がありました。つきましては、内容についてご理解を賜り、改正割賦販売法の施行までに必要な対応を行っていただきますようお願い申し上げます。

なお、改正割賦販売法により加盟店に義務付けられる具体的なセキュリティ対策の内容については、今後改正される予定の省令、監督の基本方針等において示されることとなりますが、この加盟店の義務の実務上の指針となりうる「クレジット取引セキュリティ協議会」の「実行計画2017」においては、以下の対応が求められておりますのでご参照ください。

【クレジットカードを取り扱う加盟店にご対応いただくこと】

- カード情報保護※について適切な保護措置をとること（非保持化又はPCIDSS準拠）。
- 不正使用対策として、対面加盟店ではICカード決済が可能な端末を設置し、EC（ネット取引）加盟店では、なりすましによる不正使用防止対策をとること。

※カード情報保護について

- 非保持化とは、電磁的に送受信しないこと、すなわち自社で保有する機器・ネットワークにおいて「カード情報」を電磁的情報として『保存』、『処理』、『通過』しないことをいいます。なお、決済専用端末から直接、外部の情報処理センター等にカード情報を伝送している場合は、非保持とします。
- PCIDSS（Payment Card Industry Data Security Standard）とは、クレジットカード会員データを安全に取り扱う事を目的として策定された国際ブランドが策定した基準です（下記の日本カード情報セキュリティ協議会のホームページ参照）。
http://www.jcdsc.org/pci_dss.php
- カード番号を保持する場合には、原則PCIDSS準拠が必要ですが、対面加盟店において、暗号化等の処理によりカード番号を特定できない状態とし、自社内で復号できない仕組みであれば、非保持化と同等／相当のセキュリティ措置として扱うことができます。

決済専用端末（CCT）を設置している加盟店

- カード会社より貸与されているICカードに対応した決済専用端末（カードをスワイプするのではなく差し込んでデータを読み取り、暗証番号を入力する方式）を設置し、外部の情報処理センター等に直接伝送している場合には、カード情報保護対策も不正使用対策（偽造防止対策）もすでに対応が済んでいますので、新たな対応は必要ありません。ご不明な点があれば、契約先のカード会社にご確認ください。
- 一方、ICカードが読み取れない端末であれば、ICカードが読み取れる端末への置換えが必要です。

POSシステムと端末間で、取引金額、決済結果等を連動させている加盟店

- カード情報保護については、非保持化（上記の非保持化と同等／相当のセキュリティ措置を含む。以下同じ。）又はPCIDSS準拠が必要です（上述の「※カード情報保護について」参照）。
- ICカードに対応した決済端末（暗証番号の入力方式）が設置されていれば、不正使用対策（偽造防止対策）はすでに対応が済んでいますので、新たな対応は必要ありません。
- 一方、ICカードに対応していない端末であれば、ICカードに対応した端末への置換えが必要です。
- ご不明な点があれば、POS機器メーカーにご照会ください。

カード処理機能を持ったPOSを設置している加盟店

- カード情報保護については、非保持化又はPCIDSS準拠が必要です（上述の「※カード情報保護について」参照）。
- ICカードに対応したPOS（暗証番号を入力する方式）が設置されていれば、不正使用対策（偽造防止対策）はすでに対応が済んでいますので、新たな不正使用対策（偽造防止対策）は必要ありません。
- 一方、ICカードに対応していないPOS（スワイプして磁気で読み取る方式）であれば、ICカードに対応したPOSに置換えを行うか、ICカードに対応した決済端末を導入しPOSに接続する必要があります。
- ご不明な点があれば、POS機器メーカーにご照会ください。

EC（ネット取引）加盟店

- カード情報保護については、非保持化又はPCIDSS準拠が必要です（上述の「※カード情報保護について」参照）。
- EC加盟店において、決済代行業者（PSP）が提供するシステムを利用する場合があります。この場合、加盟店の機器・ネットワークを通過する「通過型」と、通過しない「非通過型」に大別されますが、通過型の場合には、カード情報を窃取されるリスクがあるので、「非通過型」を推奨しております。どちらの仕組みを導入しているかについては、契約先の決済代行業者にご確認ください。なお、「通過型」の場合には、カード情報を保持することになりますので、EC加盟店においてPCIDSS準拠が必要です。
- なりすましによる不正使用防止のため、パスワードの入力等により本人が利用していることを確認できる仕組みや申込者の過去の取引情報などから不正な取引かどうかを判定する手法の導入等、各加盟店の業種・取扱商材、リスクの状況に応じて、多面的・重層的な不正使用対策をする必要があります。