

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、2016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、2018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、別記の内容を周知するよう要請がありました。つきましては、別記の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、当社にお問い合わせください。
- 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。
- 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）。

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

- 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、多面的・重層的な不正使用対策をする必要があります。

<一般社団法人日本クレジット協会ホームページ>

◆改正割賦販売法

(割賦販売法の一部を改正する法律について)

http://www.j-credit.or.jp/download/170126_news_a1.pdf

(「割賦販売法が改正されました」リーフレット)

http://www.j-credit.or.jp/download/170126_news_a5.pdf

◆クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画

<http://www.j-credit.or.jp/security/document/index.html>

◆具体的なセキュリティ対策

<http://www.j-credit.or.jp/security/understanding/member-store.html>

◆その他

(クレジットカード不正使用被害の発生状況 2016年12月)

http://www.j-credit.or.jp/download/170126_news_a3.pdf

(「クレジットカードがより安全・安心なIC取引に変わります！」リーフレット)

http://www.j-credit.or.jp/download/170126_news_a4.pdf

<本件に関するお問合せ先>

株式会社 日専連旭川 営業部

〒070-0032 旭川市2条通8丁目

T E L : (0166) 23-2000

受付時間：9：30から18：00（年末年始・土日祝日除く）

<別記記載の説明会の要請先>

一般社団法人日本クレジット協会

担当：「業務企画部」又は「セキュリティ対策推進センター」

〒103-0016 東京都中央区日本橋小網町14-1

TEL:03-5643-0011 email: gykikaku1@jcredit.jp 又は gykikaku2@jcredit.jp

法改正・セキュリティ対策に関するFAQ

クレジット協会のホームページより、質問の多い事項についてのFAQを抜粋いたしました。ご参考にさせていただければ幸いです。

1. 改正割賦販売法について

(1) 割賦販売法とはどのような法律ですか。

「かっぱはんぱいほう」と読み、クレジットに関する法律です。従来はクレジット会社の義務を主に規定しておりましたが、2016年12月に改正され、クレジットカードが使える加盟店の義務についても規定が設けられました。

(2) なぜ改正されたのですか。

加盟店に対する義務が追加された改正については、近年加盟店におけるクレジットカード番号等の漏えい事件や不正使用被害が増加しているからです。安全・安心なクレジットカード利用環境を実現するために改正されました。

(3) 加盟店に課された義務にはどのようなものがありますか。

大きく分けて「クレジットカード番号等の適切な管理」と「不正使用の防止」の二つの義務が課せられました。

また、加盟店契約を締結しているクレジットカード会社に、加盟店調査（悪質加盟店の是正・排除、クレジットカード番号等の適切な管理、不正使用の防止）を行い、調査結果に基づいた必要な措置を行うこと等が新たに義務付けられており、これに加盟店は応じる必要があります。

(4) 加盟店の義務には罰則はありますか。

罰則はありません。ただし、義務を果たさない場合は、クレジットカード会社から(3)の要請があり、この要請に応じない場合は、将来的にクレジットカードの取扱ができなくなる可能性があります。

(5) 法改正について、問合せはどこに行えばよいですか。

個別の契約に基づく内容については、当社（加盟店契約を締結したクレジットカード会社）にお問合せください。また、割賦販売法の改正一般については経済産業省商取引監督課にお問合せください。

2. 加盟店が取り組まなければならないこと

(1) 加盟店が取り組まなければならないことは何ですか。

課せられた二つの義務のうち、一つ目の「クレジットカード番号等の適切な管理」については、カード番号等の非保持化(非保持化と同等/相当のセキュリティ措置を含みます。)、非保持化ができない場合はセキュリティに関する国際規格であるPCIDSSに準拠する必要があります。二つ目の、「不正使用の防止」については、クレジットカード決済端末を用いている加盟店はIC対応が必要です。また、EC加盟店については、ネット上でのなりすまし防止対策が必要です。

(2) なぜ「クレジットカード番号等の適切な管理」においては、非保持化か、PCIDSSへの準拠が必要なのですか。

クレジットカード番号等の適切な管理をするにあたり、そもそもカード番号等を持っていない場合(非保持)は、漏えいする心配はありませんので一番安全です。しかし、営業の都合等でカード番号等を持たなければならない場合は、厳密な管理が必要です。このためカード番号等を保持する場合は、セキュリティに関する国際規格であるPCIDSSに準拠する必要があります。なお、自社開発のシステム(POS等)においては、意図せずにカード情報を持っていることがあるため、注意が必要です。必ず、システムを開発した会社等に問合せ対応してください。

(3) 「クレジットカード番号等の適切な管理」および「不正使用の防止」について、どのような対策が必要になりますか。

具体的な対策はクレジットカード取引セキュリティ対策協議会が取りまとめた実行計画2017に記載されていますが、主な対策は以下のとおりです。なお、実行計画2017は次のURLを参照してください。

http://www.j-credit.or.jp/security/pdf/plan_2017.pdf

①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。

②POS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、非保持化あるいはPCIDSS準拠が必要です。

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。ご不明な点は、POS機器メーカーにご照会ください。

③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。

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。ご不明な点は、POS機器メーカーにご照会ください。

④EC（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。

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。

（4）なぜ不正使用対策としてICカードへの対応をするのですか。

現在の技術では、ICカードを複製することはほぼ不可能です。このため、偽造カードによる不正使用を防止するため、カードのIC化を進めるとともに、カード決済する端末側もIC対応を進める必要があります。

（5）すでにICカードに対応しているかは何を確認すればよいですか。

カードを差し込んで暗証番号を入力する方式の場合は、ICカードに対応しています。カードをスワイプして読み取る方式は、IC決済端末ではありません。

（6）ICカード対応で、決済時の対応は何か変わりますか。

「クレジット決済端末に磁気カードをスワイプし、売上伝票に印字された金額を確認し、サイン（署名）する」方式から、「IC対応のクレジット決済端末にICカードを差し込み、表示された金額を確認し、お客様に暗証番号4桁を入力していただき、最後に確定ボタンを押す」方式に変わります。詳しくは、次のURLをご確認ください。

http://www.j-credit.or.jp/security/pdf/ic_card.pdf

なお、食品売場などで実施しているサインレス取引においては、IC対応することにより暗証番号の入力を例外的に省略できる場合がありますので、契約するクレジットカード会社にお問合せください。

(7) 暗証番号を失念したお客様へはどのように対応したらよいのでしょうか。

お客様が暗証番号を失念した場合は、ＩＣカード取引においてもサインで取引をすることができます。ただし、セキュリティ上、より強固である暗証番号入力をバイパスするため、例外的対応であり、濫用することはできません。

(8) ＥＣ加盟店（ネット加盟店）において、なぜなりすまし対策が必要になるのですか。

近年、漏えいしたクレジットカード情報を利用したなりすまし等による不正使用被害が急増しているからです。対応については上記③「ＥＣ（ネット）加盟店」を参照してください。

(9) 複数のクレジットカード会社より漏えい対策・不正使用対策の取り組みについてのお知らせが来ました。どうすればよいですか。

クレジットカード会社は「クレジットカード番号等の適切な管理」「不正使用の防止」について、所管する経済産業省からの要請もありお知らせをしています。そのため、複数のクレジットカード会社と契約をしている加盟店には、各クレジットカード会社から通知等がそれぞれ行く場合があります。また、各クレジットカード会社から、対応状況等の回答を求められた場合等は、クレジットカード会社に調査する義務が法令上あるため、ご面倒でも、すべてにご回答ください。

(10) いつまでに対応しなければなりませんか。

改正割賦販売法が施行されるのは２０１８年５月～６月ですので、この期日が基本となります。なお、クレジット取引セキュリティ対策協議会が取りまとめた実行計画２０１７では、ＥＣ加盟店は２０１８年３月末まで、店舗加盟店は２０２０年３月までとなっていますので、遅くともこの期限までには対応することが求められています。

以上