# 「クレジットカード・セキュリティガイドライン ＦＡＱ」

策定日：2020年3月27日
更新日：2025年3月4日

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 1 | 全体 | 「実行計画」と「クレジットカード・セキュリティガイドライン」の違いは何か。 | 【クレジットカード・セキュリティガイドラインの特徴（実行計画との相違点）】<br>・推進期限の設定がありません。<br>・法令上求められている措置に該当する部分は、【指針対策】と明示しております。<br>・対象となる事業者については、今後の決済スキームの進展と新たに規制対象となる事業者があれば追加が見込まれます。<br><br>【両文書の位置付け】<br>・「実行計画」は、我が国のクレジットカード取引において「国際水準のセキュリティ環境」を整備するために、2016年2月に各関係事業者が取組むべき具体的なセキュリティ対策とその実施期限を2020年3月末としたものです。<br>・「クレジットカード・セキュリティガイドライン」は、実行計画の実施期限である2020年3月末以降も、引き続き、関係事業者が取組むべきセキュリティ対策を取りまとめたものであり、クレジットカード取引の関係事業者は、本ガイドラインに基づきセキュリティ対策を講じ、最新の状態で維持・運用し続けることが求められます。<br>・「クレジットカード・セキュリティガイドライン」は、「実行計画」の後継であり、「割賦販売法（後払分野）に基づく監督の基本方針」において割賦販売法で義務付けられているカード番号等の適切な管理及び不正利用防止措置の実務上の指針として位置付けられるものであり、本ガイドラインに掲げる措置又はそれと同等以上の措置を適切に講じている場合には、セキュリティ対策に係る法令上の基準となる「必要かつ適切な措置」を満たしていると認められています。<br>・なお、本ガイドラインは【1.0版】として2020年3月19日に制定されて以降、令和2年第201回通常国会で「割賦販売法の一部を改正する法律（令和2年法律第64号）」が成立し、クレジットカード番号等取扱業者が拡充されたことをはじめ、制定以来の環境変化を踏まえ、2025年3月4日付で【6.0版】へと改訂されております。 | 2025年3月4日 | 【6.0版】P7 |
| 2 | 全体 | セキュリティ対策は義務として対応する必要があるのか。 | 割賦販売法では、カード会社においてはクレジットカード番号等の適切な管理措置、加盟店においてはクレジットカード番号等の適切な管理措置や不正利用の防止措置というセキュリティ対策を講じることが義務化されております。<br>また、2021年4月1日に改正割賦販売法が施行されたことに伴い、クレジットカード番号等取扱業者が拡充され、「決済代行業者等（4号事業者）」、「QRコード決済事業者等（5号事業者）」及び「その委託会社（6号事業者）」、「加盟店向け決済システム提供事業者（7号事業者）」に該当する事業者についても、クレジットカード番号等の適切な管理のためのセキュリティ対策を講じることが義務化されております。<br>クレジットカード・セキュリティガイドラインは、同法で義務付けられているカード番号等の適切な管理及び不正利用防止措置の実務上の指針として位置づけられるものであり、同ガイドラインに掲げる措置又はそれと同等以上の措置を適切に講じている場合には、セキュリティ対策に係る「必要かつ適切な措置」が講じられているとみなされています。<br>なお、同ガイドラインにおいては、同法で規定される措置に該当する部分を【指針対策】と記載しています。 | 2025年3月4日 | 【6.0版】P20 |
| 3 | 全体 | 国内のアクワイアラーやPSPがセキュリティ対策の取組を行っても、国内のEC加盟店がその取組に同意せず、海外のアクワイアラーと契約してしまうと意味がなくなってしまうのではないか。 | 割賦販売法では、アクワイアラーとして加盟店契約業務を行う場合には、「クレジットカード番号等取扱契約締結事業者」としての登録が必要となります。<br>外国法人が日本国内で業務を行う場合においても国内営業所の登録が必要となり、同法の規制対象となります。 | 2020年3月27日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 4 | 全体 | 自動精算機は対面取引の認識であるが正しいか。 | 自動精算機はカードを読み取る端末内蔵型の機器でカード取引を行うことから、対面取引と整理されます。割賦販売法で規定されているクレジットカード番号等の不正利用の防止のために必要な措置として、IC対応されていることが必要です。 | 2021年4月1日 | 【6.0版】P20 |
| 5 | 全体 | 割賦販売法により加盟店にはセキュリティ対策を講じる義務があるが、違反した場合、加盟店に対する罰則規定はあるのか。 | 罰金等の罰則規定はありませんが、行政の措置として加盟店に対し、報告徴収、立入検査を行うことができる規定があります。<br>また、加盟店のセキュリティ対策措置（クレジットカード番号等の適切な管理、不正利用の防止）が不十分な加盟店については、契約先のカード会社等による加盟店調査を通じて、必要なセキュリティ対策措置を早急に講じるよう指導等が行われることになります。なお、このような指導にもかかわらず、必要なセキュリティ対策が講じられない場合には、加盟店契約が解除される場合がございますのでご注意ください。 | 2023年3月14日 | |
| 6 | 全体 | 対面時、有効性チェック済みクレジットカードで受付し、登録。次月以降、当該登録カードで決済を行う継続課金加盟店は、「対面加盟店」として扱われるのか。 | いわゆる「継続課金加盟店」において、カード登録時に端末で有効性チェックを行ったのち、当該登録されたカードの情報により売上を計上する場合、分類としては対面取引ではなく、「非対面取引」として整理されます。<br>なお、保険の申込み等、有効性チェックのみにとどまらず、初回分の決済を併せて行っている場合については、「対面取引」と整理され、IC対応されていることが必要です。 | 2021年4月1日 | |
| 7 | 全体 | 国際ブランドが付いた法人カードを取り扱っているが、クレジットカード・セキュリティガイドラインで求める対策を講じる必要があるか。 | 前身の実行計画同様、クレジットカード・セキュリティガイドラインでは、個人向けであるか法人向けであるかを問わず、世界中で共通に使用できるために不正利用リスクが高い、国際ブランド付きのクレジットカードを対象としております。<br>なお、国際ブランドが付いていないクレジットカードについても、リスクに応じたクレジットカード番号等の適切な管理及び不正利用の防止のための対策が必要である点に留意が必要です。 | 2020年3月27日 | |
| 8 | クレジットカード情報保護対策分野 | このような場合はカード情報の「保持」となるのか。<br>①紙の媒体でカード情報を保存している場合。<br>②通話録音をしており、カード情報も含まれる場合。 | 非保持化とは、以下(※)を除き、「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『保存』、『処理』、『通過』しないこと」と定義されております。<br><br>※①紙(クレジット取引伝票、カード番号を記したFAX、申込書、メモ等）、②紙媒体をスキャンした画像データ、③電話での通話記録（音声データを含む）においてカード情報を保存する場合。<br><br>そのため、非保持化（非保持と同等/相当含む）が実現されている加盟店で、紙の媒体でカード情報の保存をしている場合においては、当該加盟店は保持とはならないとされています。<br>ただし、情報保護の観点から、PCI DSSや個人情報保護法等を参考に自社の情報管理基準で保護を図ってください。 | 2024年3月14日 | 【6.0版】P26 |
| 9 | クレジットカード情報保護対策分野 | 社内サーバーにカード番号等を画像データやPDFデータ（電子帳票）として保存しているケースがあるが、このようなデータにもPCI DSS対応が必要なのか。 | カード情報を保持する加盟店については、 PCI DSS準拠が求められております。<br>なお、非保持化（非保持と同等/相当含む）が実現されている加盟店で、紙の媒体をスキャンした画像データにてカード情報を保存している場合においては、当該加盟店は保持とはならないとされています。そのため、PCI DSS準拠までは求めないとされております。<br>ただし、情報保護の観点から、PCI DSSや個人情報保護法等を参考に自社の情報管理基準で保護を図ってください。 | 2020年3月27日 | 【6.0版】P26 |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 10 | クレジットカード情報保護対策分野 | 「カード情報」からカード番号など直接決済に関係する情報を無くせばカード情報ではなくなるのか。また、カード情報はカード番号が無くとも他の情報（セキュリティコードなど）だけでもカード情報となるのか。 | 「カード情報」とは、カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CIDいわゆるセキュリティコード、PIN又はPINブロック）を指しますが、カード会員データのうち、クレジットカード番号以外のデータのみであれば「カード情報」ではないとされております。<br>また、セキュリティコードやPIN/PINブロックは「機密認証データ」に該当するので、カード情報を保持する場合のカード情報保護対策を選択した場合でも、保存すること自体が禁止されています。 | 2021年4月1日 | 【6.0版】P13 |
| 11 | クレジットカード情報保護対策分野 | 紙媒体をスキャンした画像データにおいてカード情報を保存する場合は、「保持」に該当しないとされているが、当該画像データをテキスト化した場合もカード情報の保持に該当しないか。 | 画像データからテキスト化した場合、それはテキストデータになると考えられます。<br>そのような形式で保存されるのであれば保持となります。 | 2020年3月27日 | |
| 12 | クレジットカード情報保護対策分野 | 無効処理されたカード番号はカード情報ではないという認識でよいか。 | 無効処理されたカード番号はカード情報と見做しません。ただし、完全に無効となったカード情報であることが前提となります。 | 2020年3月27日 | |
| 13 | クレジットカード情報保護対策分野 | カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）にある「クレジットカード会員名」はカード決済に係る会員名であるが、一方加盟店でもカード決済に関わらず「顧客名」は持っている。機密認証データとクレジットカード番号、有効期限、サービスコードがなければ「クレジットカード会員名」と同一人物であっても顧客名自体を保持している事はカード情報を保持していることになるか。 | カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）のうち、クレジットカード番号以外のデータのみであれば「カード情報」ではないとされております。<br>ただし、「顧客名」は個人情報にあたることから、個人情報保護法等を参考に適切な保護を図ってください。 | 2021年4月1日 | 【6.0版】P13 |
| 14 | クレジットカード情報保護対策分野 | 自社システム内において、16桁のクレジットカード番号を4分割して保存する場合、カード情報の保持にあたるか。 | トークナイゼーション(自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、自社システム内ではクレジットカード番号を特定できないもの)やトランケーション(自社システムの外でクレジットカード番号を、自社システム内では特定できない方法で安全に国際的な第三者機関に認められた桁数を切り落としたもの)、無効処理されたカード番号については、カード番号と見做さないとされています。<br><br>自社システム内で行った処理であり、かつ上記以外の処理である場合は、クレジットカード番号と見做されるため、ご質問のスキームはカード情報を保持していると考えられます。 | 2020年3月27日 | 【6.0版】P13 |
| 15 | クレジットカード情報保護対策分野 | EC加盟店において、カード情報「通過型」である場合、カード情報を「暗号化・トークン化」していればカード情報の「保持」とはならないのか。 | EC加盟店における「通過型」の場合、カード情報の通過後の処理如何に関わらず、カード情報が加盟店の機器・ネットワークを通過することになりますので、カード情報を「保持」していると考えられ、PCI DSS準拠が求められます。 | 2020年3月27日 | 【6.0版】P33 |
| 16 | クレジットカード情報保護対策分野 | PSPにカード情報(カード番号等)を連携する場合には、インターネットゲートウェイにカード番号等のログが一定期間残るが、保持していることになるのか。 | 一定期間でもインターネットゲートウェイにカード情報が保存されてしまうのであれば、保持していることとなります。 | 2024年3月14日 | |
| 17 | クレジットカード情報保護対策分野 | 顧客から電話・FAX・はがき等で入手したカード情報を自社の機器に入力して決済を行うにあたり、PSPが提供しているリンク型もしくはJavaScript型の入力フォームを用いてPSPにカード情報を送信する方法は、カード情報の保持にはならないか。 | カード情報が自社の機器を「通過」していることから、保持となります。<br>メールオーダーやテレフォンオーダーにおける非保持化実現方策については、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書1】」(※)をご確認ください。<br>（※）本資料については、ご契約のカード会社、PSP、もしくは当協会にお問い合わせください。 | 2024年3月14日 | 【6.0版】P33／【附属文書1】 |
| 18 | クレジットカード情報保護対策分野 | PCI DSSの日本語版は用意されているか。 | 日本語版については、日本カード情報セキュリティ協議会（JAPAN CARD DATA SECURITY CONSORTIUM、以下JCDSC）サイトよりご確認ください。<br>https://www.jcdsc.org/ | 2023年3月14日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 19 | クレジットカード情報保護対策分野 | 国際ブランドが付いていないカードのカード情報を保持しているが、PCI DSS準拠が求められるのか。 | 「国際ブランドが付いていないクレジットカード」は、利用できる範囲が限定され不正利用のリスクも低いことから本ガイドラインの対象とはしておりませんが、リスクに応じたクレジットカード番号等の適切な管理が必要である点には留意が必要です。 | 2023年3月14日 | 【6.0版】P20 |
| 20 | クレジットカード情報保護対策分野 | クレジットカード情報保護対策の対象範囲に電子マネー情報も含むのか。 | 国際ブランド付きのクレジットカード情報が対象です。<br>電子マネー情報は含みません。 | 2020年3月27日 | |
| 21 | クレジットカード情報保護対策分野 | 決済専用端末(CCT)のみ導入している対面加盟店は、カード情報の非保持となるのか。それとも、PCI DSS準拠の対象となるのか。 | POS等の加盟店システムにカード情報を連携や保持をせず（保存・処理・通過せず）、IC対応した決済専用端末(CCT及びそれと同等以上のセキュリティレベルのもの）のみを使用し、直接、外部の情報処理センター等に伝送している場合は非保持となり、PCI DSS準拠は求められません。 | 2020年3月27日 | 【6.0版】P26 |
| 22 | クレジットカード情報保護対策分野 | 自社(加盟店）がカード情報を保存、処理、通過しているのか分からない。 | 自社（加盟店）が提携しているPSPやシステム会社に確認してください。トランザクションログに意図せずにカード情報が記録されているということがありますので、ログを確認し、カード情報が記録されているようであれば、直ちに削除するとともに、ログにカード情報を記録しないように改修をしてください。<br>なお、業務上、カード情報の保持が必要な場合は、PCI DSS準拠が求められます。 | 2024年3月14日 | |
| 23 | クレジットカード情報保護対策分野 | 「通過型（モジュール型）」のEC加盟店で、カード情報を保存していない場合はどのような対応が必要か。 | 「通過型（モジュール型）」のEC加盟店は、カード情報が、自社で保有する機器・ネットワークに保存していなくとも通過しているため、非通過型のリダイレクト（リンク）型か、JavaScript型（トークン型）への移行もしくはPCI DSS準拠が必要となります。 | 2020年3月27日 | 【6.0版】P33 |
| 24 | クレジットカード情報保護対策分野 | JavaScript決済はカード情報非通過型(非保持）と判断して良いか。非保持の場合、PCI DSSの対象外となるのか。 | PCI DSS準拠したPSPが提供する決済方式により加盟店サーバーをクレジットカード番号が通過しない方式（トークン等）であれば、非保持として整理しています。非保持の場合はPCI DSS準拠までは求められていませんが、ネットワーク保護等必要なセキュリティ対策は実施してください。 | 2023年3月14日 | 【6.0版】P33 |
| 25 | クレジットカード情報保護対策分野 | リカーリング（継続課金）加盟店において、自社でカード情報を含め受付処理を行う場合において非保持化を実現するには、受付処理自体を回避しなければければならないか。 | 非対面取引のリカーリング（継続課金）加盟店が非保持を実現するには、業務委託のほか、以下の対応が考えられます。<br><br>非保持の対応として、非保持化ソリューション導入または、非保持と同等/相当の対応として、PCI P2PE認定ソリューションの導入が考えられます(※)。<br>※詳細は「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書1】」に記載しています。本資料については、ご契約のカード会社、PSP、もしくは当協会にお問い合わせください。 | 2024年3月14日 | 【附属文書1】 |
| 26 | クレジットカード情報保護対策分野 | PCI DSSに準拠するにはどうしたらよいか。 | 準拠方法については、各社の環境にもよりますので、詳しくは日本カード情報セキュリティ協議会（JCDSC）または認定セキュリティ評価機関（QSA）にご相談ください。<br>また、自社のセキュリティレベルを見る上での参考として、簡易診断表を利用できます。簡易診断表は、JCDSCのホームページからダウンロードできます。<br><br>以下、JCDSCサイトにてご確認ください。<br>https://www.jcdsc.org/ | 2024年3月14日 | |
| 27 | クレジットカード情報保護対策分野 | クレジットカード加盟店がクレジットカード取扱業務を外部委託する場合、PCI DSSに準拠している業者への委託であれば、当該加盟店はPCIDSS準拠の必要はないとの認識でよいか。 | 外部委託することによって、加盟店所有の機器・ネットワークにおいてカード情報を保存、処理、通過しないのであれば、クレジットカード・セキュリティガイドライン上、当該加盟店は非保持となり、PCI DSS準拠は不要となります。なお、委託先のPCI DSS準拠状況等の管理は必要です。 | 2020年3月27日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 28 | クレジットカード情報保護対策分野 | カード情報の取扱い業務を外部委託する場合の委託先のカード情報保護については、誰が確認の主体となるのか。 | 確認の主体者は委託元になります。<br><br>セキュリティ対策の実施主体者である関係事業者（加盟店、カード会社、決済代行業者等、QRコード決済事業者等、加盟店向け決済システム提供事業者）は、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持ってPCI DSS準拠等の必要な対策を講じることが求められます。また、複数の委託者からカード情報を取り扱う業務を受託する又はショッピングカート機能等のシステムを提供する事業者は、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS準拠等の必要な対策を行うことが求められます。 | 2024年3月14日 | 【6.0版】P28等 |
| 29 | クレジットカード情報保護対策分野 | 非保持と同等/相当として例示されているPCI P2PEについては、PCI DSS準拠不要という理解でよいか。 | 非保持化(非保持と同等/相当を含む)を達成している加盟店は、PCI DSS準拠は求めていません。<br>PCI P2PE認定ソリューションの導入は、非保持と同等/相当の1つの方策であるため、加盟店において、PCI DSSへの準拠は求めておりません。 | 2024年3月14日 | |
| 30 | クレジットカード情報保護対策分野 | 加盟店(対面・非対面)から委託を受けてポイント付与業務を行っている会社において、データの受信項目にはID番号の他にカード番号が含まれている（データ受信はクローズドネットワーク）。<br>この場合、PCI DSSの準拠は必要か。 | 加盟店の委託先として、加盟店の責任の下、PCI DSS準拠等を求めることになると考えられます。 | 2020年3月27日 | 【6.0版】P28等 |
| 31 | クレジットカード情報保護対策分野 | PCI DSSに準拠するための認定セキュリティ評価機関を紹介して欲しい。 | 当協会から個別に認定セキュリティ評価機関を紹介することは公正性の観点からいたしかねます。日本カード情報セキュリティ協議会（JCDSC）のホームページに連絡先が紹介されておりますのでご確認ください。 | 2024年3月14日 | |
| 32 | クレジットカード情報保護対策分野 | PCI DSS準拠の段階においてスコープ調査があるが、QSAはどのようなことをするのか。 | 例えば、システム概念図やデータフロー図等の提示を受けて、カード情報の経路を特定、PCI DSS準拠が必要な範囲の見極めを行います。また、資料・文書上の不足を指摘の上、ギャップ分析を行います。 | 2020年3月27日 | |
| 33 | クレジットカード情報保護対策分野 | PCI DSS準拠までのギャップ分析は、どのくらいの期間がかかるのか。 | 各社のPCI DSS準拠の適用範囲によって要する期間は異なるため、一概には言えません。 | 2020年3月27日 | |
| 34 | クレジットカード情報保護対策分野 | PCI DSS準拠への検証方法の自己問診について<br>①自己問診の頻度は決められているのか。<br>②結果をどこに提出することが求められるのか<br>③役員の署名はどのような意味合いになるのか。 | ①PCI DSSの原則では、自己問診（SAQ）の実施は年1回とされております。<br>②提出先は以下のとおり、当該企業の立場によって変わります。<br>・カード会社の場合：メンバー会社であれば国際ブランドから提出を求められることがあります。<br>・PSPの場合：接続先のアクワイアラーから提出を求められることがあります。<br>・加盟店の場合：アクワイアラーから提出を求められることがあります。<br>③内容に関して責任をもって認めるというものであり、企業によって、社長や役員が署名しています。<br>当該企業の決裁権限に従った形でよいと思われますが、一般的には役員クラスの署名が多いです。 | 2023年3月14日 | |
| 35 | クレジットカード情報保護対策分野 | 一つの会社で加盟店の業務とイシュアーの業務がある場合、カード情報保護はどこまで対応すべきか。<br>PCI DSSへの準拠方法はオンサイトレビューなのか自己問診なのか、もしくはどのような方法になるのか。 | 業務の中でカード番号を取り扱う業務自体をスコープとしてPCI DSSへの準拠が必要ですが、イシュアーと加盟店両方の業務を行っている場合、且つ、システムが完全に分けられている場合は、イシュアーとしての準拠、加盟店としての準拠各々が必要になります。 | 2023年3月14日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 36 | クレジットカード情報保護対策分野 | 非保持化実現後の必要なセキュリティ対策とは、具体的に何を行えばよいか。 | 継続的な情報保護に関する従業員教育やウイルス対策、デバイス管理等に関する情報漏えい防止のための必要なセキュリティ対策等、情報保護の観点から、PCI DSSや個人情報保護法等を参考に自社の情報管理基準で保護を図ってください。<br>また、自社システムの定期的な点検を行い、その結果に基づく追加的な対策や、新たな攻撃手口への対応を講じること等も重要になります。<br><br>特に、EC加盟店における最近の漏えい事故の傾向としては、「非通過型」の決済システムを導入した場合でも、カード情報の窃取が発生していることから、2025年4月以降はEC加盟店における「脆弱性対策」が指針対策となり、対応が必須となります。<br>詳細は、ご契約のカード会社（アクワイアラー）やPSPにご確認ください。 | 2025年3月4日 | |
| 37 | クレジットカード情報保護対策分野 | 非保持化(非保持と同等/相当を含む)について、達成状況を証明する主体者は誰か。 | 証明する認定機関はございません。カード会社(アクワイアラー)・ベンダー等と協議のうえ対応してください。<br>なお、割賦販売法の考え方は、クレジットカード番号等取扱契約締結事業者（いわゆるアクワイアラー）にて加盟店の対応状況を確認することとなっております。 | 2024年3月14日 | |
| 38 | クレジットカード情報保護対策分野 | EC加盟店における非通過型の2方策（リダイレクト（リンク）型とJavaScript型）に違いはあるのか。 | どちらも、EC加盟店におけるカード情報の非保持化を推進するための方策となります。<br>なお、どちらかの決済システムを導入した上で、事業者により「PCI DSSに準拠する」を選択した場合は、導入した決済システムの導入形態により求められるSAQのタイプが異なります。<br><br>リンク型：SAQ A<br>JavaScript型：SAQ A-EP<br><br>詳しくは以下、日本カード情報セキュリティ協議会（JCDSC）サイトにてご確認ください。<br>https://www.jcdsc.org/ | 2024年3月14日 | |
| 39 | クレジットカード情報保護対策分野 | 日本クレジット協会において策定した「クレジットカード情報漏えい時および漏えい懸念時の対応要領【関係文書1】」とはどのようなものか。また、公表されているものなのか。 | クレジットカード取扱加盟店からクレジットカード情報が漏えいした、又は漏えいの懸念がある場合の、対応ポイントをまとめたものになります。<br>当該文書は非公表扱いとなっております。<br>加盟店の方は、ご契約されているカード会社にお問い合わせください。 | 2023年3月14日 | |
| 40 | クレジットカード情報保護対策分野 | 「対面取引加盟店における非保持化対応ソリューションについて【附属文書2】」における11項目の対策案の中で、具体的なツールや技術名の後に「など」という文言が使用されているが、実態としては記載されたツールや技術しか使用できないのか。 | これらの対策案は想定リスクに対応することを目的に立てられたものになります。記載されたツールや技術と同等またはそれ以上の性能を有するものであれば、対策として有効であると考えられます。 | 2024年3月14日 | |
| 41 | クレジットカード情報保護対策分野 | カード情報の読み取りを想定していない機器において、従業員やカード会員が誤ってカード情報を読み取らせてしまう可能性があるが、どのような対策が考えられるか。 | 従業員やカード会員が当該機器に誤ってカード情報を読み取らせないよう、注意喚起することが考えられます。<br>注意喚起の方法としては、誤ってカード情報を読み取らせないように従業員教育を実施することや、当該機器等にカード情報を読み取らせないよう注意表示すること等が考えられます。 | 2020年3月27日 | |
| 42 | クレジットカード情報保護対策分野 | カード会社での情報保護を考える場合でも、紙、画像データ、音声データによるカード情報の保存は保持とはならないと考えてもよいか。 | 非保持化の概念が適用されるのは加盟店になります。カード会社はカード情報を保持することが前提であるため、クレジットカード・セキュリティガイドラインにおいてPCI DSS準拠を求めています。<br>従って、これらの媒体に関しても、PCI DSS準拠要件に従い適切な対策が必要です。 | 2020年3月27日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 43 | クレジットカード情報保護対策分野 | 利用している PCI PTS 端末の認定が有効であることは、どのように確認すれば良いか。 | 以下の PCI SSC 公式サイト内のページで、ご利用のPTS端末に関する認定状況を確認することができます。（ベンダー名、製品名で検索可能）<br>https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices<br><br>"EXPIRY DATE" は、認定を受けた PTS のバージョンごとに定められている失効日となります。<br>すでに失効しているPTS端末のリストは下記から参照できます。<br>https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_pin_transaction_security_expired?reference=4-30023<br><br>さらに端末ベンダーには年次の再検証も求められており、認定が延長/失効している可能性がある場合もあります。また失効後における継続利用については各ブランドで別途定められております。<br>それぞれについては端末の貸与を受けているアクワイアラーや端末ベンダーにご確認ください。 | 2025年3月4日 | |
| 44 | クレジットカード情報保護対策分野 | 利用している PCI P2PE ソリューションの認定が有効であることは、どのように確認すれば良いか。 | 以下の PCI SSC 公式サイト内のページで、ご利用のP2PEソリューションに関する認定状況を確認することができます。（ベンダー名、ソリューション名、またはリファレンス番号で検索可能）<br><br>https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions<br><br>"REASSESSMENT DATE" は再審査日となり、こちらが黒色表記であれば認定状況に問題はありません。ただしソリューションベンダーには年次での再検証も求められており、再審査日より前であっても認定が失効する場合があります。再審査日がオレンジ色表記の場合は失効猶予期間中、赤色表記の場合は失効済となります。<br>認定状況に問題がある場合はソリューションベンダーにご確認ください。また失効後における継続利用については、アクワイアラーにご確認ください。 | 2020年12月16日 | |
| 45 | クレジットカード情報保護対策分野 | 「オートローディング式自動精算機のIC対応指針」についてPCI PTSに準拠できない要件が書かれているが、具体的に準拠できない要件はPCI PTSのどの要件か。 | PCIにおける「PIN Transaction Sercurity(PTS) 」の「Modular Security Requirements」にて求められる要件のなかで、コア物理セキュリティ要件が該当します。<br>具体的な要件は各Versionごとに項番が異なり、PCI PTSのVersion間の要件番号の関係をご参照ください。 | 2023年3月14日 | |
| 46 | クレジットカード情報保護対策分野 | 「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書1】」についてPCI PTSにて想定されるリスク対策に関連したPCI PTS要件が記載されているが、具体的にはそれぞれどの項番の要件か。 | PCIにおける「PIN Transaction Sercurity(PTS) 」の「Modular Security Requirements」にて求められる要件のなかで、コア物理セキュリティ要件が該当します。<br>具体的な要件は各Versionごとに項番が異なり、PCI PTSのVersion間の要件番号の関係をご参照ください。 | 2025年3月4日 | |
| 47 | クレジットカード情報保護対策分野 | 「対面取引加盟店における非保持化対応ソリューションについて【附属文書2】」に記載の対策の一つとなっている PA-DSS準拠のPOSペイメントアプリケーション実装について、PA-DSSとは何か。 | Payment Application Data Security Standard の略で、PCI DSS の定める、決済アプリケーションを対象とするセキュリティ基準です。PCI DSS をベースとした14の要件から構成されています。<br>2022年10月28日でプログラムが終了しており、既に後継の基準となる Secure Software Standard がリリースされています。PA-DSS準拠アプリケーションから Secure Software Standard準拠アプリケーションへの移行については、アプリケーションベンダーやアクワイアラーにご確認ください。 | 2024年3月14日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 48 | クレジットカード情報<br>保護対策分野 | 「対面取引加盟店における非保持化対応ソリューションについて【附属文書2】」に記載の対策の一つとなっている PA-DSS準拠のPOSペイメントアプリケーション実装について、POSアプリケーションがPA-DSS準拠していることは、どのように確認すれば良いか。 | 以下の PCI SSC 公式サイト内のページで、ご利用のPOSアプリケーションに関する PA-DSS 認定状況を確認することができます。（ベンダー名、製品名、またはリファレンス番号で検索可能）<br>https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications<br><br>"EXPIRY DATE" は、認定を受けた PA-DSS のバージョンごとに定められている失効日となります。<br>"REVALIDATION DATE" は、年次で求められる再検証日となります。<br>新たに認定を受けた決済アプリケーションは「新規の導入が認められる（ACCEPTABLE FOR NEW DEPLOYMENTS）」の状態となります。その後、失効日以降や、年次再検証が未実施の場合に「既存の導入済のみ認められる（ACCEPTABLE ONLY FOR PRE-EXISTINGDEPLOYEMNTS」の状態となります。また、2022年10月28日でPA-DSS プログラムが終了しており、全ての既存のPA-DSS認定アプリケーションが「既存の導入済のみ認められる」の状態になります。従って、既に導入済のPA-DSS認定アプリケーションについては継続して利用可能となっております。<br>「既存の導入済みのみ認められる」の状態のアプリケーションの利用については、アプリケーションベンダーやアクワイアラーにご確認ください。一方、PA-DSS認定を受けていないアプリケーションを導入する場合は、PA-DSSの後継規準となるSecure Software Standardの認定を受ける必要があります。 | 2024年3月14日 | |
| 49 | クレジットカード情報<br>保護対策分野 | 「対面取引加盟店における非保持化対応ソリューションについて【附属文書2】」に記載の対策の一つとなっている Secure Software Standard 準拠のPOSペイメントアプリケーション実装について、Secure Software Standard とは何か。 | PCI SSCの定めるペイメントソフトウェアを対象とするセキュリティ基準で、PA-DSS の後継基準です。<br>PCI DSS をベースとしていた PA-DSS と異なり、新たに策定された基準となっています。<br>また、開発ベンダーを対象とする基準である Secure Software Lifecycle (Secure SLC) Standard と合わせて、Software Security Framework (SSF) を構成します。<br>PA-DSS が終了する2022年10月28日までは、Secure Software Standard と PA-DSS は並存期間となっておりましたが、 2022年10月28日以降は、PA-DSSが終息し、 Secure Software Standard に移行済となっています。<br>PA-DSS準拠アプリケーションから Secure Software Standard準拠アプリケーションへの移行については、アプリケーションベンダーやアクワイアラーにご確認ください。 | 2024年3月14日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 50 | クレジットカード情報保護対策分野 | 「対面取引加盟店における非保持化対応ソリューションについて【附属文書2】」に記載の対策の一つとなっている Secure Software Standard 準拠のPOSペイメントアプリケーション実装について、POSアプリケーションが Secure Software Standard 準拠していることは、どのように確認すれば良いか。 | 以下の PCI SSC 公式サイト内のページで、ご利用のペイメントソフトウェアに関する認定状況を確認することができます。（ベンダー名、ソフトウェア名、またはリファレンス番号で検索可能）<br><br>https://www.pcisecuritystandards.org/assessors_and_solutions/payment_software<br><br>"PAYMENT SOFTWARE STATUS" 列が Validated であれば、認定状況に問題はありません。<br>なお、ソフトウェアベンダーには年次での再検証も求められており、失効日("EXPIRY DATE")より前であっても認定が失効する場合があります。<br>認定状況に問題がある場合はソフトウェアベンダーにご確認ください。また失効後における継続利用については、アクワイアラーにご確認ください。 | 2024年3月14日 | |
| 51 | クレジットカード情報保護対策分野 | 1.4号事業者と契約している百貨店のような包括加盟店はすべからく4号事業者という位置づけとなるのか。また、包括代理となるSC事業者も4号事業者として法対応が必要となるのか。<br><br>2.自社は割販法改正により、「クレジットカード番号等取扱業者」の対面取引を行う4号事業者と認識しているが、同時にEC事業も展開している。こちらはリアル店舗とは異なり、自社で商品を仕入れて直接顧客へ販売しているため、2号事業者と認識しているが、この認識で正しいのか。 | 1.包括加盟店や包括代理という理由でなく、該当事業者が4号事業者の定義に該当するかで判断してください。<br>詳細については、「4号事業者、7号事業者の事業者識別の整理」をご参照ください。<br><br>2.頂戴しました情報であれば、加盟店(2号事業者)と整理できます。 | 2022年12月28日 | |
| 52 | クレジットカード情報保護対策分野 | PSPの店子紹介契約を締結しているECモール事業者は、クレジットカード番号等取扱業者としての法対応が必要か。 | モール運営者が自身で販売も行い、他の事業者の出店も扱っている場合、前者は2号事業者、後者は4号事業者若しくは7号事業者であり、4号事業者若しくは7号事業者としての対策が必要となります。取引内容、契約形態により複数の事業者に該当することがありますが、複数の事業者に該当する場合は、それぞれの該当する事業者としての対策が必要となります。 | 2025年3月4日 | |
| 53 | クレジットカード情報保護対策分野 | ECサイトを運営しているが、高齢者向けに注文を電話で受け付けるスキームを検討している。カード情報保護の観点で何か留意点はあるか。 | ECサイトに商品を掲載しても、インターネット経由でカード支払いを受け付けていないのであれば、EC決済には該当せず、MO・TO取引取扱加盟店となります。MO・TO取引取扱加盟店としてのセキュリティ対策を講じる必要があります。 | 2025年3月4日 | |
| 54 | クレジットカード情報保護対策分野 | カード情報保護対策を講じるにあたり、店頭やPOSに設置している磁気カードリーダーを撤去するよう要請を受けた。<br>磁気カードリーダーの撤去は必須であるのか。 | カード情報保護対策を講じるにあたり、磁気カードリーダーの撤去を求めているわけではありません。<br>磁気カードリーダーにおいてカード情報を読み取り、保持するのであれば、クレジットカード・セキュリティガイドラインを踏まえて適切なカード情報保護対策が講じられている必要があります。 | 2021年4月1日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 55 | 不正利用対策分野<br>（対面取引） | サインレスでクレジットカードを利用してもらっているが、ICカードの場合は運用が変わるのか。 | 本人確認ガイドラインで規定する「本人確認が必要となる業種/売場/商品等」に該当せず、かつ、「本人確認不要取引の CVM リミット金額」の範囲内については、加盟店は本人確認を不要とすることができます。<br>なお、本人確認不要取引を行うに当たっては、カード会員の保護及び不正利用発生の防止に留意しなければなりません。<br>詳細は、ご契約のカード会社（アクワイアラー）にご相談ください。<br>「本人確認不要取引」については、「クレジット取引における本人確認方法に係るガイドライン【附属文書15】」に記載しています。 | 2025年3月4日 | 【6.0版】P30／<br>【附属文書15】 |
| 56 | 不正利用対策分野<br>（対面取引） | 「クレジット取引における本人確認方法に係るガイドライン【附属文書15】」はどのように入手できるのか。 | 日本クレジット協会HPに掲載しております。<br>ホーム ＞安全・安心なクレジットカード取引への取組 ＞関連資料<br>なお、日本クレジット協会の会員については、日本クレジット協会会員専用ページから取得いただけます。 | 2025年3月4日 | |
| 57 | 不正利用対策分野<br>（対面取引） | ICカードによる取引では、本人確認は原則、PIN（暗証番号）入力により行うこととされているところ、カード会員がPINを失念している場合はサインで取引しても良いのか。 | この運用は「PIN入力スキップ機能（PINバイパス）」と言われるものですが、2025年３月をもって廃止としています。<br>詳細は、ご契約のカード会社（アクワイアラー）もしくはPSPにご相談ください。<br>なお、本人確認方法としての「サイン」の取得は、今後、加盟店の任意であり、取得しないことを推奨とすることを「クレジット取引における本人確認方法に係るガイドライン【附属文書15】」に記載しています。 | 2025年3月4日 | 【6.0版】P31／<br>【附属文書15】 |
| 58 | 不正利用対策分野<br>（対面取引） | クレジットカードのIC化の対象範囲について教えてほしい。 | クレジットカード・セキュリティガイドラインでは、クレジットカードのうち世界中で共通に使用できるがゆえに不正利用リスクの高い国際ブランド付きのカードを対象としておりますので、IC化の対象となるカードは国際ブランド付きのクレジットカードとなります。<br>一方、国際ブランドが付いていないカードについては、使用範囲が限定される点ではリスクは低いためクレジットカード・セキュリティガイドラインの対象としていませんが、リスクに応じたカード情報保護対策及び不正利用対策が必要である点には留意が必要です。 | 2020年3月27日 | 【6.0版】P20 |
| 59 | 不正利用対策分野<br>（対面取引） | 加盟店が保有するクレジットカード決済端末は全てIC対応する必要があるのか。 | 全てIC対応する必要があります。<br>特に、POSシステムでクレジットカード決済を行う加盟店は、自社のIC対応に係る実現方法を選択する際には、カード会社（アクワイアラー）や機器メーカー等に情報を求めてください。<br>ただし、①非対面取引に使用する端末、②クレジットカード継続課金の登録等に対面でカードを使う端末（有効性チェックのみに使用）はIC対応の対象外と整理されます。 | 2023年3月14日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 60 | 不正利用対策分野<br>（対面取引） | 現状、本人確認の運用としてPINを入力する方法の他、取引によっては署名（サイン）で対応するケースもあるが、このサインを取得するか否か、今後加盟店の裁量に委ねられる動きがあると聞いた。本人確認としてサインはもう使えなくなってしまうのか。 | 国際ブランドのルールが変更されたことにより、サインを取得するか否かは加盟店の裁量に委ねられており（サイン取得の任意化）、世界的にも既にサインが従来果たしてきた本人確認としての有効性は有しておりません。<br>また、海外のカード会社が発行したオフラインPIN環境に対応しないカードが利用される場合や、非接触IC取引においてCVMリミット金額を超える取引となる場合においても、サインの取得は任意としております。<br>詳細は、ご契約のカード会社（アクワイアラー）もしくはPSPにご相談ください。<br>なお、「サイン取得の任意化」については、「クレジット取引における本人確認方法に係るガイドライン【附属文書15】」に記載しています。 | 2025年3月4日 | 【6.0版】P31／<br>【附属文書15】 |
| 61 | 不正利用対策分野<br>（非対面取引） | 「動的（ワンタイム）パスワード」とは何か。 | 動的(ワンタイム)パスワードは、利用する都度変更される使い捨てパスワード（動的／可変パスワード）です。事前に登録した数値による固定パスワード（静的パスワード）よりも、不正利用のリスクを低減することが期待できます。<br>カード会社が発行する専用デバイスや顧客のスマートフォンアプリでパスワードを表示する方法とSMS等で都度顧客に送信される方法があります。<br>動的(ワンタイム)パスワードの管理は、イシュアーの認証を代行するACS（Access Control Server）ベンダー側で行うことが多いようです。<br>その他にも、指紋等の生体情報による認証（生体認証）等も認証方法として認められるものであり、有効な方策です。<br>詳細は、「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照ください。 | 2025年3月4日 | 【附属文書14】 |
| 62 | 不正利用対策分野<br>（非対面取引） | デバイス情報とは何を指すのか、具体的に教えてください。 | ECにおけるユーザーの機器デバイス（パソコン、スマートフォン等）から得られる情報となります。 | 2020年3月27日 | |
| 63 | 不正利用対策分野<br>（非対面取引） | MO・TO取引取扱加盟店が講じるべき不正利用対策を教えて欲しい。 | 不正利用被害のほとんどがEC加盟店において発生している現状を踏まえ、その被害を極小化するために、クレジットカード・セキュリティガイドラインの「５－２－３ 非対面取引（MO・TO取引取扱加盟店）＞５－２－３－２ 不正利用対策」にて、MO・TO取引取扱加盟店が講じるべき不正利用対策について取りまとめています。<br>MO・TO取引取扱加盟店が講じるべき不正利用対策としては、クレジットカード・セキュリティガイドラインでEC加盟店が講じる必要のある対策と同等以上の対策として、「オーソリゼーション処理の体制整備」と「善管注意義務」について最低限対応することが必要となります。 | 2025年3月4日 | 【6.0版】P43 |
| 64 | 不正利用対策分野<br>（非対面取引） | MO・TO取引取扱加盟店における不正利用対策を複数導入する際の考え方を教えて欲しい。 | MO・TO取引取扱加盟店で不正利用対策を複数導入する場合は、EC加盟店特有の対策（EMV 3-Dセキュア等）は導入できないため、他の対策での対応となります。なお、セキュリティコードで対応することは可能ですが、センシティブ情報にあたるため保存することができない点は運用上で考慮する必要があります。<br>「EC加盟店におけるセキュリティ対策　導入ガイド【附属文書20】」も参照ください。 | 2025年3月4日 | 【附属文書20】 |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 65 | 不正利用対策分野<br>（非対面取引） | EC加盟店の不正利用対策については、何をどこまで対応すれば対策済として良いのか。基準があれば提示して欲しい。 | EC加盟店の指針対策として、以下の不正利用対策を求めております。<br><br>・EC加盟店<br>「オーソリゼーション処理の体制整備」と「善管注意義務」に加え、「EMV 3-Dセキュアの導入」と「適切な不正ログイン対策の実施」が必要。<br><br>・不正顕在化加盟店<br>類似の不正利用の発生を防止するために、不正利用の発生状況や取扱商品、スキーム等によって異なる不正利用の手口に応じて「適切な対策の追加導入」や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」が必要。<br>※不正顕在化加盟店：カード会社（アクワイアラー）各社が把握する不正利用金額が3ヵ月連続50万円を超えた場合に該当する。 | 2025年3月4日 | 【6.0版】P36 |
| 66 | 不正利用対策分野<br>（非対面取引） | 主たる商材の扱いが変更になり、「相対的にリスクが高い商材」の取扱いがなくなったのだが、現在、導入している対策は止めてもいいのか。 | 「相対的にリスクが高い商材」を取り扱う加盟店でなくなったとしても、法令の主旨に照らして、不正利用被害を未然に防止するために有効な対策については継続して行っていただくようお願いいたします。 | 2025年3月4日 | 【6.0版】P40 |
| 67 | 不正利用対策分野<br>（非対面取引） | 不正顕在化加盟店は、アクワイアラー個社の基準により認定されるということだが、アクワイアラー毎にその評価が分かれている状態の加盟店は、1つのアクワイアラーから不正顕在化と認定された時点で不正顕在化加盟店となるのか。 | １つのアクワイアラーから不正顕在化と認定された時点で、当該加盟店は不正顕在化加盟店ということになります。 | 2020年3月27日 | |
| 68 | 不正利用対策分野<br>（非対面取引） | カード会社（アクワイアラー）各社が把握する不正利用金額が3ヵ月連続50万円を超えた場合、不正顕在化加盟店とされ、類似の不正利用の発生を防止するために適切な対策の追加導入が求められることになるが、取扱高の大小に関わらず基準を一定額とするルールはおかしいのではないか。 | 不正利用が不正を働いている犯罪者の大きな資金源となることを防ぐために、不正利用被害の絶対額を下げるという目的があります。そこで、不正利用被害が大きい加盟店の上位から重点的に下げていく考え方としており、一定の基準以上の不正利用被害が発生していた場合は、不正顕在化加盟店としています。不正利用被害も大きいが、取扱高が巨額で不正率で考えると薄まってしまい、不正顕在化加盟店としないことにした場合は、不正利用被害の全体を押し下げることは難しいと考えています。ご理解いただければと思います。 | 2025年3月4日 | |
| 69 | 不正利用対策分野<br>（非対面取引） | 不正顕在化の不正利用金額はどのようなものか。調査中の金額も含まれるのか。 | 「カード名義人が関与せず、第三者による、非対面不正利用による被害であると確定した金額」となります。 | 2020年3月27日 | |

| 項番 | カテゴリー | 質問内容 | 回答 | 更新日 | 参照元 |
|---|---|---|---|---|---|
| 70 | 不正利用対策分野（非対面取引） | 不正顕在化加盟店は適切な不正利用対策を追加導入し不正利用が収まれば不正顕在化加盟店ではなくなり、当該対策は止めてもいいのか。 | 不正利用が収まったとしても、当該対策を導入していることで不正利用が収まっていると考えられますので、導入した対策については継続して行っていただく必要があります。 | 2025年3月4日 | 【6.0版】P40 |
| 71 | 不正利用対策分野（非対面取引） | 「EMV 3-Dセキュアの導入」について、加盟店単位での例外は認められないということか。 | 「EMV 3-Dセキュアの導入」の趣旨としては、カード会社（イシュアー）による本人確認が適切に行われるための措置として、導入を求めるものです。<br>EMV 3-Dセキュアの未導入が認められる取引については、「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照ください。 | 2025年3月4日 | 【附属文書14】 |
| 72 | 不正利用対策分野（非対面取引） | EMV 3-Dセキュアの運用について、全てのクレジットカード取引にEMV 3-Dセキュアによる認証を行わなければならないのか。 | EMV 3-Dセキュアによる認証の運用方法について、原則としては決済の都度、EMV 3-Dセキュアによる認証を行うことが求められますが、加盟店がEMV 3-Dセキュア以外に講じる不正利用対策の内容や抑止効果に応じて、カード番号の登録時にEMV 3-Dセキュアによる認証を行う運用や加盟店のリスク判断によりEMV 3-Dセキュアによる認証を行う運用も認められることとしております。<br>詳細は「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照ください。 | 2025年3月4日 | 【6.0版】P38／【附属文書14】 |
| 73 | クレジットカード情報保護対策分野 | EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施について、低リスクと考えられる業種も同様に実施の対象となるのか。 | EC加盟店のシステム及びWebサイトの脆弱性対策は、EC加盟店の規模や業種、取扱商材によるリスクの大小にかかわらず、実施いただく必要があります。 | 2025年3月4日 | 【6.0版】P34 |
| 74 | 不正利用対策分野（非対面取引） | 「EMV 3-Dセキュアの安定稼働のための対応に関係事業者と連携し継続的に取り組む」とは、具体的に何をすればよいか。 | EMV 3-Dセキュアに関するシステムの安定稼働のためには、各EMV 3-Dセキュア関係事業者において、システムのキャパシティ確保や安定稼働に向けた対策とリソース確保が重要であり、万一の障害等の発生に備えるために緊急連絡体制の整備も重要となります。<br>詳細は、「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照ください。 | 2025年3月4日 | 【附属文書14】 |
| 75 | 不正利用対策分野（非対面取引） | 「不正ログイン対策」について、「カード決済前」のEC加盟店のWebサイトへの「会員登録時」「会員ログイン時」「属性情報変更時」の対策として実行する、とあるが、それぞれの場面毎に1つ以上導入しなければならないのか。 | EC加盟店における「不正ログイン対策」は、決済前の「会員登録時」「会員ログイン時」「属性情報変更時」のそれぞれの場面毎に有効な対策を1つ以上導入することが推奨されますが、不正利用の手口によって対策が必要な場面や導入すべき対策は異なってくることから、その手口による不正利用発生のリスクに応じて、それぞれの場面を考慮した適切な対策を「EC加盟店におけるセキュリティ対策　導入ガイド【附属文書20】」の第2部「3.不正ログイン対策（決済前の対策）」に記載の対策から、1つ以上導入いただくこととなります。 | 2025年3月4日 | 【附属文書20】 |
| 76 | 不正利用対策分野（非対面取引） | スマートフォンのアプリで決済サービスを展開している場合でも、「適切な不正ログイン対策の実施」は必要か。 | スマートフォンアプリにおいて、他人のID/パスワードを利用した乗っ取りやなりすましによるログインを行う不正手口も多いため、アプリ上の決済についても、不正ログイン対策の導入が必要です。<br>アプリ上の決済についての不正利用対策につきましては、「スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について【附属文書17】」を参照ください。 | 2025年3月4日 | 【附属文書17】 |