「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 ＦＡＱ」

更新日：2019年4月9日

項番	カテゴリー	質問内容	回答
1	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。	2018年6月1日付で施行された改正割賦販売法では、加盟店のセキュリティ対策が義務化されております。法令上の義務となっておりますので、必要な措置が講じられている必要があります。
2	全体	カード情報保護の対応（非保持化もしくはPCI DSS準拠）と不正利用対策については、どちらが優先されるのか。	どちらかが優先ということではなく、効率よく双方取り組むという考えです。
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。	改正割賦販売法では、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。 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。
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臓型の機器でカード取引を行うことから、対面取引と整理できます。IC対応は改正割賦販売法の施行日（2018年6月1日）までの対応が基本となりますが、最終的に2020年3月末までに完了することが求められます。
5	全体	セキュリティ対策の対応期限について教えて欲しい。	実行計画における対応期限は以下のとおりです。既に改正割賦販売法が2018年6月1日付で施行されており、必要な措置が講じられている必要があります。 ＜各主体別の対応完了期限＞ ・対面加盟店： 2018年6月1日（最終的に2020年3月末） ・非対面加盟店： 2018年3月末 ・カード会社、PSP： 2018年3月末
6	全体	実行計画2018以降、対応期限を2018年３月までとする旨の記載が削除されたが、2020年まで延びたということか。	実行計画2018公表の段において、2018年3月は期限到来直前のため敢えて記載していなかったものであり、延長という考え方自体はございません。
7	全体	実行計画にあるセキュリティ対策の対応期日に間に合わない場合、加盟店に対する罰則規定はあるのか。	実行計画上、罰則規定はありません。 しかし、加盟店のセキュリティ対策措置（情報保護対策、不正利用防止）については、改正割賦販売法に定める加盟店の義務となりますので、実行計画に掲げるセキュリティ対策措置を講じていない場合は、義務を果たしていない状況になります。セキュリティ対策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べく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。

項番	カテゴリー	質問内容	回答
8	全体	対応期限と改正割賦販売法の施行日とのギャップについて教えて欲しい。	【実行計画 P21、34 等】 対面加盟店については、実行計画の対応期限である2020年3月末の前に改正割賦販売法が施行されているため、実行計画の対応期限と改正割賦販売法の施行日とのギャップが生じております。このため、現実行計画では、「改正割賦販売法が2018年6月1日から施行されていることから、対面加盟店においても、その時までの対応を基本とし、最終的には、全加盟店が2020年3月末までにカード情報の適切な保護に関する対応（非保持化又はPCI DSS準拠）及びIC取引（クレジットカードのIC化とクレジット決済端末のIC対応により実現）が可能となるよう自社のクレジット決済端末のIC対応が完了している状態になっていることを目指す。」旨記載しております。
9	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。 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対応の対象となります。
10	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、実行計画で求める対策を講じる必要があるか。	実行計画では、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。 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留意してください。
11	情報保護対策	カード情報保護対策における実行計画2018と2019の違いは何か。	カード情報保護対策において基本的な考え方に変更はございませんが、カード情報漏えい事案の動向を踏まえ、実行計画2019では、今まで以上に機器・ネットワークの脆弱性対策、設定不備への注意喚起、新たな脅威への対応を強く呼びかけています。

項番	カテゴリー	質問内容	回答
12	情報保護対策	カード情報の定義を教えて欲しい。	【実行計画　P10　脚注4】 実行計画上は、以下のとおり定義されております。 『「カード情報」とは、クレジットカード会員データ（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）をいう。ただし、クレジット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。また、以下の処理がなされたものはクレジットカード番号とは見做さない。 ・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） ・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国際的な第三者機関に認められた桁数を切り落とし、自社内では特定できないもの） ・無効処理されたカード番号』
13	情報保護対策	紙の媒体でクレジットカード番号を保存しているが、これはカード情報の保持となるのか。	【実行計画 P12 脚注8】 実行計画における非保持化とは、以下(※)を除き、カード情報を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『保存』、『処理』、『通過』しないことと定義されております。 ※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（通話データを含む）においてカード情報を保存する場合。 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。 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。
14	情報保護対策	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。	【実行計画 P12 脚注8】 実行計画では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。 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。 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。

項番	カテゴリー	質問内容	回答
15	情報保護対策	通話録音をしており、カード情報も含まれるが、これはカード情報の「保持」となるのか。	【実行計画 P12 脚注8】 実行計画における非保持化とは、以下(※)を除き、カード情報を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『保存』、『処理』、『通過』しないことと定義されております。 ※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（通話データを含む）においてカード情報を保存する場合。 そのため、非保持化（非保持と同等/相当）を実現している加盟店で、通話録音でカード情報が含まれ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。 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。
16	情報保護対策	「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、クレジットカード会員データ（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、クレジット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。 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。
17	情報保護対策	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」に該当しないと書かれているが(実行計画 P12脚注8)、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。実行計画上、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。
18	情報保護対策	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。	【実行計画 P10 脚注4】 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。
19	情報保護対策	カード会員データ（カード番号、カード会員名、サービスコード、有効期限）にある「カード会員名」はカード決済に係る会員名であるが、一方加盟店自体でもカード決済に関わらず「顧客名」は持っている。機密認証データとカード番号、有効期限、サービスコードがなければ「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。	クレジットカード会員データ（カード番号、カード会員名、サービスコード、有効期限）のうち、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。 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。
20	情報保護対策	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。	【実行計画 P10 脚注4】 実行計画上では、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国際的な第三者機関に認められた桁数を切り落とし、自社システム内では特定できないもの)、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。 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。

項番	カテゴリー	質問内容	回答
21	情報保護対策	トークン（トークナイゼーション）やトランケート（トランケーション）を検討しているが、定義を教えてほしい。	【実行計画 P10 脚注4】 実行計画上のカード番号と見做さない処理であるトークナイゼーションとは、「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元のクレジットカード番号を特定できない」処理を施したものです。 また、同じくカード番号と見做さない処理であるトランケーションとは、「自社システムの外でクレジットカード番号を国際的な第三者機関に認められた桁数を切り落とし、自社システム内では特定できない」処理を施したものです。
22	情報保護対策	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。
23	情報保護対策	PSPの定義について教えて欲しい。	【実行計画 P2 脚注1】 本実行計画においては、インターネット上の取引においてEC加盟店にクレジットカード決済スキームを提供し、カード情報を処理する事業者をいいます。
24	情報保護対策	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。	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。 【実行計画 P12 脚注8】 実行計画で定められる「非保持化」とは、「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」です。
25	情報保護対策	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Java Script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。 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」(※)をご確認ください。 ※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。
26	情報保護対策	PCI DSSとはどのようなものか。	【実行計画 P52】 PCI DSSとはカード情報を取り扱うすべての事業者に対して国際ブランドが定めたデータセキュリティの国際基準です。安全なネットワークの構築やカード会員データの保護等、12の要件に基づいて、約400の項目から構成されており、「準拠」とは、このうち該当する要求事項にすべて対応できていることをいいます。
27	情報保護対策	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。 http://www.jcdsc.org/
28	情報保護対策	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。	【実行計画 P5】 国際ブランドが付いていないカードについては実行計画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が必要である点にはご留意ください。

項番	カテゴリー	質問内容	回答
29	情報保護対策	実行計画におけるカード情報保護対象の範囲に電子マネー情報も含むのか。	【実行計画 P5】 実行計画では国際ブランド付きのクレジットカードのカード情報を対象としており、電子マネー情報は含みません。
30	情報保護対策	カード情報を保持する加盟店は、売上（取引件数）等の規模に関係なく、全ての加盟店においてPCI DSS準拠が必須なのか（何か基準があれば、開示してほしい）。	加盟店は、カード情報の非保持化またはカード情報を保持するのであればPCI DSS準拠が必須になります。 準拠方法等については、日本クレジット協会が策定した『PCI DSS準拠にかかる基準及び検証方法等に関する実施要領』をご確認ください。 ※「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」は日本クレジット協会のホームページ『安全・安心なクレジットカード取引への取組み「関連資料」』に公開されています。
31	情報保護対策	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。	【実行計画 P12】 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。
32	情報保護対策	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ございますので、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、削除してください。 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。
33	情報保護対策	「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。	【実行計画 P13、14】 「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（リダイレクト（リンク）型かJava Script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。
34	情報保護対策	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。	【実行計画 P13、14】 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。実行計画上、非保持の場合はPCI DSS準拠までは求めていませんが、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。
35	情報保護対策	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。 【実行計画 P13～15】 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(※)。 ※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」に記載してございます。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。

項番	カテゴリー	質問内容	回答
36	情報保護対策	PCI DSSに準拠するにはどうしたら良いか。	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。 あわせて「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」(※)をご確認ください。 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。 ※「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」は日本クレジット協会のホームページ『安全・安心なクレジットカード取引への取組み「関連資料」』に公開されています。
37	情報保護対策	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が保存、処理、通過しないのであれば、実行計画上、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。
38	情報保護対策	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。 なお、実行計画には以下のように記載されております。 【実行計画 P21】 「カード情報の適切な保護を推進するためには、カード情報を取り扱う事業者全てが自主的な取組を進めることが重要である。なお、各主体が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求めていくこととする。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る。」
39	情報保護対策	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、国際ブランド合意の下、別紙「３．タイプ別SAQ」（実行計画P54）の表にあるSAQ P2PEの33項目も含めて、PCI DSS準拠不要という理解でよいか。	実行計画における非保持化(非保持と同等/相当を含む)を達成している場合は、PCI DSSへの準拠は求められておりません。 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。
40	情報保護対策	PCI DSS準拠への対応期限が対面加盟店とEC加盟店で異なるのはなぜか。	現状、カード情報の漏えいの頻度が高いEC加盟店は対面加盟店よりも早期に対策を行う必要があります。現在、我が国において最も被害額が多い番号盗用の手口を未然防止するためにもPCI DSSへの早期準拠を求めています。
41	情報保護対策	加盟店(ECサイト・対面とも)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）。 この場合、PCI DSSの準拠は必要か。またその場合、対応期限はいつになるか。	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。 なお、それら対応期限については、対面に係る部分は改正割賦販売法の施行日（2018年6月1日）までの対応が基本となるが、最終的には遅くとも2020年3月末まで、非対面に係る部分は2018年3月末までと、業務及びシステムが完全に分離されていることをもって段階的に対応していくこと（セグメント）も可能になります。PCI DSS準拠時のセグメント可否等については、QSAに確認してください。
42	情報保護対策	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。

項番	カテゴリー	質問内容	回答
43	情報保護対策	同一の加盟店で対面取引と非対面取引があり、データ分析の為にカード番号をサーバーに保存している。その場合の対応期限は対面、非対面のはどちらで考えるべきか。	対面取引と非対面取引それぞれで扱うカード情報を確実に分離できる場合は、各々の期限で対応する事も可能ですが、完全に分離できないのであれば期限が早い方かつより厳格な方法（オンサイトレビュー等）、対策が強固な方に合わせてPCI DSS準拠の対応をお願いいたします。
44	情報保護対策	PCI DSSに準拠するための認定審査機関を紹介して欲しい。	当協会から個別に審査機関をご紹介することは公正性の観点からできかねます。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。
45	情報保護対策	PCI DSS準拠への検証方法の自己問診について、その結果をどこかに提出することが求められたりするのか。また自己問診の運用はどのようになっているのか。	PCI DSSの原則では、自己問診（SAQ）の実施は年1回、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。 ・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。 ・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。 ・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。
46	情報保護対策	自己問診では、役員が署名するとあるが、どのような意味合いの署名になるのか。	内容に関して責任をもって認めるというものです。企業によって、社長や役員が署名しています。当該企業の決裁権限に従った形でよいと思われます。一般的には役員クラスの署名が多いです。
47	情報保護対策	一つの会社で加盟店の顔、イシュアーの顔がある場合、どこまでやるべきか。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。	実行計画では、主体毎にPCI DSS準拠の期限が決められているので、期限内の対応が必要となります。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。 システムが共通の場合は、期限が早い方、且つ、より厳格な方法（オンサイトレビュー等）に合わせてPCI DSS準拠の対応をお願いしております。その際の準拠の方法は、日本クレジット協会が策定した『PCI DSS準拠にかかる基準及び検証方法等に関する実施要領』をご確認ください。準拠の要領についてはJCDSCにご相談ください。 ※「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」は日本クレジット協会のホームページ『安全・安心なクレジットカード取引への取組み「関連資料」』に公開されています。
48	情報保護対策	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。
49	情報保護対策	「PCI DSS準拠にかかる基準及び検証方法等に関する実施要領」（平成29年6月21日）では、クレジットカード会社のアクワイアラーでレベルA以外の会社は、自己問診によるPCI DSSの検証方法でよいということであるが、具体的にどのような自己問診を使用することになるのか。	「PCIデータセキュリティ基準」において、アクワイアラー用の自己問診はございません。 イシュアーが利用できる「サービスプロバイダ用自己問診D」をご利用ください。

項番	カテゴリー	質問内容	回答
50	情報保護対策	非保持化を実現したとしても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ィルス対策、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。 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なども重要になります。
51	情報保護対策	非保持化(非保持と同等/相当を含む)について、誰が達成もしくは未達成を証明するのか。	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。 なお、改正割賦販売法の考え方は、カード会社(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。
52	情報保護対策	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Java script型）に違いはあるのか。	実行計画上、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。 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。 リンク型：SAQ A(24項目)　Java Script型はSAQ A-EP(192項目)
53	情報保護対策	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」(実行計画 P,20)とはどのようなものか。また、公表されているものなのか。	当該マニュアルは非公表扱いとなっております。 加盟店の方は、必要な際に契約されているカード会社にお問い合わせください。
54	情報保護対策	「対面加盟店における非保持と同等/相当のセキュリティ確保を可能とする措置に関する具体的な技術要件について」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ます。
55	情報保護対策	実行計画で求められているカード情報保護対策に準じるため、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。 実行計画に照らし、磁気カードリーダーの撤去は必須であるのか。	実行計画はカード情報保護対策を求めているものであり、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。 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、実行計画を踏まえて適切なカード情報保護対策を実施してください。
56	情報保護対策	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。 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。
57	情報保護対策	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、実行計画においてPCI DSS準拠を求めています。 従って、これらの媒体に関しても、PCIDSS準拠要件に従い適切な対策が必要です。

項番	カテゴリー	質問内容	回答
58	偽造防止対策	偽造防止対策における実行計画2018と2019の違いは何か。	①WG2分野で定めた指針等（計5点）について見直しを行い、これまで寄せられた意見等を反映するとともに、誤植等も含め改訂しました。 ・「国内ガソリンスタンドにおけるICクレジットカード取扱対応指針」 →SS給油決済での有効性チェックオーソリ依頼時のIC取引電文の対応事例を明示 ・「オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について」 →自動精算機への適正なPCI PTS端末の設置に関する注意喚起を実施 ・「ICカード対応POSガイドライン1.2版」 →自動精算機もPOSに準じてIC対応が必要であることから、自動精算機等の非有人型端末を対象外としている記載を削除 ・「ICカード対応POS導入の手引き ～ 認定・試験プロセス概要 ～」 →ブランドテスト実施上のプレーヤー毎の役割分担の明確化を目的とし、当該役割分担の一例を追加するとともに、ブランドテスト実施要否の見直しに伴い、その一覧を最新化、簡略化し反映 ・「非接触EMV対応POSガイドライン 取引処理編」 →注釈の追記 ②継続検討中であったIC対応を要する端末についての整理を行い、カードの有効性チェックのみを行う端末、撤収予定（長期未稼働端末）、POSと分類される端末についてIC対応対象から除外しました。 ※カード会社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。
59	偽造防止対策	「クレジットカードのIC化１００％」について、この「クレジットカード」の定義が示されているものはあるか。	【実行計画 P5】 実行計画では、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います。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本実行計画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すべきとなっております。
60	偽造防止対策	「IC取引における本人確認方法に係るガイドライン」、「本人確認不要（サインレス／PINレス）取引に係るガイドライン」はどのように入手できるのか。	「IC取引における本人確認方法に係るガイドライン」、「本人確認不要（サインレス／PINレス）取引に係るガイドライン」は、クレジット業界としての実行計画推進のための方策の位置づけとなっています。 ※上記ガイドラインについては、カード会社、機器メーカーを通じお取り寄せください。 ※カード会社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。
61	偽造防止対策	「ICカード対応POSガイドライン」はあらためて提示されるのか。	「ICカード対応POSガイドライン」の初版が2017年3月に策定されて以降、改訂が行われております（直近の改訂は2019年2月21日）。本ガイドライン最新版については、カード会社、機器メーカーを通じお取り寄せください。 ※カード会社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。
62	偽造防止対策	「IC取引時のオペレーションルール」とはどのような内容なのか。	当該ルールは個別具体的に示してはいませんが、「IC取引における本人確認方法に係るガイドライン」や「ICカード対応POSガイドライン」に包含されております。

項番	カテゴリー	質問内容	回答
63	偽造防止対策	「オフラインPIN」とはどのようなものか。	【実行計画 P25　脚注15】 「オフラインPINとは、カード利用時に会員が入力した数字と、カードのICチップ内に保存されたPINとを照合するものであり、一方、オンラインPINは、オンラインネットワークを経由してカード会社(イシュアー)のシステム上で照合するものである。」
64	偽造防止対策	ICカードは顧客にPIN入力をしてもらうとの事だがPINを忘れた場合は現状通りのスワイプ＆サインで計上しても良いのか。 ICカードによる取引では、顧客にPIN（暗証番号）入力をしてもらうことになるが、PINを忘れた場合は磁気ストライプの読み取り（スワイプ）とサインで取引しても良いのか。	【実行計画 P26】 原則IC対応端末において、ICカードは磁気ストライプでの取扱いはできません。 ただし、カード会員のPIN失念等の一時的な救済機能として、PIN入力スキップ機能（PINバイパス）を認めております。 なお、PIN入力スキップ機能（PINバイパス）は、一部海外のカード発行会社のカード等、PINバイパスを許容しないカードも存在し利用阻害が発生することや、PINによる本人確認を実施しないことで不正利用が発生する可能性があることから、業界として、カード会員に対するPIN認知の啓発の活動と並行して、PIN入力スキップ機能の将来的な廃止を検討しております。
65	偽造防止対策	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カード対応となった場合は運用が変わるのか。	【実行計画 P27、28】 実行計画では、IC取引においても限定的にPINレスは認められます。クレジット業界では、「IC取引における本人確認方法に係るガイドライン」及び「本人確認不要(サインレス/PINレス)取引に係るガイドライン」を策定しています（2016年9月27日初版策定、2018年1月23日改訂）。 本ガイドライン最新版については、カード会社を通じお取り寄せください。
66	偽造防止対策	SS（サービスステーション）の自動精算機について、協議会で何か課題があるのなら内容を教えてほしい。	【実行計画 P29】 SSにおけるIC対応については、精算場所ごとのオペレーション、決済端末等の情報通信・決済機器にかかる各種法規制（防爆等）対応や給油機一体型オートローディング式自動精算機のPCI PTS認定、店員による給油サービス後の車内精算におけるPIN入力等が課題であるため、2020年時点でのIC対応における実現可能な方策を示した「国内ガソリンスタンドにおけるICクレジットカード取引対応指針」がとりまとめられております。また、オートローディング方式の自動精算機については、PCI PTSの代替コントロール事例を示す「オートローディング式自動精算機のIC化対応指針と自動精算機の本人確認方法について」がとりまとめられております。 ※カード会社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。
67	偽造防止対策	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。 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。

項番	カテゴリー	質問内容	回答
68	偽造防止対策	実行計画上、クレジットカードのICカードへの切替え加速と、カード会員からの要望があれば、更新時期の到来を待たずに同カードへの切替えを可能とする環境整備が謳われている。 この切替えにあたり、セキュリティ上の観点から番号切替えをすべきか、同一番号のままでよしとするのか、考え方を教えて欲しい。	【実行計画Ｐ３６】 実行計画上求められているのは、国内で流通する国際ブランド付きクレジットカードが2020年3月末までに100%IC化されていることのみであり、磁気カードからICカードへの切替えを含め、カードの再発行にあたり、番号を切替えるか否かは発行元であるイシュアーの判断の下行われるもの、という考え方になります。 以下、実行計画記載事項 （１）クレジットカードIC化に向けた取組 ・カード会社（イシュアー）は、2020年3月末までに国内で流通する国際ブランド付きクレジットカードが100%IC化されていることを目指し、当該カードの更新時期を待たず、ICカードへの切替を加速する。
69	不正利用対策 （なりすまし防止）	不正利用対策における実行計画2018と2019の違いは何か。	①不正利用方策の内容を見直しました。 ・「属性・行動分析」の定義・メリットを再整理 ・「券面認証（セキュリティコード）」の多数回アクセスへの対策を追加 ・「３Ｄセキュア」の取組強化（リスクベース認証導入の推進） ②好事例集（実行計画上の方策導入による不正抑止の好事例の紹介）を改訂しました。 ③一部の名称を変更しました。 ・「高リスク（業種）加盟店」→「高リスク商材取扱加盟店」 ・「特定４業種」→「特定４商材」 ・「属性・行動分析」→「属性・行動分析（不正検知システム）」 ・「（カード会社の）不正検知システム」→「オーソリモニタリング」
70	不正利用対策 （なりすまし防止）	実行計画で示す方策以外で法履行ができる方策を教えて欲しい。	実行計画上の方策と同等以上の性能を満たしているものであれば認められます。なお、事業者はその方策が実行計画上の方策以上の性能であることの証明を求められる可能性があります。
71	不正利用対策 （なりすまし防止）	3Dセキュア2.0の導入可能な時期や、導入の際のメリット・デメリット及び、現行3Dセキュアとの互換性を教えて欲しい。	3Dセキュア2.0の導入可否については、契約アクワイアラーにご確認願います。実行計画2019にも記載のとおり、メリットはブラウザベースに加え、アプリケーションベースに対応していること、リスクベースの判定項目が増えて判別力の向上によりパスワード入力の機会が減少することが期待できることです。留意点は、現行3Ｄセキュアと互換性は無いので新たなソフトを組み入れる必要があることです。

項番	カテゴリー	質問内容	回答
72	不正利用対策 （なりすまし防止）	「静的（固定）パスワード」の課題に対する有効な解決策として示されている、「動的（ワンタイム）パスワード」や「生体認証」とは何か。	「ワンタイムパスワード」 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。 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。 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。 「生体認証」 指紋等の生体情報をスマートフォン等の端末と紐付けておくことで、カード利用の都度、端末における生体情報の照合により本人確認を行えるようにするものです。生体情報の管理はスマートフォン等の端末で行われる（カード会社や加盟店では生体情報を持たない）ことが多いです。
73	不正利用対策 （なりすまし防止）	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取引におけるユーザーの機器（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。
74	不正利用対策 （なりすまし防止）	オーソリゼーションと善管注意義務は追加方策になるのか。	追加方策にはなりません。全非対面加盟店が最低限行っている条件となります。
75	不正利用対策 （なりすまし防止）	MO・TO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加盟店で対応する場合は、ＥＣ特有の方策（３Ｄセキュア）は導入できないため、他の方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ございます。
76	不正利用対策 （なりすまし防止）	加盟店の不正利用防止対策については、何をどこまでや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。	実行計画2019では、リスクに応じた多面的・重層的な対応を求めております。その基準としては、全ての加盟店が対応するべき対策として、①善管注意義務と②オーソリゼーションの導入があります。その上で、高リスク商材（デジタルコンテンツ、家電、電子マネー、チケット）を主たる商材として取り扱う加盟店（高リスク商材取扱加盟店）においては、全ての加盟店が対応するべき対策＋実行計画上の方策を１つ以上、不正顕在化加盟店と認定される場合は全ての加盟店が対応するべき対策＋実行計画上の方策を２つ以上、と指針を定めております。 ※実行計画上の方策：本人認証、券面認証、属性・行動分析（不正検知システム）、配送先情報 ※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継続的に一定金額を超えた場合に該当する。
77	不正利用対策 （なりすまし防止）	不正被害発生状況等に応じた不正利用への対応基準に高リスク商材の4商材とあるが、4商材を一部でも取扱っている加盟店は高リスク商材取扱加盟店の定義になるのか。	取扱の「主たる商材」で判断されます。そのため、一部の取扱いでは「主たる商材」には該当しないと想定されますが、念のため、契約アクワイアラーにご確認ください（判断はアクワイアラーが行います）。
78	不正利用対策 （なりすまし防止）	主たる商材の扱いが変更になり、高リスク商材取扱加盟店ではなくなったのだが、現在、実行計画上の方策は１つ導入している。この場合、当該方策は止めてもいいのか。	高リスク商材を取り扱う加盟店でなくなったとしても、不正利用被害を未然に防止する方策は有効だと考えられますので、継続して行っていただくようお願いします。

項番	カテゴリー	質問内容	回答
79	不正利用対策 （なりすまし防止）	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。
80	不正利用対策 （なりすまし防止）	不正発生被害が継続的に一定額を超えた場合、不正顕在化加盟店とされ、２方策以上の対策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。	実行計画では、不正利用被害の絶対額を下げる目的がございます。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行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おります。ご理解いただければと思います。
81	不正利用対策 （なりすまし防止）	不正顕在化加盟店として実行計画上の方策２つ以上の対策を求められた場合、当社は属性・行動分析（不正検知システム）を導入しているが、もう一つ別のシステムベンダーから属性・行動分析（不正検知システム）を導入して２つ以上として良いか。	実行計画上の各方策には各々に長所、短所の特徴があり、多面的・重層的な対策の考え方として、組合せにより短所を補う意味合いがあるので、他の方策の導入をご検討ください。
82	不正利用対策 （なりすまし防止）	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、なりすまし不正行為による被害であると確定した金額」となります。
83	不正利用対策 （なりすまし防止）	好事例を取りまとめ、業界団体に配布とあるが、どの業界に配布したのか。また、その資料は協会ホームページに公開されているのか。	PSPに向けてEC決済協議会、日本通信販売協会等の協議会委員の業界団体に展開しています。資料は、一般公開はしておりません。必要に応じて契約アクワイアラーにお問い合わせください。