「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：2021年4月1日

項番	カテゴリー	質問内容	回答	更新日
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）】 ・推進期限の設定がありません。 ・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。 ・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。 【両文書の位置付け】 ・「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。 ・「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。 ・「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。 ・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、2021年3月10日付で【2.0版】へと改定されております（項番8参照）。	2021年4月1日
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、カード会社と加盟店においては、クレジットカード番号等の適切な管理や不正利用の防止といった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。 また、2021年4月1日付で改正割賦販売法が施行されることに伴い、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」、「コード決済事業者等」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。 クレジットカード・セキュリティガイドラインは、同法で求められるセキュリティ対策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を満たしていると認められます。	2021年4月1日
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。 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
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
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。	罰則規定はありません。 しかしながら、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。	2020年3月27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。 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。 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	全体	クレジットカード・セキュリティガイドライン【1.0版】から【2.0版】への改定ポイントは何か。	クレジットカード・セキュリティガイドライン【1.0版】から【2.0版】への改定のポイントは大きく２点あります。 一点目は、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に伴い、「クレジットカード情報保護対策分野」におけるセキュリティ対策の実施主体者として「決済代行業者等」、「コード決済事業者等」が追加され、これら事業者が講ずべきセキュリティ対策がとりまとめられております。 ※本件に関するFAQは、**カード情報保護対策の対象事業者の拡充について FAQ**を参照いただくとともに、併せて、**カード情報保護対策の対象事業者の拡充に伴う「クレジットカード・セキュリティガイドライン」の改定内容の追記について**、**クレジットカード・セキュリティガイドライン 新旧対照表（2021年3月改定、4月適用開始/関連部分のみ抜粋）**を参照ください。 二点目は、「不正利用対策分野のうち、非対面取引におけるクレジットカードの不正利用対策」について、加盟店における具体的方策としてEMV 3-Dセキュアの説明を追記し、これに伴い、カード会社（イシュアー・アクワイアラー）とPSPに求められる対応を追記しております。	2021年4月1日

項番	カテゴリー	質問内容	回答	更新日
9	クレジットカード情報保護対策分野	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。	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。 ※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。	2021年4月1日
10	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。 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。	2020年3月27日
11	クレジットカード情報保護対策分野	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。	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。 ※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。	2021年4月1日
12	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。 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
13	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。 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
14	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

項番	カテゴリー	質問内容	回答	更新日
15	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。 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
16	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。 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
17	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
18	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。	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。	2020年3月27日
19	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、「【追補版】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。	2020年3月27日
20	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。 http://www.jcdsc.org/	2020年3月27日
21	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カードについてはクレジットカード・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。	2020年3月27日
22	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。 電子マネー情報は含みません。	2020年3月27日
23	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

項番	カテゴリー	質問内容	回答	更新日
24	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、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。	2020年3月27日
25	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、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。	2020年3月27日
26	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。	2020年3月27日
27	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。 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。	2020年3月27日
28	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。 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。 以下、JCDSCサイトにてご確認ください。 http://www.jcdsc.org/	2020年3月27日
29	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が保存、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
30	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。 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、コード決済事業者等）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求める。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ます。	2021年4月1日

項番	カテゴリー	質問内容	回答	更新日
31	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)を達成している場合は、PCI DSS準拠は求めていません。 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。	2020年3月27日
32	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）。 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
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紹介することは公正性の観点からいたしかねます。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。	2020年3月27日
35	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、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。	2020年3月27日
36	クレジットカード情報保護対策分野	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。	2020年3月27日
37	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顔、イシュアーの顔がある場合、どこまで対応すべきか。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。	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。	2020年3月27日
38	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

項番	カテゴリー	質問内容	回答	更新日
39	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こと等も重要になります。 特に、EC加盟店においては、「非通過型」の決済システムを導入した場合でも、ECサイトの開発・運用段階でのセキュリティ対策が不十分であることを原因として不正侵入を許し、カード情報の漏えい事案へと繋がっていることが近時の傾向です。自社システムの絶え間ない点検と脆弱性対策に万全を期すことでカード情報漏えいを防止することが重要となります。加えて、コロナ禍の新常態としてEC加盟店での非対面取引が増加傾向にある中、これまで、EC取扱高の伸長に伴い不正利用被害も増加してきたことからも、引き続き実効性のある不正利用防止の取組が求められております。	2021年4月1日
40	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。 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。	2020年3月27日
41	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Java script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。 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 Java Script型：SAQ A-EP 詳しくは以下、JCDSCサイトにてご確認ください。 http://www.jcdsc.org/	2020年3月27日
42	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」とはどのようなものか。また、公表されているものなのか。	当該文書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。	2020年3月27日
43	クレジットカード情報保護対策分野	「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。	2020年3月27日
44	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。 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。 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
45	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。 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

項番	カテゴリー	質問内容	回答	更新日
46	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。 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
47	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） https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices "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。 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。 https://www.pcisecuritystandards.org/assessors_and_solutions/approved_pin_transaction_security_expired 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。 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。	2020年12月16日
48	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） https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions "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。 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
49	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やPOS端末統合セキュリティ要件などが該当します。 具体的な要件は各Versionごとに項番が異なり、添付資料（別紙）PCI PTSのVersion間の要件番号の関係をご参照ください（本FAQ最終ページ）。	2020年12月16日
50	クレジットカード情報保護対策分野	「MO/TO加盟店におけるカード情報保護対策」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。 具体的な要件は各Versionごとに項番が異なり、添付資料（別紙）PCI PTSのVersion間の要件番号の関係をご参照ください（本FAQ最終ページ）。	2020年12月16日

項番	カテゴリー	質問内容	回答	更新日
51	クレジットカード情報保護対策分野	「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。 2022年10月28日でプログラムが終了することがアナウンスされており、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。	2020年12月16日
52	クレジットカード情報保護対策分野	「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） https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications "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。 "REVALIDATION DATE" は、年次で求められる再検証日となります。 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「既存の導入済みのみ認められる（ACCEPTABLE ONLY FOR PRE-EXISTING DEPLOYEMNTS）」の状態となります。また PA-DSS プログラムが終了する 2022年10月28日以降は、全ての既存のPA-DSS認定アプリケーションが「既存の導入済みのみ認められる」の状態になります。 「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。	2020年12月16日
53	クレジットカード情報保護対策分野	「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。 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。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。 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いて、 2022年10月28日以降は、完全に Secure Software Standard に移行する予定であることがアナウンスされています。 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。	2020年12月16日

項番	カテゴリー	質問内容	回答	更新日
54	クレジットカード情報保護対策分野	「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） https://www.pcisecuritystandards.org/assessors_and_solutions/payment_software "PAYMENT SOFTWARE STATUS" 列が Validated であれば、認定状況に問題はありません。 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。 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。	2021年4月1日
55	クレジットカード情報保護対策分野	CA公開鍵(CAPK)についての鍵長等の詳細について教えてほしい。	以下の通りとなっております。ご確認ください。 CAPKは所定の有効期限まで端末側に保有すること。 更新時には、POS端末への追加登録およびデータ削除が必要。 ※各ブランドの代表アクワイアラから、更新鍵が発行される。 ※各ブランド毎に複数個のCAPK登録が必要。 ・「鍵長＝1408bits」「鍵長＝1984bit」の2種類の鍵が端末に納されている必要がある。 　　ただし、銀聯カードが「鍵長＝1152bits」を2021年まで有効とする可能性があるため、ブランドへの確認が必要である。 ・CAPKの追加・削除を可能な実装とする。 ・複数のCAPK登録を可能な実装とする。 ・CAPKの有効期限更新を想定した実装とする。	2020年12月16日
56	クレジットカード情報保護対策分野	EMV仕様のバージョンと対象ブランドについて教えてほしい。	以下の通りとなっております。ご確認ください。 2020年10月現在　EMVCL仕様対象ブランド １EMV Contctless Book A Architecture & Genl Rqmts Version2.9　ALL ２EMV Contctless Book B Entry Point Specification Version2.9　ALL ４EMV Contctless Book C－２ Kernel ２ Spec Version2.9　Mastercard ５EMV Contctless Book C－３ Kernel ３ Spec Version2.9　VISA ６EMV Contctless Book C－４ Kernel ４ Spec Version2.9　American Express ７EMV Contctless Book C－５ Kernel ５ Spec Version2.9　JCB ８EMV Contctless Book C－６ Kernel ６ Spec Version2.9　Diners Club/Discover ９EMV Contctless Book C－７ Kernel ７ Spec Version2.9　UnionPay １０EMV Contctless Book D Contactless Comm Protocol Version2.9　ALL	2020年12月16日

項番	カテゴリー	質問内容	回答	更新日
57	不正利用対策分野 （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。 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
58	不正利用対策分野 （対面取引）	「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」はどのように入手できるのか。	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。	2020年3月27日
59	不正利用対策分野 （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。	原則、IC取引では、ICチップを読み込み、PIN入力による本人確認を行うことが求められます。 ただし、カード会員がPINを失念している場合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）は許容されておりますので、ICチップが搭載されているIC化カードが提示された場合はICチップを読み込んだ上で本人確認をPIN入力に代えてサインにより行うことは可能です。 なお、PIN入力スキップ機能（PINバイパス）は、PINによる本人確認を実施しないことで従来から不正利用が発生する可能性が懸念されているところである。また、クレジット取引セキュリティ対策協議会は、今後、将来的にサインを取得することを加盟店の裁量に委ねることについて具体的に検討を行うこととされており、その結果、我が国市場にこのサイン取得の任意化が適用された場合、本機能の存在意義も失われることになるため、日本クレジット協会及びカード会社（イシュアー・アクワイアラー）は、本機能の廃止に向けて具体的を検討を開始することとしております（項番62参照）。	2021年4月1日
60	不正利用対策分野 （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カード対応となった場合は運用が変わるのか。	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。 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。	2020年3月27日
61	不正利用対策分野 （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。 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。	2020年3月27日

項番	カテゴリー	質問内容	回答	更新日
62	不正利用対策分野 （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。	割賦販売法による不正利用防止措置の義務化とクレジットカード・セキュリティガイドラインに基づくIC化の推進により接触IC取引の実現が進展したことにより、本人確認と言えばPIN入力が一般化しているところ、例えば海外のカード会社が発行したカードが利用される場合や、非接触IC取引においてCVMリミットを超える取引となる場合などにおいては、サインの取得により本人確認を行うこととされており、現状では依然として、本人確認の方法はPIN入力とサインの取得が併存している状況にあり、取引によってはサインの取得により本人確認を行う運用は認められております。 一方で、国際ブランドのルールが変更されたことにより、世界的には既に、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）、サインが従来果たしてきた本人確認としての有効性は低下している状況にあるため、我が国市場においても加盟店によるサインの取得を将来的に任意とすることについて、クレジット取引セキュリティ対策協議会は具体的な検討に着手することとされております。 なお、このサイン取得の任意化の適用にあたっては、我が国市場におけるこれまでの経緯とステークホルダーに与える影響の大きさを考慮し混乱を招くことがないよう、カード会員と加盟店への周知、準備と移行のための十分な期間を設定する予定としております。 本件に関しては、クレジットカード・セキュリティガイドライン【2.0版】に留意事項として記述されておりますので、併せてご参照ください。 「クレジットカード・セキュリティガイドライン【2.0版】」P36 Ⅱ.不正利用対策分野（A）対面取引におけるクレジットカードの不正利用対策における3.その他留意事項（1）本人確認としての有効性の低下に伴う、サイン取得を任意とすること及びPINバイパスの廃止等の検討開始について	2021年4月1日
63	不正利用対策分野 （非対面取引）	クレジットカード・セキュリティガイドラインで示す方策以外で法履行ができる方策を教えて欲しい。	クレジットカード・セキュリティガイドライン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クレジットカード・セキュリティガイドライン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。	2020年3月27日
64	不正利用対策分野 （非対面取引）	EMV 3-Dセキュア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3-Dセキュアとの互換性を教えて欲しい。	EMV 3-Dセキュアの導入時期については、契約アクワイアラーにご確認願います。 メリットはブラウザベース（PC利用）に加え、アプリケーションベースへの対応により、スマートフォンのアプリケーションを利用した取引も対象となることです。また、カード会社（イシュアー）によるリスク評価により不正利用の可能性が低いと判断される取引については、カード会員にパスワード入力を求めない対応も可能となり、利用者のパスワード忘れ等により発生していた「かご落ち」の解消にも資することが期待できることです。 留意点は、3-Dセキュア1.0と互換性は無いため新たなソフトを組み入れる必要があることです。	2021年4月1日

項番	カテゴリー	質問内容	回答	更新日
65	不正利用対策分野 （非対面取引）	「動的（ワンタイム）パスワード」や「デバイス認証（生体認証等）」とは何か。	「動的(ワンタイム)パスワード」 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。 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。 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。 「デバイス認証（生体認証等）」 クレジットカード情報と生体情報をスマートフォン等のデバイスに登録する際に、確実な本人認証が行われていれば、その後の当該デバイスによるクレジットカード利用時において登録された生体情報による認証等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デバイスで行われる（カード会社や加盟店では生体情報を持たない）ことが多いようです。	2021年4月1日
66	不正利用対策分野 （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
67	不正利用対策分野 （非対面取引）	オーソリゼーションの整備と善管注意義務の履行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。	2020年3月27日
68	不正利用対策分野 （非対面取引）	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（３-Ｄ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。	2020年3月27日
69	不正利用対策分野 （非対面取引）	加盟店の不正利用防止対策については、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。	加盟店の取り扱う商材や不正利用の被害発生状況等を踏まえた措置を求めております。 ・全ての非対面加盟店 ①善管注意義務と②オーソリゼーションの導入 ・高リスク商材取扱加盟店 高リスク商材（デジタルコンテンツ（オンラインゲームを含む）、家電、電子マネー、チケット、宿泊予約サービス）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、全ての非対面加盟店が対応するべき対策＋クレジットカード・セキュリティガイドライン上の非対面不正利用対策の１つ以上の方策導入 ・不正顕在化加盟店 不正顕在化加盟店と認定される場合は全ての非対面加盟店が対応するべき対策＋クレジットカード・セキュリティガイドライン上の非対面不正利用対策をの２つ以上の方策導入 ※クレジットカード・セキュリティガイドライン上の非対面不正利用対策：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3ヵ月連続50万円を超えた場合に該当する。	2020年3月27日

項番	カテゴリー	質問内容	回答	更新日
70	不正利用対策分野 （非対面取引）	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５商材とあるが、５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）。	2020年3月27日
71	不正利用対策分野 （非対面取引）	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、クレジットカード・セキュリティガイドライン上の非対面不正利用対策を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。	2020年3月27日
72	不正利用対策分野 （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
73	不正利用対策分野 （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、非対面不正利用対策のうち、２つ以上の方策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。	2020年3月27日
74	不正利用対策分野 （非対面取引）	不正顕在化加盟店としてクレジットカード・セキュリティガイドライン上の方策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。	2つ以上としてカウントされません。クレジットカード・セキュリティガイドライン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。	2020年3月27日
75	不正利用対策分野 （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

（別紙）PCI PTSのVersion間の要件番号の関係

青色（MO/TOにおける決済端末を利用した場合の関連要件） 黄色（オートローディング式カードリーダにおける関連要件）

注）日本語訳は参考です。正確な要件は英文を確認ください。

PTS4.1			PTS5.1			PTS6.0		
A1	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card readerB. Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours' attack time for exploitation.	デバイスは改ざん検出および応答メカニズムを使用して、デバイスを即座に操作不能にし、デバイスに格納されている可能性のある機密データを自動的かつ即時に消去するため、機密データを回復できなくなります。これらのメカニズムは、ドリル、レーザー、化学溶剤、開口部カバー、ケーシング（シーム）の分割、および換気開口部の使用（これらに限定されない）によってデバイスが物理的に侵入するのを防ぎます。メカニズムを無効化または無効化し、PIN開示バグを挿入したり、識別および初期の悪用にデバイスあたり少なくとも26の攻撃の可能性を必要とせずに秘密情報にアクセスしたり、悪用に最低13を使用する実証可能な方法はありません。、ICカードリーダーBを除く。注：前面ケーシングと背面ケーシングの両方の交換は、攻撃シナリオの一部と見なされます。すべての攻撃には、悪用のための最低10時間の攻撃時間が含まれます。	A1	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card readerB. Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario.	デバイスは改ざん検出および応答メカニズムを使用して、デバイスを即座に操作不能にし、デバイスに格納されている可能性のある機密データを自動的かつ即時に消去するため、機密データを回復できなくなります。これらのメカニズムは、ドリル、レーザー、化学溶剤、開口部カバー、ケーシング（継ぎ目）の分割、および換気開口部の使用（これらに限定されません）によってデバイスが物理的に侵入するのを防ぎます。メカニズムを無効化または無効化し、PIN開示バグを挿入したり、秘密情報にアクセスしたりするための実証可能な方法はありません。識別および初期の悪用には少なくともデバイスごとに26、潜在的には悪用には13の攻撃の可能性はありません。、ICカードリーダーBを除く。注：前面と背面の両方のケーシングの交換は、攻撃シナリオの一部と見なされます。	A1	The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings.	デバイスは改ざん検出および応答メカニズムを使用して、デバイスを即座に操作不能にし、デバイスに格納されている可能性のある機密データを自動的かつ即時に消去するため、機密データを回復できなくなります。これらのメカニズムは、ドリル、レーザー、化学溶剤、開口部カバー、ケーシング（シーム）の分割、および換気開口部の使用（これらに限定されません）によってデバイスが物理的に侵入するのを防ぎます。
						A2	There is no demonstrable way to disable or defeat the tamper mechanism/s and insert a sensitive key-press-disclosing bug. Keypads used for PIN entry require an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, as defined in Appendix B. Keypads used for manual PAN entry, but not PIN entry—e.g., a non-PED—require an attack potential of at least 16 per device for identification, with a minimum of 8 points for exploitation.	タンパーメカニズムを無効または無効にし、重要なキープレス開示バグを挿入する実証可能な方法はありません。 PIN入力に使用されるキーパッドは、識別と初期の悪用にデバイスあたり少なくとも26の攻撃能力が必要です。悪用には最低13が必要です（付録Bで定義されているICカードリーダーを除く）。 PINエントリではなく手動PANエントリに使用されるキーパッド（非PEDなど）は、識別のためにデバイスごとに少なくとも16の攻撃の可能性が必要であり、悪用には最低8ポイント必要です。
A2	Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.	単一のセキュリティメカニズムに障害が発生しても、デバイスのセキュリティは損なわれません。脅威に対する保護は、少なくとも2つの独立したセキュリティメカニズムの組み合わせに基づいています。			該当要件なし			該当要件なし
D2	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	ICカードを挿入するための開口部は、カード挿入時にカード所有者が完全に見えるようになっているため、開口部にある邪魔な障害物や疑わしい物体を検出できます。	D2	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	ICカードを挿入するための開口部は、カード挿入時にカード所有者が完全に見えるようになっているため、開口部にある邪魔な障害物や疑わしい物体を検出できます。	A14	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable. The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	ICカードを挿入するための開口部は、カード挿入時にカード所有者が完全に見えるようになっているため、開口部にある邪魔な障害物や疑わしい物体を検出できます。 ICCリーダーは、ICリーダーのスロットからレコーダーまたはトランスミッター（外部のバグ）までの配線をカード所有者が観察できるように構成されています。
D3	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	ICCリーダーは、ICリーダーのスロットからレコーダーまたはトランスミッター（外部のバグ）までの配線をカード所有者が観察できるように構成されています。	D3	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	ICCリーダーは、ICリーダーのスロットからレコーダーまたはトランスミッター（外部のバグ）までの配線をカード所有者が観察できるように構成されています。			
E3.2	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).	PIN入力POI端末には、支払いカードを保持して盗むことを目的とした攻撃（レバノンループ攻撃など）を防ぐためのメカニズムが装備されています。	E3.2	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).	PIN入力POI端末には、支払いカードを保持して盗むことを目的とした攻撃（レバノンループ攻撃など）を防ぐためのメカニズムが装備されています。	C2.2	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).	PIN入力POI端末には、支払いカードを保持して盗むことを目的とした攻撃（レバノンループ攻撃など）を防ぐためのメカニズムが装備されています。
B1	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.	デバイスはセルフテストを実行します。これには、起動時の整合性テストと信頼性テストが含まれ、少なくとも1日に1回はデバイスが危険な状態にあるかどうかを確認します。障害が発生した場合、デバイスとその機能は安全に機能しなくなります。デバイスは少なくとも24時間ごとにメモリを再初期化する必要があります。	B1	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.	デバイスはセルフテストを実行します。これには、起動時の整合性テストと信頼性テストが含まれ、少なくとも1日に1回はデバイスが危険な状態にあるかどうかを確認します。障害が発生した場合、デバイスとその機能は安全に機能しなくなります。デバイスは少なくとも24時間ごとにメモリを再初期化する必要があります。	B1	The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.	デバイスはセルフテストを実行します。これには、起動時の整合性テストと信頼性テストが含まれ、少なくとも1日に1回はデバイスが危険な状態にあるかどうかを確認します。障害が発生した場合、デバイスとその機能は安全に機能しなくなります。デバイスは少なくとも24時間ごとにメモリを再初期化する必要があります。
B2	The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting the clear-text PIN or other sensitive data.	デバイスの機能は、予期しないコマンドシーケンス、不明なコマンド、間違ったデバイスモードでのコマンド、誤ったパラメーターまたはデータの提供など、デバイスにクリアテキストのPINまたは その他の機密データ。	B12	The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting the clear-text PIN or other sensitive data.	デバイスの機能は、予期しないコマンドシーケンス、不明なコマンド、間違ったデバイスモードでのコマンド、誤ったパラメーターまたはデータの提供など、デバイスにクリアテキストのPINまたは その他の機密データ。	D2	The device's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode, and supplying wrong parameters or data, which could result in the device outputting the clear-text PIN or other sensitive data.	デバイスの機能は、予期しないコマンドシーケンス、不明なコマンド、誤ったデバイスモードでのコマンド、誤ったパラメーターまたはデータの提供などの論理的異常の影響を受けてはならず、デバイスがクリアテキストを出力する可能性があります。PINまたはその他の機密データ。
B16	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.	非PINデータ入力のすべてのプロンプトは、デバイスの暗号化ユニットの制御下にあります。プロンプトが暗号化ユニット内に保存されている場合、ユニットの暗号化キーを消去せずにプロンプトを変更することはできません。プロンプトが暗号化ユニットの外部に格納されている場合は、プロンプトの信頼性と適切な使用を保証し、プロンプトの変更やプロンプトの不適切な使用を防ぐための暗号化メカニズムが存在している必要があります。	B16	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.	非PINデータ入力のすべてのプロンプトは、デバイスの暗号化ユニットの制御下にあります。プロンプトが暗号化ユニット内に保存されている場合、ユニットの暗号化キーを消去せずにプロンプトを変更することはできません。プロンプトが暗号化ユニットの外部に格納されている場合は、プロンプトの信頼性と適切な使用を保証し、プロンプトの変更やプロンプトの不適切な使用を防ぐための暗号化メカニズムが存在している必要があります。	B15	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.	非PINデータ入力のすべてのプロンプトは、デバイスの暗号化ユニットの制御下にあります。プロンプトが暗号化ユニット内に保存されている場合、ユニットの暗号化キーを消去せずにプロンプトを変更することはできません。プロンプトが暗号化ユニットの外部に格納されている場合は、プロンプトの信頼性と適切な使用を保証し、プロンプトの変更やプロンプトの不適切な使用を防ぐための暗号化メカニズムが存在している必要があります。