ECサイトのセキュリティ対策実施状況申告書（例）
【附属文書20_別紙c】に関するＦＡＱ

2026年　3月

クレジット取引セキュリティ対策協議会

ECサイトのセキュリティ対策実施状況申告書（例）【附属文書20_別紙c】に関するFAQ

（注）本FAQは申告書（例）の記載意図を補足するものであり、個別案件の適合性判断や免責を示すものではありません。

No	申告書（例）での該当箇所	質問	回答
1	全体	不正利用が顕在化していない場合（被害が発生していない場合）でも、各対策の実施・申告は必要か。	不正利用被害の有無に関わらず、指針対策の導入状況調査として、各対策の実施および申告書の提出が必要となります。
2	全体	カード情報を保持していないが、対策が必要か。	カード情報の非保持化を実現しているEC加盟店についても、各対策が必要になります。
3	全体	ECサイトで使用できる決済方法は、国際ブランドがついていないハウスカードのみであるが、本申告書の提出は必要か。	セキュリティガイドラインでは、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。提出の要否等につきましては、契約先のカード会社またはPSPにご確認下さい。 なお、国際ブランドがついていないクレジットカードの考え方については、セキュリティガイドラインのFAQの項番7もご参照下さい。
4	全体	決済代行事業者（PSP）が提供する決済システムを利用しているため、対策状況についてはPSPが申告すべきではないか。	本申告書（例）にて申告いただく対策は、自社ECサイトの脆弱性対策、ならびにログイン機能や会員管理機能、商品表示ページ、申込画面等を含むECサイト全体を対象としたセキュリティ対策であり、対策状況については加盟店が自ら状況を把握し、申告する必要があります。 PSPが実施・把握しているセキュリティ対策の範囲は、ご契約内容等によって異なりますが、主に決済処理や決済システム部分のセキュリティ対策であると考えられます。
5	全体	なぜ申告書（例）に記載の対策を行う必要があるのか。	申告書（例）に記載の対策は、「セキュリティガイドライン」で求められているセキュリティ対策です。 割賦販売法では、加盟店に対してセキュリティ対策を講じることが義務付けられており、セキュリティガイドラインに掲げる措置を適切に講じることで、同法に規定する「必要かつ適切な措置」が講じられると見なされます。 詳細は、セキュリティガイドラインのFAQの項番2をご参照下さい。
6	全体	対策が完了しない場合に罰則はあるか。	セキュリティガイドラインのFAQの項番5では、割賦販売法上の罰則の考え方を記載しておりますので、ご参照下さい。 なお、加盟店契約上の措置につきましては、ご契約のカード会社またはPSPにご確認下さい。
7	全体	専門用語が多く、求められている対策の理解が難しい。また、自社ECサイトのセキュリティ対策状況が把握できておらず、どのように確認すればよいか。	附属文書20の本紙、別紙a、別紙bの各文書に求められている対策の説明が記載されているので参考にしてください。自社ECサイトの対策状況は、社内のシステム担当者やECサイトを構築・管理しているシステム会社等にご確認下さい。
8	【1】導入が必要な対策の確認 （1）販売方法確認	メールリンク方式での決済とはどのような決済か。	購入者に決済用のリンクを送信し、そのリンク先で支払いを完了する方式を指します。リンクの送信手段としては、一般的に以下の方法があります。 ・電子メールやSMSにて決済ページのURLを送信する。 ・メールや請求書等にQRコードを掲載し、顧客が読み取りする。
9	【1】導入が必要な対策の確認 （1）販売方法確認	メールリンク決済を導入しており、Webサイト（HP）上でのEC決済は導入していないが、「ECサイト（加盟店HPを含む）上に、金額が提示された商品・サービスの掲載」をしている場合になぜセキュリティ対策は必要なのか。また、申告書の提出が必要なのか。	加盟店のWebサイト上に金額が提示された商品・サービスの掲載がある場合、偽の決済ページへ誘導される事案や、EC加盟店のサーバ内に不正な決済機能が設置される事案が確認されていることから、対策を講じる必要があり、申告書の提出も必要です。 なお、自社のWebサイト等において、金額が記載された商品掲載がない場合には、【2】（1）脆弱性対策、（2）不正ログイン対策は導入の「対象外」となりますが、こうした場合においても、Webサイトが不正侵入や改ざんを受けた際には、フィッシングメールの送信元、または誘導先として悪用されたり、利用者を偽のリンク先へ誘導するリスクが存在するため、適切な対策が必要となることにご留意下さい。

No	申告書（例）での該当箇所	質問	回答
10	【1】導入が必要な対策の確認 （1）販売方法確認	継続課金のカード登録を加盟店サイト上で行っているが、本項目は選択可能か。	カード登録を加盟店サイト上で行っている場合は、本項目は選択できません。セキュリティガイドラインFAQの項番6で記載のように、初回決済を店頭の決済端末にて行っている場合は、「対面取引」と整理されるため、本申告書における「脆弱性対策」及び不正ログイン対策の確認の対象外となります。
11	【1】導入が必要な対策の確認 （1）販売方法確認	（1）販売方法確認　③の「カード情報を別のID番号またはQRコード情報等と結び付けて、当該決済用情報で決済を行う販売方法を提供する形態である」という項目について、QRコード決済等を販売方法として導入している加盟店は各対策の導入の対象外ということか。	本項目はQRコード決済等を販売方法として導入しているEC加盟店を対象とするものではなく、QRコード決済事業者等（割賦販売法第35条の16第1項第5号に該当する事業者）を対象とした確認項目です。「EC加盟店」は、QRコード決済等の導入有無に関わらず、本申告書における各対策の導入の対象となります。 なお、QRコード決済事業者等については、セキュリティガイドラインにおいて5号事業者のカード情報保護対策の指針対策としてのPCI DSS準拠に加え、キャッシュレス推進協議会が取りまとめたコード決済ガイドライン等の準拠等、他のセキュリティ対策が求められているため、本申告書（例）においては、脆弱性対策・不正ログイン対策の導入の確認を「対象外」としております。なお、PCI DSS準拠状況およびコード決済ガイドライン等に基づく準拠内容について、アクワイアラー・PSPから確認を求められる場合があることにご留意下さい。
12	【2】各対策の導入要否と実施状況報告	各対策について代替策は認められるか。また、代替策の妥当性の判断はどう行うか。	代替策が認められるケースもあると想定しますが、代替策の妥当性の判断は原則、提出先のカード会社、PSPが行います。 また、記載いただいている代替策が、各対策と同等程度であることの根拠の説明を求められる可能性がある点にご留意ください。 なお、ご参考までに、各対策の代替策については、以下の観点でご記載下さい。 （1）脆弱性対策：附属文書20_別紙aの「セキュリティ対策一覧」の1.脆弱性対策を参考に、①～⑤の全ての観点で対策が導入されていることが必要です。なお、代替策については、どの対策の代替であるかを具体的に記載する必要があることにご留意下さい。 （2）不正ログイン対策：①～⑧のいずれかの対策に加え、附属文書20に記載のない対策についても同等以上の対策であれば代替策となり得ます。 （3）EMV 3-Dセキュア：代替策については、「EMV 3-Dセキュア導入ガイド【附属文書14】に関するFAQ」の2. その他に関するFAQのNo.1をご参照下さい。
13	【2】各対策の導入要否と実施状況報告	WAF（Web Application Firewall）を導入しているが、代替策として有効か。	WAFの導入により脆弱性対策・不正ログイン対策の一部の代替策となることは考えられますが、代替策として有効と判断できるかは、各加盟店のシステムやリスクによって異なります。ご契約先のカード会社またはPSPにご確認下さい。
14	【2】各対策の導入要否と実施状況報告	レンタルサーバーを利用しており、サーバー側の仕様により一部のセキュリティ対策（例：ウイルス対策ソフトの導入など）が実施できないが、どうすればよいか。	レンタルサーバーを利用している場合にも各対策は必要です。レンタルサーバー事業者との契約内容や仕様を確認し、ウイルス対策の有無やセキュリティ機能の詳細を確認の上、申告下さい。