附属文書20　別紙a

EC加盟店におけるセキュリティ対策一覧 1.1版

目次

０．本書の見方
１．脆弱性対策
２．EMV 3-Dセキュア
３．不正ログイン対策（決済前の対策）
４．決済時・決済後の対策

クレジット取引セキュリティ対策協議会

2026年3月

0．本書の見方

本書の目的

「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】（以下、「導入ガイド【附属文書20】」という。）」は、セキュリティガイドライン記載の指針対策に基づく、EC加盟店におけるカード情報漏えいや不正利用を防止するために、セキュリティ対策の理解を深めるとともに、適切なセキュリティ対策を実施することができるように、EC加盟店で発生している足元の情報漏えいや不正利用の原因、不正手口等の分析に基づく必要な取組を具体的に示すものである。本書「EC加盟店におけるセキュリティ対策一覧」は、「導入ガイド【附属文書20】」記載の手口とその対策を「クレジットカード・セキュリティガイドライン（以下、「セキュリティガイドライン」という。）」6.0版から追加された指針対策別に一覧化したものであり、EC加盟店における対策選定・導入をサポートすることを目的とする。

（1）脆弱性対策

指針対策　　EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施

導入対策　　「１．脆弱性対策」の「導入対策」（g列）の表記に基づき導入

「導入対策」(g列)表記	導入条件
○	導入必須
両方またはいずれか必須	システム都合等、両方の対策導入ができない場合のみ、いずれかの対策を導入
いずれか必須	いずれかの対策の導入必須

（2）EMV 3-Dセキュア

指針対策　　EMV 3-Dセキュアの導入

導入対策　　クレジットカード決済時の対策である「EMV 3-Dセキュアの導入」。導入及び導入後の運用にあたっては、「EMV 3-Dセキュア導入ガイド【附属文書14】」を参照

（3）不正ログイン対策（決済前の対策）

指針対策　　適切な不正ログイン対策の実施

導入対策　　「３．不正ログイン対策（決済前の対策）」記載の対策より適切な対策を1つ以上導入

不正ログインとは、利用者が属性情報やクレジットカード番号等を登録して、アカウント（ID）とパスワードを作成し、EC加盟店のWebサイトにログインした上で商品購入の申込みとクレジットカード決済を行う「会員登録型」のスキームを不正利用するもので、対策の導入にあたっては、利用者の登録・利用状況や取扱商品、スキーム等を勘案し、不正利用の発生の可能性や被害状況等に応じた適切な対策を導入

不正手口	主な不正内容	対策が必要な場面
不正アカウント作成	窃取した属性情報・カード情報等を利用し、EC加盟店において不正なアカウントの登録を行う	会員登録（g列）
アカウント乗っ取り	窃取した正規のアカウント等のログイン情報等を使用し、EC加盟店への不正ログインを行う	会員ログイン（ｈ列）、属性情報変更（i列）

①適切な対策を1つ以上導入：上記の手口により不正が行われることから、「会員登録」「会員ログイン」「属性情報変更」のそれぞれの場面毎に有効な対策を1つ以上の導入を推奨

②推奨対策：不正手口への効果的な対策の導入の観点から、「３．不正ログイン対策（決済前の対策）」記載の「推奨対策」（l列）を優先的に導入することが望ましい

③②の推奨対策以外の対策を導入する場合は、「３．不正ログイン対策（決済前の対策）」記載の対策より、適切な対策を選定・導入も可能

④「会員登録」及び「属性情報変更」にてクレジットカード番号の登録・変更を行う場合には、EMV 3-Dセキュアによる認証、又は「４．決済時・決済後の対策」の「決済時」（j列）の対策を講じることが必要

（4）不正顕在化加盟店

指針対策　　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等に応じて、セキュリティガイドラインが掲げる不正利用対策から適切な対策を追加導入

導入対策　　不正顕在化加盟店は、すでに不正が発生していることから、不正利用の被害状況を把握し、取扱商品やスキーム等によって異なる不正利用の手口に応じて「不正手口別有効対策」（「３．不正ログイン対策（決済前の対策）」は（q、r列）、「４．決済時・決済後の対策」は（p、q、r列））より適切な対策を追加導入

１．脆弱性対策

対策導入必須

b	c	d	e	f	g	h	i	j
No.	対策分類	対策項目		説明	導入対策	附属文書20 掲載頁	附属文書20_ 補足資料 掲載頁	附属文書20_ 申告書(例) 項番
1	①システム管理画面のアクセス制限と管理者のID/パスワード管理	システム管理画面のアクセス制限と管理者のID/パスワード管理	IPアドレス制限もしくはベーシック制限	管理画面にアクセス可能なIPアドレスを制限する。IPアドレスを制限できない場合は、管理画面にアクセスするためにベーシック認証を設ける。	両方またはいずれか必須	5,6	13,14	(1) ①
2			推測困難なログインURL及びID/パスワードの設定とadminフォルダ削除	管理画面の URL 及びユーザーID/パスワードが admin など推測されやすいものになっていないことを確認する。変更後にadminフォルダが残存していないことも必ず確認する。			14	
3			2段階認証	取得されたアカウントを不正使用されないよう2段階認証または多要素認証（2要素認証）を採用する。	いずれか必須		13	
4			多要素認証（2要素認証）					
5			ログイン試行回数の制限(10回)	アカウントロック機能を有効にし 、10回以下のログイン失敗でアカウントをロックする。	○			
6	②データディレクトリの露見に伴う設定不備への対策	サイト設定の不備対策	特定ディレクトリの非公開	顧客データや決済データ、アクセスログなどの、加盟店において重要なファイルが配置されたディレクトリを非公開にする。 公開ディレクトリには、重要なファイルを配置しない。	○	6	15,16	(1) ②
7			アップロード可能な拡張子・ファイルの制限	Webサーバやwebアプリケーションにより、アップロード可能な拡張子やファイルを制限する等の設定を行う。	○			
8	③Webアプリケーションの脆弱性対策	脆弱性の確認	脆弱性診断	ECサイトにある諸リスクの所在を明らかにするために実施する。脆弱性診断を実施することにより、ECサイトにおける各リスクの所在を特定することができ、特定したリスクを修正することにより、ECサイトの機微なデータを外部に晒されるリスクの顕在化を回避することが期待できる。 ※ （参考）詳しくは、下記 IPA：独立行政法人情報処理推進機構も併せて参照。 https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html	いずれか必須	6	17,18	(1) ③
9			ペネトレーションテスト	悪意のある攻撃者が意図する特定の攻撃を想定し、それが成功するか否かを検証するもの。特定の脆弱性や問題点を発見することに主眼（高リスク資産を念頭に部分に特化、“専門性”を重視）が置かれる。				
10		SQLインジェクション・クロスサイト・スクリプティング対策	最新プラグインの使用/ソフトウェアのバージョンアップ	最新のプラグインの使用（既知の脆弱性が無いものが望ましい）やソフトウェアのバージョンアップを行う。（バージョンアップには必要なセキュリティパッチの適用を含む。）	○	6,7	19,20, 21,22	
11			ソースコードレビューによるセキュアコーディング有無の確認	Webアプリケーションを開発またはカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際には、入力フォームの入力値のチェックも行う。	○			
12	④マルウェア対策としてのウィルス対策ソフトの導入、運用	マルウェア対策	ウイルス対策ソフト導入と定期的な更新・フルスキャン	サーバー、業務端末にウイルス対策ソフト※を導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。 ※ウイルスを検出・削除し、ウイルスに感染するのを未然に防ぐためのソフトウェア。ワクチンソフトと同義語。ウイルス対策ソフトウェア会社から市販されている。パソコンにプレインストールされているものもあるが、その場合は3ヶ月等の有効期限があるため、継続して使用するには更新手続が必要。	○	7,8	23	(1) ④
13	⑤悪質な有効性確認、クレジットマスターへの対策	悪質な有効性確認、クレジットマスター対策	不審なIPアドレスからのアクセス制限	「不審な IP アドレスからのアクセス制限」を行う。特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。	いずれか必須	8,9	24	(1) ⑤
14			有効なカード会員データの漏えい対策	同一アカウントからの入力制限を行う。				
15				オーソリ拒否時に、エラー内容が分からないようにエラー内容を非表示にする。				
16			本人認証	EMV 3-Dセキュアや SMS 通知など本人認証ができる対策を行う。				
17			有効性確認の回数制限	有効性確認の回数制限を設けるなどの対策を行う。				

2．EMV 3-Dセキュア

b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
					決済前			決済時	決済後	対策導入必須					不正手口別有効対策	
No.	対策分類	対策項目		説明	会員登録*1	会員ログイン	属性情報変更	決済時（カード登録・変更含む）*1	決済終了後	導入対策	補足	附属文書20掲載頁	附属文書20_補足資料 掲載頁	附属文書20_申告書(例) 項番	クレジットマスターによる悪質な有効性確認	真正なカード会員データによる「なりすまし」
1	本人認証/認証強化	EMV 3-Dセキュア		現行イシュアー側の本人認証をし得る手段の一つであり、カード会社側でRBA（リスクベース認証）判定を行うことで不正リスクを低減できる。	対象外	対象外	対象外	○	対象外	○	原則、導入必須	8,10,14,18,19	24,32	(3)	○	○

3．不正ログイン対策（決済前の対策）*

b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
					決済前(1つ以上導入)			決済時	決済後	○：推奨対策（優先的に導入検討）					不正手口別有効対策	
No.	対策分類	対策項目		説明	会員登録*1	会員ログイン	属性情報変更	決済時（カード登録・変更含む）*1	決済終了後		補足	附属文書20掲載頁	附属文書20_補足資料 掲載頁	附属文書20_申告書(例) 項番	不正アカウント作成	アカウント乗っ取り
1	アクセス制限	不審なIPアドレスからのアクセス制限		・同一IPアドレスからの連続アクセスやモニタリングで検知した不審なIPアドレスの遮断などを行う。 ・海外からの攻撃も非常に多く「不審な IP アドレスからのアクセス制限」を行う。 ・WAFを導入した上で、不審なIPアドレスからのアクセス制限を行う。 ・WAFやファイアウォールなどアプリケーションの手前で遮断が可能。 ・加盟店によっては、海外との取引をされていない場合もあり、海外のグローバルIPからアクセスされない設定にしておく事で大半の不正アクセスの回避が可能だと考えられる。	○	○	○	○	対象外	○		8,9,10,11,12,13,15	24,29,30,31	(2) ①	○	○
2		スロットリング		同一IPアドレスからの一定時間内に受信可能なリクエスト数を制限し、上回るリクエストがなされた際には受信を拒否しエラーコードを返却すること。時間経過により再び受信可能となる仕組み。（＝リクエストの数を制限するプロセス） 攻撃者は、クレジットマスター/有効性確認を行う際に、攻撃プログラムを組んで機械的に真正チェックを行うため、本対策が有効と考えられる。	○	○	対象外	○	対象外	○	同一のIPアドレスやデバイスからのアクセス制限と定義	9,11,12,15	30	(2) ④	○	○
3		同一アカウントのログイン試行回数の制限強化		同一アカウントからの一定回数を超えるログイン試行があった場合にアカウントロックすることで制限を行う。10回以下で制限を行い、また、同一アカウントのロックアウトの時間は最低30分、本人認証ができるまでは使用できないようにする。	対象外	○	対象外	対象外	対象外	○		12	30	(2) ④		○
4	Bot対策	CAPTCHA認証/reCAPTCHA認証		「画像認証」と呼ばれる認証技術の一種で、人が画像を目で見て確認し、そこに描かれている文字列を読み取って入力することでコンピューターを操作しているのが人間なのかBotなのかを判定する。画像を正しく選択しなければログインすることができない。	○	○	対象外	○	対象外			9,11,12,15	-		○	○
5		その他有効なBot対策ツールの導入		上記以外の有効なBot対策ツールを導入してBot攻撃を防ぐ。	○	○	対象外	○	対象外			-	-		○	○
6	本人認証/認証強化	eKYC		スマホやPCを使用して、オンライン上で免許証などの本人確認書類の提示を求め、オンライン上で身元確認を完結できる仕組み。	○	対象外	対象外	対象外	対象外			11	-		○	
7		デバイスフィンガープリント		アクセス元のデバイスを特定するためにウェブブラウザを通して情報を収集するプロセス。デバイス情報は主に、タイムスタンプ、IPアドレス、画面解像度、インストール済みプラグインの情報などがある。ここでは上記に加えてCookieやHTTPヘッダーの情報を使って同一デバイスの特定をする仕組みとしている。	○	○	○	○	対象外	○	不正検知サービスによっては会員登録時でも不正なデバイスとして特定可能なケースもある	9,11,12,13,15	30,31	(2) ⑦	○	○
8		単純パスワード、短いパスワードの排除		以下のパスワード要件が求められる。 ・12文字以上（またはシステムが12文字に対応していない場合は、8文字以上）であること。 ・数字とアルファベットの両方が含まれていること。	対象外	○	対象外	対象外	対象外			12	-			○
9		多要素認証（2要素認証）	FIDO2/パスキーによる認証	認証の3要素である「知識情報」「所持情報」「生体情報」のうち、2つ以上を組み合わせて認証することを指す。 単一の認証要素が不正利用されてもログインを防ぐことが可能となる。 FIDO2/パスキーは、FIDOアライアンスによって策定された、パスワードに依存しない安全な認証を実現するための業界標準であり、公開鍵暗号方式を用いた認証を採用している。ユーザーの端末に保存された秘密鍵と、サービス側に登録された公開鍵を用いて認証を行う。通常、所持要素と生体要素（指紋認証等）で構成されており、本書では多要素認証の1つとして位置付ける。パスキーの構成によって単一要素（所持要素）のみとなる場合については、知識要素等との組み合わせを推奨する。	対象外	○	○	○	対象外	○		6,9,12,13,15	13	(2) ②		○
10		2段階認証		登録の携帯電話番号へのSMS（ショートメッセージ）やE-mailを送信し、そこに記載された一時的な確認コードをWeb上で入力することで認証する仕組みなど。 （例）異なるデバイスからのログイン時にSMS OTPを求めるなど） 攻撃者は、クレジットマスター/有効性確認を行う際に、攻撃プログラムを組んで機械的に真正チェックを行うため、本対策が有効と考えられる。対策は、EC加盟店またはPSPで実施する仕様が想定される。*2	対象外	○	○	○	対象外	○		6,9,11,12,13,15	13,29,30,31	(2) ②		○
11		SMS認証/電話番号認証		多要素認証の所有要素の本人認証を正しく行うために、ユーザーの携帯電話番号にSMS（ショートメッセージ）を送信し、そこに記載された一時的な確認コードをWeb上で入力することで認証する仕組み。 通話機能を利用した電話番号認証も同義。	対象外	○	○	○	対象外			9,12,13,15	-			○
12		（会員ログイン時/属性情報変更時の）メールやSMS通知		IDはメールアドレスであることが多く、また静的パスワードは推測されやすい為、「なりすまし」による、不正ログインを実行されても、会員本人及びEC加盟店は気づきにくいことから、不正ログインをされた場合でも、会員本人に気づきを与えられるように、ログイン時にメールやSMSで通知する。*2	対象外	○	○	対象外	対象外	○		12,13	30	(2) ⑤		○
13		姓カナ、名カナ入力値の検証		・会員登録時の個人情報（氏名・住所・電話番号・メールアドレス等）が不自然な表記ではないか、また不自然な組み合わせではないかを確認する。 ・攻撃者が海外である場合には、漢字やカナなどの入力されている個人情報が間違っている場合が多い。	○	○	対象外	対象外	対象外	○		10,11,13	29,31,33	(2) ③	○	○
14		デバイス認証		端末（デバイス）固有の識別情報を用いて認証を行うことにより、アクセスコントロールを行うための仕組み。 端末の持ち主となるユーザーが「だれ」であるかという認証ではなく、「どの」端末であるかという、端末そのものを認証する。	対象外	○	○	対象外	対象外			13,18	-			○
15		生体認証		スマホアプリでのサービス提供の場合はOS標準の生体認証を利用可能である。ただし、アプリを提供している事業者に限定される。	対象外	○	○	○	対象外			9,13,15	-			○
16	不正検知	属性・行動分析		ECサイトで商品・サービスが注文された際に、過去の注文情報やIPアドレスなどから注文情報を確認し、不正利用かどうか判定する仕組みであり、予めシステムがクレジットカード利用者の購入履歴や住所、名前、購入商品などの個人情報を収集し、それらの収集したデータを元に消費者の傾向を分析し、不正の判定をするもの。	○	○	○	○	○	○	附属文書19「属性・行動分析ガイダンス」に準拠	9,11,12,13,14,15,16,17,18,19	29,31,32,33	(2) ⑥	○	○

＊ ・クレジットカード決済前の各場面において有効な不正ログイン対策を○印で示している。対策項目によっては「決済時」「決済後」においても有効だが、一覧表内、横の列で○がついている全ての場面で実施しなければならないものではない。
・EC加盟店等へのサイバー攻撃等による不正アクセスやEC加盟店・カード会社等を模したフィッシングサイトにより窃取したクレジットカード情報や会員属性情報、アカウント（ID）・パスワード等を利用して不正にログインし、不正利用されることがある。このような不正に対する対策を総じて不正ログイン対策とする。
・不正ログインの手口として、「不正アカウント作成」「アカウント乗っ取り」が想定される。
・ゲスト購入のみでログイン機能がない加盟店については、4．決済時・決済後の対策 の「決済時」に有効な対策を講じる。
＊1 ・「会員登録」はクレジットカード情報の登録を伴わず、ユーザアカウント情報の登録のみを指す。カードの有効性確認としてオーソリゼーションを通じてカード登録を行うケースについては、4．決済時・決済後の対策 の「決済時」に有効な対策（○印の対策）を講じる。
＊2 ・利用者のフィルター設定でSMS未達のケースがある。
・メールアドレスや携帯番号（SMS）を第3者により勝手に変更されない仕組みが必要
・不正ログイン後、任意のメールアドレスや携帯番号に不正変更されることを防ぐため、変更するための認証コードをメールアドレス変更時には登録済みメールアドレスに、携帯番号変更時は登録済み携帯番号にSMS送信する等の変更時の追加認証が必要

4．決済時・決済後の対策 *

b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
No.	対策分類	対策項目		説明	決済前			決済時	決済後	推奨対策	補足	附属文書20 掲載頁	附属文書20_補足資料 掲載頁	不正手口別有効対策			(参考) ゲスト購入型有効対策	(参考) MO･TO取引有効対策
					会員登録*1	会員ログイン	属性情報変更	決済時 (カード登録・変更含む)*1	決済終了後					クレジットマスターによる悪質な有効性確認	真正なカード会員データによる「なりすまし」	商品等転売		
1	アクセス制限	不審なIPアドレスからのアクセス制限		・同一IPアドレスからの連続アクセスやモニタリングで検知した不審なIPアドレスの遮断などを行う。 ・海外からの攻撃も非常に多く「不審な IP アドレスからのアクセス制限」を行う。 ・WAFを導入した上で、不審なIPアドレスからのアクセス制限を行う。 ・WAFやファイアウォールなどアプリケーションの手前で遮断が可能。 ・加盟店によっては、海外との取引をされていない場合もあり、海外のグローバルIPからアクセスされない設定にしておく事で大半の不正アクセスの回避が可能だと考えられる。	○	○	○	○	対象外			8,9,10, 11,13,15	24,29, 30,31	○	○		○	
2		スロットリング		同一IPアドレスからの一定時間内に受信可能なリクエスト数を制限し、上回るリクエストがなされた際には受信を拒否しエラーコードを返却すること。時間経過により再び受信可能となる仕組み。（＝リクエストの数を制限するプロセス） 攻撃者は、クレジットマスター/有効性確認を行う際に、攻撃プログラムを組んで機械的に真正チェックを行うため、本対策が有効と考えられる。	○	○	対象外	○	対象外		同一のIPアドレスやデバイスからのアクセス制限と定義	9,11, 12,15	30	○	○		○	
3	Bot対策	CAPTCHA認証/reCAPTCHA認証		「画像認証」と呼ばれる認証技術の一種で、人が画像を目で見て確認し、そこに描かれている文字列を読み取って入力することでコンピューターを操作しているのが人間なのかBotなのかを判定する。画像を正しく選択しなければログインすることができない。	○	○	対象外	○	対象外			9,11, 12,15	-	○	○		○	
4		その他有効なBot対策ツールの導入		上記以外の有効なBot対策ツールを導入してBot攻撃を防ぐ。	○	○	対象外	○	対象外			-	-	○	○		○	
5	エラー表示制限	オーソリ拒否時に、エラー内容が分からないようにエラー内容を非表示にする（リーズンコードの表示方法）		カード番号/有効期限/セキュリティコードのどの項目がエラーであったか分からなくする。 EC加盟店がエラー理由を一般消費者に対して表示する際に、どの項目がエラーなのか、分からないようにする事で、攻撃者にとって有効性確認の効率が悪くなる為、狙われにくくなる可能性が考えられる。	対象外	対象外	対象外	○	対象外			8,9,15	24	○	○		○	
6	機能制限	同一アカウントからの入力制限		アカウントに紐付けられたクレジットカード番号の登録・変更のリトライ回数に制限を設けることで、不正なカード有効性の確認を防ぐ。 具体的には、一定時間内、同一日内などでリトライ回数を制限する。	対象外	対象外	対象外	○	対象外			8,9, 12,15	24	○				
7				同一クレジットカード番号での複数アカウント保有を許容しない。	対象外	対象外	対象外	○	対象外			8,9, 12,15	24	○				
8				同一アカウントへのクレジットカードの登録数を制限する。	対象外	対象外	対象外	○	対象外			8,9, 12,15	24	○				
9	本人認証/認証強化	デバイスフィンガープリント		アクセス元のデバイスを特定するためにWebブラウザを通して情報を収集するプロセス。デバイス情報は主に、タイムスタンプ、IPアドレス、画面解像度、インストール済みプラグインの情報などがある。ここでは上記に加えてCookieやHTTPヘッダーの情報を使って同一デバイスの特定をする仕組みとしている。	○	○	○	○	対象外		不正検知サービスによっては会員登録時でも不正なデバイスとして特定可能なケースもある	9,11,12, 13,15	30,31	○				
10		多要素認証（2要素認証）		認証の3要素である「知識情報」「所持情報」「生体情報」のうち、2つ以上を組み合わせて認証することを指す。 単一の認証要素が不正利用されてもログインを防ぐことが可能となる。	対象外	○	○	○	対象外			6,9,12, 13,15	13	○					
			FIDO2/パスキーによる認証	FIDO2/パスキーは、FIDOアライアンスによって策定された、パスワードに依存しない安全な認証を実現するための業界標準であり、公開鍵暗号方式を用いた認証を採用している。ユーザーの端末に保存された秘密鍵と、サービス側に登録された公開鍵を用いて認証を行う。通常、所持要素と生体要素（指紋認証等）で構成されており、本書では多要素認証の1つとして位置付ける。パスキーの構成によって単一要素（所持要素）のみとなる場合については、知識要素等との組み合わせを推奨する。														
11		2段階認証		登録の携帯電話番号へSMS（ショートメッセージ）E-mailを送信し、そこに記載された一時的な確認コードをWeb上で入力することで認証する仕組みなど。 （例）異なるデバイスからのログイン時にSMS OTPを求めるなど） 攻撃者は、クレジットマスター/有効性確認を行う際に、攻撃プログラムを組んで機械的に真正チェックを行うため、本対策が有効と考えられる。対策は、EC加盟店またはPSPで実施する仕様が想定される。	対象外	○	○	○	対象外			6,9,11, 12,13,15	29,30	○					
12		SMS認証/電話番号認証		多要素認証の所有要素の本人認証を正しく行うために、ユーザーの携帯電話番号にSMS（ショートメッセージ）を送信し、そこに記載された一時的な確認コードをWeb上で入力することで認証する仕組み。 通話機能を利用した電話番号認証も同義。	対象外	○	○	○	対象外			9,12, 13,15	24,30	○					
13		生体認証		スマホアプリでのサービス提供の場合はOS標準の生体認証を利用可能である。ただし、アプリを提供している事業者に限定される。	対象外	○	○	○	対象外			9,13,15	-	○					
14		認証サービス		決済代行会社・サービス提供事業者が提供する固有の認証サービスを用いて、真正なカード会員本人であることを確認する。	対象外	対象外	対象外	○	対象外			9,14,15	32	○	○		○	
15		券面認証 セキュリティコード入力必須		クレジットカード番号の登録・変更時および決済時にクレジットカードの裏面の3～4桁の番号の入力を必須とする。	対象外	対象外	対象外	○	対象外			9,14, 15,16	-	○	○		○	○
16	不正検知	属性・行動分析		ECサイトで商品・サービスが注文された際に、過去の注文情報やIPアドレスなどから注文情報を確認し、不正利用かどうか判定する仕組みであり、予めシステムがクレジットカード利用者の購入履歴や住所、名前、購入商品などの個人情報を収集し、それらの収集したデータを元に消費者の傾向を分析し、不正の判定をするもの。	○	○	○	○	○		附属文書19「属性・行動分析ガイダンス」に準拠	9,11,12,13, 14,15,16, 17,18,19	29,31, 32,33	○	○		○	○
17		ベロシティチェック		決済時において、同一カード番号での一定期間内における取引試行回数等から、取引の異常性や既知の不正取引との類似性を検知する手法。	対象外	対象外	対象外	○	対象外		同一カード番号での連続試行回数制限と定義（同一デバイスでの対策はNo.2、同一アカウントでの対策はNo.6,7,8が該当）	9,15	-	○	○		○	
18	被害防止	配送先情報の活用		自社データの蓄積或いは第三者のサービスを利用して、少なくとも属性情報である「氏名表記」「姓名カナ表記」「住所」「電話番号」の規則性や組み合わせを目検などで確認、または照合することで、クレジットカード取引成立後であっても商品等の配送を事前に止めること。	対象外	対象外	対象外	対象外	○			16	33			○		○
19		配送保留配送（アカウント）停止	配送を伴う場合	カード会社によるモニタリングにて不正利用の懸念がある場合は EC 加盟店に対して配送停止・配送保留の要請に協力する。	対象外	対象外	対象外	対象外	○			16	33			○		○
20				属性・行動分析を活用し、配送停止・配送保留を行うよう努める。	対象外	対象外	対象外	対象外	○			16	33			○		○
21			配送を伴わない場合	デジタルコンテンツ等の転売防止対策の実施。 デジタルコンテンツの無効化や認証キーの停止、電子チケットの本人確認など。	対象外	対象外	対象外	対象外	○			16,18	33			○		
22				コンテンツのダウンロード時における属性・行動分析等を活用して、アクセス拒否やログインIDの削除をする。	対象外	対象外	対象外	対象外	○			16,18	33			○		
23				宿泊等の予約サービス・チケット（イベントチケットや乗車券等）・電子マネーの販売等において不正利用の懸念がある場合は、カード会社からのEC加盟店に対する不正利用の報告や要請に基づき、サービス提供のキャンセル・他の支払方法（現地での現金払い等）への変更等の協力を行う。	対象外	対象外	対象外	対象外	○			16,18	33			○		

＊　・クレジットカード決済時、決済後の各場面において有効な対策を○印で示している。対策項目によっては「決済前」においても有効だが、一覧表内、横の列で○がついている全ての場面で実施しなければならないものではない。

＊1 ・「会員登録」はクレジットカード情報の登録を伴わず、ユーザアカウント情報の登録のみを指す。カードの有効性確認としてオーソリゼーションを通じてカード登録を行うケースについては、4．決済時・決済後の対策 の「決済時」に有効な対策（○印の対策）を講じる。