EC 加盟店における基本的なセキュリティ対策
導入ガイド

クレジット取引セキュリティ対策協議会
2024 年 3 月

目次

０. 本文書の目的 セキュリティ・チェックリスト P2、5

クレジットカード取引(以下「カード取引」)に関わる全てのステークホルダーは、「クレジットカード・セキュリティガイドライン(クレジット取引セキュリティ対策協議会)(以下「セキュリティガイドライン」)」に基づき、各々に求められるセキュリティ対策を講じている。本文書では足元の情報漏えい(以下「漏えい」)の状況を踏まえて、セキュリティガイドラインで定めていない対策について指針を示すこととする。

背景として、EC 加盟店は 2018 年 6 月施行の改正割賦販売法により、PCI DSS 準拠あるいは非保持化によるセキュリティ対策が求められているが、不正手口の変化もあり、一層のセキュリティ対策が喫緊の課題となっている。

本文書は、このような状況を踏まえ、今後の必要な取り組みを示し、EC 加盟店におけるセキュリティ意識の向上と基本的なセキュリティ対策の強化、これによる情報漏えい及び不正利用の防止を目的として取りまとめている。

なお、本文書の概要を図表も加えて視覚的に説明した資料「セキュリティ・チェックリスト【附属文書 21】-EC 加盟店における基本的なセキュリティ対策-」(クレジット取引セキュリティ対策協議会)も参考にしていただきたい。

最後に、本文書をクレジット取引セキュリティ対策協議会の許可無しにセミナー等で使用することはご遠慮頂いており、その旨のご理解を賜りたい。

第 1 部 EC 加盟店におけるセキュリティ対策義務について

１. EC 加盟店のセキュリティ対策義務の概要 セキュリティ・チェックリスト P4-6

前述の通り、EC 加盟店は改正割賦販売法により、PCI DSS 準拠あるいは非保持化によるセキュリティ対策が求められている。しかしながら、カード取引の不正利用被害額は 2022 年に過去最高の 436 億円に達し、足元の 2023 年 1 月から 9 月の不正利用は 401.9 億円(前年同期比 30%増)となり、引き続き増加傾向にある。

そのため、クレジット取引セキュリティ対策協議会では、カード会社及び非対面包括事業者(以下「決済代行会社」)が EC 加盟店からの新規契約申込時にセキュリティ・チェックリストに基づくセキュリティ対策措置状況の申告を求め、システムの脆弱性に対して適切な対策を実施している EC 加盟店と加盟店契約を締結する取り組みを行うこととなった。

一方で、最近の傾向では非保持化を達成した EC 加盟店における情報漏えいが主流となりつつあり、脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策が実施されていないことによる、外部からの不正アクセスやウイルスの侵入、システムの改ざんや機器の脆弱性により、クレジットカード情報を不正に窃取される事案が発生している。

このように非保持化を実現した EC 加盟店であっても、EC サイト構築上のリスクとその顕在化により情報漏えいに繋がり得ることを十分認識した上で、基本的なセキュリティ対策の一層の強化が求められている。

２. セキュリティ対策における一般的な留意事項 セキュリティ・チェックリスト P7-9

割賦販売法では、EC 加盟店がクレジットカード番号等(以下「カード番号等」)の適切な管理を行うことを義務として定めている。したがって、EC サイト構築や運用・保守業務を外部に委託する場合も EC 加盟店の責任におい

て適切なセキュリティ対策を講じる必要がある。

特にオープンソースソフトウェアを利用しているEC加盟店での情報漏えい事案が増加傾向にあるため、オープンソースソフトウェアを利用している場合は、導入後の運用において、セキュリティパッチ更新の不備や脆弱性対策の不備が無いようにEC加盟店の責任で対策する必要がある。

なお、EC加盟店で情報漏えいが発生した場合には、クレジットカード取引の停止に加えて、フォレンジック調査から決済再開審査などにかなりの時間を要し、またフォレンジック調査費用、不正利用被害補償額、被害カードに関わる差替え費用等がEC加盟店に請求され、多大な費用負担が発生する点に留意が必要となる。

第2部　EC加盟店における対策

0. EC加盟店における対策の概要　セキュリティ・チェックリストP11

EC加盟店はインターネットを通じて不正アクセスや、なりすましによる不正ログイン、不正利用等、様々な脅威にさらされている。また、それぞれのアクセス者が真正なカード会員であるか、攻撃者であるかの区別が難しい。

よって、様々な攻撃や脅威から自社のECサイトを守るために、社内のシステム担当者、システム開発会社等に確認の上、適切なセキュリティ対策を実施する必要がある。

1. カード会員データの漏えい等の対策　セキュリティ・チェックリストP12

セキュリティホールをついた漏えいへの対策箇所について、実際の事例等から以下を想定する。
続けて、漏えい事案に基づき不正侵入及び不正取得されやすい主な方法とそれに対する対策を掲げる。

【表：不正の手口と対策が必要な場面】

不正手段	不正の手口	対策が必要な箇所				
		1. ECサイトの管理画面	2. ECサイトの設定の不備	3. 既知の脆弱性	4. マルウェア、ウイルスなどの不正ファイル	5. 悪質な有効性確認、クレジットマスターへの対策
カード番号の漏えい	1. 設定の不備を突いた攻撃	○	○		○	
	2. 既知の脆弱性を悪用した攻撃			○	○	
	3. クレジットカードの有効性確認					○

1－1. ECサイト管理者の管理画面　セキュリティ・チェックリストP13-14

1－1－1. 管理者画面のアクセス制限不備と管理者のID/PW管理不足

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①接続元を制限しないことにより、管理画面がインターネット上のどこからでもアクセスできてしまう。

②管理者のIDとパスワードがデフォルト設定のままセットされており、変更されていない。

③管理者のIDとパスワードに「会社名」や「ドメイン名」など推測されやすい文字列が設定されている。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①管理画面にアクセス可能な IP アドレスを制限する。

②IP 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。

③取得されたアカウントを不正使用されないよう二段階認証または二要素認証を採用する。

④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。

⑤管理者の ID とパスワードをデフォルト設定から変更する。

⑥管理者の ID とパスワードに推測されやすいものを使用しない。

1－2. EC サイトの設定の不備 セキュリティ・チェックリスト P15-16

1－2－1. データディレクトリの露見に伴う設定の不備

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①EC サイトの初期構築時に、特定ディレクトリ以下全てのディレクトリが公開されてしまっている。

②パッケージログファイル等も併存しており、ログファイルのうち、ID やセッション ID が詐取されてしまう。

③パッケージのアップロード、ダウンロード機能が開放されており、データの詐取や不正ファイルが混入される。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①公開ディレクトリには重要なファイルを配置しない。

②ウェブサーバやウェブ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。

1－3. 既知の脆弱性 セキュリティ・チェックリスト P17-22

1－3－1. 脆弱性診断またはペネトレーションテストの定期実施

脆弱性診断は人間に例えると健康診断のようなものであり EC サイトにある諸リスクの所在を明らかにするためのセキュリティ対策としては非常に有効である。

ペネトレーションテストもセキュリティ対策の一環として実施するという点で前述の脆弱性診断と共通点がある。

脆弱性診断がシステム全体に存在する脆弱性やセキュリティ上の不備を診断する一方、ペネトレーションテストは、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。前者が網羅性を重視する一方で、後者は専門的に特定の脆弱性や問題点を発見することに主眼が置かれる。。

なお、既知の脆弱性の内、特に SQL インジェクション(1-3-2)とクロスサイト・スクリプティング(1-3-3)は、漏えいに直結するものなので特に重要となる。

1－3－2. SQL インジェクションの脆弱性

SQL インジェクション攻撃とはウェブアプリケーション上での対策に不足があると、攻撃者が入力した不正な命令を含む文字列がデータベースにそのまま受け渡される。これを悪用し、データベースの想定外の動作を引き起こし、データベースに保存されていたデータの取り出しや、不正なデータの書き込みを行う攻撃のことをいう。

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①パッケージをそのまま利用している場合において、セキュリティパッチを適用していない。

②カスタマイズして利用している場合において、開発部分の脆弱性に対する対処がなされていない。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①最新のプラグインの使用（既知の当該脆弱性が無いもの）やソフトウェアのバージョンアップを行う。

②ウェブ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。

1－3－3. クロスサイト・スクリプティングの脆弱性

ウェブアプリケーションの中には、検索のキーワードの表示画面や個人情報登録時の確認画面、掲示板、ウェブのログ統計画面等、ユーザーからの入力内容や HTTP ヘッダの情報を処理し、ウェブページとして出力するものがある。ここで、ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプト等を埋め込まれてしまう。この問題を「クロスサイト・スクリプティングの脆弱性」と呼び、この問題を悪用した攻撃手法を、「クロスサイト・スクリプティング攻撃」という。

クロスサイト・スクリプティング攻撃の影響は、ウェブサイト自体に対してではなく、そのウェブサイトのページを閲覧しているユーザーに及ぶ。

ウェブアプリケーションにスクリプトを埋め込むことが可能な脆弱性がある場合、これを悪用した攻撃により、ユーザーのブラウザ上で不正なスクリプトが実行されてしまう可能性がある。

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①パッケージをそのまま利用している場合において、セキュリティパッチを適用していない。

②カスタマイズして利用している場合において、開発部分の脆弱性に対する対処がなされていない。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①最新のプラグインの使用（既知の当該脆弱性が無いもの）やソフトウェアのバージョンアップを行う。

②ウェブ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。

1－4. マルウェア、ウイルスなどの不正ファイル セキュリティ・チェックリスト P23

1－4－1. マルウェア対策としてのウイルス対策ソフトの導入、運用

マルウェアとは「悪意のある」という意味の英語「Malicious」と「software」を組み合わせた造語（malware）。様々な脆弱性を利用して攻撃を仕掛けるソフトウェアの総称として使われる。

ウイルスをはじめ、ワーム、スパイウェア、アドウェア、フィッシング、ファーミング、スパム、ボット、キーロガー（キーストロークロガー）、トロイの木馬等、マルウェアの種類は様々。

ウイルス対策ソフトはウイルスを検出・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。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。

昨今の漏えい事案では、業務端末へのウイルスの侵入からサーバへの感染なども考えられる。

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①ウイルス対策ソフトの更新手続漏れ等による業務端末へのウイルスの侵入。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①サーバ、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。

1－5. クレジットマスター及び悪質な有効性確認への対策 セキュリティ・チェックリスト P24

1－5－1. クレジットマスター及び悪質な有効性確認への対策

クレジットマスター（略称：クレマス）とは、カード会員データの登録/変更時及びクレジットカード決済時において、カード番号等の採番の規則性を悪用し、機械的に生成することで真正なクレジットカード番号等を割り出す手口である。

また、悪質な有効性確認とは、クレマスで生成したカード情報やフィッシングで窃取したカード情報が、EC 加盟店での利用等を通じて実際に利用できるカード番号かを確認する手口をいう。

(1) 攻撃者は以下の点を攻撃してくる可能性がある。

①会員登録時の「なりすまし」による登録時、または会員のログインフォームへの不正ログイン後に、クレジットカード決済の登録/変更の機能を悪用されると、カード会員データの悪質な有効性確認を行われる恐れがあり、有効なカード会員データを不正取得される。また、会員登録をしない場合のゲスト購入時にもクレジットカード決済の機能を悪用されると、クレジットマスターやフィッシングなどで不正取得したカード番号等をもとにカード会員データの悪質な有効性確認を行われる恐れがあり、有効なカード会員データを不正取得される。

②攻撃者は特に日本国内の IP アドレスよりも海外 IP アドレスから悪質な有効性確認/クレジットマスターを実施することが多い。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①海外からの攻撃が非常に多いため「不審な IP アドレスからのアクセス制限」を行う。

②有効なカード会員データの漏えい対策として「同一アカウントからの入力制限」「エラー時に、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

③EMV 3-D セキュアや SMS 通知など本人確認ができる対策を行う。

④有効性確認の回数制限を設けるなどの対策を行う。

次頁の表以降で示す各種対策について、全ての EC 加盟店にとって対策の優先度が高いと思われるものについては優先度「高」として推奨する。

また優先度「高」としたもの以外の対策については、①EC 加盟店自身で現実的に対応可能なもの、②システム開発会社・サービス提供事業者などに対応を要請する必要があるもの、③データセンタなどのインフラの整備が必要なものなどによってコストや必要なリソースが異なり、また、ビジネスモデルやシステム環境等によっても有効な対策が異なるため、個別の状況に応じた検討が必要となる。

【表：悪質な有効性確認、クレジットマスターへの対策】（各対策内容の詳細については別表を参照）

クレジットカード決済の登録/変更の機能悪用への対策

対策分類	対策番号	対策（決済処理時）	優先度
アクセス制限	1-①	不審な IP アドレスからのアクセス制限	高
	1-②	スロットリング	高
機能制限	4-① 4-② 4-③	同一アカウントからの入力制限	高
エラー表示制限	3-①	エラー時に、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	高
認証強化	6-④	多要素認証	高
	6-⑤	生体認証	
	6-⑥	2 段階認証	高
	6-⑧	認証サービス	
	6-⑨	券面認証	高
	6-⑩	SMS 認証	高
	6-⑪	EMV 3-D セキュア	高
不正検知	7-①	属性・行動分析（不正検知システム）	高
	7-②	ベロシティチェック	

ゲスト購入時のクレジットカード決済機能悪用への対策

対策分類	対策番号	対策（決済処理時）	優先度
アクセス制限	1-①	不審な IP アドレスからのアクセス制限	高
	1-②	スロットリング	高
Bot 対策	2-①	CAPTCHA 認証	
	2-②	reCAPTCHA 認証	
認証強化	6-⑨	券面認証	高
	6-⑪	EMV 3-D セキュア	高
エラー表示制限	3-①	エラー時に、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	高
認証強化	6-⑧	認証サービス	
不正検知	7-①	属性・行動分析（不正検知システム）	高
	7-②	ベロシティチェック	

なお、すべての場面に共通する対策としては「不審な IP アドレスからのアクセス制限」が挙げられ、全ての場面において優先度「高」の対策と位置付けられる。特に海外からの大量な不正アクセスによって、インターネット経由のセキュリティ対策まで手が届いていないことが多い小規模な EC 加盟店においても多くの漏えい事案が発生し

ている。したがって、不正アクセスをされないように、不審な IP アドレスからの接続を制限することが重要となる。とりわけ海外の消費者を対象としていない EC 加盟店は海外 IP アドレスを遮断することが望ましい。具体的に不審な IP アドレスからのアクセス制限を実施する方法については、接続している決済代行会社に相談することによって導入できることが多い。

一方で、海外 IP アドレスの遮断をせずに取引を行う場合には、P7「1－5－1. クレジットマスター及び悪質な有効性確認への対策」の(2)に記載する対策を講じることで抑止につながる。

2. 不正ログイン対策(クレジットカード決済前の対策) セキュリティ・チェックリスト P25-26

カード会員が EC 加盟店の機能を利用する際に、EC サイトの会員となりカード会員データ及び属性情報などを登録するため、これらのデータを利用して不正利用が行われる。これらの対策を総じて不正ログイン対策とする。

不正ログインを起点とした不正利用の原因として以下が想定される。

(1)不正なアカウントが作成され、カード会員データを登録される。

(2)不正に取得したカード会員データを利用し、不正ログインによりカード番号等の変更や属性変更が可能となり不正利用される。

(3)フィッシングメール等で不正取得されたアカウント情報及びアカウント/パスワードクラッキングにより、不正ログインをされる。

【表:不正の手口と対策が必要な場面】

不正手段	不正の手口	対策が必要な場面		
		1. 会員登録時	2. ログイン認証時	3. 属性情報変更時
アカウント悪用	1. 不正アカウント作成	○		
	2. アカウント乗っ取り		○	○

不正アカウント作成とは EC 加盟店において不正なアカウントを開設の上、盗用したカード番号等を支払方法として登録する手口であり、アカウント開設時の対策が必要となる。

アカウント乗っ取りとは、流出したログイン情報の使用やアカウントクラッキングなどから正規のアカウントに不正ログインをしてアカウントを乗っ取り、支払方法として登録されている正規のカード番号等を悪用する手口である。攻撃者は合わせて属性変更(連絡先、配送先住所等の変更)を行うことも想定される。ログイン認証時、属性変更時の対策が必要となる。本項ではそれぞれの場面に応じて確認されている不正事例を説明するとともに、そのような不正を防止するための対策の方法を説明する。

なお、本項においてもすべての場面に共通する対策としては不審な IP アドレスからのアクセス制限をあげており、当該対策によって「不正アクセス」、「なりすまし」の抑止になる。一方で、海外 IP アドレスの遮断をせずに取引を行う場合には、ログイン認証時に、ID/パスワード/姓カナ、名カナを入力させるなど、ログイン認証時に本人確認の強化をするなどの工夫が必要となる。

2－1. 会員登録時の対策 セキュリティ・チェックリスト P27

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①フィッシングメールによる個人情報及びカード会員データの不正取得や他社の漏えい事案などからの漏えいされたデータを用いて、「なりすまし」の登録することが可能であり、不正に入手したカード会員データを登録/利用されるリスクがある。(Wallet へのチャージなどに悪用される。)

③海外の攻撃者が、日本の攻撃者に指示を行う手口もあり、当該手口に対しては、IP アドレスによって不正利用と見分けることが困難である。

(2)上記のリスクに対しては以下の対策が有効と考えられる。

①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。

②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。

③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く、本人確認を行う。

④不正ログインをされた場合でも、真正なカード会員に気づきを与えられるように二要素認証などによる本人確認を行う。

⑤不正検知システムを利用する。

【表:会員登録時の不正事例】

事例番号	不正の手口	不正事例(アカウント開設時)
1	不正アカウント作成	不正にアカウントを開設して、事前に不正取得したカード番号等の有効性を確認する。

【表:会員登録時の対策】(各対策内容の詳細については別表を参照)

対策分類	対策番号	対策(アカウント開設時)	優先度
アクセス制限	1-①	不審な IP アドレスからのアクセス制限	高
	1-②	スロットリング	高
Bot 対策	2-①	CAPTCHA 認証	
	2-②	reCAPTCHA 認証	
本人確認	5-①	eKYC	
認証強化	6-⑦	姓カナ、名カナ入力値の検証	高
不正検知	7-①	属性・行動分析(不正検知システム)	高

2－2. ログイン認証時の対策 セキュリティ・チェックリスト P28

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①会員用のログイン画面は、インターネットに公開する必要があるので、アクセス制限ができず、このような状況を悪用し、フィッシングメールや他社の漏えい事案などで不正取得した「ID/パスワード」を利用した、アカウ

ント/パスワードクラッキングが頻繁に行われている。
②ID 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ため、「なりすまし」による、不正ログインを実行されても、真正なカード会員及び EC 加盟店は気づきにくい。
③攻撃者は海外からクラッキングを実施することが多い。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。
①海外からの攻撃が非常に多いため「不審な IP アドレスからのアクセス制限」を行う。
②アカウント/パスワードクラッキングの対応として「ログイン試行回数の制限強化」を行う。
③不正ログインをされた場合でも、真正なカード会員に気づきを与えられるように、二要素認証などによる本人確認を行う。
④ログイン時のメールや SMS 通知、スロットリングなどを行う。
⑤その他、「デバイスフィンガープリント」等を利用する。

【表:ログイン認証時の不正事例】

事例番号	不正の手口	不正事例(ログイン認証時)
2	アカウント乗っ取り	「属性・行動分析によるリスクベース認証」や「不正ログインの Bot 対策」または「ファイアウォール」など対策からどれか一つのみ利用して対策していると、不正アカウントや海外 IP アドレスを止めることができず、アカウントクラッキングなどによりログイン認証を突破され、カード番号等の不正取得や個人情報の不正取得などを行われるなどの事例がある。

【表:ログイン認証時の対策】(各対策内容の詳細については別表を参照)

対策分類	対策番号	対策(ログイン認証時)	優先度
アクセス制限	1-①	不審な IP アドレスからのアクセス制限	高
	1-②	スロットリング	高
	1-③	ログイン試行回数の制限強化	高
Bot 対策	2-①	CAPTCHA 認証	
	2-②	reCAPTCHA 認証	
認証強化	6-①	デバイスフィンガープリント	高
	6-②	デバイス認証	
	6-③	単純パスワード、短いパスワードの排除	高
	6-④	多要素認証	高
	6-⑤	生体認証	
	6-⑥	2 段階認証	高
	6-⑦	姓カナ、名カナ入力値の検証	高
	6-⑩	SMS 認証	高
不正検知	7-①	属性・行動分析(不正検知システム)	高

2－3. 属性情報変更時の対策 セキュリティ・チェックリスト P29

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①不正ログインにより、攻撃者が不正に取得した真正なカード会員の個人情報を悪用し、結果的に当該アカウントによる Wallet チャージ等の不正利用が発生する恐れがある。

②海外の攻撃者が、日本の攻撃者に指示を行う手口もあり、当該手口に対しては、IP アドレスによって不正利用と見分けることが困難である。

(2)上記のリスクに対しては以下の対策が有効と考えられる。

①攻撃者が海外である場合には、入力されている個人情報が間違っている場合が多く、不自然な表示ではないか、また不自然な組み合わせではないかの本人確認が重要になる。そのため、個人情報などの変更時には、元々登録されていた本人に対して「二要素認証」や、SMS 認証等の「二段階認証」により本人確認を行う。

②海外からの攻撃が非常に多いため「不審な IP アドレス(特に海外)からのアクセス制限」を行う。

③その他「不正検知システム(Fraud サービス)/デバイスフィンガープリント」等を利用する。

【表:属性情報変更時の不正事例】

事例番号	不正の手口	不正事例(属性変更時)
3	アカウント乗っ取り	EC 加盟店のアカウントを乗っ取られたのちに、属性情報を変更される事例がある。

【表:属性情報変更時の対策】(各対策内容の詳細については別表を参照)

対策分類	対策番号	対策(属性情報変更時)	優先度
アクセス制限	1-①	不審な IP アドレスからのアクセス制限	高
認証強化	6-①	デバイスフィンガープリント	高
	6-②	デバイス認証	
	6-④	多要素認証	高
	6-⑤	生体認証	
	6-⑥	2 段階認証	高
	6-⑩	SMS 認証	高
不正検知	7-①	属性・行動分析(不正検知システム)	高

3. 不正利用対策

セキュリティガイドラインに記載された EMV 3-D セキュア必須化により、原則すべての EC 加盟店に対し、不正被害防止のため 2025 年 3 月までに EMV 3-D セキュアの導入が求められている。

EMV 3-D セキュアの導入推進に向け、カード会社は静的パスワードから動的パスワード等へ移行するよう取り組んでいる。

しかし、移行を行ったとしても、EMV 3-D セキュアの導入や認証が困難な決済スキームも存在することから、EMV 3-D セキュアだけですべての被害を防止できるわけではない。

そのため、多面的・重層的な観点から不正利用対策を実行することが不可欠である。

不正利用の原因は以下の流れが想定される。

(1)他社 EC サイトの情報漏えい事案やクレジットマスター、悪質な有効性確認、フィッシングメールなどにより真正なカード会員データが不正取得され攻撃者により不正利用される。

(2)不正取得されたカード会員データを利用して、「なりすまし」や「スマートフォンアプリの登録など」を行い、換金性の高い商品などを不正購入される。

(3)商品の配送の場合、攻撃者が受け取りやすい場所で商品の受け取り、または転送会社へ商品が配送される。

(4)不正利用にて販売された商品は海外または国内で転売や古物商への販売、フリーマーケットなどの EC サイトで販売され現金化される。

上記を踏まえ、セキュリティガイドラインに記載の 4 方策について、EC 加盟店が自ら対策を講じることが可能な場面として、「クレジットカード決済時」と「クレジットカード決済後」に分けて、場面ごとのリスクと対策を下記に示す。

3－1. クレジットカード決済時の対策

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①他社 EC サイトの漏えい事案やクレジットマスター、悪質な有効性確認、フィッシングメールなどにより不正取得された真正なカード会員データを利用して、EC サイトのクレジットカード決済時に真正なカード会員データを利用して「なりすまし」による商品購入が行われる。

②登録型のスマートフォンアプリに架空のアカウント或いは正規のアカウントでログインをして商品を購入される。

(2)上記のリスクに対しては以下の対策が有効と考えられる。

①真正なカード会員データによる「なりすまし」の対策として「EMV 3-D セキュア」を導入し、カード会社側の本人確認を経てオーソリを行う。

②オーソリ時にセキュリティコードを利用した券面認証を行いカード会社側の確認を行う。

③クレジットカード決済時に属性・行動分析(不正検知システム)(以下「属性・行動分析」)を活用し、真正なカード会員の利用であるかのリスク判断を行う。

④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。

3－2. クレジットカード決済後の対策

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①クレジットカード決済時に他人の真正なカード会員データを利用して購入された商品を現金化するために、攻撃者が空き家、受け子、置き配、配送事業所、不正な配送先等で商品を受け取る。

②デジタルコンテンツなどの配送を伴わない商品については、決済後即時に利用される。

(2)上記のリスクに対しては以下の対策が有効と考えられる。

①不正に購入された商品等が攻撃者などに渡らないように商品の配送時に EC 加盟店の担当者が目検などで

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確認または照合し、配送停止や配送保留を行う。

②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。

③属性・行動分析を活用し、上記を確認の上、配送停止・配送保留を行うよう努める。

④配送を伴わない商品については、同じ攻撃者によるアクセスを防ぐため、決済前の不正ログイン対策や決済時の不正利用対策を講じる。

第3部 その他の留意事項

1. その他加盟店における対策

1－1. MO/TO 加盟店の不正利用対策

非対面取引でありながら、本人の介在しない取引であり、EMV 3-D セキュアの導入ができないため、個別具体的な不正対策が必要。

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①不正な注文情報により申し込みがされて、攻撃者が空き家、受け子、置き配、配送事業所、不正な配送先等で商品を受け取る。

(2)上記のリスクに対しては以下の対策が有効と考えられる。

①クレジットカード決済時の対策は難しいが、不審な取引の場合には、券面認証を求める。

②クレジットカード決済後の対策に重点を置き、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確認または照合し、加盟店担当者が手動チェック(目検)により配送停止や配送保留をする。

③その他の対策として、決済代行会社またはサービス提供事業者の属性・行動分析(または不正配送先情報)を活用、電話番号の使用/未使用確認サービスを利用、配送先の名前の確認を行うなどの事例が挙げられる。

1－2. 登録型スマートフォンアプリ決済のセキュリティ対策及び不正利用対策

「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】」を参照すること。

2. 特定の商材における対策

2－1. デジタルコンテンツの不正利用対策

デジタルコンテンツでは、EMV 3-D セキュアの導入が必須ではあるが、クレジットカード決済後すぐにダウンロードが可能な商材のため、クレジットカード決済後の不正利用対策は現状困難である。

(1)攻撃者は以下の点を攻撃してくる可能性がある。

①インターネットサービス(クラウドサービス)などで利用するための認証キーが販売されている場合には、この認証キーが EC サイトやフリーマーケットサイトで転売される。

②会員登録後にクレジットカード決済を経てデジタルコンテンツの即時購入が可能であり、即座に転売される。

(2) 上記のリスクに対しては以下の対策が有効と考えられる。

①インターネットサービス(クラウドサービス)などで利用する際の認証キーの転売については、この認証キーを停止し利用不可にできる手段があると被害防止に役立つ。

②クレジットカード決済後すぐにダウンロードが可能な商材については、クレジットカード決済前の「不正ログイン対策」とクレジットカード決済時(特にオーソリ時)の属性・行動分析が有効である。

③その他、デバイス認証を活用する事でネガティブ情報(以下「ネガ情報」)をもとにアクセスした消費者のデバイス認証を実施できる。また、属性・行動分析では、不正なログイン ID/パスワードのネガ情報もあるため、アクセス拒否やログイン ID の削除なども可能である。

3. 特定の対策に関する補足説明

3－1. 属性・行動分析の活用方法

3－1－1. 前提

当協議会のセキュリティガイドラインでは、EC サイトにおける不正利用対策の具体的方策の 1 つとして属性・行動分析を掲げている。

本紙においては不正ログイン対策(クレジットカード決済前の対策)としても有効な対策として説明している。但し、属性・行動分析は、WAF などのセキュリティ機能のように、簡単に導入して即座に効果を期待できる仕組みではなく、不審なトランザクションのモニタリング(要注意トランザクションの目視チェック及び不正か否かの判断)や、属性・行動分析への不正取引情報の提供、業種や不正利用の動向に応じて、適切な設定、調整等を行う必要がある。また、不正利用されたカード会員の属性情報は情報の収集、共有、保存において個人情報保護に留意しなければならない。

なお、属性・行動分析は、取引情報やアクセスのログ情報等を用いて、EC 加盟店が自ら、分析のシステムや仕組みを構築し、運用することが可能だが、本項では属性・行動分析のサービス提供者等(以下「サービス提供事業者」が EC 加盟店にサービスを提供し、EC 加盟店がそのサービスを利用して属性・行動分析を運用し、不正対策を実施する形態を想定しており、属性・行動分析の活用に当たっては、関係する事業者(EC 加盟店、サービス提供事業者、カード会社、決済代行会社)が共通認識をもって対応する必要がある。

3－1－2. 継続的な運用の見直し

属性・行動分析の効果的な運用を確保し、セキュリティ対策を最適化するためには、属性・行動分析の運用を継続的に見直すことが重要である。

EC 加盟店においては、以下の対応を行うことが属性・行動分析を有効活用する上で重要と考えられる。

(1) 情報提供をスムーズに行うために、EC 加盟店のシステムと属性・行動分析を連携し、システム間で直接情報提供が行えるようにする。

(2) 不正利用されたカード会員の情報や取引の情報、不審なトランザクションに関する情報、新たな脅威や攻撃パターンに関する情報をサービス提供事業者に提供する。これは異常なトランザクションや新たな攻撃パターンを素早く特定し、追加的な不正利用防止対策を講じるのに役立つ。

(3) サービス提供事業者との間で個人情報を共有する際は、適切な個人情報保護措置を講じる。

3－1－3. ネガティブ情報の蓄積と活用

属性・行動分析におけるネガ情報とは、過去に不正取引にて使用された情報を指す。ネガ情報は、属性・行動分析の重要な要素であり、これらの情報を蓄積して分析することにより、属性・行動分析が行われるため、プライバシーとセキュリティの観点で配慮を行いつつ、常に最新性を保つことが効果的な不正利用対策を講じるうえで重要となる。ネガ情報の例として、個人属性情報、決済情報、購買情報、デバイス情報、位置情報、IP アドレス、ビヘイビア情報等が挙げられるが、この限りではない。

これらの多様な情報項目を組み合わせて分析することにより、異常なパターンや行動を検知するための効果的なルール設定、AI・機械学習モデルの学習が可能となり、属性・行動分析の精度向上に寄与することにつながる。その他、EMV 3-D セキュアの AReq に含まれる項目も参考に要件として考慮されるべきである。

なお、注文を止められた攻撃者が EC 加盟店に電話し、審査基準を聞き出そうとする手口があるため、属性・行動分析のロジックを消費者に開示してはならない。

3－1－4. トレーニングと教育、体制の整備

トレーニングと教育は、属性・行動分析の効果的な運用に不可欠な要素である。また、属人的な運用にならないよう自社の運用について文書化し維持管理する必要がある。関係事業者も含めてトレーニングと教育プログラムを整備し、定期的に実施することが求められる。AI・機械学習モデルの属性・行動分析では取引の目検チェック、ルールチューニング等、完全自動化されているものもあり、全てが対象とならない場合があるが、原則考え方は同様である。

必要なトレーニングと教育として以下が考えられる。

(1) 属性・行動分析の使用方法

自社内の担当者に対して、属性・行動分析のシステムログイン、データの入力、レポートの生成、アラートの確認などの基本的な閲覧・操作方法を教育する。教育にあたっては、サービス提供事業者にサポートを求めるとよい。

(2) アラートと対応手順

異常なトランザクションや不正が検出された場合の適切なアラートと対応手順を自社内の担当者に教育する。

(3) モニタリングの方法

自社内の担当者に対し、トランザクションのモニタリング手順やポイントについて教育し、習得させる。教育にあたっては、サービス提供事業者にサポートを求めるとよい。

(4) データの収集と報告

EC 加盟店は、自社内の担当者に対して、サービス提供事業者に対し、不正取引のデータを提供することの重要性と、どのように収集しサービス提供事業者に提供するかなどの運用手順を教育する。

(5) プライバシーとコンプライアンスの遵守

データの収集と分析に関するコンプライアンスを遵守する責任があるため、自社内の担当者には個人情報保護法やデータプライバシー規制を遵守させる。

4. (ご参考)イシュアーによる不正利用対策

国際ブランド付クレジットカードを発行する全てのイシュアーの取り組みとしては以下が挙げられる。

(1)EMV 3-D セキュアの導入 未導入イシュアーによる即時導入を進めており、95%のイシュアーが導入を完了(2023 年 10 月末現在、クレジット取引セキュリティ対策協議会 EMV 3-D セキュア等推進 WG によるアンケート調査による)。

(2)カード会員への EMV 3-D セキュアの利用登録の推進

2025 年 3 月末までに EC 利用カード会員ベースで 80%の登録を目指すこととし、カード会員に対して EMV 3-D セキュアの利用登録を要請するとともに、EMV 3-D セキュアの利用登録に関する周知・啓発を業界横断的に進める。なお、EC 利用会員は、過去 1 年間で EC 利用実績のある会員とするが、把握が難しい場合は、イシュアー各社の判断による EC 利用会員の概数の推測も許容する(法人契約カード等、個社の事情により EMV 3-D セキュアの設定ができないカードを母数に含めない場合がある)。

(3)動的(ワンタイム)パスワード等による認証の実施

2025 年 3 月末までに EMV 3-D セキュア登録会員ベースで 100%の登録を目指すこととし、①動的(ワンタイム)パスワード等による認証を実施するためのシステム構築、②カード会員への動的(ワンタイム)パスワード等の利用手続(携帯電話番号やメールアドレスの登録、アプリのダウンロード等)の要請、③動的(ワンタイム)パスワードの利用に関する周知・ 啓発(業界横断的に実施)、を進めることとする。但し、既存会員によっては連絡不能等で動的(ワンタイム)パスワード等の利用手続の案内が出来ないケースも想定されるため、母数を稼働会員とする等、個社判断とする。

5. 最後に

技術の進歩に伴い、不正利用の手口とそれに対するセキュリティ対策は変化するものであり、セキュリティ対策の取組に終わりはない。

EC 加盟店においては非保持化の実現に加えて、それ以前に基本的なセキュリティ対策を徹底し、自社で構築したシステムに対し、不断の対策を講じ続ける姿勢が求められる。

オープンソースを利用している EC 加盟店は、システム開発会社からの注意喚起を元に、あるいはシステム開発会社に積極的に情報提供を求め、早急に追加的なセキュリティ対策を講じることが重要である。

一つの EC 加盟店で漏えい事案が発生すると、すぐさま他の EC 加盟店での不正利用被害へと波及し、業界全体に相当額の損失を招くこととなる。自社の EC サイトを適切に保護するためにも、本資料を参考にすると共に、各オープンソースのシステム開発会社が公表しているセキュリティ・チェックリストを活用することも有効である。

万が一、漏えい事案を発生させた場合は、速やかに契約しているカード会社や決済代行会社に連絡の上、被害拡大防止の対応を実施することが必要となる。

以上

資料１別表

対策については、全てのEC加盟店にとって対策の優先度が高いと思われるものについては優先度「高」として推奨する。
優先度「高」としたもの以外の対策については、①EC加盟店自身で現実的に対応可能なもの、②システム開発会社・サービス提供事業者などに対応を要請する必要があるもの、③データセンタなどのインフラの整備が必要なものなどによってコストや必要なリソースが異なり、また、ビジネスモデルやシステム環境等によっても有効な対策が異なるため、個別の状況に応じた検討が必要となる。

対策番号	セキュリティ対策		優先度	説明	参考情報 ※紹介URLには国立国会図書館に保存されたWebアーカイブを含みます	クレジットカード決済前			クレジットカード決済時		クレジットカード決済後	セキュリティチェックリスト有無
	対策分類	対策項目				会員登録	会員ログイン	属性変更	カード情報入力	決済時	決済終了後	
1-①	アクセス制限	不審なIPアドレスからのアクセス制限	高	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。 ・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。	【IPAサイト紹介】 サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2019 年 1 月～3 月] https://www.ipa.go.jp/files/000073456.pdf p4.「組織としては公開ウェブサーバへの探索通信は日々多く発生しているものと考えられるが、不審なIPアドレスからの通信を禁止する等のアクセス制限を行うといった対応が必要であろう。」を参照	●	●	●	●	●		有
1-②	アクセス制限	スロットリング	高	一定時間内に受信可能なリクエスト数を制限し、制限を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。	【IPAサイト紹介】 情報セキュリティ技術動向調査（2011年下期） 2. NIST SP 800-63-1 電子認証に関するガイドラインについて. https://warp.da.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/files/000024402.pdf 「スロットリング」について触れています。	●	●		●	●		有
1-③	アクセス制限	ログイン試行回数の制限強化	高	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。PCI DSS Ver4.0の要件では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、本人確認ができるまでは使用できないようにする。	【IPAサイト紹介】 安全なウェブサイトの作り方 https://www.ipa.go.jp/security/vuln/websecurity.html P55「2.5 パスワードに関する対策」で単純パスワード、短いパスワードの排除、ログイン試行回数の制限について参照。 「セキュアプログラミング講座　Webアプリケーション編」 第2章 アクセス制御　ユーザ認証を自製する場合 https://www.ipa.go.jp/archive/security/vuln/programming/web/chapter2/2-1.html		●					有
2-①	Bot対策	CAPTCHA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。 BOT対策として有効である。UXが低下するが、現実的な対応策となり得る。	【IPAサイト紹介】 「セキュアプログラミング講座　Webアプリケーション編」 第9章 Web関連技術　CAPTCHA https://www.ipa.go.jp/archive/security/vuln/programming/web/chapter9/9-2.html 「ブラウザの通知機能から不審サイトに誘導する手口に注意」 https://www.ipa.go.jp/security/anshin/mgdayori20210309.html 偽CAPTCHA認証を装って「許可」ボタンを押させようと誘導する手口に関するものです。	●	●		●	●		無
2-②	Bot対策	reCAPTCHA認証	-	Google社が提供する認証システムで、ボット（自動化されたプログラム）によるアクセスを防ぐ。画像を選択するだけで、コンピューターを操作しているのが人間なのかボットなのかを判定する。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。 BOT対策として有効である。UXが低下するが、現実的な対応策となり得る。		●	●		●	●		無
3-①	エラー表示制限	エラー時に、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）	高	カード番号/有効期限/セキュリティコードのどのフォーマットにエラーあるか分からなくする。 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。	【IPAサイト紹介】 情報セキュリティ10大脅威2021 https://www.ipa.go.jp/security/vuln/10threats2021.html 組織８位「インターネット上のサービスへの不正ログイン」にて、アカウントの存在有無がわかるような認証エラー表示の抑止、連続アクセスの検知等を参照。				●	●		有
4-①	機能制限	同一アカウントからの入力制限	高	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。					●	●		有
4-②	機能制限	同一アカウントからの入力制限	高	・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					●			無
4-③	機能制限	同一アカウントからの入力制限	高	・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					●			無

対策番号	セキュリティ対策		優先度	説明	参考情報 ※紹介URLには国立国会図書館に保存されたWebアーカイブを含みます	クレジットカード決済前			クレジットカード決済時		クレジットカード決済後	セキュリティチェックリスト有無
	対策分類	対策項目				会員登録	会員ログイン	属性変更	カード情報入力	決済時	決済終了後	
5-①	本人確認	eKYC	-	electronic Know Your Customerの略で、電子身元確認と訳される。スマホやPCを使用して、オンライン上で身元確認を完結できる仕組みのこと。高いセキュリティレベルが求められるサービスに有効である。 免許書などの本人確認書類の提示、一部のスマホ決済事業者では、登録時に免許書の提示を求めている。		●						無
6 - ①	認証強化	デバイスフィンガープリント	高	ブラウザフィンガープリントとは、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。			●	●				有
6 - ②	認証強化	デバイス認証	-	デバイス認証とは、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です。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。			●	●				有
6 - ③	認証強化	単純パスワード、短いパスワードの排除	高	PCI DSS ver4.0では、以下のパスワード要件が求められている。 ・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。	【IPAサイト紹介】 安全なウェブサイトの作り方 https://www.ipa.go.jp/security/vuln/websecurity.html P55「2.5 パスワードに関する対策」で単純パスワード、短いパスワードの排除、ログイン試行回数の制限について参照。 「セキュアプログラミング講座　Webアプリケーション編」 第2章 アクセス制御　ユーザ認証を自製する場合 https://www.ipa.go.jp/archive/security/vuln/programming/web/chapter2/2-1.html		●					無
6 - ④	認証強化	多要素認証	高	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。	【IPAサイト紹介】 不正ログイン対策特集ページ https://www.ipa.go.jp/security/anshin/account_security.html 本ページにおいて多要素認証（SMS認証含む）の推奨事項を参照。		●	●	●	●		有
6 - ⑤	認証強化	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。 ・導入の難易度が高く、スマホアプリ以外での利用も可能な場合、効果は限定的になる懸念がある。 ・「多要素認証」同様、実装しても使うユーザは少ない懸念があり、iOS/Androidを利用した対応の普及が望まれる。	【IPAサイト紹介】 生体認証の利用促進に向けた「生体認証導入・運用の手引き」等を参照 https://warp.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/security/fy24/reports/bio_sec/documents/bio_guide_24.pdf 「生体認証システムの導入・運用事例集」改訂版等の公開 https://warp.ndl.go.jp/info:ndljp/pid/11376004/www.ipa.go.jp/files/000013963.pdf 「バイオメトリクス・セキュリティ評価に関する研究会 調査報告書」 https://warp.ndl.go.jp/info:ndljp/pid/8198317/www.ipa.go.jp/security/fy20/reports/bio_sec/documents/bio_rep_20.pdf		●	●	●	●		無
6 - ⑥	認証強化	2段階認証	高	本人確認を正しく行うために、ユーザのスマートフォンや携帯電話に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。E-mailでも同様の事をしている場合もある。 不正検知システムとの組み合わせで使用することが有効である。 （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。* 1	【IPAサイト紹介】 不正ログイン対策特集ページ https://www.ipa.go.jp/security/anshin/account_security.html 本ページにおいて多要素認証（SMS認証含む）の推奨事項を参照。		●	●	●	●		有
6 - ⑦	認証強化	姓カナ、名カナ入力値の検証	高	ID/パスワードの他に姓カナ、名カナを入力させる手法。 大手通販加盟店の一部では既に採用され効果が出ている。また、ログイン認証の強化が期待できる。		●	●					有

対策番号	セキュリティ対策		優先度	説明	参考情報 ※紹介URLには国立国会図書館に保存されたWebアーカイブを含みます	クレジットカード決済前			クレジットカード決済時		クレジットカード決済後	セキュリティチェックリスト有無
	対策分類	対策項目				会員登録	会員ログイン	属性変更	カード情報入力	決済時	決済終了後	
6 - ⑧	認証強化	認証サービス	-	加盟店が自社で本人確認をするためのもの（或いは、サービス事業者の提供サービスを利用して本人確認をする場合も含む）。 様々な場面でユーザ（消費者）が事前或いは登録後に商品購入をする際に、上記6-④から⑦までの手法によりユーザに対して本人確認をすることを目的としている。					●	●		有
6 - ⑨	認証強化	券面認証 セキュリティコード入力必須（否認時に何の情報が不一致か示さない）	高	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。 番号盗用に一定の効果が期待できるが、リトライ回数に制限がない場合、3～4桁の総当たりで承認される可能性がある。					●	●		有
6 - ⑩	認証強化	SMS認証	高	本人確認を正しく行うために、ユーザーのスマートフォンや携帯電話に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			●	●	●	●		有
6 - ⑪	認証強化	EMV3-Dセキュア	高	現行イシュア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。 ここでは、カード番号が真正であるが、本人ではない可能性がある為、そのような観点で有効と考えられる。	【IPAサイト紹介】 「組込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書」第四章：ICカード https://warp.ndl.go.jp/info:ndljp/pid/1079789/www.ipa.go.jp/security/fy18/reports/embedded/04_ICCard.pdf 4-31「表 4.7 IC カードにおける対策マップ（運用段階）」に「3D-Secure」の記述を参照。					●		有
7-①	不正検知	属性・行動分析 （不正検知システム）	高	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、不正の判定するもの。		●	●	●	●	●	●	有
7-②	不正検知	（低額取引の）ベロシティチェック		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。EMVの ICカード仕様でオフライン取引のリスク管理に使用されている。 非対面取引の場合には、一定期間内に同一カードが異常な回数使用されていないか、同一の利用者のデバイス、IPアドレスから複数のカード番号が使用されていないか、同一のアカウントであり得ない頻度で同じ高額商品を購入していないか、などのチェック方法が考えられる。 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攻撃を行うため、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。						●		無
8-①	被害防止	配送先情報の活用		不正購入された商品を攻撃者に渡さないよう被害防止の為、自社の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。							●	有
8-②	被害防止	配送保留及び配送停止		カード会社が自社の会員に対してヒアリング等により不正利用を受けた注文に対して加盟店に配送保留や配送停止を行うこと。自社の会員にヒアリングなどをしており、不正確度が高く、迅速な配送停止依頼の受け入れにより被害の水際防止に効果がある。							●	有

*1
・利用者のフィルター設定でSMS未達のケースがある。
・メアドや携帯番号（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、
メールアドレス変更時には、変更するための認証コードを登録済みメールアドレスに送信する、
携帯番号変更時には、変更するための認証コードを登録済み携帯番号にSMS送信する、
といった変更時の追加認証が必要となる。