附属文書 20

EC 加盟店におけるセキュリティ対策
導入ガイド
２．１版

クレジット取引セキュリティ対策協議会
2026 年 3 月

目次

0. 本書の目的 3
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 3
1. EC 加盟店のセキュリティ対策義務の概要 3
2. セキュリティ対策における留意事項 4
第2部　EC 加盟店におけるセキュリティ対策 5
0. EC 加盟店におけるセキュリティ対策の概要 5
1. 脆弱性対策 5
1－1. EC サイトのシステム管理画面 5
1－1－1. システム管理画面のアクセス制限不備と管理者の ID/パスワード管理不足 5
1－2. EC サイトの設定の不備 6
1－2－1. データディレクトリの露見に伴う設定の不備 6
1－3. 既知の脆弱性 6
1－3－1. 脆弱性診断又はペネトレーションテストの定期実施 6
1－3－2. SQL インジェクションの脆弱性 6
1－3－3. クロスサイト・スクリプティングの脆弱性 7
1－4. マルウェア、ウイルスなどの不正ファイル 7
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 8
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 8
2. EMV 3-D セキュア 10
3. 不正ログイン対策（決済前の対策） 10
3－1. 会員登録時の対策 11
3－2. 会員ログイン時の対策 11
3－3. 属性情報変更時の対策 13
4. 決済時・決済後の対策 14
4－1. 決済時の対策 14
4－2. 決済後の対策 15
第3部　その他の留意事項 16
1. その他加盟店における対策 16
1－1. MO・TO 取引取扱加盟店の不正利用対策 16
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 17
2. 特定の商材における対策 17
2－1. 相対的にリスクの高い商材の不正利用対策 17
2－1－1. デジタルコンテンツの不正利用対策 18
3. 特定の対策に関する補足説明 19
3－1. 属性・行動分析について 19
3－1－1. 前提 19

3－1－2. 継続的な運用の見直し..... 20
3－1－3. ネガティブ情報の蓄積と活用 20
3－1－4. トレーニングと教育、体制の整備..... 20
4. 最後に..... 21
5. 参考資料..... 21
改訂履歴..... 22

【附属文書 20 関連文書一覧】

附属文書一覧（GL6.0版）									
附属文書番号	別紙	文書名	該当指針対策						一般公開資料（○：JCA一般HP掲載）
			カード情報保護		不正利用対策				
			非保持化	脆弱性	IC化	EMV3DS	不正ﾛｸﾞｲﾝ	不正顕在化	
附属文書14		EMV 3-Dセキュア導入ガイド				●		○	○
		【EMV 3-Dセキュア】統合版_AReq設定項目及び3RIの仕様・ユースケース（公表版）				○		○	○
		加盟店におけるEMV 3-Dセキュア導入・運用ガイダンスに関するFAQ				○		○	○
附属文書17		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19		属性・行動分析のポリシー文書（公開版は、附属文書20の文中に記載）				○	○	○	
附属文書20		EC加盟店におけるセキュリティ対策　導入ガイド		●		○	●	●	○
	別紙ａ	EC加盟店におけるセキュリティ対策一覧		○		○	○	●	○
	別紙ｂ	EC加盟店におけるセキュリティ対策　導入ガイド　補足資料		○			○		○
	別紙ｃ	ＥＣサイトのセキュリティ対策実施状況申告書（例）		○		○	○		○
		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		○		○	○		○
	別紙ｄ	不正利用の抑止を実現する加盟店の事例集				○	○	○	○

●：各指針対策における対応及び対策を理解・検討するためのメインとなる文書

・別紙ａ「EC 加盟店におけるセキュリティ対策一覧」：本書記載のセキュリティ対策を網羅し、EC 加盟店が講ずるべきセキュリティ対策を対策導入の場面ごとに有効な対策を具体的に一覧として示すものであり、対策の検討・導入に活用いただくもの

・別紙ｂ「EC 加盟店におけるセキュリティ対策　導入ガイド　補足資料」：本書記載の「脆弱性対策」「不正利用対策」の理解促進のため、図表を用いて視覚的にわかりやすく説明することにより、EC 加盟店及び関係事業者のセキュリティ対策の理解と意識の向上を図り、対策強化による不正利用被害の防止を目的として解説したもの

・別紙ｃ「EC サイトのセキュリティ対策実施状況申告書（例）」：新規 EC 加盟店の契約時調査及び既存 EC 加盟店の定期調査における指針対策の導入状況調査として加盟店から申告して頂く内容の例示

・別紙ｄ「不正利用の抑止を実現する加盟店の事例集」：不正利用の抑制を実現した加盟店の具体的な取り組み内容の事例集

0. 本書の目的

クレジットカード取引（以下「カード取引」という。）の不正利用は、EC 加盟店のシステムや Web サイトの脆弱性対策の不備を原因としたカード番号等の情報漏えい事案、クレジットカード番号の採番の規則性を悪用して機械的にクレジットカード番号を生成する手法（クレジットマスター）によって大量にカード番号を生成し、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確認を行う悪質な有効性確認、EC加盟店やカード会社を模したフィッシングサイトによるカード情報や会員のログインアカウントなどの窃取による不正利用の発生が顕著となっている。

このような状況を踏まえ、クレジット取引セキュリティ対策協議会（以下「協議会」という。）では、「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。）」に基づき、カード取引に関わる全てのステークホルダーの各々に求められるセキュリティ対策を講じることを求めており、セキュリティガイドライン【6.0版】からは、EC 加盟店における指針対策として、カード情報保護対策においては「EC加盟店のシステム及びWeb サイトの『脆弱性対策』の実施」、不正利用対策においては「EMV 3-D セキュアの導入」「適切な不正ログイン対策の実施」、更に「不正顕在化加盟店は、類似の不正利用の発生の防止」を追加した。

本書は、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（以下「情報漏えい」という。）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。

さらに対策の検討・導入にあたっては、カード会社（アクワイアラー）や PSP 及びクレジットカード取引関係事業者と連携し、本書に記載の対策を網羅した別紙 a「EC 加盟店におけるセキュリティ対策一覧」を活用し、適切な対応を行っていただきたい。

なお、別紙 b「EC 加盟店におけるセキュリティ対策 導入ガイド 補足資料」は、本書のセキュリティ対策の理解促進のため、図表を用いて視覚的に分かりやすく説明した資料であり、参考にしていただきたい。

また、別紙d「不正利用の抑止を実現する加盟店の事例集」は、日本クレジット協会のインフラ整備部会調査により取りまとめられた、不正利用の抑制を実現した加盟店の具体的な取り組み内容を事例集として示す資料である。プロダクトの導入だけでなく、属性・行動分析の運用を中心に組織体制面についても説明されている事例となるため、不正利用対策の検討にあたって参考にしていただきたい。

最後に、本書を本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いただいており、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

EC 加盟店は、割賦販売法により、「クレジットカード番号等の適切な管理」（第 35 条の 16 第1項）及び「クレジットカード番号等の不正な利用の防止（以下「不正利用防止」という。）」（第 35 条の 17 の 15）をするための措置を講じることが義務付けられている。

「割賦販売法（後払分野）に基づく監督の基本方針」において、セキュリティガイドラインに掲げられる措置が割賦販売法で義務付けられているクレジットカード番号等の適切な管理及び不正利用防止のための措置の実務上の指針として位置付けられている。セキュリティ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適切に講じている場合には、クレジットカード番号等の漏えい等の事故及び不正利用を防止する措置として、割賦販売法に

規定する「必要かつ適切な措置」が講じられていると見なされており、セキュリティガイドラインにおいては【指針対策】としてこれらの措置を記載している。

この EC 加盟店の【指針対策】は、割賦販売法で義務付けられているクレジットカード番号等の漏えい等の事故及び不正利用を防止するための措置の実務上の指針として位置付けられているものであるが、被害を防止するためには、EC 加盟店だけでなく、クレジットカード取引関係事業者それぞれが、EC 加盟店の【指針対策】の内容を理解し、各々がその【指針対策】の実施及び EC 加盟店の対策の導入・運用に対してサポートを行うことが必要である。

【表：EC 加盟店における割賦販売法に基づく指針対策】

	セキュリティガイドライン【6.0 版】(2025 年 4 月)
カード情報保護対策	・EC 加盟店のシステム及び Web サイトの「脆弱性対策」◎
	・カード情報を保持しない非保持化、又はカード情報を保持する場合は PCI DSS に準拠
不正利用対策	・EMV 3-D セキュアの導入◎
	・適切な不正ログイン対策の実施◎
	・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、適切な対策の追加導入(不正顕在化加盟店)◎
	・オーソリゼーション処理の体制整備
	・加盟店契約上の善良なる管理者の注意義務の履行

◎:2025 年 4 月に新たに追加、変更された指針対策

最近の傾向では、非保持化を実現した加盟店においても、EC 加盟店のシステムや Web サイトの「脆弱性対策」が継続的に実施されていないことにより、外部からの不正アクセスやウイルス感染、システムの改ざんを許し、クレジットカード情報を不正に窃取される情報漏えいが主流となりつつあり、非保持化を実現していても、情報漏えいに繋がり得ることを十分認識した上で、セキュリティ対策の一層の強化が求められる。

また、EC 加盟店等からの情報漏えいが断続的に発生していることに加え、カード会員からカード番号、セキュリティコード、EC サイト利用者のログイン ID・パスワード等(以下「カード番号等」という)を巧みに窃取する手口である「フィッシング」、クレジットカード番号の採番の規則性を悪用し機械的に生成する手法(クレジットマスター)によって大量にカード番号を生成し、それらを EC 加盟店での利用を通じて実際に利用できるカード番号か確認を行う手口等、手口が巧妙化している。

このため EC 加盟店の取扱商品やスキーム等により、不正利用が発生する場面や不正利用の手口が異なることから、不正ログインがされる「カード決済前」、なりすましによるカードの不正利用がされる「カード決済時」、不正に購入した商品が配送・転売される「カード決済後」という「不正利用の流れ」を考慮した適切な対策を導入することが重要である。これを「線の考え方」に基づく対策の導入という。

2. セキュリティ対策における留意事項

割賦販売法では、EC 加盟店がカード番号等の適切な管理のための措置を講じることを義務として定めている。したがって、EC 加盟店が EC サイト構築や運用・保守業務を外部に委託する場合は、当該委託先に対して、委託

先自身の PCIDSS 準拠等の必要なカード情報保護対策や EC 加盟店が行うべき「脆弱性対策」「不正利用対策」を理解した上で、構築・運用を行うことを求める。

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り、オープンソースソフトウェアを利用している場合は、導入後は EC 加盟店の責任でセキュリティパッチ更新等の対応をする必要がある。

なお、EC 加盟店で情報漏えいが発生した場合には、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する必要がある。

また、自社の Web サイトを模したフィッシングサイトを確認したときは、当該フィッシングサイトの無効化等の手続をすることが望ましい。

第2部 EC 加盟店におけるセキュリティ対策

0. EC 加盟店におけるセキュリティ対策の概要

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. 脆弱性対策

EC サイトからのカード番号等の情報漏えい事例の多くは、オープンソースソフトウェアを主とする EC サイト構築パッケージや CMS（Contents Management System）の設定不備及び脆弱性を狙った攻撃により発生しており、スクリプトコンテンツ改ざん等により、会員が EC サイトに入力した情報が継続的に漏えいし続けるケースも確認されている。また、EC サイトからのカード番号等の情報漏えいだけではなく、攻撃者が他の方法で入手したカード番号等の有効性を確認するために、EC サイトのクレジットカード登録・決済機能を悪用する手口も発生している。このような事例等を踏まえ、不正侵入及び情報の窃取のリスクとその対策は以下の通りである。

1－1. EC サイトのシステム管理画面

1－1－1. システム管理画面のアクセス制限不備と管理者の ID/パスワード管理不足

(1) 攻撃リスク

①接続元を制限せず、管理画面の URL が admin など推測されやすいものになっていることにより、攻撃者から管理画面へ容易にアクセスされてしまう。

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) 対策

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管理画面の URL を推測困難なものへ変更する。更に admin フォルダを削除する。

④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。
⑤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。
⑦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

1－2－1. データディレクトリの露見に伴う設定の不備

(1) 攻撃リスク

①EC サイトの初期構築時に、重要なファイルが配置された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 が窃取されてしまう。
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、データの窃取や不正ファイルが混入される。

(2) 対策

①公開ディレクトリには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を配置しない。
②Web 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。

1－3. 既知の脆弱性

1－3－1. 脆弱性診断又はペネトレーションテストの定期実施

脆弱性診断は、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。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、情報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

データベースと連携した Web アプリケーションの多くは、利用者からの入力情報を基に SQL 文（データベースへの命令文）を組み立てている。ここで SQL 文の組立方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性がある。このような問題を「SQL インジェクションの脆弱性」と呼び、問題を悪用した攻撃を、「SQL インジェクション攻撃」という。

(1) 攻撃リスク

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) 対策

①最新のプラグインの使用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。）

②Web アプリケーションを開発又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。コーディングの脆弱性の対処にあたっては、「安全なウェブサイトの作り方」（IPA）を参考に対策を行う。

1－3－3. クロスサイト・スクリプティングの脆弱性

Web 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、Web 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、Web ページとして出力するものがある。ここで、Web ページへの出力処理に問題がある場合、その Web 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、Web サイト自体に対してではなく、その Web サイトのページを閲覧しているユーザーに及ぶ。

Web 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) 攻撃リスク

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) 対策

①最新のプラグインの使用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。）

②Web アプリケーションを開発又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。コーディングの脆弱性の対処にあたっては、「安全なウェブサイトの作り方」（IPA）を参考に対策を行う。

1－4. マルウェア、ウイルスなどの不正ファイル

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）であり、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である。

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ことを未然に防ぐためのソフトウェアで、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となる。

業務端末へのウイルスの侵入を起点にサーバへ感染拡大するケースなども考えられるため、業務端末とサーバへのマルウェア対策を講じることが重要である。

(1)攻撃リスク

①ウイルス対策ソフトの更新手続漏れ等により無防備となった業務端末へのウイルスの侵入。

(2)対策

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

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とは、カード番号等の採番の規則性を悪用し、機械的にクレジットカード番号を生成する手口である。

また、悪質な有効性確認とは、クレジットマスターで生成したカード情報やフィッシング等で窃取したカード情報を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)攻撃リスク

①「なりすまし」による会員登録時、又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、有効なカード会員データを窃取される恐れがある。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で生成したカード番号やフィッシング等で窃取したカード番号等をもとに悪質な有効性確認を行われ、有効なカード会員データを窃取される恐れがある。

②攻撃者は、日本国内の IP アドレスよりも、海外の IP アドレスから悪質な有効性確認を実施することが多い。

(2)対策

①「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。

②「同一アカウントからの入力制限」「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。

③EMV 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。

④有効性確認の回数制限を設けるなどの対策を行う。

【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紙 a_4. 決済時/決済後の対策を参照）

クレジットカード決済の登録/変更の機能悪用への対策

別紙 a の分類	No.	対策分類	対策（決済時）
4.決済時/決済後の対策	1	アクセス制限	不審な IP アドレスからのアクセス制限
	2		スロットリング
	3	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証
	4		その他有効な Bot 対策ツールの導入
	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)	
	6	機能制限	同一アカウントからの入力制限	アカウントに紐づけられたカード番号の登録・変更のリトライ回数の制限
	7			同一カード番号での複数アカウント保有の禁止
	8			同一アカウントのカードの登録数を制限
	9	本人認証/認証強化	デバイスフィンガープリント	
	10		多要素認証(2 要素認証)/FIDO2・パスキーによる認証	
	11		2 段階認証	
	12		SMS 認証/電話番号認証	
	13		生体認証	
	14		認証サービス	
	15		券面認証(セキュリティコード入力必須)	
	16	不正検知	属性・行動分析	
	17		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

別紙 a の分類	No.	対策分類	対策 (決済時)
4.決済時/決済後の対策	1	アクセス制限	不審な IP アドレスからのアクセス制限
	2		スロットリング
	3	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証
	4		その他有効な Bot 対策ツールの導入
	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)
	14	本人認証/認証強化	認証サービス
	15		券面認証(セキュリティコード入力必須)
	16	不正検知	属性・行動分析
	17		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情報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 PSP 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、「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. EMV 3-D セキュア

EMV 3-D セキュアはカード決済時の対策として有効な対策である。EMV 3-D セキュアの導入・運用の詳細については、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

3. 不正ログイン対策（決済前の対策）

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いう。

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る。

(2) フィッシングメール等で窃取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。

(3) 不正ログインによりカード番号や属性情報の変更が可能となり不正利用される。

なお、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。

【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. 会員ログイン時	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、窃取した属性情報・カード情報等を利用し、不正なアカウントを作成の上、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、会員登録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情報変更（連絡先、配送先住所等の変更）を行うことも想定される。このため、会員ログイン時、属性情報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と対策を説明する。

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、会員ログイン時に、ID/パスワード/姓カナ、名カナを入力させるなど、会員ログイン時に本人認証の強化をするなどの工夫が必要となる。

3－1. 会員登録時の対策

(1)攻撃リスク

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窃取や他社の情報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」することが可能であり、不正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。)

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)対策

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。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、確認を行う。

②「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。

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 2 段階認証などによる本人認証を行う。

④属性・行動分析を利用する。

【表:会員登録時の不正事例】

事例	不正の手口	不正事例（会員登録時）
1	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、不正なアカウントを作成の上、盗用したカード番号等を支払方法として登録し、不正利用が行われる。

【表:会員登録時の対策】(各対策内容の詳細については別紙 a_3. 不正ログイン対策(決済前の対策)を参照)

別紙 a の分類	No.	対策分類	対策（会員登録時）
3.不正ログイン対策(決済前の対策)	1	アクセス制限	不審な IP アドレスからのアクセス制限
	2		スロットリング
	4	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証
	5		その他有効な Bot 対策ツールの導入
	6	本人認証/認証強化	eKYC
	7		デバイスフィンガープリント
	13		姓カナ、名カナ入力値の検証
	16	不正検知	属性・行動分析

3－2. 会員ログイン時の対策

(1)攻撃リスク

①会員用のログイン画面は、公開する必要があり、アクセス制限が難しく、このような状況を悪用し、フィッシングメールや他社の情報漏えい事案などで窃取した「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、更に静的パスワードはパスワードクラッキング等により推測されやすい。また、「なりすまし」による不正ログインが実行されても、正常なログインであるため、EC 加盟店は不正ログインに気づきにくい。

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)対策

①「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。

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」「スロットリング」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、2 段階認証などによる本人認証を行う。

④会員ログイン時のメールや SMS 通知などを行う。

⑤その他、「デバイスフィンガープリント」等を利用する。

【表:会員ログイン時の不正事例】

事例	不正の手口	不正事例（会員ログイン時）
2	アカウント乗っ取り	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される。

【表:会員ログイン時の対策】(各対策内容の詳細については別紙 a_3.不正ログイン対策(決済前の対策)を参照)

別紙 a の分類	No.	対策分類	対策（会員ログイン時）
3.不正ログイン対策(決済前の対策)	1	アクセス制限	不審な IP アドレスからのアクセス制限
	2		スロットリング
	3		同一アカウントのログイン試行回数の制限強化
	4	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証
	5		その他有効な Bot 対策ツールの導入
	7	本人認証/認証強化	デバイスフィンガープリント
	8		単純パスワード、短いパスワードの排除
	9		多要素認証(2 要素認証)/FIDO2・パスキーによる認証
	10		2 段階認証
	11		SMS 認証/電話番号認証
	12		(会員ログイン時の)メールや SMS 通知
	13		姓カナ、名カナ入力値の検証

	14		デバイス認証
	15		生体認証
	16	不正検知	属性・行動分析

3－3. 属性情報変更時の対策

(1)攻撃リスク

①不正ログインにより、攻撃者が窃取した真正なカード会員の属性情報を変更し、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)対策

①属性情報変更時の個人情報(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く、確認を行う。

②「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。

③属性情報変更時には、元々登録されていた本人に対して気づきを与えられるように 2 段階認証などによる本人認証を行う。

④属性・行動分析や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	不正の手口	不正事例 (属性情報変更時)
3	アカウント乗っ取り	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がされたのちに、属性情報を変更され、不正利用が行われる。

【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紙 a_3.不正ログイン対策(決済前の対策)を参照)

別紙 a の分類	No.	対策分類	対策 (属性情報変更時)
3.不正ログイン対策(決済前の対策)	1	アクセス制限	不審な IP アドレスからのアクセス制限
	7	本人認証/認証強化	デバイスフィンガープリント
	9		多要素認証(2 要素認証)/FIDO2・パスキーによる認証
	10		2 段階認証
	11		SMS 認証/電話番号認証
	12		(属性情報変更時の)メールや SMS 通知
	14		デバイス認証
	15		生体認証

	16	不正検知	属性・行動分析

4. 決済時・決済後の対策

セキュリティガイドライン【6.0 版】からは、EC 加盟店の指針対策として、これまでの「オーソリゼーション処理の体制整備」、「加盟店契約上の善良なる管理者の注意義務の履行」に追加して、「線の考え方」に基づき、決済前の対策である「適切な不正ログイン対策の実施」、決済時の対策である「EMV 3-D セキュアの導入」を求めることとし、これらの対策を不正利用対策の中心とすることとした。

しかし、不正の手口は年々巧妙化してきており、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、以下の不正利用の流れの中では、決済時の EMV 3-D セキュアだけで、すべての被害を防止できるものではない。

(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情報等が窃取され攻撃者により不正利用される。

(2) 窃取されたカード情報等を利用して、「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、又は転送を行う配送会社へ商品が配送される。

(4) 不正利用により窃取された商品は、海外又は国内での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。

上記のような不正取引の実態を踏まえ、セキュリティガイドラインに記載の「線の考え方」に基づく対策のうち、EC 加盟店が自ら対策を講じることが可能な「決済時」と「決済後」に分けて、場面ごとのリスクと対策を下記に示す。

4－1. 決済時の対策

(1) 攻撃リスク

①窃取された真正なカード情報等利用して、決済時に「なりすまし」による商品購入が行われる。

②不正なアカウント登録、あるいは正規のアカウントに不正ログインをして商品を購入される。

(2) 対策

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（イシュアー）の本人認証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（イシュアー）の確認を行う。

③決済時に属性・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。

④PSP または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。

【表：決済時の対策】（各対策内容の詳細については別紙 a_4.決済時/決済後の対策を参照）

クレジットカード決済の登録/変更を含む決済時の場面への対策

別紙 a の分類	No.	対策分類	対策（決済時）

4.決済時/ 決済後の対策	1	アクセス制限	不審な IP アドレスからのアクセス制限	
	2		スロットリング	
	3	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証	
	4		その他有効な Bot 対策ツールの導入	
	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)	
	6	機能制限	同一アカウントからの入力制限	アカウントに紐づけられたカード番号の登録・変更のリトライ回数の制限
	7			同一カード番号での複数アカウント保有の禁止
	8			同一アカウントのカードの登録数を制限
	9	本人認証/ 認証強化	デバイスフィンガープリント	
	10		多要素認証(2 要素認証)/FIDO2・パスキーによる認証	
	11		2 段階認証	
	12		SMS 認証/電話番号認証	
	13		生体認証	
	14		認証サービス	
	15		券面認証(セキュリティコード入力必須)	
	16	不正検知	属性・行動分析	
	17		ベロシティチェック	

ゲスト購入時の決済時の対策

別紙 a の分類	No.	対策分類	対策 (決済時)
4.決済時/ 決済後の対策	1	アクセス制限	不審な IP アドレスからのアクセス制限
	2		スロットリング
	3	Bot 対策	CAPTCHA 認証/reCAPTCHA 認証
	4		その他有効な Bot 対策ツールの導入
	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)
	14	本人認証/ 認証強化	認証サービス
	15		券面認証(セキュリティコード入力必須)
	16	不正検知	属性・行動分析
	17		ベロシティチェック

4－2. 決済後の対策

(1)攻撃リスク

①購入し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やオンラインチケットなどの配送を伴わない商品については、決済後即時又は決済後比較的短期間に利用される。

(2)対策

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「氏名表記」「姓名カナ表記」「住所」「電話番号」等の規則性や組合せを担当者による目視などで確認又は照合し、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、カード会社からのEC加盟店に対する配送停止・配送保留の要請に協力する。

③属性・行動分析を活用し、「氏名表記」「姓名カナ表記」「住所」「電話番号」の規則性や組合せを確認の上、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の強化に努める。

⑤配送を伴わない商品については、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(配送停止依頼含む)に基づく、アカウントの停止等による購入された権利の無効化、宿泊等の予約サービスやチケット販売等における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。

【表:決済後の対策】(各対策内容の詳細については別紙 a_4.決済時/決済後の対策を参照)

<table>
<tr><th>別紙 a の分類</th><th>No.</th><th>対策分類</th><th colspan="3">対策 (決済後)</th></tr>
<tr><td rowspan="8">4.決済時/
決済後の対策</td><td>16</td><td>不正検知</td><td colspan="3">属性・行動分析</td></tr>
<tr><td>18</td><td rowspan="7">被害防止</td><td colspan="3">配送先情報の活用</td></tr>
<tr><td>19</td><td rowspan="6">配送保留/配送(アカウント)停止</td><td rowspan="2">配送を伴う場合</td><td>カード会社による配送停止・配送保留の要請への協力</td></tr>
<tr><td>20</td><td>属性・行動分析の活用</td></tr>
<tr><td>21</td><td rowspan="3">配送を伴わない場合</td><td>転売防止対策の実施</td></tr>
<tr><td>22</td><td>属性・行動分析の活用</td></tr>
<tr><td>23</td><td>サービスの提供(宿泊、チケット等)のキャンセルの実施・他の支払方法への変更</td></tr>
</table>

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 取引取扱加盟店の不正利用対策

非対面取引でありながら、決済時に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、その他の不正利用対策が必要となる。

(1)攻撃リスク

①不正な注文情報により申込みがされて、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)対策

①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」の規則性や組合せを確認または照合し、加盟店担当者が目視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、PSP 又はサービス提供事業者の属性・行動分析(又は不正配送先情報)の活用、電話番号の使用/未使用確認サービスの利用、配送先の名前の確認などを行う。

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

「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. 相対的にリスクの高い商材の不正利用対策

相対的にリスクの高い商材は、不正利用の発生リスクが高い商材であることから、追加導入する対策や既に導入している対策の設定項目の追加・変更、チューニング(不正判定レベルの最適化)においては、リスクを認識した上での対応が必要である。

また、一つの加盟店が様々な商品を取り扱っているいわゆる「総合通販」の非対面取引加盟店において、相対的にリスクの高い商材を取り扱う場合はその商材のリスクに応じた不正利用対策を追加導入することを推奨する。

相対的にリスクの高い商材としては下表に掲載の商材が想定されるが、この限りではない。

相対的にリスクが高い商材	参考解説
デジタルコンテンツ (オンラインゲームを含む)	記録媒体(CD-ROM、DVD等)に保存された商品の購入者への配送ではなく、ダウンロード配信により販売されるものをいう(但し、毎月の請求は月会費のみの定額請求で追加請求の発生しない取引は除く)。
家電(家電量販店)	家電製品を大量に仕入れることにより、消費者へより安価に提供することを基本とする家電量販店が、ネット通販として立ち上げた店舗及びネット専業として事業展開している店舗が販売するものをいう。
電子マネー	貨幣価値を電子化したいわゆる電子マネーをネット通販により販売するものをいう。
チケット	乗車券、航空券、入場券、観覧券といったいわゆるチケットをネット通販で取り扱うものをいう(但し、転売されることが想定されない商品は除く) 。
宿泊予約サービス	宿泊施設の予約手配を提供する宿泊予約サイトによる、クレジットカード決済を伴った宿泊予約サービスをいう(宿泊施設等が直接運営し、宿泊予約の受付等を行うサイトは対象に含まれない)。

「宿泊予約サービスにおけるカード情報を使用した不正手口の実態」

クレジットカード情報を盗み出した犯人(グループ)は、インターネット上又は口コミ等で自称旅行代理店として、不正な旅行商品の宣伝を行い、日本語や日本文化に詳しいことや支払いの割引を主張することなどにより、特に、日本への旅行を計画している海外の旅行者にアピールしているとみられる。

①犯人(グループ)は、旅行者から宿泊等の旅行の申込を受け付ける。
②依頼された旅行の手配を各種オンラインの宿泊予約サービスで行う際に、窃取したクレジットカード情報を使用して決済を行う。
③カードの名義人及びクレジットカード会社が情報窃取に気付いていなければ、通常通り決済は完了する。
④決済の完了により、予約を受け付けた旅行事業者等から宿泊施設等に予約者の情報が送信される。
⑤犯人が予約情報を旅行者に伝達することで、旅行者は、犯人に宿泊予約サービスの費用を支払う。
⑥旅行者は犯人からの予約情報をもとに旅行することになるが、旅行事業者・クレジットカード会社等で当該宿泊予約サービス利用における不正決済が発覚することでトラブルに巻き込まれるケースもある。



「不正トラベルの手口の実態」(日本サイバー犯罪対策センターの発表資料より)

相対的にリスクの高い商材に追加導入する対策は、本書の第2部 EC 加盟店におけるセキュリティ対策「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」より適切な対策を追加導入するとともに、既に属性・行動分析等を導入している場合は、設定項目の追加・変更、チューニング(不正判定レベルの最適化)による「対策の強化」を推奨する。

2－1－1. 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、決済後すぐにダウンロードが可能な商材のため、不正利用対策の難易度は高いが、以下のようなリスクと対策がある。

(1) 攻撃リスク

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) 対策

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停止。

②決済後すぐにダウンロードが可能な商材については、不正ログイン対策(決済前の対策)と決済時(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」という。)をもとに、当該デバイスからの取引を拒否できる。また、属性・行動分析によっては、不正なログイン ID/パスワードのネガ情報も利用可能

であるため、アクセス拒否やログイン ID の削除を行う。

④決済後に直ぐに発券もしくはダウンロードできないようにすること、またカード会社からの配送停止依頼等で不正利用を検知した場合に当該取引を利用不可にすることが有効である。

3. 特定の対策に関する補足説明

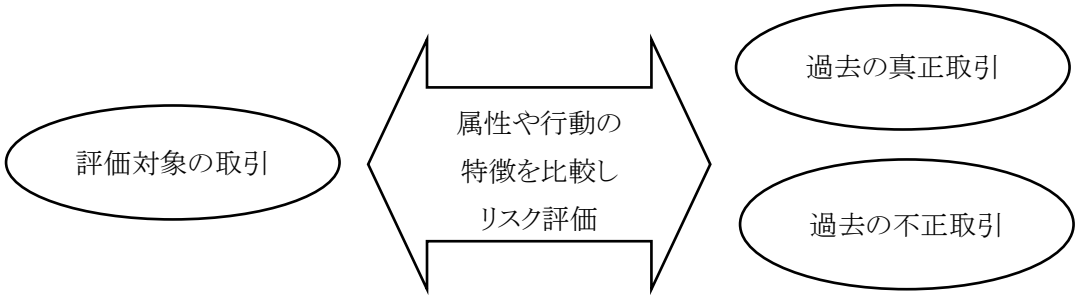
3－1. 属性・行動分析について

本書では、「属性・行動分析ガイダンス【附属文書 19】」の「公表版」としての内容を記載する。関係者版の確認が必要な場合は、契約先のカード会社または PSP に確認すること。

3－1－1. 前提

属性・行動分析は、過去の取引情報から、不正（真正）に関する属性や行動の特徴を見出し、新たな取引と比較することでその取引のリスク評価を行う手法であり、「線の考え方」における「決済前」「決済時」「決済後」の全てのタイミングにおいて効果的なセキュリティ対策である。

【図：属性・行動分析の概念】



ただし、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や不正取引情報のインプット、業種や不正利用の動向に応じた適切な設定、調整等を行う必要がある。また、不正取引情報の収集、共有、保存においては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、属性・行動分析の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、不正利用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、PSP）が共通認識をもって対応する必要がある。また、属性・行動分析の運用にあたって、専門の部署や担当者を設置できない等十分な人員が確保できない場合においても、限られた人的リソースを有効活用できるよう加盟店ごとに組織体制の整備を工夫することが望ましい。組織体制の整備にあたっては、不正利用の抑制を実現する加盟店の取組について取りまとめられた別紙 d「不正利用の抑止を実現する加盟店の事例集」も参考にされたい。

3－1－2. 継続的な運用の見直し

属性・行動分析の効率的な運用を確保し、セキュリティ対策の効果を最適化するためには、サービス提供事業者とEC 加盟店との間で、属性・行動分析の運用見直しと、改善が継続的に行われることが重要である。

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。

(4) EMV 3-D セキュアを実行した取引についても、EC 加盟店が知りうる不正取引・真正取引の情報をサービス提供事業者に情報提供する。

(5) 自社での不正利用の発生状況を適切に把握するため、加盟店が不正取引であることを認識できない EMV 3-D セキュアで認証された取引等も含めて、カード会社（アクワイアラー）・PSP に対し、カード会社（イシュアー）から提供される不正利用情報の共有を求める。

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において配慮を行いつつ、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上で重要となる。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。ネガ情報には、前述のカード会社（イシュアー）に対し、提供を要請した不正利用情報も含まれる点に留意すること。

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。属性・行動分析サービスによっては、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。

EC 加盟店において必要な自社内の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

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. 最後に

技術の進歩や加盟店のスキーム等に応じて、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、EC 加盟店においては非保持化の実現や EMV 3-Dセキュアの導入に加えて、リスクに応じたセキュリティ対策を適切に導入し、状況に応じて見直すことが求められる。

一つの EC 加盟店で情報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、業界全体として相当額の損失を招くこととなる。特にオープンソースソフトウェアを利用している EC 加盟店は、当該ソフトウェア提供者からの注意喚起に留意するとともに、積極的に最新情報を取得し、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。各オープンソースソフトウェアのシステム開発会社が公表しているガイダンス等を活用することも有効である。

万が一、情報漏えいの疑いが生じた場合は、速やかに契約しているカード会社(アクワイアラー)や PSP に連絡の上、被害拡大防止のための対応を実施することが必要となる。

5. 参考資料

- 経済産業省 : 2019 年 12 月 20 日

株式会社イーシーキューブが提供する構築パッケージ「EC-CUBE」の脆弱性等について(注意喚起)

https://warp.da.ndl.go.jp/info:ndljp/pid/11433651/www.meti.go.jp/press/2019/12/20191220013/20191220013.html

- 株式会社イーシーキューブ

01_ご利用の EC-CUBE のバージョンを確認する

EC-CUBE のバージョンにより対応・対策が異なりますので、まずは EC-CUBE のバージョンをご確認ください。

https://www.ec-cube.net/security/#securit_flow02

- IPA(Information-technology Promotion Agency, Japan 独立行政法人情報処理推進機構)

安全なウェブサイトの作り方

https://www.ipa.go.jp/security/vuln/websecurity/index.html

「EC サイト構築・運用セキュリティガイドライン」

https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

改訂履歴

改訂時期	バージョン	概要
2024 年 3 月	1.0 版	・新規作成
2025 年 3 月	2.0 版	・脆弱性対策及び不正ログイン対策の指針対策化に伴い、記載内容の変更。 ・旧附属文書 13「不正利用対策 4 方策の具体的な基準・考え方について」より、第 3 部 2-1 として、相対的にリスクの高い商材の不正利用対策の章を追加。 ・資料 1 別表を別紙 a「EC 加盟店におけるセキュリティ対策一覧 1.0 版」として改訂。 ・旧附属文書 21「セキュリティ・チェックリスト」を改訂の上、別紙 b として統合。 ・加盟店調査において加盟店から申告いただく内容の参考例として、別紙 c「EC サイトのセキュリティ対策実施状況申告書（例）」を追加。 ・その他文言等修正。
2026 年 3 月	2.1 版	・不正利用の抑止を実現した加盟店の事例集として、別紙 d「不正利用の抑止を実現する加盟店の事例集」を追加。 ・各事業者から挙げられた課題の追記（補足）。 ・問合せが多い事項の補足。

以上