# EC決済セキュリティ チェックリスト

「カード情報を持たない」を決めたあとに、必ず確認しておきたい項目

**作成：**PJ-T&C合同会社 ｜ **版：**2026年10月版（v3・最終） ｜ **対象：**EC事業者の経営者・運営担当者 ｜ **貴社名：**＿＿＿＿＿＿＿＿ **確認日：**＿＿＿／＿＿＿／＿＿＿

> クレジットカード情報を自社システムで保持せず、決済代行サービスに任せる「非保持化」は、被害の範囲を小さくするうえで有効な方針です。一方で、2025年後半から2026年に公表された国内EC事業者の漏洩事例には、カード情報の非保持化が行われていたと説明されている事例や、カード番号全桁が対象外だった事例が含まれています。このチェックリストは、非保持化とあわせて確認しておきたい設定を、使っている決済サービス別に整理したものです。すべてを一度に行う必要はありません。優先度の高いものから、順に進めてください。

**優先度** A ＝最初に確認 B ＝次に確認 C ＝体制が整ったら　**担当** 経営＝経営者・責任者 運用＝運営担当 制作＝制作会社・開発者
**根拠** GL＝クレジットカード・セキュリティガイドライン等の制度上の要請 仕様＝決済サービスの利用条件・公式推奨 推奨＝一般的なセキュリティ上の推奨（法令上の義務ではない）

## 1. 決済方式の確認（全サービス共通）

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | カード番号・有効期限・セキュリティコードを、自社の機器・ネットワークで保存・処理・通過させていない（制度上の「非保持化」が完了している。保存しないだけでは不十分） | 制作 | GL |
| ☐ | A | 購入者が決済事業者のホストするページへ遷移してカード情報を入力する方式（Stripe-hosted Checkout、PayPal標準決済、Shopifyチェックアウト等）を使っている。※iframe埋め込み型は決済事業者のオリジンを使う場合があるため、ドメインではなく「遷移するか・埋め込むか」で判別する | 制作 | 推奨 |
| ☐ | B | 自社ページ内に決済事業者のフォームを埋め込む方式（Stripe Elements / Payment Element、PayPal Advanced Card Payments等）を使っている場合、その理由が明確で、「3. 決済ページの改ざん対策」とSAQ A適格条件の確認を実施している | 制作 | 推奨 |
| ☐ | A | EMV 3-Dセキュア（3Dセキュア2.0）が有効になっている。免除対象の取引がある場合、その内容と、免除取引にはライアビリティシフトが適用されないことを把握している | 運用 | GL |
| ☐ | B | 決済代行会社・プラットフォームからの連絡先（セキュリティ通知の宛先メール）が、現在在籍している担当者のものになっている | 運用 | 推奨 |

クレジットカード・セキュリティガイドラインでは、2025年3月末までに原則として全EC加盟店でEMV 3-Dセキュアの導入が求められています（適用除外あり）。未導入の場合は、決済代行会社に状況を確認してください。非保持化によりPCI DSSの準拠範囲を削減できる場合が多い一方、適用される自己問診票（SAQ）は実装構成とアクワイアラー等の判断によります。

## 2. 管理画面とアカウントの防御（自社サイト側）

クレジットカード・セキュリティガイドライン【6.1版】（2026年3月）は、EC加盟店に対して管理画面のアクセス制限・多要素認証・脆弱性対策などを求めています。2026年の事例には、スタッフアカウントの乗っ取りや、基盤側の侵害で店舗管理画面のログイン情報が対象となったものが含まれています。

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | サイトの管理画面（WordPress、EC-CUBE等）にログインできる全員が、多要素認証を設定している | 運用 | GL |
| ☐ | A | 管理画面のURLにIPアドレス制限をかけている。固定IPがなく難しい場合は、VPN経由への限定や追加認証など実効性のあるアクセス制限を設けている | 制作 | GL |
| ☐ | A | 退職者、契約終了した制作会社・委託先のアカウントが削除されている（定期的に棚卸しする） | 経営 | GL |
| ☐ | B | ログイン失敗が一定回数（目安10回以下）続いた場合に、アカウントがロックされる設定になっている | 制作 | GL |
| ☐ | B | 各担当者に「管理者」ではなく業務に必要な最小限の権限を割り当てている | 経営 | 推奨 |
| ☐ | B | CMS本体・プラグイン・テーマを定期的に更新し、使っていないプラグインは削除している | 制作 | GL |
| ☐ | C | 脆弱性診断またはペネトレーションテストを定期的に、また大きな改修時には必要に応じて実施している（頻度は環境・リスク・契約上の要求に応じて決める） | 経営 | GL |
| ☐ | C | 管理画面へのログイン履歴を保存し、見慣れない時間帯・場所からのログインを確認できる | 制作 | 推奨 |

**多要素認証の方式について**
多要素認証には、SMS・メールのワンタイムコード、認証アプリ（TOTP）、パスキー、物理セキュリティキーなどの方式があります。ワンタイムコードは、偽サイト（フィッシングサイト）に入力してしまうと攻撃者に中継される可能性があります。一方、パスキーと物理キーが用いるFIDO2/WebAuthn方式は、認証がサイトのドメインに暗号学的に紐づくため、偽サイト上では認証が成立しないという特性があり、米国NISTの認証ガイドライン（SP 800-63B）でもフィッシング耐性のある方式として位置づけられています。2026年には、プラットフォーム運営会社を装ったフィッシングメールから認証情報を入力してしまい、スタッフアカウントが乗っ取られた事例が公表されています。
導入にあたっては、①利用するサービス（CMS・決済事業者・プラットフォーム）がFIDO2に対応しているか、②パスワードやSMSなどの弱い代替ログイン経路や復旧手順が残っていないか、③予備キー・紛失時の運用をどうするか、を確認してください。FIDO2は認証情報を盗むタイプのフィッシングに有効ですが、ログイン後のセッション窃取や決済ページの改ざんを直接防ぐものではなく、本リストの他の項目とあわせて位置づける対策の一つです。弊社では複数メーカーの物理セキュリティキーを取り扱っており、導入のご相談も承ります（https://security.pj-tc.com/）。

## 3. 決済ページの改ざん対策（自社サイト側）

2026年に公表された「決済ページ改ざん型」の事例では、カード会社からの連絡で事態を把握したものが複数あり、自社での発見や保守委託先からの連絡で判明したものもあります。改ざんされたスクリプトは、通常のサイト表示の確認だけでは検知できない場合があります。対策は、監視できる対象が異なる「自社サーバー」「ブラウザ上の決済ページ」「外部決済SDK」の3層に分けて考えます。

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | 【ブラウザ上の決済ページ】決済ページ（カート〜注文完了）でブラウザ上に読み込まれ実行されるスクリプトの一覧を文書化し、変更を監視している（計測タグ、チャット、決済SDK等） | 制作 | 推奨 |
| ☐ | B | 【ブラウザ上の決済ページ】Content Security Policy（CSP）で実行を許可するスクリプトのドメインを限定し、connect-src等で外部通信先も制御し、違反レポートを収集している | 制作 | 推奨 |
| ☐ | B | 【外部決済SDK】決済事業者が推奨する読み込み方法に従い、適用可能な固定リソースにはSubresource Integrity（integrity属性）を付けている（動的に更新されるSDKには一律に適用できない場合がある） | 制作 | 推奨 |
| ☐ | B | 【自社サーバー】サイトのファイルが変更されたときに通知が届く仕組み（ファイル整合性監視）を入れている。※補助的な対策で、これだけではブラウザ上の改ざん検知にはならない | 制作 | 推奨 |
| ☐ | C | 【ブラウザ上の決済ページ】決済ページから外部への通信先を監視し、見慣れない送信先があれば気づける体制がある | 制作 | 推奨 |

PCI DSS v4.0.1では、決済ページのスクリプト管理（要件6.4.3）と改ざん検知（要件11.6.1）が定められています。2025年1月の改訂で、決済を外部委託するSAQ A加盟店の要件からはこれらが除外されましたが、第三者の決済フォームを自社ページ内のiframe等に埋め込む加盟店には「スクリプトによる攻撃の影響を受けないこと」の確認が適格条件として追加されています（完全なホスト型・遷移型には適用されません）。PCI SSC FAQ 1588は、6.4.3・11.6.1相当の対策のほか、PCI DSS準拠の決済サービス提供者から所定の実装方法で保護が組み込まれている旨の確認を取得する方法も示しています。

## 4. 意図しない保持を防ぐ（自社サイト側）

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | B | お問い合わせフォームに「カード番号は記入しないでください」と明記している（可能ならカード番号の形式を検出して送信を止める） | 制作 | GL |
| ☐ | B | 注文確認メール・管理画面の注文詳細に、カード番号の全桁が表示・転記されていない（下4桁のみ） | 制作 | GL |
| ☐ | B | サーバーやアプリケーションのログに、決済リクエストの内容がそのまま記録されていない | 制作 | GL |
| ☐ | C | 電話・FAXでカード番号を受けている場合、その記録の保管方法と廃棄ルールが決まっている | 経営 | GL |

## 5. Stripe を使っている場合

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | ダッシュボードにログインできる全メンバーが2段階認証（認証アプリ・セキュリティキー・パスキー）を設定している | 経営 | 推奨 |
| ☐ | A | チームメンバーの権限が「管理者」一律ではなく、業務に応じたロール（開発者・アナリスト・サポート等）になっている。制作会社の契約終了後も権限が残っていない | 経営 | 推奨 |
| ☐ | A | サーバー側で使うAPIキーが、全権限のシークレットキー（sk_live_）ではなく、用途を絞った制限付きキー（rk_live_）になっている（Stripe推奨） | 制作 | 仕様 |
| ☐ | A | APIキーがソースコードやリポジトリに直接書かれておらず、環境変数または秘密管理サービスに置かれている | 制作 | 仕様 |
| ☐ | B | サーバーのIPアドレスが固定で確実に管理できる場合、APIキーにIPアドレス制限を設定している | 制作 | 仕様 |
| ☐ | B | Webhookの受信処理で署名（whsec_）を検証し、タイムスタンプの許容範囲とイベントの重複処理にも配慮している | 制作 | 仕様 |
| ☐ | B | Payment Intents APIに移行済み（3DSに対応しないCharges API・Orders APIを使っていない） | 制作 | 仕様 |
| ☐ | B | Radarの3Dセキュア関連ルールの設定内容を把握している。免除取引でも3DSを要求したい場合は request_three_d_secure を any に設定できるが、実際に認証が行われるか・ライアビリティシフトが成立するかは発行会社の判断と取引ごとの結果によることを理解している | 制作 | 仕様 |
| ☐ | C | APIキーを定期的にローテーションする手順が決まっている（旧キーと新キーの併存期間を設ける） | 制作 | 仕様 |

## 6. PayPal を使っている場合

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | PayPalアカウントの2段階認証を、開発者ダッシュボードにアクセスするアカウントも含め、利用者全員が設定している（PayPalはアカウントの2FAが開発者ダッシュボードの保護にもなると説明） | 経営 | 仕様 |
| ☐ | A | PayPal標準決済（PayPalボタン／Checkout）を使っている。カード直接決済（Advanced Credit and Debit Card）を使う場合は「3. 決済ページの改ざん対策」を実施している | 制作 | 推奨 |
| ☐ | A | Client Secret がブラウザ側のコードに含まれておらず、サーバー側でのみ使われている | 制作 | 仕様 |
| ☐ | B | Webhookイベントを処理する前に、PayPalの検証APIで署名を確認している | 制作 | 仕様 |
| ☐ | B | 使っていないAPI資格情報（REST App）を削除している | 制作 | 仕様 |
| ☐ | C | API資格情報を定期的にローテーションする手順が決まっている | 制作 | 仕様 |

## 7. Shopify を使っている場合

Shopifyは決済ページ自体をShopifyが管理するため、加盟店が直接管理する決済ページの範囲は限定されます。一方で、アカウント・権限、インストール済みアプリ、テーマと外部連携（チェックアウト拡張を含む）、決済設定と不正注文対応は事業者側の管理対象として残ります。

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | A | ストアオーナーおよび全スタッフが安全なサインイン方法を設定している（Shopify Paymentsの利用には2段階認証が必須。2段階認証は認証アプリ・セキュリティキーで設定し、パスキーは2段階認証とは別の安全なサインイン方法として扱われる。SMSは新規設定不可、既存設定は継続可） | 経営 | 仕様 |
| ☐ | A | 各スタッフに必要最小限の権限のみ付与している。特に「顧客データのエクスポート」権限を持つ人を把握している | 経営 | 推奨 |
| ☐ | B | 制作会社・代理店にはスタッフアカウントではなく、コラボレーターアカウントまたはTheme Accessアプリでテーマ限定のアクセス権を与えている（Theme Accessは受取リンクに期限があり、アクセス権はパスワードの削除で取り消す） | 経営 | 推奨 |
| ☐ | B | インストール済みアプリと、チェックアウト拡張・Web Pixels等の拡張を棚卸しし、使っていないものを削除している。各アプリが要求する権限（顧客データ・注文データへのアクセス）を確認している | 運用 | 推奨 |
| ☐ | C | 不正分析機能を確認し、リスクの高い注文の扱い（手動確認・自動キャンセル）を決めている | 運用 | 推奨 |

## 8. もしもの時に備える（全サービス共通）

公表までの期間や理由は各社で異なります。たとえばカード会社の連絡から公表まで、佐嘉平川屋は98日、ジャストカーテンは250日で、カード決済の停止が6か月を超えた事例（ビューティガレージ）もあります。平時に準備しておくことで、停止期間と混乱を短くできます。

| ✓ | 優先 | 確認項目 | 担当 | 根拠 |
|---|---|---|---|---|
| ☐ | B | カード会社・決済代行会社から「漏洩の可能性」の連絡が来た場合の初動手順を文書化している（決済停止を含む封じ込めを決定し、並行してログ・ファイルの保全、関係事業者への連絡、法的報告の要否確認、警察への相談の検討を行う） | 経営 | 推奨 |
| ☐ | B | カード決済を停止している間の代替決済手段（銀行振込・コンビニ決済・後払い等）が用意されている | 経営 | 推奨 |
| ☐ | B | 顧客への第一報の文面のひな形を用意している | 経営 | 推奨 |
| ☐ | C | フォレンジック調査を依頼できる専門会社の連絡先を把握している | 経営 | 推奨 |
| ☐ | C | 決済代行会社・カートASP・制作会社との間で、インシデント時の連絡経路と責任分界が契約または文書で決まっている | 経営 | 推奨 |

個人情報保護法上の報告義務が生じる場合（要配慮個人情報を含む、財産的被害のおそれ、不正の目的によるおそれ、1,000人超など一定の法定事由に該当する個人データの漏洩等）、個人情報保護委員会への報告は、速報が事態を知った時点から概ね3〜5日以内、確報が30日以内（不正の目的によるおそれがある場合は60日以内）が目安とされています。

**このチェックリストの使い方**

- 優先度Aの項目から確認してください。アカウント設定などすぐに確認できる項目と、開発や費用が必要な項目（CSP、スクリプト監視、脆弱性診断、API実装の変更など）があります。
- 「制作」担当の項目は、制作会社や開発者に確認を依頼してください。本リストをそのまま渡していただいて構いません。
- 項目を満たしていないことが見つかっても、それ自体は珍しいことではありません。順に対応を進めていくことが大切です。
- 各サービスの仕様は変わることがあります。設定方法の詳細は、各サービスの公式ヘルプで最新の情報を確認してください。

本チェックリストは、クレジットカード・セキュリティガイドライン【6.1版】（クレジット取引セキュリティ対策協議会、2026年3月）、PCI DSS v4.0.1およびPCI SSC FAQ 1588、NIST SP 800-63B、各決済サービスの公式ドキュメント（2026年10月時点）をもとにPJ-T&C合同会社が作成したものです。各項目は一般的な確認事項であり、個別の環境における安全性を保証するものではありません。ご不明な点は弊社までお問い合わせください。
PJ-T&C合同会社　https://pj-tc.com/　｜　認証セキュリティ製品（セキュリティキー）の取り扱い：https://security.pj-tc.com/