ECサイト運営者のための
「セキュリティ対策実施状況申告書」ガイド

近年、ECサイトにおけるクレジットカードの不正利用被害は過去最高水準に達しており、その手口は日々巧妙化しています。 セキュリティ対策が不十分なECサイトは犯罪者の標的となり、お客様のカード情報・個人情報の漏えいや、売上の取消（チャージバック）といった甚大な被害を受けるリスクがあります。

加盟店の皆様にご提出をお願いしている「セキュリティ対策実施状況申告書（以下、セキュリティ申告書といいます）」で求められている内容は、これらの脅威からECサイトを守るために最低限行うべき「セキュリティ対策」です。 「セキュリティ申告書」の項目をチェックすることで、現在のセキュリティ対策の実施状況を把握し、必要な対策を明確にすることができます。

本ガイドでは、「セキュリティ申告書」のご入力にお役立ていただけるよう、それぞれの対策がなぜ必要なのか、どのような効果を持つのかなどを分かりやすく説明しています。

加盟店様の大切なECサイトと売上を守り、お客様に安心してお買い物いただける環境を維持するために、ぜひ本ガイドを活用して対策を進めていただけますと幸いです。

2026年2月　第1.0版
ヤマト運輸株式会社

目次

「セキュリティ申告書」では、大きく分類して下記3種類の対策に関するチェック項目があります。

このうち、**（１）脆弱性対策** は、
ECサイトを侵害しようとするハッカーと呼ばれる犯罪者への対策です。
この犯罪者にECサイトを侵害されると、お客様の個人情報やクレジットカード情報を盗まれてしまいます。

（２）不正ログイン対策と **（３）EMV 3-Dセキュア** は、
ECサイトで不正利用をする犯罪者への対策です。
この犯罪者に不正利用をされてしまうと、チャージバックによる売上損失が発生したり、一定以上の不正利用が発生すると特別な対策を講じるようカード会社から求められるようになります。その対策費用は加盟店様の自己負担となります。

それぞれ戦う相手が異なりますので、全ての対策をきちんと行う必要があります。
どれか一つでもきちんと対策ができていないと、ECサイトに被害が出てしまう可能性があるのです。

★次のページからは、セキュリティ申告書と併せてご確認ください★

（１）脆弱性対策

下記①～⑤が全て導入されていることを確認し、対応済の項目に✓を入れてご回答ください。✓を入れた項目によって、実施状況（準拠しているかいないか）が自動的に入力されます。

対策の詳細は、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」(以下、「導入ガイド【附属文書20】」) 1.脆弱性対策 をご確認ください。

（１）脆弱性対策

脆弱性対策は、ハッカーからECサイトを守る対策のことです。

ハッカーは「クレジットカード情報の非保持化をしているECサイト」からでも、カード情報を盗み取ることができます。

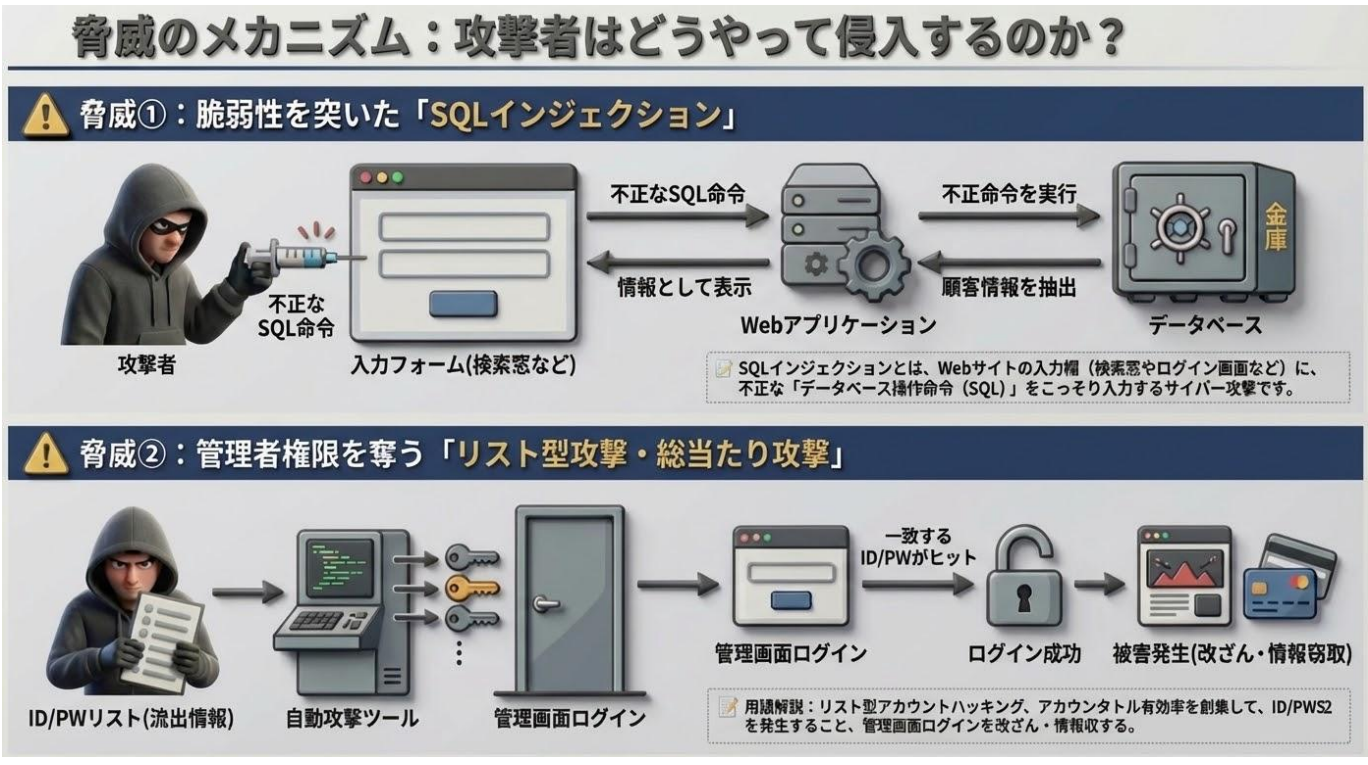
カード情報をどこにも保存していないのにどうして・・・？

ハッカーは、ECサイトに保存されているカード情報を盗みにくるのではなく、お客様が買い物をした瞬間に入力したカード情報を抜き取る「仕掛け」を作ってしまうのです。

セキュリティ申告書の脆弱性対策は、この「仕掛け」を作らせない対策です。

ひとたびカード情報や個人情報が漏えいすれば、ECサイトの長期休止に伴う売上損失、被害者に対する多額の賠償金、そして社会的信用の失墜を招き、事業の存続に関わる致命的な事態に陥りかねません。

正しく対策を実施して、ハッカーに負けないECサイトにしましょう。



①ECサイトの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

「ECサイトのシステム管理画面」とは、
店長さんや、委託先システム会社の方がECサイトの設定や管理運営に使う画面のことです。購入者様のマイページのことではございません。
例：EC-CUBEや、〇〇カートのログイン画面など。

①ECサイトの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可能なIPアドレス(*1)を制限する。IPアドレスを制限できない場合は管理画面、ＩＤパスワードによる認証等のアクセス制限を設ける。	いずれか1つ以上
☐	推測困難なログインURL及びID/パスワードを設定する。	
☐	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）(*2)を採用する。	
☐	システム管理画面のログインフォームでは、10回以下のログイン失敗でアカウントがロックされるように設定する。	

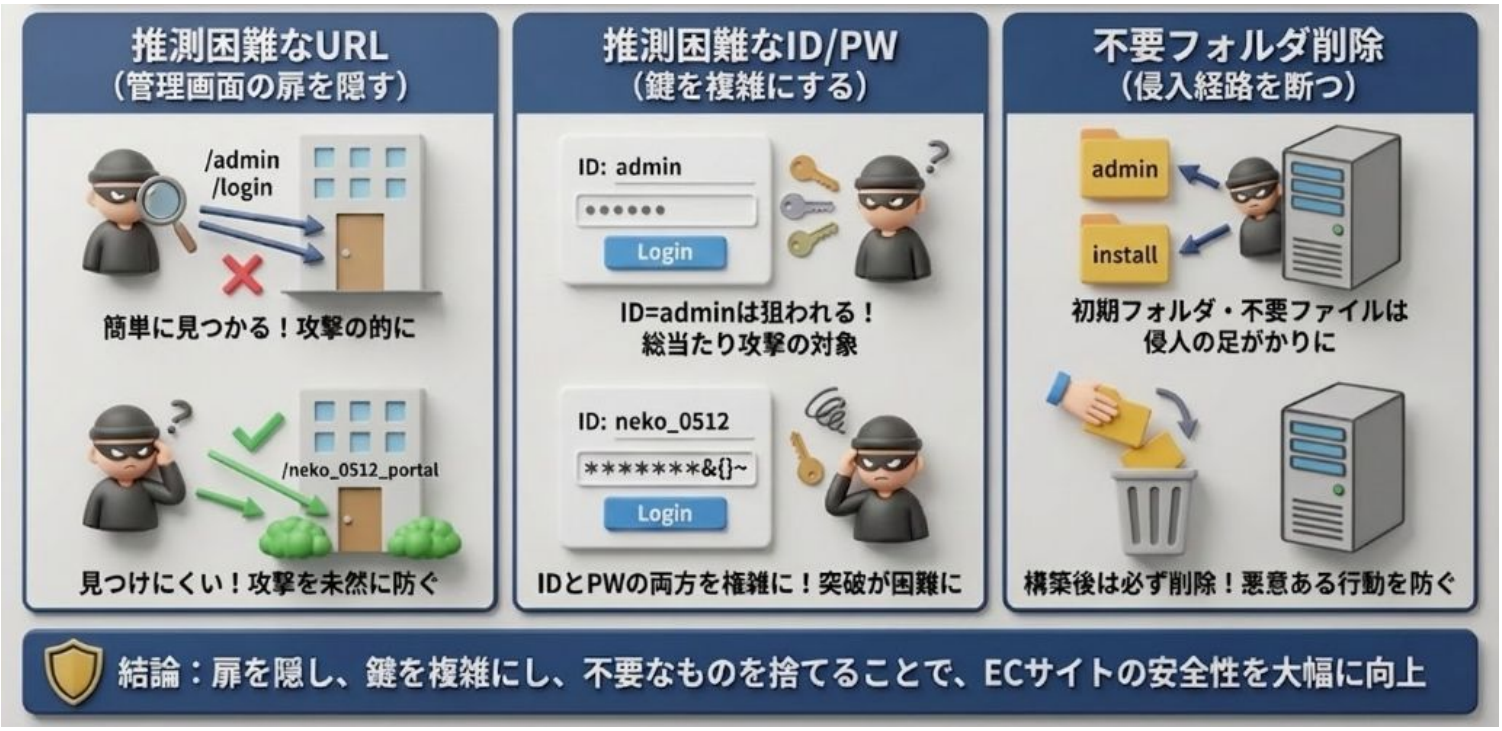
システム管理画面のアクセス可能なIPアドレスを制限する。IPアドレスを制限できない場合は管理画面にIDパスワードによる認証等のアクセス制限を設ける。

管理画面へのアクセス元を自社のネットワークのみに限定することで、ハッカーがログイン画面に到達できないようにします。万が一、IDとパスワードが流出しても、物理的に接続できないため不正ログインを防ぎやすくなります。
IPアドレス制限の機能を導入していなくても、ログインの際にIDとパスワードが必要だという一般的なセキュリティ対策をしていれば、このセキュリティ申告書の設問の要件は満たしています。
しかし、過去に発生した漏えい事案ではIDとパスワードを盗まれることを起点としているケースも多いため、IPアドレスの制限がなければ簡単にログインされてしまう可能性があるのです。

漏えい事案の発生を防ぐという本来の目的のためには、IPアドレスの制限を導入することについてもご検討ください。

①ECサイトの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可能なIPアドレス(*1)を制限する。IPアドレスを制限できない場合は管理画面、ＩＤパスワードによる認証等のアクセス制限を設ける。	いずれか1つ以上
☐	推測困難なログインURL及びID/パスワードを設定する。	
☐	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）(*2)を採用する。	
☐	システム管理画面のログインフォームでは、10回以下のログイン失敗でアカウントがロックされるように設定する。	

推測困難なログインURL及びID/パスワードを設定する。



●推測困難なURL

ハッカーはECサイトの管理画面を機械的に探しまわっていると言われています。
「URLの末尾に/adminや/loginとつけたもの」を管理画面のURLにしておくと、簡単に管理画面のURLが見つかってしまいます。
管理画面のURLを変更すると、管理画面という「扉」を見つけることが難しくなりますので、扉に対する「開けようとする攻撃」そのものを未然に防ぐ対策になります。

●推測困難なID/パスワード

扉が見つかった場合、ハッカーは「IDは adminである」と仮定して、パスワードの総当たりログインを試みることがあります。
「admin」というIDを使わず「neko_0512」のように推測困難なものに変えるだけで、攻撃者は「ID」と「パスワード」の両方の正解を当てなければならなくなり、突破が困難になります。

●不要フォルダ削除

EC構築システムでは、初期状態の管理画面フォルダ名が admin になっていることがあります。このフォルダ名を変更して、空のフォルダが残る場合は削除します。
管理画面のURLを変更するのと同様に、ハッカーが既定の場所を攻撃しても何も存在しないため、悪意のある行動をさせない効果があります。
また、ECサイトのセットアップに使った「install」フォルダなどを残しておくと、ハッカーが活用して簡単に侵入される原因になることがあります。ECサイトの構築を終えた後で不要になったフォルダやファイルは、必ず削除するようにしましょう。

①ECサイトの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可能なIPアドレス(*1)を制限する。IPアドレスを制限できない場合は管理画面、ＩＤパスワードによる認証等のアクセス制限を設ける。	いずれか1つ以上
☐	推測困難なログインURL及びID/パスワードを設定する。	
☐	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）(*2)を採用する。	
☐	システム管理画面のログインフォームでは、10回以下のログイン失敗でアカウントがロックされるように設定する。	

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。

2段階認証・多要素認証とは、ログイン時に2つの異なる種類の「鍵」を使って本人確認を行う、セキュリティを強化する仕組みです。IDとパスワードに加えて、SMSやアプリで届く確認コードや、指紋や顔認証（生体情報）などを追加で要求することで、パスワードが漏えいしたり、推測されたりした場合でも、不正にログインされる可能性を大幅に減らすことができます。

システム管理画面のログインフォームでは、10回以下のログイン失敗でアカウントがロックされるように設定する。

数回パスワードを間違えた場合に入力を受け付けなくすることで、「パスワードを機械的に何万通りも試す攻撃」で不正にログインすることが困難になります。

②データディレクトリの露見に伴う設定不備への対策

「データディレクトリ」とは、
コンピュータ上でファイルやデータを整理・保管するための入れ物（フォルダ）のことです。誰でも中身を見ることができる入れ物を「公開ディレクトリ」と言います。商品の写真などをしまう場所です。
顧客リストなどは、公開されていないディレクトリに保存しないと外部に漏えいしてしまう可能性があります。

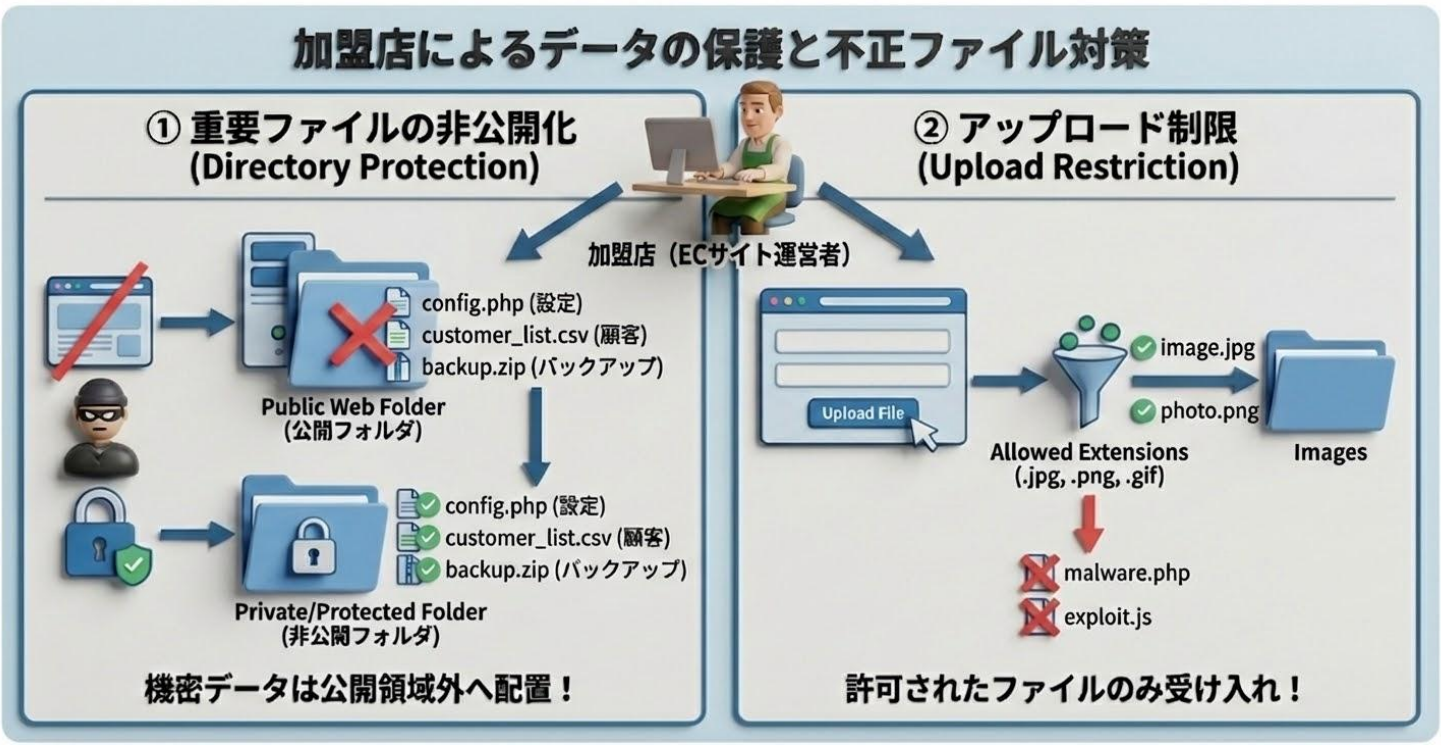
②データディレクトリ(*3)の露見に伴う設定不備への対策
☐ 公開ディレクトリには、重要なファイルを配置しない。（特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。）
☐ WebサーバやWebアプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。

公開ディレクトリには、重要なファイルを配置しない。（特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。）

設定ファイル、顧客リスト、バックアップデータなどの重要なファイルをWeb上の公開ディレクトリ（公開されているファイル置き場）に置かないことで、URLを直接指定されたり、検索エンジンに拾われたりして、非公開の情報が誰でもダウンロードできてしまう事故を防ぎます。
意図しないファイルが公開領域に置いてあることで、管理者のパスワードを盗まれてしまうこともあります。

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。

アップロード可能な拡張子やファイルを制限しておくことで、もし侵入されても「不正なファイルをアップロードさせない」ようにする対策です。
例えば、ECサイトを構成する大量の画像ファイルのなかに、不正なファイル（悪いことをするプログラムなど）をアップロードするのがハッカーの常套手段になっていますが、この対策で主流な手口の一つを使いにくくすることができます。



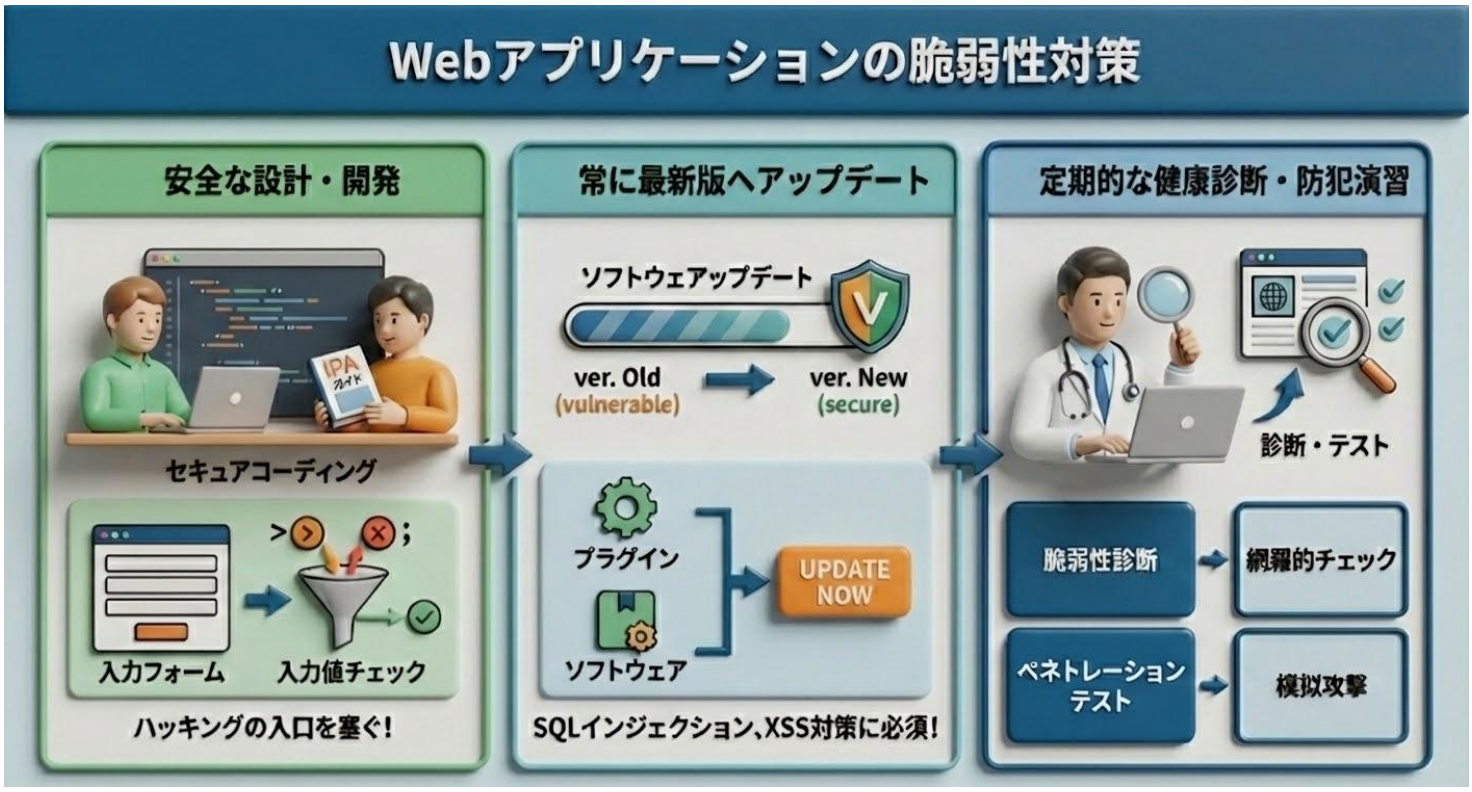
③Webアプリケーションの脆弱性対策

③Webアプリケーションの脆弱性対策	
脆弱性診断を定期的に実施し、必要な修正対応を行う。	いずれか1つ以上
ペネトレーションテスト(*4)を定期的に実施し、必要な修正対応を行う。	
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。	
Webアプリケーションの開発や改修を行う際は、必ずソースコードレビュー(*5)を実施し、セキュアコーディング(*6)が実践されているか確認する。その際は、入力フォームの入力値チェックも行う。	

脆弱性診断を定期的に実施し、必要な修正対応を行う。
ペネトレーションテストを定期的に実施し、必要な修正対応を行う。
脆弱性診断は、ECサイト全体に弱点がないか網羅的な診断をするものです。ペネトレーションテストは見つかった弱点や想定される手口でハッキングができるか、ECサイトに攻撃をしてみるテストです。どちらも、ECサイトに修正が必要な弱点がないかを調べる効果があり、その弱点を修正することで防御力を高めます。

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。
ECサイトを構成するプログラムを常に最新バージョンにしておくことで、悪意のあるプログラムが動作しないようにします。
漏えい事案における最初の一手は、多くの場合において脆弱性を狙った行動です。そして、漏えい被害の発生した加盟店様がデジタルフォレンジック調査を受けると、多くの場合でこの対策不足が漏えいの原因となっていると指摘を受けています。

Webアプリケーションの開発や改修を行う際は、必ずソースコードレビューを実施し、セキュアコーディングが実施されているか確認する。その際は、入力フォームの入力値チェックも行う。
IPA（情報処理推進機構）のガイドラインに基づいた開発ルールの採用や、セキュリティ問題が起きないようにプログラムを作り、十分なチェックをするというものです。
安全な作りではないプログラムは、ハッカーに対する重大な隙になることがあるからです。
そして、ECサイトの入力フォームはハッキングの入口としてよく利用されるため、悪意のある使い方ができないことを確認する必要があります。



④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

④マルウェア(*7)対策としてのウイルス対策ソフトの導入、運用
☐ マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、定義ファイルを最新にして、定期的に全体のチェック（フルスキャン）を行う。

マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、定義ファイルを最新にして、定期的に全体のチェック（フルスキャン）を行う。

ウイルス対策ソフトの導入と定期スキャンを実施する対策です。不正なプログラムを検知・除去することで、ハッカーの活動を阻止します。

【コラム：ウイルス対策ソフトのこと】

「店長のパソコンにはウイルス対策ソフトが入っているから、それでもう大丈夫ですよね？」……いえいえ、ちょっと待ってください！

店長さんだけでなく、「受注処理」や「商品登録」、「顧客対応」など、お店の運営に関わるスタッフ全員のパソコンが対象です。 そして、ECサイトが動いている「サーバー」にもウイルス対策ソフトが必要です。

買い物かごの仕組みをレンタルするASPサービスを使っている場合は、一般的にはASPサービスの提供会社がサーバーのウイルス対策をしてくれています。しかし、自社でサーバーを立ててサイトを作っている場合は、ご自身でサーバーにも対策ソフトを導入しなければなりません。

まさに病気の予防と同じで、「関係者全員がマスク・手洗い（＝ウイルス対策）を徹底する」という考え方が、お店を守るためには不可欠なのです。

⑤悪質な有効性確認、クレジットマスターへの対策

クレジットカードの番号には規則性があり、ソフトウェアにより自動的に大量生成することができます。犯罪者は**「クレジットマスター」**というソフトウェアでカード番号を生成し、実際にECサイトで与信を行って、与信が成功したら使える番号、失敗したら使えない番号、という判定をしています。有効期限やセキュリティコードも、総当たりで与信が成功するかどうかの実験をしているのです。

こうしたクレジットマスターの連続与信によるカードの有効性確認は、不正利用の準備行動です。まさに、ECサイトをカード番号の生成ツールの一部として利用されている状態であり、それを停止できないことは、犯罪者たちの活動を助長することに繋がります。

また、カード会社はこの有効性確認を監視しており、カードの有効性確認を止めるよう緊急対応を求められることがあります。事前に対策について設計、準備がないと対応が困難になる恐れがあります。この有効性確認は加盟店様の都合などお構いなしに数万回にも及ぶことがあり、正規のお客様にご迷惑がかかることもあります。

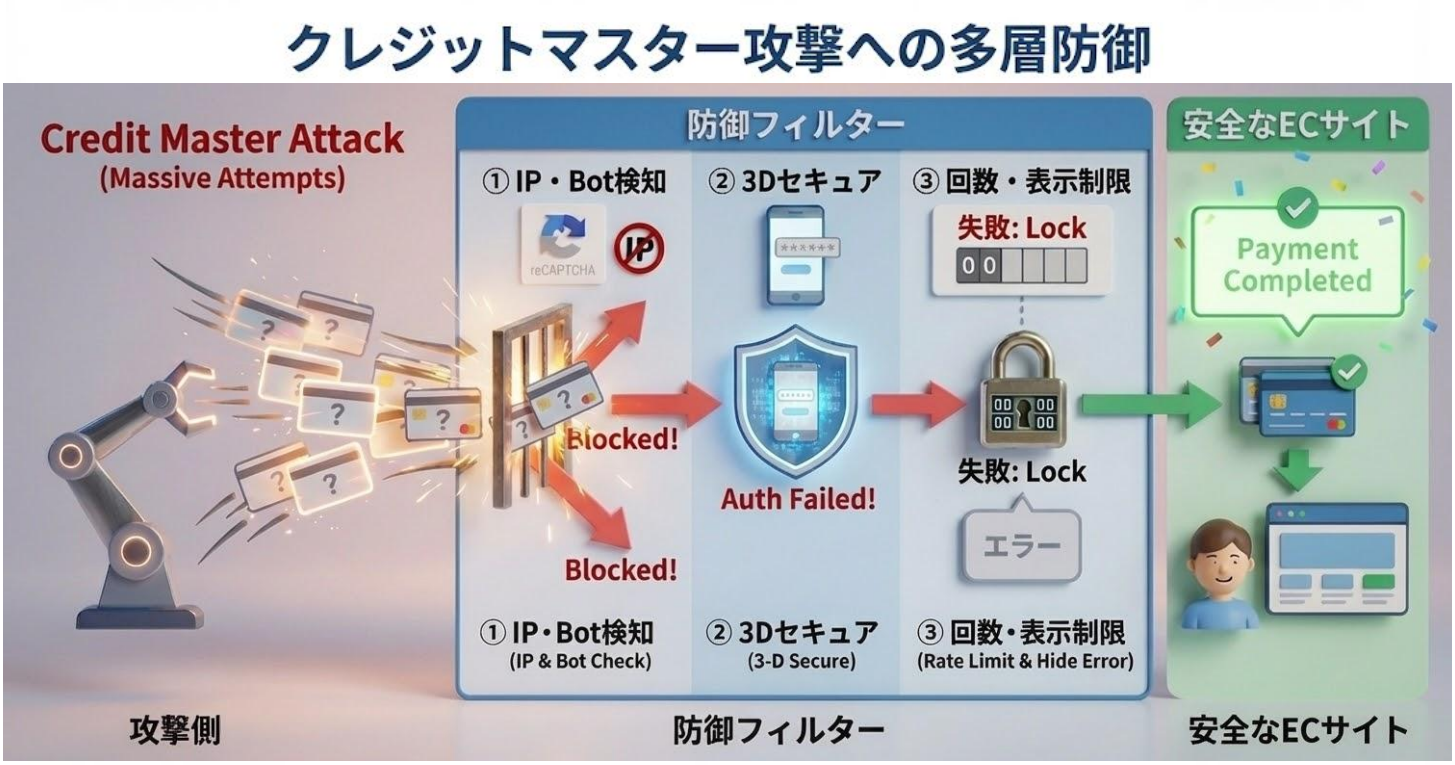
⑤悪質な有効性確認、クレジットマスター(*8)への対策（下記のいずれか1つ）	
☐ 不審なIPアドレスからのアクセス制限	いずれか1つ以上
☐ 有効なカード会員データの漏えい対策	
☐ 本人認証(3Dセキュア)	
☐ 有効性確認の回数制限	

不審なIPアドレスからのアクセス制限
クレジットカードの有効性確認をしてくる接続元のIPアドレスをアクセス禁止にすることで、その活動を阻害します。大量の与信を検知してブロックするなどの対策も有効です。

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、カード与信でエラーになった際にその理由を表示しないなどの対策です。

本人認証（3Dセキュア）
カード番号や有効期限を総当たりで解析したい犯罪者にとって、与信の都度3Dセキュアの認証を求められることは非常にやっかいですので、有効性が高い対策です。

有効性確認の回数制限
パスワードの対策のように、連続して試すことができないように回数に制限を設けるものです。プログラムで自動的に連続与信をさせないという対策としては、Bot検知の機能（reCAPTCHA等）の導入も有効です。



ログイン機能(*9)を採用していない加盟店様は下記の(２)は回答の対象外になりますので、 『ログイン機能を採用していない』のチェックボックスに✓を入れてください。 A.会員登録時／B.会員ログイン時／C.属性情報変更時の各シーンで1つ以上対策を講じる必要があります。下記の①～⑦の各対策を、A,B,Cの各場面のどこで講じているか、✓を入れてください。 ※1…ログイン機能を採用していない加盟店様は回答の対象外になりますので、『ログイン機能を採用していない』のチェックボックスに✓を入れてください。 ✓を入れた項目によって、実施状況（準拠しているかいないか）が自動的に入力されます。	**ログイン機能を採用していない** ☐

ECサイトに、会員登録機能が無い場合は、次の（２）不正ログイン対策は対象外になりますので、
セキュリティ申告書で**「ログイン機能を採用していない」**を選択してください。

（２）不正ログイン対策 A.会員登録時／B.会員ログイン時／C.属性情報変更時の各シーンで1つ以上対策を講じる必要があります。下記の①～⑦の各対策を、A,B,Cの各場面のどこで講じているか、✓を入れてください。 ✓を入れた項目によって、実施状況（準拠しているかいないか）が自動的に入力されます。	**導入が必要な対策の実施状況** **準拠していない**		
対策の詳細は、「導入ガイド【附属文書20】」3.不正ログイン対策（決済前の対策） をご確認ください。	A.会員登録時	B.ログイン認証時	C.属性変更時

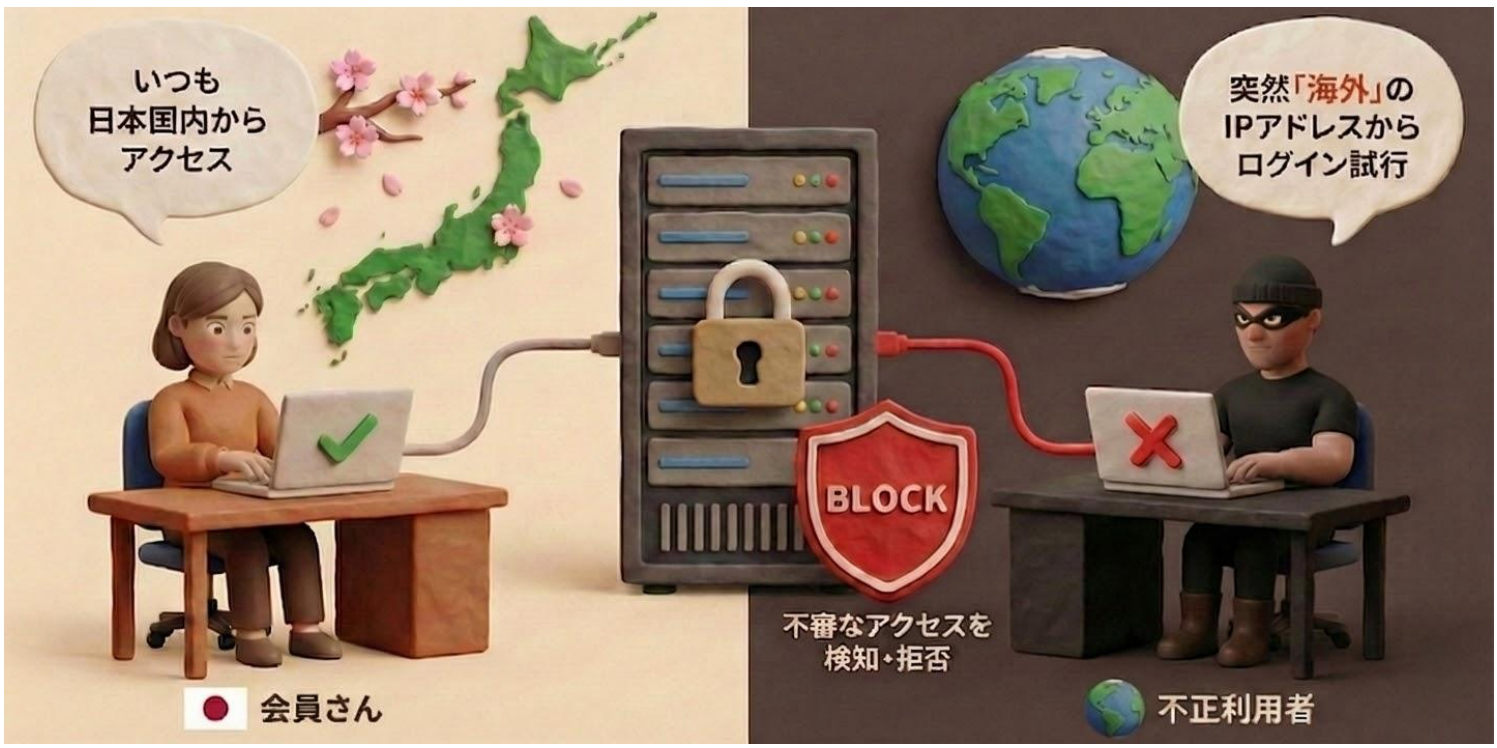
（２）不正ログイン対策

加盟店様のECサイトのお客様が、「お店の会員」として登録をする機能（会員登録機能）に関する設問です。
不正利用者は、会員登録機能の「隙」を狙って、不正利用を試みます。
A.会員登録時／B.ログイン認証時／C.属性情報変更時の3つの場面は、犯人の通り道であると同時に、お店が異常を検知して不正を食い止める最大のチャンスでもあります。
クレジットカードセキュリティガイドラインの基準では、A.会員登録時／B.ログイン認証時／C.属性情報変更時の各場面ごとに、**１つ以上**の対策を講じることを求めています。
①～⑦の対策のうち、各場面で**１つ以上**を実施していたら「準拠している」ことになります。

①不審なIP アドレスからのアクセス制限

①	不審な買い物客を見つけたときに、IPアドレス（パソコンを特定する電話番号のようなもの）を指定して、会員登録や買い物を禁止する設定ができる場合。

過去に不正利用に使われたIPアドレスや、海外サーバーなどからのアクセスを遮断する対策です。日本国内向けのサービスで、海外からの不正利用に困っている場合は、海外からのアクセスを遮断することで攻撃の「母数」を減らすという使い方もできます。



②2段階認証または多要素認証（2要素認証）による本人確認

②	IDパスワードに加えて、さらに携帯電話にSMSやメールでワンタイムパスワードを送信して、ログインする機能、または「IDパスワード」、「指紋など生体認証」、「ワンタイムパスワード」のうち2つを使ってログインする機能を設置している場合。

不正利用者が、他サイトから流出したIDとパスワードのリストを使ってログインを試みても、正規の会員の手元にあるスマホに届いた通知がなければログインができなくなる対策です。
パスワードが流出していても不正ログインを防げる可能性があるだけでなく、正規の会員が異常を知る機会も得られます。

③会員登録時の個人情報確認(*10)（氏名・住所・電話番号・メールアドレス等）

③	会員登録された個人情報に不自然な点がないか確認している場合。

会員登録された注文者の情報を確認することで、「注文者情報の不自然さ」に気づく機会が得られます。「名前のフリガナがおかしい」「電話番号の桁数がおかしい」などの怪しい登録を保留にするなど、不正利用者から犯行がやりにくいサイトだと認識されることで、ターゲットにされにくくします。

④ログイン試行回数の制限強化（アカウント/パスワードクラッキング(*11)の対応）、スロットリング(*12)

④	一定以上の連続したパスワードの間違いでアカウントをロックしたり、同じIPアドレスから一定以上の連続したアクセスがあると、しばらくアクセスできなくなるなどの対策をしている場合。

短時間に何度もパスワードを間違えた場合、アカウントをロックしたり、応答をあえて遅らせたりする対策です。
例えば、「数秒に1回」しかログインを試すことができないようにすることで、不正利用者がパスワードを特定する効率が極端に悪くなり、パスワードを試す行為を現実的に不可能にします。

⑤会員ログイン時/属性(*13)情報変更時のメールやSMS通知

⑤	会員のログイン、または登録されている名前や電話番号などの情報が変更されたことを、メールやSMSで会員に通知する機能がある場合。

正規の会員が「おかしなログイン通知が届いた」とお店に知らせてくれることは、大変貴重な「確証のある不正アクセス情報」です。
不正検知システムなどで「怪しいログイン」を検知しても、正規の会員なのか判別ができなければ対応は難しく、本当の意味での被害防止に繋がりませんから、この機能の効果の重要性がうかがい知れます。不正ログインをされても、正規の会員がお店に異常を知らせてくれた場合は、被害を食い止めることができる可能性もあります。

⑥属性・行動分析(*14)

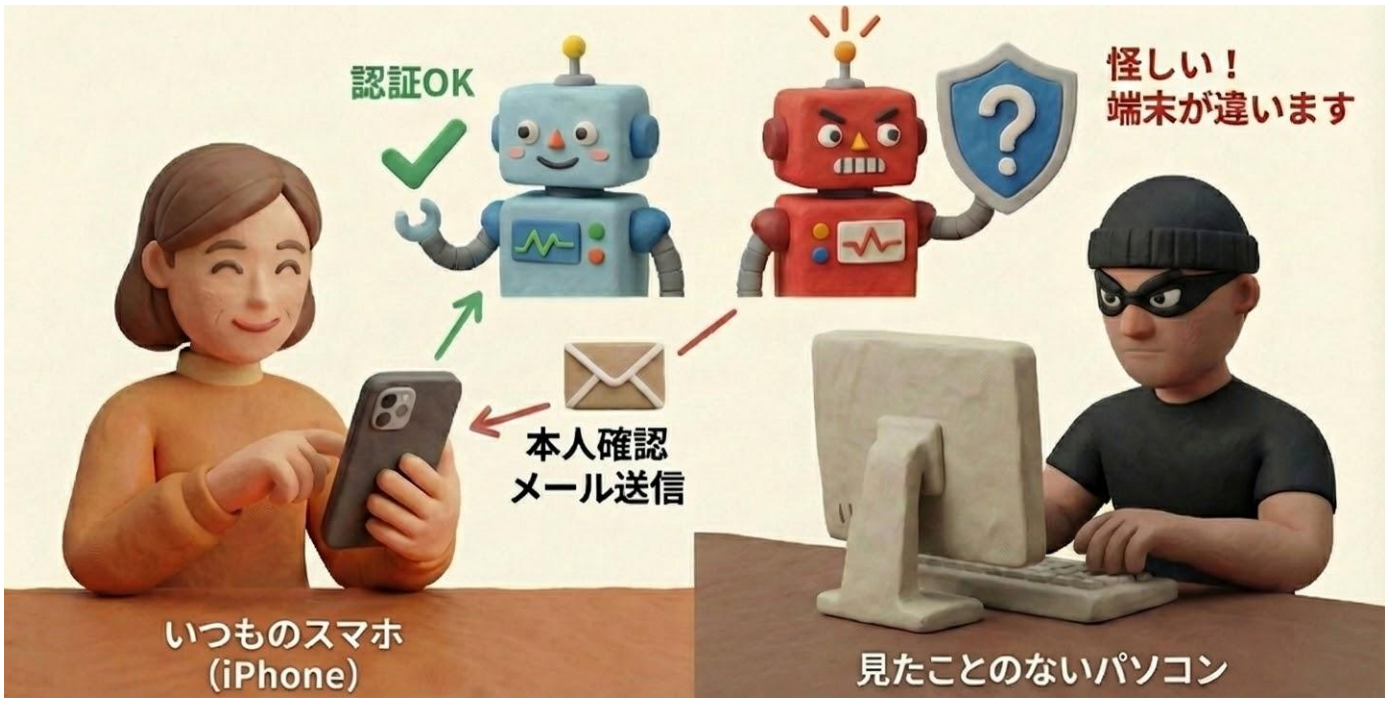
⑥ 不審な会員登録やログイン、会員情報の変更などを見つける不正検知機能を実装している場合。
※当社の不正検知機能は、決済時の分析機能であり、ログイン時の検知はしておりませんのでこれに該当しません。

いわゆる不正検知システムのことです。普段と異なる行動や、不正利用者特有の行動などを分析してくれるため、有効に機能すれば様々な場面で効果が期待できます。
当社のクロネコｗｅｂコレクト不正検知機能は、「ECサイトの不正ログイン」に関する分析はしておりませんので、不正ログインの部分を分析する不正検知システムを導入したい場合は、別途専門の提供会社とのご契約が必要になります。

⑦デバイスフィンガープリント(*15)

⑦ ECサイトにアクセスしようとする端末を、指紋で識別するように特定する機能で、不審な会員登録やログインを遮断／検知する機能として使われています。

ブラウザの種類、バージョン、画面解像度、フォント設定などの情報を組み合わせて、端末固有の「指紋（フィンガープリント）」として識別する技術です。
不正利用者の端末を識別したり、IPアドレスの偽装や正規会員へのなりすましを検知した際に、接続の遮断や多要素認証を求めるなどの使い道があります。



（３）EMV 3-Dセキュア 今回の調査対象の加盟店コードで、ECサイト内でクレジットカード決済を扱っていて、3Dセキュアを導入している場合は「準拠している」、していない場合は「準拠していない」をお選びください。	導入が必要な対策の実施状況 プルダウンからお選びください

原則として、全てのECサイトに3Dセキュアの導入が義務付けられております。
回答日時点で3Dセキュアが導入されている場合は、（３）EMV 3-Dセキュアの設問で「準拠している」を選択します。（新規ECサイト開設の場合はカード決済利用開始日時点とします。）
将来的に3Dセキュアを導入する予定である場合は、3Dセキュアを導入してからクレジットカード決済が利用可能になります。

（３）EMV 3-Dセキュア（単に3Dセキュア、3Dセキュア2.0ともいいます）

インターネット上でクレジットカード決済をより安全にご利用いただくための「本人認証サービス」です。決済時にSMSへのワンタイムパスワード発行、生体認証などによる追加認証を行うことで、カード会員本人であることを確認し、第三者による「なりすまし」を防ぎます。

進化した「3Dセキュア」とリスクベース認証

従来の3Dセキュアでは、全ての決済でパスワード入力が求められ、手間による「カゴ落ち（購入離脱）」が課題でした。 しかし、現在の「EMV 3-Dセキュア」では、「リスクベース認証」という仕組みが導入されています。

リスクベース認証とは、お客様の利用環境（いつもの地域、いつものお店など）をカード会社が分析し、不正利用のリスクが低いと判断した場合はパスワード入力を省略し、リスクが高いと判断された場合のみ、追加認証（パスワード入力など）を要求する仕組みです。これにより、お客様の利便性を損なわずに、セキュリティを大幅に向上させることを実現しました。

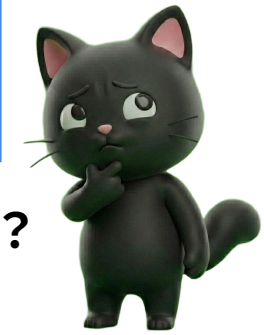
3Dセキュア導入のメリット

3Dセキュアを導入し、本人認証を通過した取引で、万が一不正利用（チャージバック）が発生した場合、原則として加盟店様はその被害額を負担する必要がなくなります。 これは、お店の売上を守る上で非常に強力な効果です。
また、与信時に3Dセキュアの認証を行うことで、機械的にカード番号や有効期限等を総当たりする「クレジットマスター攻撃」（10ページ参照）への対策としても効果を発揮します。

なお、3Dセキュアを導入いただく際に、クロネコｗｅｂコレクトでの別途のお申込みや導入・利用の代金は不要です。
対応済みのASPカートをご利用の場合はカートの管理画面やマニュアルをご確認ください。自社構築のサイトでは接続仕様書に基づいてパラメータの設定を行ってください。

2025年3月末をもって、原則として全てのECサイトに3Dセキュアの導入が義務付けられていますので、未導入の場合は、至急導入のご対応をお願いいたします。

対策が沢山あるけど、結局どれを導入したら良いのか教えてください。



・・・セキュリティ申告書をクリアすれば万全ですか？

セキュリティ申告書の条件を満たすことで、法令で求められる
最低限のセキュリティが確保できたことになります。

しかし、「漏えいに気を付けましょう！」と啓蒙をしている側のカード会社や決済代行会社ですらハッキングをされたことがありますので、どこまで対策をしても絶対に安全ということはなく、対策には終わりがありません。
そして「どの対策を導入すれば良い」という画一的な正解もありません。

しかし、予算や手間には限界があります。

ECサイトの規模や予算をもとに、どのような対策を導入するのが自社のECサイトにとって適切なのか、システムの専門家の方と相談しながら決めましょう。

【資料】
本ガイドは、クレジットカードセキュリティガイドライン6.0、およびその関連資料をもとに作成されています。

一般社団法人日本クレジット協会　資料掲載ページ
https://www.j-credit.or.jp/security/document/index.html