

⚠️ ご注意ください

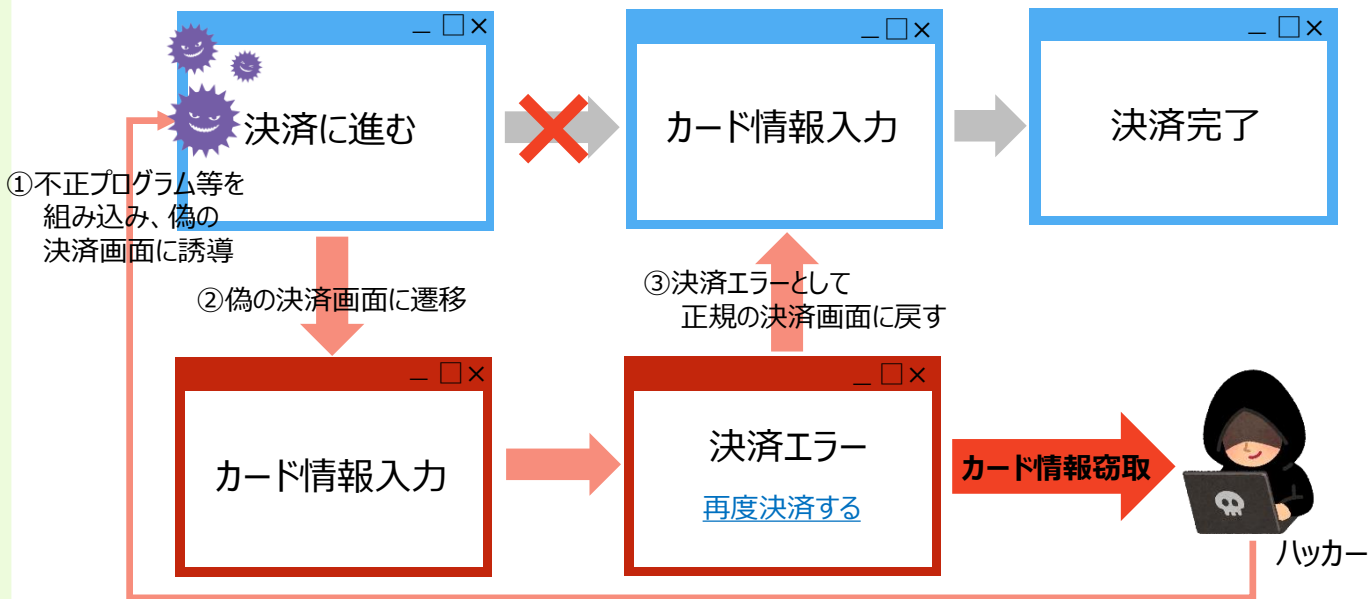
ECサイトの脆弱性による 個人情報漏えい被害について



1. ECサイトにおいて、個人情報漏えいが急増しています

EC市場の拡大にともない、セキュリティ対策が不十分な中小企業や個人事業主のECサイトが増加しています。また、それ狙ったサイバー攻撃が活発化しており、クレジットカード情報漏えい被害が後を絶ちません。

■ クレジットカード情報窃取の手口の一例



2. 運営するECサイトで個人情報漏えいが発生すると...

信頼

社会的信頼の失墜

情報漏えいは社会的な信用を失います。マスコミの報道やネットでの情報掲示でネガティブ情報として取り上げられる可能性が高く、ECサイトだけではなく、企業体そのものの信頼にも影響します。

時間

ECサイトの一時閉鎖

情報漏えいが発覚した場合、まず最初に「サイトの一時閉鎖」をしなければなりません。また、情報漏えいの原因を探る為のフォレンジック調査や顧客対応の時間も要します。

お金

フォレンジック調査の費用・損害賠償金の支払

フォレンジック調査は特定の専門機関への調査依頼が必須となり、調査費用は数百万円以上が見込まれます。また、損害賠償金の支払い等も発生します。

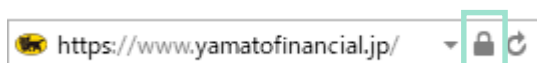
3. ECサイトで講じておくべき主なセキュリティ対策

✓ 情報の送受信を暗号化するSSLを導入する

SSLを導入することにより、インターネット上での通信が暗号化され、盗聴や改ざんを防ぎます。また、ECサイト内のログインページやフォーム等の一部のページだけでなく、すべてのページにSSLを導入（常時SSL化）することによって、webサイトのセキュリティ向上などの効果が見込まれます。

SSL証明書の発行は、認証局による認証が必要になります。自社ECサイトの場合、ご利用のカートによって導入・設定する方法が異なります。中にはASPカートの基本サービスの中にSSLの設定が可能なものもありますので、貴社に最適なSSLの導入方法をご確認ください。

🎯 SSLを導入している場合



鍵マークあり

情報が暗号化されている為、
外部への情報流出の可能性少

⚠️ SSLを導入していない場合



鍵マークなし

情報が暗号化されていない為、
外部への情報流出の可能性大

✓ セキュリティソフトを導入する

セキュリティソフトを導入・常に最新のバージョンに更新しておくことで、マルウェア感染、不正アクセス等のセキュリティリスクに有効です。

✓ IPアドレスを制限する

運営に関してのあらゆる情報を扱う管理画面への、外部からの不正アクセスを防ぐ為に、管理画面にアクセスできるIPアドレスを社内のIPアドレスに制限することが有効です。社内のネットワークがしっかり管理されていれば、不正にアクセスされる危険性が大幅に下がります。

✓ 不要なアプリケーションを削除する

不要かつ未使用のアプリケーションを定期的に削除することは、セキュリティの脆弱性改善に有効です。

✓ ID・パスワードを見直す

定期的に管理画面等のIDやパスワードの見直しをすることによる、管理画面への容易な不正アクセス対策を行うことも有効です。