

滋賀県警からのサイバーセキュリティに関するお知らせ

「ショッピングサイト等からの情報流出事案が国内各地で発生」 不正アクセスや Web サイトの改ざんに注意して下さい。

本年 8 月以降、ウェブサイトから個人情報等が流出する事案が全国的に発生しています。主な個人情報の流出事案は、企業の公式ウェブサイトやショッピングサイトがパスワードリスト攻撃を受けたり、システムの脆弱性を悪用されて不正アクセスされた上、顧客情報やクレジットカード情報が窃取されたというものです。

中には、数年前から継続して不正アクセスを受け、約 10 万人に上る個人情報が流出していたというケースも発生しています。

ウェブサイトは常に攻撃者からの脅威にさらされており、知らぬ間に情報が流出しているということもあります。

ウェブサイトやアクセスログを確認するなどしてセキュリティ対策を推進しましょう。



主な情報流出事案

業種	種別	概要等
食品販売サイト	不正アクセス	システムの脆弱性をついた不正アクセスにより、クレジットカード情報等数万件が流出。
化粧品販売サイト	ウェブサイト改ざん	システムの脆弱性について「偽の決済画面」に誘導され、クレジットカード決済を行った利用者の情報が数百件流出。
育児情報サイト	パスワードリスト攻撃	第三者から流出したパスワードにより不正アクセスされ、数名の利用者のポイントが不正にギフト券に交換される。
衣服等販売サイト	パスワードリスト攻撃	パスワードリスト攻撃により、数万件の利用者のアカウントに不正ログイン。個人情報の流出、ポイントの不正利用が発生。

※情報流出事案の発生を公表した企業が、インターネット上に掲載した情報を元に作成。(期間：2019年8月から10月まで)

サイバー攻撃概要とセキュリティ対策

ウェブサイトの改ざん

ウェブサイトの改ざんは、「システムの脆弱性」が悪用されることが多いです。脆弱性が判明した場合には「パッチ」と呼ばれる修復プログラムを早急に適用しましょう。

パスワードリスト攻撃

パスワードリスト攻撃は、攻撃者が第三者から入手したパスワードを手当たり次第にログインを試す攻撃です。ワンタイムパスワード等の二段階認証や多要素認証を導入しましょう。

[INFORMATION] Windows7 の延長サポートは 2020 年 1 月 14 日で終了します。

終了後はソフトウェア更新等のサポートが受けられません。詳しくは、「Microsoft の公式サイト」で確認して下さい。