滋賀県警察からのお知らせ

# サイバーセキュリティ情報 CSI

事業者の皆さまに、注目のサイバーセキュリティに関する情報をお届けします。

R３年度No. 2

## ショッピングサイトの利用・運営の注意点

ショッピングサイト（ECサイト）は、便利ですが詐欺やトラブルも多く発生しています。
また、ショッピングサイトを運営する側も情報流出やサイト改ざん等のセキュリティ対策が必要です。
利用する側と運営する側の注意点等をまとめましたので、それぞれの視点で確認して、安全に利用できるようにしましょう。

### ショッピングサイト利用者

偽ショッピングサイトは、本物のサイトの情報(写真や会社概要）がコピーされて使用されている場合が多く、非常に巧妙に作成されています。
ショッピングサイトには、「偽物がある」ということを念頭に利用するようにして下さい。

偽ショッピングサイトにアクセスしようとすると、ウイルス対策ソフトやブラウザが警告を表示してくれる場合があります。ウイルス対策ソフトは必ず導入して、ブラウザとともに最新の状態にしておいてください。


### 偽ショッピングサイトを見分けるポイント

- **商品の価格が相場より安すぎないか。**
  - 相場より安すぎる場合は、サイトを慎重に確認してください。
- **会社が実在しているか。**
  - 会社概要のページには会社名称、所在地、連絡先が表示されていますので、その内容をインターネット等で確認してください。
- **商品の支払い方法が銀行振込だけでないか。**
  - 偽ショッピングサイトの多くは、銀行振込しか利用できません。また口座名義人が個人名、外国人名の場合は、会社概要との整合性を確認してください。
- **URLに見慣れないドメインが使われていないか。**
  - 偽ショッピングサイトのドメインの多くに「~.top」「~.xyz」「~.site」「~.online」等が使われていますので、ドメインを確認してください。

### ショッピングサイト運営者

ショッピングサイトは、個人情報を取り扱うことになりますので、システムの適切な管理とセキュリティ対策が必要です。

〈サイバーセキュリティ上の主なリスク〉
・ID/パスワードの漏えいによる不正ログイン
・サイト脆弱性を突かれたサイバー攻撃
・設定ミスによる情報漏えい

情報漏えいが発生すると、金銭的な損失、信頼性の喪失等により事業継続が困難となるケースもあります。

### セキュリティ対策のポイント

- **システム脆弱性対策**
  - ECサイト作成サービスを利用している場合は、サービス提供者からのシステムの脆弱性や更新の情報をチェックして、脆弱性に対する対策を早期に実施して下さい。
- **アクセスの管理**
  - 管理者権限を厳格に定めて、権限を管理して下さい。またアクセスログを取得し不正なアクセスがないかを監視して下さい。
- **二段階認証やリスクベース認証の利用**
  - お客様のアカウントが不正に利用される場合がありますので、不正ログインを防ぐために二段階認証やリスクベース認証を利用して下さい。

### ランサムウエアによるサイバー攻撃が活発化

日本企業や海外子会社でランサムウエアによる攻撃を受け、実際に攻撃者にデータが公開される事例が増加しています。最近のランサムウエアは、暗号化するだけでなく情報を窃取して脅迫するという手口が使われています。不審なメールには警戒するとともに、システムや機器の脆弱性対策を行うようにして下さい。

**«注意»副業サイトに関するトラブルが発生してますので利用には注意してください。**

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）