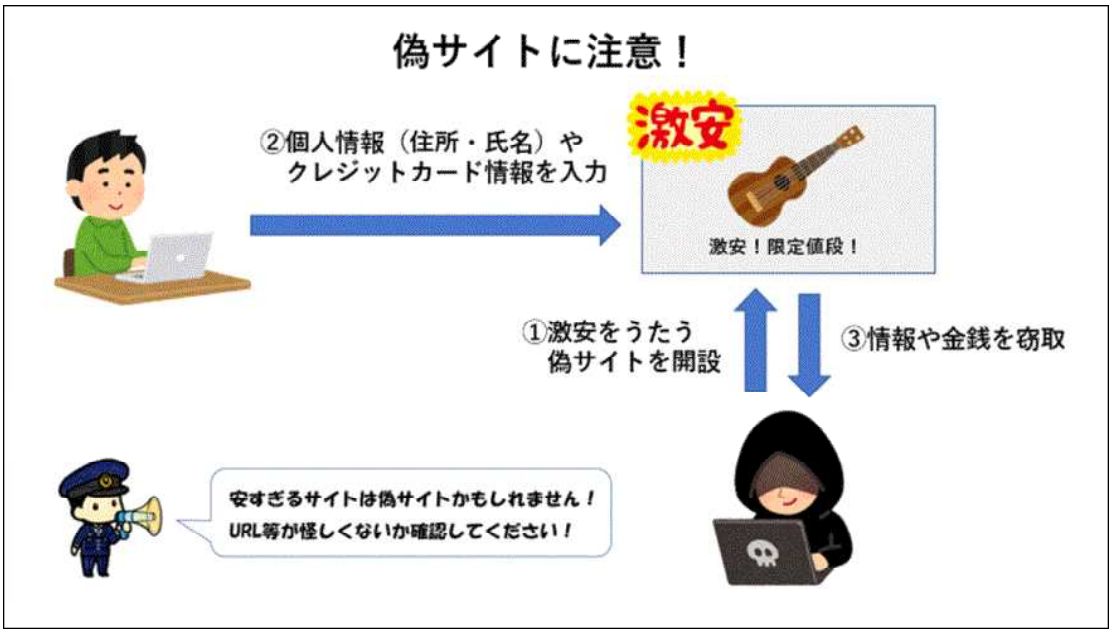
偽ショッピングサイト・詐欺サイト対策

○　偽ショッピングサイト、詐欺サイトとは

偽ショッピングサイト、詐欺サイトとは、インターネットショッピング等に係る詐欺を目的としたウェブサイトを構築し、商品の注文・代金の振込を受けた上で、商品を発送しない又は偽物の商品を発送するなどの手口をいいます。



○　よくある相談

＜相談事例１＞

インターネットで欲しい商品を検索していると、安く販売しているショッピングサイトを発見したので商品を注文したところ、メールで代金の振込先口座を指定された。案内に従って代金を振り込んだが、到着予定日を過ぎても商品が届かない。メールで問い合わせたが返信がなく、メールアドレス以外の連絡先の表示がない。

＜相談事例２＞

○○ショップというネットショップに本物とうたっているブランドバッグが出品されていたので注文して代金を振り込んだが、送られてきたのは偽物のバッグだったので届出に来た。

＜相談事例３＞

私の会社の住所や電話番号が、見ず知らずの通販サイトの運営会社として掲載されており、商品が届かないなどの全く身に覚えのない苦情の電話が入って困っている。

○　偽ショッピングサイト、詐欺サイトの手口

(1)「品薄」等の表示により商品の購入を急がせる

「品薄」「本日限り」等と表示することによって消費者心理につけ込み、商品購入を急がせることがあります。

(2)割引が過大である

通常では考えにくい販売価格の大幅な値引きを強調し、消費者心理につけ込み、商品購入を煽ることがあります。

(3)代金支払い方法が銀行振込のみなど限定的である

銀行口座等への前払いのみ、クレジットカードのみ、代金引換のみなど、代金支払い方法が限定されていることがあります。

(4)会社概要に実在しない住所が記載されている

ウェブサイトに記載されている販売業者の住所が、虚偽であったり、無関係の住所の場合があります。

○　偽ショッピングサイト、詐欺サイトの被害に遭ってしまったら

(1)クレジットカード会社等に連絡する

偽ショッピングサイト等にクレジットカード番号等を入力してしまった場合は、クレジットカード会社に連絡して、支払いの停止を依頼してください。

(2) ＩＤ、パスワード等を変更する

偽ショッピングサイト等にID、パスワード等を入力してしまった場合は、そのＩＤ、パスワード等を利用している全てのサービスにおいて、パスワードを変更してください。

(3) サイト情報や相手とのやり取りの内容等を保存する

偽ショッピングサイト等の情報（URL、トップ画面等の画像）、口座情報や振込記録等の取引情報、相手とのメール等のやり取り内容等の資料を保存してください。

- 商品が出品されていたショッピングサイトのURL、画像
- ショッピングサイト運営会社の情報（法人名、住所、電話番号等）
- 落札日時又は購入日時
- 送金先の金融機関名、口座番号、口座名義人
- 代金を振り込んだことがわかる資料（振込明細等）
- 取引相手とやりとりした際のメール（メールヘッダも含む）、電話、郵便等の情報を時系列に整理したもの

(4) 警察に通報・相談する

偽ショッピングサイト、詐欺サイト等の被害に遭った場合は、ショッピングサイトのURL、画像等の資料等を持参して、最寄りの警察署まで通報・相談してください。

警察署案内（https://police.pref.kochi.lg.jp/police-docs/2024012200010/）

なお、事前に電話で担当者と日時や持参する資料の調整をしていただくと対応がスムーズに進みます。

○　被害に遭わないために

ショッピングサイト等を利用する際は、購入手続前に次に掲げる点を確認し、手続中に支払方法等が明示された方法と異なり銀行振込のみになるなど不審点を感じたら、すぐさま手続を停止してください。また、官公庁や企業・病院等の名称を使用したサイトで不審点を感じたら、手続を進めることなく各関係機関等に問い合わせてください。

- **URLの「https://～」やドメインに違和感はないか**
- **商品価格が極端に安くないか、割引率が大きくないか**
- **「本日限り」等と記載されるなど、購入を急がせていないか**
- **日本語が不自然でないか**
- **会社概要の内容についてインターネットで検索等を行い、企業名の盗用や虚偽の内容等が記載されていないか**

偽サイトや詐欺サイトが検索の上位に表示される場合や普段から利用するSNS等の広告に表示される場合もありますので、必ず確認をお願いします。

○　ウェブサイトを運用する事業者の皆様へ

近年、国内の事業者等のウェブサイトが改ざん（ファイルを蔵置）され、偽サイト等への誘導に使用されてしまう事例が多発しています。

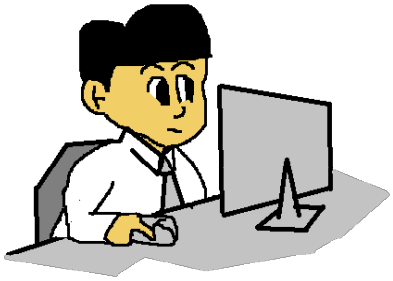
(1) 偽ショッピングサイト等への誘導手口

ソフトウェア等の脆弱性を突いたり、管理者のパスワードを何らかの方法で入手したりして、事業者のウェブサーバに不正アクセスし、偽ショッピングサイトへ転送するためのファイルを蔵置することにより、検索サイトに偽のページへ転送する検索結果を表示させる手口が確認されています。利用者が表示された検索結果にアクセスすると、偽ショッピングサイトへ転送されてしまいます。

(2) 改ざんを確認する

次の方法を参考に、ウェブサイトが改ざんされていないか定期的に確認してください。

- 大手検索サイトにおいて、「site:○○○.co.jp」など「site:」の後に自社のウェブサイトのドメイン名を入力して検索し、検索結果に見覚えのないページが表示されていないか確認する。
- 入力画面が不正なＵＲＬになっていないか、いつもと違う画面が表示されていないか
- ウェブサーバ等のログに不審なアクセスがないか



(3) ウェブサイトを改ざんされないために

ウェブサイトの改ざんの被害に遭わないためには、

- ウェブサーバの OS やソフトウェアを最新の状態に保つこと。
- 管理者の ID やパスワードを適切に管理すること。
- ウイルス対策ソフト等を導入すること。

などの対策を講じることが重要です。

また、次に掲げる対策を講じてください。

- ウェブサーバ上の不要なサービスやアカウントを削除又は停止する。
- 公開を想定していないファイルをウェブ公開用のディレクトリ下に置かない。

・　ウェブアプリケーションに対する攻撃からサーバを保護するため、WAF（Web Application Firewall）等のセキュリティ製品を導入する。
・　定期的にバックアップを取得し、正常なコンテンツと比較して、不正なファイルが置かれていないか確認する。

○　参考リンク

・　**消費者庁**
「偽サイト」にご注意ください!」（外部サイト）
（https://www.caa.go.jp/policies/policy/consumer_policy/caution/caution_033）
・　**一般財団法人日本サイバー犯罪対策センター（JC3）**
「偽ショッピングサイトに注意」（外部サイト）
（https://www.jc3.or.jp/threats/topics/article-462.html）
・　**SAGICHECK ※**（外部サイト）
（https://sagicheck.jp/）

※　JC3（一般財団法人日本サイバー犯罪対策センター）では、収集した偽ショッピングサイト情報を、インターネット利用者がウェブサイトの信ぴょう性を確認できるサービス「SAGICHECK」に提供しています。