よくあるご質問（サイバー編）

Q：　通販サイトで購入した商品が届かず、 詐欺の被害に遭ったかもしれない。

A：　対象の通販サイトの問い合わせフォームに商品の送付を求めるメッセージを送付する、販売者に対して商品の送付又は現金の返還を求める旨の内容証明郵便等を送付するなどして、債務履行を求めてください。

商品の購入に際し、自身のクレジットカードの情報を入力した場合であれば、クレジットカードの発行会社に連絡して、クレジットカードの停止や再発行手続き等を行ってください。

警察へ届出される場合は、商品の購入手続きを行ったサイトの URL や相手とのやりとりが記録されている資料をご持参のうえで、最寄りの警察署にご相談ください。

Q：　不審な通販サイトに住所・氏名等の個人情報を入力してしまった。

A：　対象の通販サイトが詐欺サイトであれば、入力した住所・氏名等の個人情報から、架空請求の通知や注文していない商品を代引きで送付されるなどの被害が予想されます。

身に覚えのない請求や商品の送り付けに対応することなく、同居の家族にもこれらの可能性について情報を共有してください。

また、電話番号やメールアドレスについては変更を検討する、又は身に覚えのない不審な電話やメールは無視をする、若しくは未登録の電話番号やメールの着信拒否設定を行う等の対策を取ってください。

今後の生活の中で、個人情報の悪用事案を認知した場合は、個人情報を入力したサイトの URL 等の資料をご持参のうえで、最寄りの警察署にご相談ください。

Q：　フィッシングサイトにクレジットカード情報を入力して、身に覚えのないクレジットカードの請求があった。

A：　自身のクレジットカードの情報を入力してしまった場合は、クレジットカードの発行会社に連絡して、クレジットカードの利用停止や再発行の手続き等を

行うとともに、早急に身に覚えの無い請求の有無を確認してください。

クレジットカードの不正利用事案について、被害の届出をされる場合は、クレジットカードの利用明細等の本件に関する資料をご持参のうえで、最寄りの警察署にご相談ください。

なお、クレジットカードの不正利用にかかる商品の売買契約の無効化や代金請求の免除等に関する要望については、クレジットカード発行会社等にお問い合わせください。

また、不審な通販サイトやフィッシング詐欺と思われるサイトにメールアドレスやパスワードを入力し、同じパスワードを他のサービスでも使いまわしているような場合には、不正アクセスの被害を受ける危険性があるため、パスワードなどの変更を行ってください。

Ｑ：　携帯電話に不審なメールやＳＭＳ（架空請求・荷物の不在通知・アカウントやカードの停止等）が届いた。

Ａ：　送信元や内容に身に覚えのない料金の請求については、対応する必要はありません。

荷物の不在通知については、宅配業者を装ったものの可能性があり、その場合、ＵＲＬに接続すると不正なアプリをインストールさせられる、またはフィッシングサイトに誘導させられる恐れがありますので注意してください。

また、銀行やカード会社が、メールで暗証番号やパスワードなどの個人情報を確認することはありませんので、絶対に個人情報を入力しないようにしてください。

心当たりのないメールに添付されたファイルの実行や、メール本文に記載されたＵＲＬへのアクセスはしないようにしてくだい。

心当たりがある場合は、対象のサービスの事業者の公式サイトや公式アプリからアクセスのうえ、確認するようにしてください。

Ｑ：　ＳＮＳや掲示板で誹謗中傷の投稿をされた、または個人情報を載せられた。

Ａ：　誹謗中傷を受けたり、個人情報を載せられた場合は、そのサービスの管理者を確認し、削除依頼を行ってください。

投稿内容が名誉毀損や業務妨害等の犯罪に該当すると思われる場合は、投稿されている内容が確認できる資料を持参のうえで、最寄りの警察署に相談してください。

なお、当該投稿の削除依頼を行った場合、事件化の際に当該投稿に関する資料の入手が困難となる場合があるため、事件化を考える場合の削除依頼については慎重に判断してください。