【個人情報の悪用（フィッシング・不正アクセス）】

クレジットカードが不正利用された

よくある相談内容

○　クレジットカードが不正利用されているとカード会社から連絡があった
○　身に覚えのないクレジットカードの利用履歴があった
○　クレジットカードが不正利用された

不正利用の被害に遭った場合の対処法（一例）

○　クレジットカード会社へ被害連絡を行い、カードの利用停止を依頼するとともに、救済措置等について相談する。
○　クレジットカード情報を登録しているサービスに不正アクセスされた可能性があるため、各アカウントのパスワードを変更し、サービス等で不正利用がないか確認する。
○　カード紛失時・盗難時に不正利用に遭った場合は、警察に遺失届や被害届を提出する。

不正利用につながる主な要因

○　フィッシングによる不正利用
　大手通販会社、宅配業者、金融機関等、実在する企業等を装ったメール（SMS、E メール）を送信し、添付した URL にアクセスさせてクレジットカード情報等を盗み取って悪用する。
○　ネットショッピング詐欺等による不正利用
　偽のショッピングサイト等で、代金の支払方法としてクレジットカード情報等を入力した場合、それらの情報が盗まれて悪用される。
○　個人情報漏洩による不正利用
　クレジットカード会社など、個人情報を管理している会社が不正アクセス等の被害に遭い、情報が漏洩した場合、その情報を入手した悪意のある者によって悪用される。
○　なりすましによる不正利用
　クレジットカード情報やクレジットカードそのものを盗んだり拾ったり

して、カード名義人になりすまして悪用する。

○　スキミングによる不正利用

ATM の挿入口にスキマーを取り付けて、カード情報を盗んで悪用する。

被害に遭わないための対策

主に前記パターンによりクレジットカード不正利用の被害に遭う可能性があることから、

○　メール（SMS）の URL リンクには安易にアクセスしない。

○　ブックマークした公式サイトや公式アプリからの利用を基本とし、パスワードや認証コード等を安易に入力しない。

○　「アカウント停止」「支払いの未納」等、不安を煽るメールは疑う。

○　迷惑メール等の受信拒否について携帯電話会社に相談する。

○　ウイルス対策ソフトを導入する。

○　カード紛失・盗難時、すぐにカード会社に連絡する。

【被害軽減策】

○　パスワード対策

・　クレジットカード情報を登録しているサービスの ID・パスワードは、できるだけ「長く」「複雑」なものに設定し、他のサービスなどで使い回しをしない。

・　多要素認証が提供されている場合は利用する。

○　３Ｄセキュア認証の利用

・　クレジットカード情報の盗用による不正利用を防止するために、大手クレジットカード会社が推奨する本人認証サービスを利用する。

・　３Ｄセキュア認証によって新たに設定するパスワード等には、他のサービスで使用しているパスワード等は絶対に使用しない。

参考サイト

前ページ「参考リンク集」を参照

○　フィッシング対策協議会

○　迷惑メール相談センター（日本データ通信協会）