独立行政法人
国民生活センター

【法人番号 4021005002918】

報道発表資料

令和４年12月21日
独立行政法人国民生活センター

通販サイト、カード会社、宅配便事業者などをかたる偽 SMS・メールに警戒を！
- 身近な事業者からの不安なメッセージ、じつは危険な“フィッシング”かも -

通販サイト、クレジットカード会社、宅配便事業者などの実在する組織をかたるメールや SMS（ショートメッセージサービス）を送信し、パスワードや ID、暗証番号、クレジットカード番号などの個人情報を詐取するフィッシングに関する相談が全国の消費生活センター等に寄せられています。

フィッシングの手口では、「支払い方法に問題がある」など消費者の不安をあおるメールや SMS が送られてきます。普段よく利用する事業者からのメッセージに見えても、じつは危険なフィッシングの手口かもしれません。こうしたメールや SMS が届いてもあせらず冷静に対応することが大切です。記載された URL には安易にアクセスせず、ブックマークした正規の URL や正規のアプリからアクセスすることを日ごろからの習慣にしましょう。メールや SMS に記載された URL にアクセスしてしまっても、個人情報は絶対に入力しないでください。

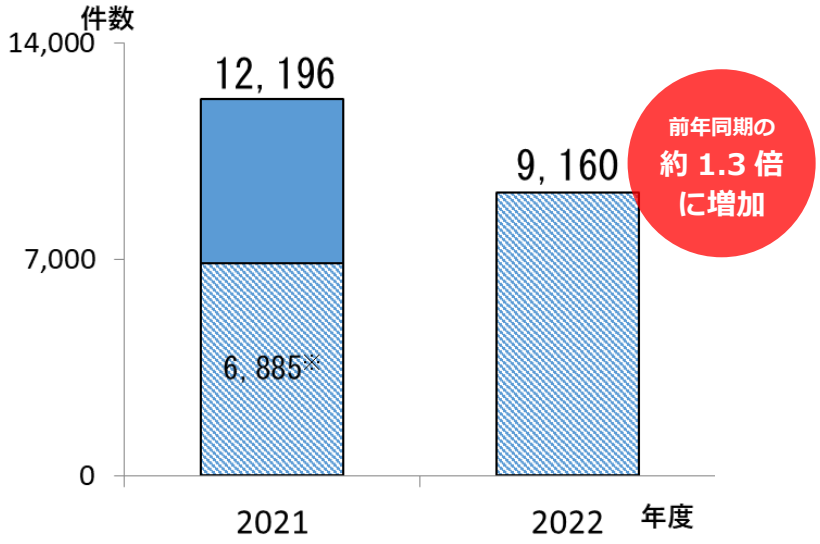
かたられる事業者等と偽 SMS・メールの内容

かたられる事業者等	偽 SMS・メールの内容（例）
通販サイト・ フリマサイト（アプリ）	・「支払い方法に問題がある」 ・「不正利用が確認された」 ・「アカウントで異常な動作が検出された」　など
クレジットカード会社・ 金融機関	・「カードの不正な取引があった」 ・「本人の利用かどうか確認させてほしい」 ・「回答がない場合、カードの利用制限が継続される」　など
宅配便事業者	・「お客様宛にお荷物のお届けにあがりましたが不在の為持ち帰りました。下記よりご確認ください」　など
携帯電話会社	・「支払いが滞っている」 ・「通信サービスの停止と契約解除通告のお知らせ」 ・「携帯電話料金未納の為、今日までに〇〇万円を支払うように」　など
公的機関	・「未払いの税金がある」 ・「納付期限を経過した税金を完納していません」　など

１．相談件数

全国の消費生活センター等に寄せられたフィッシングに関する相談を年度別にみると、2021 年度は 12,196 件になっています。その後、2022 年度は 9,160 件となっており、2021 年度の同期件数（6,885 件）の約 1.3 倍に増加しています[1]（図１）。

図１　フィッシングに関する相談の年度別件数（2021～2022 年度）



※2021年度同期件数（2021年11月30日までのPIO-NET登録分）は6,885件

２．相談事例（（ ）内は受付年月、相談者の属性）

フィッシングに関する相談事例では、通販サイトなどをかたるメールや SMS に記載されている URL にアクセスし、クレジットカード番号等を入力したあとに身に覚えのない請求がきたなどのケースがみられます。

【事例１】通販サイトから SMS が届きクレジットカード番号を入力したら覚えのない請求がきた

通販サイトから「支払い方法に問題がある」との SMS がスマートフォンに届いた。疑いもせず指示通りに添付の URL をタップし、クレジットカード番号や住所を入力した。その後、クレジットカードの請求明細を確認したら、合計約４万円の身に覚えのない決済があった。クレジットカード会社には状況を伝えたが、今後どうしたらよいか。

（2022 年１月受付　30 歳代　男性）

【事例２】フリマアプリ名でメールが届きパスワードを入力したらアカウントを不正利用された

自分が利用しているフリマアプリ名でアカウントの設定の確認を求める内容のメールが届き、メールアドレスとパスワードを入力してしまった。その後、フリマアプリにログインしたところ、自分が利用していない約 20 万円の取引履歴があり、自分のアカウントが不正利用されていることがわかった。フリマアプリで利用している決済サービスには銀行口座を登録しているが、どうし

[1] 2022 年 11 月 30 日までの PIO-NET 登録分。PIO-NET（パイオネット：全国消費生活情報ネットワークシステム）とは、国民生活センターと全国の消費生活センター等をオンラインネットワークで結び、消費生活に関する相談情報を蓄積しているデータベースのこと。消費生活センター等からの経由相談は含まれていない。

たらよいか。

（2022 年５月受付　30 歳代　女性）

【事例３】不在通知の SMS が届きアプリをインストールしたら覚えのない高額請求がきた

通販で購入した商品の到着を待っていた頃、宅配便事業者から「お荷物の住所が不明でお預かりしています」という SMS が届いた。SMS には「確認のため指定のアプリをインストールして欲しい」と書かれていたので、記載されている URL をタップしてアプリをインストールした。

その後、予定していた荷物は別の宅配便事業者から届いたので不審に思っていたところ、最近、私のスマートフォンの決済用に登録しているクレジットカードに、携帯電話会社から通常より高額な請求があがってきた。利用明細を調べると、プラットフォーム上で計 10 件以上の不審な利用があり、約６万円の身に覚えのないキャリア決済の請求があった。全て、不審なアプリをインストールした日時に近い時間帯での利用だった。どうしたらよいか。

（2022 年２月受付　40 歳代　女性）

【事例４】携帯電話会社を名乗る SMS が届き ID とパスワードを入力したら覚えのない請求がきた

契約している携帯電話会社を名乗り「ご利用料金のお支払いが確認できておりません。以下の URL からご確認が必要です」との SMS が届いたためアクセスしたところ、キャリア決済のログイン ID とパスワードの入力を求められ入力した。その後、身に覚えのない請求が約８万円あった。不正利用された分を取り消してほしい。

（2021 年 10 月受付　30 歳代　男性）

３．フィッシングの手口と事例の特徴

①かたられる組織と偽 SMS・メールの内容

フィッシングの手口では、通販サイト、フリマサイト（アプリ）、クレジットカード会社、金融機関、宅配便事業者、携帯電話会社などがかたられるケースが目立つほか、官公庁などの公的機関がかたられるケースもみられます。

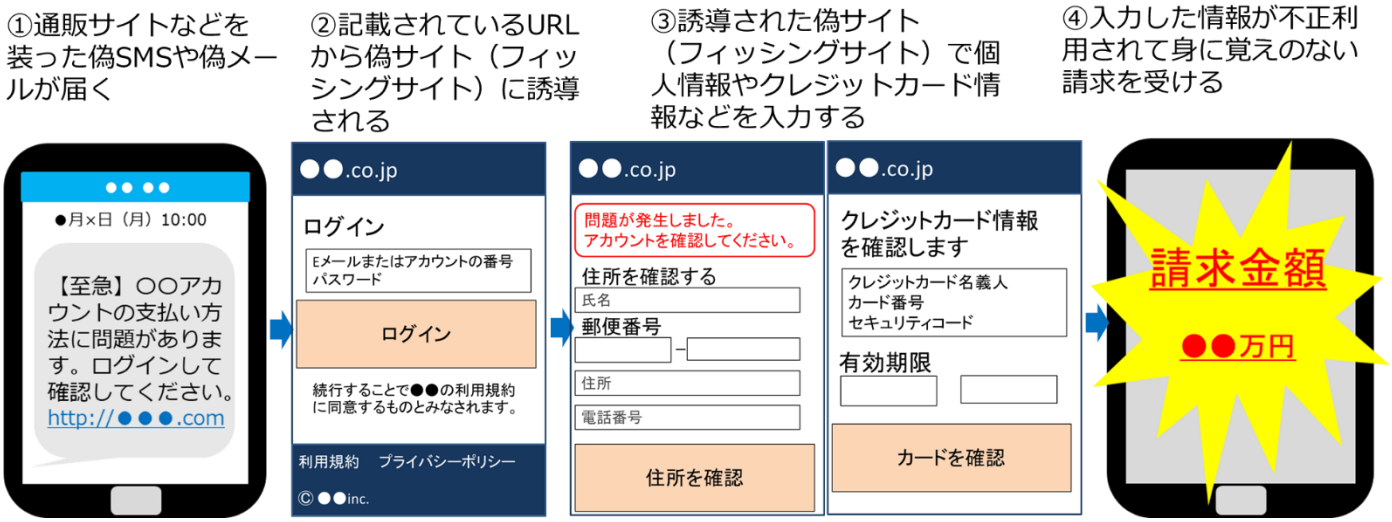
また、こうした組織をかたって送られてきた偽 SMS や偽メールには、「支払い方法に問題がある」「料金の未納がある」「不正利用が確認された」など消費者の不安をあおる記載がみられます。

②事例の特徴

フィッシングの事例では、誘導された偽サイト（フィッシングサイト）で個人情報やクレジットカード情報、アカウント情報（メールアドレス、ID・パスワード）、認証コード、暗証番号等の入力を求められるケースが目立っており、入力した情報がクレジットカード、キャリア決済などで不正利用され、身に覚えのない請求を受けるケースがみられます。

また、誘導されたフィッシングサイトで個人情報を入力したあとプリペイド型電子マネーの購入を指示されるケースや、アクセスしたサイトで不正なアプリをインストールしてしまうケースもみられます。

フィッシングのイメージ



４．消費者へのアドバイス

不安な内容のメールや SMS が送られてきた際の対応

（１）あせらず冷静に！　メールや SMS に記載された URL には安易にアクセスしないでください

消費者の不安をあおるフィッシングの手口には、あせらず冷静に対応することが大切です。メールや SMS に記載された URL はフィッシングサイトにつながる可能性があるため、安易にアクセスしないでください。事業者の正規のサイトでフィッシングに関する情報がないか確認しましょう。

（２）フィッシングサイトにアクセスしてしまっても個人情報は絶対に入力しないでください

フィッシングサイトにアクセスしてしまった場合、クレジットカード情報、ID・パスワード、認証コードや暗証番号等の個人情報の入力を求められるケースがあります。こうした情報をフィッシングサイトで入力してしまうと、クレジットカードやキャリア決済などを不正利用されるおそれがあります。万が一こうしたサイトにアクセスしてしまった場合でも、個人情報は絶対に入力しないでください。

また、フィッシングサイトにアクセスしたあと、提供元不明の不正なアプリをダウンロードするよう誘導されるケースがあります。公式マーケットにあるもの以外の「提供元不明のアプリ」をダウンロードしたりインストールしたりしないようにしましょう。また、あらかじめ「提供元不明のアプリ」はインストールしない設定にしておきましょう。

万が一重要な情報を入力してしまった場合の対応

（３）フィッシングサイトに ID・パスワード等を入力してしまったらすぐに変更し、クレジットカード会社などにも連絡しましょう

フィッシングサイトにクレジットカード情報や ID・パスワード、暗証番号等を入力したまま放置すると、クレジットカードやキャリア決済などを不正利用されてしまう状態が続きます。こうした重要な情報をフィッシングサイトに入力したと気付いた場合には、すぐに ID・パスワード、

暗証番号等を変更し、クレジットカード会社や携帯電話会社などにも連絡しましょう。

日ごろからの対策

（４）ブックマークした正規の URL や正規のアプリからアクセスすることを日ごろからの習慣にしましょう

フィッシングの被害にあわないために、ブックマークした正規の URL や正規のアプリからアクセスすることを日ごろからの習慣にしましょう。また、定期的にブックマークが正しいものかを確認しましょう。

（５）迷惑 SMS やメール、ID・パスワード等の不正利用への事前対策をしておきましょう

①セキュリティソフトや携帯電話会社の対策サービス等を活用しましょう

利用者の安全を目的に様々な対策サービスが提供されています。セキュリティソフトや、携帯電話会社などが提供するフィルタリングサービスなどを活用しましょう。また、事業者によっては不正ログイン対策として「２段階認証」などの設定が可能になっています。こうしたセキュリティ機能も積極的に利用しましょう。

②パスワード等の使い回しはやめましょう

通販サイトやアプリ、SNS などの複数のサービスで同じパスワード等を設定していると、その情報が第三者に知られた場合、同一の設定をしていたサービスも第三者に不正利用されるおそれがあります。パスワード等を複数のサービスで使い回すことはやめて、しっかり管理しましょう。

③クレジットカードの利用明細は必ず確認！　利用限度額の見直しも検討しましょう

クレジットカードの利用明細は必ず確認するようにしましょう。定期的に確認することで、不正利用の被害を早期に把握することができます。また、クレジットカードの利用限度額も利用明細などで確認することができます。万が一不正利用の被害に遭った場合の被害額を最小限にとどめるための対策として、自分が利用しているクレジットカードの利用限度額を見直しすることも一法です。

携帯電話のキャリア決済についても利用限度額を自分で設定することが可能なため、必要最低限の額に引き下げておきましょう。キャリア決済の機能自体を利用しない設定が可能な携帯電話会社もありますので、利用しないのであれば設定を変更しましょう。

（６）不安に思った場合や、トラブルが生じた場合は、すぐに最寄りの消費生活センター等へ相談しましょう

＊消費者ホットライン：「１８８（いやや！）」番

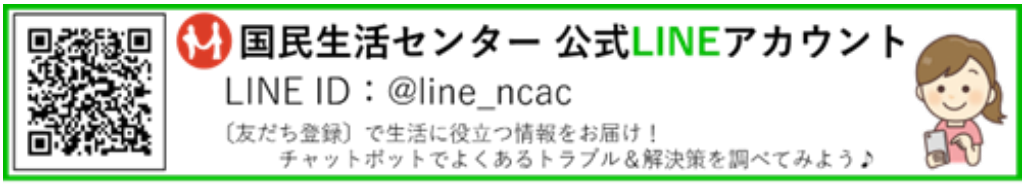
最寄りの市区町村や都道府県の消費生活センター等をご案内する全国共通の３桁の電話番号です。

５．情報提供先

本報道発表資料を、以下に情報提供しました。

・消費者庁（法人番号 5000012010024）
・内閣府消費者委員会事務局（法人番号 2000012010019）
・総務省（法人番号 2000012020001）
・警察庁（法人番号 8000012130001）
・フィッシング対策協議会（法人番号 なし）
・独立行政法人情報処理推進機構（法人番号 5010005007126）
・一般財団法人日本サイバー犯罪対策センター（法人番号 2010405013081）

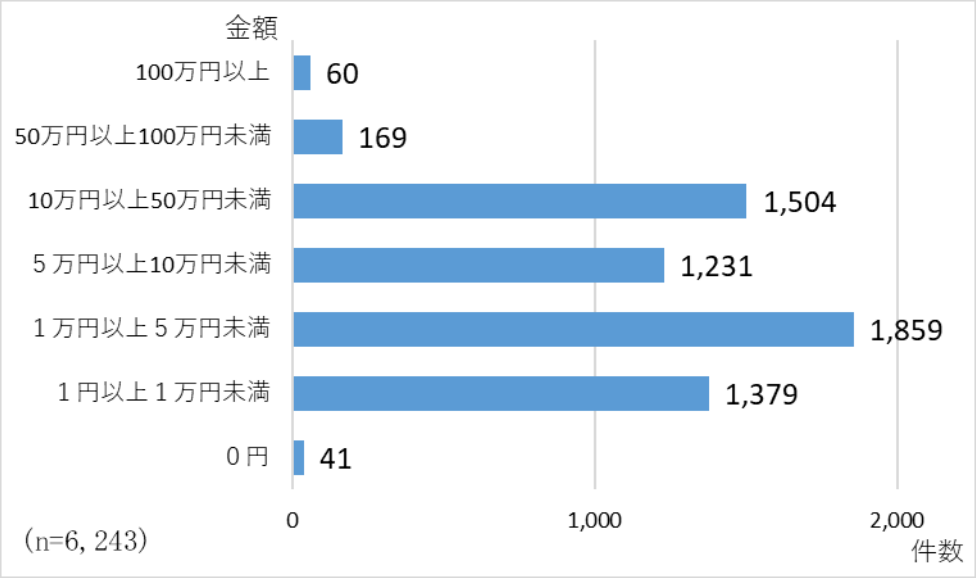
国民生活センター公式LINEアカウントでも、さまざまな消費者トラブルの情報を発信しています。



【参考１】契約購入金額別の相談件数

フィッシングに関する相談における契約購入金額[2]をみると、「１万円以上５万円未満」のケースが多くなっていますが、10 万円以上の高額なケースも多く、平均金額は約 12 万円[3]となっています（図２）。

図２ 契約購入金額別の相談件数（2021～2022 年度受付分）[4]



【参考２】国民生活センターおよび関係機関による注意喚起等

・国民生活センター見守り新鮮情報第 420 号「実在する組織をかたるフィッシングメールに注意！」（2022 年５月 24 日）
https://www.kokusen.go.jp/mimamori/mj_mailmag/mj-shinsen420.html

・国民生活センター「宅配便業者を装った『不在通知』の偽 SMS に注意しましょうーURL にはアクセスしない、ID・パスワードを入力しない！ー」（2020 年 11 月 26 日）
https://www.kokusen.go.jp/news/data/n-20201126_2.html

・国民生活センター「携帯電話会社をかたる偽 SMS にご注意！ーあなたのキャリア決済が狙われていますー」（2019 年９月５日）
https://www.kokusen.go.jp/news/data/n-20190905_1.html

・総務省「電気通信サービス Q&A」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_faq/index.html

[2] 不正利用による請求金額のほか、偽 SMS・メールに記載されている架空の請求金額等を含む。
[3] 契約購入金額が０円のものを含めて算出した平均金額。
[4] 無回答を除いて集計した。

・フィッシング対策協議会「緊急情報」
https://www.antiphishing.jp/news/alert/

・フィッシング対策協議会「マンガでわかるフィッシング詐欺対策５ヶ条」
https://www.antiphishing.jp/phishing-5articles.html

・フィッシング対策協議会「利用者向けフィッシング詐欺対策ガイドライン」
https://www.antiphishing.jp/report/guideline/

・独立行政法人情報処理推進機構（IPA）「国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意－不審なショートメッセージやメールの URL に触れないで！－」（2022 年 10 月 31 日）
https://www.ipa.go.jp/security/anshin/mgdayori20221031.html

・独立行政法人情報処理推進機構（IPA）「宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中 ～偽 SMS から不正アプリのインストールやフィッシングの被害にあう手口に引き続き注意！～」（2021 年 12 月 22 日）
https://www.ipa.go.jp/security/anshin/mgdayori20211222.html

・独立行政法人情報処理推進機構（IPA）「URL リンクへのアクセスに注意！－主な手口と、被害にあわないための対策について－」（2021 年８月 31 日）
https://www.ipa.go.jp/security/anshin/mgdayori20210831.html

・一般財団法人日本サイバー犯罪対策センター「インターネットバンキングの不正送金による被害を防ぐために」（2022 年９月 22 日）
https://www.jc3.or.jp/threats/topics/article-463.html

・一般財団法人日本サイバー犯罪対策センター「フィッシングターゲットの変遷」（2022 年２月４日）
https://www.jc3.or.jp/threats/topics/article-430.html

・一般社団法人セーファーインターネット協会　啓発コンテンツ
https://www.saferinternet.or.jp/e-commerce/studygroup/