独立行政法人
国民生活センター

【法人番号 4021005002918】

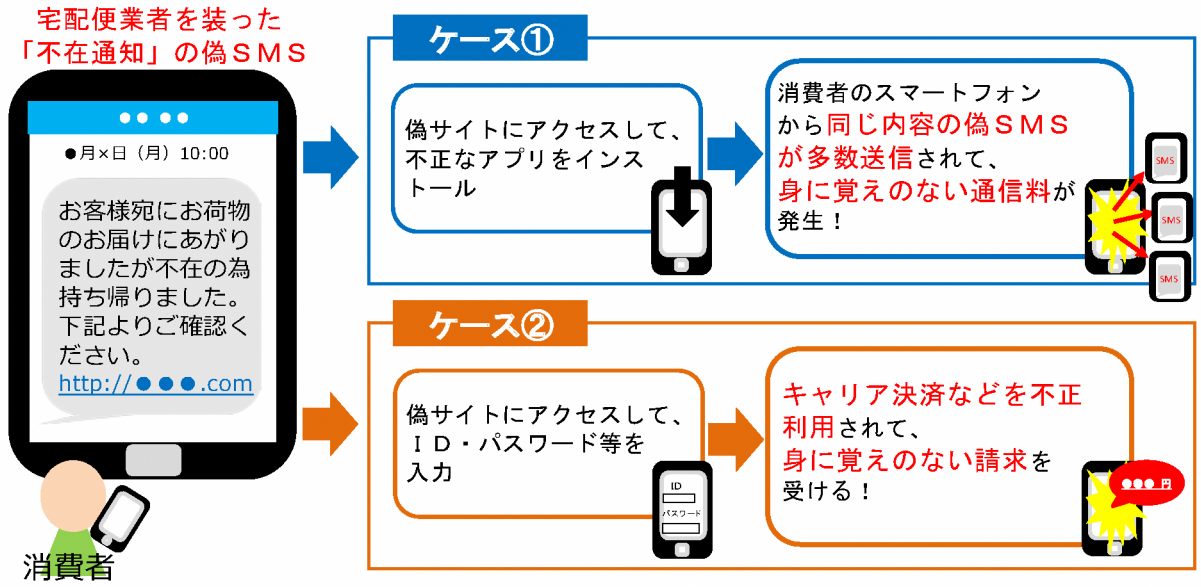
報道発表資料

令和２年11月26日
独立行政法人国民生活センター

宅配便業者を装った「不在通知」の偽ＳＭＳに注意しましょう
- ＵＲＬにはアクセスしない、ＩＤ・パスワードを入力しない！ -

全国の消費生活センター等には、宅配便業者を装った「不在通知」の偽ＳＭＳに関する相談が寄せられています。消費者に送られてくるＳＭＳ（ショートメッセージサービス）には偽サイトに誘導するためのＵＲＬが記載されており、相談事例では、偽サイトにアクセスして不正なアプリをインストールした結果、同じ内容のＳＭＳが自身のスマートフォンから自動的に多数の宛先に送信されてしまい、身に覚えのない通信料を請求されるケースがみられます。また、アクセスした偽サイトで入力したＩＤ・パスワード、暗証番号、認証コード等が携帯電話会社のキャリア決済[1]などで不正利用されて、身に覚えのない請求を受けるケースもみられます。そこで、相談事例や手口を紹介し、注意を呼びかけます[2]。

トラブルのイメージ

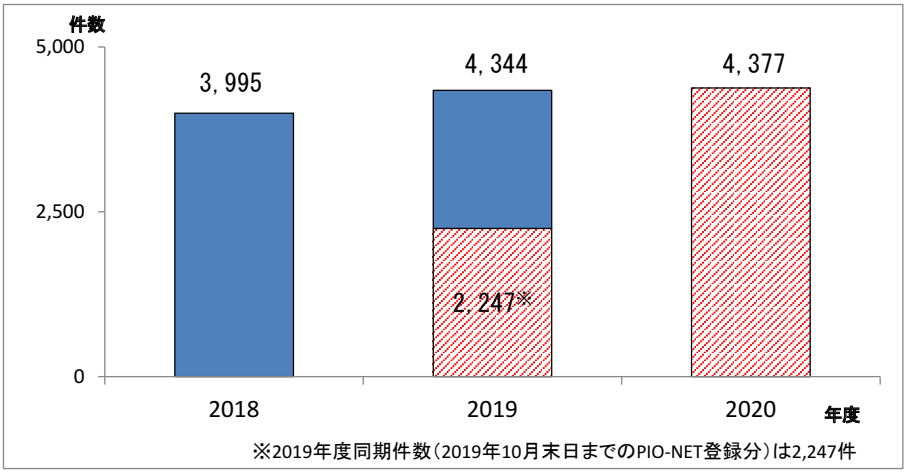


[1] 携帯電話会社のＩＤやパスワード等による認証で商品等を購入した代金を、携帯電話の利用料金等と合算して支払うことができる決済方法のこと。携帯電話会社によって名称は異なる。
[2] 国民生活センターでは、携帯電話会社をかたる偽ＳＭＳについても注意喚起を行っている（国民生活センター「携帯電話会社をかたる偽ＳＭＳにご注意！－あなたのキャリア決済が狙われていますー」（2019年９月５日）http://www.kokusen.go.jp/news/data/n-20190905_1.html 参照）。

１．相談件数の推移

「不在通知」のＳＭＳに関する相談は、2018 年度以降多くみられるようになり、年度別に相談件数をみると、2018 年度が 3,995 件、2019 年度が 4,344 件と増加しています。2020 年度も 4,377 件となっており、前年度同期件数（2,247 件）と比べると２倍近くに増加しています（**図１**）。

図１　「不在通知」のＳＭＳに関する年度別相談件数 [3]



２．相談事例（（）内は受付年月、契約当事者の属性）

ケース① 偽サイトにアクセスしたあと自身のスマートフォンからＳＭＳが多数送信されてしまった

【事例１】「不在通知」のＳＭＳが届きリンク先にアクセスしたあと、海外宛てにＳＭＳが 100 回以上送信されていた

スマートフォンに宅配荷物の不在通知のＳＭＳが届き、確認するためリンク先にアクセスした。すると何かダウンロードするような画面になったが、すぐ元に戻ったので静観していた。数日後、見知らぬ複数の相手から電話の着信があり、不在配達の荷物の受け取りについての申し出を受けたので「私は無関係だ」と伝えて電話を切った。

その後、電話番号を変更するため携帯電話のショップを訪れ、請求内容を確認したところ、ＳＭＳが届いて以降、私の電話番号から海外宛てにＳＭＳが 100 回以上送信されているとのことで、通信料を１万円以上請求されていた。請求を取り消してほしい。

（2020 年８月受付　40 歳代　男性）

【事例２】「不在通知」のＳＭＳを受け取りブラウザの更新をしたら、海外と国内宛てにＳＭＳが送信されていた

宅配便の不在通知のＳＭＳを受け取り、記載されているＵＲＬにアクセスしたところ、ブラウザのアイコンが出てきて、「更新してください」とあったので更新してしまった。この時に不正アプリをインストールしてしまったようだ。

[3] 2020 年 10 月 31 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。

その日のうちに知らない人から「いつ配達できるか」といった内容の電話が多くかかってきた。その後、携帯電話会社から請求書が来たので、明細を確認すると海外宛てのＳＭＳが 100 通、国内宛ても 100 通ほど自分のスマートフォンから送られていた。送信されたＳＭＳの料金が１万円以上となっており、支払いたくない。

（2020 年８月受付　30 歳代　女性）

ケース② 偽サイトにアクセスしたあとキャリア決済などを不正利用されてしまった

【事例３】「不在通知」のＳＭＳに記載されていたＵＲＬにアクセスしたあと、キャリア決済で電子マネーを購入されていた

数か月前にスマートフォンに宅配便の不在連絡のようなＳＭＳが届いたので、記載されていたＵＲＬにアクセスした。その時に何を入力したのか明確には覚えていないが、氏名などの個人情報を入力して返信してしまったかもしれない。その後、約 11 万円がキャリア決済されていて、電子マネーが購入されていることが分かった。

（2020 年５月受付　40 歳代　男性）

【事例４】「不在通知」のＳＭＳが来てＩＤなどを入力したら、プラットフォームで決済されてしまった

宅配便業者から不在配達のＳＭＳが来て、ＵＲＬをクリックしたらホームページが出てきた。そこにプラットフォーム事業者のＩＤ、パスワードを入力したら、約９万円をプラットフォームで決済されてしまった。もう、お金は戻らないだろうか。

（2020 年４月受付　40 歳代　男性）

３．消費者へのアドバイス

トラブルに遭わないために・・・

（１）ＳＭＳやメールで「不在通知」が届いても、記載されているＵＲＬには安易にアクセスしないようにしましょう。

スマートフォンや携帯電話に届いたＳＭＳやメールが宅配便業者からの正式なものかどうか見分けることは困難です。ＳＭＳによる「不在通知」を行っていない宅配便業者もありますので、自分で調べた宅配便業者の電話窓口や公式ホームページ等で真偽を確認し、もし「不在通知」を内容とするＳＭＳやメールが届いても、記載されたＵＲＬに安易にアクセスしないようにしましょう。

（２）ＵＲＬにアクセスした場合でも、提供元不明のアプリをインストールしたり、ＩＤ・パスワード等を入力したりしないようにしましょう

偽ＳＭＳに記載されているＵＲＬに万が一アクセスしてしまった場合、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。自分のスマートフォンなどに不正なアプリをダウンロードしてインストールしてしまうと、自動的にＳＭＳが任意の宛先に送信されるなどの被害に遭うおそれがあります。

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。

偽ＳＭＳに記載されているＵＲＬにアクセスすると、銀行や宅配便業者などを装った偽サイト（フィッシング[4]サイト）に誘導されてＩＤ・パスワード、暗証番号や認証コード、電話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。こうした情報を偽サイトで入力してしまうと、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ＵＲＬにアクセスしてしまった場合でも、ＩＤ・パスワード等を入力しないようにしましょう。

万が一、操作してしまったら・・・

（３）不正なアプリをインストールした場合にはスマートフォンを機内モードにして、アプリをアンインストールしましょう

万が一不正なアプリをインストールしてしまった場合には、スマートフォンなどを機内モードに設定し、Ｗｉ-Ｆｉ接続などもオフにしたうえで、不正なアプリをアンインストールしましょう。アンインストールの方法が分からない場合には、契約している携帯電話会社等に問い合わせてください[5]。また、より安全な対応策としてスマートフォンの初期化も検討しましょう。

自分では気付かないまま不正なアプリをインストールしていたというケースもありますので、自身のスマートフォンから勝手にＳＭＳが送信されているなどの不審な点があったら、不正なアプリがインストールされていないか確認してください。

（４）偽サイトにＩＤ・パスワード等を入力してしまったら、すぐに変更しましょう

偽サイトにＩＤ・パスワードや暗証番号等を入力したまま放置すると、キャリア決済などを不正利用されたり、自分の契約情報を閲覧・変更されたりしてしまう状態が続きます。偽サイトに情報を入力したと気付いた場合のほか、身に覚えのない２段階認証の通知やキャリア決済メールなどが届いた場合には、すぐにＩＤ・パスワード等を変更し、決済の請求が発生していないかを携帯電話会社等に確認しましょう。

日ごろからの対策を・・・

（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携帯電話会社の対策サービスやセキュリティーソフト等を活用しましょう

携帯電話会社などではメールフィルタリングサービスなどの対策サービスを提供している場合があります。携帯電話会社などが提供する迷惑ＳＭＳ・メール等への対策サービスやセキュリティーソフト等を活用しましょう。

---

[4] 実在の事業者を装ってメール・ＳＭＳ等を送り、メール内に記載したＵＲＬから実在の事業者のサイトにそっくりな偽サイト（フィッシングサイト）へ誘導し、消費者に個人情報等を入力させ、情報を詐取する手口のこと。ＳＭＳで行われるフィッシングは「スミッシング」と呼ばれる。

[5] 独立行政法人 情報処理推進機構（ＩＰＡ）のホームページでもアンインストールの方法が確認できる（「参考２」を参照）。

②ＩＤ・パスワード等の使い回しはやめましょう

通販サイトやＳＮＳなどの複数のサービスで同じＩＤとパスワード等を設定していると、そのＩＤ等の情報が第三者に知られた場合、同一のＩＤ等を設定していたサービスを第三者に不正利用されるおそれがあります。同じＩＤ・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キャリア決済の限度額を必要最小限に設定するか、利用しない設定に変更しましょう

携帯電話の契約者は自分で設定を変更しない限り、キャリア決済が利用できる設定になっています。キャリア決済の利用限度額は自分で設定可能なため、必要最低限の額に引き下げ、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ましょう。また、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利用しない設定に変更しましょう。

不安に思ったら・・・

（６）不安に思ったりトラブルに遭ったりした場合は最寄りの消費生活センター等に相談してください

宅配便業者を装う偽ＳＭＳの「不在通知」を受け取って不安に思ったり、トラブルに遭ったりした場合には、すぐに最寄りの消費生活センター等に相談してください。

※消費者ホットライン：「１８８（いやや！）」番

最寄りの市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。

※警察相談専用電話「＃９１１０」

４．情報提供先

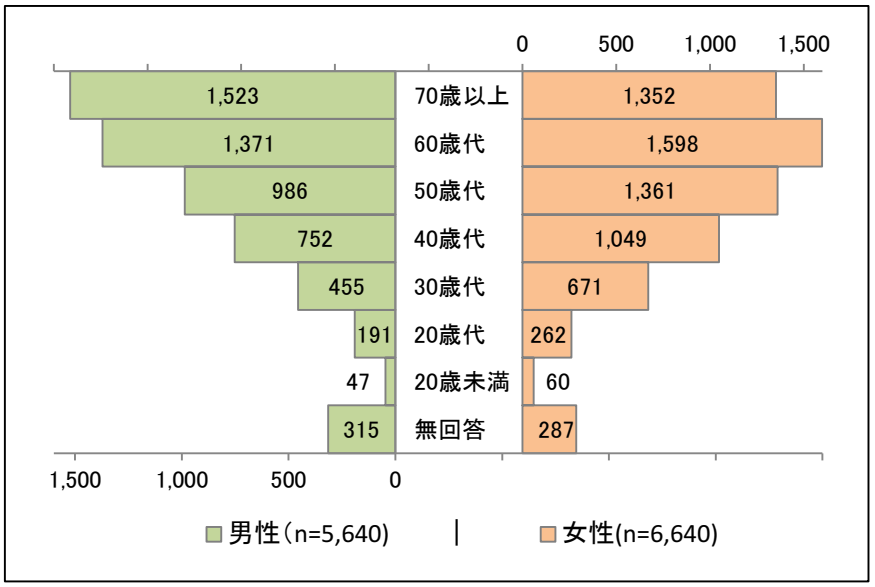
本報道発表資料を、以下の関係機関に情報提供しました。

・消費者庁 消費者政策課 （法人番号 5000012010024）
・内閣府 消費者委員会事務局 （法人番号 2000012010019）
・総務省総合通信基盤局 電気通信事業部 消費者行政第二課 （法人番号 2000012020001）
・総務省サイバーセキュリティ統括官室 （法人番号 2000012020001）
・警察庁生活安全局 情報技術犯罪対策課 （法人番号 8000012130001）
・独立行政法人情報処理推進機構 （法人番号 5010005007126）
・フィッシング対策協議会 （法人番号 なし）
・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）
・電気通信サービス向上推進協議会 （法人番号 なし）

参考１．相談における性別・年代別の傾向

「不在通知」のＳＭＳに関する相談について契約当事者（ＳＭＳを受け取った当事者等）の属性をみると、男女ともに 60 歳代や 70 歳以上の高齢者が目立ちますが、40 歳代や 50 歳代のケースも多くみられます（**図２**）。

図２ 契約当事者の性別ごとにみた年代別の相談件数（2018～2020 年度受付分）[6]



参考２．事業者および関係機関からの注意喚起等

（１）宅配便事業者

・佐川急便「佐川急便を装った迷惑メールにご注意ください」
https://www2.sagawa-exp.co.jp/whatsnew/detail/721/

・ヤマト運輸「ヤマト運輸の名前を装った『迷惑メール』および『なりすましサイト』にご注意ください」
https://www.kuronekoyamato.co.jp/ytc/info/info_181212.html

・日本郵便「当社の名前を装った迷惑メール及び架空Ｗｅｂサイトにご注意ください。」
https://www.post.japanpost.jp/notification/notice/2019/1031_01.html

[6] 2020 年 10 月 31 日までの PIO-NET 登録分。性別の不明・無回答等を除いて集計した。

（２）携帯電話会社

・ＮＴＴドコモ「宅配業者を装った迷惑ＳＭＳにご注意ください」
https://www.nttdocomo.co.jp/info/spam_mail/column/20180725/index.html

・ソフトバンク「配送業者などを装った不審なメールに関するご注意」
https://www.softbank.jp/mobile/info/personal/news/support/20201005a/
・同「迷惑行為・犯罪行為から守る（携帯電話やスマートフォンを正しく利用するために）」
https://www.softbank.jp/corp/csr/responsibility/safety/nuisance/

・ＫＤＤＩ（ａｕ）「企業を装って発信される不審なメールにご注意ください」
https://news.kddi.com/important/news/important_20201120889.html

（３）その他関係機関

・独立行政法人情報処理推進機構（ＩＰＡ）「宅配便業者をかたる偽ショートメッセージに引き続き注意！」
https://www.ipa.go.jp/security/anshin/mgdayori20200220.html

・一般財団法人日本サイバー犯罪対策センター「運送系企業を装ったフィッシングの注意喚起」
https://www.jc3.or.jp/topics/smsphishing.html

・フィッシング対策協議会「宅配便の不在通知を装うフィッシング」
https://www.antiphishing.jp/news/alert/fuzaiSMS_20201030.html