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

令和元年９月５日
独立行政法人国民生活センター

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 -

全国の消費生活センター等には、「携帯電話会社名で『不正ログインされた可能性があるので、ＩＤとパスワードを変更してください』等のＳＭＳ（ショートメッセージサービス）が届き、携帯電話会社のＩＤ、パスワード、暗証番号等を入力したら、その後携帯電話会社から身に覚えのない決済メールが届いた」など、携帯電話会社をかたる偽ＳＭＳをきっかけに消費者のキャリア決済[1]が不正利用されたという相談が寄せられています。そこで、相談事例や手口を紹介し、消費者に注意を呼びかけます。

１．相談事例（カッコ内は受付年月、契約当事者（ＳＭＳが届いた人）の属性）

【事例１】「電話代が高額になっている」とのＳＭＳがきっかけでキャリア決済が不正利用された

自分が契約している携帯電話会社名で「電話代が高額になっています」とのＳＭＳが届いた。確認しようとＳＭＳ内のＵＲＬにアクセスし、携帯電話会社の自分のＩＤ、パスワード、暗証番号を入力した。その直後に携帯電話会社から２段階認証の確認メールが届き、認証した。その１時間後から、通販サイトで決済されたというメールが携帯電話会社から次々に届き、キャリア決済で約９万円が不正利用されたことがわかった。

（2019 年７月受付　30 歳代　女性）

【事例２】「プレゼントがある」とのＳＭＳがきっかけでキャリア決済等が不正利用された

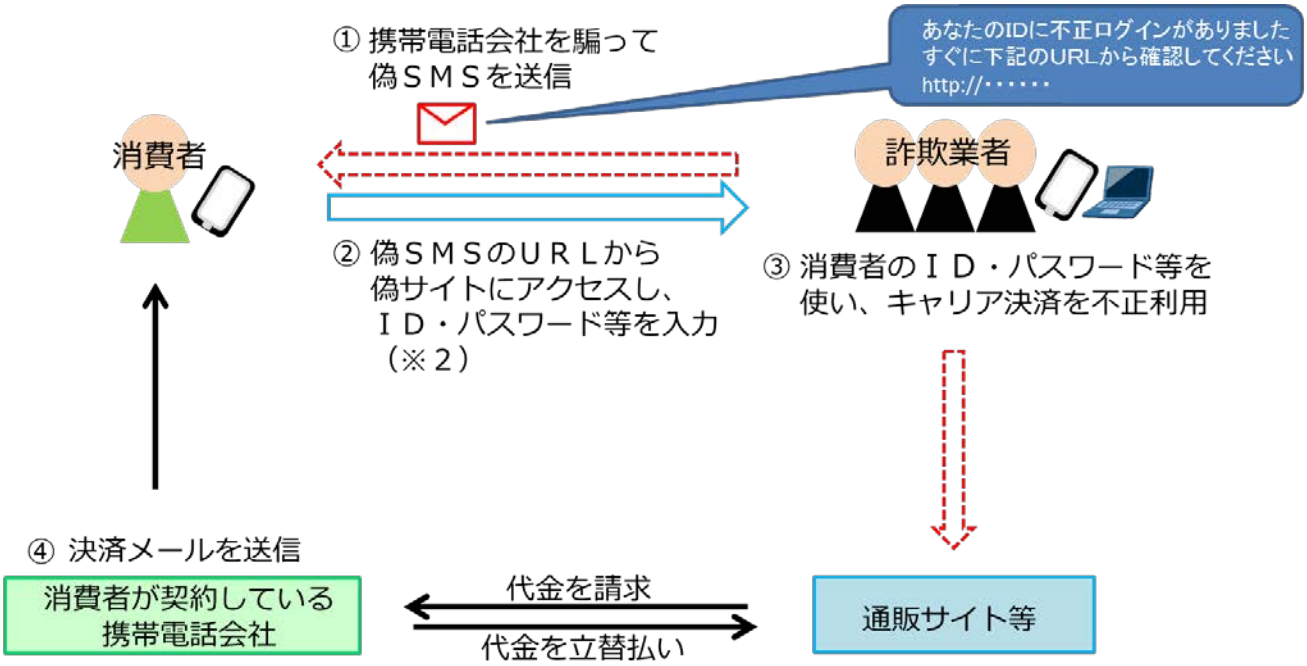
自分が契約している携帯電話会社名で「●●（携帯電話会社）会員限定に商品券 5000 円分をプレゼント致します。下記ページで確認してください」とＵＲＬ付きのＳＭＳが届いた。ＵＲＬをタップすると、いつも利用している携帯電話会社のサイトと同じだったので、よく見ずに自分のＩＤ・パスワード・暗証番号を入力した。その際に、「他の端末が使用許可を求めている」というようなメッセージが表示されたが、許可してしまった。ＩＤ等の入力後すぐに、携帯電話会社からオンラインゲーム関連の決済完了のメールが次々に届き、不正利用に気付いた。約 20 分後にパスワードを変更した後は不正利用が止まったが、キャリア決済と、携帯電話会社のＩＤにひも付いていたクレジットカードの二つで合計約 16 万円が不正利用されてしまった。

（2019 年６月受付　30 歳代　女性）

[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．キャリア決済の不正利用の流れ[2]

図１．キャリア決済の不正利用（イメージ）



①詐欺業者が消費者の携帯電話に、携帯電話会社をかたり、「不正ログインされた可能性がある」「電話代が高額になっている」「プレゼントがある」等の偽ＳＭＳを送信（※１）

②偽ＳＭＳの内容（例：「不正ログインがあったので、すぐにＩＤ・パスワードを変更してください」等）を見た消費者が、偽ＳＭＳ内のＵＲＬから携帯電話会社のサイトにそっくりな偽サイト（フィッシング[3]サイト）へアクセスし、ＩＤ・パスワード・暗証番号等を入力（※２）

③②でＩＤ等のキャリア決済に必要な情報を詐取した詐欺業者が、通販サイト、ギフト券等販売サイト、オンラインゲーム等で消費者のキャリア決済を不正利用（※３）

④消費者の携帯電話に、携帯電話会社からキャリア決済を利用したという決済メールが届き、不正利用に気付く

※１　詐欺業者がＳＭＳの発信元の情報（ＳＭＳを発信する電話番号や発信者名）を偽装して、携帯電話会社からの正式なＳＭＳが届くスレッド・フォルダに偽のＳＭＳが届いたケースもある（参考１）

※２　消費者が２段階認証[4]を設定している場合、詐欺業者が②で詐取したＩＤ等を使い、通販サイト等でキャリア決済を利用しようとする際に、携帯電話会社から消費者の携帯電話に２段階認証の通知がＳＭＳ等で届く。消費者が通知で届いた内容を偽サイト（フィッシングサイト）に入力等して認証してしまうと、消費者のキャリア決済が詐欺業者に不正利用される

※３　携帯電話会社のＩＤにクレジットカードも登録しているケースでは、クレジットカードも不正利用された事例（【事例２】）もある

---

[2] 携帯電話会社によってキャリア決済の流れや認証方法等は異なるため、必ずしも全てのケースに当てはまるわけではない。

[3] 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。

[4] 自分の携帯電話以外の端末（パソコンや他の携帯電話等）から自分のＩＤ・パスワードを使ってログインがあった際に、ＩＤとパスワードの認証の他に、「セキュリティコード」「ワンタイムパスワード」「ワンタイムＵＲＬ」等で更に認証し、第三者による不正なアクセスを防止する仕組みのこと。認証の名称や方法は携帯電話会社によって異なる。

３．アドバイス

（１）携帯電話会社の名称でＳＭＳ・メールが届いても、記載されているＵＲＬには安易にアクセスせず、ＩＤ・パスワード等を入力しないようにしましょう

偽のＳＭＳ・メールや偽サイトは巧妙に作成されており、自分の携帯電話に届いたＳＭＳ・メールが携帯電話会社からの正式なものかどうか見分けることは困難です。もしＳＭＳ・メールが届いた場合には、ＳＭＳ・メール内に記載されたＵＲＬへ安易にアクセスしないようにしましょう。万が一アクセスしてしまった場合も、ＩＤ・パスワード等をすぐに入力しないようにしましょう。自分で調べた携帯電話会社の電話窓口やホームページ等で、ＳＭＳ・メールの内容やサイトが正式なものであることを確認してからアクセス等をするようにしましょう。

あらかじめ、自分の携帯電話の電話帳（アドレス帳）や、インターネットブラウザーのブックマーク（お気に入り）等に、携帯電話会社の電話窓口やホームページのＵＲＬを登録したり、携帯電話会社が提供しているアプリをインストールしておく等、すぐに問い合わせや確認ができるように備えておきましょう。

（２）偽のＳＭＳ・メールに誘導されてＩＤ・パスワード・暗証番号等を入力してしまったら

①すぐにＩＤ・パスワード・暗証番号等やキャリア決済の設定を変更しましょう

詐欺業者にＩＤ・パスワード等を知られた状態で放置すると、再びキャリア決済が不正利用されたり、自分の契約情報を閲覧・変更され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や、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が届いた場合、不安になった場合には、自分で検索した携帯電話会社のホームページにアクセスし、すぐにＩＤ等を変更し、キャリア決済の限度額を必要最低限に引き下げるか、利用を停止しましょう。

②キャリア決済で利用された店舗（サイト）や携帯電話会社に連絡しましょう

詐欺業者が消費者から詐取したＩＤ等を悪用してキャリア決済が不正利用された場合、携帯電話会社から購入店（サイト）名、購入金額等の決済内容が記載されたメールが届きます。購入店や携帯電話会社へトラブルについて申し出ましょう。

（３）キャリア決済の不正利用や偽のＳＭＳ・メールへの事前対策をしましょう

①キャリア決済の限度額を必要最低限に設定するか、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。

②「２段階認証」を設定しましょう

自分が契約している携帯電話会社で２段階認証の仕組みが導入されている場合、２段階認証の設定をしましょう。

③迷惑ＳＭＳ・メール等の対策サービスを活用しましょう

携帯電話会社や、セキュリティーソフト等で、迷惑ＳＭＳ・メール等の対策サービスが提供されています。契約先のサービス内容を確認して活用しましょう。

④ＩＤ・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等、複数のサービスで同じＩＤ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が自分になりすまして利用される可能性があります。同じＩＤ等を複数のサービスで使いまわすことはやめ、しっかり管理しましょう。

（４）不安に思ったりトラブルになった場合は消費生活センター等や警察に相談してください

携帯電話会社の名称で送られたＳＭＳ・メールに関して不安に思ったり、トラブルになった場合は、最寄りの消費生活センター等や警察に相談しましょう。

＊ 消費者ホットライン「１８８（いやや！）」番

＊ 警察相談専用電話「＃９１１０」

４．情報提供先

・消費者庁 消費者政策課 （法人番号 5000012010024）
・消費者庁 取引対策課 （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）
・一般財団法人日本データ通信協会 （法人番号 6013305001870）
・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）
・独立行政法人情報処理推進機構 （法人番号 5010005007126）
・電気通信サービス向上推進協議会 （法人番号 なし）

参考１．相談事例を元に作成した偽ＳＭＳの内容（イメージ）

図２．ＳＭＳの発信元の情報（ＳＭＳを発信する電話番号や発信者名）を偽装して、携帯電話会社からの正式なＳＭＳが届くスレッド・フォルダに偽のＳＭＳが届くケース

図３．ＳＭＳ内で携帯電話会社の名称を記載しているケース

参考２．携帯電話会社等からの注意喚起等

（１）ＮＴＴドコモ

・ドコモ等を装ったフィッシングＳＭＳにご注意ください（2019 年７月 25 日）
https://www.nttdocomo.co.jp/info/notice/page/190725_01.html

・ドコモを装ったフィッシングＳＭＳにご注意ください！（2019 年６月 17 日）
https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/index.html

・ドコモを装ったメールにご注意ください！（2018 年５月 22 日（2019 年４月 15 日更新））
https://www.nttdocomo.co.jp/info/spam_mail/column/20170509/

（２）ＫＤＤＩ（ａｕ）

・安全にａｕのサービスをご利用いただくために
https://www.au.com/support/service/mobile/trouble/forestalling/safety/edification/?aa_oid=we-we-ow-0205

・最近多い迷惑メール・詐欺メールの事例が知りたい
https://www.au.com/support/faq/view.k20000002846/

・ＫＤＤＩ、ａｕ、Ｍｙ　ａｕ、ａｕ　ｏｎｅ　ｎｅｔ等を装ったメールが届きました。ａｕ（ＫＤＤＩ）から公式に送られたメールでしょうか？
https://www.au.com/support/faq/view.k1351318327/

・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（2018 年８月 31 日）
https://news.kddi.com/important/news/important_20180831622.html?aa_oid=we-we-ow-0207

（３）ソフトバンク・ワイモバイル

①ソフトバンク

・ソフトバンクを装うフィッシング目的の不審な電子メールに関するご注意（2018 年 11 月 16 日）
https://www.softbank.jp/mobile/info/personal/news/support/20181116a/

・ソフトバンクを装う電子メールに関するご注意（2018 年４月 18 日）
https://www.softbank.jp/mobile/info/personal/news/support/20180418a/

②ワイモバイル

・なりすましサイトに関するご注意とパスワード管理のお願い（2018 年２月７日）
https://www.ymobile.jp/info/2018/a/18020700.html

（４）一般財団法人日本サイバー犯罪対策センター

・通信事業者を騙るスミッシング詐欺の手法に係る注意喚起（2019 年６月 14 日）
https://www.jc3.or.jp/topics/smscert.html