



~.....*~*
▼△ ますます巧妙化！ネットを悪用した架空請求にご注意を△▼
~.....*~*

インターネットを悪用した手口による架空請求などのトラブルが後を絶ちません。最近では手口がますます巧妙化し、注意していたのに被害を受けてしまったケースもあります。そこで、インターネットを安全・安心に利用するためのサイバーセキュリティについて紹介します。

1.家庭での被害が多い架空請求・ワンクリック請求

「令和元年版情報通信白書」によると、世帯でのネット利用で何らかの被害を受けた割合は、自宅のPCで52.7%、スマホで62.6%となっています。内容はPCでは「迷惑メール・架空請求メールを受信」が最多で、2位に「ウイルスを発見したが感染なし」が続き、スマホでは「迷惑メール・架空請求メールを受信」で6割近くを占めています。

【架空請求】

身に覚えがない、あるいは契約したことがないにもかかわらず、「有料サービスを利用した」「有料の会員に登録した」などとして金の支払いを請求されるものです。請求の際に、「期限内に支払わなければ延滞金が生じる」「未払いならば訴訟を起こす」などと不安をあおられ、支払いを急かされることが多くみられます。架空請求は、電子メールを用いるものが大半です。

【ワンクリック請求】

特定のウェブサイトへアクセスしたり、電子メールに記載されたリンク先（URL）へアクセスしたりした後に、ワンクリック請求ウェブサイトの利用規約に同意することを意味する「はい」や「Yes」ボタンをクリックすることで、「有料サービスを利用した」「有料会員への登録が完了した」などという料金請求画面が表示され、利用者を慌てさせ、サイト使用料の名目でお金を支払わせようとするものです。このワンクリック請求の被害は、以前はパソコンを中心に発生していましたが、最近はスマホやタブレットで被害に遭うケースも増えています。特にアダルトサイトや出会い系サイト、ゲーム攻略サイト、動画サイトなどが入口となり、ワンクリック請求サイトに誘導されることで起こっています。

■架空請求やワンクリック請求に遭遇したら？

◆支払わない、連絡しない

身に覚えのない支払いを求める【架空請求】の場合は、無視してかまいません。なぜなら架空請求の大半は、無作為に選んだ複数の宛先に、大量に同一の文面をメールするもので、特に送り先を見定めて送信しているわけではないからです。

【ワンクリック請求】の場合は、料金請求画面がパソコンやスマホに表示されても、慌てて応じる必要はありません。請求画面を閉じようとしても繰り返し画面が表示されることがありますが、画面が表示されたからといって、こちらの個人情報が引き出されることはまずありません。

◆慌てて連絡をしないいづれの場合も、記載されている連絡先（メールアドレスや電話番号）には絶対に連絡をしないことが重要です。こちらから連絡をすることで、相手先（見知らぬ第三者）にこちらの連絡先を知られるためです。

■ワンクリック請求の料金請求画面を消すには？ワンクリック請求の料金請求画面が繰り返し表示される場合は、下記のような対処が有効な場合があります。

【スマートフォンなどの場合】

料金請求画面が表示されたウェブページを閉じたり、ブラウザの履歴やキャッシュ（一時ファイル）などを削除したりすることで、このような料金請求画面を消せる場合がほとんどです。

【Windows パソコンの場合は】

Windows PC（タブレット端末を含む）の場合、ウェブページを閉じても画面上に料金請求画面が繰り返し表示されることがあります。

その場合は、パソコンに悪意のあるソフトウェアをインストールしてしまった可能性があります。このようなときは、「システムの復元」（Windows に標準で備わっている機能）を行い、数日前の状態や初期化状態に戻すことで、料金請求画面を消せる場合があります。ただし、「システムの復元」では、何等かの原因でパソコンが動かなくなったり、データが消えてしまったりする可能性に備えて、事前に必要なデータのバックアップを取るなどしてから実施しましょう。

方法については、製品の説明書をよく読むか、製造会社のサポートセンターなどに確認してください。

■不安な場合は、最寄りの消費生活相談窓口にご相談しましょう。

また、ワンクリック請求の被害に遭った場合の技術的な対処方法などは、独立行政法人情報処理推進機構（IPA）情報セキュリティ安心相談窓口で紹介しており、電話やメール、FAX での相談も受け付けています。

・情報セキュリティ安心相談窓口

<https://www.ipa.go.jp/security/anshin/index.html>

2. 企業や組織を狙う「標的型攻撃メール」

一方、企業や団体などでは、情報システムの担当者を置いたり、社外の情報システム会社を活用したりして、セキュリティを整備しているところもあると思います。それでも対策のすき間を突いてくるのが、「標的型攻撃メール」です。この「標的型攻撃メール」への対応を誤ったために、従業員のパソコンがウイルスに感染し、従業員のメールアドレスなどの情報を抜き取られ、さらに組織内のネットワークに侵入されるといった被害が起きています。

「令和元年版情報通信白書」によれば、企業などがインターネットで「何らかの被害を受けた」割合は 55.6% に上り、そのうち 46.9% が「ウイルスを発見または感染」と回答しており、高い割合でウイルスに遭遇しているといえます。

■標的型攻撃メールの被害を防ぐには

◆不審なメール、あやしい添付ファイルは開かない

◆標的型攻撃メールの以下のような特徴を知っておく

●差出人

- ・差出人に心当たりがない。
- ・フリーメールアドレスから送信されている。
- ・署名が誤っている（送信元のメールアドレスと署名のメールアドレスが異なる。署名の組織名や電話番号などが実在しない・誤っている、など）

●件名

- ・自らの仕事や担当業務に関連しそうな件名

例) 製品やサービスに関する問い合わせ、クレーム、アンケートの回答依頼や取材申込など

例) 議事録や人事情報の送付、セミナー情報の案内、資料の再送や差替えなど

例) 航空券の予約確認や荷物の配送通知など

●内容・本文

- ・これまで届いたことのない企業や団体、公的機関からのお知らせ
- ・組織全体への案内
- ・添付ファイルを開かせようとしたり、URL をクリックさせようとしたりするような内容になっている。
- ・日本語の言い回しが不自然。
- ・日本語で使わない漢字が使われている。

●添付ファイル

- ・実行形式ファイルやショートカットファイルなどの注意が必要なファイルが添付されている。
- ・ファイルの拡張子と異なるアプリケーションのアイコンが使用されている。
- ・ファイル末尾にある拡張子が表示されていない。

例) 二重拡張子 (.doc.exe) となっているなど

■被害を防ぐ「サイバーセキュリティ」9か条■

- ◎1 OS やソフトウェアは常に最新の状態に
- ◎2 パスワードは貴重品のように管理する
- ◎3 ログインID・パスワードは絶対教えない
(金融機関を名乗り、銀行口座番号や暗証番号、ログインID やパスワード、クレジットカード情報の入力を促すような身に覚えのないメールが届いた場合、入力せず無視しましょう)
- ◎4 身に覚えのない添付ファイルは開かない
- ◎5 ウイルス対策ソフトを導入
- ◎6 ネットショッピングでは信頼できるお店を選ぶ
- ◎7 大切な情報は、複製して保管する
- ◎8 スマホやパソコンなどの紛失・盗難に注意
- ◎9 困ったときはひとりで悩まず、まず相談を
ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、一人で悩まず各種相談窓口(下記)に相談しましょう。

●各種相談窓口

- ウイルスおよび不正アクセスに関する技術的な相談
・情報処理推進機構 (IPA) 情報セキュリティ安心相談窓口 <https://www.ipa.go.jp/security/anshin/index.html>
【電話】
03-5978-7509 (平日 10:00-12:00, 13:30-17:00)

- 広告や宣伝目的の迷惑メールに困ったら
・日本データ通信協会 迷惑メール相談センター
<https://www.dekyo.or.jp/soudan/contents/ihan/>
【電話】
03-5974-0068 (平日 10:00-17:00)

- 犯罪に関する相談・電話による情報提供
・各都道府県警察のサイバー犯罪相談窓口 <https://www.npa.go.jp/cyber/soudan.htm>

~.....*~*

▼△ 要再検査・要精密検査を放置していませんか? △▼

~.....*~*

健康診断や人間ドックで「要再検査」「要精密検査」と判定されたのに忙しいし大丈夫だろうと放置している方はいませんか?

●「要再検査」とは、数値が基準の範囲を超えるので、一時的な変動かどうか確認するために再度検査することをいいます。再検査の結果、再度、基準範囲を超えた数値が検出される場合、詳しい原因を調べるために精密検査が必要になります。

●「要精密検査」とは、数値が基準の範囲を大きく超えるので、診断を確かめるために詳しい検査をする必要があることをいいます。緊急性があり、健康診断・人間ドックだけでは特定できない病気について、さらに詳しく調べることとなります。

「仕事が忙しくて病院に行く時間がない」「日常生活に支障がない」「自覚症状がない」「大きな病気と診断されるのが怖い」などの理由で再検査や精密検査しないで万一病気にかかっていた場合、早めの通院、治療で改善できるにもかかわらず、放置したまま病状 225-0550, FAX06-6225-0551

eメール (顧客フォロー.com 用)
shinnihon@kokyaku-follow.com
URL <https://www.kokyaku-follow.com>