



# ワンクリック請求

独立行政法人 情報処理推進機構 (IPA) セキュリティセンター

今号では、第1回の「偽警告」\*1と並んで多くの被害相談が確認されている「ワンクリック請求」について解説します。

## ワンクリック請求の手口

ワンクリック請求の手口自体は新しいものではなく、10年以上前より確認されているものです。改めてその手口について解説します。

ワンクリック請求はパソコンやスマートフォンでアダルトサイトや無料動画と書かれたウェブサイトを開覧しているときに遭遇する手口です。あたかも動画を再生する画面と見せかけて(図1)、いざ再生ボタンを押すと「登録完了」と請求画面が表示される(図2)というのが典型例です。また、こうした画面には「退会希望の方はこちら」というような文面のリンクなどが貼られており、文面を開くと業者の連絡先と思われる電話番号などが書かれています。焦って電話をしてしまうと、相手から退会費用として、またお金を請求されてしまいます。

これらの手口の特徴について、パソコンとスマートフォンそれぞれの環境に分けて見ていきましょう。

図1 動画再生と思わせる画面例

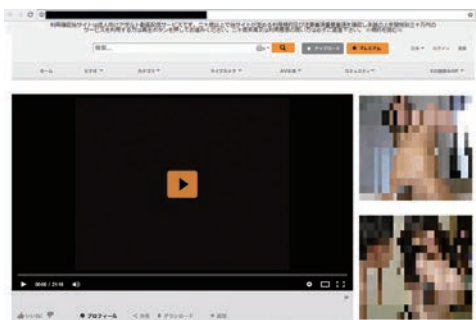


図2 ウェブブラウザ上の請求画面の例



### 【パソコンにおける事例】

以前から確認されてきた事例は主にパソコンにおけるものでした。パソコン上に表示される請求画面には次の2種類のパターンがあります。

#### <不正なプログラムによる画面表示>

このパターンでは、リンクをクリックすると、パソコン上で請求画面を表示させ続ける不正なプログラムが実行してしまいます。一度、このプログラムが実行されると、パソコン上に表示される「×」ボタンなどを押して請求画面を閉じても、1～2分後に再度請求画面が表示されてしまいます。さらに、パソコンを再起動しても再び表示されます。起動すると同時に請求画面が表示されるため、個人やパソコンを特定して請求していると思ってしまう人もいます。

#### <ウェブブラウザによる画面表示>

もう1つのパターンとして、ブラウザ上で請求画面を表示させる手口があります。この手口の技術的なしくみは本連載の第1回で解説した「偽警告」と似ています。請求画面も含めてウェブブラウザ上に表示され、ポップアップが

\*1 ウェブ版「国民生活」2018年7月号「こんなときどうしたら？インターネットのセキュリティガイド」第1回「偽警告」  
http://www.kokusen.go.jp/wko/pdf/wko-201807\_06.pdf



表れることもあります。これはブラウザ上に表示しているだけなので、ブラウザをいったん閉じて開き直す、またはパソコンを再起動することにより表示されなくなります。

## [スマートフォンにおける事例]

ここ数年で日本国内において急速に普及したスマートフォンでも、ワンクリック請求の被害が確認されています\*<sup>2</sup>。この手口ではウェブサイト閲覧中に「登録完了」を示すページへ自動的に遷移してしまいます。そのページ上でポップアップとして請求画面が表示され、「OK」などのボタンしかないのので、それを押すと業者の電話番号へ発信する通知が表示されます。その発信通知のキャンセルを押して表示を閉じて、またポップアップが表示され「OK」のボタンしか押せない、といったループから抜け出せなくなり、請求画面が消せなくなったと思わせます(図3)。

また、この手口では請求画面が表示されるタイミングで「シャッター音が鳴った」という事象も確認されています。スマートフォンでは自撮りなどに利用される内向きのインカメラが内蔵されていることが一般的です。そのため、シャッター音が再生されると、自分の顔が証拠として撮られてしまったと思い込んでしまいます。しかし、これ

はシャッター音がBGMとして流れているだけで、写真が撮られてしまったと思わせる脅し目的であり、相手に写真が送られているということもありません。



## ワンクリック請求への対策

ワンクリック請求で見られる請求画面は、アダルトサイトなどで見られる動画の再生ボタンや「無料動画はコチラ」といったリンクをクリックしてしまうことで遭遇してしまいます。そのため、事前にこうした知識を身に付けておき、不用意にリンクをクリックしないことが大切です。ここでは、請求画面が出てしまったときの対処法について解説します。

### <不正なプログラムによる画面表示の対策>

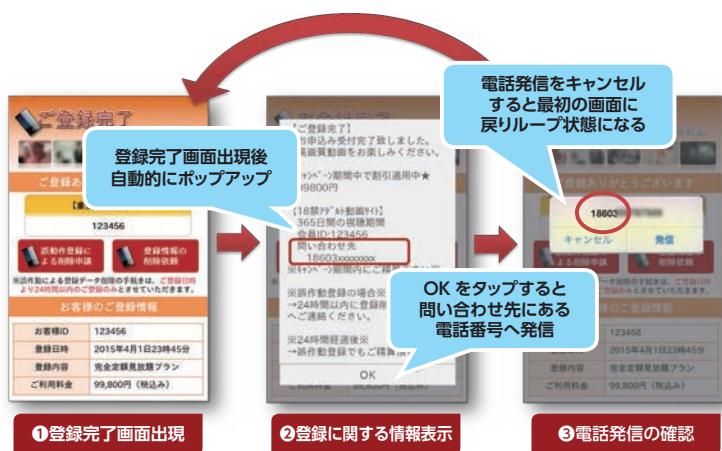
パソコンを再起動しても請求画面が再び表示される場合は、不正なプログラムが作動している可能性が高いと考えられます。不正なプログラムを作動させてしまった場合、画面を消すことは非常に困難です。そこでIPAでは安全な対処法として、Windowsの機能である「システムの復元」を実施して、請求画面が出た日付より前の日付の状態に戻すことを推奨しています。

不正なプログラムを動かしてしまう事例において、1つ頭に入れておきたい知識があります。

それは、特にWindowsのパソコンにおいては、不正なプログラムを動かす際に、必ず警告\*<sup>3</sup>が表示されることです(図4)。

図4に「発行元:不明な発行元」とあるように、ワンクリック請求の手口における不正なプログラムでは、この表示になることが確認されています。現実世界においても、製品の製造元が不明だと、信用のおけるものなのかと不審に思う人がほとんどでしょう。パソコン

図3 スマートフォンのワンクリック請求画面のイメージ

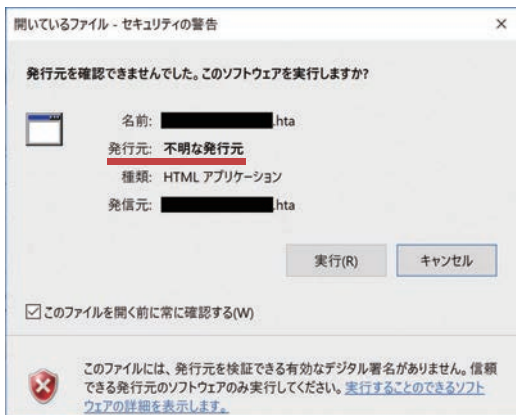


\*2 IPA「スマートフォンでのワンクリック請求の新しい手口にご用心」(2015年4月1日) <https://www.ipa.go.jp/security/txt/2015/04outline.html>

\*3 なお、このWindowsの機能を「ユーザーアカウント制御(User Account Control)」と呼び、頭文字を取ったUACと呼ぶことがある。



図4 Windowsのセキュリティの警告の例



ンの世界も同じで、不明な発行元、すなわちプログラムを開発した存在が不明瞭である場合は怪しむようにしてください。

また、この警告画面は「キャンセル」ボタンを押すことができます。キャンセルできれば、不正なプログラムを作動させることなく回避することができます。ワンクリック請求の不正なプログラムを作動させてしまうケースでは、この警告画面をよく読まずに「開く」を押してしまっていることが考えられます。今回の手口に限らず、こうした警告が出た場合は、よく内容を読んで、不審に思う場合は「開く」を押さないようにしましょう。

### <スマートフォンによる画面表示の対策>

スマートフォンでの対策は、インターネットを見るためのブラウザ画面を閉じるだけです。しかし、パソコンと違って、ブラウザ画面の閉じ方の汎用的な操作方法はなく、AndroidとiPhoneでも、それぞれ操作方法が異なります。また、ブラウザによっても操作方法が違います。利用しているスマートフォンに合った操作方法が必要になりますので、画面の閉じ方がどうしても分からない場合は、操作が分かる人に見てもらおうようにしましょう。例えば、携帯電話ショップに「インターネット(ブラウザ)の画面の閉じ方」を聞いてみるといいでしょう。これに加えて、より安全な策としてブラウザの「閲覧履歴の削除」を推奨しています。ただし、この閲覧履歴を削除するやり方もスマート

フォンによって変わるので、自分で分からない場合は携帯電話ショップなどに聞いてみるいいでしょう。

### ワンクリック請求における不審な事例

ワンクリック請求に関する一般的な手口とその対策は以上になります。ここで最近IPAに寄せられた相談の中で確認された不審な事例と、その考えられる原因について見ていきます。

- ・業者に電話したら、伝えてもいないのに、いきなり本名や住所を言われた。

請求画面で表示された電話番号に電話してしまったケースで確認されたものです。ワンクリック請求の手口では、不正なプログラムによる画面表示、ウェブブラウザ上の画面表示、どちらにおいても、ユーザー側の端末内の情報が抜き取られるといったことはありません。そのため、こうした事例で推測される原因として、電話をかけてしまったことがきっかけであると考えられます。電話をしてしまうと、当然相手業者に電話番号が知られてしまいます。さらに、スマートフォンの手口においては、発信番号に「186 (発信者番号通知)」が必ず付記されていることが確認されており(図3)、利用者の電話番号取得をねらっていることが考えられます。

もし、電話番号を業者に知られたらどうなるでしょう。固定電話からかけた場合、電話番号からインターネット上などで本名と合わせて住所も検索されることが考えられます。スマートフォンなどの携帯電話の場合、電話番号とひも付けされるサービス、例えばLINEなどのSNSでは本名で登録している人が多いため、検索の結果、本名を知られてしまう可能性があります。

SNS などを利用していない場合、想像にはなりますが、業者側で電話番号と住所の個人情報リストのようなものを持っていることも考えられます。こうした情報がいつどこで漏れたのか確認することは非常に困難です。いずれにしても、業者に電話して問題が解決することはありませんので、決して電話しないことが重要です。