

報道発表資料

令和4年2月24日
独立行政法人国民生活センター

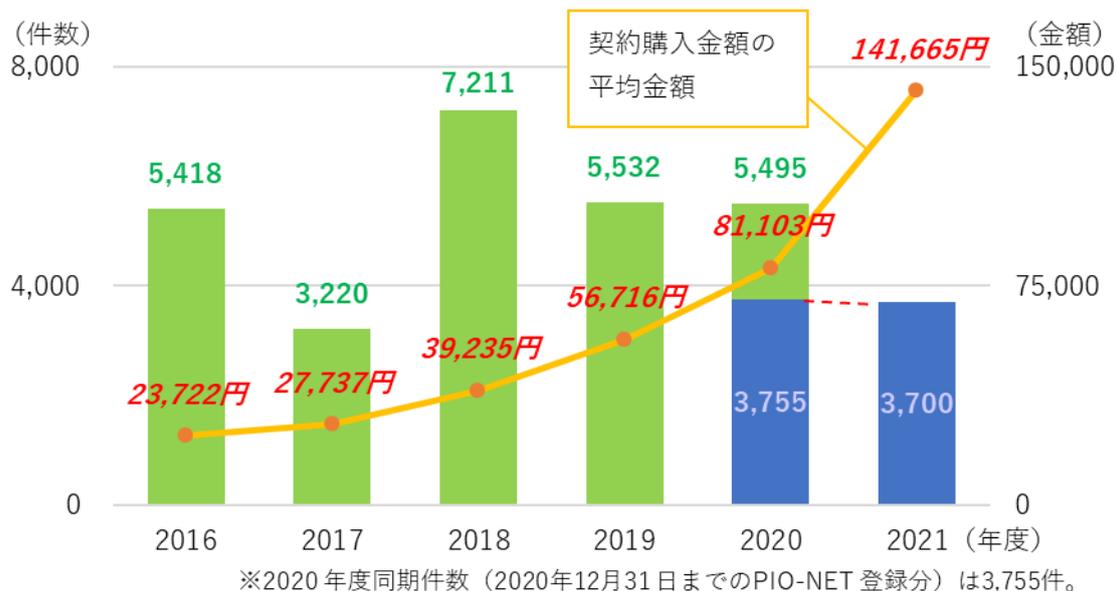
そのセキュリティ警告画面・警告音は偽物です！「サポート詐欺」にご注意！！

—電話をかけない！電子マネーやクレジットカードで料金を支払わない！—

全国の消費生活センター等には、いわゆる「サポート詐欺」（パソコンやスマートフォンでインターネットを使用中に突然「ウイルスに感染している」等の偽警告画面や偽警告音が出て、それらをきっかけに電話をかけさせ、有償サポートやセキュリティソフト等の契約を迫る手口）に関する相談が多く寄せられています。最近の相談の状況をみると、年間5000件以上の相談が寄せられ、契約購入金額の平均金額は年々高額化しています（図1）。また、最近ではプリペイド型電子マネーによる支払いが急増していたり（図2）、高齢者の被害が目立つ傾向がみられます。

国民生活センターでは2018年11月に注意喚起を行いました¹が、最近の相談の状況を踏まえ、一般財団法人日本サイバー犯罪対策センター（JC3）および独立行政法人情報処理推進機構（IPA）と連携し、再度消費者へ注意喚起を行います。

図1 PIO-NET²にみる「サポート詐欺」に関する相談と契約購入金額の平均金額の年度別推移

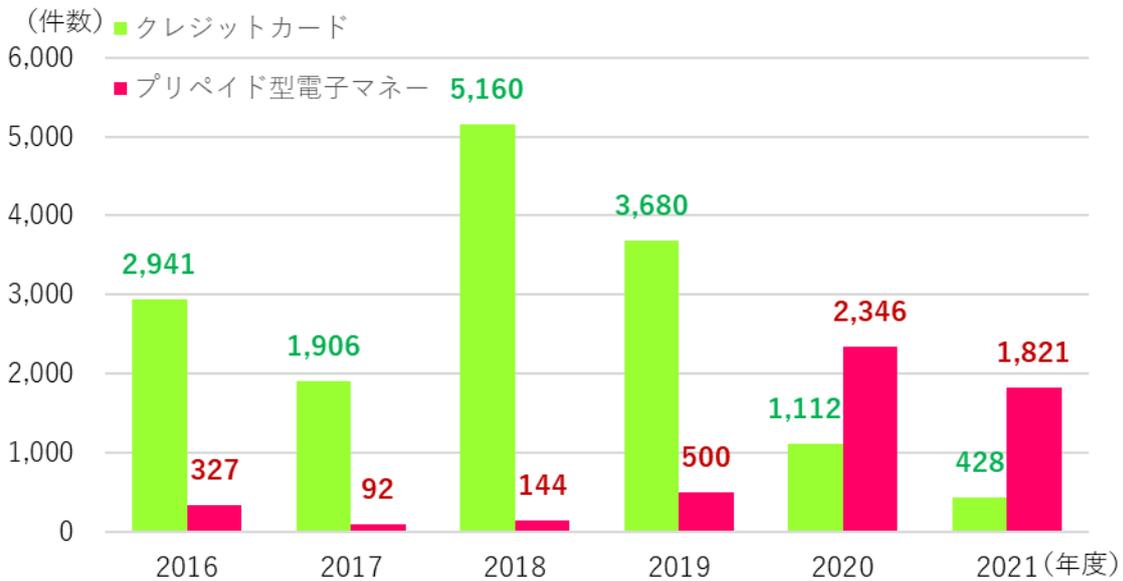


¹ インターネット使用中に突然表示される偽セキュリティ警告画面にご注意！（2018年11月7日公表）

https://www.kokusen.go.jp/news/data/n-20181107_1.html

² 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）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。相談件数は、2021年12月31日までの登録分。消費生活センター等からの経由相談は含まれていない。

図2 相手から指示される支払方法の年度別推移



1. 相談事例（()内は受付年月、契約当事者の属性）

【事例1】警告画面や警告音がきっかけで電話したところ、ウイルスの除去費用等を請求された

夜中に、パソコンでインターネットを利用していたところ、突然、警告音が鳴り、パソコン画面に、ウイルスに感染しているのではと警告画面が表示された。表示されていたサポート窓口に電話したところ、「パソコンがウイルスに感染しているのを除去します。コンビニに行って3万5000円分のプリペイド型電子マネーを買って、番号の部分の部分を削って、番号を伝えてください。このまま待っているのでは、電話はこのままにしてコンビニでプリペイド型電子マネーを買ってきてください」と言われた。指示に従って、コンビニに行って、プリペイド型電子マネーを購入し、電話の相手に番号を伝えたが、「番号が間違っている。もう一度3万5000円分購入してくるように」と言われ、不審に思って電話を切った。その後、パソコン専門店にパソコンを見てもらったが、ウイルスには感染していなかった。返金してほしい。

(2021年10月受付 70歳代 男性)

【事例2】次々に料金の支払いを要求されて、プリペイド型電子マネーで支払ってしまった

パソコンでアダルトサイトを見ていたところ、突然パソコンの操作ができなくなり、警告音が鳴り、警告画面が表示された。警告画面に表示されていたサポートの電話番号に電話すると、大手パソコンOS会社の出先機関を名乗る外国人のような女性が出て、処理すると言われ遠隔操作され、セキュリティソフトを入れるので、コンビニで7万円のプリペイド型電子マネーを購入してくるようにと言われた。コンビニで1万円のプリペイド型電子マネーを7枚購入し、カードの番号をパソコンに入力したが、「処理に失敗した。後で返金するので、再度7万円分のプリペイド型電子マネーを購入して番号を入力するように言われ、指示に従って再度7万円分のカードの番号を入力したがまた失敗したと言われ、さらに繰り返して7万円分のカードの番号を入力し、合計21万円分のカードの番号を電話の相手に伝えた。その他、氏名、住所、携帯電話番号も入力した。電話の相手からは、14万円は後で返金すると言われていたが、不安になり、大手パソコンOS会社

に電話したところ「それは詐欺です。警告画面を閉じれば何の問題もなかった。パソコンにウイルスを入れられた可能性もあるので、パソコンメーカーにみてもらったほうがいい」と言われた。詐欺だったのだろうか。 (2021年10月受付 50歳代 男性)

【事例3】コンビニの店員に詐欺と気付かされ被害に遭わなかった

パソコンでインターネットを利用中に、突然「ウイルスに感染した。連絡してください」と警告画面が表示され、連絡先の電話番号が表示されていた。慌てて電話すると、片言の日本語を話す外国人らしき人物が出て、「ウイルスですね。この問題を解決するにはセキュリティソフトを契約するしかありません」と言われ、4万円、6万円、8万円のコースがあると説明された。高額なので購入しないと言ったが、強く勧められ、4万円のコースを申し込むことになってしまった。電話を切らずに、コンビニに行ってプリペイド型電子マネーを買って、番号を伝えるように指示され、コンビニに行った。プリペイド型電子マネーを購入する前に、コンビニの店員に事情を聴かれ、経緯を答えたところ、「詐欺の可能性があるので」と言われ、慌てて電話を切った。その後、2回ほど着信があったが、電話に出ず、その後は着信を拒否している。

(2021年10月受付 40歳代 女性)

2. 相談事例からみる特徴と問題点

(1) 突然警告画面や警告音が出て、消費者を不安にさせて連絡を求めている

パソコンでインターネット使用中に突然「ウイルスに感染している」等の警告画面が出たり、警告音が大音量で鳴ることで、消費者は不安になり、警告画面に掲載されているサポート窓口などの連絡先に慌てて電話しているケースが目立ちます。

相談内容を見ると、パソコンのOS会社やセキュリティソフト会社などの実在する会社のロゴマークが警告画面に掲載されていたり、一時的にパソコンの操作ができなくなったり、警告画面や警告音を消すことができなかつたりして、消費者を不安に陥れる様々な手法が使われています。

(2) 警告画面上の連絡先に電話すると、不安をあおられ有償サポート等の契約を迫られる

消費者が警告画面に掲載されている連絡先に電話すると、パソコンOS会社等のサポート窓口などをかたる相手から、端末がウイルスに感染しているため、遠隔操作でウイルスを除去するなどと説明されます。相手は、さらに「このままでは個人情報流出してしまう」「パソコンが動かなくなってしまう」など消費者の端末がウイルスに感染した可能性があることや至急対応しなければならぬと思込ませる説明をしています。

消費者が相手の遠隔操作によるウイルスの除去に同意すると、遠隔ソフトをインストールするように誘導されます。消費者が誘導に従い遠隔ソフトをインストールすると、消費者の端末が相手に遠隔操作され、警告画面が閉じたり、警告音が鳴りやんだりすることから、消費者は電話の相手をますます信用してしまいます。

警告画面、警告音が消えると、今度は、電話の相手から、今後ウイルスに感染しないために有償サポート等の契約が必要であると迫られて、契約を結んでしまいます。

なお、相手が消費者の端末を遠隔操作できる状態になると、当該端末で画面に表示していた情報が相手に見られていることとなります。

(3) プリペイド型電子マネーで支払わせるケースが急増中／次々と支払いを迫ってくる

ウイルス除去の料金や有償サポート等の料金の支払い方法として、以前はクレジットカードで支払うように指示されるケースが多かったところ、最近ではプリペイド型電子マネーで支払うように指示されるケースが多くなっています。

プリペイド型電子マネーでの支払いの場合では、電話をつないだ状態で、近くのコンビニでプリペイド型電子マネーを購入し、レジで支払った後に、プリペイドカードのスクラッチ部分を削って表示される番号を伝えるように指示されるケースが多くみられます。(中には、コンビニに設置されているマルチメディア端末を操作して、プリペイド型電子マネーを申し込み、端末から出てきたシートをレジに持っていき、支払うことで得られた番号を伝えるように指示されるケースもあります。)そして、消費者がコンビニに行っている間に、相手が消費者の端末を遠隔操作して、ウイルスの除去などを行っているようにみせるのが典型的なケースです。

また、一度プリペイド型電子マネーで支払うと、相手は以下のような説明をして次々と支払いを迫ってきます。

- ・ 口頭で伝えた番号が間違っていたので、プリペイド型電子マネーの番号がロックされた
- ・ 入力した番号が間違っていた(数字の「0」(ゼロ)とアルファベットの「O」(オー)が間違っていたなど)
- ・ 番号が間違っていた分は後で返金するので、新しいプリペイド型電子マネーを購入してほしい

(4) 60歳以上の消費者が契約当事者となる相談が増加中

契約当事者の年代をみると、60歳以上の消費者の相談が5割を超えています。特に70歳以上の消費者が被害に遭っています。相談の中には、家族など周りの人が高齢の当事者に、警告画面や警告音が偽物であり、詐欺の可能性のあることに気付かせるケースなどもあります。

(5) 電話の相手とのコミュニケーションが難しい場合がある

消費者が警告画面に掲載されているサポート窓口で電話をすると、外国人と思われる人が片言の日本語で対応するケースが目立ちます。警告画面に掲載されている電話番号は、IP電話の一種である「050」で始まる電話番号が多く、電話の相手から、電話が海外につながっていると説明されるケースもあります。

3. 消費者へのアドバイス

(1) 「警告画面や警告音は偽物ではないか？」とまずは疑ってみましょう

警告画面に掲載されている連絡先に電話しないようにしましょう

警告画面や警告音が出て慌てて連絡してしまうと、電話の相手からさらに不安をあおられ、有償サポート等の契約を勧められてしまいます。警告画面に掲載されている連絡先には電話をしないようにしましょう。

連絡先に電話すると、片言の日本語を話す外国人と思われる人から、すぐにウイルスの感染を除去しなければならない等とさらに不安をあおられ、断りづらくなります。相手は、ウイルスを除去しているの見せかけたり、遠隔操作でパソコンの復旧などの作業をしているふりをして、ウ

ウイルスの感染を消費者に信じ込ませ、次々に料金を請求してきます。

警告画面や警告音が出た場合は、まずは偽物ではないかと疑って、すぐに電話しない、有償サポート等の契約を結ばないようにしましょう。警告画面に表示されたパソコンOS会社やセキュリティソフト会社のホームページに「サポート詐欺」に関する情報が掲載されている場合もありますので参考にしましょう。

偽警告画面等に惑わされず、掲載されている連絡先に電話しないことが重要です。

(2) 警告画面や警告音が出ても慌てず、自分でパソコン等の状態を確認しましょう

インターネット利用中に突然出る警告画面や警告音は、偽物の可能性があります。消費者の端末の状態を正確に伝えているとは限りません。

一般財団法人日本サイバー犯罪対策センター（JC3）に、警告画面、警告音への対処方法について、以下のとおり確認しました。＊詳細は【参考資料3】を参照してください。

<警告画面、警告音への対処方法>

- ① まずは警告音は慌てる原因になりますので、端末の音量調節の操作が可能であれば、**音量を「0」（無音）の状態に**しましょう。
- ② 端末に導入しているセキュリティソフトで問題の有無を確認しましょう。（日頃から、端末に導入しているセキュリティソフトのウイルスの定義は最新の状態に更新しておきましょう。）
- ③ 警告画面を消したいときは、インターネットブラウザ等を終了させます。
 - ・警告画面の ボタンで終了できる場合もあります。
 - ・それでも終了できない場合は、パソコンのキーボードの + + を同時に押して、「タスクマネージャー」を起動すれば、インターネットブラウザや問題となっているアプリだけを終了させることができます。
 - ・パソコンの電源ボタンを長押しし、パソコン自体をシャットダウン（強制終了）させる方法もありますが、作業中で保存していないファイルが失われる可能性があります。

(3) 自分で判断できない場合は周りの人に相談しましょう

60歳以上の高齢者が被害に遭うケースが多くなっています。パソコンやスマートフォンなどの端末操作に不慣れであったり、セキュリティの知識がないことにつけ込まれることがあります。警告画面や警告音が出ても焦らず、冷静に対処してください。

連絡してしまった場合でも、指示されるままにプリペイド型電子マネーを購入しに行かない、番号を伝えない、クレジットカード番号を教えないようにしましょう。

プリペイド型電子マネーでの支払いを求められたケースでは、消費者が高額なプリペイド型電子マネーを大量に購入していたり、短時間で頻繁に購入していることから、コンビニエンスストアの店員が気付いて、被害を免れたケースもあります。

自分だけで判断せず、電話したり、料金を支払う前に、周りの人に対処方法を相談しましょう。

(4) 支払い方法がプリペイド型電子マネーの場合は相手より早くチャージしたり、発行業者に連絡したりしましょう

支払方法がクレジットカードの場合はクレジットカード会社に相談しましょう

プリペイド型電子マネーで支払った場合は、相手が当該番号をチャージ等で使用してしまう前に、自身のアカウント等にチャージして使用するなど確保しましょう。すでに相手に使用されてしまっている場合は、プリペイド型電子マネーの発行業者に「サポート詐欺」でプリペイド型電子マネーの番号を相手に伝えてしまったことを連絡し、指示に従いましょう。自身の被害の回復が困難な場合は多いですが、発行業者によって今後の悪用を防止することができる場合があります。

クレジットカードで支払った場合、契約画面や契約後に相手から届くメール、利用規約等に解約に関する案内がないかを確認し、解約の条件や手続きがわかれば、契約の相手に解約を申し出ましょう。相手から返信や対応が得られなければ、クレジットカード会社に相談しましょう。また、サブスクリプション契約（サブスク）の場合は、一定の周期（月、年など）で決済されるおそれがあります。

(5) 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

契約や解約に関して等、不安に思うことやトラブルが生じた場合には、最寄りの消費生活センター等に相談しましょう。

*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。

また、表示された警告画面の消去方法等、パソコンに関する技術的な相談に対してアドバイスを求める場合は、独立行政法人情報処理推進機構（IPA）の「情報セキュリティ安心相談窓口」に電話またはメールで相談しましょう。相談の際の注意事項や関連情報などはホームページに掲載されています。

情報セキュリティ安心相談窓口：<https://www.ipa.go.jp/security/anshin/>

*情報セキュリティ安心相談窓口の電話番号：「03-5978-7509」

受付時間：10:00～12:00、13:30～17:00・土日祝日・年末年始は除く

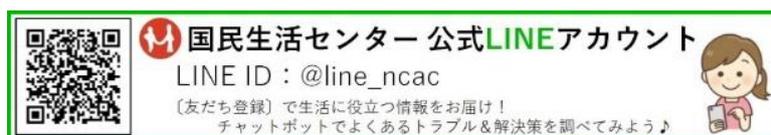
*情報セキュリティ安心相談窓口のメールアドレス：anshin@ipa.go.jp

4. 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) |
| ・警察庁 | (法人番号 8000012130001) |
| ・金融庁 | (法人番号 6000012010023) |
| ・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) |
| ・一般社団法人日本資金決済業協会 | (法人番号 6010005003495) |
| ・日本代理収納サービス協会 | |

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。

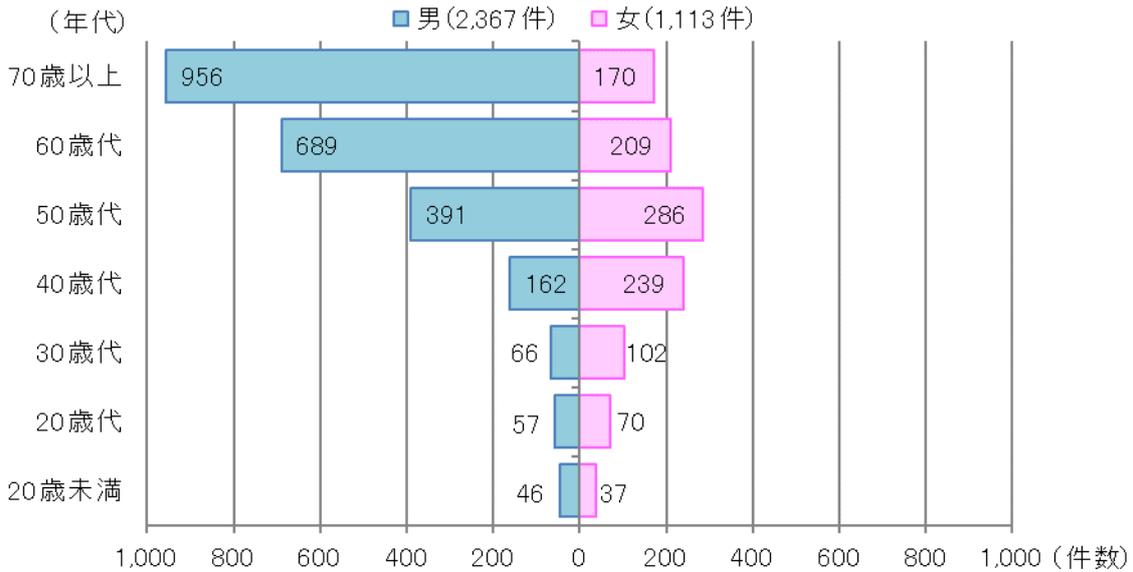


【参考資料 1】PI0-NETにおける相談の傾向（2021年度受付分[2021年12月31日までの登録分]）

（1）契約当事者の属性（図3）

契約当事者を男女別にみると、男性が2,367件（68.0%）、女性が1,113件（32.0%）で男性が約7割を占めています。男女別の年代をみると、男性は70歳以上、60歳代、50歳代の順に多く、女性は50歳代、40歳代、60歳代の順に多い状況です。

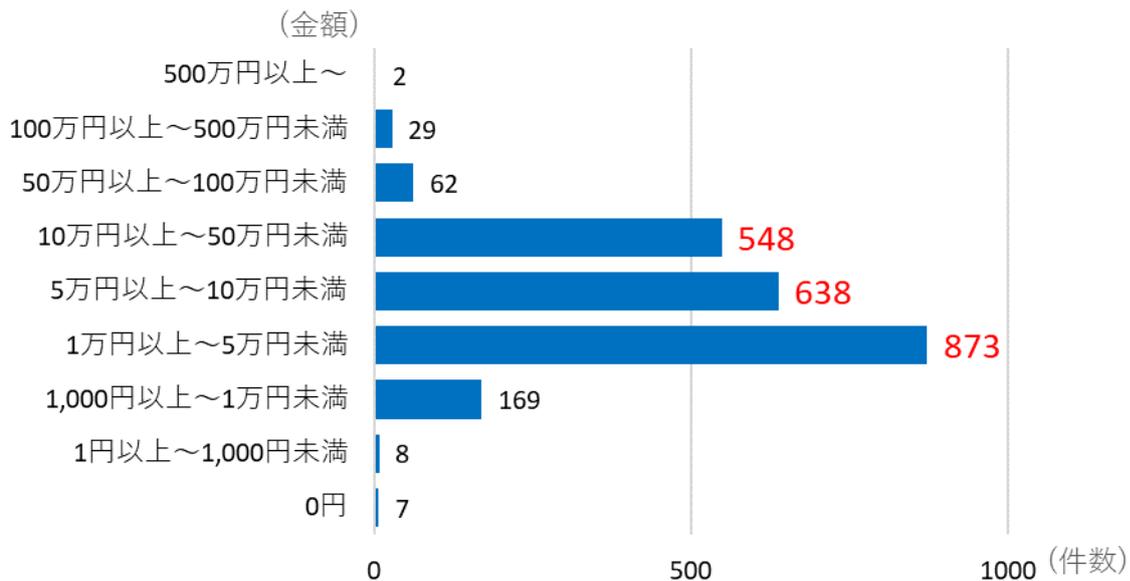
図3 契約当事者の属性（2021年度）（n=3,480）（無回答除く）



（2）契約購入金額の分布（図4）

契約購入金額は、1万～5万円未満が最も多い状況です。

図4 契約購入金額の分布（2021年度）（n=2,336）（無回答除く）

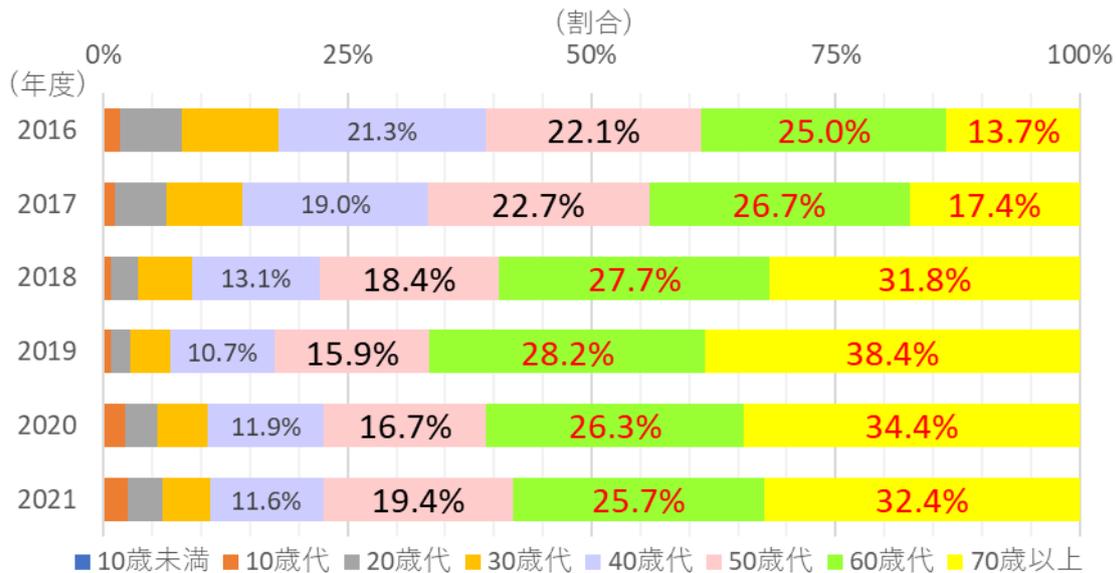


【参考資料2】PIO-NETにおける相談の年度別の傾向（2016年度以降受付分[2021年12月31日までの登録分]）

(1) 契約当事者の年代の年度別推移（図5）

2018年度以降70歳以上が3割を超え、60歳以上、50歳以上の順に多い状況です。2018年度以降60歳以上で5割を超えている状況が続いています。

図5 契約当事者の年代の年度別推移（無回答除く）



(2) 既に支払った相談件数と支払総額の推移（図6）

相談を受け付けた時点で既に支払っていた相談件数は増加傾向です。支払総額も2020年度以降は2億円を超え、増加傾向です。

図6 既に支払った相談件数と支払総額の推移



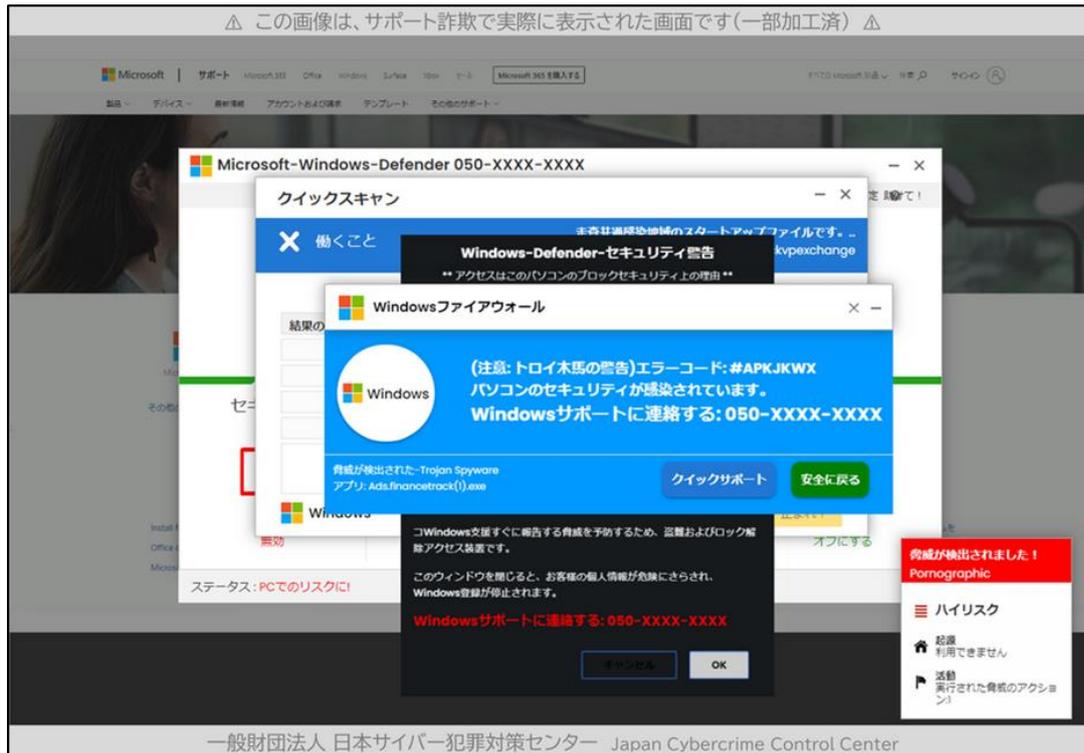
※2020年度同期件数（2020年12月31日までのPIO-NET登録分）は1,143件。

*クレジットカードによる払いで、相談を受け付けた時点では引き落とされていない場合は、既に支払った相談件数には含まれません。

【参考資料3】一般財団法人日本サイバー犯罪対策センター（JC3）からのコメント

JC3では、「サポート詐欺サイト」と呼ばれる偽警告サイトを、長期にわたり継続的に観測しています。「サポート詐欺サイト」には、「ウイルスに感染している」「パソコンをブロックした」「ハードディスクを消去する」「個人情報に危険にさらされる」などというメッセージが表示される、大きなビープ音が鳴る、問題を解決するためとして、表示された番号に電話をかけてサポート窓口にお問い合わせよという音声流れる、といった点が共通してみられます。

・サポート詐欺で実際に表示された画面の例（JC3にて一部加工済み）



そのほか、このようなサイトには、

- ・インターネットの広告ネットワークから様々なサイトに転送を繰り返したのち表示されることもある
 - ・サイトに表示される電話番号の多くは「050」で始まるが、「03」や「06」で始まる番号、「0120」で始まるフリーダイヤルの番号も確認されている
 - ・サイトのURLや電話番号は日々新しいものが観測されている
- というような特徴があります。

2022年になっても偽警告画面を表示するサイトは観測されています。そのため、インターネット利用者としては、引き続き警戒が必要であることには変わりありません。Webサイト内の広告から意図せず転送されることもあることから、ネットサーフィンをしている人は誰でも遭遇する可能性があります。上記のようなサイトが表示されたときは、決して画面に表示された番号に電話を掛けないようにご注意ください。

以下の動画を参考にしてください。

【動画1】は、富山県警察が偽警告画面に表示されたサポート窓口で電話をかけた際の相手とのやり取りを一般財団法人日本サイバー犯罪対策センター（JC3）が編集したものです。

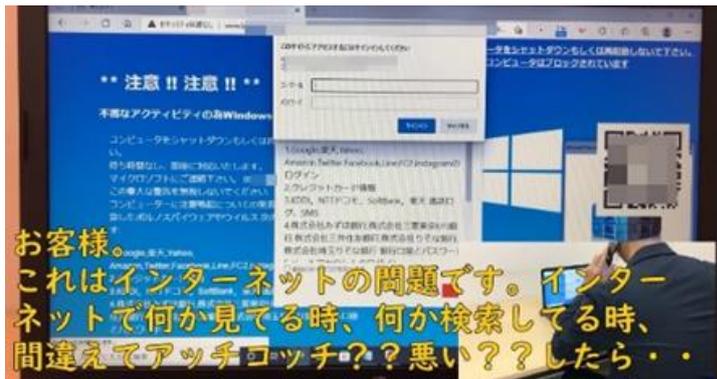
【動画2】は、サポート詐欺で、偽警告画面が表示された際の対処方法をまとめたものです。

【動画1】

テクニカルサポート詐欺サイトに騙されてみた（JC3の公式YouTubeチャンネル）

<https://youtu.be/jbuI5I0tI1A>

（注）大きな音量の警告音が出ますのでご注意ください。

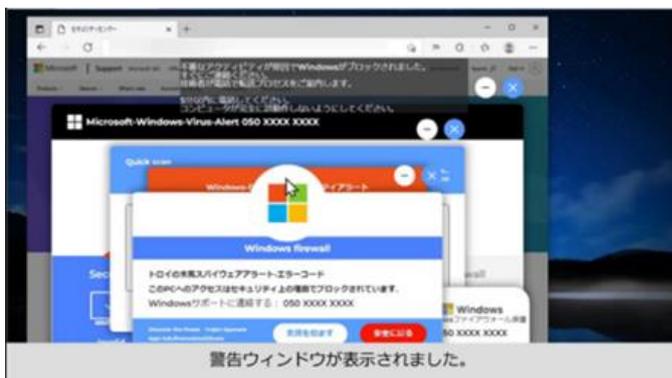


【動画2】

テクニカルサポート詐欺サイトに遭遇した際の対処方法（警告画面の消し方）（JC3の公式YouTubeチャンネル）

https://youtu.be/I0l_gRrmSJo

（注）大きな音量の警告音が出ますのでご注意ください。



【参考資料4】注意喚起情報

1. 当センターの注意喚起情報

- ・偽警告表示 プリペイド型電子マネーで支払わせる手口に注意
(第388号[2021年3月9日発行])

<https://www.kokusen.go.jp/mimamori/pdf/shinsen388.pdf>

見守り新鮮情報

突然、警告がパソコン画面いっばいに表示された。慌てて表示された連絡先に電話すると「パソコンが汚染されており、緊急を要する。電話を切らずに**プリペイド型電子マネー**で2万円を支払え」と指示された。すぐにコンビニで2万円分購入し、番号を伝えたが「番号が間違っている。再度2万円分購入してきて」と言われ、再度購入し番号を伝えた。翌日「さらに2万円支払えば4万円返金する」と意味の分からないことを言われた。
(60歳代 女性)

**偽警告表示
プリペイド型電子マネーで
支払わせる手口に注意**

ひとこと助言

- プリペイド型電子マネー（以下「電子マネー」という。）での支払いを指示する詐欺的な手口として「パソコンやスマートフォンに突然偽の警告画面を表示して慌てさせ連絡させる」というものが出てきています。
- カード番号だけで利用できる電子マネーは、番号を一度相手に伝えてしまうとお金を取り戻すことは非常に困難です。絶対に番号を伝えてはいけません。
- セキュリティ対策には、あらかじめ信頼できるセキュリティソフトをインストールしておく等の対応を行い、見慣れない警告画面の指示に従ってはいけません。
- 対処に困ったときは、お住まいの自治体の消費生活センター等（消費者ホットライン188）や、独立行政法人情報処理推進機構（IPA）の情報セキュリティ安心相談窓口にご相談したり、IPAのホームページを参考にしましょう。

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
電話：03-5978-7509
受付時間：10:00～12:00 13:30～17:00 土曜日曜日・年末年始は除く
メールアドレス：anshin@ipa.go.jp

本文イラスト：黒崎 玉
見守り新鮮情報 第388号（2021年3月9日）発行：独立行政法人国民生活センター

2. 一般財団法人日本サイバー犯罪対策センター（JC3）

- ・サポート詐欺

<https://youtu.be/FE1P4pw-Ukw>

- ・JC3 コラム ーサポート詐欺編（1）第1話「ピーー」、マイクロソフトセキュリティアラーム

<https://www.jc3.or.jp/threats/topics/article-396.html>

- ・JC3 コラム ーサポート詐欺編（2）第2話 日本フリーダイヤル？

<https://www.jc3.or.jp/threats/topics/article-397.html>

- ・JC3 コラム ーサポート詐欺編（3）第3話 ネットワーク越しに忍び寄る魔の手

<https://www.jc3.or.jp/threats/topics/article-398.html>

- ・JC3 コラム ーサポート詐欺編（4）第4話 お支払いは？

<https://www.jc3.or.jp/threats/topics/article-413.html>

- ・JC3 コラム ーサポート詐欺編（5）第5話 始まりは突然に

<https://www.jc3.or.jp/threats/topics/article-419.html>

3. 独立行政法人情報処理推進機構（IPA）

- ・“その警告メッセージ、信じて大丈夫？ ブラウザの“偽警告”にご用心！”

<https://youtu.be/sm1UMc97zRc>

- ・“【手口検証動画】偽のセキュリティ警告”

<https://youtu.be/SP00wbawM1k>

- ・偽のセキュリティ警告に表示された番号に電話をかけないで！
～ パソコンにおける最近の手口と対策を解説～

<https://www.ipa.go.jp/security/anshin/mgdayori20211116.html>

4. 日本マイクロソフト株式会社

- ・マイクロソフトのサポートを装った詐欺にご注意ください（2021年1月29日公表）

<https://news.microsoft.com/ja-jp/2021/01/29/210129-information/>