第 20-09-402 号
掲載日：2020 年 11 月 25 日
独立行政法人情報処理推進機構
セキュリティセンター

# 安心相談窓口だより

## 遠隔操作を他人に安易に許可しないで！
## ～ 偽警告からの遠隔操作でパソコンをロックされるなどの手口を確認！ ～

IPA では 2016 年 6 月に「パソコンがウイルスに感染している」など、偽の警告画面から電話をかけさせるように仕向けたうえで、遠隔操作による有償サポート契約に誘導する手口について注意喚起を行いました。(*1)

現在も継続して偽の警告画面から遠隔操作に誘導する手口についてのご相談が寄せられています。

最近では、遠隔操作をさせたことにより、「契約を断ったら、パソコンが再起動しなくなった。」、「パソコンがロックされて使えなくなった。」など、より悪質な手口も確認しています。

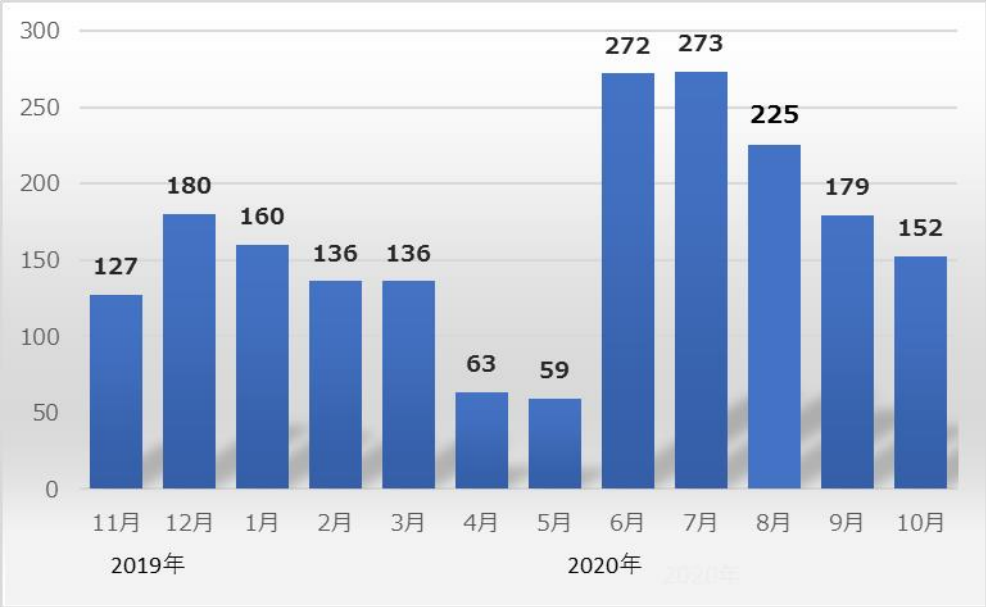


図 1 :IPA に寄せられた偽警告（有償サポート契約へ誘導）に関する相談件数の推移 (*2)

本来、遠隔操作ソフトは、遠隔地にあるパソコンを監視、操作するなどの目的で利用されるもので、例えば、パソコンメーカーがユーザーサポートを行うために、遠隔操作ソフトを利用することがあります。

一方で、第三者の言葉を鵜呑みにして遠隔操作ソフトをパソコンにインストールしてしまうことは、見知らぬ訪問者を家に招き入れる行為と同じようなものであり、遠隔操作する側に悪意があれば、パソコン内のデータが窃取される、設定を変えられる、などの被害の恐れがあります。

また、パソコンがウイルス感染したという偽警告への対処のために遠隔操作を相手に許可した場合は、パソコンの有償サポート契約や、有償のソフトウエア購入に誘導される可能性があります。

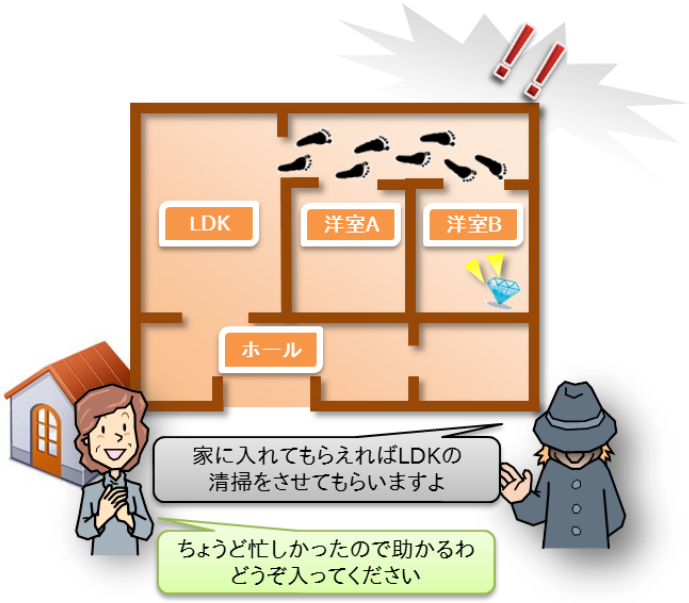


図 2：遠隔操作ソフトのインストールを家に人を招き入れることに例えたイメージ

そこで、今回は、遠隔操作を許可する場合のリスクと、遠隔操作サービスを受ける際の注意点について解説します。

---

(*1) 安心相談窓口だより「“ウイルスに感染した”という偽警告でサポートに電話するように仕向ける手口に注意」
https://www.ipa.go.jp/security/anshin/mgdayori20160621.html

(*2) 2020 年 4 月 9 日～2020 年 5 月 31 日の期間において新型コロナウイルスの感染拡大防止と職員の安全確保を図るために、相談電話対応業務を停止していました。そのため当該期間中は電子メール、FAX、郵送による相談件数の統計になっています。

## 1. 遠隔操作の仕組みとリスク

### 1-1. 遠隔操作の概要

遠隔操作には様々な方法がありますが、ここでは「自分のパソコン上に遠隔地にあるパソコンの画面を表示して操作ができる」ソフトを使用した遠隔操作の概要を説明します。

操作される側が遠隔操作ソフトをインストールして起動したり、遠隔操作のための実行ファイルをダウンロードし実行したりすると、操作する側はネットワーク経由で当該パソコンの遠隔操作が可能となります。


図 3：遠隔操作ソフトによる遠隔操作のイメージ

### ■ 遠隔操作成立の３つの条件

- 実際に「操作される側」のパソコンに対して遠隔操作を成立させるためには、下記の 3 つの条件を満たす必要があります。
  1. 「操作される側」のパソコンで遠隔操作ソフトが起動され、遠隔操作可能状態となっている。
  2. 「操作される側」のパソコンがネットワークに接続され、通信が可能となっている。
  3. 「操作される側」のパソコンの IP アドレスや遠隔操作ソフトを利用する際のアカウント情報（ID、パスワードなど）を「操作する側」が知っている。
- パソコンに偽のウイルス警告が出た際に相手に電話をかけ、相手に指示された内容をパソコンに入力したため、**自分では気づかないうちに３つの条件を満たしてしまい、遠隔操作が始まったというご相談が多く寄せられています**。

## 1-2. 遠隔操作ソフトを悪用された場合のリスク

### ■ 遠隔操作ソフトを悪用されると、以下のようなリスクが発生します

- 不審なソフトをインストールされる。
- パソコンをロックされて使えないようにされたり、パソコン内のデータを消去されたりする。
- メールの文面、保存している写真、オンラインショッピングの購入履歴などを画面に表示していれば、それらに含まれる様々なプライベート情報を知られてしまう。

# ２． 遠隔操作ソフトを利用したサービスを受ける際の注意点

パソコンの設定やサポートを、遠隔操作ソフトを利用して行うサービスは、利用者にも提供者にもメリットがあります。一般的に遠隔操作ソフトを利用したサービスは、次のような流れで行われます（図４）。

サービス提供者は、サイトの URL を指定して、遠隔操作される側にソフトや実行ファイルをダウンロードさせます。[*3]


図４： 遠隔操作ソフトを利用したサービスの一般的な流れ

### ■ 万が一のトラブルに備えた実践事項

図４のような遠隔操作ソフトを利用したサービスを受ける際には、万が一のトラブルに備えて、下記を実践してください。

- 遠隔操作を行う担当者の企業名、所属、名前、連絡先をできるかぎり確認してください。
- 遠隔操作による作業の内容や目的を事前に確認してください。
- 遠隔操作ソフトや遠隔操作の実行ファイルの名称、開発元、ダウンロードサイト（URL）、主な機能を確認してください。
- 遠隔操作による作業実施中はパソコンから目を離さず、操作内容を確認してください。

- 作業完了後は、遠隔操作ソフトを確実にアンインストール（削除）してください。
- なお、作業途中に事前説明のない操作がされるといった、不審な動きが見られた場合には無線 LAN 機能をオフにする、ネットワークケーブルを抜く、ルータの電源を落とす等、パソコンのネットワークを切断することで、それ以上の遠隔操作を強制的に中断させることができます。その場合は、改めて作業内容を確認し、十分に理解、納得した上で遠隔操作の継続可否を判断してください。

## ■ 偽のセキュリティ警告による遠隔操作の手口と考えられる場合

- 自分が普段から利用しているセキュリティソフトによる警告ではない場合、特にインターネット利用中にブラウザ画面上に表示される警告は偽物である可能性が高いと考えられます。
- 偽の警告画面が表示された場合、相手に電話をかけると遠隔操作に誘導されますが、電話もせず遠隔操作もさせないでください。
- 偽警告画面かどうかの判断が難しい場合は、画面をそのままの状態にして IPA の安心相談窓口へご相談ください。
- 偽のセキュリティ警告の場合は、「Microsoft」やセキュリティ事業者を騙っていたというご相談を多く受けております。しかし、Microsoft では、メッセージと警告メッセージに電話番号が記載されていることはないと説明しています。[(*4)]

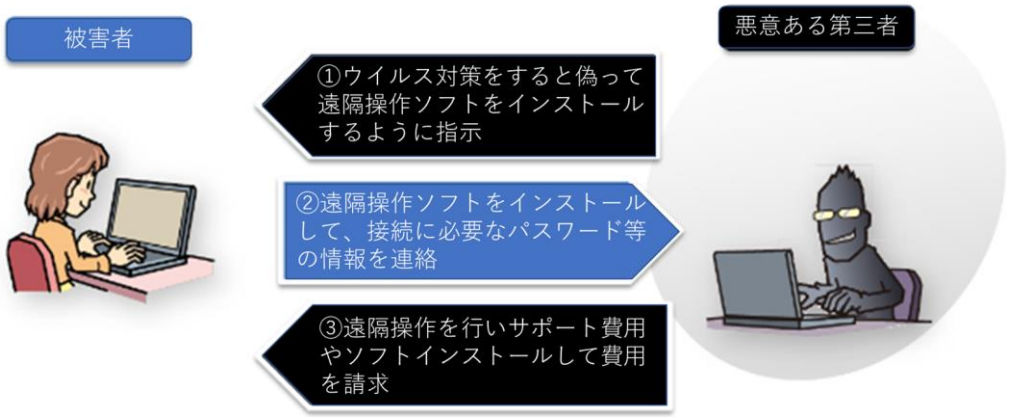


図 5：遠隔操作ソフトを悪用した被害に遭う例

利用目的を理解せずに遠隔操作ソフトのインストールや、遠隔操作の実行ファイルをダウンロードしてしまうと、思わぬトラブルに巻き込まれてしまう可能性が考えられます。言われるがままパソコンに遠隔操作ソフトをインストールしたり、遠隔操作の実行ファイルをダウンロードしてしまうことは絶対に避け、偽のセキュリティ警告による誘導ではないかと考えたり、上記の実践事項を行ってください。

---

(*3) ウイルスの偽警告の相談でよく聞く遠隔操作ソフトには、「LogMeIn」、「TeamViewer」、「AnyDesk」といったものがあります。

(*4) Microsoft:テクニカル サポート詐欺から保護する方法
https://support.microsoft.com/ja-jp/windows/テクニカル-サポート詐欺から身を守る-2ebf91bd-f94c-2a8a-e541-f5c800d18435

## 更新履歴

2020 年 11 月 25 日　掲載

## 本件に関するお問い合わせ先

情報セキュリティ安心相談窓口

Tel: 03-5978-7509　Fax: 03-5978-7518
E-mail: anshin@ipa.go.jp
セキュリティセンター　伊藤（よ）／中島