第 14-18-323 号
2014 年 11 月 4 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 遠隔操作ソフトは利用目的を理解してインストールを！ 」

2014 年 4 月、知り合った女性にセキュリティソフトと偽ってインストールさせた**遠隔操作ソフトを悪用して個人情報を窃取する**という事件[※1]がありました。この事件で使われた遠隔操作ソフトは、ウイルスや不正なソフトではなく一般に市販されている正規のものでした。

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す。見知らぬ訪問者に悪意があれば、部屋の物色や貴重品の盗難などの被害の恐れがあるように、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などの被害の恐れがあります（図 1）。

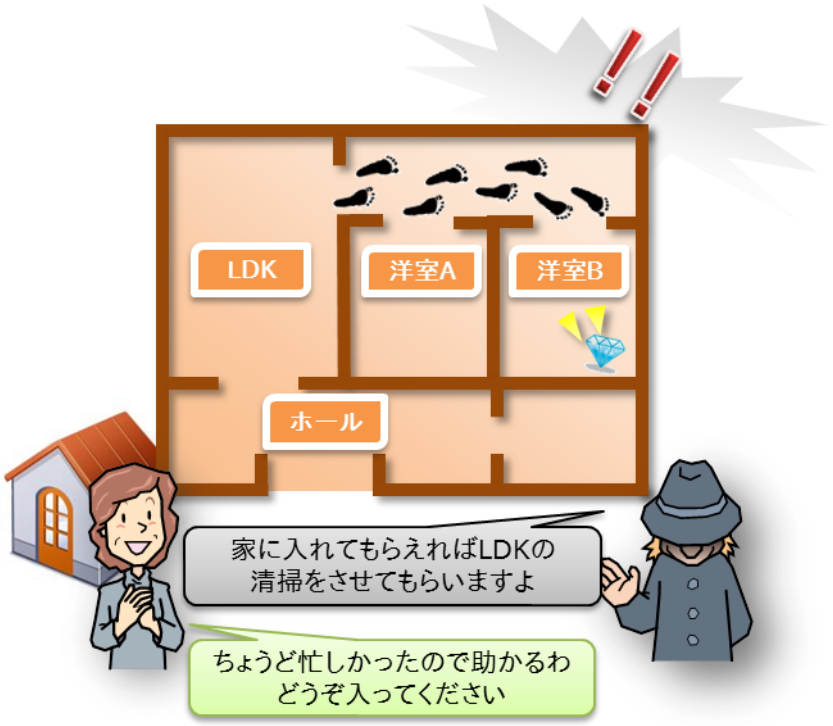

図 1：遠隔操作ソフトのインストールを家に人を招き入れることに例えたイメージ

また、2014 年 8 月以降、IPA の安心相談窓口に「勧誘電話でプロバイダ料金が安くなると言われ、遠隔操作ソフトをインストールしてパソコンの設定を変更してもらったが、パソコンをこのまま利用していても問題ないのか」という相談が相次いで寄せられています。

[1] 産経ニュース：東京の男に PC 乗っ取られた京都女性の“無謀”
http://www.sankei.com/west/news/140613/wst1406130075-n1.html

国民生活センターによれば、遠隔操作によるプロバイダ変更の勧誘トラブルに関する相談件数が2013年度から急増[※2]しており、2013年度の相談件数は、2012年度と比べて約8.5倍となる1,596件でした。さらに、2014年度の相談件数は9月5日の時点で、前年度とほぼ同数となる1,537件もの相談が寄せられています（図2）。

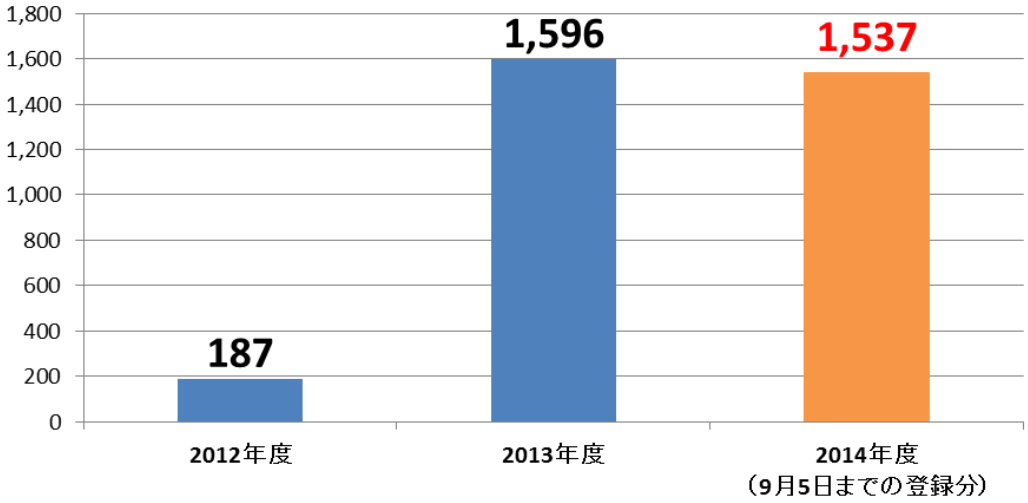

図2：遠隔操作によるプロバイダ変更勧誘トラブルに関する相談件数推移
（国民生活センターの発表資料を元に作成）

遠隔操作ソフトは、本来、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[※3]。しかし、遠隔操作ソフトを悪用されると、冒頭の事件のような被害に遭う可能性もあります。

今月の呼びかけでは、遠隔操作ソフトを悪用された場合のリスクと、遠隔操作ソフトを利用したサービスを受ける際の留意点を紹介します。

（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いると、操作する側が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）。

[2] 国民生活センター：相談激増！遠隔操作によるプロバイダ変更勧誘トラブルにご注意
http://www.kokusen.go.jp/news/data/n-20140918_1.html
[3] TOSHIBA：遠隔支援サービス
http://dynabook.com/assistpc/remote/index_j.htm

図 3：遠隔操作ソフトによる遠隔操作のイメージ

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」のパソコンに遠隔操作ソフトがインストール（実行）され、サービスが有効となっている
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

（2） 遠隔操作ソフトを悪用された場合のリスク

冒頭の事件のように騙されて遠隔操作ソフトをインストールしてしまうと、悪意ある第三者からメールの内容を盗み見られたり、本人になりすまして掲示板や SNS に書き込みをされたりという被害に遭う可能性があります（図 4）。

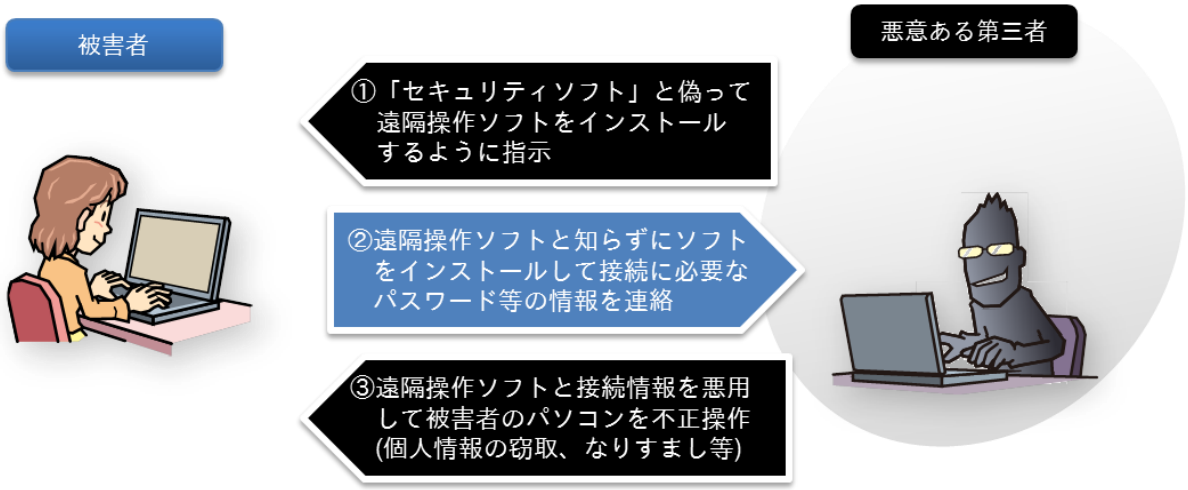

図 4：遠隔操作ソフトを悪用した被害に遭う例

しかし、パソコンの画面を見ていれば勝手にマウスカーソルが動く、ウィンドウが開く、ファイルが増える（または減る）といった悪意ある第三者による遠隔操作の内容が確認できるため、被害者は不正な操作に気づくことができます。

そのため、遠隔操作ソフトによる被害が疑われる場合はパソコンの利用中に不審な動きがないか画面に注意を払い、パソコンから離れないことが重要です。ただし、パソコンの画面上で特に不正な操作がないからといって被害に遭わないとは限りません。遠隔操作はされてなくても、表示されている画面や操作内容を見られている可能性があるからです。

例えば、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が悪意ある第三者に知られてしまう恐れがあります。

（３） 遠隔操作ソフトを利用したサービスを受ける際の留意点

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。しかし、IPA の安心相談窓口に寄せられている相談のように、遠隔操作ソフトを利用してパソコンの設定を変更されたことに対して後から不安を感じる利用者もいます。

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 5）。

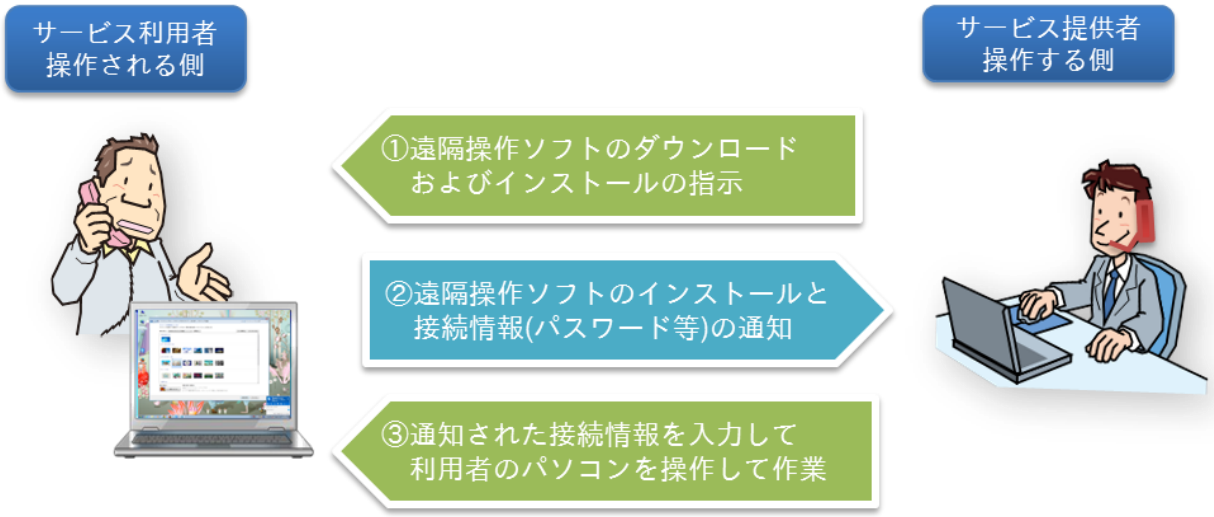

図 5：遠隔操作ソフトを利用したサービスの一般的な流れ

図 5 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。

【実践事項】
- 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。

利用目的を理解せずに遠隔操作ソフトをインストールしてしまうと、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てしまうことは絶対に避け、上記の事項を実践する**よう心がけてください。

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／野澤
Tel: 03-5978-7591　Fax: 03-5978-7518
E-mail: isec-info@ipa.go.jp