偽セキュリティ警告に注意

相談件数が増加 5月は過去最高に

独立行政法人情報処理推進機構（ＩＰＡ）では、一般的な情報セキュリティに関する技術的な相談窓口「情報セキュリティ安心相談窓口」を運用している。最近は、パソコンのブラウザ画面に表示される「偽セキュリティ警告（別名：サポート詐欺）」の手口に関する相談件数が継続して増加しており、月間相談件数が、２０２３年５月は過去最高の４４６件となった。一般ユーザーと比べると少ないものの、企業からも当該被害に関する相談が寄せられているので、注意していただきたい。

企業ではテレワークで従業員が自宅で業務用パソコンを使って仕事をする機会が増え、「偽セキュリティ警告」の手口に遭遇した際に、同僚、上司、システム管理者が近くにいないため、自分で解決しようとして被害が発生していることも要因の一つと思われる。表示された電話番号に電話をかけて、相手にパソコンを遠隔操作されると、パソコン内に機密情報や個人情報が保管されていた場合に、情報漏えい事故としての対応が必要になるかの判断や調査を迫られることとなる。

代金支払いへ誘導 情報漏えいの懸念も

偽セキュリティ警告の手口は、パソコンでインターネット閲覧中のブラウザ画面上に、本物に見せかけたセキュリティ警告が表示され、解決のために記載してある電話番号に電話をかけるように誘導されるというもの。電話をかけると、オペレーターにパソコンを遠隔操作され有償サポート契約と代金支払いへ誘導される。支払い手段はプリペイドカードを指定されるため、ほとんどの場合はコンビニエンスストアにそのカードを買いに行くように指示される。

一般ユーザーからの相談では、相手にプリペイドカードを何度も買いに行かされ、カードの番号を相手に伝えてしまった結果、被害額が数十万円になるケースを多く確認している。

一方、企業の場合は、パソコンを遠隔操作されたことで情報が漏えいしたのではないかという心配の相談が多くなっている。

手口の周知徹底・対応ルールづくりを

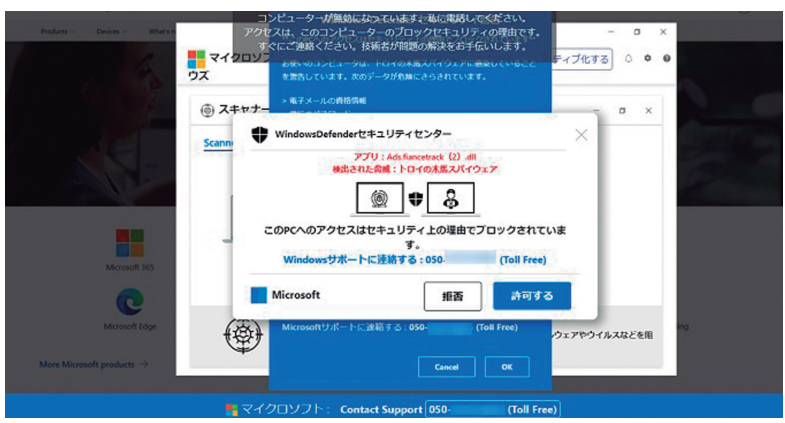
被害に遭わないための対策として、管理者は、社内で偽セキュリティ警告の手口について、周知や研修を行っていただきたい。その際はＩＰＡの注意喚起などを参考にしてほしい。また、偽セキュリティ警告に限らず、パソコンに異常があった場合の対応ルールを定めて徹底していただきたい。特に、テレワーク時に発生した異常の連絡や、管理者の許可なく業務用のパソコンを第三者に遠隔操作をさせないことを徹底してほしい。

従業員は、パソコンにセキュリティ警告が出たら、対処を自分一人で判断せず、会社の対応ルールに従い、落ち着いてシステム管理者または上司に連絡していただきたい。冷静な対処が、ご自身、会社の情報資産を守ることにつながる。

また、画面に表示された電話番号に電話をしない、システム管理者または上司の許可なく相手からの遠隔操作の要求を許可しないでいただきたい。特に、パソコンの異常に対処するといったサポート名目の誘いに注意してほしい。

企業で偽セキュリティ警告に遭遇した相談事例や情報漏えいの有無の判断材料、従業員研修のための参考情報などはＩＰＡのホームページで確認してほしい。

（独立行政法人情報処理推進機構・江島将和）



「警告画面が次々と全画面で開く」画面事例

安心相談窓口だより「会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡！」はこちら