サイバー防犯かわら版

第3号
生活安全部
サイバー犯罪対策課
令和8年6月

サポート詐欺被害が発生！身近に潜む罠にご注意！！

サポート詐欺とは

1　大手IT企業を装った**偽の警告画面**等を表示します。
2　警告音や警告メッセージを音声で流したりして不安を煽り、偽の警告画面の電話番号に電話をかけさせようとします。
3　電話をかけると**遠隔操作してサポート**するなどと言い、パソコンに**遠隔操作アプリ**のインストールを勧められます。
4　**サポート料**として、クレジットカード決済や各種ギフトカード、電子マネー等を要求し、**金銭を騙し取ります！**

※　金銭だけでなく、顧客リスト等を盗られるなど、情報流出するおそれもあります。

（例）サポート詐欺の画面

サポート詐欺にあわないポイント！

○　国際電話の利用停止（ほとんどが国際電話が使われています）
○　不審な（わけのわからない）ソフトウェアはインストールしない、させない
○　遠隔操作の許可をしない（サポートと見せかけて遠隔操作しようとします）
○　インターネットバンキングは二段階（要素）認証を導入する

ランサムウェア　その備えは大丈夫ですか？

ランサムウェアとは

ランサムウェアとは、「身代金」を意味するランサムとソフトウェアを組み合わせた造語で、企業等の*データを暗号化*したり利用できなくしたりして、*復旧と引き換えに金銭を要求*するサイバー攻撃です。

※　データの暗号化のほか、情報を盗られることもあります。

ランサムウェアは、VPN機器などのネットワーク機器の脆弱性を狙って攻撃してきます。

ランサムウェアの被害にあわないために備えましょう!

○　ＶＰＮ機器などのネットワーク機器を最新の状態に保ちましょう(更新を忘れずに)。
○　基本的なセキュリティ対策をしましょう（セキュリティ対策ソフトウェアの導入など）。
○　アクセス管理を徹底しましょう（アクセス権の厳格な管理と権限ごとのアクセス範囲の切り分けなど）。
○　オフラインバックアップを定期的に取得しましょう(復元可能な状態で保管することで、ランサムウェア攻撃を受けた場合も、データを復旧することができます)。
○　平時から復旧手順を確認し、復元訓練を行いましょう(バックアップがあっても復旧できなければ意味がありません)。

YouTube沖縄県警警察公式チャンネルでも広報動画を配信しています