

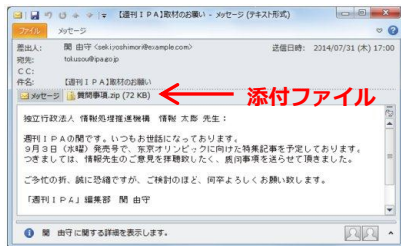
音声で脅迫するランサムウェアの感染に注意!!

ランサムウェアとは、身代金要求型の不正プログラムであり、感染するとパソコン内に保存しているファイルが勝手に暗号化され、復号の引き換えとして金銭を要求されます。

本年3月中旬頃には、合成音声（英語）を使ってユーザーを脅迫するランサムウェアの存在が確認されており、今後、日本国内で被害が発生するおそれがあります。注意してください!

代表される2つの主な感染原因

【受信メールの添付ファイル等からの感染】



不用意に受信したメールに添付のファイルを開いたり、メール本文中のURLをクリックすることにより、不正プログラムが組み込まれたファイルが起動したり、ウェブサイトへ誘導され感染する被害が急増しています。

【ウェブサイトの閲覧等による感染】



最近では、改ざんされたウェブサイトを閲覧したり、不正プログラムが組み込まれたファイルをダウンロードすることによる感染被害が確認されています。

その結果、データが暗号化され使用不能に!!

【脅迫文を表示】



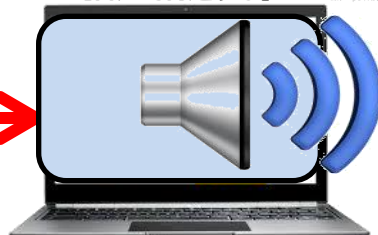
ファイルの暗号化及び復元の見返りに金銭を要求する内容を強制的に表示

【音声言語の選択画面を表示】



言語は、英語のほか日本語の選択が可能

【音声で脅迫する】



音声「あなたのドキュメント、写真、データベース、その他重要ファイルが暗号化されました。復号して欲すれば、指示に従ってビットコインで支払うこと」等の内容

*上記画像は、トレンドマイクロ株式会社から引用

~感染リスクの低減策（100%の対策は存在しないことに留意!!）~

- ◎ 不審なメールは開かず、送信者・添付されたファイル（拡張子が.zip・.exeなど）、添付されたURL、文面を確認してください!!
- ◎ ウェブサイトの改ざんは、URL等に変化がないため容易に見えません!! 不用意にファイルやソフトをダウンロードせず、ウイルスチェックを徹底してください。
- ◎ ウィルス対策ソフトやソフトウェアを最新の状態に更新してください!!（更新されていないければ、効果はありません。）
- ◎ 大切なデータのバックアップを定期的に取りましょう。万が一、ランサムウェア等に感染してもバックアップデータがあれば復元が可能です。ただし、バックアップに使用する媒体等は、バックアップ時のみパソコンと接続することが重要です。

京都中小企業情報セキュリティ支援ネットワーク (Ksisnet)
IT 相談窓口 (公益財団法人京都産業21 お客様相談室)

相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の9:00～17:00（祝日を除く）

TEL 075-315-8660 メールアドレス okyaku@ki21.jp

公益財団法人京都産業21 お客様相談室 (〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内)

