



STOP! ランサムウェア

ランサムウェアは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラムです。



ランサムウェア攻撃の手口



◆ メールから感染させる

メールの添付ファイルやメール本文中のリンクを開かせることで感染させる。知人や取引先を装うこともある。

◆ ウェブサイトから感染させる

ぜい弱性を悪用し、ランサムウェアをダウンロードさせるよう改ざんしたサイトや攻撃者が用意したサイトを閲覧させて感染させる。

◆ ぜい弱性によりネットワーク経由で感染させる

ソフトウェアのぜい弱性を未対策のままネット接続されているVPN機器等に対しネット経由で感染させる。

◆ 公開サーバーに不正アクセスして感染させる

外部に公開しているサーバーにリモートデスクトップ等で不正アクセスして感染させる。



被害防止のための対策



- ・ 受信メールの添付ファイルやリンクを安易にクリックしない
- ・ 機器のぜい弱性対策を迅速に行う（サポート切れOS、ソフトの利用停止）
- ・ 共有サーバー等へのアクセス権の最小化と管理の強化
- ・ 定期的なバックアップの取得

※ストップ!ランサムウェア 特設サイト (NISC) はこちら→

