# ランサムウェアによる攻撃に注意！

「ランサムウェア」とは、端末（パソコンやスマートフォン）の画面をロックさせたり、端末内の文書、画像、動画などのファイルを使用できなくして、その復旧と引き替えに金銭を要求するウイルスです。

【ｒａｎｓｏｍ(ランサム)＝身代金】

## ランサムウェアの脅威

ファイルを使用できなくする前に端末やファイルサーバの情報を盗み取り、ファイルの復旧だけでなく、盗み取った情報の公開を止めるために金銭を要求する、新たな手口のランサムウェアに注意してください。

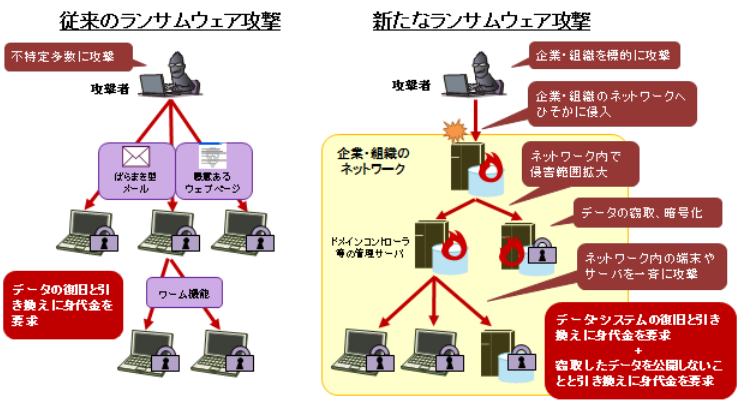
### 従来のランサムウェア

これまでは、「メールの添付ファイルや記載されたＵＲＬのリンク」「ランサムウェアが仕込まれたウェブサイト」などを利用して不特定多数への感染が主なものでした。

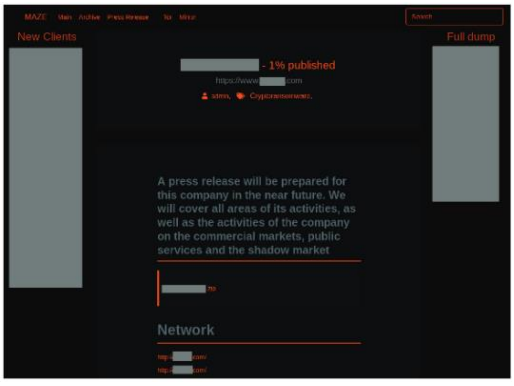
### 新たな手口のランサムウェア

従来の手口に加えて、金銭を支払わなければ盗み取った情報を公開するとの脅迫内容が追加。要求に応じない場合、下図のような情報公開サイトに会社名や盗み取った情報を公開するケースも。

**従来／新たなランサムウェア攻撃の差異**




**盗み取られた情報などが公開されているサイト【例】**




出典：独立行政法人情報処理推進機構(IPA)

## 被害防止対策

- ✓ 身に覚えのないメールは開かない
- ✓ メールの添付ファイルや本文中のリンクを不用意に開かない
- ✓ ＯＳやソフトウェアを最新の状態に保ち、脆弱性を解消する
- ✓ ウイルス対策ソフトを導入し、常に最新の状態を保つ
- ✓ 認証強化やアクセス制限などの不正ログイン対策を行う
- ✓ 内部の不審を可視化するためのネットワーク監視を行う
- ✓ 大切なデータはバックアップしておく
- ✓ バックアップを確実に取得し、ネットワークから切り離して保管する

トレンドマイクロ株式会社ホームページ（https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/ransomware.html）や同社動画チャンネルfor Business(https://www.youtube.com/watch?v=A_vl6_rC98U)にランサムウェアへの感染防止や被害低減について掲載されていますので参考にしてください。