Ksisnetだより
発行:Ksisnet事務局
令和 4年8月4日
Vol.108

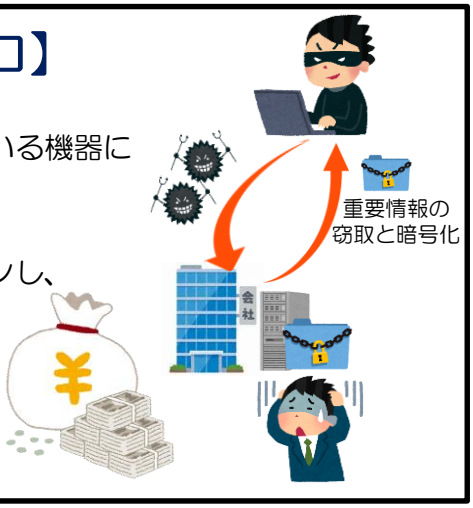
「情報セキュリティ10大脅威2022」（組織）
1位　ランサムウェアによる被害

パソコン等の端末やサーバ上のデータを暗号化する等して使用不可にし、それらを復旧することと引き換えに身代金を支払うよう脅迫するランサムウェア攻撃については、引き続き注意が必要なサイバー攻撃であり、**「情報セキュリティ10大脅威2022」の組織部門で第１位**に選出されています。暗号化前に重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する攻撃**「二重の脅迫」**が近年確認されています。

【企業・組織を標的とする攻撃手口】

● **脆弱性によりネットワーク経由で感染させる**
ソフトウェアの脆弱性を未対応のままインターネットに接続されている機器に対して、その脆弱性を悪用してインター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ログインし、ランサムウェアに感染させる。



二重の脅迫

① データ・システムの復旧
② 窃取したデータを公開しないこと
を引き換えに身代金を要求

【 対　策 】

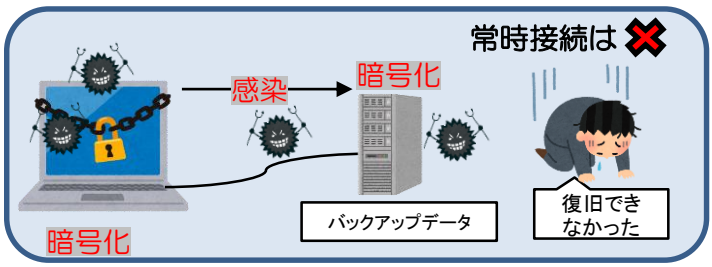
- 迅速、継続的に対応できる体制を構築する
- 多要素認証の設定を有効にする
- 不審なメールに添付されたファイルやリンクを安易にクリックしない
- 提供元が不明なソフトウェアを実行しない
- 機器の脆弱性対策を迅速に行う
  パッチ適用を迅速に行い、サポート切れのＯＳは利用しない
- セキュリティ対策ツールの利用や設定見直し
  アプリケーション実行制限や、メールおよびウェブのフィルタリングを行う。ポリシー設定を見直し、遮断設定を極力有効にする。
- 共有サーバ等へのアクセス権の最小化と管理の強化
- 公開サーバへの不正アクセス対策
- ネットワーク分離

過去には、被害に遭い金銭を支払った企業もあったが、必ずしもデータの復旧や漏洩した情報の削除が行われるとは限らない！

まずは被害に遭わないようしっかり対策をとりましょう！

【バックアップについて】

環境を更新すればバックアップは必ず取り、保存されたバックアップデータが巻き添えにならないよう常時接続はさけましょう！！



（IPA「情報セキュリティ10大脅威2022」を基に作成）

「情報セキュリティ10大脅威 2022」の詳細については、下記ウェブサイトで公開されています。
https://www.ipa.go.jp/security/vuln/10threats2022.html