ランサムウェア被害の実態（R4上）

MiCS みやざきサイバーセキュリティ
宮崎県企業・警察ｻｲﾊﾞｰｾｷｭﾘﾃｨ連携協議会
宮崎県警察本部サイバー犯罪対策課

1　ランサムウェアとは

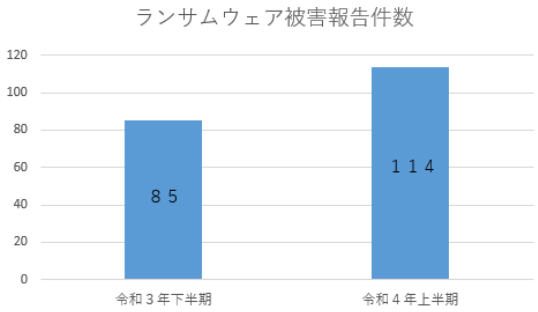
コンピュタウイルスの一種でransom(身代金)とsoftware(ソフトウェア)を組み合わせた造語。感染するとデータを暗号化して使用できない状態にした上で、そのデータを復元する対価として金銭を要求する。

2　被害の概要

(1)　被害報告件数

令和３年下半期　85件

令和４年上半期　114件



(2)　内訳等

○　被害企業規模別

企業・団体等の規模を問わず被害が発生。

（大企業31%、中小企業52%、団体等17%）

○　データ復元名目の金銭要求、更には支払わなければデータを公開すると要求する二重恐喝の手口が65%を占める。

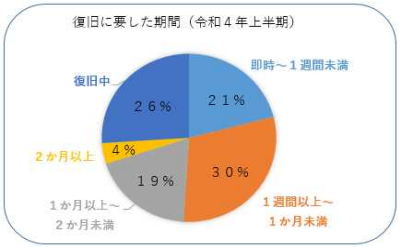
3　被害の実態

(1)　復旧に要した期間･費用

○　復旧に１週間以上要したケースが53%以上。

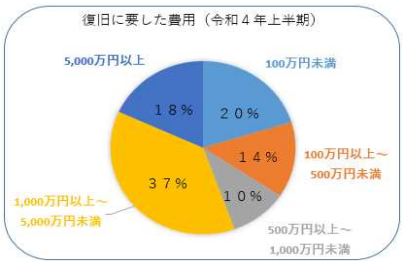
○　1,000万円以上の費用を要したケースが55%。

中には、復旧まで２か月以上、5,000万円以上を要するケースがあるなど、被害は甚大である。



(2)　感染経路

ウイルスの感染経路としてＶＰＮ機器から侵入したケースが約68%あり、テレワーク対応等により導入したと思われるＶＰＮ機器の管理が適切でなく、被害に遭った事例が増えていることが示唆される。



(3)　ウイルス対策ソフトの導入状況

○　ウイルス対策ソフトを導入していたにもかかわらず、88%が被害に遭っている。

○　ウイルス対策ソフトを導入していても「ソフトやシステムが古い・未対応」等の理由によりウイルスを検知できず、被害に遭ったケースがみられた。

4　被害防止対策

(1)　電子メール等への警戒、ＯＳ等の脆弱性対策（更新、修正）、認証情報の管理。

(2)　バックアップからの復元はシステム・機器の再構築よりも復旧時間が短くて、復旧費用も安く済むケースがあるため、データのバックアップを取得しておく。

（バックアップのデータも暗号化されないように注意する。）

(3)　情報セキュリティポリシーを策定し、アクセス権限等の限定、ネットワークの監視を行い、定期的に情報セキュリティポリシーの監査を実施する。