



サイバーセキュリティの置き薬

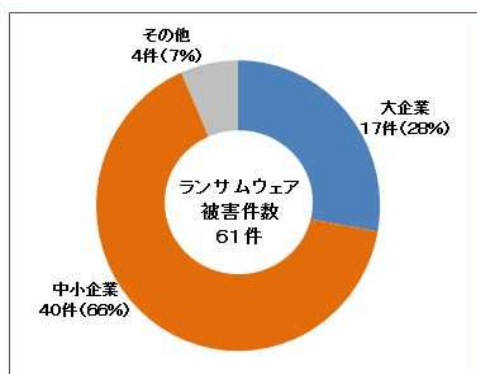
2021年
第11号

(警察庁広報資料：令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について)

ランサムウェアの情勢について

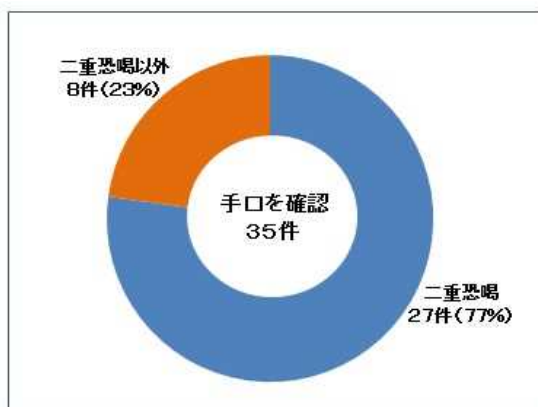
ランサムウェアの被害は、企業・団体等の規模を問わず発生しています。(図表1)

最近の事例では、データの暗号化のみならず、データを窃取した上、「対価を支払わなければ当該データを公開する」などと金銭を要求する二重恐喝(ダブルエクストーション)という手口が認められています。

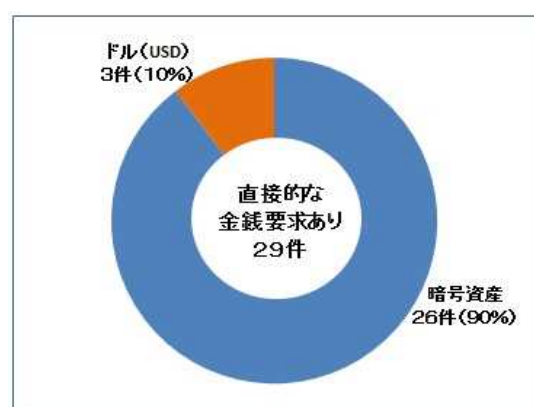


図表1：ランサムウェア被害の規模別報告件数

令和3年上半期(全国)：大企業17件、中小企業40件



図表2：ランサムウェア被害の手口別報告件数



図表3：要求された金銭支払い方法別報告件数

<主な特徴>

○ 被害件数が大幅に増加

令和3年上半期に都道府県警察から警察庁に報告のあった件数は61件であり、令和2年下半期(21件)と比べて大幅に増加しました。

○ 二重恐喝(ダブルエクストーション)による被害が多くを占める

被害件数(61件)のうち、警察として金銭の要求手口を確認できた被害は35件であり、このうち、二重恐喝の手口によるものは27件で全体の77%を占めています。(図表2)

○ 暗号資産による金銭の要求が多くを占める

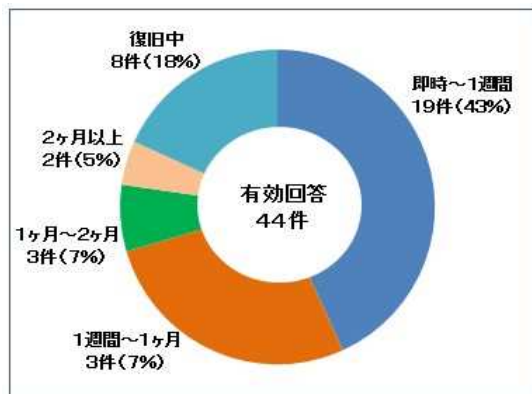
被害件数(61件)のうち、直接的に金銭の要求があった被害は29件あり、このうち、暗号資産による支払いの要求は26件で全体の90%を占めています。(図表3)



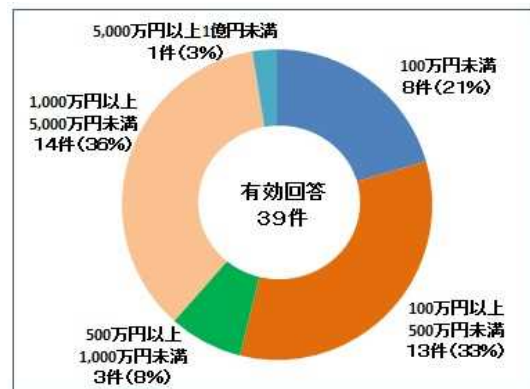
<ランサムウェア被害の実態>

従来のランサムウェアは、不特定多数の利用者を狙って電子メールを送信するといった手口が一般的でしたが、現在では、VPN機器からの侵入等、特定の個人や企業・団体等を標的とした手口に変化しており、企業のネットワーク等のインフラを狙うようになっています。

警察庁では、企業・団体等におけるランサムウェア被害の実態を把握するため、被害件数(61件)のランサムウェア被害に関し、アンケート調査を実施したところ、令和3年8月末までに50件の回答が得られたことから、その回答結果について分析を行いました。



図表4：復旧に要した時間



図表5：調査・復旧費用の総額

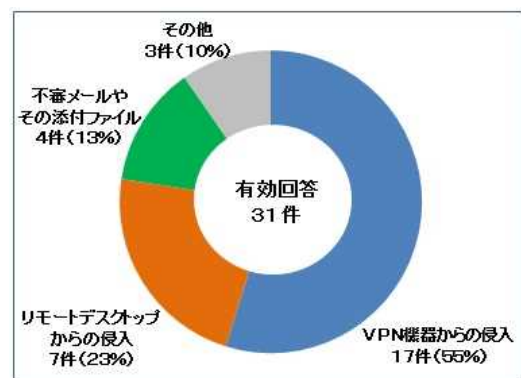
○ 復旧等に要した期間・費用

復旧に要した期間について質問したところ、44件の有効な回答があり、このうち、1週間以内に復旧したものが19件と最も多かったが、復旧に2か月以上要したものもありました。(図表4)

また、ランサムウェア被害に関連して要した調査・復旧費用の総額について質問したところ、39件の有効な回答があり、このうち、1,000万円以上の費用を要したものが15件で、全体の39%を占めています。(図表5)

○ 感染経路

ランサムウェアの感染経路について質問したところ、31件の有効な回答があり、このうち、VPN機器からの侵入が17件で全体の55%を占め、次いで、リモートデスクトップからの侵入が7件で全体の23%を占めており、テレワーク等の普及を利用して侵入したと考えられるものが全体の8割近くを占めています。(図表6)



図表6：感染経路

【参考サイト】

ランサムウェア被害防止対策ページ「<https://www.npa.go.jp/cyber/ransom/index.html>」

(警察庁サイバー犯罪対策プロジェクト)



ランサムウェア被害を受けた際は、警察への通報をお願いします！