サイバーニュース

2023年1月
第２号

石川県警察サイバー犯罪対策イメージキャラクター「サイビット」

ランサムウェア感染時の措置について

感染端末のデータを暗号化し、データの身代金として暗号資産（仮想通貨）を要求するランサムウェア。このコンピュータウイルスによって、大企業だけでなく、中小企業や医療機関、教育機関、行政機関など様々な組織が被害に遭っています。

過去のサイバーニュースで、未然防止対策について紹介してきましたが、今回は**万が一感染した場合の措置**について説明します。

☆感染した端末を ネットワークから隔離

ランサムウェアはネットワーク上に接続されている他の端末にも感染を広げます。

ＬＡＮケーブルを抜く、ルータの電源を切る、端末を機内モードにするなどして、**ネットワークから隔離**しましょう。

☆感染した端末は 電源を切らないように

感染した端末（パソコン等）には、暗号化を解除（復号）するのに必要な情報が残っていることがあります。

端末の電源を切ってしまうとその大事な情報が消えてしまう可能性があるので、**電源を切らない**ようにしましょう。

☆組織全体で対応

組織内での感染が広がる前に、速やかに組織内で情報を共有しましょう。

場合によっては、支店や提携会社などにも**速やかに連絡**することで、感染拡大を防げる可能性があります。

☆警察に相談・通報

サイバー犯罪の実態を明らかにするため、自社を管轄する**警察署や本部サイバー犯罪対策課に通報**しましょう。

業種によっては、所管省庁や取引のあるセキュリティ企業、ＩＰＡ、ＪＰＣＥＲＴ／ＣＣに連絡し、事後対応の指示を受け、行動しましょう。

復号（暗号化の解除）について

<u>一部のランサムウェア</u>について、**復号ツールが公開**されています。ただし、全データを復号できない場合や、復号ツールによって不具合が生じる場合があるなど、様々な注意点があります。それぞれの復号ツールについての情報や、その使用方法など、詳しくは「ＪＣ３」のＷｅｂサイト『ＪＣ３　ランサムウェア』で検索してみてください。

Twitter @IP_cybertaisaku

石川県警察本部生活安全部サイバー犯罪対策課
０７６－２２５－０１１０　cyber@police.pref.ishikawa.lg.jp

Instagram IP_cybertaisaku