



医療機関にランサムウェアによるサイバー攻撃! 電子カルテが閲覧できないなど深刻な影響

大阪府内の医療機関がランサムウェアによるサイバー攻撃を受け、電子カルテが閲覧できず、通常どおりの診療ができない、手術ができないなど医療現場に深刻な影響が発生しています。

ランサムウェア被害を防止するため、万一被害に遭った場合でも損害を最小限に抑えるための措置を確実に実施願います。

ランサムウェアとは?

感染したパソコンをロックしたり、ファイルを暗号化することによって使用不能にした後、元に戻すことと引換えに「身代金」を要求する不正プログラム



被害防止対策

- ・ ウイルス対策ソフトを導入して定期的に更新する!
- ・ 機密情報は外部からアクセスできない設定にする!
- ・ セキュリティ保守管理事業者との情報交換を密にし、セキュリティ対策を最新の状態に設定する!

万一被害に遭った場合のために「3・2・1ルールの実践」

ランサムウェアに感染したことを想定し、データを復旧できるように適切にバックアップを確保しておくことが必要です!「バックアップのための3・2・1ルールを実践しましょう。」

- ・ データを**3**つ持つ。(元データのコピーを2つ作成する)
- ・ **2**種類の異なるメディアでバックアップをとる。
(クラウドストレージとHDDなど)
- ・ バックアップのうち**1**つは離れた別の場所で保管する。

サイバー犯罪被害に関する届出・相談などは最寄りの警察署又は警察本部サイバー犯罪対策課へ連絡ください。
長崎県警察本部生活安全部サイバー犯罪対策課 095-820-0110 (3451・3452)