

サイバー攻撃を受けた半田病院の状況(～覚知)

徳島県つるぎ町 人口:約8,200人
 半田病院 病床数:120床 外来患者数:250~300人/日 10年前に電子カルテに切り替え、紙の記録は残っていない
 県西部で唯一の分娩可能な施設 2市2町の西部医療圏の夜間・休日小児救急医療は他1病院と交代で輪番制で担当

10月31日午前0:30

十数台のプリンターから一斉に大量の紙が吐き出された

「データを暗号化した。身代金を払わなければ公表する。復元してほしいければ連絡しろ」と英語で脅迫内容と連絡先が記されていた

Your data are stolen and encrypted...



ランサムウェアに感染



電子カルテが使えない!



何にもできないんだけどー!!

看護師がシステム担当者に連絡

午前3:00ごろ

回線を遮断するなどの対応を始めた

バックアップ用も含めた、院内のサーバーのデータがほぼ暗号化

受付～会計まで全ての電子システムがダウン

午前9:00ごろ

徳島県警に通報

県警はコンピューターウイルス犯罪に適用される不正指令電磁的記録供用などの疑いで捜査

国際的ハッカー集団「LockBit 2.0」の仕業だった

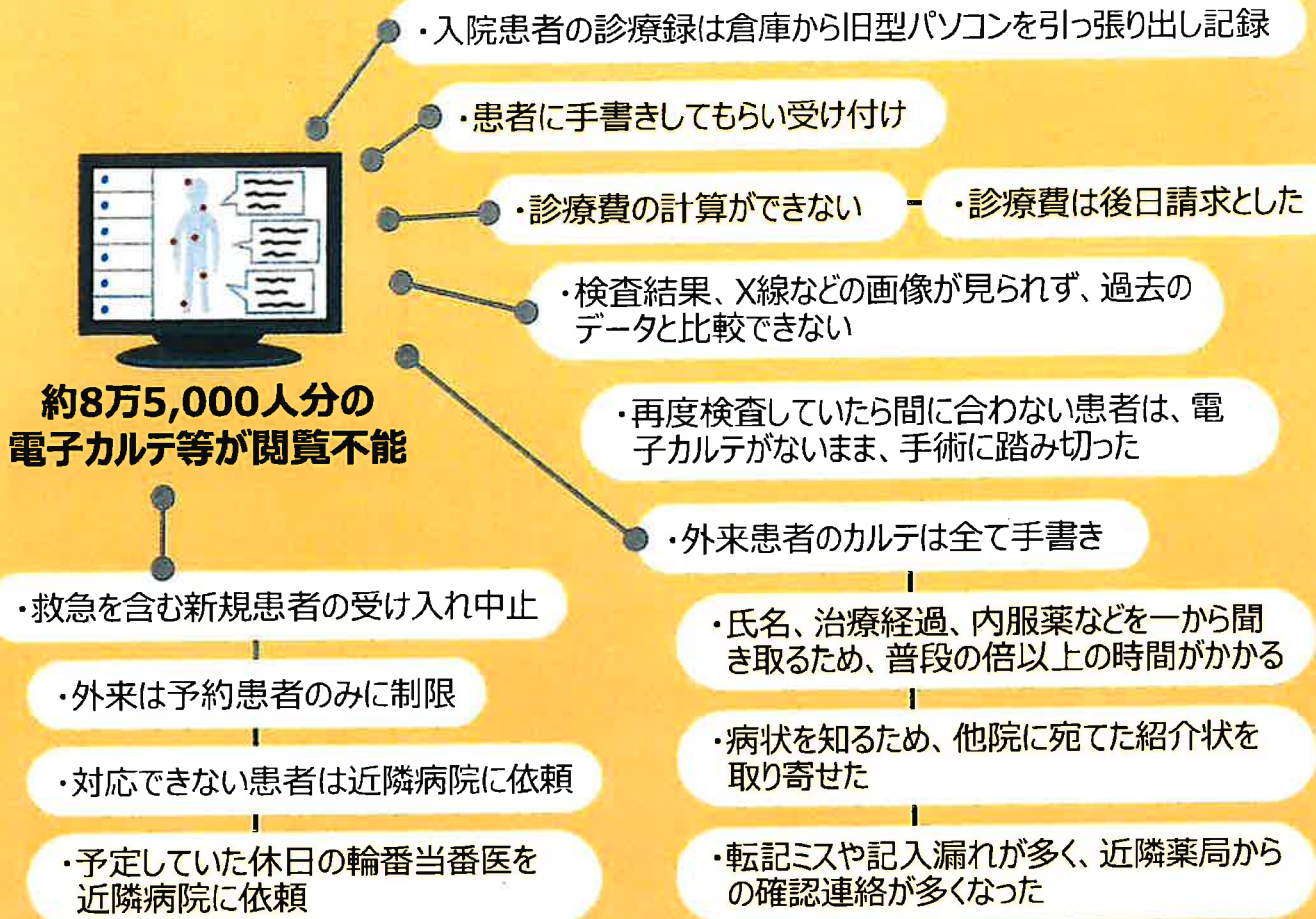
- システム構築時は自然災害を想定し、**サイバーテロは想定していなかった**
 - メインサーバーを1階、地震・水害対策のためバックアップサーバーを2階に設置していたが、**両サーバーは同一回線につながっていた**
 - 米フォーティネット製の「VPN」と呼ばれるシステムの機器の**古いタイプ**(過去に脆弱性が指摘されていた)を使っていた



電子システムがダウンした影響



Medical safety club (2021/12/03)



約8万5,000人分の電子カルテ等が閲覧不能

11月15日

小児科の通常診療を再開

11月19日

夜間・休日小児休日診療を再開
産科で新規妊産婦や救急受け入れを再開(婦人科は、予約のある再診患者に限定)

11月25日

2億円かけ新システムに切り替えカルテを再構築する方針に決定

犯行側は指定URLにアクセスし、交渉のテーブルにつくよう求めているが、身代金を支払っても、データが戻る保証もないことからアクセスせず、交渉を行っていない

11月30日に放射線科、12月1日に内視鏡検査、12月13日に健康診断、**2022年1月4日をめどに全ての診療を再開する予定**

電子カルテシステムに入るIDとPWがネット上に漏洩していたことも判明

ハッカー集団は弱点のあるシステムを無作為に探し、侵入するとも言われています。早急にシステムの安全性を確認しましょう!



【出典】(all accessed on 2021-12-02)
・警察庁「ランサムウェア被害防止対策」<https://www.tpa.go.jp/cyber/ransom/index.html>
・NEC「VPN構築ルータ VPN構築について」https://www.necplatforms.co.jp/product/vpn_router/vpn/index.html
© 2021 Sampo Risk Management Inc. All Rights Reserved.