

ついに日本でも病院がサイバー攻撃の標的に!

海外では以前から問題となっていました。近年、日本国内でも医療機関がサイバー攻撃の標的となっていることはご存じでしょうか。医療機関は患者の病状というセンシティブ情報を取り扱っているにも関わらず、情報を管理するシステムが脆弱であることが指摘されていました。そんな中、10月31日に発生した医療機関へのサイバー攻撃では、情報は戻ってこない上、2億円をかけてシステムを再構築するという甚大な被害をもたらされましたので、その概要をご紹介します。(各報道をもとに当社で作成)

● 国内外の医療機関へのランサムウェアによるサイバー攻撃

発生	病院名	概要
2017年8月以降	国内大学附属病院	放射線の撮影装置に不具合が出て、画像の再撮影が必要になった
2018年1月	アメリカの ハンコック・リージョナル病院	被害時は紙カルテなどで対応し、約5万5,000ドル支払い、4日後にすべてのシステムが復旧
2018年10月	国内市立病院	電子カルテデータが暗号化され、患者1,100人余りの診療記録の一部が開けなくなった 身代金は支払わず、翌3月に復元成功
2019年5月	国内共済病院	システム障害が発生し、患者の受け入れ制限を行った
2019年7月	アメリカのスプリングヒル・メディカルセンター	医療機器が停止 。攻撃中に患者が出産し、子供はへその緒が首に巻き付いた状態だったが、モニター機器が停止していたため、異常に気付かず、新生児が脳に重い損傷を受け、後に 死亡
2020年5月	英国の複数の病院	システムが停止し、手術のキャンセル などに追い込まれた
2020年9月	ドイツの大学病院	救急患者の受け入れができず 、患者を別の病院に搬送することになった患者が 死亡 するという事例も発生した
2021年3月	オーストラリアの病院	ITシステムをすべて停止し 、緊急度の低い手術を延期した
2021年5月	アメリカの病院	14万人以上の 患者・職員の個人情報等 が漏えいした可能性がある



疑問

ランサムウェアとは?

- ・感染すると端末等に保存されているデータを暗号化して使用できない状態にしたうえで、そのデータを復元する対価として金銭を要求する不正プログラム(マルウェア)
- ・従来は、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だったが、2020年頃から、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る
※「VPN(Virtual Private Network)」は、インターネットなどの共有ネットワークにVPNルータなどを接続することで、仮想的な通信トンネルを構成し、プライベートネットワークを構築すること
- ・最近では、データの暗号化のみならず、データを窃取した上、企業等に対し「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という手口が確認されている

次頁では、日本の医療機関で発生したランサムウェアによる

上記以外の事例をご紹介します。



サイバー攻撃を受けた某病院の状況(～覚知)

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！

看護師がシステム担当者に連絡



いたずらかな…
何にもできないんだけどー!!

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

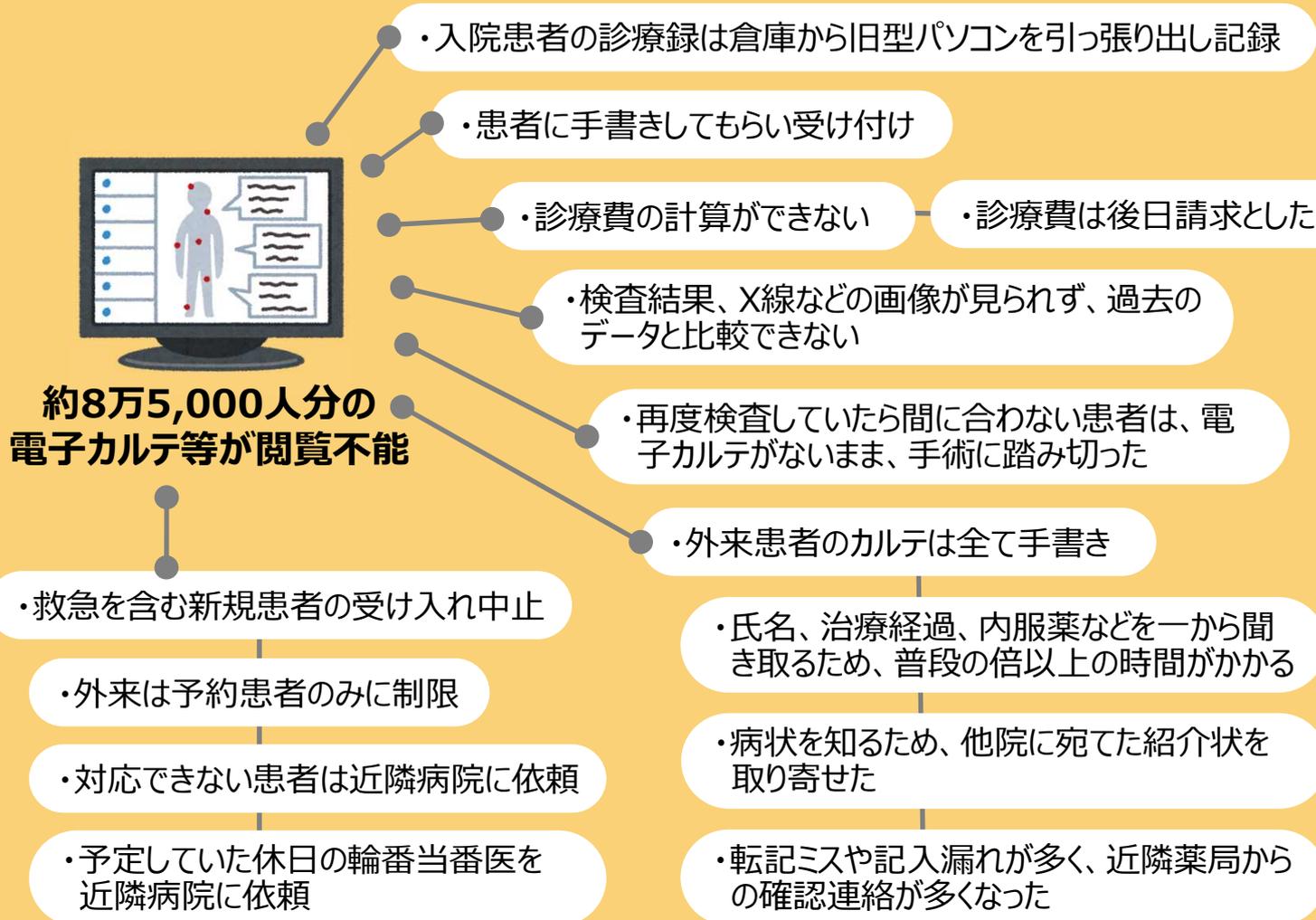
徳島県警に通報

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でつながっていた**
 - 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





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.npa.go.jp/cyber/ransom/index.html>.

・NEC:「VPN構築ルーター VPN構築について」https://www.necplatforms.co.jp/product/vpn_router/vpn/index.html.

© 2021 Sompo Risk Management Inc. All Rights Reserved.





こちらの記事は



みんなで支える医療安全
Medical safety club

に掲載されています

「Medical safety club」は医師賠償責任保険等にご加入の皆様、医療機関のリスクマネジメント活動に資する様々な情報をWebサイトとメールマガジンでご提供するサービスです。

●URL入力

<https://www.sjnk-rm-medical.com/>

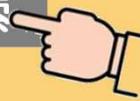
●QRコード



●検索

メディカルセーフティークラブ

検索



専門家によるコラムや判例の解説、
医療安全に取り組む病院などのご紹介

- 専門家コラム
- 判例に学ぶ
- 安全対策事例

医療安全に関する
最新情報

- 回覧用イラストニュース
- 共同通信ニュース



ご利用
無料



ご利用いただくためには、認証コードが必要となります。
詳しい情報は、損保ジャパン「医師賠償責任保険」を
取り扱う代理店などにご確認ください。