先生！狙われてますよ！

サイバー空間の脅威のターゲットは今や企業や官公庁だけではありません。
最近では病院を始めとする医療機関を狙った攻撃が増加しています。

病院の医療システムがランサムウェア被害!!

ランサムウェアとは、金銭を脅し取ることを目的としたマルウェアで、感染するとコンピュータ内のファイルが暗号化され、ファイルの使用が不可能になる上、暗号化の解除などの名目で「身代金」を要求される手口です。

発生要因/手口

①ソフトウェア（VPN等）の脆弱性によりネットワークに不正侵入して感染
②外部公開しているサーバに不正アクセスして感染
③メールの添付ファイルや本文中のURLリンクを開かせて感染

【ランサムウェアにより想定される被害の例】

・電子カルテや画像情報システムが停止、医療業務に支障が出る。
・既往症や服薬歴が不明になることで医療事故のリスクが増大する。
・新患や救急の受け入れ制限により地域医療に深刻な影響を与える。
・病院経営にとっても膨大な経済損失が発生する。

感染リスクを減らすため

①VPN等の周辺機器やソフトウェアは適宜、修正プログラムを適用して脆弱性を残さない。
②パソコンや周辺機器のOS、ウイルス対策ソフトなどは常に最新の状態にアップデートしておく。
③公開サーバのログイン試行回数の制限やパスワードの複雑化など不正アクセス対策を行う。
④不用意にメールの添付ファイルや本文中のURLリンクを開かない。

万が一感染した場合に備えて

①重要なデータは必ずバックアップを取る。
②バックアップを取った媒体は、必ずネットワークから切り離して保管する。
③有事に備えて担当部門(CSIRT)を設置し、対応手順の策定や教育等を行う。

被害に遭った場合は、所在地を管轄する警察署に通報してください

北海道警察サイバーセキュリティ対策本部