特集1
今そこにある危機
放射線診療のBCPを考える
Business Continuity Plan

3. セキュリティベンダーが考える医療機関におけるサイバー攻撃のリスクと対応

松山　征嗣　トレンドマイクロ（株）業種営業推進部

医療機関におけるマルウエア（コンピューターウイルス）感染によるシステム障害は，以前より散見されていたが，この数年に被害報告が相次いでいるランサムウエアは多大な業務影響をもたらす，特に重大な脅威である。病院情報システム・ネットワーク（以下，HIS）とともに，医療機器もネットワークに接続されることが当たり前となった今日，各種システムが業務へ深く浸透している医療機関にとっては，事業リスクとして勘案すべき重要な課題である。

ランサムウエア感染被害事例

2020年12月，福島県立医科大学附属病院より，「コンピュータウイルスが原因と疑われる放射線撮影装置による再撮影事案の発生について」という公表[1]があった。その内容は，2017年にランサムウエア“WannaCry”の亜種に感染したことによるシステム障害が発生，放射線画像の再撮影に至ったセキュリティインシデントである。過去に発生した事案ではあるが，これまで一般に公開されることが少なかった医療機関におけるセキュリティインシデントについて情報共有がなされたことは，大変価値があり，貴重な教訓として学ぶべきものである。

医療機関におけるサイバーリスクと脅威

先の被害事例で述べられていた下記の点を参考として考えてみたい。

・撮影中，読影中に装置が再起動して使用できなかったこと
・放射線画像の再撮影を行ったこと

被ばくの問題は専門外の筆者が論じるべきものではないが，ここで伝えたいことは，医療システム，医療機器がマルウエアの侵害によって正常な動作を阻害されることがあり，その結果として患者に対して悪影響を及ぼす可能性があるということである。仮に，より侵襲度の高い治療装置や検査装置，重篤な患者の生体モニターなどで発生した場合，より大きな事故に発展しかねないということは，リスクとして考慮しておかなければならない。

・撮影画像が保存，参照できなかったこと

撮影画像は電子診療録の一部として，法定保存義務のある情報である。それが参照可能な状態で保存できていないことは，厚生労働省「医療情報システムの安全管理に関するガイドライン」で示される電子保存の三原則（真正性・見読性・保存性）を満たさないことになる。診療報酬請求において，このガイドラインを施設基準としている加算にも影響が出る問題であることを認識しなければならない。1件や2件であれば請求せずに処理するだけですむかもしれないが，マルウエアによって大量のデータが毀損されることによるリスクも考慮しておかなければならない。

また，情報セキュリティ要素としては，診療業務を円滑に行うための可用性，法定記録のための完全性が損なわれたことを示している。医療関係者の多くは個人情報の保護，つまり機密性への意識が強く，それ自体は良いことなのだが，その意識が強すぎるあまり，併せて考慮すべきリスクへの対応が疎かにならないよう，経営層を含めたリスクマネージメントを共有すべき関係者の認識合わせには注意してもらいたい。

医療機関におけるセキュリティの実態

医療系のシステムでは，安定運用の継続を理由にセキュリティ対策をあえて実施しない運用が多く見られる。OSやアプリケーションのセキュリティパッチ適用が，システム障害の要因になることが多いということで，見送られることが多い。そのため，インターネット接続しないことでサイバー脅威によるリスクを回避するという考えに至ったものと思われる。しかし，インターネットにつながらない閉域のネットワークだから安全かというと，必ずしもそうではない。

・業務上の必要性により，データの持ち込みや取り出しを行う際，職員が汚染されたUSBメモリを使用してHIS内システムにマルウエア感染を引き起こした。
・装置の保守業者がオンサイト作業に入る際に，出荷段階ですでにマルウエア感染していた装置を持ち込んだ。

〈0913-8919/21/￥300/ 論文 /JCOPY〉