勤務医部会だより

医療機関へのサイバー攻撃

幹事　**葛谷雅文**
（名鉄病院　院長）

日本の医療機関にも身代金要求型のコンピューターウイルス「ランサムウェア」を使ったサイバー攻撃により、医療業務に多大な影響を与えたのみならず、復旧にも長期間要したとの報道がされているのはご存じのとおりである。現在ほとんどすべての医療機関では電子カルテは言うに及ばず、オーダリングシステム、画像情報、予約システム、医事会計など、ありとあらゆるものがデジタル化されてきている。これにより、効率化が図られているのは有難いのではあるが、これらに対するサイバー攻撃による脆弱性も指摘されているところである。

先般、当院でも万が一そのような攻撃を受けた時、または何らかの要因で院内のデジタルシステムが動かなくなった時のための模擬訓練を実施したが、想像した通り多くの問題があることが判明した。電カルを含む院内のデジタルシステムが稼働しない状態でトリアージを含めどのように外来患者さんに対応するのか、処方内容をどのように確認・発行するのか、検査オーダーはどうするのか、画像はどのように確認するのかなどキリがない。私のようなロートルはむしろ紙カルテ時代のほうが長く経験しているわけだが、若い医師は紙カルテの経験や紙でのオーダリングの経験がない。

サイバーセキュリティ事業を展開しているProofpoint, Inc.とITのセキュリティに関する研究機関であるPonemon Instituteが、最近“Cyber Insecurity in Healthcare：The Cost and Impact on Patient Safety and Care”を報告している*)。それによると医療機関のITおよびITセキュリティ担当者641名（国の明示が無いが、本社や研究所のある米国の可能性が高い）を対象にしたこの調査では、回答した89％が過去12カ月間に平均43回の何らかのサイバー攻撃を経験し、ほぼ毎週１回のペースで攻撃を受けているとのことであった。多いと思われるかもしれないが、この中にはこの下に記載のあるビジネスメール詐欺やフィッシングメールも含まれている。私のようなものでも自分のビジネスメールアドレス宛に一日に山のような怪しいメールが届くことを考えれば納得ができる。具体的には回答した54％の機関が過去２年間に少なくとも一度は「クラウドへの侵入や攻撃」を受けていた。「ランサムウェア」は最も恐れられているサイバー攻撃であり、回答した医療機関の過去２年間の平均ランサムウェア攻撃回数は３回とのことであった。また、過去２年間に50％の機関が少なくとも一度は「Supply chain attacks（取引先や委託先を介した攻撃)」を受けていた。「ビジネスメール攻撃・詐欺／なりすましフィッシング」も過去２年間で51％の回答を寄せた機関で少なくとも一度は受けていた。サイバー攻撃による１回の高額被害の総計平均は440万ドルにもなるとのことであった。

また、最も一般的な上記の４種類のサイバー攻撃に遭った組織の20％以上が、患者の死亡率の上昇など患者の被害に関与していた。このサイバー攻撃による医療への被害の中で最も多いのは医療処置や検査の遅れで、医療従事者の57％が患者の予後不良を、約半数が医療処置による合併症を増加させたと報告している。患者の診療に最も悪影響を及ぼす可能性が高い攻撃の種類はランサムウェアで、64％の組織で医療処置や検査の遅延が発生し、59％の組織で患者の入院期間が遅延するとの報告である。

これらのサイバー攻撃により早急に医療が必要な患者に不利益が及ぶのみならず、日本で報道されているランサムウェアの被害報告を聞いていても復旧にも莫大な費用や時間が費やされることにより、周囲の地域住民の健康にも大きな影響が及ぶことは明らかである。

現在私を含め多くの病院管理者やスタッフが自分たちの医療機関のサイバーセキュリティは万全だと思っている方はおられないだろう。医師を含めた医療者がこのセキュリティに関して十分な知識を会得するのは不可能であり、できるだけの対策を取るにしてもITおよびセキュリティの専門家に多くの部分を依存せざるをえないのが現状である。ただ、この問題は米国の実情を知ると、今後日本の医療機関もサイバー攻撃の標的になるリスクが高まることを考えておかねばならない。

＊）https://www.proofpoint.com/us/cyber-insecurity-in-healthcare