JSRT企画
⑤医療情報班

放射線部門のサイバーセキュリティ対策の勘所
ー情報セキュリティについて考えるー

みやぎ県南中核病院 医療情報管理課　○坂野 隆明(Banno Takaaki)

【はじめに】

病院をはじめとする医療機関では、施設内にネットワークが構築され様々なシステムのインフラとして利用されている。医療機関で情報システムの構築と同時にネットワーク構築が普及した頃インターネット環境のオープンなネットワークとは別のクローズドネットワークとして構築されてきた。また、院内でインターネットが利用できるネットワーク環境も物理または論理的に別のネットワークとして整備され、医療機関内には、医療情報システムで利用するネットワークとインターネットを利用するネットワークと二つのネットワークが存在する。このことが、医療情報システムで利用するネットワークのセキュリティ対策を進める上での阻害要因の一因として「院内ネットワークはクローズドネットワークで外部に接続していないのでセキュリティ対策は不要」と妄信する担当者を生み、サイバーセキュリティ対策に積極的に取り組む施設が少なかった。

このような背景から、他の業種に比較し医療機関ではサイバーセキュリティ対策が脆弱な状態となっている場合があり、コンピュータウイルスの被害は発生している。放射線部門でもランサムウエアに代表されるコンピュータウイルスによる被害報告や報道などで公表され、社会的に関心が高まっている。しかしながら、有効なサイバーセキュリティ対策については、ネットワークの構成、投資できる予算、運用体制など様々な条件から施設ごとに異なるため、明確で絶対的な対策は存在しない。

【サイバーインシデントの現状とその影響】

医療機関がサイバーインデントの被害にあった事例は、報道などで広く知られるようになってきている。近年では、コンピュータウイルスによる標的型攻撃などサイバー犯罪が組織化とビジネス化している。特に、ランサムウエアと呼ばれるコンピュータウイルスによる情報の搾取と暗号化をするものが多く、情報を人質とする身代金が二重に要求される二重脅迫の被害が大きい。一般企業だけなく医療機関でもサイバーインシデントによる経済的損失は大きく、経営に与える影響は想像を超えるのが現状である。医療機関では、被害により医療機能が大きく低下し患者の治療にも影響が発生するため、昨今の被害状況を鑑み管理監督官庁でも令和5年3月に医療法施行規則（医療法施行規則第14条第2項を追加）を改正し、病院や診療所などの医療機関の管理者へサイバーセキュリティ確保のための措置を義務化した。これにより、医療法に基づく医療機関への立ち入り検査項目にその取り組み状況を確認することが盛り込まれた。

【医療法に基づく立入検査】

法令に基づく医療機関への立ち入り検査は、実施主体が医療機関により異なるが、検査時の確認事項を均霑化するためや取組事項として医療機関として優先的に取り組むべき事項を取りまとめチェックリストとして、各医療機関へ通知した。このチェックリスト（サイバーセキュリティ対策チェックリスト）は、厚生労働省により策定されている「医療情報システムの安全管理に関するガイドライン第6.0版」（令和5年5月）をもとに作成されている。チェックリストは、令和5年度中に取り組む事項と令和6年度中に取り組む事項が、医療機関向けと事業者確認用に分けて作成されており、すべての項目内容が期限内に達成できるよう取組むよう促されている。

チェックリストは、大項目として、「1.体制構築」「2.医療情報システムの管理・運用」「3.インシデント発生時に備えた対応」の三つに分かれており、「2.医療情報システムの管理・運用」「3.インシデント発生時に備えた対応」の詳細項目への取り組みが対策の中心となる。「2.医療情報システムの管理・運用」の内容としては、

(1) サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。
(2) リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。
(3) 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。
(4) 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
(5) 退職者や使用していないアカウント等、不要なアカウントを削除している。

(6)アクセスログを管理している。
(7)セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
(8)接続元制限を実施している。
の項目となっている。「3.インシデント発生時に備えた対応」の項目としては、
(1)インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。（令和5年度）
(2)インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。（令和6年度）
(3)サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和6年度中に策定予定である。（令和6年度）
の3項目となっている。

【放射線部門でのサイバーセキュリティ対策】

セキュリティ対策の原則的には、「組織的安全対策」「物理的安全対策」「技術的安全対策」「人的安全対策」からなる四つの視点（Fig.1）で対策を総合的に講じる必要があり、部分的な対応や取組みでは不足となり脆弱な取組み部分から被害が発生するリスクとなる。

Fig.1 セキュリティ対策の四つの視点

放射線部門では、部門システム（RIS）などの情報システムのみならず検査機器や治療機器の医療機器も含めた対策や取組みが必要な点が留意すべき点として挙げられる。部門システムやPACSなどの情報システムと医療機器がネットワークを介して接続し運用しているため、対策も一体的に取り組む必要がある。また、医療機器には医療機器自体の内部でネットワークを構築し一つの装置となっている機器や安定稼働やトラブル対応のためのリモート保守回線（遠隔保守回線）のネットワーク接続など様々なネットワーク形態や構成が存在する。リモート保守回線は、情報システムと医療機器それぞれに存在し、接続方式にも必要時に都度接続する形態や常時接続する形態など様々な方式がある。

リモート保守回線の存在は、医療機関の内部ネットワークが外部とのネットワーク接続があり、冒頭で述べたクローズドネットワークではない状態であることを強く認識することが必要であることが理解できると思われる。

医療情報システムや医療機器のリモート保守回線がどのような接続形態になっているか、また、その接続本数はどのくらいか、など自施設の状況を確認し資料として文書化することが、最初の取組みとして考えられる。これら資料を基にそれぞれのリモート保守回線毎に安全性を確認する作業へと移行する。

ネットワークの状況を把握することは、直接的なネットワーク接続の状況についての取組みであるが、忘れがちなのが、間接的なネットワーク接続としての媒体が存在すことも忘れず対応が必要である。医療機関では、ポータブルメディアを施設内で利用する運用があり、これらポータブルメディアは、院内でのみ利用されていれば良いが、インターネット環境にある機器で利用されている場合には、内部ネットワークと外部ネットワークがポータブルメディア内のファイルや保存領域を経由し接続することになる。これら、間接的な接続点にも留意が必要となる。

【ネットワーク管理の必要性】

サイバーインシデントのもう一つの側面として、自施設のみの対策では不足する状況が顕在化した。リモート保守回線により内部ネットワークと外部ネットワークとの接続点が発生したことで、外部ネットワークの接続元のセキュリティ対策も確認することが必要となっている。これは、サプライチェーンの脆弱性を悪用した攻撃であり、近年増加傾向にある攻撃手法となっている。ランサムウエアによる被害では、内部ネットワークへ侵入が確立できた後は、内部ネットワークの内偵調査を行い、機密情報などの情報資産を収集する。このため、平時より外部ネットワークと内部ネットワークの接続状況の管理が必要であり、管理運用体制も必要となる。

管理運用体制として必要な情報を取りまとめる目的で資料を整備することも必要となるが、主に次にあげる資料を取りまとめる。ネットワーク構成図として、医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したもの。その他にもサーバ構成図、システム機能構成図なども作成する。これら資料は、関係者への説明や状況の把握・理解のために使用されることでその効果が発揮できるものと考えられる。

【まとめ】

放射線部門におけるセキュリティ対策について概要的ではあるが取りまとめて解説した。対策として四つの視点「組織的安全対策」「物理的安全対策」「技術的安全対策」「人的安全対策」で総合的に取り組むことが重要であり、リスクの管理を行う。リスクの管理では、一般的にPDCAサイクルを管理することで進められるが、サイバーセキュリティ対策では、PDCAサイクルとともにOODAループによる対策立案も有効である場合があることに留意する。

また、様々な対策には、投資（予算）が必要であり、被害状況からも医療機関の経営への影響は決して少なくないことから経営層の理解を得ながら取組みを進めることが重要な事項でもある。

様々な取組みを策定することでサイバーセキュリティ対策となるが、サイバーインシデントの被害状況からもわかる通り、セキュリティリスクは多数あり、また、そのリスクも自施設の状況や外部の環境により変化するため継続した取組みがサイバーセキュリティ対策の勘所ではないかと考える。

【参考文献】

1）医療情報システムの安全管理に関するガイドライン第6.0版 厚生労働省 令和5年5月
2）医療機関向けセキュリティ教育支援ポータルサイト https://mhlw-training.saj.or.jp/