Ⅰ　医療AIをめぐる動向

5. AIサービス普及のための情報セキュリティのあり方

宇賀神　敦　医療AIプラットフォーム技術研究組合

医療AIサービスの普及は，医療従事者の働き方改革（2024年問題）や医療・介護の担い手不足（2025年問題）の解決に大きな貢献が期待できる。普及のためには，安全・安心にリーズナブルなコストで利用できるネットワーク環境の提供が不可欠である。本稿では，医療AIプラットフォーム技術研究組合（Healthcare AI Platform Collaborative Innovation Partnership：HAIP）にて取り組んでいる医療機関に向けたクラウド型医療AIサービスやネットワークセキュリティ普及の取り組みについて述べる。

サイバーセキュリティ被害の現状

警察庁によれば，国内の医療・福祉分野におけるランサムウエア被害件数は，2022年20件，2023年10件と，前年比で半減している[1]。感染経路を見ると，VPN機器からの侵入が63%，リモートデスクトップからの侵入が18%であった。医療機関は，クラウドシステムの利用や自宅から院内システムへのアクセスがいまだ限定的であるため，VPN機器からの侵入が主な感染経路ということが推察できる。厚生労働省は，2022年10月31日に発生した大阪急性期・総合医療センターへのサイバー攻撃から10日後に，サイバーセキュリティ対策強化の注意喚起を全医療機関に行ったが，それでも10件の被害があったことから，具体的な対策が進まない体制面，費用面などの根深い課題が内在していると考える。

英国調査会社コンパリテックによると，2023年，米国の医療機関へのサイバー攻撃は147件発生しており，ここ数年深刻な状況が続いている。米国では，電子カルテ導入率が95%を超え，医療機関や薬局などとのデータ連携も日本より進んでいる。日本が国を挙げて推進する医療DX[2]，地域医療DX[3]や医療AIサービスのクラウド化が進むと，米国と同様にサイバー攻撃のさらなる激化が予想される。サイバー攻撃の被害を防ぐためには，医療DXの進展と併せて，各医療機関に最適なサイバーセキュリティ対策や定期的なシステムセキュリティ監査を行うことにより，安全・安心なネットワーク環境が継続的に維持されることで，医療DXを支える必須のインフラに成長していく。

情報処理推進機構が2024年1月に発表した「情報セキュリティ10大脅威2024」[4]によれば，2023年と同様ランサムウエアによる被害（1位），サプライチェーンの弱点を悪用した攻撃（2位）が最大の脅威である。注意すべきは，内部不正による情報漏えい等の被害（3位），不注意による情報漏えい等の被害（6位）が増加していることである。従業員への定期的なセキュリティ・プライバシー教育や定期的なシステム監査による現場のプロセスをチェックすることが肝要である。

医療機関が対応を迫られる変化

政府の政策や医療提供環境の変化の中で，医療機関は下記の対応が必要となる。

1点目は，2024年4月から適用された医師の時間外労働の上限規制による働き方改革であり，医療機関の業務効率化やタスクシフトが求められる中，医療AIサービスの活用が増えていく。

2点目は，団塊の世代800万人がすべて後期高齢者となる2025年問題である。全人口の18%（2180万人）が75歳以上となることで，医療費の増大や人口減少が加速し，医療・介護の担い手不足が深刻化する。また，地域によって今後の人口構成の推移も大きく異なるため，必要とされる医療（高度急性期，急性期，回復期，慢性期）を見越した先手の対応が必要となる。具体的には，オンライン診療や在宅医療への対応，医療機関内外を含めたデータ連携や医療AIサービスによる専門医と非専門医のギャップを埋める対策や院外からの電子カルテへのアクセスが必須となる。医療従事者と医療AIサービスとの協働は，医療従事者の働き方改革や医療の均てん化の実現には欠かせない要素であり，それを支える安全・安心にリーズナブルなコストで利用できるネットワーク環境の提供も不可欠である。

HAIPとは

HAIP[5]は，医療AIサービスの普及に必要な医療AIプラットフォームの研究開発を行うことを目的として，2021年4月1日に厚生労働大臣および経済産業

〈0913-8919/24/￥300/論文/JCOPY〉