特集1
Operation BCPで止めない放射線診療
災害・サイバー攻撃・DX停止リスクに備える実装戦略

V　未来編

AI・DX時代の放射線診療BCP

鳥飼　幸太　群馬大学医学部附属病院システム統合センター

生成AIとDX（デジタルトランスフォーメーション）の技術的・社会的進展に伴い，放射線診療における業務継続計画（BCP）は，装置，電源，PACS，RISの継続性を確保する段階から，知識処理，説明支援，優先順位づけ，問い合わせ応答を含む，情報処理機能の継続性を設計する段階へ移っている。放射線部門は，救急，手術，集中治療，入院診療の画像基盤部門であり，停止の影響は，検査室内にとどまらず，院内の判断速度と診療の順序に及ぶ。本企画における「止めないBCP」は，停止確率の低減に加え，停止後に維持する機能，切り替える機能，人が引き受ける機能を工程ごとに定義する設計として整理する試みであると解釈される。

本稿では，このような観点の下，生成AI・DX時代の放射線部門のBCPについて解説する。

生成AIに関連するBCP

人工知能（AI）依存リスクの対象について検討する（**表1 左**）。放射線診療におけるAI活用として想起されやすいのは画像診断支援であるが，病院業務全体として見た場合，紹介状や前回所見の要約，検査説明文の作成，問い合わせ文への応答，障害時手順の検索，検査プロトコール候補の提示，部門内ナレッジの参照といった，周辺業務での活用の浸透が急速に進んでいる。要配慮個人情報を含まない院内情報では，生成AI技術の利用が容易であることから，画像生成や病変検出と並ぶ情報整理機能が診療の流れに組み込まれている。このため，生成AI関連機能の停止は，画像診断の正答率の比較に加え，受付，患者説明，検査前確認，読影準備，結果伝達の各工程で，必要な職種，所要時間，使用文書，承認経路にわたって，影響範囲の把握と代替手段を準備する必要がある。

サイバー攻撃による生成AIに関連した障害要因の主なものとして，コンタミネーション，乗っ取り，破壊などが挙げられる。コンタミネーションは，学習データ，検索拡張生成（RAG）で参照する文書，テンプレート，辞書，ルール集合に誤情報や不適切な記述が混入し，出力傾向が変化する状態である。乗っ取りは，プロンプトインジェクションや外部文書を通じ，本来予定した目的から外れた応答へ誘導される状態である。破壊は，推論API，認証基盤，GPU資源，ネットワーク接続，モデル配信基盤の停止によって，AIを利用した複数の業務機能が同時に利用不能となる状態である。米国立標準技術研究所（NIST）が作成したチェック項目であるGenerative AI Profileは，生成AIに対して，セキュリティ，プライバシー，情報の真正性，説明責任を含む継続管理を求めている[1]。これを放射線部門での業務に適用した場合，生成AI停止の被害は検査オーダの処理，患者案内，優先順位の決定，前回所見の比較，報告補助などに及ぶことから，AI障害は単なる読影不能としてではなく，放射線検査ワークフロー全体が停滞する状況を想定することが必要である。

重要であるが，あまり議論されない話題として，生成AIに入力が許容される情報ならびにその安全管理があり，AI依存リスクに含める必要がある。厚生労働省の「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Q&A」[2]は，生成AIのプロンプトとして医療情報を入力する場合，「学習等のために保存されないことが契約等で担保される」場合にかぎり利用可能と整理している。また，個人情報保護委員会においては，個人データを含む入力について，提供事業者が機械学習へ利用しないことなどを十分に確認するよう求めている[3]。ここで対象となる情報は，患者属性，検査結果，画像所見に加え，構成図，保守連絡先，障害時の暫定運用，問い合わせ履歴，部門内の注意喚起文も含む。放射線部門で生成AIを利用する際には，患者情報の匿名化に加え，院内運用情報の分類，入力可能な文書種別の定義，ログの保存先，ベンダー保守経路，再利用条件まで含めて管理する必要がある。

加えて，生成AIへ入力した内容は，保存説明の有無のみで安全性を評価しにくい。近年発表されたlanguage model inversionの考察では，モデルの出力確率などから入力列を再構成しうることを示している[4]。これを医療機関の実務に当てはめると，プロンプト本文，システム指示，下書き文，部門内メモ，障害対応記録，RAGで参照した院内文書が，条件次第で再構成可能な情報として残りうることを意味する。したがっ

〈0913-8919/26/￥300/論文/JCOPY〉