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

企画協力：池田 龍二
佐賀大学医学部附属病院放射線部技師長

近年，大規模自然災害や，医療機関を標的としたランサムウエア被害など基幹システム停止事例が顕在化しています。事業継続計画（BCP）は，策定や文書整備にとどまらず，「誰が，いつ，何を判断し，どう動くか」という運用設計が不可欠です。本特集では，さまざまなリスクを体系的に報告し，「備えるBCP」から「止めないBCP」への転換を図るための方策を提示します。

I 総 論

放射線部門BCP：「計画」から「運用設計」への転換

池田 龍二 佐賀大学医学部附属病院放射線部

近年，医療機関を取り巻くリスク環境は劇的に変化している。2024年の能登半島地震に代表される大規模自然災害に加え，ランサムウエアによる電子カルテシステムの暗号化や，基幹ネットワークの障害といったサイバー・システムリスクが顕在化している。これらは単なる局所的なトラブルにとどまらず，病院全体の機能を長期間停止させる脅威となっている。

とりわけ放射線部門は，現代の医療において救急，集中治療，外科手術といった中核機能を支える最重要インフラの一つである。X線撮影，CT，MRI，血管造影といったモダリティが稼働しなければ，重症患者のトリアージも緊急手術の術前評価も不可能となる。災害時において「放射線部門が動くか否か」は，病院が地域医療の砦として機能し続けられるかどうかのカギを握る。したがって，放射線部門の業務継続計画（BCP）は，病院全体の生存戦略と直結するきわめて重要な課題である。

従来型BCPの限界と「オールハザード」への転換

従来のBCP策定において主流であったのは，地震，火災，感染症といったハザード（原因）ごとに個別のマニュアルを作成するアプローチであった。「地震対策マニュアル」「新型インフルエンザ対応計画」といった文書が積み上げられていく一方で，現場では「どの棚のどのファイルを見ればよいかわからない」という事態に陥りやすい。また，想定外の複合災害（例：地震による停電とシステム障害の同時発生など）には対応できないという脆さも露呈している。

こうした課題に対し，近年推奨されているのが「オールハザードアプローチ」である。これは「何が起きたか（原因）」ではなく，「何が失われたか（結果）」に着目する手法である。原因が地震であれサイバー攻撃であれ，放射線部門にとって致命的なのは「電源の喪失」「通信の寸断」「ITシステムの停止」「人員の不足」「医療機器の破損」という5つの重要資源（リソース）の欠乏である（図1）。この考え方に基づけば，対策はシンプルかつ汎用的になる。例えば，「ITシステムが使えない」という状況への対策（紙運用への切り替え，ローカル保存での撮影など）を定めておけば，それがサーバ故障であれサイバー攻撃であれ，あるいは

〈0913-8919/26/￥300/論文/JCOPY〉