特集1
今そこにある危機
放射線診療のBCPを考える
Business Continuity Plan

2. 放射線部門におけるサイバー攻撃対策

原瀬　正敏　豊橋市民病院事務局医療情報課

サイバー攻撃を想定したIT-BCPの策定

医療機関のデジタル化が急速に進み，電子カルテの導入や医療機器のネットワーク化により，大量の患者の個人情報や医療記録などが医療システムで管理されるようになった。放射線部門においては，放射線部門システム（以下，RIS）や医用画像管理システム（以下，PACS）などが導入され，大量のデータを保管するようになってきている。また，以前は，医療システムは医療機関内のクローズドなネットワークであったが，外部のネットワークに接続したシステムを利用する施設も増加してきている。このようなIT化の流れは，業務効率を大きく向上させる一方で，サイバー攻撃を受ける危険性がある。

医療機関において検査・治療の要である放射線部門がサイバー攻撃を受けた場合，重大な被害につながる可能性がある。今後，サイバー攻撃への事前対策は必須であり，攻撃の検知，対応，復旧などをまとめたBCP（business continuity plan：事業継続計画）を策定することが重要となってきている。また，厚生労働省の「医療情報システムに関するガイドライン　第5版」[1]では，サイバー攻撃を想定した事業継続計画（IT-business continuity plan：IT-BCP）が求められている。

災害とサイバー攻撃で想定されるリスクの違い

近年，自然災害，大火災，テロ攻撃などの緊急事態に遭遇した場合において，事業の損害を最小限にとどめつつ，事業の継続あるいは早期復旧を可能とするために，緊急時における事業継続のための方法，手段などを取り決めておく，災害リスクに対するBCPが策定されてきている。厚生労働省が行った「病院の業務継続計画（BCP）策定状況調査の結果」[2]では，すべての災害拠点病院で2019年度にはBCPが策定されているとの調査結果であった。

しかしながら，従来の災害リスクに対するBCPは，電気・ガスなどの社会インフラの供給停止や建物損壊などを前提とした医療システムの損壊や停止などのリスクであり，サイバー攻撃特有のリスクが想定されていないことが考えられる。

医療機関における災害とサイバー攻撃で想定されるリスクの違い（**表1**）は，サイバー攻撃による医療システムの障害のみならず，データの漏えいや改ざんがあり，データの復旧費用や漏えいがあった際には賠償費用が発生する点である。さらに，災害発災時のBCP発動に比べ，攻撃があってからしばらくして気づくケースや外部からの通報で初めて認知するケースなど，BCP発動が遅れてしまう場合があり，被害が拡大してしまうといったリスクも存在する。また，システム復旧においては，サイバー攻撃による被害を受けたシステムやサーバは，バックアップしたデータを単に元に戻すだけではなく，特定した改ざん・漏えいの原因に対処した上で再開することになる。そのため，サイバー攻撃によるIT-BCPの策定では，システム障害発生時の対応に加え，想定されるリスクを最小限に抑えるためのセキュリティ対策を同時に検討する必要がある。

放射線部門におけるサイバー攻撃へのIT-BCPの策定

多くの医療機関において放射線検査機器はデジタル化され，RIS，PACS，検像システム，線量管理システムなど，複数のシステムで構成されている。近年では，外部ネットワークに接続されたクラウドソリューションのPACSなども利用されてきている。このように，放射線部門の医療システムは複雑化していることに加え，各システムで大量のデータを管理するようになってきており，サイバー攻撃によるシステム障害は，業務の遅滞あるいは停止，データ改ざんや漏えいなど，病院運営に大きく影響する可能性がある。そのため，放射線部門におけるサイバー攻撃へのセキュリティ対策は重要であり，IT-BCPを策定する際には次の事項を押さえておく必要がある。

〈0913-8919/21/￥300/ 論文 /JCOPY〉