Ⅲ　IT-BCP・サイバーBCP

2. ランサムウエア感染時の初動対応と運用設計の要諦

倉橋　達人　市立東大阪医療センター医療技術局

「それは，午前4時50分の病院からの一本の電話から始まった」

異変の予兆は，その2時間前にさかのぼる。2021年5月31日，午前3時。静寂に包まれた市立東大阪医療センターのMRI室で，それは起きた。PACSが沈黙したのだ。他院から搬送された患者のCT画像を取り込んだ際，電子カルテ上では情報が見えているにもかかわらず，PACSには一切の画像が表示されない。MRIやCTによる検査自体は実行可能であったものの，PACSへの画像送信および全院的な閲覧が完全に停止していた。「ただの故障ではない」。当直者は直感的な不安を抱えながら，保守ベンダー（A社）への第一報を入れた。だが，事態は「システムエラー」などという生易しい範疇（はんちゅう）を超えていた。A社エンジニアによるリモート接続が拒絶され，現地へ急行したエンジニアが目の当たりにしたのは，制御不能に陥ったシステムの姿だった。

午前4時50分，筆者の携帯が鳴った。受話器越しに響く当直者の声は，未知の事態に対する強い不安と戸惑いに震えていた。

「PACSがダウンしました。画像もレポートも見られません。普段の異常，トラブルとは……何かが違うんです」

ただならぬ気配を感じ，「進捗があれば即刻報告を」と告げ電話を切った。少しして出勤の準備を始めたその時だった。午前5時58分，決定的な一報が入った。

「ウイルス感染のようです」

その報告を受けた瞬間，戦慄が走った。脳裏をよぎったのは，同年の5月7日に発生した米国パイプライン施設へのサイバー攻撃である。これは単なるウイルストラブルではない。医療機関の心臓部をねらったランサムウエア攻撃であり，対応を一歩誤れば電子カルテを含む全病院機能が破壊される。「現在電源がオフになっている電子カルテ端末，および画像診断装置は絶対に起動させるな!!」という厳命を下し，関係者の緊急招集をかけた。

本稿は，この緊迫した初動対応の経験を紐解き，従来の形式的な業務継続計画（BCP）から，サイバー攻撃を前提とした実戦的な「止めないBCP」への転換を図るための方策を，当時の状況と最新のガイドラインを交えて論じるものである。

サイバー攻撃の検知と初動対応のタイムライン

初動対応において最優先されるべきは，正確な事象の把握と，被害拡大を阻止するための物理的なネットワーク遮断である。市立東大阪医療センターにおける初動対応は，きわめて限られた情報の中で，システムを物理的に切り離し，影響範囲を特定することから始まった。

後に判明した事実だが，攻撃者は3日前に脆弱性が放置されていた遠隔読影用ルータから侵入し，PACSサーバ群に壊滅的な被害を与えていた。しかし，不幸中の幸いか，紹介情報管理システムが電子カルテ側のネットワークに接続されていたことが，その後の診療継続において決定的な救いとなった。

午前7時10分，事務局情報管理課，放射線科部長，そして，医療情報技師の認定を持つ診療放射線技師らが緊急協議を実施した。調査の結果，PACS機能は全滅しているものの，電子カルテシステムおよびCT，MRIなどのモダリティ自体は稼働可能であることが確認された。この迅速な状況把握が，「どの機能を生かし，どの機能を止めるか」というトリアージ決断を可能にした。

表1に，障害発生から代替運用確立までの時系列と判断ポイントを示す。このタイムラインにおいて特筆すべき教訓は，午前9時30分に発生した施設管理部門とのやり取りである。当時，筆者は自院のCT装置が密かに感染している

〈0913-8919/26/￥300/論文/JCOPY〉