Ⅲ　IT-BCP・サイバーBCP

3. 医用画像バックアップによるBCP対策

伊藤　孝　(株)インフィニットジャパン ソリューション事業部

医用画像は診断・治療を支える基盤情報であり，その保存性や可用性は，医療提供体制の継続に直結する。近年は，地震や豪雨などの自然災害，機器故障やシステム障害，さらにはランサムウエアをはじめとするサイバー攻撃など，医療機関を取り巻くリスクがいっそう多様化している。こうした状況の中で重要なのは，医用画像を単に保管することではなく，非常時にも必要な医用画像へ安全かつ迅速にアクセスできる環境を整えておくことである。

医用画像の業務継続計画（BCP）対策は，いまや情報システム部門だけの課題ではなく，病院経営や地域医療の継続性を支える重要テーマと言える。非常時への対策をしながら，平常時の運用性や管理性も損なわないことが重要である。そこで本稿では，医用画像のBCP対策において求められるポイントを整理しながら，その具体策の一つとして当社製品を紹介する。

バックアップのルール

医用画像のバックアップでは「3-2-1-0ルール」が推奨されている。これは，従来の「3-2-1ルール」に，「0＝復元エラーをゼロにする」という考え方を加えたものである。この「0」が重要とされる理由は，例えば，バックアップファイル自体が存在していても，そのファイルが破損していたり，暗号化されていたり，あるいは復元手順が事前に検証されていなかったりすると，障害発生時に実際には利用できないためである。つまり，バックアップは，「存在すること」だけではなく，「確実に復旧できること」まで確認されて初めて意味を持つ。さらに，近年では，増加するランサムウエアの対策として，オブジェクトロック機能などを活用した「3-2-1-1-0ルール」として説明されることもある。これは，「3-2-1-0ルール」に加えて，「1つの不変（イミュータブル）なコピーを保持する」という考え方を取り入れたものである（表1）。

バックアップの考え方

バックアップの方法を検討する際には，施設の環境などを考慮して，何を重視してバックアップするかを検討する必要がある。どれだけ手作業の部分があるか，どれだけ短時間でシステム復旧できる計画を立てるか，どれだけコストをかけるか，などが主なポイントになる。

加えて，実際に復元できるかを定期的に検証し，非常時に医用画像閲覧までの手順と，閲覧可能になるまでの必要時間を含めてバックアップ方法を検討することが求められる。

多くのシステムでは，メインストレージに障害が発生した場合，複数HDDでRAID構成を構築しているため，メインストレージ内で復元することができる。また，バックアップストレージも同様の構成がされていれば，一般的なハードウエア障害についてはBCP対策用である3つ目のバックアップを利用することはない。しかし，ランサムウエアなどの災害を含めたBCP対策となると，3つ目のバックアップをどのような形式で保存しているかが重要となる。加えて，日本の病院経営は非常に厳しい状況で，赤字となる施設が6割以上と報告されている[1)]。そのため，コストを重視して3つ

表1　3-2-1-1-0ルールの意味

要　素	意　味	詳細【具体例】
3	データを3つ持つ	本番データ＋バックアップ2世代
2	2種類の保存先に置く	オンプレミスストレージ＋クラウド or LTOテープ
1	1つは遠隔地（別拠点）に保管	別病院拠点，データセンター，クラウドリージョン
1	1つは不変なコピーを持つ	オブジェクトロック機能の活用
0	復元エラーを0にする	定期的なリストア試験，整合性確認，起動確認

〈0913-8919/26/￥300/論文/JCOPY〉