Canon

Solution REPORT
ソリューションレポート

導入事例 つるぎ町立半田病院

リストア先を選ばないバックアップシステム「Barracuda Backup」が、非常時の臨機応変な業務継続を支援

ランサムウェア被害に遭遇し、一時は診療停止に追い込まれたつるぎ町立半田病院。各所の協力や職員の努力で2ヶ月後に診療再開。困難な対応を迫られる中でも、未曾有の体験を通じて多くの学びがあった。同院はそれらの教訓を生かし、「危機管理に本当に必要なことは何なのか？」を見据えた上で、BCP対策強化に貢献する柔軟で堅固なデータバックアップ体制をBarracuda Backup（バラクーダバックアップ　以下Barracuda）を利用して整えた。

課題

- サイバー攻撃などの影響を受けにくい堅牢なバックアップ環境を作りたい
- 非常時でも必要最低限の診療体制を維持するための臨機応変なバックアップ体制を構築したい
- 復旧後の正常診療への移行作業も考慮した非常時の診療体制を整えたい

効果

- Barracuda導入によりファイル単位で臨機応変にリストアできるバックアップ体制を構築
- 臨機応変なバックアップ体制により、非常時の診療情報を入力できるシステムが稼働可能になり、正常稼働への移行作業負荷が軽減した
- 独自OSでファイルを細分化して暗号化するため、バックアップデータのウイルス感染リスクが無くなった

＜お客さまプロファイル＞

旧半田町立半田病院を経て、2005年の市町村合併によりつるぎ町立半田病院となる。開業当時の外科に内科や産婦人科、小児科、整形外科などを加えて、総合病院として地域医療の拡充に貢献。徳島県西部医療圏では唯一「お産」ができる産婦人科として、地域外から訪れる患者も多い。また、地域医療の要として、県西部医療圏における中核病院の役割も担っている。

https://www.handa-hospital.jp/

お話を伺った方

写真左から、丸笹さま、山本さま

つるぎ町立半田病院
事務長
丸笹　寿也 さま

システム管理課　課長
山本　高也 さま

半田病院さまのランサムウェア被害の経緯※1

2021年10月31日未明、院内の複数のプリンターから一斉に犯行声明を印刷し始めたことから事態が発覚。ランサムウェアに感染し、電子カルテを含むサーバーのデータが暗号化されたことで、使用できない状態となった。感染確認後、ネットワーク遮断や端末を停止するなどの処置を実施。救急や新規患者の受け入れを中止するとともに、手術も可能な限り延期するなど、病院としての機能を事実上停止する状態に陥った。事態発生後は、病院としての機能をできるだけ早く取り戻すため、患者データの復元や端末の利用再開に焦点を当てて対応。フォレンジック※2を請け負った企業が、データが確認できる範囲でのデータ復元に成功。さらに、端末の初期化やシステムおよびネットワークの見直しにより、翌2022年1月4日に通常診療を再開した。

導入前の課題と背景

ランサムウェア被害で2ヶ月間診療停止状態に

今回のランサムウェア被害ではかなりご苦労されたとお聞きしましたが。

「とにかく最初は『何が起こっているのか分からない』という状態で、通常診療再開までの2ヶ月は文字通り地獄のような体験でした。当時は各所でまだしっかりとした体制が整っていなかったこともあり、専門機関や国・自治体などからの効果的な支援をすぐには受けることができず、手探り状態で進めていたのが実状です。とにかく復旧の見込みが全く立たず、先の見えない不安で一杯でしたが、当初からマスコミ対応を含めあらゆる情報を公開していたことで、各所から助言や支援の申し出をいただけるようになり、徐々に良い方向に動き始めました」（丸笹さま）

今回の事案の対応では主にどのようなことがポイントになりましたか。

「まず、早急に災害モードに切り替えたこと。発生当日の朝の時点で迅速な復旧は不可能だと判断し、災害モードに切り替えたことが大きなポイントだったと考えています。さらに、つるぎ町長をはじめ、警察や支援を申し出いただいたSoftware ISAC※3などと相談。さまざまなアドバイスをいただきながら対応できたことも好材料でした。そして何より、職員が一致団結して協力してくれたことが大きな糧となりました。1人も脱落者を出すことなく2ヶ月対応してきました」（丸笹さま）

導入の必然性

臨機応変なリストアやファイル暗号化など、柔軟性と堅牢性を兼ね備えたBarracuda Backupを採択

今回どのような背景がありデータバックアップ体制を強化しようと考えられたのでしょうか。

「サイバー攻撃や災害などによって電子カルテが使用できなくなった場合、紙カルテによって診療を継続する方法が考えられます。しかし、電子カルテ情報が無ければ来院理由や患者さんの年齢すら分かりませんので、診察時に改めて一からお聞きする必要があります。当然平常時よりも対応可能な患者数が減ります。さらに、復旧後は電子カルテでの運用に戻す際に紙カルテの内容を改めて入力する必要がありますが、入力には膨大な工数が必要となり、あまり現実的とは言えません」（丸笹さま）

「電子カルテの情報以外にも、薬剤情報や新型コロナのワクチン接種の情報内に患者さんの情報があります。これらの情報をうまく紐づけることができれば、一から情報をお聞きする必要がなくなります。仮に電子カルテシステムが停止しても、それらのデータを参照しながら診療を続けることができるような簡易システムを構築しようとしています。また、電子カルテ停止中の診察データを一時的に入力・保存しておけるシステムを構築しておけば、復旧後のデータ入力が不要になりますので、スムーズに正常診療へ移行することができます。これらを非常時に稼働させるためには、そのような仕組みに対応したバックアップシステムが必要でした」（山本さま）

どのような経緯や理由で「Barracuda」をご採択いただいたのでしょうか。

「以前から当院のICT面のさまざまなサポートをいただいている四国チエルクリエイトさんから、Barracudaとキヤノンマーケティングジャパンさんをご紹介いただいたのがきっかけです。四国チエルクリエイトさんが、当院が持つ課題解決にBarracudaが最適だと判断して紹介いただかなければ今回の導入はありませんでした」（丸笹さま）

「先ほどの簡易システムを稼働させるためには、非常時において最小限のシステム環境を準備する必要があります。そのためには、バックアップデータを臨機応変かつ早急にリストアして使用できるようでなければなりません。Barracudaは一般的なバックアップシステムとは違いファイル単位でバックアップができ、なおかつバックアップ前と同一環境でなくても臨機応変にリストアできます。このため、必要な最低限の端末やネットワークなどさえ用意すれば簡易的なシステムが稼働できます。また、『今必要なデータだけ』をリストアできるので、従来のように何時間もかけてリストアする必要もありません。さらに、独自OSを使用しファイルを細分化して暗号化するため、バックアップデータがウイルス感染することがありませんので、仮に院内がウイルス感染してもバックアップデータは影響を受けません」（山本さま）

Barracudaの特徴

取り組みの成果

BarracudaによるBCP対策が非常時の地域医療体制を強化

本日Barracudaの導入作業が完了したとお聞きしましたが。

「はい、導入作業は特に問題なく完了し、すでにバックアップシステムとして稼働を開始しています。電子カルテデータは専用のバックアップシステムが必要となるため、Barracudaによるバックアップの対象外。今回Barracudaでバックアップする対象は、先ほど申し上げた電子カルテデータ以外のさまざまな医療データが対象です。それらをBarracudaでバックアップしておくことで、もしもの時に簡易的なシステムを速やかに立ち上げ、最低限必要な医療体制を維持できるようになります」（山本さま）

「ランサムウェアの攻撃にあって一番困ったことは、リストア先のサーバーやPCが感染しているため、たとえバックアップデータが生きていたとしても、それをリストアして使うことができなかったこと。当院は災害拠点病院でもあり、Barracudaによってリストア先が柔軟に選択できるようになったことは、BCPの観点からも非常時の地域医療確保に非常に有効な手段だと考えます」（丸笹さま）

今後のBarracudaの利活用や貴院のセキュリティ対策に対する取り組みについて教えてください。

「現在レントゲンなどの院内の画像ファイルはPACS（医療画像管理システム）で管理していますが、容量が4テラバイトを超えてしまいバックアップもリストアも非常に時間がかかります。これをBarracudaでバックアップすることができれば、システム更新時に画像閲覧できない時間を短縮でき、非常時にレントゲン画像を参照することが可能になりますので、検討したいと考えています」（山本さま）

「当院としては今後セキュリティポリシーを整理、拡充させることで、院内の運用はもちろん、外部のベンダーとの責任の明確化などを進めていくことが必要だと考えています。また、電子カルテの運用は、現代の病院にとっては経営を左右する最重要事項です。当院が被ったランサムウェア被害の教訓を交えて、『電子カルテを適切に運用できる管理者の育成が必須である』という意識をあらゆる病院経営者に持っていただければ嬉しいです」（丸笹さま）

※1『徳島県つるぎ町立半田病院　コンピュータウイルス感染事案　有識者会議調査報告書』から抜粋

※2 セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取り組み

※3 一般社団法人ソフトウェア協会の略称

パートナー企業紹介

四国チエルクリエイト株式会社

情報通信機器やオフィス用品、教育ICT機材などの分野のプロフェッショナルとして、四国地域の企業や教育機関の課題解決に貢献。地域創生に寄与することで「地元に愛される100年企業を創る」ことを目指している。2023年7月、株式会社南海MJEから現社名へ社名変更した。

https://shikoku-chieru-c.jp/

お問い合わせ先

Canon キヤノンマーケティングジャパン株式会社

〒108-8011　東京都港区港南 2-16-6 CANON S TOWER

canon.jp/business/case