信州大学医学部附属病院

長野県民の「医療の最後の砦」として迅速なデータ復旧が実現できるRubrikを採用

41億円
ランサムウェア攻撃による想定被害額

120TB
バックアップしているデータのサイズ

5クリック
データ復旧に必要な操作の回数

課題

- 閉域網だけでは防ぎ切れない攻撃への対応
- サイバーセキュリティ対策の予算不足
- 「医療の最後の砦」としてサービスを継続すること

ソリューション

- 確実かつ迅速にデータを復旧できる環境の構築
- 「RRT（専門チーム）」による無償のデータ復旧サービス
- 医療業務を止めないための徹底的な支援

効果

- シンプルな操作でスピーディなデータ復旧が実現
- 仮に攻撃を受けた場合の41億円の被害抑止
- 自前でデータ復旧できるので、迅速かつ柔軟な対応が可能に

1945年に開院し、80年の歴史を持つ信州大学医学部附属病院（以下、信大病院）。717床の病床、34の診療科、31のセンター／部門を擁する長野県内最大規模の総合病院です（2025年4月時点）。大学病院として、高度な医療技術の開発、導入、評価を行っており、次世代を担う医学生の教育や、県内の研修医を育成する中心的な拠点として機能しています。

また、信大病院は県内唯一の「特定機能病院」にも認定されています。特定機能病院とは、他の病院または診療所から紹介された患者に対し、医療を提供する病院のこと。そのため、他の病院や診療所では対応が困難な患者が来院するケースも多く、長野県の「医療の最後の砦」としての役割を果たしています。

信州大学 SHINSHU UNIVERSITY | 医学部附属病院

組織名
信州大学医学部附属病院

URL
https://wwwhp.md.shinshu-u.ac.jp/

業界
医療機関

従業員数
2,045名
※2024年5月1日現在

rubrik

医療機器を経由して攻撃される可能性や対策に十分な費用がかけられないことを懸念

長野県の「医療の最後の砦」である信大病院にとって、患者の電子カルテなどをサイバー攻撃から守り、医療サービスを止めない取り組みは極めて重要です。

「医療サービスが提供できなければ、大切な県民の命を守れなくなる恐れがあります」と語るのは、信大病院 医療情報部 部長の北口良晃氏です。

そのため信大病院は、診療のために欠かせない電子カルテなどのデータを災害やサイバー攻撃から守るため、早くからサイバーセキュリティ対策を講じてきました。2009年ごろには、院内におけるシステム間のデータのやり取りには閉域網だけを使用し、ネットワークには接続しないようにする環境を構築しました。

しかし、医療現場で使用される医療機器はネットワークに接続して使用するものが多く、それらを経由してシステムに侵入される危険があります。また、運営予算が限られ、サイバーセキュリティ対策に十分な費用をかけられないことも課題でした。

> **運営予算が限られている中で、いかに導入コストを抑えながら、有効なサイバーセキュリティ対策を講じられるかが大きな課題となっていました。Rubrikは、そんな課題に応えてくれるソリューションでした。**

信州大学医学部附属病院 医療情報部 部長 北口 良晃氏

元のデータを100%復旧してすぐに利用できるRubrikは理想的なソリューションだと評価

どうすれば、導入コストを抑えながら、有効なサイバーセキュリティ対策ができるのか？　その答えとして、信大病院が選んだのがRubrikでした。

Rubrikは、企業や団体等がデータ保護のために保存するバックアップデータを確実に守り、迅速に復旧できるソリューションです。仮にシステム本体のデータがサイバー攻撃を受けて使えなくなっても、すぐさま最新のバックアップデータが利用可能となります。業務が元通りに継続できるのが大きな特徴で、患者に医療サービスを提供し続けることが最も重要な使命である信大病院にとっては、非常に頼もしいソリューションでした。

じつは信大病院は、Rubrikを導入する以前から、複数のデータバックアップ手段を活用していました。しかし、「いずれも災害時の復旧だけを想定したものなので、サイバー攻撃によってアクセス権限が奪われた場合、バックアップしたデータまで使えなくなることが懸念されました。その点、サイバー攻撃にさらされても、元のデータを100%復旧してすぐに利用できるRubrikは理想的なソリューションであり、追加導入するに足る価値を持っていると判断したのです」と語るのは、信大病院 経営推進課 医療情報戦略室 室長の白木康浩氏です。

専門チームがデータ復旧を支援してくれることも Rubrikを選んだ大きな決め手に

信大病院がRubrikを採用したのには、他にも大きな理由があります。

Rubrikは、ユーザー企業や団体がランサムウェア攻撃を受けた場合、専任のインシデントマネージャーを任命し、「ランサムウェア・レスポンス・チーム（RRT）」という専門チームを編成してデータ復旧を支援するサービスを提供しています。このサービスが無償で利用できるということも、選定の大きな決め手になりました。

「サイバーセキュリティ対策の予算が限られている医療機関にとって、専門家集団による対策チームが無償で支援してくれるというのは非常にありがたいことです。我々は病院の情報システムの管理運用を担う立場ですが、サイバーセキュリティやネットワークに関する深い知識や経験を持っているわけではないので、何かあっても経験豊富なプロに支援してもらえる。しかも、無償で提供してもらえるというのは、大きな安心感につながっています」と白木氏は語ります。

バックアップソリューションは他にもありますが、白木氏は「『Rubrikは、サイバー攻撃を受けたお客様を絶対に見捨てません』と言っていただいたことが、強く印象に残っています」と振り返ります。顧客にしっかりと寄り添い、業務を止めないために徹底支援するというRubrikの姿勢も、導入を決定づける大きな要因となったようです。

信大病院は、サイバーセキュリティ対策に大きく3つの柱を掲げて取り組んでいます。1つ目は、攻撃されないための「予防」。2つ目は、万が一、攻撃を受けた場合の「被害の最小化」。そして3つ目は、喪失したり、アクセス権限を奪われたりしたデータの「迅速な復旧」です。

「中でもデータの『迅速な復旧』は、一刻でも早く医療サービスを再開するために重要な柱です。それを担保してくれるRubrikは、まさに当院が求めるソリューションでした」と北口氏は評価します。

> 無償でデータ復旧支援を行ってくれることも、Rubrikを選んだ決め手でした。『お客様を絶対に見捨てません』と言っていただいたことが、強く印象に残っています。

信州大学医学部附属病院
経営推進課
医療情報戦略室
室長
白木 康浩氏

“

**仮に信大病院が攻撃を受け、システムが2カ月間停止した場合、
被害額は約41億円に上ると試算されています。
そうした被害を食い止めるためにも、Rubrikを導入して正解だったと思います**

信州大学医学部附属病院 医療情報部 部長 北口 良晃氏

バックアップしたデータをスピーディに復旧
操作がシンプルで、使い勝手も良い

こうして信大病院は24年Rubrikを導入。同年3月に本稼働させました。現在、Rubrikを使って、院内に設置したサーバにおよそ120TB（テラバイト）のデータをバックアップしています。「いまのところオンプレミス環境だけでバックアップデータを保護していますが、将来的にRubrikを使って遠隔でバックアップすることも視野に入れています」と白木氏は語ります。

実際に使ってみて、信大病院はRubrikの良さを改めて実感しているようです。

「導入後、何度かリストア試験を行ってみましたが、バックアップしたデータの復旧が非常にスピーディに行われること。しかも、操作が非常にシンプルで、5クリック程度で完了することに使い勝手の良さを感じました」と語るのは、信大病院 経営推進課 医療情報戦略室 診療情報管理士の渡邊寿史氏です。

信大病院ではこれまで、データバックアップや復旧作業の一部を外部ベンダに委託していましたが、Rubrikなら自前での管理が可能なので、万が一のときにも柔軟かつ迅速な対応ができるようになるのではないかと期待しています。

最後に北口氏は、今後のサイバーセキュリティ対策について、「患者さんの命を守るため、サイバー攻撃を受けてもすぐに医療サービスを復旧できる態勢づくりを、より強固にしていきたい。そのためにもRubrikを主軸に置いた形で病院全体のバックアップシステムを検討し、迅速なデータ復旧が実現できる環境を整えていきたいと思います」と語りました。

“

導入前は使い方に関する勉強会を行うことも考えていましたが、その必要すらないほどRubrikの操作は簡単でした。サイバーセキュリティに関する知識や経験がない新人でも、すぐに使いこなせるのではないかと思います。

信州大学医学部附属病院
経営推進課
医療情報戦略室
診療情報管理士
渡邊 寿史氏

rubrik

Rubrik Japan株式会社
https://www.rubrik.com/ja

ご質問・お問い合わせ
https://www.rubrik.com/ja/contact-sales

サイバーセキュリティ企業であるRubrikは、世界のデータを安全に保護することをミッションとしており、The Zero Trust Data Security™の先駆者として、企業がサイバー攻撃、悪意のあるインサイダー、および業務の中断に対するビジネスの回復力を達成できるよう支援します。機械学習を活用したRubrik Security Cloudは、オンプレミス、クラウド、およびSaaSアプリケーション全体のデータを安全に保護します。またRubrikは、データの安全性を維持し、厳しい条件下でのデータの可用性を実現するとともに、データのリスクと脅威を継続的に監視し、インフラストラクチャが攻撃された場合でもデータと共にビジネスの復旧を支援します。

20251010_v1