

Nutanix上で稼働する基幹システムなどの データバックアップ環境をRubrikで刷新 運用工数を3分の1に削減するとともに ランサムウェア対策の高度な基盤を確立

RYOKI

菱機工業株式会社

業界：建設業

導入前の課題：

- ランサムウェアに代表されるサイバー攻撃への対策の強化
- 複雑化、属人化したデータバックアップ環境の改善
- リストア対応を含めたバックアップ運用プランの策定と工数削減

導入効果：

- バックアップ運用に関わる工数を従来の3分の1に削減
- ランサムウェアの迅速な検知、復旧が可能な基盤の構築
- Nutanixとの親和性も高く、運用が容易なバックアップ環境の構築

ITトランスフォーメーションの

成果：

バックアップ運用の効率化、ランサムウェア対策の強化に向けて既存のデータバックアップ環境をRubrikで刷新。一元的な管理画面、優れた操作性によって従来の工数を3分の1に削減すると同時に、イミュータブル・ファイルシステムによってバックアップデータの安全性を確保。さらにRansomware Investigationによってランサムウェアの迅速な検知が可能となり、セキュアで信頼性の高いバックアップ環境が実現。

1954年に石川県金沢市で冷凍機販売及び冷暖房設備の設計・施工の専門事業者として創業し、現在は空気調和設備、給排水衛生設備、消防設備、さらに太陽光発電をはじめとする再生可能エネルギー事業など幅広い事業を展開する菱機工業株式会社。早期にHCI（ハイパーコンバージド・インフラストラクチャ）を導入するなど積極的なIT投資を続ける同社では、IT担当者の運用負荷やセキュリティ面で課題を抱えていたデータバックアップ環境をRubrikで刷新。従来の運用工数を3分の1に削減すると同時に、ランサムウェア対策の高度な基盤を構築しました。

バックアップ運用の負荷軽減とデータセキュリティの強化が急務に

「エンジニアリングを通じてお客様の課題を解決し、最適なビジネス環境を提供する」というミッションを掲げ、設備の提供にとどまらず、その先の課題解決に大きな力を注ぐ菱機工業。省エネルギー空調管理システム「RiCS」をはじめ、古くからIT活用を積極的に展開するなど、行政、医療、製造など、幅広い業界から高く評価されています。さらなる事業の成長に向けてIT活用に取り組む同社ですが、一方で継続的な課題となっていたのがNutanix上で稼働する基幹システムなど、肥大化し複雑になっていたデータバックアップでした。経営企画部 システム企画課の小川弘幹氏は次のように話します。

「約10年前までは基幹システム、グループウェアのデータが中心で容量も数百GB程度だった当社のバックアップ対象は、この数年でNutanix上の基幹システム、グループウェアのみならず、多数のアプリケーションサーバやWindowsのファイルサーバなどを含めると、総容量は数十TBにまで拡大しています。こうした中、ランサムウェア攻撃が企業にもたらす被害が大きく報じられるようになったことから、オンライン上のバックアップデータが攻撃を受けた場合のリスクに備えて、当社ではバックアップデータのオフライン保存も行っていました」

しかし、この運用はハードディスクを使ったもので、容量の問題から対象は基幹システムに限られ、データの定期的なリストア試験などはIT担当者にとって非常に負荷の高いものでした。また、同社ではバックアップ運用の属人化も早期の解決が求められる課題だったと話すのは、取締役 執行役員 経営企画部長の北川裕章氏です。

「長期にわたって増強を繰り返してきたことでバックアップの仕組みが複雑化し、データの構造を理解している社員がわずかであることは大きな課題でした。これを解消するためには、もはやバックアップの仕組みそのものの刷新が急務だと考えました」新たなバックアップの仕組みを検討する中で、候補として浮上したのがRubrik製品です。独自のイミュータブル・ファイルシステムによってデータの改ざんができないRubrikであれば、オフラインでの対応は不要になります。またNutanixとの親和性、さらにランサムウェアの迅速な検知を行うRansomware InvestigationなどのSaaSサービスが充実していることも評価ポイントとなりました。こうして同社はRubrikの導入を正式に決定し、2022年10月にライセンスを購入。あとは導入を待つばかりとなりました。

ランサムウェアの被害からの復旧を通じて データセキュリティの重要性を再認識

しかし、その直後の2022年11月17日に予期せぬ事態が発生します。入社したばかりの小川氏のもとに、複数の部署から「ファイルを開くことができない」という連絡が入りました。各所のプリンターからは脅迫文が出力され、すぐに共有フォルダを確認したところ、ランサムウェア「LockBit」の攻撃を受けたことが判明しました。

この事態を受けて、菱機工業は速やかに個人情報保護委員会などの関係機関と連絡をとるとともに、状況を把握するために社内関係者との協議を開始しました。

「これは数日で解決する問題ではないと覚悟を決め、各協力会社様にご迷惑をおかけすることのないよう、少なくとも基幹システム上の支払データだけは翌日までに復旧しようと考えました」(小川氏)

幸いにも同社の場合、基幹システムのバックアップデータは被害を免れており、また定期的なリストア試験も実施していたため、被害を受けた当日のうちに直近の支払いデータの生成を完了することができました。

「事業が完全に停止するという最悪の事態は回避できたものの、この被害によってランサムウェアの脅威を身をもって知ると同時に、データセキュリティの重要性をあらためて認識することとなりました」(北川氏)

一元的な管理画面でバックアップの状況を可視化 運用工数は従来の3分の1に大幅削減

ランサムウェアの被害からの復旧のめどが立った12月下旬、菱機工業ではまず金沢本社でRubrikの導入に着手しました。

「Rubrikから初歩的なアドバイスをいただいた後、各システムのバックアップ設定はわずか数ステップで完了しました。こんなにシンプルな操作でバックアップがとれるのかと驚いたくらいです」(小川氏)

金沢本社での導入が無事に完了したことで、同社は基幹システムのデータを本番環境に戻すにあたって、Rubrikを使って新たにバックアップを行い、データの安全性を確保してから実運用を開始する対応を行いました。今後は2023年3月に新潟支店への導入を行い、これですべての拠点でRubrikを使用できる環境が整備される予定となっています。

実運用がスタートしてからまだ間もない状況ですが、すでにRubrikは明確な成果を生み出しています。北川氏はRubrikによるバックアップ運用の効率性について、「すべてのシステムのバックアップ状況が1つの画面で可視化されたことで、運用工数は以前と比べて3分の1程度に削減されています」と強調します。



菱機工業株式会社
取締役 執行役員
経営企画部長
北川 裕章 氏



菱機工業株式会社
経営企画部
システム企画課
小川 弘幹 氏

Ransomware Investigationについても、小川氏は「実際にランサムウェアが検知される状況は発生していませんが、何か問題があったときはアラートによって瞬時に状況を把握できるため、新たな管理負荷が生じることもなく、安定した運用を続けることができている」と評価します。

属人的なバックアップ運用が解消され データ資産管理の最適化にも大きな期待

Rubrikの導入が決定した直後にランサムウェアの被害に見舞われるなど、さまざまな困難に直面した菱機工業ですが、一貫したポリシーに基づく経営判断によって、事業の社会的信頼を支える強固なセキュリティ基盤を構築することができました。

今後の展望について、小川氏は「ソフトウェア・デファインドな製品であるRubrikによって、今後も新たな機能が継続的にリリースされる点は心強いです。またインスタント・リカバリなどの機能を、可用性を維持するための手段として活用できるのではないかと考えています」と期待を寄せます。

また北川氏も、Rubrikの導入によってバックアップ運用の属人化が解消された点を高く評価します。

「以前の複雑なバックアップの仕組みが刷新され、今後は若手社員への技術継承が容易になることは間違いありません。この他にも、当社のシステムに蓄積されたデータには、日々の業務で必要なもの、今すぐには必要がなくても長期間にわたって保存しなければならないものなど、さまざまなデータがあります。こうしたデータ資産管理の最適化といった点でも、Rubrikから価値を引き出せるのではないかと思います」

サイバー攻撃の脅威がますます高まる中、データ資産の安全性の確保は事業の根幹ともいえる重要なテーマです。Rubrikのバックアップソリューションは、今後も同社のIT戦略の中で大きな役割を果たしていくはずで



ルーブリック・ジャパン株式会社
〒105-0001
東京都港区虎ノ門1-10-5
KDX虎ノ門1丁目ビル11F

お問い合わせ先
japan-info@rubrik.com
050-3733-1850
www.rubrik.com/ja/

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。

RubrikはRubrik, Inc.の登録商標です。本ドキュメント中に記載された会社名、製品名などは、各社の登録商標 または商標です。