
rubrik

# ランサムウェアからの保護と オンプレミスとクラウドを一元管理する 先進的な統合バックアップ管理を実現

上田八木短資株式会社

**業界 ： 金融機関**

**導入前の課題:**

- ランサムウェアに対する バックアップデータの保護
- 重要データの日次バックアップ によるタイムラグの発生
- バックアップの運用にかかる 作業負荷
- 対象外となっていたMicrosoft 365データのバックアップ

**導入効果:**

- 重要データを1時間単位で バックアップ
- バックアップに関する 運用管理負荷の軽減
- オンプレミスデータと Microsoft 365データの 統合バックアップ管理
- 本番環境に影響することなく リストアテストが可能

1918年の創業以来、国内短期金融市場におけるスペシャリストとして、様々な金融商品の仲介やサービスを提供している上田八木短資株式会社 （以下、上田八木短資）。同社では、ランサムウェアによる脅威からバックアップデータを保護するため、最新のWeb分散技術とAI技術を搭載したRubrikのバックアップアプライアンスを導入。Microsoft 365とオンプレミスで運用する基幹システムの統合バックアップ環境を実現するとともに、運用のシンプル化と自動化を図っています。

## ランサムウェアからバックアップデータを保護するためRubrikを導入

銀行や証券会社などの主要金融機関や一般事業法人などが資金の運用 ・調達を円滑に行う金融インフラを担う上田八木短資。同社では、地震などの自然災害だけでなく、感染症によるパンデミック、さらにはシステム障害やサイバー攻撃などによるインシデントの発生に備え、強固なBCP体制を構築しています。
業務拠点は東京と大阪に加え、都内にバックアップオフィスも併設。勘定 ・決済システムといった基幹システムを含むすべてのシステムについて、仮想化を進めることで業務拠点を問わずに利用できる環境を構築するとともに、東日本と西日本2か所のデータセンターで二重化したDR （ディザスタリカバリー）構成で運用しています。システムや業務データも定期的にバックアップを実施することで、被害の極小化と業務の早期復旧による事業継続体制の構築に努めています。
一方、この数年、ランサムウェアによる攻撃手法が高度化 ・複雑化しており、平時に利用している業務データだけでなく、バックアップデータを暗号化して人質とする攻撃手法も多く見られるようになってきています。そのため、バックアップデータをランサムウェアから保護する仕組みの導入が急務となっていました。
「当社においても、NDR（Network Detective and Response）やEDR（Endpoint Detective and Response）などを導入し、ランサムウェアを含む様々なサイバー攻撃への対策に取り組んでいます。しかし、現状の攻撃は多様化しており、水際の対策だけでは完全にすべての攻撃を防ぎきることができません。万が一、侵入を許してしまった場合でも、最後の砦となるバックアップデータを保護すると同時に、運用自体の効率化を図るために、Rubrikのバックアップアプライアンスを導入しました」と情報システム部長を努める佐藤勝利氏は説明します。
オンプレミスの仮想ストレージで管理している約10TBのシステムおよび業務データと、Microsoft OneDriveやMicrosoft SharePointなどクラウドで利用しているMicrosoft 365のデータに関して、Rubrikを用いて定期的にバックアップを実施しています。

## バックアップの運用や設定に関する業務が大幅に効率化

従来の環境はMicrosoft Azureにはネイティブで対応しておらず、Microsoft 365のデータはバックアップの対象外でした。また、バックアップサーバーのリソースには限界があり、多くても4多重程度しかバックアップジョブを実行させることができなかったため、重要なシステムのデータであっても日次単位でしかバックアップを更新することができませんでした。
Rubrikを導入したことで、手間をかけることなくMicrosoft 365のデータもバックアップができるようになりました。そして、差分バックアップの処理時間が高速で、12多重程度で同時に制御できることから、更新頻度の高いデータや重要なデータに関しては1時間ごとにバックアップを更新することが可能となっています。

更新頻度が高まったことで、誤って削除してしまったファイルなどをリカバリーする場合はもちろん、インシデント発生時に復旧するバックアップデータも、1時間以内に更新されたデータを、ファイル単位で簡単にリカバリーできるようになり、失ってしまうデータを最小限に抑えることができます。
また、バックアップジョブのポリシー設定も、従来は取得対象ごとに設定をしなければならず、設定作業に1時間以上かかっていましたが、Rubrikでは仮想マシングループに対してポリシー割り当てが可能となり、設定時間も数分以内で済むといった対応時間の削減効果が出ています。
さらにジョブの実行もAIによる自動運用が可能で、バックアップに失敗した際には、その内容や原因の詳細が管理者に送られてくるので、トラブルの切り分けが容易で、迅速な対応が可能になるなど、バックアップの運用に関する業務が効率化されました。

## バックアップの運用や設定に関する業務が大幅に効率化

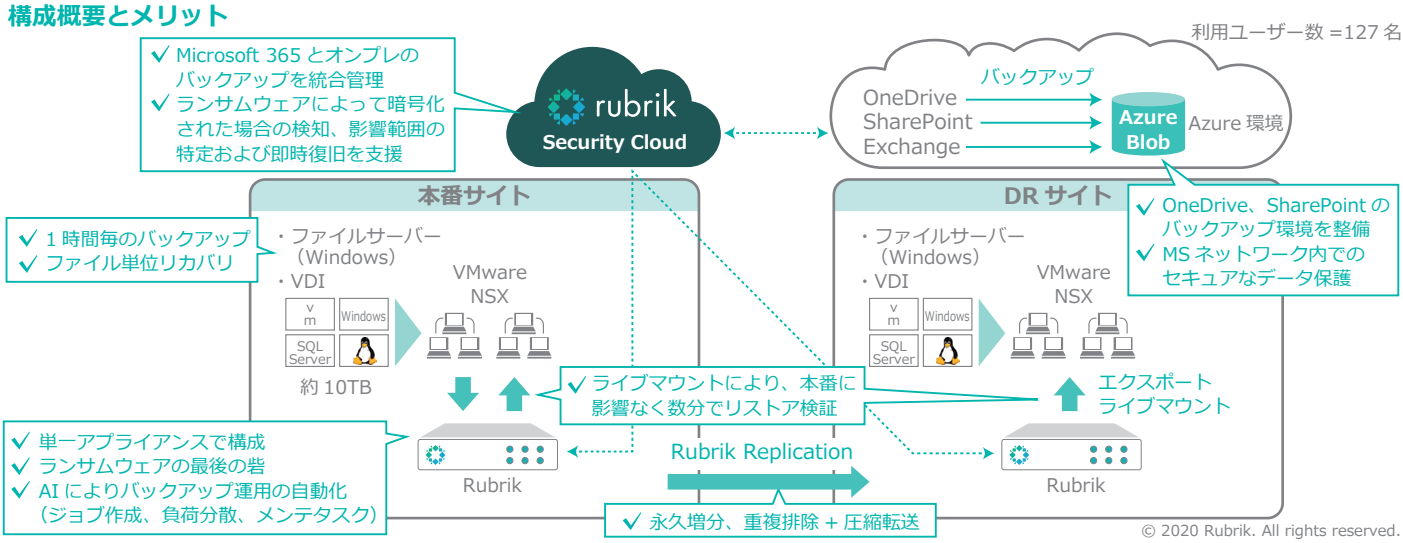
従来の環境はMicrosoft Azureにはネイティブで対応しておらず、Microsoft 365のデータはバックアップの対象外でした。また、バックアップサーバーのリソースには限界があり、多くても4多重しかバックアップジョブを実行させることができなかったため、重要なシステムのデータであっても日時単位でしかバックアップを更新することができませんでした。
Rubrikを導入したことで、手間をかけることなくMicrosoft 365のデータもバックアップができるようになりました。そして、差分バックアップの処理時間が高速で、12多重のジョブを同時に制御できることから、更新頻度の高いデータや重要なデータに関しては1時間ごとにバックアップを更新することが可能となっています。
更新頻度が高まったことで、誤って削除してしまったファイルなどをリカバリーする場合はもちろん、インシデント発生時に復旧するバックアップデータも、1時間以内に更新されたデータを、ファイル単位で簡単にリカバリーできるようになり、失ってしまうデータを最小限に抑えることができます。
また、バックアップジョブのポリシー設定も、従来は取得対象ごとに設定をしなければならず、設定作業には1時間ほどかかっていましたが、Rubrikでは仮想マシングループに対して割り当てが可能となり、設定時間も数分程度で済むようになっています。
さらにジョブの実行もAIによる自動運用が可能で、バックアップに失敗した際には、その内容や原因の詳細が管理者に送られてくるので、トラブルの切り分けが容易で、迅速な対応が可能になるなど、バックアップの運用に関する業務が効率化されました。

上田八木短資株式会社
情報システム部　佐藤勝利 氏

## 顧客から強く信頼される業務運営の継続を下支えするRubrik

今後、上田八木短資ではシステムインフラの全面更改を計画しています。佐藤氏によれば、「本来はインフラの更改に合わせてバックアップ環境も見直す予定でしたが、ランサムウェア対策を優先してRubrikの導入を先行して進めました」と説明しています。
なお、Rubrikの同期機能を利用することでDRサイトのサーバーリソースを一部削減できるとのことで、現在、Rubrikの活用を前提にコストダウンも意識した新インフラの設計が行われています。
金融インフラを担う事業者として、顧客から強く信頼される堅確な業務運営を継続するためのシステムインフラをRubrikが支えています。

## 構成概要とメリット




rubrik

**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ー企業である 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 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。

Webサイト: https://www.rubrik.com/ja/"

20230000_v1