

# そのデータ保護は サイバーリカバリに 対応できますか

ランサムウェア  
によって  
暗号化された  
データの復旧



ランサムウェアに  
侵害された  
影響範囲の特定



二次感染  
リスクのない  
バックアップ  
データの特定

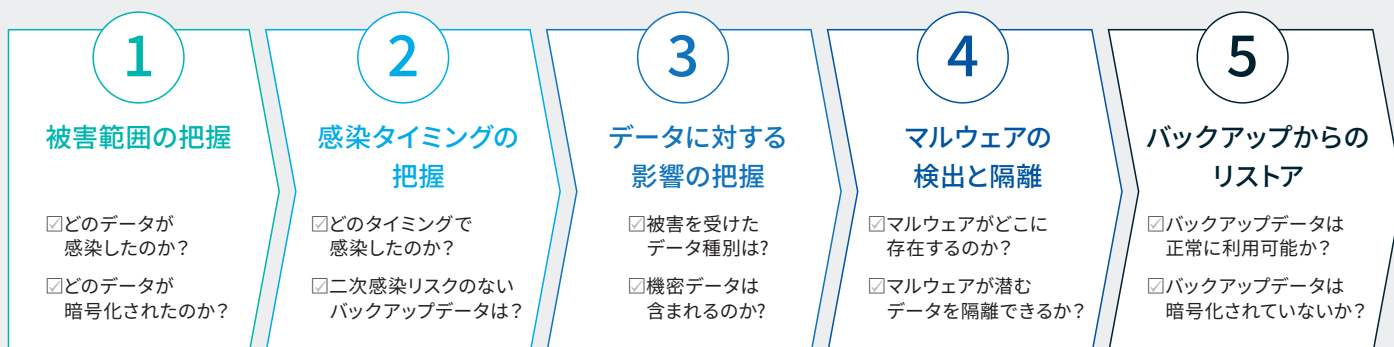
ビジネス影響を  
最小化する  
迅速な復旧

サイバー攻撃からの  
「確実な復旧手段」の確立を  
お急ぎください

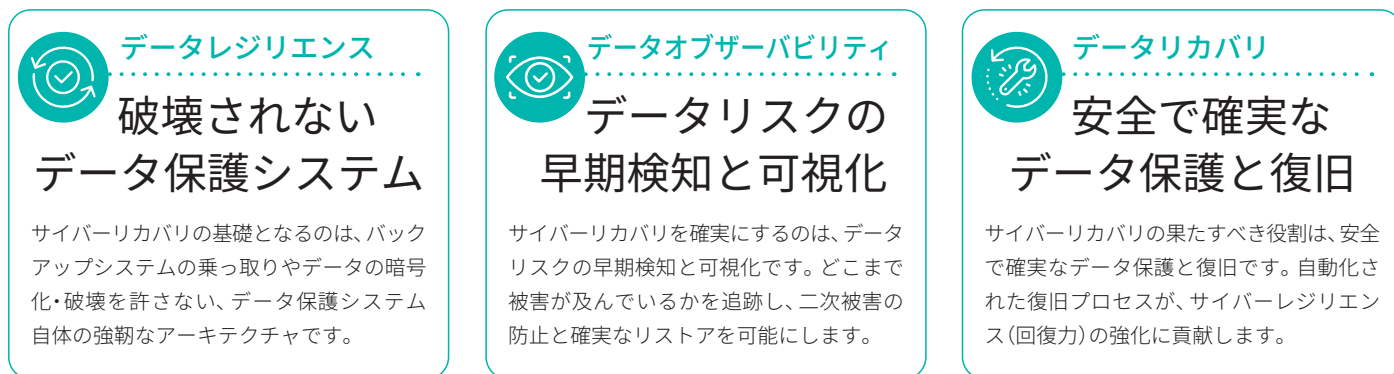
# サイバー攻撃の脅威に備える データ保護・復旧の新たなデザイン

ランサムウェア被害によりデータの破壊・暗号化とサービスダウンが発生し、数か月のビジネス停滞を余儀なくされた事案は、日本企業が標的にされたサイバー攻撃の脅威を象徴する出来事でした。企業のセキュリティ対策は高度化しているものの、それでも被害は増え続けています。たとえサイバー攻撃に遭っても、確実にデータとビジネスを復旧できる手段の確立が急がれています。

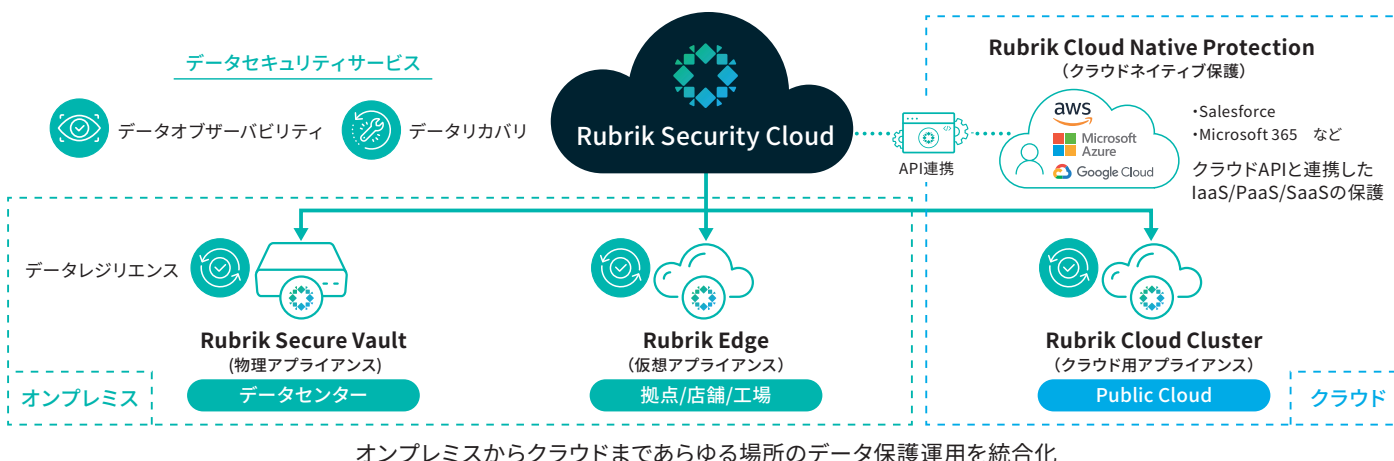
サイバー攻撃からデータを復旧させる「サイバーリカバリ」は、通常のリストアとは異なることに留意しなければなりません。  
あなたのデータ保護環境は、次のような状況に対応できますか。



## Rubrikの「サイバーリカバリ」で脅威に備える



## Rubrikが実現する「サイバーリカバリ」のための統合プラットフォーム



# 実効性が証明された Rubrikのサイバーリカバリ

2014年に創業したRubrikは、サイバーリカバリのためのゼロトラストアーキテクチャを開発しました。バックアップデータの改変を許さない《イミュータブルファイルシステム》、不正なデータアクセスを防止する《論理エアギャップ》、あらかじめ組み込まれた《ネイティブのデータ分析エンジン》が最大の特徴。Rubrikは、データ保護とサイバーリカバリに必要な機能を統合した“強固な金庫”そのものです。

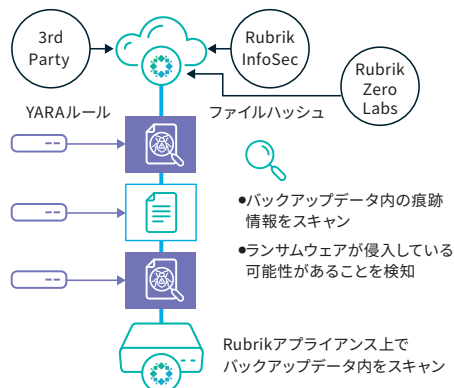


## Rubrikのネイティブなデータオブザーバビリティ

Rubrikは、サイバーリカバリをより安全で迅速に行うために、データリスクを早期に検知して可視化する「データオブザーバビリティ」を備えています。Rubrik独自のゼロトラストアーキテクチャに、追加機能でなくネイティブに統合されていることが特徴です。

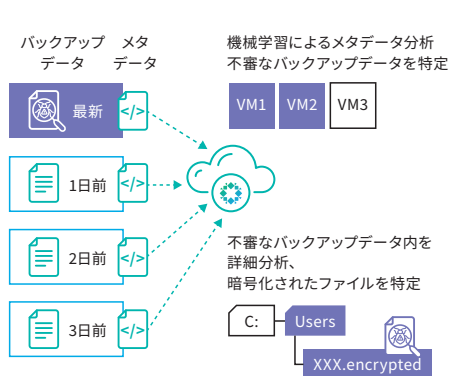
### 【侵入監視】脅威モニタリング Threat Monitoring

バックアップデータを取得後に自動スキャンしてマルウェア侵入の兆候を検出するとともに、潜在的な脅威を可視化します。リスクの早期検出、調査の迅速化によりビジネス影響を最小化するとともに、二次感染のリスクも低減します。



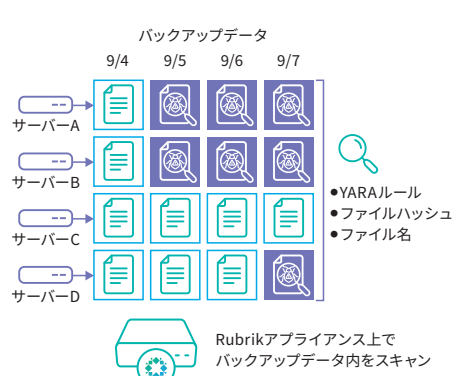
### 【被害調査】ふるまい検知 Anomaly Detection

バックアップのメタデータを独自の機械学習モデルが分析し、ランサムウェアにより暗号化されたシステムやファイルを高精度に検出・可視化。これにより、被害状況の調査からデータ復旧までの期間を大幅に短縮します。



### 【安全調査】脅威ハンティング Threat Hunting

バックアップデータをオンデマンドでスキャンして、最初に感染したのがどのファイルか、いつ感染したのかを調査し、データ復旧に使用可能なクリーンなバックアップデータを正確に特定。二次感染のリスクを排除します。



# 信頼を裏づける豊富な事例

## 日本でも導入が進む Rubrik

Rubrikは、業種や事業規模を問わず幅広いお客様に採用されています。プライベートクラウド、拠点・店舗・工場だけでなく、パブリッククラウドとクラウドアプリケーション/SaaS、これらが連携するハイブリッドクラウドまで、様々な環境でデータ保護とサイバーリカバリに貢献しています。

### 情報・通信

#### データ保護のモダン化とサイバーリカバリの強化

- バックアップの所要時間を最大70%削減
- バックアップデータの重複排除率80%を達成
- サイバーリカバリ/レジリエンスの強化を推進

国内およそ70社、8万ユーザーが利用するプライベートクラウドのバックアップシステムをRubrikにより最新化。初期設定工数とバックアップ取得時間を大幅に削減するとともに、データ保護の安全性・確実性を大幅に高めました。さらに、ふるまい検知と脅威ハンティングを活用したサイバーリカバリの導入を進めています。

### 金融

#### ランサムウェアの脅威から重要なデータを保護

- システムやデータの重要性に合わせた柔軟なバックアップ運用を実現
- ランサムウェアなどによるデータ消失リスクの回避
- Microsoft 365とオンプレミスの統合バックアップを実現

ランサムウェアなどへの防御を強化しても、高度化・巧妙化するサイバー攻撃を防ぎ入れないリスクは残ります。そこで、たとえ侵入を許してしまってもバックアップデータを安全・確実に保護するためにRubrikを採用。Microsoft 365とオンプレミス基幹システムに適用できる「統合的なデータ保護基盤」を実現しました。

### 建設・総合電機

#### ランサムウェアの迅速な検知とレジリエンス向上

- ランサムウェアなどのサイバー攻撃への備えを強化
- イミュータブルファイルシステムによりオフラインでのデータ保護が不要に
- HCIと親和性が高く運用が容易なデータ保護環境の整備

ランサムウェアの被害を受けた経験をもとにRubrikを導入。データの改変を許さないイミュータブルファイルシステムによりオフラインでのデータ保護を不要にするとともに、ランサムウェアの迅速な検知を実現しました。主要システムを運用するHCI環境との親和性が高く、データ保護環境の運用負荷を大幅に軽減しています。

### より詳細な情報はこちら

#### 導入事例

あらゆる業種での成功事例を多数ご紹介しております。ぜひご確認ください。  
<https://www.rubrik.com/ja/customers/all-customers>



#### ご質問・お問い合わせ

Rubrikの社員が皆様の質問にお答えします。お気軽にお問い合わせください。  
<https://www.rubrik.com/ja/contact-sales>



Rubrik Japan株式会社

URL : <https://www.rubrik.com/ja>

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。