rubrik

ホワイトペーパー

Preemptive Recovery Engine：迅速なサイバーリカバリのためのアーキテクチャ基盤

目次

概要

企業規模でのサイバー攻撃からの復旧には、事業継続やデータ整合性に直接影響を与える特有の技術的課題が伴います。復旧プロセスが少しでも遅れれば、事業運営が大きく混乱する可能性があります。攻撃の検出後のみに重要な分析を開始するという従来の事後対応的なサイバーリカバリのアプローチでは、既存のバックアップ・リカバリアーキテクチャやサイバーセキュリティツールを改善していくだけでは解消できない根本的なボトルネックが生じます。

このホワイトペーパーでは、リカバリの必要性に先立って調査と準備作業を継続的に実施することで事後対応型のリカバリモデルが抱える制限に対処する、「Preemptive Recovery Engine」テクノロジーの設計と実装について説明します。このアーキテクチャにおける中核的な技術革新となっているのは、集中的なデータ分析処理を重要なリカバリパスから切り離すことです。これは、基盤となるバックアップデータブロックにアクセスせずにサイバー攻撃の分析を可能にする包括的なメタデータレイヤーによって実現されています。このアプローチにより、復元したシステムの整合性を確保しながら、従来は数日から数週間を要していたリカバリ処理を数時間で完了できるようになります。

はじめに — リカバリ危機

午前3時17分、アラートが発生しました。SOCチームは、ランサムウェアによって組織全体の重要システムが暗号化されたという衝撃的な事態を確認しました。CIOが緊急対応センターに到着すると、すぐに質問が飛び交い始めます。攻撃の影響はどこまで広がっているのか？ 被害に遭ったのはオンプレミス環境のシステムだけなのか、それとも、クラウドやSaaSプラットフォームにも及んでいるのか？ 攻撃者が最初に侵入したのはいつなのか？ 機密性の高いデータにアクセスされたのか？ 正常なバックアップを確保できているのか？ 復旧にどれだけの時間がかかるのか？

技術チームがこのような状況に陥った場合、プレッシャーのかかる中でこれらの疑問に即座に答えることは困難です。SOCチームは何年にもわたってバックアップを真摯に実行してきましたが、データがバックアップされ、復旧の準備が整っていたとしても、それは乗り越えなければならない数々の難題のほんの始まりに過ぎないという厳しい現実に直面します。

主任エンジニアがバックアップ管理コンソールを開き、複数のVPN接続、認証情報、認証トークンを処理するものの、目の前にあるのは、数百に及ぶアプリケーション、システム、プラットフォームにまたがる数千のリカバリポイントだけです。正常なバックアップはどれか？ 潜伏中のマルウェアを含んでいる可能性があるのはどれか？ SOCチームが復旧すべきワークロードはどれか？ 従来のリカバリアーキテクチャの場合、システムの復旧に着手する前に、環境全体のさまざまなデータコピーを復元してフォレンジック分析を実施する必要があり、その作業だけで数日を要する可能性がありました。

PREEMPTIVE RECOVERY ENGINEアーキテクチャ

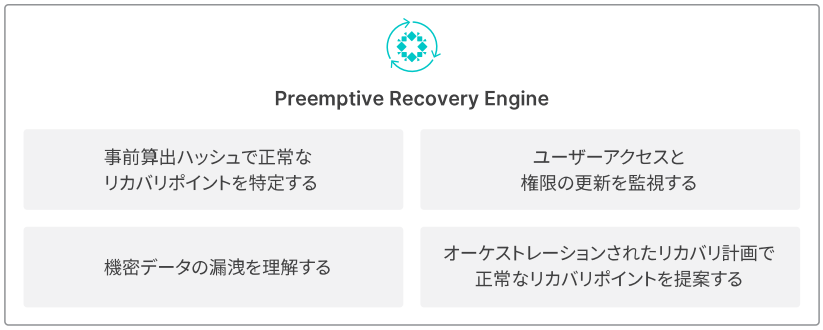
「質問される前に答える。」

10年前、Rubrikは、インフラの構成要素とソフトウェアを単一のセキュアなスケールアウトソリューションに統合し、バックアップ・リカバリアーキテクチャを刷新しました。この進化により、IT部門にとって重大な課題であり、事業運営の足かせとなっていた（現在もなおそうである）構成要素の分散が解消されました。このソリューションにおけるユーザーエクスペリエンスと信頼性は高く評価されていましたが、実はRubrikがデータおよびメタデータ管理に独自のアプローチを採用していたことはほとんど知られていませんでした。

長年にわたり、バックアップメタデータはバックアップソリューションで作成および保管されていて、バックアップおよびリカバリスタックの「カタログ」と呼ばれるコンポーネントを動かす基本情報（ファイルの種類やサイズなど）を把握するようになっていました。その後、保存されるメタデータはより詳細になり、バックアップソリューションがバックアップコピーのファイルを個別に参照できるようになりました。その結果、ファイル単位での復旧など、主要な機能が実現可能になりました。しかし、この段階でほとんどのイノベーションはストップしてしまいました。なぜなら、アーキテクチャのプロセスが過剰な負荷となってソリューションが重くなったり、カタログが維持できないほど肥大化したりしたからです。

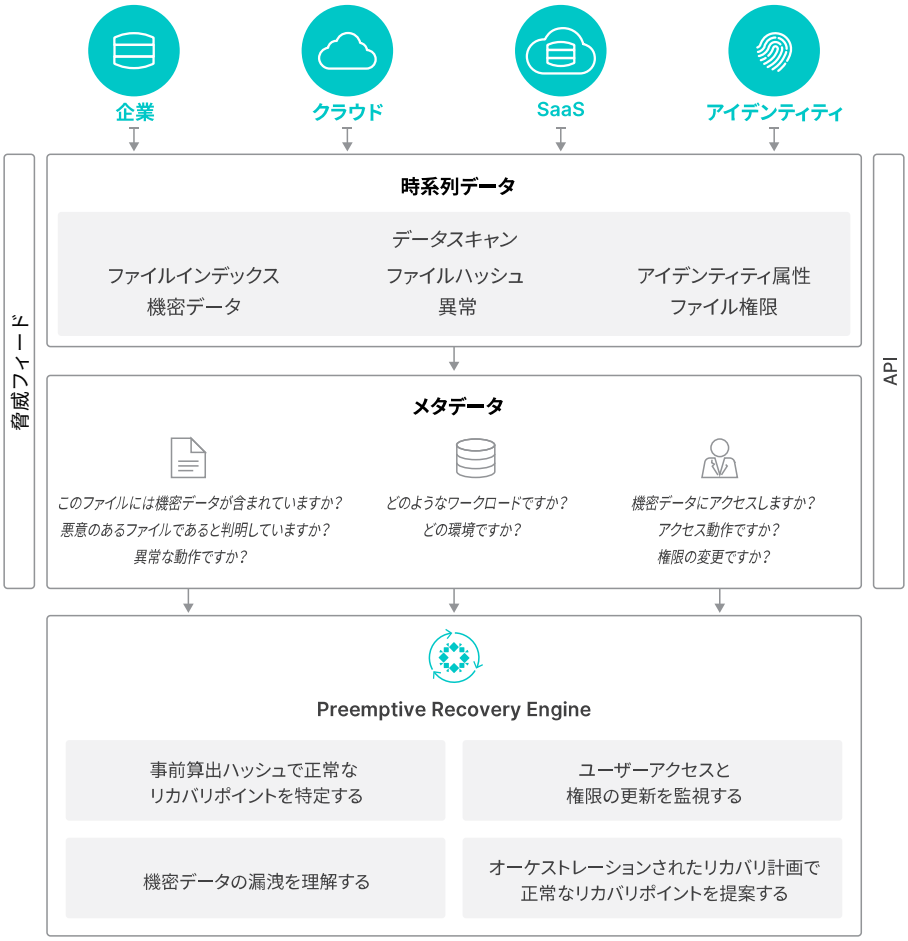
この事態を認識したRubrikのエンジニアリングチームは、データとメタデータを新たな視点で捉え、プラットフォームアーキテクチャにクラウドスケールの原則を取り入れることで、単一のプラットフォームでメタデータの収集だけでなく、作成と強化も可能になりました。このアプローチにより、Rubrikのプラットフォームは共通のフレームワークでさまざまなメタデータを関連付けることが可能になり、顧客向けのインサイトやツールが提供しやすくなりました。

そして現在、Rubrikは、インシデントが発生してしまった場合でも、より高速かつ確実なリカバリを可能にする独自のソリューション「Preemptive Recovery Engine」により、顧客のサイバーリカバリ時間の短縮に重点的に取り組んでいます。このイノベーションでは、データとメタデータに関して自社のアーキテクチャ基盤を活用することで、手動による介入なしに、プラットフォームがオンプレミス、クラウド、SaaSの各環境をまたがるバックアップを継続的かつ自動的にスキャンできるようにしています。これにより、プラットフォームが攻撃の発生後ではなくデータ作成時に分析を実施するため、顧客はリカバリウィンドウにおける貴重な時間を節約できる有利な立場に立てます。



さらに、Rubrikは、メタデータを関連付けてさらなるインサイトを導き出すとともに、サイバーリカバリプロセスを事前に開始する機能も備えています。Rubrikのエンジンは、あらかじめ算出したハッシュと時系列インテリジェンスを組み合わせて正常なリカバリポイントを迅速に特定し、さらに、ネイティブに統合された脅威スキャンにより、追加のサーバーやサードパーティ製ツールが不要になります。

Rubrikの特徴は、アイデンティティインテリジェンスを統合して潜在的な攻撃の全体像を提示するとともに、隔離機能を備えたエンドツーエンドのオーケストレーションされたサイバーリカバリソリューションを提供する、統合プラットフォームのアプローチにあります。この包括的な単一プラットフォームソリューションは、従来の断片化したソリューションに比べて、サイバーリカバリの目標復旧時間の短縮を可能にします。



以下、アーキテクチャの詳細とその仕組みを詳しく解説します。

時系列データとデータスキャン

Preemptive Recovery Engineは、オンプレミス、クラウド、SaaSの各ワークロードにまたがるバックアップおよびアイデンティティデータの上に構築されています。時間の経過とともに、バックアッププロセスで作成されたデータポイントが時系列のデータとメタデータを形成し、Rubrikが活用できる履歴レコードとなります。基本的なメタデータを追跡する従来のバックアップカタログとは異なり、このシステムは以下のデータを取得します。

履歴バージョン管理：保護対象システムの時点ごとの状態を保持します

変更追跡：データ、権限、設定、アクセスパターンの変更を継続的に記録します

リビジョン分析：環境全体におけるデータの変更時期と方法を特定します

この時系列フレームワークにより、環境を時系列で可視化し、チームはビジネスを支えるシステムとデータを把握できるようになります。ランサムウェアがファイルを暗号化したり、攻撃者が構成ファイルを変更したりした場合、データにパターンを生み出し、それがバックアッププロセス全体で補足されます。

このような時系列の基盤を基に、システムはバックアッププロセスにおいて追加の分析手法を適用します。

暗号ハッシュ：データバックアップの指紋を生成し、変更を追跡して整合性を検証します

詳細なファイルインデックス：クラウド、SaaS、オンプレミスの各ワークロードについて、保護されたファイル、オブジェクト、テーブルを含む検索可能なインベントリを作成し、評価や細かいリカバリに使用できるようにします

関係マッピング：SaaSプラットフォームの構造化データの親子関係を統合し、シームレスで機能的なデータリカバリを実現します

異常検出：ファイルやハイパーバイザ単位で外れ値や予期しない変更を特定します

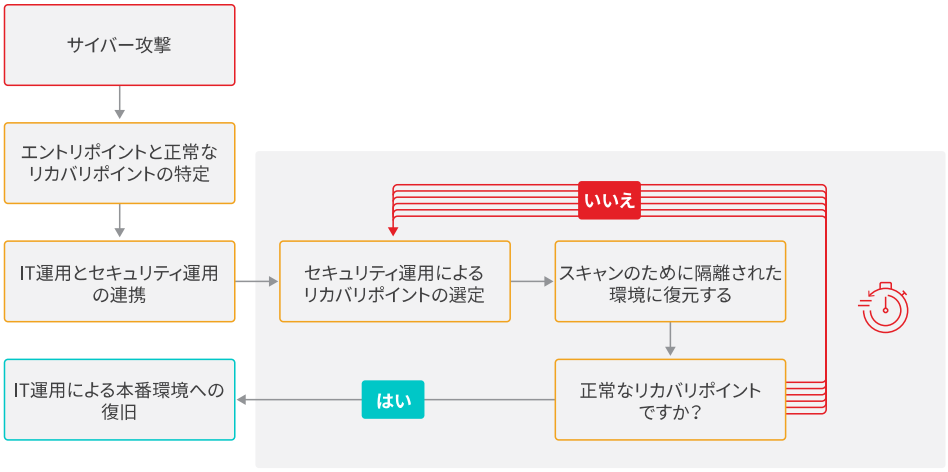
機密データ分類：個人識別情報（PII）や財務データといった機密性の高い情報とその所在を特定します

権限マッピング：ファイルやフォルダ単位で権限を詳細に追跡し、過剰なアクセス権限を特定します

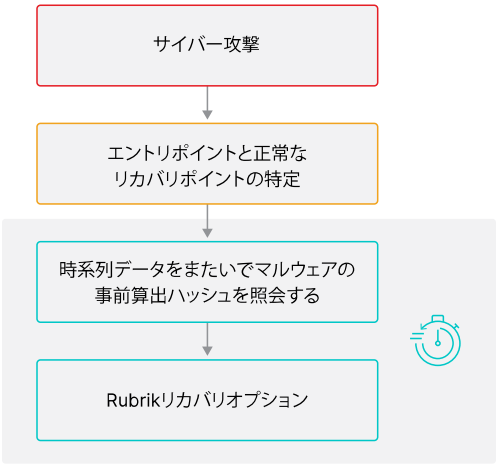
アイデンティティ属性分析：ユーザー権限、アクセスパターン、権限の変更をカタログ化します

この分析は通常のプラットフォーム運用中に行われ、Rubrikの中核的な基盤であるポリシー駆動型モデルによって実現されています。これにより顧客は、管理構成に不要な時間をかけずにプラットフォームから得られる成果に集中できます。さらに、サイバーリカバリウィンドウは常に時間との競争であるため、プラットフォームがこれらのアクションをインラインで実行できることは、リカバリを成功させる上で欠かせません。

この機能の具体例として「Turbo Threat Hunting」があります。これにより、データの復元処理を必要とせずに、最大75,000個のスナップショットを60秒以内に処理できます。従来、この処理は手間のかかるプロセスであり、チームは正常なリカバリポイントを検索・特定するために、システムとデータの完全なコピー復元を別のインフラやテナントに実行する必要がありました。その結果、リカバリワークフローがループ状態に陥り、時間がかかるだけでなく、エラーが発生しやすい状態になっていました。



Preemptive Recovery Engineでは、侵害の痕跡を探すために複数の大規模なデータセットを復元するのではなく、通常のバックアップサイクル中に作成された事前算出ハッシュにアクセスして、正常なリカバリポイントを迅速に特定できます。



この点を詳しく説明するため、機能の概要を示します。

従来のアプローチ：

- 5,000ワークロード × 15日分の保存 = 75,000個のバックアップスナップショット
- 75,000個のバックアップスナップショット × 1分のスキャン時間 = 75,000分 = 1,250時間 = 50日以上
- ***結果：50日以上のダウンタイム、評判の低下、収益の損失***

Rubrikのアプローチ：

- ***結果：75,000個のバックアップスナップショットを60秒以内にスキャン可能***

ペタバイト規模の環境を持つ組織の場合、このアプローチを採用することで、分析時間を数日～数週間から数時間に短縮できます。

METADATA INTELLIGENCE

Preemptive Recovery Engineは、保護対象ワークロードに関する情報を継続的に抽出・分析します。この情報は、データセットの量ではなくカーディナリティに比例して拡張する分散メタデータレイヤーに保存されます。これにより、効率的なクエリや分析が線形にスケールします。

包括的なインデックス：ファイル属性、権限、ハッシュ、アクセスパターンを保存します

アプリケーションコンテキスト：カスタマイズされたリカバリ計画を通じて、構成パラメータ、依存関係、状態情報をマッピングします

ユーザー行動分析：認証イベント、権限の変更、アクセスパターンを監視します

セキュリティポスチャ評価：脆弱性とポリシー違反を特定することで、環境をまたがって不要なリスクを軽減します。

数千台のサーバーやペタバイト規模のデータを持つ企業の場合、サイバーリカバリで環境全体を分析するには、数日や数週間かかることもあります。メタデータアプローチの場合、復元されたコピーや隔離された本番環境から取得したデータ自体を調べるのではなく、データに関する必要なすべての情報が事前にインデックス化されており、それを検索するため、同様の分析が数分で完了することもあります。

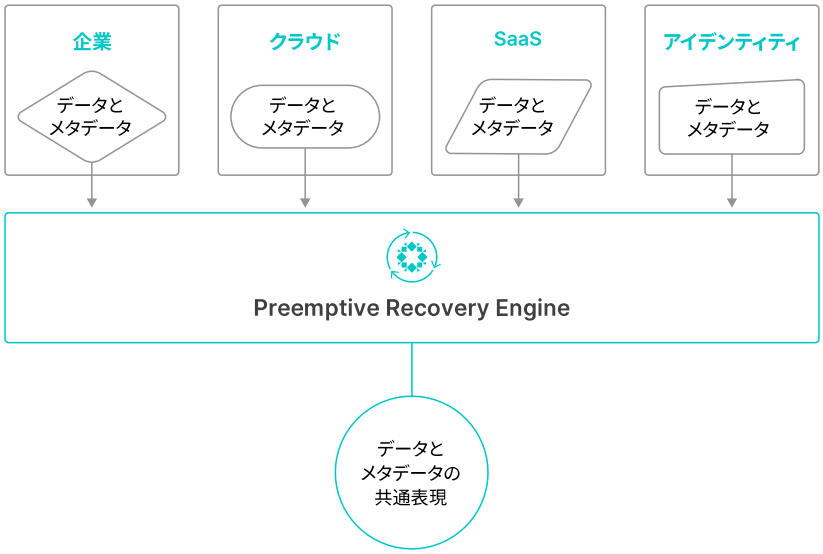
データとメタデータの共通表現

これらのコアコンポーネントに加え、Preemptive Recovery Engineは、データとメタデータの表現について統合アプローチを取り入れています。

統合可視性：環境全体にわたり、データ、メタデータ、アプリケーション、アイデンティティ間の関係をマッピングします

ドメイン横断的な把握：クラウド、オンプレミス、SaaSの各環境にまたがるハイブリッドインフラの全体像を可視化します

依存関係マッピング：カスタマイズ可能なリカバリ計画を通じて、アプリケーションの機能を維持するリカバリシーケンスを可能にします



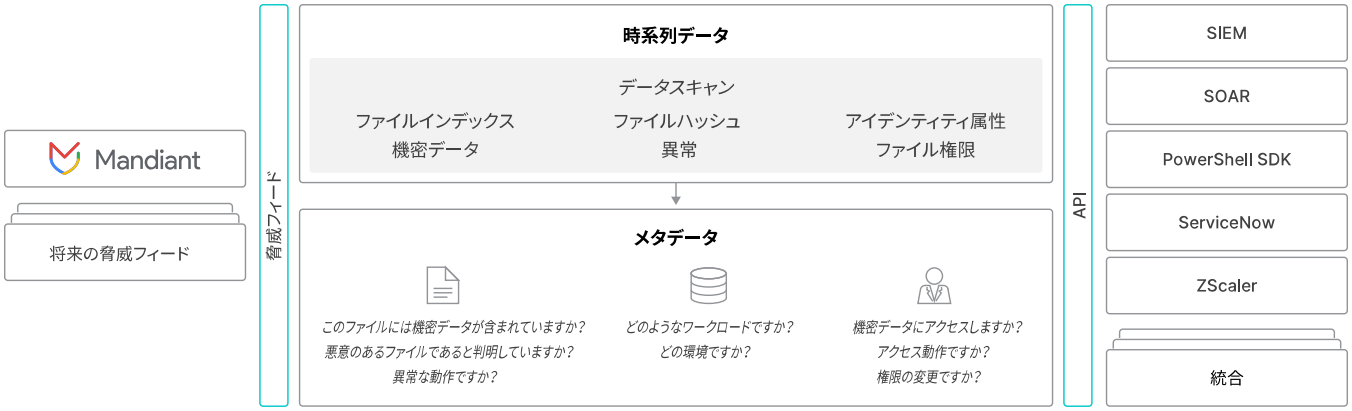
この共通表現により、従来の複数製品にまたがるバックアップソリューションに伴うデータサイロの問題が解消されます。リカバリとは、単にデータを復元することではなく、正常に動作するアプリケーションを復旧することです。バックアップシステムに対する従来のアプローチでは、仮想マシン、ファイル、データベースを個別に認識しているものの、これらの相互作用への理解が欠けていました。

この機能の具体例として「Recovery Plans」があります。これにより、組織が手順をカスタマイズして、ブート順序、IP構成、スクリプトなどの追加オプションを使いながらアプリケーションのリカバリをオーケストレーションできます。Rubrikはデータとメタデータの汎用的な表現を提供しているため、システムがプラットフォーム全体の情報を解釈し、システムごとに正常なコピーに関する提案や予測を行うことができます。そしてエンジンは、異常がなく隔離されていないスナップショットを把握し、UIのリカバリ計画ワークフローで提案を行います。これにより、システムごとに意図した時点のコピーに復元するために必要な時間が短縮されます（例：20システムのアプリケーションのうち、5システムは4日前のコピーから、残りの15システムは前日のコピーから復元する必要がある場合）。

エコシステム統合と脅威インテリジェンス

Preemptive Recovery Engineは拡張性を中心に据えて設計されています。これは、現在のセキュリティの課題には、単独で動作するツールよりも、連携可能なソリューションが求められているという認識に基づいています。システムはオープンAPIと戦略的な統合を通じて幅広いセキュリティエコシステムと連携しており、セキュリティチームはリカバリに関するインサイトを総合的なサイバーレジリエンス戦略に取り入れることができます。

このような拡張性により、Preemptive Recovery Engineはセキュリティ業務のための貴重なインテリジェンスソースとなります。システムは、バックアップで特定された潜在的な脅威に関する詳細なメタデータを、セキュリティ情報・イベント管理（SIEM）プラットフォームやセキュリティオーケストレーション・自動化・対応（SOAR）ツールに直接提供します。この連携により、セキュリティチームは、バックアップベースの脅威インテリジェンスを、より広範なセキュリティ監視・対応ワークフローに取り入れることができます。



このようなエコシステムアプローチの代表的な例として、RubrikとMandiant（インシデント対応、コンサルティング、脅威インテリジェンスを専門とする著名なセキュリティ企業）が提供する脅威インテリジェンスフィードとの連携が挙げられます。各ソリューションは個別に大きな価値をもたらしますが、それらを組み合わせることで、より包括的なセキュリティポスチャが実現します。

検出対象の拡大：エンドポイント保護は、攻撃者による回避テクニックを排除し、本番システム上の脅威検出に重点を置いていますが、Rubrikは、バックアップ内の静止データを調査することで、検出できる範囲を拡大しています。

高度な脅威認識：世界中の数千件のインシデントから収集した脅威インテリジェンスをバックアップデータの分析に活用し、サイバーレジリエンスを強化します。

効率的な対応：バックアップで脅威が検出されると、Rubrikは確立済みの統合チャネルを通じて管理者とセキュリティツールに通知します。

このような「一緒がベター」アプローチにより、バックアップがセキュリティ業務から切り離されていた従来のセキュリティモデルに変革をもたらします。従来のモデルに代わり、Preemptive Recovery Engineと、Rubrik Security Cloudのデータおよびメタデータは、統合セキュリティ戦略におけるインテリジェンスソースとなり、検出機能を強化すると同時にリカバリへの備えも向上させます。セキュリティチームは、主要な防御策をすり抜けた可能性のある脅威を可視化し、リカバリ業務において、利用できる最も包括的な脅威インテリジェンスを活用することが可能になります。

PREEMPTIVE RECOVERY ENGINEがもたらすリカバリの変化

Preemptive Recovery Engineの利用企業がサイバー攻撃を受けた場合、復旧プロセスは従来のアプローチとは根本的に異なるものとなります。この違いを理解するために、典型的なランサムウェアからの復旧プロセスをたどってみます。

従来の復旧プロセス

従来の環境では、復旧プロセスは不確実性とプレッシャーの中で始まります。技術チームは明確な答えのない数々の難問に直面します。攻撃はいつから始まったのか？ どのシステムが侵害されたのか？ どのバックアップが安全に使用できるのか？ どのシステムを最初に復旧すべきか？

これらの疑問に答えるには、システムを停止したまま何日もかけて調査する必要があります。セキュリティアナリストはログを細部まで調査し、フォレンジックチームは侵害を受けたシステムを調査し、バックアップ管理者は攻撃前と思われるリカバリポイントを手動で探します。このようなプロセスには、利用可能なインフラの制約や完全なコピーの復元に必要な時間といった要因のため、どうしてもパフォーマンス面で限界があります。

従来の復旧プロセスは以下のように順次的に進むため、期間が数週間から数か月にも及ぶ可能性があります。

調査：攻撃の範囲とタイムラインを明らかにします
リカバリポイントの特定：正常と思われるリカバリポイントを特定します
リカバリ計画の策定：リカバリの手順と依存関係を計画します
システムの復元：マルウェア検査のために頻繁に一時停止しながら実際の復元を進めます
アプリケーションのリカバリ：テストと再構成を行って機能を復元します

調査の完了後、チームは復旧手順の計画策定において別の問題に直面します。どのシステムが他のシステムに依存しているのか？ 特定の順に復旧すべきアプリケーションはどれか？ Active DirectoryやEntraIDなどのアイデンティティプロバイダー（IdP）をゼロから構築し直すのか？ このような不測の事態への対応が前もって計画されていない場合、通常は、スプレッドシート、ホワイトボード、個別のドキュメントなどを用いて計画の策定を進めることになり、復旧への着手がさらに遅れることになります。

一方で、ビジネスリーダーは、侵害された恐れのある機密データの特定に苦慮しています。規制により、当局や影響を受けた個人に対してデータ侵害を速やかに通知することが義務付けられているため、該当する情報を迅速に特定する必要があります。

ようやく復元に着手しますが、復元したシステムにマルウェアが再び潜り込まないよう、頻繁に中断してテストを行います。中規模の環境では、プロセスの完了までに数週間かかることがあり、その多くはデータの復元作業ではなく、調査や計画に費やされます。

この長期間のリカバリウィンドウを通じて、時間とともに経済的な影響が増大していきます。重要システムが停止すると、組織は生産性の低下、収益の損失、顧客の信頼の低下によるコストが増加していきます。取締役会や経営幹部は往々にして、技術チームが確実な答えを出せる前に、より正確な復旧期間や影響評価を求めてくるようになります。ダウンタイムが数時間から数日、さらには数週間と長期化するにつれ、ステークホルダーからのプレッシャーが強まり、技術的な判断はビジネス上の必要性に左右されるようになります。このような財務面でのプレッシャーにより、確実性と速度との間で難しいトレードオフを迫られることが多くなり、その結果、リカバリを早まったり、修復が不完全になったりする可能性があります。当初は技術的な復旧の問題だったものが、急速にビジネス上の危機へと変貌し、復旧時間が組織の財務の安定性に直接影響するようになりかねません。

PREEMPTIVE RECOVERY ENGINEの実際の動作

Preemptive Recovery Engineを利用した場合、リカバリウィンドウの流れが根本的に異なります。攻撃が発見された時点で、Preemptive Recovery Engineはすでに環境を継続的に監視・分析しています。

1. **Metadata Intelligence**は、ファイル、フォルダ、ユーザー、ワークロード、アプリケーションを理解するため、すでにシステムやデータのメタデータを収集・作成しています

2. **Data Threat Analytics**は、正常なリカバリポイントや攻撃の影響範囲を判断する指標をチームが特定できるよう支援するため、すでにバックアップスナップショットをスキャンしています

3. **Recovery Plans**は、すでに異常な動作によって影響を受けるシステムを明らかにし、推奨されるリカバリポイントを前もって特定しています

4. **Time-Series Data**は、システム内のデータリカバリポイントに関する履歴コンテキストを提供し、追加のセキュリティ調査に必要な脅威分析を深めます

5. **Sensitive Data Discovery**は、攻撃活動で影響を受ける可能性がある機密データを可視化します（すべての処理が本番環境外で行われるため、本番システムへのアクセスは不要です）

復旧プロセスが効率的な手順に変換されます。

スコープ評価：事前算出メタデータを照会して、正常なリカバリポイントを特定し、潜在的な攻撃範囲とタイムラインを把握します

リカバリポイントの選定：異常検出から得られた情報に基づき、定義済みのRecovery Plansから正常なリカバリポイントの候補を選定します

自動復旧：定義済みのRecovery Plansを用いてアプリケーションを考慮した復旧を実行し、ブート順序やIP構成のほか、アプリケーションを有効にするために必要な処理をオーケストレーションします

システム検証：アプリケーションを検証し、本番環境に戻します

監査レポート：攻撃の影響を受ける可能性がある機密データを文書化します

事後対応型の調査から事前準備のアプローチへの根本的な移行により、リカバリにかかる時間が急速に短縮され、サイバーリカバリのタイムラインが加速します。組織は、大規模なサイバー攻撃を受けた際の復旧時間を、数週間から数日、さらには数時間にまで短縮できる可能性があります。

まとめ：アーキテクチャ変革がビジネスに与える影響

「サイバーリカバリはサイバーイベントの発生前から始まる。」

サイバーリカバリのビジネス上の重要性は、これまでになく高まっています。サイバー攻撃によってダウンタイムが発生すると、時間の経過とともに、収益の損失、顧客への影響、ブランドへの潜在的な損害が発生します。技術チームは、リカバリのタイムラインやデータの漏洩について、ビジネスリーダーに確信を持って回答するのに苦慮します。その間も、断片化したリカバリツールでは、複数のシステム間で手動による関連付けが必要となり、ダウンタイムが長期化してコストが増大します。

Rubrik Preemptive Recovery Engineは、組織がこの課題に対処する方法を根本的に変革します。このアーキテクチャでは、データ保護と高度なメタデータインテリジェンスを単一のプラットフォームに統合することで、従来のリカバリ作業の断絶を排除します。さらに重要なのは、攻撃の発生前に継続的にデータを分析することで、従来は事後対応的で不確実なプロセスを、事前準備型のデータ主導の対応に変えることができます。

このアーキテクチャアプローチにより、技術的な指標だけでなく、具体的なビジネス成果を得ることができます。

財務上の影響の軽減：攻撃の発生前に分析作業を完了し、復旧までの時間を短縮することで、長時間のダウンタイムに伴う多大なコストを最小限に抑えることができます。

危機管理の信頼性：事前にリカバリポイントを算出・分析することにより、インシデント発生時の重要なビジネス上の疑問に確信を持って答えることが可能になり、経営陣は十分な情報に基づいて事業継続措置やコミュニケーションに関する意思決定を行うことができます。

規制遵守上のメリット：影響を受けたと思われるシステムやデータの可視性が向上することで、規制当局に対してより正確な評価を報告できるようになり、必要な通知の範囲が縮小される可能性があります。

事業継続の優先度付け：事業の優先度に応じてリカバリ作業を実行することで、支払処理、取引機能、患者ケアシステムなどの重要な機能を早く再開できるため、困難な時期でも顧客関係を維持することが可能です。

オペレーショナルレジリエンス：リカバリポイントに関する不確実性を軽減することで、大規模なリカバリ作業の完了後に再感染が判明するという事態を回避し、コストがかかる不備のある開始ややり直しを防ぐことができます。

Rubrikのアプローチは、既存のバックアップやサイバーレジリエンス技術を少しずつ改善するようなものではなく、技術的なリカバリ機能と事業継続の必要性との隔たりを埋めることになるアーキテクチャの変革です。たとえセキュリティツールが異常を検出してもリカバリに活かせないなら、またバックアップシステムがデータを保存してもセキュリティコンテキストが不足しているなら、さらにはコンプライアンスチームがインサイトを必要としても手動によるレポートを待たなければならないなら、こうしたギャップは、重要なリカバリ期間においてビジネス上の損失に直結することになります。

サイバーレジリエンスが事業継続に直接影響する現在の環境において、Rubrikが提供する統合プラットフォームアプローチは、IT部門を超えて多大な成果をもたらします。組織は危機的状況下でより多くの情報に基づいて意思決定を行い、極めて重要な場面で不確実性を減らし、復旧の優先度とビジネス上の重要事項を一致させることができます。

要するに、サイバー脅威との戦いでは、単にリカバリを完了させるだけでは不十分です。守りたいビジネスを保護するには、迅速かつ安全に復旧する必要があります。

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

wp-preemptive-recovery-engine_JA / 20250919