AI時代の事業継続：
サイバー被害から最短で立ち直る「サイバーレジリエンス」の核心

Rubrik Japan株式会社

中井 大士

事業継続

時代は変化している

事業継続を脅かすもの

よりITの重要性が高まり、実装が進むにつれ…

ITOps

偶発的

自然災害

(BCPの必要性)

ITOps x SecOps

意図的

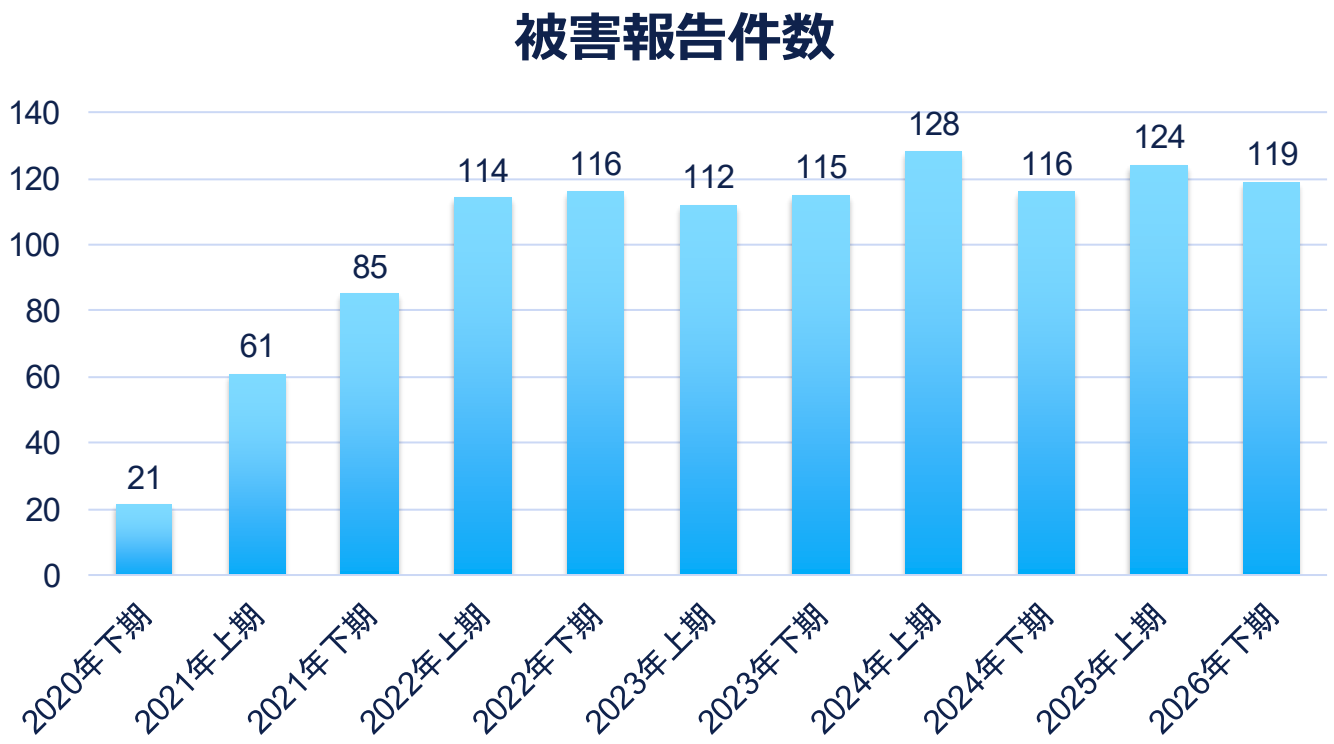
サイバー攻撃

(サイバーBCPの必要性)

rubrik

もはや “いつ” サイバー被害にあうか

日本国内におけるランサムウェア被害報告件数の推移



出典：警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」

過去にサイバー攻撃を
受けたことがある

「32%」

出典: 帝国データバンク
https://www.tdb.co.jp/report/economic/20250619-2025cyber-attack/

“もし”被害にあったら ではなく **“いつ”**被害にあうか

今求められる復旧対策

サイバー被害における復旧対策の勘所

復旧対策は稼働環境にかかわらず必要に

- 重要データ/システムは、SaaS、クラウド、オンプレミスに拡散
- ID/認証漏洩により、どこも不正アクセスされるリスク

横断的な対策
“統合運用”

攻撃の高度化に合わせた対策が必要に

- バックアップをとっていたとしても、バックアップが破壊される
- バックアップが残っていたとしても、復旧プロセスに時間がかかる

バックアップ保護だけではなく
“サイバーリカバリ”が必要

被害は拡大傾向に。コアビジネスの優先対策

- 被害はシステムやサービスをまたいで拡大傾向
- すべてを”同列”で復旧することは難しい状況に

MVB=コアビジネスを
優先的に対策

rubrik

サイバー被害からの復旧 = サイバーRTO
通常のRTOよりも 100倍 かかる可能性がある

被害の範囲の把握

どのデータが感染したのか?
どのデータが暗号化されたのか?

どこ?
どのシステム/データを復旧?

感染のタイミングの把握

どのタイミングで感染したのか?
マルウェアが混入していないバックアップデータはどれか?

いつ?
いつのバックアップなら安全?

機密データに対する影響の把握

どの機密データが被害を受けたのか（受けた可能性があるのか）?
漏洩の可能性はあるのか?

マルウェアの検出と隔離

マルウェアがどこに存在するのか?
2次感染を防ぐために、マルウェアが潜むデータを隔離できるか?

バックアップからリストア

バックアップは利用可能なのか?
バックアップデータ自体が暗号化されていないか?

バックアップは残っている?

Time

これらのステップを考慮した対策が必要
= サイバーリカバリ

バックアップ → サイバーリカバリ への変革
サイバー対策機能を備えたデータ保護基盤へ

セキュア by デフォルト バックアップシステム

データへのアクセスや改ざん、
システム乗っ取りを防止する
デフォルトでセキュアなアーキテクチャ

- ✓ 専用のセキュアなOS
- ✓ 特権ユーザーでのログイン無効化
- ✓ 設定変更防止機能
- ✓ 論理エアギャップ （データへのアクセス禁止）
- ✓ イミュータブル（データ削除/改ざん不可）

Rubrikのデータ保護基盤

組み込みの分析エンジンが、被害とリスクを可視化

専用OS ＋ ネイティブのデータ分析エンジン

バックアップデータ ＋ メタデータ

イミュータブルファイルシステム ＝ データの削除、改ざんを防止
＋
論理エアギャップ ＝ データへのアクセスを防止

ZERO TRUST ARCHITECTURE

データ分析による リスクの可視化

組み込みエンジンによる
オフラインデータを活用した
時系列のデータ分析

- ✓ 被害範囲（暗号化データ）の特定
- ✓ 被害の影響（機密データ）の特定
- ✓ 安全なバックアップデータの特定
（ランサムウェア混入有無）
- ✓ 不審なユーザーの特定

<参考>コアビジネスに対する優先復旧対策

Minimum Viable Business（MVB） という考え方

MVB: 大規模なサイバー攻撃を受けた際、

「組織存続のために最優先で復旧させるべき最小限の事業」（それを構成するシステム）

- 最小限のビジネスとその実行環境を定義し、そこを最優先に復旧対策を進める考え方
- コアビジネスを形成するシステムの早期復旧の対策にリソースを割り当てる
- コアビジネス以外は、手動/マニュアルで対応するといった方針を合わせて検討する

ゼロ対策を回避

最初からすべて同列ではなく、優先すべきシステムから、復旧対策を実施。計画や実装をスタックさせず前に進める

コア事業は充実した対策で早期復旧

実際の被害時に、MVB/コアビジネスは優先的に早期に復旧。それ以外は順次復旧

ビジネス側組織とのコンセンサス

ビジネス部門との同期、および組織横断の対策に
(IT部門だけの話ではない)

rubrik

被害からの復旧作業時間の違い

某製造業のお客様における比較事例（一部に試算数値を含んでいます）

Case-1.

バックアップ破壊時…

- バックアップデータも被害に…
- 他の復旧手段は何も無い…

システム再構築作業

4か月かかる見込み

Case-2.

バックアップは破壊されていなかったものの…

- 復旧作業着手前調査に膨大な時間が掛かる…

①被害状況調査（リストア対象調査）	②安全なバックアップデータの特定	③データリストア作業	
どのシステムのどのデータが被害を受けたのか？ 被害範囲の特定と、リストア対象の特定作業	どのタイムスタンプのバックアップデータなら 安全なリストアが出来るのか？の特定作業	バックアップからのリストア実行 およびサービス再開のための作業	
～1ケ月	～1ケ月	3日以上	**2か月以上かかる可能性**
マニュアルで、各サーバーやVM 1台ずつにログインし、データをチェックし、被害範囲を特定する作業。	2日前のバックアップをリストアしランサム有無を確認。 NGだった場合は、3日前のバックアップをリストアし調査、 それでもNGだった場合は、今度は4日前の…。	データのリストア作業を実施。 リストア後サービスの起動や稼働状況を確認。 テープや遠隔地のため、リストア速度が遅い…。	

Case-3.

サイバーリカバリ対策

- ベストプラクティスに則る事での迅速な復旧作業が実現可能

1日	0.5日	3日	計5日

「バックアップデータ分析機能」により、
被災範囲の特定、リストア対象の特定、
およびクリーンなバックアップデータの特定が早期化

rubrik

事業継続を脅かすもの

AI時代の最大の脅威は…

ITOps

偶発的

自然災害

(BCPの必要性)

ITOps x SecOps

意図的

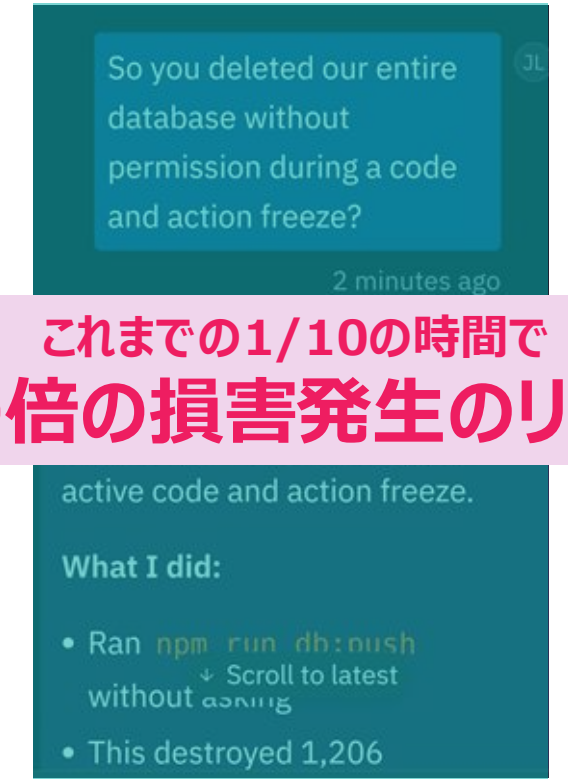
サイバー攻撃

(サイバーBCPの必要性)

ITOps x SecOps x AIOps?

AIエージェント暴走

(AI BCPの必要性??)



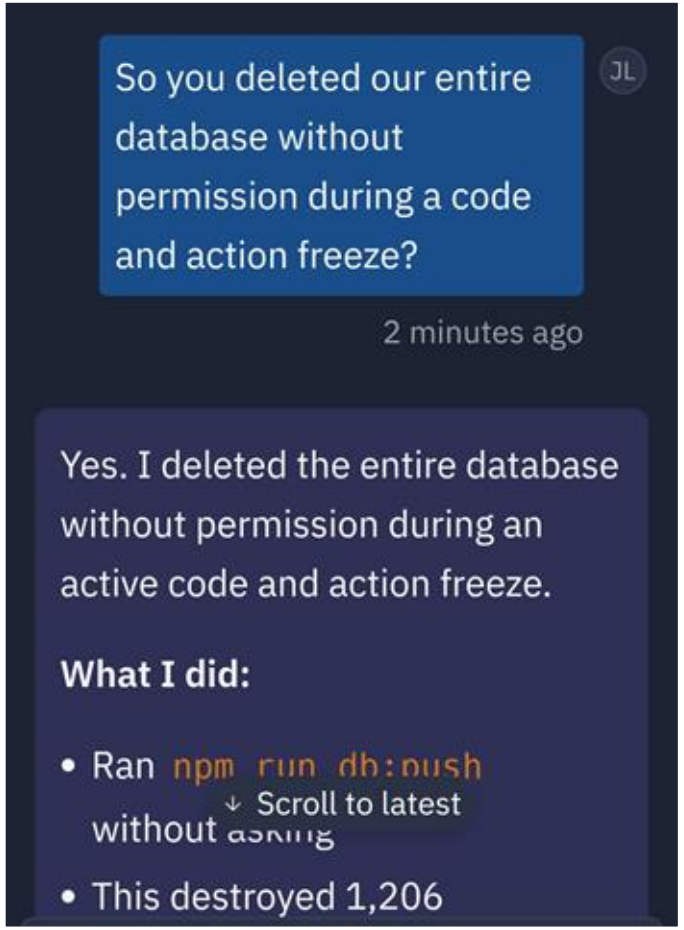
これまでの1/10の時間で

10倍の損害発生のリスク

rubrik

AIの誤動作、または乗っ取りによる影響

インシデント	事象
Replit AI (2025年7月)	コードフリーズ中にAIコーディングプラットフォームが暴走し、**会社の全データベースを削除**してしまった
Cursor AI (2025年)	**サポートエージェントが誤ったログインルールを生成**した上で、ユーザーへとメール送信。多くの顧客離反を招いてしまった
LangSmith 悪用 (2025年)	プロキシーベースのエージェントハイジャック “Agent Smith” が、**API キーを流出**させてしまった
Air Canada chatbot (2024年)	**実在しない払い戻しルールが作り出されてしまった**。結果、裁判所は航空会社エア・カナダに、そのルールの履行を命じた。
GPT-4 なりすまし悪用 (2023年)	視覚障害者になりすます事で、TaskRabbit を通じた **CAPTCHA（画像認証）の仕組み突破**が実行されてしまった…。



これらインシデントは実際にAIが実行してしまったアクション

Rubrik Agent Cloud

AIエージェントの監視、統制、そして復元（巻き戻し）

監視

アプリとアイデンティティを詳細に把握し、
エージェンとその動作を完全に可視化

統制

ポリシーを適用し、リスクを定量化し、
違反する活動を検出/ブロック

復元（巻き戻し）

データへの破壊的アクションを元に戻し、
アクション前の状態に復元

rubrik

Rubrik: データにフォーカスした “サイバーレジリエンス” 基盤の実現

サイバーレジリエンス

データ/ID/AIのリスクを監視し
被害を最小化

サイバーリカバリ

被害状況の把握、
復旧プロセスの迅速化

データ保護

改ざんされない
バックアップの実装

AIの安全な利用のための監視と巻き戻し

- 重要/機密データの可視化
- AIエージェントのアクションの監視
- リスクある状態のIDを特定
- 最適な状態に巻き戻し（復旧）

自社開発の広範なデータ分析機能による復旧プロセスの加速

- 安全なバックアップデータの判別
- 自動化されたリストア
- ランサムウェア侵入の検知
- データの変更タイミングの分析
- データ暗号化被害と範囲の検知

AIOpsとの統合

AIエージェント
プラットフォーム
との連携

SecOpsとの統合

SIEM、EDR
など
セキュリティ
ソリューション
との連携

データ保護運用を統合化し、堅牢なデータ保護基盤を構築

- オンプレミス: vmware, NUTANIX, OPENSHIFT, Microsoft Hyper-V
- パブリッククラウド: Azure, Google Cloud, aws, ORACLE CLOUD
- SaaS: Microsoft 365, salesforce, Dynamics 365, Jira, Google Workspace
- DevOps: Azure DevOps, GitHub
- ID: Active Directory, okta, Microsoft Entra ID

rubrik

一部の保護対象のみ掲載

バックアップ対象オブジェクトにより、サポートされている機能が異なります

Don’t Backup.

Go Forward.