最新アプリの障害が引き起こす問題

最新のアプリは高速に動作しますが、障害はより速く発生します。ビジネスを止めないもの、それが回復力です。

最新アプリケーションの障害は単なるデータ消失イベントではありません。発生する問題が個別のインシデントであることはめったにありません。多くの場合は、依存関係の破綻、設定エラー、導入の問題、可視性のギャップといった問題が原因です。

何が壊れるのか、どう対処すべきか



最新アプリに問題が生じる理由

最新アプリは（従来のモノリシック型ではなく）分散型インフラストラクチャ上で実行されます。分散環境は、アジリティを実現し開発サイクルの短縮を可能にする一方で、従来の保護戦略の限界を超える新たな複雑さや障害の可能性ももたらします。

従来の戦略は、ユーザーが少数のサーバー1台が停止する状況に対応するよう設計されています。残念ながら、それは何百人ものユーザーや多数の依存関係に影響を及ぼす現代の停止の範囲まで対応できません。

回復力への新しいアプローチ

最新アプリのコンポーネントは相互に依存しているため、変更にはリスクが伴います。これらのリスクや脆弱性を理解することが重要です。

APIやハイブリッド環境が拡大する中では、システムレベルで考えることがカギとなります。最良の結果を得るには、アプリケーション全体を保護しなければなりません。データ、構成、ポリシー、依存関係、メタデータ、コンテキストまで幅広く対象範囲とする必要があります。

プロアクティブな対応も重要です。回復力のギャップは問題が発生するまで表面化しないことがあるからです。インサイトが豊富なシステム健全性ツールにより、こうしたギャップが問題となる前に特定できます。

最新アプリケーションには頻繁に運用上の障害が発生している

2/3超

ITインシデントにより1時間あたり30万ドル以上の損失を被っている組織の割合。

* PagerDuty 2026 State of AI-First Operations Report

54%

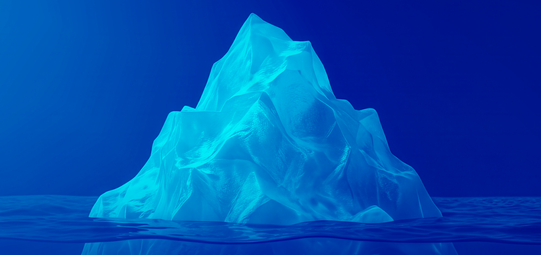
ランサムウェア被害者のうち、過去1年間にバックアップを利用して暗号化されたデータをリストアした割合。

* Sophos State of Ransomware 2025

200万ドル

重大なIT停止における、1時間あたりのコストの中央値。

* New Relic 2025 Observability Forecast



急激な侵害

01 依存関係の破綻

アプリケーションの依存関係が破綻。1つのサービス障害が連鎖的にトランザクションの停止を引き起こす。

02 ランサムウェア攻撃

ランサムウェアが最新の環境に打撃を与える。攻撃者はデータだけでなく、バックアップも標的に。

03 設定ミス

設定ミスが停止を引き起こす。小さなエラーにより、アプリが表面的には「健全」に見えるものの、実際には障害のある状態で維持される。

04 導入の失敗

導入の失敗はビジネスの中断につながる。欠陥のあるリリースでは、データや設定がすぐに破損する。

05 停止の波及効果

停止は波及する。ツールがKubernetes、VM、SaaSにまたがって断片化していると、何が実際に保護されているのかが把握しづらくなる。

06 データの不整合

バックアップが成功しても、コンテキストやメタデータ、依存関係が失われることがある。

ビジネスへのリスクは現実

ダウンタイム＝リスクです。主な影響は以下のとおりです。

運用
修正作業が増え、イノベーションは減る。

財務
ダウンタイムには分単位でコストが発生する。

セキュリティ
ランサムウェアやエラーにつながるリスクが生じる。

戦略
組織全体で自信が失われる。

最新の回復力がカギ

最新の回復力は、組織が最も必要とする時に、アプリケーション、データ、管理、そして信頼をリストアすることで、アプリケーションエコシステム全体を保護します。

効果的な回復力ソリューションの重要な基準

自動リストア
復元には再現性があり、検証済みで、あらかじめ組み込まれています（インシデント発生時に初めて行われるものではない）。

クリーンで一貫性のあるデータ
データ、ポリシー、メタデータ、設定、依存関係を一括して保護します。

ポリシーガードレールの適用
ポリシーガードレールは、すべてのクラスター、クラウド、アプリケーションタイプでワークロードの一貫性を維持します。

アプリケーション継続性
手動で再構築するのではなく、アプリケーション全体とその運用状態を復元します。

コンプライアンス検証
監査可能なコンプライアンスは、ポリシーが適用されていることと、復元が想定ではなく確実に繰り返し実施できることを証明します。

確実な運用
信頼と確信を築きます。インシデントが発生する前に、何が保護され、何がリスクにさらされ、何が復元可能かを把握できます。

最新のアプリケーションには最新の回復力が求められる

Veeam Kastenによって最新アプリを簡素化、保護、合理化する方法をご紹介します。複雑さを解消し、リスクを最小限に抑えて、ビジネス継続性の維持に向けてあらゆる事態に備えましょう。

もっと深く探ってみませんか？「最新のアプリケーションがネイティブの保護を必要とする理由」**ebook**をご覧になり、最新のアプリケーションが障害を起こした際に、ネイティブの保護によって、完全な復元に必要なデータ、コンテキスト、ポリシー、依存関係がどのように保護されるかをご確認ください。

KASTENを試す　　EBOOKをダウンロード

© 2026 Veeam Software。機密情報。複製不許可。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。