

Acronis



ホワイトペーパー

**ダウンタイムのコストを削減:**

製造業IT部門がデータ保護の問題を解決する10の方法

新しいAcronisはクラス最高のデータ保護を製造業に提供

## ダウンタイムのコスト

業界を問わずダウンタイムのコストは非常に高くなる場合があります。しかし、製造部門の組織にとっては、ダウンタイムが何百、何千もの従業員に悪影響を及ぼすため、ダウンタイムのコストが壊滅的になることがあります。

**Aberdeenの最近の調査によると、製造セクターにおけるダウンタイムの平均コストは時間当たり\$260,000です。<sup>1</sup>**

予期せぬダウンタイムによって金銭的被害が出るだけでなく、顧客への納品が遅れたり、サプライチェーン全体に壊滅的影響を与えたりします。ダウンタイムが発生した場合、組織は障害が発生したシステムを回復し、迅速に稼働させるために、できることはなんでも実施する必要があります。

完全復元とは停止前とまったく同じ状態で工場が再稼働することを意味します。機器の修理、サイバー攻撃からの修復、またはダウンタイムの原因となった障害の修復は復元プロセスのほんの一部にすぎません。より複雑で、より困難な作業となるのは、障害を起こしたアプリケーションサーバーや仮想マシン、クラウドワークロード、エンドポイントを正確かつ完全に復元することです。強力なデータ保護ソリューションが配置されていないと、バックアップから確実に復元を実施するのに、実際の障害を修復するより時間がかかる可能性があります。

コストの高い製造業のダウンタイムには、高速で信頼性が高く、管理の容易なバックアップ&リカバリソリューションが必要です。これには、ダウンタイムのコストを考慮してビジネス上意味のあるバックアップ計画の作成と維持が含まれており、

また、このコストには目標復旧時点 (RPO、停止が発生した場合にオペレーションで合理的に損失を許容できるデータ量の尺度)、および目標復旧時間 (RTO、オペレーションがどれくらいの時間合理的にオフラインでいられるかの尺度) も含まれます。

ダウンタイムに対し、非常に敏感な製造環境ではバックアップからの復元は高速であるばかりでなく、完全に正確でなければなりません。しかし、そのようなソリューションはほとんどありません。

**Kroll Ontrack Researchの調査によれば、ITマネージャーの75%はバックアップから損失データを復元できないことが判明しています。<sup>2</sup>**

製造データへのアクセスが阻害されるばかりでなく、バックアップファイルを破壊するランサムウェアのようなマルウェアの蔓延により問題は悪化しており、それに応じてデータ損失やダウンタイム、そしてコストが増大しています。

**このようなデータ損失は製造業にとっては大惨事です。**

製造システムへのITの関与が制限されると、データ保護のような不可欠な管理作業がたやすく見逃されてしまいます。さらに、多くのデジタル製造システムは古い、もしくは独自環境であるなど、普通でないソフトウェア環境で実行されているため、比較的旧式のオペレーティングシステム、アプリケーション、データフォーマットのみを保護できるITツールを使ってのデータ保護はより困難になります。

<sup>1</sup>「製造でのダウンタイム: 原因、影響、リスク軽減」 BlackBerry AtHoc、2018年8月

<sup>2</sup>「Kroll Ontrack Research: 企業の3分の1がデータ損失を経験」 Kroll Ontrack 著、2018年3月

## Acronis、クラス最高のデータ保護を製造業に提供

データの保護には数多くのオプションがあります。しかし、ITスタッフの数が限られている場合やITスタッフがいない環境で、高速復元が強く求められる製造環境では、Acronis Backupが活躍します。この製品は従来のデータセンター、エッジ環境を保護するために必要な信頼性とデータ整合性を提供し、また製造セクター固有のニーズに対応します。さらに、Acronis Backupは専門家でもなくとも管理でき、特別トレーニングや専門スタッフは必要ありません。また、Acronisは、あらゆる機能を備えた包括的なソリューションも提供し、1つのソリューションで広範な製造向けITシステムを保護します。

すぐれた操作性がAcronis Backupの大きな利点であり、シンプルかつ柔軟にバックアップを作成し、組織内のあらゆるデバイスに対応します。バックアップはローカル、リモートストレージ、クラウドのいずれかに保存できます。ローカルデータのバックアップはダウンタイムからの復元をスピードアップするのに便利です。25言語をサポートしているため、オフショア従業員が母国語で業務を行うことができ、翻訳の問題は発生しません。

### 製造データを保護する10の重要な機能

製造環境においてデータ保護の最適ソリューションを提供するために、Acronis Backupは以下に示す10の重要な機能を備えています。

- 1. 高速データ復元**— Acronis Instant Restore技術を統合することで、Acronis Backupのユーザーはどのようなサーバーでも（物理、仮想、クラウドプラットフォームを問わず）、新たに作成した仮想マシンとしてライブで復元できるようになり、業界最短の目標復旧時間（RTO）を実現します。例えば、WindowsまたはLinuxの物理マシンをバックアップし、VMwareまたはHyper-Vの仮想マシン（VM）として秒単位で瞬時にリストアできます。
- 2. 計画およびオンデマンドのバックアップ**— Acronis管理コンソールを使えば、いつでも必要な時に手動バックアップを高速かつシンプルに起動します。またバックアップ計画を作成してその実行を繰り返すこともできます。さらに、企業ネットワークから切断されたマシンのバックアップを柔軟に設定できるようになります。

このような機能によって、バックアッププロセスを管理するIT運用の負担を大幅に削減し、熟練したスタッフが戦略的なプロジェクトや他の主要タスクに専念できるようになります。

- 3. 独自で旧式のサーバー環境に対するサポート**— 多くの製造ITシステム（例えば、プロセスコントロールシステムや製造ライン管理アプリケーションなど）は高度にカスタマイズされており、しばしば旧式のハードウェアやオペレーティングシステムバージョンで実行されています。このようなシステムを安定した状態で稼働させることが重要であり、パッチや最新バージョンへのアップグレードはできません。Acronis Backupのイメージベースのバックアップとベアメタル復元によって、これらのシステムを完全に保護し、どのようなシステム障害が発生しても復元できるようにします。
- 4. 蔓延しているマルウェア攻撃に対する積極的な防御**— 製造セクターは最も頻繁に、かつ被害額も大きなマルウェア攻撃の標的になっており、脆弱性やパッチ管理よりもシステムの安定を優先するため、多くの製造ITシステムはランサムウェアやクリプトジャッキング攻撃といった様々なサイバー脅威にさらされています。Acronis Active Protection技術をビルトインしているAcronis Backupは人工知能と機械学習を使用して、ランサムウェア攻撃の損害を検出・終了・復元するだけでなく、リソースを消耗するクリプトジャッキング攻撃を検出・終了します。
- 5. バックアップの強化**— 最新のマルウェアの多く、特にランサムウェアは、本番サーバーに侵入するためだけでなく、バックアップエージェントやマルウェアからの復元に必要なバックアップアーカイブに損害を与えたり、破壊したりすることを意図しています。その戦術は効果的です：被害に遭った企業に利用できる最新バックアップがない場合、データをアンロックするために必要な復号化キーの代金を犯人に支払う確率が高くなります。Acronis Backupエージェント、バックアップアーカイブ、クラウドインフラはこのような種類のマルウェア攻撃を防護するために特に強化されており、本番システムへの攻撃から確実に復元できるようになっています。

**6. フルイメージバックアップ** — Acronis Backupは真のイメージベースのバックアップを提供し、ストレージ媒体全体のブロック単位のコピーを作成し、ソースシステムのもっとも完全な保護を実現しています。このアプローチによって、必要に応じて新しいハードウェアに移行でき、本番モードに戻る前に、オペレーティングシステムやアプリケーション、構成ファイルの再インストールを省き、復元時間を最短にすることができます。

**7. ホスト外でのバックアップ管理** — 厳しいRPOやRTOに対する製造業界のニーズは旧式のハードウェアで稼働する古いサーバーにとっては処理上の問題になる場合があります。このような旧式のシステムは主要な機能を果たしながら、バックアップを同時に実行するのが困難である可能性があるため、バックアップウィンドウを逃したり、失敗した場合に非常に高額な代償を支払うことになるデータ保護のすき間につながります。Acronis Backupはバックアップレプリケーションや他のマシンへの保持ポリシー適用のようなバックアップ管理プロセスの負担を軽減し、本番システムの貴重なCPUサイクルやメモリを節約します。結果的に短い時間でバックアップサイクルを完了し、データ保護のすき間を解消することができます。

**8. ベアメタル復元** — 製造ダウンタイムによって生じる高いコストを考慮し、本番サーバー停止からの復元をスピードアップできる機能が強く評価されるようになります。これを実現するひとつの方法はバックアップから「ベアメタル」システム（オペレーティングシステムや他のソフトウェアがインストールまたは構成されていないサーバー）に復元することです。Acronis Backupによって、ソースシステムのオペレーティングシステム、アプリケーション、構成設定およびデータを含めて障害の発生したサーバーをベアメタルターゲットに一回の高速オペレーションで復元できるようになります。これによって、本番ステータスに戻る前にコストが高く、時間のかかる再インストールプロセスと再構

成プロセスを回避できます。また、マルウェア攻撃から迅速に復元する確実な方法を実現します。すなわち、攻撃前に作成したクリーンなイメージを使って侵入されたシステムを復元するだけです。

**9. 異なるハードウェアへの復元** — 生産停止を短縮するもうひとつの方法は、たまたま手元にある、しかも基本的なパフォーマンス仕様を満たす新しいハードウェアに、障害が発生したサーバーを復元することです。しかし、異なるハードウェアにバックアップイメージを復元すると、新しいハードウェアとソースイメージに互換性がない場合（通常、ブートメディア、ストレージコントローラー、ネットワークインターフェース）、ブート障害の原因になることがあります。

Acronis Universal RestoreはAcronis Backupに統合された別の技術であり、必要なブートイメージ、ストレージドライバ、ネットワークドライバを自動的に挿入することで、復元プロセス中に互換性の問題を解決します。これによって、さらなる構成や他のオペレーターへの介入なしに、ソースシステムのイメージが新しいハードウェアで迅速かつ自動的に実行できるようになります。

**10. 仮想環境のサポート** — 大半の製造環境は今や物理サーバーはもちろんオンプレミス、プライベートクラウド、パブリッククラウドサービスで実行されるVMを使用しています。製造業では、このような異なるプラットフォームをすべて保護する必要があります。しかし、ワークロードをプラットフォームタイプ間で移動できることによって（例えば、物理サーバーをVMに復元、超高速に本番稼働に戻す、またはVMサーバーイメージをパブリッククラウドサービスに移行してディザスタリカバリを達成するなど）、パフォーマンスとアップタイムで顕著な利点があります。

Acronis Backupによって物理、仮想、クラウドプラットフォームの完全な保護が可能になり、簡単、高速、確実に実施できるようになります。

## まとめ

製造環境での計画外のダウンタイムはビジネスの利益、顧客関係、企業評価、システム保護に携わるITプロフェッショナルのキャリアなどに対する脅威です。製造業のIT環境には妥協できない特別の要件があります。これには特殊プロセス制御サーバーのように古くなったレガシーシステムの保護、多大な損害をもたらすダウンタイム、マルウェア脅威の増加、停止からの高速で効率的な復元などが該当します。このような要件があることから、データ保護ベンダーが克服できない問題が生じることも多々あります。

Acronis Backupは高度で統合されたデータ保護のアプローチを提供しており、製造業がIT運用を確実に実行するために必要なパフォーマンス、広範なプラットフォームサポート、優れた操作性を提供しています。

詳細については、[www.acronis.com/business](http://www.acronis.com/business)をご覧ください。



Acronis  
バック  
アップ

今すぐ  
試用

