Petri IT Knowledgebase Resource
BWW Media Groupブランド

Petri IT Knowledgebase

製造業の可用性について7つの主要な問題を解決

提供:
Acronis

目次

工場のフロアで実行されている様々な処理は製造ビジネスに不可欠で、ダウンタイムが発生すれば、ただちに生産性や収益の損失につながります。プロセスコントロールサーバーをはじめとする重要な製造アプリケーションを保護し、高可用性を維持することが常に重要です。

こうした高可用性へのニーズは製造業界に固有なIT問題ももたらします。例えば、アプリケーションは通常、個々のプロセスに高度に専門化されていますが、多くの場合、Windows XPのような古いオペレーティングシステムで実行されています。ソフトウェアはほとんどの場合、非常に安定しており、ほとんど（皆無ではないにしても）アップデートされません。

このホワイトペーパーでは、製造業でのダウンタイムのコストについて解説し、アップタイムを維持する際の主要な問題を調べ、製造ITインフラをサポートするデータ保護ソリューションを考察します。

製造業のダウンタイムの代償は高くつく

製造業界は、信頼性の高い持続的な生産プロセスに依存しているため、ダウンタイムの一分一分が高くつきます。そうだとしても、ダウンタイムはこのセクターでは珍しい出来事ではありません。業界研究によると、ほとんどすべての工場で、少なくとも5パーセントの生産能力がダウンタイムのせいで失われており、最大で20パーセントを失うケースも多いと言います。

> 平均的な製造業は年間最大800時間を費やしてダウンタイムに対応しています。

Aberdeen Researchによれば、過去3年間に82パーセントの企業が計画外のダウンタイムを経験しています。また、Arimoの調査によると、製造業は平均するとダウンタイムの対応に年間最大800時間を費やしています。工場のダウンタイムは複数の重要分野でビジネスに悪影響を及ぼしています：

- **生産の損失** – 信頼性の高い製造プロセスは収益に直結します。生産時間を失うとビジネスの業績に直接影響を及ぼし、収益が減少します。

- **生産能力の損失** – 工場のダウンタイムは全体的な生産高を減少させます。

- **直接労務費の増加** – 直接固定労務費は工場が稼働していてもいなくても変わりません。ダウンタイムによって、製造した製品当たりの労務費が増加します。

- **風評被害** – ダウンタイムによって受注処理と製品納品が減少するため、顧客関係に損害を与え、企業ブランドと評価が低下します。

- **サイバー攻撃による財務上の損失** – ダウンタイムの原因になるばかりでなく、ランサムウェアのような標的型サイバー攻撃によって企業は重要なサービスを復元するために、サイバー犯罪者に支払いを行わざるを得なくなり、会社の評判を下げます。

最近公開されたAberdeenのレポートでは、計画外のダウンタイムがセクター全体で年間500億ドルの損害を引き起こし、システム障害が停止の42%を占めていると推定しています。Aberdeenによると、「計画外のダウンタイムによるコストは壊滅的になる可能性があり、工場では時間当たり$10,000～$260,000の範囲と推定されています」

企業によってはこれらのレポートを知っていたり、または直接影響を受けたりしているかもしれませんが、信頼性を高めようとする取組みにもいくつかの課題があるため、様々な課題に対処しなければなりません。しかしながら、幸いにも、信頼性を高めるだけでなく、容易で効率的に達成できるソリューションがあります。

1 レガシーデータの保護ソリューションは動作が遅く、複雑で不十分

工場フロアへのIT配備には通常、個別の専門タスクを実行する複数のサーバーが含まれ、サーバーごとにバックアップを実行します。アプリケーションの多くはWindows XPのような古いオペレーティングシステムで実行されます。複数のバックアップにより複雑さが増して手動介入が増えるため、復元にかかる時間が長くなります。

ソリューション

集中管理コンソールへのネットワークアクセスの有無を問わず、プラットフォーム（物理、仮想、クラウド）、オペレーティングシステム、アプリケーションのワークロードをサポートする保護ソリューションを選定すること。IT部門以外の人にもわかりやすく直観的な管理インターフェースを備え、高度に自動化されたバックアップ計画を作成できるソリューションを選択すること。

> "...ダウンタイムによるコストは膨大になる可能性があり、工場では時間当たり$10,000～$260,000の範囲と推定されています。"

2 ランサムウェア、クリプトジャッキングマルウェアによるパフォーマンスへの影響を排除

ランサムウェアは製造セクターに蔓延しているマルウェアで、標的になるサーバーのファイルを暗号化し、ファイルのロックを解除してサービスを回復するのと引き換えに身代金（ランサム）を要求します。ランサムウェアには多くの変種があり、バックアップサーバーなどの他の標的にネットワークを通じて蔓延するワームコンポーネントが含まれます。

例えば、2019年にノルウェーのアルミニウム製造企業Norsk Hydro社は、ランサムウェア攻撃によって社内ネットワークをシャットダウンせざるを得なくなりました。これはこの会社に限ったことではありません。- NTT Securityによる2019年グローバル脅威インテリジェンスレポートによれば、製造業はサイバー犯罪攻撃における最大の標的のひとつです。

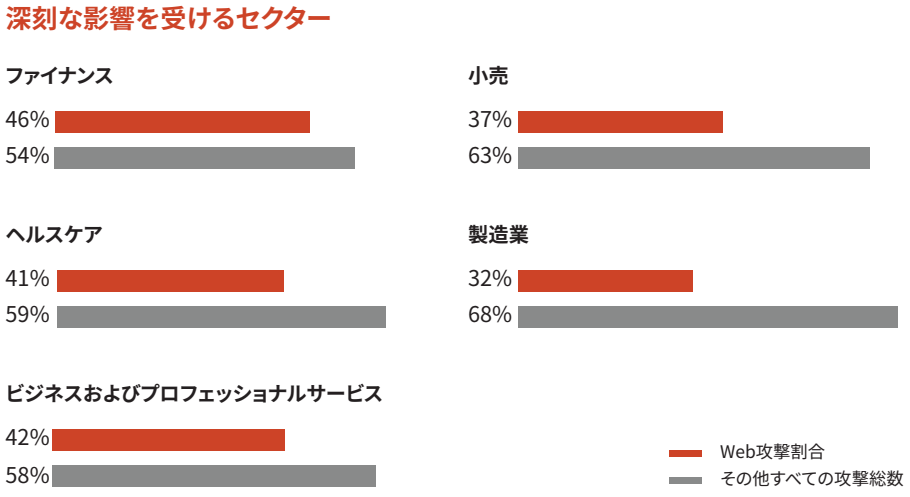

図1 - 業界別の脅威による影響度

クリプトジャッキングは蔓延している別のマルウェア脅威で、IBMの2019年X-Force 脅威インテリジェンスインデックスによると2018年には450%増加しています。クリプトジャッキングマルウェアに感染したサーバーとワークステーションは、サイバー犯罪者に乗っ取られることで、ひそかに暗号通貨のマイニングためにシステムリソース（CPU、メモリ、電力、冷却システム）を勝手に利用されてしまいます。そのためシステムパフォーマンスと可用性が低下しハードウェアの動作寿命が短縮され、電力とHVAC（空調システム）のコストが増加します。

ソリューション

人工知能や機械学習に基づくいないマルウェア対策機能を備えたデータ保護ソリューションを配備する。このような高度な技術は、ランサムウェア（ゼロデイ攻撃含む）やクリプトジャッキングのように優先順位の高い脅威を識別し、停止させるために活用できます。

3 工場には熟練したITサポートスタッフがいない

Enterprise Strategy Group 2018 調査は、調査に応じた企業の26%が組織内のITスキル不足によって悪影響を受ける領域として、バックアップと復元を挙げています：製造業も例外ではありません。ITスキルが不十分な工場エンジニアは、バックアップから障害の発生したITシステムを復元する際、手順書に頼らざるを得ません。

データ保護ソリューションを配備する...これにより、ボタンを押すだけで工場環境全体のバックアップと復元が可能に

ソリューション

管理者やスタッフがプッシュボタンを押すだけで工場IT環境全体をバックアップしたり、復元したりできる自動化機能を備えた操作の容易なデータ保護ソリューションを配備すること。

4 製造環境には古くなったオペレーティングシステムとアプリケーションがある

製造アプリケーションの多くは古くても安定稼働するものが好まれます。ほとんどアップデートされず、多くの場合旧式のハードウェアやオペレーティングシステムで実行されています。ARC Advisory Groupsは、「現在のオートメーションシステムのインストールベースの大半は少なくとも20年経過しており、適切なメンテナンスを行うのがますます困難で、コストがかかるようになっています」と報告しています。Enterprise Strategy Groupによる2018年の調査によると、31パーセントの企業がデータバックアップと復元の更新に最も多く投資する計画であることが判明しました。

新しいバージョンのOSのインストールしない、またはパッチを適用しない場合、それはセキュリティ脆弱性の原因になります。

アプリケーションおよびそれを支えるOSとハードウェアを安定した状態に保とうとすると、データ保護が複雑になります。
新しいバージョンのOSのインストールしない、またはパッチを適用しないことは、セキュリティ脆弱性の原因になり、さまざまなマルウェア攻撃にさらされる可能性があります。

ソリューション

物理、仮想、クラウドなどどのようなプラットフォームでもオペレーションシステムやアプリケーションワークロードを問わず、また必要に応じて異なるハードウェアにでも復元できるデータ保護ソリューションを配備すること。

5 動作の遅いデータ保護は手間がかる上に不完全なバックアップ対策になりがち

製造業で使用されるレガシーデータの保護ソリューションには通常、広範な手動介入と膨大な工数が必要です。システムの停止が長引けば、それによって生産時間が低下し、直接労務費が増加します。動作の遅い、労働集約型のバックアップ操作だとバックアップサイクルを逃したり、データ保護にギャップが生じたりします。組織がシステム障害に遭遇する場合、復元プロセスが複雑で、マルチステップで、エラーが生じやすく、潜在的なデータギャップに悩まされるようになります。

ソリューション

組織の目標復旧時間と目標復旧時点を達成できる速さで、さらに自動スケジュールされるバックアップ計画と高速復元操作に対応できる高性能のデータ保護ソリューションを配備する。

6 バックアップからの復元では遅すぎる

Infoneticsの調査によると、ほとんどの企業は平均すると月2回停止を経験し、1回の停止が約6時間続きます。その一方で、Industry Weekは、従来のバックアップからのデータ復元では時間がかかり、手動プロセスが多く終了までに数時間から数日かかると報告しています。

障害の発生したシステムを、時間単位ではなく分単位で復元でき、さらにベアメタルと復元オペレーションを実行できる高性能データ保護ソリューションを実現することができます。

問題を診断してシステムの復元が必要かどうかを決定するのに時間がかかる可能性がありますが、最も重要なのは復元プロセス自体に時間がかかることです。復元プロセスに時間が掛かると、ダウンタイムが延びることになります。旧式のバックアップと復元の技術だと障害の発生した1つのシステムを復元するのに何時間もかかる可能性があります。

ソリューション

障害の発生したシステムを、ベアメタルおよび自動復元操作を実行する機能も含めて、バックアップから迅速に（理想的には時間単位ではなく、数分単位で）復元できる高性能データ保護ソリューションを配備すること。

7 バックアップオペレーションが遅すぎてバックアップウィンドウに納まらない

工場環境では、バックアップオペレーションを実行する適切な時間を探すのに苦労する場合が見受けられます。それは、生産システムの多くが24時間年中無休で稼働しているため、バックアップのための時間を確保したり、スケジュールを立てるのが難しいためです。このような生産環境では、システムの稼働状態について厳しく管理されており、コンピューティングリソースが限定されていることがよくあります。バックアップ処理が遅い場合、予定される終了時間までにバックアップ処理が終わらないことがあります。
こうした場合、バックアップがきちんとできない場合もあり、その際には次のバックアップ処理時にバックアップ対象となるデータが増え、さらにバックアップ処理時間が掛かるという悪循環に陥るケースに至ります。バックアップウィンドウ内にバックアップ処理が納まらないことでデータ保護がきちんと実施できない可能性があります。

ソリューション

割り当てられたバックアップウィンドウ内でバックアップ処理を完了できるような処理速度で、なおかつサーバーの処理性能に悪影響を与えず、バックアップ処理以外の生産アプリケーションを継続的に稼働させることができ、さらには、必要に応じてバックアップのオーバーヘッドを補助サーバーや仮想マシンに負荷移動できるようなデータ保護ソリューションを配備すること。データ量とバックアップ実行時間を減少させるために、ソリューションは差分バックアップと増分バックアップもサポートする必要があります。

アクロニスは製造データ保護の問題を解決します

アクロニスは、製造セクターにデータ保護製品とサービスを提供するトッププロバイダーです。アクロニスのフラッグシップソリューションであるAcronis Backupは、広範なプラットフォームサポート、信頼性、単純性を統合して製造ITインフラ向けに完全なデータ保護を提供します。

この製品は世界中で50万社以上の企業に採用されており、Windows XPやLinux、Mac、Windows 7、Windows 8、Windows 10、Windows Serverはもちろん、VMware、vSphere、Microsoft Hyper-V、Red Hat Virtualization、Oracle VM Serverといった21種類以上のプラットフォームに操作が容易で、効率的でセキュアなバックアップを提供します。また、障害の発生したシステムをベアメタル物理サーバーのような異なるハードウェアならびに仮想環境やクラウド環境に復元できます。

Acronis Backupは、製造業界の問題に対応するために複数の機能を備えています。Acronis Instant Restoreは、数分以内にバックアップから完全なシステムを迅速に復元することで、ダウンタイムを減少させます。さらにAcronis Backupに搭載されているのAcronis Active Protectionは、ランサムウェアやクリプトジャッキングのような優先順位の高いマルウェア脅威を検出・遮断し、シグネチャベースのアンチウイルスソリューションを補完するAIベースのマルウェア対策防御を提供します。

ケーススタディ：Marquardt Group、Acornisを使用して高速復元を実現

Marquardt Groupは、電気機械式スイッチ、電子式スイッチ、およびスイッチングシステムのトップメーカーで、米国、中国、インドを含め、4大陸、19ヵ所で製造を行っています。Marquardt Groupにとって、データ損失やシステム障害が発生すると生産遅延や納品ボトルネックにつながる可能性がある、製造システムの可用性を確保・維持することが最重要課題です。生産データを迅速に使用し、復元時間を短縮することが非常に重要です。

> **"Acronis Backupはセキュアで簡単で高速なバックアップであり、当社を前進させてくれ..."**
>
> **Marquardt システム管理者Catalin Dragoman氏**

Marquardtのデータ保護にかかる負荷は、さまざまなオペレーティングシステム上の1600エンドポイントで実行される40テラバイトのデータです。同社は迅速かつ確実にさまざまなシステムのバックアップと復元を行えることからAcronis Backupをデータ保護に選択しました。また、Acronis Backupは実装と使用が簡単で、システムとネットワークのリソース消費が少なく、必要に応じてシステム全体または個別ファイルを復元できます。

Marquardtのシステム管理者であるCatalin Dragoman氏は、「Acronis Backupはセキュアで、簡単に使える高速なバックアップ製品です。当社の生産システムの可用性を大幅に改善し、当社を前進させてくれました。」と述べています。Marquardt Groupがどのようにacronis Backupを活用し、その重要な製造データをどのように保護しているのかについては、こちらをご覧ください。

ケーススタディ：欧州の自動車メーカーのトップ企業がアクロニスを使用してプロセスコントロールの復元を改善

ある大手欧州自動車メーカーは、自社のバックアップ、復元、およびデータ保護の機能を強化しようと考え、Acronis Backupを導入しました。

以前のソリューションでは、この自動車メーカーは30～60分の範囲でシステムの復元を行っていましたが、そのプロセスは時間のかかる処理であり、さまざまな手動操作が必要でした。各工場には平均して100種類のコントロールシステムがあり、復元するには年間数千時間もの工数が必要でした。生産ラインのメンテナンスウィンドウも時間がかかったため、システムバックアップが完了できなかったケースが数多くありました。Marquardtも増え続けるランサムウェアの脅威から生産プロセスを守りたいと考えていました。

そのため、この自動車メーカーはAcronis Backupを導入、バックアップエージェントを経由して生産オペレーションを中断することなく、すべてのシステムのバックアップを以前の半分の時間で実行できるようになりました。Acronis Backupは自動バックアップを提供し、障害が発生した場合に、IT部門に通知を出します。スペシャリストは数分以内に障害が発生したシステムを復元し、リブートして生産ラインを再稼働させます。プロセスコントロールサーバーがすぐに修理できないほどの損害を受けている場合、Acronis Universal Restoreを使って、新たに交換したサーバーまたは異なるハードウェア構成に復元できます。一方、Acronis Backup に搭載されているAcronis Active Protectionは、最新のパッチが適用されていないシステムに対してもランサムウェア攻撃を自動的に検出・遮断することができます。

Acronis

欧州の主要自動車メーカーで、アクロニスがプロセスコントロールの復元を改善した方法ついての詳細はこちらをご覧ください。

Acronis Backupの詳細と30日間無償試用版のダウンロードは www.acronis.com/businessをご覧ください。