

運用技術(OT)環境の稼働率向上

OT システムの停止に伴う多額のコスト

運用技術 (OT) システムは、安定的なオペレーションにより企業の事業継続を支えます。ひとたび OT システムが停止すれば、生産ライン、パイプライン、電力系統、サプライチェーンまでが機能不全に陥る可能性があります。その結果発生する障害に関わるコストは、1 時間あたり数万ドルから数十万ドルに上ることもあります。ABB の調査によると、最近、企業の 69% が 月に 1 回はダウンタイムを経験しており、障害による損失は 1 時間あたり 15 万ドルに上っています[1]。OT のダウンタイムが及ぼす他の影響として、以下が挙げられます。

- 納期遅延、リードタイムの長期化に伴う販売機会の損失。
- 製造工数の増加。
- 納期遅延や不履行による顧客との信頼関係の悪化やブランドイメージの低下。
- 投資家からの信頼失墜による企業価値の低下。
- サービスレベル契約やその他の契約不履行による制裁金。
- サイバーレジリエンスの規制要件の未遵守やコンプライアンス違反による罰金や刑事罰。

上記の通り、サイバー攻撃、自然災害、ハードウェア障害、ソフトウェア不具合、人為的なミスなどから OT システムを守ること、また、これらの障害が発生した場合に、システムを速やかに復旧させることが重要になります。

自動車、エネルギー、電力、製薬、物流など、多くの業界がリアルタイムの生産プロセスにおいて、オートメーション化を進めています。オートメーション技術の多くは、Windows や Linux を搭載した PC によって制御、設定、監視されており、 OT (運用技術) 、ICS (産業制御システム) 、サイバーフィジカルインフラなどのカテゴリーに分類されます。一般的な OT アプリケーションには、監視制御およびデータ収集 (SCADA) システム、分散制御システム (DCS) 、ヒューマンマシンインターフェース (HMI) 、およびリアルタイムプロセスデータを取得する運用履歴システムが含まれます。

[1] ABB。「信頼の価値: ABB 調査レポート 2023 」

Copyright © 2003-2026 Acronis International GmbH.

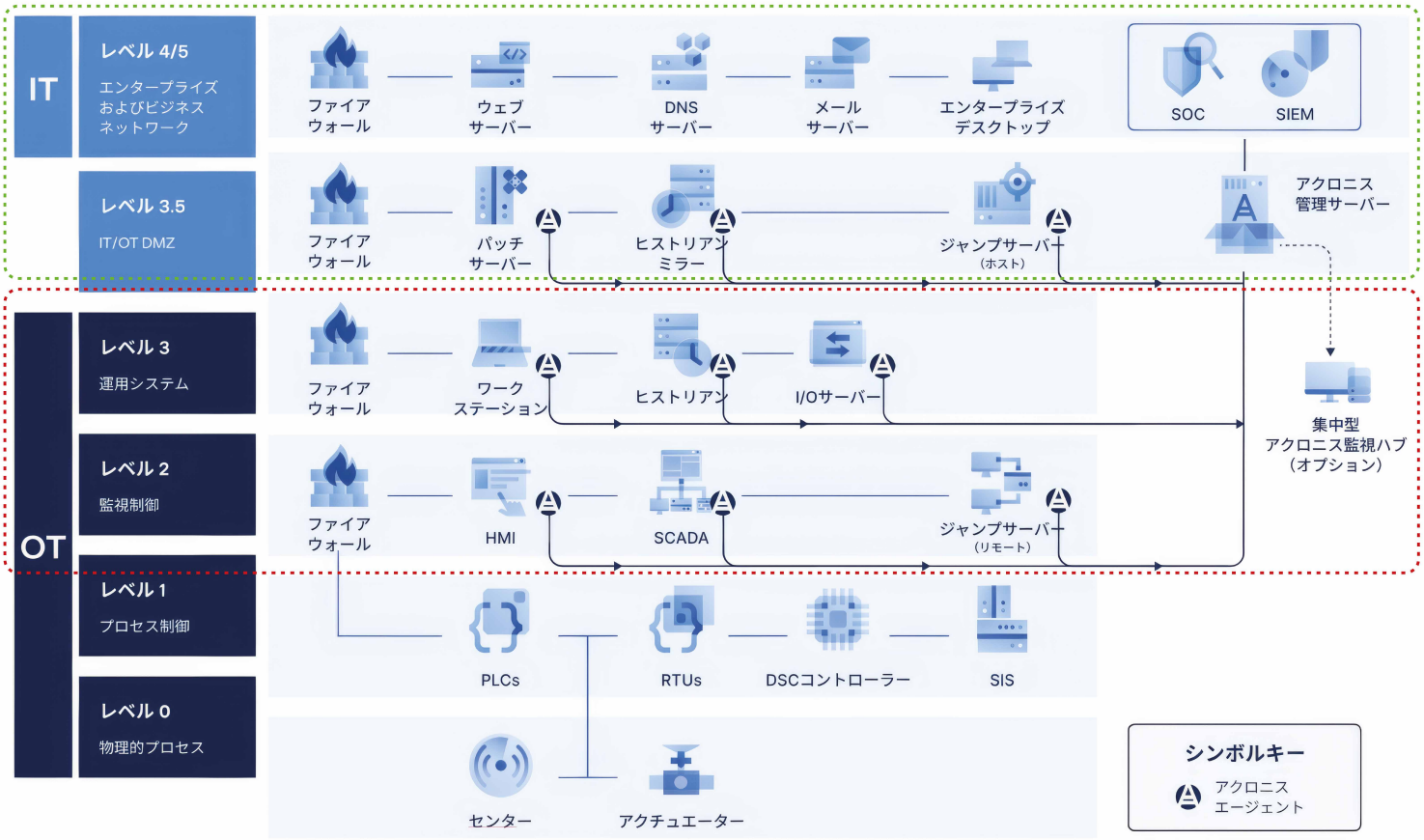
OT システムの稼働率を維持するための課題

OT 環境には、従来のバックオフィスやフロントオフィスの IT システムと比較して、安定稼働を維持するのが難しい特殊な事情があるため、ダウンタイムを最小限に抑えなければならないというプレッシャーにさらされています。

- 多くの OT システムは、何年も前のハードウェアと OS で稼働しており、中には Windows XP 時代にまで遡るシステムもあります。新しいハードウェアや OS リビジョンにアップグレードすると、OT アプリケーションの機能に障害が起きたり、制限されたりするリスクが発生します。
- システムの老朽化が、エンドポイント検出と応答（EDR）などの最新のサイバーセキュリティ対策の導入を難しくしたり、不可能にする要因となっています。
- Microsoft が 2014 年 4 月に Windows XP のサポートを終了したように、OS ベンダーが特定の製品バージョンのサポート終了日を発表すると、主要なバックアップベンダーは通常、そのバージョンのサポートを 5 年以内に終了します。主要なバックアップベンダーのサポートを得られらくなると、OT エンジニアは時間がかかりエラーが発生しやすい手動のバックアッププロセスに頼ることになります。このプロセスの実行には、コストのかかる計画的ダウンタイムが必要になります。
- OT システムが設置されている施設は、現地の IT サポートがほとんどなく、多くの場合、中央の IT チームから離れた場所にあります。さらに、OT 環境はサイバーセキュリティのリスクを低減するために、エアギャップ環境になっていることが多いため、IT チームは、リモート監視および管理ツールを使用することができません。IT スタッフを物理的に製造施設に派遣するには、時間とコストがかかり、障害が長期化して費用がかさむ恐れがあります。

アクロニスは、OT 環境特有のサイバーレジリエンス要件に対応

Acronis Cyber Protect は、製造業をはじめとするさまざまな現場で、工場設備や生産ラインを支える制御システム（OT）の保護に活用されています。



SIEM/SOCとの連携による監視の一元化: バックアップ、セキュリティ、遠隔監視・運用管理（RMM）に関するアラートやイベント情報を、syslog やファイル出力を通じて他社の SIEM（ログ監視基盤）と連携させられます。これにより、工場設備や制御システム（OT）を含む環境全体をまとめて監視でき、異常の早期発見や迅速な対応に役立ちます。

Copyright © 2003-2026 Acronis International GmbH.

Acronis Cyber Protect は、OT システムのバックアップとリカバリを提供し、高い稼働率を要求される生産環境に必要な機能を提供しています。主な機能は以下のとおりです。

- OT システムをオフラインにしたり再起動したりすることなく、Acronis Cyber Protect エージェントをインストールしてバックアップを実行できます。
- 高速で信頼性が高く、完全に自動化されたバックアップを実行することで、OT システムのバックアップ処理とストレージのオーバーヘッドが軽減されます。
- データ保護計画により、システムやサイト全体でバックアップを標準化（またはカスタマイズ）できます。
- EDR、マルウェア対策、ランサムウェア対策など、同じ Acronis エージェントを使用するサイバーセキュリティ機能のオプションが提供されます。

アクロニスはレガシーOSも保護

アクロニスは、XP 時代から現在に至るあらゆる OS を保護することで、OT 環境の安定化を図ります（他のベンダーによって長期間サポートされていない OS も含まれます）。これにより、古いレガシーシステムでも高速かつ信頼性の高いリカバリを実現できます。必要に応じて、ベアメタルリカバリと呼ばれるプロセスにより、システムを新しい PC ハードウェアにレプリケーションするオプションもあります。この機能により、新しいハードウェア上で OS と OT アプリケーションを正常に実行するために必要な新しいドライバが自動的にインストールされます。Windows XP 世代から最新環境まで、さまざまな OS やハイパーバイザーに対応しています。
とくに、工場設備や制御システム（OT）で利用されることの多い Windows および Linux を幅広くサポートしています。

業界屈指のカバレッジで多様なOSとハイパーバイザーをサポート

Windows
- Windows Server 2003 SP1/R2 以降、2008、2008 R2、2012/2012 R2、2016、2019、2022（Nano Server を除く）
- Windows Small Business Server 2003/2003 R2、2008、2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows XP Professional SP1、SP2、SP3
- Windows 7、8/8.1、10, 11（Windows RT を除くすべてのエディション）

Microsoft SQL Server
2022、2019、2017、2016、2014、2012、2008 R2、2008、2005

Microsoft Exchange Server
2019、2016、2013、2010、2007

ハイパーバイザー

VMware vSphere
4.1、5.0、5.1、5.5、6.0、6.5、6.7、7.0、8.0

Microsoft Hyper-V Server
2022、2019、2016、2012/2012 R2、2008/2008 R2

Citrix XenServer/Citrix Hypervisor
8.2〜4.1.5

Linux KVM
8〜7.6

Scale Computing Hypercore
8.8、8.9、9.0

Red Hat Enterprise Virtualization（RHEV）
3.6〜2.2

Red Hat Virtualization
4.0、4.1、4.2、4.3、4.4

Virtuozzo
7.0.14〜6.0.10

Virtuozzo Infrastructure Platform
3.5

Nutanix Acropolis Hypervisor（HV）
20160925.x 〜 20180425.x

MacOS
- **OS X** Mavericks 10.9、Yosemite 10.10、El Capitan 10.11
- **macOS** Sierra 10.12、High Sierra 10.13、Mojave 10.14、Catalina 10.15、Big Sur 11、Monterey 12、Ventura 13、Sonoma 14

Linux: カーネル 2.6.9〜5.19
- RHEL 4.x、5.x、6.x、7.x、8.x*、9.0*、9.1*、9.2*、9.3*
- Ubuntu 9.10 〜 23.04
- Fedora 11 〜 23
- SUSE Linux Enterprise Server 10、11、12、15
- Debian 4.x、5.x、6.x、7.0、7.2、7.4、7.7、8.0、8.8、8.11、9.0- 9.8、10.x、11.x
- CentOS 5.x、6.x、7.x、8.x*、Stream 8*、9*
- Oracle Linux 5.x、6.x、7.x、8.x*、9.0*、9.1*、9.2*、9.3*
- CloudLinux 5.x、6.x、7.x、8.x*
- ClearOS 5.x、6.x、7.x
- AlmaLinux 8.x*、9.0*、9.1*、9.2*、9.3*
- Rocky Linux 8.x*、9.0*、9.1*、9.2*、9.3*
- ALT Linux 7.0

アクロニスは IT スタッフのサポートなしで OT システムをリストア可能

アクロニスは、One-Click Recovery と呼ばれる独自機能を提供しています。これは、現場の IT スタッフが不在である、またはエアギャップ環境であるために、IT スタッフがリモート管理ツールを使用できない OT 環境において欠かせない機能です。Acronis One-Click Recovery により、IT スキルのレベルに関係なく、現場の作業者が数回のキー操作で、障害の発生した OT システムをローカルバックアップからリカバリできます。OT システムの障害を解決するために数時間または数日かかることもあり、IT スタッフが現場に派遣されるまでの時間も含めると、生産停止によるコストは膨れ上がりますが、これを数分に短縮することができます。この機能により、OT システムをローカルディスクバックアップまたは Acronis Cloud からリカバリし、Bitlocker 暗号化とリカバリパスワードによりバックアップを保護できます。

Copyright © 2003-2026 Acronis International GmbH.

アクロニスの OT システム保護ソリューションを、業界を代表するオートメーションベンダーが採用

ABB、Siemens、Honeywell をはじめとする主要な OT / ICS ベンダーでも、Acronis Cyber Protect がバックアップ基盤として採用され、自社ブランドまたは共同ブランドのサービスとして顧客へ提供されています。アクロニスのように、オートメーション業界との幅広い提携や支持を得ているデータ保護ベンダーは他にありません。

アクロニスのは OT サイバーレジリエンスのリーダーとして認知されています

Forrester Research、TAG Infosphere、Omdia などの大手テクノロジー調査会社が、アクロニスを OT システム保護のリーダーとして評価しています。

TAG Infosphere レポート 読む

Omdia レポート 読む

結論

Acronis Cyber Protect は、世界中の製造業や産業生産環境で OT システムを保護するために使用されています。XP 時代から現在に至る OS のデータ保護、非 IT 従業員によるOne-Click Recovery を使用した OT システムのリストア、主要な自動化ベンダーによる採用。こうした独自の強みの組み合わせが、OT サイバーレジリエンスのリーダーとしてアナリストコミュニティに高く評価される要因となっています。



関連記事

OT 向け Acronis Cyber Protect の詳細を知る

- アクロニスの製造業向けソリューション
- インフォグラフィック: One-Click Recovery で OT のアップタイムを維持
- 導入事例: タタスチール
- 導入事例: ABB
- 導入事例: Schaeffler
- 導入事例: BDR Pharma
- Acronis Cyber Protect の無償トライアルを試す
- OT サイバーレジリエンスの専門家と話す

Acronis

詳細は、www.acronis.com をご覧ください

Copyright © 2003-2026 Acronis International GmbH.無断複製禁止。Acronis および Acronis ロゴは、米国および/またはその他の国における Acronis International GmbH の商標です。その他の商標または登録商標はそれぞれの所有者に帰属します。事前の予告なく技術的な変更や図の変更が行われる場合があります。品質には万全を期していますが、誤りが含まれている場合があります。2026 年 7 月