医薬品製造工場の稼働率を向上

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、生産ラインの稼働維持や企業の収益確保に直結する重要な要素です。このシステムに障害が発生すると、製造ラインが停止し、その結果発生する損失は、製薬会社にとって 1 時間当たり数万ドルから数十万ドルに及ぶことがあります。ABB の調査によると、最近、企業の 69% が 月に 1 回のダウンタイムを経験しており、障害による損失は 1 時間当たり 15 万ドルに上っています[1]。OT が停止すると、他にも以下のような影響が生じます。

- 納期遅延、リードタイムの長期化に伴う販売機会の損失
- 製品単位当たりの直接労働費の増加
- 納期遅延や不履行による顧客との信頼関係やブランドイメージの毀損
- 安定した生産能力に対する投資家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

したがって、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必須になります。

製薬企業の研究設備や製造 OT システムの多くは、WindowsやLinux を搭載した PC によって制御・設定・監視が行われています。創薬ラボの OT システムには、高速液体クロマトグラフィー、質量分析装置、液体分注ロボット、環境監視、クリーンルーム制御、バイオリアクター制御、分散制御システム、監視制御およびデータ収集システム（SCADA）、定置洗浄システムなどがあります。医薬品製造業の OT システムには、SCADA、HMI、バッチ可視化、製造実行システム、バッチおよび機器制御（バイオリアクター、凍結乾燥機、クロマトグラフィースキッド、打錠機用）、環境監視システム（工場、クリーンルーム、コールドチェーン、冷凍庫用）、ビル管理システム、包装・シリアライゼーションラインコントローラー、ビジョンシステムコントローラー、データヒストリアン、エンジニアリングワークステーションが含まれます。

[1] ABB。「信頼の価値：ABB 調査レポート 2023 年」

医薬品業界における OT システムのアップタイム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、エンドポイント検知および対応（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なくなると、OT エンジニアは時間がかかりミスを生み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現場に派遣するには、時間とコストがかかり、障害が長期化して費用がかさむおそれがあります。

アクロニスは、 製薬業界の製造環境に特有なサイバーレジリエンス要件に対応

Acronis Cyber Protect プラットフォームは、図 1 に示す Purdue モデルの例を含む（ただしこれに限定されません）さまざまな OT システムを保護することから、製薬業界で広く使用されています。

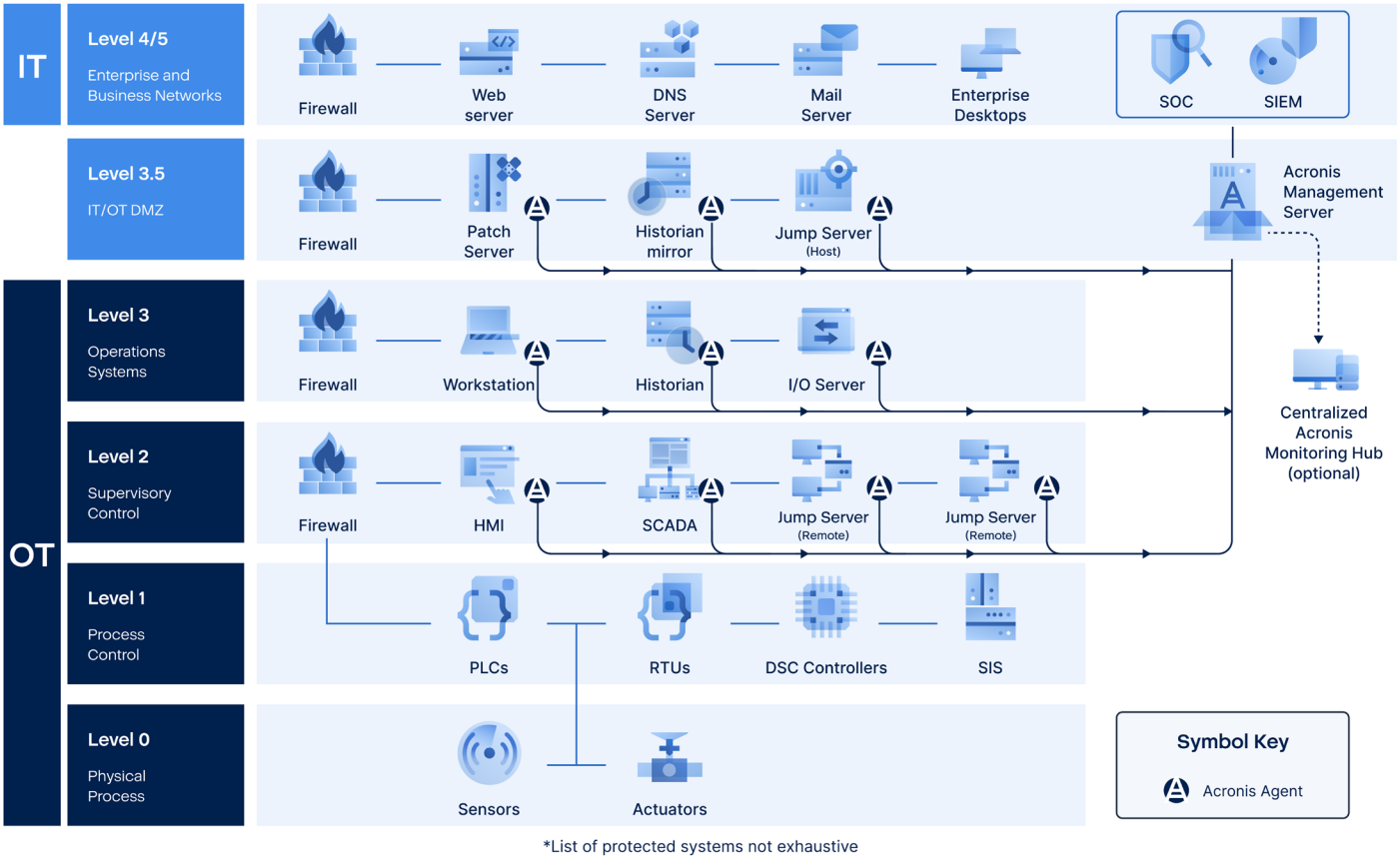

図 1: アクロニスで保護された OT システムの Purdue モデルの一例

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、高いアップタイムを要求される製薬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することなく、バックアップエージェントをインストールし、バックアップを実行できる、オンプレミスのバックアップ管理コンソール
- 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を軽減
- 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）
- 共通のアクロニスエージェントで利用できるマルウェア対策、ランサムウェア対策などのサイバーセキュリティ機能

アクロニスはレガシー OS システムも保護

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（他ベンダーが既にサポートを打ち切った OS も含む）。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。図 2 は、XP 時代から現在までの OS およびハイパーバイザーに対する アクロニスのサポート範囲を表し、OT 環境で最も一般的に使用される Windows および Linux バージョンが示されています。

図 2：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、11（全エディション）、10（Windows RT を除く全エディション）

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 11〜31
- 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 システムを復元可能

アクロニスはワンクリックリカバリと呼ばれる独自機能を提供しています。これは、現場に IT 要員が不在、またはエアギャップ化された OT 環境において、中央の IT スタッフがリモート管理ツールを使用できない場合に威力を発揮します。アクロニスのワンクリックリカバリは、IT スキルレベルに関係なく、現場の作業員であれば誰でも、わずか数回のキー操作でローカルバックアップから障害が起きた OT システムをリカバリすることができます。OT システムの障害を解決するためには、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 からリカバリでき、Bitlocker 暗号化とリカバリパスワードによりバックアップを安全に保護できます。

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

ABB、Siemens、Honeywell などの主要 OT/ICS ベンダーは、Acronis Cyber Protect をホワイトラベルや共同ブランドソリューションの一部として、顧客向けバックアップソリューションに採用しています。アクロニスほど、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、OT サイバーレジリエンスのリーダーとしての地位を確立

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、世界中の製薬研究および製造環境で OT システムを安全に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、オンプレミス管理コンソール、非 IT 従業員による OT システムのセルフサービスリカバリ、主要オートメーション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: ワンクリックリカバリで OT のアップタイムを維持
- ケーススタディ: タタ・スチール下流製品
- ケーススタディ: ABB
- ケーススタディ: Johnson Electric
- ケーススタディ: 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

詳細は以下をご覧ください。
acronis.com