TAG

ACRONISが運用技術（OT）サイバーレジリエンスのリーダーである理由

DR. EDWARD AMOROSO
TAG INFOSPHERE CEO

Acronis

ACRONIS が運用技術（OT）サイバーレジリエンスのリーダーである理由

TAG CEO、EDWARD AMOROSO

はじめに

数十年にわたり、サイバーセキュリティは、主に悪意のある攻撃から情報技術（IT）を保護することと同義でした。こうした流れを踏まえて、最高情報セキュリティ責任者（CISO）が任命され、従来の課題に対応する役割を担ってきました。しかし、最近では、サイバーセキュリティの範囲は拡大し、運用システムをはじめ、産業、物理環境、そして実体のあるあらゆるシステムが対象になっています。その結果、私たちが「運用技術（OT）セキュリティ」と定義する新たな分野が誕生しました。

OT セキュリティは IT セキュリティをきっかけに開発されたため、数多くの同種類の制御機能を共有しています。たとえば、可視性を確保し、緩和策を配置することは、IT と OT の両セキュリティ戦略の中核を成しています。OT セキュリティが広範な IT イニシアティブと組織的に統合され続けていることから、こうした共有が大いに役立っています。このことは、現在、多くの CISO が OT セキュリティに対する全責任を担っていることからも明らかです。

しかし、予想される通り、従来の IT セキュリティスキームに存在する多くの弱点が、産業での保護にもそのままの形で受け継がれることになります。そのような弱点の中で、恐らく最も明白なものは、攻撃を受けた際に多くの OT システムが示す典型的なレジリエンスの脆弱性でしょう。たとえば、ランサムウェアは、大規模な運用環境をダウンさせるのに効果的であり、顧客に深刻な影響を与えます。

しかし、OT セキュリティの領域においては、さまざまな固有の問題も発生します。こうした問題は、ほとんどの OT 環境に、セキュリティトレーニングを受けた現地スタッフがいないこと、これらのネットワークには古いプロプライエタリシステムが多数存在していること、工場や製造プラントなどの環境で進行中の業務に影響を与えることなくアップデートやパッチのインストールを行うことが困難であることなどに起因しています。

本レポートでは、CISO が率いる OT セキュリティチームが、バックアップとリカバリという重要機能に焦点を当てることで、運用のレジリエンスを向上させる方法について解説します。こうしたサイバープロテクションの側面は、IT セキュリティチームにとっては常に挑戦でした。なぜならば、効果的なソリューションを実現するためには、インフラに関する深い知識が必要であり、この分野に取り組んでいるほとんどのベンダーは、セキュリティではなく IT 運用に注力してきたからです。

一方で OT 環境 においては、セキュリティの改善に向けたあらゆる取り組みの中でも、バックアップとリカバリが最も重要な要素であると考えられます。確かに、OT スタッフのセキュリティトレーニングを強化し、レガシーシステムの数を減らすという補完的な目標も必要となることは間違いありません。しかし、ここで力説したいのは、OT セキュリティエンジニアが製造環境におけるこの最も重要な要素に注力することで、最大の効果が得られるという点です。

本稿では、商用ベンダーであるアクロニスの最新サイバーレジリエンスソリューションを例に挙げて説明します。IT または OT にかかわらず、インフラにおけるアクロニスのバックアップおよびリカバリのアプローチは、製造、輸送、エネルギー、電力、軍事などのセクターにおいて、あらゆる種類の中断を受け入れることができない産業活動を標的とするサイバー脅威の増加に十分対応していると考えられます。[1]

OT システムに対する現在のセキュリティ

前述の通り、レジリエンスが不十分であった場合、IT インフラと OT インフラでは被害に大きな違いが生じる理由として、運用上のセキュリティ問題がより深刻な結果を招く点が挙げられます。たとえば、産業制御システムにおけるレジリエンスの問題は、セーフティシステムの故障、製造ラインの停止、原子力発電所の運用上の課題などを引き起こす可能性があります。人命が失われる可能性のあるシナリオが容易に想像できます。

これは、OT 環境においては、セキュリティが最優先事項であるべきということを示唆しています。しかし、これらの環境は、異種のプロプライエタリ技術による課題に悩まされており、しばしば時代遅れのハードウェアやオペレーティングシステムが未だに使用されています。このため、パッチやアップデートの適用が制限されます。さらに、このような環境では、IT リソースやトレーニングを受けた専門家が不足していることが多く、バックアップできる時間帯も限られています。

さらに、IT 環境と OT 環境の間にゲートウェイを挿入して ハッカーから OT 環境を隔離するという目標は、うまく機能していません。IT/OT 間に境界を設けてインターネットから OT システムを隠すという当初の目的は、境界が常に崩れるのと同じ理由で破綻しました。内部の脅威を認識することを怠り、境界のアクセス経路を見逃し、本来境界が穴だらけであることを無視するなど、さまざまな理由があります。

また、IT/OT ゲートウェイアプローチでは、上記のように、プロプライエタリシステムの存在、パッチ適用の難しさ、セキュリティトレーニング未受講のスタッフなどの要因により、OT の重要なセキュリティ問題に対処することができません。以下の図は、IT/OT ゲートウェイではこれらのセキュリティ問題が解決されないことを示しています。また、今回の核心であるバックアップおよびリカバリ機能を必要とする、OT セキュリティのレジリエンスについても対応していません。

図 1.OT システムのセキュリティの課題

つまり、包括的な OT セキュリティには、これらすべての問題に対する解決策が求められていることが分かります。しかし、ランサムウェア、サボタージュ、または破壊的なサイバー攻撃に対して、運用を継続することを保証することが、今日の OT セキュリティの導入において最優先すべき目標であると考えています。商用のアクロニスプラットフォームとその OT セキュリティサポートの視点から、このケースを説明します。

OT および ICS（産業用制御システム）向けアクロニスバックアップおよびリカバリソリューション

TAG Infosphere の経験から、OT セキュリティプログラムは、3 つの補完的な分野に対処する必要があることが分かっています。第 1 に、OT 環境への可視性を確保する必要があります。これは、Claroty や Dragos などの商用プラットフォームを使用することで可能です。可視性の確保は不可欠であり、その実践的な運用を向上させることに力を注ぐ必要があります。これには、より優れたトレーニングと、OT サイバーシミュレーションに重点を置くことが求められるでしょう。

第 2 に、OT システムが IT と統合されるにつれて、経営者は、IT セキュリティチームがより集約された制御機能を構築するよう求めるべきであると考えています。たとえば、ゼロトラスト OT の動向を受け入れるべきです。これは、より多くのオペレーティングシステムがクラウドや他の従来型の IT システムと接続することを意味します。これにより、クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）などの IT 制御機能を拡張することで、OT インフラをカバーできます。

そして第 3 に、これが最も重要なのですが、OT セキュリティチームが運用のレジリエンスにもっと重点を置くことを推奨します。実際には、自動バックアップおよびリカバリソリューションを通じて、継続的な運用を確保する必要があるということです。これは、IT システムにも当てはまりますが、上記のように、OT サポートが崩れると、人間の命にかかわるより深刻な結果をもたらす恐れがあります。そしてアクロニスのソリューションにより、こうした問題を回避することができます。

OT インフラに最も適用されるセキュリティとレジリエンスの要件は、アクロニスのプラットフォームで十分にカバーされます。これは朗報です。なぜならば企業のチームは、たとえハードウェアやソフトウェアが陳腐化したり、プロプライエタリであっても、独自のローカルバックアップやリカバリソリューションを開発しなくても済むからです。具体的に言うと、OT レジリエンスに不可欠なアクロニススイートには、以下の主要機能が含まれています。

1. **OT システムの迅速なリカバリ** – アクロニスは OT コンピュータ向けの高性能な保護を提供し、費用負担がのしかかる工場の停止を防ぐために迅速なリストアを実現します。この迅速なリカバリ機能は、ダウンタイムを最小限に抑え、運用を維持する上で極めて重要です。
2. **Universal Computer Recovery** – Acronis Cyber Protect は、Windows XP 時代のレガシーシステムを含む、あらゆるコンピュータのベアメタルリストアオプションを備えた、迅速かつ信頼性の高いリカバリを実現します。この機能は、OT 環境で一般的な老朽化したレガシーシステムとの連続性を維持するために必要になります。
3. **カスタマイズ可能なバックアップ計画** – アクロニスにより、OT および ICS 環境の特定要件に合わせてカスタマイズ可能なバックアップ計画を作成できるため、機密データとシステムを万全に保護できます。AI を駆使して OT インフラを最新化し、より持続可能な提供方法を採用するにつれ、カスタマイズのニーズは増大していきます。
4. **サードパーティツールとの統合** – アクロニスは、サードパーティツールとの統合オプションを備えた、集中管理による統一バックアップおよびリカバリビューを提供することで、管理を簡素化し、運用効率を向上させます。OT 環境は、セキュリティ統合にとって特に難しい環境です。このため、この機能が特に重要になります。
5. **データ主権オプション** – 組織は、Amazon S3 や Microsoft Azure などのオプションを含む、アクロニスのグローバルデータセンターを利用するか、自社内のストレージを利用するかを選択できます。これにより、データ主権要件に対するコンプライアンスを確保できます。アクロニスは、顧客と協力して最適なホスティング環境を構築します。
6. **リモートワーカー向けのセルフサービスリカバリ** – アクロニスは、リモートワーカー向けにセルフサービスリカバリのオプションを提供します。これにより、技術者でなくてもリカバリ処理を開始できるようになり、IT の負荷を分散し、インシデント後の運用再開を加速できます。

ACRONIS PLATFORM アーキテクチャ

Acronis Cyber Protect Platform は、実際のデータ、履歴データ、およびその他の主要な OT 企業のデータのソースを安全に保管する、データウェアハウスを中心に構築されています。Acronis Cyber Protect プラットフォームの複数のコンソールインスタンスを OT 環境全体にインストールし、関連する複数のエージェントをデータ収集とリストアの目的で環境全体に配置することができます。メタデータは、コンソールからデータウェアハウスにストリーミングされます。

各 Acronis Cyber Protect の配置と Acronis Centralized Monitoring Hub には、バックアップおよびリカバリ処理のあらゆる側面を監視するためのダッシュボードとコンソールが備わっています。このハブにより、バックアップやリカバリタスクの実行中に、カスタマイズ可能なレポートや監視機能を含む履歴ビューが提供されます。明らかに、ここでの目的はインシデント、攻撃、その他のレジリエンスに関連する問題を通じて、継続的な運用を確保することです（図 2 を参照）。

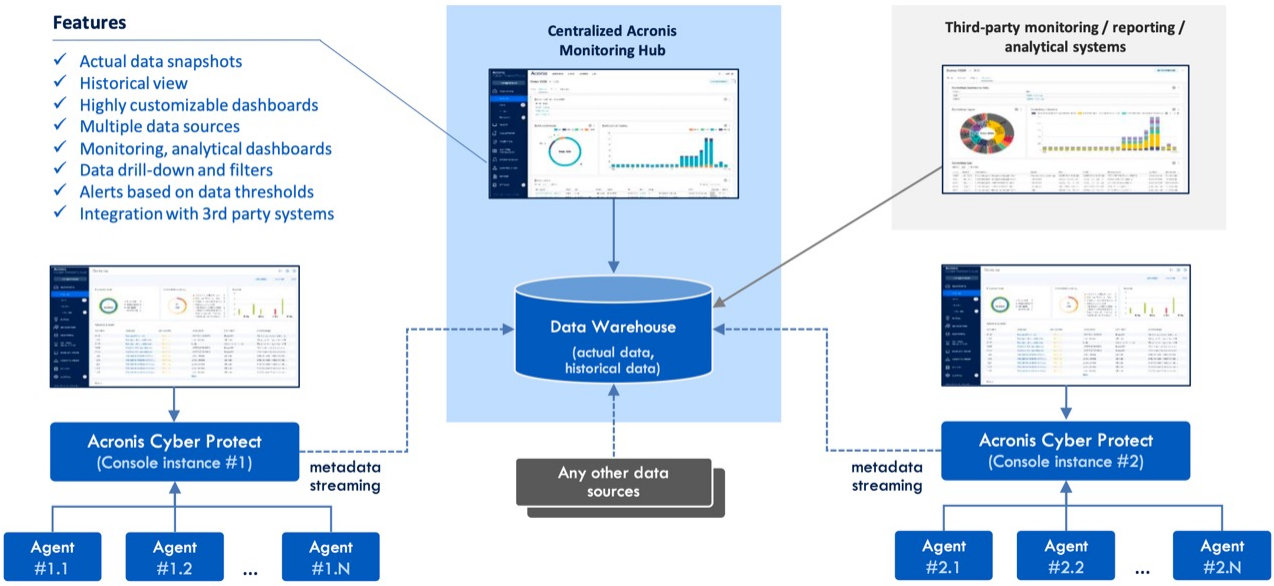

図 2.アクロニスシステムアーキテクチャ

アクロニスの統合

図に示されている 2 つのインスタンスをご覧ください。Acronis Cyber Protect は、バックアップ、ディザスタリカバリ、AI ベースのマルウェア保護、リモートアシスタンス、セキュリティツールを 1 つのプラットフォームに統一することで、OT を含むセキュリティチームの統合を支援します。この統合により、OT セキュリティチームを含むすべての企業が、1 つのインターフェイスでサイバープロテクションのさまざまな側面を管理できるようになり、複雑さが解消され、作業が効率化します。

プラットフォームの柔軟なアーキテクチャ、アプリケーションプログラミングおよびコマンドラインインターフェイスにより、アクロニスとサードパーティの両者によるサードパーティアプリケーションの開発および統合がサポートされます（図 2 に示されているように、サードパーティからのデータは、集中管理されたデータウェアハウスに供給されます）。この設計により、追加の保護、管理、および自動化サービスを組み込むことができるダイナミックなエコシステムを促進し、プラットフォームが進化するサイバーセキュリティ環境に適応し続けることを可能にします。この柔軟性により、組織はアクロニスのソリューションを既存のインフラに統合し、特に OT 環境において全体的なレジリエンスとセキュリティを強化できます。

アクロニスフォレンジックバックアップ

Acronis Cyber Protect には、ディスクレベルのバックアップからデジタル証拠を収集して、その後の分析を簡素化するように設計されたフォレンジックバックアップ機能が備わっています。この機能は、コンプライアンス要件を管理し、内部調査を効率的に実施する必要がある組織にとって欠かせません。また、フォレンジックは重要なインフラや重要なサービスを狙った攻撃を特定するのに役立つことから、OT 環境にも不可欠な機能です。

アクロニスのフォレンジックバックアップ処理では、アクティブデータ、空き容量、メモリダンプを含む包括的なディスクイメージを取得します。この徹底したアプローチは、OT セキュリティ要件として大きく浮上しており、すべての潜在的なデジタル証拠が適切に保存されることを保証し、インシデント後の詳細な分析を促進し、法的および規制上の義務の履行を支援します。

収集したフォレンジックデータを通常のバックアップルーチンと統合することで、アクロニスは、IT 環境と OT 環境の企業が、運用を継続しながら、重要なフォレンジック情報を必要なときにすぐに利用できるようにします。この統合により、別個のフォレンジックデータ収集プロセスが不要になり、運用が合理化され、インシデント発生時のデータ損失リスクが低減されます。

アクロニス統合型ディザスタリカバリ

Acronis Cyber Protect は、複雑さとコストを最小限に抑える統合型ディザスタリカバリソリューションを提供します。このプラットフォームは、バックアップとディザスタリカバリ機能を組み合わせることで、自然災害、人的エラー、サイバー攻撃、ハードウェア障害などのイベント発生後に、ワークロードの迅速なリストアを実現します。前述の通り、OT システムの環境でこれらのイベントが発生すると、深刻な事態を招くことがあります。

ディザスタリカバリ機能には、災害発生時に IT または OT ワークロードを迅速に起動できる機能、リカバリ処理を自動化するランブック、およびフェールオーバーをテストして実際のイベント中にシステムが期待どおりに機能することを確認する機能などが含まれます。これらの機能は、ビジネス継続性を維持し、ダウンタイムを最小化するために欠かせませんが、特に OT 環境では一般的なリアルタイムアプリケーションにとって不可欠です。

ディザスタリカバリにサイバーセキュリティやエンドポイント管理を統合することで、アクロニスはサイバー保護に対する包括的なアプローチを提供します。この統合により、組織の IT インフラのあらゆる側面が確実に保護され、広範な潜在的破壊に対するレジリエンスが向上します。また、IT と OT の両本番システムに責任を担う CISO の管理も簡素化されます。

規制要件との整合

バックアップとレジリエンスの運用ニーズに加えて、OT セキュリティチームは、さまざまな新規の社外コンプライアンスや規制フレームワークに対応する必要があります。その結果、OT サイバーセキュリティのコンプライアンスは、脅威が増加するにつれて要件も厳しくなっていくため、企業のセキュリティプログラムの中で大きな課題となっています。

より具体的には、EU のデジタルオペレーショナルレジリエンス法（DORA）や、重要インフラセクターにおける堅牢なサイバーセキュリティ対策の必要性を強調するバーゼル銀行監督委員会のガイドラインなどの枠組みから、国際的な規制機関が運用のレジリエンスを重視していることが分かります。アクロニスのソリューションは、以下の分野で支援することにより、これらの規制要件のコンプライアンスをサポートします。

1. **包括的なリスク管理フレームワーク** – アクロニスのソリューションにより、セキュリティ組織は、適応可能なリスク管理フレームワークを実装し、レジリエンスを定期的にテストし、ステークホルダーや規制当局とのオープンなコミュニケーションを維持することができます。これにより、IT と OT に対して、グローバルな運用レジリエンスフレームワークと整合させることができます。
2. **インシデント対応計画** – アクロニスは、単独またはビジネス継続性計画の一環として、インシデント対応計画の書面による作成を支援し、潜在的なサイバー脅威に対する準備を確実にします。これは多くの OT セキュリティチームにとって新たな作業になります。そのため、アクロニスによる支援が特に有効です。

3. **サードパーティリスク管理** – アクロニスの統合機能により、規制当局が重視している運用レジリエンスの重要な要素である、強固なサードパーティによる監視が促進されます。前述の通り、サードパーティとのサイバー統合は、これまで無視されたり、重要視されなかったことから、困難な場合があります。

OT および ICS（産業用制御システム）における先進の自動化ベンダーがアクロニスに信頼を寄せる

世界最大の OT および ICS プラットフォームベンダーによる、アクロニスバックアップおよびリカバリソリューションの採用は、このソリューションが OT および産業環境におけるレジリエンスの確保において重要な役割を果たしていることの表れと言えます。ABB、Emerson、Siemens、Schneider Electric、Rockwell Automation、横河電機などの業界リーダーは、ホワイトラベルまたは共同ブランドソリューションとして Acronis Cyber Protect を自社のプラットフォームに統合し、顧客に運用レジリエンスを提供しています。これらのグローバル巨大企業がアクロニスを標準採用している事実は、OT バックアップおよびリカバリにおけるアクロニスプラットフォームの信頼性、柔軟性、およびリーダー的地位を裏付けるものです。

サマリとOTセキュリティチームのアクションプラン

アクロニスのバックアップおよびリカバリソリューションは、OT インフラストラクチャのレジリエンスとセキュリティを強化したいと考えている顧客に最適です。アクロニスは、迅速なリカバリ機能、レガシーシステムのサポート、カスタマイズ可能なシステムのバックアップ計画、規制要件への整合を提供することで、組織が運用の継続性を堅持し、運用レジリエンスのグローバルスタンダードの厳格化に対応できるようにします。

この責任を担う CISO や、OT のサイバーレジリエンスに対処するために働く他のあらゆる経営陣や経営者は、すぐにアクロニスに連絡を取って、その機能について詳しく知ることをお勧めします。また、私たち TAG Infosphere のチームは、読者の皆様がサイバーセキュリティと人工知能の関連トピックについてより深いインサイトを得ることができるよう、いつでもご支援します。ご連絡をお待ちしております。

[1] アクロニスの技術チームと経営幹部チームには、顧客が運用している OT 環境で見られるさまざまなリスクへの理解を助けていただき、特に感謝しています。アクロニスのチームは、TAG Infosphere に製品ドキュメントを提供し、IT と OT セキュリティの両製品のロードマップに関する有益な情報を提供していただきました。

TAG INFOSPHERE について

TAG Infosphere は、サイバーセキュリティ、人工知能、気候科学に関するインサイトと助言を数千の商用ソリューションプロバイダーおよびフォーチュン 500 企業に提供する、信頼できるリサーチおよびアドバイザリー企業です。2016 年に設立され、本社をニューヨーク市に置いています。実務者の視点から、公平で詳細なガイダンス、マーケット分析、プロジェクトコンサルティング、およびカスタマイズされた内容を提供することで、有料型リサーチのトレンドに従わない姿勢を取っています。