発行日:
2025 年 2 月 25 日
著者:
主任アナリスト Hollie Hennessy

On the Radar（注目ベンダー）：アクロニスの OT サイバーセキュリティレジリエンスに向けたバックアップとリカバリ

概要

変革の推進者

アクロニス の運用技術（OT）ソリューションは、サイバーセキュリティの要件の中でも「復旧」に重点を置いています。こうしたアプローチに基づいて、OT 環境に対してバックアップ、リカバリ、データセキュリティを提供し、サイバーセキュリティのレジリエンスを高めています。アクロニス は強力なパートナーおよびチャネルのネットワークを有しており、OT セキュリティ分野における同社の評判を確固たるものにしています。

Omdia の見解

OT セキュリティには、複数の目的があります。その 1 つがインシデントまたは攻撃が発生した際の復旧です。製造オペレーションインフラおよび重要インフラの環境においては、おそらく一部の IT 環境以上にビジネス継続性が重要視されます。重要インフラを運用する多くの組織は、規制要件を遵守しなければならず、ダウンタイムによって多大な財務上の影響や潜在的な損害が生じるケースが多くなっています。

どのような環境においても、効果的で実証済みのバックアップおよびリカバリ計画を策定することが極めて重要になります。たとえ最善の防御を施していても、攻撃を被る可能性はあります。したがって、こうした事態に対処する方法を熟知し、できる限り短時間でシステムをオンラインに復旧できる能力は、あらゆるサイバーセキュリティ戦略の基本要素となるべきです。データの外部流出を迅速かつ効率的にリストアするプロセスとともに、定期的なバックアップが鍵を握ります。

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、特にチャネル戦略を重視しています。このため、サービスプロバイダーや産業向けベンダーは、提供しているサービスやプラットフォームにバックアップおよびリカバリ機能を組み込むことができるとともに、OT 中心の組織に向けてソフトウェア製品として提供することもできます。

アクロニス に注目する理由は？

アクロニス は、OEM ベンダーとも提携しており、製造、医療、エネルギーの各業界をリードする数多くの産業オートメーションベンダーに向け、バックアップおよびリカバリソリューションを提供しています。こうしたベンダーの製品は、規制要件（NIS2 など）や標準（ISA/IEC 62443 など）の遵守を支援します。さらに、産業用オートメーションベンダーのソリューションが強化され、顧客により堅牢で信頼できるサービスを提供することが可能になります。アクロニス は、バックアップおよびリカバリ分野の専門知識を活かすことで、OT 環境、およびその中で現在も使用されているレガシーシステムのニーズに適したソリューションを開発することができたのです。

市場の状況

OT セキュリティ市場では、アセット管理、監視、検出および対応が中心となっており、この分野の多くの主要ベンダーが、これらの分野のすべてまたはほとんどを網羅する機能を提供しています。しかし、この市場において、規制要件と製造業および OT に焦点を当てた組織のニーズの両方を満たすためには、さらなる追加機能が必要になります。

こうした環境下では、安全性、運用上、財務上の理由に関わらずビジネス継続性が最重要です。したがって、侵害や攻撃を検出できることはもちろん、既知の脅威を未然に防ぐことが鍵となります。後者に対処するために、予防的な自動化やリスク管理、脆弱性管理、侵害および攻撃シミュレーション、攻撃対象領域の管理など、よりプロアクティブなアプローチの追加機能が登場しました。

しかし、いかなるシステムも完全ではないため、あらゆるインシデントの被害からでも復旧できる能力が求められます。この市場では、インシデント対応ツールとサービス、フォレンジック、データとシステムのリカバリを含むサイバーセキュリティレジリエンスに焦点が当てられており、この分野おいて アクロニス のソリューションが OT に対して有効です。

NIST サイバーセキュリティフレームワーク（CSF）2.0 は、重要組織（実際にはすべての組織）のサイバーセキュリティ要件を示す優れた指標です。当初、重要インフラに焦点を当てていた アクロニス のフレームワークは、今では広く採用および参照されており、その範囲は拡大しています。このフレームワークのアップデートバージョンには、さまざまな機能が含まれています。

- 特定
- 保護
- 検出
- 対応
- リカバリ
- 統治（最新の追加機能）

製品/サービスの概要

アクロニス のデータ保護機能は、そのプラットフォームである Acronis Cyber Protect の一部機能を構成する「バックアップ」と「ディザスタリカバリ」の 2 つの領域にまで及んでいます。具体的な機能として、以下が挙げられます。

- 実行中のシステムに対するフルイメージバックアップ。フェールセーフパッチにより、システムまたはアプリケーションにパッチが適用される前にイメージバックアップが作成される
- 「ワンクリックリカバリ」による、セルフサービス
- ユニバーサルリストアによる、あらゆるハードウェアやハイパーバイザーへのリカバリ
- インスタントリストアによる、リカバリを継続しながらの起動/実行
- イミュータブルバックアップによる、セキュリティの強化
- Windows、Linux、その他の OS/アプリケーションのサポート（Windows XP など、現在も OT 環境で使用されているレガシーバージョンを含む）
- リカバリプロセス内で自動化された、マルウェア対策スキャンとウイルス対策アップデート
- 完全に統合されたディザスタリカバリ・アズ・ア・サービス

OT 環境に合わせて設計された　Acronis Cyber Protect は、インストールとバックアップを本番稼働中に実行するため、システムをオフラインにする必要はありません。また、再起動も不要です。さらに、アクロニス のソリューションは、必要に応じて新しいハードウェアへのリカバリに対応できます。これは、Acronis Cyber Protect エージェントを通じて実行されますが、マルウェア対策コンポーネントの有無にかかわらず、顧客の制約や要件に応じてインストールすることができます。

ワンクリックリカバリにより、リカバリ処理が簡素化されます。IT やセキュリティの専門家でなくても、特別な技術知識なしに、システムを復旧して稼働させることができます。これは現場へのアクセスが困難な深海石油掘削装置などの遠隔地の分散環境や、製造ラインでの操業再開など

、時間的制約のあるシナリオで特に重要になります。また、ローカルディスクバックアップまたは Acronis Cloud からの再起動によるリカバリのオプションもあります。さらに、バックアップされたデータは、マルウェアのスキャンが自動的に実施され、最新のウイルス対策にアップデートされます。

Centralized Acronis Monitoring Hub と呼ばれる一元化されたダッシュボードに、インサイトと制御が集約されています。このダッシュボードは、分析にメタデータを使用し、サードパーティ製のソフトウェアと統合されています。

企業情報

背景

2003 年にシンガポールで設立され、2008 年にスイスで法人登録された アクロニス は現在、45 ヵ国に 1,800 人 以上の従業員を擁します。また、 150 ヵ国の 750,000 を超える顧客企業にサービスを提供しています。

同社は近年、データ保護というルーツを基に、パートナーや顧客に広範なサイバーセキュリティ製品を提供することで大きな成長を遂げてきました。また、Acronis Cyber Protect プラットフォームにより、2 つの分野を融合するという新たな概念を切り開いてきました。

さらに、Acronis Lab を通じて研究開発に注力しています。Acronis Lab には、500 人以上のエンジニアが在籍しており、そのうち 20 人以上が博士号を保有しています。また、17 年の歴史の中で 200 件以上の特許を取得しています。Acronis Threat Research Unit（TRU）は、既存および新興のサイバー脅威に関する知見とリサーチの結果を定期的に公開しています。

2024 年 8 月、欧州のプライベートエクイティファームである EQT が、推定 40 億ドルの評価額で、アクロニス の過半数の株式を取得することが発表されました。株式取得は、2025 年の第 1 四半期または第 2 四半期に完了する見込みです。これまでに アクロニス は、CVC Capital Partners、BlackRock、Goldman Sachs などの投資家から 5 億ドル以上の資金を調達しています。

現在の状況

アクロニス は、新たにリリースされた XDR（Extended Detection and Response）製品や、それをサポートする AI（生成 AI）アシスタントなど、OT 分野のバックアップとリカバリを超えた幅広いサイバーセキュリティ技術を誇っています。同社のポートフォリオは、広範囲にわたっており、以下の分野をカバーしています。

- データ保護（前述の通り）
- サイバーセキュリティ（エンドポイントセキュリティ、マルウェア対策、EDR/XDR など）
- エンドポイント管理（パッチ管理、脆弱性管理、リモートアクセスなど）

アクロニス の製品の一部はエンドユーザーへの直接販売ですが、主要な販売チャネルとして、リセラー、マネージドサービスプロバイダー（MSP）、OEM などのチャネルを有しています。産業オートメーション分野では、ABB、Emerson、Siemens, Schneider Electric、Rockwell Automation、横河電機など、多くのベンダーがこのチャネルに含まれています。

注目すべき点として、アクロニス は、従量課金制で支払う高度な機能を備えたプラットフォームの基本的な機能をも提供しています。

今後の計画

アクロニス は、サイバーセキュリティ機能をさらに強化した AI プラットフォームの開発を検討していますが、現時点で IoT や OT を対象とする計画はありません。

主要データ

表 1 : データシート: アクロニス

製品名	Acronis Cyber Protect	**製品分類**	エンドポイント保護とバックアップ/リカバリ
バージョン番号	v16	**リリース日**	2024 年 2 月
対象業界	製造業 医療 研究開発（バイオファーマ） 石油/ガス 発電/エネルギー 物流 自動車 小売 教育/政府 建設	**対象地域**	北米 中南米 欧州/中東/アフリカ アジア太平洋
対象企業の規模	大企業/中規模企業/小規模企業	**ライセンスオプション**	サブスクリプションライセンス
URL	www.acronis.com https://www.acronis.com/en-us/products/cyber-protect/trial/	**販売経路**	直販 チャネル販売 OEM 販売
本社	スイス、シャフハウゼン	**従業員数**	～1,800

出典: Omdia

アナリストのコメント

アクロニス は数多くのイノベーションおよびデータ保護/リカバリ分野での専門知識によって、産業環境にとって魅力的なソリューションを実現しました。導入、バックアップ、リカバリに対して、いくつものオプションを提供し、個々の顧客のニーズに応える柔軟性を備えています。サービスプロバイダーや産業用オートメーションベンダーが提携している OT セキュリティベンダーの多くは、データリカバリ機能を提供していません。このことが、アクロニス にとって大きなチャンスとなっています。データリカバリ分野での競合他社は、IT の側面により注力する傾向があります。競合他社には、アクロニス が有する OT 環境での専門知識が欠けています。また、競合他社は、アクロニス が産業界の先進 OEM ベンダーとの緊密な統合やパートナーシップを通じて得たような高い評価を受けていません。

しかし、アクロニス がチャネルやパートナーに提供しているのは、より広範なプラットフォームであり、「復旧」を超えた OT セキュリティ要件を満たしていず、現時点では計画も予定されていません。MSP/マネージドセキュリティサービスプロバイダー（MSSP）のパートナーは、IT をエンドユーザーに提供することにより重点を置いています。また、セキュリティ運用ソリューションを使用して、IoT/OT 市場に進出する場合、デバイスの動作とプロプライエタリプロトコルを考慮すると、大規模な開発が必要になる可能性があります。このプラットフォームにより、パートナーは主要な IT セキュリティ関連機能を提供できますが、産業界の顧客をサポートする必要が生じた場合は、検出、防止、および可視性が提供できる他の OT セキュリティベンダーに頼ることになるでしょう。現在、OT セキュリティのリーダー企業は、データ保護とリカバリには注力していませんが、これらのベンダーには、このギャップを埋め、競争力のある状況を作り出す機会があります。

付録

On the Radar（注目ベンダー）

On the Radar は、革新的なアイデア、製品、あるいはビジネスモデルを市場にもたらすベンダーに関する調査シリーズです。On the Radar に取り上げられたベンダーは、そのアプローチ、最新の開発、または戦略により破壊的創造を起こし、技術系バイヤーやユーザーが関心を持つ可能性があり、市場に影響を与えるポテンシャルを有していることから、注目する価値があります。

詳細情報

Omdia Market Radar: OT サイバーセキュリティプラットフォーム、*2025*（2025 年 1 月）

2025 年の注目トレンド: IoT サイバーセキュリティ（2024 年 9 月）

「Xage Security、Armis および横河電機エンジニアリングアジアとの新たなパートナーシップを発表し、安全なリモートアクセスを提供」（2024 年 9 月）

『Omdia による 2023 年産業ネットワークセキュリティ調査: 全体調査結果』（2023 年 12 月）

著者

IoT サイバーセキュリティ
主任アナリスト　Hollie Hennessy、

askananalyst@omdia.com

引用規定

Omdia の調査およびデータの外部引用および使用については、citations@omdia.com までお問い合わせください。

Omdia コンサルティング

この分析結果が、情報に基づいた創造的な経営判断の一助となることを願っています。さらに詳しい情報が必要な場合は、Omdia のコンサルティングチームがお手伝いします。Omdia のコンサルティングサービスに関する詳細情報については、consulting@omdia.com まで直接お問い合わせください。

著作権および免責事項

ここで参照されている Omdia の調査、データ、および情報（「Omdia 資料」）は、TechTarget, Inc. およびその子会社または 関連会社（総じて「Informa TechTarget」）またはそのサードパーティのデータプロバイダーの著作権で保護された財産です。また、それらはデータ、調査、意見、または Informa TechTarget によって公開された視点であり、事実を表すものではありません。

Omdia の資料は、このドキュメントの日付からではなく、最初の発行日からの情報と意見を反映しています。Omdia 資料に記載されている情報や意見は、予告なしに変更される場合があります。結果として、Informa TechTarget は、Omdia の資料またはこの出版物を更新する義務または責任を負いません。

Omdia の資料は、「現状有姿」および「利用可能な状態」で提供されます。Omdia の資料に含まれる情報、意見、結論の公平性、正確性、完全性、または正当性に関して、明示または黙示を問わず、いかなる表明または保証も行われるものではありません。

Informa TechTarget およびその関連会社、役員、取締役、従業員、代理人、およびサードパーティのデータプロバイダーは、Omdia の資料の正確性、完全性または使用に関しては、法律で認められる限りにおける範囲で、いかなる責任も負いません（過失または不注意に起因する責任を含みますがこれに限定されません）。Informa TechTarget は、いかなる状況においても、Omdia の資料に基づいて、または Omdia の資料に依拠して行われた取引、投資、商行為、またはその他の決定に対して一切責任を負いません。

お問い合わせ

omdia.com

askananalyst@omdia.com