Acronis
Server Protection

サーバーおよび仮想マシン向けの
ネイティブ統合サイバープロテクション

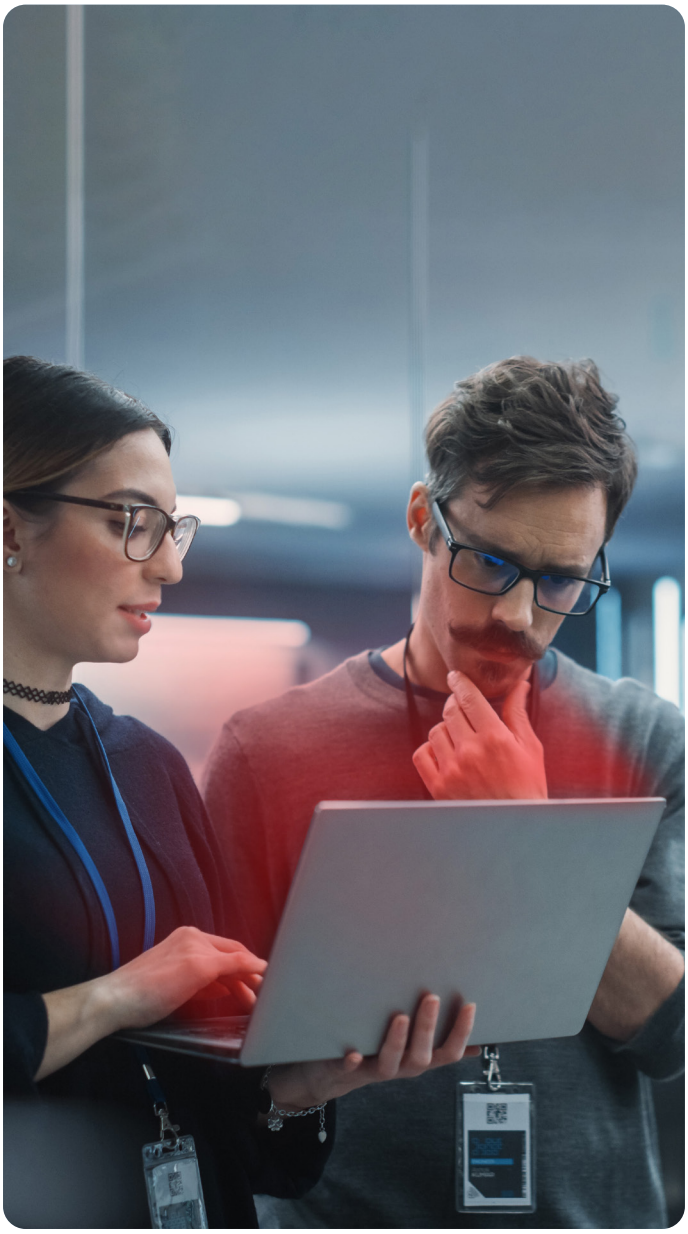
サイバーレジリエンスは、従来のサイバーセキュリティを超えた概念です。単に攻撃を防ぐだけでなく、インシデントが発生しても事業を確実に継続する能力を意味します。NIST は「サイバーレジリエンスとは、システムに対する悪条件、ストレス、攻撃、侵害を予測し、それに耐え、そこから回復し、適応する能力のことである」と定義しています。

サービスプロバイダー、企業に求められるのは、「事業をどれだけ早くリカバリできるか」です。明確なインシデント対応プレイブック、ツール、そして目標復旧時間（RTO）および目標復旧時点（RPO）が定義されていなければ、障害が起こるたびに収益の損失、顧客の信頼低下、そして長期におよぶ風評被害を引き起こすリスクが生じます。

レジリエンスの悩みどころ

企業の大小にかかわらず、ダウンタイムに起因するコストはデータ損失よりもはるかに大きいといわれています。これらの企業は、コンプライアンスへの高まるプレッシャーと戦い、規制当局の監督に対応しています。備えが足りなければ、コンプライアンスを遵守できずに、罰金や制裁、風評被害のリスクにさらされることになります。

分断化したツールでインシデントを管理すると、不要な複雑さを生む原因にもなります。統一された戦略がなければ、IT運用管理者は混乱状態に陥り、複数のコンソールやエージェントにまたがる検知、対応、リカバリをつなぎ合わせるのに苦労します。こうした非効率性はコストを増加させ、対応時間を遅らせ、責任リスクの拡大を招きます。サイバー保険の保険料が高騰していることも懸念材料であり、レジリエンスが低いと保険が適用されないことさえあります。



レジリエンスを阻む技術の壁

企業がデジタルトランスフォーメーションを加速させる中、レジリエンスの実現はより困難になっています。ハイブリッド IT 環境は、オンプレミスシステム、クラウドプラットフォーム、リモートエンドポイントにまたがっており、攻撃対象領域は拡大する一方です。その結果、システム間の依存関係が複雑化し、単一障害点が増えることになります。同時に、脅威は一段と巧妙化しています。ランサムウェア、サプライチェーン侵害、内部リスクは、サイロ化されたソリューションが生む間隙を突きます。特定の専業ソリューションは、特定のリスクを減らしても、同時に死角や手作業が増えることで、攻撃者がすぐに悪用するギャップも生み出します。

サイバーレジリエンスへの道

真のサイバーレジリエンスを達成するためには、強力な防御だけでは不十分です。どのような障害が発生しても、事業継続性を確保することが求められます。企業は、資産のマッピング、脆弱性診断、パッチ管理を通じてリスクを**予測する**ことから始まる、体系的な取り組みを通じて、真のレジリエンスを手に入れることができます。今、企業は、高度なプロテクション（AI サポートのエンドポイント保護や ML ベースの監視など）により、脅威をリアルタイムで検出して封じ込める**対策**を必要としています。こうした事前対策は、強力なリカバリ戦略と組み合わせてこそ効果を発揮します。

リカバリが次の重要なステップです。マルウェアに感染することなく、迅速かつ確実にデータとシステムを復元することで、ダウンタイムを最小限に抑えます。深刻な障害が発生した場合、最も重要なのは事業を止めずに継続させることです。Acronis Cloud Disaster Recovery により、企業はワークロードを即座に Acronis Cloud または Microsoft Azure にフェイルオーバーできます。この即時フェイルオーバーにより、最も深刻な障害時でも継続性が確保され、プライマリシステムの完全復元が完了するまで、安全な縮退運転として機能します。

最後に、レジリエンスは静的なものではありません。組織は、インシデントから学び、すべての関連メンバーを訓練し、時間をかけて防御体制を洗練させることによって、**動的に適応する**必要があります。

ディザスタリカバリの全体像

これらの戦略は、単に災害後のリカバリだけを目的とするものではなく、どのような逆境下でも、重要業務を継続するための運用上のレジリエンスを支えるためのものなのです。数日ではなく数分でサービスをリカバリできることが、財務的損失を最小限に抑え、顧客の信頼を維持する鍵となります。

ディザスタリカバリ戦略は通常、達成可能な RPO と RTO に基づいて分類されます。最もよく採用されている戦略には、次の 2 つがあります。

ウォーム DR

このアプローチは、コストとリカバリスピードを両立させることができます。あらかじめ準備されたシステムを活用することで、すばやく稼働させることができ、ダウンタイムを最小限に抑える「復旧」目標に適合しつつ、RPO と RTO も確実に管理できます。

コールド DR

純粋にシステムの再構築とデータ復元に焦点を当てたアプローチで、バックアップからの完全リカバリに依存するため、時間はかかりますが、運用コストは抑えられます。

検知、保護、リカバリを統合することで、企業は危機を乗り越えるだけでなく、より強靭な企業として再起できるというアドバンテージが得られます。Acronis Cloud Disaster Recovery では、ワークロードごとに最適なレジリエンスレベルを選択できます。ウォームからコールド DR によるリカバリオプションで障害後のサービスを再構築することも、統合型ホット DR でほぼ瞬時に事業を継続することも可能です。 この柔軟性により、サイバーレジリエンスのあらゆる段階において防御力が強化されます。

アクロニスサーバー保護ソリューション

アクロニスサーバー保護ソリューションでは、バックアップ、ディザスタリカバリ、エンドポイントセキュリティ、リスク評価、データ損失防止を、ネイティブに統合した単一のサイバープロテクションプラットフォームに集約しています。このアプローチは、サイロ化を防ぎ、ツールの乱立を抑え、複雑化を解消し、サイバーレジリエンスを可能にします。当該プラットフォームは、レジリエンス実現に向けての、予測、防御、復旧、適応の各ステージに対応します。企業は、1 つのプラットフォーム、1 つのエージェント、1 つのコンソールで、脅威を迅速に検知し、システムを中断することなくオペレーションをリカバリし、進化するリスクに継続的に適応します。

予測	防御	リカバリ	適応
• デバイスの検出 • データ保護マップ • 資産管理 • 脆弱性診断 • パッチ管理	• リアルタイムの脅威検出 • AI 活用の EDR（エンドポイント検出および対応） • ML（機械学習）による監視 • 進行中の脅威の迅速な封じ込め	• 安全かつ自動化されたデータリカバリ • クラウドディザスタリカバリ（CDR） • 不変バックアップストレージ • ハイパーバイザーの可搬性 • マルウェアのないポイントへリカバリ	• RMM（エンドポイントの監視および管理） • SAT（セキュリティ意識向上トレーニング） • ガイド付きインシデント対応テンプレート

企業に支持されるアクロニスのソリューション

サイバー攻撃が必然的な環境において、アクロニスは AI を活用した脅威対策とクラウド型ディザスタリカバリを単一プラットフォームに統合することで、サイバーレジリエンスを実現しています。断片的で予防のみにに偏ったアプローチとは異なり、アクロニスは不変バックアップ、AI によるランサムウェア検出、クリーンで安全なリカバリの検証により、重要なデータが保護されていることと確実にリカバリすることの両者を実現します。

アクロニスサーバー保護ソリューションでは、完全なクラウドマネージ型ディザスタリカバリにより、Acronis Cloud への即時フェイルオーバー、従量課金、ユーザー環境のテストの実行により、レガシーインフラのコストや複雑さを解消し、エンタープライズクラスのサイバープロテクションを実現します。その結果、リカバリはより迅速になり、運用リスクは低減され、最も重要な局面でもビジネス継続性を維持します。

アクロニスに相談する

事業を継続するには、保護だけでは十分ではありません。レジリエンスが求められます。アクロニスが、脅威の予測、攻撃への耐性、迅速なリカバリ、そして将来への適応をどのように支援できるかをご確認ください。

お問い合わせ