Acronis Cyber Resilience

サーバーおよび VM（仮想マシン）向けにネイティブ統合されたサイバーレジリエンス

アクロニスで実現するサイバーレジリエンス

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。

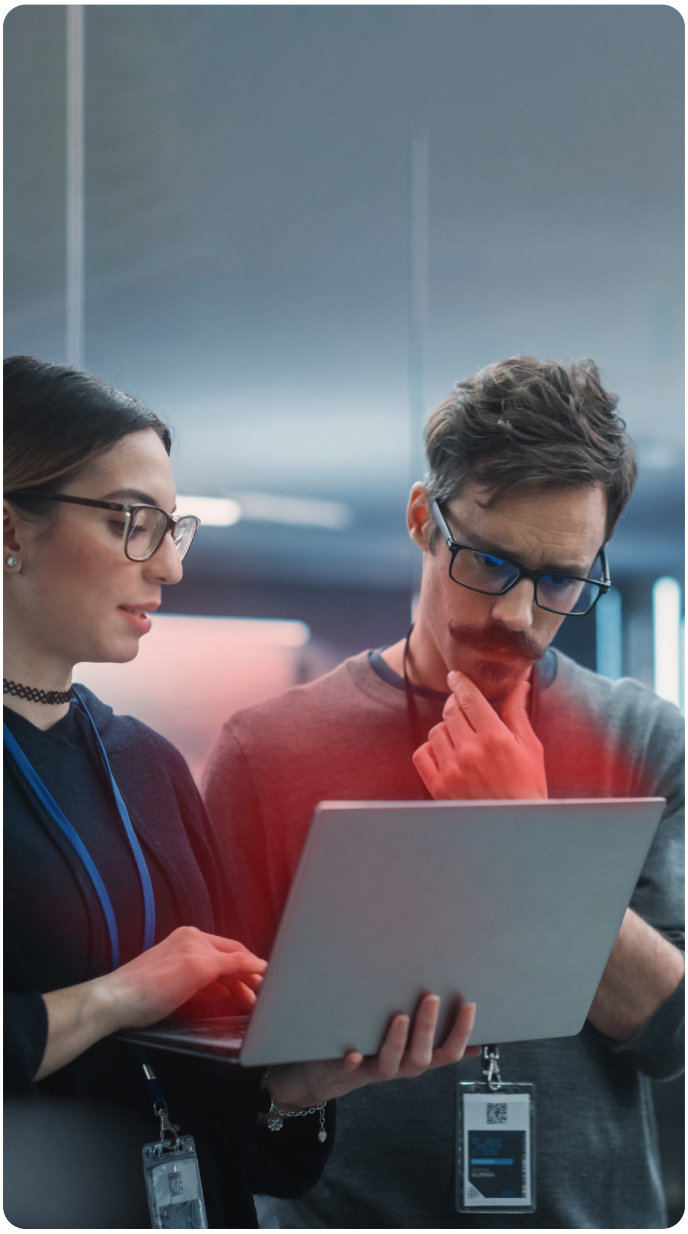
サービスプロバイダー、企業に求められるのは、「事業をどれだけ早くリカバリできるか」です。明確なインシデント対応プレイブック、ツール、そして目標復旧時間（RTO）および目標復旧時点（RPO）が定義されていなければ、障害が起こるたびに収益の損失、顧客の信頼低下、そして長期におよぶ風評被害を引き起こすリスクが生じます。

レジリエンスの悩みどころ

あらゆる規模の企業が、システムダウンによるコストはデータの損失よりもはるかに大きいことを痛感しています。サービスプロバイダーは、度重なる障害により顧客の信頼が損なわれると、顧客離れのリスクにも直面します。

一方、企業は厳格化するコンプライアンス要件や規制監督への対応に追われています。準備に不足があれば、罰金や制裁、風評被害のリスクにさらされます。

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チームは混乱状態に陥り、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。さらに、企業はリアルタイムで脅威を検知し封じ込める**能力を備える**必要があります。そのために、エンドポイント検知および対応（EDR）、拡張検知および対応（XDR）、データ損失防止（DLP）などの高度な機能が活用されます。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、チームを訓練し、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。

Acronis Cyber Resilience ソリューション

ディザスタリカバリに加え、アクロニスはバックアップ、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プラットフォームを提供しています。このアプローチにより、サイロ化を防ぎ、ツールの乱立を抑え、余計な複雑さを増すことなくレジリエンスを確保できます。企業、サービスプロバイダー両者に最適なこのプラットフォームは、レジリエンスの行程のあらゆる段階（予測し、それに耐え、そこからリカバリし、適応するまで）をカバーしています。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、事業を中断することなくリカバリし、進化するリスクに継続的に適応することができます。

予測する	耐える	リカバリする	適応する
• 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 • EDR（エンドポイント検知および対応） • XDR（拡張検知および対応） • DLP（データ喪失防止） • 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	• 遠隔監視および管理（RMM） • セキュリティ意識向上トレーニング（SAT） • マネージド検知および対応（MDR） • ガイド付きインシデント対応テンプレート

サービスプロバイダーと企業に支持されるアクロニス

サービスプロバイダーに対して、アクロニスは継続的収益を加速させるための道筋を提供しています。高利益率のサイバーレジリエンスサービスをサービスポートフォリオに加えることで、MSP はサービスを拡大できるだけでなく、コモディティ化した市場で際立った存在感を示すことができます。統合プラットフォームは、ツールの乱立を減らして運用を簡素化する一方、わかりやすいライセンスモデルが利益率を最大化し、顧客の成長に合わせてシームレスに拡張することができます。

アクロニスは、大企業や中小企業に対して、迅速でマルウェアのないリカバリを可能にし、ダウンタイムと財務上の損失を最小限に抑えることで、事業継続性を確保します。ビルトインのレポート機能とコンプライアンス対応により、規制監査も容易になります。強力なレジリエンス能力は、サイバー保険への適格性を高め、保険料の引き下げも期待できます。同じく重要なのは、強固なレジリエンス戦略を示すことで、顧客、パートナー、規制当局との信頼関係が構築されることです。

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

Acronis

詳細は、www.acronis.com をご覧ください