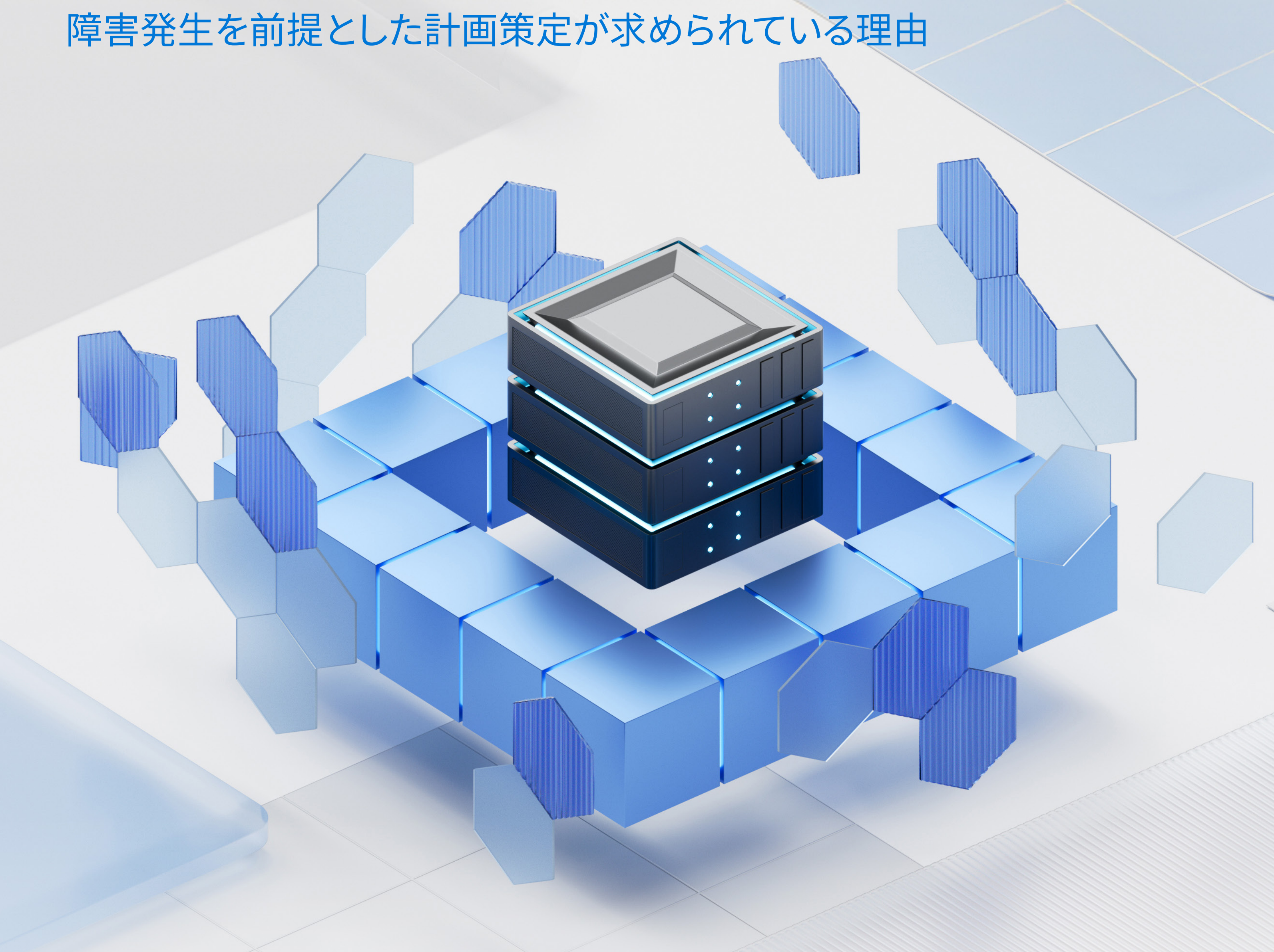
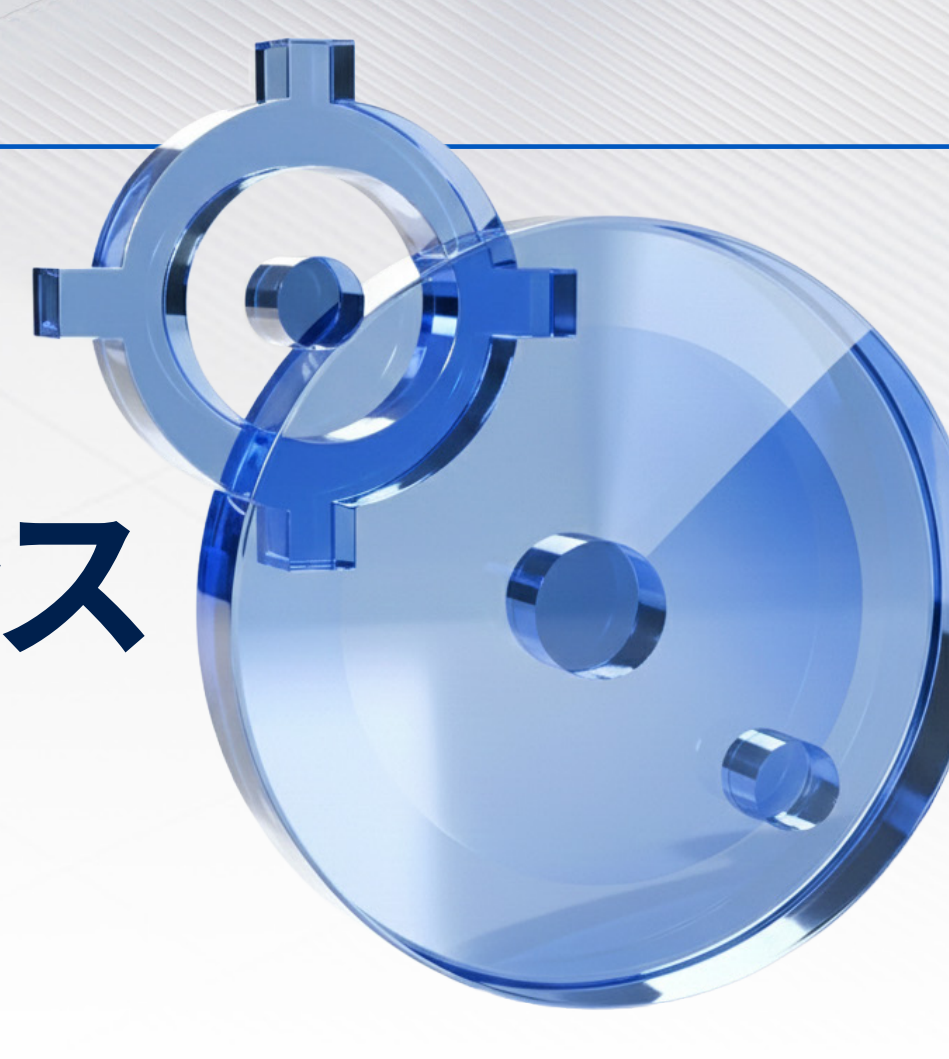
Acronis

サイバーセキュリティの先へ：ビジネス継続のためのサイバーレジリエンス構築

現代の IT 管理者に、単なる予防だけではなく、
障害発生を前提とした計画策定が求められている理由





サイバーセキュリティ vs サイバーレジリエンス

サイバーセキュリティは、攻撃を止めることに焦点を当てます。サイバーレジリエンスは、攻撃の最中および攻撃後もビジネスを継続させることを保証します。

サイバーセキュリティ
防御 、境界線防御、侵害の回避

サイバーレジリエンス
適応力、復旧、事業継続

業界別のビジネス継続性への影響

なぜ主要産業においてサイバーレジリエンスが重要なのか

ダウンタイムとサイバー攻撃による混乱はあらゆるセクターに影響を及ぼしますが、その結果は業界によって異なります。

ヘルスケア

60%

医療機関の60%は、サイバーインシデントが患者のケアを直接妨げているとレポートしています。[1]

なぜ重要？
ダウンタイムは治療の遅れを招き、患者を別の施設へ迂回させ、さらには安全性を損なう可能性があります。

小売

43%

小売業者の43%は、過去 1 年間に IT またはサイバーインシデントによる大規模な障害を経験しています。[2]

なぜ重要？
わずかな中断であっても、収益、在庫の可視性、そして顧客体験に影響を及ぼします。

金融サービス

91%

金融機関の91%は過去 1 年間に少なくとも 1 件のサイバーインシデントを経験しています。[3]

なぜ重要？
ダウンタイムは取引処理、顧客の信頼、および規制遵守に影響を与えます。

物流および輸送[4]

94%

企業の94%はサイバー攻撃による混乱がサプライチェーンの連鎖的な失敗を引き起こす可能性があると述べています。[5]

なぜ重要？
ダウンタイムは出荷トラック、倉庫業務、ジャストインタイム配送を停止させます。

行政/政府

60%

60% の機関が、ネットワーク障害によって運用上の混乱から少なくとも 100 万ドルの損失を被っています。[6]

なぜ重要？
システム停止は市民サービス、緊急対応、社会的信頼に影響を及ぼします。

ダウンタイムは事業継続の失敗

ダウンタイムは、IT システムだけでなく、収益、業務、評判にも影響を及ぼします。

96%

組織のうち96%が過去 3 年間に少なくとも 1 回のダウンタイムを経験しています。

80%

組織の80%がシステム停止の深刻度が増していると回答しています。[7]

従来の冗長化がランサムウェア対策を失敗させる理由

冗長化はハードウェアの故障を防ぐものであり、高度で拡散する攻撃を防ぐものではありません。

レプリケーションが感染を拡大させる可能性がある

断片化したディザスタリカバリおよびバックアップツールは盲点を生む

ツールの乱立が復旧時間を長期化させ、運用の足かせとなる

現代のレジリエンスには新しい復旧指標が必要

スピードだけでは不十分。復旧はクリーンであり、ビジネスと整合している必要があります。

RTO
業務復旧までの最大時間

RPO
許容可能な最大データ損失

MTD
事業が破綻するまでの最大許容ダウンタイム

MTCR
検証済みのマルウェアのない環境を復元するまでの時間

クリーンな復旧は、今や事業継続の必須要件

復元されたシステムが汚染されていれば、迅速に復旧しても意味がありません。

- データ侵害の平均コスト：445 万ドル。
- 業務の中断は、データ侵害における最大のコスト要因です。[8]

ビジネス IT リーダーが優先すべきこと

レジリエンスは、経済的および運用上の意思決定です。

優先すべきアクション（ハイレベル）

資産の重要度に合わせて保護を最適化する。

実際のサイバー攻撃シナリオを想定した復旧テストを実施する。

復旧前にバックアップを検証する。

統合プラットフォームによって複雑さを軽減する。

サイバーレジリエンスにより、たとえ攻撃が避けられない場合でも、継続性、信頼性、および制御が可能に

アクロニスのソリューションで、サイバーセキュリティからサイバーレジリエンスへ

サイバーセキュリティは、単なる保護以上のものを必要とします。それにはレジリエンスが必要です。アクロニスが、脅威の予測、攻撃への耐性、迅速な復旧、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

---

[1] 米国保健福祉省 (HHS)
https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute。「Annual Outage Analysis 2023（2023年 年間障害分析）」
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] 世界経済フォーラム。「Global Cybersecurity Outlook 2024（グローバルサイバーセキュリティ展望 2024）」
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] 世界経済フォーラム: グローバルリスクレポート
https://www.weforum.org/reports/global-risks-report-2024

[5] 同上

[6] Intelligent CIO。「米国の政府機関は、平均的なネットワーク停止または侵害により数百万ドルを失っている」
https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute。「Annual Outage Analysis 2023（2023年 年間障害分析）」
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM。「Cost of a Data Breach Report 2025（データ侵害コスト報告書 2025）」
https://www.ibm.com/reports/data-breach

Acronis