サイバー
レジリエンスの実例

保護/検出/復旧におけるグローバル エンタープライズの対応状況ベンチマーク
インサイト考察
（2026年1月）

DELL Technologies

アジェンダ

- 目的と企業特性
- サイバー レジリエンスのギャップ
- 高度なセキュリティ
- 検出
- 復旧
- 複雑性、文化、次のステップ

ビジネスの目標

- Dellを、サイバー レジリエンス分野におけるソート リーダーおよび戦略的パートナーとして位置付ける
- 「データ保護」から「サイバー レジリエンス」への移行を再確認する

調査の目的

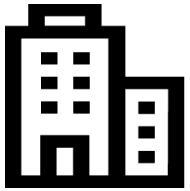
- サイバー レジリエンス戦略の成熟度と統合を評価する
- 組織における保護、検出、復旧の取り組みの有効性を評価する
- スキル ギャップ、予算、複雑さなど、サイバー レジリエンスの向上を妨げる障壁を理解する
- 組織がIT環境をどのように保護し、ランサムウェアの脅威からデータを守っているかを調査する

調査対象

回答者インタビュー
実施時期：2025年7月
および10月

グローバル企業のIT
導入決定者850人

社員数1,000人以上
の組織



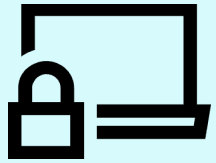
官民の幅広い業界の
組織が対象

回答者：取締役、経営幹部、
上級管理職、中間管理職

主な調査結果

39%

サイバー レジリエンス戦略を十分に確立し、継続的に最適化している組織の割合



継続的な最適化が重要です。これがなければ、進化する脅威に対する戦略はすぐに時代遅れとなり、組織のリスクが高まります。

46%

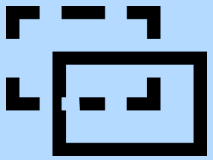
バックアップ データが本来あるべき方法で保護されていないと認識していた回答者の割合

プライマリー システムが侵害された場合でもリカバリーを可能にするには、バックアップ保護の強化が不可欠です。

高度なセキュリティ

30%

ネットワーク、バックアップ、プライマリー ストレージ全体で脅威を検出する包括的なプラットフォームを使用している組織の割合



統合された検出がなければ、脅威の可視性が低下し、対応が遅れることで、侵入を見逃すリスクが高まります。

検出

55%

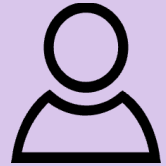
ドリル/サイバー インシデントからの復旧に月1回以上の頻度で成功している回答者の割合

頻繁なテストは、実際のインシデントへの備えとして有効です。準備が不十分なチームは、最も重要な局面で対応や復旧が遅れるリスクがあります。

復旧

63%

大規模なサイバー イベントに対する組織の準備状況を、経営層が過大評価していると考えている回答者の割合



自信過剰は、投資を停滞させ、対応計画を遅延させ、重大な脆弱性に対処できない可能性があります。

セクション1：サイバー レジリエンスのギャップ

現状の課題と、進化の必要性を明らかにする

レジリエンス戦略の継続的な最適化はリカバリーを向上させるが、成功は保証されない

99.5%

何らかのサイバー レジリエンス戦略を策定している組織の割合

39%

完全に確立され、継続的に最適化されている（成熟した戦略）と考えている組織の割合

57%

前回のテストまたはインシデント時に効果的な封じ込めとリカバリーができなかった回答者の割合

成熟したサイバー レジリエンス戦略を持つ組織は、**リカバリーに成功する可能性が2.6倍高い**

65% vs。**25%**

63%

主要なサイバー イベントへの対応力を、**経営層が過大評価している**と考える回答者の割合

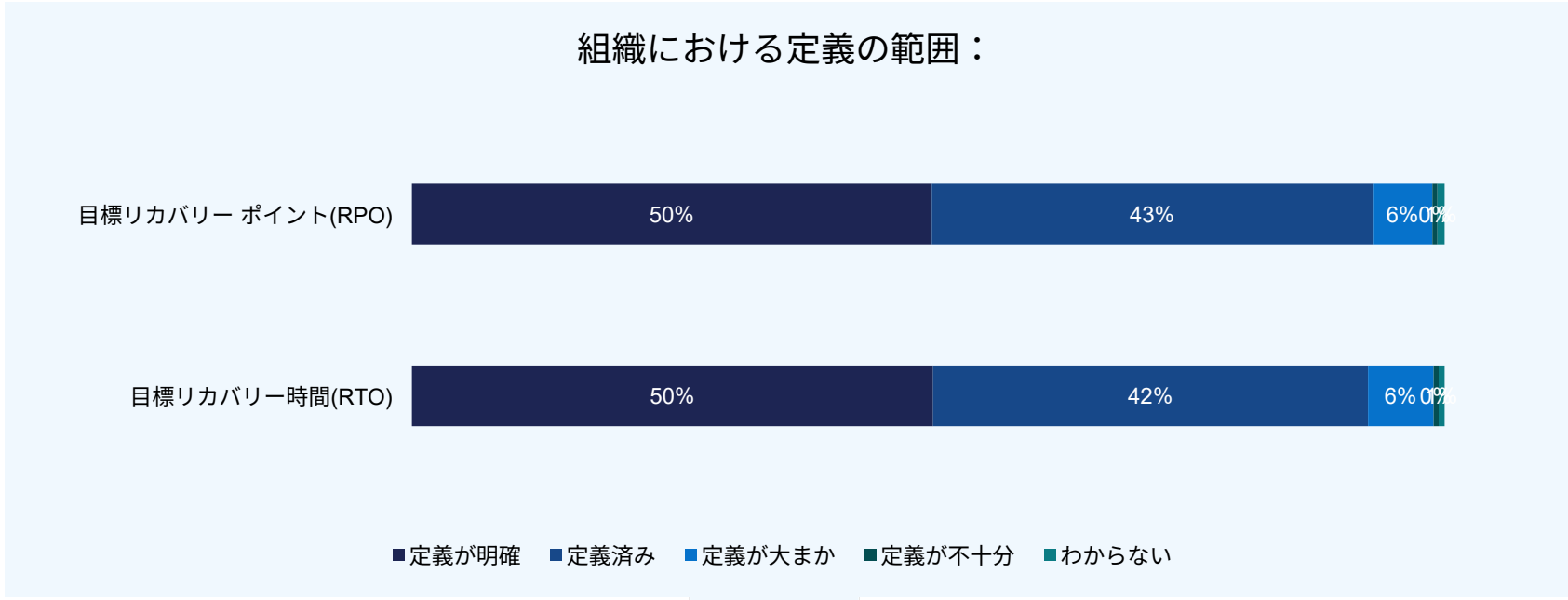
今、なぜ重要なのか

97%

脅威の進化に対応して、組織のセキュリティを継続的に強化する必要があると考える回答者の割合

78%

組織が、攻撃からのリカバリーへの備えよりも、攻撃の防止に重点を置いていると考える回答者の割合



32%

両方の領域が明確に定義されている両方の領域が明確に定義されている

成熟したサイバーレジリエンス戦略を持つ組織のうち

58%

RTOとRPOの両方が明確に定義されている

セクション2：保護

攻撃の防止とデジタル資産の強化

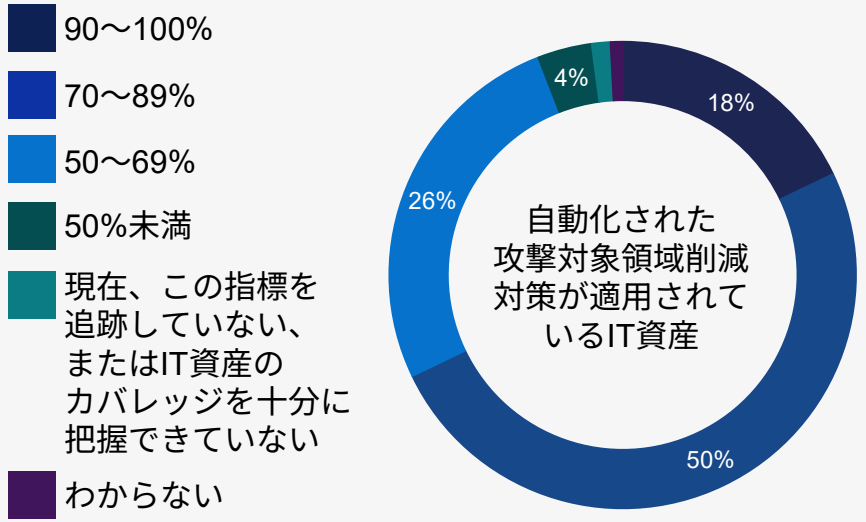
可視性の欠如と保護の不備

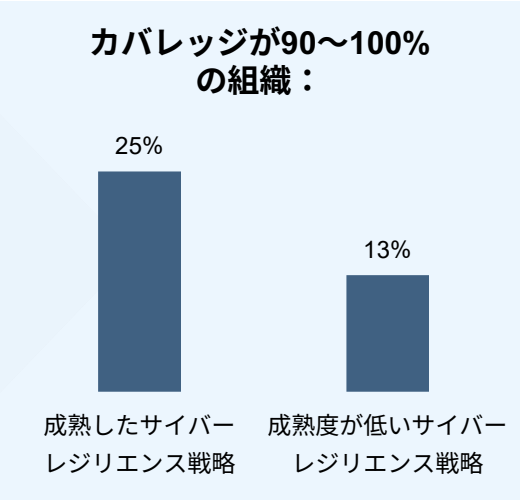
46%

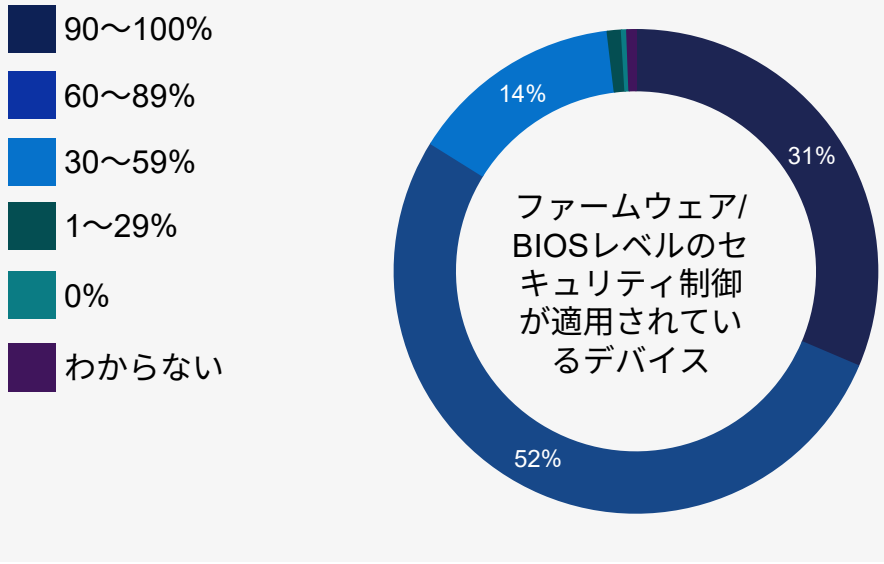
バックアップ データが本来あるべき水準で保護されていないと認識している回答者の割合

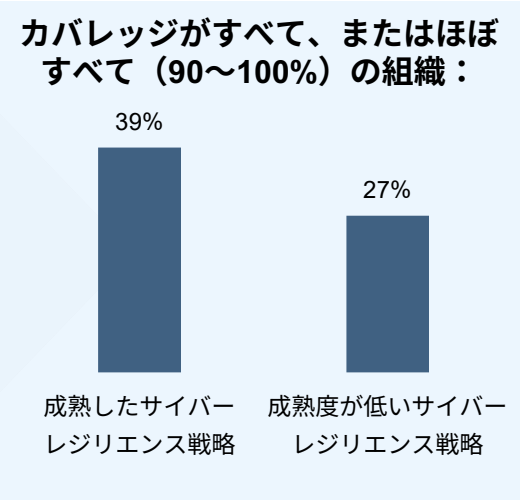
NA	**59%**
EMEA	**43%**
LATAM	**41%**
APJ	**39%**

継続的な最適化だけでカバレッジ ギャップを解消できるわけではないが、レジリエンスにおいて重要な優位性をもたらす









導入前の完全性から攻撃後のリカバリーまで：セキュリティの両端を強化

ITハードウェア/ソフトウェアの完全性を確保するために組織が用いるプロセス/方法

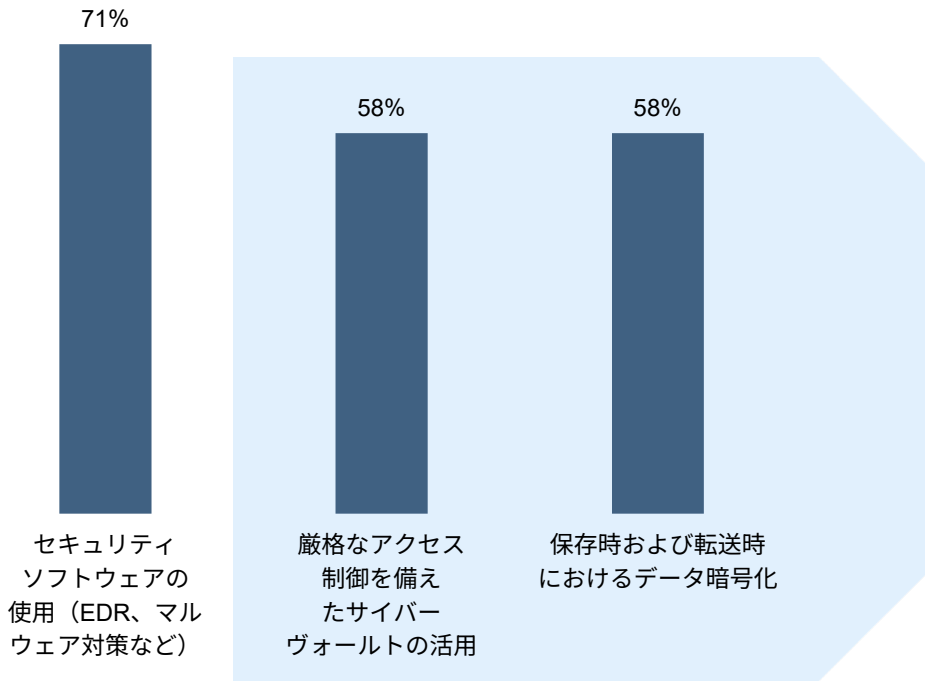
72%

認証や証明、ならびにコンポーネントの完全性を検証する組み込みツールを備えたシステムについて、ベンダーに依存している回答者の割合

64%

ステージング/導入時に内部監査または手動レビューを実施する割合

ランサムウェア攻撃から重要なデータを保護するために組織が用いる方法



成熟したレジリエンス戦略を持つ組織は、次の手法を利用する可能性が高い：

- **データ暗号化 (59%vs 57%)**
- **サイバー ヴォールト (63%vs 55%)**

（レジリエンス戦略の成熟度が低い組織との比較）

セクション3：検出

被害が及ぶ前に脅威を検知し、対応する

AIと自動化の活用により、バックアップが侵害される前に脅威を発見できる可能性がある

38%

プロアクティブな緩和策および対応プレイブックを備えたAI/MLツールを使用している組織の割合

成熟したサイバー レジリエンス戦略を持つ組織は、これを実施する可能性が**3.1倍高い**

65% vs。**21%**

48%

侵入の兆候を検出するために、**バックアップ データのスキャンにAI/MLを広範に使用している**組織の割合

成熟したサイバー レジリエンス戦略を持つ組織では、AI/MLの**広範な使用が2.3倍の頻度で見られる**

72% vs。**32%**

83%

ランサムウェア攻撃時に、攻撃者が**バックアップを狙うケースが増えている**と考えている回答者の割合

62% が、自動化およびAI/MLを活用した脅威検出への投資を優先している

可視性の不足によりリスクが増大

54%

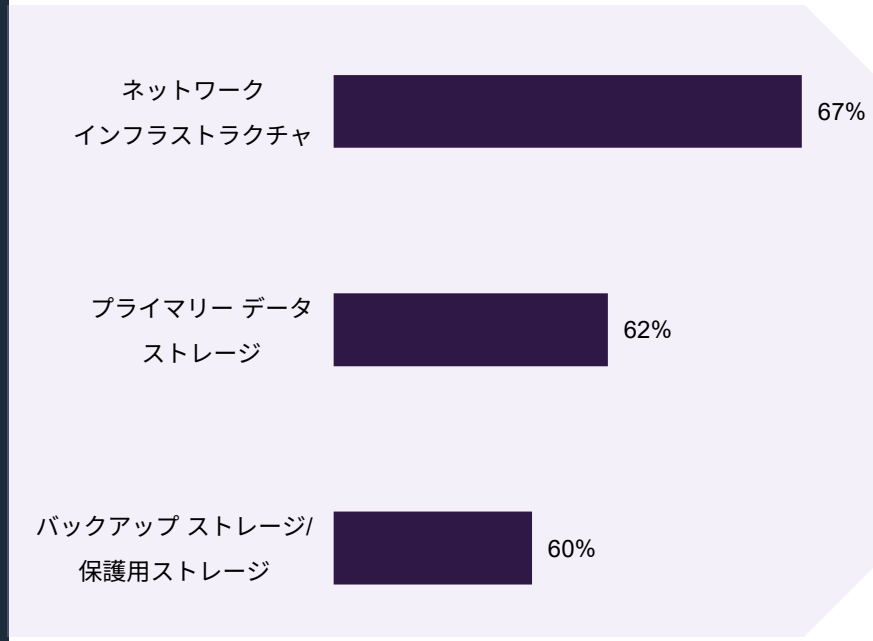
バックアップ システム内の疑わしい活動や侵害されたデータについて、高い可視性を確保していると回答している割合

74% 成熟したサイバー レジリエンス戦略を持つ組織の割合

vs

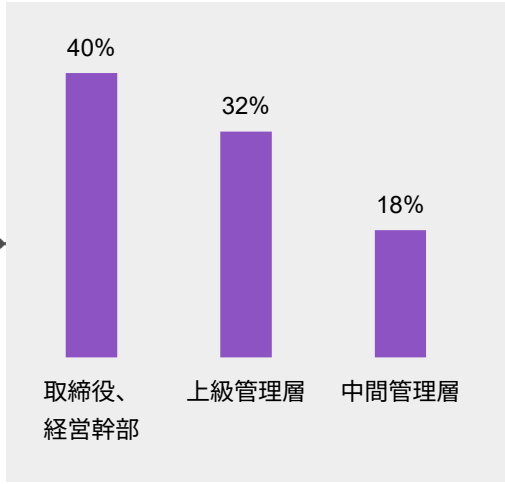
42% サイバー レジリエンス戦略の成熟度が低い組織の割合

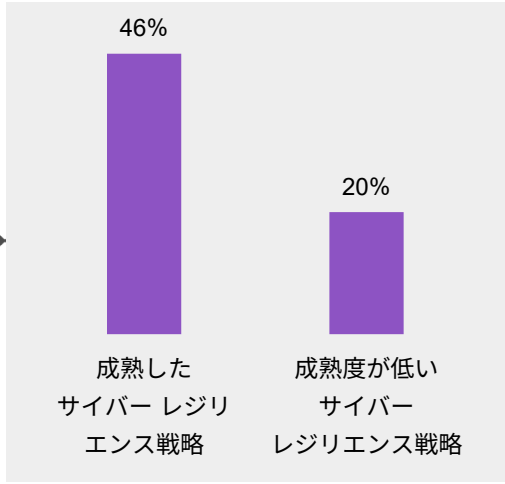
次の領域にわたって脅威を検出するための堅牢なプラットフォームを持つ組織



30%

3つの領域すべてをカバーする包括的なプラットフォームを導入している割合





セクション4：復旧

SLAで期待される範囲内で迅速に復旧

復旧の状況：多くの組織は目標を達成しているが、脅威環境に追随し続けるには継続的な改善が不可欠

40%

最小限の影響で**封じ込めと復旧に成功したと回答している組織の割合**

取締役(53%)は、**中間管理職(30%)**よりもこのように回答する割合が高い

54%

RTO/RPOの目標を達成した組織の割合

役職別：取締役(66%) / 中間管理職(45%)

第4位

サイバーセキュリティ投資の主な推進要因は、組織における**最近のサイバー インシデントやニアミス**

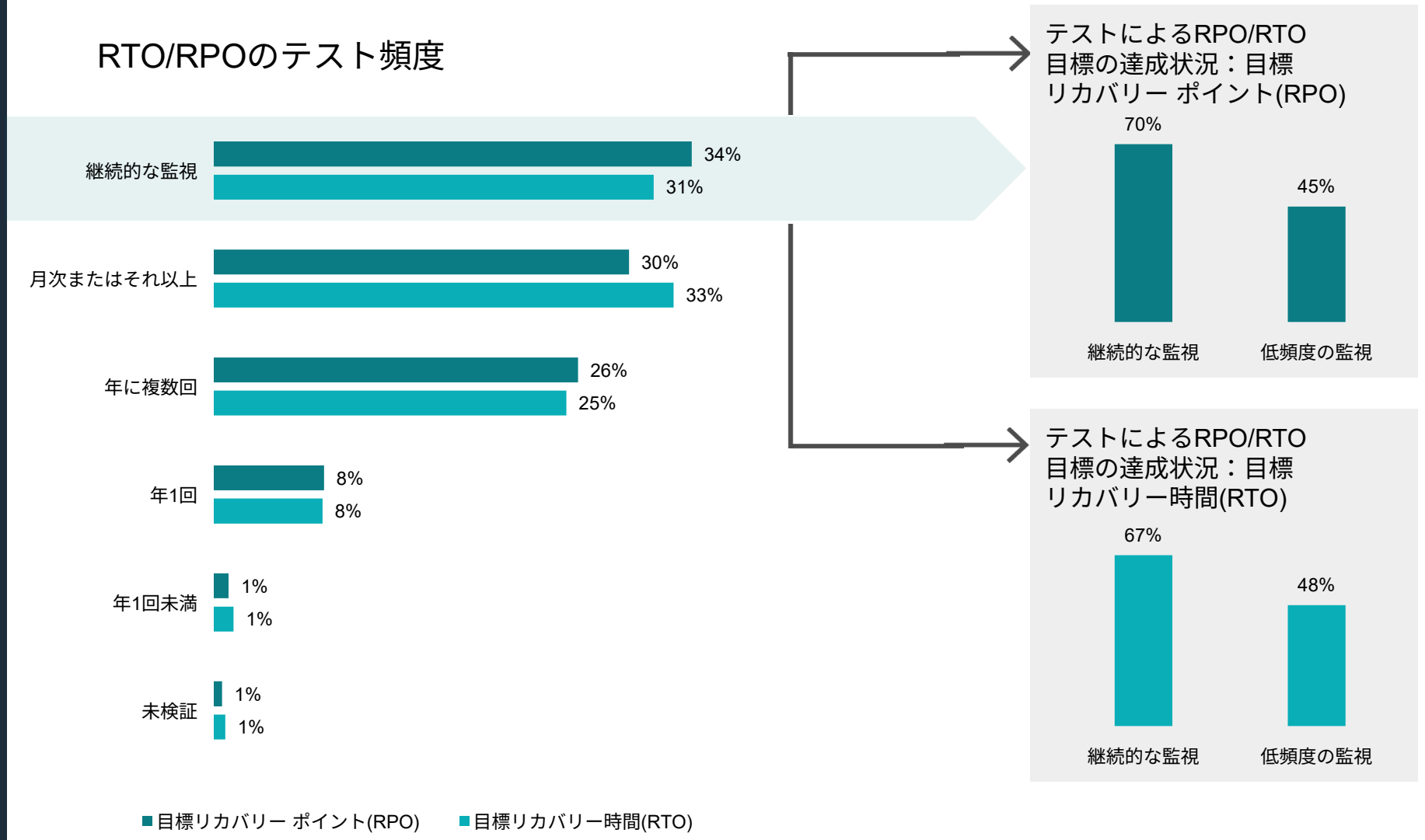
57% が、**規制またはコンプライアンス要件を満たす**ためにレジリエンス機能を強化している

テストはレジリエンスに不可欠であり、組織の復旧成功率を高める

頻繁なテストは、リカバリーの向上につながる可能性がある

最終的にレジリエンスを築くのは、常に注意を怠らず、継続的に改善する文化です

ブラジルの消費者サービス業界におけるシニア マネージャー



テストはレジリエンスの基盤

48%

サイバーセキュリティ テストが現代の攻撃手法を現実的に再現していないと回答した組織の割合

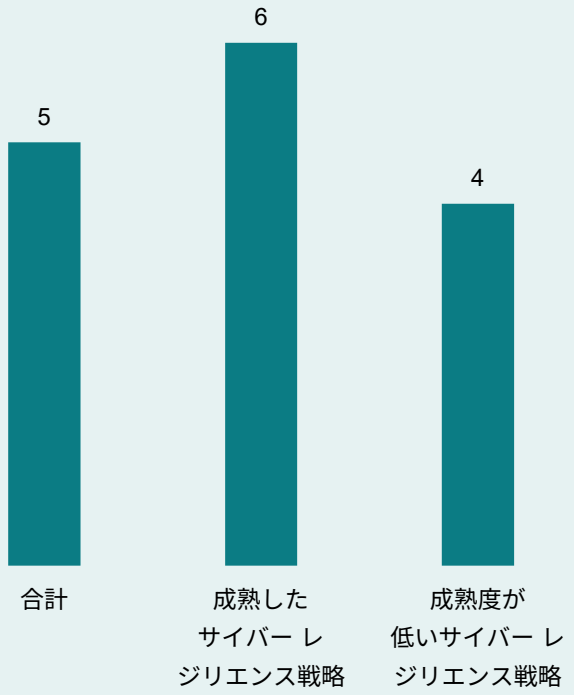
53% 取締役、経営幹部の割合

vs

48% 中間管理層の割合

復旧力を高めるには定期的な訓練が不可欠だが、進化する脅威に備えて継続的な計画も求められる

組織がサイバー攻撃の模擬訓練を実施する年間平均回数



55%

ドリル/サイバー インシデントからの**復旧に月1回以上の頻度で成功**している回答者の割合

35%

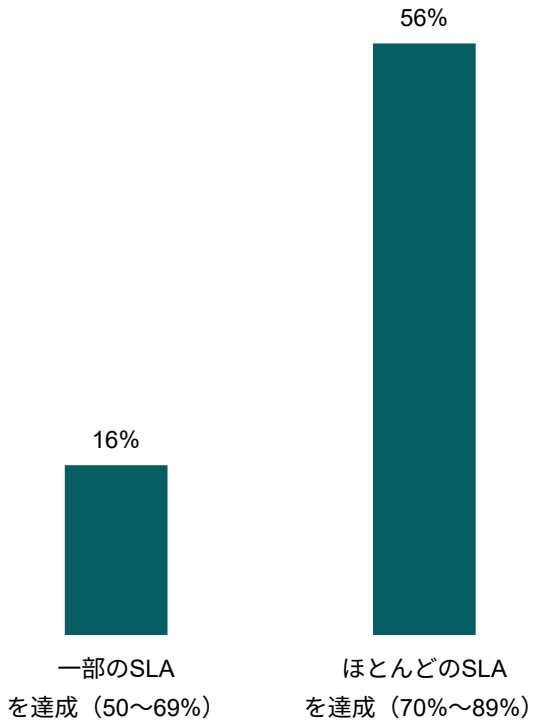
ドリル/サイバー インシデントからの**復旧に月1回未満の頻度で成功**している回答者の割合

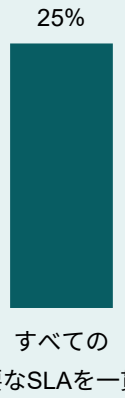
> *個別ポイントのカバレッジやテストに注力するのではなく、すべての潜在的な脅威領域を横断して総合的にテストと評価することが重要です*
>
> 英国のITテクノロジーおよび通信分野のシニア マネージャー

> *サイバー攻撃は、定期的なセキュリティ ドリルの重要性を改めて認識させてくれます。*
>
> *セキュリティ意識向上トレーニングを強化したことで、すべての従業員が潜在的な脅威を特定できるようになりました*
>
> オーストラリアの建設/不動産分野の取締役

SLAは証明となる指標：成熟した戦略を持つ組織は、復旧に関する約束を実行できている

重要なシステムの復旧において、SLAを達成している組織の頻度



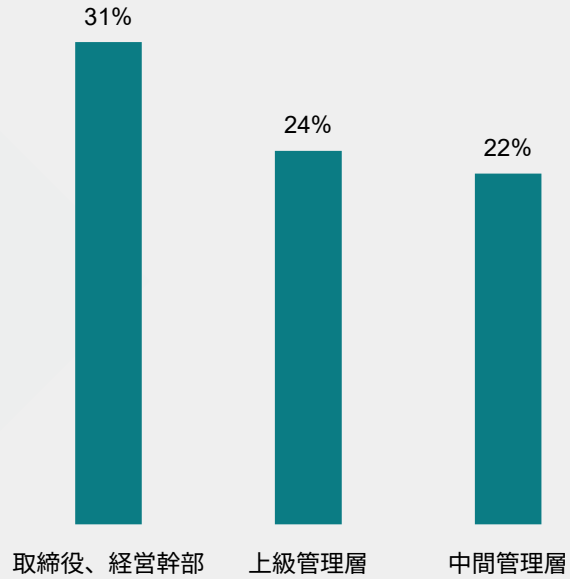


2倍

成熟したサイバー レジリエンス戦略を持つ組織は、SLAを一貫して達成できる可能性が高い

36% vs 。**18%**

職位別：



セクション5：複雑性、文化、次のステップ

組織的な障壁と将来の投資計画

複雑性、スキル ギャップ、自信過剰がサイバー レジリエンスを脅かす一方で、AIとトレーニングが打開策となり得る

主な課題：

複雑なIT環境	49%
予算の制約	42%
熟練人材の不足	39%
ベンダー/ツールの断片化	38%
経営層による優先度の低さ	23%

大規模な組織ほど直面しやすい課題：

- 50% 従業員5,000人以上
- 50% 従業員3,000～4,999人
- 46% 従業員1,000～2,999人

63%

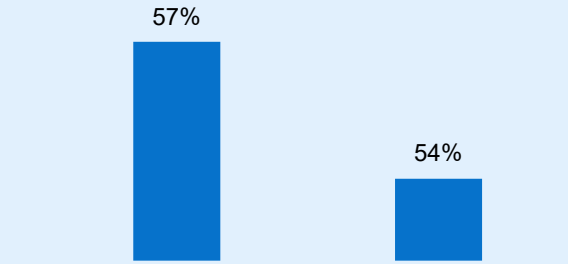
大規模なサイバー イベントに対する組織の準備状況を、経営層が過大評価していると考えている回答者の割合

96%

サイバー セキュリティのスキルや専門性の不足を認識している割合

しかし...

組織が取っている対応：



今後の投資に向けた展望

第1位

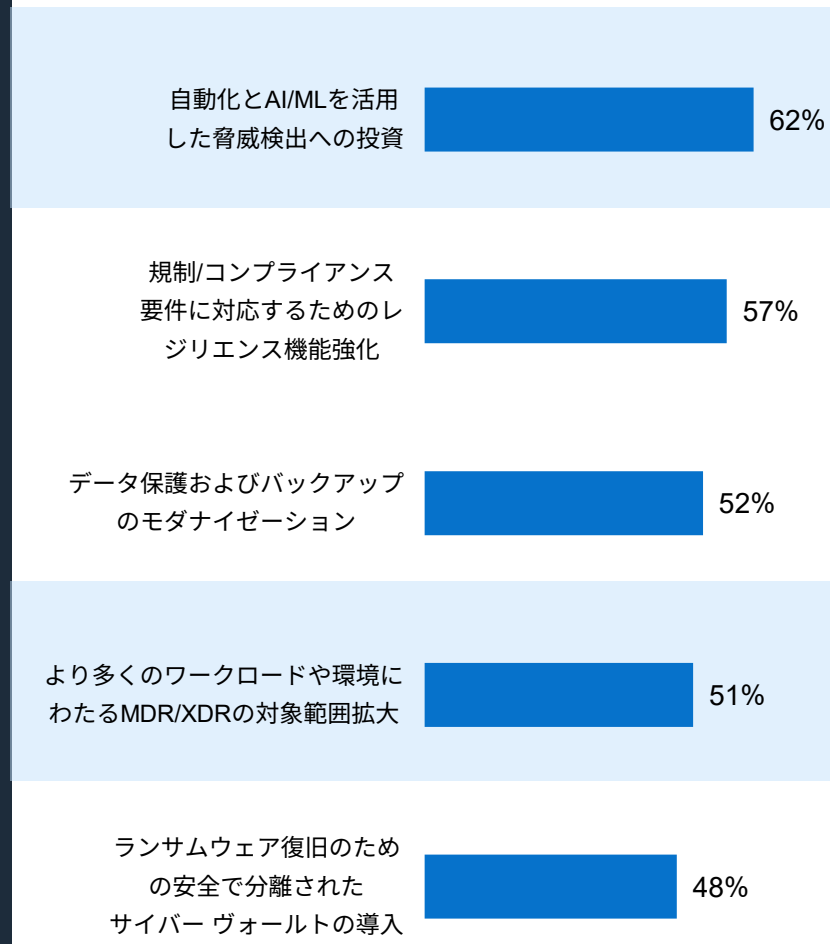
投資の原動力は、
進化する脅威環境

97%

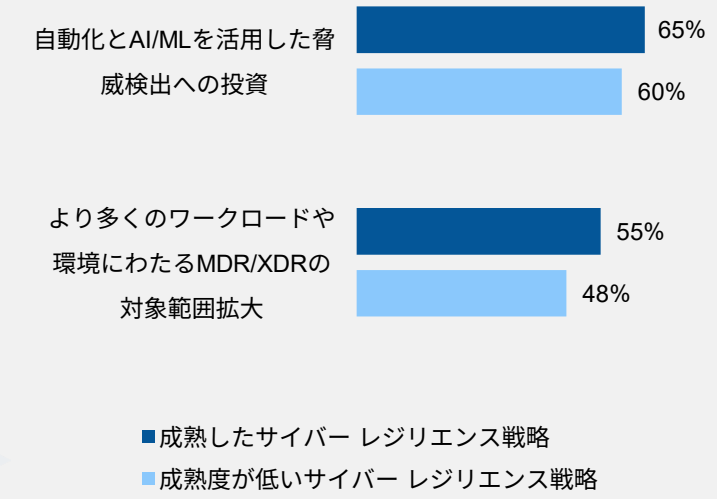
「脅威が進化する中で、
私たちの組織は
セキュリティを継続的
に強化する必要があります」

成熟した状態を維持するには、継続的な投資と最適化が不可欠

今後12か月間におけるサイバー レジリエンス投資の優先分野



成熟したサイバー レジリエンスを備える組織は、継続的に投資している

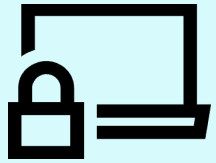


重要なポイント

主な調査結果

39%

サイバー レジリエンス戦略を十分に確立し、継続的に最適化している組織の割合



継続的な最適化が重要です。これがなければ、進化する脅威に対する戦略はすぐに時代遅れとなり、組織のリスクが高まります。

46%

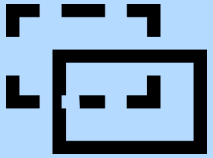
バックアップ データが本来あるべき方法で保護されていないと認識していた回答者の割合

プライマリー システムが侵害された場合でもリカバリーを可能にするには、バックアップ保護の強化が不可欠です。

高度なセキュリティ

30%

ネットワーク、バックアップ、プライマリー ストレージ全体で脅威を検出する包括的なプラットフォームを使用している組織の割合



統合された検出がなければ、脅威の可視性が低下し、対応が遅れることで、侵入を見逃すリスクが高まります。

検出

55%

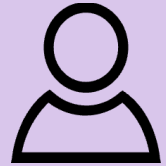
ドリル/サイバー インシデントからの復旧に月1回以上の頻度で成功している回答者の割合

頻繁なテストは、実際のインシデントへの備えとして有効です。準備が不十分なチームは、最も重要な局面で対応や復旧が遅れるリスクがあります。

復旧

63%

大規模なサイバー イベントに対する組織の準備状況を、経営層が過大評価していると考えている回答者の割合



自信過剰は、投資を停滞させ、対応計画を遅延させ、重大な脆弱性に対処できない可能性があります。

DELL Technologies