サイバー レジリエンスに関するインサイト

APJにおけるサイバー レジリエンスのギャップ、進化する脅威、AI主導の防御、およびリカバリー戦略の調査

サイバー攻撃とデータ保護のギャップにより、中断のリスクが高まる中、サイバー レジリエンスの課題が深刻化しています。成熟したレジリエンス戦略*を持つ組織は、リカバリーに成功する可能性がおよそ3倍高くなっています。レジリエンス戦略をモダナイズし、検出機能を強化し、継続的な最適化を優先することで、ITリーダーはリスクを最小限に抑え、進化する脅威に適応する能力に対する自信を深めることができます。

リーダーの自信過剰

ITプロフェッショナルの74%が、自社の経営陣がサイバー イベントの準備状況を過大評価していると考えています。自信過剰な人が主導権を握ると、重要な投資が遅れ、脆弱性に対処できない危険な死角が生まれます。

自信と機能のギャップ

99.3% サイバー レジリエンス戦略を実施している組織の割合

さらに、**55%** 前回のテストまたはインシデントから効果的にリカバリーできなかった割合

予防とリカバリー：アンバランスなアプローチ

87% 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

しかし、わずか **30%** プライマリー ストレージ、バックアップ ストレージ、ネットワーク インフラストラクチャ全体で脅威を検出するための包括的なプラットフォームを持っている組織の割合

そして、わずか **41%** 攻撃またはサイバー インシデントの訓練において、最小限の影響で封じ込めとリカバリーに成功した割合

結果として、侵害が避けられない形で発生した場合に、多くの組織はビジネスの存続を左右する回復フェーズの準備ができていません。

今後の取り組み：
成熟した組織が成果を達成

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およそ2.8倍高い

3本の重要な柱に関する戦略の成熟による相乗効果で、破られることのないレジリエンスを生み出す

安全性：
信頼基盤の構築

成熟したサイバー レジリエンス戦略を持つ組織には、次の特徴があります。

- ファームウェア/BIOSレベルのセキュリティ制御を使用してデバイスを保護している可能性が**1.8倍**高い
- 静止データと転送中のデータに暗号化を活用している可能性**が高い**
- サイバー ヴォールトを使用して進化する脅威から重要なデータを保護している可能性**が高い**

ただし、セキュリティは始まりにすぎません。真のメリットは、最も価値ある資産が侵害される前に脅威を検出するインテリジェントな検出機能です。

検出：
常時稼働のインテリジェンス

可視性の課題：
バックアップ ストレージ、プライマリー データストレージ、ネットワーク インフラストラクチャ全体で堅牢な脅威検出を行っている組織はわずか30%

AIを活用したソリューション：

- **57%が**AI/MLを活用した脅威検出への投資を優先している
- **52%が**AI/ML技術を用いてバックアップ データを詳細にスキャンし、侵害の兆候を検出している
- 成熟した戦略を持つ組織は、AI/ML脅威検出ツールとともにプロアクティブな緩和および対応のプレイブックを活用している可能性が**2.3倍高い**

リカバリー：
備えとパフォーマンスを両立

テストのメリット：

- サイバー攻撃のシミュレーションを実施する頻度が月1回以上の組織の**61%**がインシデントからのリカバリーに成功
- テストの頻度が月1回未満である組織の**59%**が、インシデントから正常にリカバリーできなかった

結果：
頻繁にテストを行う組織は、散発的にテストを行う組織よりも、目標リカバリー時間と目標リカバリー ポイントの両方を達成する可能性が大幅に高くなります。

卓越したサイバー レジリエンスへの道筋

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2.3倍高い

堅牢な基盤の構築
予防と迅速なリカバリーの両方を優先します。

- ✓ **安全性**： BIOSレベルのセキュリティ制御、データ暗号化、重要なデータのサイバー ヴォールトにより、リスクを軽減します。
- ✓ **検出**： リアルタイムのAI/MLを使用して、プライマリー ストレージと保護ストレージを含むすべてのストレージにわたって脅威を検出し、対応します。
- ✓ **リカバリー**：リカバリーのテストを頻繁に実施 - 毎月リカバリーをテストする組織は、リカバリー目標を達成する可能性が大幅に高まります。

サイバー レジリエンスを強化する準備はできていますか？

サイバー レジリエンスを強化する準備はできていますか？『*Dell 2026 Cyber Resilience Insights Research*』の主な調査結果をすべてお読みください。

DELL Technologies

出典：Vanson Bourneとデル・テクノロジーズによる2025年サイバー レジリエンス調査

*成熟したサイバー レジリエンス戦略を持つ組織は、予測分析、自動化、リアルタイムのインサイト（脅威インテリジェンス フィード、ML主導の調整、改善を導くKPIなど）を使用して完全に確立された、また継続的に最適化される戦略を持つ組織として定義されます。