

デジタル トランスフォーメーション期のデータ保護

サイバー脅威、マルチクラウド、コンテナなど

APJ (中国を除く)

突発的で混乱を引き起こすような出来事は壊滅的な影響を及ぼす可能性があります。組織としてデータ保護対策を定期的に評価することでリスクを最小限に抑えることができます

65%

今後12か月の間にデータ ロスやシステムのダウンタイムなど、ディスラプティブなイベントの発生を懸念している割合

\$640,239

過去12か月間のデータ ロスの平均被害額 (米ドル)

サーバー攻撃の脅威が組織に迫っており、テレワーク社員の増加により状況は悪化していますが、防御や復旧の能力が十分であると確信している組織はほとんどありません。

68%

既存のデータ保護手段ではマルウェアやランサムウェアの脅威に対抗するには不十分だと感じている組織の割合

72%

テレワーク社員の増加に伴い、サイバー脅威によるデータ ロスの可能性が高まっていることを認めている組織の割合

66%

壊滅的なサイバー攻撃が発生した場合、重要なビジネス データのすべてを必ず復旧できるという確信がない組織の割合

最新のテクノロジーによって組織にデータ保護の課題が発生し、準備状況に影響することがある

82%

既存のデータ保護ソリューションでは、将来的なビジネス課題のすべてには対応できないと考えている組織の割合

70%

クラウド ネイティブ アプリケーションに投資または投資を計画している組織のうち、その適切なデータ保護手段の特定に苦労している組織の割合

67%

SaaSアプリケーションに投資または投資を計画している組織のうち、その適切なデータ保護手段の特定に苦労している組織の割合

パブリック クラウドまたはハイブリッド クラウドを採用しても、そうした環境向けに設計された専用データ保護ソリューションがなければ、データは新たなリスクに晒される可能性がある

15%

マルチ クラウド環境におけるワークロード保護は、契約しているクラウド サービス プロバイダーが責任を負うと考えている組織の割合

70%

長期的な保存のためにパブリック クラウドを利用している組織の割合

67%

パブリック クラウドをディザスタリーカバリー目的で利用している組織の割合

63%

パブリック クラウドまたはハイブリッド クラウドを利用している組織のうち、その環境全体にあるすべてのデータを保護できると自信がない組織の割合

As-a-Service製品は、多くの組織の関心を引き付け、保護の導入をシンプルにするための新たな可能性をもたらす

As-a-Service製品で優先度が高い3つの要素は、ネットワーク、バックアップ、ストレージ



77%

As-a-Serviceを求める理由として、柔軟性と最適化されたITオペレーションを挙げる組織の割合

86%

複数のベンダーから、As-a-Service製品の購入を希望する組織の割合

デジタル トランスフォーメーション期に組織がデータ保護を強化する方法とは？

データ保護の準備状況を評価する



サイバー レジリエンスを最優先にする



Dell EMCのデータ保護に統合する



DellTechnologies.com/gdplにアクセスして、先手を打つ方法をご確認ください。

デル・テクノロジーは、デジタルの未来を切り拓き、働き方、生き方、遊び方を変革しようとする組織や個人を支援します。データの時代に向けて、業界で最も広範かつ革新的なテクノロジーとサービスのポートフォリオをお客様に提供します。

Methodology

本調査は、Vanson Bourneが2021年2月～4月に実施したものです。回答者は、従業員数250名以上の民間および公共組織のIT導入決定者です。4つの地域から計1,000名を抽出しました。内訳は、南北アメリカ (米国、メキシコ、ブラジル) 200名、EMEA (英国、フランス、ドイツ、イタリア、南アフリカ、アラブ首長国連邦) 450名、APJ (オーストラリア、インド、日本、シンガポール、韓国) 250名、中国100名。

デル・テクノロジーの委託による