Global Data Protection Index：スペシャルエディション2024

主な調査結果：2023年10月

VansonBourne

DELL Technologies

主な調査結果における着目点

1
データ保護リスクの現状

2
増大するサイバー攻撃の脅威

3
マルチクラウドの利用

4
クラウド環境のセキュリティ確保

5つの重要なポイント

サイバー攻撃は
増加し続けている

サイバー攻撃の
コストが増加している

保険契約では
攻撃のコストを
十分にカバー
できない

生成AIの利用増が、
データの価値増大に
つながる可能性がある

サイバー攻撃のリスク
増大と財務的な影響の
増加につながっている

調査対象

IT導入決定者とITセキュリティ導入決定者1,500人を対象に、2023年9月と10月に聞き取り調査を実施

さまざまな業界の公共組織と民間組織が対象

従業員数250人以上の組織

4つの地域：

南北アメリカ(300)
EMEA (675)
APJ (375)
中国(150)

1. データ保護リスクの現状

データ保護手段に関する懸念が広がっており、組織は自信を持てず、脆弱な立場にいると感じている

60%

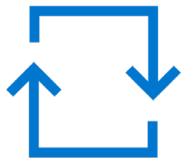
自分の組織が**バックアップ/リカバリーのサービス レベル目標(SLO)を満たしているかどうか**について、**「とても自信がある」以外**の回答を選んだ回答者の割合

79%

今後12か月以内に**破壊的な事象が発生することを懸念している**と答えた回答者の割合

75%

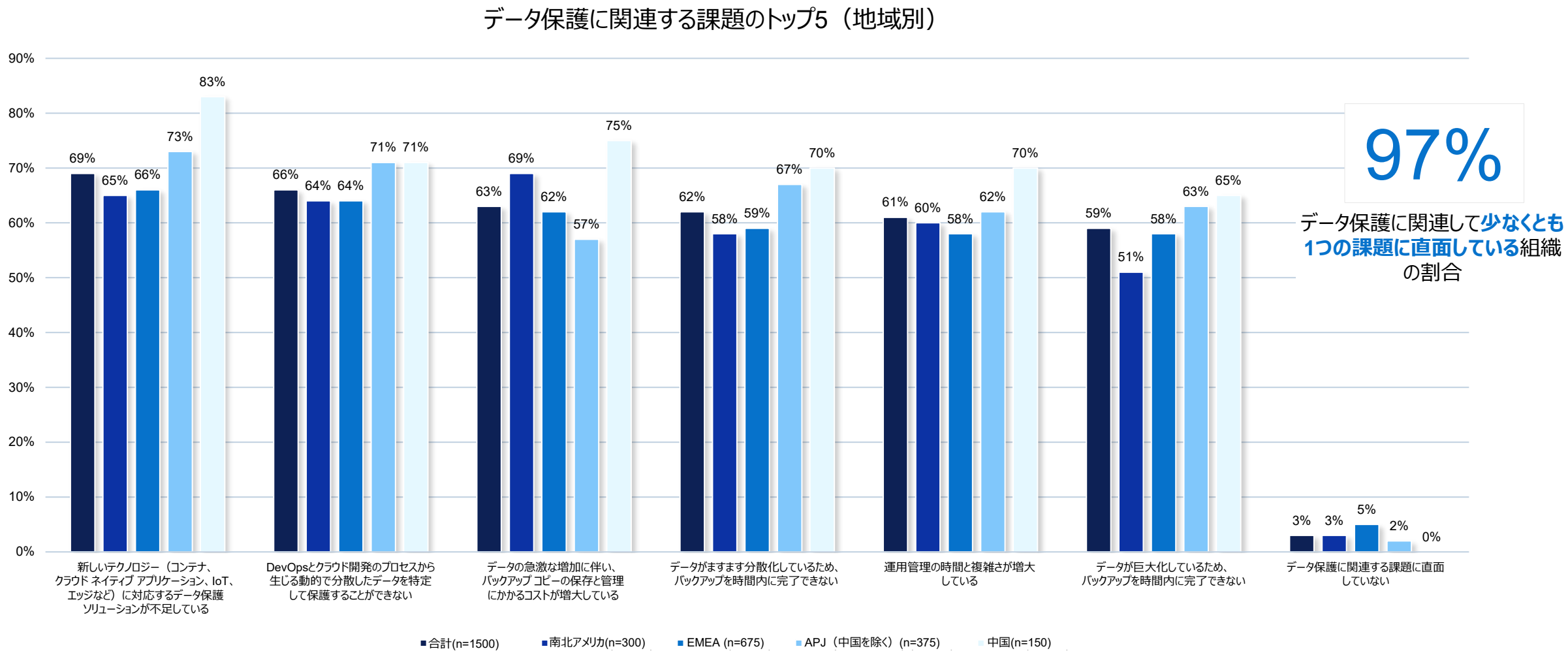
組織の既存のデータ保護手段では**マルウェアやランサムウェアの脅威に対処するのに十分でない可能性があると懸念**していると答えた回答者の割合



65%

データ ロス インシデントが発生した場合に、組織が**すべてのプラットフォームのシステムやデータを完全に復旧できるかどうか**について、**「とても自信がある」以外**の回答を選んだ回答者の割合

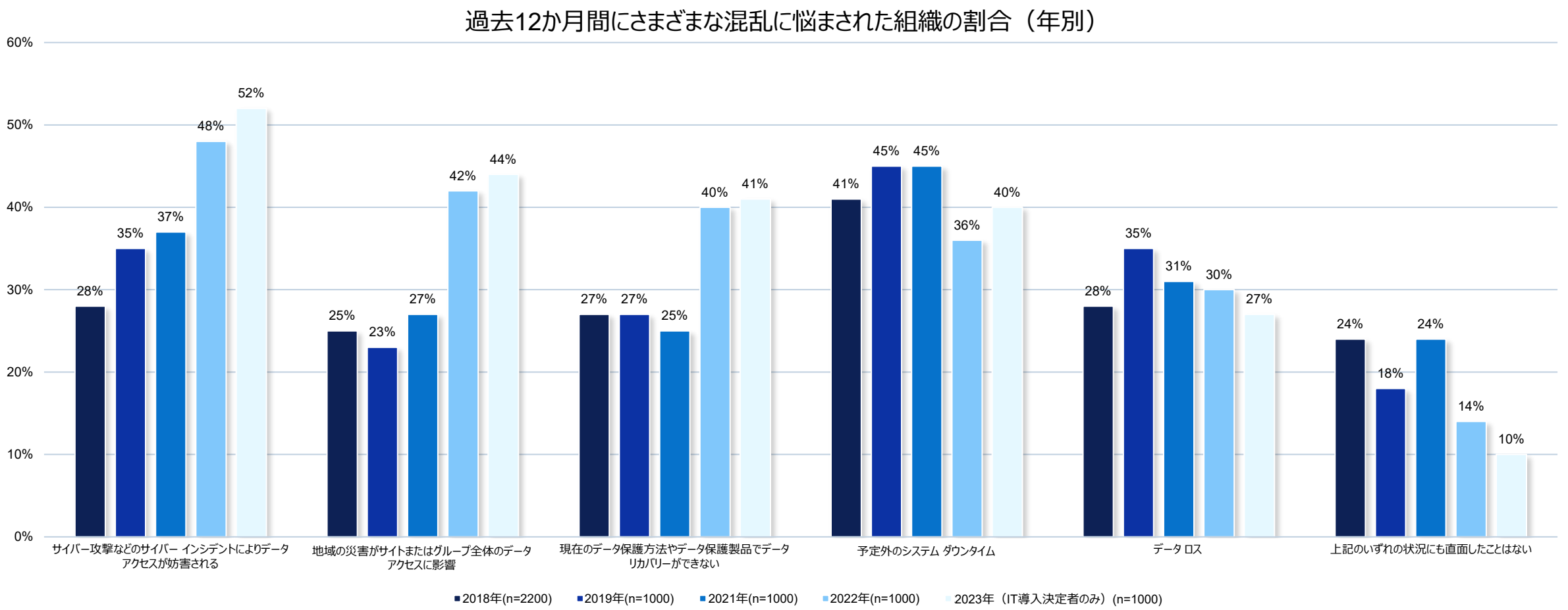
データ保護に関する懸念に加えて、多くの組織が課題に直面している



97%

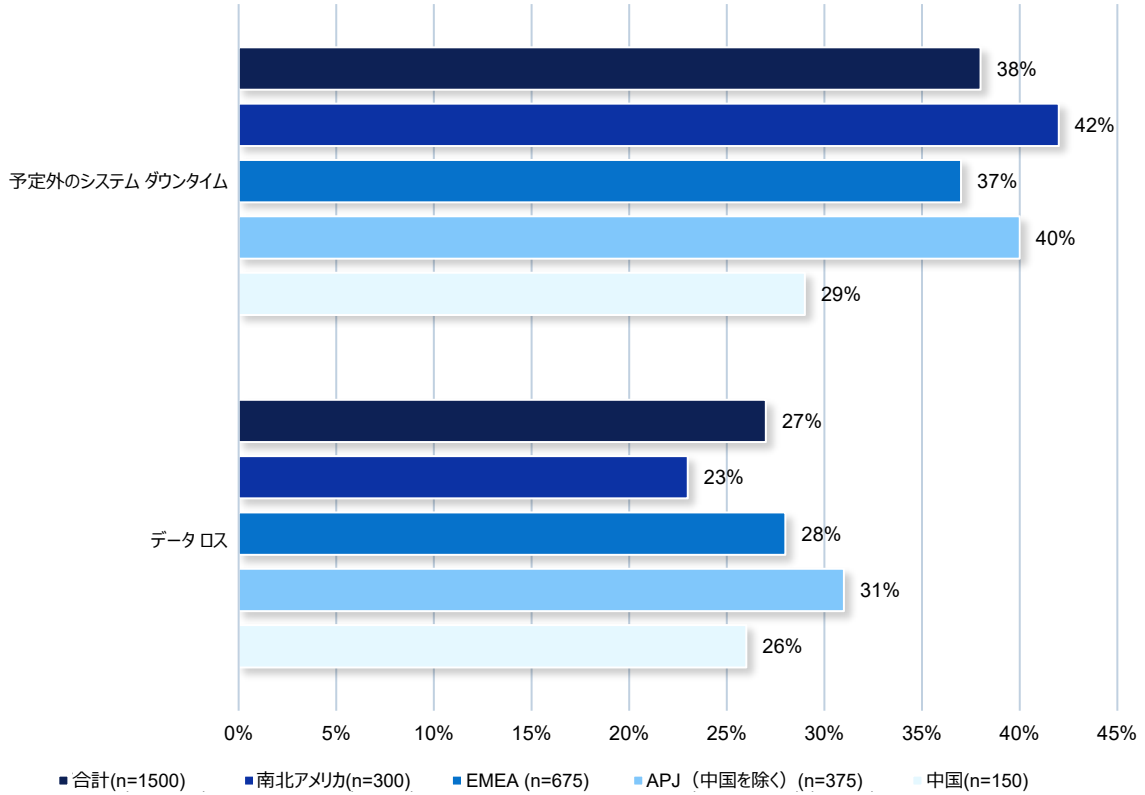
データ保護に関連して**少なくとも1つの課題に直面している**組織の割合

過去12か月間で、組織は重大な混乱に直面している。
また、サイバー攻撃による脅威は常に存在し、さらに増加している



データ ロスは混乱の要因となっただけでなく、最終損益にも影響を及ぼした

過去12か月間に予定外のシステム ダウンタイムやデータ ロスを経験した組織の割合（地域別）



過去12か月においては次のような状況でした。

26時間

組織が経験した**予定外のシステム ダウンタイム**（平均）

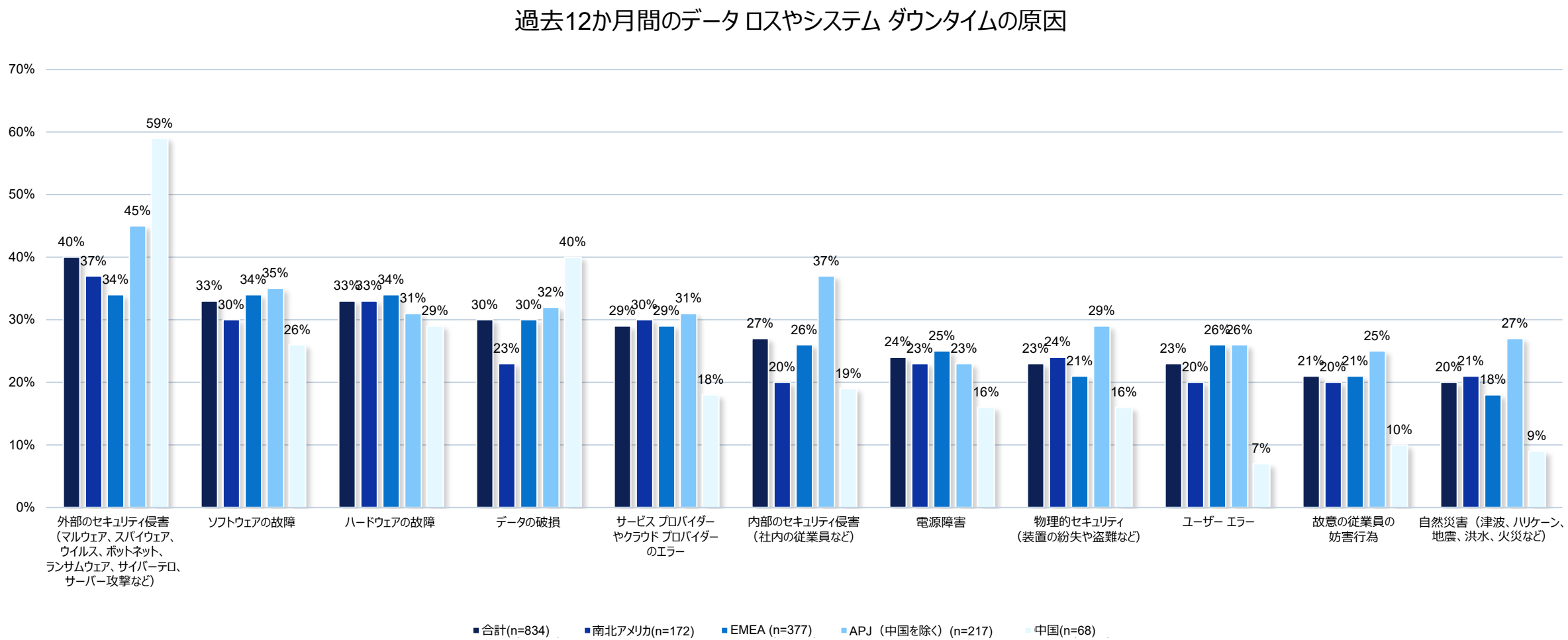
2.45TB

データ ロスの量（平均）

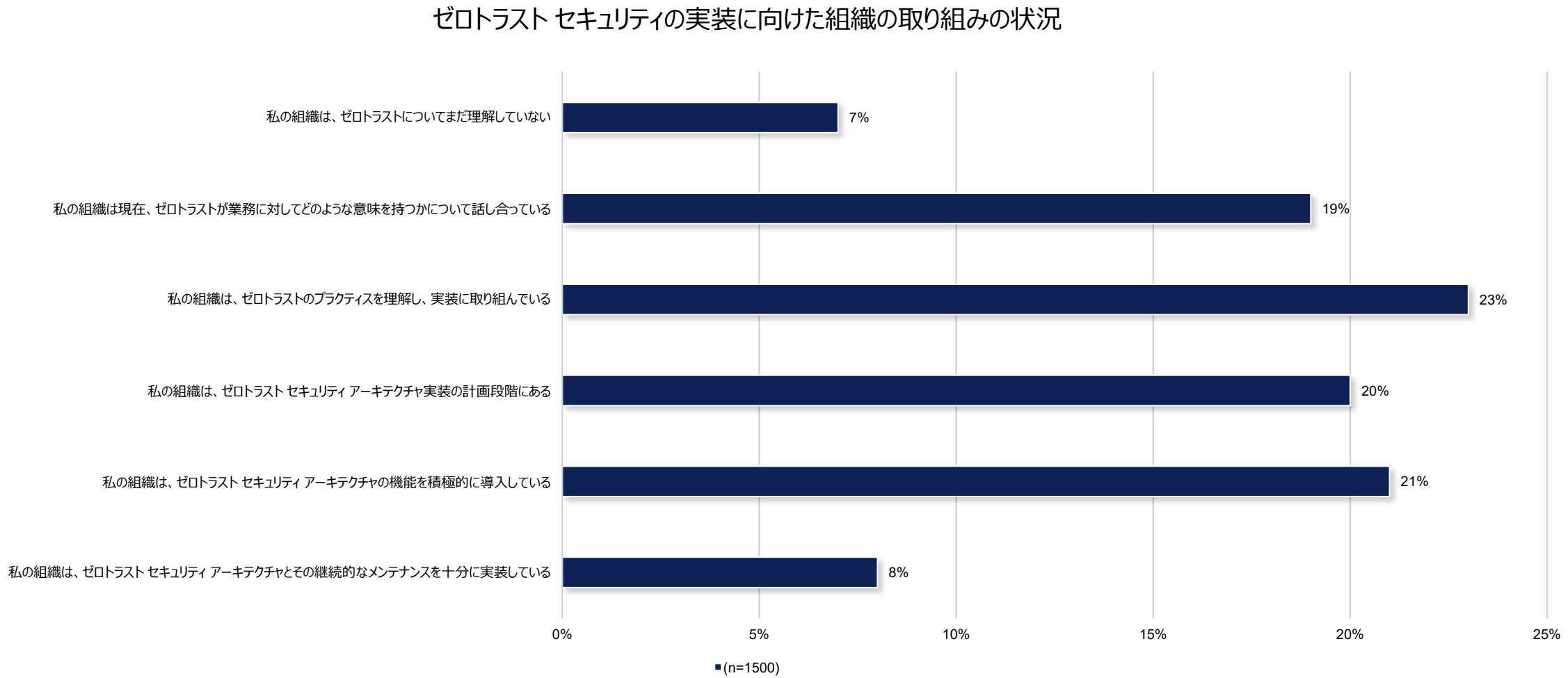
261万ドル

データ ロスのコスト（平均）

過去12か月間に発生したデータ ロスや予定外のシステム ダウンタイムの原因として最も多く挙げられたのは、外部のセキュリティ脅威



データ保護に関する課題や懸念があるにもかかわらず、ゼロトラスト セキュリティを十分に実装している組織はわずか

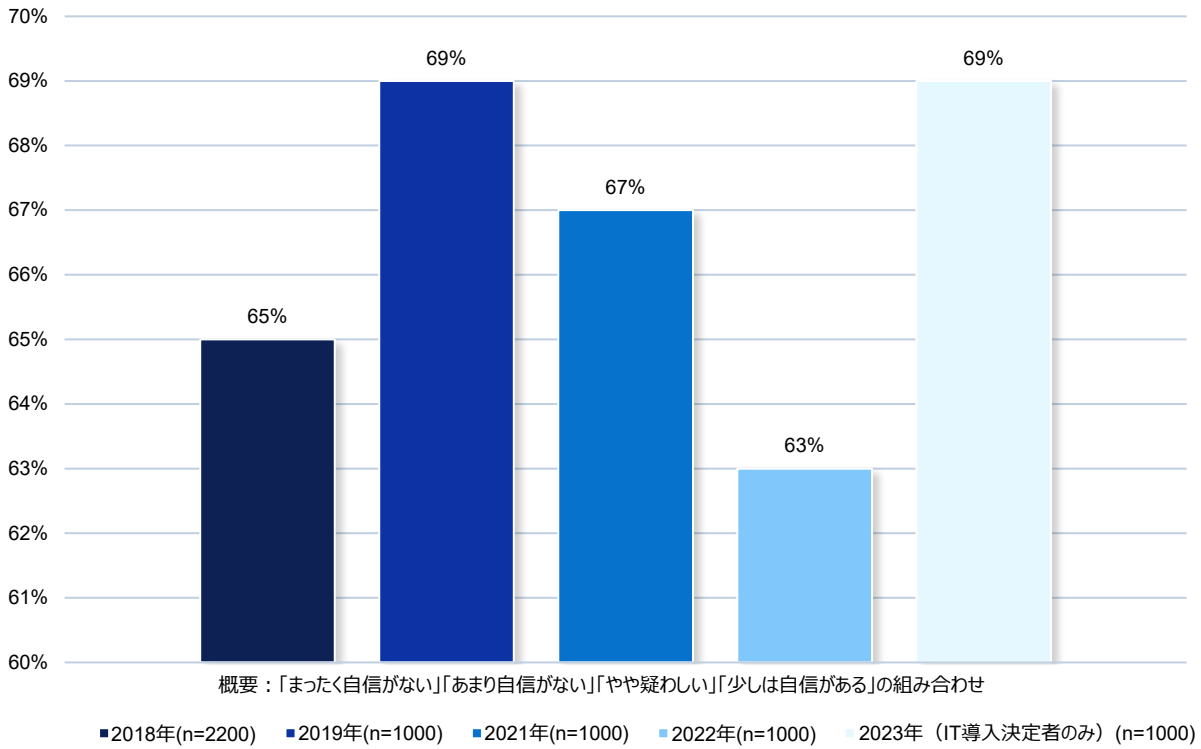


フィルター：データ、分割：地域 = 合計

2. 増大する
サイバー攻撃の脅威

データ保護手段に関する懸念が広がっており、組織は自信を持てず、脆弱な立場にいると感じている

壊滅的なサイバー攻撃が発生した場合、ビジネスクリティカルなデータすべてを復旧できるかどうかについて、「とても自信がある」以外を選んだ割合（年別）



81%

在宅で勤務する従業員の増加に伴い、自分の組織で**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**ことを認識している回答者の割合

74%

ランサムウェア攻撃によってバックアップ データの**感染または破損の可能性があることを懸念**していると答えた回答者の割合

リスクに加えて、ランサムウェア攻撃の結果に関する誤った過信が存在している

72%

業務と組織内の従業員が**ランサムウェア攻撃による影響を受けることはない**、と**考えている**回答者の割合

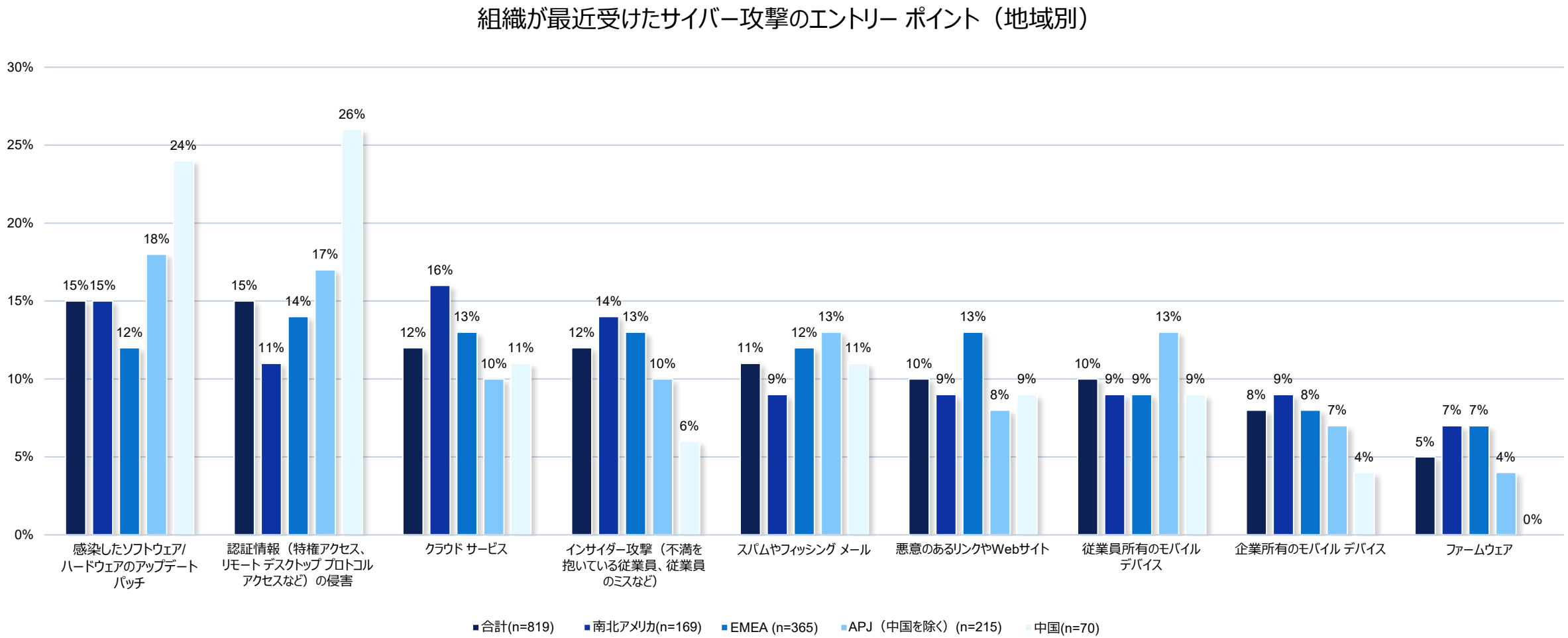
74%

組織がランサムウェア攻撃を受けた場合、**身代金を支払えばデータをすべて取り戻して**ビジネスを再開できる、と**考えている**回答者の割合

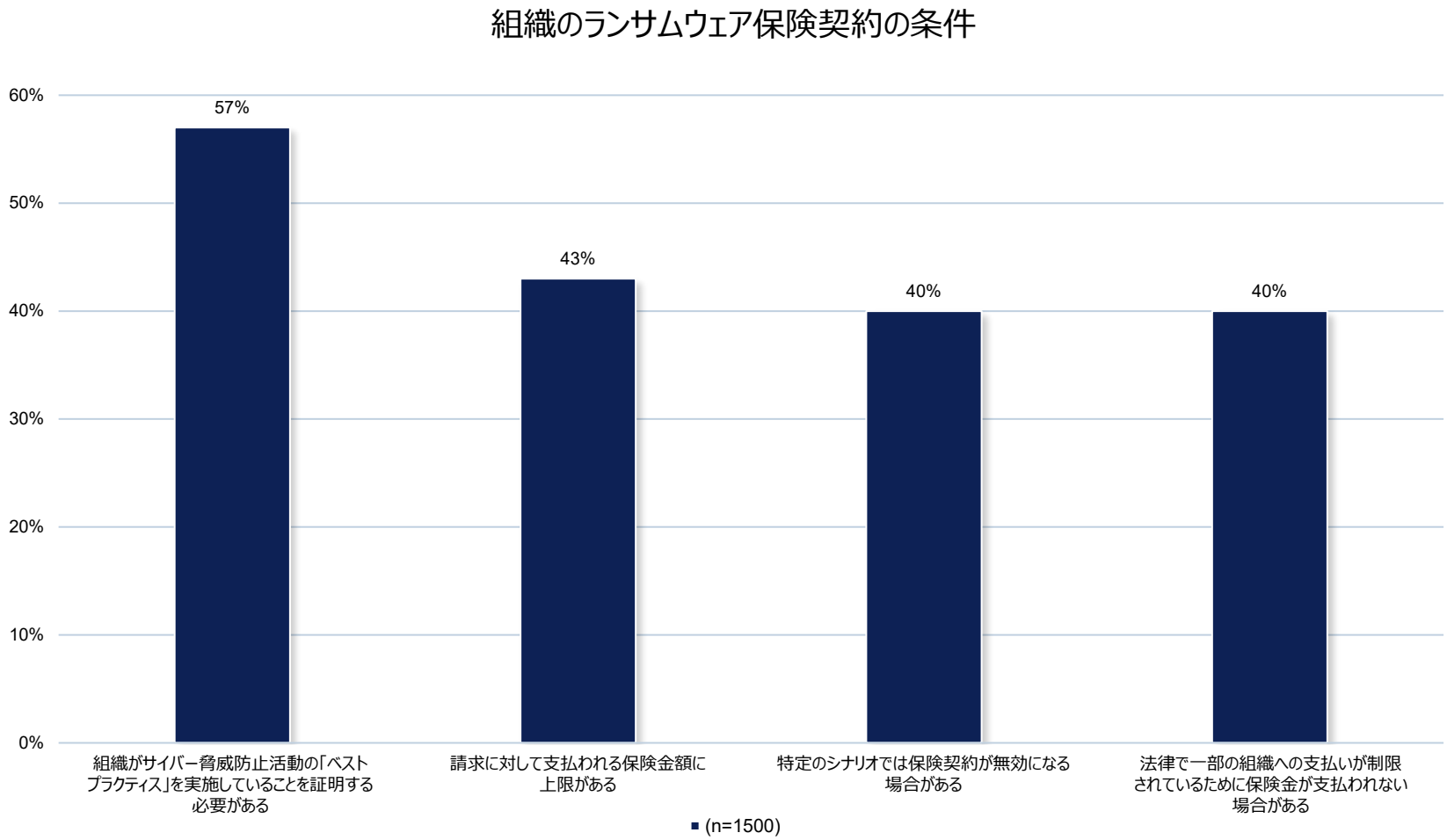
66%

組織がランサムウェア攻撃を受けた場合、一度身代金を支払えば**再度攻撃されることはない**、と**考えている**回答者の割合

サイバー犯罪者はさまざまなエントリー ポイントを標的にしており、攻撃が発生する可能性が高いのは外部ソース



組織の間でランサムウェア保険契約は一般的だが、十分注意すべき事項がある

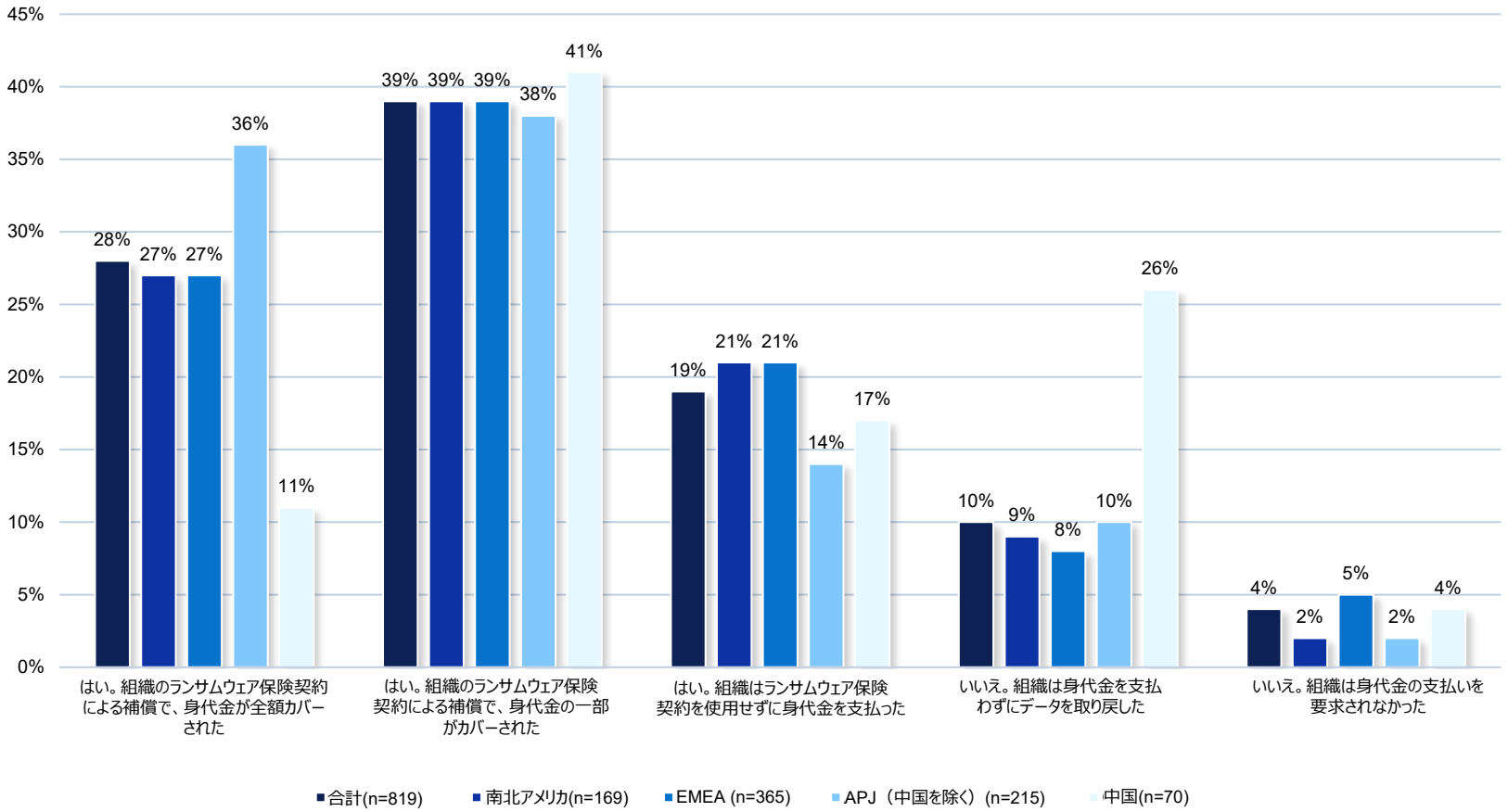


93%

ランサムウェア保険契約を結んでいる組織の割合

多くの組織がランサムウェア保険契約を結んでいるにもかかわらず、依然として財務的に脆弱であると考えている

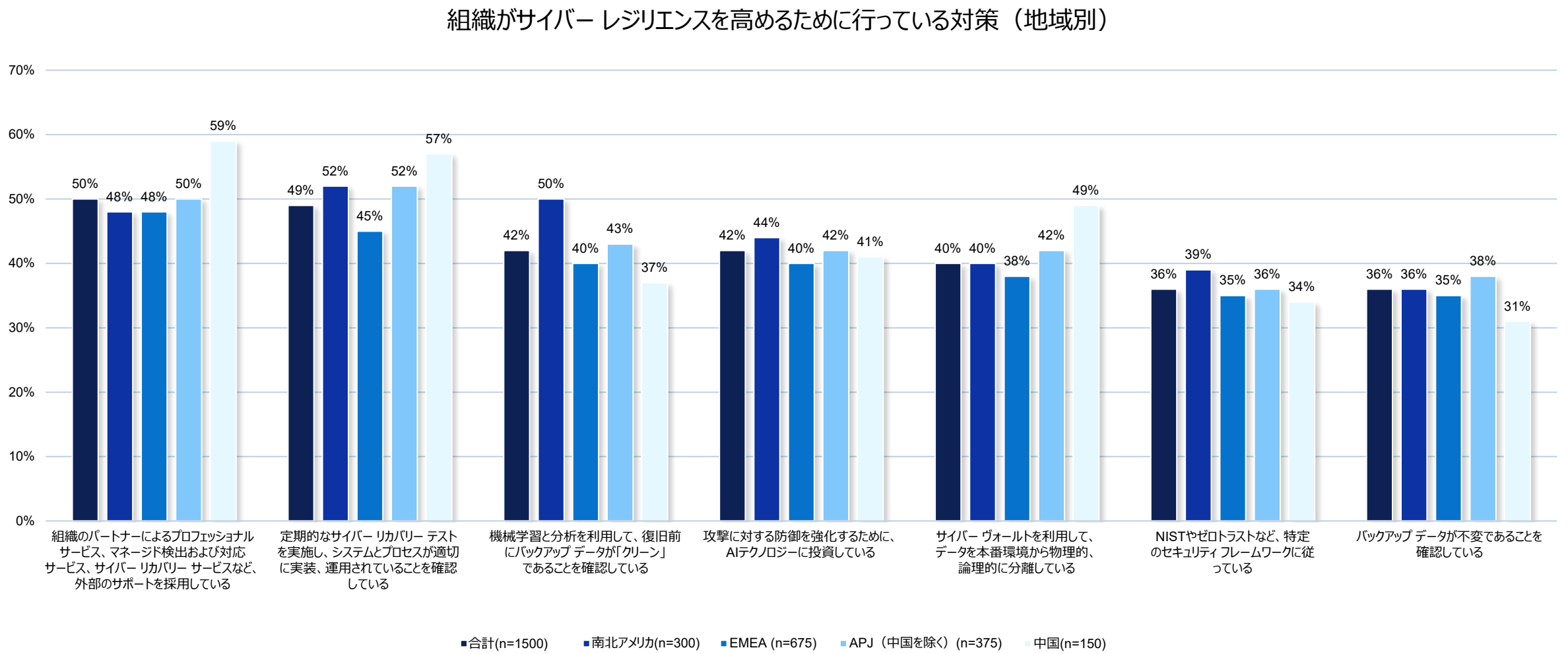
組織のデータへのアクセスを取り戻すために、身代金を支払ったか（地域別）



192万ドル

過去12か月間に、**サイバー攻撃やその他のサイバー関連**インシデントが原因で組織が負担した平均コスト

前向きな材料として、組織はサイバー レジリエンスを高める対策を講じている

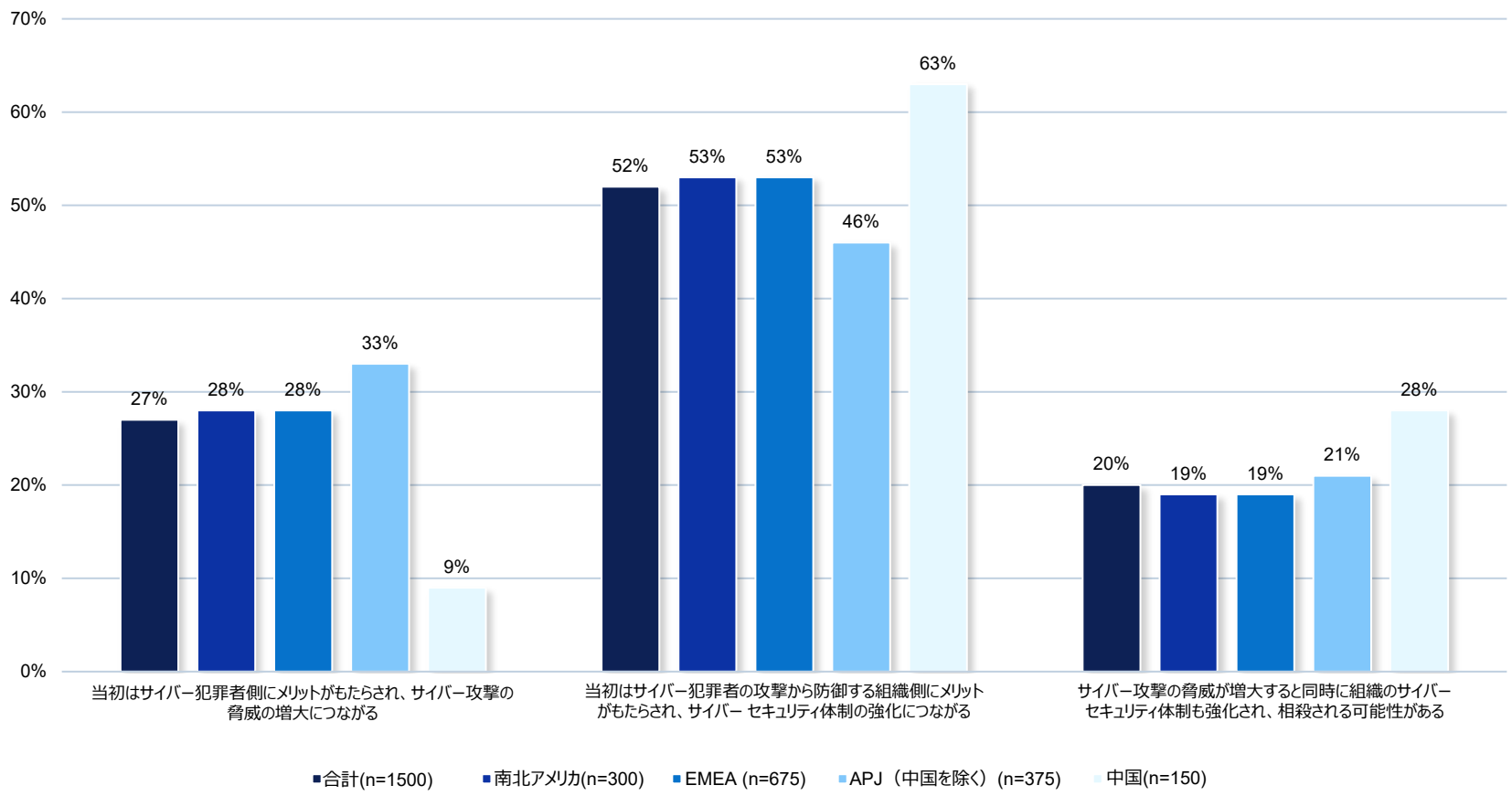


ただし、すべての組織が生成AIによりサイバー レジリエンス上のメリットを得られると考えているわけではない

81%

先端テクノロジー（AI、IoT、エッジなど）が**データ保護にリスクをもたらすことに同意**した回答者の割合

生成AIがサイバー脅威とデータ セキュリティに与える影響（地域別）



実際、組織は既にデータ保護に関する懸念を抱いており、その多くは生成AIが新たな課題を生み出すと考えている

88%

生成AIによって大量のデータが新たに生成され、その**保護とセキュリティ確保の必要がある**、ということに**同意**した回答者の割合

88%

生成AIによって特定のデータ タイプの価値が増大し、その結果**より高いレベルのデータ保護サービスが必要になる**、ということに**同意**した回答者の割合

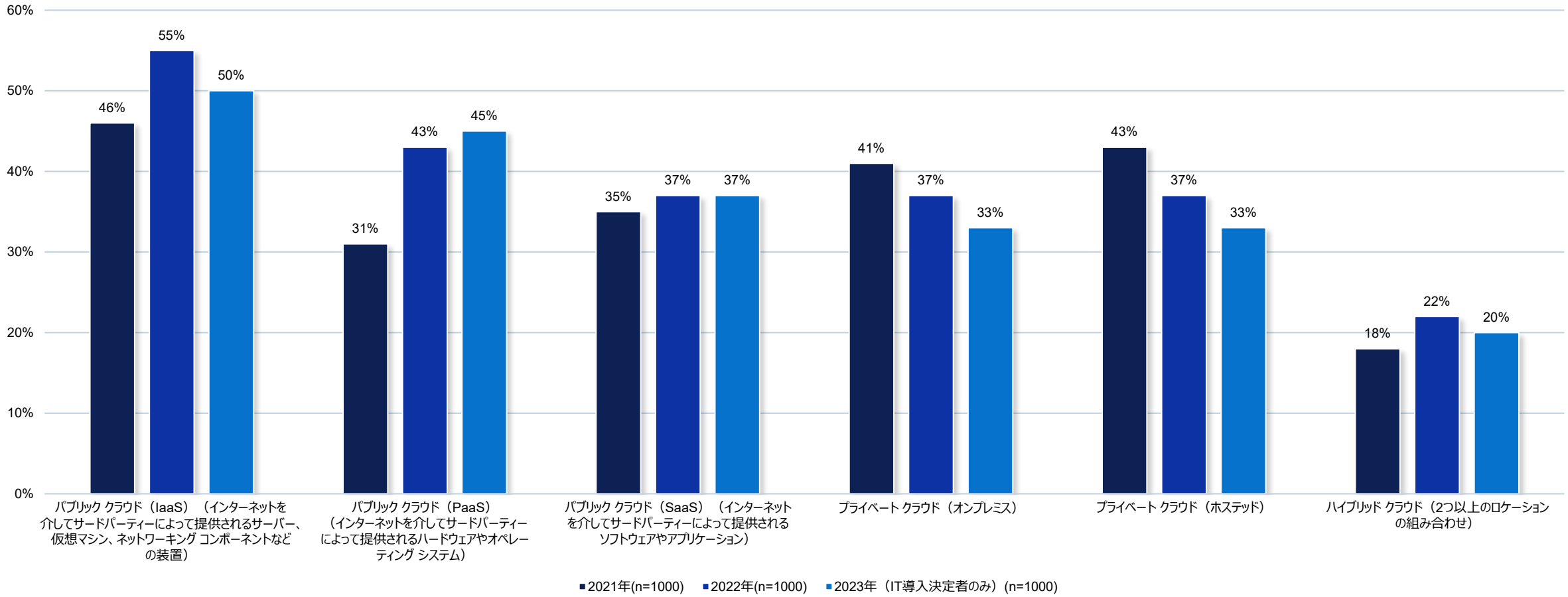
85%

生成AIに使用されるデータ セットが**破損**した場合、**生成AIの出力に影響が及ぶ**、ということに**同意**した回答者の割合

3. マルチクラウドの利用

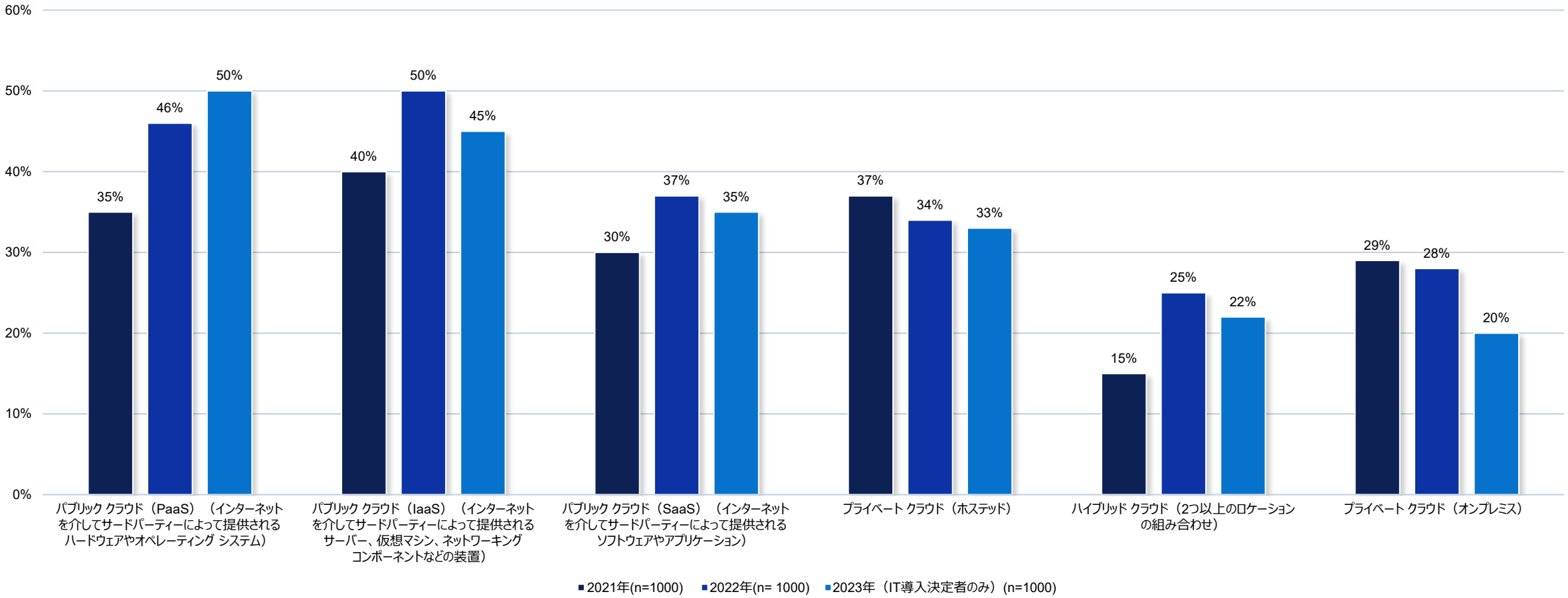
パブリッククラウドは依然として、既存アプリケーションを更新する際の選択肢として人気が高い。一方、プライベートクラウドを選択する組織は減少している

既存アプリケーションを更新する際の方向性（年別）

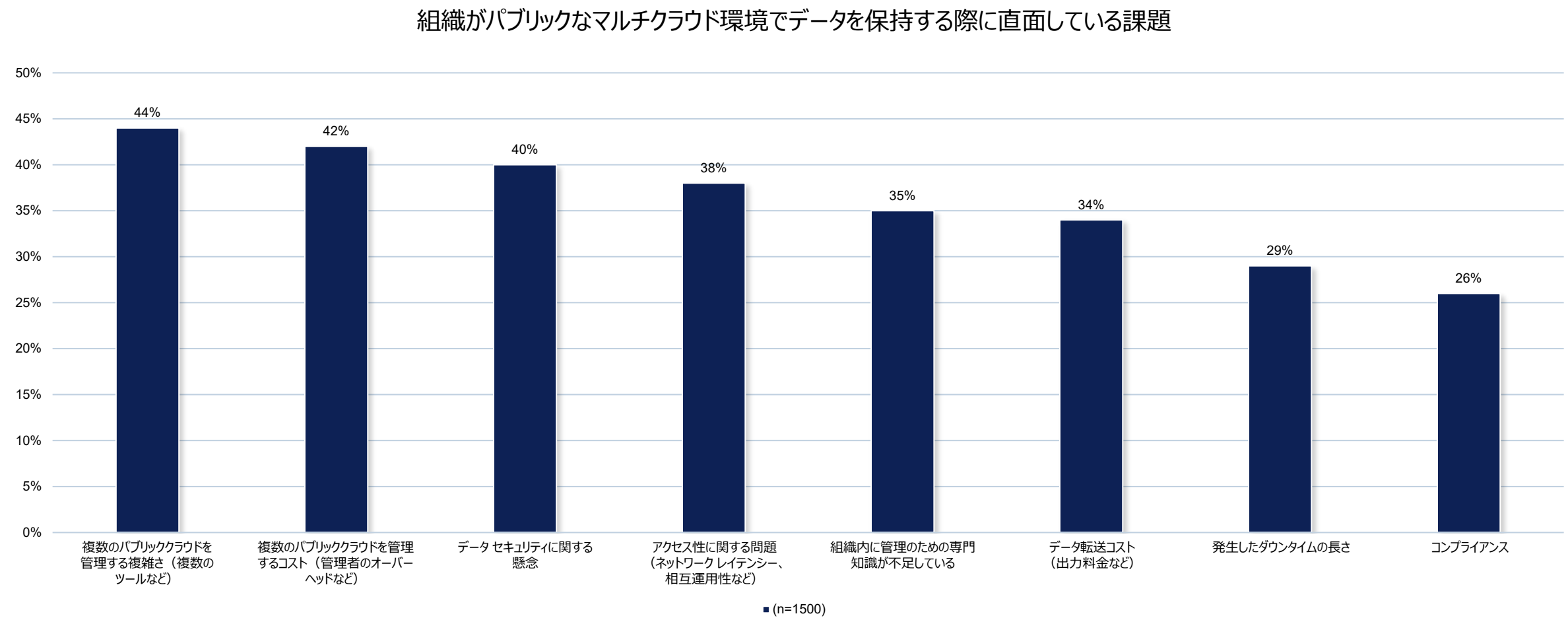


パブリッククラウドは依然として、新規アプリケーションを導入する際の選択肢としても人気が高い。しかし、その人気は低下傾向にあるといえる

新規アプリケーションを導入する際の方向性（年別）

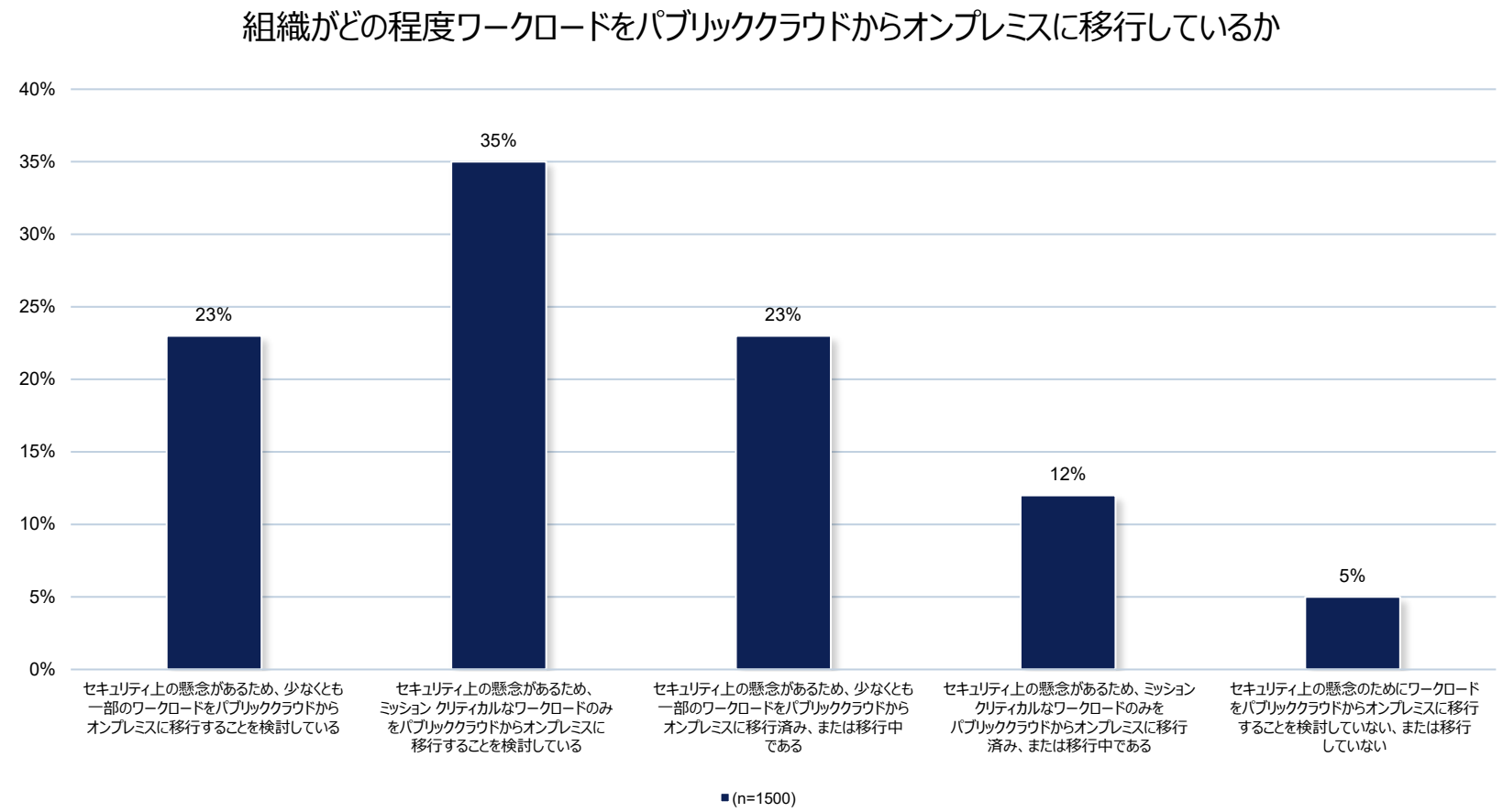


パブリッククラウドが普及しているにもかかわらず、多くの組織がデータを保持する際の課題に直面している



フィルター：データ、分割：地域 = 合計

セキュリティ上の懸念があるため、多くの組織はワークロードの一部をパブリッククラウドからオンプレミスに移行している、または移行を検討している



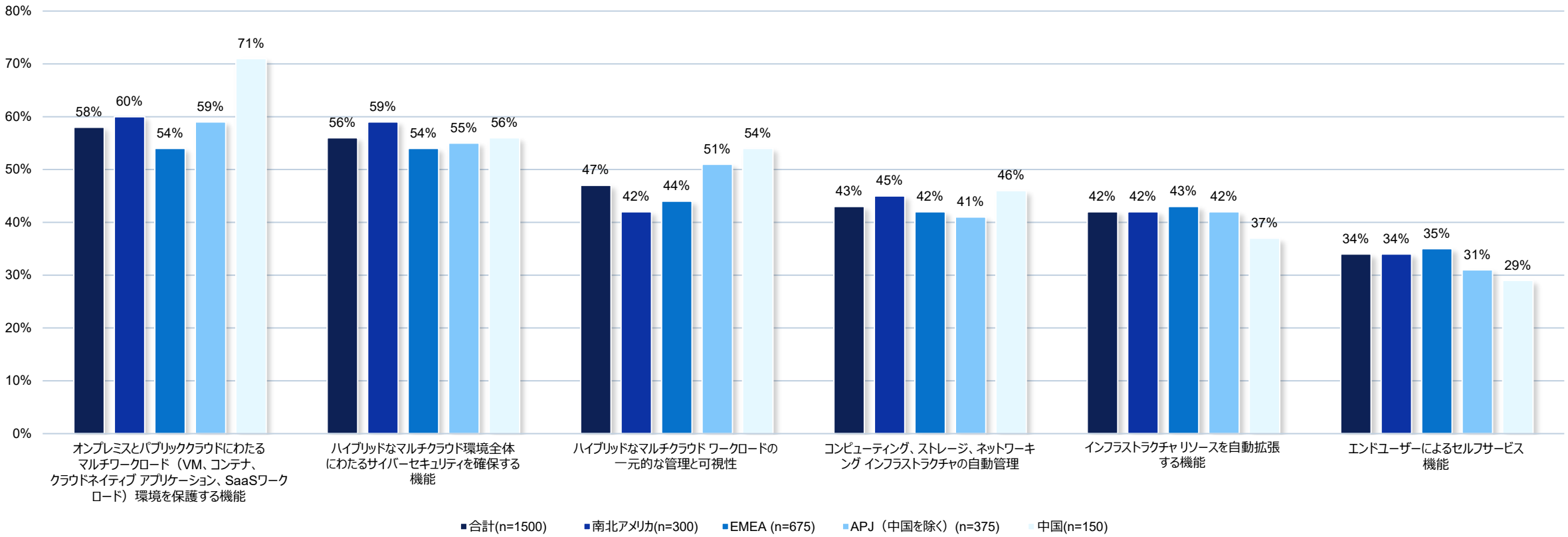
フィルター：データ、分割：地域 = 合計

79%

パブリッククラウド環境全体にわたる**データすべてを保護する**組織の能力について、**「とても自信がある」以外**の回答を選んだ回答者の割合

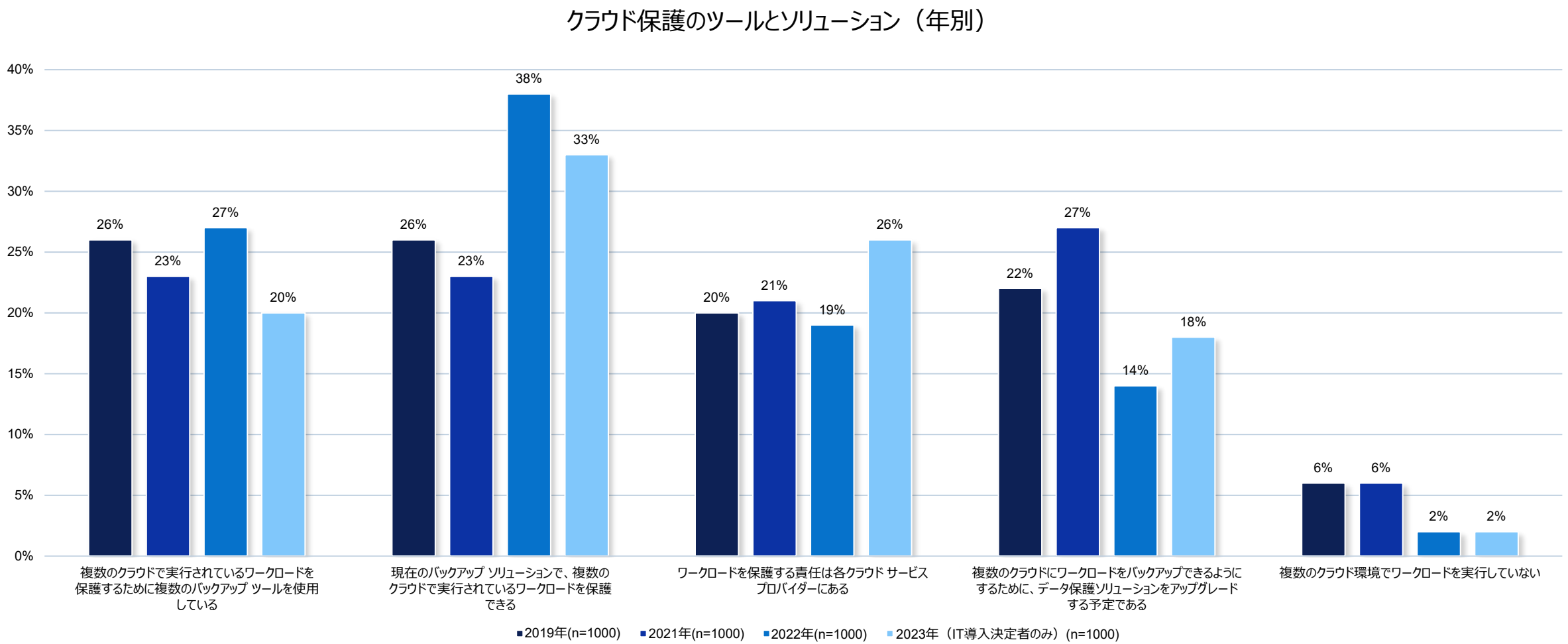
サイバー関連のインシデントが増加し、データ保護戦略に対する自信が低い中、多くの組織がハイブリッドなマルチクラウド運用を実現する際にセキュリティが最も重要な能力であると考えている

ハイブリッドなマルチクラウド運用を実現する際に最も重要な機能（地域別）



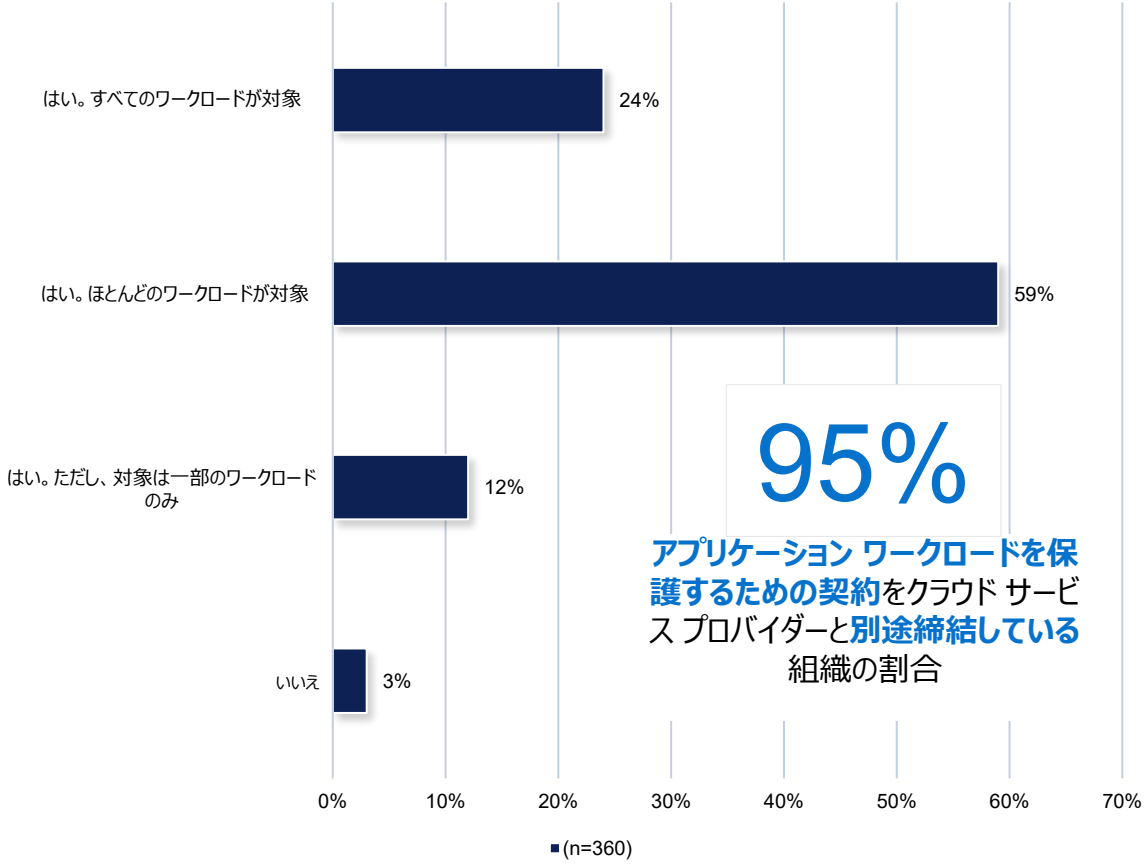
4. クラウド環境のセキュリティ確保

組織は現在、さまざまなバックアップ ツールとソリューションを使用してワークロードを保護しているが、アップグレードの必要性を認識している



組織は、複数のクラウド環境にわたるワークロード保護のために、クラウド サービス プロバイダーにますます依存するようになっている

アプリケーション ワークロードを保護するための契約をCSPと別途締結している

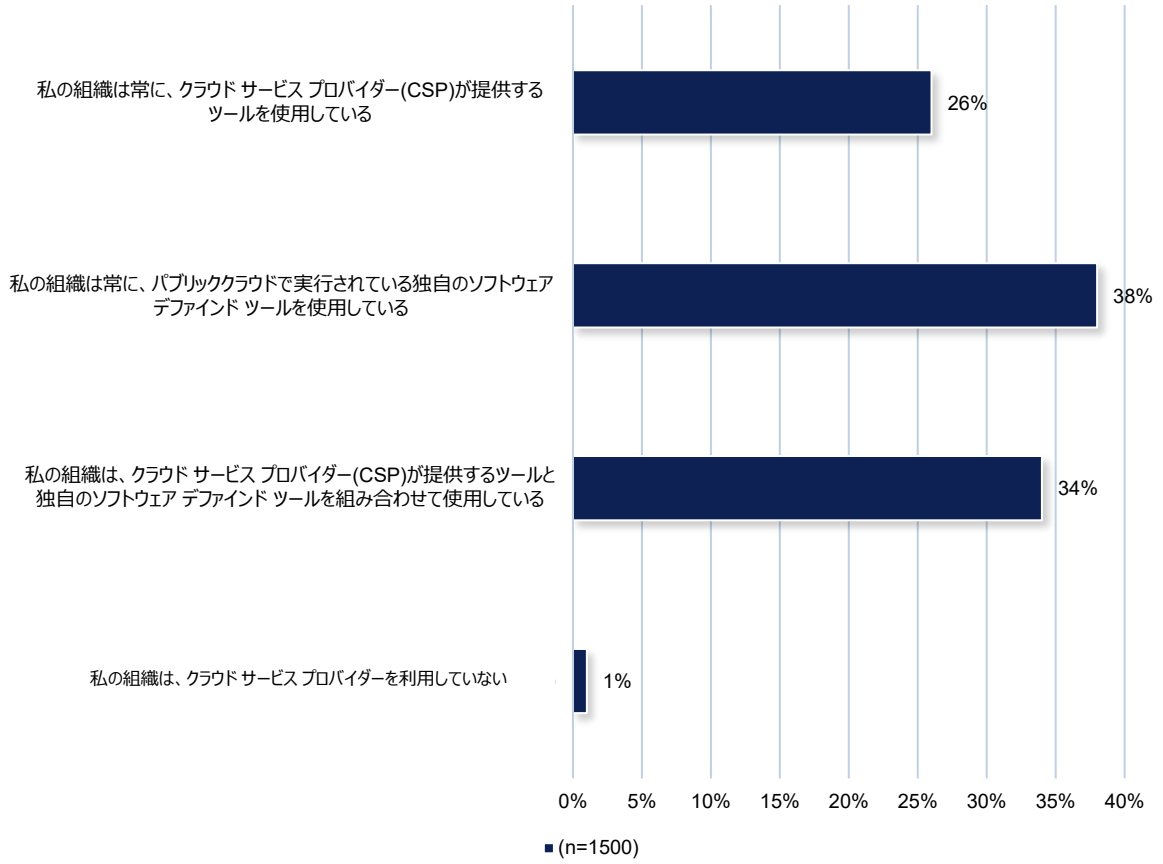


95%

アプリケーション ワークロードを保護するための契約をクラウド サービス プロバイダーと**別途締結している**組織の割合

フィルター：データ、分割：地域 = 合計

クラウド サービス プロバイダーが提供するバックアップ/リカバリー ツール



フィルター：データ、分割：地域 = 合計

主な調査結果：要約

データ保護リスクの現状

- データ保護手段に関する懸念が広がっており、組織は自信を持てず、脆弱な立場にいると感じている
- ほぼすべての組織がデータ保護に関連する課題に直面しており、多くの組織が過去12か月間にデータ ロスや予定外のシステム ダウンタイムによる重大な混乱を経験している
- 過去12か月間に発生したデータ ロスや予定外のシステム ダウンタイムの原因として最も多く挙げられたのは、外部のセキュリティ脅威
- データ保護に関する課題や懸念があるにもかかわらず、ゼロトラスト セキュリティを十分に実装している組織はわずか

増大するサイバー攻撃の脅威

- 過去12か月間にサイバー攻撃やインシデントを経験した組織が増加し、企業が負担したコストは平均で192万ドルにのぼっている
- 多くの組織が、ランサムウェア攻撃によるバックアップ データの感染や破損の可能性があることを懸念している
- リスクに加えて、ランサムウェア攻撃の結果に関する誤った過信が存在している
- ランサムウェア保険契約は一般的になっているものの、十分注意すべき事項があるため、組織は依然として財務上の脆弱性を抱えている

マルチクラウドの利用

- パブリッククラウドは依然として、既存アプリケーションの更新や新規アプリケーションの導入の際の選択肢として人気があるものの、データ セキュリティに関する懸念が存在する
- セキュリティ上の懸念があるため、多くの組織はワークロードの一部をパブリッククラウドからオンプレミスに移行している、または移行を検討している
- サイバー関連のインシデントが増加し、データ保護戦略に対する自信が低い中、多くの組織がハイブリッドなマルチクラウド運用を実現する際にセキュリティが最も重要な能力であると考えている

クラウド環境のセキュリティ確保

- 組織は現在、さまざまなバックアップ ツールとソリューションを使用してワークロードを保護しているが、アップグレードの必要性を認識している
- 組織は、複数のクラウド環境にわたるワークロード保護のために、クラウド サービス プロバイダーにますます依存するようになっている