持続可能な成長に向けてセキュリティを優先するアジアのデジタルネイティブ企業

2024/25 Tech Insider

エグゼクティブサマリー

デジタルネイティブ企業（DNB）はインターネット時代に誕生した企業であり、誕生時に利用可能だった最新のテクノロジーを中心に構築されています。

ゲーム、小売、教育などのさまざまな業界で、古いテクノロジーやプロセスという足枷のないデジタルネイティブ企業が、テクノロジーと同じスピードで動き、オンラインでの仕事、生活、遊びに対する顧客の需要に対応しています。

テクノロジー調査会社の IDC によると、DNB は 2026 年までに最大 1,289 億ドルをテクノロジーに費やすと予測されています。

2024 年 3 月から 5 月に、Akamai はサードパーティの調査会社 TechnologyAdvice とオンライン調査を実施し、アジアの DNB のテクノロジー投資の優先順位と、IT リーダーたちを悩ませている要因を調査しました。

オーストラリア、東南アジア、インド、および中国の 200 人以上のテクノロジーリーダーが、この調査に回答しました。

アジアの DNB のビジネス上の優先事項とテクノロジーに関する懸念事項は？これらのテクノロジー主導型企業は、ソリューションプロバイダーに何を求めているのか？すべてのデジタルネイティブ企業が類似しているのか？

市場競争の激化や消費者層の急速な成長に伴い、調査に応じた DNB の 9 割以上が、次の 12 か月で効率と生産性を重視することを目指しています。

この結果は、DNB 間でのクラウドの急速な普及を裏付ける業界データと一致します。2021 年から 2026 年までのクラウドベースのソリューションに対するテクノロジー支出の伸び率は、非クラウドソフトウェア（16%）と IT サービス（11%）を上回る 37% と予測されています。

個別に動作し、API を介して通信するマイクロサービスを中心に構築されたクラウドネイティブのモジュール型アーキテクチャにより、この地域の DNB は急速に拡張し、増加する顧客のデジタル化に対応できます。

しかし、ソフトウェア、システム、サービスの環境が複雑になりやすく、より大きなサイバー脆弱性にさらされる可能性があります。

クラウドへの移行のどの段階にいるかに関係なく、DNB は、セキュリティがクラウドインフラのパフォーマンスにおける最大のギャップであることを強く認識しています。

実際、IT インフラがますます複雑になっていることは、サイバーセキュリティ体制を強化する上での弱点となる可能性があり、大多数の企業が予算やコンプライアンス以上の問題として挙げています。

クラウドの導入を検討している企業や、クラウドへの移行を目指している企業にとって、そのようなテクノロジーの複雑化に関する問題の増大は警戒すべきかもしれません。

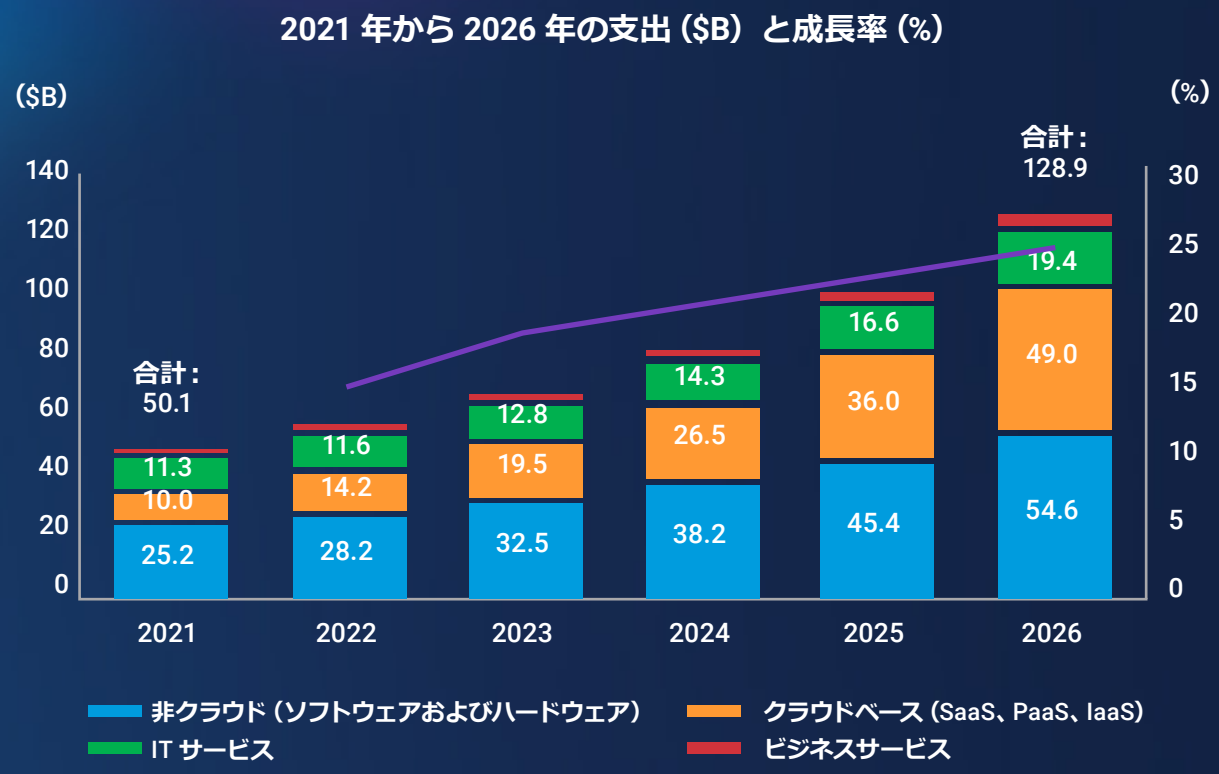
このホワイトペーパーでは、こうしたリスクを緩和するために実行可能な戦略を紹介しています。

クラウドを活用して、スピードと効率性を実現する DNB

IDC Digital Native Business, Start-Ups and Scale-Ups CIS によると、デジタルネイティブ市場セグメントは「急成長中の組織群であり、明らかに非常にテクノロジー中心的です。テクノロジーがこの業界のビジネスモデルの基盤であるため、テクノロジーに多額の資金を投入しています」。

DNB は、業界や市場に関係なく、差別化要因としてテクノロジーを活用し、アジリティを高めています。

DNB は、その性質上、テクノロジーインフラの構築においてクラウドネイティブ設計の原則を採用しています。実際、DNB はクラウドベースのテクノロジーへの支出を増加させており、2021 年から 2026 年の成長率は 37.3% と予測されています。



選択したセグメントの成長率

- クラウドベース（SaaS、PaaS、IaaS）：CAGR 37.3%
- 非クラウド（ソフトウェアおよびハードウェア）：CAGR 16.7%
- IT サービス：CAGR 11.5%
- ビジネスサービス：CAGR 10.4%

市場全体の CAGR
20.8%

出典：IDC プレスリリース、「Asia/Pacific Digital-Native Business Tech Spending from 2022-2026 to Grow at a CAGR of 20.8% and Hit US$128.9B in 2026, IDC Forecasts」、2023 年 4 月 19 日

DNB のテクノロジーインフラは、マイクロサービスの構成可能なアーキテクチャを基盤としており、デジタル空間の急速な変化に対応する上で必要不可欠な、柔軟性、アジリティ、迅速な市場投入を実現しています。

調査によると、地域全体の DNB のうち 4 社に 3 社は、効率性と生産性を優先するために、クラウドテクノロジーを導入しています。

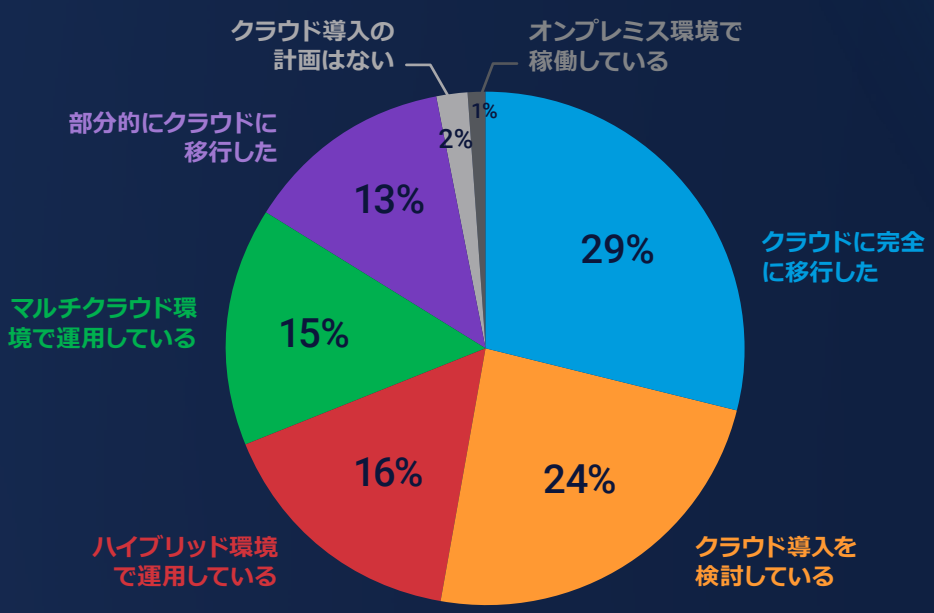
回答者の 74% はクラウドに完全に移行しているか、またはクラウドテクノロジーを採用しています。

ただし、回答者の 26% はクラウド導入の計画を立てていないか、まだ検討中であり、この傾向は地域全体（オーストラリア 19%、インド 20%、ASEAN 29%）でみられます。

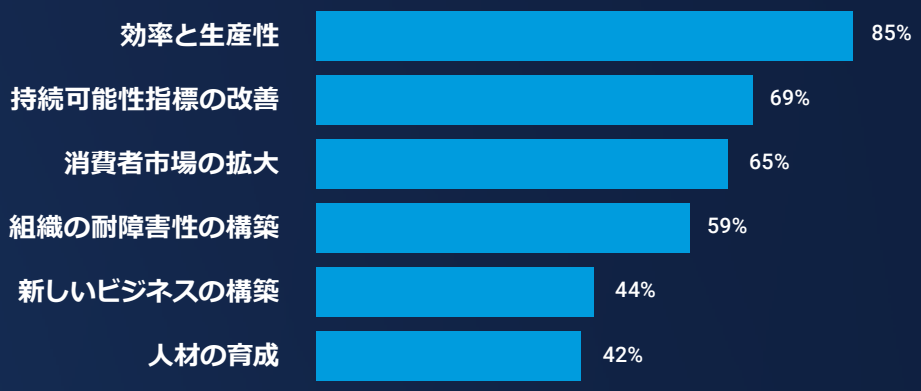
このように停滞している原因はおそらく、規制の厳しい業界の既存の大規模エンタープライズと、クラウドに対する長年の慎重な姿勢がクラウド導入の妨げとなり続けているためです。

しかし、DNB がクラウドへの投資を増加させていることに伴い、状況は改善されつつあります。これは、クラウドテクノロジーの支出が増加していることからも明らかです。

貴社はクラウド導入プロセスのどの段階にありますか？



今後 12 か月間の最優先事項



オンラインライフのセキュリティ確保

一般に、DNB は技術的なスキルに秀でていると言われています。ただし、この習熟度は専門的な分野に限定される場合があります。

DNB はクラウドネイティブかもしれませんが、クラウド、データ、人工知能(AI) における新たなテクノロジーの可能性を最大限に活用することに苦労しているかもしれません。

回答者がクラウド移行で経験した課題と、クラウド移行のどの段階にあるのかを対応付けました。

既にクラウドに完全に移行した回答者とクラウド導入を検討中の回答者の間に、クラウド支出の理解に関する問題が一貫してあることがわかります。

ほとんどのクラウドプロバイダーは価格について透明性がありますが、コストの内訳は複雑になりがりです。DNB は、マイクロサービスとマルチクラウド導入のコストを予測して理解するための適切な知識と時間を備えている必要があります。これらはすべて、さまざまな要因に応じて様々にスケーリングします。たとえば、スケーラビリティイベントを促進する要因は何か、それはエンドユーザーの要求か、それともプロセス間の通信か、などです。

クラウド移行の過程で直面する課題のトップ 3

	セキュリティ関連事項の管理	適切なクラウドプロバイダーの選択	技術的な実現可能性の評価
クラウドに完全に移行した	45%	53%	57%
クラウド導入を検討している	63%	62%	52%
ハイブリッド環境で運用している	74%	49%	54%
マルチクラウド環境で運用している	50%	44%	47%
部分的にクラウドに移行した	45%	41%	41%

その他の課題：
クラウドの速度割り当ての把握、移行するアプリの優先順位付け、最適なインスタンスの適切なサイジング／選択、オンプレミスとクラウドのコストの比較、技術的な専門知識の欠如、アプリの依存関係の把握

このため、DNB はパフォーマンス、可用性、サポートを犠牲にすることなく価格をわかりやすく提示するクラウドプロバイダーを利用しています。

しかし、DNB がクラウド移行のどの段階にあるか（ハイブリッド環境で稼働している、マルチクラウド環境で稼働している、クラウドへ部分的に移行済みなど）に関係なく、セキュリティ関連事項を管理することは常に課題です。

実際、ほとんどの回答者の間で、セキュリティは現在、クラウドインフラの最大のギャップと考えられています。

Akamai では、非常に低いエグレス（出方向の通信）料金、余裕のある月間のエグレス許容量、データセンターとクラウドトラフィックのオフロードを最大化するツールを活用して、シンプルで透過的な価格設定を維持しています。

これらのソリューションを組み合わせることで、Akamai のグローバルなフットプリントを活用して、データ量の多いアプリケーションやトラフィック量の多いアプリケーションのコストを最適化する多くの機会が得られます。

クラウドプロバイダーの選定にあたって、セキュリティ機能はパフォーマンス、評判、スケーラビリティ、コストさえ上回る要因になります。

クラウドインフラのパフォーマンスや機能の最大のギャップはどこにありますか？

	セキュリティ	ネットワークのレイテンシー	データの保存と取得	コンピュートリソース
クラウドに完全に移行した	65%	65%	67%	47%
クラウド導入を検討している	81%	58%	67%	62%
ハイブリッド環境で運用している	74%	66%	49%	46%
マルチクラウド環境で運用している	84%	66%	66%	63%
部分的にクラウドに移行した	69%	62%	62%	24%

クラウドプロバイダーを選択する際の要因

技術第一の考えが DNB の弱点になり得る?

テクノロジーは DNB にとってメリットにもデメリットにもなる可能性があります。

回答者の大半は、複雑な IT インフラを、サイバーセキュリティ体制を強化する上で最大の課題として挙げています。

デジタルネイティブ企業は、構成可能なマイクロサービスとそれらを繋げる API を重視する、クラウドネイティブ設計の原則を取り入れています。

こうした API は、テクノロジーの導入を加速し、市場投入までの時間を短縮し、DNB が迅速に反復し、機能を迅速に提供できるようにします。

しかし、さまざまなサービスに関わっている開発者に DNB の業務に集中的に取り組むインセンティブがない場合、そのようなスピードと構成可能性には複雑さというコストが伴います。

ほとんどのセキュリティツールはハイブリッド環境をサポートしておらず、組み込みのクラウドセキュリティはプロバイダーのクラウドだけに焦点を絞る傾向があるため、セキュリティチームとテクノロジーはその課題に直面することとなります。

たとえば、ゲームプロバイダーは、ゲーム開発に数年かかるため、ベンダーよりも、信頼できるパートナーであるクラウド・インフラ・プロバイダーと連携したいと考えています。

ゲーム会社とその開発チームは、パフォーマンス、リソース割り当て、レイテンシー、スループットなど、クラウドコンピューティングのあらゆる側面に関する知見を求めています。また、予測可能な価格設定と請求の透明性も必要としています

必要な分だけ支払う分散型クラウド・コンピューティング・インフラは、ゲームの開発やアップグレードに直接関係しない運用コストを厳密に監視したいゲームプロバイダーにとって非常に魅力的です。

調査結果によると、DNB は IT インフラの複雑化に直面しており、これが組織のサイバーセキュリティ体制に影響を及ぼしています。

サイバーセキュリティ体制を強化する上での最大の課題

	複雑な IT インフラ	地域のコンプライアンス要件	熟練した人材の不足	予算の制約	迅速に進化する脅威
クラウドに完全に移行した	43%	7%	13%	12%	25%
クラウド導入を検討している	37%	6%	10%	27%	21%
ハイブリッド環境で運用している	49%	3%	9%	23%	17%
マルチクラウド環境で運用している	59%	13%	13%	6%	9%
部分的にクラウドに移行した	31%	7%	17%	14%	31%

リスクとリターンのバランスを取る

現実問題として、クラウド全体に一貫したセキュリティポリシーを適用することは困難です。

比較的新しい DNB は、クラウドテクノロジーによって実現できるペースに期待を寄せているかもしれませんが、ビジネスの成熟に伴い、DNB は各テクノロジーイノベーションによって得られるリスクとリターンのバランスを取る必要があります。革新的なテクノロジーが登場すると、複雑さがさらに増します。

では、市場投入および顧客導入までの時間と、セキュリティ、コンプライアンス、ガバナンスのバランスを取り、侵害や誤使用を防止するためにはどうすればよいでしょうか。

このことは、DNB がクラウド移行のどの段階にあるかに関係なく、サイバーセキュリティを強化する上での最大の課題となっています。

> ***Akamai Connected Cloud は、オープンソースアーキテクチャとマルチクラウドアーキテクチャを採用したオープンプラットフォームです。このアーキテクチャは、開発者がグローバルにスケーラブルで地域ごとに最適化された低レイテンシーのワークロードを実現するために、必要なアプリケーションやソフトウェアを必要なサービスとあわせて容易に活用できるように設計されています***

クラウドテクノロジー自体は、インフラのみの提供から、インフラ管理を含む幅広いサービスの提供に至るまで、形を変化させています。

クラウドネイティブのインフラを稼働すると、集中化のリスクと複雑なインフラの課題が発生します。

クラウド導入プロセスのどの段階にいるかに関係なく、検討すべき事項をいくつかご紹介します。

マルチクラウド戦略を導入する

組織は、ベンダーロックインを回避し、柔軟性を高め、クラウドサービスの使用率を最適化するマルチクラウドアプローチを採用する必要があります。

Forrester Research の調査に回答した IT リーダーによると、クラウドベンダーにとって最も重要な要件は、クラウドからエッジに展開して実行する能力です。

特定のベンダーに過度に依存すると、将来のテクノロジーの選択肢が減り、ベンダーの影響力が組織のテクノロジー将来を左右することがあります。

デジタルネイティブ企業は、ベンダーに依存しない分散プラットフォームを活用することで、シームレスかつ迅速に生データにアクセスし、さまざまなシステムに分散したデータから知見を得ることができます。

レビューと反復を定期的に実施

クラウドのコストを定期的に見直して、クラウドの支出を分析して最適化し、コスト削減の領域を特定し、リソース使用率を最適化します。

モニタリングデータとリアルタイム分析を活用して、リソース割り当て、コスト管理、セキュリティの改善など、最適化できる領域を特定します。

定期的な監視と最適化により、クラウドへの投資から最大限のビジネス価値を引き出すことができます。

クラウドガバナンスフレームワークを実装する

アプリケーション（およびビジネスプロセス）が特定のクラウドプロバイダーに依存すればするほど、クラウドサービスの問題がもたらす影響の幅が大きくなり、ビジネス継続性に関する懸念が高まる可能性があります。

クラウドガバナンスポリシーを開発して適用し、クラウドリソースを効果的に管理し、コンプライアンスを確保し、コストを管理します。

このモデルには、アクセス制御、セキュリティ対策、コスト管理、コンプライアンス要件が含まれている必要があります。明確なガバナンスモデルは、組織全体で一貫性とベストプラクティスを維持する上で役立ちます。

また、集中化のリスクに対するアプローチは規制当局によって様々なので、集中化のリスクに対処するために様々な規制当局による規制上の要求に応えることが困難になる場合があります。

高度な API セキュリティを重視

DNB では、非クラウド、クラウド、およびマルチクラウドアーキテクチャを繋げるにあたり、API が中心的役割を果たします。

また、内部アプリケーションの接続、ビジネスパートナーとのプロセスの高速化、消費者へのデータサービスの提供によって、DNB は新たなレベルの接続性、生産性、アジリティを実現できます。

スピードとテクノロジー主導のイノベーションを追求するにあたり、セキュリティチームが体制を評価する前に、API を使用するアプリケーションやビジネスプロセスが開始および展開されることがよくあります。

誤設定や脆弱性に加えて、API セキュリティに関する専門知識の不足により、革新的な DNB は潜在的なサイバー脅威にさらされています。

実際、**631 人のサイバーセキュリティ専門家**を対象とした別の業界調査によると、開発者のうち 2 人に 1 人が API のリファクタリングと修復に、最大で業務時間の半分を費やしています。

> ***Akamai* が保護したトラフィックのうち *31%* は *API* トラフィックです。*Akamai* は、統合されたユーザー体験最適化機能により、アプリケーションとワークロードを一貫して制御するためのツールを提供します。**

アジアの DNB は、持続可能なビジネスの成長を実現にするために、API セキュリティを最優先に考えています。

オーストラリアでの拡大を推進している場合も、インドや ASEAN での市場シェアの獲得に取り組んでいる場合も、DNB は高度な API セキュリティを最も重要なサイバーセキュリティ投資分野に位置づけており、Web ／アプリケーションセキュリティやフィッシング防止テクノロジーよりも重視しています。

以下のサイバーセキュリティ投資分野を、最も重視する（上）から最も重視しない（下）にランク付けしてください

1. 高度な API セキュリティ
2. Web アプリケーションセキュリティ
3. フィッシング防止テクノロジー
4. 分散サービス妨害（DDoS）の緩和
5. ゼロトラスト関連のテクノロジー

API セキュリティのエラーが発生する条件

API を使用した、ビジネスクリティカルなプロセスの展開を急いでいる **+** API の可視性が欠如している **=** API の設定にミスがある、または API が脆弱

Akamai のトラフィックデータを見ると、製造業界はアジア太平洋および日本の全域で API 攻撃を受ける割合が最も高くなっています。

この原因の 1 つに、重要なインフラであるこの業界において API を介した接続が増加していることや、サプライチェーンが混乱している可能性があることなどがあります。

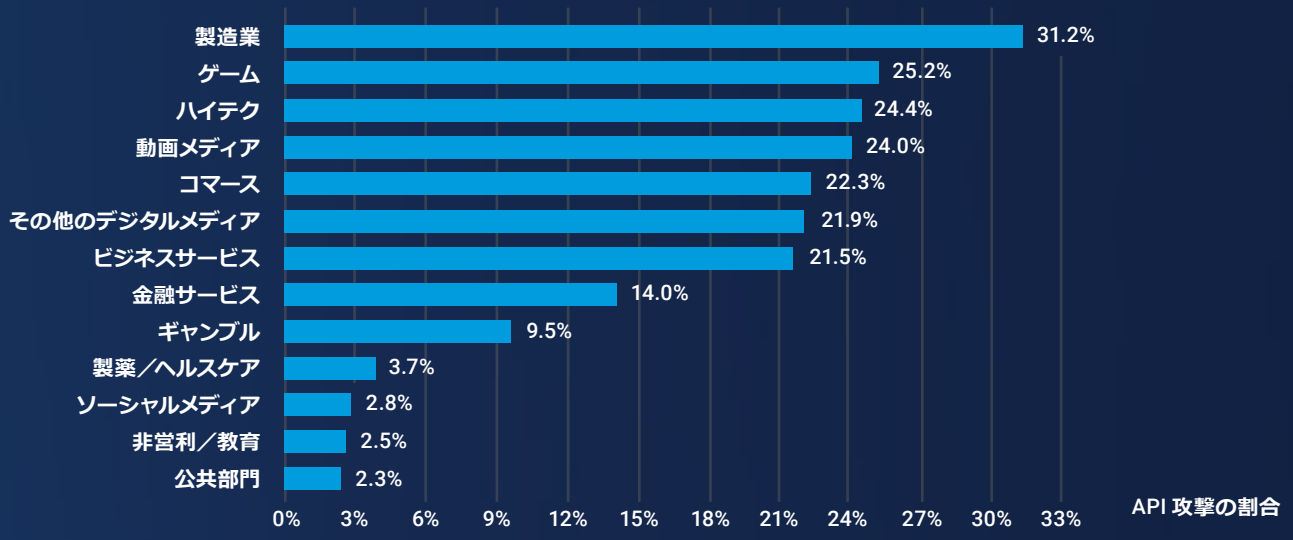
また、ゲームやハイテク、動画メディア、コマースなど、デジタル産業全般が API 攻撃の標的となっています。

デジタルネイティブ企業が最もターゲットになっている理由は、ビジネスの大部分が API に依存していること、インフラが最もクラウドに展開されていること、従来の企業やアーキテクチャと比較してフィッシング、アカウント侵害、ランサムウェアの最も魅力的なターゲットであることです。

ローカル・ファイル・インクルージョン（LFI）は依然として上位の API 攻撃ベクトルですが、2023 年のデータセットではコマンドインジェクション（CMDi）やサーバーサイド・リクエスト・フォージェリー（SSRF）などの新たなベクトルが表面化しました。これらのベクトルは、脆弱である API、誤設定されている API、または文書化されていない API に重大なリスクをもたらします。

ボットリクエストも懸念される分野です。12 か月間の同一レポート期間において、2 兆以上の不審なボットリクエストを検出しましたが、その 40% が、API を標的にしていました。

APJ：業界別の API 攻撃（2023 年 1 月 1 日～ 2023 年 12 月 31 日）



APJ: ベクトル別の API 攻撃（2023 年 1 月 1 日～2023 年 12 月 31 日）

API セキュリティの重要な考慮事項

API の脆弱性は常に進化しています。API セキュリティの最大のリスクを把握することで、組織は常に脅威の一歩先を行くことができます。

探索と可視性

廃止されていないか、適切なドキュメントを持たない、古いまたは以前のバージョンの API は、企業に対するリスクを高めるおそれがあります。たとえばシャドウ API などが存在して管理の範囲外で動作し、脆弱点となる可能性があります。

ランタイム保護

API はデータを積極的に交換するために実行されるため、従来のセキュリティツールで、API による正当な要求と悪性の要求を識別するのは困難な場合があります。検知を逃れようとする脅威（API ロジックの悪用など）は、通常の API リクエストに溶け込むことができるため、検知が困難であることが知られています。

API テスト

API セキュリティテストを開発のあらゆる段階に組み込むことで、速度を犠牲にすることなくセキュリティを向上させることができます。コストと修正の両方の観点から、API を本番環境にリリースして積極的に使用した後よりも、API の開発段階で問題を修正する方が簡単です。

認証されていないリソースアクセス

マシン間のシナリオでは、認証と認可はより複雑です。API の実装や設定に欠陥がある場合など、ユーザーやシステムが何の認証も提供することなく API リソースにアクセスできることがあります。

URL 内の機微な情報

URL 内の機微な情報は、攻撃者がアクセスできる場所（ログやキャッシュなど）に保存されることもあり、機微な情報の漏えいやコンプライアンス問題に発展する重大なリスクが生じます。

寛容なクロスオリジン・リソース・ポリシー

API を使用すると、必要以上に幅広いオリジン（プロトコル、ドメイン、ポートなど）からリクエストを送信できます。

最初から API セキュリティ第一の文化を確立

調査に参加した DNB の 9 割は、クラウド／セキュリティ・ソリューション・プロバイダーを評価する際の重大または重要な製品機能として、API セキュリティをあげました。

技術革新とサードパーティ接続のペースが加速するにつれ、DNB は、サイバー攻撃者が悪用する可能性のある脆弱なリンクを特定するために、ベンダーからのサポートを必要としています。

API セキュリティは、開発プロセスのすべての段階に組み込む必要があります。API テストフレームワークと特定の API テストツールが不足していると、ますます多くの脆弱な API が公開されてしまい、API セキュリティ関連のインシデントが増加する可能性があります。API ビジネスロジックの不正使用に対する可視性が欠如していることも、API データの侵害や不正行為につながるもう 1 つの要因です。

たとえば、運用中に API が悪用されていることをセキュリティチームはどのように知るのでしょうか。いずれかの時点で、組織の API に対してどのような攻撃が実施されているのでしょうか。

たとえば、セキュリティチームは API エンドポイントの目的を完全に理解していない場合があり、どのバックエンドワークロードがどのように相互作用しているのか、またどのようなデータタイプが交換されているのかを把握することは困難です。開発チームは、開発サイクルの後半にバグを修正する自らの能力を過信しがちです。

AI を活用した探索とプロファイリングは API セキュリティの重要なトレンドですが、開発プロセス（DevSecOps）の初期段階でセキュリティ第一の姿勢をとることは、DNB の脆弱性を早期に軽減し、設計から安全であるという API 開発哲学の確立に役立ちます。

API セキュリティの盲点を早期に特定することで、より強力なサイバーセキュリティ体制を構築することができます。

クラウドまたはセキュリティ・ソリューション・プロバイダーの評価において、次の製品機能はどの程度重要ですか？

	非常に重要	重要	やや重要	どちらでもない	あまり重要でない
API セキュリティ	45.60%	45.10%	7.40%	1.90%	0.00%
カスタマイズ可能なクラウド・セキュリティ・ポリシー	31.20%	53.90%	8.40%	6.50%	0.00%
エッジコンピューティング機能	29.80%	47.00%	15.80%	6.00%	0.90%
可観測性	28.40%	52.10%	11.20%	7.00%	0.90%
リアルタイム分析とレポート	45.60%	34.40%	11.20%	7.40%	1.40%
ゼロトラスト	32.60%	39.10%	14.40%	9.30%	0.90%

一般的な API セキュリティの盲点

未認証のリソースへのアクセス試行

これは、前述の体制に関するアラートにおける未認証リソースへのアクセスから派生した問題ですが、緊急性はそれよりも高くなっています。適切な認証なしで機微な API リソースへの具体的なアクセスが試行されています。その試行が実際に失敗したとしても、API の脆弱性を発見して悪用しようとするアクティブな活動であったことを示しており、即座に介入しないと、いずれ成功する可能性もあります。

異常な JSON プロパティ

予期しないデータタイプ、異常なサイズ、過度に複雑な構成など、異常な JSON ペイロードを使用する API 活動は、API の脆弱性を悪用しようとするアクティブな活動を示しています。この活動は、インジェクション攻撃、サービス妨害、データ窃取、API ロジック欠陥の悪用など、さまざまな悪性の行為を実行する試みと捉えることができます。

パス・パラメーター・ファジングの試み

パス・パラメーター・ファジングは、API リクエストの一部として予期しないまたは不正なデータを故意に送信するもう 1 つの事例です。RESTful API が特定のリソースやオペレーションを指定するために使用する URL の一部が主に対象となります。攻撃者が偵察として脆弱な API を探索し、データ窃取やサービスの混乱を仕掛けるためのテクニックと言えます。

不可能なタイムトラベル

API 活動を分析する際に、タイムスタンプ、ジオロケーション、API コールのシーケンスが論理的になっていない場合があります。これは、攻撃者が何らかの方法でそれらを操作しようとした兆候と考えられます。さらに、こうしたふるまいは、不正行為の一部であるデータ操作など、複数の脅威を示す場合もあります。

データスクレイピング

データスクレイピングとは、API からデータを自動的に抽出する操作のことです。API の意図した用途やサービス規約と一致しない方法と規模で行われます。攻撃者はこのデータをゆっくりと収集することで、検知を回避し、知的財産を盗み出し、機微な顧客情報を収集し、何らかの利益を得ます。API 内で検知されない場合、この Low & Slow（少しずつ時間をかけた）のデータスクレイピングは、大規模なデータ漏えい攻撃に発展する可能性があります。

最新の API セキュリティアプローチ

最新の API は、マイクロサービスやマルチクラウド、シームレスな統合、急速な拡張の結合組織となります。これらは任意のアプリケーションやワークロードの弱点であり、正しく設計・開発・展開することで、ビジネス成果を最適化します。

しかし、最新の API トランザクションには、高頻度のトランザクションなど、固有の特性がある傾向があるにもかかわらず、組織は同じセキュリティ対策を適用する傾向があります。

1 自動 API 探索を実装する

API 関連のセキュリティ侵害、不明な依存関係、予期しない不整合から保護するために、自社が提供する API や使用する API が適切に識別されていることを確認します。API データソースへのネイティブ統合により、複雑さと運用上のオーバーヘッドを軽減できます。

2 API の体制の管理

API セキュリティの評価には、誤設定の検知、侵入テストの実施、または構成の問題（URL 内の機微な情報を公開する API など）をプロアクティブにスキャンする自動評価ツールの使用が含まれます。応答ワークフローの一部として、自動応答によって API 開発チームなどの関係者に問題解決を要請できるようにします。

3 API ランタイム保護

これには、悪性のアクティビティを示すパターンの検知が含まれます。同様の攻撃のデータセットに基づいてトレーニングを行った異常検知エンジンは、脅威を特定し、関係者にアラートを送信できる必要があります。応答ワークフローをトリガーすることで、修正チケットを発行したり、異常な API トラフィックを検知したときに潜在的な脅威をブロックしたりすることができます。

4 プロアクティブなセキュリティテスト

動的スキャンおよびファジングによる API セキュリティテストでは、初期評価中に誤った設定として検知されない可能性のある、技術的な脆弱性を発見できます。

API セキュリティの成熟度が高まるにつれ、セキュリティテストは API 開発プロセスに密接に統合され、脆弱性が発見された瞬間に対処し、脆弱性が本番環境に及ぶ前に解決されることが望ましいです。つまり、セキュリティチームと開発チームの間で機能横断的な連携を行うことが必要です。

5 API セキュリティエコシステム

API セキュリティソリューションをサードパーティのテクノロジーとネイティブに統合して相互運用できるようにする、豊富で堅牢なテクノロジーエコシステムにより、コストと実装時間を削減できます。また、データソースからの API トラフィックの可視性を高め、自動化されたワークフローで脅威への対応を迅速化し、全体的に優れた API セキュリティ体制を実現します。

オーストラリア／ニュージーランド：立ち上げからスケールアップまで

アナリストレポートによると、今後数年間、オーストラリア／ニュージーランド（ANZ）では国内需要と労働需要が低迷すると指摘されています。

顧客は、賃金の伸び率が鈍く、インフレが持続するという経済的圧力を感じています。

現在の経済状況に応える形で、ANZ の DNB の回答者たちは、効率化と組織の耐障害性を重視していると思われます。

また、クラウドテクノロジーがビジネスに不可欠となってきたため、考え方も変化してきています。回答者の合計 97% がクラウドを採用しているか、クラウドの導入を検討しています。

ANZ の組織はクラウド導入をさらに先へ進めて、景気が冷え込む中で経営効率をさらに高めようとしています。

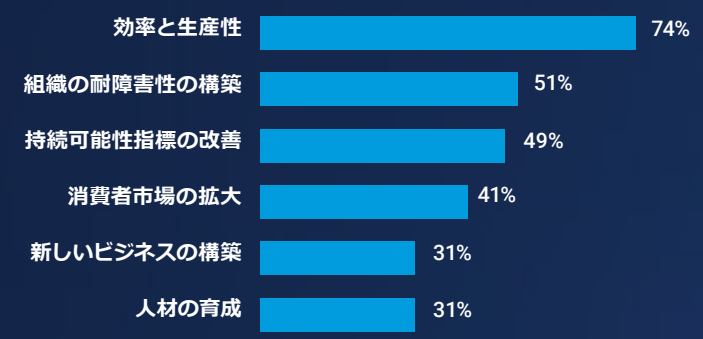
主な予測の概要

暦年	2020	2021	2022	2023	2024f	2025f	2026f
実質 GDP[1]（年間平均変化率）	-1.4	5.6	2.4	0.6	0.5	1.5	2.5
失業率（12 月四半期）	4.9	3.2	3.4	4.0	5.1	5.5	5.0
消費者物価指数上昇率（年間変化率、12 月四半期）	1.4	5.9	7.2	4.7	2.6	2.0	2.0
公式キャッシュレート（12 月四半期末）	0.25	0.75	4.25	5.50	5.50	4.75	4.00

[1] 生産ベース

出典：Statistics NZ、REINZ、Bloomberg、ANZ Research

今後 12 か月間の最優先事項



たとえば、ANZ のパブリッククラウドの採用は、災害復旧など、インフラ交換のための個別の Software as a Service ベースのソリューションを超えて、組織全体のデジタルトランスフォーメーションとイノベーションを推進する高度なユースケースに移行しています。

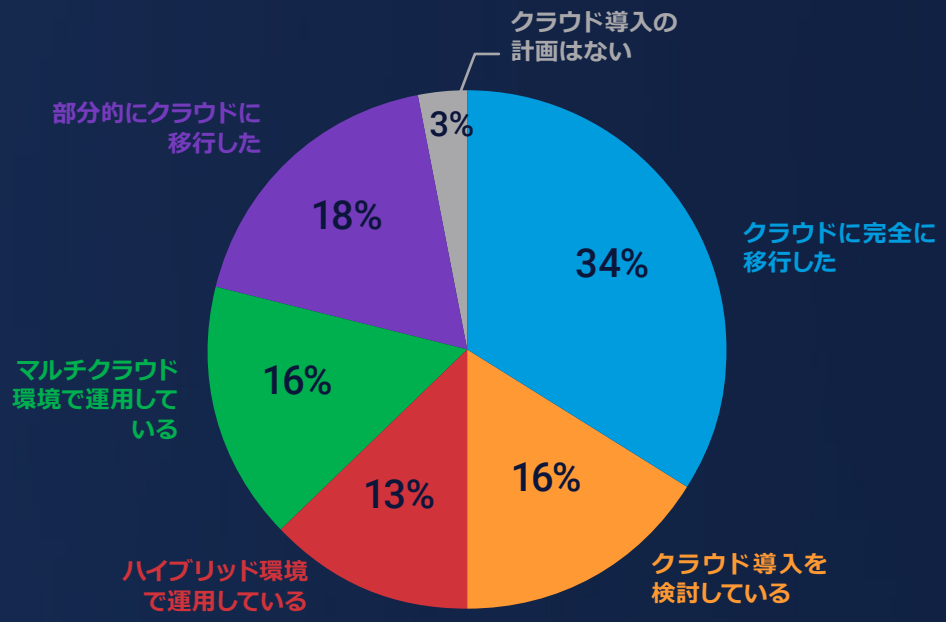
この相対的なクラウド導入の成熟度には、クラウドをビジネス改革の手段ではなく、ビジネスに不可欠なものとしてとらえるという、考え方の変化が表れています。

オーストラリアとニュージーランドでは、公的セクターもクラウド採用の主要な推進力であり、ニュージーランドは 2012 年に、オーストラリアでは 2015 年にクラウドファーストの政策を打ち出しました。

オーストラリア企業は、2024 年にパブリッククラウドに 154 億米ドルを支出すると推定され、2023 年から 19.7% 増加しています（出典：Gartner）。

デジタル化を進めている最中であるということは、ANZ の組織はクラウド向けに設計されていない、コンテナ化されていない、またはマイクロサービスベースではない従来のアプリケーションを所有している可能性があり、クラウドネイティブアプリケーションより高いコストを負担することになることを意味します。

貴社はクラウド導入プロセスのどの段階にありますか？



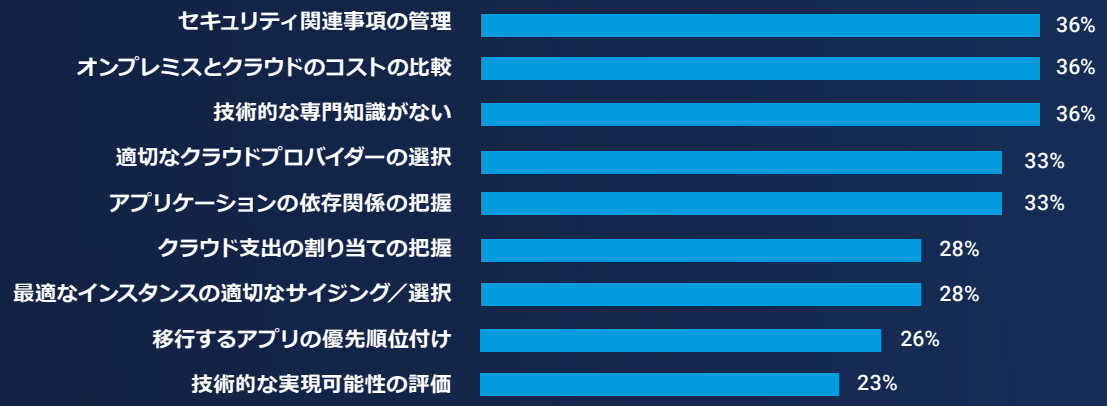
ANZ の調査回答者は、クラウド移行で直面する最大の課題の 1 つとして、セキュリティへの影響と技術的な専門知識の欠如と共に、クラウドコストを挙げています。

テクノロジー導入の規模に加えて、イノベーションへの圧力と経済の低迷によって、クラウドの無駄を最小限に抑えることへの関心が高まっています。

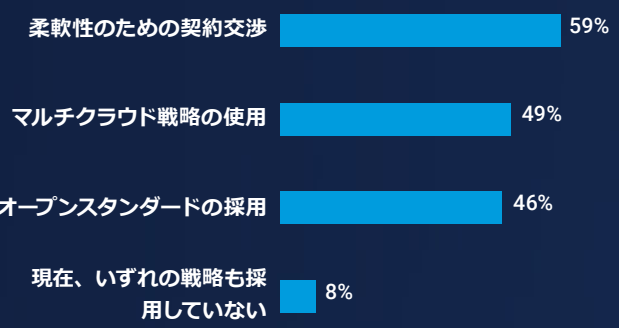
クラウドコストは、さまざまな要因に応じて様々にスケーリングするマイクロサービスやマルチクラウド展開の予測と理解に必要な専門知識と時間によって、複雑になりかねません。

FinOps などのクラウドコスト管理ソリューションを用いることで、クラウドの変動する支出モデルを、財務的に説明できるようになります。ユーザーは、組織のクラウド使用状況と生産性の最適化の機会を可視化して、支出の決定に責任を負います。

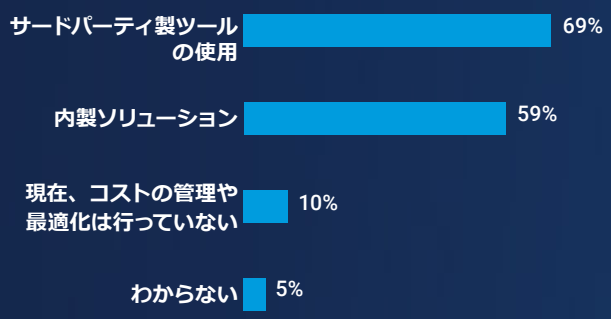
クラウド移行で直面した主な課題は何ですか？



ベンダーロックインを回避するための戦略



クラウドコストを最適化するサードパーティ製ツール



ANZ の IT リーダーは、サードパーティツールやマネージドサービスを活用しているほか、より多額の支出や大きな成長率をコミットする代わりに割引を得られるよう契約交渉を行っています。

クラウド運用管理と財務ガバナンスを統合することで、年間のクラウド予算を超える無制限の自動スケーリングによるリスクから組織を守ることができます。

DNB は効率的で持続可能なスケーリングを実現するためにサードパーティツールやマネージドサービスを活用して専任のスタッフを増員しているため、これは相対的なクラウド導入の成熟度を示しています。

Akamai のグローバルネットワークは世界中の 1,200 のネットワークに統合されており、すべての主要クラウドプロバイダーとの最適化された相互接続を維持して、高可用性、低レイテンシー、無限の拡張性を確保します。

顧客体験の向上が機微な情報の増加につながる

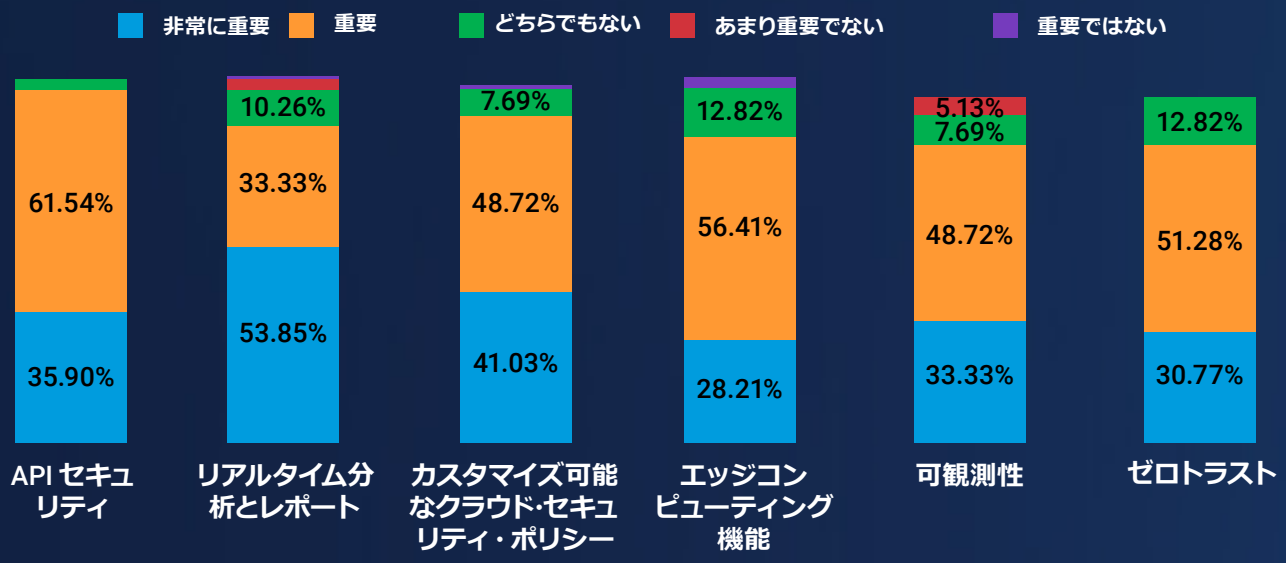
顧客のデジタル化が比較的進んでいるため、ANZ の企業は最適なユーザー体験を提供するために、リアルタイムデータをインジェスト、処理、分析し、そのデータに基づいて行動する能力を求めています。

ANZ の回答者の約 87% が、クラウド/セキュリティ・ソリューション・プロバイダーの評価において、リアルタイム分析やレポートなどの製品機能を非常に重視/重視していると回答しています。

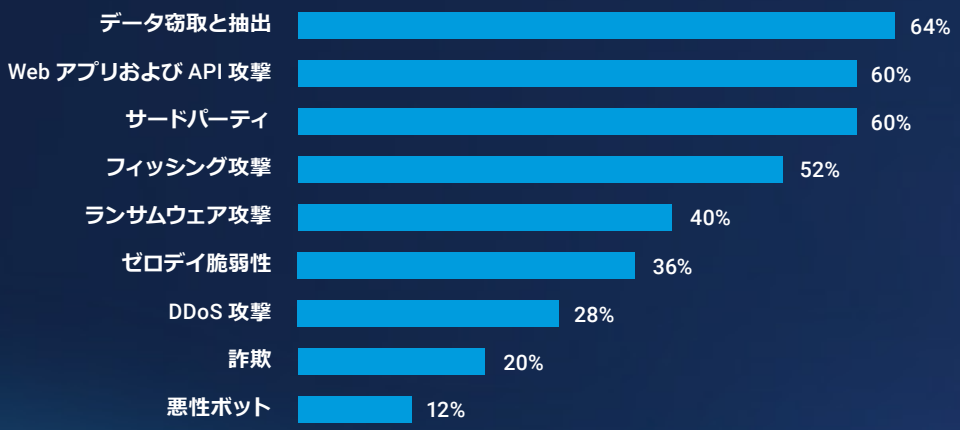
同時に、ANZ のデジタルネイティブ企業の中でより豊かな顧客体験を追求することにより、豊かな個人データや財務データを標的としたサイバー攻撃にさらされるリスクが生じます。

Akamai の金融サービスにおけるサイバーセキュリティに関するレポートによると、Web アプリケーションおよび API 攻撃に加えて、データ窃取や抽出が、オーストラリアの IT リーダーの懸念する主なサイバー脅威となっています。

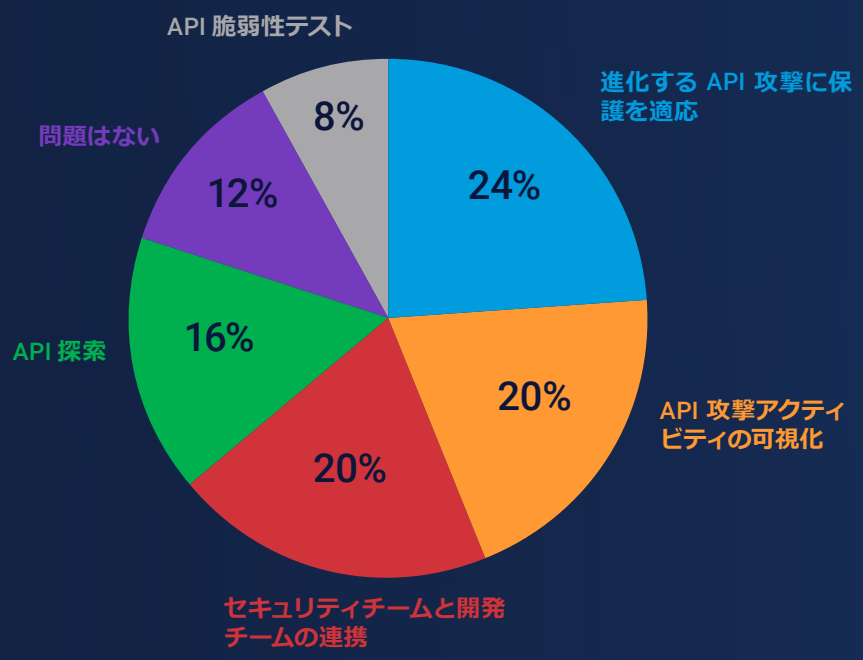
クラウド/セキュリティ・ソリューション・プロバイダーの評価において、次の製品機能はどの程度重要ですか?



オーストラリアの IT リーダーの懸念する主なサイバー脅威



API セキュリティに関して直面している最大の問題は何ですか?



また、セキュリティ面においても、ANZ の IT リーダーたちは、API セキュリティの最大の課題として、API 攻撃アクティビティに対する可視性の向上（20%）と、進化する API 攻撃に対する対策の適応（24%）を挙げています。

「見えないものは守れない」という格言があります。多くの企業は自社の API の数を把握してさえいないため、リスクを定量化することが困難になっています。

API アクティビティの可視性の向上に成功した多くのエンタープライズを驚かせたのは、環境内で誰にも知られることなく動作しているシャドウエンドポイントの多さでした。

そのため、ANZ の回答者の 97% がクラウド／セキュリティ・ソリューション・プロバイダーを評価する際の非常に重要または重要な製品機能として API セキュリティをあげています。

リアルタイムの分析とレポートにより、サイバー攻撃の発生時に迅速な検知と対応が可能になり、被害を軽減できます。

繋がる ASEAN：デジタル経済が地域の成長を促進

東南アジアは世界で最も急速に成長しているインターネット市場であり、毎日 12 万 5,000 の新しいユーザーがインターネットにアクセスしています（出典：世界経済フォーラム）。

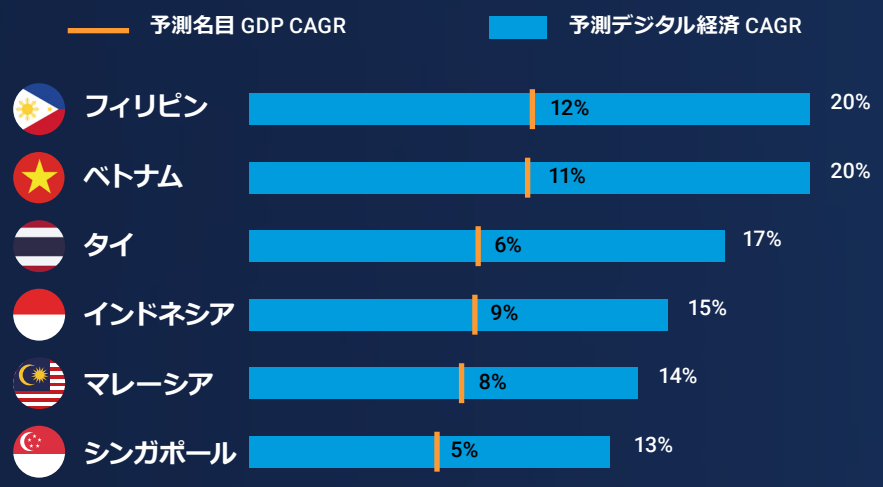
デジタルネイティブのコネクテッドミレニアル世代と Z 世代は、2030 年までに ASEAN の消費者の 75%、インドネシアの消費者の 70% を占めると予想されています（出典：世界経済フォーラム）。

実際、デジタル経済の総市場価値の伸びは、ASEAN 諸国全体の GDP 成長率を上回っています（出典：e-conomy SEA 2023）。

ASEAN の消費者はデジタルライフを急速に受け入れていますが、同地域のインフラは依然として改善が必要です。デジタルに精通した若い世代は、サービスのアップタイムと低レイテンシーに対する高い期待を抱いています。

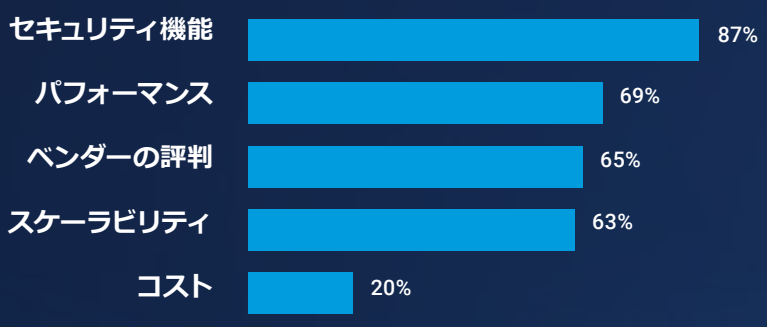
そのため、ASEAN の回答者はベンダーの選定においてパフォーマンスとベンダーの評判を重視していると考えられます（それぞれ 69% と 65%）。

デジタル経済の GMV 成長率対 GDP 成長率（2023 年 ~2025 年）



（出典：e-conomy SEA 2023、Google、Temasek、Bain & Company）

クラウドベンダーの選定に影響する要因



同時に、ASEAN の DNB が絶えず直面している問題として、ネットワークのレイテンシーがあります。

この地域では依然として、高速で信頼性の高いインターネット接続と、都市部や農村部での電力の普及を確保する必要があります。17,508 の島（非公式な情報によると 25,000 近くの島）があるインドネシアのように地理的に分散している国では、接続がまだ不安定です。

回答者のうち 3 人に 2 人以上が、ネットワークのレイテンシーを、組織のクラウドインフラのパフォーマンスと機能のギャップとして挙げています。

この地域の政府は、継続的な成長を支えるため、接続性に積極的に投資してきました。

インドネシアは最近、Palapa Ring プロジェクトを完了し、国内で 35,000 km 以上の陸上および海底光ファイバーケーブルを使用して、最も離れた地域にも 4G インターネット接続を提供しました。

> ***Akamai は、他のプロバイダーよりも広い地域でインフラを提供しており、コアとエッジでクラウド・コンピューティング・リソースを提供します。また、地域の嗜好を満たすように設計された低レイテンシーでデータ量の多いアプリケーションを強化し、グローバルにスケーリングできる能力を備えています。***

API セキュリティは ASEAN にとって重要な製品機能

ASEAN の DNB は、API によって自社の運営が維持され、他のベンダーやエコシステムパートナーとのコラボレーションが促進されていることを痛感しています。

ASEAN の回答者は、ANZ（69%）とインド（91%）の回答者と比較して、高度な API 攻撃の認識と緩和に対して最も自信を持っています（99%）。

実際、ASEAN の回答者のほぼすべて（99%）が API セキュリティを非常に重要または重要と評価しています。

しかし、API スプロールは現実であり、急速な成長は可視性の欠如を意味し、すぐにセキュリティやコンプライアンスの課題となる可能性があります。

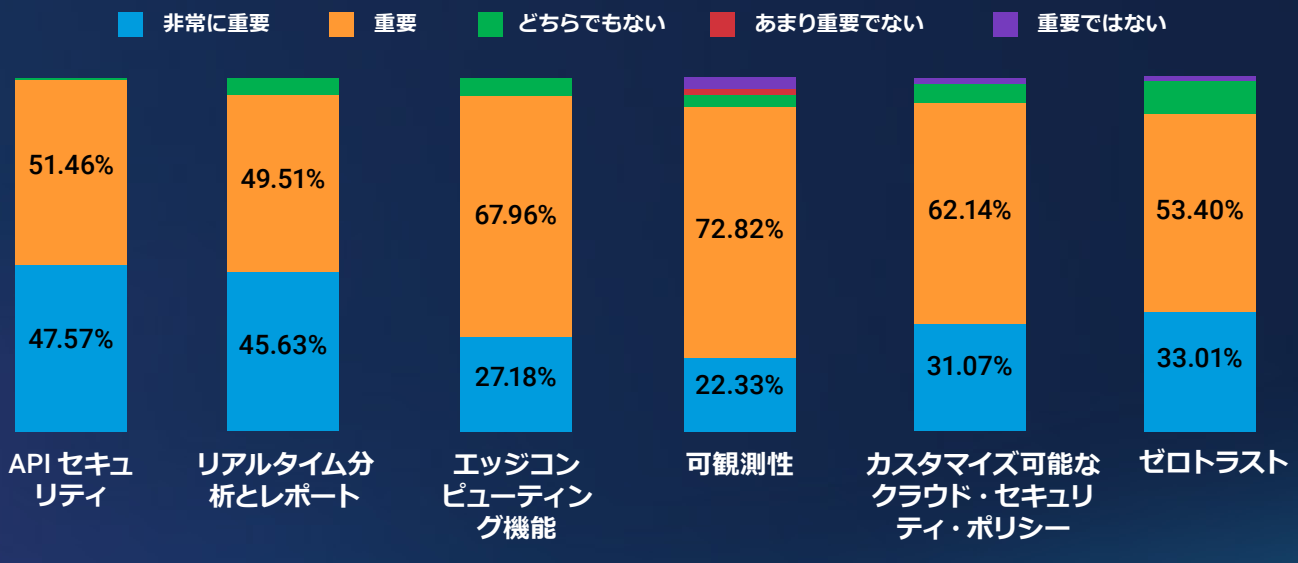
API のセキュリティを確保するためには可視性が重要です。シャドウ API やローグ API などの盲点が明らかになれば、セキュリティチームはそれまで認識していなかった脆弱性に対処できます。

したがって、リアルタイムの分析やレポートは、ASEAN の回答者の 95% 以上が非常に重要／重要と評価しています。適切な注意を払わなければ、API はデータ漏えい、コンプライアンス違反、ガバナンスの欠如などの原因になる可能性があります。

OWASP API Top 10 に記載されたような高度な API 攻撃について、把握と緩和にどれほど自信がありますか？

地域	自信がある／非常に自信がある
ASEAN	99%
ANZ	69%
インド	91%

クラウド／セキュリティ・ソリューション・プロバイダーの評価において、次の製品機能はどの程度重要ですか？



前例のないデジタル化の急速な進展により、フィッシングに関する懸念が高まる

デジタル採用率の高さは、ASEAN の DNB にとって両刃の剣になっています。

デジタル化があまりにも急速に進んでいるため、顧客はオンラインで情報を交換する際に必ずしもプライバシーに細心の注意を払っていません。フィッシングは、E メールベースの攻撃から、モバイルデバイスやソーシャルメディアをも含めた攻撃へと進化しました。

その結果、この地域ではフィッシングの被害が顕著で、2023 年だけでも約 50 万件以上の被害が報告されています。

ASEAN 全体のデータ保護とプライバシーに関する法律は、各国政府の、急速に変化するデジタル通信のトレンドに対応する能力に大きく依存しています。たとえば、テキストメッセージ内のクリック可能なリンクは、依然として人気のある詐欺戦術ですが、多くの国でこの一般的なフィッシング手段をブロックするポリシーが実装されています。

調査対象となった ASEAN DNB は、同地域の同業他社よりもフィッシング防止技術への投資を優先しています。

フィッシングはなくなりません。

生成 AI の登場により、フィッシング攻撃がより有力になり、犯罪者が被害者を標的とするための選択肢が増加します。結局のところ、フィッシングは、ソフトウェアの脆弱性やシステムの悪用ではなく、人間の性質を利用する攻撃と言えます。

このような場合、攻撃が最大の防御になります。フィッシングシミュレーションと強固なエンドポイント防御を組み合わせることで、DNB はフィッシングを巡る戦いで先手を取ることができます。

2023 年に東南アジアで検知およびブロックした金融フィッシング

国	金融フィッシングの件数
フィリピン	163,279
マレーシア	124,105
インドネシア	97,465
ベトナム	36,130
タイ	25,227
シンガポール	9,502
合計：	455,708

出典：Kaspersky、2024 年

以下のサイバーセキュリティ投資分野を、最も重視する（上）から最も重視しない（下）にランク付けしてください

1. フィッシング防止テクノロジー
2. 高度な API セキュリティ
3. Web アプリケーションセキュリティ
4. ゼロトラスト関連のテクノロジー
5. 分散サービス妨害（DDoS）の緩和

インド：イノベーション（Innovation）の「I」

インドは 10 年以上にわたってイノベーションと DNB の中心地であり、クラウドネイティブアーキテクチャと実験の主要な拠点でした。

インドの DNB は、成長とイノベーションに重点を置いており、地域のクラウドインフラ内で最も高い AI 統合（98%）を実現しています。また、ほとんどの DNB は、クラウドをすでに導入しているか、クラウド導入を検討しています。

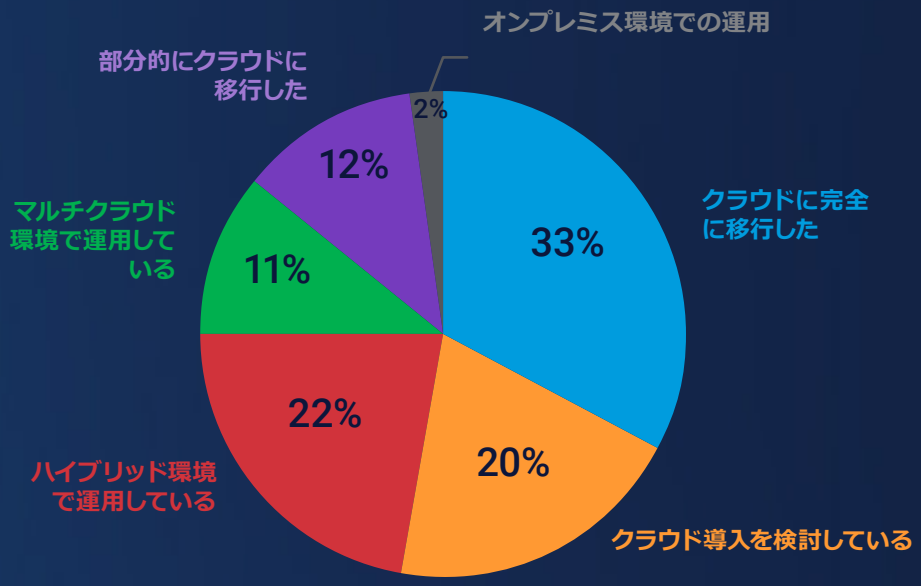
しかし、インドの DNB は成熟に伴い、セキュリティとコストの最適化に重点を置き、ベンダーの選定を慎重に検討することで、持続可能な成長に目を向け始めています。

インドにおける設立直後の DNB の顧客は、多くの場合、テクノロジー企業自身です。

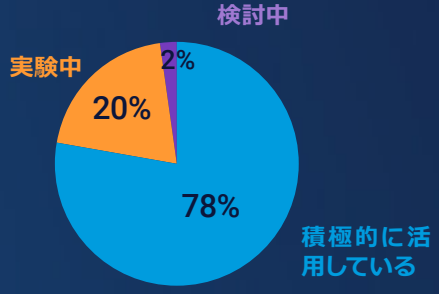
インドの DNB は、API を活用して、顧客のデータに直接アクセスすることなく、技術サポートと専門知識を世界中の企業に提供してきました。インドの DNB は、専門知識、API、専用構築のシステムに早くから投資しています。

インドのデジタルネイティブは、技術的な優秀性に根ざした伝統を持っており、ASEAN や ANZ 地域の競合他社よりもベンダーのパフォーマンスを重視しています（ASEAN では 2 番目、ANZ では 4 番目）。

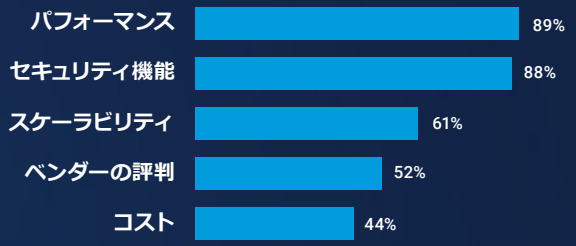
貴社はクラウド導入プロセスのどの段階にありますか？



クラウドインフラ内における AI テクノロジーの現在の統合レベル



クラウドベンダーの選定に影響する要因



社内（In-house）専門知識の「I」

インドのデジタルネイティブ企業には、他の地域のデジタルネイティブ企業と比較して、クラウドコスト管理に DIY のアプローチで取り組んでいるという特徴もあります。

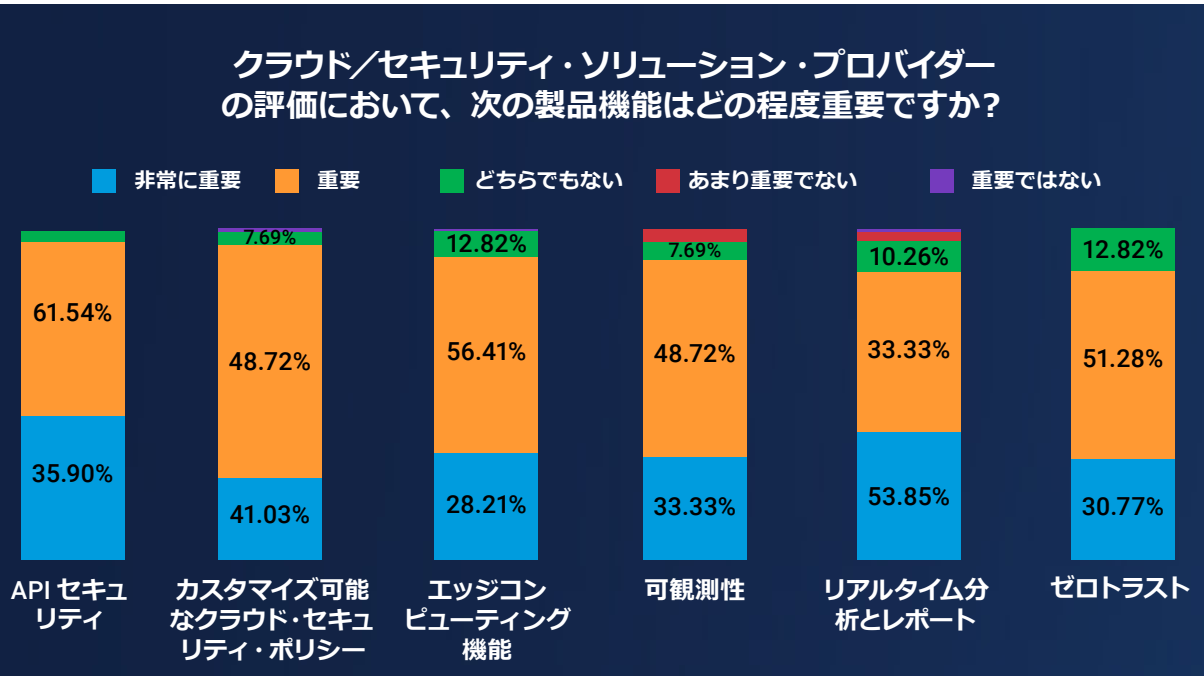
インドでは、全体の 73% の回答者が社内ソリューションを使用してクラウドコストを管理および最適化していると回答しています。一方、ASEAN（78%）と ANZ（69%）の回答者は、サードパーティツールの使用を好みます。

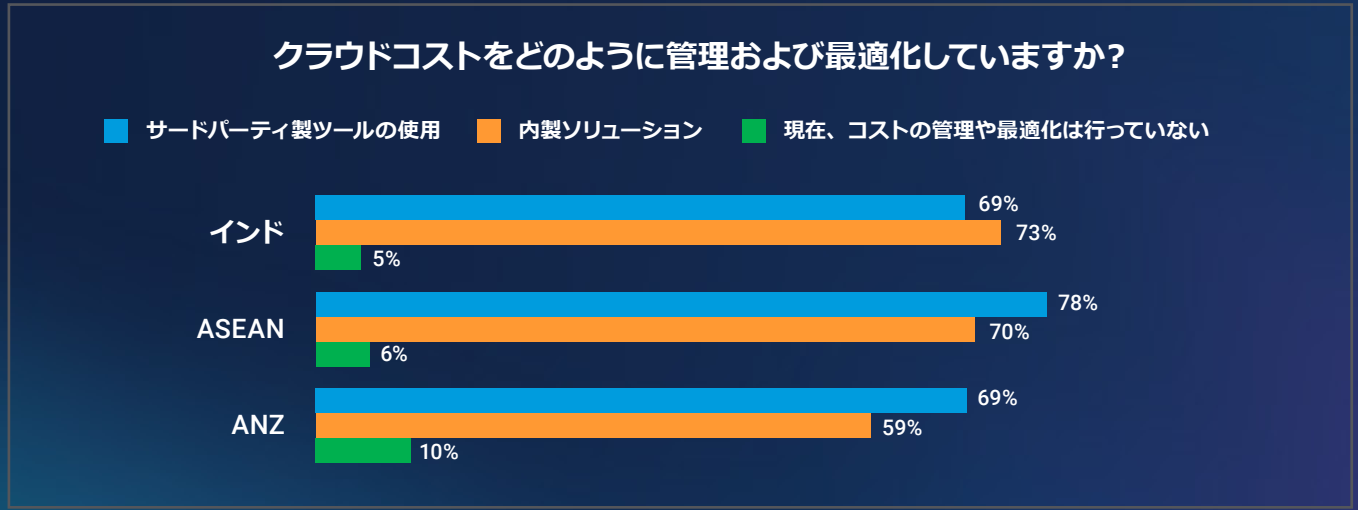
ANZ の回答者がサードパーティ製ツールを好む理由として、ローカルの IT スキルが不足していることが挙げられます。

ANZ においては、毎年 **5,000 人のサイバーセキュリティ人材**の需要がありますが、現地の教育システムによると、2026 年までに見込まれるサイバーセキュリティ専門家は 2,000 人程です。

一方、インドには、世界のテクノロジーサービスのハブとしての歴史が強みとしてあるインドには、スキル豊富な人材が多く存在します。

現在、インドの **1,600 以上のグローバル・ケイパビリティ・センター**（GCC）では、世界中の組織にテクノロジーサポートを提供しています。2030 年までに増加が計画されており、約 2,500 の GCC で 450 万人を超える従業員を雇用し、1,000 億ドルの収益を生み出します。





DIY が原因でインドの DNB は脆弱性にさらされている

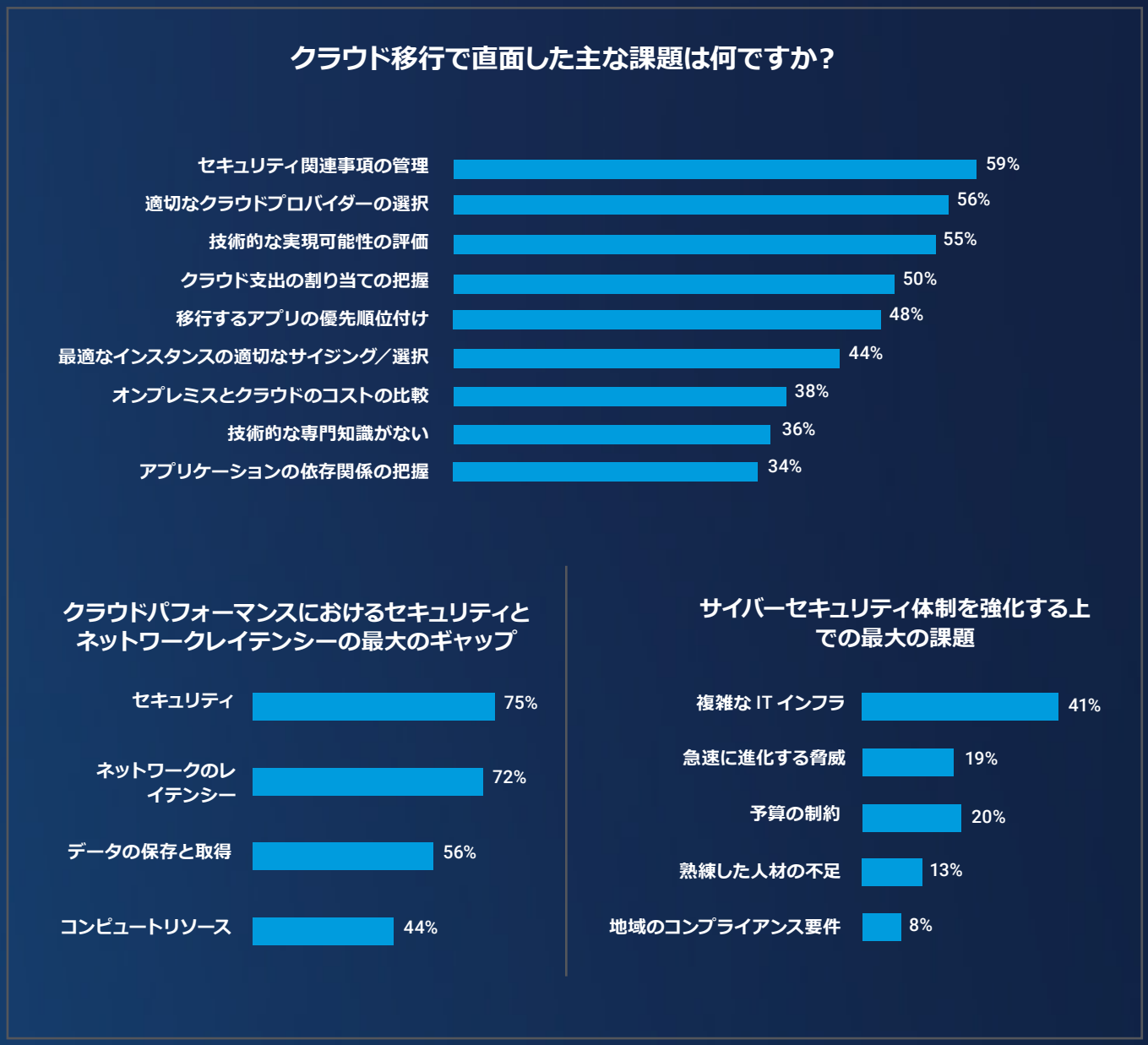
インドのデジタルビジネスは、テクノロジーインフラの管理に DIY のアプローチを採ることが原因で、組織として規模を拡大して成熟するにつれて脆弱性に晒される可能性があります。

複数のシステムを複数の API と統合することで、潜在的なアタックサーフェスが増大します。クラウドネイティブの組織や全面的にサービスをオンラインで展開している企業にとって、この問題は更に深刻なものとなります。

インドの回答者のうち 5 人に 3 人が、クラウドインフラとクラウド移行に関するセキュリティへの影響の管理を最優先課題として挙げています。実際、回答者のうち 4 人に 3 人が、組織のクラウドインフラにおける最大のギャップとして、セキュリティを挙げています。

インドの DNB は、自社の脆弱性と潜在的な攻撃シナリオをあらゆる角度から確認する必要があります。サイバー脅威の現状は急速に進化しており、新たな攻撃方法やツールはますます巧妙化しています。

インドの DNB は、専門的なスキルを備え、新しいテクノロジーの効率性を活用しているサードパーティと提携することで、テクノロジーの自給自足という制約から抜け出す必要がある可能性があります。



調査回答者の 41% が、組織のサイバーセキュリティの姿勢を強化する上での最大の課題として、複雑な IT インフラを挙げています。一方、ANZ の回答者の 36% が、複雑な IT インフラを課題として挙げています。

24 時間体制の専門家のサポートなしに社内でサイバーセキュリティを管理することは、現実的な選択肢ではなくなっています。インドはサイバー攻撃の主な標的となっており、こうした国のような急成長市場では特に当てはまります。

これこそが、インドの技術インフラのジグソーパズルの中核となる部分です。

> ***Akamai の分散型クラウドプラットフォームは、開発者がコンピュートリソースの展開場所と拡張場所を制御できるようにします。開発者は、データをキャプチャ、処理、管理する場所を定義する能力と柔軟性を手に入れられます。***

共に強くなる

この調査では、アジアのデジタルネイティブ企業がAI、クラウドコンピューティング、ビッグデータを活用して、より豊かで高速な顧客体験を実現する中で、こうした企業のテクノロジーリーダーが直面している課題について、画期的な知見を提供しています。

しかし、すべてのデジタルネイティブ企業を画一的に扱うのは安易です。

この調査では、アジア太平洋地域のさまざまな地域や業界における、クラウド／API の成熟度と、デジタルネイティブのサイバーセキュリティ体制の、微妙な違いを区別しています。

例えば、規制の厳しい業界や地域では、セキュリティとプライバシーのバランスとともに、ユーザー体験を実現することが求められます。

1 ミリ秒が重要であるデジタルネイティブ企業にとっては、地域ごとの最適化によってパーソナライズされた体験を実現する最先端の機能が極めて重要です。

そのすべての根底には、クラウドネイティブアーキテクチャを支える、適切に設計された API とエンドポイントがあります。デジタルネイティブ企業はそれによってスケーリングアップ／アウトして、パーソナライズされた豊かな体験を提供することができます。

ほとんどの組織では、クラウドを効果的にロックダウンするために必要なネイティブの可視性とセキュリティ制御が欠如しています。パブリック環境とマルチクラウド環境のセキュリティを確保するためには、セキュリティ担当者は、環境内でどのアプリケーション、ワークロード、トラフィックフローが移動しているかを確認できる必要があります。

Akamai は、組織がクラウドアーキテクチャにアプローチする方法を変革し、分散型、脱中央集中型、低レイテンシー、グローバルにスケーラブルな設計を強調しています。これは、エンドユーザー近くで実行する必要のある高性能のワークロードに最適です。

Akamai は世界中のアクセス困難な市場でコア・コンピューティング・リージョンを確立する取り組みを推進しており、131 か国の 4,100 以上のエッジ PoP にまたがる超分散型フットプリントを構築しました。

世界のトップ企業が Akamai を選び、デジタル体験の構築、提供、セキュリティ保護を行っている理由を、ぜひご覧ください。

手法

この調査では、地域の IT リーダーに対する現場調査からこのような知見を明らかにしました。
本調査は、2024 年 3 月から 5 月の期間に実施されました。

目的

このレポートは、デジタルネイティブ企業が今後のトレンドや脅威をどのようにとらえているのかを把握することを目的としています。これらの調査結果は、現在の現場での知見に基づいた、貴重なベンチマークとなります。

対象者

最高情報責任者、最高技術責任者、IT ディレクター、および以下の業界の VP：

- 航空会社
- メディア／放送／出版
- e コマース／インターネット
- ゲーム
- サービス業
- 情報テクノロジー
- 小売／卸売

場所

- オーストラリア
- ニュージーランド
- インド
- シンガポール
- インドネシア
- タイ
- マレーシア
- ベトナム