

2022年の アジア太平洋地域における 顧客ID&アクセス管理の状況

顧客ID&アクセス管理を推進する
トレンドと課題

Okta Inc.
80 Pacific Hwy
North Sydney, NSW 2060
info_apac@okta.com
+61 2 8310 4484



目次

Contents

- 3 セキュアでシームレスなユーザ体験に対するニーズ
- 4 調査方法
- 5 CIAMの重要性
- 7 企業におけるCIAMの実装
- 8 ソリューションの選択
- 11 CIAMの活用における課題
- 15 結論
- 16 直感的で一貫性のある、信頼性の高いオムニチャネル体験を

セキュアでシームレスな ユーザ体験に対する ニーズ

新型コロナウイルスの影響によってデジタル化が進み、デジタルサービスが私たちの生活の隅々まで広がっています。また、企業はお客様に対してより良いデジタル体験を届けるためにさまざまな取り組みを進めています。

より良いデジタル体験を提供していくためには、セキュアでシームレスなサービスをできるだけ早く市場投入する必要があり、そのために、あらゆる企業がCIAM（顧客ID&アクセス管理）ソリューションを活用しています。企業はコンシューマー向けアプリケーションやSaaSアプリケーションに安全なID管理の仕組みを組み込むことが可能になります。また、パートナーやサプライヤー、委託先が適切なリソースにアクセスできるようにすることで、効率的な協業ができるようになります。

アイデンティティ・レイヤーの構築は、複雑で多くの時間がかかることがあります。製品開発や機能強化・運用など、コアなタスクに割くべき開発者の時間がとられ、重要アプリケーションの市場へのリリースが遅れてしまうことがあります。実装を適切に行えなければリスクは高まり、また、使い勝手の悪い認証フローでは、お客様に不満が募るだけでなく、決済の手間によって、せっかくカートに入れた商品の購入も諦めてしまいかねません。欠陥のあるセキュリティ態勢では侵害リスクが増加し、ユーザの信頼を得られず、お客様離れにつながるリスクを伴います。

CIAMは組織のデジタルの入り口を守るカギ。

企業はどのように取り組むべきか

当社の調査によって、アジア太平洋地域全体におけるCIAMの認知度は高く、組織のセキュリティ戦略においても、その重要性が理解されていることが分かりました。企業は、顧客体験こそが将来的に製品やサービスを差別化できるカギであることを認識しています。CIAMを複雑であると認識している一方で、CIAMが顧客ロイヤルティを確立し、パートナーやサプライヤーとの協力を向上させ、収益を増加させるのに不可欠であると評価しています。



調査方法

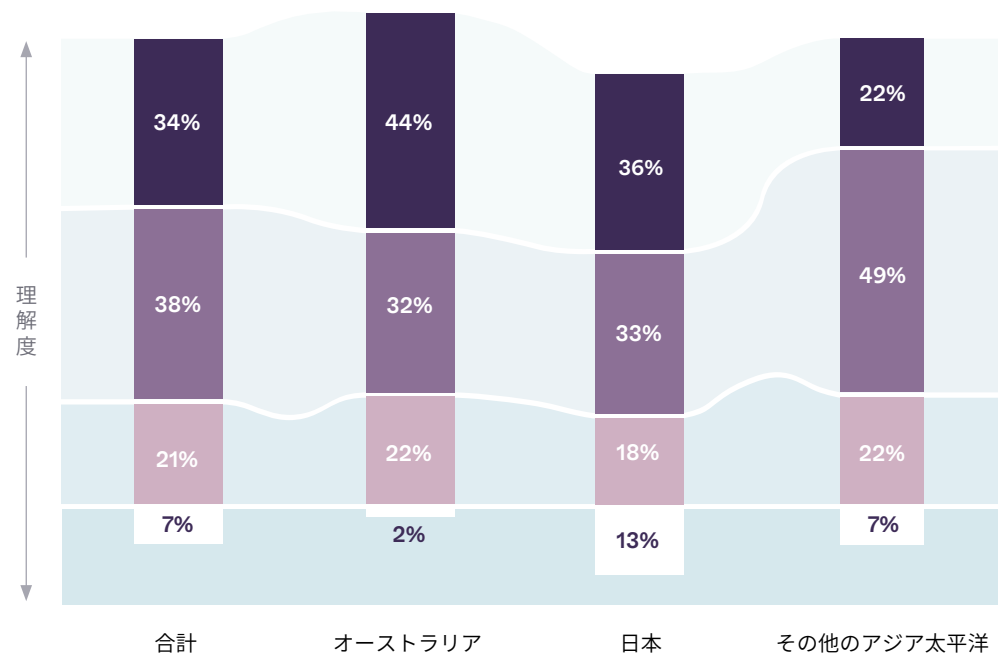
Oktaは2022年2月28日から3月4日まで、調査会社のStatistaと共同でオンライン調査を実施。調査では、日本、韓国、香港、シンガポール、フィリピン、オーストラリアにおいて、役員、IT部門・エンジニアリング部門のマネージャーやディレクター、エンタープライズ・アーキテクト、コンプライアンス・マネージャー、デジタル部門のディレクターおよび開発者など、合計320人に調査を実施しました。この調査は、アジア太平洋地域において、企業がどの程度CIAMを優先し実装されているか、また、採用をするうえで主な動機付けとなる要因は何かを探る目的で行われました。



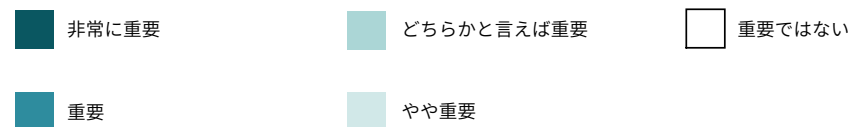
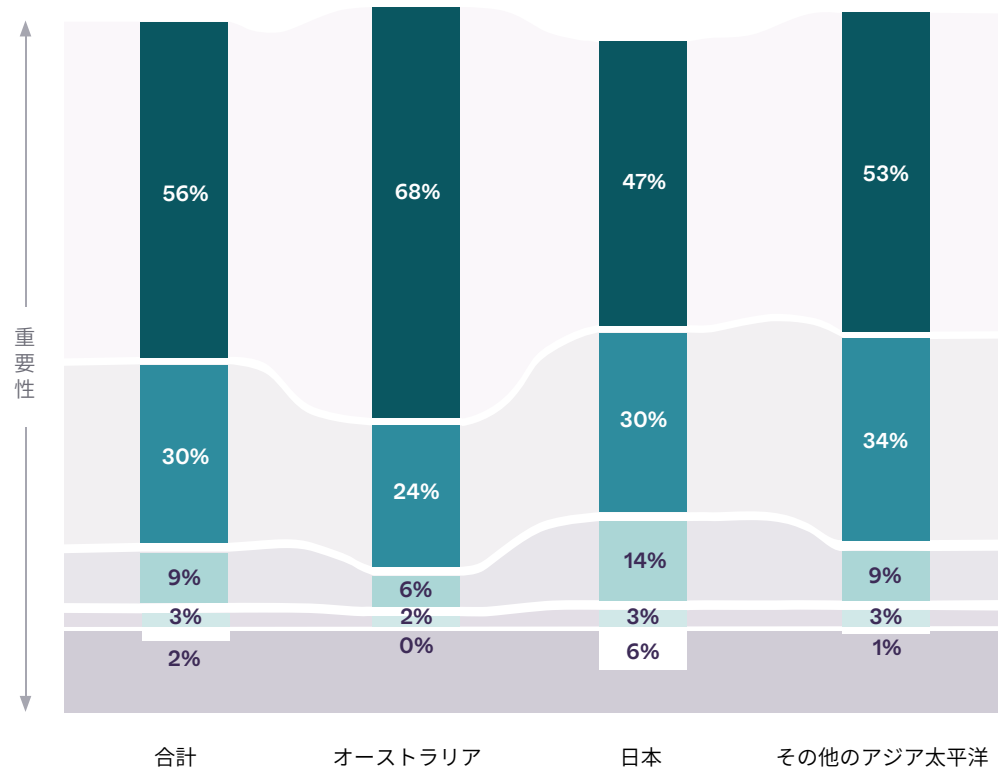
CIAMの重要性

手軽で安全なデジタル体験が広がるにつれて、CIAMの重要性は、アジア太平洋地域全体で議題に上るようになりました。新型コロナウイルスの影響によってすべての事業部門でデジタルシフトが加速し、アイデンティティ・レイヤーにおけるサイバー攻撃もこれまでに多く増えています。こうした背景のもとで、デジタルにおける取引を保護することは、かつてないほど重要になっています。

これにより、CIAMソリューションの存在感が高まってきており、今では、地域全体にわたってCIAMの認知も広がっています。回答者の72%が「CIAMを十分理解している」または「専門的に理解している」と回答しており、全く知らないと回答したのはごく少数(7%)に限定されました。特にオーストラリアでの理解度は高く、回答者の44%が自身をCIAMのエキスパートであると述べています。

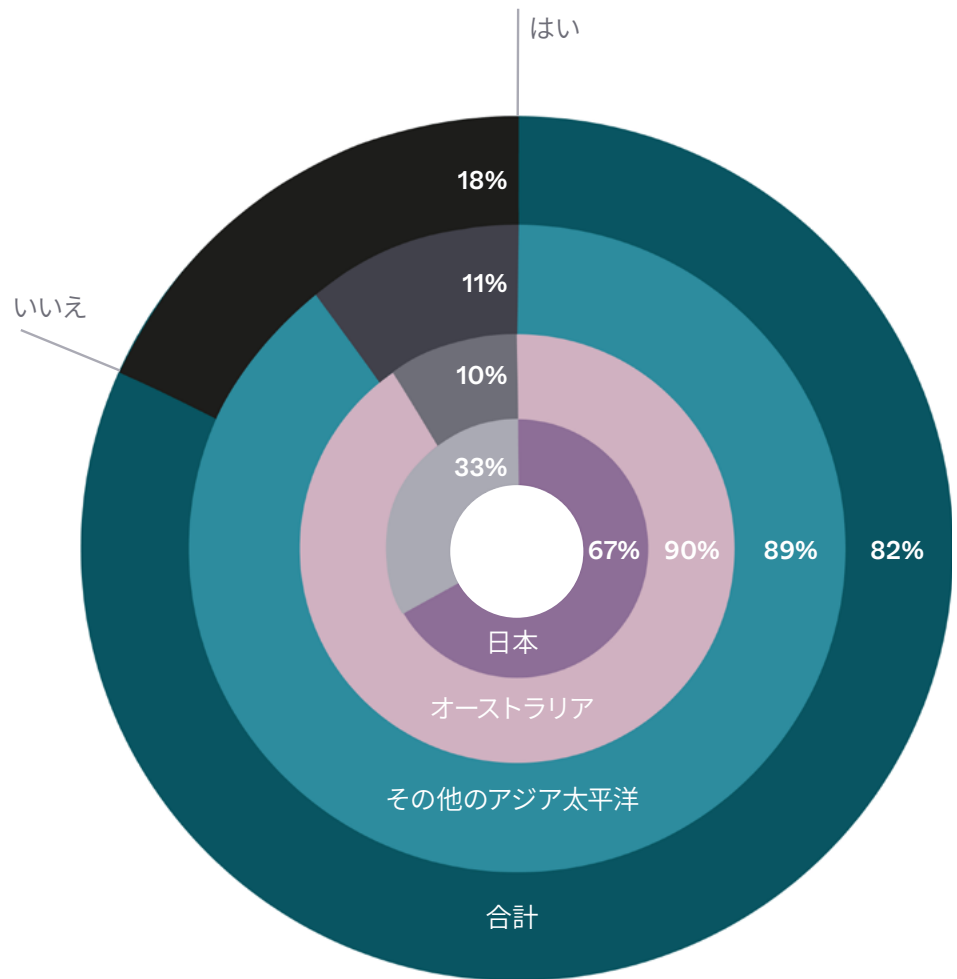


「CIAMの認知」と「その重要性の認識」には相関関係があります。最もCIAMへの理解度が高い（76%が専門的または十分な理解をしていると回答）オーストラリアでは、68%がCIAMをととても重要であると述べており、オーストラリア以外の地域全体の56%と比べて高くなっています。



82%の回答者が、社内またはアウトソーシングによりCIAMソリューションを構築しています。日本は他の国と異なり、1/3がまだCIAMを採用していません。現時点でCIAMソリューションを実装していない企業のうち48%は今後12カ月から18カ月の間に実装する予定としており、その割合はオーストラリアでは2/3に上ります。

企業における CIAMの実装



信頼性の高いセキュアな体験が採用を促進

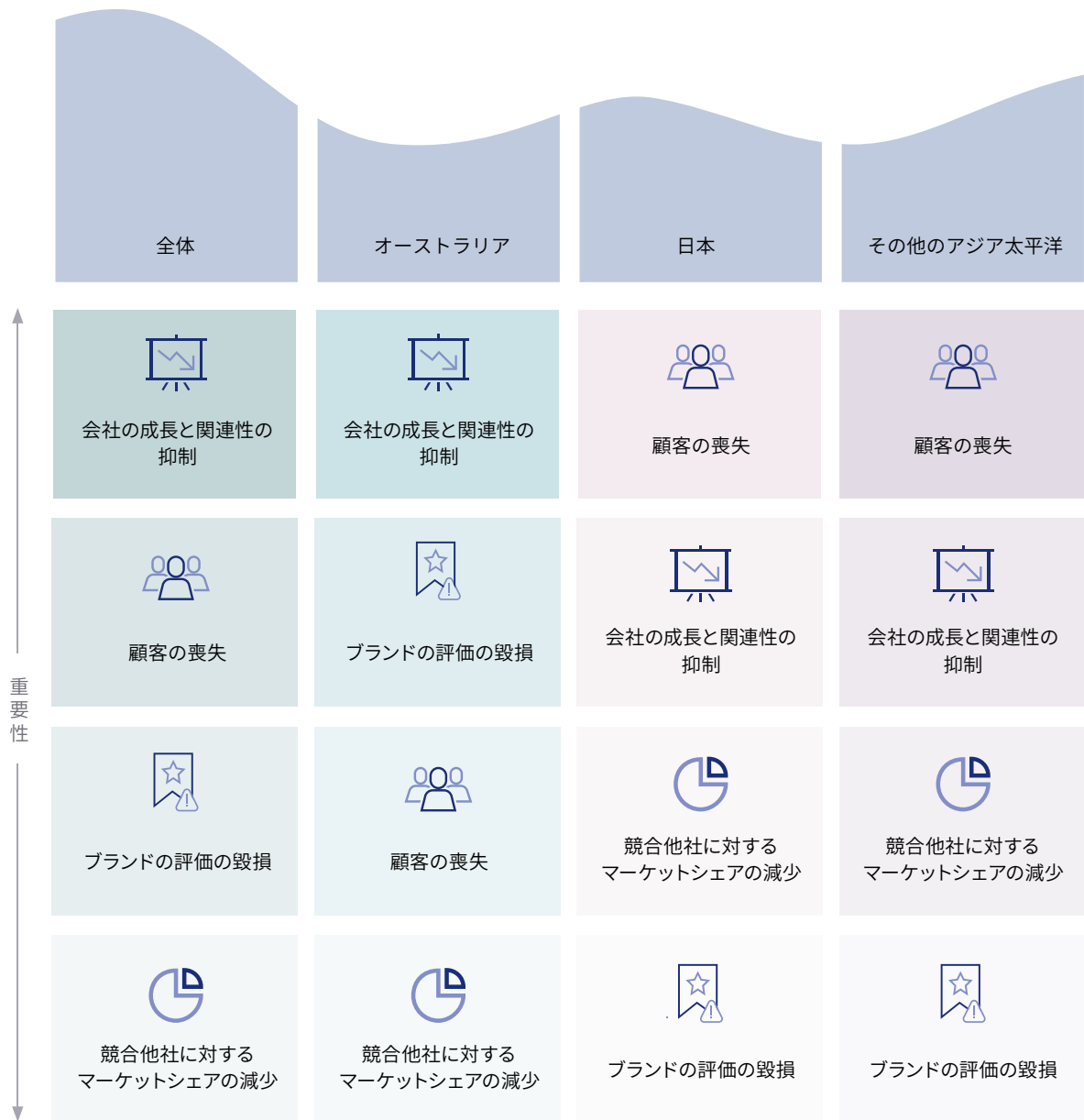
世界的にサイバー攻撃の脅威が高まっており、とりわけアイデンティティが攻撃の対象になっています。Verizonの2021年データ漏えい/侵害調査報告書によると、侵害の61%は認証情報の悪用に起因しているとしています。セキュリティがCIAMの採用の主な要因になっていることは驚くことではありません。実際89%の回答者が、CIAMは自社全体のセキュリティ戦略にとって重要と答えており、全く重要でないと答えたのはわずか3%でした。

お客様が期待するセキュアでシームレスなデジタル体験を提供できないリスクは、常につきまといます。そのリスクで最も懸念されていることは、会社の成長の抑制(34%)、顧客の喪失(30%)、ブランド評価の毀損(21%)、マーケットシェアの減少(15%)です。

64%

現時点でCIAMソリューションを利用していないオーストラリアの回答者で、今後12カ月から18カ月の間に実装を予定している割合

優れた顧客体験を提供できないことで起こるビジネス上の重大リスクとは？

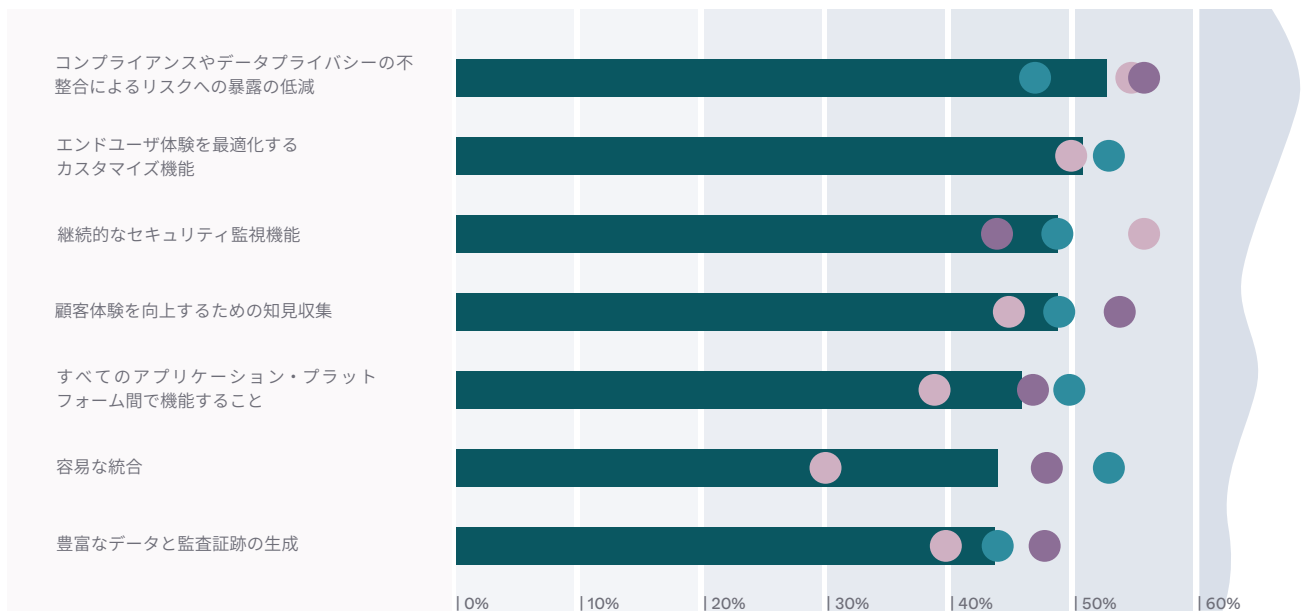


ソリューションの選択

CIAMソリューションのメリットは幅広く、組織は収益の向上、セキュリティリスクの低減と開発者への影響の最大化を支援するさまざまな主要機能に対して、ほぼ同等に重きを置いています。

データ保護およびプライバシーの法律により、この地域で企業に求められるコンプライアンス要件が高まっていることから、コンプライアンス違反や一貫性のない同意管理によるリスクを低減することが最優先となります。半数以上（53%）が、適切なCIAMソリューションを選ぶ際に、この機能を最も重要視すると述べています。これに続き、エンドユーザ体験を最適化するカスタマイズ機能（51%）、継続的なセキュリティ監視機能（49%、ただし日本では56%）、統合の容易さ（44%）となっています。また、企業は顧客に関する知見を利用してユーザ体験を改善する機能がカギとなるとみなしており、49%がこの重要さに同意しています。

ビジネスにとって適切なCIAMソリューションを選択するうえで最も重要なことは何か



- 合計
- オーストラリア
- 日本
- その他のアジア太平洋

56%

日本においてCIAMの継続的なセキュリティ監視を優先する回答者の割合

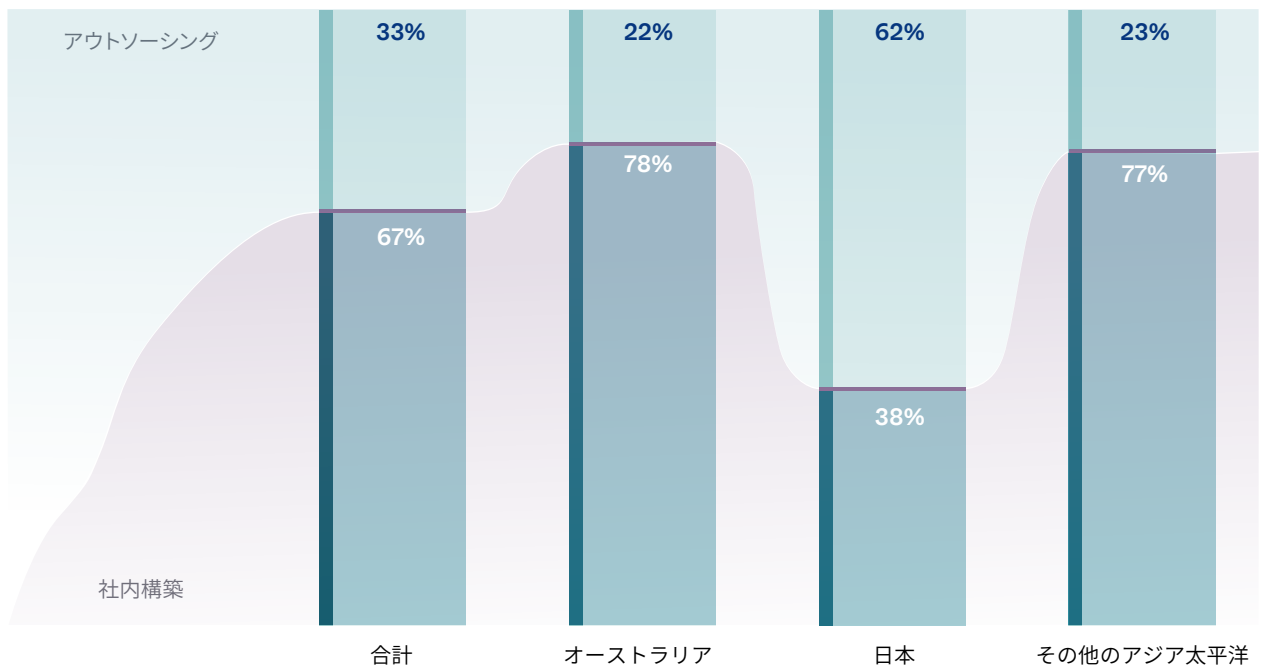
開発者が第一に考えるセキュリティと利便性

開発者にとって最も重要なCIAMの側面は何かと尋ねると、セキュリティが最も高く（33%）、信頼性（22%）、使い勝手の良さ（16%）、高いユーザ体験（15%）と続きます。日本では他の国と比較して「信頼性」に33%と高い価値が置かれており、セキュリティ（34%）とほぼ同等でした。

日本を除き、社内ソリューションが優勢

CIAMの実装では、「自社が独自でソリューションを構築」する方法と、「専門ベンダーから購入する」という2つの選択肢があります。これまで、アジア太平洋地域の企業のうち2/3は自社ソリューションを選択してきましたが、日本は他の国と異なり、62%がベンダーにアウトソーシングしています。ほとんどの企業で意思決定はIT部門が行っており、大半の回答者は、この部門がデジタル顧客体験に関するほとんどの権限を持っていると回答しています（地域全体で54%、オーストラリアでは72%）。

CIAMの実装方法構築VS購入

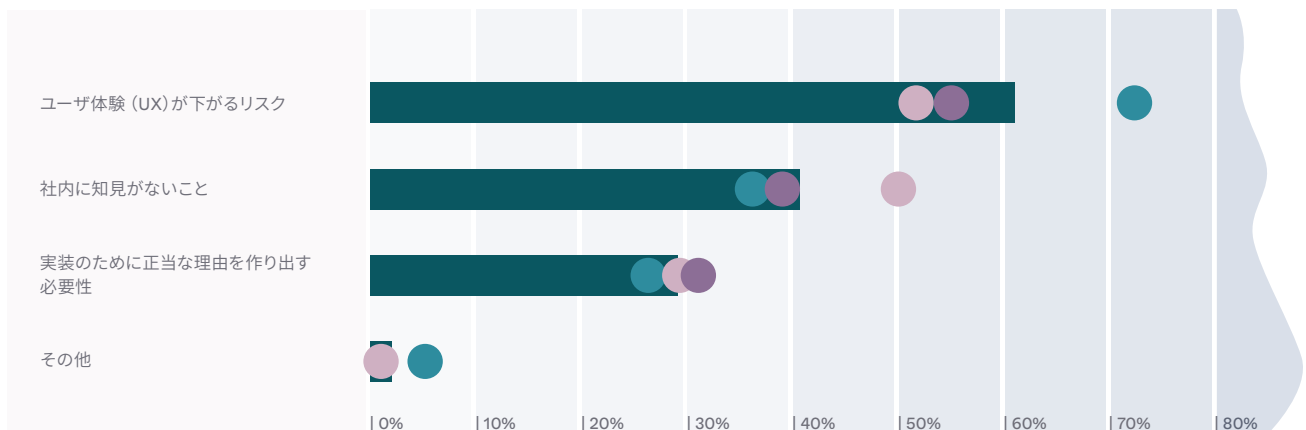


ユーザ体験 (UX)に関する懸念が実装の障壁に

CIAMの実装は複雑で、間違えると企業の大きな代償を伴うという重大な懸念があります。ほとんどの回答者が、最初にCIAMを構築する際、最も大きな障壁はユーザ体験が下がるリスク (61%) で、それに続いて社内に知見がないこと (42%)、実装のための正当な理由を作り出す必要性 (30%) を挙げています。

このうち、CIAMソリューションを持たない企業では、どこから始めたらよいかを理解していません。多く (56%) がアイデアしか持っておらず、1/3以上がどこから始めたらよいか知るための支援が必要だと述べており、オーストラリアおよび日本以外の国では50%に上っています。

CIAMの実装における最大の障壁は



- 合計
- オーストラリア
- 日本
- その他のアジア太平洋

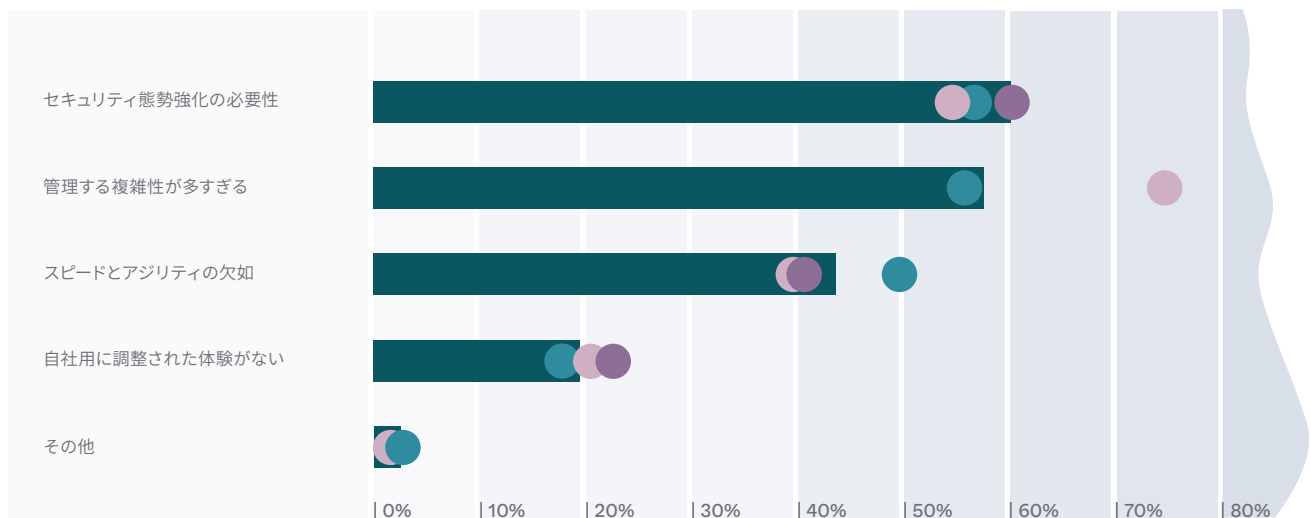
61%

CIAMの実装において、ユーザ体験に対するマイナスの影響を懸念する回答者の割合

CIAMの活用における課題

CIAMソリューションに関する課題と複雑性は実装の後も続き、自社でソリューション構築すると回答した企業は、巧妙化し続けるサイバー攻撃に耐えられる堅牢性を備えていなければなりません。CIAMソリューションを持つ組織のうち60%が、ソリューションを管理するうえでの最大の障壁はセキュリティ態勢強化の必要と述べており、57%が高度な複雑性が課題であると回答しています。

急速に変化する脅威の状況と、常に進歩を遂げている監査やコンプライアンス要件のため、スピードと俊敏性がCIAMにおいて必要不可欠になっています。このことが、企業にさらなる課題を突き付けており、企業の40%以上が既存のCIAMソリューションを使ううえでの主要な障壁になっていると述べています。



- 合計
- オーストラリア
- 日本
- その他のアジア太平洋

61% の社内ソリューション企業

49% のアウトソーシング企業

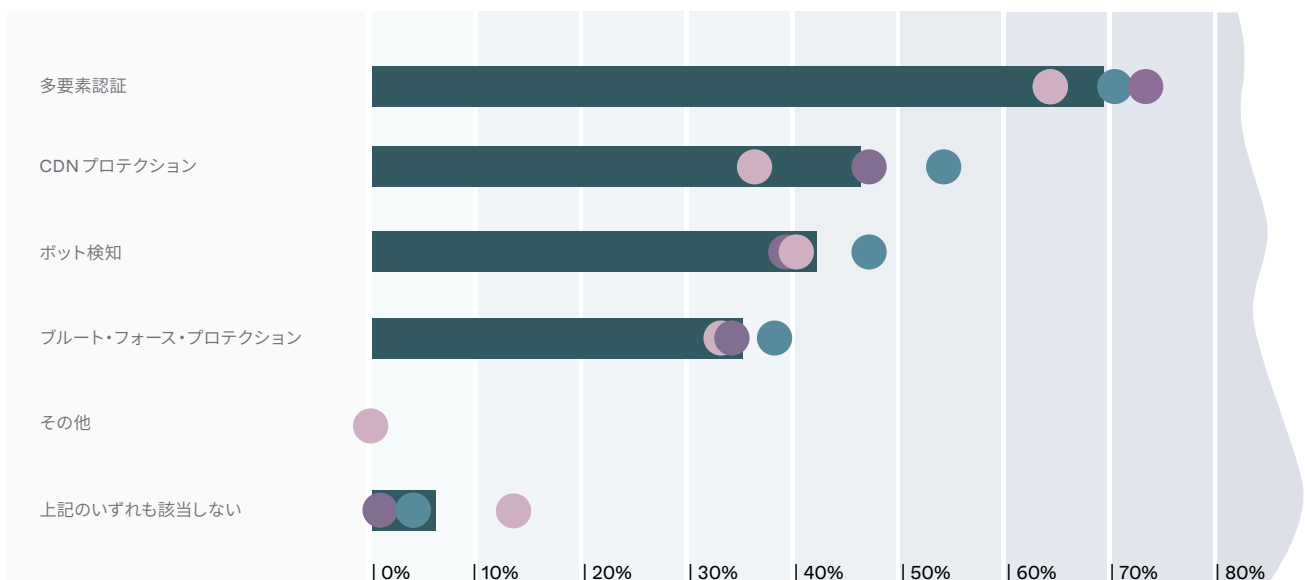
は、「複雑性が顧客アイデンティティ管理における最大の障壁である」と回答

多要素認証が最も利用されているセキュリティ対策

ほとんどの企業が、さまざまなセキュリティ対策を実施しています。その中で最も多く利用されているのは多要素認証です(69%)。コンテンツ・デリバリー・ネットワーク(CDN)プロテクションは2番目に多く利用されており(46%)、続いてボット検知(42%)、ブルート・フォース・プロテクション(35%)となっています。

これらのいずれの対策も行っていないと答えた回答者は10%に満たず、CIAMソリューションの原動力として、セキュリティの重要性が強調されています。

今までに導入したセキュリティ対策



- 合計
- オーストラリア
- 日本
- その他のアジア太平洋

33%

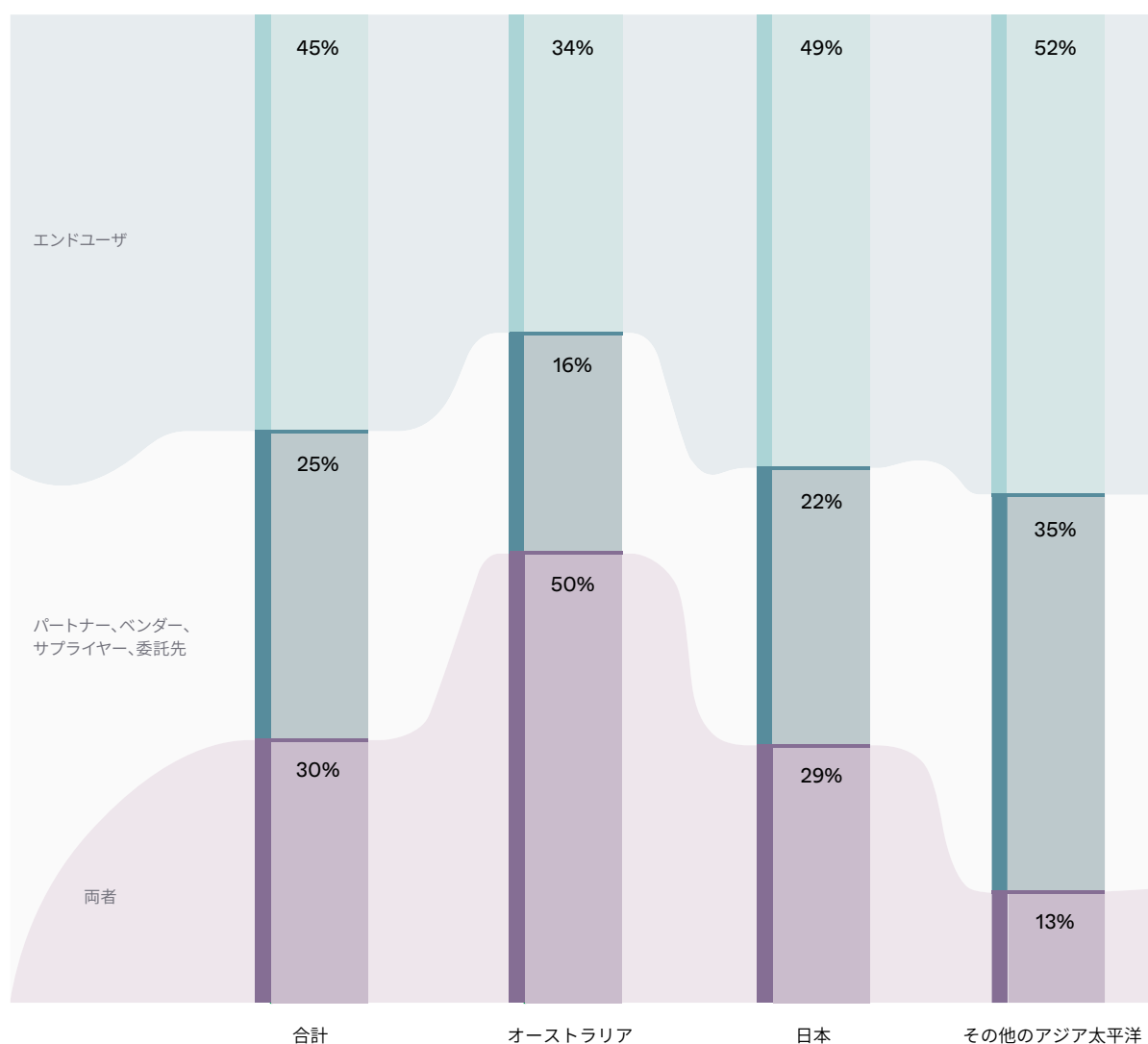
セキュリティがCIAMソリューションの最も重要な側面であると答えた回答者の割合

CIAMの関連性は消費者を超えて拡大

CIAMソリューションは消費者とのやりとりを超えて活用されています。パートナー、サプライヤー、委託先企業などに対して、企業のシステムへ迅速でセキュアなアクセスを提供することにも役立っています。

これは、企業の30%が自社のCIAMソリューションを消費者向けと外部の企業向けに使用していることを示す、当社の調査結果を反映しています。

CIAMの主な対象者



結論

今日のデジタルファーストと呼ばれる時代では、高いセキュリティ対策と、高度なユーザ体験の両立が、企業にとって急務となっています。これがアジア太平洋地域全体でCIAMの認知度と採用を後押ししていると言えます。しかしCIAMは、消費者とのやりとりのみならず、パートナーやサプライヤー、委託先との迅速なアクセスや協業をセキュアに実現することで大きな価値を生み出します。

ソリューションを持たない企業が導入に対して行く手を阻まれてしまうのは、ユーザ体験やセキュリティが実装の障壁となっていることへの懸念があります。また、自社製のソリューションを持つ企業は、多くの場合、維持が複雑で安全性が低いため、開発者やエンジニアがその運用に依存せざるを得ない状況になっています。

人材不足の状況が進む一方で、セキュリティ対策が最優先でイノベーションのスピードが成長と収益の分かれ道となり得る世界では、CIAMのアウトソーシングを行うことで、組織を複雑さから解放し、より良いソリューションの構築とカスタマーロイヤリティの確立に集中できることにつながります。

そして、ベンダーニュートラルなCIAMを選択することは、組織に対してより多くの選択肢を与え、既存のソリューションとのより迅速な統合を実現するため、成功に欠かせないものとなります。お客様がプロバイダーに関係なく自社の顧客に対して最も価値を提供できるテクノロジーを求めるようになるなか、テクノロジースタック全体で単一のベンダーと協働する時代はすでに過去となっています。

成功する組織とは、CIAMを自社のデジタルトランスフォーメーションの中心に据え、セキュリティ格差の排除、イノベーションの強化、開発時間の短縮を実現し、長期にわたる信頼を確立するシームレスな体験を届けられることができる組織と言えるでしょう。



直感的で一貫性のある、 信頼性の高い オムニチャネル体験を

Oktaは、CIAMを自社製のソリューションから切り離し、最も大切な業務に集中できるようにします。ここでは、より良いビジネスの成果を生み出す方法について解説します。



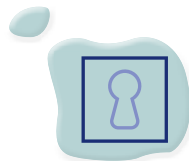
収益の増進

OktaのCIAMソリューションにより、デジタルおよび物理的チャネルにわたり、エンドユーザの嗜好に対する深い知見を得て、直感的かつ信頼性の高い体験を実現します。ユーザとの摩擦を抑え、一元管理されたアイデンティティデータを活用することで、パーソナリ化されたエンゲージメントを提供します。



開発者やエンジニアへの影響を最大化

開発者やエンジニアのリソースを解放して、ビジネスを前進させ、価値の高い業務に集中させることができます。そして、クラウドベースでかつアイデンティティをもとにした管理、オーケストレーションや自動化で日々のタスクをシンプルにします。



セキュリティとコンプライアンスのリスクを低減

ビルトインされた脅威プロテクション機能の活用により、Oktaがセキュリティやコンプライアンス、可用性に関するタスクを担います。組織の認証、コンプライアンスおよびデータレジデンシーの要件を満たすための支援をOktaが行います。

Oktaについて

Oktaは、業界をリードする独立系アイデンティティプロバイダーです。Okta Identity Cloudにより、企業では適切な人材が適切なタイミングで適切なテクノロジーに安全に接続できるようになります。Oktaでは、7,000以上のアプリケーションやインフラプロバイダーへの統合が事前構築されており、あらゆる場所にいる人々や組織に対して、シンプルで安全なアクセスを提供し、人々の能力を最大限に発揮できるようにしています。15,000以上の組織が、従業員と顧客のアイデンティティ保護でOktaに信頼を寄せています。