IBM Security

組織全体の CIAMをモダナイズするために ステークホルダーを結集

IBM

始めに

概要

アカウントの新規登録、購入、あるいはニュースレターの購読を申し込まれた場合、お客様はご自身の個人情報を組織に託すことになります。このような最初のやり取りの後、同意した目的以外で情報が使用されることは望まれませんが、お客様の同意があれば、パーソナライズされた顧客体験やリコメンデーションを喜んで受けとっていただける場合があります。重要なことは、これはお客様次第であり、いつでも考えを変えることができるということです。また、何らかの理由でその組織とのやりとりに摩擦が生じたり、信頼を失ったりすると、その組織に見切りをつけて別の組織を探すことになるでしょう。サービス利用者ID管理とアクセス管理（CIAM）は、こうしたお客様とブランド間のオンデマンドでパーソナライズされた信頼できる顧客体験を実現できます。また、自身が消費者であれば、競争力を維持するために組織のデジタル戦略の見直しを実施する際、自らのお客様に共感することができるでしょう。

しかし、CIAMはウェブサイトの更新やマーケティング・プロジェクトにとどまらず、お客様とのタッチポイントを評価し、モダナイズすることで、組織全体の機能分野に影響を与えるものなのです。利便性と安全性のバランスが崩れないようにするためには、組織はビジネスと技術の両方のステークホルダーを集め、CIAMをデジタル変革の成果に焦点を当てたサブセットとして認識し、ワークフォースIAMと技術コンポーネントを共有する必要があります。戦略的かつ目的をもって実施すれば、組織は消費者とのつながりを最大化しながら、ITおよびセキュリティー担当者のリスクを最小限に抑えることができます。

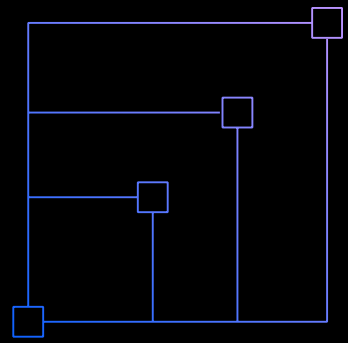
CIAM戦略がなければ、企業は顧客離脱により収益を失うリスクがあります。また、代替品がすぐ見つかる中でブランド・ロイヤリティーは脆弱なままになります。同様に公共部門においても、依然としてレガシーなインフラストラクチャーやプロセスに固執する政府機関は、市民の信頼を失い、理想的なレベルの公共サービスを提供できない可能性があります。民間企業と公共企業は、その使命に違いはあるものの、プライバシーを考慮した情報共有を促進し、摩擦がなく安全なデジタル体験を消費者に提供するという点で共通しています。そして、多くの組織がそのことに注目し、CIAMはIAM市場全体の中で最大のセグメントとなり、2025年まで年間15.1%[1]の成長が予測されています。まだデジタル・モダナイゼーションに着手していない企業にとって、最初で最も重要なステップの1つは、複数の機能的役割にまたがるリーダーシップの調整を行い、全員がプロジェクトから恩恵を受けられるようにすることです。

最高マーケティング責任者（CMO）

CIAMの目標：プライバシーを意識し、ユーザーがコントロールできるパーソナライズされたエクスペリエンスを通じて、ユーザーを獲得、育成、成長させる。

民間セクターでは、マーケティング担当者が潜在顧客の注目を集めるために奮闘しています。マーケティング担当者が最も避けたいことは、登録が難しいために直前になってお客様が離れてしまうことです。お客様の離脱は収益に直結するため、CIAMプログラムはこの問題を回避し、将来の見込み客をビジネス機会に変えるために、登録とオンボーディングのエクスペリエンスを効率化することを目的としています。理想的なオンボーディング・フォームは、お客様情報をできるだけ要求せず、お客様との関係が深まるにつれて、お客様について徐々に知ることができるようにタッチポイントが適切に設定されていることです。

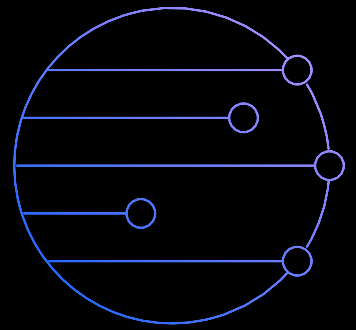
複数のサブ・ブランドを持つ大企業は、顧客関係管理（CRM）やその他のサード・パーティー・ツールやシステムと統合して、お客様のIDを一元化するようにデータストアを設計する必要があります。お客様IDを一元化することで、CIAMのベスト・プラクティスを戦略的に導入することで、マーケティング担当者はお客様の行動をより深く理解し、よりターゲットを絞ったパーソナライズされたマーケティング・キャンペーンを実施できるようになります。CIAMは、見込み客とお客様の両方のデジタル体験にて中心的な役割を果たしています。だからこそ、マーケティング・リーダーがモダナイゼーション計画のプロセスで重要な役割を果たすのは当然のことなのです。



業務の責任者

CIAMの目標：組織の目標を達成するために、最新のインターフェイスとエンゲージメントを備えた合理的で摩擦のないエクスペリエンスを提供する。

ビジネス・マネージャーや代理店オーナーも同様に、必ずしも収益のためではないものの、お客様とのスムーズな交流を実現したいと考えています。例えば、政府機関では、市民に対して公共サービスを効率的に提供し、膨大な数のユーザー嗜好やチャネルに対応したエンゲージメントをモダナイズする必要がありますが、通常、組織内に真のマーケティング機能がないのが一般的です。代理店オーナーは、登録を簡素化し顧客の離脱を減らし、サービスの提供を成功させるために、同様のユーザー・ジャーニーの変革することを求めています。マーケティングキャンペーンは行っていないかもしれませんが、これらのビジネスマネージャーは、各顧客に対して単一のIDを実現することで、部門を超えた顧客とのやり取りを効率化し、冗長性を排除し、行動の理解を深めることを目指しています。

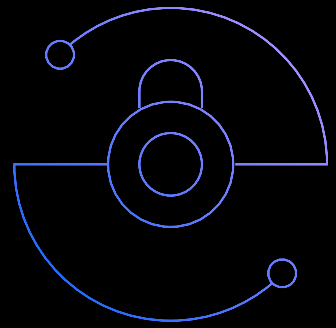


セキュリティーおよびプライバシー担当者

CIAM目標：安全なお客様とのやりとりを通して、ユーザーによる不正行為やアカウントの漏洩を防ぎ、透明性が高くユーザーにカスタマイズされた体験を提供し、コンプライアンスを維持することです。

原則として、お客様はご自分のデータを誰がどのように管理しているかを知るべきであり、いつでもご自分のデータを提供し、同意を変更する機会を持つべきです。このことは、企業がデジタル体験におけるプライバシーと同意の管理を優先させる十分な理由となりますが、グローバルな規制により、この問題は緊急性を帯ています。企業は、各地域のルールに従わなければならず、それに従わなければ多額の罰金や罰金を科せられる恐れがあります。また、プライバシーに関する法律では、組織が何をする必要があるかについて詳細に規定されていますが、そこに至る具体的な方法については通常説明されていません。適切なCIAMの実装は、個人を特定できるすべての情報 (PII) の唯一の情報源として機能します。プライバシー担当者とコンプライアンスの専門家は、さまざまな同意管理の目的に応じてルールやポリシーを定義し、技術スタッフは必要なアプリケーションに適用するだけでよいのです。これにより、プライバシーおよびコンプライアンス担当者は、スプレッドシートを超えて、プライバシー法のダイナミックな現実に対応し、より親しみやすいものにすることができます。

CISOは、プライバシーやコンプライアンス担当者とともにプライバシーや同意の管理について課題を共有することになりますが、CISOは時にCIAM全体をマーケティング・プロジェクトとして考え、他の優先事項と比較して関心を失いがちになることがあります。従来の従業員向けIAMとお客様向けIAMの成果はまったく異なりますが、どちらもデータを安全に保存し、データ漏洩のリスクを軽減する商用ソリューションからメリットを得られます。従業員とお客様両方のIDは保護する価値があります。さらに、IAMインフラストラクチャーの現状を戦略的に考慮せずにCIAMの取り組みを進めると、CISOは組織の環境に断片的なソリューションの断片を追加することになり、アクセス・ポイントが増やしてリスクを高めることになるかもしれません。不必要なデータのサイロ化を防ぐために、従業員とお客様のIAMユース・ケースを可能な限り単一のソリューションにまとめることは、CISOにとって最善の策となります。

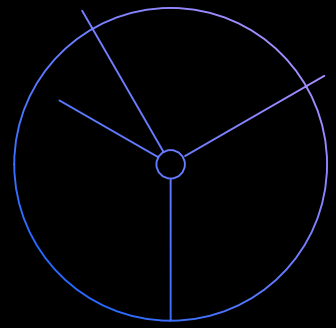


最高情報責任者(CIO)

CIAM目標：最新のセキュリティー体制を維持するために最新のアイデンティティー標準に準拠しながら、IAMソリューションの導入と運用の複雑さを軽減する

CIAMがもたらすお客様とつながるメリットはさておき、CIOは組織の総合的なインフラストラクチャーと運用計画に適合するように、新しいテクノロジーに関する意思決定を評価する必要があります。シンプルさと標準化は理想的であり、IAMとCIAMの機能を1つのツールに統合することは、セキュリティーと同様にITリーダーシップに共鳴するはずです。このアプローチでは、IT環境全体が複雑になったり、既存のスタッフに新たなスキルを要求することはありません。同じソリューションを外部のユーザーにも再利用することで、全体的なIT運用コストを最小限に抑えることができ、コスト面でのメリットが得られる可能性があります。

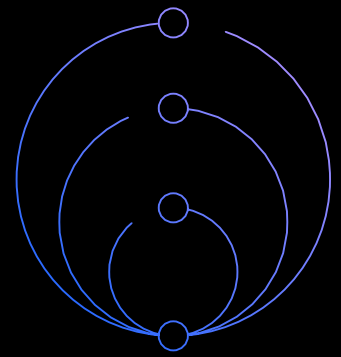
CIAMソリューションが稼働すると、ダウンタイムが発生するたびに、お客様がアカウントにアクセスできない組織では、時間と収益の損失が発生します。これだけでも、多くのITリーダーが投資対効果の観点からCIAMのユース・ケースにクラウド・ベースのソリューションを好む理由が説明できます。オンプレミスの代替品よりもはるかに高い可用性と拡張性を提供する傾向があるからです。それでも、クラウドIAMは、インフラストラクチャーの運用負荷の削減、ソフトウェアの自動更新、および価値を生み出すまでの時間短縮など、ITスタッフにとってさらなるメリットをもたらします。



IAM管理者および開発者

CIAM目標：ローコードと構成ベースのワークフローにより、開発作業を簡素化し、アプリケーション・ポリシーを保護および維持する

エグゼクティブ・ステークホルダーがより高いレベルのビジネス目標、運用コスト、リスク軽減について調整する一方で、IAM管理者と開発者は、ソリューションの技術的能力を全面的に評価することによって、CIAMプログラムの開発に影響を与えることができます。データソースやアプリケーションの移行や統合のためのロジスティクスに加えて、サポートされている認証プロトコル、MFA方式、および配信チャネルなどの主要な項目を確認することができます。価値を生み出すまでの時間を短縮するために、このチームは、ソリューションのAPIドキュメント、ガイド付きリソース、ローコード体験を評価し、ソリューションの実装とメンテナンスを通じてチームが十分にサポートされることを確認します。CIAMツールの同意管理のようなワークフロー・ベースの機能は、例えば、個人情報保護法から、変化する要件を自動的に説明する単純なAPI呼び出しまで、詳細を抽象化することによって、開発者の頭痛の種を軽減することができるかもしれません。さらに別のツールを追加する前に、技術担当員は既存のIAMソリューションとの互換性と統合性を総合的に評価し、長期的に最適な状態にする必要があります。



IBMの統合CIAMアプローチ

IBMの統合CIAMアプローチによるデジタル体験のモダナイゼーション

IBM Securityは、ID戦略、デジタル設計の専門知識、クラウドネイティブなCIAMテクノロジーを組み合わせて使用し、オンデマンドでパーソナライズされた安全なオムニチャネル契約を通じて、お客様を見つけつながることを可能にします。IBM Security Verify と IBM Security Services を組み合わせて使用することで、組織の連携を構築し、お客様情報を丁重かつ正確に追跡し、シンプルで安全なブランドのデジタル・エクスペリエンスを提供してお客様を喜ばせることができます。

次のステップ

CIAMでさらに深く
CIAMのベストプラクティス、プランニングの考慮点、回避すべき落とし穴についての詳細を読む

ガイドをダウンロードする →

IBM Security Verifyの概要
IDaaSを使用して、ソーシャルログインや適応型認証によりユーザー体験をモダナイズするとともに、同意管理によりプライバシーを保護する。

検証について学ぶ →

IBM Security CIAMサービス
独自のコンサルティングと協力的なアプローチを用いて、ビジネス目標に沿ったCIAMプログラムを計画、設計、展開、実行

CIAMのヘルプを表示 →

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

Produced in the United States of America
2021年2月

[1] 市場と市場、2025年までの消費者IAM市場の世界予測