

CIAM と IAM :

従来の IAM を

顧客に対して使用すべきでない理由



CIAM と IAM の違いについて

デジタルアイデンティティは、すべての企業のデジタル変革の要と言えます。顧客のアイデンティティに関連付けられている顧客プロフィールデータの価値は急激に高まり、今では多くの企業にとって成功に不可欠な要因となっています。顧客プロフィールは、顧客の行動やカスタマージャーニー（最初の連絡から購入決定までの長期間のブランドロイヤルティ）の分析、理解、予測の基盤を成すものです。

カスタマー・アイデンティティ・アクセス管理（CIAM）に必要なテクノロジーは従来のアイデンティティアクセス管理（IAM）と同じであるという誤解をよく耳にします。従来の IAM ソリューション（エンタープライズまたは従業員 IAM と呼ばれることもあります）は、従業員または企業の既知のビジネスパートナーのみをリソースにアクセスできるようにする IT システムです。

一般的に従来の IAM は十分に確立されているため、「社内にはすでにこのテクノロジーがあるのだから、これを顧客に拡張することは難しくはないはず」という誤った臆測をする企業もあります。このような考え方をしてしまうのは、従業員向けの IAM と顧客向けの IAM の違いや、公開している企業のデジタルプロパティに対するカスタマーアイデンティティ管理の複雑さを極端に過小評価しているからです。CIAM の要件は、従業員 IAM とはまったく異なり、はるかに厳しいものです。そのため、従業員向けの IAM ソリューションを再利用すると問題が生じる可能性があります。

従来の IAM は、ユーザーが誰なのか、ユーザーがとるアクション、ユーザーのデジタル行動を左右するものに関する知見を提供できません。

従来の IAM を CIAM として使用しても解決にはならない

従来の IAM は、従業員が社内システムに便利にアクセスできるように設計されているため、ユーザーが誰であるかについての知見は提供できません。実際、アイデンティティは想定されていて、高度なデータ（ユーザーがとるアクションや、デジタルの世界でユーザーのジャーニーや行動を左右するものなど）の追跡はできません。しかし、企業は顧客を理解し、デジタル市場での競争力を得るために、この種のデータ知見を必要としています。

さらに、最大規模の企業でも、従来の IAM システムで管理している従業員のアイデンティティは最大数万件程度と考えられます。しかし、大量の商品を扱うブランドでは、数千万または数億規模の顧客アカウントを同時に処理する必要があります。現在の消費者はゼロフリクションを期待するので、アイデンティティソリューションのスケールアウトとスケールアップの両方で処理負荷に対応し、知覚できるレイテンシーをほとんど、あるいはまったくなくすることも必要です。

最新の Akamai の調査から、ウェブページの読み込み時間が 2 秒遅れると直帰率が 103% 上昇し、モバイルサイトの訪問者の 53% は読み込みにかかる時間が 3 秒を超えるとそのページから離脱することがわかっています。¹ そのため、アイデンティティ管理システムに障害が発生したり、読み込みを処理できずに速度が低下したりすると、コンバージョン率と収益に影響が生じる可能性があります。皮肉にも、読み込みの急上昇や顧客トラフィックの増大は、通常、キャンペーンの成功が原因で生じます。つまり、アイデンティティ管理システムの反応が遅いと、慎重に検討し悪戦苦闘した成果の足を引っ張ることになります。

アイデンティティ管理システムの反応が遅いと、慎重に検討し悪戦苦闘した成果の足を引っ張ることになります。

Akamai Identity Cloud のような専用の CIAM プラットフォームは、企業が顧客プロファイルデータから最大限の価値を引き出すことができるように設計されています。このようなソリューションは、ログイン、認証、設定管理などのタスクがアクティビティを妨げることがないように、シームレスでフリクションのない顧客体験を実現します。さらに、CIAM テクノロジーは、公衆ネットワーク全体で個人データのセキュリティを確保するという重要なニーズにも対応します。世界でビジネスを展開する企業は、CIAM を使用することで、頻繁に変化するさまざまなプライバシー要件を遵守することができます。

以下の表は、従来の IAM と CIAM との差異と用途をまとめたものです。

従来の IAM 	顧客向けの IAM 
社内の 従業員のアイデンティティ を管理します。	顧客が接続するデジタル・マルチチャネル・サイト (Web、モバイル、IoT) の 顧客のアイデンティティ を管理します。
ユーザーの 登録は会社が行い 、主要なプロフィールデータは HR または IT 部門が入力します。	ユーザー 自身で登録し 、ユーザー固有のデータもユーザー自身が作成します。
社内 ディレクトリサービス に対する認証	OpenID やソーシャルメディアのような パブリックサービス に加え、ディレクトリサービスおよび外部 Credential 検証サービスに対する認証
従業員、契約者、パートナーなど、既知のユーザーに限定されています。 アイデンティティは想定可能です 。	ユーザーは登録されるまで 未知 であり、複数のアカウントや偽りのアカウントを作成することもあります。 アイデンティティを想定することはできません 。
従業員であるユーザーは、 代替手段がないため 、レイテンシーや低パフォーマンスに 比較的寛容 です。	顧客や見込み客は、 魅力的な代替手段がたくさんあるため 低パフォーマンスに対して あまり寛容ではありません 。
各ユーザーに単一のアイデンティティで 数十から数十万ものユーザー まで拡張可能。	コンシューマーアイデンティティ数は数十億まで、 ユーザー数は数億まで 拡張可能。
従来のアイデンティティプロバイダー (IdP) は通常、 単一の集中管理型社内 IT システム です。	多数のアイデンティティプロバイダーに分散 (Facebook、Google、LinkedIn などによるソーシャルログインと従来のログイン)。
多くの異種 IT システムが閉じた 社内ネットワーク 上に存在。	多くの異種 IT システムが 公衆ネットワーク (インターネット) 上に存在。
従業員のプロフィールデータは 管理と運用を目的として 収集されます。	顧客のプロフィールデータは 非常に重要な事業目的 (取引、マーケティング、パーソナリ化、分析、ビジネスインテリジェンス) のために収集されます。
HR および ERP のシステムと統合されます。	さまざまな マーケティングおよび販売自動化テクノロジー、分析システム、セキュリティおよびコンプライアンスソリューション と統合されます。
個人データおよびユーザーの プライバシー/設定/同意 の管理は、 厳格に制御された同種の社内環境内でのみ発生 します。	個人データの処理は、 多様なプライバシーおよびデータ保護規制 に従う必要があり、またユーザーが設定や同意の表示、変更、取り消しを実行できるようにすることも必要です。



出典

1) <https://www.akamai.com/jp/ja/about/news/press/2017-press/akamai-releases-spring-2017-state-of-online-retail-performance-report.jsp>



世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有する Akamai は、デバイスや場所に関係なく、最高、かつ最もセキュアなデジタル体験をお客様に提供します。Akamai のプラットフォームは、比類のないスケールで展開されており、お客様に優れたパフォーマンスとセキュリティを提供しています。ウェブ/モバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、優れたカスタマーサービスと 365 日/24 時間体制のモニタリングによって支えられています。グローバルトップの金融機関、eコマース事業者、メディア・エンターテインメント企業、政府機関等が、Akamai を信頼する理由について、www.akamai.com/jp/ja/ または blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。公開日：2019 年 4 月。