

カスタマーアイデンティティハンドブック： プロダクト部門とエンジニアリング部門の リーダー向けガイド



目次

セクション1

- 5 基本の理解：セキュアでシームレスなユーザーエクスペリエンスを支える構成要素

セクション2

- 9 最新の基本要件：シングルサインオン（SSO）と多要素認証（MFA）

セクション3

- 11 アイデンティティの保存と管理：アイデンティティプロバイダー（IdP）

セクション4

- 15 ユーザー中心で拡張性のある製品の制作：プロダクトリーダーにとって重要な考慮事項

セクション5

- 18 AI機能のセキュリティ強化

セクション6

- 19 安全で拡張性のあるシステムの構築：エンジニアリングリーダーにとって重要な要素

セクション7

- 21 拡張性により統合を簡素化

セクション8

- 23 不正登録の防止

おわりに

はじめに：最新のカスタマーアイデンティティの戦略的重要性

カスタマーアイデンティティは、カスタマーアイデンティティおよびアクセス管理（CIAM）とも呼ばれており、組織の多様な技術スタック全体を一体化して、各顧客のアイデンティティについて信頼できる単一のレコードを確立します。これにより、プライバシーが保護された便利で安全なカスタマーエクスペリエンスを実現できるだけでなく、コンプライアンスにも役立ち、顧客中心のアナリティクスの基盤としての役割も果たします。

コンシューマー向けアプリケーションでも、マルチテナント型B2B SaaSプラットフォームでも、カスタマーアイデンティティは製品の成功に欠かせない役割を担います。

- コンシューマー向けアプリケーションでは、スムーズなサインアップ、パーソナライズ、信頼を支える基盤となる。
- SaaS環境では、セキュアなコラボレーション、きめ細かなアクセスコントロール、APIセキュリティ、エンタープライズレベルのスケラビリティを支える。
- いずれの場合でも、パーソナルアシスタントから、ユーザーの代わりに行動する自律型AIエージェントまで、さまざまなAI搭載機能が製品に組み込まれる中で、アイデンティティはますます重要になっている。

しかし、ITや開発の専門家がCIAMに取り組む際には、認証情報の管理、ログインボックス、APIといった要素ばかりに重点を置きがちです。これらは重要であるものの、アイデンティティ全体の一部にすぎません。

このように限られた見方をしているために、多くの開発チームは、実際の使用に耐えうるカスタマーアイデンティティの実装に必要な時間、労力、専門知識をあまりにも過小評価しています。

開発者がカスタマーアイデンティティを学び、自社アプリケーションや関連業務システムに統合できるよう支援するため、Auth0は創業以来、詳細なハンドブック、オンラインプレイグラウンド、豊富なコードサンプル、SDKなど、開発者向けリソースの作成に力を入れてきました。

```
(!result || !result.allowed) {  
  return res.status(403)  
    .send({ code: 'missing_permission:  
: Not allowed to access object ${1
```

同じ考えから、このガイドは次の2つの目的を掲げています。

- 1 プロダクト部門や開発部門のメンバーが、カスタマーアイデンティティに関して共通の理解を持てるようにすること
- 2 開発コミュニティの中で長く利用されてきたカスタマーアイデンティティ関連の主要なリソース、つまり当社ライブラリ内の代表的なコンテンツを、チームメンバーが活用できるようガイドすること

まずは、カスタマーアイデンティティの基本について、その中核機能とそれを可能にする基盤プロトコルなどを大まかに説明します。

次に、アイデンティティがユーザー中心でスケーラブルな製品の構築にどのように役立つかを見ていきます。

さらに、セキュリティや拡張性など、エンジニアリング上の考慮事項を取り上げます。

全体を通じて、関心を持った読者（主に開発者やエンジニア）がさらに詳細を理解できるよう、関連リソースを随所で紹介しています。

さあ、始めましょう！

カスタマーアイデンティティの意義

本ガイドでは、なぜカスタマーアイデンティティソリューションが必要なのか、読者の方がすでに理解していることを前提としています。

ただし、その疑問が未解決なら、堅牢なカスタマーアイデンティティ機能を活用することで、以下のことが同時に実現できるから、というのがその答えです。

- 収益の増加
- コスト削減、効率化、市場投入までの時間（TTM）の短縮
- セキュリティとガバナンスの強化

詳しくは、『[カスタマーアイデンティティが重要な理由](#)』をご覧ください。



基本の理解：セキュアでシームレスなユーザーエクスペリエンスを支える構成要素

情報に基づいてカスタマーアイデンティティを検討するためには、基本的な要素や概念の理解が不可欠です。本セクションでは、よりセキュアで拡張性に優れ、ユーザーフレンドリーなデジタル製品を構築するために必要な基本概念と技術的な基礎を解説します。

- デジタルアイデンティティとユーザーコンテキストにおけるその役割
- カスタマーアイデンティティの3つの中核機能
- 主な機能のうち一般的な要件となったもの
- アイデンティティプロバイダーの種類
- 現代のカスタマーアイデンティティを可能にする標準とプロトコル

基盤：デジタルアイデンティティ

デジタルアイデンティティとは、個別のユーザーを定義する属性の集合であり、特定のアプリケーションやWebサービスなどが提供する機能のコンテキスト内で利用されます。

多くの場合、デジタルアイデンティティはユーザー名やその他の識別子（Eメールアドレス、政府発行のID番号など）と、それに関連する情報（配送先住所、支払い情報、アカウント設定など）の組み合わせで構成されます。



カスタマーアイデンティティの中核機能：認証、認可、ID管理

アイデンティティの観点から見て、効果的なCIAMの実装に最低限必要な機能は次のとおりです。

- 認証
- 認可とアクセスコントロール
- ID管理（ユーザー登録やアカウント作成など）

これらの機能の組み合わせで、組織（貴社または顧客の組織）はサインアップやログインといったユーザージャーニーを管理し、基本的なアイデンティティ保護を加え、コンプライアンスのニーズに対応できます。

認証

認証は、ユーザーアイデンティティの検証を処理します。基本的に認証のステップは、パスワードや生体認証など1つ以上の要素を用いて、アカウントにログインしようとしているユーザーが本人であることを妥当な信頼度で証明しようとするものです。

優れた認証システムは、攻撃者には多くの摩擦を与えつつ、正規ユーザーには「ちょうど良い」レベルの摩擦を設けます（適切な場所、適切なタイミングで若干の摩擦があることは、信頼の構築に役立ちます）。

ただし、現実の利用環境では「利便性」と「摩擦」の間でトレードオフが発生することが少なくありません。そのためアプリケーションプロバイダーは、次のようにさまざまな認証方法を提供する必要があります。

- ユーザー名とパスワードの組み合わせ（よく使われているがリスクがある）
- パスワードレスのオプション（ソーシャルログイン、マジックリンクをメールで送信、生体認証、SMSなど）
- パスキー

上記の方法やその他の認証方法を、多要素認証（MFA）と組み合わせて使用することで、さらに強固なセキュリティを実現することもできます（MFAについては後ほど詳しく説明します）。



認可とアクセスコントロール

認可とは、アプリケーション内の権限、リソース、機能などに対して、ユーザーが適切なアクセス権を持つようにすることです。

ユーザーが認証されると、実行できる操作に関して一定の許可が付与されます。たとえば、給与計算アプリケーションでは、経理担当者は全従業員の給与を処理し、詳細を確認できますが、それぞれの従業員は自分の詳細情報だけを確認、更新できるように制限されています。

認可とアクセスコントロールは密接に連携していますが、微妙に異なります。認可はポリシーを定義し、アクセスコントロールはそのポリシーを実際に適用する役割を担います。認可ポリシーとアクセスコントロールの両方が進化するにつれて両者を区別する境界線は曖昧になってきていることは事実ですが、いずれの用語についても、その区別は理解しておくべき重要なポイントです。

また、次の点も押さえておく必要があります。

- **認可の対象は人間のユーザーだけではありません。**システムは非人間アイデンティティ（NHI）の認可も行う必要があります。NHIには、サービス、API、デバイス、そして近年ではユーザーやシステムの代わりに動作するAIエージェントなどがあります。
- **ユーザー認証を直接行わなくてもアクセスコントロールを適用できます。**たとえば、デバイスポスチャ、ネットワークの場所、証明書の信頼性、その他のコンテキスト信号に基づいてアクセスを許可または拒否できます。
- **認可とアクセスコントロールのどちらもAIアプリケーションにとって極めて重要です。**設定漏れや不備があれば、AIエージェントが誤ったデータにアクセスし、本来の目的を超えて機密性の高い操作を実行してしまう可能性があります。制御方法が攻撃者に見つかった場合、悪用される可能性は極めて大きいでしょう。不正利用を別にしても、コントロールが不十分な場合は、規制やコンプライアンスに抵触する恐れもあります。

以下の表は、主なアクセスコントロールの手法4つを、登場順にまとめたものです。

ロールベースのアクセス コントロール (RBAC)

RBACでは、システムや組織内でのユーザーの役割（ロール）に基づいて権限が割り当てられます。

属性ベースのアクセス コントロール (ABAC)

ABACでは、ユーザーやリソースが持つ属性（部署、勤務地、職位、職務内容など）に基づいて権限が付与されます。

ポリシーベースの アクセスコントロール (PBAC)

PBACは、アプリケーションのコードから独立した形で、認可ポリシーを一元的に管理する仕組みです。PBACはABACの拡張であり、属性やロールに加えて追加の要素（ポリシー）を作成できます。

関係性ベースの アクセスコントロール (ReBAC)

ReBACでは、ユーザーと特定のオブジェクトとの関係や、そのオブジェクトが他のオブジェクトと持つ関係に基づいてアクセスルールを条件付きで設定できます。ReBACを利用することで非常にきめ細かい認可ポリシーの実装が可能になり、いわゆるFine Grained Authorization (FGA) を実現できます。これは、密接に連携動作する今日のSaaSアプリケーションに求められている機能です。

ID 管理

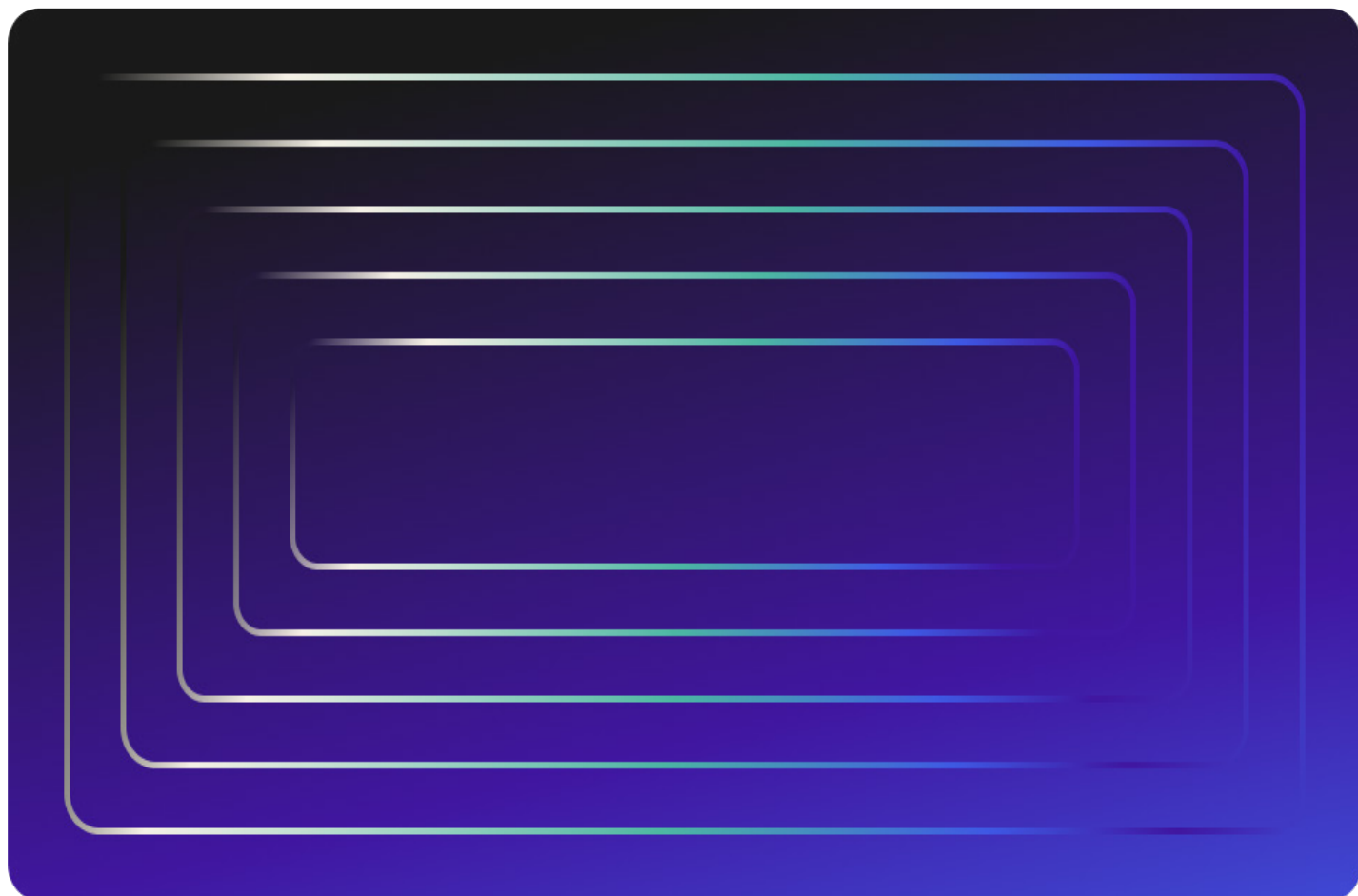
ID管理とは、アプリケーション内でユーザーのライフサイクルを通じて、重要な詳細情報を追跡・維持することを目的としています。以下のような機能があります。

- ユーザーの作成、更新、削除
- ユーザー属性の管理
- ユーザーの状況の変化に応じた、機能、コンテンツ、サービスへのアクセス制御

コンシューマー向けアプリケーションでは、ID管理によってスムーズなオンボーディング、プログレッシブプロファイリング、リアルタイムのパーソナライゼーションが可能になります。多くの場合、これらは複数のデバイスやチャネルをまたいで提供されます。たとえば、ユーザーが匿名でアプリケーションを使い始め、後からアカウントを作成して機能の利用制限を解除し、最終的にプレミアム版へアップグレードする、といった流れが可能になります。

B2B SaaS環境では、ID管理はさらに複雑になります。マルチテナントアクセス、組織内のユーザーロール、管理の委任に加えて、アカウントタイプや利用階層、他システムとの統合状況に応じた動的な権限付与などをサポートする必要があります。ユーザーが同一のセッションやワークスペース内で、チーム間の切り替えや複数アイデンティティの管理を行ったり、他者に代わって操作を実行したりする場合もあります。

いずれの場合でも、現代のアイデンティティレイヤーは単にユーザー情報を保存するだけでは不十分です。リアルタイムでのアイデンティティ関連ロジックのオーケストレーション、拡張可能なプロファイルモデルのサポート、そしてAPI・デバイス・AIワークフロー全体にわたるユーザー属性のスケラブルかつセキュアな処理が求められます。



最新の基本要件:シングルサインオン(SSO)と多要素認証(MFA)

B2B SaaSプラットフォームであれ、通信量の多いコンシューマー向けアプリケーションであれ、シームレスでよりセキュアな認証は、今や差別化要素ではなく当たり前求められる前提条件となっています。

つまり、シングルサインオン(SSO)や多要素認証(MFA)は、もはやオプションではなく必須機能であり、ユーザーの信頼を獲得し、機密データを保護しながら、デバイスやサービスを越えて一貫した体験を提供するための基盤となっています。

シングルサインオン(SSO)

シングルサインオンを使用すると、ユーザーは複数のアプリケーションで同じ認証情報を利用できるようになるため、各アプリケーション内で個別に認証を行う必要がなくなります。

それが何のためのものか認識していなかったとしても、おそらくあなたも以前にSSOを見たことがあるでしょう。Googleを例にとってみましょう。

- Gmailなど、Googleのサービスにログインすると、YouTubeやAdSense、Googleアナリティクス、その他のGoogleアプリに自動的に認証されます。
- 同様に、Gmailやその他のGoogleアプリからログアウトすると、すべてのアプリから自動的にログアウトされます。

SSOは、管理を簡素化し、セキュリティを強化し、利便性と生産性の高い作業環境を実現します。そのため、従業員が日常的に多数のアプリケーションやサービスを利用するIT環境で、広く普及しつつあります。

コンシューマー向けのSSOは「ソーシャルログイン」として知られています。これは、あるサービスへの新規登録やログインに、Google、Facebook、GitHubなど別のサービスの認証情報を使える仕組みです。ユーザーにとっての最大のメリットは利便性です。ソーシャルログインを認証オプションとして提供するアプリケーション側にとっては、登録プロセスの負担軽減、リスク低減、そしてサインインパートナーが共有するユーザーデータへのアクセスといった利点があります。

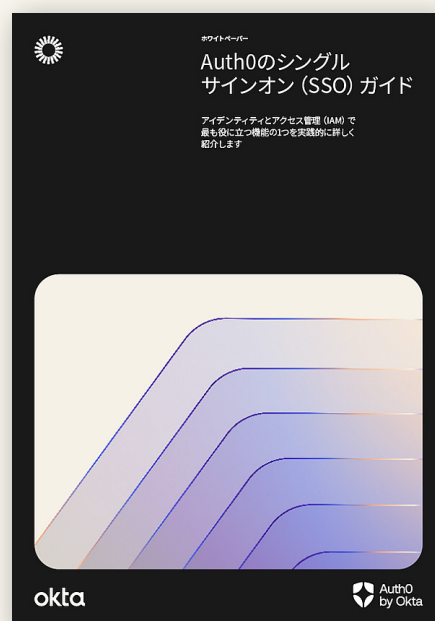
さらにソーシャルログインによるSSOは、利便性だけでなくセキュリティ面でも優れています。ソーシャルログインを利用することで、パスワードの使い回しや認証情報の盗難リスクをかなり抑えられます。

SSOのすべてを理解するためのガイド

シングルサインオン(SSO)は一見シンプルに聞こえますが、SAML設定やOIDCフローに踏み込むと複雑さが増します。開発者向けに作成された『Auth0のシングルサインオン(SSO)ガイド』では、SSOが実際にどのように機能するのか、どこから始めればよいのか、そして適切なアーキテクチャ上の判断をどう行うかを解説しています。

ダウンロードして、以下の詳細をご覧ください：

- SSOの実際の仕組み（最近の流行語は使いません）
- 自社構築か、購入か、組み合わせか——決断を後悔しない方法
- 重要なプロトコル：SAML、OIDC、WS-Fed、LDAP
- 始め方とAuth0との統合方法



多要素認証 (MFA)

ユーザーのアイデンティティを認証するために使用できる要素は、大きく3種類に分けられます。

- **知識情報**: パスワードやセキュリティ質問の答えなど
- **所持情報**: 認証済みデバイスを所持している証明など
- **生体情報**: 指紋や顔認証といった生体識別子

多要素認証では、単に複数の要素を組み合わせるだけでなく、異なる種類の要素を2つ以上用いることによって認証の強度を高めます。

代表的な第2要素（ユーザー名+パスワードに追加して利用されるもの）には以下があります。

- SMSコード
- 認証アプリのコード
- 通知をプッシュ
- キーベース認証

多要素認証 (MFA) の重要性は日ごとに高まっています。これは組織にとっても、セキュリティ意識の高い消費者にとっても同様です。攻撃者がフィッシングや情報窃取マルウェアを通じて共有シークレットを取得する手法を巧妙化させているためです。

特に、従来の脆弱な手法（特にSMSコード）を回避する方法が編み出されたことから、強固なMFAの必要性は日ごとに増しています。

MFAは「両刃の剣」でもあります。認証プロセスに摩擦を増やすことで攻撃者に対する防御を強化できますが、当然ながら、正規ユーザーにとっても不便さが増します。特にコンシューマー向けアプリケーションでは、このトレードオフが課題となり、リスクシグナルを使ってMFAチャレンジの可否を判断するアダプティブMFAの発展につながりました。

さらに、パスキーが登場したことで、このトレードオフはほぼ解消されました。パスキーは所持情報を知識情報または生体情報と組み合わせで一体化した利便性の高い方式で、フィッシング耐性のある認証を提供します。厳密な定義上パスキーがMFAに該当するか否かについては、アイデンティティの専門家や技術通の間で活発な議論が続いているものの、ほぼ同等の形式で、パスワードと比べると圧倒的に優れたセキュリティを提供する点は広く認められています。



アイデンティティの保存と管理:アイデンティティプロバイダー(IdP)

アイデンティティプロバイダー (IdP) は、ユーザーのアイデンティティを実際に保存し、管理する役割を担います。このセクションでは、SSOやID管理などを目的としてアプリケーションがやり取りする必要がある、さまざまな種類のIdPについて簡単に説明します。

ローカルデータベース

ID管理の一般的な方法として、ユーザーとそのロールを格納するローカルデータベースを利用するやり方があります。データを完全に自社で管理したい組織は通常、この方法を選択します。

従来、ユーザーはユーザー名とパスワードによる認証でデータベースにログインするのが一般的でしたが、組織は徐々に強力な認証やその他のセキュリティ強化対策を導入しつつあります。

Microsoft : Active Directory、ADFS、Entra

Microsoftはアイデンティティの連携に精通しており、ユーザーアイデンティティを管理するためのさまざまな製品とソリューションを提供してきた長い歴史があります。

Active Directoryは、Microsoftのエンタープライズ分野で広く使われているアイデンティティプロバイダーです。Active DirectoryはWindows Serverテクノロジーと連携して、WebアプリケーションだけでなくWindowsエコシステム全体にシングルサインオン機能を提供しました。

近年、MicrosoftはMicrosoft Entra (旧称Microsoft Azure Active Directory、またはAzure AD) などのさまざまなオンラインサービスの提供を開始し、アイデンティティプロバイダーとしての機能をクラウドへと拡張しています。

ソーシャルプロバイダー

ソーシャルプロバイダーは優れたIdPとして利用されることが多く、FacebookやGoogleなどの企業は通常、OpenID Connect (OIDC) 認証プロトコルを用いてユーザーアイデンティティを管理しています。

大手ソーシャルプロバイダーをIdPとして利用する大きな利点のひとつは、世界でも有数のアカウント乗っ取り (ATO) 防御策を備えている点です。ただし、小規模なソーシャルプロバイダーでは、このような厳格な対策が講じられていない場合があります。

さらに、ソーシャルプロバイダーをIdPとして利用することにはリスクも伴います。基本的にソーシャルプロバイダーがすべての制御権を握ることになるため、アクセスの取り消しやAPIの変更、さらにはアイデンティティサービス自体の提供中止が予告なく行われる可能性があります。

クラウドアイデンティティプロバイダー

Auth0のようなクラウドIdPは、ユーザーアイデンティティを管理し、クラウドベースのリソースやアプリケーションにアクセスします。これらのサービスは、ユーザーがサポートするプロトコル (OAuth 2.0、OIDC、SAML、WS-Fedなど) をサポートする、ほぼすべてのアプリケーションとの連携機能を提供する中間的なサービスと考えると良いでしょう。

この考え方は、アプリケーションをクラウドIdPと連携するだけで、IdPが「スーパー」認証サーバーとして動作する、というものです。その時点から、クラウドIdPは認証機能を担うことができます。

最新のクラウドIdPでは、組織がカスタムロジックを直接、認証フローに組み込める場合が多く、開発チームは認証が幅広い業務プロセスに適合するよう柔軟に調整できます。たとえば、エンタープライズアクセスポリシーの適用、コンプライアンス関連イベントのログ記録、またはパーソナライゼーションやアナリティクス向けのユーザーコンテキストの取得などを、すべてログイン時に設定できます。



実現に必要な要素：仕様、標準、プロトコル

最新のアイデンティティ機能は、異なるシステムやサービス間の相互運用性も含めて、広範かつ常に進化する仕様、標準、プロトコルに左右されます。

しかし、これらの要素が存在するだけでは、相互運用性（さらに言えばセキュリティ）を確保するには十分ではないと理解することが重要です。これには、主に2つの理由が考えられます。

- **たいていの場合、これらの仕様や標準、プロトコルで実現される機能は多岐にわたります。**これらの機能はアイデンティティ管理の最小要件を超えて拡張されることが多いため、特定のアイデンティティのコンテキストでは重要ではない機能が含まれる場合もあります（エンタープライズ環境とコンシューマーアプリケーションの違いなど）。
- **仕様の多くはフレームワークであり、オプション項目を含むため、2つの別々な実装があった場合に、別途調整をせずに相互運用できる保証はありません。**

つまり、開発者にとっては、単にドキュメントを読んで理解し、ドキュメントを解釈した内容に沿って実装をしたとしても、アプリが適切に動作するとは限らないということになります。

以下に、最も一般的な仕様、標準、プロトコルの概要をまとめました。いずれもアイデンティティにとって不可欠なものです。

OAuth 2.0とOpenID Connect (OIDC)

OAuth 2.0仕様群は、OpenID Connect (OIDC) の基盤として使用され、サードパーティAPIにアクセスするための委任機能を実現します。

OAuth 2.0がリソースへのアクセスと共有を目的としているのに対して、OIDCはユーザー認証に特化しています。OIDCは通常、ソーシャルアイデンティティプロバイダーが使用しており、OAuth 2.0プロトコルを介して提供されるJSON Web Token (JWT) を使用して認証を処理します。

JSON Web Token (JWT)

JSON Web Token (JWT) は、オープンな業界標準のトークン形式で、当事者間での情報の安全な送信に使用されます。最新のアプリケーションで認可、認証、情報のやり取りのために一般的に使用されており、特にマイクロサービスやクラウドベースの環境などの分散システムで使用されています。

SAML (Security Assertion Markup Language)

Security Assertion Markup Language (SAML) はSSO実装で最も広く使用されているプロトコルです。

SAMLの歴史は2001年にさかのぼり、最後の大きな改訂が行われたのは2005年にSAML 2.0がリリースされたときです。長い間SSO実装のデファクトスタンダードとして使用され、今でも広く使用されているものの、現在ではレガシーの地位になりつつあります。

WS連携 (WS-Fed)

WS連携 (WS-Fed) は、SSO実装で一般的に使用されるもう1つのプロトコルです。大部分がSAMLによく似ています。

クロスドメイン アイデンティティ 管理システム (SCIM)

クロスドメインアイデンティティ管理システム (SCIM) は、ユーザープロビジョニングを可能にするために設計されたもので、組織内のユーザーや他のリソースを管理するスキーマとプロトコルを提供します。しかし多くの仕様と同じように、SCIMは非常に機能が豊富で柔軟性があるという特徴があるため、実際には、相互運用性が限られた特注の実装になりがちです。

LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol) は、IPネットワークを介して分散ディレクトリ情報サービスへのアクセスと維持管理に使用されるアプリケーションプロトコルです。LDAPは、既存のユーザーディレクトリへのアクセスを可能にすることで機能します。Microsoft Active Directoryの基盤であり、管理者はユーザーアイデンティティを一元管理できます。

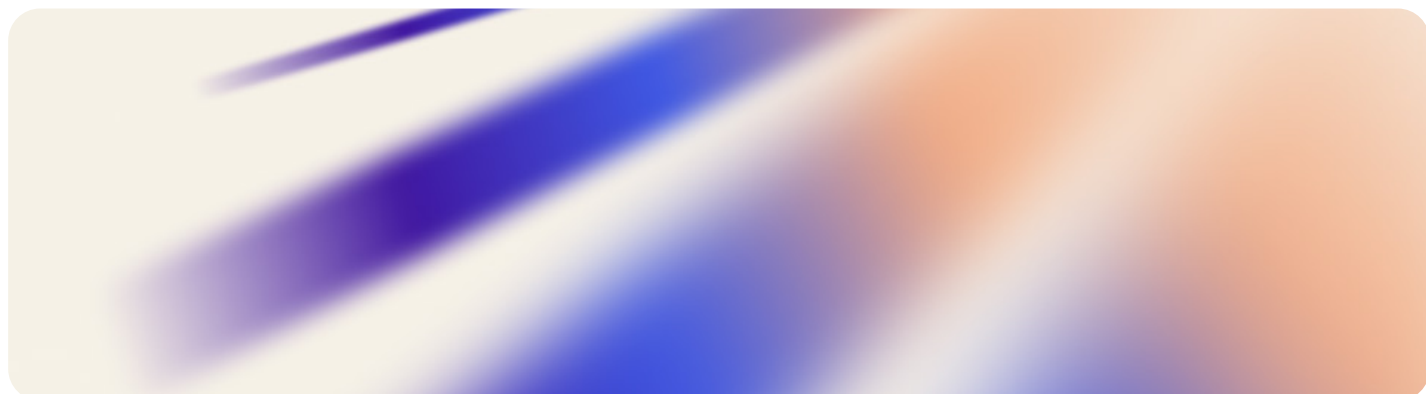
WebAuthnとFIDO2

Web認証API (WebAuthn) とFIDO2は密接に関連するテクノロジーで、安全でパスワードレスなWeb認証への移行において、重要な役割を果たします。

WebAuthnは、World Wide Web Consortium(W3C) が公開したWeb標準で、Webアプリケーションがクライアント側の認証者を組み込む方法を規定します。ユーザーは自分が好きな方法 (セキュリティキー、携帯電話、生体認証など) で、パスワードを使うことなくインターネットアカウントにログインできるようになります。

パスキーはWebAuthnを基盤に構築されています。しかしパスキーの登場前に、WebAuthnは第1認証要素または第2認証要素のいずれかにYubikeyなどの認証者を使用して、キーベースの認証を可能にしていました。

FIDO2は包括的な標準であり、WebAuthnはその主要コンポーネントの1つです。



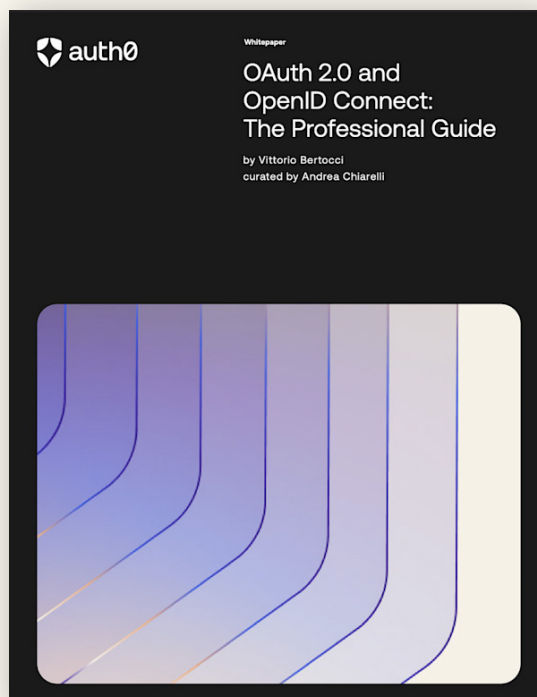
OAuth 2.0とOIDCの活用にあたる

『OAuth 2.0とOpenID Connect：プロフェッショナルガイド』は、OAuthや、OpenID Connect、認証と認可の委任の実現に付随する多くの変動要素を理解するのに役立ちます。

本書は、以下の理解を目的としています。

- 認証と認可の委任の典型的な問題を理解する
- これらの問題を解決するためにオープンプロトコルが提供する最新のツールを把握する
- OAuth 2.0とOpenID Connectについて実用的な知識を得る

上記の知識を得て、情報に基づいた意思決定ができるようになるほか、トラブルシューティングやネットワークトレースも理解できるようになります。



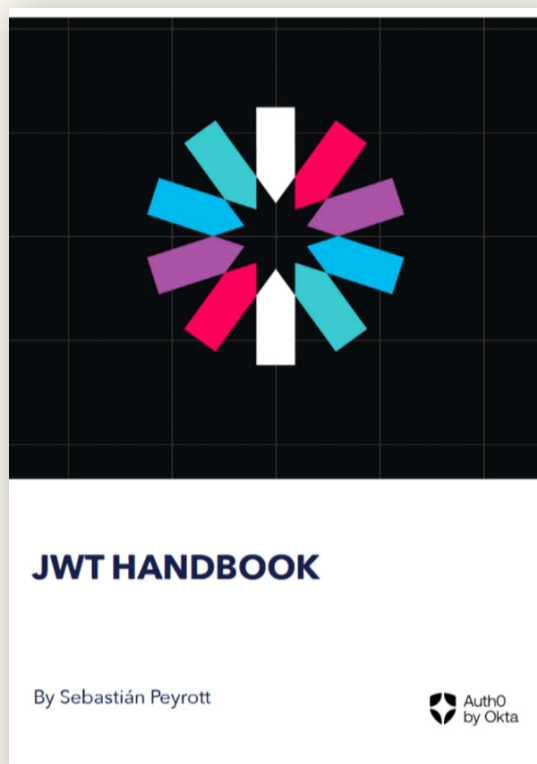
JWTを徹底的に知る

JWTがどのようにして誕生し、どのような課題を解決するために設計されたか疑問に思ったことはありませんか？

JWTの署名と暗号化で利用できる豊富なアルゴリズムについて、関心がありますか？

または、JWTを素早く理解して、すぐに業務で活用したいとお考えですか？

そのような方のために、詳細な『JWTハンドブック』をご用意いたしました。



ユーザー中心で拡張性のある製品の制作： プロダクトリーダーにとって重要な考慮事項

単純化し過ぎかもしれませんが、プロダクトリーダーが関心を持っているのは、さまざまな要素の中でもとりわけ、次を実現するアプリケーションを考案し市場に投入することでしょう。

- 優れたカスタマーエクスペリエンスを提供する
- 会社の戦略的目標をサポートする

実際には、カスタマーアイデンティティの観点から見ると、上記の目標を達成するには、以下のようなアプリケーションが必要になります。

- 拡張性と可用性に優れている
- 新規ユーザーの新規登録や、既存ユーザーのログインを素早く簡単にすることで、ユーザーの増加と定着をサポートする
- さまざまなチャネル（モバイルアプリ、Webアプリなど）全体で一貫したブランドエクスペリエンスを提供する
- 適切な認可とアクセスコントロールを適用する
- パーソナライゼーションとユーザー管理を可能にする
- 顧客データの収集と使用について顧客の同意を取得し、そのデータを収集する手段を提供できる
- アプリ内の生成AI機能を保護する

SSOとパスキーによる認証の簡素化とセキュリティ強化

コンシューマーアプリケーションでは、素早くスムーズで安全性の高いログインが不可欠です。そのようなエクスペリエンスを実現するための実績ある方法として、ソーシャルログインの使用とパスキーのサポートの2つがあります。

- ソーシャルログインは、利用する消費者にとって、アプリケーションにアクセスするための信頼性が高く便利な方法なので、当然サポートすべき機能です。
- パスキーは認証情報ベースの攻撃に対して強固なセキュリティを提供する上、MFAへの従来のアプローチと比べると摩擦が少なくなります。
- ビジネス顧客にとって、SSOが必要な機能に最も近いものと言えるでしょう。SSOが組織に歓迎されるのは、シンプルなユーザーエクスペリエンスと管理者エクスペリエンスを提供しながら、組織全体に導入できる強力なセキュリティ対策となるからです。
- 優れたユーザーエクスペリエンスを実現するには、一貫性も重要です。それだけで、コンバージョンを改善することができます。この点においては、慣れ親しんだログインフローとブランディングが非常に重要になりますが、この2つは[Auth0のユニバーサルログイン](#)で実現できます。

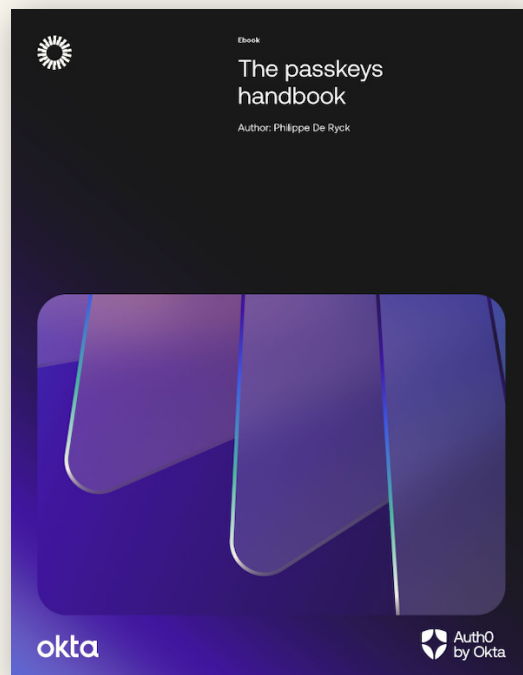


アプリにパスキーを実装する

『パスキーハンドブック』は、パスキーがオンラインセキュリティをどのように強化するかを理解したいと望むユーザーから、アプリケーションへのパスキーテクノロジーの実装を検討している開発者やソフトウェアアーキテクトまで、幅広い方を対象に作成されました。

本書ではパスキーをさまざまな観点から取り上げ、次のトピックを扱っています。

- パスキーの内容とその意義
- パスキーを使用したアカウントの保護
- パスキーの技術的な詳細
- アプリケーションへのパスキーの組み込み



認可とアクセスコントロールの適用

コンシューマーアプリケーションもビジネスアプリケーションも、人間のユーザーとNHI（急増するAIエージェントへの対応も含めて）が、許可された情報、機能、特権だけにアクセスでき、承認されたアクションだけを実行できるように、何らかの手段を備える必要があります。

きめ細かな認可(FGA)は、柔軟性が非常に高いことに加えて、今日のアプリで一般的になりつつある連携と共有の機能を実現できるため、ますます支持を得るようになっていきます。

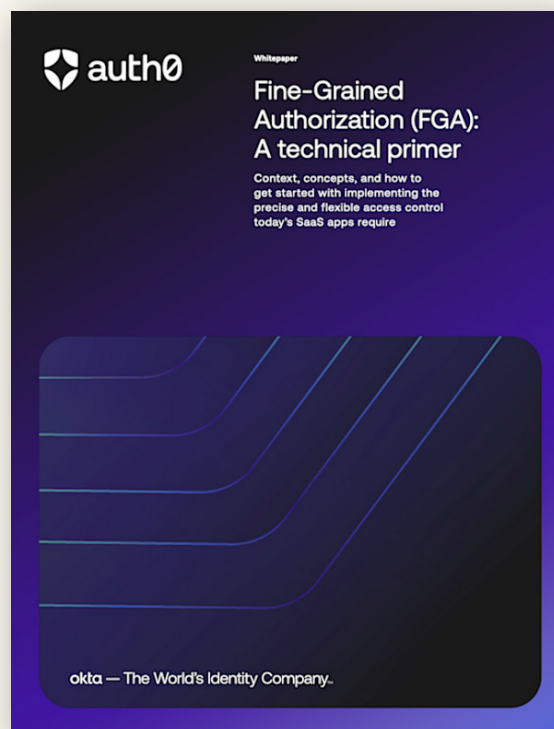
組織にとって、認可とアクセスコントロールを適用する最も効果的な方法は、SSOの利用です。ユーザー権限の細かさはアプリケーションにより異なるため、SSOを利用しない場合にはIT管理者の業務は非常に困難になります。

SSO環境では、ユーザーが一度認証されると、IdPはユーザーのアイデンティティデータと権限をアプリケーションに送信できるため、管理がシンプルになり、エラーが減り、詳細な監査が可能になります。

FGAの準備を整える

開発者、アーキテクト、セキュリティの専門家のために作成された『Fine-Grained Authorization: 技術的な手引き』では、FGAの効果的な実装に必要な技術的知見を提供します。内容は以下のとおりです。

- アクセスコントロールの仕組みの進化
- 主要なアクセスコントロールモデルの技術的な比較
- Auth0 FGA、OpenFGA、GoogleのZanzibarを中心にした、FGAソリューションの徹底的な分析
- Auth0 FGAの重要な詳細情報（主要コンセプト、構成言語、詳細な実装ガイドなど）



パーソナライゼーションとユーザー管理を実現

効果的なCIAMを実装することで、複数の顧客の入口に加えて、フロントエンドやバックエンドのシステムを統合する単一のカスタマーアイデンティティレイヤーが作成され、結果として、カスタマージャーニーを効果的に調整し、ロイヤリティと追加の収益を促進する優れた戦略的意思決定を行うことができます。

Auth0のユーザー管理と、双方向の統合を通じたアイデンティティオーケストレーションによって、CIAMは、一貫性があり高度にパーソナライズされたカスタマーエクスペリエンスをすべてのデジタルチャネルで実行できるようにします。

プライバシーを尊重しながら、顧客データを収集

プライバシーとユーザーエクスペリエンスを重視する新たな環境では、次の2つのタイプの顧客データがマーケティング担当者にとって価値あるものになります。

- **ゼロパーティデータ (ZPD):** 顧客が自発的に共有する、サインアップフォームの入力項目、配送先の詳細、Eメールによる調査への入力など
- **ファーストパーティデータ (FPD):** ユーザーがサイトやアプリケーションを操作したときに生成される、検索履歴、分析情報、セッションメタデータなど

CIAMは、アプリを支えるテクノロジー群において、特に価値のある要素です。CIAMはバックエンド機能を提供し、顧客向けのやり取り（プログレッシブプロファイリングなど）を管理するほか、コンプライアンスに準拠して（つまり、顧客のインフォームドコンセントを得て）ZPDとFPDを適切に取得、活用できるようにします。

AI機能のセキュリティ強化

AIシステムやAI搭載アプリケーションは複雑で、さまざまなリスクにさらされています。通常、AIシステムの脆弱性は、そのシステムに依存するAI搭載アプリケーションにも影響を与えます。AIエージェントを構築する際には、誰もが注意しなければならないセキュリティ上の課題がいくつかあります。

1. **ユーザー認証。** エージェントやアプリは、ユーザーが誰であるかを知る必要があります。たとえば、返信をカスタマイズするために、チャットボットはあなたのチャット履歴を表示したり、あなたの年齢や居住国を知る必要があるかもしれません。これには何らかの識別が必要であり、それが認証によって行われます。
2. **ユーザーに代わってAPI呼び出し。** AIエージェントは、通常のWebアプリケーションよりもはるかに多くのアプリと連携しています。生成AIアプリがさらに多くの製品と統合される中で、APIを呼び出し、それを安全に維持することが重要になります。
3. **非同期ワークフロー。** AIエージェントは、タスクを完了するのに時間がかかる場合や、複雑な条件が満たされるのを待つ場合があるかもしれません。それは数分や数時間かもしれませんが、場合によっては数日かかることもあります。しかし、ユーザーがそれほど長く待つことはありません。今後、こうしたケースは主流となり、エージェントがバックグラウンドで動作する非同期ワークフローとして実装されることになります。このようなシナリオでは、人間が監督者として機能し、チャットボットとのやり取りが行われていない間にAIエージェントのアクションを承認または拒否します。
4. **検索拡張生成 (RAG) の認可。** ほとんどすべての生成AIアプリは、RAGを実装するために、複数のシステムからAIモデルに情報を提供することができます。機密情報の漏洩を避けるため、ユーザーの代わりに応答したり行動したりする際にAIモデルに提供されるデータは、すべてユーザーがアクセスを許可されているデータでなければなりません。

AIエージェントのセキュリティ強化

AIエージェントは、もはや単なる会話ツールにとどまらず、技術スタック全体で実務を遂行する存在へと進化しています。APIを呼び出し、意思決定を行い、さらには機密データへのアクセスまで担うようになっていきます。

しかし、従来のIAMシステムの多くは、人間以外のアクターを想定して設計されていませんでした。

『AIエージェントのセキュリティ強化：新たなアイデンティティの課題』では、生成AIがアイデンティティに与える影響と、セキュリティ、製品、開発チームが安全な状態を保つために再考すべき点について詳しく解説しています。ダウンロードすると、以下の内容をご確認いただけます。

- 生成AIに対して、従来のアイデンティティフレームワークがうまく機能しない点
- ログイン中だけでなく、ログイン前後にもエージェントを保護する方法
- 人間による承認とFGAが重要である理由



安全で拡張性のあるシステムの構築： エンジニアリングリーダーにとっての重要な要素

エンジニアリングリーダーと開発リーダーは、効果的で効率的かつ持続可能な実装によって、製品のビジョンを実現する責任を担っています。

そのために、実際には、目に見える機能的な製品要素だけでなく、セキュリティや拡張性などの検討事項も考慮する必要があります。

きめ細かく柔軟性が高いアクセスコントロールの実装

セキュリティやコンプライアンスを損なわず、よりきめ細やかで柔軟なアクセスコントロールの必要性がますます高まっています。

ところが、そのような機能の構築は、それほど簡単ではありません。アクセスを保護し、管理する従来の方法（第一世代のポイントソリューションやアプリケーションに組み込まれた自社開発のコーディングなど）は、次のような最新の認可要件を満たしていないからです。

- **低レイテンシー**：認可にわずかに数ミリ秒の遅延があっても、アプリケーション全体のレイテンシーに影響を与える可能性があります。
- **可用性と信頼性**：認可はミッションクリティカルであり、ダウンタイムが発生するとアプリケーションでのユーザーのアクセスに支障をきたす可能性があります。
- **拡張性**：認可ソリューションは、ユーザーベースが拡大した場合（ユーザーやシステムに代わって行動するAIエージェントを含む）に、組織を支えられる機能を備えている必要があります。場合によっては、突然の大規模な急増にも対応できる必要があります。
- **ポリシーの柔軟性**：RBACやABACなど、さまざまな種類のポリシーをサポートすることで、アプリに最適なポリシーを選択でき、ニーズの変化に応じてポリシーを更新できるようになります。
- **セキュリティとコンプライアンス**：監査や管理が難しい認可ロジックは、セキュリティやコンプライアンスのリスクにつながります。目指すべきことは常に、脆弱性につながる箇所の削減であり、増やすべきではありません。これは、アプリケーションにAIエージェントが組み込まれると、さらに重要になります。

OpenFGAは、Auth0が設計した後、Auth0も主な管理者として加盟しているCloud Native Computing Foundation (CNCF) に寄贈したオープンソースの認可ソリューションで、開発者は読みやすいモデリング言語と使いやすいAPIを使用して、きめ細かいアクセスコントロールを構築できます。

ただし、OpenFGAを選択する組織は、運用管理における多くの責任も引き受けなければなりません。

これに対し、Auth0 FGAはOpenFGAを認証エンジンとして使用していますが、ホスティングや拡張などの複雑な作業を代行します。そのため、開発チームはインフラストラクチャの構築や保守ではなく、認可の実装に集中できます。

開発者向けFGAリソース

きめ細かい認可の実装について知りたい開発者の方には、まず当社の[FGA Playground](#)を確認することをおすすめします。FGA Playgroundでは、インタラクティブな環境でAuth0 FGAを実際に体験できます。

その他にも、次のリソースがあります。

- [fga.dev](#)は、Auth0 FGAについてあらゆることを学べるため、出発点として最適です。
- [Auth0 FGAドキュメント](#)では、多くのコードや構文のサンプルを確認できます。
- [Zanzibar Academy](#)では、GoogleのZanzibar (Auth0 FGAとOpen FGAの両方の基盤となるReBACモデル) について解説する、さまざまなリソースを提供しています。

The screenshot displays the Auth0 Fine-Grained Authorization (FGA) Playground interface. On the left, the 'AUTHORIZATION MODEL (4 TYPES)' is shown in a code editor, containing JSON and DSL definitions for various entities and their relationships. The right side features a 'TYPES PREVIEW' with a graph visualization showing the relationships between entities like 'repo', 'organization', 'team', 'user', 'admin', 'maintainer', 'owner', 'reader', 'writer', 'triger', 'repo_reader', 'repo_writer', 'repo_admin', and 'member'. A legend at the bottom right indicates 'STORE' (grey), 'TYPE' (blue), and 'RELATIONS' (green).

拡張性により統合を簡素化

多くの基本的なCIAMのユースケースは、あらゆる種類の組織に共通するものですが、次の2つの要素も検討する必要があります。

1. 技術スタック、広範なIT環境、企業の優先事項の組み合わせは、組織によって異なる
2. 各組織には固有のニーズがあり、カスタマーアイデンティティの基本を超えて拡張する必要があるか、少なくともアイデンティティスタックと他のシステムとのトランザクションが必要になる

システムで必要とされる処理の例としては、次のような機能が挙げられます。

- 顧客が標準のログインを使用して商品を閲覧し、カートに追加できるようにするが、購入を完了する前には多要素認証 (MFA) を要求する
- 同意管理システムと統合することで、サインアップ時に利用規約 (ToS) を表示して同意を得る
- その後のログインで、必要な場合のみ更新されたToSを表示する
- 不正防止管理ソリューションとのデータ交換により、金融詐欺やクレジットカード詐欺のリスクを低減する
- IDプルーフニングソリューションを利用して、ユーザーの実際のアイデンティティを確認する

同様に、組織の成熟度が高くなると、カスタマーアイデンティティスタックは一般的に、より多様で汎用的なビジネスシステムと統合されていきます。

拡張性は、CIAMソリューションがこれらの要素に対応し、組織全体としての目標を追求することを可能にする重要な要素です。

こうした機能をゼロから構築することは（または単に統合するだけでも）、オープンソースのコンポーネントを活用したとしても、ただでさえ多忙な開発者にとってさらなる負担となり、結果として永続的に維持すべきカスタムコードが増えることになります。

これに対し、拡張可能ですぐに使えるソリューションは、適応性を向上させ、特殊なユースケースや予期しないユースケースの実装を、開発者のリソースを大量に消費することなく可能にします。

たとえば、優れたソリューションでは、次のようなさまざまな拡張性オプションが提供されています。

- **ノーコード**：プラグアンドプレイ、ドラッグアンドドロップ、空欄を埋める形式、事前作成済みの統合により、コードを必要とすることなく、カスタマイズや統合を実現する
- **ローコード**：開発者がすぐに採用でき、コードの知識を持たない人でも（特に、適切なチュートリアルなどのサポートを利用することで）習得できるコードスニペットを使用することで、強力な制御と柔軟性を実現する
- **プロコード**：複雑なカスタマイズをアイデンティティフローに組み込む機能により、拡張性を最大限に活用する



すぐに使えるAuth0の拡張性

Auth0では拡張性が後付けではなく中核機能であり、ニーズに合わせてアイデンティティ機能をカスタマイズするために必要なツールが揃っています。

- **Actions**：ノーコード、ローコード、プロコードのオプションを使用して、アイデンティティフローの拡張とカスタマイズができます。デバッグ、ログ記録、バージョンコントロールも完備しています。
- **Forms**：ノーコードのビジュアルエディターで、フォームの作成とカスタマイズができます。
- **Auth0 Marketplace**：アプリケーションやAPIに対し、保守しやすいActions統合を迅速に見つけて追加でき、簡単にアイデンティティソリューションを拡張できます。

詳細は、『[カスタマーアイデンティティと拡張性の役割](#)』をご覧ください。



攻撃からの保護

ログインボックスの先にある情報へのアクセスを望んでいるのは、正当なユーザーだけではありません。攻撃者は目当てのものを手に入れるために、大きな労力を払うことも厭いません。こうした単純な理由から、どのアプリケーションやサービスのプロバイダーにとっても、カスタマーアイデンティティの保護は最優先事項であるべきです。

Auth0の『[Customer Identity Trends Report 2025](#)』は、サインアップ詐欺、クレデンシャルスタッフィング、MFAの悪用が日常的に実行されており、インターネットに接するログインボックスやAPIを使用するほぼすべての組織が、こうした脅威に対処しなければならないと指摘しています。

このような攻撃により、標的となる組織に大きな影響が及んでいます。不正利用の調査や修復にコストをかけなければならない、データ侵害が発生した場合には規制上の厳しい罰則や評判に傷がつくリスクに直面します。

サイバー犯罪者は、ログインボックスを突破するため、より多くの労力と専門知識を駆使しています。社会やビジネスを変革しつつある生成AIも、犯罪者に活用されるようになっていきます。このように、ログインボックスを保護するためには、これまで以上に洗練された防御のレイヤーが必要とされています。

今日の攻撃に対抗するには、次のような対策が必要です。

- **ホストレイヤー、プラットフォームレイヤー、アプリケーションレイヤーの防御**：悪意のあるエンティティがログインボックスやAPIにアクセスする前に排除
- **ログインレイヤーの防御**：不正なサインアップやアカウントの乗っ取りを防止
- **ログイン後の防御**：ユーザーが認証された後にセッション保護を強化し、アクセスを管理
- **可観測性ツール**：潜在的な攻撃の傾向を把握し、リアルタイムで迅速に対応可能
- **強力な暗号化、最新のハッシュアルゴリズム、APIセキュリティ、堅牢なデータ管理とシステムアクセス手順**などのバックエンドのインフラストラクチャ

進化する攻撃者の戦術、技術、手順（TTP）に対応し続けるだけでも、多大な努力が必要になります。このような脅威に対抗するための高度なセキュリティ機能を自ら開発するとなると、それはまったく別次元の問題であり、大半の組織が保有するリソースの範囲を遥かに超えてしまいます。これに対して、Auth0のような最新のカスタマーアイデンティティソリューションは、「セキュアバイデザイン」に基づく多層防御のアジャイルなアプローチを採用しており、攻撃者のビジネスモデルを崩壊させることで、攻撃を効果的に阻止し、攻撃者を思いとどまらせることができます。

不正登録の防止

悪意あるユーザーがログインボックスを越えた先にある権限、サービス、情報にアクセスするための最も簡単な方法は、自分が制御するパペットアカウントを最初から作成することです。

偽のサインアップは、大規模に行われる場合に特に重大な問題を引き起こし、不必要な出費を発生させることがあります。たとえば、偽ユーザーは次のような行為を行う可能性があります。

- 後に古いアカウントとして利用され、制御を回避するための足掛かりを作る
- 既存のユーザーアカウントを列挙/発見する
- サインアップボーナスなどの特典を消費する
- リソースの消費とレート制限超過をサービス拒否攻撃を実行するために利用する

さらに、コンバージョンフロー全体は、ユーザーとサービスとのやり取りに基づき最適化されることがよくあります。不正登録はこのデータを汚染するため、アナリティクスが複雑化し、クリーンアッププロジェクトのコストが増大する可能性があります。

CIAMプラットフォームは、サインアップ攻撃に対抗するために、次のような一連の多層防御能力を提供するものでなければなりません。

- ボット検出
- CAPTCHAベースの対策
- 不正なIPアドレスと総当たり攻撃をブロックする機能

さらに、不正な登録を減らすために適用できるサインアップ攻撃特有のテクニックがいくつかあります。以下に例をあげます。

- **サインアップ前のルールとアクション:** チャレンジの適用、追加情報の要求などにより、新規ユーザーが不正である可能性をさらに低減する
- **ソーシャルログイン:** 不正サインアップの防止を「アウトソーシング」する
- **IDプルーフィング:** リスクが特に高いと考えられる場合に適用する
- **連絡先情報の検証:** ワンタイムパスコードやマジックリンクなどにより、メールアドレス、電話番号などを確認する

しかし、おそらく最も効果的なのは、**ユーザーにパスキーを使用したサインアップを促すこと**です。パスキーは暗号化されているため、サインアップ攻撃での悪用は非常に困難です。実際、Auth0 Platformのテレメトリ分析によると、攻撃者はパスキーによるサインアップやログインフローに対して大規模な攻撃をまだ行っていないことが示されています。



認証のセキュリティ強化

不正登録は(最低でも)費用のかかる迷惑行為ですが、アカウント乗っ取り(ATO)はセキュリティとプライバシーにとってより大きな脅威となります。

B2C環境では、攻撃者がリソース(ロイヤルティポイントなど)、権限(商品の購入、特に限定品の購入など)、貴重な属性データや個人識別情報(PII)にアクセスする可能性があります。

B2B環境では、攻撃者がユーザーアカウントを侵害すると、機密データにアクセスされる恐れがあります。これによって情報漏洩が起きると、攻撃の標的となった組織が厳しい規制上および契約上の制裁を受ける可能性があります。

一部のATO攻撃は個人を狙いますが、大半はパスワード認証を標的にした総当たり攻撃手法を用い、できるだけ多くのアカウントを侵害しようとします。

CIAMプラットフォームは、ログイン攻撃に対抗する一連の防御能力を提供するものでなければなりません。繰り返しになりますが、最も効果的なのは複数レイヤーのソリューションで、テクニックを実装するほど、顧客と組織は安全になります。

- **ユーザーに漏洩したパスワードの再設定を要求:** 漏洩パスワードを検知できる方法があることを前提として、オンライン上に認証情報を投稿された顧客には、パスワード再設定プロセスが強制されなければなりません。このアプローチは辞書攻撃に対する防御にはなりませんが、そちらは総当たり攻撃のしきい値を上げることで対応できます。
- **不要/不使用な機能を無効化:** 使用していないエンドポイントや機能は、攻撃対象領域を不必要に広げかねず、攻撃者がコントロール(ボット防御など)を回避できるようにしてしまいます。ある機能がユースケースにとって必要不可欠でない場合は、攻撃者による悪用を避けるため、無効にすることをおすすめします。
- **移動不可能な場所からのログインをブロック:** 前回のログイン成功から経過した時間内に到達できない地理的位置から行われたログイン試行をブロックします。
- **侵害されたアカウントにMFAを要求:** このアプローチでは、侵害されたことが判明しているアカウントのユーザーにMFAを使用することで、不必要な摩擦を避けます。
- **アダプティブMFAを実装:** このアプローチでは、事前に定義したリスク基準を超えたログイン試行にMFAチャレンジを使用することで、不必要な摩擦を避けます。
- **強力でフィッシング耐性のあるMFAを要求:** MFAを導入する場合は、優先的にオーセンティケーターアプリとWebAuthnベースの手法を利用します。すでに長い間MFAをサポートしている場合は、既存のユーザーを従来のアプローチから脱却させ、強力な第2要素に移行させるよう取り組みます。

とはいえ、パスワードベースのATOに対する最も効果的な防御はおそらくパスワードからの脱却です。パスキーの出現とともに(特に消費者市場では)、実現の見通しはより現実的になっています。

おわりに

多くの開発者や製品所有者が把握しているように、アイデンティティは一見したところ概念としては単純に思えますが、次のような複雑さもあります。

- **アイデンティティの適切な実装は非常に困難です。** 経験豊富なエンジニアリングチームでさえ、アイデンティティは認証情報のペアやログインボックス以上のものだとすぐに気づかされます。
- **アイデンティティは絶えず変化しています。** 新しい標準が定義され、バグが特定され、顧客の期待する内容が変わり、生成AIのような新しいテクノロジーがアイデンティティと認可にまったく新しい課題をもたらします。このように変化する環境では、独自のソリューションを構築することは最初のステップに過ぎず、その後には広範囲にわたる複雑で結果的にコストのかかる取り組みが続きます。

代わりに、すぐに使えるソリューションを統合すると、次が可能になります。

- 開発者がコア製品のニーズに専念できるようになる
- 市場投入までの時間を短縮できる
- 新たな脅威、標準、顧客ニーズに後れを取らず対応する
- 製品の俊敏性と拡張性を向上させる
- ログイン前、ログイン中、ログイン後のアイデンティティ攻撃に対して自衛する
- 規制やコンプライアンスへの準拠をサポートする
- 一貫性がありブランドに合ったユーザーエクスペリエンスを大規模に実現する
- エンタープライズ顧客の獲得に向けて有利な立場を築く
- 貴重な開発者リソースと運用サポートにアクセスできるようになる
- 特に自社開発のアプローチと比較した場合に、長期的なコスト効率を実現する

導入の準備はできていますか？ Auth0がサポートします

CIAM分野のパイオニアとして10年以上の経験を誇るAuth0は、最先端のテクノロジーとアーキテクチャを開発、活用して、次のように魅力的な一連の機能を備えた最新ソリューションを生み出してきました。

- さまざまなニーズに対応するパフォーマンス階層と割引プラン（豊富な機能はそのまま）
- カスタマイズ可能なアクション（Actions）と事前構築済みのパートナー統合
- 60を超えるソーシャルプロバイダーやアイデンティティプロバイダーとの接続
- オープン標準（OIDC、SAML、FIDO、OAuthなど）の幅広いサポート
- マルチクラウド暗号化アーキテクチャと、AWSおよびAzure上での実行のサポート（パブリッククラウドとプライベートクラウドのオプションを含む）
- HIPAAからPCIまでのコンプライアンス要件と規制要件の広範なサポート
- カスタマイズとブランディングが簡単に行えるサインアップとログインのインターフェイスおよびフロー

Auth0を選ぶことで、今日も明日も、そして未来にわたって貴社のCIAMニーズを満たせるようになります。なぜなら、Oktaが次のような負荷の高い取り組みを代行しているからです。

- 仕様や標準への対応。新しい相互運用性を追加したり、パスワードなどの最新機能を提供したりすることが、設定のオン/オフを切り替えるのと同じくらい簡単になります。
- 規制の新規導入や変化に対応し、コンプライアンスを確保するための基盤整備。心配事がひとつ減ります。
- 攻撃者の戦術、技術、手順（TTP）の調査と、これらの脅威に対抗するために必要となる高度なセキュリティ機能の導入
- 生成AIなどの新しいテクノロジーをカスタマーアイデンティティにどのように適用できるかの探索

上記の結果、お客様にとっては2つの大きなメリットがあります。

- 常に最先端のカスタマーアイデンティティ機能を活用できる
- 組織の限られたリソースを本業の価値提案に集中できる



その他の開発者向けリソースを見る

Auth0を使用してアプリに認証、認可、その他のアイデンティティ機能を実装する方法については、developer.auth0.com/resourcesをご覧ください。



開発者の目的を見る

Auth0を異なるフレームワークや言語に組み込む方法について学べます。



コードサンプルを見る

さまざまな言語やフレームワークでのAuth0の動作をご覧ください。



開発者向けラボを見る

Auth0の基本的な使い方からさらに踏み込んで、その活用方法を楽しく魅力的な演習を通して学べます。



カスタムコードサンプルの構築

Auth0を使用して、選択したフルスタックアプリケーションのアクセスを保護しましょう。



Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

本資料および本資料に含まれる推奨事項は、法律、プライバシー、セキュリティ、コンプライアンス、またはビジネスに関する助言ではありません。本資料は、一般的な情報提供のみを目的としており、最新のセキュリティ、プライバシー、法律の動向、また関連する問題をすべて反映していないことがあります。本資料の利用者は、自身の責任において、自身の弁護士またはその他の専門アドバイザーから法律、セキュリティ、プライバシー、コンプライアンス、またはビジネスに関する助言を得るものとし、本書に記載された推奨事項に依存すべきではありません。本資料に記載された推奨事項を実施した結果生じるいかなる損失または損害に対しても、Oktaは責任を負いません。Oktaは、これらの資料の内容に関して、いかなる表明、保証、またはその他の保証も行いません。