ホワイトペーパー

社内構築からの脱却

カスタマーアイデンティティ /
アクセス管理の導入に向けて

okta

目次

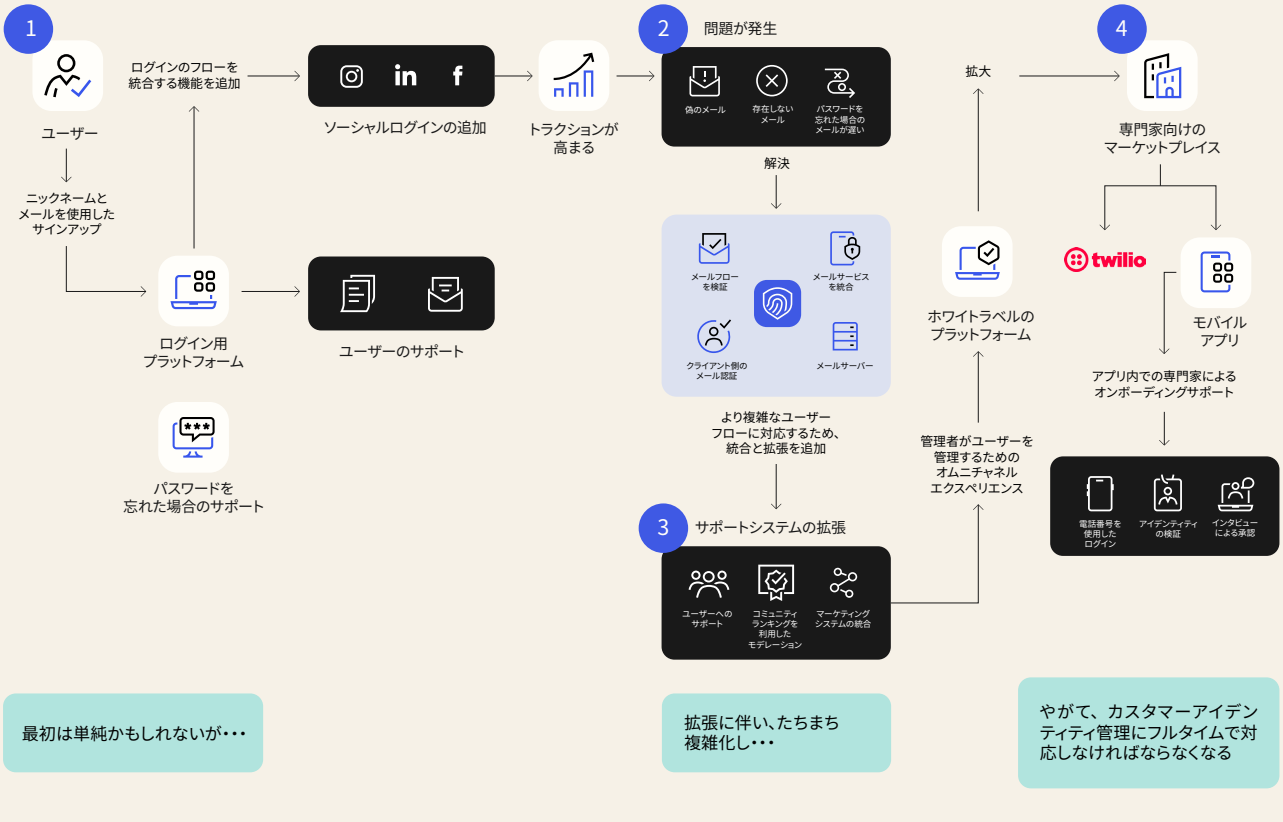
適切なカスタマーアイデンティティの実現は難しい

Web アプリやモバイルアプリを開発するチームは、新しい機能を追加するたびに同じジレンマに直面します。社内で構築すべきか、あるいは即座に利用開始できるサービスを利用して作業を容易化 / 迅速化すべきか、という 2 つの選択肢に悩まされるのです。

「社内の開発者は、カスタマーアイデンティティに対応可能だが、ログインボックスの作成はどの程度難しい作業なのか」と考えることになります。

しかし、カスタマーアイデンティティ / アクセス管理（CIAM）はログインボックスだけの問題ではありません。CIAM システムを自社構築した場合、堅牢さを維持することは複雑な取り組みとなります。ビジネスが成長して機能を追加し続ける中で、予想以上のリソースを CIAM のために消耗することになりかねません。開発者の時間は貴重です。自社構築のアイデンティティ、セキュリティ、プライバシーコンプライアンスの維持に費やした時間の分だけ、ビジネスの中核的イノベーションに投じる時間が奪われることになります。

自社構築を選択すると、さらに難しくなる



では、セキュリティ、リリースまでのスケジュール、あるいは予算を犠牲にすることなく、イノベーションを推進し、開発者の時間を最大限に活用するにはどうすればよいのでしょうか。

そのような課題の解決策の一つとなるのが、事前構築された CIAM システムです。API、SDK、そして即座に利用できカスタマイズ可能なコンポーネントで構成されるデジタルアイデンティティレイヤーは、市場投入を高速化し、開発コストを削減し、社内開発者をアプリケーションの中核機能に集中させるための基本要素として役立ちます。顧客向けアプリケーションには、認証、認可、ユーザー管理に関連する基本機能の共通セットが必要です。アプリケーションは、アカウント作成、ユーザーログイン、パスワードのリセット、アカウント回復、多要素認証（MFA）の登録といった一般的なワークフローをサポートしなければなりません。さらに、ユーザーによって異なるアクセスレベルに対応する必要があります。

このホワイトペーパーでは、「構築か、購入か」を判断する際の主な検討事項と、事前構築済みソリューションの利点について解説します。

「アイデンティティのコンポーネントとして、（Okta は）非常に役立ちます。おかげで、当社の歩みを速める準備ができたと自信をもって言うことができます」

MGM Resorts International、CISO
Scott Howitt 氏

アプリケーション開発の総所有コスト（TCO）を削減

アイデンティティ管理は、コスト超過のリスクが非常に高い領域です。これは、機能やシステムの複雑さが過小評価されがちであり、また常に進化しているためです。自社構築のアプローチは、この状況に大きな不確実性を招くことになります。また、社内チームの取り組みが横道にそれて、詳細なユーザー機能を構築することになったり、環境の変化に伴って要件が変化したことに気づいたりすると、コストが大幅に増加します。それでもスケジュールどおりに完了できるかもしれませんが、そのために高額な請負業者の支援を仰がねばならなくなることもあります。信頼できるプロバイダーにアイデンティティを委託することで、開発チームはプロジェクト全体のデリバリを予算内で確実に遂行できるようになります。

アプリケーション開発における TCO 削減の例 [1]

3 人	x	6 か月	x	20 万ドル	x	90%	=	27 万ドル
開発者		アイデンティティのタイムライン		総人件費		改善		TCO の削減

「アイデンティティ分野は急速に変化しており、当社は日々進行する変化のペースについていけるテクノロジーパートナーを必要としています」

JetBlue Airways、イノベーション担当 EVP、
最高デジタル & 技術責任者
Eash Sundaram 氏

[1] テクノロジーを主な収益源とする企業におけるエンジニアの価値についての、一般的な Google 式の計算方法。ここでの計算では、エンジニアの平均的な年間収益貢献率に、アイデンティティレイヤーのデリバリのためにエンジニアプールから除かれたエンジニア数を乗じています。

アプリケーションの中核機能にリソースを集中

アプリケーションの中核は、エンドユーザーにとっての有用性を実現する機能であり、これをどれだけうまく実行できるかがビジネスの成功を左右します。最新のアイデンティティレイヤーを導入することで、チームは収益と顧客エンゲージメントを高める機能に集中でき、開発者は顧客が求める第 2、第 3、第 4 のアプリに迅速に移行できます。

セキュリティ侵害 / コンプライアンス違反のリスクを低減

チームが最後にパスワードのハッシュ化アルゴリズムを更新したのはいつでしょうか。ユーザーデータと個人情報（PII）は攻撃の最も一般的な標的ですが、効果的な暗号化アルゴリズムの平均寿命は 18 か月です。成長や収益を促進する要件を優先させるため、ユーザーの保護はないがしろにされがちです。さらに、安全なアイデンティティサービスを提供するには、オペレーティングシステムからデータベース、トランスポートレイヤー、アプリケーションスタック、コードの脆弱性まで、インフラストラクチャの各レイヤーで脆弱性に対処するための専門知識（と時間）が必要です。こうした高いレベルのセキュリティ専門家が、開発チーム内に含まれていることは稀です。そのため、機密データが脆弱な状態になるまで、ユーザーセキュリティの不備に気づかない可能性があります。また、アルゴリズムが侵害されたり、攻撃ベクトルが発見されたりといった、セキュリティの状況の変化に気づかないケースも少なくありません。

ユーザーデータを攻撃者から保護するには、適切なアイデンティティ管理サービスを選ぶ必要があります。アイデンティティとアクセスの攻撃ベクトルに対応する高度なセキュリティに焦点を当てた専門家チームでなければ、こうしたサービスを構築することはできません。セキュリティ対策には、強力な暗号化、API のセキュリティ、ファイアウォールの高度な保護、堅牢なデータ管理、システムアクセス手順が含まれます。これらのセキュリティ対策やインフラストラクチャは、HIPAA、FedRamp、GDPR など、地域や業種に特化した規制へのコンプライアンスを可能にします。

「National Bank of Canada は、カナダ国内の数百の支店で数百万人の顧客にサービスを提供しています。組織として明確な目標があり、カスタマーエクスペリエンスの簡素化もその一つです。Okta のスマート認証とコンテキスト対応機能によって、シームレスで安全なオンラインエクスペリエンスを顧客に提供できます」

Heal、CTO
Rish Tandon 氏

開発者のモチベーションを維持

アイデンティティは顧客向けアプリケーションを成功させる上で重要です。しかし、アイデンティティとセキュリティのインフラストラクチャ構築をすべての開発者が楽しんでいるわけではありません。リスクの高い領域であり、複雑さを伴うことが多い一方で、ユーザー管理は平凡な職務として認識されることもあり、多くの開発者は製品の差別化の中核的機能や最先端システムに関連する機能に取り組みたいと考えています。また、ユーザーセキュリティの実装に伴って、大きなリスクやガイダンスの矛盾といった間接的負担の重い領域でもあります。この点も、特にやる気を失わせる原因となっています。その一方で、最新の REST-JSON API サービスについては、多くの開発者が興味深くアクセスしやすいと認識しています。

高い拡張性と信頼性を実現

ユーザー管理で障害が起こると、ユーザーはロックアウトされます。可用性の低下によってログインエクスペリエンスに問題が発生した場合、エンドユーザーがその理由を知ることも気にすることもありませんが、組織やブランドに対する評価が下がります。コンシューマーの負荷レベルは予測不可能であり、マーケティング部門は、プロモーションがユーザーの流入を促進するタイミングを常に把握しているわけでも、共有しているわけでもありません。これを開発チームが管理する場合、複数の可用性ラインを提供し、ユーザーベースが拡大しても容易に拡張できる能力を確保していなければなりません。データセンターで、あるいは IaaS プロバイダーと協力して、二重、三重の冗長性を提供する準備が必要です。中断のないサービスを保証するには、シームレスなアップグレードと保守を提供することも重要です。組織がこのように大きな責任を引き受ける場合、保守の負担に対処しきれないことがあります。ユーザー管理サービスを提供する外部のプロバイダーを利用することで、オペレーションの頭痛の種を完全に取り除くことが可能になります。

「エコシステム全体で統合を促進し、アイデンティティがシステム間で持続するようにし、高い信頼性と可用性を備えたアイデンティティを顧客関係の中心に据えることが、当社にとって非常に重要でした」

Pitney、E コマーステクノロジー担当シニアバイスプレジデント
James Fairweather 氏

カスタマーアイデンティティ / アクセス管理を購入するメリット

アイデンティティ管理を自社構築ではなく購入すべきであることには、説得力のある理由があります。

アプリの市場投入の高速化により収益を拡大
顧客のニーズは気まぐれに変化することがあります。今日の組織には、市場機会を生かすための十分な俊敏性が求められ、さもなければ収益低下のリスクにさらされます。適切なカスタマーアイデンティティソリューションは、安全なカスタマーエクスペリエンスのためのアイデンティティレイヤーを提供できます。このため、開発チームは認証、認可、ユーザー管理に関連する作業を一から始める必要がなく、代わりにアプリを差別化する機能の構築に集中し、コンシューマーに機能を提供できます。収益を維持することも、収益を創出することと同等に重要であり、拡張性がこれに関連します。認証、パスワードの暗号化、検索といったリソース集約的なアクションは、ピーク時のユーザー需要に対応する必要があります。

エンジニアリングコストを削減
サードパーティのアイデンティティ管理ソリューションは簡単に導入でき、スイッチのボタンを押すような容易さで強力な機能を有効にできます。何百時間、何千時間にも上る貴重な開発期間を、認証の構築に費やすのではなく、ビジネスロジックの記述に振り向けることができます。認証のためのテストやセキュリティに割いていた時間を、アプリの中核機能の作業に戻すことができるのです。アイデンティティプロバイダーの統合とマッピングは、時間も労力もかかる作業です。適切なサードパーティソリューションでは、こうした統合はすでに構築済みであり、すぐに利用できる状態になっています。さらに、即座に利用開始できる CIAM ソリューションは、一般的な開発スタック向けの SDK も提供し、認証システムを統合するために必要な追加のコーディングをさらに削減します。企業のエンジニアリングチームは、コーディングやカスタマイズではなく、構成に集中できます。

セキュリティを強化
チームが最後にパスワードのハッシュ化アルゴリズムを更新したのはいつでしょうか。攻撃の最も一般的な標的となっているのが、ユーザーデータと個人情報です。効果的な暗号化アルゴリズムの寿命は平均 18 か月です。しかし、ユーザーの保護は、成長や収益を促進する要件を優先させるために、ないがしろにされがちです。CIAM ソリューションは、ユーザーデータを安全に格納 / 転送する責任を負い、地域のコンプライアンスポリシーと認定を遵守します。さらに、CIAM ソリューションはフェデレーションアイデンティティを提供します。これによって、ユーザーが複数のログイン資格情報を記憶せずに済ませようと同じパスワードを使いまわすといった悪習を防止できます。

さまざまな業界での導入事例

Schneider Electric — 統合アイデンティティ管理で成長を促進
100 か国以上で 17 万人以上の従業員を抱える Schneider Electric は、エネルギー管理 / 自動化の世界的リーダーです。同社は、リソースの利用を最大限に効率化しながら、企業としての次なる成長段階に合わせて拡張できるアイデンティティ管理戦略を必要としていました。CIAM を選定する上での主なニーズは、シングルサインオンシステムにより統一的な認証プロセスを構築することでした。これにより、社内の多様なシステムやアプリケーションのすべてで、共通のアイデンティティと資格情報を使用できるようになることを目指しました。

費用対効果を分析した結果、中核となるビジネス目標 / 目的を達成するために従業員のリソースを活用する方が望ましいことがすぐに判明しました。サードパーティのアイデンティティ管理は、企業内の障壁を取り除き、アイデンティティを統合するという困難な問題を解決できます。また、堅牢で柔軟なソリューションを提供する Okta Customer Identity Cloud（旧 Auth0）は、開発者に焦点を当て、統合を容易にします。このプラットフォームは、Web とモバイルに対応し、オープンスタンダードをサポートするとともに、堅牢な機能と幅広いアイデンティティプロバイダーのサポートと容易な移行を通じて将来のニーズにも対応します。

Okta CIC を選び、導入した後、多くのメリットが実現しました。Okta のアイデンティティ管理ソリューションを使用することで、追加の開発作業がなくなりました。これによって、より多くのリソースを IT のイノベーションのために開放できました。市場投入が加速し、セキュリティの向上とベストプラクティスの恩恵がシステムにもたらされました。また、Okta CIC は脆弱性に対する迅速かつ徹底的な対応も提供しました。

「昨年の Heartbleed のゼロデイ脆弱性について、どのニュースサイトが報じるよりも前に、Auth0（現在の Okta Customer Identity Cloud）からメールで警告を受けました。Auth0 のシステムから Heartbleed の脅威を排除するパッチがすでに提供されており、Auth0 がこのパッチを Auth0 のサービスの Schneider Electric のインスタンスにインストール済みであることを示す確認メールが届きました。

当社のプラットフォームチームは、Auth0 に本当に助けられています。このシナリオでは、セキュリティの問題が修正されただけではありません。IT チームは、問題の緩和方法の詳細なステップを活用して、社内チームに直接報告することで、貴重な時間を節約できました。さらに、チームが実行するには非常に大きな労力を要する証明書の循環も、Auth0 により実行されました。

Auth0 プラットフォームのおかげで、アイデンティティアーキテクチャを早期に計画 / 統合できます。これにより、重要な時間を節約できるとともに、安全なシステムを準備した上でプロジェクトを開始できます」

Schneider Electric、シニアグローバルソフトウェアアーキテクト
Stephen Berard 氏

Bluetooth — オンプレミスとクラウドのアプリ全体でアイデンティティを統合
ワイヤレステクノロジーの世界的リーダーである Bluetooth は、拡大するエコシステムでさまざまな課題を抱えていました。たった 1 つのアプリケーションから始まったビジネスは、急速に複数の異なるアプリへと成長しました。社内開発したアプリだけでなく、サードパーティの SaaS アプリ（Sharepoint、ServiceNow、SiteCore）も、すべて異なる資格情報を認証に必要としていました。Bluetooth の既存の自社構築ソリューションはフォームベースであり、ユーザー名とパスワードの資格情報を使用していました。このプラットフォームは、フェデレーションアイデンティティには適していませんでした。同社は、自社構築アプリとサードパーティの SaaS アプリをすべてサポートする、シングルサインオンを備えた最新のアイデンティティソリューションを必要としていました。また、既存のプラットフォームを稼働させながら、将来的には完全に新しいソリューションに移行する計画で実装する必要がありました。機密文書への適切なアクセスレベルを確保するために、ユーザーの役割とアクセス権限も重要でした。

サードパーティのアイデンティティは、こうした条件に合致するものでした。実装は簡単で、チームは SSO と最新の認証を追加できました。レガシーシステムはそのままに、移行計画が履行され、実行されました。実装期間も、自社構築のプラットフォームの場合は数か月を要したのに対して、わずか数日で済みました。詳細なコードサンプルを含む優れたドキュメントが、初歩的なトピックから高度なトピックまで網羅しているので、Bluetooth の SIG エンジニアは最新のアイデンティティソリューションを迅速に理解して実装できます。同社は開発者支援の担当エンジニアと連携して、プラットフォームの能力を共同で示す概念実証を開発しました。サポートの応答時間は短く、解決も迅速でした。

まとめ

妥協のないイノベーション
現代のアイデンティティは、管理が困難です。進化し続ける標準やベストプラクティスに対応し、セキュリティの不具合にパッチを適応し続けるために、中核のビジネスから時間とコストが奪われていきます。組織のニーズに合わせて成長する機能を検討し、他社がどのように独自ソリューションの評価と実装を成功させたかを理解することで、セキュリティ、ユーザーエクスペリエンスといった面で妥協することなく、また開発工数を増加させることなく、アイデンティティ管理ソリューションのメリットを享受できるようになります。

重大なリスクを抱える領域、ビジネスの潜在的障害としての CIAM を、収益を促進する能力を与えるだけでなく、実際に収益を増加させるシステムへと転換できます。Okta Customer Identity Cloud は、最も簡単で包括的、かつ拡張性の高い CIAM です。このソリューションにより、従来のように数か月ではなく数日で CIAM を導入でき、また組織の将来性を確保できます。

Okta を活用

Okta は、ユーザーのアイデンティティ管理を支援します。セキュリティの専門家として、Okta は最先端のセキュリティを設計から考慮した IDaaS（Identity-as-a-Service）プラットフォームを構築しました。世界 167 か国、8 万人以上の開発者が、Okta Customer Identity Cloud をアイデンティティ管理ソリューションとして信頼し、活用しています。

Okta は、以下の機能とメリットを提供します。

- エンタープライズフェデレーションとシングルサインオンの構成と実装では、基本的な構成のみを必要とし、コーディングが不要です。
- エンタープライズ接続には、Active Directory、LDAP、ADFS、SAML、Google Apps などを含みます。
- LinkedIn、Facebook、Twitter、Google など、あらゆる主要プロバイダーとのソーシャル接続に対応します。
- Auth0 DB またはカスタム DB を介した従来のユーザー名とパスワードによる認証に、多要素認証、パスワード漏洩検知、ブルートフォース攻撃防御、異常検知などの強化されたセキュリティ機能を追加します。
- ユーザーを既存のシステムから円滑に移行でき、強制的なパスワードのリセットが不要です。
- 組織のコンプライアンスとアップセルの機会を確保するための、アイデンティティベースのアナリティクスを監査 / 表示する方法を提供します。
- きめ細かなアクセス許可と強力なカスタムルールにより、ユーザーアクセスを簡単に管理できます。
- 管理の委任により、顧客のきめ細かなアクセス、可視性、ユーザー管理を実現できます。
- Okta Customer Identity Cloud の場合、開発者は、堅牢でカスタマイズ可能なアイデンティティ管理を、あらゆるテクノロジースタックに 30 分未満でセットアップできます。

リソース

Okta Customer Identity Cloud（旧 Auth0）に関する他社の評価については、Okta Web サイトの顧客セクションおよび価格セクションをご覧ください。または、営業担当までお問い合わせください。