ホワイトペーパー

アイデンティティの成熟に向けたガイド

アイデンティティを通じて生産性、ユーザーエクスペリエンス、セキュリティを向上させるためのロードマップ

目次

アイデンティティによってビジネス目標を達成する

デジタルアイデンティティはかつて、ユーザー名とパスワードを管理するだけの簡易なサービスでした。今ではアイデンティティは、現在のビジネスにとって不可欠な基盤となっています。アイデンティティは、従業員、クライアント、およびパートナーがどこにいても、どのようなデバイスを使用していても、安全にやり取りできるようにし、その関わりを追跡および制御できるようにするエンジンとしての役割を果たしています。アイデンティティは、オンラインファーストの世界のあらゆる領域に深く入り込んでいます。アイデンティティは、ユーザーエクスペリエンスを大きく左右し、明確な情報を使用してセキュリティ調査を進められるかどうかの鍵を握っています。また、IT スタッフの時間とコストの削減、そしてガバナンス、リスク、コンプライアンス（GRC）の取り組みを前進させるためにも役立ちます。そのため、アイデンティティは、運用効率とコスト管理、収益の増加、サイバーセキュリティの強化など、多くのビジネス成果において重要な役割も担っています。これだけ多くの要素が絡み合っているため、多くの組織は顧客や従業員のアイデンティティサービスの最新化と改善に苦労していますが、これは当然のことです。

アイデンティティは、企業とユーザー間のやり取りの方法を変革し、以下のビジネス目標の達成に貢献します。

収益の増加：

多くの業界ではカスタマーエクスペリエンスを巡る競争が行われており、アイデンティティはこれらのエクスペリエンスを最適化するために不可欠になっています。

60%

簡単かつ安全で摩擦のないログインを提供できる場合に、より多く支出する可能性が高いと回答したユーザーの割合 [1]。

コストの削減と効率性の向上：

アイデンティティプラットフォームによって集約、統合、および自動化という利点がもたらされ、IT と従業員の効率性を向上させ、ソフトウェア支出を最適化し、製品をより迅速に市場に投入できるようになります。

22%

自動化に多額の投資を行っている企業は、自動化の取り組みが遅れている企業と比較して、コストを 22% 削減している [2]。

サイバーセキュリティの強化：

現在の脅威情勢においてアイデンティティは最大の攻撃ベクトルであり、セキュリティスタックでも重要な役割を果たしています。

61%

デジタルアイデンティティの管理と保護をセキュリティプログラムのトップ 3 の優先事項と考えている企業の割合 [3]。

[1] Okta Customer Identity Trends Report、2023 年

[2] Bain and Company、2023 年

[3] 「2023 Trends in Securing Digital Identities」レポート、Identity Defined Security Alliance

アイデンティティ成熟度モデル

調査結果[4]から、従業員のアイデンティティの成熟度でリーダーに位置付けられる組織は以下のメリットを実現していることがわかりました。

3.9 倍

アイデンティティソリューションによってビジネスの俊敏性が向上したと回答した割合

3.4 倍

アイデンティティソリューションがインシデント対応に大きく役立っていると回答した割合

3.6 倍

アイデンティティソリューションによって従業員の生産性が向上したと回答した割合

3.2 倍

アイデンティティソリューションが脅威を軽減するために役立っていると回答した割合

Okta のアイデンティティ成熟モデルは、自社のアイデンティティ能力の現状と有効性を評価し、改善計画を策定し、成功や価値を継続的に測定するためのフレームワークです。アイデンティティ環境の成熟度と、成熟度の向上がビジネス成果の達成とさらなる価値の実現にどのように役立つかを理解すれば、労力と投資を最も集中させる方法が見えてきます。

Okta は、Okta を導入している数千のお客様組織で観察されたパターンとベストプラクティス集に基づいて、アイデンティティ関連のすべての取り組みと評価基準の両方を示す包括的な成熟度モデルを開発しました。このホワイトペーパーでは、従業員、契約社員、パートナーを含む従業員のアイデンティティと、コンシューマー、サプライヤー、およびその他の構成員を含むカスタマーアイデンティティの成熟度の側面について説明します。Okta の調査とお客様の声はいずれも、アイデンティティの成熟度が進むほど、アイデンティティがビジネスの成功に貢献することが明らかになっています。

アイデンティティの成熟度と成功の評価

この取り組みで最初のステップとなるのは、アイデンティティに関する自社の既存のアプローチを徹底的かつ現実的に評価することです。Okta による評価では、運用の俊敏性、エンドユーザーエクスペリエンス、セキュリティとコンプライアンスの 3 つのカテゴリの視点を通してアイデンティティを調査しています。アイデンティティを成熟させるときには、その努力がビジネス成果にどのように貢献しているかを考える必要があります。アイデンティティの 5 つの成熟度カテゴリごとに、表 1 に示す主要業績評価指標（KPI）を継続的に測定してビジネス成果にマッピングすることで、進捗状況を把握し、組織からの賛同をさらに得ることが可能になります。

これら 3 つのカテゴリに加えて、各ステージでは、組織全体のアイデンティティ戦略を定義、改良、実装、評価するためのアクションが提案されます。

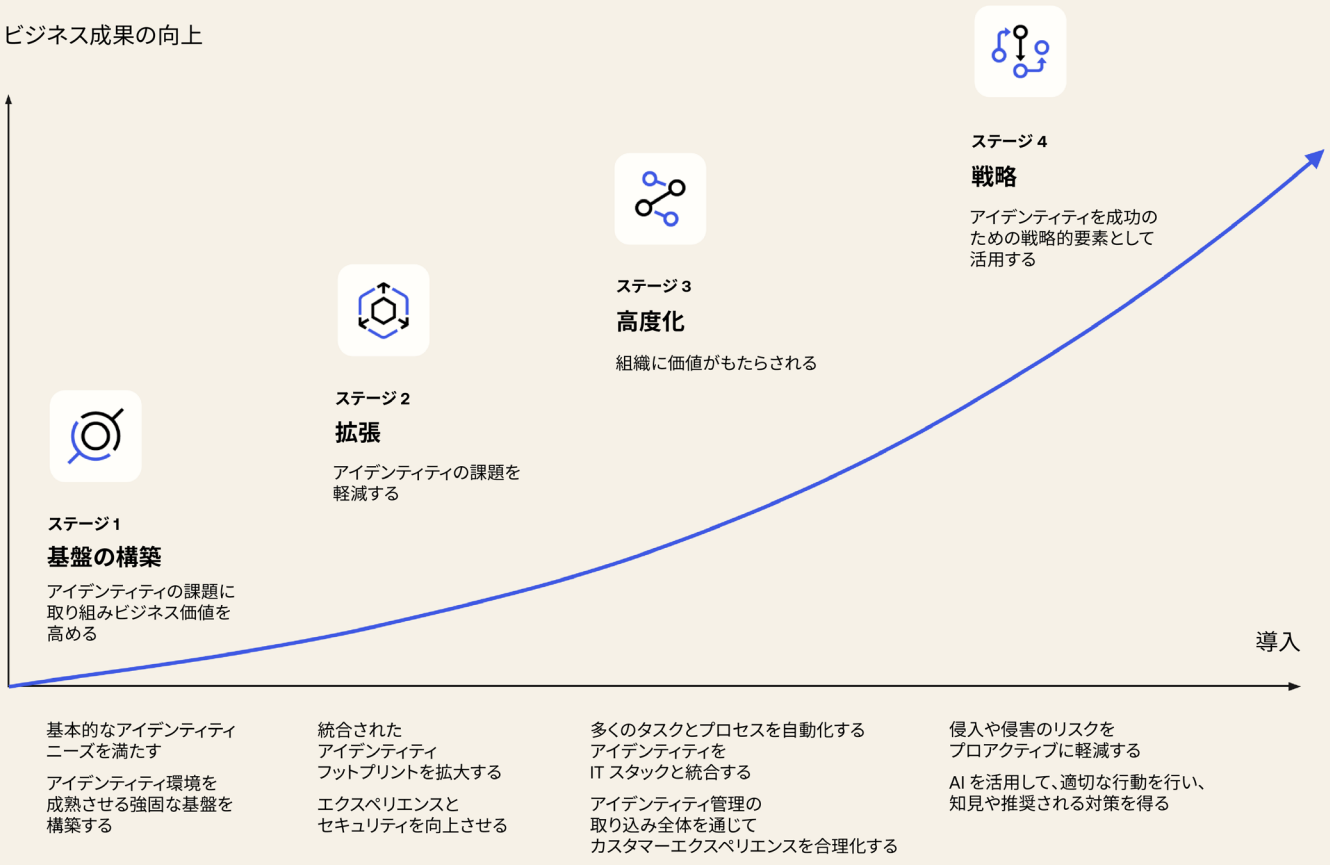
[4] アイデンティティ管理に対する成熟したアプローチの利点、Okta の委託によって Enterprise Strategy Group が実施した調査

カテゴリ	能力の説明	アイデンティティ管理の成功を評価する測定基準	ビジネス成果への貢献
運用の俊敏性	**アイデンティティ関連のサービスとフローの開発、展開、管理** • 新しいデジタルプロパティやアプリケーションにアイデンティティを統合する • 従業員のライフサイクル管理 • 新しいアイデンティティ機能や拡張機能を展開する • 顧客に新しいサービスを迅速に展開する • 需要の変化に合わせて簡単かつ迅速に拡張する	• アイデンティティ管理とサポートに特化した IT 担当の従業員の勤務時間 • アプリケーションの導入と展開の時間 • アイデンティティインフラストラクチャの維持に費やすコストや時間 • アクセスの問題やアプリケーションのリクエストに関連するヘルプデスクチケットの数 • ヘルプデスクがアイデンティティの問題を解決する時間 • 顧客向けのアプリケーションを市場に投入するまでの時間	コストを削減し、効率性を向上させる • より少ない労力でアイデンティティを構築および維持する • M&A を簡素化し、価値実現までの時間を短縮する 収益の増加 • 市場投入を加速する
エンドユーザーエクスペリエンス	**ユーザーに寄り添った効果的で利便性の高いユーザーエクスペリエンスを提供する** 全ユーザー： • デジタルプロパティとチャネル全体で一貫性のある信頼性の高いエクスペリエンスを提供する 従業員： • シームレスなリモートアクセス • 入社初日からアプリケーションを利用可能にする • 依頼者とレビュアーのための効率的なセルフサービス 顧客： • 登録やサインインなどで摩擦が少ないエクスペリエンスを実現する • セルフサービス • パーソナライゼーション	• 従業員満足度（eSAT）スコア • カスタマーエクスペリエンスの測定基準（NPS、CSAT など） • ユーザーがログインしたり、ステップアップ認証プロンプトに応答したりした時間 • 従業員が新しいアプリケーションへのアクセスを待機した時間、またはオンボーディングに費やした時間 • 登録およびログイン時の顧客離脱率 • 顧客のコンバージョン率（アクセスしてアカウントを登録する） • 計画外のダウンタイムの月間発生時間（分）	効率の向上 • エンドユーザーのアクセスを合理化する 収益の増加 • サインアップとログイン時のコンバージョン率をアップする • カスタマーエクスペリエンスをパーソナライズする • シームレスなオムニチャネルエクスペリエンスを創り出す • 大企業の顧客のオンボーディングを簡素化する
セキュリティとコンプライアンス	**脅威をプロアクティブに軽減および修復し、最小権限の原則を維持し、法規制の遵守をサポートする** • 従業員と顧客のアクセスを保護する • アイデンティティの攻撃対象領域を縮小する • アイデンティティガバナンスの取り組みをサポートする • 特権アクセスを管理する • ゼロトラストの実践をサポートする • プライバシー要件をサポートする • アイデンティティ詐欺から自社を保護する	• アイデンティティ関連のセキュリティインシデントの数 • アイデンティティ関連のセキュリティインシデントと侵害を検出して対応するための時間とコスト • 監査およびコンプライアンス関連のレポート作成にかかる時間とコスト • 従業員向けの高度な認証を採用する • アカウント乗っ取り攻撃（ATO）のインシデント数	コストを削減し、効率性を向上させる • ガバナンスとコンプライアンスを簡素化する • ソフトウェア支出を最適化する • 収益の増加 • エクスペリエンスに影響を及ぼすことなく顧客の信頼性を高める セキュリティの強化 • アイデンティティの脅威をプロアクティブに軽減する • フィッシング攻撃を阻止する • コンシューマーの信頼を得る

各ステージにおけるアイデンティティ管理の計画

Oktaのアイデンティティ成熟度モデルには4つの段階的なステージがあります。各ステージでは、アイデンティティに関連するさまざまな能力の項目が設定されています。これらの能力を使用してビジネスの成果を達成し、組織の価値を高める方法を以下に説明します。各ステージでは、組織が直面する一般的な課題について概説します。また、これらの課題を解決し、次の成熟度レベルに進むためのステップに関するガイダンスと期待されるメリットを説明します。各ステージで、組織全体のアイデンティティ戦略を構築、実装、評価するためのアクションについて提案します。あらゆる企業にそのまま適合できるアイデンティティ管理のアプローチは存在しませんが、アイデンティティ態勢を進化させることを検討しているあらゆる企業は、このアプローチによるガイダンスを柔軟に活用することができます。

アイデンティティ成熟度モデル



ステージ1 - 基盤の構築

各機能の集合体としてではなく、アイデンティティ管理を総合的に捉える

アイデンティティ成熟度の最も初期の段階では、以下の取り組みを行うことができます。

- デジタルサービスやオンラインポータルを顧客に拡張するプロセスを開始する
- 従業員とパートナーのアイデンティティソリューションが連携されていないために発生する非効率性と攻撃対象領域の広がりに対応する

アイデンティティ戦略が定義されていなければ、開発者はオンプレミスまたは自社開発のアイデンティティサービスの構築と維持に膨大な時間とリソースを費やすことになります。合併と買収（M&A）、クラウドの拡大、および残存するレガシーアプリケーションによって、従業員のアイデンティティは、いくつものストアとシステムに断片化されています。このような状況では、ユーザーエクスペリエンスの低下を招くことになります。顧客は基本的なサインアップを何度も行う必要があり、その方法もアクセスする対象によって異なります。フェデレーションが制限されており、複数のパスワードを使用しなければならない場合、従業員の生産性に影響が及びます。アイデンティティの信頼性と可用性を確保しなければなりませんが、自動化が最小限あるいはまったく自動化されていないこともあります。他のシステムとの統合も限定されているか、複雑な操作が求められるため、管理者による膨大な手動の作業が必要となっています。アイデンティティが無秩序に増加し、十分に可視化できなければ、セキュリティリスクが増大し、アイデンティティセキュリティの問題が発生してから対応に追われることになります。

このステージでは、顧客を単一のポータルにオンボーディングしたり、いくつかのアイデンティティセキュリティコントロールを実装したりするなど、重要なアイデンティティのニーズを満たすことに重点を置きながら、強力で信頼性の高い基盤を作成し、成熟させていきます。

このステージで取り入れるべき戦略手順：

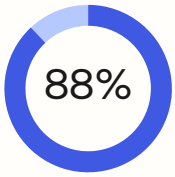
- 組織が使用しているオンプレミスアプリとクラウドアプリのインベントリを作成する
- 顧客と従業員のアイデンティティプログラムを、ビジネスとガバナンスの共通の目標に合わせて調整することを検討する

自社開発のカスタマーアイデンティティの開発・運用が市場投入までのスピードに与える影響 [5]

3 番目

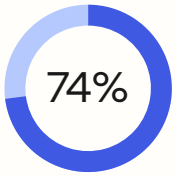
構築と維持に最も多くの時間がかかるアプリケーション

認証は、自社開発の際に 3 番目に多くの時間を要するアプリケーションである



認証にサードパーティSaaSを利用することで、過去1年間で市場投入までの時間が短縮したと報告した組織の割合

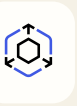
比較



認証を自社構築したことで、過去 1 年間で市場投入までの時間が短縮したと報告した組織の割合

[5] 開発チームの SaaS 調達状況レポート、Okta の委託によって SD Times が実施した調査

カテゴリ	アイデンティティの課題	実行するアクション	ビジネスのメリット
運用の俊敏性	• オンプレミス、自社開発、断片化しているアイデンティティサービスを構築して維持することは困難であり、管理者と開発者が多くの時間を費やすことになる	• 統合型のユーザーディレクトリを実装して、レガシーディレクトリと記録システム全体でユーザーリポジトリを統合および同期する • ユーザーライフサイクルに対応する基本的なアイデンティティ管理 UI を実装する	IT 部門の時間の削減 • ユーザーストアを維持および同期する • ユーザー / グループアクセスを管理する
エンドユーザーエクスペリエンス	• 信頼性 / 可用性の問題 • ログイン時の摩擦が大きく、ユーザーエクスペリエンスをカスタマイズできない • 部署ごとにアイデンティティソリューションが異なる	• フェイルオーバーや障害回復機能を実装し、99.9% を超える SLA 基準を満たす高可用性（HA）インフラストラクチャを採用する • 基本的な従業員のシングルサインオン（SSO）と認証をクラウドアプリに展開する • いくつかのソーシャル認証オプションがある基本的な顧客向けの SSO を展開し、既存の認証情報を活用する • シンプルなセルフサービス機能（パスワード回復など）を実装する	• アプリケーションの導入とアクセスを迅速にして、従業員の生産性や顧客の利用率を向上させる • 基本的なアカウント管理にセルフサービスオプションを提供し、顧客の摩擦を軽減する
セキュリティとコンプライアンス	• パスワードの無秩序な増加、アプリケーションのアクセスコントロールの可視化の欠如、ユーザーストアのサイロ化、ポリシーの適用の欠如などによるセキュリティリスク	• 最新の標準と API の基本アクセスポリシーに準拠した認可サーバーをインストールする • 基本的な暗号化とハッシュによりアイデンティティデータを保護する • 最新のアプリとレガシーアプリをサポートするための、RADIUS、LDAP 認証を含めた従業員の多要素認証（MFA）を確立する • ユーザーグループのニーズとネットワークゾーンを反映した、従業員のアクセスポリシーを作成する	• セキュリティ態勢の強化 • 悪意のある攻撃による顧客アカウントのロックアウトの削減



ステージ2 - 拡張

アイデンティティのフットプリントと機能を拡張し、自動化を開始する

このステージでは、以下の取り組みが進められている場合があります。

- 複数の顧客アプリケーションやポータルを立ち上げており、さらに多くのアプリケーションやポータルの提供に向けて取り組んでいる
- 従業員のアイデンティティの統合で一定の成功を収めており、さらに多くのアプリに拡張し、追加のアイデンティティ機能を実装することを検討している

このステージでは、ステージ 1 での成功に基づき、統合したアイデンティティフットプリントを新しいアプリ、サービス、ユースケース、ユーザーに拡大することに重点が置かれます。企業が市場シェアを獲得するために新しいデジタルサービスを提供し、顧客基盤を拡大するときには、消費者と企業の顧客の両方で差別化され信頼できるエクスペリエンスを創り出すことに重点が移ります。

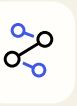
重要なオンプレミスの IT インフラストラクチャと独自のテクノロジーを持つ組織の場合、アイデンティティ機能をこれらのリソースに拡張することで、ユーザーエクスペリエンス、管理プロセス、セキュリティ態勢を向上できます。

フットプリントが拡大する場合、サービス品質に妥協したり、IT 部門が拡張とサポートを常に管理したりしなくても、アイデンティティインフラストラクチャが需要の増加に対応できるようにしなければなりません。また、企業は、拡張によって IT やアプリケーションの所有者に大きな負担が生じないように、一部のアイデンティティプロセスの自動化を開始する必要があります。多くの企業がサイバーセキュリティにゼロトラストアプローチを採用している今が、アイデンティティを活用してゼロトラストの取り組みを促進する好機です。

このステージで取り入れるべき戦略手順：

- IT、テクノロジー、セキュリティの各チーム間でアイデンティティ管理の足並みを揃え、円滑にコミュニケーションし、担当する領域と専門分野を定義する
- アイデンティティギャップを評価して、修復と投資計画を進める

カテゴリ	アイデンティティの課題	実行するアクション	ビジネスのメリット
運用の俊敏性	• 従業員、顧客、パートナーの手動のオンボーディングとオフボーディング • レガシーシステムのアイデンティティリポジトリが断片化されており、保守が困難 • 需要の増加や急増が、パフォーマンスまたは可用性の問題につながる	• オンボーディングとオフボーディング、ダウンストリームアプリのアクセス許可の管理など、ユーザーライフサイクル管理とプロビジョニングの自動化を開始する • 一部のレガシーシステムは、維持やアップグレードが困難、独自のユーザーストアがある、統合機能がないあるいは統合が難しい、SSO / フェデレーション機能がないといったデメリットがあるため、これらの利用を最小限に抑制するか、廃止を検討する • SAML OIDC、OAuth2 などの標準を使用してアイデンティティとアプリケーションを統合する • 一部の SDK と API の導入を開始する • インフラストラクチャがサービス品質を損なうことなく、需要の増加や急増に確実に対応できるようにする	削減効果 • アイデンティティインフラストラクチャを維持するための時間とコスト • アクセスの問題に関連するヘルプデスクのチケット • ユーザーストアの維持および同期 • ユーザー / グループアクセスの管理 • 開発者がアイデンティティの拡張に費やす時間 ユーザーのプロビジョニングとプロビジョニング解除の迅速化 M&A プロセスにおける従業員と顧客のアイデンティティの簡素化
エンドユーザーエクスペリエンス	• ログインエクスペリエンスに一貫性がない複数のアプリ/ポータル • 新入社員のオンボーディングの遅延 • オンプレミスの RADIUS サーバーなどによる安全な認証の可用性	• 顧客ログイン統合を、Apple、Google などの他のソーシャルアイデンティティプロバイダーに拡張する • サードパーティのアイデンティティプロバイダーのアイデンティティをすでに利用している顧客、パートナー、および契約社員の SSO フェデレーションをサポートする • 必要な属性の入力のみを求めることで、顧客のサインインと登録の煩雑さを最小限に抑制する • 従業員の SSO をオンプレミスのビジネスクリティカルなアプリケーションに拡張する • 従業員にパスワードレス認証を導入する • より多くのセルフサービス機能を立ち上げる	• サインインと登録のエクスペリエンスを向上してユーザーの摩擦を削減する • 主要なアプリで必須となるアクセス権限を付与し、他のアプリへのアクセスを迅速化することで、従業員の生産性と満足度を向上させる • オンプレミスまたは非冗長構成のサーバーによって中断を減らして信頼性を向上させる
セキュリティとコンプライアンス	• グローバルなアクセスポリシーにより、従業員のアクセスが過度に許容される環境が生まれる • 従業員のMFAが制限されており、セキュリティギャップが生まれる • カスタマーエクスペリエンスの目標がセキュリティの妨げになる	• クラウドとオンプレミスのアプリ全体で従業員のアクセスコントロールを統合する • ロールベースのアクセスコントロール（RBAC）を実装する • 従業員向けの強力な MFA（所有要素または生体認証要素を利用）をパートナーや契約社員、オンプレミスのビジネスクリティカルなアプリ全体に拡張する。または、パスワードレスアクセスを実装する • 顧客向けの MFA（所有要素または生体認証要素を利用）を実装する。またはパスワードレスアクセスを実装する • ゼロトラストに向けた初期段階（ダイナミックアクセスポリシーなど）を開始する • 標準ベースの API ゲートウェイと統合して、消費者認証で一貫性のあるビューを提供する • 監査および監視ツールを一部導入する	• セキュリティ態勢を強化する • 最小権限アクセスの原則の遵守と MFA アクセスコントロール（SOX など）によってコンプライアンスを向上させる • 監査とコンプライアンスレビューの準備にかかる時間とコストを削減する



ステージ3 - 高度化

自動化と統合を促進して、エクスペリエンスを向上させる

この段階の組織は、アイデンティティ管理による大きな価値がもたらされています。このステージでは、以下の取り組みが中心になります。

- カスタマーエクスペリエンスを合理化し、コンバージョンを最適化する
- アイデンティティと広範なテクノロジースタックとの統合を開始して、効率性を向上させる
- プロアクティブなアイデンティティセキュリティを開始する

アイデンティティを他のシステムと統合することで、タスクとプロセスを自動化し、ユーザーと環境をより明確に可視化できます。たとえば、人事システムと緊密に統合することで、ユーザーアイデンティティの作成、オンボーディング、オフボーディング、および従業員のプロビジョニングを自動化でき、従業員の生産性を向上させ、IT 管理の効率を高め、オーバープロビジョニングによるソフトウェアコストとセキュリティリスクを削減できます。カスタマーアイデンティティをマーケティングエンジンやデータエンジンと統合することで、データサイロを統合し、ユーザープロファイルを一元的に把握し、チャネル全体で一貫したブランドエクスペリエンスを実現できます。また、顧客と顧客の好みについて深い知見を得ることができ、パーソナライゼーションが可能になります。また、自動化を推進することで、開発者と IT チームはビジネスを前進させる優先事項に注力できるようになります。

組織の業務とデジタルフットプリントが拡大するにつれて、より巧妙なサイバー攻撃の標的になることが多くなります。また、これらの攻撃に対抗するさまざまなセキュリティツールが登場しています。アイデンティティ脅威検出と対応（ITDR）およびアイデンティティセキュリティ態勢管理（ISPM）ツールは、セキュリティギャップを解消し、脅威への対応を改善するために役立ちます。これらの機能をアイデンティティシステムに統合すれば、アイデンティティリスクの変化を評価し、自動的に対応できます。

このステージで取り入れるべき戦略手順：

多様なチームと協働し、従業員と顧客のアイデンティティ戦略に取り組む

アイデンティティのセキュリティ態勢の正式かつ継続的なプロセスを導入する

アイデンティティ関連の KPI に基づいて測定して意思決定を行う

カテゴリ	アイデンティティの課題	実行するアクション	ビジネスのメリット
運用の俊敏性	• テクノロジーの進歩を活用していない非効率的なビジネスプロセス、遅延やエラーのリスクがある手動の作業 • 開発者に負担をかけずにさまざまなアイデンティティのユースケースを支援することが困難	• 必須のプロビジョニングやアクセス要求など、ほぼすべてのライフサイクル管理プロセスを自動化し、開発者と IT 部門が介入する必要があるケースを最小限に抑える • ビジネスシステムやマーケティングシステムを連携させるためにすぐに利用可能な統合を活用する • ロールまたはジョブが変更された場合の従業員アクセスの再認定を自動化する • さまざまな SDK と API をサポートし、高度なサポートとドキュメントを提供する	時間の削減 • IT とエンジニアリングチームは独自の統合に時間を費やすことができる • IT チームと GRC チームは、再認定と監査の手動による実行に時間を費やすことができる • マネージャーとアプリの所有者は、アクセスのレビューに時間を費やすことができる 新しいビジネスシステムとアプリケーションをより迅速に導入する
エンドユーザーエクスペリエンス	• 摩擦がなく、一貫性があり、シームレスなエクスペリエンスに対する顧客からの期待の高まり • ユーザーやコンテキストを考慮していない厳格なアクセスポリシーの適用やアプリへのアクセスに時間がかかるプロセスによって、従業員アクセスで摩擦が生じている	• 冗長なサーバーとロードバランサーによってレジリエンスを確保する • ユーザーアカウントのリンク / 統合を自動化する • プログレッシブプロファイリングを使用して、時間の経過に伴う顧客属性の変化を取得し、プロファイルを拡充する • すべてのユーザーのタッチポイント（デバイス、アプリ、アカウント）にパスワードレスを実装し、必要に応じてパスキー、ハードウェアまたはソフトウェア認証システムを使用する • アイデンティティプルーフィングとアカウント検証によって顧客のオンボーディングを改善する • 従業員のセルフサービスアクセス要求を有効にする	• シームレスなオムニチャネルのカスタマーエクスペリエンスを創造する • 高度なターゲティングとパーソナライゼーションにより、サインアップとログインのコンバージョンを増加する • 自動化したセルフサービスの増加とアクセスの高速化により、従業員の生産性を向上させる • 高度なアカウント検証による詐欺の削減
セキュリティとコンプライアンス	• リモートワーカー、デバイス、ネットワークに関連するリスク • 増大および巧妙化するサイバー脅威の標的にされる	• 安全性の高い従業員向け MFA をコンピューターログインに拡張する • すべてのリソースで従業員にフィッシング耐性のある MFA を適用する • 属性ベースのアクセスコントロール（ABAC）を確立する • ITDR および ISPM ツールと統合する • サーバー、Kubernetes クラスタ、データベースなどの重要なインフラストラクチャへの安全なパスワードレスアクセスを実装する • アイデンティティセキュリティ態勢管理を導入して、設定ミスやユーザーへの過剰な権限の付与などのリスクを検出する • 継続的な認証を導入してゼロトラストをサポートし、最新のデータに基づいてアクセスに関する意思決定を行う • アイデンティティリスクに対する自動化されたセキュリティ対応を実装する • ユーザーアクセスの再認定をスケジュールに基づき定期的に行い、最小権限アクセスの原則を適用する • プライバシーおよびコンプライアンスツールと統合して、顧客の好みを追跡する	• 攻撃対象領域を縮小する • アクセスレビューとアクセス要求フローを自動化し、ガバナンスとコンプライアンスを合理化する • フィッシング攻撃を阻止する

ステージ4 - 戦略

アイデンティティを使用して戦略的優位性を獲得する

このステージでは、アイデンティティは、ビジネス成果に大きく貢献し組織を成功に導く戦略的な重要な要素と捉えられるようになっています。多くの場合、組織は強固でグローバルなデジタルプレゼンスを確立しており、従業員を強化して複数のチャネルで顧客との良好な関係を構築するアイデンティティ管理の取り組みを、チームが協力し継続的に改善しています。

このステージでは、以下の取り組みが主に進められています。

- アイデンティティインフラストラクチャを最適化し、業務の効率性と営業利益率を向上させる
- アイデンティティをセキュリティスタックと統合し、脅威をリアルタイムで検出して対応する
- 人工知能（AI）とクラウド環境を活用して、優れたユーザーエクスペリエンスを推進し、アイデンティティセキュリティをプロアクティブに改善する

アイデンティティがテクノロジスタックに完全に統合されると、インフラストラクチャ全体でデータを収集、正規化、相関付けることができます。アイデンティティは、リソースへのアクセスを管理するための主要なコントロールプレーンになり、あらゆるサイバーセキュリティ戦略の重要な要素になります。GRC の観点では、アイデンティティを統合することで、組織内の特定のデジタルリソースにアクセスでき、許可が付与されるユーザーとデバイスの可視化ときめ細かなアクセスコントロールが可能になり、プライバシーに関する顧客の好みを適切に追跡できるようになります。アイデンティティの自動化を進め、AI による知見と推奨事項を組み合わせることで、組織は変化する顧客の期待、ビジネス要件、規制要件、脅威の状況にこれまで以上に簡単かつ迅速に適応できます。

このステージで取り入れるべき戦略的なアクション：

成熟したガバナンスと運用手法を取り入れて、ビジネスニーズを満たし、ビジネス価値をもたらすようにアイデンティティ管理を継続的かつ着実に進める

カテゴリ	アイデンティティの課題	実行するアクション	ビジネスのメリット
運用の俊敏性	• クラウド、オンプレミス、ハイブリッドクラウド環境全体でアイデンティティを統一的に把握することが困難 • 変化する市場のニーズ、ユーザーパターン、規制などに適応することが困難	• ユーザー、アプリケーション、およびエンタイトルメント全体ですべてのアイデンティティデータを一元的に管理する • ポリシー、ユーザーライフサイクル管理、アイデンティティ関連の運用と脅威対策ワークフローを完全に自動化する • AI を活用して、アイデンティティセキュリティとガバナンスを強化し、ユーザーエクスペリエンスを向上し、構成と開発を容易にする	• IT 担当者、管理者、開発者の効率性を向上して、製品やサービスの市場投入を迅速化できる
エンドユーザーエクスペリエンス	• デバイスやチャネルによってカスタマーエクスペリエンスが異なる • ターゲティングとセキュリティのために顧客の行動を把握することが困難	• チャネル全体で顧客アクセスエクスペリエンスをカスタマイズおよび拡張可能にする • 顧客が登録およびログインする時にコンテキストに応じた質問を行い、ゼロパーティデータを取得する	• シームレスなオムニチャネルエクスペリエンスを創出できる • ゼロパーティデータを統合してハイパーパーソナライゼーションを実現できる
セキュリティとコンプライアンス	• 従来型のスタンディング特権がアプリケーションとインフラストラクチャ全体にわたって存在する • クラウドまたはその他のアイデンティティの設定ミス • セキュリティイベントへの迅速な対応	• ゼロスタンディング特権の環境を確立し、特権アクセスが必要なリソースについて共有される認証情報を安全なボールトで管理する • アイデンティティセキュリティを統合する(IAM、PAM、IGA) • サードパーティのセキュリティツールからシグナルを取り込み、脅威に関する有用な知見を得る • リスクベースのきめ細かな認証を展開する • リスクシグナルに基づくユーザーアクセスの再認定を自動化する • 需要の急増に合わせてインフラストラクチャを動的に拡張できるようにし、信頼性とセキュリティに関連する規制を遵守していることを実証する	• アイデンティティの脅威をプロアクティブに軽減して修復できる • 脅威の検出と対応にかかる時間を短縮できる • カスタマーエクスペリエンスを犠牲にすることなく信頼性を向上できる • 高度なセキュリティと不正防止機能によって消費者の信頼を獲得できる

アイデンティティ管理によってビジネス価値を高める

アイデンティティ成熟度のどの段階に自社が達しているかを把握すれば、次のステップを適切に評価し、成功に近づいているかを監視できます。アイデンティティがどのように革新的なデジタルエクスペリエンスを支援し、セキュリティ脅威から組織を保護し、ビジネスの成長にどのように役立つかを理解することで、競合他社の一歩先を行くことができます。

Okta は、アイデンティティ管理を主導する独立したパートナーとして、世界中のさまざまな業界の企業や組織と協力して、デジタルトランスフォーメーションを推進し、アクセス、認証、自動化の目標を確実に達成できるように支援しています。Okta は、アイデンティティとセキュリティの状況を監視し、イノベーションを実現して、組織の時間とリソースを解放し、主要な製品とサービスに注力できるようにします。

アイデンティティに関する用語集については、https://www.okta.com/resources/identity-and-access-management-glossary/ を参照してください。