ホワイトペーパー

ワークフォースアイデンティティの成熟に向けた包括的ガイド

4 つのステージを通じて
成熟レベルを高める

あらゆる場面でビジネスを支援する IAM

今日の IT リーダーは、ビジネスをより迅速に進め、優先事項を実行し、持続的な成長を促進するために、常に新しいテクノロジーを把握していなければなりません。クラウドファースト戦略は、より高い柔軟性を提供することから、こうした戦略的目標を達成する上での鍵となります。これが特に当てはまるのが、分散して活動する「ダイナミックワークフォース」であり、その中にはデータ規制やプライバシーを最大の関心事とする請負業者やビジネスパートナーも含まれます。今日のデジタルファーストのワークフォースは、安全で摩擦のないエクスペリエンスを求めており、それを実現する組織でなければ競争を勝ち抜くことはできません。

このような状況において、アイデンティティ / アクセス管理（IAM）は、現代のビジネスにとって必要不可欠であると同時に、あらゆる場面で力を発揮するための推進要素となっています。IAM によって、重要なツールやリソースへのシームレスで安全なアクセスが可能になり、どこからでも作業できるようになります。また、ダイナミックワークフォースを舞台裏でサポートする IT チームは、ユーザー管理の簡素化、主要なアイデンティティプロセスの自動化、アイデンティティを利用したサイバー攻撃からの保護に IAM を役立てています。

アイデンティティに対しては、堅牢で包括的なアプローチで臨まなければならないことは明らかです。しかし、アイデンティティの成熟には、セキュリティ、効率性、拡張性などの課題を解決する必要があり、これらの取り組みの進捗にはばらつきがあります。多くの組織は、アイデンティティの導入と戦略を成功させるために邁進しています。ただし、直線的な道を単純に進むことができるケースはほとんどありません。

今求められているワークフォースアイデンティティへの道のり

持続可能なアイデンティティファブリックは、ユーザーエクスペリエンスとセキュリティの間で効果的なバランスをとる必要があります。しかし、このようなファブリックを確立するには、適切なツール、スキル、アプローチが求められ、これらをチームが備えているとは限りません。皆様のチームが IAM を成熟させる最善の方法を判断するため、ここでは数千に上る Okta 導入組織で最も成功しているプラクティスとパターンをまとめました。

本書は、カスタマーアイデンティティの成熟に向けたガイドの姉妹版として、従業員、請負業者、パートナーといったワークフォースユーザー向けに、従来の IAM 戦略をいかに進化させるべきかに焦点を当てています。以下に、Okta の包括的な成熟モデルを紹介し、評価基準と、アイデンティティのあらゆるニーズに対応する最適な道のりを解説します。このガイダンスを読み進めることで、アイデンティティ管理を簡素化し、アイデンティティ態勢を強化するための具体的な手順を理解できます。新しいデジタルエクスペリエンスの提供、セキュリティ脅威からの保護、最新の IT インフラストラクチャによる運用効率の向上に向けて、どのように前進すべきかが明らかになります。

アイデンティティ成熟モデルとは？

Okta のアイデンティティ成熟モデル（IMM）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、各ステージで成功と価値を継続的に測定するためのフレームワークです。IAM の状況を理解し、組織の長期的なビジネス目標（現状と今後の方向性）を達成するために必要なアイデンティティとセキュリティの能力を評価することで、労力と投資を最も効果的に集中させる方法を理解できます。これによって、アイデンティティとセキュリティの新しい要件、そしてエンドユーザーの要求の変化に応じたビジネスの拡張が容易になります。

アイデンティティの成熟度に関連する 5 つの評価領域

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主要な能力 / 課題を含め、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。この評価では、俊敏性、エクスペリエンス、セキュリティ、信頼性、戦略の 5 つの重要カテゴリを検証します。

俊敏性
アイデンティティ関連のサービスとフローを展開・管理・開発する能力

エクスペリエンス
効果的で望ましく、利便性に優れたエクスペリエンスをエンドユーザーに提供する能力

セキュリティ
セキュリティのリスクやインシデントを積極的かつ効果的に緩和・修復する能力

信頼性
弾力性があり、パフォーマンスが高く、将来にも対応するアイデンティティサービスを、規模を問わず提供する能力

戦略
イノベーションに焦点を当てて、包括的かつインテリジェントな計画を立案し、提供する能力

ワークフォースアイデンティティの成熟度については、以下の項目を評価する必要があります。

1. アイデンティティ関連のサービスとフローを展開・管理する**俊敏性**

- 自社のアイデンティティサービスは、IT スタック全体（クラウドベースの SaaS アプリケーションやインフラストラクチャストラクチャから、レガシーシステム / オンプレミスのリソースまで）で最新の IAM を提供しているか？
- セキュリティに妥協することなく、ビジネスが求めるペースに合わせて、カスタムまたはベストオブブリードのテクノロジーの導入を加速できるか？
- 自社の管理者は、プロファイルを管理し、すべてのアイデンティティのライフサイクルを管理するための直感的で一元的なコンソールを使用しているか？
- アイデンティティプロバイダーは、IT スタックを容易に拡張・カスタマイズするための自動化とオーケストレーションを提供しているか？

2. シームレスで利便性に優れた**従業員エクスペリエンス**の提供

- 従業員は、アプリケーションの要求や認証関連の問題解決をセルフサービスで実行できるか？
- シームレスで安全なリモートアクセスを提供することで、ハイブリッドな業務環境全体での生産性向上を支援しているか？
- 新入社員に必須のアプリケーションを、自動プロビジョニングによって入社初日までに提供しているか？
- 従業員の生産性と俊敏性を高めるため、アイデンティティベースのプロセスをコーディングなしで自動化できるか？

3. **セキュリティ**のリスクやインシデントの緩和・修復

- 自社の IAM ソリューションは、従業員だけでなく、ビジネスパートナー（サプライヤー、再販業者、販売業者、子会社やフランチャイズなどの関連組織）の情報サプライチェーン全体に対して、リソースへの安全なアクセスを可能にしているか？
- 異常な状況でのアクセスを防止するため、行動パターンに関するコンテキストに応じた洞察とインテリジェンスをポリシーに組み込んでいるか？
- アイデンティティ関連のセキュリティインシデントを迅速に検出し、解決できるか？また、これらのプロセスに関するセキュリティ SLA（サービスレベル合意）を確立済みか？
- 攻撃対象領域を減らし、脅威を緩和するために、アイデンティティに基づくゼロトラストのセキュリティモデルを導入済みか？

4. パフォーマンスが高く**信頼できる**アイデンティティサービスを、規模を問わず提供する能力

- 特に収益を生み出すビジネス部門において、従業員の生産性に影響を与えるサービス障害が発生することがあるか？
- 自社のアイデンティティサービスは、不測の事態でも中断せずに需要の変動に対応できるか？
- ダイナミックワークフォースの成長に合わせてアイデンティティサービスを拡張できるか？

5. アイデンティティの将来のニーズとイノベーションに向けた**戦略的**な焦点とビジョン

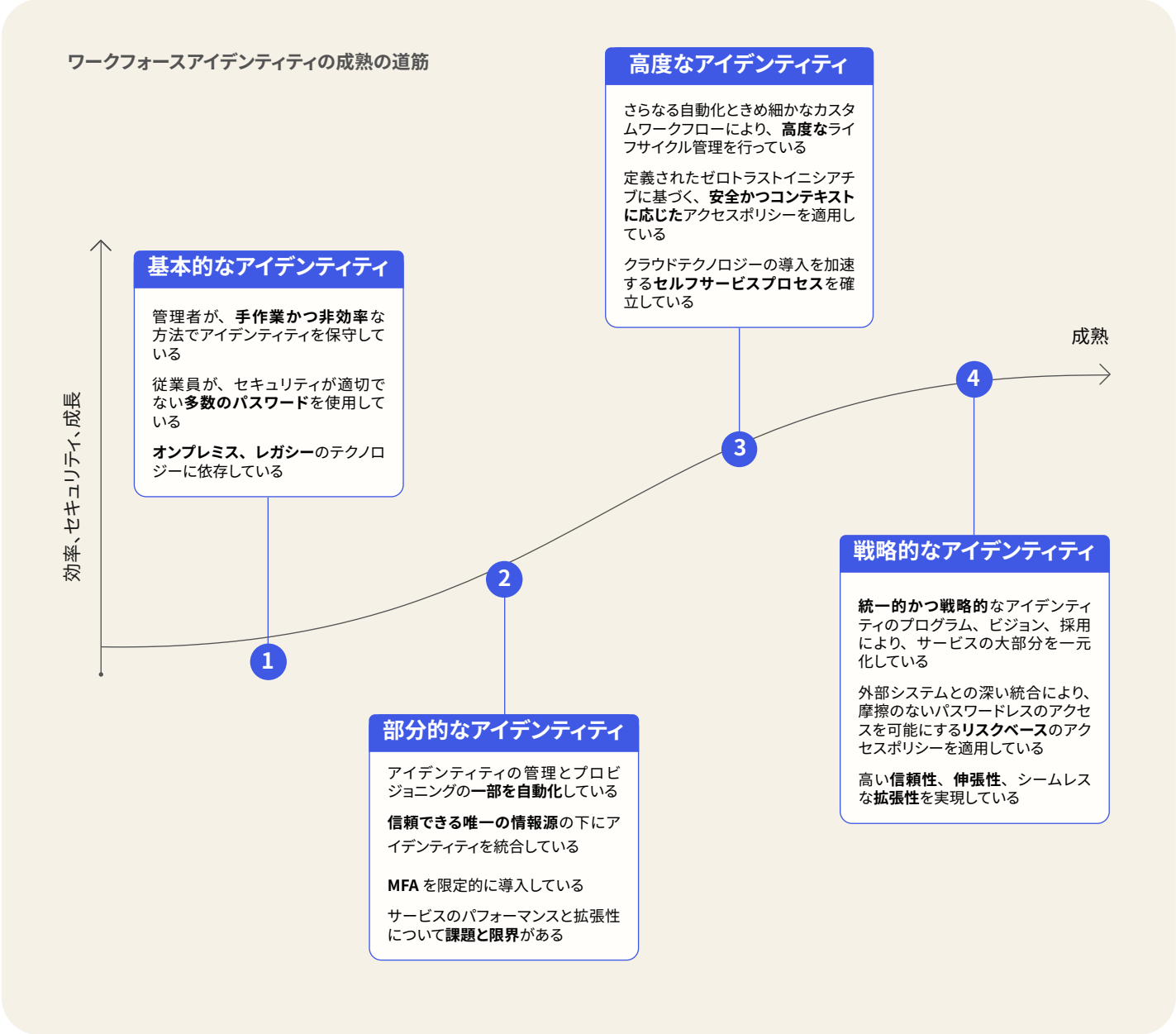
- 自社のすべての地域やビジネス部門で、足並みが揃った統一的なアイデンティティ戦略を採用しているか？
- ビジネスニーズを満たすためにアイデンティティサービスをどのように進化させるかについて、明確かつ包括的なビジョンを持っているか？
- それは、十分な資金提供を受け、経営幹部の賛同を得た、複数年のビジョンか？
- アイデンティティサービスの投資収益率（ROI）、総所有コスト（TCO）、ビジネス上の利点を積極的に測定し、最大化できるか？

ワークフォースアイデンティティの成熟に向けて道筋を定める

ワークフォースアイデンティティ能力の成熟度について現状を評価したら、次のステップとして、Okta が提唱するアイデンティティ成熟モデル（IMM）の主要 4 ステージを理解しましょう。

- 基本的なアイデンティティ
- 部分的なアイデンティティ
- 高度なアイデンティティ
- 戦略的なアイデンティティ

IAM の高度化に段階的に取り組むことで、組織にとってより大きな価値が引き出されます。



Okta のモデルは、「手作業」の「非効率」で「断片的」なアイデンティティ機能を、「自動化」された「インテリジェント」で「拡張可能」な機能へと組織を進化させるための出発点として、伸張可能なアイデンティティ戦略を立ち上げるためのガイダンスを提供します。ただし、必要とされる成熟レベルはビジネスごとに異なる可能性があるため、すべての組織がステージ 4 を目指すわけではない点に留意してください。

IAM の成功を評価する主な指標

組織が 4 つの段階を経て成熟度を高めていく中で、ビジネスの主要な成果に向けていかに投資すべきかを考えることが重要です。アイデンティティの 5 つの成熟度カテゴリごとに、以下のような主要業績評価指標（KPI）を継続的に測定することで、進捗状況を把握できます。

俊敏性の KPI

アイデンティティ管理に費やす FTE（フルタイム当量）時間、アプリの採用と展開に要する時間、レガシーインフラストラクチャの保守にかかるコストと時間

エクスペリエンスの KPI

アプリへのアクセスやリクエストに関連するチケット量、従業員満足度スコア、認証、新規アプリへのアクセス、新規ユーザーのオンボーディングに費やした時間

セキュリティの KPI

アイデンティティ関連のセキュリティ問題の数、検知（および対応）に要する時間、セキュリティ侵害のコスト、監査と報告に費やす時間、従業員による高度な認証の導入率

信頼性の KPI

計画外ダウンタイムの月平均発生時間とコスト、生産性の低下や従業員からの苦情につながったインシデントの数

戦略の KPI

アイデンティティ関連テクノロジーへの年間投資額、十分な資金提供を受けたアイデンティティプログラムの期間、アイデンティティサービスの ROI と TCO

IAM ソリューションの ROI を計算する方法については、www.okta.com/roi/ をご覧ください。

成熟ステージ別ガイド

このセクションでは、Okta コミュニティ全体で観察された一般的な目標や課題を含め、各成熟ステージの概要を説明します。また、各ステージでアイデンティティ能力を向上させるための、Okta が推奨する主な方法を紹介します。こうした方法は、業務効率の改善、セキュリティギャップの解消、さらに大きな価値の提供を実現する上で役立ちます。

ステージ 1：基本的なアイデンティティ

目標と課題

多くの企業では、バラバラなアイデンティティストアが次第に蓄積され、オンプレミスとクラウドのアプリケーションが異種混在する断片的なアイデンティティを IT チームが管理しています。IT 以外の部門が独自のビジネスニーズのためにアプリやツールを取得・活用している場合には、単一の IAM プログラムの下でソリューションを追跡・統合する必要があるため、状況がさらに複雑化します。IT 組織は、広範なビジネス戦略にアイデンティティをどのように適合させるべきかについて、かならずしも深い専門知識や洞察を持ち合わせているわけではありません。このため、基本的なアイデンティティサービスであっても、構築と保守に多大な時間とリソースを投じることになる場合があります。

IAM の成熟に向けた初期の段階では、ビジネスはユーザーやアプリケーションを管理するため、主として手作業のプロセスと必要最低限の能力に依存する傾向があります。このステージで、従業員に加えて、より広範な意味でのワークフォースのメンバーを対象とした管理を強化しようとする場合、一般的に以下のような目標を掲げます。

- 孤立アカウントや管理されていないロール / グループ / アプリを最小限に削減
- ハイブリッドワークフォース向けにリモートアクセスを増やす
- ユーザーが記憶する必要のある多数の（おそらく安全でない）パスワードを減らす
- パスワードのリセットやアカウントのロックアウトへの対応に関して、IT の負担を軽減する
- セキュリティの脆弱性に対処する

Okta が推奨するステップと能力

このステージにある組織には、次の成熟レベルに進むために、以下のワークフォースアイデンティティソリューション / 能力を導入することをお勧めします。

俊敏性

Active Directory（AD）ドメイン、LDAP サーバー、HR システムなど、レガシーのディレクトリや記録システム全体で、ユーザーリポジトリを統合・同期（カスタムスクリプトを使用）

ユーザーとポリシー管理のための基本的なアイデンティティ管理ユーザーインターフェイス（UI）。ただし、IT チームの手作業が依然として多い場合もある

エクスペリエンス

基本的なシングルサインオン（SSO）の導入とエンドユーザー認証。AD/LDAP ユーザーの委任認証サポートや、すべてのユーザー（特権アカウントを含む）に対する単一の多要素認証（MFA）ポリシーを含む場合がある

資格情報のリセットやパスワードのリカバリなど、基本的なセルフサービス機能。ただし、ヘルプデスクによる頻繁なサポートが必要になる場合がある

セキュリティ

OpenID Connect（OIDC）、Open Authorization（OAuth）2.0、Security Assertion Markup Language（SAML）といった最新の標準に準拠する認可サーバー

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、基本的なロールベースのアクセスポリシー

信頼性

基本的な高可用性アーキテクチャ、フェイルオーバー、ディザスタリカバリ能力、SLA 標準などを備えたアイデンティティインフラストラクチャ

戦略

ワークフォースが使用するオンプレミス / クラウドの全アプリを対象とする包括的なインベントリ。これにより、アプリのオーナーシップを明確化し、未知のビジネス IT（シャドウ IT）のリスクを低減する

アイデンティティの改善に向けた予算配分と経営幹部の支持を確保するためのビジネスケース

ステージ 2：部分的なアイデンティティ

目標と課題

ステージ 1 の条件を満たした企業は、一元的な「信頼できる唯一の情報源」と管理プレーンにすべてのアイデンティティを統合する取り組みを進めます。また、SSO と限定的な MFA を導入したことで、パスワードの増大を抑制し、アプリケーションへのアクセスの安全性を高めました。

多くの場合に、IT 管理者の負担軽減が今後の焦点になります。これは、直感的に操作できるアイデンティティ管理ポータルと、手間がかからない一元化されたユーザーライフサイクル管理により、従業員の入社 / 異動 / 離職に関連するタスクを自動化することで実現できます。通常、ステージ 2 の企業は、自動化されたインテリジェントな IAM サービスの多くの利点を理解し始めると同時に、セキュリティのギャップをさらに埋めるべき必要があることを認識します。

Okta が推奨するステップと能力

次の成熟レベルへと進むために、以下のカスタマーアイデンティティソリューション / 能力を導入することをお勧めします。

俊敏性

ユーザーディレクトリの統一、レガシーテクノロジー（AD などのオンプレミスサービス）の廃止

従業員のオンボーディング / オフボーディングと、下流のアプリケーションアクセスのプロビジョニングに関する部分的な自動ライフサイクル管理

エクスペリエンス

サードパーティのアイデンティティプロバイダー（IdP）のサポートなどにより、従業員 / 請負業者 / パートナー向けの SSO 能力を拡張し、アクセスを簡素化

従業員向けセルフサービス機能の運用を拡充して、IT チームの負担を軽減

セキュリティ

2 つ以上の保証要素（SMS、メールなど）を使用し、アプリケーション横断的にアクセスポリシーを適用する MFA。ただし、MFA はデバイス、方法、アプリアクセスでの使用といった面で依然として限定される可能性がある

アプリへのダイナミックアクセスポリシーの適用など、ゼロトラストアーキテクチャに向けた初期のソリューションとステップ

セキュリティ上の不規則性を定期的に評価するための監査 / 監視ツール

信頼性

パフォーマンスと信頼性を大規模にサポートするための、アイデンティティインフラストラクチャの拡張

臨時の投資や手作業の介入を伴うバースト / スパイクへの対応計画

戦略

IAM テクノロジーを活用するビジネス部門間の連携とコミュニケーション。具体的な領域で、オーナーシップと責任を定義する

IAM のギャップと要件を現実的に評価し、改善と投資計画を推進する

ステージ 3：高度なアイデンティティ

目標と課題

このステージの組織は、ダイナミックワークのレベルを高め、リモートやオフィスで働く従業員 / 請負業者 / パートナーをサポート・拡張するための強固な基盤を構築しています。IT チームは、シンプルでシームレスなアクセス（複数のクラウドを含め、主要なアプリケーションやシステムにアクセスするため、各個人に 1 セットの資格情報を使用するなど）を提供する必要があります。さらに、データのセキュリティとプライバシーを保護し、厳格化が進むコンプライアンスと監査の要件を遵守しなければなりません。

ユーザーが誰で、どこから、どのアプリケーションにアクセスしようとしているのか、そして現在のデバイスとネットワークのセキュリティリスクといった豊富なシグナルに基づく、コンテキストに応じたアクセスポリシーによって、セキュリティ態勢を改善し始めます。さまざまなユーザータイプとアクセス権があるため、特権アカウントが引き起こすリスクに対処し、必要に応じて常設の特権を排除することが重要です。

アイデンティティと人事のソースの統合を深め、複雑なライフサイクルタスクを合理化・自動化することなどを通じて、新入社員の生産性を向上させることにも注力します。ステージ 3 の IT チームは、より高度な自動化とプロセスの効率化を導入することで、バックエンドのアイデンティティシステムとインフラストラクチャを強化することを目指します。全体的な目的は、可能な範囲で IT の介入を最小限に減らすことです。これにより、人的エラーの可能性を低減し、ビジネスを前進させるための戦略的優先事項にチームの労力を振り向けることができます。

Okta が推奨するステップと能力

このステージでは、次の成熟レベルに進むために、以下の IAM ソリューション / 能力を導入することをお勧めします。

俊敏性

高度な自動化。ユーザーライフサイクル管理に関するビジネスルールの大部分を体系化し、開発者と IT が手作業で介入する必要性を最小限に抑える

即座に利用可能な人事システムとの統合。より高度な自動化により、ライフサイクルの変化を迅速に把握する

エクスペリエンス
シームレスな新入社員エクスペリエンスのため、主要システム / アプリへのアクセスを入社初日から提供

利用の多いアプリのリクエスト、パスワード管理、MFA の要素変更など、従業員のセルフサービス機能を完備

パスワードレステクノロジーを部分的に採用。リスクの高いログイン試行時にのみユーザーに第 2 要素を求めるアクセスポリシーを通じで強化する

セキュリティ
アダプティブな機能を備えた MFA。さまざまな高保証要素と行動インプットを活用してリスクを割り当て、必要な状況でのみステップアップ認証を実施する

即座に利用可能なサードパーティツール / システムとの統合。セキュリティイベント / シグナルを捕捉・管理する

ゼロトラストイニシアチブの定義、最小特権を維持するコンテキストベースの個別ポリシー、API/ サーバーへの安全なアクセス拡張

信頼性
冗長サーバー、ロードバランサー、高可用性インフラストラクチャにより、サービスの回復力を組み込む

戦略
アイデンティティ態勢のための正式かつ継続的なプロセス、計画、組織的オーナーシップ

アイデンティティ関連の多様な KPI / 指標を追跡・数値化し、測定可能な改善を実証する能力

訓練された専任の IAM 専門家を社内に配置

ステージ 4：戦略的なアイデンティティ

目標と課題

必要とされる成熟レベルはビジネスごとに異なるため、かならずしもすべての組織がステージ 4 に到達する必要があるわけでも、その道を選択するわけでもありません。この段階に到達したビジネスは、一般的にダイナミックワークフォースを受け入れ、チームがどこにいても摩擦なく効率的に作業できるように確保する必要性を認識しています。このレベルでは、組織はアイデンティティを成功の要とみなし、堅牢で持続可能な IAM の実装を達成しています。ステージ 4 は最終的な状態を表すものではなく、漸進的な最適化と改善を続けている状態を反映するものとなります。

この時点で、従業員はユーザーエクスペリエンスとセキュリティの両方を最適化した最新のデジタルアクセスを利用でき、IT 管理者はより戦略的な取り組みに注力できるようになります。組織は、IT とセキュリティに対するクラウドネイティブなアプローチ、包括的なゼロトラストセキュリティ戦略を採用しています。また、ノーコード / ローコードソリューションにより、あらゆるビジネス部門や地域が各々異なる要件に対応するカスタムワークフローを構築できるようになります。

ステージ 4 のビジネスは、最新の豊富な IAM 機能を備えたデジタルワークプレイスツールのイノベーションと強化を続行する必要があります。この段階では、きめ細かなリスクベースのアクセスポリシー、パスワードレス認証、データベース化されたリスク管理といった、さらなる能力強化のための取り組みを優先すべきです。組織のリスク許容度を理解し、データに基づく検討事項を人間には対処できない方法で考慮できる最新のテクノロジーを探す必要があります。

Okta が推奨するステップと能力

このステージでは、アイデンティティの効果を最大限に高めるために、以下の IAM ソリューション / 能力を導入することをお勧めします。

俊敏性

アイデンティティとセキュリティポリシー管理、ユーザーライフサイクル管理、アイデンティティ関連の複雑なビジネスワークフローの完全な自動化

すべてのユーザーと権限を統一的に表示する、一元的された直感的な管理 UI

エクスペリエンス
従業員 / 請負業者 / パートナーのアクセスエクスペリエンスを、デバイス横断的に高度に伸張可能にし、摩擦を排除

強力な MFA 要素を使用したパスワードレスログインを広範に導入

セキュリティ
継続的かつアダプティブな認証と認可のための、リスクベースのきめ細かなアクセス制御

多様なソースからのリスクシグナルを取り込み、分析する機能を備えたインテリジェントな MFA エンジン

インシデント対応とアイデンティティのオーケストレーションをサポートする、完全に自動化されたセキュリティワークフロー

信頼性
不測の高トラフィックイベント時など、需要の急増に対応し、シームレスかつダイナミックに拡張する、回復力のあるインフラストラクチャ

戦略
十分な資金提供を受け、経営幹部の賛同を得た、複数年のアイデンティティプログラム

社内の多様なステークホルダーチームが、入念に設計されたマシンのごとくアイデンティティの戦略とプログラムで協働

ステージ1：基本的なアイデンティティ	ステージ2：部分的なアイデンティティ	ステージ3：高度なアイデンティティ	ステージ4：戦略的なアイデンティティ
目標と課題			
• ユーザーとアプリの管理で手作業から脱却 • パスワードを削減 • 孤立アカウントや管理されていないロール / グループ / アプリを最小限に削減 • ビジネス戦略にアイデンティティをどのように適合させるかを理解	• 「信頼できる唯一の情報源」の下にアイデンティティを統合 • パスワードの増大を抑制 • IT 管理者の負担を軽減 • セキュリティ態勢を改善	• ダイナミックワークフォースのための拡張と効率化 • コンテキストに応じたアクセスポリシーにより、セキュリティ態勢を改善 • 高度な自動化とプロセスの効率化により、IT の介入を最小化	• ユーザーエクスペリエンスとセキュリティを最適化 • 継続的かつインテリジェントな認証と認可を組み込み • アイデンティティプロセスのカスタマイズ作業を簡素化
成熟レベル別の推奨ステップと能力			
俊敏性			
• レガシーのディレクトリや記録システム全体でユーザーリポジトリを統合・同期 • ユーザーとポリシー管理のための基本的なアイデンティティ管理 UI	• 統一的な最新のユーザーディレクトリ • レガシーシステムの廃止 • ユーザーライフサイクル管理とプロビジョニングの部分的な自動化	• 高度なライフサイクル管理と自動化 • 即座に利用可能な人事システムとの統合	• 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ビジネスワークフローを完全に自動化 • 一元化された直感的な管理 UI
エクスペリエンス			
• 基本的な SSO の導入とエンドユーザー認証 • 基本的なセルフサービス機能（パスワード回復など）	• サードパーティ IdP のサポートにより、従業員 / 請負業者 / パートナー向けの SSO 能力を拡張 • セルフサービス機能の運用を拡充	• 新入社員のアクセスを入社初日から提供 • 利用の多いアプリのリクエスト、パスワード管理など、従業員のセルフサービス機能を完備 • コンテキストに応じたアクセスポリシーでパスワードレスを強化	• 従業員 / パートナーのアクセスエクスペリエンスを、デバイス横断的に高度に伸張可能にし、摩擦を排除 • パスワードレスログインの広範な導入
セキュリティ			
• 最新の標準に準拠した認可サーバー • 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、基本的な MFA とロールベースのアクセスポリシー	• アプリケーション横断的にアクセスポリシーを適用し、2 つ以上の保証要素を使用する、MFA の限定的な導入 • 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） • 監査 / 監視ツール	• アダプティブ MFA • 最小権限、API とサーバーへの安全なアクセス • 即座に利用可能なサードパーティツールとの統合により、セキュリティイベントを捕捉 • ゼロトラストイニシアチブの定義	• 多様なソースからのリスクシグナルを分析する機能を備えたインテリジェントな MFA • インシデント対応とオーケストレーションをサポートする完全に自動化されたプロセス • リスクベースのきめ細かなアクセス制御
信頼性			
• 基本的な高可用性アーキテクチャ、フェイルオーバー、ディザスタリカバリ能力、SLA 標準など	• 臨時の投資や手作業の介入を伴うバースト / スパイクへの対応計画	• 冗長サーバー、ロードバランサー、高可用性インフラストラクチャ	• シームレスかつダイナミックに拡張する、回復力のあるインフラストラクチャ
戦略			
• オンプレミス / クラウドの全アプリを対象とする包括的なインベントリ • アイデンティティ向上のために予算配分と経営幹部の支持を確保するためのビジネスケース	• ビジネス部門間の連携とコミュニケーション • ギャップと要件を評価し、投資計画を推進	• アイデンティティ態勢を評価するための正式かつ継続的なプロセス • アイデンティティ関連の KPI • 社内のアイデンティティ専門家	• 経営幹部の賛同を得た、複数年のアイデンティティプログラム • 多様なステークホルダーが、アイデンティティ戦略で協働

アイデンティティの成熟がもたらすメリット

この IAM 成熟モデルは、以下のような価値あるビジネス成果の実現を促進します。

- **アイデンティティ管理の有効性と ROI を向上：**各成熟ステージが前のステージよりも高い価値を提供します。
- **従業員エクスペリエンスを向上：**アイデンティティの一元管理とプロセス自動化のための直感的なツールにより、IT を効率化します。
- **収益増加を加速：**新たなビジネス機会を増やすクラウドテクノロジーの迅速な導入により、従業員の生産性とビジネスの俊敏性を高めます。
- **ブランドの評判を保護：**セキュリティリスクを緩和し、インシデント発生時には迅速な回復を可能にします。
- **将来を見据え、一貫したアイデンティティ戦略：**ビジネスとともに成長し、成功に導きます。

IAM の究極のメリット：ビジネスの俊敏性

Okta のワークフォースアイデンティティ成熟モデルは、ビジネスと IT の重要な機会に関する洞察を提供し、組織はこれを差別化に役立てることができます。成熟の各レベルでは、進捗を振り返り、次のステップを検討し、デジタルエクスペリエンスの革新、セキュリティ強化、ビジネスの成長に向けて成功を追跡することが重要となります。

成熟度ガイドの次のエディションでは、ワークフォースアイデンティティ態勢を成熟させることが、企業の価値を生み出す実際のビジネス能力にどのように役立つかを紹介します。

Okta のような業界をリードするソリューションは、IT の時間とリソースを解放することで、この価値を引き出します。アイデンティティとセキュリティのリスクと要件については、一歩先の取り組みを Okta に任せ、お客様のチームは最も有意義な作業に専念できます。Okta の実績ある IAM ソリューションは、ワークフォースアイデンティティの成熟への歩みを迅速に進めるための支援を提供しています。詳しくは、okta.com/workforce-Identity をご覧ください。