Oktaの アイデンティティ 成熟度モデル

ゼロトラストを通じてセキュリティとコンプライアンスを強化し、エンドユーザーエクスペリエンスを向上させて、アイデンティティで運用の俊敏性を高めるためのロードマップ

リンク

セキュリティを強化 ― さらなる価値も実現

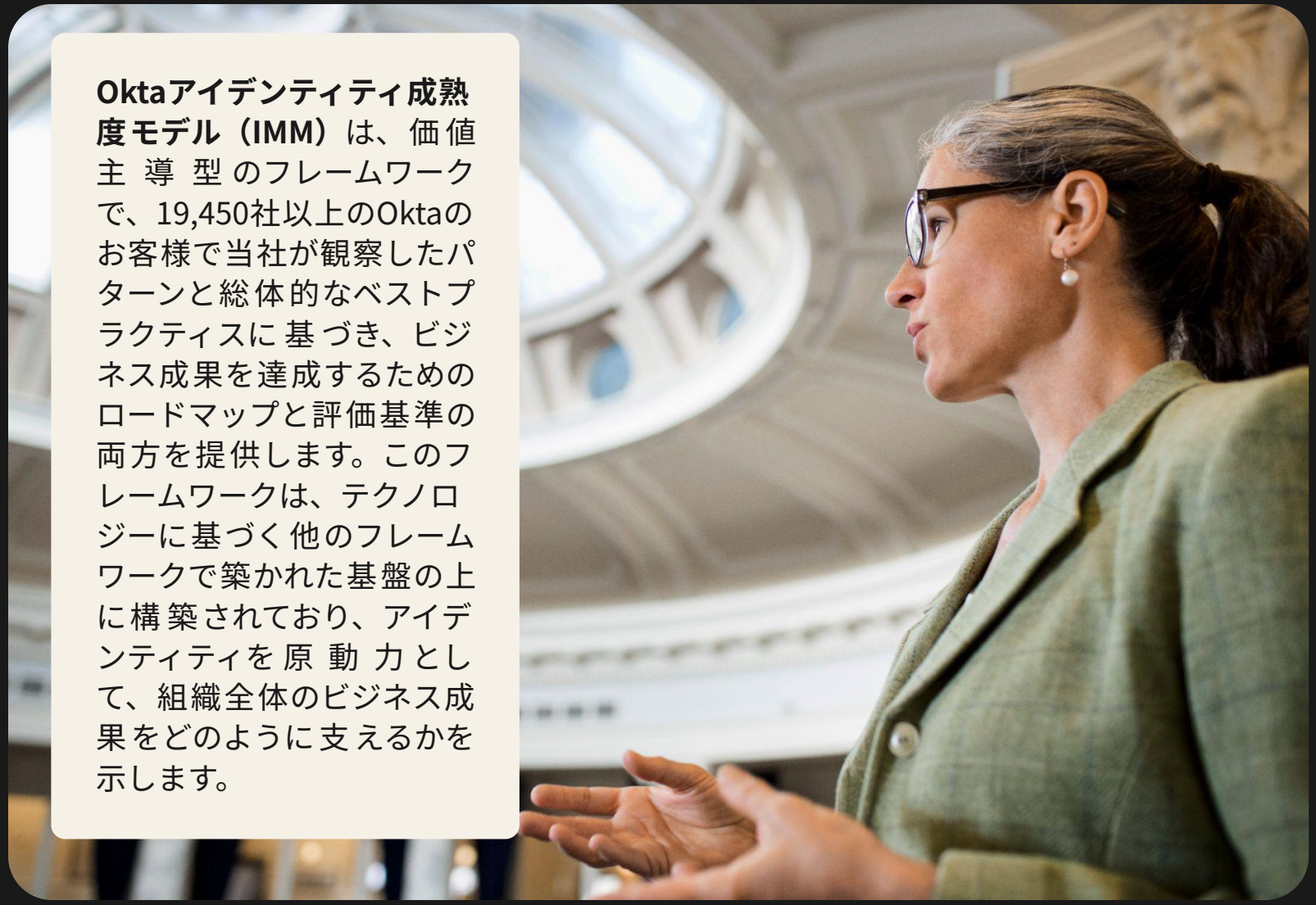
アイデンティティとアクセス 管 理 （IAM）は、かつてはユーザー 名 とパスワードを管理するサービスを指していました。現在ではそれだけにとどまらず、組織が従業員、顧客、パートナーと、場所や時間、使用デバイスを問わずセキュアにやり取りできるように支援する役割を担っています。

アイデンティティが強力な場合

- セキュリティが 強 化され、ガバナンス、リスク、コンプライアンス（GRC）が 簡素化される
- 広範な自動化とエラーの削減により、業務のスピードが向上
- 必要なときに必要なリソースへ、ユーザーがより容易にアクセスできるようになる

ところが、アイデンティティは対象となる範囲や影響が大きく、複雑であるために、どこから着手するかを把握し、自社の現状を評価して、組織の目標を達成するロードマップを作成することが難しい場合があります。

Oktaのアイデンティティ成熟度モデル（IMM）



Oktaアイデンティティ成熟度モデル（IMM）は、価値主導型のフレームワークで、19,450社以上のOktaのお客様で当社が観察したパターンと総体的なベストプラクティスに基づき、ビジネス成果を達成するためのロードマップと評価基準の両方を提供します。このフレームワークは、テクノロジーに基づく他のフレームワークで築かれた基盤の上に構築されており、アイデンティティを原動力として、組織全体のビジネス成果をどのように支えるかを示します。

IMMでは、成熟の過程に沿ってアイデンティティ機能を4つの段階にマッピングしています。

基盤の構築
必要不可欠なアイデンティティ要件を満たしつつ、成熟に向けた強固で信頼性の高い基盤を構築する

拡張
統合されたアイデンティティ管理の適用範囲を新たなアプリケーション、サービス、ユースケース、ユーザーに拡大する

高度化
自動化と統合を進め、エクスペリエンスを向上させ、俊敏性を高め、セキュリティを強化する

戦略
従業員が力を発揮できるイニシアチブを通じて戦略的メリットを獲得し、効率を最適化し、アイデンティティを利用してリアルタイムで脅威を検知して対応する

次の表では、これらの段階での成熟を通じて、セキュリティとコンプライアンス、運用の俊敏性、エンドユーザーエクスペリエンスという重要な価値の柱において、有意義かつ測定可能な成果をどのように実現するかを示します。

okta

価値の柱	成果の例	ステージ1：基盤の構築	ステージ2：拡張	ステージ3：高度化	ステージ4：戦略
		組織は、アイデンティティベースの攻撃から保護しながら、アプリケーションやユーザーを有効にするのに苦労することがよくあります。成熟するには、アイデンティティインフラストラクチャを統合し、簡素化する必要があります。	基本的なアイデンティティ機能は整備されており、運用の基盤を支え、拡張するための改良に重点が移ります。これには、セキュリティ制御の多層化と自動化の拡大が必要です。	組織は広範なアイデンティティシステムを確立済みで、自動化やセキュリティポリシーの強化により、影響が大きく、簡単に達成できる制御を進めることに重点を置いています。	この最終の継続的ステージでは、可能な限りの組織に制御と自動化を拡張し、改良と最適化が特徴的な安定した状態に達することを主に目指します。
セキュリティとコンプライアンス	• アイデンティティの脅威を事前に軽減・対処する • 重要なコンプライアンス認定を取得・維持する • 最小権限の原則に基づいたアクセスにより、エンドユーザーのアクセスを効率化し、安全に保つ	ロールベースのアクセスコントロール（RBAC）ポリシーを備えた、基本的なシングルサインオン（SSO）と多要素認証（MFA）を実装することで、アイデンティティ攻撃に対する防御を強化します。	ダイナミックアクセスポリシーを利用したゼロトラストアーキテクチャの初期ステージを開始します。	リスクを考慮したフィッシング耐性のある認証と認可を実装します。	最新の侵入のペースに対応できる、インテリジェントでコンテキストを考慮した継続的な認証と認可を導入します。
運用の俊敏性	• 運用効率を向上する / 運用コストを削減する • 従業員の効率を向上する • 合併と買収時の統合作業を効率化する	ユーザーとアプリの管理で手作業から脱却します。	ユーザーライフサイクルとプロビジョニング全体を自動化します。	高度なライフサイクル管理（LCM）を導入し、アクセス要求と承認、アプリのプロビジョニングなどの一般的なタスクを自動化します。	クラウドアプリとサービス全体で、ポリシー、ユーザーLCM、アイデンティティ関連のITおよびセキュリティ運用ワークフローを完全に自動化します。
エンドユーザーエクスペリエンス	• エンドユーザーのデジタルエクスペリエンスを向上する • 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	すべてのアプリケーションのインベントリと、MFA、ボット検出、強力なパスワードポリシーなどのベースラインの保護を備えた、安全なログインフローを確立します。	SSOとMFAをすべてのユーザータイプに拡張し、FastPassやパスキーなどのパスワードレスオプションを早期に導入し、一般的なニーズに対するセルフサービスによるアクセスを標準化します。	デバイスとチャネルでパスワードレスアクセスを拡張し、シームレスなセルフサービスに対応し、アイデンティティシグナルを使用してアクセスをリアルタイムでパーソナライズします。	検証可能な認証情報、アダプティブポリシー、リアルタイムのセッションコントロールなどの高度な機能を使用して、すべてのタッチポイントで完全にパスワードレスのパーソナライズされたアクセスを提供します。

注：この表は、アイデンティティの対象範囲の広さを示すことを目的としています。
各段階またはビジネス成果を定義する特性や動作を網羅的に表現したものではありません。

okta

このドキュメントについて

Oktaは、組織がアイデンティティ戦略を策定・改善できるよう、実践的で価値に基づいた、成果重視のガイダンスを提供するために、Oktaアイデンティティ成熟度モデルを作成しました。

テクノロジーに基づいたフレームワークや成熟度チェックリストは、機能の説明やテクノロジーの推奨を行う傾向があるため、価値または成果の詳細な検討は除外されています。IMMのアプローチは、それらとは異なるものです。

また、IMMはセキュリティ（およびコンプライアンス）を超えて広がる点も、他のリソースとは異なっています。

しかし、アイデンティティプロジェクトが始まる主な理由はセキュリティであることが多いため、このガイドでは、人気のCISAゼロトラスト成熟度モデル（ZTMM）の4つのアイデンティティ機能と分野を横断した3つの能力というお馴染みの視点を通して、アイデンティティ成熟度を検証します。

認証	アイデンティティストア	リスク評価	アクセス管理
可視性と分析	オートメーションとオーケストレーション	ガバナンス	

この検証を通じて、以下を行います。

- インサイトと実際のコンテキストの提供
- 必要に応じ、ZTMMとの比較・対比
- 貴社がアイデンティティ成熟度の目標を達成するために役立つOktaソリューションのご提案

アイデンティティ成熟度とゼロトラスト

アイデンティティは、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）が開発した「ゼロトラスト成熟度モデル（ZTMM）」の重要な5つの柱の1つ目に挙げられています。

同モデルのアイデンティティに関する項目では、米国の政府機関は以下を実行する必要があると明記されています。

- ユーザーおよびエンティティに対し、過度のアクセス権を付与することなく、適切なリソースに適したタイミングで、適格な目的のために、アクセスが適用されるようにする。
- 可能な場合は、組織全体でアイデンティティ、認証情報およびアクセス管理ソリューションを統合し、強力な認証を適用し、カスタマイズしたコンテキストベースの認可を付与し、機関ユーザーおよびエンティティに対するアイデンティティリスクを評価する。
- 必要に応じて、アイデンティティストアと管理システムを統合し、エンタープライズアイデンティティおよび関連する責任と権限に対する認識を強化する。

テクノロジーに基づいたZTMMは米国の政府機関向けに開発されたものですが、民間の多くの組織でも使用されています。CISAモデルは、継続的な検証や最小権限などの原則を概説する「NISTゼロトラストアーキテクチャ（SP　800-207）」のアーキテクチャに関するガイダンスを補完しています。ただし、CISAのガイドは規範というよりも説明的な内容であるため、Oktaの多数のお客様から、CISA　ZTMMに沿ってアイデンティティの取り組みを成熟させる方法について、質問が寄せられています。

そのため、このガイドでは、CISA　ZTMMの特定の側面を特に参照し、Okta IMMとCISAモデルとの関連を説明します。

Oktaアイデンティティ成熟度モデルが規制対象の業界におけるゼロトラストをどのようにサポートするかについて、詳細をご覧ください。

okta

認証

認証は、アプリケーション、サービスまたはその他のリソースに対するアクセスを要求するユーザーやエンティティのアイデンティティを確認し、本人であることを保証します。

攻撃者は一般的に、以下を含む方法を使用して認証を攻撃します。

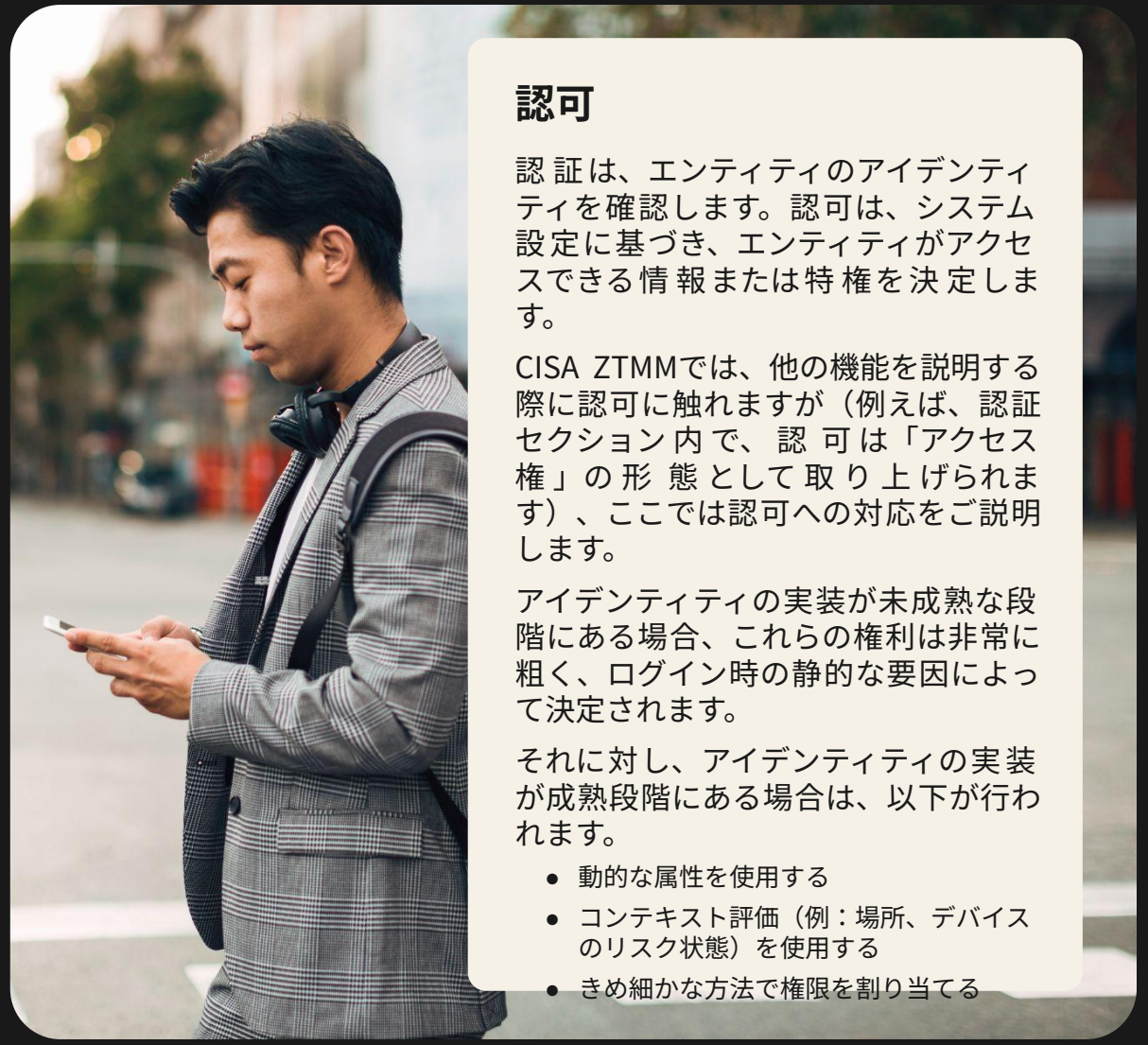
- 認証情報の多くの組み合わせを試す総当たり攻撃
- ユーザーを騙して認証情報を提供させるソーシャルエンジニアリング
- 認証情報、Cookie、トークンを盗む情報窃取
- MFAの脆弱な形態をバイパスするSIMスワッピングおよび中間者攻撃

認証がセキュリティの重要な要素であることは明らかですが、認証はユーザーエクスペリエンスや従業員の生産性にも影響を与え、重大な結果をもたらす場合もあります。

例えば、「Auth0 Customer Identity Trends Report 2025」では、ユーザーの約4分の1が、サインアップやログインプロセスの問題により、常に（6%）または頻繁に（17%）オンライン購入を断念していると答えており、さらに40%がときどき断念していると報告しています。同様に、アプリケーションや情報にアクセスできない従業員は、業務を遂行することができません。

成熟した認証機能は、強力でフィッシング耐性のあるセキュリティ（リスクシグナルを組み込むことを含め）を組み合わせ、使用も簡単です。これにより、攻撃者がアクセスを手に入れることは非常に困難で費用がかかるようになる一方、正規のユーザーには便利なアクセスを提供できます。

さらに、成熟した認証機能はリスクを一度（ユーザーのログイン時に）評価するだけでなく、セッションハイジャックや類似したログイン後の脅威から保護するために、継続的に評価を行います。



認可

認証は、エンティティのアイデンティティを確認します。認可は、システム設定に基づき、エンティティがアクセスできる情報または特権を決定します。

CISA ZTMMでは、他の機能を説明する際に認可に触れますが（例えば、認証セクション内で、認可は「アクセス権」の形態として取り上げられます）、ここでは認可への対応をご説明します。

アイデンティティの実装が未成熟な段階にある場合、これらの権利は非常に粗く、ログイン時の静的な要因によって決定されます。

それに対し、アイデンティティの実装が成熟段階にある場合は、以下が行われます。

- 動的な属性を使用する
- コンテキスト評価（例：場所、デバイスのリスク状態）を使用する
- きめ細かな方法で権限を割り当てる

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	リスクの高い本段階では、認証は主にユーザー名とパスワードの組み合わせに依存しています。MFAが使用される場合もありますが、従業員全員には求められず、フィッシング詐欺にあいやすい方法（例：SMS、Eメール）が使用される可能性があります。 さらに、認可は事前定義され固定されており、リアルタイムの条件やコンテキスト条件が考慮されません。	• Multi-factor Authentication • Adaptive MFA • Single Sign-On • Universal Directory
 **拡張**	組織はMFAをすべてのエンティティに適用し、フィッシング耐性のある所有要素と固有要素を導入してセキュリティを強化します。シングルサインオン（SSO）と組み合わせると、認証がより強力かつ便利になります。 簡素化され集約されたユーザーストアにより、認可管理の効率と効果を向上できます。ロールベースまたは属性ベースのアクセスコントロール（RBACまたはABAC）が導入され、エンティティの場所、現地時間、デバイスタイプなど、リスク評価に使用できる動的要素が組み込まれます。	• Adaptive MFA • Single Sign-On • Universal Directory • Fine Grained Authorization
 **高度化**	組織はパスワード、ワンタイムパスワード/パスコード（OTP）、セキュリティの質問、プッシュ通知の段階的な廃止を始めます。 フィッシング耐性のあるMFAが組織全体に展開され、FIDO2によるパスワードレスMFAの導入、または適用される場合は個人ID検証（PIV）などの安全な政府認証情報の導入が含まれます。 関係性ベースのアクセスコントロール（ReBAC）により、正確で動的な認可が可能になります。コンピュータを使用したユーザーログインに、アクセス管理とMFAが拡張されます。 信頼性の高いシステム（コールセンター、サービスキオスク、AIを使用したエージェントなど）によるセキュアなパスワードレスの開始では、認証フローが分離されているため、セキュリティの質問、OTP、PINなどが必要なくなります。	• Adaptive MFA • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine Grained Authorization • Okta Device Access • CIBA（Client-Initiated Backchannel Authentication）
 **戦略**	すべてのアイデンティティが、フィッシング耐性のあるパスワードレス認証で確認されます。アクセスコントロールがデバイスのログインからアプリケーションのサインインに拡張され、統合セキュリティを実現するとともに、ユーザーエクスペリエンスが簡素化されます。 アクセス権は動的変数を使用して継続的に評価されるようになり、認証後の脅威を検出できるようになります。 リスクの高いトランザクションやプロファイル変更などの機密性の高い顧客のアクションは、リアルタイムの確認メカニズムにより認証・保護され、エクスペリエンスを妨げることなくセキュリティを強化します。 バックエンドでは、顧客のコミュニケーションチャネルとデータ交換が金融機関レベルの基準で強化され、エンドツーエンドのカスタマージャーニー全体で改ざんや傍受を防ぎます。	• Adaptive MFA • Single Sign-On • Universal Directory • Identity Threat Protection • Okta FastPass • Fine Grained Authorization • Okta Device Access • Strong Customer Authentication • Financial-Grade APIs（FAPI）

okta

アイデンティティストア

アイデンティティストアはユーザーとエンティティデータ（名前、ロール、属性など）のレポジトリで、従業員、パートナー、契約社員、顧客、サービス、およびその他のサードパーティのアイデンティティの認証、証明書の確認、ライフサイクル管理に使用されます。アイデンティティストアはサービスアカウント、デバイス、ボットおよびAIエージェントなどの非人間アイデンティティ（NHI）も対象にするようになりました。

大半の組織は自己管理によるオンプレミスのアイデンティティストアから始めますが、拡張性、可視性およびセキュリティに関連する制約にすぐに直面します。

組織が成長し、より多くのアプリケーションを展開するようになると、単一の信頼できる情報源の維持が難しくなります。人間でも非人間でも、アイデンティティが連携していないシステム全体で急増し、「アイデンティティの無秩序な増加」につながります。このような状況により管理が複雑になり、一貫したポリシーの適用が難しくなるため、業務スピードが遅くなり、セキュリティリスクが発生してしまいます。

アイデンティティを統合して同期することで、組織は単一の信頼できる情報源を築くことができ、安全なアクセスの完全な自動化、リスクの削減、効率的なライフサイクル管理に必要な基盤を構築できます。

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	組織は、Active DirectoryやLDAPなどの自己管理型（例：計画、展開、保守）のアイデンティティストアのみを使用します。これらのストアは一般的に人間のユーザーに焦点を当てているため、多くの場合、サービスアカウントなどのNHIは管理されていないか、非公式に追跡されています。	• Single Sign-On • Universal Directory
 **拡張**	アイデンティティの無秩序な増加を減らすため、組織は自己管理型とクラウドホスト型の両方のアイデンティティストアの統合を始めます。同時に、自動化およびコードとしてのインフラストラクチャにより作成されたNHIと人間の両方に、一貫したガバナンスを適用します。 さらに、ディレクトリ間で同期を行い、ライフサイクル管理の実践を標準化し、NHIを公式に追跡し始めます。これらの段階により重複を減らす基礎が築かれるため、可視性が向上し、拡張可能な自動化されたワークフローを確立できます。	• Single Sign-On • Universal Directory • Lifecycle Management • Workflows
 **高度化**	アイデンティティストアが統合され、ガバナンスポリシーが人間と非人間アイデンティティで適用されるため、アイデンティティの無秩序な増加を減らし、アイデンティティ運用（SSOなど）と管理（プロビジョニング、LCMなど）の安全と効率を向上できます。 サービスアカウント、API、ボットがオンボーディングされ、さらに公式な形で追跡されます。可視性が向上し、アイデンティティライフサイクルイベントが集約されます。	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **戦略**	アイデンティティストアがすべての環境で一元化され、使用されるアイデンティティストア数を最小限に抑えて、アイデンティティストア間での自動化されたLCMを可能にします。 NHI（出現し始めたAIエージェントも含む）は、人間のユーザーと並んで管理されます。組織は、アダプティブポリシー、自動LCM、態勢管理を、共有されたアイデンティティファブリック全体で有効にします。	• Universal Directory • Single Sign-On • Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access • Identity Security Posture Management

okta

リスク評価

Oktaはアイデンティティリスクを幅広くとらえ、*「組織のアイデンティティとアクセス管理プロセスにおける、あらゆる脆弱性」*と定義しています。

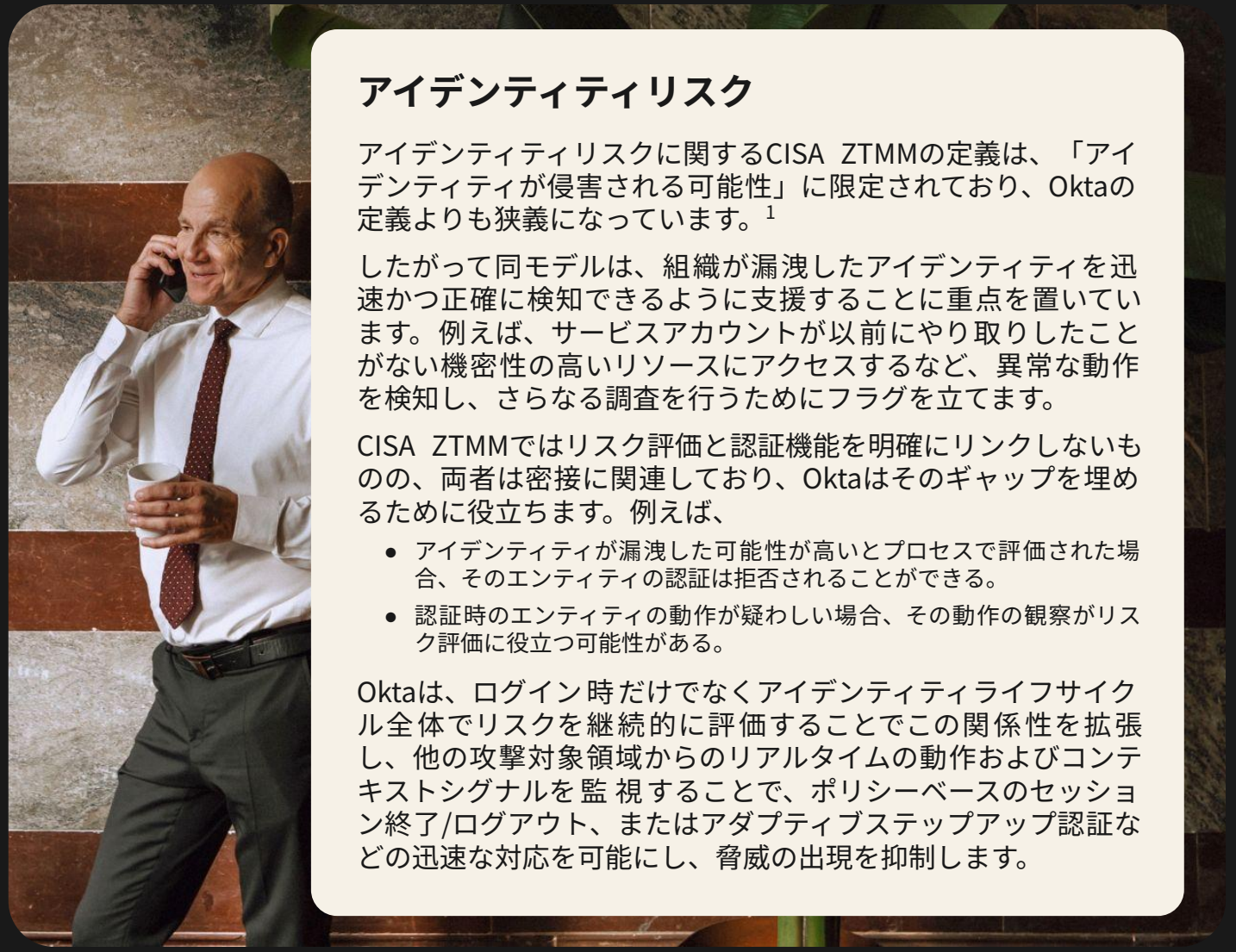
この広範な定義には、個人のアイデンティティに付随するリスクと、以下に関連するリスクの両方が含まれます。

- 脆弱なIAM対策（例：孤立アカウント、過剰なプロビジョニング）
- セキュリティギャップにつながる設定ミス
- 時代遅れのテクノロジーの使用

組織が戦略的な段階に向けて成熟するにつれ、セキュリティ態勢を強化する機能を優先し、アイデンティティ、エンドポイント、ネットワーク、デバイスのリスク状態を含む環境全体でセキュリティシグナルを取り込み、分析することで、アイデンティティ関連のリスクを劇的に低減する必要があります。

これらのリアルタイムのシグナルは、アダプティブポリシーに情報を提供するために役立ち、組織はアイデンティティ攻撃の対象領域を積極的に削減し、以下を通じてセキュリティを向上できます。

- **検知：**アイデンティティプロバイダー、SaaS、クラウドインフラストラクチャ（IaaS）で隠れた脅威や設定ミスを検知する。
- **優先順位付け：**MFAバイパス、過剰プロビジョニングされたユーザー、不適切なオフボーディングなどの脆弱性を検知し、優先順位を付ける。
- **修復：**実用的なセキュリティインサイトを取得して、迅速に修復する。
- **継続的な監視：**組織のアイデンティティセキュリティのリスクに関する継続的な分析を取得して迅速に展開し、セキュリティ、IAM、コンプライアンス基準（例：NIST、CIS、ISO、SOXおよびPCI-DSS）に関するリスクベースの監視を可能にする。



アイデンティティリスク

アイデンティティリスクに関するCISA ZTMMの定義は、「アイデンティティが侵害される可能性」に限定されており、Oktaの定義よりも狭義になっています。[1]

したがって同モデルは、組織が漏洩したアイデンティティを迅速かつ正確に検知できるように支援することに重点を置いています。例えば、サービスアカウントが以前にやり取りしたことがない機密性の高いリソースにアクセスするなど、異常な動作を検知し、さらなる調査を行うためにフラグを立てます。

CISA ZTMMではリスク評価と認証機能を明確にリンクしないものの、両者は密接に関連しており、Oktaはそのギャップを埋めるために役立ちます。例えば、

- アイデンティティが漏洩した可能性が高いとプロセスで評価された場合、そのエンティティの認証は拒否されることができる。
- 認証時のエンティティの動作が疑わしい場合、その動作の観察がリスク評価に役立つ可能性がある。

Oktaは、ログイン時だけでなくアイデンティティライフサイクル全体でリスクを継続的に評価することでこの関係性を拡張し、他の攻撃対象領域からのリアルタイムの動作およびコンテキストシグナルを監視することで、ポリシーベースのセッション終了/ログアウト、またはアダプティブステップアップ認証などの迅速な対応を可能にし、脅威の出現を抑制します。

[1] CISA、Zero Trust Maturity Model、バージョン2.0（2023年4月）、14ページ。2025年6月9日にhttps://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdfから取得。

okta

これらの機能は、CISA ZTMMのアクセス管理機能および分野を横断した3つの能力（可視性と分析、自動化とオーケストレーション、およびガバナンス）と重なります。

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	この段階の組織は、アイデンティティリスクを評価し、アクセスポリシーに取り入れるための能力が非常に限定されています。評価を使用している場合でも、静的属性に基づいていたり、関連ポリシーが単純（二元的など）である可能性があります。	• Multi-Factor Authentication • Adaptive MFA
 **拡張**	ポリシーが多少豊富になり、ログイン時に認証テレメトリを組み込める評価機能があります。 しかし、評価はどちらかというと基本的なものであり、手作業の手法と静的ルールに引き続き依存している部分があるため、アイデンティティ攻撃に対して脆弱なままです。	• Adaptive MFA
 **高度化**	評価には自動化と動的ルールが使用され、アクセスに関する決定をする場合は、多数の認証シグナル（デバイス保証と管理ソリューションからのシグナルを含む場合あり）を使用します。 しかし、依然として評価は主にログイン時のみに実行され、ユーザーセッションのライフタイム中に再評価されることはありません。	• Adaptive MFA • Identity Threat Protection • Identity Security Posture Management
 **戦略**	リスク評価が継続的にリアルタイムで実施され、アイデンティティインフラストラクチャおよび補助セキュリティシステムとITシステムからの豊富なシグナルと動的コンテキストを使用します。Okta AIを使用したアイデンティティ脅威からの保護 さらに、自動化と統合により、安全な即時ログアウトとセキュリティのアクティブ化やIT運用ワークフローを含む、適切な応答とポリシー適用が可能になり、組織と侵害されたユーザーを保護します。	• Adaptive MFA • Identity Threat Protection • Identity Security Posture Management • Workflows

okta

アクセス管理

アイデンティティガバナンスと管理（IGA）は、CISA ZTMMにおけるアクセス管理の焦点を絞ったものです。IGAに従い、4段階は技術的なソリューションへの対処ではなく、実装とプロセスの成熟度を説明しています。それでも、組織がIGAポリシーを実装するには、特定の機能の導入が求められます。

広範に言うと、成熟度が低い組織では、手作業によるアクセスレビュープロセス、長期間付与されたままのアクセス権限、非常に粗い認可設定が見られます。この組み合わせは、多くの場合、過剰なアクセス権限や不適切な権限の組み合わせ（1人のユーザーが特権のエスカレーションの要求と承認の両方を行えるなど）を招き、悪用の機会を与えてしまいます。さらに、単に拡張性にも欠けています。

対照的に、成熟した組織は自動化を最大限に活用し、必要なときにのみアクセスを付与し、ゼロスタンディング特権を維持します。また、アクセスの付与については、最小権限アクセスの原則に従い、極めて精緻な方法で行われます。

アイデンティティガバナンスと管理

CISAのZTMMにおけるアクセス管理機能は、一般的にIGAとして知られるものに関連しています。IGAとは、アイデンティティ管理とアクセスコントロールに対するポリシーベースのアプローチで、以下が組み合わされています。

- **アイデンティティガバナンス：**職務分離、ロール管理、ログ記録、アクセスレビュー、分析、レポートを対象にしたプロセスとポリシー
- **アイデンティティ管理：**アカウントと認証情報の管理、ユーザーとデバイスのプロビジョニング/解除、およびエンタイトルメント管理

okta

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	小規模組織によく見られることですが、この段階では、特権アカウントでも標準アカウントでも、アクセスは恒久的に承認され、定期的なレビューのみが行われます。 アクセスはコンテキストに応じてではなく、適用も限定的で、おそらく手作業（例：スプレッドシートで）で追跡されています。	• Okta Identity Governance • Identity Security Posture Management
 **拡張**	特権アカウントと標準アカウントのアクセスは、自動レビューによって追跡されています。 拡張段階における主な違いは、特に延長されない限り、アクセスは自動レビューにより有効期限が切れることです。 アクセスの判断に使用される情報は依然として限られており、恐らくニーズや過去のアクセスログではなくロールに基づいている可能性があり、長期間にわたりアクセスが付与される可能性があります。また、アクセスコントロールの細かさが限られているため、エンティティに過剰な権限が与えられる可能性もあります。	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine Grained Authorization
 **高度化**	アクセスはニーズとセッションベースで管理されており、アクションとリソースに合わせてカスタマイズされ、自動的に取り消されます。特にサーバーなどの重要なインフラストラクチャに対し、期限付きのジャストインタイム（JIT）パスワードレスアクセスによる最小権限の原則が適用されます。これは、リスクベースでポリシーに基づいたデバイスログインに対するアクセス管理にも拡張されます。 デバイスのリスク状態、ネットワーク、動作リスクシグナルに基づいた、きめ細かな条件を組み込んで適用します。	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine Grained Authorization • Workflows • Okta Device Access
 **戦略**	最小権限とJITアクセス認可ポリシーが自動化されるようになり、個別のアクションやリソースニーズに応じてアクセスが調整されるため、ゼロスタンディング特権が実現されます。 アクセスの適用は完全にアダプティブで、技術スタックでリアルタイムのシグナルに対応します。認証とセッションの判断は、継続的な評価に基づきます。リスクベースのステップアップ認証およびその他のアクションは自動化され、リアルタイムで実行されるため、ユーザーエクスペリエンスが向上すると同時に、セキュリティ態勢が維持されます。	• Okta Identity Governance • Identity Security Posture Management • Okta Privileged Access • Fine Grained Authorization • Workflows • Okta Device Access

okta

可視性と分析

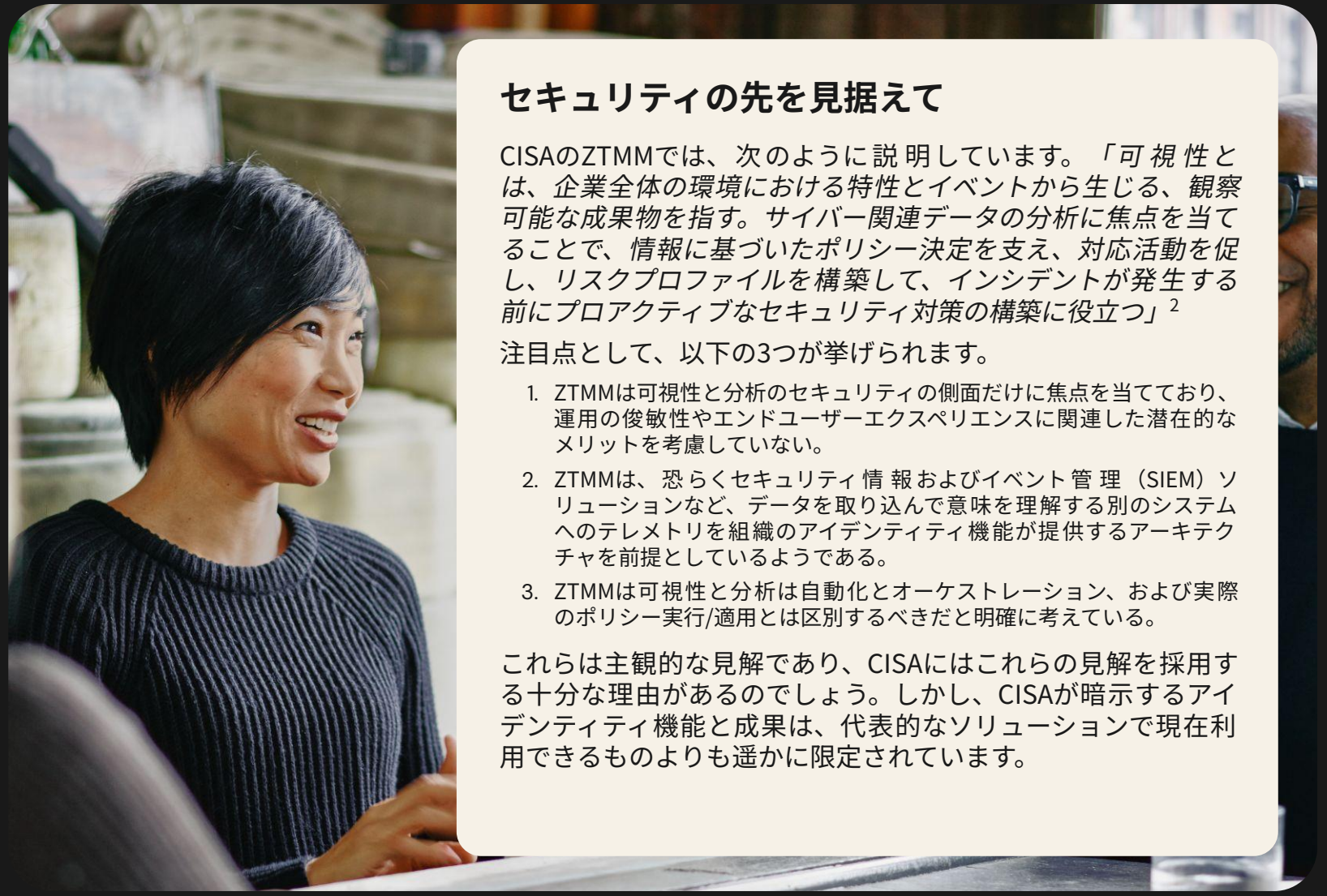
エンティティがアイデンティティシステムをどのように使用するかについて組織の理解が深まるほど、以下が可能になります。

- 運用の俊敏性の向上
  （例：ワークフローの自動化により）
- ユーザーエクスペリエンスの最適化
  （例：アクセス管理ポリシーの調整により）
- セキュリティの強化
  （例：予防、検知、対応機能の実装により）

一部のアイデンティティソリューションはリアルタイムでリスクを検知でき、SIEMにデータを送信する必要もないため、一般的なセキュリティツールよりも迅速かつ正確です。重要なのは、ローカルでの分析により外部システムを補完できることです。

一部のアイデンティティソリューションでは、認証の阻止や侵害されたユーザーのログアウトなど、脅威に対応してポリシーを直接強化することもできます。同一ソリューションが提供するリアルタイム検知により、この緊密な連携は脅威を迅速に軽減し、組織のセキュリティ態勢を強化します。

ただし、達成される成果は、アイデンティティプラットフォームやその送信機能に応じて変わります。



セキュリティの先を見据えて

CISAのZTMMでは、次のように説明しています。*「可視性とは、企業全体の環境における特性とイベントから生じる、観察可能な成果物を指す。サイバー関連データの分析に焦点を当てることで、情報に基づいたポリシー決定を支え、対応活動を促し、リスクプロファイルを構築して、インシデントが発生する前にプロアクティブなセキュリティ対策の構築に役立つ」*[2]

注目点として、以下の3つが挙げられます。

1. ZTMMは可視性と分析のセキュリティの側面だけに焦点を当てており、運用の俊敏性やエンドユーザーエクスペリエンスに関連した潜在的なメリットを考慮していない。
2. ZTMMは、恐らくセキュリティ情報およびイベント管理（SIEM）ソリューションなど、データを取り込んで意味を理解する別のシステムへのテレメトリを組織のアイデンティティ機能が提供するアーキテクチャを前提としているようである。
3. ZTMMは可視性と分析は自動化とオーケストレーション、および実際のポリシー実行/適用とは区別するべきだと明確に考えている。

これらは主観的な見解であり、CISAにはこれらの見解を採用する十分な理由があるのでしょう。しかし、CISAが暗示するアイデンティティ機能と成果は、代表的なソリューションで現在利用できるものよりも遥かに限定されています。

[2] CISA、Zero Trust Maturity Model、バージョン2.0（2023年4月）、11ページ。2025年6月9日にhttps://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdfから取得。

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	この段階では、組織は特権付き認証情報に特に注意して、アイデンティティアクティビティログを収集します。 ログ分析はルーチンとして行われることもありますが、手作業で分析されます。そのため、そのような分析ではリスクをタイムリーに特定したり、高度な脅威を特定したりすることが比較的難しくなります。	• Universal Directory
 **拡張**	手作業のログ分析に加え、組織は一部に自動分析を使用します。 自動分析により脅威をタイムリーに検知する能力は向上するものの、ログタイプの相関関係が限定的であるため、高度な脅威の検知は依然として妨げられます。	• Universal Directory • Workflows
 **高度化**	分析は完全（またはほぼ完全に）自動化され、ログタイプの相関関係も考慮されていますが、すべてのユーザーおよびエンティティのログタイプが含まれているわけではありません。 アイデンティティログは他のソースにもリンクされているため、可視性のギャップが埋まり、より包括的な脅威検知機能が提供されます。	• Universal Directory • Workflows • Identity Threat Protection
 **戦略**	組織は、他のソースと連携されたすべてのユーザーおよびエンティティログタイプの自動分析により、包括的な可視性を達成・維持できます。	• Universal Directory • Workflows • Identity Threat Protection

okta

オートメーションとオーケストレーション

組織がアイデンティティの自動化とオーケストレーション機能をどの程度成熟させることができるかは、組織が展開するアイデンティティプラットフォームとアイデンティティ製品により大きく変わります。

最も強力なアイデンティティソリューションは、幅広い技術スタックの統合により自動化とオーケストレーションをサポートするだけでなく、そのような機能をソリューション自体にも備えています。

これらの組み込み機能により、組織はワークフローを作成して、入社・異動・退社（JML）プロセスを含むアイデンティティライフサイクルを管理し、強力なガバナンスを支え、特権アクセスを慎重に管理し、セキュリティ態勢を強化することができます。汎用自動化ツールやオーケストレーションツールは必要ありません。

ゼロトラストのコンテキスト

CISAのZTMMでは、次のように説明しています。「ゼロトラストは、製品とサービスでセキュリティ対応機能をサポートする自動化されたツールとワークフローをフル活用すると同時に、そのような機能、製品、サービス向け開発プロセスの監視、セキュリティ、インタラクションを維持する」[3]

実際には、自動化およびオーケストレーション機能は、他の場所で対応したアイデンティティプロセスと機能がどのように実装されるかであり、これらのプロセスと機能が*何であるか*ではありません。その結果、自動化とオーケストレーション、および認証、リスク評価、アクセス管理機能には、かなりの重複があります。

[3] CISA、Zero Trust Maturity Model、バージョン2.0（2023年4月）、11ページ。2025年6月9日にhttps://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdfから取得。

okta

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	この段階では、組織はほぼすべて自己管理型のアイデンティティを使用して機能し、オンボーディングとオフボーディングを含むライフサイクル管理プロセスを手作業で実行します。これらは、主にEメール、コラボレーションアプリ、サービスデスクチケット、および類似のユーティリティを使用して行われます。 異なるシステム間での統合はわずかで、レビュー（例えば、アクセス特権に関するもの）は、事前に決定された頻度で手作業で実施されます。	• Lifecycle Management • Workflows
 **拡張**	この段階では、組織はある程度の自動化の実装を始め、非特権ユーザーと自己管理型アイデンティティに関するプロセスをオーケストレーションします。ユーザーのプロビジョニングとプロビジョニング解除は、ますます自動化により処理されます。 組織は依然として特権付きアイデンティティを手作業でオーケストレーションしていますが、外部のアイデンティティも管理するようになっています。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **高度化**	この段階では、組織はすべての環境で十分に統合されており、内部アイデンティティと外部アイデンティティの自動化とオーケストレーションが可能です。特権付きアイデンティティは依然として手作業でオーケストレーションされます。 アイデンティティリスクの検知と修復は自動化され、潜在的な脅威を事前に特定し、対応することができます。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **戦略**	戦略的段階では、アイデンティティオーケストレーションのすべてのプロセスが自動化され、すべてのアイデンティティと環境に拡張され、行動・登録・デプロイメントのニーズに基づいています。 組織はリスクが検知された場合に、自社の特定のニーズに合わせたダウンストリームプロセスをトリガーすることで、修復対応を柔軟に自動化できます。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

okta

ガバナンス

アイデンティティガバナンスとは、組織の目標を支えるポリシー、手順、プロセスの定義と施行（例：ゼロトラスト原則の実装、効率性の改善、生産性の向上）、および規制、フレームワーク、標準および契約上の義務への準拠を指します。

ガバナンスにおける成熟化とは、分断され手作業に依存したアプローチを、包括的かつ自動化されたアプローチへと変えることに重点を置きます。これには、人間のアイデンティティと非人間アイデンティティ（NHI）の両方にまたがるポリシーの統一、ロールベースおよびリスクベースのアクセスコントロールの適用、ライフサイクルと認証プロセスの拡張が含まれます。

組織が成熟するにつれ、ガバナンスはその場しのぎの制御から、API、サービスアカウント、ロボットプロセスにも等しく適用される継続的かつインテリジェントな自動化へと拡大します。NHIはアイデンティティライフサイクルの各段階で、ガバナンスにおいて、人間と同等の管理対象となり、最小権限、アクセスレビュー、コンプライアンス監視が適用されるようになります。

okta

ステージ	説明	対応するOktaソリューション
 **基盤の構築**	アイデンティティガバナンスがほとんど整備されておらず、既存のプログラムも（共通のビジネスやガバナンス目標に沿ったものではなく）分断されていたり、スタンドアロンであったり、人間のアイデンティティだけに焦点を置いたりしています。NHIの一元的な監視体制がなく、多くの場合は未確認のNHIが急増し、リスクが増加します。	• Lifecycle Management • Workflows
 **拡張**	組織はアクセスレビューとアクセスリクエストフローを自動化することで、ガバナンスとコンプライアンスの一部の側面を合理化しています。 ロールベースのモデルにより、ガバナンスがより構造化されます。プロビジョニング/解除はライフサイクルイベントに基づいて自動化され、アクセス認定は定期的に予定されています。 一般的に、サービスアカウントとボット向けの基本的なライフサイクル自動化により、NHIの初期段階の制御が導入されることがあります。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **高度化**	組織は強化されたガバナンスと運用手法を取り入れ、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ています。 アクセスは、ユーザー属性、リスクレベル、ビジネスルールを考慮した動的かつポリシーベースの制御によって管理されます。また、ジャストインタイムや時間制限のあるアクセスが実装されています。リスクの高いリクエストは、人間による承認プロセスを必要とし、職務分離を強化することで、競合するアクセスを防ぎます。 NHIに対するガバナンスが体系的に導入され、人間のユーザーに適用されるものと同様に、最小権限、レビュー、ライフサイクル制御が適用されます。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access
 **戦略**	組織はAIを活用してアイデンティティの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させ、構成や開発を容易にします。 ガバナンスは継続的かつプロアクティブで、アクセス決定は予測分析とクラウド、ハイブリッド、オンプレミス環境全体で統一されたポリシーに基づき、リスクを考慮して自律的に行われます。 認定は定期的な認定からイベント駆動型となり、NHIはアダプティブなガバナンスプロセスに完全に統合されます。 人間による監視はリスクの高いシナリオにのみ適用され、自動化とインテリジェントな介入のバランスが取れたアダプティブガバナンスを実現します。NHIの自律型ガバナンスは、リスクスコアリング、アクセス自動化、インテリジェントな修復に補完され、重要な機能になります。	• Lifecycle Management • Workflows • Okta Identity Governance • Okta Privileged Access

okta

おわりに

組織のアイデンティティへの取り組みはそれぞれ異なる、というのは真実に根付いた常套句ですが、一定のパターンもあります。

アイデンティティ成熟度を優先することで、組織は強化されたセキュリティ態勢、生産性の高い人材、運用効率の向上、継続的な事業成長といったメリットを得ることができます。

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。お客様に対するOktaの契約上の保証に関する情報は、okta.com/agreementsをご覧ください。© Okta and/or its affiliates. All Rights Reserved.

okta