電子書籍

アイデンティティをセキュリティの要に

最新のアイデンティティ戦略を
推進するための 3 つの原則

okta

「アイデンティティ」というと、何を思い浮かべますか？

おそらく最初に思い浮かぶのは「セキュリティ」でしょう。それには十分な理由があります。認証情報の窃取やフィッシング攻撃が横行する脅威環境において、攻撃者にとってアイデンティティは、重要なネットワークを侵害し機密情報へアクセスするための中心的な要素であることは明白です。だからこそ、未来に対応する組織は、最新のエンドツーエンドのセキュリティ戦略の中核にアイデンティティを据える必要があります。

それにもかかわらず、依然として多くの組織の対策は後手に回っており、境界の安全性を確保するという時代遅れの考え方から脱却できていません。そうした状況で、従来のネットワークやデバイス中心のセキュリティツールでは、アイデンティティベースの高度な攻撃の防御が十分でないことを認識しつつあり、リスクを正確に把握して効果的に対処するための可視性を確保しようと苦戦しています。

最新のアイデンティティ戦略の定義

最新のアイデンティティ戦略は、アイデンティティ環境全体の可視性を確保し、脆弱性を特定してセキュリティ態勢を強化し、潜在的な攻撃に迅速かつ効果的に対応するための道を提供します。また、この強固な保護を実現しながら、今日のビジネスの成功に不可欠なシームレスな接続とスムーズなエクスペリエンスを提供できる点も重要です。

この資料では、アイデンティティが企業のセキュリティとテクノロジーの基盤であるべき理由を解説し、以下の情報を提供します。

- アイデンティティに関連する脅威が加速している現状
- 従来のアイデンティティ管理手法が組織の脆弱性を引き起こしている理由
- 最新のアイデンティティを導入するための 3 つの原則

エンタープライズ セキュリティスタックの断片化

この 10 年で、エンタープライズ技術スタックは大きく変化しました。クラウドサービスや SaaS アプリケーションの急速な導入、そしてリモートワークの普及により、コラボレーションや接続のあり方が根本的に変わりました。テクノロジーを活用した差別化が求められるビジネス環境において、特定の企業 1 社とエンタープライズライセンス契約（ELA）を結び、技術的な統一性を維持するという考え方はもはや時代遅れです。競争力のある企業は、俊敏性と高いパフォーマンスを確保するために、従業員向けテクノロジー、顧客向けテクノロジー、そして製品提供で、ベストオブブリードのソリューションを組み合わせて活用する必要があることを認識しています。

最新の技術スタックは極めて高度であると同時に、非常に複雑です。増え続けるポイントソリューションが断片化した IT 環境を形成し、その中ではビジネスリソース（およびそれに紐づくアイデンティティ）が、絡み合いつつも分断されたシステム、アプリ、インフラストラクチャのネットワーク全体に分散しています。

テクノロジーのサイロ化が セキュリティの盲点を生む

こうした断片化は重大なセキュリティリスクを生み出します。アイデンティティのサイロ化によって、さまざまな場所で攻撃対象領域が拡大し、認証情報の窃取や悪用が見過ごされる可能性が高まります。また、セキュリティチームにとって、脆弱性を修復しリスクを特定するために必要な、広範かつ詳細な可視性を確保することがほぼ不可能になります。

アイデンティティが多くの企業で拡大する盲点となっていることは、攻撃者も理解しているため、アイデンティティが最大の攻撃ベクトルとなっています。Okta も参加した 2024 年版 Verizon データ漏洩 / 侵害調査報告書によると、侵害の 80%には何らかの形で認証情報の漏洩が関与しています。さらに懸念すべきは、この新たな現実に対して多くの組織で根本的な備えができていないことです。データ漏洩の検知から封じ込めまでに要した平均日数は、2024 年には 290 日という驚異的な長期に及びました。

okta

今こそアイデンティティを変革すべき時

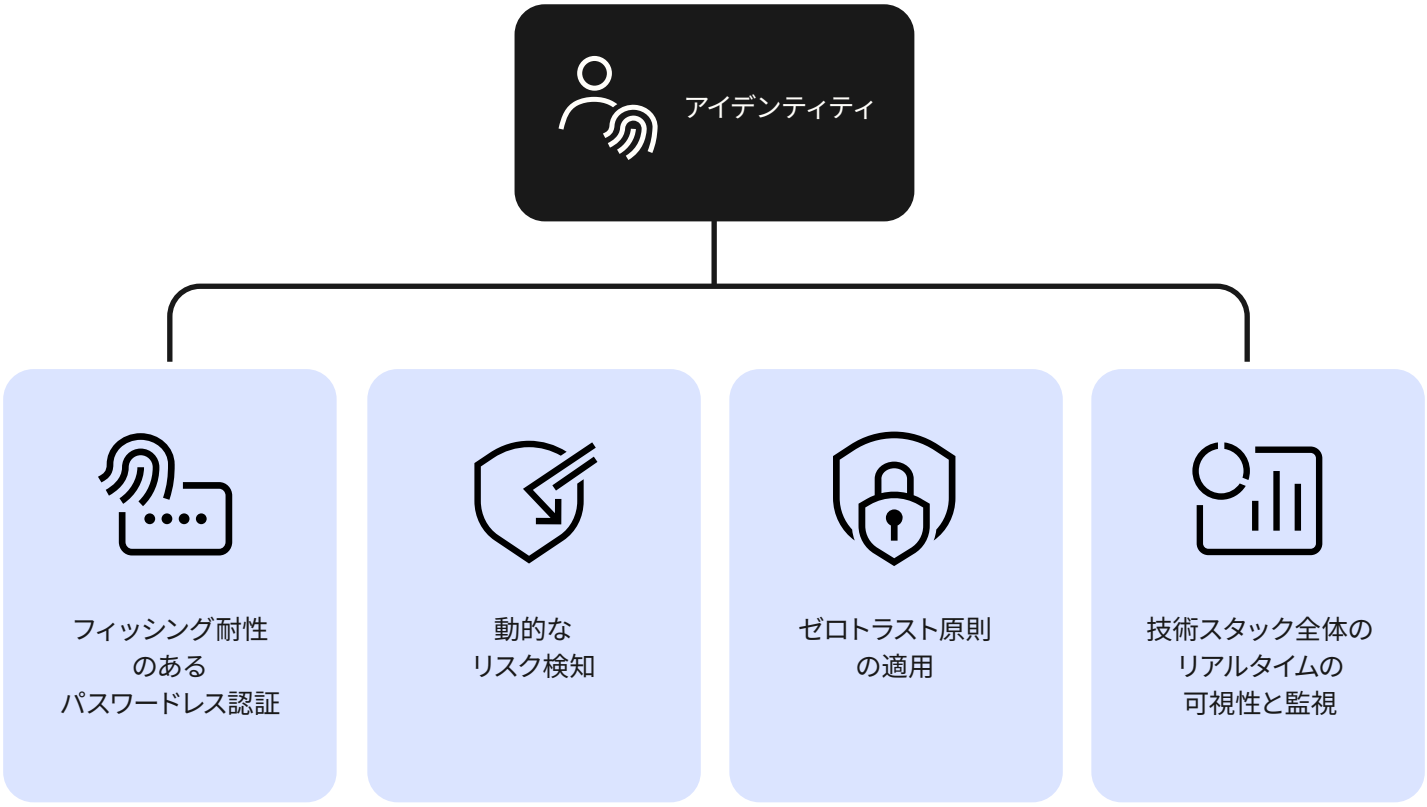
アイデンティティがセキュリティにおいて重要な役割を果たすことは、どの組織も理解しています。しかし、従来のアイデンティティはあくまで「門番」の役割を果たすものでした。その一方で、アイデンティティは、エンタープライズ全体のセキュリティの可視性とインテリジェンスの基盤という、同等に重要な役割も担っており、この意味でアイデンティティを活用している組織はごく少数に限られます。

たとえば、ほとんどの企業は、安全な認証を通じてシームレスなアクセスを実現するためにアイデンティティを活用しています。しかし、アイデンティティの機能をテクノロジーやセキュリティのエコシステムにより深く統合することで、リアルタイムの動的なリスク検知を可能にしたり、窃取された認証情報を使用して攻撃者が認証を成功させた後の自動修復戦略を支援したりといったことが可能になります。この他にもさまざまな方法により、セキュリティチームはアイデンティティを活用して、より自信を持って積極的にセキュリティ態勢を強化できます。

アイデンティティを中心とするセキュリティエコシステム

この可能性を無視することは、すでに明らかになっている事実を見過ごすことにほかなりません。アイデンティティは、エンタープライズサイバーセキュリティにおける主戦場となっています。攻撃者の多くはアイデンティティを足がかりに侵入し、対策を最も成功させているセキュリティチームはアイデンティティを通じて攻撃を阻止しています。最新のアイデンティティ戦略は、ますます高度化する脅威に対して、より強固で統合された即応性の高いセキュリティ態勢を実現し、セキュリティ環境のあらゆる要素をつないで強化する役割を果たす潜在力を秘めています。

この状況に対応するためには、アイデンティティとは何か、そしてアイデンティティの活用方法について、より広範かつ戦略的な視点を持つ必要があります。



脅威の詳細な分析

攻撃者は、時代遅れのアイデンティティ管理手法を狙っています。断片化したIT/ セキュリティ環境では、重要なリソース、アプリ、アイデンティティが異なるシステムやインフラストラクチャに分散するため、アイデンティティに関連する攻撃が見過ごされ、対処されずに放置されるリスクが高まります。これによって、不便な程度のものから壊滅的な影響を及ぼすものまで、さまざまな結果を引き起こす可能性があります。

手作業のプロセス

許可設定の手順が煩雑で時間がかかるため、重要なアクセスの判断で人的なミスが起きやすい

見落とし

組織のリアルタイムのセキュリティ態勢や、各種システムやアプリケーションにおける個々の許可を十分に把握できない

対応の遅れ

対応が遅れることで、攻撃者がアイデンティティ関連の脆弱性を悪用できるようになり、高コストで深刻な侵害へと発展する可能性がある

この問題は解決するどころか、加速しています。AI を活用したアプリケーションやサービス、ユーザーの増加により、アイデンティティに関連するリスクの検知と防御がますます困難になっています。状況をさらに悪化させているのは、アイデンティティ関連の攻撃が単なる認証情報の窃取にとどまらないことです。認証後のセッション Cookie 窃取の脅威なども加わり、不審なログ情報を監視する作業は一層複雑化しています。さらに、国家が支援する資金力のある攻撃や、発見が難しい内部脅威といった常に存在するリスクも重なり、現在のリスクの状況、そして今後の方向性が一層深刻なものとなっています。

80%

データ漏洩の 80% 以上が、アイデンティティを狙った攻撃に起因している

（出典：Verizon）

180%

アイデンティティを狙った攻撃は、前年比 180%のペースで増加している

（出典：Verizon）

19 億

2023 年には、Fortune 1000 企業から従業員のセッション Cookie 19 億件が窃取された

（出典：Fortune）

アイデンティティこそがセキュリティの根幹

脅威環境を見ると、アイデンティティを狙う脅威が増大し、リスクが拡大しています。

しかし、アイデンティティは、最大のリスクの発生源であると同時に、最大のチャンスでもあります。

アイデンティティをセキュリティ戦略の中心に据え、その基盤とすることで、アイデンティティを単なるリスク要因として放置せず、攻撃者に先手を打ち、深刻な侵害を防ぎ、テクノロジーやセキュリティ投資の価値を最大化する戦略へと転換できます。

最新のアイデンティティ戦略を推進するための3つの原則

ここまで、アイデンティティ優先のセキュリティの重要性について検討してきました。次に、より実践的な内容に踏み込み、組織のアイデンティティを現在の状態からあるべき姿へと導く方法を見ていきましょう。

最新のクラウドネイティブなアイデンティティソリューションは、管理の断片化がもたらす課題を迅速に解決するための近道を提供します。こうしたソリューションは、すべてのシステムやアプリケーションを一元的に制御してリアルタイムで可視化するので、IT およびセキュリティチームは盲点を排除し、リスクを特定し、対応速度を向上できるようになります。

ソリューションがもたらす大きな価値は、次の 3 つに分類できます。

全体的な可視性
脆弱性が見落とされたり、対処されずに放置されたりすることがないようにする

オーケストレーションの強化
潜在的な侵害が発生した際に、リアルタイムで修復を徹底する

広く深い統合
セキュリティおよび技術スタック全体にわたって、完全な接続性の価値を引き出す

最新のアイデンティティソリューションを選定する際には、プラットフォームがこれら 3 つの要素をすべて満たすこと確認してください。

okta

第 1 の原則

全体的な可視性

個別のアプリケーションやシステムごとにアクセス許可を管理すると、悪用されやすいセキュリティの抜け穴が生じやすくなり、人的ミスによるアクセスポリシー違反が頻繁に発生するリスクが高まります。

最新のアイデンティティソリューションであれば、チームがアクセスのプロビジョニング / プロビジョニング解除を一元化して簡素化するためのツールを備えています。また、管理時と実行時の両方において、組織全体のアイデンティティ脅威を包括的かつリアルタイムに可視化し、従業員、パートナー、顧客に対して安全でシームレスなエクスペリエンスを確保することが求められます。

管理時

- ガバナンスツール：きめ細かい制御と自動化対応のプロビジョニング / プロビジョニング解除を提供し、すべてのシステムやアプリケーションにわたるアクセスを包括的に可視化する
- セキュリティ態勢管理ツール：組織全体のセキュリティの脆弱性やカスタマーアイデンティティの分析・監視を容易にする

実行時

- 特権アクセス管理（PAM）ツール：IT チームやエンドユーザーに過度な負担をかけることなく、特権情報を保護するために特化した機能を提供する
- リアルタイムの脅威対策：自動化と組織全体のリスク監視を活用し、潜在的な脅威に迅速かつ効果的に対応する

チェックリスト：貴社のアイデンティティソリューションは ...

- ☐ すべての社内のシステム、デバイス、タイプ、顧客アカウントにわたって、包括的に脅威を可視化できますか？
- ☐ アイデンティティプロバイダーからのファーストパーティシグナルだけでなく、技術スタック全体からのサードパーティシグナルも取り込み、脅威に対する包括的かつリアルタイムの可視化を実現できますか？
- ☐ すべてのツールを自動スキャンし、統合されたゼロトラストフレームワークのセットに基づいて設定を評価できますか？
- ☐ 脆弱性やセキュリティの抜け穴を事前に特定し、悪用される前に対処できますか？
- ☐ MFA 適用の不備、アカウントの無秩序な増加、脆弱な顧客認証ポリシーなど、重大な構成ミスやセキュリティの抜け穴を継続的に監視・特定できますか？
- ☐ 従業員の異動時や顧客のリスクプロファイルが変化した際の、プロビジョニング / プロビジョニング解除を自動で実行できますか？
- ☐ 特権情報に対して、ユーザーやユースケースに応じてカスタマイズ可能なセキュアなアクセスを提供できますか？
- ☐ 人間以外のアイデンティティを検出し、きめ細かい許可を設定することで、自社の攻撃対象領域を縮小できますか？
- ☐ 従業員の情報と許可を一元管理するために、人事ソフトウェアやディレクトリと統合できますか？
- ☐ 顧客アカウントを大規模に管理・保護するために、カスタマーアイデンティティと連携できますか？

第 2 の原則

オーケストレーションの強化

断片化されたセキュリティスタックは、リスクや潜在的脅威に関する膨大なデータを生み出します。しかし、これらのデータを分析し対応するための、アイデンティティを基盤とした統合ツールがなければ、チームはログの精査に追われ、どのリスクに即時対応すべきかの判断が遅れてしまいます。その結果、セキュリティ対策が後手に回り、リアルタイムの修復が不可能になります。

最新のアイデンティティソリューションであれば、チームが潜在的脅威をリアルタイムで防止・検知し、迅速に修復できるツールを備えています。前のページで述べた包括的な可視性に加えて、組織にはアイデンティティを基盤とした機能が必要です。これにより、この包括的な可視性を理解して適切に対応するプロセスが簡素化され、攻撃者が実害を及ぼす前に阻止できるようになります。

チェックリスト：貴社のアイデンティティソリューションは ...

- ☐ 自動修復アクションの設定作業を簡素化できますか？
- ☐ リスク要因、ポリシーなどのコンテキストに基づいて修復アクションをきめ細かくカスタマイズできますか？
- ☐ 潜在的な侵害を防ぐために、ユニバーサルログアウトなどの堅牢な対応をトリガーできますか？
- ☐ フィッシング耐性のある認証ツールと継続的に連携し、修復戦略を改善し続けることができますか？
- ☐ アクティブなセッション中にデバイスのセキュリティチェックを実行できますか？
- ☐ 悪意のある IP アドレスを事前にブロックできますか？
- ☐ 安全かつ簡単な利用のため、従業員や顧客がセルフサービスでフィッシング耐性のある要素の回復を設定できますか？
- ☐ ユーザー認証後も継続的に脅威を検知できますか？

第 3 の原則

広く深い統合

技術スタックの強みは、どれだけのレベルの統合を実現できるかにかかっています。技術スタックの各要素がシームレスに統合されていなければ、テクノロジーやセキュリティへの投資の価値を最大限に引き出し、最大限の ROI を達成することは不可能です。

最新のアイデンティティソリューションであれば、あらゆる要素を連携させることで、新たなレベルのリスク管理と効率性を実現できます。ベンダーニュートラルなアイデンティティプラットフォームなら、このような統合を実現し、開発者や IT チームがカスタムのコードを記述する負担を担う必要もありません。

チェックリスト：貴社のアイデンティティソリューションは ...

- ☐ 自社の主要エンタープライズ SaaS アプリケーション（CRM、生産性向上、コラボレーション、ERP、IT 運用管理など）とシームレスに統合できますか？
- ☐ 高度なアイデンティティセキュリティ機能を備え、シンプルなプロビジョニングやシングルサインオンだけでなく、ログイン前からログイン時、そしてログイン後まで含めたアプリの保護を提供できますか？
- ☐ セキュリティスタックの中核部分と統合して、リスク監視、脅威検知、修復を強化できますか？
- ☐ 開発者や IT チームがノーコードオプションを利用して、アプリケーション全体で機能をトリガーする自動化フローを簡単に構築できますか？
- ☐ 将来的に追加で導入するアプリケーションやシステムとも継続的に接続するために、拡張機能を利用できますか？

統合セキュリティ戦略の成果

アイデンティティ優先の統合セキュリティは、単なる概念ではありません。現実の運用においては、一連の具体的な成果が組み合わさることで、重要な資産の保護、日常業務の効率化、そしてあらゆるビジネス運営におけるパフォーマンス向上といった、測定可能な影響をもたらします。

- あらゆるアイデンティティ脅威の可視化とリアルタイムの修復
- 完全かつ信頼性の高いゼロスタンディング特権 / 最小権限の原則
- 実績のあるゼロトラスト
- 人間以外 / マシンのアイデンティティに対するコントロールの強化
- テクノロジーおよびセキュリティ投資の最大活用

統合セキュリティ戦略の主な 5 つの成果に関する詳細をご確認ください。

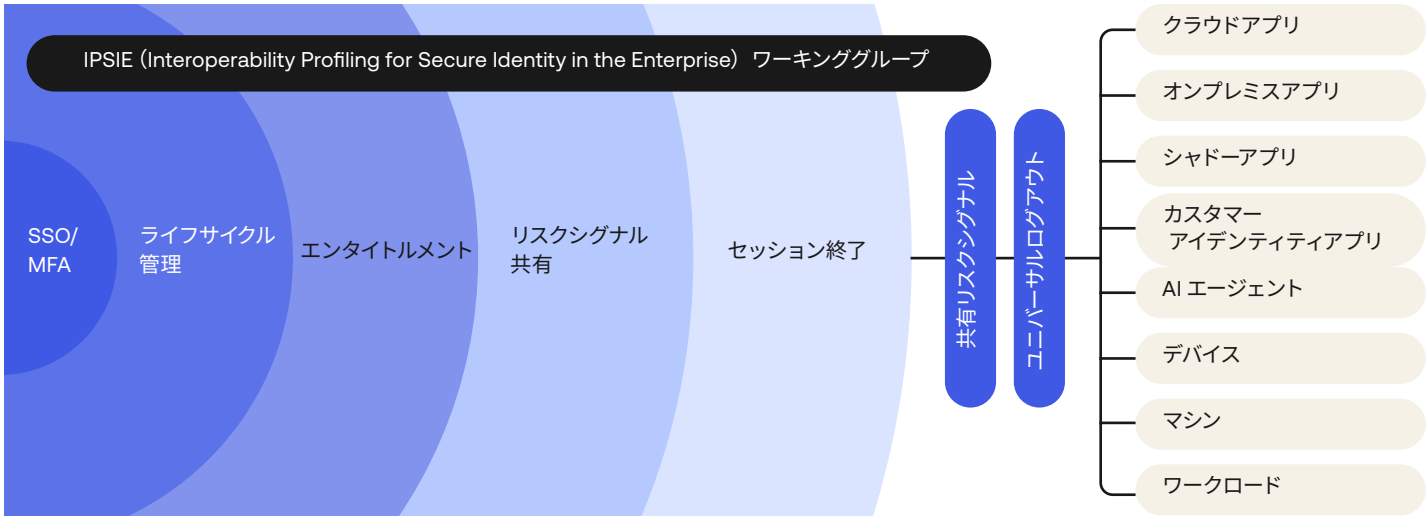
アイデンティティ優先のセキュリティの実現に向けて

アイデンティティ優先のセキュリティを全面的に実現することで、オープンなエコシステムを支え、あらゆるアプリ、システム、ツールの構築と利用を容易にして効率化し、保護できるようになります。これにより、セキュリティと管理性をデフォルトで確保できます。

アイデンティティのサイロ、高コストで時間のかかるカスタム統合、そして IT 環境や顧客環境におけるセキュリティの抜け穴や盲点も排除できます。デフォルトで安全を確保し、シームレスな機能を設計に組み込み、高パフォーマンスな技術スタックを実現できます。

最新のアイデンティティセキュリティ標準

OpenID Foundation の IPSIE（Interoperability Profile for Secure Identity in the Enterprise）ワーキンググループは、この理想を実現するための最新の取り組みです。



IPSIE は、初の統一的なアイデンティティセキュリティ標準として、現代の環境に適合し、完全に統合されたエコシステム実現への道を示します。これにより、企業はアイデンティティセキュリティに関する主導権を取り戻すことができます。

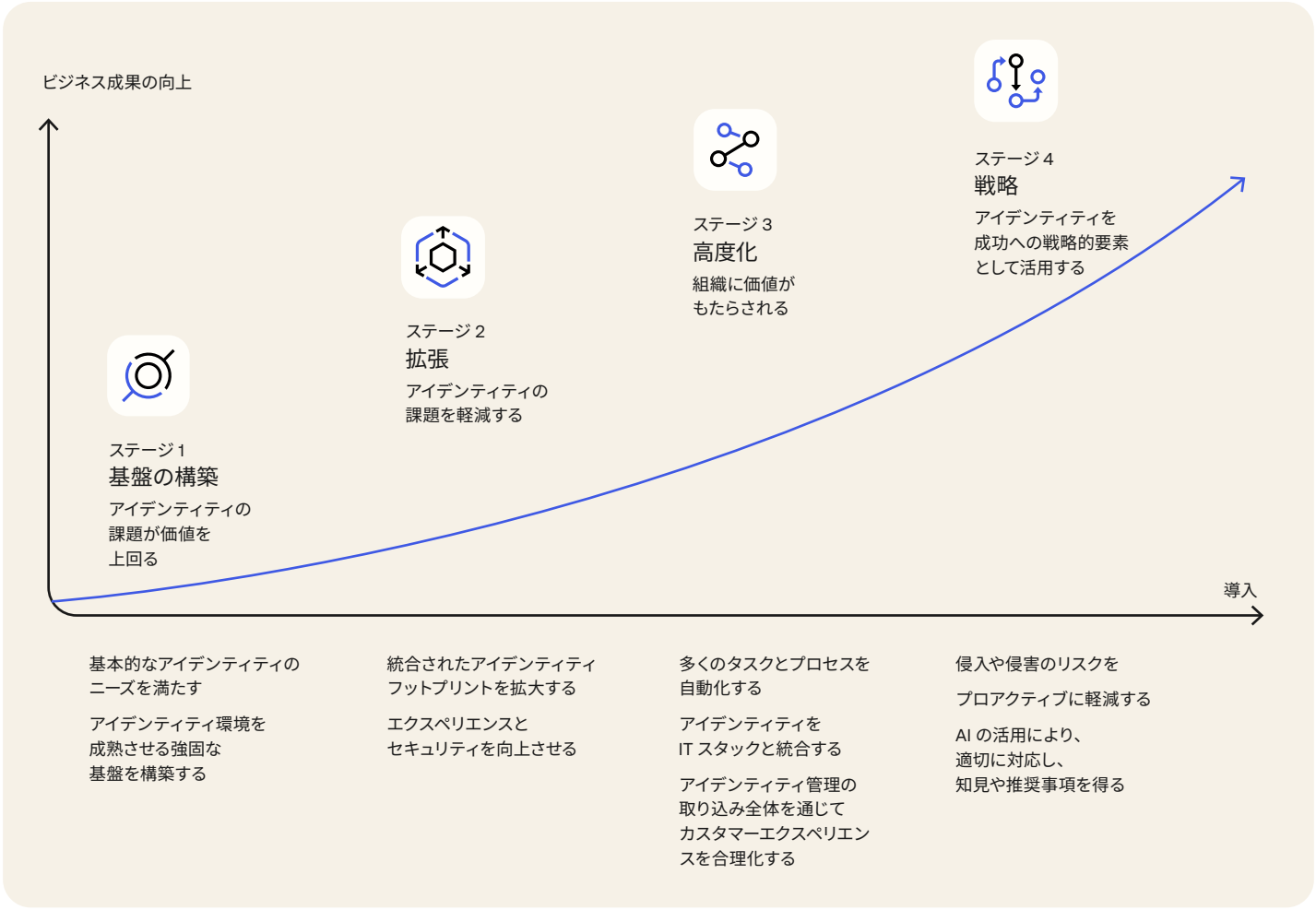
アイデンティティの成熟度を高める方法：

Okta のアイデンティティ成熟度モデル

アイデンティティの最新化とセキュリティ戦略の統合は、セキュリティチームや IT チームにとって大きな負担となります。さらに、これは一度の取り組みで完了するような単純な課題ではなく、最新のアイデンティティ戦略を構築するには、継続的な改善の積み重ねが必要です。

こうした理由から、Okta はアイデンティティ成熟度モデルを開発しました。このモデルは、あらゆる業界の組織に対し、専門家の知見や業界のベンチマークに基づくフレームワークを提供します。これを指針として活用することで、複雑な課題を乗り越え、自信を持って組織を前進させることが可能になります。

組織が直面する課題は、アイデンティティ成熟度の段階によって異なります。アイデンティティ成熟度モデルはこの点を考慮し、各段階に応じた具体的なガイダンスを提供します。優先課題の特定、進捗の測定、望ましいビジネス成果の達成において、非常に有用なリソースです。



アイデンティティをセキュリティの要に

これ以上ないほど重要なことですが、アイデンティティこそがセキュリティの根幹です。攻撃者の一歩先を行き、回復力と持続可能性のあるセキュリティを確立することが重要です。そのために、セキュリティおよび IT のリーダーは、アイデンティティソリューションの近代化とその可能性を最大限に引き出す具体的な取り組みを進める必要があります。

アイデンティティを保護することは、組織の未来を守ることにつながります。巧妙化する脅威や、AI を活用した新たな攻撃に対抗することで、シームレスかつ自動化されたセキュリティ、IT、顧客環境がもたらす競争優位性を確保できます。

アイデンティティ成熟度の向上を目指し、Okta の専門家から的確な推奨を受けるには、こちらで詳細をご確認ください。また、当社のチームにお問い合わせください。

okta

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