ホワイトペーパー

アイデンティティガバナンス バイヤーズガイド

目次

なぜ今、アイデンティティガバナンスが重要なのか

世界中でより多くの人がより多くのデバイスやリソースを利用するようになり、それに伴って職場でのデジタルアイデンティティが爆発的に増加しています。クラウドや SaaS の導入、リモートワーカーや契約社員のアクセス、モバイルデバイスの利用といった要因によって、アイデンティティ管理がさらに複雑化しています。IT チームとセキュリティチームは、従業員の生産性を維持しながら、適切なユーザー、適切なリソース、適切な時間にアクセスを制限する必要がありますが、これは難しい課題です。アイデンティティの管理が不十分だと、アイデンティティのライフサイクル全体にわたってセキュリティギャップが生じ、組織が侵害の危険にさらされる可能性があります。同様に、ユーザー、リソース、アイデンティティストアが相互に関連し合うエコシステムを管理する中で、手作業のプロセスやワークロードが発生する可能性があります。その負担は、社内の人材やテクノロジーのフットプリントの拡大に応じて大きくなります。このため、企業の 61% が、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 の優先事項と考えるようになっています[1]。

アイデンティティガバナンス / 管理（IGA、Identity Governance and Administration）は、多様なリソースとアイデンティティのリポジトリにわたって複雑なアクセス権を管理します。IGA は、以下を組み合わせたものとなります。

- アイデンティティガバナンス：ロールの管理、アクセスのレビューまたは認定、職務分掌、ログ管理、アナリティクス、レポーティングを対象範囲とする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、サービスアカウント、デバイスのプロビジョニング / プロビジョニング解除、エンタイトルメントの管理

アイデンティティガバナンス / 管理（IGA）は、以下の質問に答えます。

- 誰が何にアクセスできるのか？
- いつアクセス権を取得したのか？
- どのようにアクセス権を取得したのか？
- 今後もアクセス権を持ち続けるべきか？
- アクセスがコンプライアンスに抵触するか？

[1] 2023 Trends in securing digital identities、Identity Defined Security Alliance

IGA を導入するメリット

IGA ソリューションは、コンプライアンスやアイデンティティのコントロール要件に重点を置いていると考えられがちですが、他にも利点があります。

- **最小権限アクセスで、セキュリティ結果を改善：**ゼロトラスト戦略の一環として、リソースへの最小権限アクセスを導入し、ユーザーに与える許可を業務に必要な最小限に抑える組織が増えています。IGA は、ユーザーとリソース全体に一貫した最小権限のアクセスコントロールをきめ細かく実装することで、リスクベースのサイバーセキュリティプログラムに反映させることができます。
- **運用を効率化：**IGA を適切に導入することで、ユーザーや IT チームの一般的なタスクを自動化し、生産性と満足度を向上させることができます。たとえば、アクセス要求の自動化によって、ユーザーに新しい許可を与えるプロセスを合理化できます。また、プロビジョニング / プロビジョニング解除に自動化を活用することで、手作業によるデータ入力を減らし、入力ミスに伴うリスクを軽減できます。
- **SaaS の可視化とソフトウェアの合理化：**アプリとエンタイトルメントへの最小権限アクセスを実装することで、過剰なプロビジョニングと、余分なソフトウェアのライセンスと保守に関連するコストも削減できます。IGA は、過剰にプロビジョニングされたアプリケーションを検出して修復する機能も持ちます。

IGA の導入におけるテクノロジー面の課題

大多数の組織が IGA ソリューションへの投資を優先事項と考えている一方で、採用には大きな障壁があります。

- **アイデンティティストアの断片化：**クラウド、オンプレミス、ハイブリッドの環境ごとに異なるアイデンティティリポジトリを使用している組織が多く、そのような場合には「信頼できる唯一の情報源」が確立されず、アイデンティティのサイロ化が発生します。同様に、フルタイム従業員には人事システムを使用する一方で、それ以外の契約社員などの人材は別のシステムで管理しているケースも多く見られます。セキュリティとアイデンティティの専門家に、自社がアイデンティティの安全性を高める上でどのような障壁があるかを尋ねたところ、以下の理由が最も多く挙げられました。

> 「複数のベンダーとさまざまなアーキテクチャを使用するために、アイデンティティのフレームワークが複雑化し、これが障壁となっている[2]」

- **多様なテクノロジーエコシステム：**テクノロジー環境が複雑化すると、多くの異なるリソースと IGA システムの接続や統合が必要となり、採用の障壁となります。それぞれのコネクタや統合の作成には、開発、テスト、保守の専門スキルが必要です。パブリッククラウドと SaaS の導入がそれぞれ年率 21%、18% の勢いで増加[3]する中、ユーザーが各自のロールや許可を使用して幅広いリソースに適切なアクセスと許可を持つように確保することは、非常に複雑なタスクになりつつあります。これが過剰なプロビジョニングにつながり、ビジネスをリスクにさらすこともあります。ある報告では、IaaS のアカウントの 95% 以上は、付与されたエンタイトルメントの 3% 未満しか使用していないことが示されています[4]。
- **複雑なテクノロジーオーナーシップ：**事業部門や部署は、組織のコンプライアンスポリシーにしたがって独自のソフトウェアツールを使用していることがあります。このために、IT チームやガバナンス / リスク / コンプライアンス（GRC、Governance, Risk, and Compliance）チームは、最小権限を有効にし、チームの管理対象外となるリソースのコンプライアンス監査を監督するという困難な立場に置かれます。このような可視性とコントロールの欠如は、セキュリティとコンプライアンスのギャップにつながります。

以上の課題を念頭に置いて、IGA ソリューションを選定する際の考慮事項を見ていきましょう。

[2] 2023 Trends in securing digital identities、Identity Defined Security Alliance

[3] Forecast: Public Cloud Services Worldwide, 2021-2027, 1Q23、Gartner

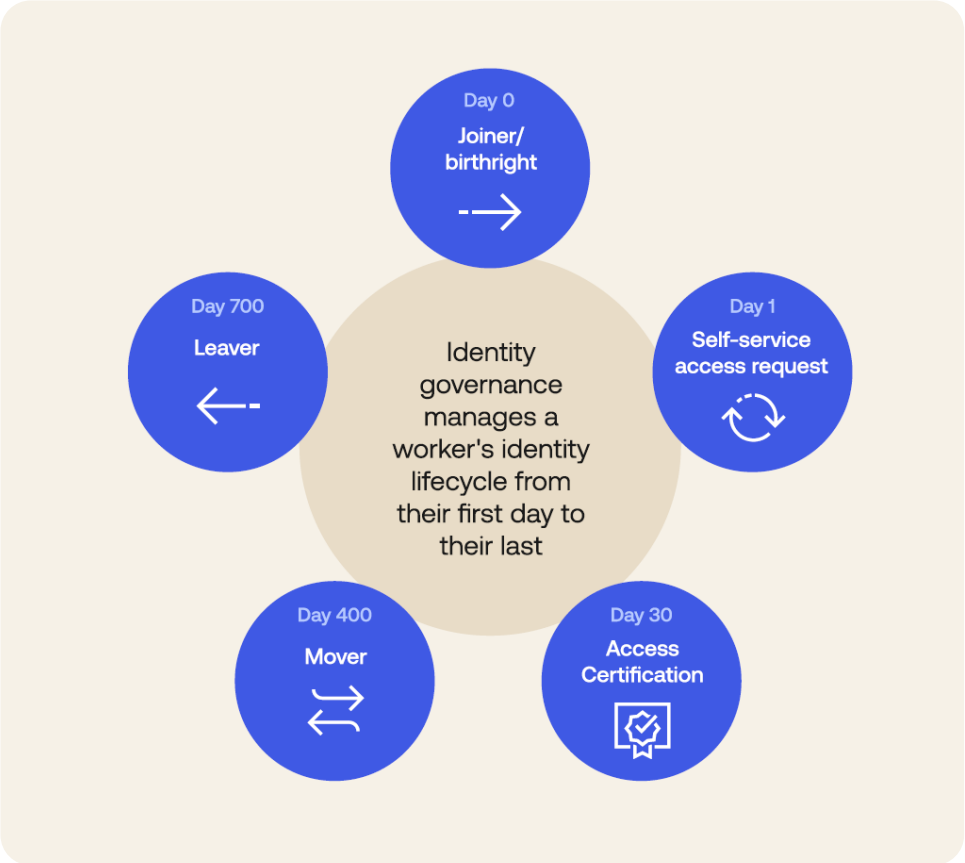
[4] Innovation Insight for Cloud Infrastructure Entitlement Management、Gartner

IGA のユースケース

IGA ソリューションを選択する前に、組織がどのような機能を必要としているかを最初に明確化する必要があります。アイデンティティガバナンスには多くの用途がありますが、以下が最も一般的なユースケースとなっています。

- **アイデンティティのライフサイクル管理：**クラウドとオンプレミスのリソースにまたがる組織の入社 / 異動 / 離職プロセスを管理します。たとえば、アプリケーションのアクセス要求や、アプリケーション内のきめ細かなエンタイトルメントベースのアクセスコントロールなどを対象とします。
- **最小権限アクセス：**ゼロトラスト戦略をサポートし、アイデンティティリスクの管理を強化します。そのために、ロールやプロジェクトごとに必要なアクセスのみに制限するプロセスを作成します。
- **コンプライアンス：**アクセス要求、正当化、承認、レポーティング、および定期的なアクセス認定を文書化するプロセスを確立します。これにより、さまざまな規制枠組みのコンプライアンス要件を満たします。

組織によっては IGA ソリューションのユースケースが複数ある場合もあるでしょうが、まずは 1 つのユースケールに絞って導入するのがベストプラクティスとなります。



IGA の機能

組織のユースケースや目標によっては、IGA ソリューションのすべての機能が必要でない場合もあります。以下の表は、各機能の概要と、自社に必要な機能を選択する際に考慮すべき特徴や要素を示しています。

機能	詳細	考慮事項
ユーザーとアプリケーションのプロビジョニング / プロビジョニング解除（アイデンティティライフサイクル管理とも呼ばれる）	人事部門などのシステムと統合して、新しいユーザーアカウントを作成し、ユーザーの属性に基づいて必要なアプリをプロビジョニングし、各ユーザーの開始日にアイデンティティやアカウントが有効になるようにスケジュールを設定する。同様に、ユーザーの離職、異動、契約終了についても、人事部門などのシステムからのデータに基づいてプロビジョニング解除を設定する。これらのタスクを自動化することで、多くの手作業に頼ることなく、従業員が初日から円滑に業務を開始できる。	• 統合が必要なデータソースの数と種類（人事システム、LDAP、Google ディレクトリ、ダウンストリームのアプリケーション、CSV ファイル） • オンデマンドですべてのアプリのプロビジョニング解除を迅速に実行する機能（離職や契約終了の場合） • ダウンストリームのアプリケーションやリソースとの統合を容易に実行する機能
アクセス要求	ユーザーが新しいアプリへのアクセスを要求し、承認者が要求のレビューと承認 / 拒否を行うプロセスを合理化し、正式に文書化する。最小権限のアクセスは、多くの場合に、ユーザーがロールやプロジェクトの変更に基づいてアクセスを要求する必要があることを意味する。	• アクセスレビューのフローと承認の柔軟性 • 時間制限のある要求フローを作成できるか • ユーザーがセルフサービス要求を簡単に開始できるか • ユーザー / 承認者に要求の進捗状況をどのように通知するか • レビュアーにユーザーコンテキストを提供できるか
アクセスのレビュー / 認定	リソースへのユーザーアクセスを定期的にレビューすることで、監査に対応し、不適切なアクセスのリスクを軽減し、特権の累積を回避し、非アクティブなアカウントを特定する。	以下の機能を利用できること： • ユーザー、グループ、リソース別にキャンペーンを実施する • アクセスキャンペーンをスケジュールする • オンデマンドでキャンペーンを実施する • ユーザーの異動などのイベントに基づいて、認定プロセスを自動的に開始する

機能	詳細	考慮事項
ワークフローのオーケストレーション	テクノロジー環境全体で運用されるワークフローの自動化 / オーケストレーションにより、コンプライアンス / リスクベースのアイデンティティガバナンスプロセス全体にわたる運用の最適化と効率化を実現する。	• 管理者がワークフローを作成できるか（専門の開発者を必要とせずに、ノーコードまたはローコードで作成できるか） • 管理者が複雑なワークフロー（ループや分岐）を作成できるか • 監査 / コンプライアンス向けのプロセスと結果がどのように記録されるか • 管理者がカスタムのワークフローを作成できるか
レポーティングとアナリティクス	アイデンティティガバナンスのデータを追跡および提示する。アクセスリスクの低減、アクセス要求の合理化などの目標を達成するために、データを収集して分析する。	• 標準搭載レポートを利用できるか • カスタムレポートをどの程度簡単に作成できるか • レポーティングやリスクシグナルの検出のために、エコシステム全体の可視性を提供するか • オンデマンドでレポートを実行し、監査向けに証拠を提供できるか
エンタイトルメント管理（きめ細かなエンタイトルメント）	エンタイトルメント（ユーザーがアプリケーションで特定のアクションを実行できるようにする許可）の検出、プロビジョニング、更新、取り消しを実行する。	以下の機能を利用できること： • オンプレミスとクラウドアプリを検出 / 管理する • 休眠状態のエンタイトルメントを検知する • 規制対象のエンタイトルメントを特定する
職務分掌 (SoD、Segregation of Duties)	個人が単独で機密性の高いタスクを遂行できないように、コントロールを定義し、管理する。不正行為、妨害行為、窃取、ポリシー違反、情報の不正使用など、データ侵害につながるセキュリティインシデントの発生を最小限に抑えるため、IT アクセスの過剰付与を防ぎ、悪意ある活動が行われないようにする。	• 不適切な権限の組み合わせを構成で防止できるか • 適用可能なアプリや組み合わせの数に基づいて、適切な規模を維持する

ベストプラクティスの導入

緩和策

IGA ソリューションには多彩な機能が含まれ、多くの用途に対応します。しかし、どのようなプロジェクトにも当てはまることですが、目に見える成果を上げる最善の方法は、ユースケースを1つだけ選んで完了まで見届けることです。IGA の導入を成功させるためには、どのユースケースを最初に導入し、どの要素をプロジェクトに組み込むかについて、ビジネスレベル（理想的には経営幹部レベル）で合意を得る必要があります。この選択は、組織がどのような優先課題や悩みを抱えているかによって異なります。たとえば、現場チームが大規模で広範囲に分散している場合には、CRM アプリへのアクセス要求やエンタイトルメントの自動化とガバナンスを最優先事項と判断するかもしれません。スタッフの入れ替わりが激しく、IT サポートの待ち時間が長い場合には、入社 / 離職プロセスを自動化することを優先するかもしれません。 また、金融規制のコンプライアンスを満たしていることを実証するために多くの費用と労力を投じている場合には、規制関連アプリケーションへのアクセスやエンタイトルメントのガバナンスを優先するかもしれません。プロジェクトを定義するためには、以下のような情報が必要になります。

- ソフトウェア資産のインベントリ（技術面とビジネス面のオーナーをそれぞれ明確化するため）
- アイデンティティのデータソース
- プロジェクトで優先させるアプリケーション

最初のユースケースが試験導入であれ、本格的なプロジェクトであれ、アプリケーションとエンタイトルメントの数を制限することをお勧めします。Okta やお客様の経験から、まずは少数のアプリケーションを対象とし、大まかなアクセス設定で開始しましょう。エンタイトルメントを使用する場合は、1つのアプリケーションから始めます。これにより、得られた教訓をその後の IGA フェーズに生かすことができます。

設計段階からコンプライアンスに準拠したアイデンティティ管理プロセスを確立する

どのテクノロジーを導入する場合も、事前にステークホルダーが協力して、リソースのアイデンティティ管理ポリシーを定義し、「誰がいつ、何に、どのくらいの期間アクセスできるか」を正式に文書化することが重要です。IGA の展開では、典型的なテクノロジーステークホルダーには IT チーム、GRC チーム、セキュリティチームが含まれます。対照的に、ビジネスステークホルダーは多くの場合に、人事チームなど、データソースシステムを所有しているか、または IGA ソリューションと重要な関わりを持つ部門となります。適用範囲内のリソースについて、規制コンプライアンスの最高水準を満たすプロセスを確立することで、四半期または年次の監査に関連する負担の多くを取り除くことができます。

こうしたプロセスは、どのようなユースケースを優先させるかによって異なりますが、以下のような例が挙げられます。

- 必須アクセスのために、属性またはロールに基づくアクセスコントロールのアプローチを定義する
- 入社 / 異動 / 離職といったライフサイクルのプロセスを定義する
- 機密性の高いアプリケーションやデータに対する適切な認証ポリシーを決定する
- アクセス要求による臨時アクセスのプロビジョニングについて、プロセスを正式に文書化する
- 定期的かつ自動化されたアクセス認定を確立し、ユーザーやアプリ、接続先リソースに適切な承認者を特定する
- ユーザーの異動など、アドホックのユーザーレビューを実施するタイミングを決定する
- ビジネスプロセス全体で不適切な権限の組み合わせを特定し、違反を防止して監査に対応するための対策を導入する

この作業は、要求のワークフローを簡素化して標準化する絶好の機会となります。Gartner は、「Critical Capabilities for Identity Governance and Administration」（2018 年 6 月）レポートで、IGA プロジェクトはビジネスプロセスのリエンジニアリングに焦点を当て、アプリケーションごとに独自の承認ワークフローではなく、すべての要求に統一的で一貫性のある承認ワークフローを採用するよう努めるべきであると強調しています。さらに、ポリシーの分析、マネージャーの承認、リソースの承認、コントロールの承認という 4 段階のシンプルなパターンすらも推奨しています。当然ながら、分岐やループなどのアクションが必要なビジネスプロセスもあり、これをすべてに適用できるとは限りません。しかし、IGA を導入する前にこうしたプロセスを定義することが、製品の選択とプロジェクト範囲の絞り込みに役立ちます。

この作業には、IGA システムが接続する必要があるアプリケーションやリソースを定義し、必要な統合の深さを明確にするという利点もあります。

「信頼できる唯一の情報源」を確立する

ユーザーアクセスを効果的に管理するには、アイデンティティストアとの統合、そしてガバナンス対象となるダウンストリームリソースとの統合を実現することが前提となります。

組織はさまざまなアイデンティティストアを特定して、IGA ソリューションと深く統合するよう取り組む必要があります。これにより、属性のマッピングと同期が可能になり、複数のソースを密接に反映できるようになります。IGA システムは、人事情報システム（HRIS）、LDAP、ダウンストリームアプリケーション、CSV ファイルなど、幅広いディレクトリや複数のソースと統合できる柔軟なソーシングモデルを備えている必要があります。

IGA システムはさらに、プロビジョニング / プロビジョニング解除のアクションを通じて、ダウンストリームリソースに属性やロールを適用できなければなりません。クラウドとオンプレミスのユースケースに適合するように、広範なアプリケーションにまたがって、大まかなエンタイトルメントときめ細かなエンタイトルメントの両方の統合が可能かどうかを確認してください。このとき、実装に大規模な専門サービスを必要とする統合ではなく、簡単に構成できる統合であることが重要です。

アイデンティティプロセスを自動化する

プロセスを自動化することで、運用を効率化し、エンドユーザーエクスペリエンスを向上させ、リスクの原因となり得る構成ミスを削減できます。まずは、人事システムから取得したアイデンティティを使用して、プロビジョニングを行い、属性ベースまたはロールベースのアクセスコントロールを構築します。従業員の入社や異動があると、人事の更新が新しい属性やロールに自動プッシュされます。これにより、グループのメンバーシップやリソースへのアクセスが更新され、この変更が監査向けに文書化されます。

アクセス要求やアクセス認定のプロセスでも、自動化が大きな役割を果たすことがあります。手作業の必要性を排除し、正当な理由や管理者の承認タイミング、期限付きのアクセスなど、GRC チームが監査人に提供するための一貫したデータ収集を確立できます。

GRC チームがより深く、より広範に自動化を設計することで、監査人がプロセスをテストする頻度は少なくなります。自動化の設計が機能していることを IT チームや GRC チームが証明できれば、個々のアクセスコントロール手段に頼るのではなく、所定の設計に対する変更をチェックするだけで、監査人がコンプライアンス違反の有無を確認できます。

定期的なフロー以外にも、特定のイベントをきっかけとして自動プロセスを開始するように構築できることを確認します。たとえば、重要なリソースに対して高リスクのログインイベントが発生した場合に、そのイベントをきっかけとしてユーザーのアクセス能力のレビューを自動的に開始するように設定できます。

意思決定の強化を支援する

情報に基づいて適切なタイミングでアクセス決定を行うには、適切な人を適切なタイミングで適切なプロセスに結び付ける必要があります。適切なステークホルダーをガバナンスのワークフローに組み込むことで、マネージャーやアプリケーションオーナーを追跡する手間を省き、コンプライアンスを証明するための監査証跡を作成できます。具体的には、以下の点を検討します。

- **ワークフローの構成：**アクセス要求や認定キャンペーンについて、適切なレビュアーを適切な順序で選択します。アクセス要求のベストプラクティスであれば、まずユーザーの管理者にレビューしてもらい、次にリソース / アプリケーションのポリシーオーナーにレビューしてもらい、その後に情報セキュリティ担当者にレビューしてもらうといった流れが考えられます。
- **シンプルで一貫したエクスペリエンスの提供：**レビュアーが意思決定を行うために必要なコンテキスト情報を、できれば単一画面で確認できるようにします。重要な情報の例としては、アクセス要求を申請しているユーザーの役職 / 所属部署 / 申請理由、特定のプロジェクトへのアクセスの必要性に関するマネージャーのコメント、適切なアクセス期間に関するセキュリティチームのコメントなどが挙げられます。
- **自動プロセスの確立：**チームの情報共有と生産性を維持するため、アクセスガバナンスの要求と決定を自動配信します。たとえば、あるユーザーがアクセスを取り消された場合には、ユーザー本人とマネージャーに通知し、アクセスの復元を希望する場合に備えます。同様に、ユーザーがアクセスを要求した場合には、すべてのステークホルダーが要求の進捗状況を簡単に確認できるようにし、レビュアーが簡単にフォローアップできるリマインダーにより生産性を維持します。

IGA ソリューションの評価ポイント

ユースケースに関係なく、導入を迅速化・効率化して成功させるためには、以下の主要ポイントをおさえることが重要です。

統合アイデンティティプラットフォーム

オンプレミスシステムを廃止してクラウドにワークロードを移行するのに伴い、アイデンティティおよびアクセス管理（IAM）、特権アクセス管理（PAM）、IGA システムが対応する課題の領域が重複するようになります。2025 年までに、新たに導入されるアクセス管理、ガバナンス、特権アクセス管理の 70% は、IAM プラットフォームの機能として集約されるようになると予想されます [5]。

統合プラットフォームには、運用上の利点が多くあります。組織のすべてのアイデンティティを一元的に管理することで、以下のメリットが実現します。

- **アイデンティティリスクの軽減：**統合プラットフォームが提供する包括的なビューは、アイデンティティ脅威を検知して対応するための貴重な洞察を提供できます。たとえば、IAM が提供するリスクシグナルは、ガバナンスや特権アクセスの意思決定に役立つとともに、レビューを促す要因となります。ログイン時のユーザーの行動に基づいてリスクプロファイルが上昇したことをきっかけとして、認定キャンペーン、ユーザー権限の制限、リソースへのアクセス停止などを開始することが可能です。
- **価値実現の迅速化：**アイデンティティ、アクセス、ガバナンスを一元的に管理することで、導入に要する期間を短縮し、複数のシステムを保守するコストを削減できます。
- **ユーザーエクスペリエンスの向上：**エンドユーザーと管理者が単一のインターフェイスで要求、プロセス、決定を実行できるようにすることで、ミスが減り、組織内のすべての人々の生産性が向上します。

統合サポート

最低でも、アイデンティティガバナンスソリューションは、人事情報システム（HRIS）、その他の記録システム、データストア、IAM システムなど、多様なアイデンティティソースと情報を交換する必要があります。自動化を追加すると、IGA システムは技術スタックの多くのアプリケーションと統合できるようになります。たとえば、IT サービス管理（ITSM）システムとの統合により、アクセス要求を開始するユーザーのプロセスを簡素化でき、コラボレーションツールとの統合により、アクセス要求をレビューするユーザーの承認プロセスを簡素化できます。

[5] Gartner Research

それぞれの統合は、構築に数週間から数か月かかり、継続的な保守とサポート費用を必要とします。統合の数が増えると、アプリやデータストアへのコネクタの作成と保守も複雑になっていきます。統合のサポートは、IGA ソリューションの導入を検討しているお客様が抱える最大の懸念となっています。開発やカスタマイズの必要性が高ければ高いほど、導入が長期化します。

必要なアプリやリソースとの構成可能な統合が標準搭載された IGA ソリューションは、カスタム統合の構築、テスト、保守に伴う負担を軽減します。

使いやすさ

IGA を導入することによる成果としては、セキュリティとコンプライアンスの実現が重視されますが、そのために使いやすさが損なわれてはなりません。IGA の導入により、ユーザーがアプリケーションやシステムへのアクセスを要求して許可を得る方法が変更されるため、組織内のすべてのユーザーが影響を受けます。エンドユーザーがアプリケーションへのアクセス要求やアクセス許可の変更を簡単に実行できるようにすることで、トレーニングの必要性を減らし、アクセス要求の利用を促進し、生産性にプラスの影響を与えます。

エンドユーザーエクスペリエンスは、以下のような方法で改善できます。

- IGA システムと使い慣れたコラボレーションツールを接続し、エンドユーザーが使い慣れたインターフェイスからアクセス要求を管理できるようにする
- リアルタイムのワークストリームを通じて、エンドユーザー自身がアクセス要求を追跡し、承認プロセスを監視できるセルフサービスエクスペリエンスを構築する

また、IGA ソリューションを管理する担当者にとっての使いやすさも考慮する必要があります。管理の効果は、以下のような方法で高めることができます。

- スクリプトに頼らず、ノーコードツールを活用してワークフローを構築する
- アクセス認定の開始やレポート作成に必要なコンソールとタスクの数を最小限に減らす
- プロジェクトグループに対するアクセス要求やエンタイトルメントなど、一括アクションを活用する
- フィルタリング機能により、ユーザー別やリソース別のレポートをダウンロードできるようにする

GRC チームにとっての使いやすさも考慮すべきです。たとえば、GRC チームがアクセス認定キャンペーンを実行できれば、管理者に頼る必要がなくなり、利点となり得ます。

Okta の活用

Workforce Identity Cloud は、IAM、IGA、PAM を集約したクラウドネイティブなプラットフォームであり、比類ない視点でユーザーアイデンティティを包括的に把握できます。

Workforce Identity Cloud の SaaS 形式ソリューションとして提供される Okta Identity Governance は、複数のシステムにわたってアイデンティティとアクセスのライフサイクルを簡素化して管理し、組織のセキュリティ態勢を改善します。Okta は 7,000 以上の統合をあらかじめ組み込んで提供しており、そのうち 600 以上はアイデンティティガバナンスに直接関連するものです。こうした統合を利用することで、迅速な導入と大規模なアイデンティティプロセスの自動化が可能になります。

Okta Identity Governance は、以下のメリットを提供します。

- 重要なリソースへのアクセスの作成、保護、監査を効率化する
- セキュリティを強化する
    - 把握しきれていないアイデンティティや、昇格されたアクセスや特権アクセスの蓄積に伴うリスクを軽減する
    - サインインの頻度、リソースの最終アクセス日など、統合 IAM ソリューションからの洞察を活用することで、実効性の高いアクセス認定を実現する
    - 機密データやアプリに適切なアクセスとエンタイトルメントを与え、自動ワークフローにより適切なレビュアーがアクセスを評価・承認できるようにする
    - 不審なユーザー活動の検知や、ユーザーのロール変更をきっかけとして、ユーザー認定を開始する
- 従業員の生産性を高める
    - ユーザープロファイルの属性に基づいて、新入社員への必須アプリのプロビジョニングを自動化し、初日から生産性を発揮できるようにする
    - 業務コラボレーションツールを使用して、Okta リソースへのアクセス要求をセルフサービスで実行できる利便性を提供する

- 孤立アカウントや、アプリケーションへのアクセス許可を過剰に付与されたアカウントを検出することで、コストを抑制する
- 運用を効率化する
    - タスクを自動化して、手作業でのデータ入力やプロビジョニングにかかる時間やエラーを削減する
    - 標準搭載された統合機能を利用して一般的なアプリと接続し、他のソリューションよりも迅速かつ容易にガバナンスソリューションを導入する

Okta Identity Governance の概要は、https://www.okta.com/ja-jp/products/identity-governance/ をご覧ください。または、こちらの短い動画をご覧ください。Okta Identity Governance を利用したコンプライアンス対応の詳細については、ホワイトペーパーをダウンロードしてご覧ください。