



ID・アクセスマネジメント(IAM)のモダナイズ支援サービス

ビジネス変革・デジタルトランスフォーメーションを支えるIAM基盤の整備

今、必要なID・アクセスマネジメント(IAM)のモダナイズ

ビジネス環境の激しい変化に追従して競争上の優位性を維持・確立するために、データとデジタル技術を活用して、製品、サービス、ビジネスモデルを変革するとともに、業務・組織・プロセス・企業文化・風土をスピード感をもって変革していくデジタルトランスフォーメーション(DX)の推進が企業において不可欠となっています。

DXにおいて必要となる新しいサービスやデータを扱うITシステム・サービスでは、セキュリティ維持のため、利用者のID管理とアクセス管理(IAM)が必要不可欠な要素です。一方で、これまでのレガシーな社内システムを対象としたレガシーなID・アクセス管理では、変化していくニーズに対応することが困難です。レガシーなID・アクセス管理を場当たりに使用し続けた場合、変革の阻害、セキュリティリスクの拡大や効率の著しい低下などの弊害が発生するリスクが高まります。

変化していくニーズに対応するIAMのモダナイズの成否が、ビジネス/業務変革における成否の重要な一要素となっています。



ID・アクセスマネジメントに求められてくる新しいニーズ

IT環境の変革に伴い、新たなニーズとしてアジリティ(俊敏性)、セキュリティ、コンプライアンス、効率化が挙げられます。どのニーズへも漏れなく対応するには新しい方式が必要です。

アイデンティティ・アクセス管理に求められる新たなニーズ



アジリティ(俊敏性)

新サービス導入、新システム構築、新しいビジネスパートナーとコラボレーション開始などの変化に、俊敏な対応が必要です。IAMの対応が遅れることで変革のスピードを妨げることは機会の損失につながります。



セキュリティ

IT環境が多様化・複雑化する一方、流通・蓄積されるデータは増大とともに、機密度・重要度は増加しています。これらを守るセキュリティ施策の進化に対応できるIAMが求められています。



コンプライアンス

セキュリティやプライバシーに関して各国の法令やルール・基準が高度化しています。企業はこれらに対応できていることを証明する必要があり、ガバナンスの徹底、ログの集中管理が求められています。



効率化

新しいニーズへの対応を、利用者・管理者の工数を増加させずに実施するために、アイデンティティ情報とライフサイクルプロセスを一元管理し、定められたルールに則って極力自動的に判断・処理できる基盤が必要です。

レガシーなIAMとモダンなIAMの違い

社内ネットワーク内の業務システムのID・アクセス管理を対象として社内で独自に構築され、機能も限られていたレガシーなIAMにくらべ、モダンなIAMは、最新の業界標準方式をサポートし、多くのシステムに柔軟に対応するとともに、ガバナンス機能等の新しい機能を備え、日々発展しています。

		レガシーなIAM		モダンなIAM
 アジリティ (俊敏性)	新しいシステムへのIAM適用期間	数か月	▶	数週間
	クラウドサービス対応	独自開発	▶	標準方式
 セキュリティ	シングルサインオン	独自方式	▶	標準方式
	認証強度	弱	▶	強
 コンプライアンス	入社・退職の反映	数日	▶	即日
	IDや権限の棚卸工数	大	▶	小
 効率化	ルールの徹底工数	大	▶	小
	ログ・証跡の管理	分散	▶	集中

モダンなIAMに関連する主な技術・考え方

モダンなIAMを提供する最新の業界動向は以下のようなコンポーネントで構成されます。機能として重複している部分もあり、導入に当たっては各社の方針に合わせて選択・組み合わせが必要です。

技術・コンポーネント	概要/利点
アイデンティティ・ガバナンス (IGA)	IDとアクセス権限の運用をルール・ポリシーに沿っておこなうためID/権限のライフサイクル管理(退職者のID削除の徹底等)、プロビジョニング機能、職務分掌(SoD)のチェック機能のほか、ID/権限の申請/承認、棚卸機能をもつ。 これらの機能を整備することで、セキュリティ・ガバナンスの強化を効率的に行うことができる。
IDaaS (Identity as a Service)	IAM機能を提供するクラウドサービス。 IDaaSではIDフェデレーションや多要素認証などの認証を強化する機能を持ち、標準的なプロトコルで実装済みのため、特にクラウドシステムに対するID/権限のライフサイクル管理、プロビジョニング、認証機能の提供に有用。
IDフェデレーション (ID連携)	異なる組織(セキュリティドメイン)間でID/認証を連携する機能。これにより、クラウドサービスのログインに社内の認証基盤が利用でき、また、社外のメンバーに個別パスワードの発行が不要になる。利用者と管理者のクレデンシャル管理工数を削減できIDフェデレーションの標準規約としてSAMLやOpenID connectがあり、多くのクラウドサービスが対応している。
多要素認証 (MFA)	利用者の本人認証方式には知識認証、所持認証、生体認証の3要素があるが、このうち2要素以上を利用して認証すること。セキュリティの向上が求められている現在、特にインターネットからのアクセスや機密度に応じて、多要素認証の導入の検討が必要となる。
ゼロ・トラスト	守るべきシステムやデータに対するすべてのアクセスを信用せず、アクセスの都度リスクに応じて必要なレベルの本人確認を行う考え方。アクセス先、アクセス元、利用デバイス、時間帯、アタック動向などの情報をもとに動的にアクセスの可否を判断し、追加の認証を求めたりすることでセキュリティを維持する。その判断の中心となるアイデンティティ情報の一元管理が構築においては重要となる。

ID・アクセスマネジメント(IAM)のモダナイズプロジェクトのステップとハードル

IAMは、人事・セキュリティ・システム・DX・内部統制など多くの部署に関わるプロジェクトとなるため、各ステップにおいて陥りやすいハードルがあります。デロイトでは豊富な知見によりハードルを越えるための支援を行います。

	よくあるハードル	デロイトグループの支援例
プロジェクト立上げ	<ul style="list-style-type: none"> ・IAMモダナイズの重要性認識不足による予算の先送り ・既存の部署の職務にないミッションのため、プロジェクトオーナーの選定ができない 	<ul style="list-style-type: none"> ・トップ(CxO)向け説明・勉強会 ・IAMアセスメントサービスによる成熟度評価 ・プロセス・体制・テクノロジーのベストプラクティス紹介
構想策定	<ul style="list-style-type: none"> ・ステークホルダーが多く調整に時間がかかる ・システムのブラックボックス化で現状把握が困難 ・スコープが広がりすぎ、ロードマップが描けない ・ソリューションが多くあり選定が難しい 	<ul style="list-style-type: none"> ・ビジョンの明確化と適切な態勢作成の助言 ・現状分析・GAP分析の支援 ・優先度を考慮した現実的なロードマップの策定 ・最新技術動向を踏まえたソリューション選定に係る助言
設計・構築導入	<ul style="list-style-type: none"> ・コンポーネント間でのコミュニケーション不足 ・既存業務システムに対応にコストがかけられず移行プランが遅延する 	<ul style="list-style-type: none"> ・PMO全般支援 ・効果的なコミュニケーションプランの作成 ・チェンジマネジメントのサポート
拡張・運用	<ul style="list-style-type: none"> ・構築後の放置による技術の陳腐化 ・既存システムへの適用展開の遅延 	<ul style="list-style-type: none"> ・進化し続けるIAMの継続的サポート

デロイトの方法論

デロイトの方法論は、成功事例をベースにしたアプローチ、各種テンプレート、ツールを活用して、実現すべき要件の絞り込み、採用するソリューションの決定、投資効果の算出に関するフレームワークを提供し、プロジェクトを成功に導きます。

Deloitte's Methods™



Deloitte's Methodは、ID・アクセス管理の統合的なフレームワークであり、実効性の高いプロジェクト推進を実現します。



Deloitte's Methods™ の利点

- ✓ 現状と理想のギャップにフォーカスし、要件(守るべき情報/管理すべき対象)を明確化
- ✓ 成熟度モデル、優先順位を基にスコープ/期間/コストを考慮したロードマップの策定
- ✓ 主要ベンダーとのリレーション、Deloitteグローバルとの連携を活用したグランドデザインの策定

デロイトの方法論を活用し、構想策定、設計、システム構築、システム運用の各段階において、クライアントの個別ニーズに合わせたサービスを提供します。

またシステム導入のみならず、PMOやチェンジマネジメントを通してクライアントのプロジェクトを成功に導きます。



構想策定支援 (Strategy and Roadmap)

- 目的、全体ビジョンの策定
- As-IsとTo-Beのギャップ分析
- プロジェクト体制策定
- 期間・コストを考慮したロードマップ作成
- 必要となる予算およびコストの分析
- 上申等クライアント内でのプロジェクト推進



設計・構築支援 (Design and Implementation)

- 業務プロセス、運用フロー設計
- 要件定義書、基本/詳細設計、テスト仕様書作成
- ベンダーとのコミュニケーション
- 構築、導入作業実施
- 単体/結合/総合テスト実施
- ユーザ受入テストのサポート



業務運用支援 (Operation and Maintenance)

- 運用・サポートチームへのナレッジ展開、追加トレーニング実施
- 活用状況のアセスメント(KPI確認)
- 活用改善の提案



PMO・チェンジマネジメント支援 (PMO and Change Management)

- テンプレート、ツールを活用したプロジェクト推進
- 各フェーズ、マイルストーンのレビュー
- ステークホルダーとのコミュニケーション
- 運用定着化、トレーニング計画の策定
- 業務プロセス、ガイドライン類等の整備
- リリースコミュニケーション計画の策定、実施

デロイトの強み

デロイトグループではグローバルで多数のIAMプロジェクトの実績があります。世界140カ国でサービスを展開しており、各地域にIAM専門家を配置しています。

グローバル アライアンス

主要なCIAMベンダーとのグローバルアライアンス、各リージョンで各ベンダーと連携可能な体制

IAM プロフェッショナル

グローバル各リージョンで200人を超えるIAMプロフェッショナルと連携した支援体制

コンプライアンス

監査や法規制の専門家による各国のプライバシー規制、セキュリティ監査対応を踏まえた支援体制

デロイトでは、15,000名以上の情報セキュリティおよびITリスクマネジメントのプロフェッショナルが存在、デロイトネットワークを活用してグローバルプロジェクトに参画しています。

North America
> 7,200 professionals

EMEA
> 4,200 professionals

Asia Pacific
> 3,600 professionals

Rest of the world
> 500 professionals

※貴社および貴社の関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス 内容をご提供できない可能性があります。詳細はお問合せください。

デロイト トーマツ サイバー合同会社

Mail iam_advisory@tohmatsumatsu.co.jp

URL www.deloitte.com/jp/dtcy

【国内ネットワーク】東京・名古屋・福岡

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人(有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ コーポレート ソリューション 合同会社を含む)の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスク アドバイザリー、コンサルティング、ファイナンシャル アドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト(www.deloitte.com/jp)をご覧ください。

Deloitte (デロイト)とは、デロイト トウシュ トーマツ リミテッド ("DTTL")、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数を指します。DTTL (または "Deloitte Global")ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。

デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市(オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、上海、シンガポール、シドニー、台北、東京を含む)にてサービスを提供しています。

Deloitte (デロイト)は、監査・保証業務、コンサルティング、ファイナンシャル アドバイザリー、リスク アドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク(総称して"デロイト ネットワーク")を通じFortune Global 500®の8割の企業に対してサービスを提供しています。"Making an impact that matters"を自らの使命とするデロイトの約312,000名の専門家については、(www.deloitte.com)をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的な事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.
2020.07_0328