IAM実務者ガイド

IAMソリューションが対応すべき5つの重要領域

リスクを軽減し、
アイデンティティで信頼を獲得

内容

01

全体的な課題と目標

IAM実践者として、適切な人だけが適切なリソースに適切なタイミングでアクセスできるようにする責任があります。アクセスの保護、生産性の向上、組織全体にわたるコンプライアンスの実現は、常に最優先事項です。しかし、アイデンティティの乱立、分断されたツールによる可視性の欠如、従業員アカウントのプロビジョニングといった手作業の業務などが、継続的な課題となっています。

以下の目標に重点を置きながら、最も効率的な作業を可能にするIAMソリューションが必要です：

1. より高い可視性と制御
2. 運用効率
3. セキュリティの向上
4. 自動統合
5. ガバナンスとリスク低減

最適なIAMソリューションが成功への道を切り開きます。監査と統合がスムーズになり、自分とチームの手作業が減り、適切なユーザーが必要なときに適切にアクセスできます。

02

断片化されたツール

労働力向け、顧客向け、パートナーIAMやワークロード向けなど、用途ごとに寄せ集められたアイデンティティ・ソリューションは、どのエンティティが何にアクセスできるのかを把握することを困難にします。ポリシーがユーザーの実際のアクセスと一致しているかどうかを判断することも困難です。攻撃者は、生成AIを使用して、フィッシングや特権の乱用などの攻撃キャンペーンを加速できます。

ますます複雑化するIAMの世界で必要なのは、以下のメリットを提供する、単一で統合されたアイデンティティ・ファブリックです。

1. 統合アイデンティティ・プラクティスを推進する
機密システムに誰が、何を、どのようにアクセスしているかをより正確に把握できます。セキュリティリスクを軽減し、コンプライアンスを強化します。スタック全体を刷新することなく、複数のベンダーと連携できます。

2. IDライフサイクル管理を自動化する
IDのセキュリティーを確保するための強力なメカニズムを設定して適用し、最小権限と必要十分なアクセス権の原則によるコンテキストベースのポリシーを確立します。

3. セキュリティーとユーザー体験のバランスをとる
時間のかかる手動プロセスを、リスクと脅威ベースのインテリジェントなライフサイクル管理に置き換え、入社・異動・退職のシナリオを管理します。逸脱を監視し、権限をポリシーにリアルタイムで準拠させます。

03

NHIの増加

IAM 実務者は、NHIの急増により、複雑さが増す問題に直面しています。ガバナンスがなければ、API、サービスアカウント、チャットボット、マシン・アイデンティティは、巨大で管理されていない攻撃対象領域となってしまいます。

生成AIとエージェント型AIと相まって、NHIの野放しな成長は、脅威アクターの新たな標的も生み出し、誰が、または何がクリティカルシステムにアクセスしているのか可視性の喪失につながります。

NHIのセキュリティーを人間のユーザーと同じ優先度に引き上げます。一貫したIAMの結果を得るために、ライフサイクルの自動化、AI搭載の脅威検知、適応型管理、強力な認証プロセスは人間のIAMプロセスと連携する必要があります。

ガバナンス、アクセス制御、認証、脅威検知をNHIに拡張することで、エンドツーエンドのシナリオでより優れたセキュリティーを実現するためのベースラインが確立されます。

40:1

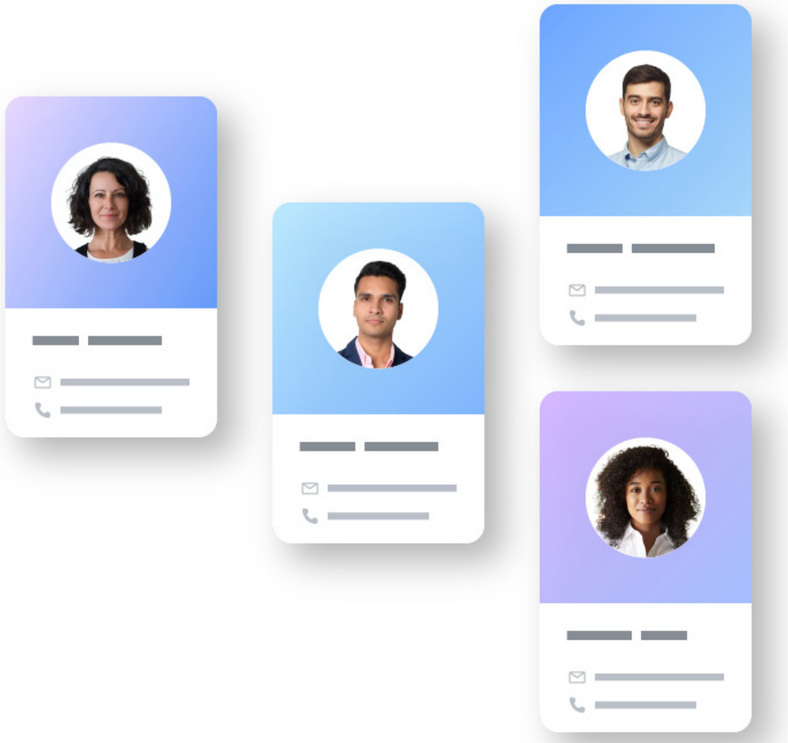
NHIsと人間の割合—あなた方は圧倒的に数で劣っています

97%

AI関連のセキュリティー・インシデントを報告し、適切なAIアクセス制御を行っていなかった組織の共有

04

適切な
セキュリティー
の調整



機密データへの承認済みアクセス権を付与する際、本人確認に過度に厳格な制御が行われて動作が遅くなったり、生産性が妨げられたりすると、ユーザーは不満を感じます。誰もが利便性を望んでいますが、それによって保護が弱まる可能性があります。

適応型のコンテキスト認識セキュリティーにより、リスクやユーザーの不便さを増大させることなく、安全なアクセスのバランスを保ちます。 ユーザーの行動、デバイスの信頼性、場所、リスク状況などのシグナルを継続的に評価し、適切なアクセス・レベルを決定するプラットフォームを使用してください。

AIを活用した分析と動的なポリシーを適用することで、認証がシームレスに適応し、リスクが高い場合には制御を強化し、信頼性が高い場合にはアクセスをスムーズに維持します。

リスクの高いアクセス試行は自動的に拒否またはブロックされるため、信頼できるユーザーの操作速度が低下することはありません。また、侵害を減らし、認証情報の悪用を減らし、生産性を向上させることもできます。アイデンティティ・パターンを強化することで説明責任を確保します。特に新しいエージェント型AIシナリオ向けに、人間のアイデンティティとNHIをジャストインタイムの必要十分なだけのアクセス・アプローチに統合します。

05

手動プロセスとアイデンティティの乱立

組織への従業員の入社時や退職時に手動でアカウントのプロビジョニングとデプロビジョニングを行うと、時間の無駄になるだけでなく、コストとアイデンティティの乱立も増大します。 代わりに、IAMを自動化することで、ユーザーとマシンが必要な時にのみアクセスできるようになります。

自動化によりユーザーまたはマシンのアイデンティティの作成、更新、停止が一貫して処理されます。従業員の退職直後にすべての重要なアプリケーションへのアクセス権を取り消して、退職後の不正アクセスを防ぐことができます。

シンプルに始めてモジュール方式で拡張していきます。そうすることで、アカウントのプロビジョニングとプロビジョニング解除は、全体的な見直しを必要とせずに、組織に合わせて段階的に拡張されます。

あなたの成果は次のとおりです：

- 人為的ミスの減少
- ITスタッフの生産性向上
- アイデンティティの乱立を抑制
- 潜在的なデータ侵害のチャンスが減少
- 孤立したアイデンティティに関連する無駄なコストの削減

06

オープンで
スケーラブルな
アイデンティティ層

アイデンティティ・ガバナンスは常に急速に進化しているため、アカウントのプロビジョニングとデプロビジョニングを超えて、モジュール方式で拡張する必要があります。

オープンでスケーラブルなアイデンティティ層を使用すると、次のことが可能になります：

01

IAM戦略フレームワーク内にAI駆動型セキュリティー・ソリューションをより簡単に導入

02

ベンダー・ロックインなしで最高のツールを選択可能

03

システム内で新しいツールをデプロイする必要性を回避

04

クラウドやオンプレミスを含むハイブリッド環境全体であらゆるベンダーと容易に統合

05

データ・アクセスおよび移動に関するGDPR、HIPAA、PCI-DSSなどの法律や規制の変化に応じて、より効率的にコンプライアンスを維持

06

API主導のNHIフローを提供して、チームをクリティカルビジネス・アプリケーション・イニシアチブに取り込むことで、アプリケーション・チームの迅速な移行をサポート

オープンでスケーラブルなアイデンティティ層を実装すると、会社全体のセキュリティーとコンプライアンスを向上させ、自動化を通じてオーバーヘッドを削減し、モダナイゼーションをサポートし、ゼロトラストストラテジーを強化できるようになります。

07

アイデンティティに基づく脅威対策

貴社が直面している課題
脅威アクターは生成AIを使用してフィッシング詐欺、ブルート・フォース攻撃、認証情報スタッフィング（盗んだ大量のパスワード・リストを使用してログイン試行を自動化する最近の技術）を推進しています。サイバー攻撃者は、脆弱な認証情報、再利用された認証情報、盗まれた認証情報をエクスプロイトし、アカウントを乗っ取ることも行っています。

反撃に必要なもの
これらの脅威から防御するには、高度な異常検知、適応型多要素認証（MFA）、そして継続的な監視が必要です。リアルタイムの脅威検知、リスクベースの認証、そして自動化された攻撃からの保護も不可欠です。

ITDRとISPMが重要な理由
ITDRの主要な機能が組み込まれているため、異常なトラフィックをリアルタイムで検知し、ブロックすることが容易になります。ISPMは、組織全体のアイデンティティ管理体制の向上に役立ちます。ユーザーとそのデータはより安全になり、保護はより包括的になり、侵害を検知、防御するための最適な準備が整います。

08

開始する

あらゆる点を考慮して、貴社とそのチームが目の前の課題に対処するのに役立つ重要ポイントを以下に示します：

01

統一されたアイデンティティ・プラクティスを推進
断片化されたIAMツールを単一のファブリックに統合して、盲点を減らし、保護を強化し、監査を簡素化し、コンプライアンスを強化します。

02

アイデンティティ・ライフサイクル管理を自動化
手動ライフサイクルを、シャドウ・アカウントを採用してポリシーの逸脱を修正する自動ワークフローに置き換えて、コストを削減し、最小限の特権アクセス権を維持します。

03

セキュリティーとユーザー・エクスペリエンスのバランスをとる
パスキーなどの強力な認証と、適応型のコンテキスト対応セキュリティーを組み合わせることで、ユーザーの操作速度を低下させることなく安全を確保します。

04

ハイブリッド環境全体を統合
IAMソリューションをクラウド、オンプレミス、既存のシステム全体で確実に機能させ、組織が大幅な更新を行わなくてもIAMプラクティスをモダナイズできるようにします。

05

アイデンティティの脅威に先手を打つ
ITDRが組み込まれたプラットフォームを採用し、ISPM機能を使用して認証情報攻撃を検知し、インフラストラクチャーのギャップを特定して、ユーザーを保護し、攻撃者を制限します。

06

エージェント型AIの新しい世界に備える
ビジネスの説明責任基準を満たすために、人間とNHIのシナリオを統合するパターンを開発します。

09

最新のIAMは
ここから始まる

これで、最新のIAMソリューションが実現すべきものがわかりました：

- 可視性
- 強力な保護
- 自動化とのオープン統合
- すべてのアイデンティティを対象とするガバナンス
- プロアクティブな防御

日々の混乱に直面しても平静を保つために、IBM Verifyをご検討ください。次の方法でプロセスを簡素化し、モダナイズします：

- 特権IAM全体にわたる強力な保護の標準化
- 管理されていないことが多いマシン・アイデンティティにガバナンスを拡張
- 脅威とリスクを重視した体でアイデンティティ・プログラムの有効性を実現
- すべての環境をクリーンに統合してサイロを削減

組み込みの検知機能と継続的な体制管理により、追加のツールを必要とせずに、より厳密な制御が可能になります。手作業による煩わしさを軽減し、より強力なレジリエンスを実現し、実行するあらゆるものに合わせて拡張できる統一されたアイデンティティ・ファブリックを提供するソリューションの詳細はこちら。

Verifyの詳細はこちら →

Vaultの詳細はこちら →

本書は最初の発行日時点における最新情報を記載しており、IBMにより予告なしに変更される場合があります。IBMが事業を展開している国または地域であっても、特定の製品を利用できない場合があります。

本書の情報は「現状のまま」で提供されるものとし、明示または暗示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとします。IBM製品は、IBM所定の契約書の条項に基づき保証されます。

ITシステムや製品は完全に安全であると捉えるべきではなく、不適切な使用やアクセスを防止する上で完璧な効果のある、製品、サービス、セキュリティー対策は1つもありません。IBMでは、いずれの当事者による不正行為または違法行為によっても、いかなるシステム、製品もしくはサービスまたはお客様の企業に対して影響が及ばないことを保証することはありません。IBMの計画、方向性および意図に関する記述は、IBMの単独の裁量により、予告なく変更または撤回される場合があります。将来の潜在的製品に関する情報は、一般的な製品の方向性を概説することを目的としており、購入の決定はこれに依存するべきではありません。今後提供される可能性のある製品に関するこれらの情報は、いかなる資料、コードまたは機能を提供することを確約したり、保証したり、法的義務を負ったりするものではありません。将来の潜在的製品に関する情報は、いかなる契約にも組み込まれるものではありません。IBM製品向けに記載された将来の主要な機能や機能拡張の開発、リリースおよびその時期は、IBMの単独の裁量により決定されます。

お客様は、自己の責任ですべての関連法規および規則を遵守するものとします。IBMは法律上の助言を提供せず、IBMのサービスまたは製品を使用することでお客様による法律または規則の遵守が確約されると表明することも保証することもありません。