IBM Security Verify

クラウドに最適な Identity-as-a-Service (IDaaS) でユーザーの生産性を確保

ハイライト

- クラウドに最適なプラットフォームを B2E、B2B、B2C のユース・ケースに活用
- ビジネス環境への新しいクラウド・アプリケーションの導入を促進
- 外部向けアプリケーションおよびサービスをセキュリティーで保護
- シームレスな MFA によってセキュリティーと利便性のバランスを維持
- 日常的な ID 管理のプロセスを迅速化
- SSO によってあらゆるデバイスにおけるユーザー生産性を確保

アイデンティティー (ID)は、エンタープライズ・セキュリティーの重要課題の中核を成すものです。脅威や攻撃が絶え間なく変化する世界では、効果的な ID およびアクセス管理 (IAM) プログラムは、依然として大半の脅威に対する最良の防御策であり続けています。組織にとって、ユーザーの身元を確認し、その行動を監視することは非常に重要です。
過去 20 年間、健全な IAM の基本的な考え方には大きな変化はありません。しかし、クラウド・コンピューティングやモバイル・アプリケーション、ソーシャル・メディアなどの急激な進化により、IT とセキュリティー部門への新たな負担が増大し、古いアーキテクチャーやプロセスを広範囲に渡って見直す必要に迫られています。ユーザーは以前にも増して激しく変化し、このような変化を踏まえて強固なセキュリティー・ハイジーン (衛生状態の管理) を維持することは、かつてないほど複雑になっています。

IBM Security Verify は、IAM の機能を統合した包括的なプラットフォームです。クラウドで提供されるインターフェースは明瞭で使いやすく、企業はこれを利用して総所有コストを削減し、専門的で希少なセキュリティー人材への依存を軽減することができます。IT、セキュリティー、およびビジネス・リーダーは、Verify を使用することで、現在のクラウド・コンピューティングに適応するだけでなく、ユーザーの生産性の次世代のイノベーションに対しても、自社の IAM プログラムを将来にわたって対応させることを可能にします。

Verify は、ユーザーが求めるアプリケーションへの速やかなアクセス、ビジネス・リーダーに必要な生産性の向上、開発者が求める新規サービスの迅速な展開、IT チームが必要とするビジネスの変化への即時対応をサポートします。

SSO によるユーザーとアプリケーションの接続

クラウドの大きな利点は、時と場所を問わず必要なビジネス・ツールに簡単にアクセスできることです。しかし、ツールとアクセスに必要なパスワードが増えると、この利点が欠点に変わる可能性があります。ユーザーが求めるクラウド・ベースのアプリケーションの多くには、セキュリティーと認証機能が組み込まれていません。Verify を使用すると、Microsoft Office 365、Concur、Workday、IBM Box、IBM Verse など数千のクラウド・ベースのアプリケーションに対応したアクセス制御ポリシーを設計し、適用することができます。Verify には、社内アプリケーションの統合に利用できるテンプレートもあらかじめ組み込まれています。

- 任意のアプリケーションにアクセスできる従業員向けランチパッド
- ユーザー・ディレクトリーを持っていない組織向けのクラウド・ディレクトリー
- オンプレミス・ディレクトリー（Microsoft AD など）をクラウド・アプリケーションで使用できるように同期させる機能
- 複数のフェレデーション規格（SAML、OAuth、OpenID Connect など）のサポート

シームレスな MFA によるユーザー ID の検証

認証ポリシーの利便性とセキュリティーの適切なバランスを実現することは、今日のセキュリティー・リーダーにとって重要な課題です。消費者向けサービスでは、快適な認証エクスペリエンスを提供することが、ビジネスにおいて必要不可欠です。従業員向けのプログラムでは、適切な人物だけが企業のリソースにアクセスできるようにするために、最新かつ最も安全な方法を実装することが重要です。Verify の MFA 機能は、認証プログラムの対象となる社内外のユーザーに、快適なエクスペリエンスを提供します。

- シンプルなユーザー・インターフェース（UI）- アクセス制御の定義と修正ができます。
- e メール、SMS、モバイルのプッシュ通知で送信されるワンタイム・パスワード
- 生体認証（指紋、顔、声、ユーザー・プレゼンスなど）
- 仮想プライベート・ネットワーク（VPN）用の第二要素認証
- リスク・ベースの認証機能 - エンタープライズ・モビリティー管理およびマルウェア検知ソリューションのコンテキストを使用します。
- ソフトウェア開発キット（SDK）- モバイル・アプリケーションと広範囲なアクセス・セキュリティー・プラットフォームを簡単に統合できます。
- リスク・ベースのユーザー認証と認証ポリシー - 以下が使用されます。
    - エンドポイントに関するコンテキスト（デバイス・指紋、ジェイルブレイク・ステータス、EMM 登録状況）
    - ID（グループ、ロール、不正インジケーター）
    - 環境（地理的位置、ネットワーク、IP レピュテーション）
    - リソース/アクション（要求の内容）
    - ユーザーの行動（位置、速度）

アクセス権のガバナンスによる適切なアクセスの保証

多くの組織では、コンプライアンス要件を満たすためのアプリケーションへのユーザー・アクセスのプロビジョニングと再認証は、煩雑で手間がかかり、高い運用コストが発生する作業となっています。Verify のガバナンス機能は、重要な ID ガバナンスと管理機能をクラウドから提供することで、新しいテクノロジーの迅速な導入を支援します。これにより、組織は必要なツールを利用して、従業員によるアクセスのライフサイクルとコンプライアンス要件をより低い運用コストで管理可能になります。

ID 分析によるアクセス・リスクの理解の向上

一般的な IAM 環境では、ユーザーが誰で、何にアクセスしているかに関する情報が保管されています。ただしこの情報は、必ずしもアクセス関連のリスクを正確に把握しているわけではありません。アクセス・リスクの全体像を把握するには、ユーザーがアクセス権限を使って実際に何をしているのかを十分に理解する必要があります。Verify の ID 分析機能は、リスクを総合的な視点で捉えて既存のプロセスを強化することで、よりスマートな IAM を可能にします。例えば、機械学習を使用して推奨される緩和措置を特定し、意思決定を支援します。

適応型アクセスによるセキュリティーと利便性のバランス

ユーザーがアプリケーションにログインする際、どの程度の認証をユーザーに求めればいいのでしょうか?ビジネス上必要とされるシームレスなエクスペリエンスと、組織のセキュリティー要件との間でバランスを保つことは容易ではありません。さらに、ほとんどの認証アプローチでは、決まった数の属性（場所、デバイスなど）に基づいて静的ポリシーが設定されます。Verify は、適応型アクセスによって、リスクに動的に配慮し、ストレスのないアクセス・エクスペリエンスを提供します。適応型アクセスでは、ユーザーがデジタル・サービスにアクセスしようとすると、高度なリスク検知機能と堅牢なアクセス・ポリシー・エンジンを組み合わせて、ユーザーの ID の完全なコンテキストを評価します。このソリューションは、カスタム・アプリケーション用の API や、一般的に使われているクラウド・アプリケーション向けの組み込みテンプレートを使用して、簡単にアプリケーションに統合できます。コーディングはほとんど、またはまったく必要ありません。

- 人工知能を搭載したリスク検知 - モバイル・デバイス、Web セッション、VPN アクセスなどのコンテキストを総合的に考慮して、必要とされるユーザー認証のレベルを調整します。
- シンプルなポリシー・エディター - 管理者は適応型認証ポリシーを素早く設計し適用できます。
- ユーザー属性の異常を検知する機能 – 挙動、生体認証、既知の不正パターン、デバイス、場所、IP アドレスに基づいて判断します。
- 開発者用リソース - ネイティブ、Web、モバイル、およびクラウド・アプリケーションに適応型認証を追加するために使用します。コーディングはほとんど必要ありません。
- 複数のフェデレーション標準規格（SAML、OAuth、OpenID Connect など）のサポート

組織は事業拡大に向けて、新しい画期的なデジタル・サービスの開発に取り組んでいます。これらのサービスを強力な消費者 ID とアクセス管理（CIAM）制御で保護することが、ブランドの信用にとって非常に重要です。ただし、簡単でスムーズにアクセスできなければ、お客様はブランドから離れてしまう可能性がありま

す。Verify は、セキュリティーと利便性の適切なバランスを実現し、新規・既存顧客へのサービスをシームレスなセキュリティーで保護可能なツールを提供します。

- API、ソフトウェア開発キット、開発者用リソース - ブランドに適した ID エクスペリエンスをカスタマイズするために使用します。
- 適応型認証 - リスクが検知された場合のみ、お客様に MFA を要求します。
- ソーシャル・ログイン機能 - ユーザーは自身の LinkedIn、Google、Facebook、Twitter のアカウントや、その他の地域固有のソーシャル・ネットワークを使用して、登録とログインを行えます。
- 組み込みのテンプレート - 加入、登録、ユーザー名/パスワードのリセット、その他の ID 操作に使用できます。
- お客様の同意とプライバシー設定を追跡する機能 - EU 一般データ保護規則 (GDPR)とカリフォルニア州消費者プライバシー法 (CCPA)の遵守をサポートします。

IBM をお勧めする理由

クラウドへの転換を成功させるには、既存のエンタープライズ IAM ポリシーを統合して拡張する方法が必要です。これにより、ビジネスを中断することなく、セキュリティーを確保できます。IBM は、モバイル、クラウド、およびオンプレミスのアプリケーションを適切に統合し、全社的なコスト削減と運用効率の向上を可能にします。Verify はインストールやインフラストラクチャーは必要とせず、これら全てをクラウドで実現します。

IBM Security ソリューションについて

IBM Security は、エンタープライズ・セキュリティー製品とサービスを高度かつ適切に統合したポートフォリオを提供しています。世界的に有名な研究開発機関である IBM X-Force によってサポートされたこのポートフォリオは、組織が人員、インフラストラクチャー、データ、アプリケーションを総体的に保護できるセキュリティー・インテリジェンスを提供しています。また、ID とアクセス管理 (IAM)、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどに関するソリューションを提案します。これらのソリューションによって、組織はリスクを効果的に管理し、モバイル、クラウド、ソーシャル・メディア、その他のエンタープライズ・ビジネス・アーキテクチャー向けに統合されたセキュリティーを実装することができます。IBM は世界最大級のセキュリティー研究、開発、提供機関の一つを運営しており、130 を超える国々で 1 カ月あたり 1 兆件以上のイベントを監視し、3,000 件を超えるセキュリティー関連の特許を保持しています。

詳細情報

IBM Security Verify について詳しくは、IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、https://www.ibm.com/jp-ja/products/verify-for-workforce-iam をご覧ください。

IBM Global Financing は、事業拡大に必要な技術の取得を支援するために、多数の支払いオプションを用意しています。IBM は IT 製品およびサービスのライフサイクルを、入手から廃棄まで全体にわたって管理します。詳しくは、ibm.com/ja-jp/financing をご覧ください。