IBM Security
ソート・リーダーシップ・ホワイト・ペーパー

2015 年 3 月

ID ガバナンスによる重要資産の保護

IBM の堅固な統合 ID ガバナンスを使用して、組織のゲートウェイを保護

はじめに

ユーザーの ID およびアクセス特権を企業ポリシーと効果的に合わせることは、今日の企業にとって不可欠なセキュリティー制御です。グローバルな企業は、従業員、顧客、パートナー、ベンダーに加え、これらの人々全員の ID が組織へのもっとも主要なエントリー・ポイントであることを認識しています。クラウド・ソリューション、モバイル・コンピューティング、個人所有デバイスの持ち込みプログラムの急速な受容に伴って、企業の境界は急激な拡大を遂げており、エントリー・ポイントの数が劇的に増加しています。そして、資格情報の盗用や、企業内部のアカウントのハッキングを狙う世界中の犯罪者が暗躍しています。

企業における、外部との従来の境界が拡張することで、企業によるすべてのアクセス・ポイントの効果的な保護がさらに困難になっています。結果として、組織は企業のすべてのエントリー・ポイントにわたり、不正なアクセスまたは犯罪者によるアクセスからアプリケーションおよびデータを防御することに新たな注意を向けています。ID 管理およびアクセス管理は一般的な従来型の IT プロセスと考えられてきましたが、これはセキュリティー対策としてますます重要なものになっています。ID ガバナンスはデータのリスクまたは不正アクセスを軽減するための支援を行います。これは、ポリシーに準拠していないアカウントを攻撃ベクトルとして削除することにより、不正行為から組織を保護する際に、防御の鍵となる方針です。

正しい ID ガバナンスおよび管理ソリューションは、ユーザー役割、アクセス・ポリシー、リスクを管理するための、ビジネスに基づく自動化された ID ガバナンスによって、組織がアクセス・リスクや職務分離 (SoD) 違反を制御するための支援を行います。これにより、適切なレベルのアクセスが確実に適用され、企業のアプリケーション全体で強化されます。アクセスがどう利用されているかを確認するための可視性が改善され、「いつ、誰が、どのリソースに対するアクセス権を所有しているか」などの重要なコンプライアンス上の質問への回答、さらに「ユーザーがリソースへのアクセス権を取得した方法と理由」という質問へのフォレンジックな回答を支援することができます。

このホワイト・ペーパーは、堅固で統合された ID ガバナンスおよび管理ソリューションを重要なセキュリティー制御として使用し、組織の広範囲なエントリー・ポイント全体で、企業の機密データや重要資産を保護できるようにすることのメリットについて検証しています。

ID は組織および組織の重要資産へのゲートウェイ

適切なユーザー ID ガバナンスおよびプロビジョニング・システムを既に実施済みであると考えている IT 管理者や経営層は、企業の安全が確保されていることをよく検討し、確認することが重要です。堅固で統合された ID ガバナンスおよび管理ソリューションを使用してセキュリティーを強化する方法を見つけるという概念を、企業の経営層は真剣に受け止めています。

今日では情報漏えいが頻繁にニュースになります。情報漏えいはさまざまな形で発生し、ますます高度な策略を用いています。これらの漏えいの多くは、膨大な数の従業員、パートナー、ベンダー、および顧客に影響を与え、何百万ドルものコストが発生し、ブランドの評判に損害を与え、潜在顧客が漏えい被害者との将来の取引を控える要因となります。たいていの場合、適切に管理されていないユーザー・アカウントは、多くの侵入計画を成功させる脆弱性の主要因です。次の例を見てみましょう。

とあるグローバルな銀行では、ある従業員が自らに許可されていた取引限度額を超えて取引を行うことが可能でした。この従業員に合計で何百万ドルもの取引を作成して実行するためのアクセス権を与えたため、銀行は数十億ドルを失いました。このトレーダーは、以前は IT 関連の部署に所属していたため、目的を隠して偽の取引を作成することなど、取引規則をくぐり抜ける方法を知っていました。もしこの従業員が適切に管理され、SoD 制御が備わっていたとしたら、銀行が多大な損害を被る前に、高い確率でこのトレーダーを捕まえられていました。

ID 管理は多重境界を保護するために最初に使用される防御です

あるグローバルな業者が攻撃され、何百万人もの顧客の課金情報および連絡先が盗まれました。ハッカーは、クローズされていない古いベンダー・アカウントを経由してアクセスしました。包括的な ID ガバナンス・プログラムおよび効果的な制御があれば、この業者は「孤立した」アカウントを認識でき、この漏えいの防止を支援できたかもしれません。

セキュリティー上の脆弱性と ID および ID のアクセスとの関連

これらの攻撃や他の多くの攻撃は、高度な ID ガバナンスおよび管理ソリューションによって防御されていた可能性があります。ID ガバナンス制御が十分に実装されていない場合に、セキュリティーがどのように脆弱になるか、その経緯について、いくつかの例をここに示します。

使用されていないアカウントがアクティブのままになっている (孤立アカウント)

あらゆる組織において、正しい担当者が正しいデータとアプリケーションに正しくアクセスする必要があります。今日のような恒常的に変化する環境では、従業員は頻繁に出入りしたり、新しいポジションに異動したりします。これは従業員だけではありません。顧客、ベンダー、パートナーとの関係にも開始、発展、終了があります。ユーザーのために確立したアクセス権の正確性および最新性を確保することは、ますます困難になっています。また、組織の重要資産に対する悪意のあるアクセスを防御するために、非アクティブなアカウントを確実にクローズすることがますます重要になっています。

例えば、従業員が退職したら、アカウントがクローズされない限り、アカウントへのアクセスが終了しません。このような場合、孤立したアカウントが、退職者自身も含む悪意のある攻撃者に、企業の重要データおよび資産にアクセスするための門を開きます。このようなアカウントは、誰もモニターしてないため、容易に不正侵入が行われます。しかし ID ガバナンスおよび管理システムは、この問題に対するセキュリティーの対応策を提供できます。

不適切なアクセス権および特権

組織のユーザー数が増加した場合は、エントリー・ポイントごとにセキュリティーを高め、過剰および不正な資格付与を防止するために、アクセスを認証するための容易で効果的な手段を持つことが重要です。例えば、以前人事部に在籍していて、従業員の個人情報や機密情報にアクセスできる特権を持っていた従業員がマーケティング部に異動します。この新しい役割にはそのようなレベルのアクセスは不要です。このアクセス・ループをクローズし、「不要な資格」、つまりユーザーが人事異動時に不適切な特権を過剰に獲得する動きを防ぐことは、攻撃者がハッキングを行って特権的情報にアクセスするために使用できるゲートウェイを遮断するための重要なステップです。

従業員のアクセス権や特権が最新に保たれるようにすること、および職能要件に合わなくなったアクセス権や特権を適切に無効化することは、機密資産を漏えいから保護するために不可欠です。アクセス権と特権は 2 つのステップで管理されます。アクセス認証は、アクセス権がユーザーとアプリケーションにとって適切であることを確認するプロセスです。プロビジョニングは、目的のアプリケーションおよびデータに、ユーザー・アカウントとアクセス権を作成し、管理し、保守するプロセスです。機密資産へのアクセスの安全性を確保するためには、正確な管理と適切な管理の両方が重要です。

内部者による脅威および職務分離違反

最近の研究によると、データ漏えいの主な要因は内部者です。多くの場合は従業員によるデータの意図的な悪用が関係しています。[1] また、従業員による意図的な盗用および詐欺も主なセキュリティー・リスクです。両方の例において、内部 ID の間隙は、侵入を試みているサイバー犯罪者が待ち望んでいるものです。

内部者による攻撃は、ユーザーが所有するべきではないアクセス特権を獲得した場合、または明確な SoD ポリシー違反が行われた場合に発生する可能性があります。例えば、管理者は自らの管理下にあるアプリケーションへのユーザー・レベルでのアクセス権を所有するべきではありません。なぜなら、ユーザー・アクセスと管理者アクセスの両方を所有するユーザーは、アプリケーション内でユーザーとしてのアクティビティー (注文の作成など) を実施することができ、さらにそのアクティビティーを管理者として隠蔽することができるためです。しかしながら適切な可視性と制御が用意されていれば、組織はこの SoD 違反、そしてこれに付随して発生する内部者による脅威を防ぐことができます。ユーザーに比較的機密度の高いデータへのアクセス権がある場合、SoD 違反は、不注意による間違いから意図的な不正行為に至るまで、深刻な被害を生み出します。

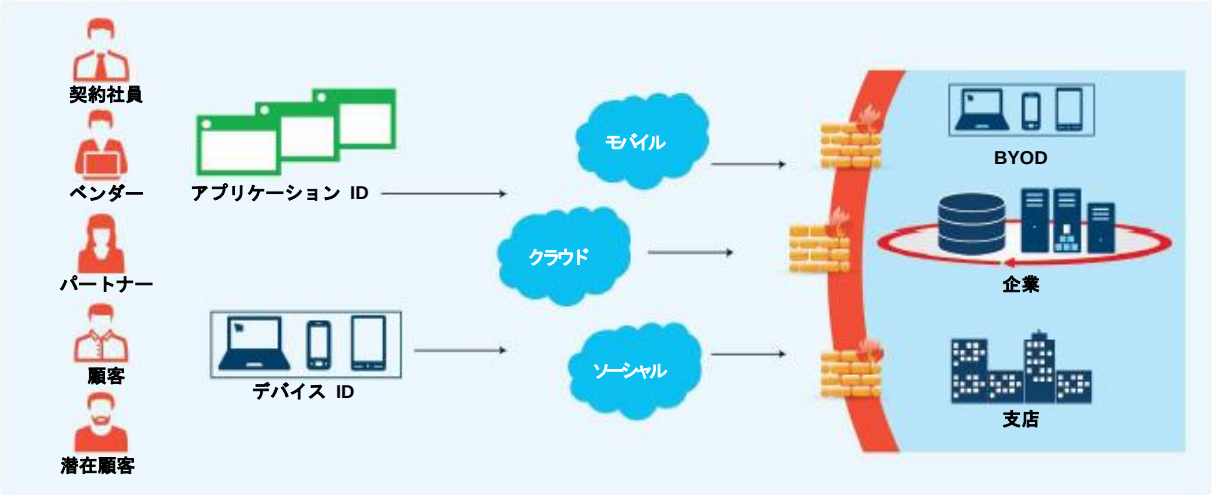
企業のセキュリティー担当役員および IT 担当役員は、企業の重要資産、つまり事業の生存および成功にとって不可欠である重要なデータにアクセスできるのは、組織の内部にいる人間だということを認識しつつあります。したがって、企業および IT 担当役員が内部構造の安全性を全面的に確保することが重要です。次のことを保証することによって、企業のアクセス・ガバナンス・プログラムを開始することができます。

- すべてのアクセス特権に対して十分な可視性が存在する
- 特権ユーザーのアクセスが効果的にモニターされている
- 適切なアクセス権が許可ユーザーに対してのみ付与されている
- いつ、誰が、誰に対してアクセス権を付与したかを証明するための文書が保持されている
- ユーザーにアクセス権および資格を付与する場合は、SoD 違反の可能性がある ID にアクセスできる

極めて寛容な ID アクセス手順

安全な ID ガバナンス・プロセスは多くの場合複雑で、セキュリティーに間隙が生まれる可能性が高まります。ある分野でユーザーにアクセスを付与するには、ユーザーの業務上の役割について、アプリケーション固有の情報を含めるプロセスが必要です。このユーザーが別の分野でさらにアクセス権を要求した場合、組織は再びプロビジョニングを行う必要があります。各ユーザーが新しい職能要件やアプリケーションをサポートするために新しくアクセス資格を要求するたびに、このサイクルが繰り返されます。結果として、ID 管理のインフラストラクチャーの複雑性、およびセキュリティー侵害のリスクが飛躍的に高まります。

今日の多重境界型の企業にとって、ID はセキュリティー制御の鍵です



また、アクセス特権の管理は紛らわしい会話の連鎖を引き起こしかねません。そういった状況では、IT スタッフはアプリケーション・アクセスに割り当てる職務を理解することができませんし、アプリケーション管理者はアクセス権が適切かどうかを確認することができず、ビジネス・リーダーはアクセス権の意味が理解できません。多くの場合、この混乱は意図的ではないが不適切なアクセス特権をユーザーに提供し、結果として一連のセキュリティー上の脆弱性を生み出します。必要なのは、ビジネス・アプリケーション、人事のシステム、既存のプロビジョニング・プラットフォームを含むさまざまなソースから、ユーザー情報と許可情報を収集するための集中型プラットフォームを備えた ID ガバナンス・ソリューションです。こうしたプロセスの簡潔化によって、ユーザー・アクセスが適切に管理されるようになり、不正な行為をもたらしかねない間隙を埋める支援を行います。

ID ガバナンスを使用してセキュリティーの強化を推進

組織に ID セキュリティーが侵害された経験があるか、あるいは侵害についての懸念がある場合は、アクセス・ポイントの安全性を確保するために実行できる明確な手順があります。これらの具体的な項目としては、従業員の監査、パスワード・ポリシーと手順の再評価、プロセスの自動化、ガバナンス・ポリシーを実行可能な制御へと容易かつ迅速に発展させるソリューションの選択があります。

従業員の監査

外部と組織の境界線の安全性を確保するためには、外部監査を行って自らの組織が政府や業界の規則から取り残されていないことを確認するよりも、従業員、契約社員、ビジネス・パートナーに内部監査を行うことが重要です。適切な追跡および監査によって、全ユーザーのすべてのアカウント、アクセス特権、資格に対する深い洞察および重要な可視性を得ることができるようになります。このインテリジェンスを使用すると、現行の ID 管理ポリシーと実践を効率的に評価できます。そして収集した情報を使用して、非アクティブ、不正、または失効したアカウントのクローズ、ガバナンス・ポリシーの推進、ID セキュリティー制御の導入の準備を行うことができます。

プロセスの自動化およびパスワード・セキュリティーの強化

従来、ID ガバナンスは、価値のあるセキュリティー防御を実現する包括的な監視手段というよりも、IT チーム主導のチェック・ボックス型のアクティビティーとみなされてきました。従来のアプローチは負荷が大きく、高価ならびに複雑で、組織を ID 違反に対して脆弱な状態のままにする可能性があります。より有効なアプローチは、ID ガバナンスおよび制御プロセスを効率化し、自動化します。自動化されたガバナンスおよび管理ソリューションは、以下のような多くのメリットを提供します。

- 認証プロセスおよび再認証プロセスの効率化
- プロビジョニング・プロセスおよびプロビジョニング解除プロセスの自動化
- アクセス権要求管理プロセスの簡潔化
- セルフサービス式のパスワード管理によってコストを削減する一方で、パスワード・ポリシーの強化を実現
- 役割管理および資格管理の最適化 (個人ではなく、組織の役割、グループ・メンバーシップ、ジョブ・アクティビティー、アクセス要件ごとにユーザーを分類することにより、IT ビジネス・チームと監査員の視点が統一される)
- SoD 違反の検出および阻止

これらのメリットはすべて、不適切なアクセスを最小化することにつながります。

迅速な行動を取る

監査が実施され、深い洞察が提言され、ガバナンス・ポリシーが導入された後は、その情報 (監査員によって提供されたスプレッドシードなど) を企業のセキュリティー施策として迅速に展開することが重要です。正しい ID ガバナンスおよび管理ソリューションは、ID ポリシーを事前対応的な仕組みおよび容易に使用できるアクセス管理ツールと統合することによって、セキュリティー・ガバナンス・ポリシーを実用的な制御へ迅速に変換することができます。

例えば、特定のアプリケーションへのアクセス権を持ったある従業員の役割が変わり、この資格が不要になった場合、ポリシーを基に動作する ID ガバナンスおよび管理ソリューションの実施によって、役割が変わると、資格は自動的に使用不能になります。

IBM は今日の企業が所有する重要資産の保護を支援するためのソリューションを提供します

ID ガバナンスと管理は、システム全体の ID およびアクセスを管理して、重要資産であるデータや他の企業資産に対するセキュリティーの改善を支援するために設計された、一連のプロセスおよびツールです。IBM® Security Identity Governance and Administration は統一されたビジネス中心のソリューションであり、IBM Security Identity Governance と IBM Security Identity Manager から成り立っています。

IBM Security Identity Governance は、ユーザー・アクセスとアクセス・リスクに関して、組織による理解、制御、および意思決定の実行を支援します。IBM Security Identity Manager は、ユーザーの資格管理およびプロファイル管理における効率と正確性を高める支援を行います。IBM はこれら 2 つを統合することによって単一のベンダー用ソリューションを提供します。このソリューションは、重要な ID ゲートウェイにおける組織のセキュリティー手段の改善を促進し、さらに全体の複雑性、および総所有コストを軽減します。

ビジネスにフォーカスしたアプローチ

IBM Security Identity Governance and Administration は、ビジネスに合わせたアプローチを提供することによってセキュリティーの改善を支援できます。このアプローチは内部チームに対してアクセスのレビューおよび認証を簡潔化するため、混乱が低減され、エラーが回避され、セキュリティー上の間隙が解消されます。これによって IT チーム、ビジネス管理者、監査員の視点が 1 つの統合された ID ガバナンス・プラットフォームに統一されるため、すべてのチームが ID セキュリティーを最適化するために同じ言語と同じツールを使用することになります。ビジネス管理者は、簡潔で直接的なビジネス言語を使用するツールによって、適切なユーザー役割とアクセス特権を素早く割り当てて評価することができ、その結果セキュリティー上の脆弱性が低下します。IT スタッフはこのソリューションによって、追跡記録と詳細な報告、特権の定期的再認証、および非準拠アカウントの検出と修正といった機能を使用し、ユーザー・アクセスの作成、修正、終了を自動化することができます。

可視性の最適化

IBM Security Identity Governance and Administration は、ユーザー・アクセスおよびポリシーの可視性を最適化します。これは重要な ID セキュリティー機能です。ソリューションは、中央リポジトリーで企業のアプリケーションからアクセスの資格付与を統合することによって可視性を最適化します。そして、事業部門、IT スタッフ、監査員によって共同で定義されるように、それらをビジネス役割およびアクティビティーに構築します。事業部門、IT スタッフ、監査員は、このソリューションによって定期的なレポートを素早く実行し、ユーザーがいつどこでアクセス権を獲得したか、実行中のユーザーは誰かを特定することができます。SoD 違反は強調表示されるため、セキュリティー上の脆弱性は容易に明らかにすることができます。

セルフサービス式の機能

IBM Security Identity Governance and Administration はユーザー・アクセスとパスワード管理の簡潔化、さらに SoD などのセキュリティー上の懸念に対応する機能の強化を目的として設計されています。また、これらの機能はすべて、ビジネス・プロセス、IT プロセス、コンプライアンス・プロセスの間の連携を支援するものです。容易に使用および理解できる、さまざまなセルフサービス式の機能を提供します。アクセス権の要求は、直観的で使いやすいインターフェースを使用しており、ショッピング・カートのようなエクスペリエンスです。セルフサービス式の機能によって、アクセス権に関連するタスクがより正確、適切、安全になります。

結論

IBM Security Identity Governance and Administration はポリシーとガバナンスの制御を ID 管理プロセスと統合することによって、組織がアクセスおよびリスクに関連する事柄を理解し、制御し、より良い意思決定を行うための支援をします。これによって高度で効果的なソリューションが実現し、ID セキュリティーおよび重要資産へのアクセスの保護が強化されます。

詳細情報

IBM Security Identity Management and Administration の詳細については、IBM の営業担当員またはビジネス・パートナーにお問い合わせいただくか、**ibm.com**/security/jp の Web サイトをご参照ください。

IBM セキュリティー・ソリューションについて

IBM セキュリティーでは、きわめて先進的で、統合されたエンタープライズ・セキュリティー製品/サービス群を取り揃えています。これらの製品/サービス群は世界的に名高い IBM X-Force® 研究/開発に支えられています。この支援を基に、これらの製品/サービス群では、組織におけるひと、インフラストラクチャー、データ、およびアプリケーションの全体的な保護に役立つセキュリティー・インテリジェンスを備えるさまざまなソリューションを、ID およびアクセス管理、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の領域で提供しています。これらのソリューションを使用することによって、モバイル、クラウド、ソーシャル・メディア、およびその他のエンタープライズ・ビジネス・アーキテクチャーに対するリスクの管理と統合セキュリティーの実装を効果的に行えます。IBM は、セキュリティーの研究/開発/提供をきわめて広範に行っている世界有数のセキュリティー組織を運営しており、130 カ国以上の国々で 1 日当たり 150 億件のセキュリティー・イベントをモニタリングし、3,000 件以上のセキュリティー関連の特許を保有しています。

さらに、IBM Global Financing は、ビジネス上必要なソフトウェアの機能を、もっともコスト効率が高く可能な限り戦略的な方法で入手できるよう支援します。信頼性が証明されたお客様とは協力関係を結び、資金面でのソリューションをビジネスおよび開発目的に合わせてカスタマイズすることができます。これによって効果的なキャッシュ管理が可能となり、総所有コストが改善します。無くてはならない IT に対して投資を行い、IBM Global Financing と共にビジネスを推進しましょう。詳細情報については、**ibm.com**/financing/jp の Web サイトをご参照ください。

IBM Security
Route 100
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in the United States of America
2015 年 3 月

[1] Grant Hatchimonji 著 “Report indicates insider threats leading cause of data breaches in last 12 months,” CSO、2013 年 10 月 8 日 http://www.csoonline.com/article/2134056/network-security/report-indicates-insider-threats-leading-cause-of-data-breaches-in-last-12-months.html