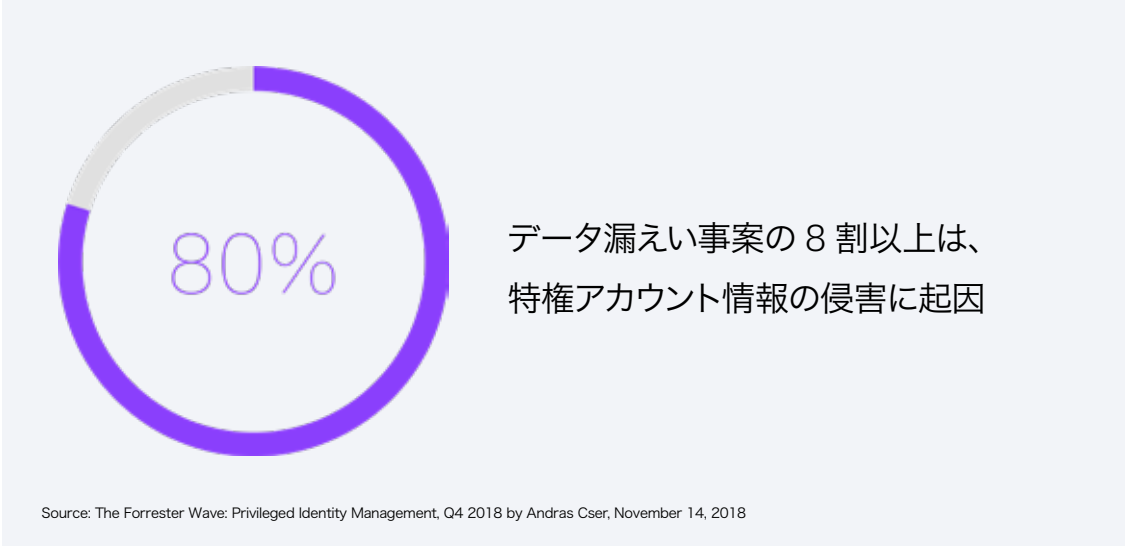
IBM Privileged Access Management
特権アカウントの管理と保護

1 特権アカウントの管理と保護が求められる背景

サイバー攻撃者が狙いを定める特権アカウント情報



特権アカウントを侵害すると、組織の IT インフラストラクチャーに自由にアクセスできるようになることから、特権アカウントが攻撃の標的として狙われています。多くの既知の情報漏えい事案は、管理や監視が不十分な特権アカウントから発生しています。攻撃者は、多くの場合、単一のエンドポイントから管理・制御能力を得て、組織に重大な損害を与えます。

特権アクセス管理で脅威をブロック

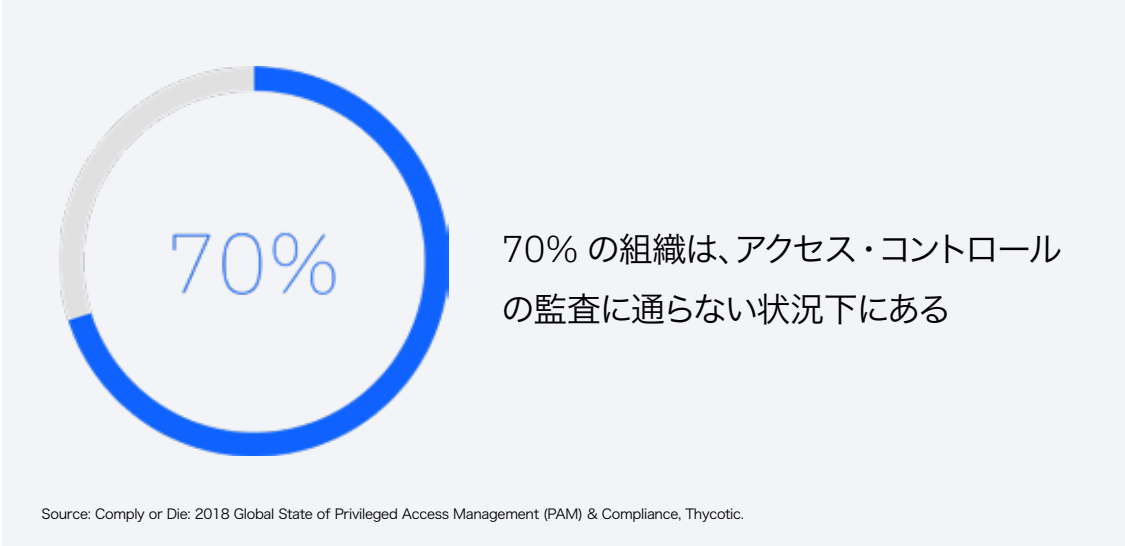
企業が特権アカウントへのアクセスを適切に保護、管理、監視できるようにすることで、IT インフラストラクチャーへの招かれざる客による侵害リスクを軽減することができます。

特権アクセス管理（PAM）は、より広範な ID のガバナンスと管理戦略の重要な要素です。パスワードを保護してエンドポイントを守り、特権アカウントを安全に保護することで、不審な詐欺師の手に渡らないようにすることできます。

2022 年までに、70% の組織が企業の全ユース・ケースに対して PAM を適用し、リスク対象を低減すると予想

特権アクセス管理の実践

最新のGartner 社調査の回答では、2022年までに90%の組織が特権アクセスに関するリスクを軽減することがセキュリティーを管理するうえでの基本的な要件であると認識するようになると示唆しています。[2] しかし、現段階では 70% の組織はアクセス管理の監査に合格しないと言われています。[3] つまり、大多数の組織が近い将来 PAM の重要性と価値を理解するようになる一方で、現在はそれを実践するために必要なPAMソフトウェア、コントロール、専門家のサポートが得られていない組織が半数以上を占めています。



IBM は、IBM Security Secret Server と IBM Security Privilege Manager という企業向けソリューションによって、包括的な PAM を提供します。専門家によるコンサルティングと 24 時間 365 日のサポートに支えられた IBM Secret Server と IBM Privilege Manager により、お客様は PAM の提供するすべての価値を活用できる一方、ID ガバナンス・ソリューションと統合して特権アカウント・ユーザーの完全なライフサイクル管理を実現することもできます。組織を保護する鍵となるのは、IDをより広範なセキュリティー・エコシステムに統合して、社内外の脅威を軽減することです。
以下2つの管理が重要になります。

1. **特権アクセス管理** – 企業の IT インフラストラクチャー内で権限の高いアカウントを管理するための特殊な要件に焦点を当てています。
2. **特権昇格と委任の管理 (PEDM)** – エンドポイントからローカル管理権限を削除することで、外部の脅威を防ぎ、マルウェアやランサムウェアによるアプリケーションの悪用を阻止します。

組織にこれら 2 点が必要な理由を説明します。

2 IBM Security Secret Server

特権アカウントを容易に検出、制御、変更、監査

特権アカウントの管理における最初のステップは、未知のアカウントを検出することです。手作業での処理やエラーによって、IT 部門が把握・管理していないアカウントが存在していることがあります。

IBM Security Secret Server を使用すれば、ITインフラストラクチャー全体を自動的にスキャンし、特権アカウント、共有アカウント、サービス・アカウントを検出することができます。検出された機密情報は、暗号化されて中央管理されたボールト（金庫）に保管され、高度な暗号標準によって適切に保護されます。すべてのアカウントに対してパスワード・ポリシーを実施・適用することができます。環境内のすべての特権アカウントを完全に可視化し、制御することができるようになります。

特権アクセスのスプロール化を阻止

IBM Secret Server を使用してインフラストラクチャー全体のすべての特権アカウントを検出したら、サービス・アカウント、アプリケーション・アカウント、管理者アカウント、root アカウントをすべて特定します。これにより、以前は検出されていなかった特権資格情報を完全に可視化し、制御します。

SSH 鍵の生成、保管、ローテーション、管理

SSH 鍵の生成、ローテーション、制御、保護を直接IBM Secret Server で行います。SSH 鍵はユーザー名とパスワードに似ていますが、自動化プロセスと、システム管理者によるシングル・ サインオンの実装に使用されます。役割に基づいて設定されるアクセス制御と権限セットを使用すると、ロケーションや IP アドレスに関係なく、誰がどの鍵セットへのアクセス権を持つかを制御することができます。

特権セッションの監視と記録

ユーザーのキー・ストロークをすべて把握します。IBM Secret Server は、リアルタイムでセッションの監視を行うことができ、リスクのある行動が見られた場合にセッションを終了させることができます。また、特権ユーザーのアクティビティーを記録することもできます。これにより、ユーザーが機密事項を調べた時間から、システム上で行った作業内容、最後にログオフした時間まで、監査証跡を取ることができます。最も重要なアカウントで何が起きているか、詳しい洞察が得られます。

有効期限が切れた時にパスワードを自動的に変更

有効期限の切れたパスワードは、定期的に変更する必要があります。 IBM Secret Server にはパスワード変更と有効期限のスケジュールが組み込まれており、重要なパスワードを手作業で変更することなく、自動的に変更されます。

すべての特権アカウントへのアクセス権の委任

承認者に対して、説明責任を常に果たし、背景を適切に説明することで、承認者はユーザーがアクセス権を必要とする理由を正確に把握することができます。サード・パーティー用に、役割ベースのアクセス制御（RBAC）や、透明性の高いアクセスを可能にする承認ワークフロー、時間制限など、アクセスとパスワードの承認のパラメーターも個々に設定可能です。

IBM Secret Server によるすべての特権アカウントの完全な可視化と制御

バックドア・アクセスや不正な構成変更が行われると、それを検知できるようになります。誰がシステムにアクセスしたかを特定し、そのアクションを確認して適宜対応することができます。また、セッション・モニターと記録により完全な監査証跡を取得できます。

拡張された監査機能とレポート作成機能

すぐに使用可能な数十のレポートを活用し、システムの状況とコンプライアンスに関するより適切な洞察を得ることができます。パスワード・ボールトのアクティビティーについて完全なレポートを生成し、必要に応じてデータベース照会からカスタム・レポートを作成することができます。

IBM Secret Server を統合してセキュリティーを強化

IBM Secret Server は、IBM Cloud Identity、QRadar®、Guardium® Data Protection、IBM Security Identity Governance & Intelligence を含む重要な IBM Security ソリューションとシームレスに統合します。

3 特権アクセス管理と ID ガバナンス

ID ガバナンス機能と統合することで、継続的なユーザー・ライフサイクル管理とコンプライアンスを実現します。

IBM Security Identity Governance and Intelligence (IGI)は、IBM Secret Serverと統合してライフサイクルの自動管理を実現します。PAMの実装は、単体のプロジェクトとして扱うことができません。IDガバナンスが機能しなければ、資格の集約、役割や役職、所属が変わるたびに特権アカウントへのアクセス権が増え続けてしまう、そして共有パスワードを限定的に見えるようにしてしまうなどといった問題が時間と共に表面化する可能性があります。これらの問題を防ぐためには自動化された ID ガバナンス機能が必要です。IBM Secret Server と IBM IGI を統合することで、特権資格情報とそれ以外のビジネス・ユーザー・アカウントの両方にわたる全体的な視点から、有害なアクセス権の組み合わせを防ぐことができます。IBM Secret Server は暗号化されたボールトで特権資格情報を安全に保管・監視し、IBM IGI はユーザーのアクセス・レベルが規制に準拠しており、SoD 違反になっていないか確認します。

有害なアクセスの組み合わせによる分類

1. **PAM ソリューション自体に関連した組み合わせ**
   例：特権アカウントの作成とアクセス権を付与する権限
2. **特権アカウントに関連した組み合わせ**
   例：アプリケーションと該当アプリケーションを稼働するサーバーを管理する権限
3. **ビジネス・サービスと特権アカウントに関連した組み合わせ**
   例：アプリケーションと該当アプリケーションを稼働するサーバーを管理する権限

リスクにつながるアクセス権の組み合わせを回避

PAM ソリューションによって、誰がアクセス権を持ち、特権アカウントを使用するかを簡単に把握できるようになりますが、それでも各ユーザーの持つ特権アクセスの独自の組み合わせを可視化し、洞察を得ることが必要です。アクセス権の「有害な」組み合わせを持つユーザーが、組織にリスクをもたらすためです。

あるユーザーが、データを保管するデータベースを使用するアプリケーションへのアクセス権を持っているとします。同一ユーザー(把握されていないユーザー) が、データベースを管理するために必要な特権アカウントのアクセス権も保持していたらどうなるでしょう。データベースの編集権限を持つ一方で、アプリケーションの業務利用と権限管理の制御が効かなくなってしまう可能性があります。また、そのユーザーが OS を管理する特権資格情報を持っていたとしたら、監査証跡が消去されてしまう可能性もあります。

アクセス権の棚卸しの自動化

IBM IGI を使用すると、アクセス権の確認を自動的に行うことができます。また、企業に有効な情報を管理者に提供することで、企業の認証プロセスを支援します。一括承認につながる可能性がある不可解な IT 業界用語からも解放されます。

IBM IGI を IBM Secret Server と統合することで、認証制御が拡張され、特権ユーザーだけでなく非特権ビジネス・ユーザーも含めることができます。エラーの起こりやすい手作業によるプロセスを、承認者がその対象をより理解しやすい自動化再認証プロセスに変更できます。

アクセス権の棚卸しは、特権と非特権アプリケーションへの明確で正常かつ適切なアクセス権を維持し、コンプライアンスに準拠していることを証明するのに役立ちます。

統合の利点

IBM Secret Server を IBM IGI と統合すると、次のような利点があります。

- 資格の集約を回避し、継続的なアクセス管理を保証できます。
- アクセス権の棚卸しによってコンプライアンスの遵守を容易に証明できます。
- 特権ユーザーと非特権ユーザーに対する SoD 制御により、リスクと、有害なアクセス権の組み合わせを回避します。

4 IBM Security Privilege Manager

エンドポイントから行き過ぎた特権を削除し、ポリシー・ベースの制御を使用してマルウェア攻撃を阻止

最小特権ポリシー

セキュリティーの規制では、攻撃対象を減らすために、アクセス権限の付与を最小限に止めるという原則が求められます。

最小権限では、すべてのユーザー、アプリケーション、システム・アカウントがそれぞれのジョブに必要なリソースへの最小アクセス権を持つことが要求されます。多くの顧客、ユーザー、アプリケーションは、機密データ/オペレーティング・システムへのアクセス権が含まれた管理権限または root 権限を持っています。最小権限モデルでは、管理者特権を持つ管理アカウントは、本当にそれが必要な人にしか付与されません。その他のユーザーはすべて、適切な特権セットを持つ標準ユーザーとなります。

PCI DSS、HIPAA、SOX、NIST および CIS セキュリティー・コントロールなどの規制では、コンプライアンス・ソリューションの一環として最小権限モデルを実装することを推奨あるいは要求しています。監査時に、管理アカウントを管理するために組織内で最小権限の原則がどのように適用され、施行されているかを実証しなければならない可能性があります。

最小権限ポリシーへの準拠を成功させるには、管理が必要な特権を把握する必要があります。つまり、どのエンドポイントとローカル・ユーザーが管理者資格情報または root 資格情報を持つかを明らかにし、どのアプリケーションが使用されているのか、実行するために管理者権限が必要かどうかを識別し、管理者特権セットを持つサービス・アカウントとアプリケーションのリスク・レベルを把握します。

ビジネス・ユーザーをローカル管理グループから除外しつつ、承認済みのアプリケーションをインストールする方法を提供できたら、どれほど多くの損害とリスクを取り除けるか、想像してみてください。

一つのエージェントで最大の攻撃対象を保護

IBM Privilege Manager は、一度に数十万台のマシンと通信できます。合理化された一つのダッシュボードから、自分の権限範囲の下で、ポリシーを確認し、すべてのデバイスとアプリケーションにわたって24時間 365 日のコントロールを実行できます。どのユーザーとエンドポイントが、ドメイン・マシンと非ドメイン・マシン全体の非表示またはハードコーディングされた特権も含め、ローカル管理権限を持つかを検出し、これらの権限を必要に応じて自動的に削除できます。これは、全ローカル・グループとユーザーの正確なメンバーシップをコントロールし、バックドア・アカウントのリスクを軽減するのに役立ちます。

摩擦のないユーザー・エクスペリエンスを保証する柔軟なポリシーを定義

IBM Privilege Manager は、資格情報を要求せず、ユーザーが IT サポートを依頼する必要もなく、組織全体のユーザーが必要とするアプリケーションとデータを自動的に昇格させます。信頼できるアプリケーションとプロセスへのアクセス権を判別して維持するきめ細かいポリシー・ベースのコントロールが提供されます。このソリューションでは、高度なリアルタイムの脅威インテリジェンスにより、ユーザーが定義した柔軟なポリシーに従ってアプリケーションをホワイトリスト、ブラックリスト、グレーリストに追加します。

- ホワイトリスティング - 信頼できるアプリケーションはホワイトリストに追加されて昇格し、ユーザーは IT サポートなしでそれらに容易にアクセスできます。
- ブラックリスティング - ブラックリストに追加されるアプリケーションは、リアルタイムの脅威インテリジェンスに 基づいてリストに加えられ、実行が阻止されます。
- グレーリスティング - 脅威の可能性のあるアプリケーションはグレーリストに追加され、隔離されたサンドボックス環境に移動してさらに検証されます。

さらに、リストの指定にかかわらず、必要と判断されたときはいつでも、任意のアプリケーションを隔離して「サンドボックス化」することができます。隔離されたアプリケーションは、システム・フォルダーや基盤となるOS 構成が露出されるというリスクを伴わずに、安全に実行し、テストできます。

ローカル管理権限を容易に管理・削除

システム管理者を含め、どのアカウントがローカル・グループのメンバーであるかを判別します。必要であれば、すべてのローカル管理特権を一度に削除することで、すべてのエンドポイントを「クリーン状態」に素早くリセットすることができます。

ユーザーとサポート・スタッフの生産性を改善

ポリシー・ベースのコントロールはアプリケーション・レベルで定められるため、ユーザーは自分たちが必要な信頼できるアプリケーション、システム、データにアクセスできます。ローカル管理権限は不要で、IT サポートにチケットを送信する必要もありません。

透明性による監査コンプライアンスの達成

すべてのアプリケーション・ポリシー、管理資格情報、特権昇格アクティビティーの分かりやすい監査証跡を監査員と共有します。必要に応じて、コンプライアンス・レベルと対応策について、明確なイメージを提供できます。

5 IBMの特権アクセス管理をお勧めする理由

比類ないサービスとサポートに支えられた、拡張が容易な企業向けセキュリティー・ソリューション

IBM Security Secret Server と IBM Security Privilege Manager を導入すると、次のソリューションにより PAM の可能性を十分に引き出すことができます。

Fast

15分でデプロイし、すぐに開始

Easy

特権アカウントを、直感的に管理

Simple

複雑で時間のかかるプロセスを自動化

IBM サービスの特徴

- IBM サポートを24時間 365日利用可能
- IBM Secret Server 内の機能セットを無制限で利用可能
- シンプルな料金体系とパッケージ・オプション
- 価値実現までの時間の短縮。数分でインストールが完了し、すぐに価値を実現
- オンプレミスからクラウド環境まで、大規模な分散環境に対応
- IBM Security ポートフォリオとの統合
- IBM Security PAM Professional Services の利用
- 実装と構成時に IBM Security Expert Labs の利用

[1] 出典 : The Forrester Wave: 特権アイデンティティー管理、2018 年 第 4 四半期、Andras Cser 著、2018 年 11 月 14 日
[2] 出典 : PAM の 4 つの柱によって管理された特権アクセスのベスト・プラクティス、Gartner、2019 年 1 月 28 日
[3] 出典 : 決死の準拠 : 2018 年 特権アクセス管理 (PAM) リスクおよびコンプライアンスのグローバル状況、Thycotic

IBM Security Secret Server の無料トライアル	→ ibm.biz/secret_server_trial
セキュリティー・インテリジェンス・ブログ	→ ibm.biz/security_blog
お問い合わせ	→ ibm.biz/security_contact

〒103-8510 東京都中央区日本橋箱崎町 19-21