DATA SHEET

CA Privileged Identity Manager

概要

CA Privileged Identity Managerは、特権アイデンティティ管理（PIM）向けの総合的ソリューションを物理環境と仮想環境の両方で提供します。事前対応的なアプローチによって機密情報と重要なシステムが保護されるため、通常のビジネスやITの活動に影響が及ぶことはありません。CA Privileged Identity Managerは、IT環境全体で特権ユーザによる企業のシステムおよびデータへのアクセスと使用を制御することでリスクを軽減し、コンプライアンスを確保します。これにより、高度なセキュリティ、管理コストの削減、監査/コンプライアンス プロセスの簡素化を実現できます。

主なメリット / 成果

特権ユーザのアカウンタビリティの有効化： 特権ユーザがシステムおよびデータにどのようにアクセスし、それを使用するかを制御します。

物理環境と仮想環境のセキュリティ保護： 物理システム、仮想マシン、およびハイパーバイザ上で特権アイデンティティを制御します。

コンプライアンスの推進： PCI および ISO 27002 などの要件に対応します。

主要な特長

- 共有アカウント・パスワード管理
- 仮想化に対応したセキュリティ制御の自動化
- 詳細設定可能なアクセス制御
- Unix 認証ブリッジング
- ユーザ・アクティビティ・レポート
- 職務分掌
- ハイパーバイザの強化
- Amazon Web Services（AWS）向けの保護
- 二要素認証のサポート

ビジネス上の課題

企業は増え続けるセキュリティ上の課題だけでなく、複雑な規制要件の問題にも直面しています。このため、特権ユーザの操作を制御し、システムへのアクセスを管理するとともに、特権ユーザの操作権限を検証できる必要があります。

特権アイデンティティを制御できなければ、データの損失や破壊、悪意ある損害、罰金、訴訟、株主価値の損失を招くおそれがあります。さらに、監査担当者はクライアントに対し、特権ユーザに対する制御機能があることを率先して立証し、特権ユーザのアクティビティを報告するよう要求しています。

標準規格や要件は、仮想化に伴うリスクももたらします。Payment Card Industry Security Standards Council（PCI SSC）は、データ・セキュリティ標準のバージョン 2.0 を使用した仮想化を導入するよう要件を更新し、仮想化ガイドラインに関する個別の補足情報も発表しました。

仮想化には多くの IT 上の利点がある一方、ハイパーバイザの柔軟性と性能によって特権ユーザ関連のリスクは拡大の一途をたどっています。現在では、1 つの特権アカウントが組織の IT インフラストラクチャに広範囲かつ修復不可能な損害をもたらす可能性もあります。

ソリューションの概要

CA Privileged Identity Manager は、特権アイデンティティ管理（PIM）向けの総合的ソリューションを物理環境と仮想環境の両方で提供します。CA Privileged Identity Manager は拡張性の高いソリューションで、共有アカウント・パスワード管理、詳細設定可能なアクセス制御、ユーザ・アクティビティ・レポート、および、サーバ、アプリケーション、デバイス間の UNIX 認証ブリッジングを中央管理コンソールから実行できます。CA Privileged Identity Manager for Virtual Environments はインフラストラクチャから仮想マシンに至るまで、仮想環境で特権アイデンティティを管理し、セキュリティを自動化します。

重要な差別化要因

CA Privileged Identity Manager は、多様性と専門性を兼ね備えた、総合的な特権アイデンティティ管理向けのソリューションを提供します。詳細設定可能なアクセス制御から仮想環境でのセキュリティポリシー自動化に至るまで、CA Privileged Identity Manager は物理データおよび仮想データを保護するための重要な顧客ニーズに対応し、企業を支援します。

特権ユーザのアカウンタビリティの有効化：特権ユーザがどのように企業データにアクセスしてそれを使用するかを制御および監視し、アカウンタビリティと職務分離を実現します。

物理環境と仮想環境のセキュリティ保護：物理システム、仮想マシン、およびハイパーバイザ上で特権ユーザを制御します。

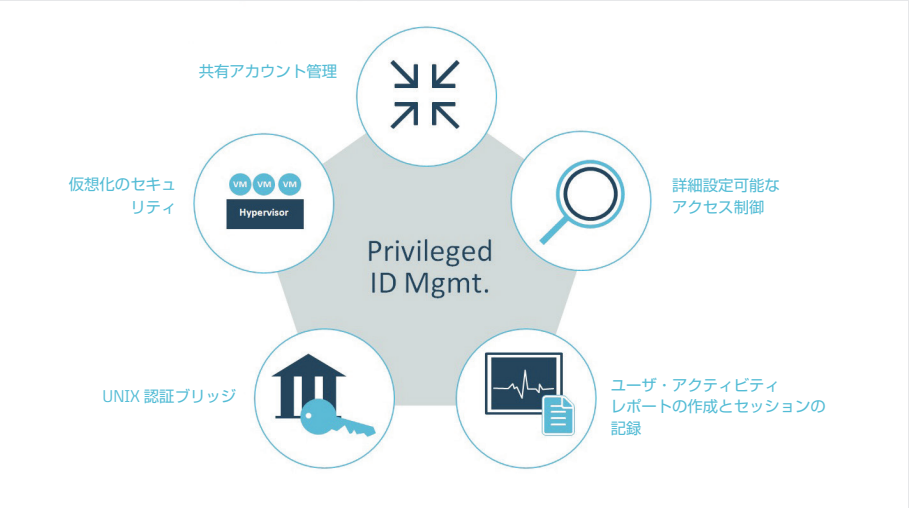
コンプライアンスの推進（仮想データセンタを含む）：ハイパーバイザのセキュリティ制御と特権アイデンティティの管理を通じて、重要なコンプライアンス・ポリシーの状態を率先的に報告することで規制遵守に対応します。

自動化による IT コストの削減：物理システムと仮想システムの両方で、パスワード管理などの自動化を促進します。

自動化によるセキュリティの向上：ポリシーベースの自動化を利用することで人的エラーを低減し、必要な変更をリアルタイムで実施できるようにし、セキュリティを向上させます。

仮想化の導入促進：仮想マシンおよびハイパーバイザでの特権ユーザの操作を制御することで、最も重要なサーバの仮想化も可能にします。

CA Privileged Identity Manager は、物理環境と仮想環境の両方を保護します。



CA Privileged Identity Manager では、オペレーティング・システムレベルのアクセスだけでなく、個々のアプリケーションへのアクセスも制限できます。

パスワードの盗用および共有の防止：パスワード共有や「肩ごし」のパスワード盗用を防止できる一方、パスワードをカットアンドペーストする必要もありません。

セキュアなマルチテナント環境の構築：ネットワークのゾーニングとハイパーバイザ強化機能を使用して、セキュアなマルチテナントを実現します。

UNIX/Linux 管理コストの削減：Microsoft® Active Directory でユーザを認証し、シングルサインオン機能を使用することで、UNIX/Linux アカウント管理のコストを削減します。

強化された特権アイデンティティの保護：特権アイデンティティへのアクセスには、CA Strong Authentication（旧 CA AuthMinder™）の二要素認証を要求します。

AWS 向け Infrastructure-as-a-Service（IaaS）PIM: AWS 向けの総合的な参照アーキテクチャ。

関連製品およびソリューション

CA Identity Governance: 資格認定や役割管理も含め、アイデンティティおよびアクセス・ガバナンスを保護します。

詳細については **ca.com/jp/PIM** をご覧ください。

CA Technologies（NASDAQ:CA）は、企業の変革を推進するソフトウェアを開発し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

CS200-86967_0914