WHITE PAPER | 2017 年 9 月

最も重要なサーバにおけるデータ侵害のリスク緩和:CAの活用

Table of Contents

概要

課題

今日の企業はセキュリティ侵害のリスクを軽減して、組織内の重要なデータを保護することが求められています。また、IT 監査で企業に課される要件はますます厳しくなっています。これは、特権アカウントと特権アクセスがハッカーの新しい攻撃のターゲットとなっていることが原因です。そのために、監査では特権アカウントの制御を強化することが重視されているのです。

ビジネス・チャンス

適切な特権 ID アクセス管理ソリューションでは、オペレーティング・システム・レベルのアクセスと特権ユーザのアクションに対して強力で詳細な制御が提供されるため、ミッションクリティカルなサーバを包括的に保護できます。また、システム・レベル、ホストベースの特権 ID アクセス管理ソリューションによって、強力なネイティブのスーパ・ユーザ・アカウント（UNIX® と Linux® のルート、Microsoft® Windows® 管理者など）のアクセスを制御できるため、特権ユーザの活動の制御、監視、監査を通してセキュリティを強化し 監査と遵守性を簡略化できます。

メリット

CA Technologies の容易に展開できる包括的な特権 ID アクセス管理ソリューションを使用すると、クレデンシャル管理の統合、強力な本人認証、ゼロトラストのアクセス制御、プロアクティブなコマンド・フィルタリング、セッションの監視と記録、重要なサーバの詳細な制御などが行えます。CA Privileged Access Management では、攻撃の主要な構成要素の実行をプロアクティブに防止でき、リスク軽減や運用効率の改善に役立つ機能と制御が提供されます。その主な利点には、リスク緩和、説明責任の履行の向上、監査と遵守性の改善、複雑性の緩和などがあります。

はじめに

今日の企業はセキュリティ侵害のリスクを軽減して、組織内の重要なデータを保護することが求められています。また、IT 監査で企業に課される要件はますます厳しくなっています。これは、特権アカウントと特権アクセスがハッカーの新しい攻撃のターゲットとなっていることが原因です。そのために、監査では特権アカウントの制御を強化することが重視されているのです。

残念ながら、あらゆる高度な攻撃では本来の目的にかかわらず、ハッカーの重要な成功要因になっているのは特権アカウントの盗用や侵害です。特権アカウントには特権ユーザ、アカウントおよびクレデンシャルが含まれ、これらには社員、サードパーティの請負業者のほか、IT インフラストラクチャに存在し、特権クレデンシャルを含む無数のアプリケーションやスクリプト（多くの場合、ハードコードで不特定多数が表示可能）が含まれます。

また、UNIX、Linux、Windows などのオペレーティング・システムは、システムのセキュリティコントロールの大半を迂回できる「スーパ・ユーザ」という概念を基盤に構築されています。このように高位の特権アカウントは通常、正当な目的で管理者によって使用されますが、悪意の内部関係者や外部の攻撃者によって悪用される可能性もあります。

このようなユーザとそのクレデンシャルを保護することは、攻撃を防止するための重要な要素です。また、特権 ID アクセス管理は徹底防御の戦略の新しい重要な要素として、ファイアウォールやアンチウイルスと同様に、ビジネスの保護には不可欠です。適切な特権 ID アクセス管理ソリューションでは、オペレーティング・システム・レベルのアクセスと特権ユーザのアクションに対して強力で詳細な制御が提供されるため、ミッションクリティカルなサーバを包括的に保護できます。また、システム・レベル、ホストベースの特権 ID アクセス管理ソリューションによって、強力なネイティブのスーパ・ユーザ・アカウント（UNIX と Linux のルート、Windows 管理者など）のアクセスを制御できるため、特権ユーザの活動の制御、監視、監査を通してセキュリテを強化し 監査と遵守性を簡略化できます。

このホワイト・ペーパーでは、ミッションクリティカルなサーバと今日利用可能なアプローチの課題を検証します。また、ミッションクリティカルなサーバの保護で最も成熟し、実績ある強力なソリューションを提供する CA Privileged Access Manager Server Control について説明します。CA Privileged Access Manager Server Control は実績あるメインフレーム・セキュリティ・モデルをベースにしているため、スーパ・ユーザに対してもプロアクティブなアクセス制御と優れた監査を効果的に適用できます。

ミッションクリティカルなサーバのセキュリティにおける今日の課題

悪意のある内部関係者や外部のハッカーは、ミッションクリティカルなサーバの特権ユーザ・アカウントを乗っ取り、悪用しようと常に狙っています。たった 1 つでも違反があれば、組織の評判や財務に莫大な被害が及びます。IT 部門は標的型攻撃を阻止し、内部の脅威を緩和すると同時に、コンプライアンスを達成および維持するために業界のセキュリティの要件と標準を遵守するという大きな責任を担っています。また、ますます複雑化するハイブリッド・インフラストラクチャの管理とセキュリティを確保しながら、自動化とスケーラビリティによって運用効率を向上させることも重要な任務になっています。その責任は広い範囲に及びます。

通常、サーバに保存されているデータのリスクは、ミッションクリティカルのレベルによっては許容レベルまで低下します。クレジット・カード情報、社会保障番号、個人識別情報、医療レコード、E メール・アドレス、あるいは、図面などの知的財産、財務結果、内部関係者情報が含まれているサーバは他のサーバーよりも価値があります。特権 ID アクセス管理によってリスクは緩和されますが、最も重要なサーバを保護するためには特別な手順が必要です。それでは、その主なアプローチを説明しましょう。

主なアプローチ：基本以上の「強化」が必要な重要なシステムの保護

IT にとって最も差し迫った課題の 1 つは、顧客データ、金融レコードおよび知的財産など、企業の機密の電子アセットをホストしているサーバのセキュリティを確保することです。これらのアセットは多くの企業の生命線であり、何らかの違反があると、取り返しのつかない損失を被ることになります。

一般的な「サーバ強化」の手段として以下の方法があります。

- ネットワークに接続する前にすべてのパッチをインストールする
- 不要なサービスを削除する
- 使用していないソフトウェアやサンプル・ファイルを削除する
- アンチウイルス / アンチスパイウェア / アンチフィッシング・ソフトウェアをインストールする
- 機密度の高いドライブを暗号化する
- 強力なパスワードを使用する
- スーパ・ユーザのパスワードは限られた小数の重要な管理者だけが共有する

上記の手順のほとんどは有効であり、一般に認められたセキュリティの考え方に従っていますが、最後の手順は、システムに対する管理アカウントを効果的に制御することは不可能であるという基本的に誤った思い込みによるものです。これは、悪意のある内部関係者だけでなく外部の攻撃者も悪用できる大きな穴を、サーバのセキュリティに残すことになります。どのような攻撃であっても、最も大きな被害をもたらす攻撃は特権アイデンティティの使用に関するものです。この種のアカウントは本来、システムやアプリケーション、データベースに重大な変更を加える権限があります。したがって、これらのアカウントを使用したアクションは、甚大な被害をもたらす可能性があるため、詳細に監視する必要があります。

ネイティブのオペレーティング・システムのセキュリティ

ネイティブのオペレーティング・システムの制御におけるセキュリティの課題は、基本的にスーパ・ユーザの概念に基づいています。つまり、サーバ上のすべてのセキュリティ制御を迂回して無効にしてしまう特権レベルが原因になっています。これは、Linux/UNIX の「ルート」アカウントや Windows の「管理者」アカウントなどに共通して見られます。

これらのオペレーティング・システムは、スーパ・ユーザのアカウントに制約がないことを前提に設計されています。そのため、スーパ・ユーザ・アカウントは攻撃者に狙われ、標的にされるのです。攻撃者がアカウントを制御すると、アカウントは名前のある個人と関連付けられていないため、実質的にサーバー上のあらゆるデータに匿名で無制限にアクセスできます。このような理由から、多くの商用サーバベースのソリューションでは、ユーザを制御しスーパ・ユーザ・アカウントをなるべく使用しないよう制限します。このようなアプローチの大きな欠点は、すでにスーパ・ユーザの権限を悪用しているユーザからサーバを保護できないことです。セキュリティコントロール自体も、確かな動機を持つ熟練した攻撃者に侵害される可能性があります。また、セキュリティコントロールは通常、システム管理者が管理と保守を担当しますが、その管理者もソリューションによって制御されるグループの 1 つを代表しているにすぎません。それでは、きつねに鶏小屋を監視させるようなものです。

上記のような理由から、ネイティブのオペレーティング・システムの機能では、不注意や攻撃に対して十分な保護が提供されず、サーバ環境全体で信頼性の高い監査が提供されないため、顧客データベースや病院の患者レコード、専有情報など、組織にとって最も機密性の高い電子アセットを保護することは困難です。この問題は、外部顧客向けのホスト・システムに機密データや重要なアプリケーションが含まれる場合や、重要なシステムや情報を請負業者に公開したり、そのホスティングをサービス・プロバイダに任せる場合はさらに深刻になります。

また、オペレーティング・システムのアクセス制御は**既知の制御**であるため、分析されて回避されるリスクがあります。不正なアクセスを行う外部の人物であれ内部関係者であれ、悪意ある攻撃者が特権アカウントへのアクセスを獲得したとき、共通して行う最初の作業はセキュリティ設定について調べることです。オペレーティング・システムの権限を確認したり、利用できる制御の脆弱性を探すこともその一部です。また、悪意あるユーザは自分の痕跡を隠蔽するために、オペレーティング・システムのログを変更しようとします。アクセス制御が厳密に実施されているシステムであっても、熟練した攻撃者はアラートを生成したり検出につながるアクションを簡単に避けて通ります。完全に外部化され、スーパ・ユーザも制限されたセキュリティ・システムでなければ、攻撃者が**予期できない不可知**の要素でセキュリティ・システムを構成し、アクセス制御とユーザの活動記録を活用してシステムの安全を確保することはできません。

また本来、オペレーティング・システムがそれ自体の制御の完全性を確保することは不可能です。すべてのシステムで、特権アカウントを使用してシステムのセキュリティコントロールが変更されたり迂回される可能性があります。適切なアクセス権を持つユーザであれば、必要な制御を無効化して権限のないアクションを行い、システム・ログ・ファイルを変更してその作業のレコードを消去することができます。

オペレーティング・システムのセキュリティコントロールによるもう 1 つの問題は、**統一性の欠如**です。

セキュリティコントロールの機能と可用性はプラットフォームによって大きな差異があります（UNIX ファイル / ディレクトリの制御は Windows® と顕著に異なります）。次のような、実際のセキュリティ上の問題につながる可能性があります。

- ビジネスニーズを満たすためではなく、システムの限界に合わせてセキュリティ・ポリシーが作成される。
- セキュリティ管理の複雑さが増すことでエラーや不手際が生じる。

シェル・ラッパー

オペレーティング・システムの制御を使って特権ユーザを制御する共通の手法では、シェル・ラッパーを使用して、指定された個人による特定のコマンドへのアクセスを許可 / 拒否するように設定します。シェル・ラッパーは、コマンドがカーネルで実行されるオペレーティング・システムのユーザ・モードで動作します（オペレーティング・システムの下位レベル・コンポーネント）。

シェル・ラッパーには次をはじめ、多くの弱点があります。

- シェル･ラッパーはスーパ･ユーザ･アカウントそのものに対する防御にはなりません。ルート･アカウントへのアクセス権を持つユーザや、技術に精通したユーザは、次の技法を使っていつでもシェル・ラッパーを迂回できます。
  - ルート・ユーザが現在のシェル・プロセスを強制終了させると、カーネルによってラッパーの制限のない新規のシェルが作成されます。
  - ユーザがターゲット・システムにスクリプトをアップロードし、そのファイルを実行します。すべてのコマンドがオペレーティング・システム・カーネルの実行するシェル・ラッパーを迂回します。このスクリプトでは、機密データを変更または削除したり、システムの外へ送信することができ、シェル・ラッパーから完全に隠れてその制御を受けないようにすることができます。
- また、シェル･ラッパーが保護できるのは、シェルに入力されたコマンドだけです。システム上にある他のアプリケーション（Oracle など）がセキュリティ・ホールとなって、悪意のあるコマンドの実行に悪用される可能性があります。シェル・ラッパーではそれを検出することも、制御したりログに記録したりすることもできません。
- さらに、キー・ロガーがシェル・ラッパーの一部である場合、どのコマンドを実行したかではなく、どのキーを押したかだけが記録されるため、キー・ロガーも有効ではありません。悪意のあるユーザ（管理者など）は、複数のアクションを実行するスクリプトをアップロードできます。キー・ロガーには、スクリプトが実行されたことだけが記録され、実際に何が実行されたかは記録されません。そのため、キー・ロガーの目的である説明責任を果たすことはできません。
- シェル・ラッパーを奨励するベンダーは通常、ルート・パスワードを共有しないことを推奨しています。これは運用上、実用的とはいえません。多くのアプリケーションでは、インストールや機能のためにルート・パスワードが必要になります。

sudo

sudo（superuser do）は、システム管理者が特定のユーザ（またはユーザ・グループ）にルートとして一部（またはすべて）のコマンドの実行を許可することができ、使用されたコマンドをすべてログに記録するフリーウェア・プログラムです。sudo は、大半の UNIX/Linux 環境で使用されます。その場合、運用スタッフがルートのシェルにアクセスする必要はありませんが、プロセスの開始 / 停止、特定の構成ファイルの更新、サーバの再起動など、特定のコマンドをルートとして実行する必要があります。sudo では重要な機能（特権タスクの委任）が提供されますが、sudo 単独の制御では不十分です。

sudo には次をはじめ、多くの弱点があります。

- sudo は 1 つまたは複数の sudoers ファイルの使用に依存しますが、sudoers ファイルの管理には時間がかかり、多くのリソースを必要とするだけでなく、エラーも発生しがちです。さらに、危険に晒される可能性がある特権 ID で管理するため、sudoers ファイルとその管理がセキュリティ・リスクにつながる可能性があります。
- sudo には、エンタープライズ規模のログ記録機能はありません。sudo は、UNIX syslog に依存しており、ルート・ユーザによって改ざんされる可能性があります。sudo の各アクションに関する説明責任に役立ちません。sudo で実行されたすべてのコマンドが、元のユーザまで追跡できるようにログに記録されるわけではありません。そのため、PCI や SOX の要件への遵守性は確保できません。
- sudo では、たとえユーザがシェルに侵入してきた場合でも、「vi」を起動したユーザの ID に基づいてアクションを監査および追跡することはありません。ユーザがルートとして sudo で「vi」を起動しても、「vi」を抜け出し、ルート特権でシェル・コマンドを実行するオプションがあります。CA Privileged Identity Suite では、このように実行されたシェル・コマンドを sudo を起動したユーザまで追跡できます。
- sudo には機能上、致命的な制約があります。sudo では、ユーザ固有のファイル / フォルダやコマンドに対するアクセス権の割り当て / 制限はできません。
- sudo の制約は、ユーザが上位の特権に変更すると機能しません。正規のユーザが OS の脆弱性を悪用して「ルート」アクセスを取得すると、sudono すべての制約を回避できます。
- ネイティブのオペレーティング・システム制御を使用すると、サーバとプラットフォーム間でセキュリティ・ポリシーが一貫して適用されなくなることがあります。プラットフォーム間の差異を排除するには、異種プラットフォームに適用できる強力な単一のアクセス制御のセットが必要になります。

プロキシ制御

アクセスを制御するもう 1 つの手法として、プロキシがあります。この手法では、一元化された「チョーク・ポイント」をすべてのコマンドが通過し、ルール・セットで指定したコマンドがフィルタリング（拒否）されます。必要なコマンドを認識およびブロックすることで、特権ユーザがシェルを「停止」するのを防止できます。

プロキシには以下をはじめ、多くの弱点があります。

- プロキシはアプリケーションを使って迂回できます。ユーザは（vi などの）テキスト・エディタを使用して実行可能ファイルを作成し、制限されたコマンドを挿入できます。プロキシはアプリケーション内でユーザが実行しているアクションを把握することができません。プロキシは「自動完了」または結合されたコマンドを検出できません。
- プロキシは外部ダウンロードを使って迂回できます。シェル・ラッパーと同様に、制限されたコマンドを含むファイルを多様な方法を使ってターゲット・システムにダウンロードすることで（FTP、SSH、物理 USB ドライブなど）、プロキシを完全に迂回できます。このようなファイル転送ユーティリティは、管理とシステムの共通タスクで必要となるため、アクセスを拒否することは必ずしも可能ではありません。
- セキュリティ保護されていない単独のコマンドは、プロキシ制御を回避するバックドアとして使用できます。
- プロキシは、ソフトウェアの脆弱性に対しては効果を発揮できない可能性があります。プロキシ・ベースの制御は、ゼロデイ攻撃など、ソフトウェアの脆弱性を悪用した攻撃に対してはまったく役に立ちません。

アクセス制御 / ホストのセキュリティ

前述のように、共有スーパ·ユーザ·アカウントを使用すると、通常、特権ユーザはアクセスする必要のない重要なシステムやデータにもアクセスできるようになります。これは、「最小限の特権」および「職務の分離」というセキュリティの考え方に反します。オペレーティング · システムには、共有アカウントを使用する複数のユーザのアクションとアクセスを制限する機能がありません。詳細設定可能なアクセス制御なら、OS のセキュリティの枠を超えて**ユーザの本来の ID を調査して、アクションを許可するか拒否するかを判断できます**。これにより、完璧な最小特権アクセスを実現できます。

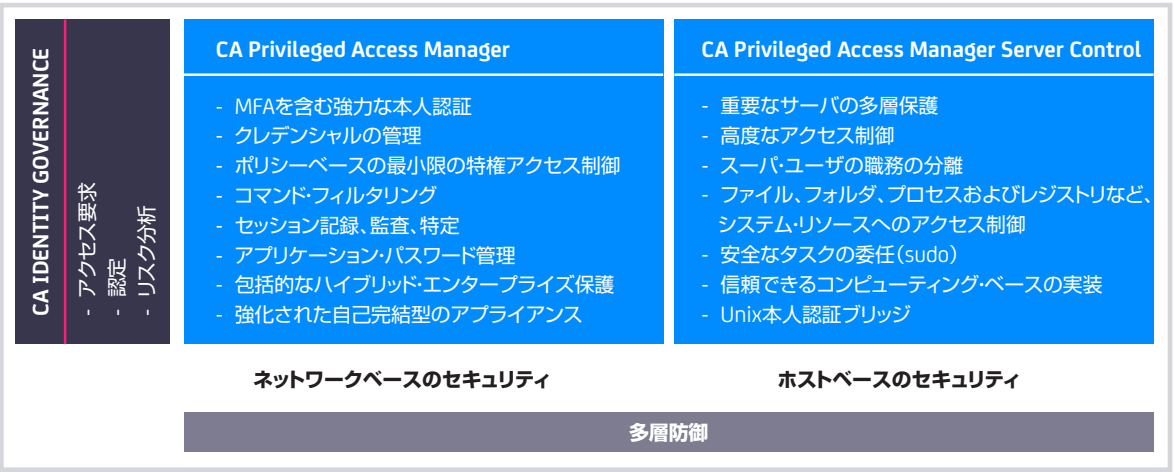
管理者の権限を職務に必要な範囲のみに制限するには、次で説明する機能が必要です。

CA の活用

CA Technologies の容易に展開できる包括的な特権 ID アクセス管理ソリューションを使用すると、クレデンシャル管理の統合、強力な本人認証、ゼロトラストのアクセス制御、プロアクティブなコマンド · フィルタリング、セッションの監視と記録、重要なサーバの詳細な制御などが行えます。このソリューションでは 2 つのデプロイ · オプションによってセキュリティのニーズに適切なレベルの防御が提供され、特権アカウントの徹底した防御によってセキュリティと遵守性のリスクを最小限に抑えることができます。

- **CA Privileged Access Manager** では、違反の防止、遵守性の実証、運用効率の向上に必要な包括的な機能が提供され、データセンタ、ソフトウェア定義の仮想データセンタ、ネットワーク、パブリック / プライベート · クラウドなど、どんなに広範で複雑なインフラストラクチャも保護できます。
- **CA Privileged Access Manager Server Control** では、オペレーティング · システム · レベルのアクセスと特権ユーザの活動を強力かつ詳細に制御して、重要なサーバー上の特権ユーザの活動を制御、監視、および監査できるため、セキュリティが強化され、監査と遵守性の確保が簡略化されます。
- **CA Threat Analytics for PAM** では、強力なユーザ動作分析と機械学習アルゴリズムを使用して、ビジネスに影響する前に違反を検出および防止できます。

図 A
CA の徹底防護のセキュリティ · アプローチで保護される主要な要素



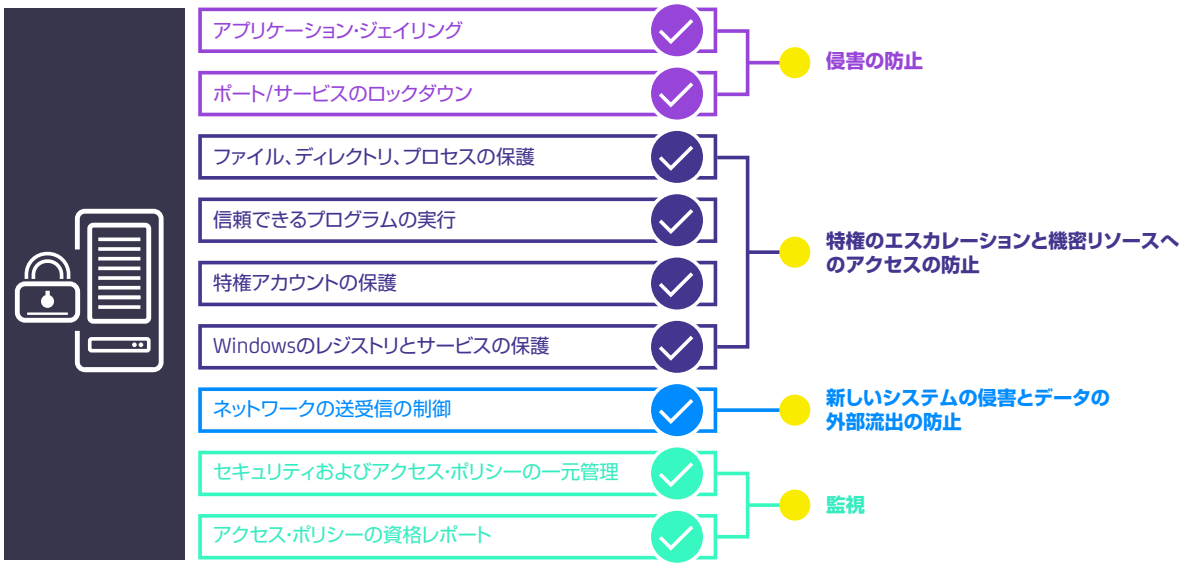
CA Privileged Access Manager Server Control の詳細

CA Privileged Access Manager Server Control では、オペレーティング・システム・レベルとアプリケーション・レベルのアクセスに、ローカルライズされたきめ細かいアクセス制御と保護が提供されるため、ビジネス・クリティカルなアセットをホストする重要なサーバの追加のセキュリティ要件に対応できます。また、各ホストのポリシーやきめ細かい制御に基づいて、個々のファイルやフォルダ、特定のコマンドをエージェントベース、カーネルレベルで保護できます。

不適切なスーパ・ユーザベースのセキュリティ・モデルをミッションクリティカルなサーバに使用することに起因するセキュリティ・ギャップも、CA Privileged Access Manager Server Control の独自の機能によって容易に解消できます。CA Privileged Access Manager Server Control の特長：

- スーパ・ユーザ・アカウントを使用している場合でも、職務の分離と説明責任に必要な元のユーザの ID を追跡できます。これにより、スーパ・ユーザベースのセキュリティ・モデルを根本的に変革できます。たとえば、Linux のルート・アカウントを使用するユーザ A とユーザ B には異なる権限を割り当てることができます。また、改ざん防止用の監査ログを使用して、すべてのスーパ・ユーザの操作の背後にあるユーザの実際の身元を識別できます。
- ファイル、ディレクトリ、システム・プロセス・リソースへの詳細設定によるアクセス制御
- ユーザ ID とログイン操作の保護
- UNIX/Linux のカーネル・モジュールのロード / アンロード
- Windows レジストリの保護
- 送受信に使用する TCP/IP の保護
- UNIX/Linux および Windows 用タスクの委任（安全な sudo への置換）
- ルートのパスワードを隠す機能
- ファイルとプログラムの完全性監視
- 迂回や終了に対する自己防衛

図 B
CA Privileged Access Manager Server Control の詳細



ソリューションのメリット

CA Privileged Access Manager では、攻撃の主要な構成要素の実行をプロアクティブに防止でき、リスク軽減や運用効率の改善に役立つ機能と制御が提供されます。CA Privileged Access Manager の主な特長は次のとおりです。

- **リスク緩和 :** ネットワークへの接続が許可されても、不正アクセスを防止するため、アクセスを事前に承認されたリソースのみに制限します。パスワードその他のクレデンシャルを不正な使用や侵害から保護します。ユーザがシステム上で実行できるアクションを制限します。不正なコマンドの実行とネットワーク内の横方向の移動を防止します。
- **説明責任の向上 :** 共有アカウントが使用されている場合でも、ユーザの活動のすべての属性を観察します。包括的なログ記録、セッション・レコード、ユーザの警告によって活動をキャプチャし、不正な動作を阻止します。
- **監査の改善と遵守性の簡略化 :** 新しい本人認証とアクセス制御要件によって遵守性の確保を簡略化し、ネットワークの論理区分を使用して遵守性の要件の範囲を制限します。
- **複雑性の低減とオペレータの生産性の向上 :** 特権シングル・サインオンはリスクが制限されるだけでなく、管理するシステムやリソースへの管理者のアクセスが容易になるため、管理者の生産性が大幅に向上します。一元的なポリシーの定義と適用によって、セキュリティ制御の確立と適用が簡略化されます。このソリューションは従来の物理的なデータセンタ（サーバ、ネットワーク・デバイス、データベース、スイッチ、関連リソース）に加え、急増する仮想化とクラウドのプラットフォームにも対応しているため、幅広いハイブリッド IT インフラストラクチャを保護することができます。また、ソフトウェア定義のデータセンタやネットワーク、IaaS 環境、SaaS 製品に展開している基本的な管理インフラストラクチャやリソースも保護されます。

CA のソリューションは採用が容易で、採用後にハードウェアのコストが発生することもありません。容易な管理や使用によって価値実現までの時間が短縮されるだけでなく、優れた拡張性によってハイブリッド IT インフラストラクチャの長期的な利用が保証され、リスク緩和、遵守性の維持も可能になります。現在、CA Privileged Access Manager を使用され、ミッションクリティカルなサーバの保護を希望されるなら、CA Privileged Access Manager Server Control へのアップグレードをお勧めします。徹底防御のプログラムによるセキュリティの向上にすでに着手されている場合は、内部の脅威と特権アカウントの悪用のリスクを軽減するために、CA Privileged Access Manager の使用をご検討ください。

まとめ

賢明な企業は、コストのかかるデータ違反を防ぐために、重要なサーバー上の特権アカウントへのアクセスを自動化して保護しています。特権 ID アクセス管理などの徹底防御のセキュリティ・アプローチを活用したゼロトラスト・モデルを採用すると、進化を続ける脅威から組織を保護できます。CA Privileged Access Manager では、攻撃の主要な構成要素の実行をプロアクティブに防止でき、リスク軽減や運用効率の改善に役立つ機能と制御が提供されます。

次のステップ

アクセス保護とデータ侵害対策の詳細については、「**CA Technologies Privileged Access Management Buyers Guide**」を参照してください。

CA の特権 ID アクセス管理の詳細については、次のサイトを参照してください。**ca.com/jp/pam**

CS200-305094_0917