SOLUTION BRIEF

従来型および仮想のデータセンタ、プライベートおよびパブリック・クラウド、ハイブリッド環境で特権クレデンシャルを保護するには

ca technologies

特権クレデンシャルの管理と保護は、リスクを減らしコンプライアンス要件に対応するために不可欠です。企業は特権パスワード管理ソリューションについて、制御の深さ、対応範囲、提供するクラウドの適合の程度を評価する必要があります。CA Privileged Access Manager はこれらの 3 つの側面すべてに対応し、従来型、仮想、ハイブリッド・クラウドのインフラストラクチャを同じようにサポートすることで、IT リスクの低減、運用効率の改善、企業の投資の保護を促進する特権クレデンシャル管理のための次世代ソリューションを提供します。

概要

課題

仮想化とクラウド・コンピューティングの採用によって、特権アカウントのパスワードを効果的に管理および保護するという、以前からある問題の重要性と複雑性は増大しています。従来のインフラストラクチャ（ネットワーク・ギア、サーバ、メインフレームなど）上で特権パスワードを管理することは、セキュリティおよびコンプライアンス上の長年の課題でした。さらに問題を複雑にしているのが、アプリケーションにハードコードされた多数の特権クレデンシャルです。こうしたクレデンシャルの例が、Amazon Web Services（AWS）リソースへのアクセスに使用される SSH の鍵ペアと PEM エンコードされた鍵です。

ビジネス・チャンス

ハイブリッド・エンタープライズ全体で特権クレデンシャルを効果的に保護すれば、企業は外部の攻撃者や悪意ある内部関係者によるリスクの悪用を低減できます。企業は本書で説明する 12 の必須機能を達成する特権アクセス管理アプローチを採用することで、監査の失敗やコンプライアンス違反、高価値データの喪失、高コストにつながるサービス中断のリスクを低減できるビジネス・チャンスがあります。

メリット

CA Privileged Access Manager はあらゆる種類のリソースのあらゆる種類のクレデンシャルを、どこに保管されていても、現在のハイブリッド・クラウド環境に対応する方法で保護し管理するための包括的な制御のセットを提供します。これは制御の深さ、対応範囲の幅広さ、クラウド・コンピューティングへの適合を十分に提供できない他の方法に比べて、リスクや所有コスト、運用ワークロードの大幅な低減を可能にします。

セクション 1 :

特権パスワード管理の基本

特権ユーザ・パスワード（以降「特権パスワード」）は、管理アカウント（admin、root、SYS、sa など）や組織の IT インフラストラクチャを構成し制御するために使用される関連機能など、組織の最も機密性の高いリソースに一様にアクセスできる点で、通常のエンドユーザ・パスワードとは異なります。それに伴うリスクを考えると、こうしたクレデンシャルの管理と保護が重要であることはきわめて明白です。これは NIST Special Publication 800-53 やクレジットカード業界のセキュリティ基準（PCI-DSS）など、一般的に思いつくセキュリティ関連の標準や規制に膨大な関連要件がまとめられていることにも示されています。

規制要件は脇においても、特権パスワード管理はリスク管理の観点から優れたプラクティスであるだけでなく、現在の組織に共通する多くの安全性の低いプラクティスに対応する上でも不可欠です。脆弱なパスワードや時代遅れのパスワード、無防備なパスワード（付箋やスプレッドシートに書かれたままなど）、あるいは多すぎるパスワードの使用、パスワードの共有、共有アカウントの実行者を明確に特定できない、強力な認証の選択肢がない、中央からの失効の選択肢がないなど、日常的に目にする例は枚挙にいとまがありません。

しかしこれらの状況が本当に問題なのは、コンプライアンス違反は言うまでもなく、スピア・フィッシングや標的型攻撃、最終的にはデータ盗用にまで発展する恐れがあることです。証拠が必要ですか ?2015 年に Verizon が実施したデータ漏えい調査報告によると、漏えい事件の 95% で盗まれたクレデンシャルが使用されており、別の 10% は信頼できる内部関係者がクレデンシャルを誤用した結果です。[1] こうした報告からも、現在の組織が特権クレデンシャルの管理、保護、アクセス制御に CA Privileged Access Manager のようなエンタープライズレベルのソリューションを活用すべきである理由は非常に明白です。

2015 年、Verizon Data Breach Investigations Report、「95 percent of breaches could be traced to stolen credentials, while another 10 percent were the result of credential misuse by trusted insiders」[1]

ハイブリッド・クラウドの影響

上記に挙げた従来からある問題は、氷山の一角にすぎません。魅力的なコスト、適応性、応答性というメリットを考えると、ハイブリッド･クラウド構成が広く採用されることは避けられません。ハイブリッド･クラウド構成では、IT サービスとアプリケーションが企業のデータセンタとクラウド・データセンタにまたがる従来型および仮想のインフラストラクチャの両方を使用しています。その豊富なメリットに加えて、ハイブリッド･クラウドは特権パスワード管理に以下のようないくつかの新たな課題ももたらしています。

- 規模の拡大 / スケーリング — 運用上のニーズと仮想マシンのデプロイの容易さから、ますます多くのエンティティが特権アクセス（つまり特権パスワード）を必要としている
- 範囲の拡大 — 仮想化およびクラウド管理コンソールの権限の集中によって、新しいタイプの特権リソース / アカウントが増える
- ダイナミズムの増大 — 新しいサーバ / システムをオンデマンドで追加でき、一括した追加も可能（一度に 10 台、20 台またはそれ以上）
- アイデンティティの孤立した集団を作る可能性 — クラウド・サービスごとに異なるアイデンティティ・ストアとインフラストラクチャがあるため [2]

ハイブリッド・クラウドが提示する課題以外に、IT セキュリティ・マネージャは特権パスワード管理の問題の他の 2 つの側面も念頭において、候補のソリューションを評価する必要があります。第一に、マシン間またはアプリケーション間（A2A）のシナリオについて明示化することが必要です。このシナリオでは、1 つのシステムまたはアプリケーションが別のシステムまたはアプリケーションへのアクセスに使用するパスワードを、アクセス元のアプリケーションでハードコードするか、平文の構成ファイルで使用可能にします。第二の考慮点は見過ごされがちな問題ですが、大部分の組織は数千個の鍵（SSH の実装用など）を保持しており、これらは従来のフレーズ指向パスワードではありませんが、いまだに特権アカウントの認証クレデンシャルとして動作しており、そのため、関連リスクを低減するために管理と保護を必要とします。

その結果、現在のハイブリッド・クラウドの時代において、特権パスワード管理はかつてないほど重要で複雑なものになっています。

セクション 2 :

CA Technologies の特権アクセス管理ソリューション

CA Privileged Access Manager は、特権アクセス管理の包括的なソリューションです。そのため、ハイブリッド・クラウド環境における特権ユーザのアクセスを制御し、アクティビティを監視および記録することに加え、特権パスワード管理のための次世代ソリューションに求められる機能が組み込まれています。実際、パスワードの管理と保護はそれ自体重要であるものの、それはより大きな目的のための手段でもあることを認識することは、IT セキュリティ・チームにとって重要です。それは特に、リスクの高いリソースへのアクセスの実際の制御と管理という、より幅広く等しく重要なプロセスにおける最初の（相補的な）ステップです。この違いがわずかなものに思われるとしたら、それは主に、認証メカニズム（パスワードなど）やアクセス制御の機能の実装にいずれか一方のみが含まれることはまれで、ひとまとめに考えられることが多いことが原因です。

いずれにせよ、CA Privileged Access Manager に含まれる特権パスワード管理機能の設計の目的は、このソリューションの他の部分の目的と同じです。具体的に言えば CA の目標は、包括的な一連の制御と、包括的な一連のターゲットと使用事例のための機能を提供するだけでなく、クラウドの時代のデリバリ・オプションやプラクティス、アーキテクチャに沿った方法でそれを行うことです。

包括的な制御

特権パスワード管理ソリューションを評価する場合、第一に、機密管理クレデンシャルの作成、管理、使用のための従来のアプローチによって引き起こされるリスクを、セキュリティ・チームが克服するために役立つ包括的な一連の制御機能がソリューションに組み込まれているかどうかを確認することをお勧めします。調べるべき具体的な領域としては検出、ボールティング、ポリシーの適用、抽出、また、フル機能の特権アクセス管理の実装へのシームレスな移行をサポートする機能などがあります。

セクション 3 :

特権アクセス管理のための上位 12 の必須機能

#1. 検出の自動化 / 容易化

検出の自動化 / 容易化の手段がなければ、特権パスワードを管理下に置くプロセスは非常に手間がかかることがあります。また、エラーや不注意が多くなり、現在の高度な攻撃に対してコンピューティング環境が脆弱になる可能性があります。こうした理由から、CA Privileged Access Manager には既知のポートの関連付け、ディレクトリ情報、管理コンソール、API の活用を含め、デバイス、システム、アプリケーション、サービス、アカウントを検出するさまざまな方法が組み込まれています。 たとえば新規の仮想マシンが構築されると、CA Privileged Access Manager はサポート対象の仮想化およびクラウド管理ソリューションに利用可能な API を活用し、管理者にアラートを送信します。また、テキスト・ファイルからシステムのリストを容易に一括インポートでき、管理コンソールからアドホック・エントリを行えます。最後に、これはローカル TCP スタックをフックまたは shim するターゲットベースのエージェントを必要として混乱を生じさせる（リスクの可能性の高い）検出手法を回避するために CA が選択した、「意図的」なものであることを理解することも重要です。

#2. 安全なストレージ / ボールティング

暗号化されたボールトは一元的な制御ポイントを提供し、クレデンシャルの共有と侵害が容易になる安全性の低いストレージ方式（スプレッドシートなど）を排除するための鍵です。CA Privileged Access Manager のボールトはクレデンシャルの金庫であり、FIPS 140-2 のレベル 1 準拠ソリューションで、パスワードだけでなく、あらゆる種類のクレデンシャルを安全に保管するための AES 256 ビットの暗号化を活用しています。このソリューションのさらに魅力的な機能は以下のとおりです。

- SafeNet や Thales などの統合ハードウェア・セキュリティ・モジュール（HSM）を活用し、FIPS 140-2 レベル 2 またはレベル 3 の実装を処理するオプションが含まれます。これは特に知名度が高くリスクを回避したいクライアントや使用事例にとって重要です。たとえば、金融および銀行のシステムなど、クレデンシャルの暗号化に使用した鍵を、暗号化されたクレデンシャルとは分けて保管することが望ましい場合です。複数のデプロイ・オプションがサポートされ、オンボード PCI カードを備えた CA Privileged Access Manager のハードウェア・アプライアンス、ネットワーク添付 HSM アプライアンスにコールを行う CA Privileged Access Manager 仮想アプライアンス、AWS の「サービスとしての HSMCA」製品にコールを行ういずれかのタイプの CA Privileged Access Manager アプライアンスなどがあります。
- 実証済みのホワイトボックス暗号ルーチンが、システム上で（つまりメモリ内で）使用中に暗号鍵を保護します。このアプローチは、ハッカーが標準的な暗号 API とメモリを監視し、鍵のチャンキングまたは単純な難読化に基づく効果の薄い他のアプローチを乗り越えて、鍵を盗む / 全貌を知ることを防ぐことを目的としています。この技術を含めることは特に、アクセスしているシステムがクレデンシャルを「ボールトに保管」しなければならず、システムが侵害される可能性が高い A2A の使用事例（比較的無防備な場所に保管されているなど）にとって重要です。

#3. ポリシー適用の自動化

CA Privileged Access Manager はパスワードの生成、使用、変更を自動化するため、パスワードを再利用したり脆弱なパスワード（覚えやすいパスワード）を使用したりする傾向を排除できます。CA Privileged Access Manager を使用すれば、パスワードの複雑性を適用し、変更要求を実施するために柔軟なポリシーを設定できます。時間ベースで（毎日または毎週など）あるいは特定のイベントに応答して（使用するたび毎回など）パスワードを更新するなどして、使用を管理するようにできます（特定の時間枠でのみアクセスを許可する、あるいはパスワードのアクセスに 2 つまたは複数の認証を要求するなど）。これらのポリシーは、ターゲットのリソース・グループに階層的に適用でき、異なる要件や機能を異なるターゲットに適用できるだけでなく、グループに追加されたリソースは自動的にそのグループのポリシーを受け継ぐため、適用は実際に動的なものになります。CA Privileged Access Manager はまた、影響を受けたターゲット・リソースと直接インタラクトし、すべてのクレデンシャルの同期を維持します（一方に変更があった場合に、他方でも変更される）。

#4. 安全な抽出と提示 / 使用

特権クレデンシャルをボールトに保管しても、安全に抽出して使用できなければ意味がありません。このプロセスの最初のステップは、アプリケーションとスクリプトの場合、クレデンシャルにアクセスし使用しようとしているのが誰であっても、あるいは何であっても、正確な認証を行うことです。この観点から、CA Privileged Access Manager は既存のインフラストラクチャを Active Directory や LDAP 準拠ディレクトリ、RADIUS などの認証システムと統合して十分に活用します。また、以下についてもサポートしています。

- 二要素トークン（CA Advanced Authentication または RSA や SafeNet など）
- X.509/PKI 証明書
- 米国の連邦行政機関の HSPD-12 および OMB-11-11 指令へのコンプライアンスに必要な、PIV/CAC（Personal Identity Verification および Common Access Card）
- SAML
- 複合的な多要素の手法（パスワードと RSA トークンの組み合わせなど）

望ましい運用方法では、CA Privileged Access Manager は次に、アクセス元のエンティティ（ユーザまたはアプリケーション）に代わって、要求されたクレデンシャルをターゲット・システムに提示します。このアプローチは、いくつかの追加のセキュリティ上のメリットをもたらします。1 つは、単純なチェックイン / チェックアウト・ソリューションと比べて、クレデンシャルがアクセス元のエンティティによって見られることがなく、また、アクセス元のエンティティに配布されることもありません。これは漏えいの可能性を大幅に減らします。また、ターゲット・システムへの認証は完全に自動化され、ユーザがパスワードを処理したり覚えたりする必要がないため、パスワードの複雑性を大幅に上げるポリシーを実装できます。ターゲットへのアクセスはすべて CA Privileged Access Manager を介して行われるため、特権ユーザ・アクティビティの実行者を完全に特定でき、共有管理アカウントについても特定が可能です。

完全性のために、アクセス元のエンティティ、CA Privileged Access Manager、管理されたターゲットの間のネットワーク通信はすべて、SSL で暗号化されます。また、CA Privileged Access Manager は別の運用モードをサポートしているため、アクセス元のエンティティは必要なクレデンシャルを直接抽出し、自分でターゲット・システムへ送信することが可能です。

#5. フル機能の特権アクセス管理へのシームレスな移行

初めはパスワード管理のみに焦点を当てていた組織がフル機能の特権アクセス管理の実装に移行する必要性を認識した場合、CA Privileged Access Manager はそのために必要なものすべてを提供します。IT セキュリティ部門の準備が整えば自由に活用できる機能のうち、特に重要なものは以下のとおりです。

- きめ細かい役割ベースのアクセス制御と関連するワークフロー（追加の権限の要求 / 許可のため）
- ターゲット・リソースとの接続 / セッションの確立の自動化（RDP、SSH、Web および他の複数のアクセス・モード / オプションのサポート）
- 特権ユーザ・セッションのリアルタイムの監視と、許可 / 拒否されたアクティビティのポリシーベースの適用（特定のユーザがどのコマンドを使用できるかなど）
- Syslog ベースの SIEM 統合を含む、ログ記録
- DVR などでの完全なセッション・レコーディングで、関心のあるイベントへ直接「ジャンプ」する再生
- ユーザが許可を迂回し、アクセス可能なターゲットを活用して他の許可されないターゲットへのアクセスを獲得することがないようにする、迂回の防止

さらに、これらの追加の機能の実装は非常に容易です。CA Privileged Access Manager は特権パスワード管理とアクセス制御機能のすべてを、1 つの緊密に統合されたソリューションとしてお届けします。また、ソリューション全体で統合されたポリシー管理機能を提供します。これは実装と管理をさらに簡略化するアプローチです。

包括的な対象範囲

特権パスワード管理向けのソリューションを選択する際に、2 番目に重要な評価すべき領域は、そのソリューションが対応する範囲です。つまり、上述した包括的な一連の制御に関して、ソリューションが実際にどのような種類のアクセス元エンティティ、クレデンシャル、ターゲット・システムをサポートするか、ということです。

#6. 従来のターゲットの包括的な対象範囲

CA Privileged Access Manager には以下のようなあらゆる種類の IT インフラストラクチャ、ネットワーク・デバイス、システム、アプリケーションとすぐに統合できる、ターゲット・システムへの幅広いコネクタが含まれています。

- Windows® ドメイン、ローカル管理者、サービス・アカウント
- 一般的な Linux® と UNIX® のディストリビューション
- AS/400
- Cisco と Juniper のネットワーク・デバイス
- Telnet/SSH ベースのシステム
- SAP
- Remedy
- ODBC/JDBC データベース
- システムおよびアプリケーション・サーバ

また、CA Privileged Access Manager は拡張可能なソリューションで、柔軟なカスタマイズ機能を提供するため、組織は専有の自社開発システムに容易にサポートを拡張できます。

#7. 仮想化およびクラウド管理コンソールのサポート

CA Privileged Access Manager のクレデンシャルの管理および保護の革新的な対応範囲は、従来のターゲットにとどまりません。VMware vSphere、VMware NSX、Amazon Web Services、Microsoft® Online Services など、一般に普及している仮想化およびクラウド・ソリューションにも拡張できます。また、これらのソリューションに適用される機能は、関連づけられた仮想マシンやアプリケーション、サービスの個別のインスタンスに限定されません。対象範囲は対応する管理コンソールにも拡張されます。管理コンソールが扱える権限から、それ自体を特権リソースとしてみなす必要があります。

#8. マシン間の認証のサポート

前述のように、特権クレデンシャルのユーザは人間だけではありません。ほとんどの組織にとっては、膨大な数のアプリケーションやシステムも、他のアプリケーションやデータベースなど機密性の高いリソースへのアクセスが許可されています。これは通常、アクセス元のアプリケーションのコードに関連するクレデンシャルが埋め込まれていたり、ランタイムに構成ファイルから使用できるようにすることで可能になっています。しかしこれらの方法はどちらも特に安全性や管理性が高いわけではありません。CA Privileged Access Manager は、開発者が軽量の CA Privileged Access Manager クライアントをアプリケーションに注入できるようにすることで、こうした A2A の使用事例に対応しています。このアプローチは「特権アプリケーション」が CA Privileged Access Manager に登録し、必要なパスワードを動的に抽出し、その後ローカル・システムのメモリでそれを保護するために必要なすべてを提供します。さらに CA Privileged Access Manager が要求されたクレデンシャルをリリースする前に、複数のメカニズムを使用して特権アプリケーションを認証でき、整合性を検証します。

A2A のシナリオに CA Privileged Access Manager を活用することで、組織は無防備な / 安全性の低い A2A クレデンシャルを効果的に排除でき、A2A クレデンシャルの管理とポリシー適用を自動化し、関連する監査およびコンプライアンス・アクティビティを簡略化できます。

#9. 重要な管理のサポート

暗号化作業をサポートするために、多くの種類の鍵もアイデンティティを確認するためのトークンとして使用されています。こうした鍵は従来の意味でのパスワードではありませんが、パスワードのように機能し、複製、共有、意図しない開示、監査されないバックドアなど、いまだに同様の脅威やリスク、問題にさらされる可能性があります。こうした鍵は通常、ユーザを関連する複雑性から遮断する目的でソリューションに埋め込まれていたりトランスペアレントに使用されるため、孤立したり、時間の経過とともに増えてしまうことがよくあります。したがって、パスワードの管理と保護に使用されるのと同じ制御の多くを、これらの代替クレデンシャルにも適用することは理にかなっています。実際、関連する脅威を阻止するために推奨されるベストプラクティスには以下があります。

- 許可された鍵を保護された領域に移動する
- すべての鍵を定期的に更新する（鍵が漏えいされた場合にアクセスの最終的な終了を確実に行えるようにするため）
- 許可された鍵に対するソースの制限を実施する [3]
- 許可された鍵に対するコマンドの制限を実施する

その結果、CA Privileged Access Manager は、AWS リソースや管理コンソールへのアクセスに使用される SSH 鍵や PEM エンコードされた鍵など、代替クレデンシャルのタイプについて把握する制御その他の機能を確保できます。つまり CA Privileged Access Manager を使用すれば、こうしたクレデンシャルを（1）ボールトに保管でき、（2）構成ポリシーによって更新し制御でき、（3）盗用や開示の可能性を最低限に抑える方法で抽出し使用できます。

クラウド時代のデリバリ

ハイブリッド･クラウドの時代には、特権パスワード管理ソリューションの成功を左右するもう 1 つの重要な要因は、ソリューションが物理的にのみでなく、クラウド・ネットワークのニーズと機能に合わせてうまく「適合」できるかどうかです。

#10. オンプレミス、仮想マシン、クラウドベースのデリバリ・オプション

CA Privileged Access Manager は 3 つの利便性の高いデプロイ・オプションをサポートし、組織が以下のような複雑なハイブリッド・クラウド・アーキテクチャに対応できるようにします。

- 強化された物理アプライアンス — 企業のデータセンタにある従来のラックマウント向けの多数のモデルで使用可能
- Amazon Machine Instance（AMI）— Amazon EC2 インフラストラクチャでのデプロイ向けに事前構成済み
- OVF 準拠仮想アプライアンス — 既製品で VMware 環境のデプロイ向けに事前構成済み

使用するデプロイ・オプションに関係なく、組織はハイブリッド・クラウド・インフラストラクチャ全体の管理を可能にするソリューションを入手できます。

#11. クラウドに適合したアーキテクチャとアプローチ

CA Privileged Access Manager はハイブリッド・クラウド環境に最適な多数の機能を組み込むことを目的として設計されています。以下のような 3 つの例があります。

- 自動検出および保護 — ハイブリッド・クラウド環境で、オペレータは 1 つのコマンドを使用して必要な数のシステムを構築（または廃止）できます。CA Privileged Access Manager は適用可能な API を活用して自動的に仮想およびクラウド･リソースを検出し、適切なクレデンシャルとアクセス管理ポリシーをプロビジョニング（プロビジョニング解除）することで、この状況を明示化します。
- アイデンティティの孤立した集団の回避（アイデンティティ連携など）— CA Privileged Access Manager がアイデンティ情報の孤立した集団を排除する方法の 1 つは、組織がすでに持っているアイデンティティ・インフラストラクチャが何であれ、それを十分に活用することです。もう 1 つの方法は、AWS 実装に固有の方法で、短期のユーザをサポートすることです。このアプローチでは、組織が AWS アイデンティティ / アクセス管理サブシステムで個別のアイデンティティ情報を管理する必要がありません。
- 自動化の実施 — 包括的な API によって、すべての CA Privileged Access Manager の機能へのプログラム的なアクセスと自動化を可能にします（外部の管理とオーケストレーション・システムによって）。

#12. クラウドに対応したスケーラビリティと信頼性

特権クレデンシャル管理は組織の IT インフラストラクチャにとって重要な要素です。完全に自動化された方法で動作する A2A の使用事例をサポートするよう実装を拡張する場合、これは二重の意味で当てはまります。この目的のために、CA Privileged Access Manager には、大規模で要求の厳しい環境の高い可用性とスケーラビリティの要件にも対応できる、ネイティブのクラスタリングおよびロード・ディストリビューション機能が含まれています。一般的な代替製品と比較すると、CA Privileged Access Manager では個別の外部のロード・バランサに投資する必要がなく、アクティブ / パッシブ・アプローチによくある性能の遅延もなく、追加の「オプション」機能のライセンスを付与する必要もありません。必要であれば、運用上レイテンシの観点から受け入れ可能である場合、CA Privileged Access Manager のクラスタは地理的に分散したデータセンタとクラウド環境に冗長性を構成することも可能です。

CA Privileged Access Manager は、ハイブリッド・エンタープライズ・インフラストラクチャのセキュリティ・リスク軽減と運用効率の向上の促進を目的とした、特権クレデンシャル管理の次世代ソリューションを提供します。

セクション 4 :

まとめ : クラウドの時代の特権クレデンシャル管理の克服

特権クレデンシャルの管理と保護は、リスクを減らし、関連する規制要件のコンプライアンスを確保するために不可欠です。また、ハイブリッド・クラウド環境が導入する管理コンソールには以前はなかった権限が備わり、数回のマウス・クリックで数百ものターゲット・システムを追加 / 削除できる機能があるため、特権クレデンシャルの管理と保護の複雑性と重要性はさらに増大しています。

情報セキュリティ戦略におけるこのきわめて重要な領域への対応を検討している組織は、制御の深さ、対応範囲、提供するクラウドとの適合の程度などの観点から、採用候補のソリューションを評価しなければなりません。前述のとおり、CA Privileged Access Manager はこれら 3 つの側面のすべてに対応でき、現在の組織がまさに必要としているものを提供します。それはつまり、従来型、仮想、ハイブリッドのインフラストラクチャを同じようにサポートすることで、IT リスクの軽減、運用効率の向上、投資の保護を促進するよう設計された特権クレデンシャル管理の次世代のソリューションです。

ca.com/jp/でCA Technologiesにアクセスしてください。

CA Technologies（NASDAQ:CA）は、企業の変革を推進するソフトウェアを作成し、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。

1 2015 年、Verizon Data Breach Investigations Report

2 「**New Platforms, New Requirements.Privileged Identity Management for the Hybrid Cloud**」、CA White Paper、2013 年 3 月

3 「**Managing SSH Keys for Automated Access - Current Recommended Practice**」、IETF ドラフト、2013 年 4 月