WHITE PAPER | 2017 年 6 月

特権アクセス管理総所有コスト計算のロードマップ

PAM 実装アプローチの隠れたコストと利益の解明

ca technologies

目次

セクション 1

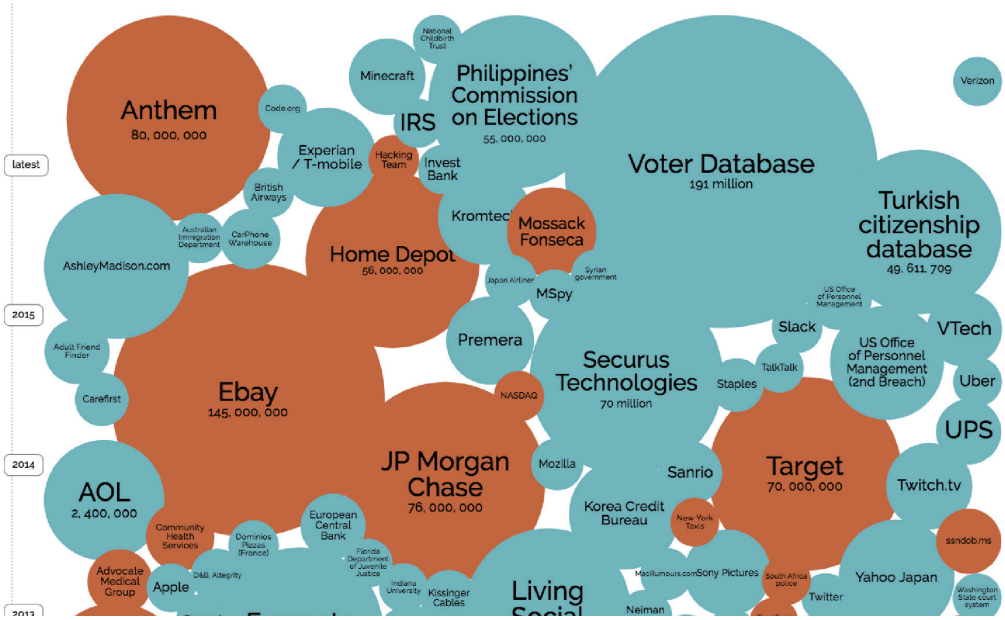
はじめに

乗っ取りや悪用、単なる誤用であっても、データ侵害のほとんどに特権ユーザ・アカウントが関連しています。セキュリティ・チームは、高位の特権を持つ不正ユーザや、疲れやストレス、不注意などからミスをする特権ユーザが引き起こす損害を回避するために、ますます包括的特権アクセス管理（PAM）ソリューションを評価するようになっています。ビジネスに対するリスクを削減するように求めるエグゼクティブや監査チームからの圧力により、取り組みが強化されますが、包括的 PAM ソリューションは実装や戦略によっては見えないコストがかかる場合があります。パスワード・ボールト、セッションの管理と監視、ユーザ動作分析、脅威情報など複数の機能を備えた PAM ソリューションを実装する場合、その方法によってはコストや利益に大きく影響する場合があります。このレポートでは、PAM の実装により時間の経過とともに発生する直接的、間接的、および目に見えないコストを明らかにするための青写真を示します。

セクション 2

大規模な侵害につながる特権アカウント

最近、大規模なセキュリティ侵害が頻繁にニュースになっています。専門家によればその 80 ～ 100 パーセントは特権アカウントが利用されたものです。IT 管理者、アプリケーション開発者、営業管理職、パートナー、サプライヤ、経営幹部などのアカウントが利用される攻撃が急増しています。いったんシステム内に入った攻撃者は、水平方向にも垂直方向にも移動でき、機密情報にアクセスしたり、将来損害を引き起こすマルウェアをインストールすることができます。しかし、特権ユーザが機密領域にアクセスした場合に、そのアクセスは日常的な普通の活動である可能性もあるため、IT 管理者がそれに問題があるかどうかを判断するのは困難です。



結論：どのような組織でも、その規模や所在地に関係なく、特権ユーザの役割がセキュリティ・チェーンの最も弱いリンクになる可能性があります。これに適切に対処することで、この先の優れたコスト・パフォーマンスを実現できます。

セクション 3

PAM による特権アカウント侵害からの保護

情報セキュリティには多くの面があり、特権アクセス管理はその 1 つでしかありません。一般に、組織が PAM を真剣に検討するのには、次のいずれかの理由があります。

- 深刻な問題に直面している（侵害を受けていたり、コンプライアンス要件を遵守できていないなど）
- ベスト・プラクティスを実装する準備ができている

いずれの理由にしても、PAM ソリューションの実装について根拠のない思い込みをするのは珍しいことではありません。短期的な見地から、限られた機能のセットから始めて、実装の対象範囲と規模を徐々に増大させていけると想定することもあるでしょう。これは、他の一部のセキュリティ手段では妥当な方法ですが、経験上、PAM の場合は技術的にも経済的にも実用的ではありません。実際、これは長期的見地をとることが非常に重要な分野です。デバイス、エンドポイント、ユーザ、およびアカウントを保護し、コンプライアンスの問題と会社のロードマップを考慮に入れる必要があるからです。これらの要素はすべて、総所有コストに影響します。

デバイス

セキュリティ担当者の任務は、もはや従来のエンドポイントを保護することだけではありません。今日、保護の対象は大きく広がって、仮想環境、コンテナ、クラウドベースのシステムまで及びます。ハイブリッド IT インフラストラクチャ、管理コンソール、大量のリソース、そして絶え間ない変更により、利用できる攻撃対象が拡大する可能性があります。　適切な保護には、環境全体を最初から組み込んだ防御が必要です。それによって脅威に即した幅広く深い保護を提供できます。PAM の実装を計画するときには、このような将来のニーズを考慮に入れる必要があります。

ユーザ

特権ユーザのクレデンシャルを取得する方法として現在一般的なのは、フィッシングとソーシャル・エンジニアリングです。外部の攻撃者からの脅威（そしてますます増えている内部関係者からの脅威）に対処するには、完全なコンテキスト情報が必要です。特権ユーザの異常な動作を特定するには、彼らの通常の動作を理解する必要があります。特権ユーザの概念は、クラウド、ハイブリッド、およびアジャイル開発手法の導入とともに変化しつつあります。たとえば、事業部門の所有者は、クラウドベースの CRM ソリューションに対する管理特権を割り当てられていると考えられます。状況をさらに複雑にする要因として、ユーザの動作は時間とともに変化し、標的型攻撃も変化するため、アカウントが悪用されているかどうか断言することは困難です。特権ユーザ管理ソリューションは、潜在的な侵害を特定できるように、継続的に研究と改善を行っていく必要があります。

コンプライアンス

どのような規模の組織でも、コンプライアンスを遵守し続けること（そしてそれを証明すること）が常に要求されますが、規制もその対象範囲も大幅に変更されるため、「規制疲れ」を招くことがあります。

PAM テクノロジは、サイバー・セキュリティを確保するために使用されるコントロールとプロセスに対する規制をサポートする必要があります。これには、構成の設定および個人情報へのアクセスの文書化、ITIL® の施行、そして HIPAA（1996 年に制定された医療保険の相互運用性と説明責任に関する法律）、PCI DSS（PCI データ・セキュリティ・スタンダード）および他の規制に対する明確な監査証跡の提供が含まれることになるでしょう。コンプライアンスの証明は、後回しにせずに最初から組み込む必要があります。

セクション 4

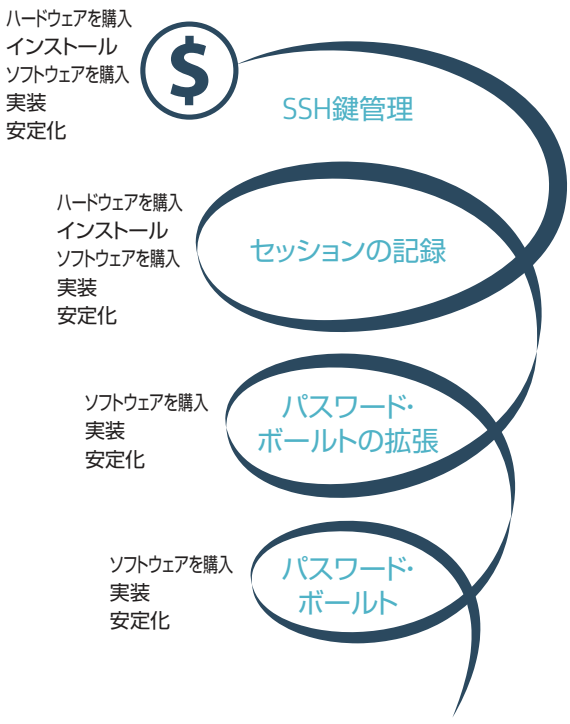
TCO に大きな影響を及ぼす PAM 実装戦略

選択する PAM ソリューションの実装方法によって、総所有コストに大きな影響を及ぼします。PAM を実装するための 2 つの方法を理解することが重要です。

第 1 の方法（「包括的」な方法）は、主要な要件のロードマップを策定し、すべての機能（将来の要件も含めて）を提供する製品を調達しておき、機能の規模と対象範囲を段階的に広げていく方法です。たとえば、パスワード・ボールト、セッション記録、および SSH（Secure Shell）鍵管理機能が必要であれば、これらをすべて備えた製品を購入し、必要に応じて各機能を有効にすることができます。すべての機能が統合されているので、安定するまでに長い期間は必要ありません。

第 2 の方法（「段階的」な方法）は、必要に応じて製品買い足して行く方法です。始めにロードマップを策定するのは同じです。たとえば、ロードマップに第 1 の方法と同じ 3 つの機能が含まれているとすれば、まずパスワード・ボールトを購入して実装し、数か月かけて安定させます。その後、そのベンダーからセッション記録機能（および必要な追加ハードウェア）を購入して実装し、6 か月かけて安定させます。さらに、SSH 鍵管理についても同じ手順を繰り返します。

選択した方法によって、TCO と価値実現までの時間の両方に影響する可能性があります。情報収集機能をベースとした包括的な統合 PAM ソリューションを実装すれば、迅速な価値実現と低い TCO の両方を実現できます。コストは最初からわかっているので予測可能です。これとは対照的に、段階的な実装では最初のデプロイは単純です。たとえば最初は少数のアカウント用のパスワード・ボールトのみを実装し、ボールト内のアカウント数の増加と、その後のセッション記録機能の追加に伴って規模を拡大していきます。しかし、追加するモジュールによってコストが異なるため、インフラストラクチャのコストを予測できなくなります。さらに、顧客が特定のベンダーに縛られがちで、これは顧客にとって最適ではありません。TCO の計算には、段階的実装の規模と対象範囲の拡大から生じるコスト、時間、およびリスクへの露出を計算に入れる必要があります。このコストには、目に見えるコスト（ライセンス、インフラストラクチャなどのコスト）と、目に見えないコストの両方が含まれます。価値実現までの時間、リスクにさらされる時間の長期化、統合と保守にかかるコストなどは目に見えないコストです。たとえば、パスワード・ボールト用にエンドポイントを追加するためのスクリプト作成と保守は、SSH 鍵管理に必要なものとは大きく異なる可能性があります。



考慮すべき点と評価すべき機能をより的確に把握するには、包括的 PAM ソリューションの構成要素と、質的および量的利益と経済的コストのバランスの決定方法を理解することが有用です。

セクション 5

包括的 PAM ソリューションの構成要素

包括的 PAM ソリューションには中核的なコンポーネントがいくつかあります。すべてのリソースについて特権アクセスを制御する機能、特権クレデンシャルを安全に保存する機能、活動を監視、記録する機能、ハイブリッド・クラウド・コンソールと管理 API を保護する機能、ユーザの動作を分析して侵害の可能性がある異常を検出する機能などです。PAM の評価に際して念頭に置く必要があることを以下に示します。

パスワード・ボールト:堅牢な暗号化されたパスワード・ボールト（金庫）。クレデンシャル管理パスワードや、他のクレデンシャルおよびトークンをポリシーごとに設定可能な間隔で変更することで安全に保存します。これにより、管理アカウント、共有アカウント、およびサービス・アカウントを保護できるだけでなく、アプリケーション間のアカウントやハイブリッド・クラウド環境も保護できます。ただし、パスワード・ボールトだけでは不十分です。

セッション監視 : この重要なコンポーネントは、段階的デプロイの初期段階では欠如していることがよくあります。特権ユーザ・セッションを記録、分析、監視するリモート・セッションを自動的に開始する機能があれば、リアルタイムでの監視とセッション後の分析が可能になります。この機能は、問題が起きてから追加したのでは間に合いません。特権ユーザがポリシーに違反したり異常な動作を見せた場合、6 か月後ではなく今すぐ監視を始める必要があります。

ハイブリッド環境 : 包括的 PAM ソリューションは、従来の物理データセンタ環境に加えて、クラウド・リソース、仮想マシン、およびハイパーバイザへの特権アクセスも制御できます。新しいリソースを数分で環境に追加できるため、自動検出が鍵となります。

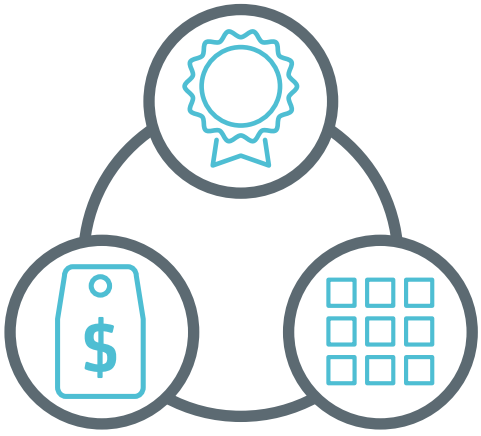
ユーザ動作分析 : 包括的 PAM ソリューションは、特権ユーザの通常の動作から異常を識別して、異常が見つかったときに追加の保護メカニズムをトリガします。ドメイン固有のコンテキスト・データを収集して高度な分析を実行し、以前の動作パターンに基づいてリスク・モデルを構築します。通常と異なる動作を検出した場合は、追 加 認 証（Radius、TACACS+、CA Advanced Authentication など）またはセッション記録を自動的にトリガできます。

包括的 PAM ソリューションは、これらの機能を備えているだけでなく、すばやく実装でき、導入後すぐに使用できる検出機能と洞察を提供します。特別なスキルがほとんどなくても、このソリューションからすぐに利益を引き出せます。管理者はインシデントを簡単に調査して、特権アカウントがどのように使用されているかを理解できる必要があります。

セクション 6

包括的 PAM が組織のビジネスに与える影響の評価

上記の要件から考えて、コストと利益の判定に影響する要素は何でしょうか。高レベルでは、経済的コスト、質的利益、量的利益という 3 の要素を評価する必要があります。量的利益の判定は比較的簡単で、業界の平均や組織の特定のプラクティスに基づいて行います。質的利益の測定はそれより少し難しくなりますが、検出までの時間、使いやすさなどの問題が影響します。次のセクションでは、これらの要素それぞれにアプローチする方法を説明していきます。



経済的コスト計算の要素

経済的コストの計算は、通常は単純な作業で、以下の項目を含みます。

- 製品ライセンスのコスト（ワンタイム、サブスクリプション）
- 製品の保守コスト（第 2 段階以降、内部サポートのコスト）
- 製品のデプロイ・コスト（専門サービス、デプロイ、設定）
- トレーニング・コスト（内部顧客のトレーニング、エンドユーザのトレーニング）

経済的コストを計算する際、いくつかの問題を考慮する必要があります。1 つ目は、包括的ソリューション実装のコストと、段階的実装のコストの比較です。包括的ソリューションの場合は、初期コスト（ライセンス、デプロイ、トレーニングを含む）と、その後の保守コストがかかります。しかし、段階的実装の場合は、統合のコストも計算に含める必要があります。このコストは、統合するシステムの数とサイズに直接関係します。PAM ソリューションを段階的に購入していく場合は、上記の基本コストの他に、個々の購入に応じて調達、トレーニング、およびデプロイのコストがかかります。段階的実装を行う場合は、運用コスト（OPEX）も計算に入れる必要があります。追加機能では専用ハードウェアを必要とすることが多く、そのための予算確保、調達、セットアップ、および保守も必要です。段階的アプローチを選択した場合、コスト計算ではリソース、時間、およびスキルも考慮する必要があります。予想できない要素が多く、実際、予算策定プロセスにとっては難しい問題です。

質的な経済的利益の判定に影響する要素

質的な経済的利益は評価が難しいこともありますが、包括的ソリューションを実装するか段階的実装を行うかを決定するときには大いに役立ちます。まず、段階的実装について考えてみましょう。少数のアカウント用のパスワード・ボールトから始めて、徐々に特権アカウントを追加していき、後日セッション記録を導入し、システム全体ができあがってからユーザ動作分析の導入を検討します。

長所：

- 初期費用を節約できる

短所：

- 価値実現までに時間がかかる：リスクの効果的な低減に十分な早さで可視性を実現することは不可能です。
- 侵害発生時のリスクが大幅に増大：セッション記録などの機能を実装するときに、必要なハードウェアを入手できるまで数週間から数か月待つ必要があります。
- 長期間にわたりリスクにさらされる範囲が増える
- 実装を拡張するためにスクリプトやコードの作成が必要になる場合がある
- ハードウェア、バックアップ、冗長性確保のための追加コスト：長期的コストが高くなる傾向があります。
- ベンダ･ロックイン: 新しいモジュールの導入が検討されるたびに、調達プロセスが開始します。以前実装したモジュールのクロックがリセットされる可能性があり、その場合は最初の計画よりその製品に関わる時間が長くなります。

フル機能を備えた包括的な統合ソリューションは一度で実装できますが、その一方で、必要な機能をすべて備えたソリューションを最初に選択する必要があります。必要に応じて機能を有効にしていくこともできますが、すべての機能がいつでも使用可能な状態です。この種の実装では、特にアプライアンスという形で提供される場合、導入後すぐにリスク低減が実現され、特別なスキルがなくともすぐに利益を得られます。これにより、侵害を防ぎながらワークロードを軽減できます。

長所：

- 短時間でのデプロイと迅速な価値実現
- 侵害の発生が疑われる場合の即座の保護：セッション記録が必要となれば、ただその機能を有効にするだけで済みます。
- 分析などの追加機能がすぐに利用できるため、環境全体の制御と可視化を実現できる
- 攻撃対象が大幅に削減される
- 総コストの低減：独自のコードやスクリプトを作成する必要がなく、ハードウェアを追加する必要もありません。

短所：

- 初期費用が高額になる可能性がある

一部の技術的要因も、質的な経済的利益に影響することがあります。PAM ソリューションがユーザ動作分析を活用し、脅威情報と緊密に統合されれば、異常な活動を検出してすぐにアクションを実行する能力が大幅に強化されます。複数のサイトがクラスタ化されている場合は、これによって可用性と応答時間が向上します。ソリューションが仮想または物理アプライアンスとして提供される場合は、実装にかかる時間がソフトウェアベースのソリューションよりはるかに短くなります。最後に、保守コストを計算に入れることが重要です。各自が専用のハードウェアを必要とするソフトウェア製品のスイートよりも、アプライアンスの方が保守コストははるかに安くなります。

つまり、上記すべての質的要素が、総所有コストの低減と価値実現の迅速化に影響する可能性があります。

量的な経済的利益の判定に影響する要素

量的な経済的利益を評価する場合は、コストの削減、生産性の向上、収益の保護という 3 つの主要な要素を考慮します。

コストの削減

コストの削減には、インフラストラクチャのコスト、侵害に関連したコスト、監査人とコンプライアンスの費用、および予定外のシステム停止のコストを回避することが含まれます。過小評価できないもう 1 つの要素は、デプロイ、保守、およびサポートにかかるコストの削減です。

インフラストラクチャのコストは、段階的なソリューションやソフトウェアのみのソリューションではなく、アプライアンスベースの包括的 PAM を選択することで回避できます。これは、既存または競合する PAM ソリューションに必要なサーバーとアプライアンスの数、サーバーあたりのコスト、必要なロード・バランサの数とその 1 台あたりのコスト、およびアプライアンスベースのソリューションによって回避できるはずのインフラストラクチャ・コストの比率を見積もって計算されます。

侵害に関連するコストには、収益への影響、顧客への通知のコスト、PR とインシデント対応のコスト、法的費用が含まれます。これらのコストを計算するには、侵害が発生する可能性（現在の見積は 2 年間で 22%）、漏えいの可能性があるレコードの量とレコードあたりのコスト、および修復のコストと、包括的 PAM によって回避できるはずのこれらのコストの比率を見積もる必要があります。80 パーセント以上の侵害がクレデンシャルの悪用によって引き起こされているため、この利益は大きなものになります。

外部の監査人やコンプライアンスのコストは、包括的 PAM の使用により削減できます。可能なコスト削減を計算するには、コンプライアンス問題の年間件数、コンプライアンス違反の年間コスト、報告可能な問題を修復するための外部の監査人のコスト、包括的 PAM を使用していれば回避できたはずの監査所見料金、修復、およびコンプライアンスの罰金の比率を見積もる必要があります。

もう 1 つの経済的利益は、予定外のシステム停止が低減することです。これが起きると従業員の不満が募って生産性が落ち、顧客離れが増えることもあり得ます。この計算では、特権ユーザ・アカウントの悪用に起因する潜在的な事業中断の年間回数、システム停止 1 回あたりの平均ダウンタイム、1 分あたりのコスト、および可用性向上の影響を見積もります。

PAM ソリューションの段階的実装における主要な問題の 1 つは、各モジュールを購入し、実装し、安定していくにしたがって、保守とデプロイのコストが大幅に増加することです。特定のスクリプト作成のスキルが必要ですが、ソリューションの管理、保守、およびデプロイのためにフルタイムの従業員を喜んで雇う顧客がどれほどあるでしょうか。包括的ソリューションを購入し、必要に応じて機能を実装していけば、このコストは回避できます。

生産性の向上

生産性が 2 つの形で向上します。IT システム管理者の労働コストの低減と、実装およびアプリケーション運用のコストの低減です。

包括的 PAM ソリューションを採用すると、検出、ポリシー施行、パスワードの取得または再生成に費やされるシステム管理者の時間が減って、ビジネスを前進させる革新的ソリューションの実装に使える時間が増えます。IT システム管理者の労働コストの削減を計算するには、特権アクセス・クレデンシャルを持つリソースおよびデバイスの数と、リソース / デバイス / アプリケーションあたりのアカウント数を考慮します。その後、IT 管理者が特権アクセスを提供または更新するために必要な時間（分数）と、1 時間あたりの平均総コスト、包括的 PAM の使用によって予想される特権アクセス・クレデンシャル更新の削減時間を明らかにします。

実装コストと運用コストは、アプライアンスベースの包括的 PAM を使用すると大幅に削減されます。これらの節約を計算するには、既存または競合ソリューションの実装、ホスティング、および管理に必要な IT システム管理者の数と、その 1 時間あたりおよび 1 年あたりの平均総コストを考慮した後、アプライアンスベースの包括的 PAM を選択した場合に予測できるコスト削減率を適用します。

収益の保護

包括的 PAM は、データ侵害による最も深刻な経済的影響の緩和に大きな効果を発揮します。この経済的利益を計算するには、システムまたはデータが侵害されたために会社のブランドが傷ついた場合の収益に対する影響と、クレデンシャル侵害のリスク低減によって保護される収益の比率を見積もります。Ponemon Institute の最近のレポートによると、2016 年に調査した米国の企業では、ブランドの評判と信用の低下が収益に与えた経済的影響が年間で 397 万ドルに上ったとされています。したがって、PAM は大きな経済的影響を及ぼす可能性があります。

セクション 7 :

すべてを統合

包括的 PAM の必要性は明らかであり、総所有コストを計算する方法には考慮すべきさまざまな要素が含まれています。コストは、包括的 PAM を実装して必要に応じて機能を有効にしていくか、それとも専門知識が必要で後日追加コストが発生する段階的実装を選択するかによって異なります。包括的アプローチのコストと利益を頭に置いてください。

- コストは予測可能で予算を立てやすく、段階的アプローチの場合のような追加コスト（調達、ライセンス、トレーニング、デプロイ、リソース、追加のインフラストラクチャ）はありません。
- 質的利益は多大です。迅速な実装と価値実現、侵害発生時の即時保護、攻撃対象の減少、TCO の低減を実現できます。
- 量的利益も同様にすばらしいものです。インフラストラクチャ・コストの回避、侵害に関連するコストと監査 / コンプライアンスに関連するコストの削減、予定外のシステム停止の回避、デプロイ / 保守 / サポートのコスト削減を実現できます。

これらの計算の結果は、状況や組織の意向によって当然異なりますが、PAM の実装では包括的実装アプローチの方が段階的実装アプローチよりはるかに好ましい TCO をもたらすことは確かです。

セクション 8 :

まとめ : TCO の長期的見通し

攻撃の対象が保護されないまま放置されて拡大し続けると、組織のリスクが増大します。包括的 PAM ソリューションは、攻撃対象を低減し、驚くべき早さで価値を実現できます。それこそが、組織が侵害の危機に瀕したときに真を問われる問題です。包括的 PAM ソリューションは 1 日目からすべての機能を提供できますが、最初は一部の機能だけを有効にすることもできます。侵害の疑いが検出された場合は、ソリューションの力を全開して即座に活用できます。ここで説明したすべての計算により、包括的なアプライアンスベースの PAM ソリューションが、経済的にもビジネス面でも生産性の面でも長期的に有意義であることは明らかです。

CAの特権アクセス管理ソリューションが組織に与えるメリットの詳細については、**ca.com/jp/pam**をご覧ください。

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 Thomson Reuters、「Cost of Compliance 2016」、https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html

2 Ponemon Institute、「2016 Cost of Data Breach Study: Global Analysis」、2016 年 6 月、https://securityintelligence.com/media/2016-cost-data-breach-study/

3 同上

CS200-282765_0617