WHITE PAPER • 2017 年 5 月

PCI DSS（Payment Card Industry Data Security Standard）とCAの特権アクセス管理

目次

はじめに

PCI DSS（PAYMENT CARD INDUSTRY DATA SECURITY STANDARD）は、クレジット・カード所有者のデータに関する制御を強化し、クレジット・カード詐欺を減らすことを目的として、2004 年に登場しました。年に 1 度の検証と長期的な検証が求められており、定期的に新しい改定が行われ進化してきました。最新のバージョン 3.2 は、2016 年 4 月に発表されました。PCI DSS と PA-DSS（Payment Application Data Security Standard）は、2018 年 1 月末までは実装すべきベスト・プラクティスとみなされますが、2018 年 2 月 1 日以降は必要条件とみなされます。

セクション 1

PCI DSS 3.2 の主な要件

PCI DSS 3.2 の主な要件は以下のとおりです。

PCI データ・セキュリティ基準 - 高度な概要

安全なネットワークおよびシステムの構築と維持	1. カード所有者データを保護するためのファイアウォール構成を設置し、維持すること 2. システム・パスワードやその他のセキュリティ・パラメータに、ベンダから提供されたデフォルト値を使用しないこと
カード所有者データの保護	3. 保存されたカード所有者データを保護すること 4. 公開された公共ネットワーク経由でカード所有者データを伝送する場合、暗号化すること
脆弱性管理プログラムの維持	5. すべてのシステムをマルウェアから保護し、アンチウイルス・ソフトウェアまたはプログラムを定期的に更新すること 6. 安全性の高いシステムおよびアプリケーションを開発し、維持すること
強力なアクセス制御手段の実装	7. 業務上の知る必要性に応じてカード所有者データへのアクセスを制限すること 8. システム・コンポーネントへのアクセスを識別し認証すること 9. カード所有者データへの物理アクセスを制限すること
ネットワークの定期的な監視およびテスト	10. ネットワーク・リソースおよびカード所有者データに対するすべてのアクセスを追跡および監視すること 11. セキュリティ・システムおよびプロセスを定期的にテストすること
情報セキュリティ・ポリシーの維持	12. 全社員の情報セキュリティに対応するポリシーを保持すること

これらの要件は、セキュリティの広範な測定基準に高度なレベルで対応しています。ただし本書では、特権ユーザの管理に関連する要件について見ていきます。

特権アクセス管理の重要性

よく言われることですが、鎖の強さは最も弱い輪によって決まります。多くの場合、最も弱い輪は一見しただけではわかりません。特権アイデンティティについても同じで、漏えいが起きたりコンプライアンス監査で不合格になったりするなど、問題が表に出るまで気づかない例はよくあります。以下は特権アクセスの重要な特徴です。

至るところに存在：どの企業にも、通常より高いレベルで特定のアプリケーションへのアクセス権を付与されたユーザがいます。わかりやすいのは管理権限を持つユーザです。しかしソフトウェア開発の変化とデジタル・トランスフォーメーションによって、特権アクセスを持つアイデンティティの性質は大きく変化しつつあります。企業がインフラストラクチャ、プラットフォーム、アプリケーションに関連して仮想環境やクラウドへ移行していることで、部門内のユーザはさらに多くの特権を担うようになっています。また、アジャイル開発の採用が、アプリケーション・ツー・アプリケーション（A2A）・インタラクションの増加につながっています。こうした傾向は数多くあり、拡大する一方です。

影響が大きい：当然のことですが、アプリケーションやインフラストラクチャへの特権アクセスには大きな責任が伴います。特権を持つユーザやアイデンティティは機密性の高いデータにアクセスできるため、不正なアクセスや偶発的なミスが起きれば、多大な損害や企業イメージの低下につながりかねません。先に挙げた例のいずれでも、不注意か意図的かによらずユーザがミッションクリティカルなサーバからデータを削除したり、何の監視もなく本番サーバの設定を変更したりすれば、実際にビジネス・インパクトが生じ、懸念材料となります。

標的にされやすい：特権ユーザや特権アイデンティティが持つアクセス権が非常に重要であるということは、つまり、攻撃しようとする側から狙われやすいということです。特権ユーザや特権アイデンティティは攻撃者の標的となることが多いため、企業が適切なセキュリティの状態を維持しなければ、攻撃の影響を受ける可能性は非常に高くなります。

上記のような理由から、特権ユーザ・アクセスを管理することは非常に重要です。また業種によっては、直接または間接的に規制によって特権ユーザ・アクセスの管理が義務付けられている場合もあります。PCI DSS もこのような対応を義務付けています。バージョン 3.2 の変更箇所では、特権アクセスの管理の仕方について直接間接に何度も触れられています。本書ではこれ以降、PCI DSS 3.2 の具体的な要件について、特権アクセスに該当する部分を見ていきます。

特権アクセス管理と PCI DSS 3.2

バージョン 3.2 では変化するビジネスの現状を反映すべく、PCI DSS 標準の複数のセクションが強化されました。これらの変更点の一部は特権アクセスの管理方法に関するものです。以下の表に、PCI DSS で定義されている要件と、その要件が特権アクセス管理にどう関係するかについて詳細を示します。

要件	バージョン 3.2 における変更点	特権アクセス管理へのインパクト
要件 1： カード所有者データを保護するためのファイアウォール構成を設置し、維持すること	意図を明確にする目的で複数のセクションが変更され、1.3.3 は削除されました。	この要件では、ファイアウォールの設定へのアクセス権を持つユーザのグループや役割を管理することが求められています。また、この要件では以下のような特権アクセス管理を行うことが明示的に求められています。 ▪ カード所有者データの環境からアウトバウンドのトラフィックが送信されないようにすること ▪ 設定ファイルへの変更をすべて管理し監視すること
要件 2： システム・パスワードやその他のセキュリティ・パラメータにベンダから提供されたデフォルト値を使用しないこと	このバージョンでは主として、内容を明確にするための変更が追加されただけです。	このセクションでは特権アイデンティティおよびアクセスについて、広範囲にわたり取り上げられています。現在のソフトウェアとハードウェアの多くは出荷時にデフォルトのパスワードが設定されています。また、こうしたパスワードに対するポリシーは企業によって大きく異なります。まず、要件の対象となるアセットをすべて特定する必要があります。これらのアセットはオンプレミスや仮想環境、複数クラウド環境などに常駐している可能性があります。特権アクセス管理ソリューションはこうしたアセットの検出だけでなく、パスワードのポリシー設定、セッションの記録、すべての境界（クラウド、仮想、オンプレミス）でのこれらのアセットへのアクセス制御を行えることが必要です。最後に、きめ細かいアクセス制御を設定し、すべてのシステム上で行われたセキュリティ設定に対する変更を保護し監視するよう規定する必要があります。

要件 5： **すべてのシステムをマルウェアから保護し、定期的にアンチウイルス・ソフトウェアまたはプログラムを更新すること**	変更なし。	マルウェアからの保護には多くの方法があります。要件ではアンチウイルス·ソフトウェアを使用するよう明記されていますが、ベスト·プラクティスとしては、企業はマルウェアに対するあらゆる防御策を検討する必要があります。そこで、特権アクセス管理ソリューションを使用すれば、企業はマルウェアに対する複数の防御策を講じることができます。たとえば、アンチウイルス·プログラムをインストール済みのシステムの場合、そのアップグレードと保守のための管理者によるアクセスを十分に制御する必要あります。カード所有者データを含む他のシステムについて企業は、分離戦略の実施、アプリケーションやインフラストラクチャの分類、これらのシステムへのアクセス制御を実施できます。また、ユーザが実行するコマンドを制限できます。さらに、機械学習とユーザ動作分析の進歩によって、疑わしいアクティビティをプロアクティブに抑制でき、アカウントの乗っ取りに対しても効果があります。企業が直面する課題の規模と範囲を考えれば、なおさらこれは重要であり、手作業による手法を正当化することはできません。また、特権アクセス管理ソリューションではキーロギングや画像記録などのテクノロジを使用して、すべてのアクティビティを監視し記録できます。
要件 6： **安全性の高いシステムおよびアプリケーションを開発し、維持すること**	変更は特定のセクションに限られ、手引きとして加えられています。	このセクションでは、カード所有者データにアクセスするソフトウェアやシステムの開発と保守を行う際に従うべき、セキュリティの全体的なベスト·プラクティスを扱っています。この要件に関する手引きでは、以下のような側面に対応しています。 ▪ 最新のパッチがシステムに適用されていることを確認すること ▪ 適切なセキュリティ手順に沿うよう規定するソフトウェアを開発すること ▪ 本番と本番以外のアプリケーションとサーバの分離に従うこと 特権アクセス管理ソリューションはこの要件への対応に非常に役立ちます。たとえば、システムを維持管理したりパッチを適用したりする際などに、企業は適切なレベルの認証と監視を行い、十分な制御手順を備える必要があります。例として、管理ユーザはサーバへのパッチ適用コマンドの実行を許可されているかもしれませんが、これを本番システムで行う場合は追加の制御と承認を適用する必要があるかもしれません。アプリケーションはプログラム上カード所有者データにアクセスする可能性があり、そのためのクレデンシャルが必要です。この要件はまた、さまざまな環境（開発者、テスト、本番環境）にアクセスするユーザの職務の分離の必要性に対応しています。特権アクセス管理ソリューションは、こうしたクレデンシャルをアプリケーションに組み込むのではなく、管理するために役立ちます。職務の分離要件は特権アクセス管理ソリューションと自動化ツールの統合によって対応できます。

要件 7： **業務上の知る必要性に応じてカード所有者データへのアクセスを制限すること**	複数のシステムに対応するよう手引きとテストへの変更が加えられました。	この要件は、機密データを含むアプリケーションやシステムへのさまざまなユーザのアクセスを、役割、ビジネス・ニーズ、最小限の特権に基づき制御することを求めています。この種のアクセスはログに記録し監査可能にする必要があります。 特権アクセス管理ソリューションは、グループ内のユーザを管理し、特定のアプリケーションやアプリケーションのグループに対してユーザが何を実行できるかを定義することで、この要件に対応します。また特権アクセス管理ソリューションを他のソリューションと統合すると、各種のアプリケーションやシステムへのアクセス権を、ワークフローに基づきプロビジョニングおよびプロビジョニング解除するよう規定できます。このアクセスは最終的にレコードとログが記録され、監査可能になります。
要件 8： **システム・コンポーネントへのアクセスを識別し認証すること**	最新バージョンのおそらく最も重要な変更点は、この要件に関する部分です。機密データに対する Web ベース以外のアクセスとリモート・アクセスのすべてを、多要素認証（MFA）で保護しなければならないという要件が加わりました。また、これまでは二要素認証を必要としていた要件が拡張され、多要素認証が必要になりました。	この要件はおそらく、特権アカウントに広範囲な影響を与えるものです。特権アカウントはすべて、アクセスが直接的でも間接的でも、また、リモート・アクセスが行われる場合はすべて、MFA で保護する必要があります。すべてのユーザ・アクセスのログを記録し、追跡可能にする必要があります。この要件では、このようなシステムにアクセスするすべてのユーザに一意のアイデンティティを付与することを義務付けています。ユーザのアクセス権は最小限の特権に基づいて設定する必要があり、すべての操作を監査可能にする必要があります。適切なユーザ・ライフサイクル管理機能（プロビジョニング、プロビジョニング解除、修正）を備え、ユーザとそのアクセス権の作成、削除、修正について規定する必要があります。クレデンシャルを含むユーザ情報はすべて、強力な暗号化を使用して管理する必要があります。パスワードとパスフレーズはすべて、強度とローテーションに関する明確なポリシーに従う必要があります。この要件はまた、特定のアプリケーションに共有クレデンシャルを使用しないよう求めています。カード所有者データを含むデータベースで実行されるコマンドを、役割とビジネス・ニーズに基づいて制限し（データベース管理者のみ）、それ以外のアクセスはすべて拒否するよう規定する、適切な制御が必要です。
要件 10： **ネットワーク・リソースおよびカード所有者データに対するすべてのアクセスを追跡および監視すること**	追加の要件では、サービス・プロバイダ環境のセキュリティ障害について、適切なタイミングでの検出とレポーティングが義務付けられました。	この要件はネットワーク上のすべてのリソースで、全ユーザの完全な監査証跡とそのアクセスについて記録し、特定フィールドのすべてのルール、設定、アクセス制御に加えられた変更をすべて記録することを求めています。

要件 11： セキュリティ・システムおよびプロセスを定期的にテストすること	ここでの変更のほとんどは、侵入テストの要件に関連するもので、特権アクセス管理には直接影響しません。	この要件の 1 部として、リスクを判断するための侵入検知システムを実装することが義務付けられました。ただし現在はコンピューティングの状況の変化によって、機械学習を使用して、ユーザ動作に基づき脅威をプロアクティブに軽減できるようになりました。
要件 12： 全社員の情報セキュリティに対処するポリシーを保持すること	この要件に関する最新バージョンでの変更点は、主に内容を明確にしたことと、テスト手順に関することです。	特権アクセス管理ソリューションは、アクセスを管理し、特権ユーザが全社員についてのセキュリティ・ポリシーを作成、修正、削除できるようにするポリシーをサポートする必要があります。すべての操作を監査可能にする必要があり、そのトランザクションを実行した特定のユーザまでたどれることが必要です。

セクション 2

CA Privileged Access Manager と PCI DSS 3.2 の要件のサポート

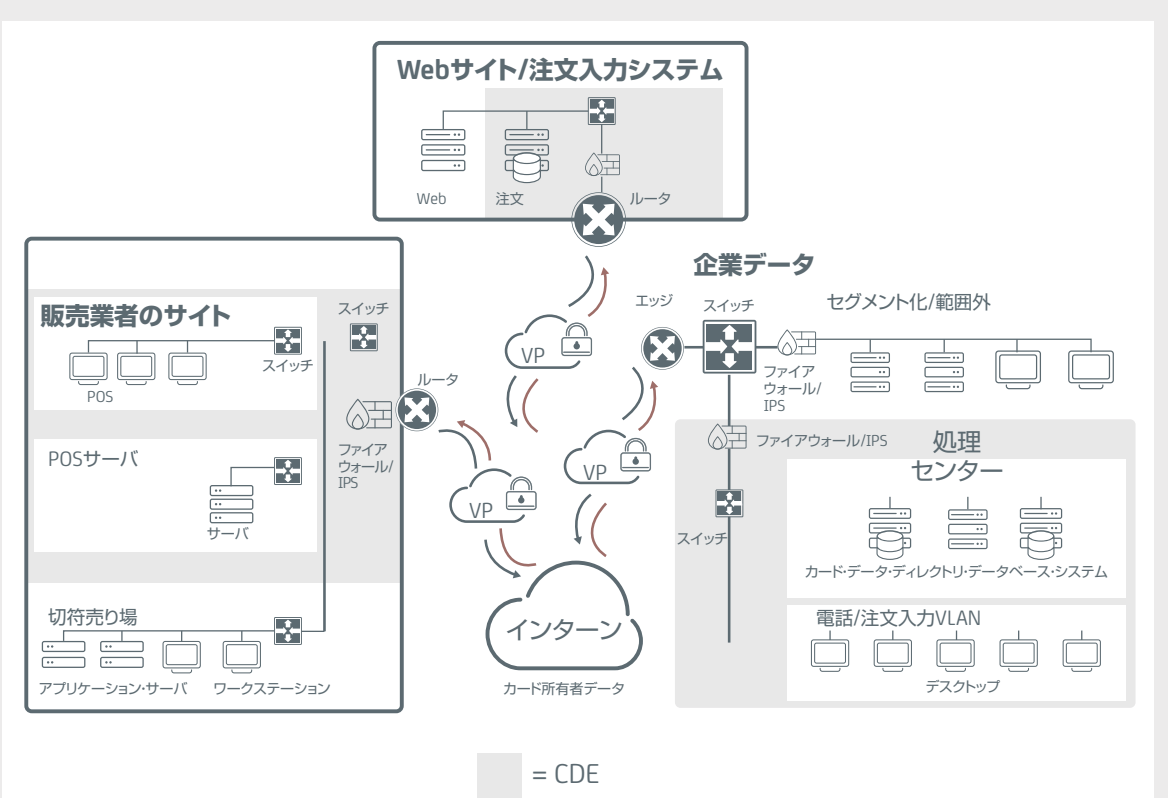
セキュリティ侵害のキル・チェーンの分断

キル・チェーンの基本的な概念は、攻撃者がシステムに繰り返しアクセス（またはそのアクセスを拡大）し、特権レベルを引き上げるというものです。攻撃者はこうして得た特権を使用して水平または垂直方向に移動し、別のシステムにアクセスしたり既存のアクセスを拡大したりして再度特権レベルを引き上げ、最終的な標的に達するまでこの一連の作業を繰り返します。このような一連の作業をそのサイクル内のどこかの地点で分断できれば、最終的な標的に達する前に攻撃を阻止することができます。

CA Privileged Access Manager(CA PAM) は、このような一連の作業、すなわちキル・チェーンの分断に役立つ機能を提供します。たとえば、CA PAM は特権アカウントに対する多要素認証をサポートしています。攻撃者は 1 つのアカウントに対して複数のクレデンシャルを入手しなければならないため、攻撃ははるかに困難になります。また、カード所有者データ環境（CDE）の各コンポーネントに対して各特権アカウントが発行できるコマンドについて、最小限の特権を使用することで、機密情報へのアクセスが低減され、攻撃者は目的のデータへの不正アクセスがさらに難しくなります。

CA PAM によるキル・チェーンのもう 1 つの分断方法は、ネットワーク・セグメンテーションのサポートです。これによって特定の特権アカウントがアクセスできるサブセットと、各サブネット上で管理できるシステムを限定することができます。ネットワーク・セグメンテーションは 1 つのシステムから別のシステムへの攻撃の水平方向の拡大を制限し、攻撃者に組織のネットワークを把握しづらくさせます。同様に、CA PAM にはソケット・フィルタ・エージェント（SFA）があり、これによって管理者は CA PAM ポリシーに反しているホストへの SSH や telnet を試みるなど、別なシステムへの不正なネットワーク接続が確立できなくなります。

図 1.
セグメンテーションに基づいた PCI DSS のコンプライアンス



CA の特権アクセス管理ソリューションは、PCI DSS 3.2 の要件への対応を可能にします。このセクションではソリューションの各種の機能について説明します。また、他の統合された CA セキュリティ・ソリューションと組み合わせることで、企業は堅牢でスケーラブルな、フル機能のソリューションを採用し、PCI DSS のニーズに対応することが可能です。下記の表は、CA PAM がどのように PCI DSS の最新の要件に対応できるかについて、詳細を示しています。

要件	バージョン 3.2 における変更点
1.1：ファイアウォールとルータ設定標準を構築し実装すること	CA の特権アクセス管理ソリューションは、指定された一連の特権ユーザのみが、ファイアウォールとルータ構成の確立、構築、実装を行えるようにします。
1.1.5：ネットワーク・コンポーネントの管理のグループ、役割、職務についての説明	CA のソリューションはユーザ・グループを作成し、特定の役割と特権をこれらのユーザに割り当てることで職務の分離を行い、ネットワーク・コンポーネント、サーバ、アプリケーションの管理の責任を適切に分担させます。また、包括的でスケーラブルなソリューションを提供し、VMWare NSX など仮想ネットワーク環境の管理を支援します。CA のアイデンティティ管理 / ガバナンス・ソリューションと統合すれば、グループや役割へのユーザの割り当てプロセスの自動化が可能です。

1.2.1 : カード所有者データ環境に必要なものへのインバウンドおよびアウトバウンドのトラフィックを限定し、その他のすべてのトラフィックを明確に拒否すること	この要件はインバウンドおよびアウトバウンドのトラフィックの監視の必要性に焦点を当てています。CA Privileged Access Manager Server Control を使用すれば、特定のコマンドが一連のサーバで許可されないよう指定できるため、データが企業のネットワークの外に送信されないよう防止できます。
2 : システム · パスワードやその他のセキュリティ · パラメータに、ベンダから提供されたデフォルト値を使用しないこと	CA PAM はデフォルト·パスワードの変更や、管理者に許可されたネットワーク · アクセス方法など他のセキュリティ · パラメータの変更に対応します。
2.1 : ネットワークにシステムをインストールする前に、必ずベンダ支給のデフォルトを変更し、不要なデフォルト · アカウントは削除するか無効にすること	CA PAM は管理者パスワード / クレデンシャルを保管し管理します。これにはデフォルト · パスワードの変更の強制が含まれます。
2.3 : 強力な暗号化を使用し、コンソールによらないすべての管理アクセスを暗号化すること。Web ベースの管理およびその他のコンソールによらない管理アクセスに対して、SSH、VPN、または SSL/TLS などの技術を使用すること。	CA PAM はアクセス·ポリシーを適用し、個人が承認された（暗号化された）プロトコルを介してのみシステムにアクセスできるように規定します。すべての管理パスワードとクレデンシャルが暗号化されたボールトに保持されるため、管理者はこれらのアクセス · ポリシーを回避することはできません。CA PAM は SSL VPN を提供し、盗聴や改ざんから管理トラフィックを保護します。また、CA PAM コンソール自体へのアクセスも同様に TLS (HTTPS) で保護します。
5.1 : 悪意あるソフトウェアによって一般的に影響を受けるすべてのシステムに、アンチウイルス · ソフトウェアをデプロイすること（特に個人用のコンピュータとサーバ）	CA の特権アクセス管理ソリューションは、一連のシステムでの特定のアプリケーションのインストールとアップグレードを、特定のユーザが管理できるよう許可します。これは管理ユーザのグループや役割に基づいて指定できます。侵入したマルウェアが拡散しないよう、システムとサーバのホワイトリストやブラックリストも作成できます。CA Threat Analytics for PAM を使用すれば、疑わしいアクティビティを検出し、軽減措置を始動できます。

6 : 安全性の高いシステムおよびアプリケーションを開発し、維持すること	CA PAM を使用すれば、カード所有者データの処理システムの一部であるアプリケーション間（A2A）のパスワードを、スクリプト、コード、設定ファイルから排除できます。そのため、アプリケーション開発者やテスト担当者がプレーンテキストで保管された管理パスワードにアクセスできるという、重大な脆弱性を防止できます。この脆弱性は PCI DSS の要件では特に指摘されていませんが、いまだにリスクが非常に高い問題です。たとえば、レポーティングや上流または下流へのトランザクションの目的で、自社開発のシステム、アプリケーション、スクリプトがカード所有者データベースと統合されている場合は、特にリスクが高くなります。
6.3 : 内部および外部のソフトウェア · アプリケーション（アプリケーションへの Web ベースの管理アクセスを含む）を以下のように安全に開発すること ▪ PCI DSS に従うこと（安全な認証とログ記録など） ▪ 業界標準やベスト · プラクティスに従うこと ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込むこと	要件 6.3.1 参照
6.3.1 : アプリケーションが有効になり顧客にリリースされる前に、開発、テスト、カスタム · アプリケーション · アカウント、ユーザ ID、パスワードを消去すること	CA PAM を活用すれば、パスワードをアプリケーション · コードから暗号化されたボールトへ移動できます。また、CA PAM API を使用することで、指定された権限を有するアプリケーションのみが、パスワードを要求できるよう規定できます。ボールトからターゲット · システムまで、ネットワーク上でもメモリ内でもパスワードを暗号化したままにできます。さらに、CA アイデンティティ管理 / ガバナンス · ソリューションと統合すれば、権限を有するユーザのみがアプリケーションのアカウント、ユーザ、クレデンシャルのプロビジョニングとプロビジョニング解除の管理を行えるよう制限できます。
6.4 : システム · コンポーネントに関するすべての変更について、変更制御プロセスおよび手順に従うこと。プロセスは以下を含むこと。	要件 6.3.1 参照
6.4.2 : 開発 / テスト環境と本番環境の職務の分離	CA PAM は開発、テスト、本番で使用されるシステムの特権アカウントに、役割ベースのアクセス制御を適用します。CA PAM を CA のアイデンティティ管理 / ガバナンス · ソリューションと統合することで、役割、特権、職務の分離ポリシーに基づいて、適切なレベルのユーザ·アクセスを可能にします。

7 : 業務上の知る必要性に応じてカード所有者データへのアクセスを制限すること	CA PAM はシステム・コンポーネントとカード所有者データへのアクセスを制限する、一連の包括的な制御機能を実装します。これらの制御機能によって企業は、最小限の特権の考え方を、「明確な許可がなければ特権なし」という考え方へ拡張する、ゼロトラスト・モデルを導入できます。CA のゼロトラスト・モデルはきめ細かいアクセス制御を適用し、特権ユーザのセッションをすべて監視し記録します。また、特権のガバナンス（CA PAM と CA アイデンティティ管理 / ガバナンス・ソリューションの統合）によって、すべてのシステムについて作成、読み取り、更新、削除の操作を含むユーザ・ライフサイクル全体を制御するよう規定できます。これによって職務の分離が可能になり、コンプライアンスのレポーティングを簡略化できます。
7.1 : システム・コンポーネントとカード所有者データへのアクセスを、職務上アクセスが必要なユーザのみに制限すること	CA PAM は最小限の特権の考え方を多くの方法で実践します。特権ユーザにきめ細かいアクセス制御を適用し、特権ユーザはサーバ、ネットワーク・デバイス、その他のシステム・コンポーネントへのアクセスを明示的に許可される必要があります。CA PAM はまた、コマンド・フィルタリング（ホワイトリストとブラックリスト）を使用し、権限を有するユーザがどのコマンドを実行できるかを制限します。また、特権のガバナンス（CA PAM と CA アイデンティティ管理 / ガバナンス・ソリューション）によって、完璧な承認プロセスを通じてこうしたデータへのアクセスがユーザに許可されます。特権へのすべての変更を管理し、すべての特権アクセスを報告できるため、規制準拠の証明に役立ちます。
7.1.1 : 以下のような各役割のアクセス・ニーズを定義すること ▪ 各役割が職務でアクセスする必要があるシステム・コンポーネントとデータ・リソース ▪ リソースのアクセスに必要な特権のレベル（ユーザ、管理者など）	CA PAM は役割ベースのアクセス制御に全面的に対応するため、各管理者の役割（データベース管理者、ネットワーク管理者、システム管理者など）のアクセス・ニーズを定義するのに適したメカニズムを提供します。これには各管理者の役割が、システム・コンポーネントとシステム・コンポーネント内のデータ・リソースのどれにアクセスできるかについての制限も含まれます。
7.1.2 : 特権ユーザ ID へのアクセスを、職務の実行に必要な最小限の特権に制限すること	これは CA PAM の中核的な機能です。特権ユーザ ID または特権ユーザ ID のグループは、許可された各システム・コンポーネントに必要なコマンドのみにアクセス権が制限されます。
7.1.3 : 個々の社員の職務の分類と職能に基づきアクセス権を割り当てること	CA PAM は個人またはグループに適用されたポリシーを強制します。グループと役割の定義は、CA PAM で直接行うか、ソリューションの統合を活用して行えます。企業のディレクトリにすでに存在するグループや役割の定義を使用して定義することも可能です。また、CA アイデンティティ管理 / ガバナンス・ソリューションと統合すれば、ビジネス上の役割、グループ、場所に基づきユーザにアクセス権をプロビジョニングおよびプロビジョニング解除するプロセスによって、プロセスの管理が容易になります。管理ユーザに特権が誤って許可された場合も、修正が可能です。
7.1.4 : 必要とされる特権の指定権限を持つ当事者からの、書面による承認を必要とすること	CA PAM はパスワードを発行する前に、権限を有する個人による承認を要求（および記録）する、二重の認証を強制します。
7.2 : システム・コンポーネントのアクセス制御では、ユーザの知る必要性に基づいてアクセスを制限し、明確に許可されない限り「すべて拒否」するように設定すること。このアクセス制御システムには以下を含むこと。	CA PAM は本人認証と権限認証を区別します。ユーザは強力な（多要素）認証方式を使用して CA PAM にログインします。その後、明示的にアクセスを許可されたコンポーネントのリストがユーザに提供されます。ユーザは許可されないコンポーネントの閲覧やアクセスは行えません。

7.2.1 : すべてのシステム · コンポーネントを網羅すること	PCI DSS が定義するとおり、システム·コンポーネントにはサーバ、ネットワーク·デバイス、アプリケーションが含まれます。CA PAM は市販のアプリケーションをはじめ、PCI DSS が定義するすべてのコンポーネントに対応します。
7.2.2 : 職務の分類と職能に基づき個人に特権を割り当てること	CA PAM では個別またはグループのポリシーによって個人が明確にアクセスを許可されない限り、すべてのアクセスが拒否されます。
7.2.3 :「すべて拒否」をデフォルト設定とすること	CA PAM では個別またはグループのポリシーによって個人が明確にアクセスを許可されない限り、すべてのアクセスが拒否されます。
8 : システム · コンポーネントへのアクセスを識別し認証すること	CA PAM では各ユーザを識別するために一意のユーザ · ログインを必要とし、多数の認証技法をサポートします。また、共有アカウントへのアクセスは、実際のユーザまでたどれるようにすることが重要です。システム · コンポーネントへの自動アクセスの場合、どのユーザの操作がアクセスを起動したかを把握することも必要です。CA PAM はこうしたアクセスにソリューションを提供します。これらのシステム · コンポーネントに対する高リスクのアクセスを最小限に抑えるために、CA Threat Analytics for PAM はアクセスにフラグを付ける方法を提供します。
8.1 : すべてのシステム · コンポーネントで、コンシューマ以外のユーザと管理者について適切なユーザ識別管理を実施するためのポリシーと手順を、以下のように定義し実装すること	CA PAM はすべてのシステム · コンポーネントですべての特権アカウントのアイデンティティを管理するための、ポリシーの適用をサポートします。詳細については後述の 8.1.1 ～ 8.1.8 を参照してください。
8.1.1 : システム · コンポーネントやカード所有者データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てること	CA PAM は CA PAM プラットフォームへの一意のユーザ·ログインを要求し、その後、許可されたシステム · コンポーネントへの特権セッションを確立します。この設定によって企業はインフラストラクチャ·コンポーネントの「共有アカウント」（ルートなど）を活用することで管理を簡略化でき、また、各特権セッションを特定の個人（IP アドレスだけではなく）までたどることができます。
8.1.2 : ユーザ ID、クレデンシャル、その他の識別子の追加、削除、修正を制御すること	CA PAM は職務の分離を適用し、明確に許可された管理ユーザのみが、特権 ID やその他のクレデンシャルに変更を行えるようにします。CA PAM のこれらの特別な管理ユーザは、強力な多要素認証方式を使用する必要があり、そのセッションはすべてログとレコードに記録されます。これは CA アイデンティティ管理 / ガバナンス · ソリューションと統合することで、さらに強化できます。
8.1.3 : 資格が終了したユーザのアクセス権を直ちに取り消すこと	CA PAM では資格が終了した特権ユーザについて、すべてのシステム · コンポーネントへのすべてのアクセス権を即座に取り消すことができます。
8.1.4 : 少なくとも 90 日ごとに、非アクティブなユーザ · アカウントを削除 / 無効化すること	CA PAM では一定期間使用されなかった CA PAM アカウントを自動的に無効化できます。
8.1.5 : リモート · アクセスを介してシステム · コンポーネントへのアクセス、サポート、保守を行うためにベンダが使用する ID を、以下のように管理すること 必要な期間のみ有効化し、使用しない期間は無効化する 使用中は監視する	CA PAM は特権ベンダ ID に対しても、他の特権 ID と同じ管理機能を備えています。これには期間を制限したアクセス権を、ベンダに適用する機能が含まれます。また、各特権セッションの監視と記録を行い、アラートを送信できるほか、ポリシー違反の試行があった場合のアクセス権の自動取り消しも行えます。
8.1.6 : 繰り返しのアクセス試行を制限するために、6 回以内の試行でユーザ ID をロック · アウトすること	CA PAM は、管理者が定義した回数アクセス試行が失敗した場合、CA PAM アカウントをロック·アウトするなどの、アクセス試行失敗時のポリシーを適用します。

8.1.7 : ロック · アウトの期間は最低 30 分、または管理者がそのユーザ ID を有効化するまでの期間に設定すること	CA PAM では、権限を有する管理者が再度有効化するまでそのアカウントをロック · アウトするというように、オプションを適用できます。
8.1.8 : セッションが 15 分以上アイドルになった場合、端末またはセッションを再アクティベートするためにユーザに再認証を求めること	CA PAM ではセッション · タイムアウトを設定でき、デフォルトでは 10 分に設定されています。
8.2 : 一意の ID を割り当てることに加え、すべてのシステム · コンポーネント上の消費者以外のユーザおよび管理者向けに、適切なユーザ認証管理を行うこと。これには以下の 1 つ以上の方法を使用して、すべてのユーザを認証すること : 本人が知っている情報（パスワードやパスフレーズなど） 本人が持っているもの（トークン · デバイスやスマート · カードなど） 本人の一部（生体認証など）	CA PAM は強力な多要素認証方式を含め、多数の認証方式との統合が可能です。CA PAM は選択した認証方式（AD、RADIUS、スマート · カード）に認証要求を渡します。ユーザが正常に認証されると、CA PAM 内の個別またはグループ · ポリシーに基づき、明示的に権限を許可されたアクセス可能なリソースと、使用可能なアクセス方式のリストをユーザに提供します。これによって本人認証と権限認証を分けることができます。
8.2.1 : 強力な暗号化を使用し、すべての認証クレデンシャル（パスワード / パスフレーズなど）を、すべてのシステム · コンポーネント上で、送信中および保管中に読み取り不可にすること	CA PAM はパスワードやその他の認証クレデンシャルを、暗号化されたボールトに保管します。すべての暗号化操作に、FIPS 140-2 セキュリティ·カーネルを使用しています。ハードウェア · セキュリティ · モジュール（HSM）と統合することで、より高度な FIPS 140-2 への準拠が可能です。パスワードその他のクレデンシャルは、安全な暗号化されたチャネル上で送信されます。
8.2.2:パスワードの再設定、新しいトークンのプロビジョニング、新しいキーの生成など、認証クレデンシャルを変更する前にユーザ · アイデンティティを検証すること	CA PAM では、認証が正常に完了してからでなければ、パスワード再設定の有効化や新しい暗号化キーの生成などを行えないように設定できます。
8.2.3 : パスワード / パスフレーズは以下の条件を満たすこと 最小の長さを 7 文字以上にすること 数字と英文字の両方を含むこと もしくは、上記で指定した条件と同等以上の複雑性と強度を持つパスワード / パスフレーズにすること	CA PAM は最小パスワード長や異なる種類の文字の使用など、業界標準のパスワード長と強度 / 構成のポリシーを適用します。
8.2.4 : ユーザのパスワード / パスフレーズは少なくとも 90 日ごとに変更すること	CA Privileged Access Manager は任意の期間ごとにパスワード変更を強制します。システムのパスワード管理機能が、システムに確立されたポリシーに基づき自動的に変更を実行します。
8.2.5 : 個人がこれまで使用したパスワード / パスフレーズのうち、最後に使用した 4 つと同じものは新規のパスワード / パスフレーズとして設定できないようにすること	CA PAM は業界標準の完全に設定可能なパスワードの再使用ポリシーを適用します。このポリシーには、パスワードを再使用できるようになる前に何回の反復が必要か、また、パスワードを再度変更できるようになる前に何日間パスワードを使用しなければならないかについて、管理者が決定した設定が含まれます。
8.2.6 : 初回に使用するためと、各ユーザの一意の値への再設定用のパスワード / パスフレーズを設定し、初回の使用後すぐに変更すること	CA PAM はパスワードの構成、再利用、有効期限設定を含めた一連の包括的なパスワード · ポリシーを実装します。これらのポリシーは 1 回のみの使用にも対応し、毎回使用後に新規パスワードが自動設定されるよう設定することも可能です。 別の選択肢として、パスワードをチェックアウトし、このパスワードを有効とする短い期限を自動的に設定することもできます。

8.3: CDE（カード所有者データ環境）に対するアクセスについては、コンソールによらないすべての個別の管理アクセスと、すべてのリモート・アクセスを多要素認証を使用して保護すること	CA Privileged Access Manager は多数の多要素認証方式と、RADIUS、X.509 証明書、およびスマート・カードをサポートします。CA Privileged Access Manager は、許可されたリソースへの特権ユーザのアクセス権を有効化する前に、強力な多要素認証を適用できます。さらに、業界をリードする CA Advanced Authentication の機能と統合することで、企業は多要素認証を開始できます。PAM の Threat Analytics を使用すると、特権ユーザの動作が正規の動作に反する場合、そのセッションを終了できます。多要素認証は次回のログイン時に強制できます。
8.3.1:社員（ユーザと管理者を含む）およびすべてのサードパーティ（サポートや保守目的のベンダによるアクセスを含む）によるネットワーク外からのリモート・ネットワーク・アクセスに、多要素認証を組み込むこと	CA PAMは多数の多要素認証方式と、RADIUS、X.509証明書、およびスマート・カードをサポートします。CA PAM は、許可されたリソースへの特権ユーザのアクセス権を有効化する前に、強力な多要素認証を適用できます。さらに、CA の業界をリードする高度な認証機能と統合することで、企業は多要素認証を開始できます。CA Threat Analytics for PAM を使用すると、特権ユーザの動作が正規の動作に反する場合、そのセッションを終了できます。多要素認証は次回のログイン時に強制できます。
8.5：以下のように、グループ、共有、汎用の ID やパスワードその他の認証方式を使用しないこと ▪ 汎用ユーザ ID は無効化または削除すること ▪ システム管理やその他の重要な機能には、共有ユーザ ID が存在しないようにすること ▪ すべてのシステム・コンポーネントで管理者には共有および汎用ユーザ ID を使用しないこと	従来の設定では、共有アカウントについて誰が何を行ったかを確認する方法がないことが問題でした。全員がルートまたは管理者としてログインすると、それぞれの特権ユーザは実際上、匿名と同じです。しかし共有、汎用、グループのアカウントは、 システム・コンポーネントの設定と管理を大幅に簡略化するメリットがあり、特に大規模なネットワークではその効果が大きくなります。CA PAM ではこの 2 つのメリットを両立させており、共有アカウントの使用を、その使用者まで完全にたどる（および検証する）ことが可能です。企業は共有アカウントを使用してサーバ、ネットワーク・デバイス、その他のコンポーネントの設定を続行でき、同時に、どの個人が共有アカウントにログインし、何を行ったかの具体的で検証可能なレコードを保持できます。これらの共有アカウントのパスワードは CA PAM のボールトに保管され、ユーザは共有アカウントへのアクセスを許可される前に、CA PAM へのログインを強制されます。ユーザが共有アカウントにログインすると、CA PAM はすべてを監視して記録するため、共有アカウントを使用して実行された特権ユーザのアクティビティはすべて、特定のユーザまでたどることが可能です。

8.6 : その他の認証メカニズムが使用されるところでは（たとえば物理または論理セキュリティ・トークン、スマート・カード、証明書など）、これらのメカニズムの使用を以下のように割り当てること 認証メカニズムは個別のアカウントに割り当て、複数のアカウントで共有しないこと 物理および / または論理的な制御を用意し、目的のアカウントのみがそのメカニズムを使用してアクセス権を得られるようにすること	CA PAM はセキュリティ・トークン、スマート・カード、デジタル証明書など、多数の認証メカニズムの使用に対応します。これらのメカニズムはそれぞれ、併用する追加の認証メカニズムと共に個人や一意の ID に割り当てることができます。これによって、許可されたユーザのみがセキュリティ・トークン、スマート・カード、デジタル証明書を使用してアクセス権を取得できるように設定できます。
8.7 : カード所有者のデータを含む任意のデータベースへのアクセスはすべて（アプリケーション、管理者、その他のすべてのユーザを含む）、以下のように制限されること データベースへのすべてのユーザ・アクセス、ユーザのクエリ、ユーザの操作は、プログラミングによって行われること データベース管理者のみが、データベースに直接アクセスまたは照会できる。 データベース・アプリケーションのアプリケーション ID は、アプリケーション（個人のユーザやその他のアプリケーション以外のプロセスではない）によってのみ使用できる。	CA PAM はカード所有者のデータベースへのアクセスを、許可された管理者のみに制限します。また、アプリケーション・アカウントはアプリケーションによってのみ使用できることを規定します。
10.1 : システム・コンポーネントへのすべてのアクセスと、個別の各ユーザを結びつける監査証跡機能を実装すること	CA PAM はすべての特権アクセスを特定のユーザに結びつけます。強力な多要素認証をサポートし、許可された個人のみが特権アカウントを使用してシステム・コンポーネントにアクセスできるようにします。これによって、各特権セッションを許可されたユーザまで明確にたどることができます。
10.2 : 以下のイベントを復元できるように、すべてのシステム・コンポーネントに自動監査証跡機能を実装すること	システム・コンポーネント（サーバ、データベース、ネットワーク・デバイス、アプリケーションなんど）上で特権ユーザが行うすべての操作は、CA PAM の改ざん防止ログに記録されます。この記録は許可された個人のみがアクセスしレビューできます。詳細については後述の 10.2.1 ～ 10.2.7 を参照してください。
10.2.1 : 個別のユーザからカード所有者データへのすべてのアクセス	カード所有者データベースへの管理者によるすべてのアクセス（許可されたデータベース管理者からのアクセスなど）は、CA PAM によって監視および記録されます。
10.2.2 : ルート権限または管理者権限を持つ個人が行ったすべての操作	CA PAM はすべての特権アクティビティを監視し記録します。企業が共有管理アカウントを使用している場合でも、CA PAM は実行された操作をそれぞれ一意のユーザまで明確にたどることができます。
10.2.3 : すべての監査証跡へのアクセス	CA PAM は職務の分離を規定し、特別に許可されたユーザのみが CA PAM のログ・ファイルとレコードをレビューできるようにします。許可されたユーザがログをレビューすると、その事実も毎回記録され、レコードに保存されます。

10.2.4 : 無効な論理アクセス試行	CA PAM は、CA PAM プラットフォームを介して行われた無効な論理アクセス試行をすべて追跡します。まず、CA PAM へのアクセス権が付与されるのは許可されたユーザのみで、付与された場合、明示的に許可されたシステムへのアクセス権のみが許可されます。許可されたシステムへのアクセス後も、許可されたシステムを使用して許可されていないシステムにアクセスしようとすると、CA PAM が防止します。CA PAM は、たとえばサーバに直接接続しログインしようとする試みなど、プラットフォームの外でログイン試行が行われ失敗した場合はログに記録しません。ただし、すべてのパスワード / クレデンシャルは CA PAM ボールトに保管され、ユーザには知られないため、個人は CA PAM プラットフォームを経由する以外に、これらのシステムにログインする方法がありません。
10.2.5 : 身元確認と本人認証の使用と変更 メカニズム—新規アカウントの作成など 特権レベルの引き上げ—およびルートまたは管理特権のあるアカウントへの変更、追加、削除のすべて	CA PAM は特権アカウントに関する身元確認および本人認証のアクティビティをすべてログに記録します。これにはそのアカウントに関するすべての変更と、そのアカウントの使用がすべて含まれます。
10.2.6 : 監査ログの初期化、停止、一時停止	CA PAM にはログ記録が開始されたことを示すログ · エントリはありませんが、デフォルトで常にログを生成します。
10.2.7 : システム · レベルのオブジェクトの作成と削除	CA Privileged Access Manager では対象とするサーバ、アカウント、パスワード、グループ、ユーザなどの作成と削除を、許可された管理者が行えます。
10.3 : すべてのシステム · コンポーネントについて、イベントごとに少なくとも以下の監査証跡エントリを記録すること	CA PAM はすべてのシステム · コンポーネントでの特権アクセスについて本格的な監査証跡を記録します。詳細については後述の 10.3.1 ～ 10.3.6 の対応欄を参照してください。
10.3.1 : ユーザの身元確認	ユーザは強力な多要素認証方式で認証されるため、CA Privileged Access Manager が保持するログとレコードでは一意のユーザが捕捉されます。
10.3.2 : イベントの種類	CA PAM syslog イベントは、ログイン / ログアウトの試行、ポリシー違反の試行、リモート · セッションの確立などにカテゴリ化されています。
10.3.3 : 日時	日時は syslog とセッション · レコーディングのストリームの一部として捕捉されます。
10.3.4 : 成功と失敗の指標	ログイン / ログアウト試行など成功または失敗を伴う各イベントについて、CA PAM は成功または失敗のログを記録します。
10.3.5 : イベントの発生元	CA PAM は各イベントでソリューションへのアクセスに使用された一意のユーザ · アイデンティティとソース IP アドレスを捕捉します。
10.3.6 : 影響を受けたデータ、システム · コンポーネント、リソースのアイデンティティまたは名前	システム · コンポーネント、リソースなどに影響を及ぼすイベントについて、影響を受けたターゲットと、システムへのアクセスを試行しているユーザのアイデンティティを捕捉します（ホスト名など）。

10.4：時刻同期技術を使用し、重要なすべてのシステム・クロックと時刻を同期し、時刻の取得、配布、保管のために以下を実装すること	CA PAM は業界標準の時刻同期技術、Network Time Protocol（NTP）をサポートしています。
10.4.1：重要なシステムの時刻が正確で一貫していること	CA PAM は NTP を使用して時刻同期を実行し、監査ログとレコードで正確で一貫したタイムスタンプが得られるように規定しています。
10.4.2：時刻データを保護すること	CA PAM は、基本的な NTP より高度な統合を可能にする、NTP 認証を使用するよう設定できます。
10.4.3：時刻設定は業界が認めた時刻ソースから受信すること。	2 つのデフォルトの時刻サーバが指定され、許可された CA PAM 管理者はこれらを補強および / または変更できます。
10.5：監査証跡を改変できないように保護すること	CA PAM のログとレコードは不正なアクセスや改ざんから保護され、変更が行われた場合はすべて検出されます。
10.5.1：監査証跡の閲覧は、職務で必要とする個人に限ること	CA PAM のログとレコードは、最小限の特権の考え方と役割ベースのアクセス制御に従い、明示的に許可された社員のみがアクセス可能です。
10.5.2：監査証跡ファイルを不正な改ざんから保護すること	CA PAM のログとレコードにはすべて、暗号ハッシュ技術を使用した改ざん防止機能が備わっています。ファイルが改ざんされた場合、そのことが通知されます。
10.5.3：迅速に監査証跡ファイルのバックアップをとり、改ざんされにくい中央ログ・サーバまたはメディアに保管すること	CA PAM は syslog の転送機能によって、CA PAM のすべてのログのバックアップを中央 syslog サーバ、一度だけ書き込み可能なメディア、その他の形式のログ・ストレージやアーカイブに保管します。
10.5.5：ファイル整合性監視または変更検出ソフトウェアをログに使用し、既存のログ・データが変更された場合、必ずアラートを生成するようにすること（ただし新規データが追加された場合はアラートを生成しないようにすること）	CA PAM のログとレコードには、暗号ハッシュ技術を使用した改ざん防止機能が備わっています。新規データの標準的な追加以外に既存のログまたはレコードが変更された場合は削除されます。
10.6（10.6.1 ～ 10.6.3 を含む）：すべてのシステム・コンポーネントのログとセキュリティ・イベントをレビューし、異常や疑わしいアクティビティを特定すること	CA Threat Analytics for PAM は、堅牢な機械学習に基づくユーザ動作分析（UBA）ソリューションを提供します。このソリューションは SIEM ソリューションやその他のエンタープライズ・ログ記録ソリューションと連動し、ユーザベースのアクティビティに関連するリスクを判断するために使用できます。判断したリスクは、各種の技術を使用して軽減できます。
10.7：監査証跡履歴は少なくとも 1 年間保持し、少なくとも 3 か月間は分析に即座に対応できるようにしておくこと（オンライン、アーカイブ、バックアップから復元可能など）	CA PAM は syslog を使用するため、監査証跡が必要と見なされる限り syslog サーバに保持できます。これによってローカルの CA PAM システム上のストレージ領域が解放され、ログ・データは即座に分析に使用できます。ローカルの CA PAM システムは 4 か月間ログを保持できます。

12 : 全社員の情報セキュリティに対処するポリシーを保持すること	CA PAM を使用すれば、カード所有者データを保護する特権ユーザ · ポリシーを捕捉して適用できます。また、カード所有者データの処理に携わる各システム·コンポーネントに必要な制御を、容易に備えることができます。
12.2 : 以下のようなリスク評価プロセスを実装すること 年 1 回以上、および環境への重大な変化があった際に実施（合併吸収、移転など） 重要なアセット、脅威、脆弱性を識別 正式なリスク評価を実施	CA PAM を使用すれば、企業はログとレコードをレビューできます（DVR のような再生機能）。ポリシー違反の試行はすべてログに記録されるため、管理セッションのレビューでは、ポリシー違反の試行が起きた場所を集中的にレビューし、その後、その他の不規則イベントのセッションを抽出調査できます。

セクション 3

まとめ

2018 年 2 月から PCI DSS バージョン 3.2 への準拠が必須となり、企業が継続的にコンプライアンスを確保するには、スケーラブルなソリューションを検討することがきわめて重要になっています。そのために、以下の要素について検討する必要があります。

- **スケーラビリティと高可用性：**PCI DSS の対象となるシステムとアプリケーションには機密性の高いカード所有者データが含まれるため、これらのアプリケーションだけでなく、それを保護するソリューションにも高い可用性が必要です。そのため、特権アクセス管理ソリューションには高度なスケーラビリティが必要で、ユーザとそのアクセスの本人認証と権限認証だけでなく、セッションの管理と記録も行えることが必要です。
- **拡張可能：**PCI DSS の対象となるシステムやアプリケーションが増加する中、特権アクセス管理ソリューションはビジネスの成長やデプロイのフェーズに応じて容易に拡張でき、新規のインフラストラクチャやアプリケーションに迅速かつ効率的に対応できることが必要です。また、ユーザやシステム、アプリケーションの急増で、ユーザ・アクティビティの手作業による監視はさらに困難になっています。特権アクセス管理ソリューションは、分析に基づくリスク緩和戦略を提供する必要があります。特権アクセス管理は他のソリューションと統合でき、PCI DSS に包括的に対応できることが必要で、これは検討事項として重要です。
- **総所有コスト：**特権アクセス管理ソリューションに必要な機能が増えているため、長期的な所有コスト（通常は 3 ～ 5 年）は極端に高額になるべきではありません。特権アクセス管理ソリューションはたとえば、パスワード・ボールトだけを備えたものなど、簡単に構築できる場合もありますが、PCI DSS はパスワード・ポリシー、認証、セッションの管理と記録の機能など、それ以上の対応を要求しています。これらの機能が別々に提供される場合、企業はインフラストラクチャ、スキル・セット、ライセンスや、各フェーズのデプロイ・コストのニーズなどを考慮する必要があるかもしれません。また、保守と統合のコストはそれぞれの段階によって異なる場合があり、最初の段階では最小構成価格が低くても、将来的には価格が高くなりすぎる場合があります。

CA の特権アクセス管理ソリューションが企業にどのようなメリットを提供するかについての詳細は、[ca.com/pam](ca.com/pam) をご覧ください。

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。

CS200-298517_0817