

2017 年 10 月 4 日

日本 CA、顧客のハイブリッド IT 環境を保護する 次世代特権 ID アクセス管理ソリューションを発表

～ハイブリッド IT 環境における管理者認証情報の保護と、
特権ユーザのアクセス制御、活動の監視・記録を通じて不正行為を防止～

(2017 年 10 月 4 日、東京発)

日本 CA 株式会社（東京都千代田区、社長：反町 浩一郎）は、オンプレミス、クラウド、ハイブリッドの IT 環境での不正アクセス行為を防止する次世代の特権アクセス管理ソリューションである [CA Privileged Access Management \(PAM\)](#) の提供を開始することを発表しました。日本での同製品の提供は初めてとなります。

CA PAM は、特権 ID／特権アクセスにおける不正行為の防止、コンプライアンスの遵守、運用効率の向上に必要な幅広い機能を提供します。不正行為の防止では、包括的なプラットフォームを保護する特権アクセス管理機能を提供しており、その保護対象には、従来のデータセンターのリソース、仮想化データセンターおよびクラウド・ベースのインフラストラクチャに導入されたリソース、並びに仮想化、IoT 環境、IaaS/SaaS 管理に対して網羅しており、管理コンソールと API を提供しています。

特権アクセス管理ソリューションのスケラビリティは、企業が多様な環境においても、信頼できるユーザによるサイバー・リスクに対処し、管理できるようにするために不可欠な要素です。アクセスの管理・監視機能の導入が多く地域や部門、およびハイブリッド環境全体に広がるにつれて、アーキテクチャ上の判断によっては、インフラストラクチャの割当てとオペレーティング・システムやデータベースとの整合性を確保することが困難になりかねません。CA PAM は、ユーザーアクセスポイントの多様性をより詳細に制御できる重要な機能を備えたこれらの要件をサポートしています。また、セキュリティ管理者がユーザ管理の強制、制御、および監視を簡単にする機能も備えています。

さらに、CA Threat Analytics for PAM (TAP) の追加導入により、統合型ユーザ行動分析 (UBA) のサポートを得られ、特権ユーザに関連する従来よりも優れた脅威検出と不正行為防止のための機械学習機能も利用可能となります。

特権アクセスが「root」、「administrator」、「super_user」アカウントの形式で提供されるのか、あるいは高度な特権付きのアプリケーション、API、またはサービスなどのアカウントの形式で提供されるのかに関わらず、あらゆる特権アクセス環境を効果的に管理することが、これらの動的なクラウド環境においては、ますます困難になってきています。このことは、これらのハイブリッド環境が本質的に安全でないからではなく、セキュリティの側面（特に特権 ID/特権アクセスのさまざまなレベルに関して）がしばしば見落とされていることに起因しています。*

CA PAM は以下の問題に対応します：

不正行為の防止： 認証情報を保護し、特権ユーザ(社内、信頼できるサードパーティ、自動化のアプリケーション/システムなど)を積極的に認証し、特許技術を用いてユーザの振る舞いや行動をプロアクティブに制御することで、ポリシー違反を防止し、行動を監視・記録します。

コンプライアンス： 特権ユーザに対する制御は、さまざまな業界/セクターにまたがる多くの規制、標準、および権限に則して統一されています。PCI DSS、HIPAA、NERC-CIP、FISMA、およびその他のコンプライアンス基準は特権アクセスの機密性を認めています。

アドミニストレータ/運用効率と生産性： データセンター全体、仮想インフラストラクチャ、パブリックおよびプライベート・クラウドにまたがる特権ユーザ向けに、シングル・サインオンとフェデレーション ID を提供します。また、アプリケーション毎のパスワード管理の容易化、操作の簡素化、ダウンタイムの防止などの機能も提供します。また、大企業における可視性と管理性をより向上させるために、サービスとしてのセキュリティと複数部門への導入をサポートするように特別に設計された新しい管理コンソールも組み込まれています。

CA Privileged Access Manager には、このほかにも以下のような特徴が含まれています：

- 多数のタスク管理のためのシンプルなユーザ・エクスペリエンス
- エンタープライズ・クラスタリングの強化
- 米国連邦政府の認定
- 拡張自動ディスカバリ (Win ローカル、svc)
- セッション記録の暗号化と暗号モジュールの拡張

ガートナーは、セキュリティおよびリスク管理ソリューションのリーダーは IAM (ID / アクセス管理) 機能の提供を推奨しています。「セッション記録機能をできる限り早期に導入すべきである。この機能によって特権による活動の説明責任と可視性が得られるからです。選定プロセスの構成要素としてこの機能を入れておきましょう。」**

CA Technologies セキュリティ・ソリューション営業部 部長 四宮 康典

セキュリティが企業の成長と進化の足かせとなるようなことがあってはなりません。そうではなく、ユーザ体験を阻害しないセキュリティを実現しなければ、企業の競争優位は構築できません。特権 ID アクセス管理のニーズは、日々生み出されるビジネスのデジタル化の増大とスピードアップに後押しされて大きくなっています。特権アクセス管理ソリューションの成熟の鍵は、デジタル・トランスフォーメーションの過程を通じて企業の事業に応じて調整、適応、スケーリングできるようにすることです。

株式会社アシスト 執行役員 東日本技術本部長 星 博 様

株式会社アシストは、このたびの日本 CA 様の「CA Privileged Access Management」(CA PAM) 提供開始に関する発表を心より歓迎いたします。弊社は昨年より CA PAM の日本語版ベータテストに参画し、ハイブリッドクラウド管理、モバイルをはじめとする多種多様な管理対象の増加、ランサムウェアのような巧妙化するサイバー攻撃への対応など、最新の特権 ID アクセス管理に求められる様々な要件に包括的に対応可能な製品として、国内での展開に大きな期待を寄せております。今後は弊社が提供している「特権 ID 管理ソリューション」の中核製品として CA PAM を位置付け、日本 CA 様との緊密なパートナーシップのもと、両社共同で CA PAM に関する各種プロモーション活動などを積極的に展開し、お客様企業の情報漏えい対策をより一層強力に支援して参ります。

CA Privileged Access Manager は本日より提供を開始。

*Gartner Securing Privileged Access to Your IaaS Environment, Lori Robinson 著, (ガートナー: IaaS 環境への特権アクセスのセキュリティ確保), 2017 年 8 月 3 日刊

**Gartner Market Guide for Privileged Access Management (ガートナー: 特権アクセス管理の手引) Felix Gaehtgens, Anmol Singh, Dale Gardner 共著. 2017 年 8 月 22 日刊。

ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高の評価を得たベンダーのみを選択するようテクノロジーの利用者に助言するものではありません。ガートナー・リサーチの発行物は、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。

CA Technologies について

CA Technologies (NASDAQ: CA) は、ビジネスの変革を推進するソフトウェアを提供し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスをつかめるよう支援します。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。CA Technologies の詳しい情報については、<<http://www.ca.com/us.html>>(米 CA Technologies)、<<http://www.ca.com/jp>> (日本)をご覧ください。また、ツイッターについては、https://twitter.com/ca_japan をご覧ください。

***本文中に記載されている会社名、製品名は、各社の登録商標または商標です。**

この件に関する報道機関からのお問い合わせ先:

CA Technologies
〒102-0093 東京都千代田区平河町 2-7-9 JA 共済ビル 9 階
コーポレート・コミュニケーション部
TEL: 03-6272-8110 FAX: 03-6272-8115
e-mail: kosuke.nakamura@ca.com