WHITE PAPER | 2017 年 5 月

大規模なデジタル・トランスフォーメーションと自動化に対応する特権アクセス管理の成熟度モデル

ca technologies

目次

概要

課題

デジタル・トランスフォーメーションを進めている組織は、リスクとセキュリティをめぐって増幅する懸念に対処していますが、これは意外なことではありません。デジタル・トランスフォーメーションの取り組みを推し進めていくと、既存の管理の対象から外れた企業インフラストラクチャへのアクセス・ポイントが必然的に増加します。そのため、以前よりはるかに多い多様なアイデンティティからアクセス可能になり、分散化した動的インフラストラクチャ全体でアクセス・ポイントが急増します。

ビジネス・チャンス

特権ユーザについて知ることがリスクを知ることにつながります。特権アクセス管理用ツールは、それ自体が権限認証プロセスの自動化をサポートできる必要があり、動的運用と一時的インフラストラクチャ（人のアイデンティティ用の Amazon Web Services（AWS）管理アカウントなど）の両方をサポートすることで、スケーラビリティを実現する必要があります。

メリット

クレデンシャルの盗用による攻撃をより確実に特定するには、単により多くのデータを蓄積すれば済むという問題ではなく、特権ユーザの動作に関するより有用なデータを組み込む必要があります。それにより、現実のリスクを示す大きな変化を特定できます。このアプローチは、特権アクセス・ガバナンス・システムとの統合によって強化され、同等の役割を持つユーザ間の動作分析が可能になります。

セクション 1

はじめに

21 世紀において、企業の競争力と効果的な運用の中核はソフトウェアにあるといえます。テクノロジは長い間、ビジネス戦略において非常に重要な役割を果たしてきました。しかし、デジタル・トランスフォーメーションによって、ソフトウェア・デリバリ・サイクルとアプリケーション開発プロセスの変革と迅速化はビジネス全体にとって不可欠なものとなり、重役会議室における他の差し迫った懸案であるサイバーセキュリティとの関わりもますます増大しています。

トランスフォーメーションには必然的に変化が伴い、その延長線上でリスクも伴います。 企業がデジタル・トランスフォーメーションを推進するにつれて、そのリスクが顕著になってきます。それに対処するには、アクセスのセキュリティとガバナンスに対する計画を策定し、イニシアチブに厳密に従って作業を進め、以下を始めとする多くのデジタル・トランスフォーメーション計画の優先度を反映させる必要があります。

- 説明責任と可視性を備えた自動化を実現する
- 企業の資産を守りつつデリバリを迅速化する
- 統合されたアクセス・ガバナンスと脅威検出の規模を確保する

コンプライアンス、セキュリティ、およびガバナンスの可視性と説明責任を確保しながら、デジタル・トランスフォーメーションに必要な柔軟性を実現するには、すべてにつながる鍵である特権アクセスの付与対象（人、アプリケーション、サービス、マシン、モノなど）に対して、より整合性の高い、新しいアプローチが必要です。

現在デジタル・トランスフォーメーションの実践的な行程の定義に取り組んでいる多くの企業と同様に、セキュリティ・チームもビジネス・ニーズに応じて着実にアクセス管理とリスク緩和の自動化、迅速化、および拡張を進めていく上で、高額な投資をせずに使用できる適切なツールと統合機能を求めています。

セクション 2

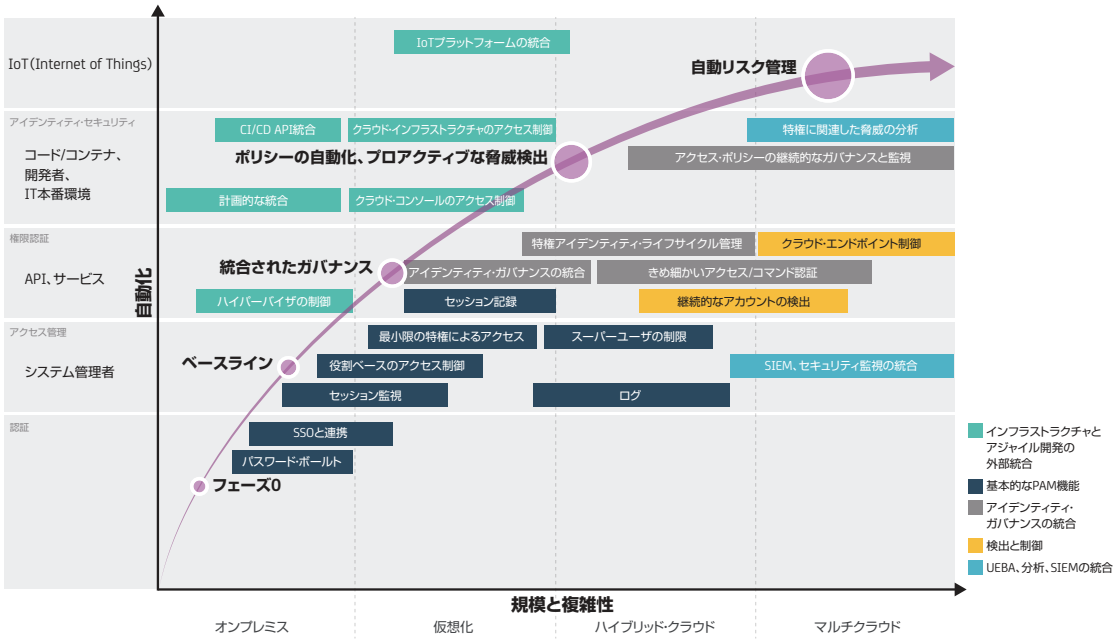
デジタル・トランスフォーメーションによる特権アクセス・リスクの増大

デジタル・トランスフォーメーションは必然的に、コード、マシン、および人のアイデンティティの相互作用を変化させ、加速、自動化します。デジタル・トランスフォーメーションの取り組みを推し進めていくと、既存の管理の対象から外れた企業インフラストラクチャへのアクセス・ポイントが必然的に増加し、以前よりはるかに多い多様なアイデンティティからアクセス可能になります。また、分散化した動的インフラストラクチャ（オンプレミス、仮想、クラウド）全体でアクセス・ポイントが急増し、その結果、リスクとセキュリティに関する懸念が増大します。

特定のサービスやリソースにアクセス可能なアイデンティティの決定、そのリソースに対するクレデンシャルの管理、人的介入を最小限に抑え、ポリシーに則った適切なアクセスを確保することが、自動化、規模、およびスピードを実現するための重要な課題です。

また、企業はモバイル革命に対処するためには、IoT（Internet of Things）によってインフラストラクチャ全体で桁違いに急増しているトランザクション量に対する準備も整える必要があります。デジタル・トランスフォーメーション・ツール導入の結果として、IoT デバイスが環境に組み込まれる前でさえ、アクセス管理という等式の「誰が」という要素が大幅に変化しています。

特権アクセス管理がデジタル・トランスフォーメーションのネックではなく重要な推進要因として機能するには、トランスフォーメーションによって生じるリスクに対し、統合された拡張可能なソリューションをテクノロジとツールを駆使して提供する必要があります。



統合されたガバナンス

デジタル・トランスフォーメーションによって、従来のシステム管理者の役割から外れた特権アクセスを必要とするユーザ数と、特権アイデンティティとして動作できるエンティティ数が増加した場合、人物認証プロセスに頼る手作業のアプローチでは対応できません。新たなアクセス・シナリオに合わせてアジリティとセキュリティのバランスをとるには、統合されたガバナンス・プロセスによって認証要求と役割要求を管理する必要があります。これは、そのアクセス・シナリオが、本番環境、仮想コンテナ、およびデータ・ソースに対する権限を持つホストにおいて特権クレデンシャルへのアクセス権を持つ開発者であっても、クラウド・サービスへのスーパーユーザ・アクセス権を持つ管理者であっても同じです。

ポリシーの自動化

オンプレミス・リソース、仮想データセンタ、およびパブリック・クラウド環境に広がるハイブリッド・クラウド開発 / デプロイ・アーキテクチャでは、特権アイデンティティに対するアプローチが断片化し、サイロ化しがちです。一貫性を維持するには（そしてベンダ・ロックインを回避するには）、環境固有の特権アカウント（AWS の superadmin アカウントなど）に一元的なガバナンスおよびアクセス制御ポリシーを動的に適用する必要があります。

プロアクティブな脅威検出

物理データセンタ・サーバなどの静的インフラストラクチャの共有パスワードのアクセス管理とは対照的に、企業は現在、特権クレデンシャルへのアクセスの認証、監視、ロギングを時間、日、または分単位で管理するだけでなく、それらのクレデンシャルに対する変更やアクションの正当性とリスクの可能性を分析する必要があります。機械学習と動作分析を活用した状況対応型のアプローチをとれば、たとえ動的で一時的な環境でも、リアルタイム検出を推進し、リスク緩和手順をトリガすることができます。

自動リスク管理

IoT を採用すると、IoT デバイス・コントローラという形で新しい種類のマシン特権アイデンティティが導入されるだけでなく、このテクノロジの使用によってトランザクション数が急増する可能性があるため、攻撃に備えてそれらのトランザクションを明示的に認証して監視する必要があります。特権アイデンティティによるアイデンティティの規模とトランザクション量に対処するには、脅威検出に効果的で、ビジネス・プロセスに重大な影響を与えずにリスクを評価し緩和策を実装するためのメカニズムをサポートする自動化モデルが必要です。

セクション 3：

統合されたガバナンスとポリシー自動化の達成：段階的な推進

デジタル・トランスフォーメーションを背景とした特権アクセスの管理と保護は、差し迫った課題ですが、克服できないわけではありません。

ただし、特権ユーザのクレデンシャルを悪用して不正アクセスを試みる（そして成功する）攻撃者が増えているため、ポリシーを制限して盲点を監視するために、成熟度モデルが必要です。さらに、機械学習に基づく分析を通じて、これまでの投資の価値を高め精度を改善できるプロアクティブな検出モデルを実現するためにも、成熟度モデルが必要です。

デジタル・トランスフォーメーションを妨げるのではなく促進するには、インフラストラクチャ、機密性の高いシステム、および機密データに対する特権アクセスを、現実的でよく調整された成熟度モデルの各段階に基づいたものにする必要があります。最も明確なアクションは、特権クレデンシャルへのアクセスのプロビジョニングに必要な手作業の数を減らすことと、認証に関する判断と明確に定義されたポリシーとを結び付けることです。

その結果として、特権アクセス管理プロセスとアイデンティティ・ライフサイクル管理プロセスがより緊密に統合され、セキュリティ・チームが大規模な自動化を実現できる範囲が大きくなります。特権アイデンティティに割り当てられた役割とアクセス権に自動チェックを適用すれば、本番コードに対するクレデンシャルへのアクセス権が開発者に付与されるなどの違反に、プロアクティブにフラグ付けできるようになります。

ここで重要な点は、特権アクセス管理ツール自体が権限認証プロセスの自動化をサポートできる必要があることです。また、動的運用と一時的インフラストラクチャ（人のアイデンティティ用の AWS 管理アカウントなど）の両方に対するサポートによって、スケーラビリティを確保できることが必要です。

特権アクセス管理に対する既存のアプローチの多くは、特権アイデンティティの一部しかカバーしておらず、最近の IT インフラストラクチャを念頭に置いて設計されたものではありません。企業が成熟度モデルの各段階を進んで行くためには、特権アクセス管理に対するアプローチが特権アイデンティティの増殖、分散、トランスフォーメーションにどのように対処するかを、以下の能力に基づいて考慮する必要があります。

- オンプレミスから仮想データセンタおよびクラウド・サービスまで特権アイデンティティのガバナンスと可視性を拡張する。
- 手作業の承認プロセスではなく、アイデンティティ管理の役割ベースのポリシーとの統合を通じて、運用要件に基づいて特権アクセスの認証を自動化する。
- 制御と監視を拡張して、動的で一時的なインフラストラクチャに統合する。
- 一元的かつ継続的な監視とガバナンスを促進し、過剰な権限がいつ最初に付与されたかを特定して修復ワークフローをトリガできるようにする。
- 機械学習とデータ主導のモデルを通じて、新たに進化した脅威を検出して修復する機能を組み込む。

セクション 4：

リスク背景の考慮

デジタル･トランスフォーメーション･プログラムは、分散ネットワーク、高頻度の変更、トランザクション量の増大、および特権アイデンティティの増加につながります。特権クレデンシャルの誤用や盗用を検出するための従来のルールベースのアプローチは、すでに既存の脅威に対してさえ不適切であることが証明されているため、このような状況への対応が課題となります。

特権分析への一般的なアプローチを採用し、より多くのデータをセキュリティ情報 / イベント管理（SIEM）システムに投入したとしても、セキュリティ・アナリストや IT 運用担当者が一貫性の欠如や深刻な異常、および修復が必要な高リスクの行動を明確に識別するために必要な重要なコンテキストが欠けています。

必要なのは、特権ユーザの役割と動作に関するコンテキストと知識を活用して対象を絞り、膨大なデータから攻撃や侵害の具体的証拠を示すアクションを検出して対応できる、ドメイン固有のアプローチです。

ドメイン固有のアプローチは、動作の基準を定義する場合と同じ原則に基づいて機能します。特権ユーザが実行しているアクション、特権ユーザが過去に実行したアクション、それらのアクションに関連するレベルまたはリスク（ターゲット・リソースの機密性、特権ユーザがシステムにアクセスする方法を含む）などの基準です。ただし、このアプローチでは、動作をコンテキストに組み込んだエンティティ・リレーションシップ（ER）図も含める必要があります。

セクション 5

特権ユーザについて知ることがリスクを知ることにつながる

クレデンシャルの盗用による攻撃をより確実に特定するには、単により多くのデータを蓄積すれば済むという問題ではなく、特権ユーザの動作に関するより有用なデータを組み込む必要があります。それにより、現実のリスクを示す重大な変化を特定できます。

このアプローチは、特権アクセス・ガバナンス・システムとの統合によって強化され、同等の役割を持つユーザ間の動作分析が可能になります。特権ユーザまたはマシンがその役割と矛盾するシステムにアクセスしたり、同等の役割のユーザやマシンと異なるシステムにアクセスしている場合や、通常とは異なる IP アドレスからシステムにアクセスして過去のパターンと矛盾するアクションを実行している場合、システムは攻撃を示す動作をより正確に検出して適切な修復を実行できます。

セクション 6：

まとめ

デジタル・トランスフォーメーションは一夜で達成できるプロセスではありません。必然的に、高リスクのアイデンティティに対するセキュリティ・ポリシーの適用と、特権アイデンティティの誤用に起因する潜在的脅威の検出の両方を自動化する能力が必要になります。リスクベースのアプローチを実装することで、セキュリティ・コントロールおよび分析をデジタル・トランスフォーメーションの進行に合わせて実施でき、他を犠牲にすることなく高いコスト・パフォーマンスで自動化、拡張、および迅速化を実現できます。このデジタル・トランスフォーメーションの旅では、数年にわたる明確なロードマップを考慮する必要があります。このロードマップでは、特権アクセス管理ソリューションから短期的および長期的な要件を予測し、ライフサイクル全体の対象範囲と規模のニーズを妥当な所有コストで確保するようにします。

セキュリティは不可欠ですが、その対象範囲、規模、およびコストがデジタル・トランスフォーメーションの阻害要因になってはいけません。

CA PAM がビジネスに与えるメリットの詳細については、**ca.com/jp/ppm** 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・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。

CS200-270334_0517