**SOLUTION BRIEF**
CA IDENTITY SUITE

# ビジネス・ユーザを強化するアイデンティティ管理およびガバナンス

ITとビジネス・ユーザのギャップを埋める

ca technologies

# 概要

## 課題

IT リーダー、セキュリティ・エグゼクティブまたはビジネス・マネージャは、変化と課題の多い時代に直面しています。IT 環境では、分散化、複雑化および異種混合化が進んでいます。しかし、誰がどこにアクセスするかを判断し、ポリシーを高信頼性で実施することは、IT、セキュリティおよびビジネスの 3 つの部門のすべてが取り組む必要のある多面的な課題です。

その一方で、IT の予算は削られ、限られたリソースでその責任を果たすことが求められます。したがって、以下のような重大なアイデンティティの課題に対応する、高信頼性でコスト効果に優れた手法が必要となります。

- 新しいユーザを迅速にオンボーディングし、できるだけ早期に生産性を高める
- 現在の役割に基づいて、すべてのユーザに正しいアクセス権限を割り当てる
- 主要なアイデンティティ・プロセスを自動化して、効率を改善し、コストを削減する
- 潜在的なポリシー違反（孤立アカウント、不正な権限など）を発生する前に特定し、防止する
- 誰がどこへアクセスできるかを把握することで、監査要件を満たす

さらに、これらの今日の環境で実現するには、以下が重要です。

- シンプルでわかりやすいエクスペリエンスを提供して、ビジネス・ユーザがコア・アイデンティティ・サービスに簡単にアクセスできるようにする。

## ビジネス・チャンス

ビジネス・ユーザの強化が優先される中で、現在、既存のアイデンティティ管理ソリューションのユーザに多くの課題が生じています。残念ながら、数少ないながらも妥当なユーザ・エクスペリエンスを提供するソリューションでは、幅広いプロビジョニング、ロール管理およびガバナンス機能や、拡大したエンタープライズ全体でアイデンティティ管理をサポートするスケーラビリティが欠如しています。このため、幅広い機能か使い易さかのどちらかを選ばなければなりません。

CA Identity Suite は、現在の IAM テクノロジとビジネス・ユーザ間のギャップを埋めるユニークなソリューションです。このソリューションは、アイデンティティ管理およびガバナンス機能の統合スイートで、堅牢な機能と、便利で直観的に使用できるビジネス指向エクスペリエンスが盛り込まれています。このスイートを使用すると、アイデンティティ管理プロセスを簡略化し、ユーザ満足度を改善し、オンプレミスおよびクラウド・アプリケーションの両方をサポートし、消費者レベルのスケーラビリティを実現できます。そして、なによりも簡単にデプロイできます。

# 優れたアイデンティティ管理およびガバナンスの主な課題

この資料では、現在のオープン・エンタープライズにおける主要なアイデンティティ管理の課題の一部を紹介し、これらの課題がビジネスに及ぼす影響と、組織がこれらの課題に正しく対処できるようにする CA Identity Suite の機能について説明します。

以下に示した課題はそれぞれ、ビジネス的要素と IT 的要素の両方が関連します。従来、アイデンティティ・サービスのユーザ·エクスペリエンスでは、IT の視点が最優先され、面倒なインタフェースや満足度の低下につながっていました。しかし、現在の環境では、IT とビジネス・ユーザのギャップを埋め、アイデンティティ・サービスの利用を拡大し、ユーザ・エクスペリエンス全体を向上することが必要です。CA では、このような課題のビジネス要素と技術要素を追求します。

これらの課題には、広範囲な計画が必要であり、すべての投入計画に含める必要があります。

- **ユーザの採用** —ユーザ・エクスペリエンス全体を改善および簡略化し、ユーザによるアイデンティティ・プロセスの採用を拡大する
- **アクセス要求** —ユーザが必要とするアプリケーションへのアクセス権取得のプロセスを簡略化する
- **権限リスク管理** —権限ポリシー違反を防止する
- **アクセス認定** —マネージャの生産性を向上する
- **ユーザのアプリケーション・アクセス** —ユーザに主なアプリケーションにアクセスする便利な方法を提供する
- **リアルタイムのアイデンティティ分析** — 中核のアイデンティティ・サービスを効率化する
- **デプロイの課題** — 投資対効果を改善し、価値実現までの時間を短縮する

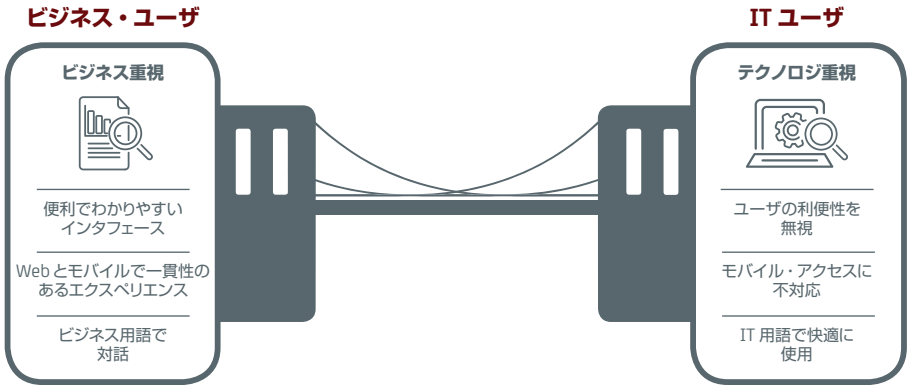
## 課題：ユーザによる採用

**「アイデンティティ機能の多くでユーザ・インタフェースが使いにくいことが、ユーザの不満になっています。そのために、社内でサービスをロールアウトしても、利用するユーザは大きく制限されてしまいます」**

正しいアイデンティティ管理のデプロイでは、通常、ユーザ・エクスペリエンスが IT に偏りがちであることが最大の課題の 1 つです。従来はそれでも問題になりませんでした。しかし、アイデンティティ管理が IT ユーザに限定されずに拡大する今、このアプローチはもはや有効ではありません。IT に慣れ親しんだユーザにはごく自然な用語やプロセスでも、大半のビジネス·ユーザにはわかりにくく、不満の元になります。その結果、アイデンティティ・プロセスの採用率が低下し、IT の負担が増加し、規制要件に適合できず、ユーザの不満が溜まってしまいます。ユーザは、簡単で使いやすい、すぐに使えるビジネス・アプリケーションを、自分の好みのデバイスで利用できることを求めています。ユーザを基本的なアイデンティティ・プロセスに取り込む必要がありますが、そのエクスペリエンスが簡単でわかりやすく、IT ユーザではなくビジネス・ユーザを重視していない限り、成果は望めません。

## CA Identity Suite ソリューション

CA Identity Suite は、現在の IAM テクノロジとビジネス・ユーザ間のギャップを埋めるユニークなソリューションです。このソリューションは、アイデンティティ管理およびガバナンス機能の統合スイートで、堅牢な機能と、便利で直観的に使用できるビジネス指向エクスペリエンスが盛り込まれています。CA Identity Suite のユーザ・エクスペリエンスによって、ビジネス・ユーザの生産性と満足度が向上することで、大企業における IAM ソリューションの価値が大幅に向上するだけでなく、IT 組織の管理作業が大幅に軽減されます。




このスイートが提供する多くの重要なユーザ・エクスペリエンスのメリットには、以下があります。

- ビジネス言語権限カタログ
- Web およびモバイル・アプリケーション・ダッシュボードとランチャー
- ワンストップ・ショップ - ビジネス・ユーザ向けに、すべてのアイデンティティ・サービスへの簡単な一元化アクセス
- アクセス要求および追跡にショッピング・カートのエクスペリエンス
- アクセス要求の追跡にソーシャル・ネットワークのエクスペリエンス
- プロアクティブなアドバイス・ツール
- ユーザがアイデンティティをいつでもどこでも管理できるようにするモバイル・アプリケーション

また、CA Identity Suite では、エグゼクティブ、セキュリティ・オフィサーおよびビジネス・パートナーなど、特定の役割固有のニーズに合わせたパーソナライズ・カスタム・ダッシュボードを簡単に作成できます。管理者は、ユーザの役割やアクセス可能なサービスに基づいて、インタフェースを構成できます。このスイートのインタフェースは、組織のブランド・ニーズに合わせてフルカスタマイズも可能です。これには、企業ロゴ、配色、フォント、選択した背景画像などが含まれます。ポータルには、ビジネスのアイデンティティが完璧に反映されます。

「外部アナリスト企業による調査では、調査対象顧客の 97% が Identity Suite のユーザ・エクスペリエンスは他社より優れていると報告しています」

出典 : TechValidate の調査

## 課題 : アクセス要求

**「ユーザが、仕事に必要なアプリケーションやシステムへのアクセスを簡単に要求できません。ビジネス・ユーザにとって、プロセスは面倒で、リソース名が複雑すぎます」**

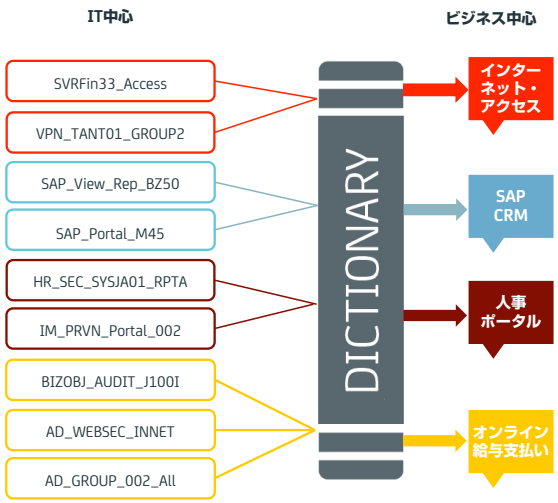
ユーザは、規制要件とのコンプライアンスを維持しながらも、必要なアプリケーションやデータに容易にすばやくアクセスする必要があります。しかし、アクセス要求システムは一般に、管理者だけが理解している一連の権限に基づいており、ユーザは、「IT 専門」用語の新しい言語をほとんどーから学ぶことを求められます。企業アイデンティティ・プロセスに関与するビジネス・ユーザが増えるにつれて、このようなわかりにくいエクスペリエンスでは採用の障害となり、満足度を低下させ、混乱したビジネス・ユーザに IT スタッフが対応せざるを得なくなります。

ビジネス・ユーザとのインタフェースには新しい手法が必要であり、アクセス要求の分野は、このような新しいアプローチが実現できるメリットの典型的な例です。また、IT にも、基本アクセス要求プロセスの自動化や、要求と承認の簡単な監査など、この分野に対するニーズがあります。つまり、IT の自動化ニーズを満たすと同時に、ビジネス・ユーザの使い勝手が良いことが必須の要素となります。

## CA Identity Suite ソリューション

CA Identity Suite は、わかりやすく簡単な「ショッピング・カート」のエクスペリエンスを提供し、アクセス要求プロセスを大幅に簡略化します。ユーザは、小売ショッピング・サイトによく似たプロセスのモデルによって、職務を実行するときに必要な役割（ロール）や権限をカートに入れたり、現在のアクセス特権を表示して以前の要求のステータスを確認したりできます。

ユーザ重視のビジネス権限カタログは、簡単でビジネス指向のエクスペリエンスを実現する CA Identity Suite の中核となります。このカタログは、「TSS_MNG_per_view」のようなわかりにくいリソース名を、「オンライン給与支払い」などのわかりやすい名前に変換し、ビジネス・ユーザが必要なリソースを簡単に見分けられるようにします。また、アクセスをさらに容易にするため、アプリケーションを論理的カテゴリにグループ化することもできます。たとえば、ビジネス･ユーザが一般に必要とする SAP アプリケーション、Oracle アップリケーションおよび SalesForce 機能を含む「SRM access」という名前のグループを作成し、ビジネス・ユーザにも見慣れた用語ですべてを定義できます。以下の図に、カタログが実行する IT 重視の用語とビジネス重視の用語の対応を示します。




Identity Suite には、アクセス要求プロセスを大幅に簡略化できるプロアクティブなアドバイス・ツールが含まれています。ユーザは推奨される役割や、類似する他のユーザのアクセス権を表示できます。このようなプロアクティブなアドバイスにより、ユーザは必要なアクセスに関する正しい要求を実行できます。また、要求したアクセスとそのアクセスの「リスク度」に基づいて、リスク・スコアも提供されます。そのため、ユーザは要求するアクセスについて適切な決定を下すことができます。

## 課題 : 権限リスク管理

**「セキュリティ・ポリシーに違反して、ユーザに誤って権限が割り当てられることがあります。このような違反は、発生する前に防止する必要があります」**

不適切なユーザ権限は、最近報道されたセキュリティ侵害の多くでその根本原因となっています。特に、特権ユーザには幅広い権限があるため、こうした原因で侵害が起きています。ただし、考え方はすべてのユーザで同じです。セキュリティ・ポリシーに違反する不適切な権限が承認される前に訂正し（「予防型管理」）、すでに承認されている不正な権限は中止する必要があります（「対応型管理」）。どちらも場合も、有効な管理手段が導入されていない限り、リスクが拡大し、コンプライアンス監査が難しくなります。

同様に、ポリシーの変更や以前に承認されたアクセスが、新しいポリシーに違反することがあります。通常のアクセス認定時に、このような違反をマネージャに警告し、アクセス権限を持つユーザの認定を解除できることが必要です。

## CA Identity Suite ソリューション

CA Identity Suite では、一連のビジネス・プロセス・ルール（BPR）を作成、実施および検証し、職務の分離や、ユーザ、役割および特権間の関係に関する他の論理制約条件を実行できるようにします。たとえば、BPR は、「X へのアクセスが許可されたユーザは、Y へのアクセスが許可されない」という制約条件や、「アクセス A を持つユーザのみが B を実行する許可権を持つ」という依存関係をモデル化することができます。そのため、このようなセキュリティ・ポリシーに違反するインスタンスは、発生する前に回避できます。

また、このスイートでは、矛盾する権限を要求すると警告を出力できます（前述の予防型管理）。要求されているアクセスと関連するポリシーに基づいて、リスク・スコアが割り当てられます。このリスク・スコアは、ユーザ、他の権限および該当するコンテキスト要素に基づきます。承認要求を実行すると、要求者にはリスク・レベルが示され、不正な要求の可能性が警告されます。同様に、承認者は、承認プロセス中にこのリスク・スコアを確認できるため、優れた可視性で高リスクのアクセスの承認を防止できます。

さらに、このスイートでは、すでに承認済みの不適切なアクセスを修復する対応型の管理も可能です。認定時に、アクセスに対するポリシー・チェックが実行され、このユーザがポリシーに違反する不適切なアクセス権を持っているかどうかが通知されます。各ユーザに明確に違反が示されるため、マネージャは、直ちに是正措置を取ることができます。どちらの型の管理も、不適切な権限が承認されたり、見逃されたりするリスクを大幅に低減します。

## 課題 : アクセスの認証

**「マネージャの生産性を向上し、コンプライアンス監査を容易にするには、簡単でわかりやすい認定が必要です」**

すでに説明したように、認定キャンペーンのタイプに合わせて、ユーザのアクセス情報を適切な言語と形式に自動で変換する機能は重要です。ビジネス・ユーザが直観的に理解できるアクセス名、それぞれのニーズに合わせた柔軟なワークフロー構成、各キャンペーンの追跡とステータスのわかりやすい表示が可能であれば、認定プログラムは成功したも同然です。

## CA Identity Suite ソリューション

CA Identity Suite の認定機能は、ビジネス権限カタログに基づきます。このカタログにより、マネージャは、各社員のアクセス権を容易に把握でき、各ユーザのアクセス権を簡単に承認、拒否または委譲できます。また、マネージャは、特定のアクセス権またはアクセス権の組み合わせが特にリスクが高いことをリスク・スコアで確認できます。このようなリスク評価を確認できれば、認定プロセスでは、「はい / いいえ」を提示するだけでなく、従来は把握が容易ではなかったリスクを特定できるようになります。

CA Identity Suite は、以下のように、さまざまな異なるタイプの認定キャンペーンを柔軟にサポートします。

- **エンティティの認定** - マネージャ、役割オーナーまたはリソース管理者が、選択したユーザ、役割、またはリソース・エンティティに関連するアクセス権を認定するときに使用します。
- **再認定** - 以前のキャンペーンに基づいて、認定プロセスを反復できるようにします。
- **差分** - 以前のキャンペーン以降に変更された権限だけに基づいて、認定キャンペーンを開始します。
- **自己認定** - マネージャまたはリソース・オーナーとは異なり、各ユーザが自分の特権を認定できるようにします。このタイプのキャンペーンは、データ・セキュリティ認定の法的要件の一部に適合する場合があります。

認定キャンペーンは、手間と時間がかかり、リスク低減作業のように明らかな効果が得られるものではありません。CA Identity Suite は、セキュリティおよびコンプライアンスの観点から、このプロセスの有効性を改善するだけでなく、マネージャに好まれる簡単でわかりやすいエクスペリエンスによってプロセスを実行します。

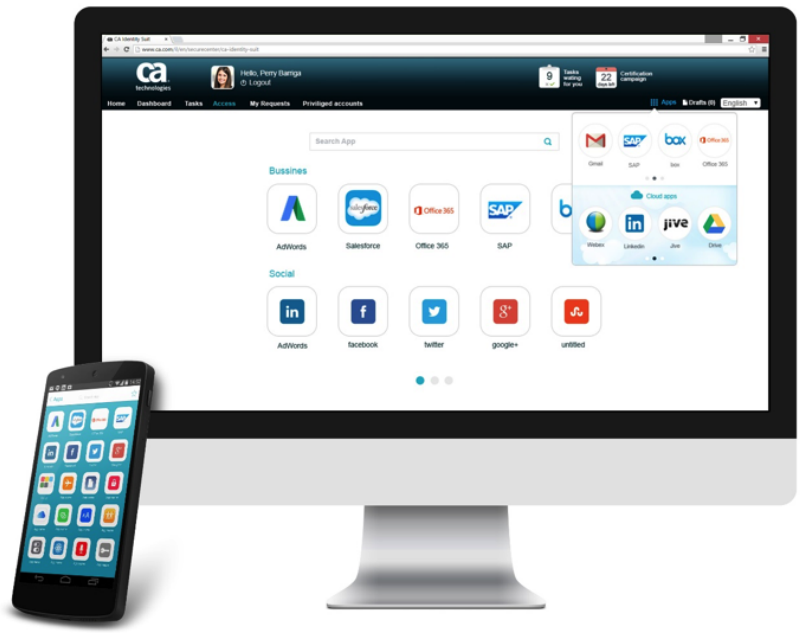
## 課題 : アプリケーションへの容易なアクセス

**「ユーザが、クラウドでもオンプレミスでも、すべてのアプリケーションに簡単にアクセスできることが必要ですが、アクセスできるのは正しいアクセス権を持つアプリケーションのみとします。また、ユーザのすべてのデバイスで簡単にアクセスできることも必要です」**

ユーザは、さまざまなアプリケーションの 1 つにアクセスするときに、面倒な手順に直面すると不満を募らせます。共通する不満は、複数のログインや、アプリケーションをすぐに起動できないことです。また、モバイル機能が向上し、ユーザがモバイル・デバイスの簡単なインタフェースに慣れてしまうと、不満と生産性の課題が拡大することがあります。必要なのは、各ユーザのアプリケーションにすばやく容易にアクセスできる便利な方法で、すべてのアプリケーションでシングル・サインオンを実現するだけでなく、各ユーザにアクセスを認証されたアプリケーションだけを許可することです。

## CA Identity Suite ソリューション

CA Identity Suite には、Web and Mobiel Application Launchpad が組み込まれており、ユーザは、1 つのダッシュボードを使用して、認証されたすべての Web/ クラウド / モバイル・アプリケーションにすばやく容易にアクセスできます。Launchpad は、どのデバイスからでもアクセスでき、拡張検索機能を利用できます。ユーザが CA Identity Portal にログインすると、すべての Web アプリケーションにワン・クリックでアクセスでき、ユーザがデスクトップでアクセスするすべてのアプリケーションは、CA Identity Portal Mobile からも利用できます。この Launchpad では、モバイルに対応した形式でモバイル Web アプリケーションへのシングル・サインオンが可能なため、モバイル・デバイスを利用する社員の生産性を維持できます。



## 課題 : SLA 遵守のためのプロセス効率化

**「アイデンティティ・プロセスの一部がスムーズに機能しないため、提供しているサービスレベルについて他のマネージャから苦情を受けています。しかし、修復のためにボトルネックを特定するのに十分な情報を入手することができません」**

アイデンティティ関連のプロセスは複雑である場合が多く、複数段階のワークフローが構成されることがあります。これらのプロセスを効率的に運用しないと、ユーザが予定通りに作業を終了できないなどの問題が発生し、システム全体が停滞して、サービスレベルの目標を達成できません。合意されたサービス目標に従ってアクセス認定などの基本的なプロセスを完了できなければ、効率が大幅に低下したり、監査で問題になったりする可能性があります。これらのプロセスの運用の詳細を適切に把握できなければ、このような問題の原因を特定することができず、ましてや迅速な修復は不可能です。

### CA Identity Suite ソリューション

CA Identity Suite では、多様なリアルタイム分析によって中核のアイデンティティ・プロセス運用を完全に把握して最適化することができます。これはボトルネックの特定に役立ち、重要な SLA を遵守できます。たとえば、次の図は、現在の SLA の過去 1 か月分を時間ベースで表示し、特定のプロセスの平均値、最大値、および最小値などの主要な数値を示しています。また、前月の毎日の新規要求の到着率、およびこれらの要求の処理（完了、拒否）の概要も示されています。このような機能によって、マネージャに提供される洞察が大幅に改善されるため、プロセスが最適化され、プロセスの状態も容易に把握できます。

## 課題：複雑なデプロイ

**「アイデンティティ管理ソリューションのデプロイは時間がかかり、複雑です。まず、ソフトウェアをインストールして設定するだけで何日もかかります。カスタム・コードが必要な上にワークフロー、ポリシー、UI も定義しなければならないため、基本的なユースケースを稼働させるには数週間かかることがあります」**

堅牢なアイデンティティ管理ソリューションのデプロイは、課題が多く、コストも嵩みます。基本機能 no 一部を稼働させるのに数週間かかることもあります。また、カスタム・アプリケーションのコネクタなどの要件によって、リソースが大量に消費され、時間が大幅に浪費される可能性があります。

### CA Identity Suite ソリューション

CA Identity Suite では以下の機能を使用して、稼働までに要する時間を大幅に短縮できます。

- **Virtual Appliance（vApp）：** vApp では、事前インストールおよび設定された仮想マシン・イメージが提供されるため、従来のインストールが不要になり、共通の仮想化プラットフォームを使用して本番構成で実行できます。仮想アプライアンスには強力なオペレーティング・システム、アプリケーション・サーバおよび CA Identity Suite ソフトウェアが組み込まれています。また、高可用性の設定、キャパシティの調整、ログの集約、プラットフォームのパッチ、ソフトウェアの更新などの DevOps 共通の手順の組み込みサポートも含まれています。

  アイデンティティ・サービスをデプロイする場合、サービス名を適切なマシン名にドラッグするだけで自動的にインストールされます。同じサービスを複数のマシンにドロップすると、高可用性（ロード・バランシング、フェイルオーバなど）のためのすべての通信メカニズムが自動的にインストールされます。時間がかかりミスの多い手作業の構成は必要ありません。時間は飛躍的に短縮されます。

  このアプローチによって、価値実現にかかる時間と TCO が大幅に減少し、同じチームと予算でより多くの成果を上げることができます。また、追加のライセンスを必要とせずにすべての中核のシステム・コンポーネントを自由にデプロイできるため、ソフトウェア・ライセンスのコストを年間で何千ドルも節約することができます。
- **Deployment Xpress（Depx）：** DepX は、アイデンティティ管理ソフトウェアのデプロイ方法を根本的に改善した機能です。ユーザ・オンボーディング、パスワード・リセット、アクセス認証、パートナー・オンボーディングなど、多くの組織が共通して必要とするユースケースのための事前設定されたシナリオで構成されています。各シナリオには、テンプレートのユーザ・インタフェース、ワークフロー、およびポリシー定義など、デプロイを簡略化するのに必要なすべての要素が含まれています。マネージャは必要なシナリオを選択し、ショッピング・カートに入れてチェック・アウトするだけです。それだけで、これらの主要な要素はすべて自動的に Identity Suite にロードされ、デプロイされます。これらの要素（インタフェースのコーポレートブランドなど）はカスタマイズ可能で、しかもカスタム・コードは必要ありません。これらのシナリオはデプロイ・プロセスをスピードアップし、通常のアイデンティティ・サービスのデプロイにかかる時間を大幅に短縮することができます。
- **その他の Xpress ツール：** Identity Suite には、デプロイ環境の管理プロセスを大幅に合理化する以下のような追加のツールが含まれています。
  - Connector Xpress では、自社開発アプリケーションのコネクタを作成するプロセスが簡略化され、OOTB コネクタのないシステムへも容易に接続できます。
  - Config Xpress では、ステージング環境間でコンポーネントをすばやく容易に移動でき、構成管理が簡略化され、機能テスト時間が短縮されます。
  - Policy Xpress では、独自の複雑なビジネス・プロセスを実行するポリシーを構成できます。通常はカスタム・コードが必要ですが、このウィザード式のツールでは何週間もプログラミングに費やすことなく、数時間でカスタム・ポリシーを構築できます。

# 主要機能

CA Identity Suite の主要な機能は以下のとおりです。

- セルフサービスのアイデンティティ・ポータル（「ワンストップ・ショップ」）— 資格データを一元管理し、アクセス要求の直観的なショッピング・カートを提供します。
- デプロイにかかる時間が数日から数分と、大幅に短縮されます。
- ビジネス用語による権限カタログ — ビジネス・ユーザでもアクセス要求や権限認定を容易に理解できます。
- プロアクティブな分析機能 — ポリシー違反を防止するため、ビジネス・ユーザに通知およびアラート出力します。
- 幅広いオンプレミス・アプリケーション、SaaS サービス、および接続されていないシステムへのユーザ・プロビジョニングが可能です。
- ユーザ・セルフサービス — ユーザが、各自の情報を管理できるようにすることで、IT の負担を軽減します。
- Deployment Xpress — 事前定義のユースケース・テンプレートによって、最初のデプロイと継続的な管理が大幅に簡略化されます。
- カスタム・コードなしのカスタマイズ — ConfigXpress、PolicyXpress、ConnectorXpress などのパワフルな機能により、カスタム・コードを開発しなくても、アイデンティティ管理インフラストラクチャをカスタマイズできます。
- 特権クリーンアップ — 既存システムの権限を確認し、過剰または不要な特権を強調表示します。
- 特許取得の高度な分析エンジンによる役割モデル化 — 膨大な量のユーザおよび権限情報を効率よく分類し、使用できる役割を検索できます。

**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。



CS200-230014_1016