okta

# ADFS から Okta に移行するメリット

**Okta Japan 株式会社**
〒 150-0002 東京都渋谷区渋谷 2 丁目 24 ー 12
渋谷スクランブルスクエア 38 階

Marketing-Japan@okta.com

## シングルサインオン導入の課題

クラウドアプリケーションの普及率はここ数年で急増しています。中でも、Salesforce.com、Box、Office 365 などのクラウドアプリケーションは全社的な導入が進んでいます。そのため、多くの企業が、クラウドアプリケーションに関するポリシーを策定するか、近いうちに策定を予定しています。

現在、多くの企業は、ユーザーがクラウドアプリケーションや Web アプリケーションで個々に認証を行う手間を省いて、すべてのアプリケーションに簡単にアクセスできるように、シングルサインオン（SSO）の導入を検討しています。SSO を実装するには、すべてのクラウドアプリケーションを、信頼できる唯一の情報源と連携させる必要があります。多くの企業でその情報源となるのが Microsoft Active Directory です。そのため、Active Directory を中心とした SSO ソリューションとして、同じ Microsoft 社製品である Active Directory フェデレーションサービス（ADFS）が最適だと考えがちです。

しかし、Active Directory の統合ソリューションはどれも同じではありません。ADFS の導入を検討する際は、SSO の実装方法についてあらゆる面から調査を行うことをお勧めします。ADFS のライセンスは無料ですが、セットアップ、継続的なサポート、ハードウェアなど、いくつかの隠れた関連コストが発生します。また、統合的なアイデンティティ管理ソリューションを構築するには、プロビジョニング、モバイルデバイス向けのコンテキストに応じたアクセス管理、一元的なレポートの作成、現在企業で使用されるさまざまなアプリケーションとの事前統合のサポートなどの機能も考慮する必要があります。

このホワイトペーパーでは、Active Directory の統合と SSO の導入を成功に導くための重要ポイント、およびオンプレミスの ADFS から 100% クラウドベースの Okta の統合サービスに移行するメリットについて説明します。

## SSO ソリューションの導入を成功に導くための重要なポイント

SSO の実装方法を決める際には、数多くの検討事項があります。そのため、実装を成功に導くための重要なポイントを抑えておくと調査が円滑に進みます。これらの多くは、最初はあまり重要に思えないかもしれませんが、将来、企業が成長して導入するアプリケーションが増えたときに役立ちます。

- **Active Directory との統合**
  Active Directory を使用している場合は、SSO の対象となるクラウドアプリケーションと Active Directory を同期させて、既存の資産を活用できる SSO ソリューションが最適です。
- **アプリケーションの統合と将来的な対応**
  ソリューションを全社的に導入する場合は、現在使用しているアプリケーションだけでなく、今後追加するアプリケーションにも対応できるかどうかを確認することが重要です。現時点で統合したいクラウドアプリケーションが 1 つか 2 つしかなくても、長期的には増えていくはずです。アプリケーションの数が増えた場合、時間がたつにつれてそれぞれのアプリケーションの設定要件が変わる可能性があり、IT 管理者はバージョンアップのたびに個々のアプリケーションに対応する必要が出てきます。その労力は人的にも予算的にも大きな負担になります。
- **高可用性**
  SSO に関するダウンタイムはユーザーのダウンタイムに直結します。ダウンタイムは計画的なものもあれば、予期せず生じることもあります。SSO サービスとそのサポート機能は、アプリケーションの設定を変更する時間を含めて常に稼働状態を保てるよう、十分な柔軟性を備えている必要があります。

  社内サーバーに問題が発生した場合でもアプリケーションの変更時であっても、ダウンタイムが発生すれば、エンドユーザーの生産性が低下し、ビジネス全体に悪影響を及ぼします。

- **ユーザーとクラウドアプリケーションのプロビジョニング**
  プロビジョニングでは、アプリケーションやその他のリソースへのアクセスを設定、更新、削除します。IT 管理者が1回のプロビジョニングまたはプロビジョニング解除に費やす時間は平均30分ほどです。このほかにも、ヘルプデスクに対するパスワードリセット要求への対応や、従業員が使用するすべてのデバイスでのユーザー設定を行う必要があります。プロビジョニングとユーザーのライフサイクル管理を自動化できれば、IT 部門とユーザー部門のどちらも貴重な時間を節約して満足度を高めることができます。
- **モバイルデバイスでのコンテキストに応じたアクセス管理**
  モバイルデバイスの活用範囲が広がれば、さらなる生産性の向上が見込めます。しかし、そのためにはセキュリティの問題を解決しなければなりません。その点で、SSO ソリューションを選ぶときは、既存のモバイルデバイス管理（MDM）ソリューションと統合できるかどうかが重要になります。また、管理対象外のデバイスからアプリケーションやデータにアクセスできないようにポリシーを設定できることや、セキュリティを強化するためにモバイルデバイスとその他の要素を使った多要素認証がサポートされていることも大切です。
- **効率的なドメイン統合**
  合併や買収によって異なる企業のリソースを統合する必要が生じた場合は、ドメイン、ツール、セキュリティ体制の統合が大きな課題になります。最新のクラウドベース SSO ソリューションなら、このプロセスを迅速かつ簡単に行うことができます。
- **ログとレポート**
  多くの規制当局（SOX、HIPAA など）は、従業員がどのアプリケーションやシステムにアクセスしているかまたはアクセスしたかを可視化するなど、ユーザーの監査証跡を記録することを企業に求めています。IT 部門は、退職した従業員に対するアプリケーションのプロビジョニング解除について詳細に報告する必要があります。優れた SSO ソリューションを使用すれば、企業や業界に求められる報告要件にすばやく対応するための使用状況データを収集できます。

## SSO ソリューションとしての Active Directory フェデレーションサービスの利用

Active Directory によるアイデンティティ管理の対象をファイアウォール外のクラウドアプリケーションに拡大する方法としてまず候補に挙がるのは、Microsoft Active Directory フェデレーションサービス（ADFS）です。ADFS は無料で利用できますが、複数のハードウェアコンポーネントと追加の Microsoft 社製ソフトウェアの導入、および大規模な設定とメンテナンスが必要になります。ADFS で SSO を実装する場合、SSO ソリューションとしての最小要件を満たすだけでも、複雑な設定要件に対応し、ほかのリソースとの依存関係を解決する必要があります。

### ADFS のコンポーネント

ADFS で SSO を実装する場合、その基本となるすべてのコンポーネントを理解することが重要です。ADFS 自体は、「ADFS サーバー」、ADFS サーバーファームと外部アプリケーション間にインストールする「フェデレーションサービスプロキシ」、「ADFS 構成データベース」[1]の3つのコンポーネントで構成されます。

ADFS はもともと、Windows Server の追加機能であるツールキットとして開発されたものであり、SSO 向けのエンドツーエンドソリューションではありません。ツールキットには柔軟性がありますが、総合的なソリューションを構築するには大量のサポート機能を追加する必要があります。IT 部門はその負担をすべて担わなければなりません。

[1] SQL または Windows Internal Database（WID）

対象となるクラウドアプリケーションへの SSO 接続を確認、設定、維持するには、ADFS コンポーネントごとにカスタム開発を行い、継続的に管理する必要があります。そのため、規模を拡大して多数のアプリケーションに対応するのは容易ではありません。

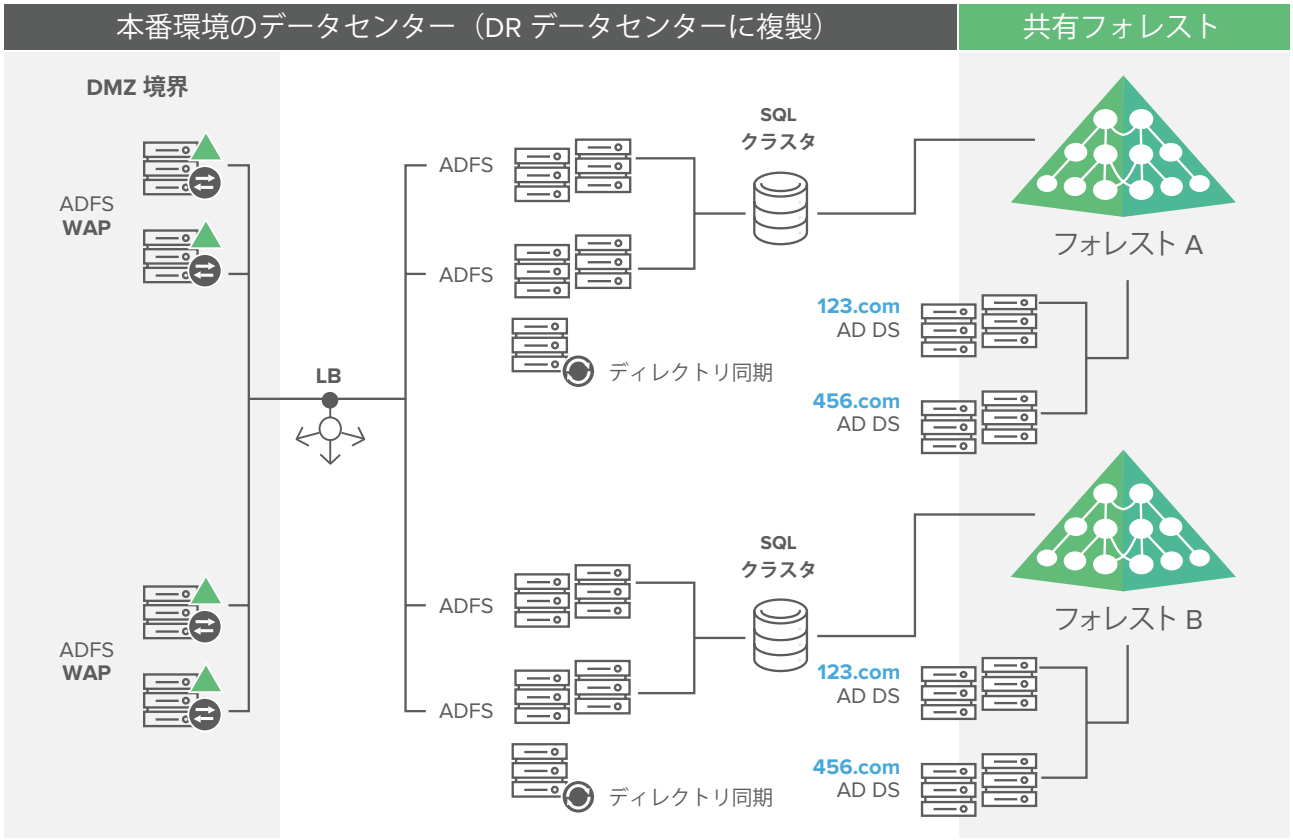


図1: ADFS と Active Directory の統合には複雑なオンプレミスインフラが必要

**ADFS のカスタマイズ**

ADFS で SSO を実装するには、認証を有効にするクラウドアプリケーションごとに、ユーザー認証、アクセス許可、クレームルール生成のためのポリシーを設定する必要があります。そのためには、ADFS サービスにバインドした有効な SSL 証明書を使って、ADFS と各アプリケーション間に信頼関係を確立する必要があります。テスト目的では自己署名証明書でも問題ありませんが、本番環境では第三者機関が署名した証明書が求められます。信頼関係が確立されたら、クラウドアプリケーションで認証を行うためのクレームルールを生成します。以前は、各アプリケーションのクレームルールを ADFS 管理者が手動で記述する必要がありましたが、ADFS 2016 では多少改善され、新しいアクセス制御ポリシーテンプレートを使用できるようになりました。

将来、各アプリケーションのルールが変わったときは、SSO 統合が無効になることがあります。そのため、アプリケーションの変更に常に注意を払い、必要に応じてアクセス制御ポリシーを更新する必要があります。

ADFS インフラを構築して、各クラウドアプリケーションに適切なクレームルールを生成しても、まだ終わりではありません。ユーザーが実際に SSO を使ってこれらのアプリケーションにアクセスするための方法を考える必要があります。最も一般的なのは、Azure Active Directory を使用する方法です。

### シングルサインオンとプロビジョニング

ADFS を使用する場合、SSO の対象となるアプリケーションが現時点で1つであっても、数年後にそれが５つか６つほどに増えたときは、それぞれ手動で設定を行う必要があります。また、各アプリケーションと社内ネットワークおよびインフラとの接続を維持するには、定期的なメンテナンスも必要になります。つまり、導入コストは比較的安価に思えても、導入後にアプリケーションを追加するたびにかかる労力を考えると、スケールメリットは期待できません。

Active Directory の ADFS を使ってアプリケーションの SSO を統合するには、Azure Active Directory に各ユーザーのレプリカを追加する必要があります。そのためには、Microsoft 社が提供する Azure Active Directory 向けのクラウドベースのアイデンティティおよびアクセス管理ソリューションである Microsoft Enterprise Mobility + Security（EMS）のライセンスが必要です。

さらに、ADFS でプロビジョニングとライフサイクル管理を行うには、Microsoft Identity Manager（MIM、旧称 Forefront Identity Manager）の購入と設定も必要です。

## ADFS から Okta に移行するメリット

ADFS をすでに導入しており、規模を拡大して対応するクラウドアプリケーションを増やし、機能も強化ししたい場合は、Okta を追加することでさまざまなメリットが得られます。

### シンプルな管理

Okta は、ADFS の機能を参考にしながら、その中で特に優れた機能を拡張性の高いクラウドプラットフォーム上に実装しています。導入の詳細やサービスの可用性確保は Okta が担い、オンプレミスの大規模かつ複雑なアイデンティティフェデレーションインフラより優れた信頼性を提供します。

Okta は、ユーザーがいつ、どこでも、どのデバイスからでもアプリケーションに安全にアクセスできるように設計された、総合的なアイデンティティ管理サービスです。

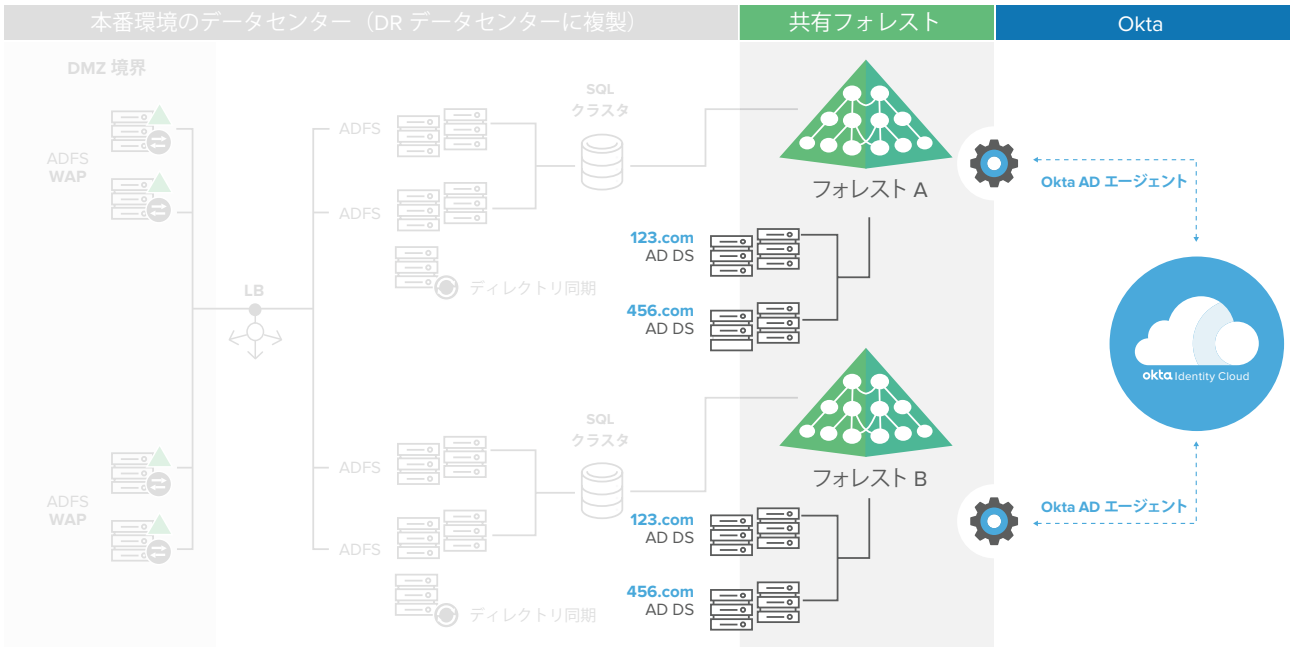


図2: 既存の Active Directory インフラと安全に統合できる Okta の軽量 AD エージェントとクラウドプラットフォーム

### Active Directory との統合

Okta は、既存の Active Directory インフラと安全に統合できる、100% オンデマンド型のクラウドプラットフォームです。

Okta のコアサービスは、Active Directory エージェントをローカルにインストールするマルチテナント方式のソリューションで、アプライアンスやサーバーを別途購入したり、メンテナンスしたりする必要はありません。Okta の軽量エージェントは、HTTPS 経由でセキュリティ保護されたアウトバウンド接続のみを行うため、ファイアウォールの設定を変更する必要もありません。Okta でクラウドアプリケーションのユーザー認証が完了した後は、Okta は関与せず、その後のトラフィックはすべてユーザーとアプリケーション間でやり取りされます。

Okta では、認証、プロビジョニング、プロビジョニング解除、ディレクトリ同期、AD パスワード管理の委任がサポートされます。Active Directory と Okta のいずれかで変更を行うと、変更内容が増分で同期されます。また、Okta のユニバーサルディレクトリでユーザーを無効にすると、Active Directory 内のそのユーザーの記録もただちに無効になります。

### 簡単なアプリケーション統合によるシングルサインオン

Okta インテグレーションネットワークには、事前統合済みのさまざまなビジネス/個人向けアプリケーション、インフラ、デバイスが用意されています。これを主要アプリケーションポータルとして使用すれば、エンドユーザーは自身にプロビジョニングされたアプリケーションに簡単にアクセスできます。図 3 に示すように、Okta は総合的なクラウドプラットフォームであるため、Active Directory からの SSO、SSO のフェデレーション、密接なアプリケーション統合をすばやく実装できます。

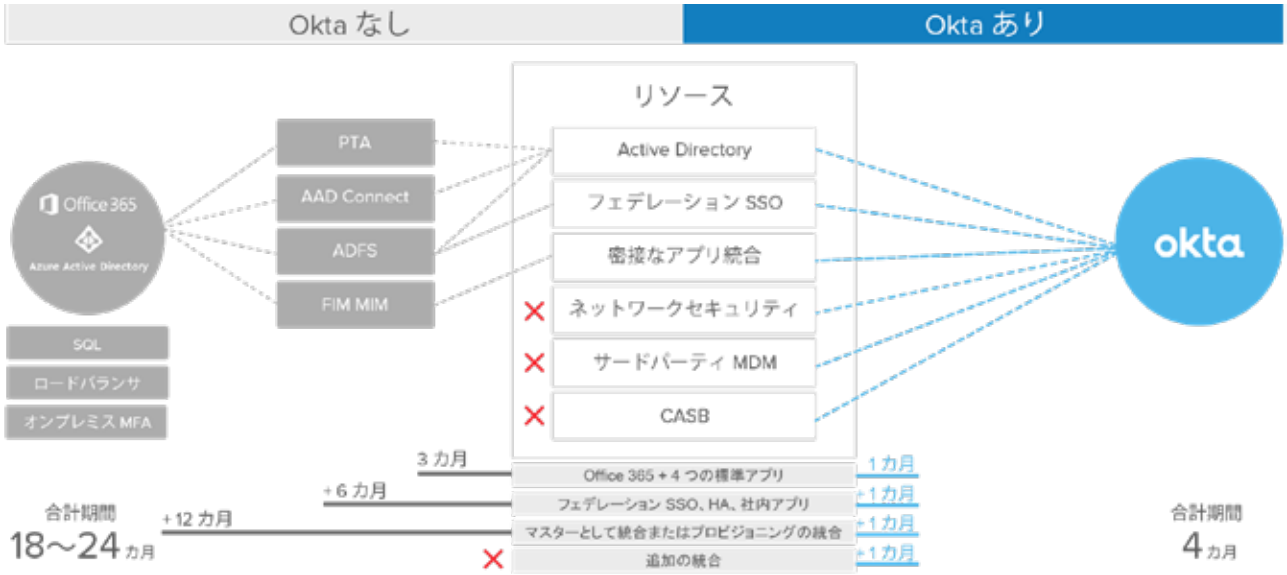


図 3: Okta によって SSO、プロビジョニング、ほかのアプリケーションやサービスとの統合をすばやく簡単に実現

### 高可用性

SSO ソリューションのサービス停止は、たとえ計画メンテナンスであっても避けたいものです。Okta のクラウドプラットフォームは、99.9% の稼働率と計画ダウンタイム 0 を保証しています。[2] Okta のクラウドアーキテクチャは、100% マルチテナント方式のステートレス型で、複数のアベイラビリティゾーンと地域を拠点として高度に冗長化されています。クラウドアプリケーションの統合については Okta が継続的に管理および監視しているため、アプリケーションの変更に気を使う必要もありません。従業員、パートナー、顧客に、ビジネスクリティカルなアプリケーションへのアクセスを途切れることなく提供できます。

[2] https://www.okta.com/a-secure-reliable-service-you-can-trust/

### ユーザーとアプリケーションのプロビジョニング

Okta のグループベースの管理システムでは、Active Directory で定義されたジョブロールに基づいて、ユーザーに一連のアプリケーションをプロビジョニングできます。社内で従業員のロールが変更されたときは、Active Directory での従業員レコードの変更内容に基づいて、その従業員がアクセスできるアプリケーションが Okta 内で自動的に更新されます。従業員が退職したときは、Active Directory でのユーザーのステータス変更が Okta で検出され、すべてのアクセスが自動的に削除されます。

Okta には、80 を超える優れた SaaS アプリケーションの事前統合済みのプロビジョニングが用意されています。また、Workday や SuccessFactors などの人事管理システムに登録されたアイデンティティ属性を使って、ユーザーのアイデンティティを学習およびプロビジョニングすることもできます。

### デバイスごとのコンテキストに応じたアクセス管理

Okta のコンテキストに応じたアクセス管理では、ユーザーとデバイスに対する社内リソースへのアクセス許可を管理することによってリスクを低減できます。アダプティブ多要素認証と Device Trust 登録ポリシーを組み合わせて、承認されたユーザーとデバイスのみに社内のアプリケーションやデータへのアクセスを許可できます。Okta では、幅広いアプリケーションと一般的に使用されるデバイスに詳細なアクセス制御を適用できます。Okta アダプティブ多要素認証では、管理者が、アクセスを許可するか、ステップアップ認証を要求するか、アクセスを拒否するか、ユーザーのアクセス範囲を特定のアプリケーションに制限するかを選択できます。その判断基準には、パスワード、セキュリティの質問、トークンだけでなく、ユーザー、接続元のネットワークや国、ユーザーが使用しているデバイスも含めることができます。

### ADFS 向けの多要素認証

特定のアプリケーションのアイデンティティプロバイダ（IdP）として ADFS を使い続ける場合でも、オンプレミスの多要素認証インフラを追加せずに、Okta の多要素認証機能を使って強力な認証手段を提供できます。[3]

### 効率的なドメイン統合

Okta のユニバーサルディレクトリでは、無制限数のディレクトリを接続して、レガシーデータを Web に集約できます。AD フォレストの信頼関係を設定したり、ファイアウォールのポートを開いたりする必要はありません。たとえば、社内に複数の AD ドメインがあり、信頼されているものと信頼されていないものが混在している場合、Okta なら、ファイアウォールの内側に AD エージェント（内蔵の高可用性設定を使用する場合は 2 つ）をインストールするだけで、Okta の管理コンソールからすべてのディレクトリを一元管理できます。

### ログとレポート

Okta の統合ダッシュボードでは、IT 管理者が簡単にユーザー、アクセス、アプリケーションのステータスを確認して、コンプライアンスレポートを生成できます。

### 常時アクセス可能で常に最新

Okta は、お客様の利便性を重視して、製品の新しいアップデートをダウンタイムなしで定期的に適用しています。エンドユーザーは、主要アプリケーションポータルから、自身にプロビジョニングされたアプリケーションにアクセスできます。ADFS で同様のソリューションを実現しようとすると、自社で開発を行うか開発会社に依頼する必要があり、追加コストが発生します。

[3] https://help.okta.com/en/prod/Content/Topics/integrations/adfs-okta-int.htm

Okta の SaaS（Software as a Service）プラットフォームなら、ADFS だけでなく、SSO ソリューションの実装に必要なその他の Microsoft 社製ツールのすべてのメリットを、単一のクラウドベースプラットフォーム上で利用できます。

**コスト面でのメリット**

図 4 に示すように、ADFS では、ハードウェアとソフトウェアの導入、メンテナンス、カスタム統合、仮想マシンのライセンス、Enterprise Mobility + Security（EMS）と Microsoft Identity Manager（MIM）ソフトウェアなど、さまざまなコストが発生します。また、導入と稼働に費やす数カ月分の生産性が失われることによって機会コストも発生します。

EMS が無料でバンドルされていても、導入、メンテナンス、カスタム統合のコストはかかります。また、ADFS を導入済みの場合、高度な機能を追加するには、MIM と EMS の導入コストとライセンスコストがかかることがあります。

Okta の最小カスタマイズ要件とライセンス管理機能なら、総所有コスト（TCO）を最大 60% 節約できます。新しいアプリケーションを追加してもコストが増えることはないため、長期的にもコスト効果が高く、将来、社内インフラにクラウドアプリケーションを安心して追加できます。

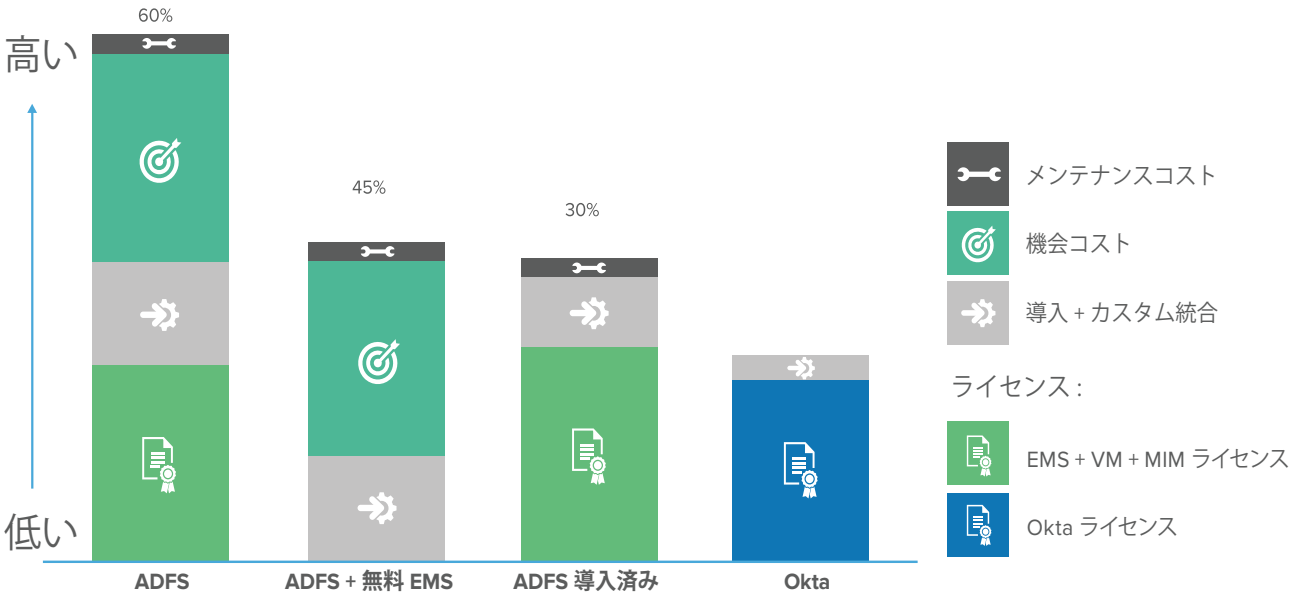


図 4: 1 つのアプリケーションを統合する場合の ADFS とのコスト比較

## Okta と ADFS の概要比較

| 機能 | Okta のアプローチ | ADFS のアプローチ |
|---|---|---|
| アプリケーション統合 | • 数千の事前統合済みアプリケーション<br>• アプリケーション統合の設定とメンテナンスが不要 | • 統合ごとに設定とメンテナンスが必要 |
| 可用性 | • 100% マルチテナント方式のソリューション<br>• ダウンタイムなしで常時アクセス可能<br>• AD インフラの変更は不要 | • 導入、設定、管理が必要<br>• アプリケーションの変更に応じてメンテナンスが必要<br>• 可用性を確保するための冗長化が必要<br>• 複数のサーバーが必要（導入とフェールオーバー） |
| アクセスとユーザー管理 | • すべてのアプリケーションのアクセスを制御<br>• ユーザー名の形式が異なっても簡単にマッピング<br>• ユーザーとアクセス権を簡単に追加、変更、削除<br>• AD のセキュリティグループから直接インポート<br>• すべての統合済みアプリケーションで自動設定 | • カスタム AD 属性の作成と管理が必要<br>• アプリケーションごとに変更が必要<br>• ユーザーのインポートや照合機能なし |
| レポート | • メトリクスダッシュボードでユーザーとアプリケーションの全体的な健全性を確認<br>• コンプライアンス向けのユーザーレポートに簡単にアクセス | 該当なし |

## まずは無償試用版で

Okta なら、簡単に導入して、クラウドアプリケーションを安全に拡張できます。まずは www.okta.com/freetrial にアクセスして、無償試用版をお試しください。

### Okta について

Okta は、エンタープライズのためのアイデンティティ管理ソリューションを提供する、業界トップの独立系プロバイダです。Okta Identity Cloud は、世界各地にある多くの大規模企業のユーザーをつなぎ、そのセキュリティを確保しています。さらに、企業をパートナー、サプライヤー、顧客と安全につないでいます。Okta Identity Cloud は、5,000 以上のアプリケーションとの密接な統合により、あらゆるデバイスからの簡単かつ安全なアクセスを実現します。

20th Century Fox、Adobe、Dish Networks、Experian、Flex、LinkedIn、News Corp の各社を始めとする多くのお客様が、Okta のソリューションを活用して業務の効率化、収益拡大、セキュリティの確保を実現しています。Okta は、重要な業務の遂行に必要なテクノロジーを安全かつ簡単に活用できるようにすることで、お客様のミッション達成を支援します。

さらに詳しい情報については、Okta の Web サイトをご覧ください：www.okta.com


okta