

SafeNet Trusted Access

ワンタイムパスワードとシングルサインオン クラウドサービス



企業におけるクラウド導入

クラウドベースのアプリケーションは、企業における生産性、運用、インフラのニーズを満たす上で極めて重要な役割を果たします。しかし、クラウドアプリケーションの使用が増大するにつれて、ユーザーのクラウドアクセス用 ID は増加し、管理負担も増していきます。新しいクラウドサービスが組織に追加されるたびに、クラウドアクセスの統一した可視性が実現しにくくなり、コンプライアンスリスクも増大します。ユーザーは覚えきれないほどのユーザー名とパスワードを記憶するのに苦労し、一方でパスワードリセットを必要とするヘルプデスクコールは山のように積み上がります。クラウドアプリケーションは、初期設定では脆弱な静的パスワードでしか保護されていないため、データ漏洩のリスクを高めています。

SafeNet Trusted Access – クラウドアクセスをスマートに管理

SafeNet Trusted Access は、こうした課題に対処し、クラウドアプリケーションのより効果的なユーザー管理を可能にします。シングルサインオンの利便性ときめ細かなアクセスポリシーを組み合わせることで、アクセス制御が強化されるだけでなく、日常的に過剰な数のパスワードを作成、記憶、更新、リセットし続けねばならない多くのユーザーが経験する蓄積疲労、すなわちパスワード疲れを防止できます。ID の認証、アクセスポリシーの適用、スマートシングルサインオンの利用によって、多数のクラウドアプリケーションへのセキュアで便利なアクセスが実現し、また 1 つのコンソールからアクセス制御を一元的に定義し適用できるため、管理オーバーヘッドも減少します。

迅速かつ簡単な設定を提供する SafeNet Trusted Access は、クラウドの導入を簡素化し、可視性とコンプライアンスを向上させ、クラウドから提供される簡易ワークフローによって拡張性を提供します。

柔軟でカスタマイズ可能な認証とアクセス制御により、SafeNet Trusted Access はエンドユーザーの不満や複雑さを解消し、1 つの ID ですべてのクラウドアプリケーションにアクセスすることを可能にします。

SafeNet Trusted Access の利点

- **スマートシングルサインオン**が、定義されたポリシーに基づいてインテリジェントに SSO を適用します。これにより、ユーザーは一度の認証で許可されたすべてのクラウドアプリケーションにアクセスできます。
- **IT 管理者向けのシングルペイン**により、すべてのクラウドアプリケーションの一元的なアクセス制御を提供します。
- **セキュリティの最適化と漏洩リスクの軽減**が、きめ細かなアクセスポリシーを通じて実現し、必要な場合にのみ認証を強化できます。
- **完全な可視性**により、クラウドアクセス状況が把握できるため、コンプライアンス準拠が容易になり、活用されていないクラウドアプリケーションライセンスも識別できます。
- **セキュアな外部アクセス**を実現し、ビジネスパートナーや協力会社にスマートシングルサインオンを利用した安全なアクセスを提供します。
- **クラウドの効率性**が、as-a-service (アズ・ア・サービス) として提供されるアクセス管理によって向上します。

動作のしくみ

ユーザーがクラウドアプリケーションにログインすると、SafeNet Trusted Access は以下を行います。

1. ユーザーの ID を検証する
2. どのアクセスポリシーを適用すべきかを評価する
3. スマートシングルサインオンで適切な認証レベルを適用する

SafeNet Trusted Accessのコア機能

SafeNet Trusted Accessは、企業に4つのコア機能を提供します。

スマートシングルサインオン

スマートシングルサインオンを使用すると、1つのIDですべてのクラウドアプリケーションにログインできるため、パスワード疲れ、不満の蓄積、パスワードリセット、停止時間を排除できます。SafeNet Trusted Accessは、同じSSOセッションの以前の認証と各アクセスに適用される特定のポリシー要件に基づいて、ユーザーのログイン要求を処理しSSOをインテリジェントに適用します。これにより、ユーザーが一度の認証ですべてのクラウドアプリケーションへのアクセスを可能とし、また追加の認証をポリシーで設定することができます。

シナリオベースのアクセスポリシー

アクセスポリシー設定では、どのユーザーがどの認証方式を使用してどのアプリケーションにアクセスできるかをきめ細かく定義することができます。アクセスポリシーは、セキュリティの考慮事項とユーザビリティへの期待のバランスを取るように定義できます。たとえば、時間管理アプリケーションでは最小のアクセス制御で十分ですが、企業VPNではより厳格なアクセスポリシーが必要です。

データに基づく最適化

SafeNet Trusted Accessは、アクセスに関するデータログを提供するため、アクセスポリシーをそれに基づいて調整できます。日常のアクセスイベント、アプリケーションごとのアクセスアクティビティ、ポリシーごとのアクセスアクティビティにより、アクセスポリシーが緩すぎたり厳しすぎたりしないようにし、活用されていないクラウドアプリケーションを識別することもできます。

広範な認証オプション

コンテキストベースの認証は、コンテキストパラメータに基づきログイン操作が安全かどうかを判断し、ユーザーの利便性を向上させます。ログイン操作が安全であるとみなされた場合、ユーザーは即時アクセスが許可されます。安全でないと疑われる場合には、追加の認証を求めるように設定できます。

容易なアプリケーション管理

SafeNet Trusted Accessは、Salesforce、AWS、Office 365などの主要なクラウドアプリケーションに簡単に接続できるように、あらかじめ定義済みの統合テンプレートを提供します。

なぜSafeNet Trusted Accessなのか？

デジタルセキュリティ分野のリーダーが構築

SafeNet Trusted Accessは、革新的なアクセス管理機能を市場最高の認証システムに追加します。数々の賞を受賞したジェムアルトのSafeNet Authentication Serviceの進化形となるSafeNet Trusted Accessは、クラウドで提供される自動化された強力な認証に、スマートシングルサインオンときめ細かなアクセスポリシーを追加します。

クラウドの効率性

SafeNet Trusted Accessは、直観的なアクセス管理と、クラウドで提供される強力な認証を組み合わせることで、現在のインフラをそのまま活用でき、ハードウェアやソフトウェアの自社での維持及び運用管理は不要です。

ステップアップ認証方式の幅広い選択

SafeNet Trusted Accessは、ステップアップ認証方式とフォームファクタ(認証手段)の幅広い選択をサポートしています。

- プッシュOTP
- アプリケーションOTP
- ハードウェアOTP
- パターンベース(マトリクス)認証
- メールやSMSによるアウトオブバンド

- パスワード
- Kerberos
- PKI 証明書
- Google Authenticator
- パスワードレス認証
- バイオメトリクス
- ボイス
- サードパーティ

企業向けの設計

シナリオベースのアクセスポリシーは、従業員やビジネスパートナーによる主要なクラウドアプリケーションへのセキュアなアクセスなど、企業用途に特化して設計されています。直観的な自動化された管理により、セキュリティ担当者やITチームの日常のオーバーヘッドが軽減されます。

SafeNetアクセス管理と認証ソリューションについて

タレスの業界をリードするアクセス管理と認証ソリューションは、アクセスを一元管理することで、エンタープライズIT、Webおよびクラウドベースのアプリケーションを保護します。ポリシーベースのアクセス管理とSSO、そして多様な認証方式のサポートにより、企業は情報漏えいを効果的に防止し、クラウドに安全に移行し、規制遵守を簡素化します。

主要アプリケーションのアクセス管理



タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。

その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

> cpl.thalesgroup.com <

お問い合わせ先 - cpl.jp.sales@thalesgroup.com

すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-usをご覧ください。