Product Brief

THALES
CYBERSECURITY



SafeNet Trusted Access

従業員を保護し、企業のセキュリティを強化

cpl.thalesgroup.com

THALES

CYBERSECURITY

世界でも有数となる高度な技術力と生産性を誇るクラウドファースト企業は、現代のワークフォースにおける新たな基準を示しています。 世界中の従業員が、クラウドベースのアプリケーションやサービスに常時アクセスする必要がある一方で、セキュリティチームにとっては、最も機密性の高いデータやアプリケーションを保護するという課題も生じています。加えて、「セキュアアクセスはユーザーの負担を増大させる」との誤解が広がっているため、組織のセキュリティ担当者は従業員認証に新たなアプローチを導入することについて、周囲の理解や同意が得られにくくなっています。

クラウドネイティブな企業が妥協する必要はありません。適切なソリューションを導入すれば、業務を中断することなくアプリケーションやデータへのアクセスを保護し、組織として確約したセキュリティ基準を維持しつつ、ストレスのないユーザー体験を実現することができます。

従来型の認証とアクセス管理は現代の脅威環境に応じた進化を遂げていない

一律のMFAが生む大きなセキュリティギャップ

アプリケーションの機密性やユーザーの職務、コンプライアンスの要件などは多種多様であるため、一律のMFAポリシーを適用するとユーザーの利用率が低下するほか、場合によっては過度な負担やセキュリティ上の抜けが生じる原因となります。

ハイブリッドおよびリモートワークがもたらすアクセスの複雑化

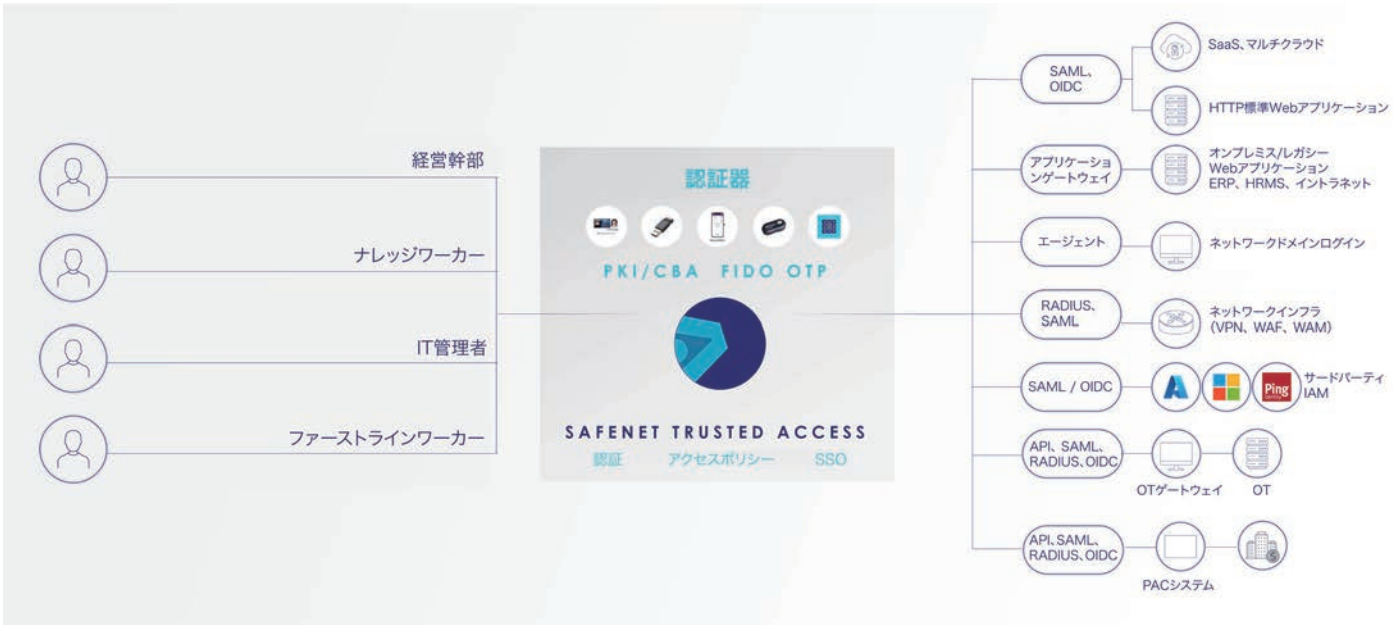
多くのオンプレミスアクセス管理ツールは、現代のニーズに対応できるまで進化しておらず、リモート化やハイブリッド化が進む従業員に対して適切なアクセス環境を提供できていません。

規制当局による監視の強化

PCI DSS、NIS 2、ISO 27001などの標準規格は、個人を特定できる情報（PII）およびその他の保護対象データへのアクセスに対し、最小権限の原則とMFAポリシーを適用することを義務付けていますが、旧来のソリューションはこれらの要件を効果的に満たしていないため、本来ならば回避できる金銭的ペナルティにつながる可能性があります。

狙われやすいパスワードベースのログイン

攻撃者は今もなお、ログイン認証情報の窃取という実証済みの手法を用いています。たった一つの認証情報を入手するだけで、複数のシステム間を水平移動し、極めて利用価値の高いデータにアクセスできるようになります。



SafeNet Trusted Accessで、お客様独自のアプリケーション環境へのアクセスを保護

SafeNet Trusted Access（STA）は、シングルサインオン（SSO）と多要素認証（MFA）を備えたアクセス管理ソリューションであり、クラウドとオンプレミス両方のアプリケーションに対応しています。STAには以下のような利点があります。



ユーザーアクションやデータアクセスなどに基づいた多様な認証トークンを使用して、MFAの導入を促進できる



ユーザー固有のニーズ、動作、特性に合わせてワークフローを自動化できる



ユーザーエクスペリエンスを低下させることなく、高度なセキュリティを維持できる

STAは基本的な認証やアクセス管理ツールとは異なり、ユーザーエクスペリエンスを損なうことなく不正アクセスを防止することで、組織がクラウドおよびオンプレミスアプリケーションへのアクセスを保護できるようにします。また、最新の認証ソリューションであるSTAは、あらゆる従業員におけるMFAの導入を促進します。

主な機能とThalesの特長

アプリケーション環境全体に対応したシームレスなシングルサインオン（SSO）

SSOにより、複数のログインを管理する手間やストレスが無くなります。ユーザーは一度認証を行えば複数のアプリケーションにシームレスにアクセスできるため、パスワード認証のたびに業務を中断する煩わしさから解放されます。さらに、STAと任意のIDPを統合することで、統一的な認証エクスペリエンスも実現できます。

パスワードレス認証

FIDO、Windows Hello、PKI、その他多数の先進的でフィッシング耐性の高い認証方式を使用することで、従来の脆弱なパスワードは不要になります。

最新のMFA方式を幅広く提供

- モバイルおよびデスクトップ向けOTPプッシュ
- OTPハードウェア
- パターンベースの認証
- EメールおよびSMS経由の帯域外認証
- コンテキストに基づく機動的な認証
- FIDO 2
- PKIスマートカードおよび認証情報
- Google Authenticator
- パスワードレス認証
- 生体認証
- 音声認証

リスクスコアリングと条件付きアクセス

厳格なポリシーの設定、リスクスコアリング、エンドポイントのリスク評価により、正当なアプリケーションとユーザーに適切なアクセスポリシーを適用し、すべての認証の整合性を維持することができます。

迅速な価値実現とユーザー主導のセルフ登録

STAは、使いやすさを重視して設計されたSaaSソリューションとして、アクセスポリシーを迅速に設定し展開することができます。セルフ登録機能では、認証トークンの設定および登録をユーザー自身で行えるよう、手順が表示されるため、IT担当者の負担が軽減されます。

データに基づく知見とシームレスなワークフロー統合

詳細なイベントログをユーザーのSIEMに自動的にエクスポートすることで、アクセスに失敗した際の状況を詳しく把握し、今後の認証ポリシーの策定に生かすことができます。

柔軟かつレジリエントなデリバリーアーキテクチャ

信頼性の高いフォールバックメカニズムであるAccess Continuumを通じて、システム障害やサービスの停止が発生した場合でも、データアクセスを途切らせることなく業務の継続を可能にします。

多様なプロトコルをサポート

- SAML
- OIDC
- WS
- Fed
- クラウドベースRADIUS
- エージェント
- RESTおよびSCIM API
- アプリケーションゲートウェイ
- レガシーアプリケーション

Thalesについて

Thalesはサイバーセキュリティのグローバルリーダーとして、世界中から信頼を得ているブランドの機密データ、ID、アプリケーション、ソフトウェアを保護します。高度な暗号化、IDおよびアクセス管理、アプリケーションセキュリティ、ソフトウェアエンタイトルメントを通じて、クラウド環境の保護、サイバー脅威に対する防御、さらには信頼できるデジタルエクスペリエンスを実現します。





cpl.thalesgroup.com

お問い合わせ先

Email：cpl.jpsales@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。

© Thales - September 2026·EHv4