

知っておくべき10のこと

Salesforceの多要素認証（MFA）要件 対応準備はできていますか？



1. 新たなSalesforceのMFA要件とは何か？

モバイルやデスクトップデバイスから、ユーザーインターフェイスを通じてSalesforce製品にログインするすべての内部ユーザー（従業員であるかどうかを問わず、従業員権限を持つすべてのユーザー）は、MFAを使用する必要があります。

2. 準拠期限

SalesforceのMFA要件は、2022年2月1日から適用されます。

3. 準拠しないとどうなるか？

2022年2月1日までに適切なMFAを有効化していない場合は、契約上の義務を遵守していないことになります。Salesforceは、顧客に法務部門と相談し、その影響を理解しておくことを勧めています。

4. MFAとして認められない手段は何か？

Salesforceは、NISTおよびセキュリティ業界の一般的なコンセンサスと足並みをそろえています。脆弱な認証手段は推奨されないか、または認められません。Salesforceは、MFAについて下記の手段を認めていません。

- メール
- SMSテキストメッセージ
- 電話連絡

5. SalesforceのMFA要件を満たすには、どのような選択肢があるのか？

- a. Thales SafeNet Trusted Accessなど、サードパーティの認証およびSSOプロバイダーのソリューションを使用する。
- b. Salesforce認証サービスを使用する。



6. 採用するアプローチを決定する際に考慮すべき事項は何か？

ハッキングの90%が資格情報の侵害から生じていることを考えると、多くの組織がそうであるように、貴組織もSalesforceアプリだけでなくSaaS資産全体にMFAを導入する方法を探しているかもしれません。

今日の企業の現実では、ユーザーごとにさまざまな認証ニーズがあります。一部のユーザーは、モバイルカバレッジが一貫していません。多くのユーザーが複数のデバイスを使用しています。すべてのユーザーが多数のアプリに安全にアクセスする必要があります。

最適なセキュリティを維持し、便利なログインエクスペリエンスを確保するには、以下を実現するソリューションを探する必要があります。

fido ユーザーに適したMFAエクスペリエンスで、どのデバイスでも状況に関係なくSalesforceやその他のアプリにログインできるというユーザーの期待を満たす

 リモートによって最小限の関与で安全に、数千人のユーザーをサポートおよびオンボードする必要がある、ITチームのニーズに対処する

 世界中の複数のビジネスユニットをサポートし、各地の言語に対応したエクスペリエンスを提供する

 すべてのアクセスおよび認証イベントの監査証拠を提供し、コンプライアンスを維持する

7. 組織がSalesforceの要件を満たすうえで、タレスはどのように役立ちますか？

タレスのSafeNet Trusted Accessを使用すると、Salesforceおよびその他数百のエンタープライズアプリ用のウィザードベースのテンプレートにより、数分でポリシーを有効にできます。Salesforceの2022年2月の期限までに簡単かつ迅速に対応できます。

SafeNet Trusted Accessを使用することで、エンタープライズアプリケーションを保護し、幅広い認証機能を使用してクラウドで安全に拡張できると同時に、スマートSSOとポリシー主導のアクセス制御でセキュリティを確保できます。

「数分でポリシーを有効にする」

Thales SafeNet Trusted Access

ユニバーサルな認証方式



OTPプッシュ



FIDO



生体認証



ハードウェア



パターンベース



PKI



パスワードレス



サードパーティ



Google
Authenticator



パスワード



音声



メール



SMS

- 安全なアクセスを迅速かつ効率的に導入する
- ベンダーロックインを回避し、アクセスセキュリティの制御を維持する
- セキュリティ侵害を防ぎ、金銭的責任と罰則を回避する
- 予算およびビジネス目標を達成する



- a. SafeNet Trusted Accessは、MFAオプションの選択肢を広げるほか、実装、管理、統制を効率化します。

Salesforce製品、その他のクラウドサービス、オンプレミスアプリについて、SafeNet Trusted Accessはスマートシングルサインオン(スマートSSO、「セキュアSSO」とも呼ばれる)を提供します。これは、各アクセス試行をシームレスに評価し、ユーザーに適切な認証方式を適用する機能です。

スマートSSOは、利便性とセキュリティの最適なバランスを提供し、アクセスセキュリティを継続的に評価してアクセス試行が許容設定と一致しない場合は、認証手段を強化することでゼロトラストセキュリティを実現できるようにします。通常のSSOとは異なり、スマートSSOでは、ユーザーの資格情報が単一障害点になる可能性があるシナリオを回避できます。

- b. タレスは、ユーザーの多様な認証ニーズのすべてをサポートし、あらゆるユーザーと作業環境に対応したさまざまなフォームファクタと証明書による幅広い認証方式を提供することで、「どこでも認証」を実現できるようにします。タレスは以下に焦点を当てています。

1. リスクに見合った認証
2. エンドツーエンドのセキュリティ
3. フリクション(摩擦や抵抗)が少ない優れたユーザーエクスペリエンス
4. 最小限の認証方式/ユーザー
5. コンプライアンス規制を満たすための監査証跡と証明書

8. タレスはNISTのセキュリティカテゴリの分類にどのように対応しているか?

Salesforceには通常、GDPRが適用される情報、個人情報(PII)、主要企業や競合他社の情報が含まれているため、これは、より高保証の認証を選択する説得力のある理由となっています。

タレスは、ソフトウェアおよびハードウェアソリューションで、すべてのNIST保証レベルに対応する認証方式を提供しています。これには、OTP + PIN + パスワード、モバイルプッシュ+生体認証、FIDOデバイス、パターンベースのオプションなどが含まれます。つまり、ユーザーに複数の認証方式を導入したり、ユーザーグループに異なる認証方式を導入したりすることができ、ユーザーのニーズ、セキュリティの制約、ログインコンテキストに応じて、適切な認証方式を適用できます。

9. タレスの認証の概要

タレスのSafeNet Trusted Accessは、Salesforce製品、その他のクラウドサービス、オンプレミスアプリに対応するスマートSSOなどの、認証およびアクセス管理サービスを提供します。SafeNet Trusted Accessは、実装、管理、統制を効率化し、ユーザーの多様な認証ニーズを満たしてすべてのアプリに最適なアクセスセキュリティを確保できるようにします。スマートSSOは、セキュリティとユーザーエクスペリエンスの向上、生産性の改善、ヘルプデスクのコスト削減を実現します。



認証

幅広い認証方法とフォームファクタを提供するSafeNet Trusted Access認証ソリューションを使用することにより、ユーザーはクラウドまたはオンプレミスで提供される1つの認証バックエンドから管理される一元管理された統合ポリシーによって、多数のユースケース、保証レベル、脅威ベクトルに対応できます。



サポートされている認証方式には、ステップアップ機能と組み合わせたコンテキストベースの認証、ワンタイムパスワード(OTP)、FIDO、X.509証明書ベースのソリューション、アウトオブバンド(OOB)が含まれます。すべての認証方式は、モバイル認証アプリやパターンベースのソフトウェア認証、スマートカード、USBセキュリティ鍵/トークンのハードウェア認証など、さまざまなフォームファクタで利用できます。

物理アクセス

タレスは、幅広い選択肢のカード本体オプションと非接触技術を備えたコンタクトカードや、NFCと互換性のあるインターフェイスカードなど、物理的および論理的なデュアルアクセス機能を備えた、さまざまなFIDOデバイスとスマートカードを提供しています。使用事例には、建物へのアクセス、印刷、コンピューターログイン、電子メール暗号化、ドキュメント署名があります。これによりユーザーは、Salesforceやその他のクラウドサービスにログインし、物理的な施設やデバイスにアクセスするための単一の認証デバイスを持つことができます。



特権アクセスに対する強力な認証

SafeNet Trusted Accessは、ユーザーの役割とリソースの機密性に応じてさまざまな認証方式とセッション管理ルールを適用し施行する機能を備えた、ポリシーベースのアクセスをサポートしています。Salesforce管理者には、一般的なSalesforceエンドユーザーよりも高い頻度で強力な認証を使用するよう強制することができます。

10. なぜタレスなのか?

タレスは、クラウドアクセス管理、FIDO、PKI、証明書ベースの認証(CBA)、ワンタイムパスワード(OTP)認証、IDフェデレーション、包括的なライフサイクル管理および監査ツールを含む、認証およびアクセス管理ソリューションの唯一の完全なポートフォリオを提供しています。

またタレスは、認証およびアクセス管理ソリューションと連携して機密データの永続的な保護と管理を可能にする、データ保護および暗号化ソリューションも提供しています。