

Salesforce 多要素認証(MFA)設定・利用マニュアル

多要素認証(MFA)とは

多要素認証（MFA: Multi-Factor Authentication）とは、ログイン時に「知っている情報（パスワード）」に加えて、「持っている端末（スマホアプリ等）」や「生体情報（指紋・顔認証など）」といった2つ以上の異なる要素を組み合わせることで本人確認を行う仕組みです。

パスワードが万が一漏洩した場合でも、第三者による不正アクセスを強力に防ぐことができます。Salesforce ではセキュリティ強化のために必須となっています。

事前準備

スマートフォン（iOS / Android）に、無料アプリ「Salesforce Authenticator」をインストールします。アプリの通知設定を「オン」にしておくと、ログイン時のプッシュ通知がスムーズに受け取れます。

初回アカウント接続（ペアリング）手順

1. ブラウザから、Salesforce へログインします。
2. 多要素認証（MFA）の接続画面が表示されたら、接続方法として「Salesforce Authenticator」を選択します。
3. スマートフォンでアプリを起動し、「アカウントを追加」をタップします。
4. PC 画面に表示される QR コードをスマートフォンのカメラで読み取ります。
5. 画面に表示される2語のフレーズ（または確認コード）を確認し、接続を完了させます。

*** ペアリングの接続の変更 ***

機種変更や、スマートフォンの初期化などに伴いペアリング（アカウント接続）を解除・再設定（変更）する場合ペアリングの再設定が必要となります。

旧端末が手元にあり事前に操作できる場合

1. 旧端末でのバックアップ設定を確認
事前に旧端末の Salesforce Authenticator アプリ内で「アカウントのバックアップ」が有効になっていることを確認します。
2. 新端末へのアプリインストールと引き継ぎ
新しいスマートフォンに Salesforce Authenticator アプリをインストールします。バックアップからアカウントを復元、または新端末側で新しくセットアップを行います。
3. Salesforce 上での接続解除と再ペアリング
PC などから Salesforce にログインし、[設定] > [ユーザー] から対象ユーザーの詳細画面を開きます。
「アプリケーション登録: Salesforce Authenticator」項目から現在の接続を [切断] し、その後もう一度 [接続] をクリックし、新端末のアプリでペアリングを完了させます。

※ 旧端末が使えない・手元にない場合は、管理者(システム管理者)が該当ユーザーの Salesforce Authenticator の切断/再接続を行ってください。

ログイン

Salesforce にログインをすると、ペアリング設定をしたスマートフォンにログインの通知が届きます。

届いた通知を開き、アクセス元（場所・IP 等）を確認して「承認」をタップします。

通知が届かない場合や圏外時は Authenticator アプリを開き、
表示される 6 桁の検証コードを入力してください。

位置情報の許可:

アプリの位置情報を有効にすると、会社や自宅など「信頼済みの場所」からのログインが自動承認されます。

アカウントのバックアップ:

機種変更やアプリ削除に備えて、アプリ設定から「アカウントのバックアップ」を事前に有効化しておくことをおすすめします。

パスキーの設定

Salesforce のセキュリティ強化（アップデート）に伴い、従来のパスワードや一般的な MFA（プッシュ通知等）に加えてパスキーの登録・使用が必須となりました。
ログイン時に、パスキーの登録が求められた場合は、以下のいずれかでパスキーを作成してください。

- Google Chrome(Google パスワードマネージャ)を使用
Google アカウントにログインしてからパスキーを作成してください。
- Microsoft Edge(Microsoft アカウント)を使用
Microsoft アカウントでログインしてからパスキーを作成してください。
- Windows の PIN(Windows Hello)を使用
[設定] - [アカウント] - [サインインオプション] から PIN(Windows Hello)を設定します。
再起動し、PIN を使用して Windows にログインしてからパスキーを作成してください。



MFA（多要素認証）のセキュリティ要件強化と「パスキー」について

Salesforce では、サイバー攻撃の巧妙化に伴うセキュリティ対策の強化として、システム管理者や特権権限を持つユーザーを対象に「フィッシング耐性 MFA」の適用を順次義務付けています。
これに伴い、Salesforce Authenticator だけでは要件を満たさないケースがあり、管理者権限でのログイン時に強制的に「パスキー」の登録・利用が求められる仕様となっています。

「Salesforce Authenticator」の導入や接続手順については、以下の公式ヘルプをご参照ください。

Salesforce 公式ヘルプ：[Salesforce Authenticator の設定方法](#)

Salesforce 公式ヘルプ：[Salesforce Authenticator を使用した多要素認証](#)

本件に関する詳細な仕様や公式の案内については、以下の Salesforce 公式情報をご参照ください。

Salesforce 公式ヘルプ：[特権ユーザーのフィッシング詐欺耐性 MFA 要件](#)

Salesforce サクセスナビ：[2026 年 6 月から開始されるセキュリティ強化に備える](#)