

多要素認証 (MFA) 設定マニュアル



[contents]

- P.01 本手順書の目的／MFAの概要／前提事項
- P.02 設定手順(約15分)
- 全員が行う作業
 - 1：モバイル(スマホ)へのSalesforce Authenticatorのインストール
 - 2：ユーザアカウントとSalesforce Authenticatorの接続
- P.08 ■ システム管理者の作業
- 3：権限セットの作成
 - 4：権限セットのユーザへの割り当て
- P.11 ログイン手順
- SalesforceにMFAを使用してログイン
- P.13 (設定手順実施後に)よくある問い合わせ
- Salesforce Authenticatorを家に忘れた場合はどうすればいいですか？
 - Salesforce Authenticatorを紛失した場合どうすればいいですか？
 - 他のユーザがSalesforce Authenticatorと接続ができているかの確認はできますか？
(対象ユーザが少ない場合)
 - 他のユーザがSalesforce Authenticatorと接続ができているかの確認はできますか？
(対象ユーザが多い場合)
 - MFAを使用したログイン状況を確認することはできますか？
 - これから新規ユーザを作成する場合の多要素認証の設定方法は？
 - MFAが有効な新規ユーザがログインする時の操作方法を教えてください。
 - 本手順書以外に、MFAに関するリソースはありますか？
- P.22 Appendix：MFAの有効化方法

本手順書の目的

Salesforce製品(パートナーソリューションを含む)に画面からログインするすべての内部ユーザは、MFA(多要素認証。以降「MFA」と記載)を有効にいただく必要があります。本手順書では、MFAの対象となる全てのユーザに対して、SalesforceのMFAを有効にする手順をご説明します。

本手順書は、既にSalesforceのコア製品(Sales CloudやService Cloudなど)をご利用のお客様を対象にしております。

MFA の概要

MFAは、ログインセキュリティを強化し、セキュリティ上の脅威からビジネスやデータを保護するための最も簡単で効果的な手段と言えます。

MFAを有効にすると、ユーザ名とパスワードだけではログインができなくなります。ログインするためには、追加でSalesforce Authenticator等の(第2の認証方法)で[承認]をする必要があります。

なお、組織内のユーザがMFAを使用してログインする準備が整っていない状態で、Salesforceユーザ全員に対してMFAを有効にすると、**誰もログインができなくなってしまいます!** そのため、まずは一般ユーザやテスト用ユーザでMFAを有効化してみましょう。(所要時間は約15分です)その後、皆様へ操作方法の説明をして展開するようにしましょう。

前提事項

- 本手順書では、権限セットを使用する方法で説明しています
- 組織の設定によっては、本手順書の画面とお客様の画面が異なる場合があります
- モバイル端末はiPhoneの画面ショットです。Android端末をご利用の場合は表示が異なります
- 第2の認証方法として、Salesforce Authenticatorを使用する手順です
- 本手順書は、SalesforceのMFAを有効化する手順です (SSOをご利用のお客様の手順は含まれません)
- MFA移行のベストプラクティスは、Salesforceの設定画面にある[多要素認証アシスタント]をご確認ください
- 不明点は弊社テクニカルサポートへお問い合わせ下さい(お問い合わせ方法は[こちら](#)※)
※ <https://help.salesforce.com/s/articleView?id=000340173&type=1&language=ja>

設定手順(約15分)

設定は、以下4ステップです。(約15分)

- 1 全員が行う作業：モバイル(スマホ)へのSalesforce Authenticatorのインストール
- 2 全員が行う作業：ユーザアカウントとSalesforce Authenticatorの接続
- 3 システム管理者の作業：権限セットの作成
- 4 システム管理者の作業：権限セットのユーザへの割り当て

では、ここから設定手順を説明します。

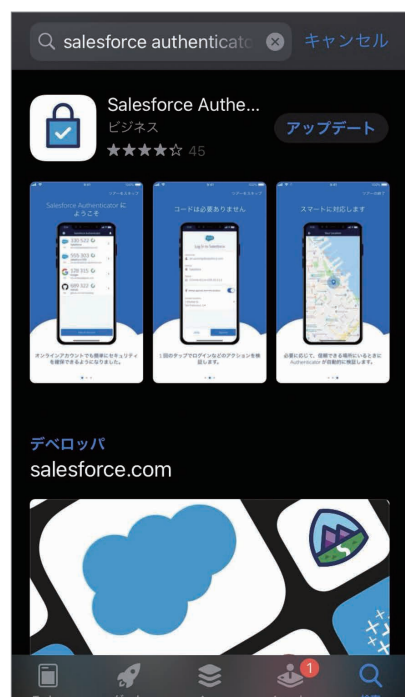
以後の設定は、お客様のPCとモバイル(スマホ)の両方を使用して行います。

注意事項

- システム管理者で設定手順を実施した場合、失敗すると(システム管理者が)Salesforceにログインができなくなる可能性があります。
- ライセンスに余裕がある場合は、テストユーザを作成することもできます。(ユーザの作成方法は[こちら](#)※)
※<https://successjp.salesforce.com/article/NAI-000020>
- 社内ユーザへ協力してもらうこと、テスト用ユーザの作成共に困難な場合は、操作ミスをした場合の影響を考慮し、注意深く設定を行ってください。

全員が行う作業

1 モバイル(スマホ)へのSalesforce Authenticatorのインストール

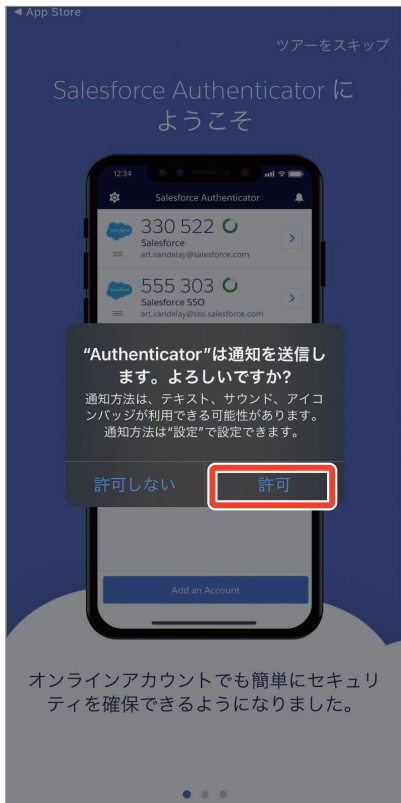


- 1 iOSのモバイル(スマホ)の場合
App Storeで[Salesforce Authenticator]を検索します。

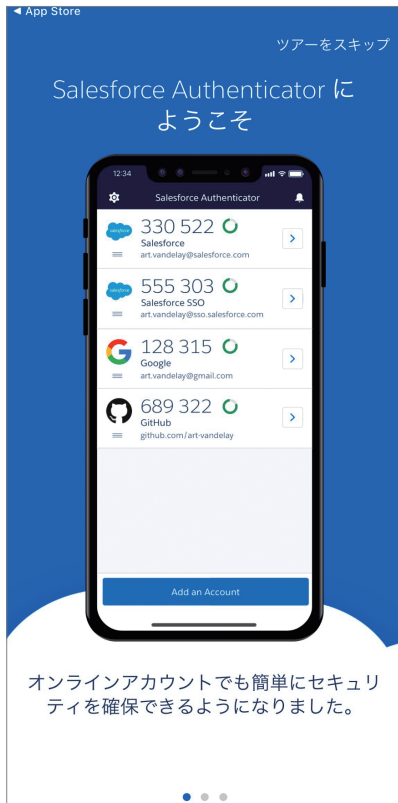
Androidのモバイル(スマホ)の場合
Google Playで[Salesforce Authenticator]を検索します。

検索にヒットしたアプリケーションの[インストール]をタップします。(左図は既にインストール済みのため[アップデート]と表示されています)

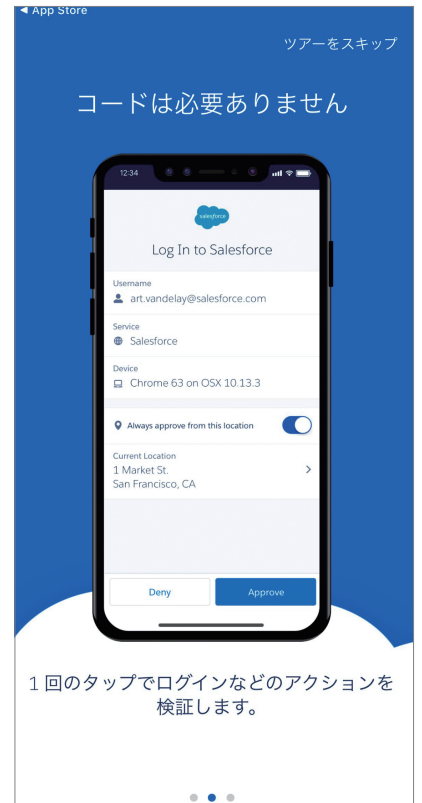
インストールが完了したら[開く]をタップします。



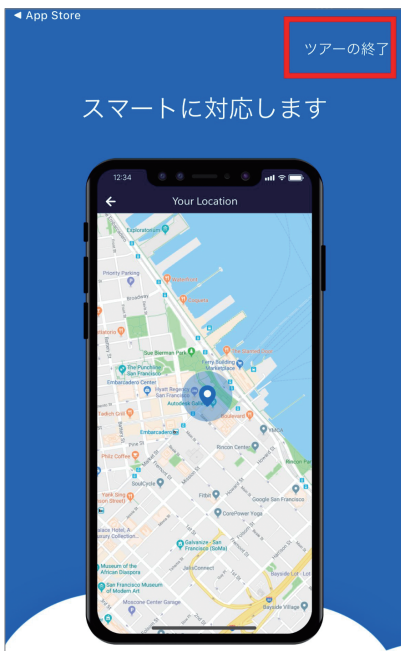
2 [許可]をクリックします。



3 右にスワイプします。



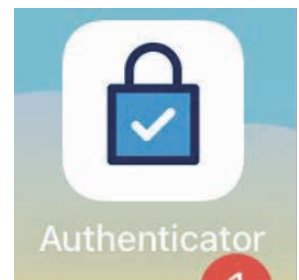
4 右にスワイプします。



5 [ツアーの終了]をタップします。



6 この画面が表示されたら、初期設定完了です。



7 ホーム画面に上図のようなアイコンが表示されていることを確認します。



このアイコンをタップして、いつでもSalesforce Authenticatorを開くことができます。

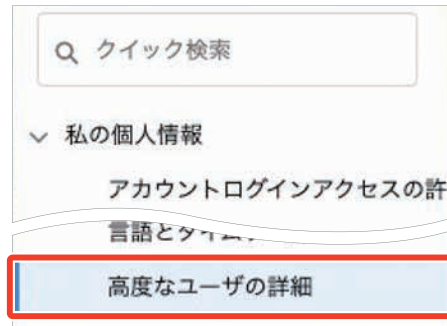
ご利用頂いている携帯電話の入れ替えや紛失に備えて、接続済みのアカウントを別の携帯電話で復元するためのバックアップ用のパスコードを設定することが可能です。
必要に応じて下記のヘルプドキュメントをご参照の上、ご設定ください。
Salesforce Authenticator モバイルアプリケーションでの接続済みアカウントのバックアップ作成
https://help.salesforce.com/s/articleView?id=sf.salesforce_authenticator_backup.htm&type=5&language=ja

② ユーザアカウントとSalesforce Authenticatorの接続

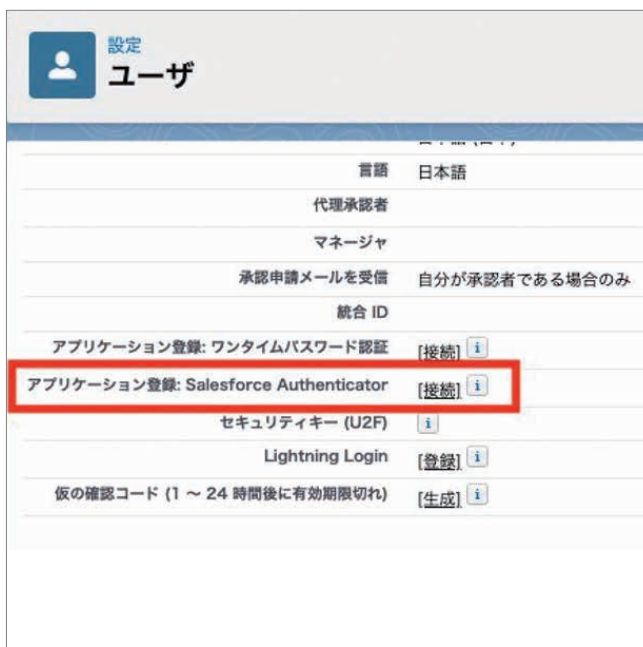
多要素認証を有効化する前に、ユーザとSalesforce Authenticatorを接続しておきます。



1 画面右上の[自分の顔写真]から[設定]をクリックします。



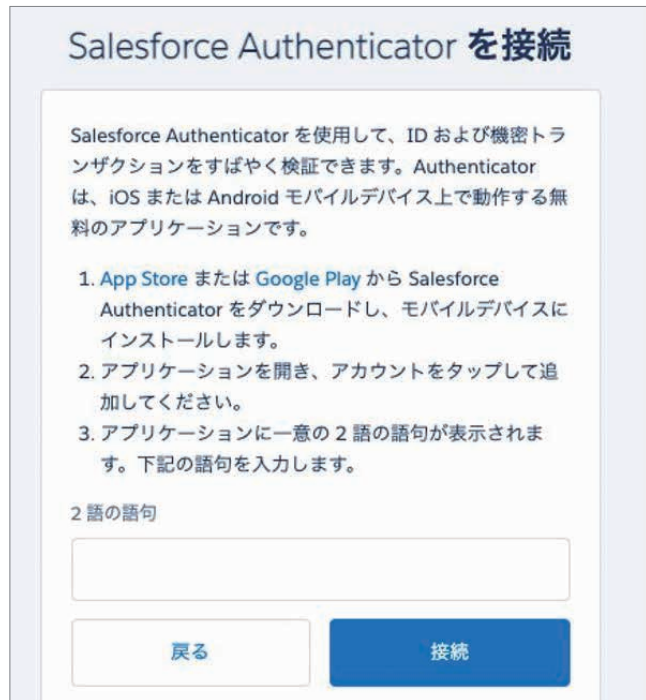
2 画面左側のサイドメニューから[高度なユーザの詳細]をクリックします。



3 ユーザの詳細画面の左列の下の方に表示されている[アプリケーション登録:Salesforce Authenticator]の[接続]をクリックします。



4 [IDを検証]画面が表示されます。



5 メールを受信箱に届いた[SalesforceでIDを確認]という件名のメールを開き、6桁の確認コードをコピーして、**4** に入力して、[検証]をクリックします。

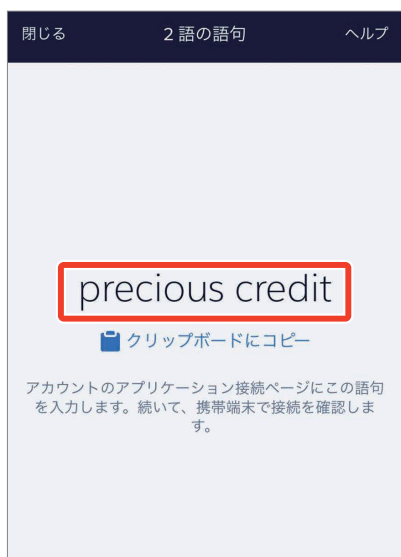
6 [Salesforce Authenticatorを接続]画面が表示されます。

先程モバイル(スマホ)にインストールしたAuthenticatorアプリを開いて、次のステップへ進みます。

モバイル(スマホ)



7 [アカウントを追加]をタップします。



8 [2語の語句]が表示されます。

次のPCでのステップで、この情報を使用します。



PC



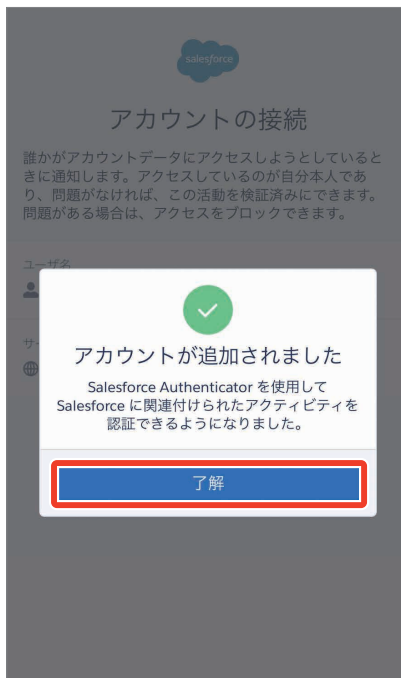
9 PCの[Salesforce Authenticatorを接続]画面に 8 の2語を入力し、[接続]をクリックします。



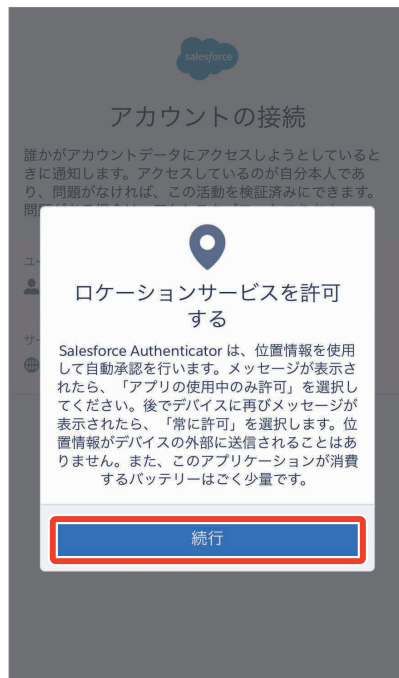
10 Salesforceにログインした状態になります。



モバイル(スマホ)



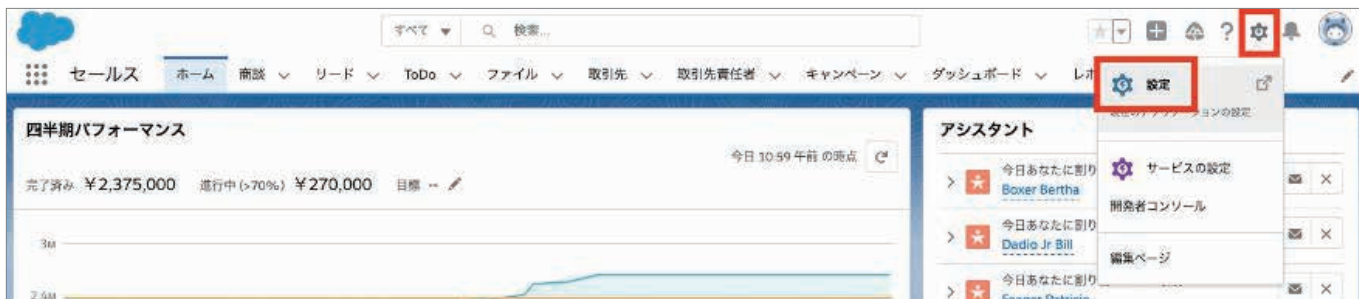
11 [アカウントが追加されました]と表示されるので、[了解]をタップします。



12 [ロケーションサービスを許可する]と表示されるので、[続行]をタップします。

位置情報を使って自動承認をする機能を使用することもできます。[続行]をクリックした後、許可するかどうかを選択します。

3 権限セットの作成



1 画面右上の[歯車]から[設定]をクリックします。

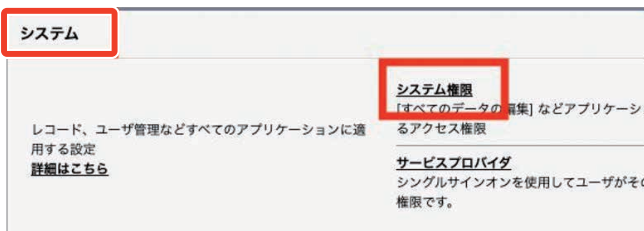


2 画面左上にある[クイック検索]に[権限セット]と入力し、検索します。
検索結果に表示された[権限セット]をクリックし、[新規]をクリックします。



3 [表示ラベル]、[API参照名]を入力し、[保存]をクリックします。

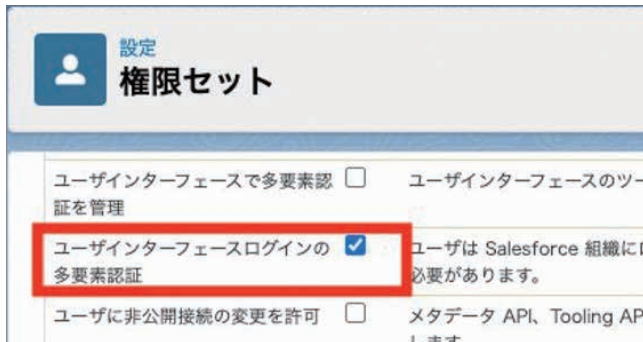
- 表示ラベル：日本語で設定できます
- API参照名：英字で始まる英数字で設定してください(ハイフンは利用できません)



4 画面下方にある[システム]セクション配下の[システム権限]をクリックします。



5 [編集]をクリックします。



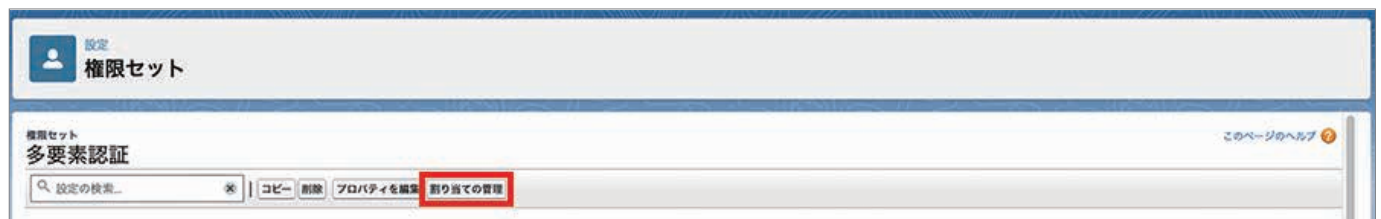
- 6 画面下方にある[ユーザーインターフェースログインの多要素認証]にチェックを入れて、画面上部の[保存]をクリックします。
 ※「多要素認証」を含む似た項目が複数あるので、ご注意ください



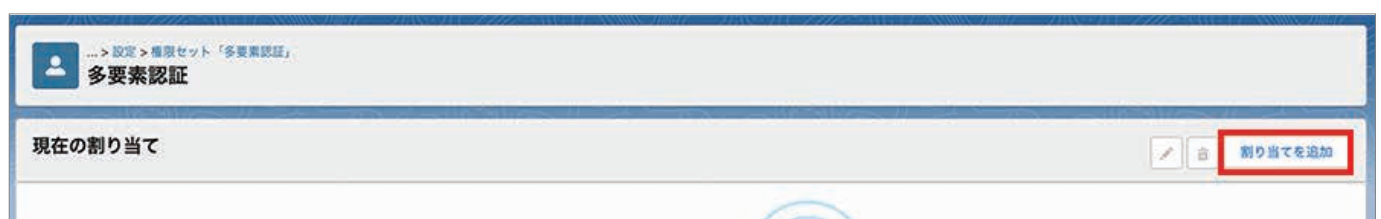
- 7 確認画面が表示されます。以下権限の名前に間違いがないか、再度確認します。
- ユーザーインターフェースログインの多要素認証

システム管理者の作業

4 権限セットのユーザへの割り当て



- 1 [割り当ての管理]をクリックします。



- 2 [割り当てを追加]をクリックします。

... > 権限セット「多要素認証」 > 割り当ての有効期限を管理
多要素認証

割り当てるユーザを選択

最近参照したデータ ▼

1個の項目が選択されました

このリストを検索...

氏名 ▼ 役職 ▼ 電話 ▼ メール ▼

キャンセル **次へ**

3 対象ユーザにチェックを入れて、[次へ]をクリックします。

... > 権限セット「多要素認証」 > 割り当ての有効期限を管理
多要素認証

割り当てられたユーザの有効期限オプションを選択

有効期限なし 有効期限を指定

1日 1週間 30日間 60日間 カスタム日付

タイムゾーン
タイムゾーンを選択...

キャンセル 戻る **割り当て**

4 [割り当て]をクリックします。

割り当ての概要

氏名	ユーザライセンス	有効期限	タイムゾーン	状況
				Success
				Success

5 画面に、対象ユーザが表示されることを確認します。

ログイン手順

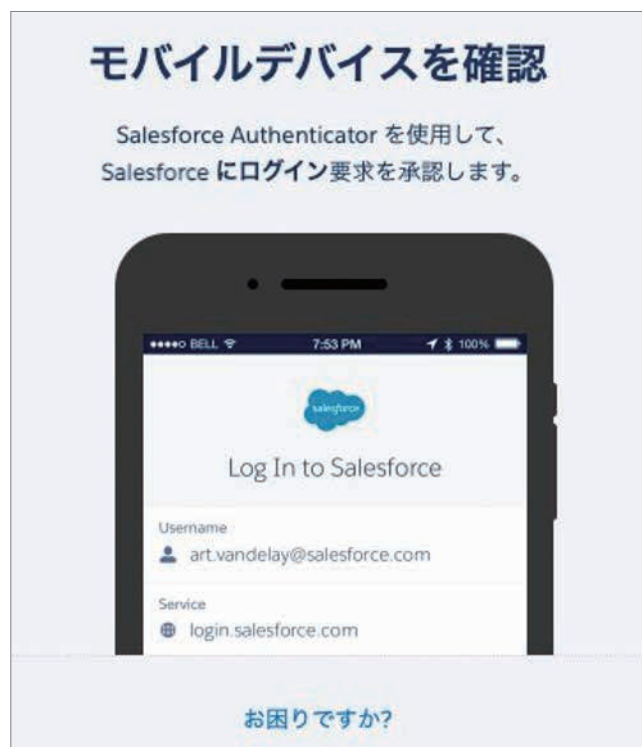
SalesforceにMFAを使用してログイン



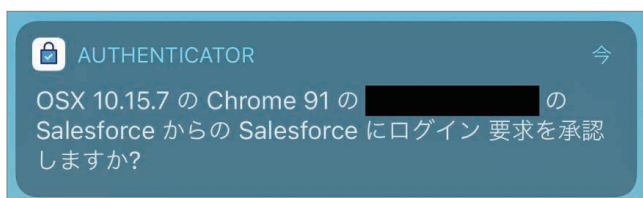
- 1 まずは、Salesforceからログアウトします。



- 2 ユーザ名とパスワードを入力し、[ログイン]をクリックします。



- 3 先程接続したSalesforce Authenticatorを使用した多要素認証が求められます。



- 4 プッシュ通知が届くので、タップします。

salesforce

Salesforce にログイン

ユーザ名
[Redacted]

サービス
Salesforce

デバイス
OSX 10.15.7 の Chrome 91

この場所では常に承認

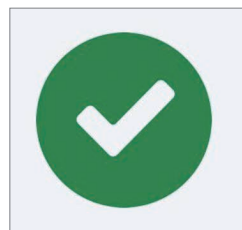
現在の場所
[Redacted]

拒否 承認

5 ユーザ名などの情報を確認し、問題ない場合は[承認]をタップします。

もし、自分がログインしようとしていない時に届いたら、誰かが自分のユーザ名でログインしようとしているので、拒否します！

- [この場所では常に承認]をONにすると、次回同じコンピュータ(ブラウザ)からログインしたときに電話が同じ場所にあり、3回以上の繰り返しパターンがすべて同じである場合、電話は自動的に応答します。
- 詳細は、[Salesforce AuthenticatorアプリケーションでEinstein Automationを設定する](#)^{*1}(ナレッジ)をご確認ください



6 認証が成功しました!



パスワードが嫌いですか? 私たちもです。

Lightning Login ではパスワードが廃止されており、Salesforce に簡単にアクセスできます。

さあ始めましょう

パスワードの代わりに Salesforce Authenticator を使用してログインします。
登録は短時間で簡単にできます。

Lightning Login に登録

後で知らせる
次回からこのメッセージを表示しない

7 [後で知らせる]をクリックします。

- [Lightning Loginに登録]をすると、パスワードなしですばやく安全にログインができるようになります。
- 詳細は、[Lightning Loginの有効化によるパスワードを使用しないログイン](#)^{*2}(ヘルプ)をご確認ください。

セールス ホーム 商談 リード ToDo ファイル 取引先 取引先責

四半期パフォーマンス

今日 10:59 午前の時点

完了済み ¥2,375,000 進行中 (>70%) ¥270,000 目標 --

8 ログイン後の画面が表示されます。

*1 <https://help.salesforce.com/s/articleView?id=000317978&type=1&language=ja>

*2 https://help.salesforce.com/s/articleView?id=sf.security_ll_enable.htm&type=5&language=ja

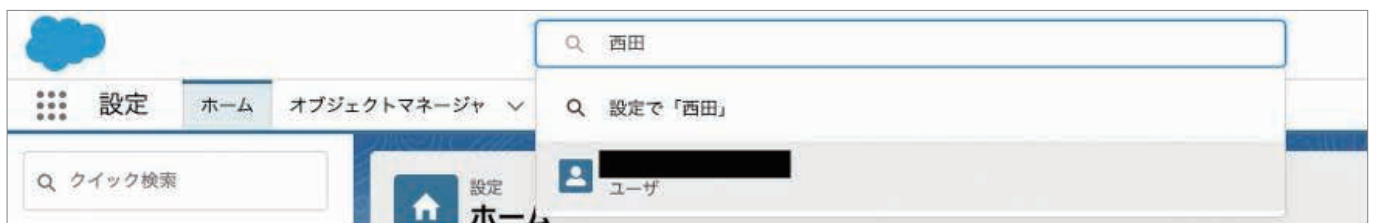
(設定手順実施後に)よくある問い合わせ

Salesforce Authenticatorを家に忘れた場合はどうすればいいですか？

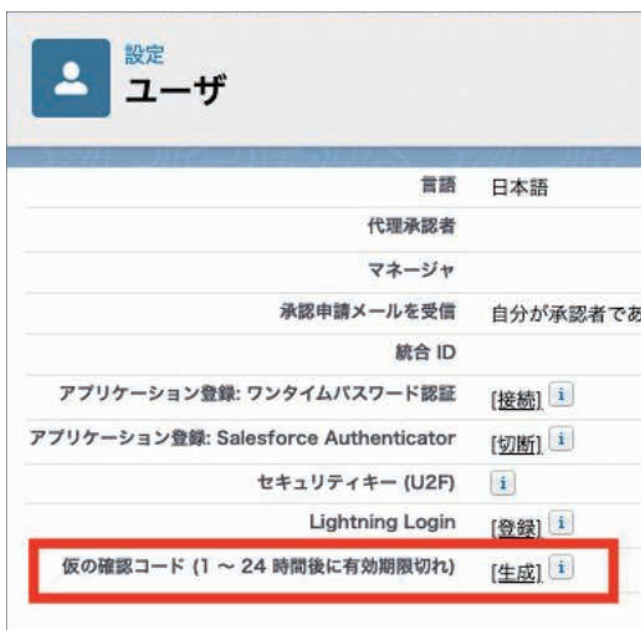
システム管理者 (もしくは[ユーザインターフェースで多要素認証を管理]権限を持つユーザ)は、以下手順で仮の確認コードを生成することができます。



1 画面右上の[歯車]から[設定]をクリックします。



2 画面上部にある検索窓に、ユーザの名前を入力し、候補に表示されたユーザをクリックします。



3 ユーザの詳細画面の左列の下の方に表示されている[仮の確認コード(1~24時間後に有効期限切れ)]の[生成]をクリックします。



4 モバイルデバイスで確認が必要な旨が表示されます。



モバイル(スマホ)

salesforce

仮の確認コードを生成

ユーザ名
[Redacted]

サービス
Salesforce

デバイス
OSX 10.15.7 の Chrome 91

この場所では常に承認

現在の場所
[Redacted]

拒否 承認

- 5 ユーザ名などの情報を確認し、問題ない場合は[承認]をタップします。

身に覚えがない場合は、拒否します!



PC

仮のコードを生成

fy22@mfa.com のコードの有効期限はいつにしますか?

1 時間

2 時間

4 時間

8 時間

12 時間

24 時間

キャンセル コードの生成

- 6 有効期限を選択して、[コードの生成]をクリックします。

ユーザ用に生成されたコード

このコードをユーザに付与するときに、有効期限までこのコードを何度も使用できることを説明してください。

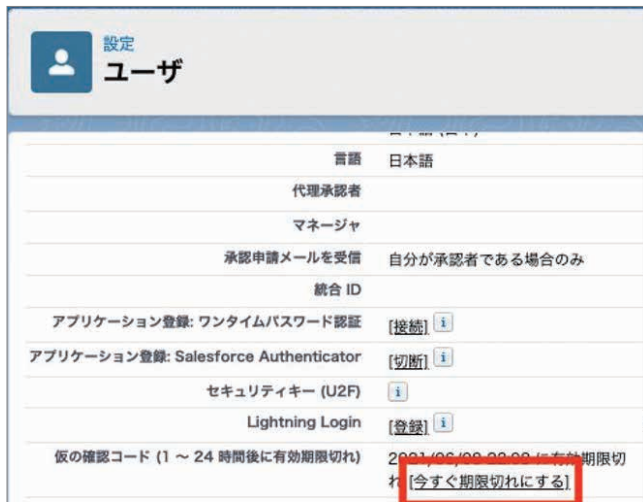
ユーザ名
fy22@mfa.com

仮のコード
9GA0M5Z09K

有効期限
2021/06/08 22:08

完了

- 7 仮のコードと有効期限を控えて、ユーザに共有します。
- ユーザにもメールが送信されますが、仮のコードや有効期限の情報は含まれません。そのため、管理者様よりユーザへ仮のコードを知らせる必要があります。



- 有効期限前に仮のコードを削除する場合は、対象ユーザ詳細画面の[今すぐ期限切れにする]をクリックします。

Salesforce Authenticatorを紛失した場合はどうすればいいですか？

システム管理者が、ユーザアカウントとSalesforce Authenticatorを切断することで、ユーザは新しいモバイル (スマホ) にインストールしたSalesforce Authenticatorを (ユーザアカウントと) 接続できるようになります。



- ユーザ詳細画面の [アプリケーション登録 : Salesforce Authenticator] の [切断] をクリックします。

他のユーザがSalesforce Authenticatorと接続ができているかの確認はできますか？

●対象ユーザが少ない場合

対象ユーザの詳細画面で、ユーザとSalesforce Authenticatorの接続状況を確認できます。



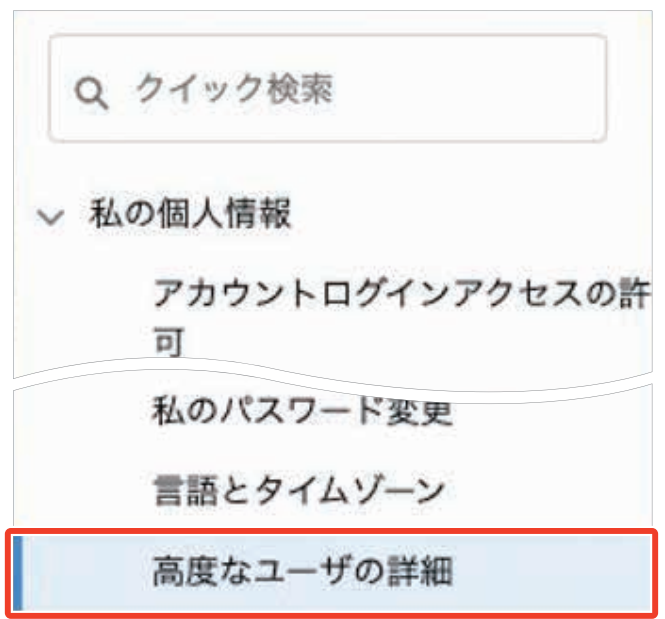
1 画面右上の[歯車]から[設定]をクリックします。



2 画面上部にある検索窓に、ユーザの名前を入力し、候補に表示されたユーザをクリックします。



3 画面右上の[自分の顔写真]から[設定]をクリックします。



4 画面左側のサイドメニューから[高度なユーザの詳細]をクリックします。



5 ユーザの詳細画面の左列の下の方に表示されている[アプリケーション登録: Salesforce Authenticator]の[接続]が[切断]に変わっていることを確認します。

他のユーザがSalesforce Authenticatorと接続ができているかの確認はできますか？

●対象ユーザが多い場合

ユーザのリストビューを作成し、確認することができます。



1 画面右上の[歯車]から[設定]をクリックします。



2 画面左上にある[クイック検索]に[ユーザ]と入力し、検索します。
検索結果に表示された[ユーザ]をクリックし、[新規ビューの作成]をクリックします。



3 [ビュー名]と[ビューの一意の名前]を入力します。

- ビュー名：日本語で設定できます
- ビューの一意の名前：英字で始まる英数字で設定します(ハイフンは利用できません)

ステップ 3. 表示する項目を選択

選択可能な項目	選択済みの項目
名	氏名
姓	別名
ニックネーム	ユーザ名
メール	最終ログイン
電話	Salesforce Authenticator
内線	ロール
Fax	有効
携帯	プロフィール
町名・番地	マネージャ
市区郡	
都道府県	
郵便番号	
国	
会社名	
ディビジョン	

追加

ステップ 4. 表示を制限

自分のみ表示

すべてのユーザに表示 (パートナー/カスタマーポータルユーザを含む)

特定のユーザグループに表示

保存 名で保存 削除 キャンセル

4 画面下方の[ステップ3.表示する項目を選択]セクションの[選択可能な項目]にある[Salesforce Authenticator]を[選択済みの項目]に追加します。



[保存]をクリックします。

Authenticator接続確認用

このページで、ユーザを作成、表示、および管理できます。

さらに、モバイルデバイスからユーザ詳細の表示と編集、パスワードのリセット、およびその他の管理タスクを実行するには、SalesforceA をダウンロードしてください: [iOS](#) | [Android](#)

ビュー: **Authenticator接続確認用** 編集 | 新規ビューの作成

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ア カ サ タ ナ ハ マ ヤ ラ ワ その他

新規ユーザ パスワードのリセット 複数のユーザを追加

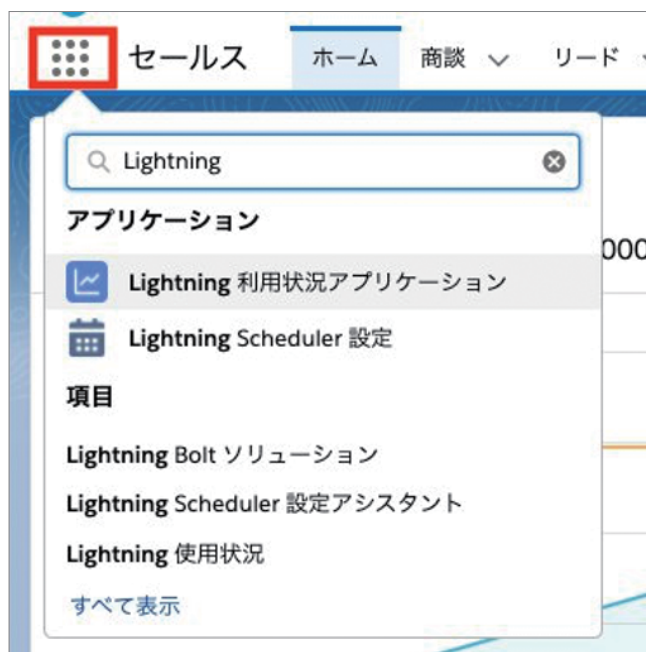
アクション	氏名 +	別名	ユーザ名	最終ログイン	Salesforce Authenticator	ロール
<input type="checkbox"/> 編集	Chatter Expert	Chatter	chatty.00d5h000001uyneegas.cgx4e4mq3kng@chatter.salesforce.com		<input type="checkbox"/>	
<input type="checkbox"/> 編集	User Integration	integ	integration@00d5h000001uyneegas.com		<input type="checkbox"/>	
<input type="checkbox"/> 編集	User Security	sec	insightssecurity@00d5h000001uyneegas.com		<input type="checkbox"/>	
<input type="checkbox"/> 編集	西田			2021/06/08 15:11	<input checked="" type="checkbox"/>	切断

新規ユーザ パスワードのリセット 複数のユーザを追加

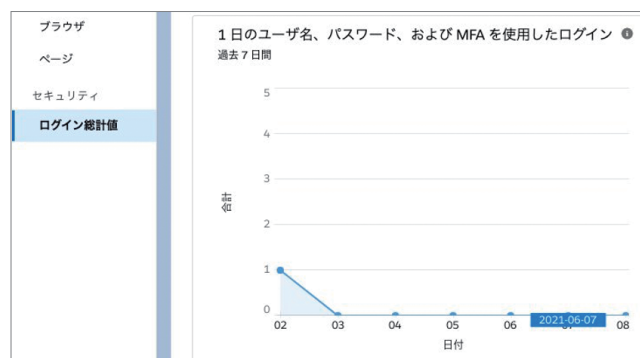
5 [Salesforce Authenticator]列にチェックが入っているユーザは、接続済みです。

MFAを使用したログイン状況を確認することはできますか?

(デフォルトで用意されている)[Lightning利用状況アプリケーション]を使うと、MFAの使用状況などを確認することができます。



- 1 画面左上の[アプリケーションランチャー]で [Lightning]で検索をして表示される[Lightning 利用状況アプリケーション]をクリックします。



- 2 画面左側のメニューの[ログイン統計値]をクリックします

画面下方、左列の[1日のユーザ名、パスワード、およびMFAを使用したログイン]グラフを確認します。

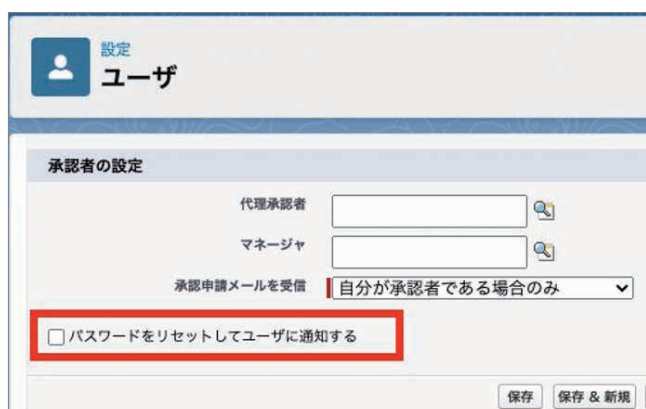
- 当日のログイン数は表示されません
- ログイン数が少ない時は、ユーザに状況をヒアリングして、サポートが必要な場合はログイン方法などの支援を行いましょ

これから新規ユーザを作成する場合の多要素認証の設定方法は？

まず、以下の流れで設定を行います。

- 3 システム管理者の作業：権限セットの作成 (P.08) ※既存の権限セットがあれば、それをご利用いただけます。
- 1 全員が行う作業：モバイル(スマホ)へのSalesforce Authenticatorのインストール (P.02)

続いて、以下の手順でユーザを作成します。



- 1 新規ユーザを作成する際、[パスワードをリセットしてユーザに通知する]のオプションをOFFにして、ユーザを作成します。
※デフォルトでONになっているので、手動でOFFにします。
- 2 作成したユーザにMFAの権限セットを追加します。(4 システム管理者の作業:権限セットのユーザへの割り当て (P.10))
- 3 新規ユーザのパスワードをリセット*します。

* https://help.salesforce.com/s/articleView?id=sf.resetting_and_expiring_passwords.htm&type=5&language=ja

MFAが有効な新規ユーザがログインする時の操作方を教えてください。

以下の前提条件のもと、操作方を説明します。

- ユーザーに権限セットを追加済みである
- モバイル(スマホ)にSalesforce Authenticatorをインストール済みである



1 新規ユーザでログインします。

2 [Salesforce Authenticator を接続] 画面が表示されたら、事前にモバイル(スマホ)にインストールした Authenticator アプリを確認します。



3 [アカウントを追加] をタップします。

4 2語の語句が表示されます。

次のPCでのステップで、この情報を使用します。



PC



5 PCの[Salesforce Authenticatorを接続]画面に4の2語を入力し、[接続]をクリックします。



6 Salesforceにログインした状態になります。

本手順書以外に、MFAに関するリソースはありますか？

組織のユーザにMFAを展開するために必要な準備やリソース、ベストプラクティスに関する情報は、Salesforceの設定画面の[多要素認証アシスタント]に纏まっており、ぜひご活用ください。



PC



また、以下リソースも参考になると思いますので、お役立ていただければ幸いです。

- [Salesforce多要素認証に関するFAQ](#)^{*1}(ナレッジ)
- [多要素認証 \(MFA\) の よくあるトラブルシューティング](#) ^{*2}(ナレッジ)
- [セキュリティ・運用「はじめてガイド」](#)^{*3}(サクセスナビ)
- [多要素認証\(MFA\)コミュニティ日本](#)^{*4}(Trailblazer Community)
- [ご質問いただくにはSalesforceへのログインが必要です](#)

※1 <https://help.salesforce.com/s/articleView?id=000352937&type=1&language=ja>

※2 <https://help.salesforce.com/s/articleView?id=000389576&type=1&language=ja>

※3 <https://successjp.salesforce.com/security-operation/guide>

※4 <https://trailhead.salesforce.com/ja/trailblazer-community/groups/0F945000000Gy6x?tab=discussion>

Appendix : MFAの有効化方法

SalesforceでMFAを有効化するには、「権限セット」を使用してユーザー単位で[ユーザーインターフェースログインの多要素認証]権限を付与する方法と、ご利用の組織で一括で機能を有効化する方法の 2 種類があります。

機能名	説明
権限セット	<ul style="list-style-type: none">● MFA関連のデフォルトで用意された権限セットはありませんので、<u>お客様にて作成頂く必要があります</u> (本手順書にて説明)● 1つの権限セットを複数ユーザに割り当てることができます● 1つの権限セットに複数の権限を追加することができます。そのため、既存の権限セットに追加で[ユーザーインターフェースログインの多要素認証]権限を追加しても構いません (本手順書では新規作成のみ説明)● 動作確認中は、ユーザ単位で権限を付与/削除できる権限セットの使用を推奨します
組織全体でMFA有効化	<p>組織のすべての内部ユーザの MFA を有効にする手順は、次のとおりです。</p> <ul style="list-style-type: none">● [設定] の [クイック検索] ボックスに[ID]と入力し、[ID 検証] を選択します。● [Salesforce 組織へのすべての直接 UI ログインに多要素認証 (MFA) が必要] を選択します。 <p>詳細はこちらのヘルプドキュメントも併せてご参照下さい。 https://help.salesforce.com/s/articleView?id=sf.security_mfa_org_wide_setting.htm&type=5&language=jp</p> <p>※組織全体で MFA 有効化を行っても、Single Sign On (SSO) でのログインには影響はありません</p>

※ プロファイルに権限を付与する形での制御については今後EOL(ライフサイクル終了)が予定されています。権限セットもしくは組織全体での有効化にてご対応頂くことを推奨します