

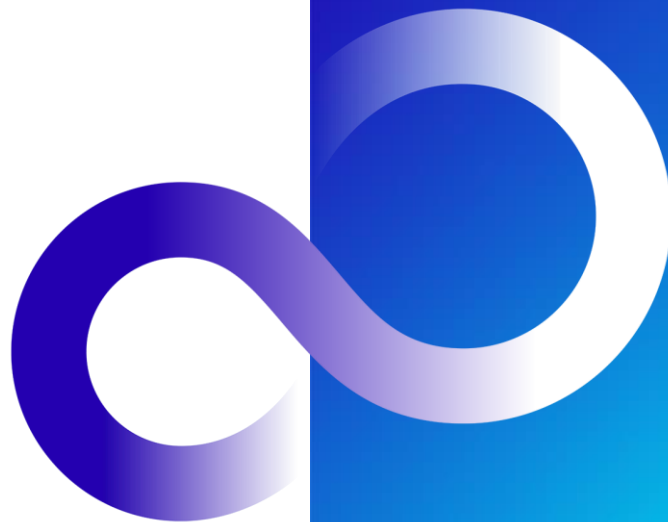
Appendix.1

新SupportDesk-Web 多要素認証（MFA）の設定方法

5 版：2025年7月14日

初版：2025年3月12日

富士通株式会社
エフサステクノロジーズ株式会社



版数	改版日	改版内容
初版	2025年3月12日	初版発行
2 版	2025年4月16日	① 共用メールアドレスでの運用方法を特例として追加（1-5）
3 版	2025年5月12日	① Microsoft Edgeの拡張機能を利用した方法を追加（5章/6章）
4 版	2025年6月9日	① 特例（共用のメールアドレス）を実施する際の注意事項を追加（1-6）
5 版	2025年7月14日	① PCでのMFAとしてWinAuthを追加

1. 多要素認証の概要

1-1. 多要素認証の前提条件と選択肢

前提条件

- ✓ 利用者アカウント（Salesforceアカウント）： MFA端末 = 1 : 1
- ✓ MFA端末は スマートフォン or パソコン から選択

▶ 併用不可

- 利用者アカウントが発行された際に速やかにSupportDesk-Webにアクセスできるように、事前に多要素認証の方法をご決定頂き、必要なアプリケーションをインストールしておいてください。

認証デバイス	認証方法	実施方法
スマートフォン	1. Salesforce Authenticator	➤ App Store / Google Play から事前にインストールしてください。 ✓ 設定方法は2章にて解説
	2. その他の認証アプリ (Microsoft Authenticator など)	—
パソコン	3. Google Chrome の拡張機能	■ 事前準備：3章にて解説 ■ 設定方法：4章にて解説
	4. Microsoft Edge の拡張機能	■ 事前準備：5章にて解説 ■ 設定方法：6章にて解説
	5. WinAuth	■ 事前準備：7章にて解説 ■ 設定方法：8章にて解説

1-2. 作業環境とMFAの関係性

作業環境	想定する状況	MFA端末	MFA可否	制約	備考
個人の専用PC	一般的な環境	スマートフォン	可能		
		PC (Chrome)	可能		
個人の専用PC (2台以上)	事務所用・モバイル用など複数端末を保有している方	スマートフォン	可能		
		PC (Chrome)	制限有り	MFAの専用PCが必要	実質的に想定なし
1台の共用PC	システム保守業務において常に1人しか従事しない（単一シフト体制）	スマートフォン	可能		
		PC (Chrome)	可能		1-3章 にて解説
複数台の共用PC	システム保守業務において複数人が従事し座席・作業端末が流動的（複数人シフト体制）	スマートフォン	可能		
		PC (Chrome)	制限有り	MFAの専用PCが必要	1-4章 にて解説

➡ **スマートフォンアプリを利用したMFAを推奨（作業PCが流動的でも対応が容易）**

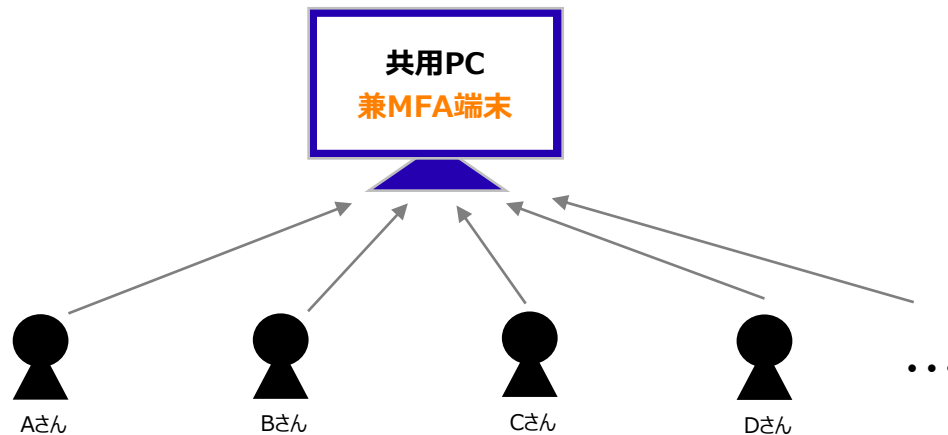
1-3. 1 台の共用PC環境でのMFAの実施方法

想定

- ✓ 社給・個人問わずスマートフォンの業務利用は禁止
- ✓ 1 台の作業PCでシフト勤務
- ✓ インターネット接続端末として 1 台をタイムシェア

▶ 利用者全員分のMFAを1つのPCに設定*

*設定方法は3-4章にて解説



1-4. 複数の共用PC環境でのMFAの実施方法

想定

- ✓ 社給・個人問わずスマートフォンの業務利用は禁止
- ✓ シフト勤務体制などで作業PCが1台／人ではない



利用者全員分のMFAを1つのPCに設定*

*設定方法は3-4章にて解説



DAY1



Aさん



Bさん



Cさん



Dさん



Eさん

B,C,DさんはSupportDesk-Webログイン時に
AさんからOne-Time認証コードを教えてください

DAY2



Bさん



Cさん



Aさん



Eさん



Dさん

A,C,EさんはSupportDesk-Webログイン時に
BさんからOne-Time認証コードを教えてください

1-5. 共用メールアドレスでの運用方法【特例】

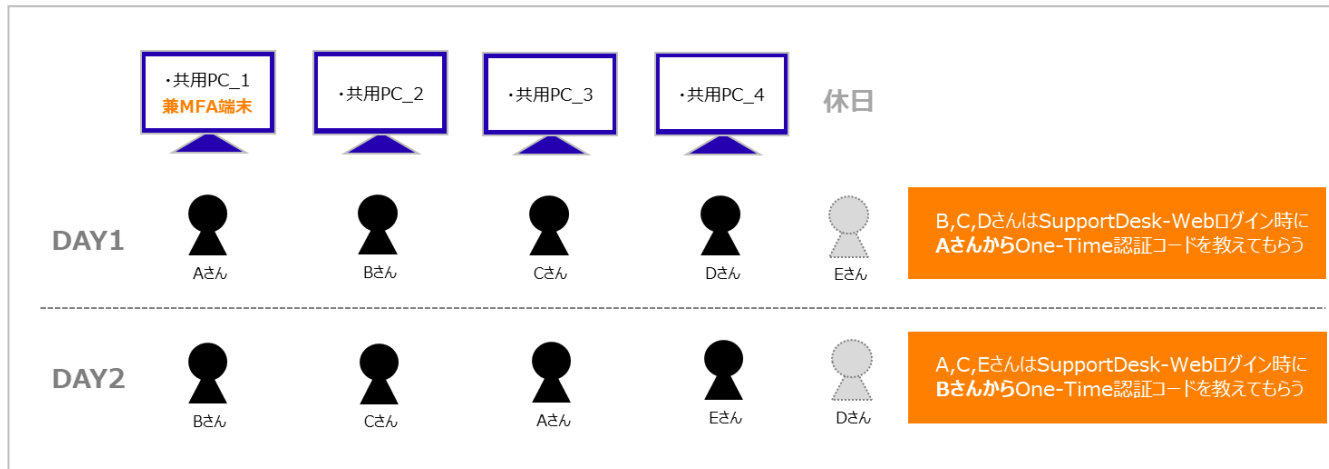
状況

- ✓ 複数人が**同一のメールアドレス**を使用
(注: メーリングリストの利用ではありません)



1つのSalesforceアカウントしか発行できない

- Salesforceは1つのアカウントで複数端末からの同時ログインが可能なため、以下の環境で多要素認証が実現可能です。



注意事項

- ✓ メールアドレスを個人に付与せず共同利用されているお客様に限定した手段です。
セキュリティの観点から、この運用方法を推奨するものではありません。
- ✓ ご登録においては代表者の氏名で申請ください。

1-6. 特例を実施する場合の注意事項

- 複数名で共同利用されているメールアドレスに対して利用者アカウント（Salesforceアカウント）を発行される。



- 利用者アカウント通知のメールが複数名に同時に届く



- 利用者アカウントに対する①パスワード設定②MFA設定が競合する可能性がある。

次章以降で解説する作業は事前に実施者を決めてから進めてください。

2. Salesforce Authenticator を使用する場合

2-1. メール受信から初回ログインまでの流れ

(1) アカウント発行のメールが届きます。

- ・ 件 名 :
【SupportDesk】ご利用開始に関するお知らせ
- ・ 送信元 :
fj-ss-noreply@dl.jp.fujitsu.com

- ・ 内 容 :
●●●●様
SupportDesk-Webへようこそ！
使用を開始するには、以下のURLにアクセスしてください。
※初めてご利用される場合には、パスワード登録画面が表示されます。

<https://xxxxxxxxxxxxx/xxxxxxxxxxxxx/xxxxxxxxxxxxx>

URL

ユーザー名 : zzzzz.yyyyy@fujitsu.com.xxxxxxx.fsdk

以上、よろしくお願いいたします。

(注) 上記はイメージであり実際のメール本文とは異なります。

(2) 本文中のURLにアクセスしてパスワードを設定してください。

(3) 設定完了したら自動で初回ログインされます。

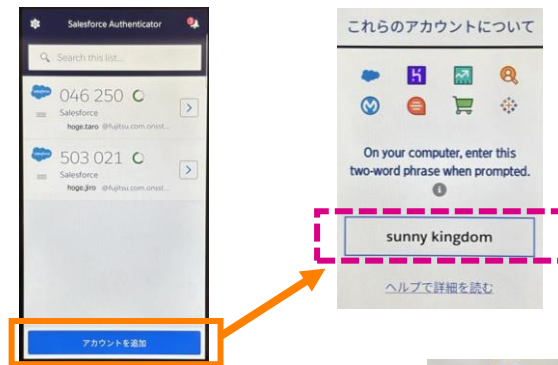
※初回ログインでは多要素認証は行われません

2-2. 2回目ログイン時の流れ

(1) メール本文中のURLにアクセスするとログイン画面が表示されますので、メール本文中のユーザ名（アカウント）とパスワードを入力してください。以下の画面が表示されます。



(2) スマートフォンの「Salesforce Authenticator」を起動して下記の画面で「アカウント追加」をタップすると2語が表示されます。



(3) スマートフォンに表示された2語をPC側のブラウザに入力して「接続」をクリックします。（右画面に遷移）



(4) スマートフォンが右画面に遷移するので「接続」をタップします。



(5) ログインが完了します。



2-3. 3回目以降のログイン（正常系）

- (1) メール本文中のURLにアクセスして、ユーザ名（アカウント）とパスワードを入力してください。以下の画面が表示されます。



- (2) スマートフォンに通知が来るので「承認」をタップしてください。



- (3) ログインされました。



2-3. 3回目以降のログイン（異常系①）

- (1) メール本文中のURLにアクセスして、ユーザ名（アカウント）とパスワードを入力してください。以下の画面が表示されます。



(2) スマートフォンに通知が来ないことがあります。

- (3) 「お困りですか?」をクリックします。

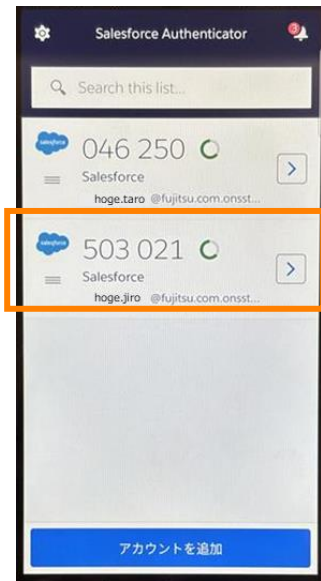


- (4) 「別の検証方法を使用してください」をクリックします。



2-3. 3回目以降のログイン（異常系②）

（５）スマートフォンの「Salesforce Authenticator」を起動して、ログイン対象のアカウントをタップします。



（６）表示されている6桁の数字をPC側のブラウザに入力して「検証」をクリックするとログイン完了です。



アカウントはここで再確認

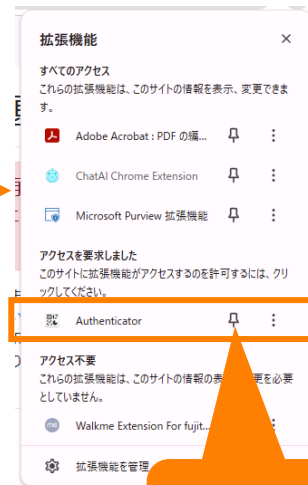
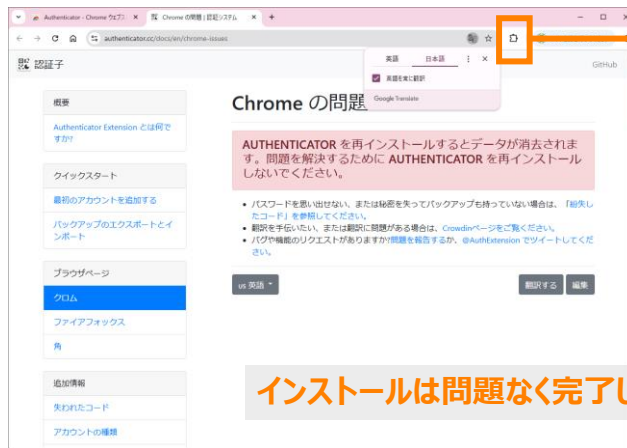
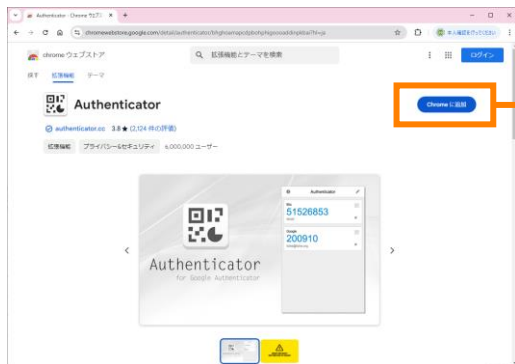


3. Google Chromeの拡張機能を使用する場合 (アカウント発行前の準備作業)

3-1. Google Chromeへの設定

➤ chromeウェブストアから「Authenticator」を追加します。

<https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai?hl=ja>



追加されているので
ピン止めしてください。

4. Google Chromeの拡張機能を使用する場合 (アカウント発行後の設定方法)

4-1. メール受信から初回ログインまでの流れ

(1) アカウントが発行のメールが届きます。

- ・ 件 名 :
【SupportDesk】ご利用開始に関するお知らせ
- ・ 送信元 :
fj-ss-noreply@dl.jp.fujitsu.com

- ・ 内 容 :
●●●● 様
SupportDesk-Webへようこそ！
使用を開始するには、以下のURLにアクセスしてください。
※初めてご利用される場合には、パスワード登録画面が表示されます。

<https://xxxxxxxxxxxxx/xxxxxxxxxxxxx/xxxxxxxxxxxxx>

URL

ユーザー名 : zzzzz.yyyyy@fujitsu.com.xxxxxxx.fsdk

以上、よろしくお願いいたします。

(注) 上記はイメージであり実際のメール本文とは異なります。

(2) 本文中のURLにアクセスしてパスワードを設定してください。

(3) 設定完了したら自動で初回ログインされます。

※初回ログインでは多要素認証は行われません

4-2. 2回目ログイン時の流れ①

(1) メール本文中のURLにアクセスして、メール本文中のユーザ名（アカウント）とパスワードを入力してログインします。

(2) 以下の画面で「別の方法を選択」をクリックします。

Salesforce Authenticator を接続

セキュリティの都合上、Salesforce Authenticator をアカウントに接続する必要があります。アプリケーションから ID の検証が必要になるときに通知が送信され、1 回のステップのみで検証できます。ロケーションサービスを利用して、信頼できる場所からアプリケーションを使用して自動検証することもできます。アプリケーションから、代替検証方法として使用するコードが提供されます。

1. App Store または Google Play からモバイルデバイスに Salesforce Authenticator をインストールします。
2. Salesforce Authenticator を開き、アカウントを追加します。
3. アプリケーションに 2 語の語句が表示されます。ここに語句を入力します。

2 語の語句

キャンセル 接続

別の検証方法を選択

(3) 後者を選択して「次へ」をクリックします。

検証方法を選択してください

ID をどのような方法で検証しますか?

☐ Salesforce Authenticator モバイルアプリケーションを使用

☒ Authenticator アプリケーション (Google Authenticator や Authy など) からの確認コードを使用

次へ

(4) 事前にインストールしてピン止めた Authenticator をクリックします。

サードパーティ Authenticator アプリケーションを Salesforce アカウントに接続して、これを使用して ID を確認できるようにします。

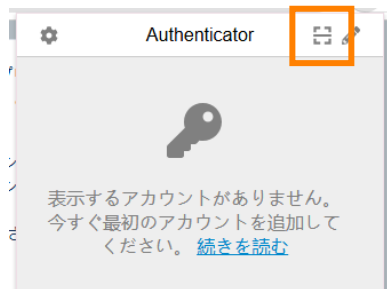
1. Authenticator アプリケーションを開きます。
2. Authenticator アプリケーションを使用してこの QR コードをスキャンします。
3. アプリケーションによって生成されたコードを入力します。

確認コード

QR コードをスキャンできません
別の検証方法を選択

4-2. 2回目ログイン時の流れ②

(5) 「QRコードをスキャン」のアイコンをクリックします。



(6) ナビゲーションの通りにマウスを左クリックしながらQRコードを囲みます。



(7) ポップアップで「OK」をクリックします。



4-2. 2回目ログイン時の流れ③

(8) 表示された6桁の確認コードを入力し、「接続」をクリックします。

認証アプリケーションを接続

サードパーティ Authenticator アプリケーションを Salesforce アカウントに接続して、これを使用して ID を確認できるようにします。

1. Authenticator アプリケーションを開きます。
2. Authenticator アプリケーションを使用してこの QR コードをスキャンします。
3. アプリケーションによって生成されたコードを入力します。

983053

戻る 接続

(9) ログイン完了です。

SupportDesk Web

SupportDeskをご契約のお客様をサポートする専用ホームページです

サポートメニュー

- ご契約確認・製品サポート情報**
お客様ご契約製品の一覧、および各製品に対するセキュリティパッチ/修正/アップグレード等のサポート情報が確認できます。
- ご契約製品に関するお問い合わせ**
選択した製品から、お問い合わせ・修理申し込みができます。
- ご利用者情報管理**
ご利用者情報の参照、編集ができます。また、アクセス管理機能をお持ちの場合は、利用者管理（登録/削除/Welcomeメール再送など）ができます。
- サービス全般に関するお問い合わせ・お申込み**
ご利用方法・ご契約内容・ご利用IDに関するお問い合わせ・お申込みができます。
- お問合せ履歴**
お問い合わせ履歴の確認と、未完了のお問い合わせに対する追加補修/追加資料のアップロードができます。
- 保守サービス報告書の参照**
製品修理や定期保守、障害修正の適用などを実施した際に発行している「保守サービス報告書」をWebで参照できます。作業開始日や対象設備、作業内容などの報告をご確認いただけます。

複数アカウントを登録した場合はアカウントの数だけ確認コードが表示されます。@以前で照合して適切に選出します。

4-3. 3回目以降のログイン

(1) メール本文中のURLにアクセスして、ユーザ名（アカウント）とパスワードを入力してください。

(2) 以下の画面で
Authenticatorをクリックします。

(3) 表示された6桁の確認コードを入力し、
「検証」をクリックします。

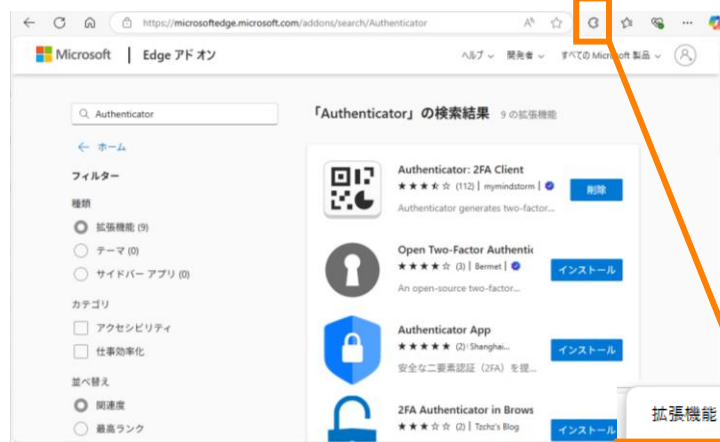
(4) ログイン完了です。

複数アカウントを登録した場合はアカウントの数だけ確認コードが表示されます。
@以前で照合して適切に選出します。

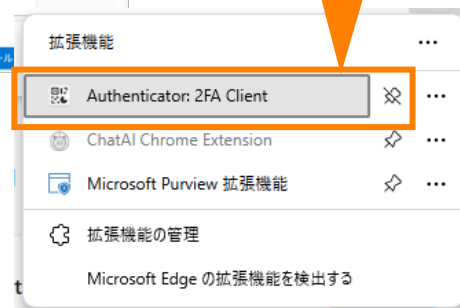
5. Microsoft Edgeの拡張機能を使用する場合 (アカウント発行前の準備作業)

5-1. Microsoft Edge への設定

- Edgeアドオンストアから「Authenticator:2FA Client」を追加します。
[Microsoft Edge アドオン - Authenticator](#)



追加されているので
ピン止めしてください。



6. Microsoft Edgeの拡張機能を使用する場合 (アカウント発行後の設定方法)

6-1. メール受信から初回ログインまでの流れ

(1) アカウントが発行のメールが届きます。

- ・ 件 名 :
【SupportDesk】ご利用開始に関するお知らせ
- ・ 送信元 :
fj-ss-noreply@dl.jp.fujitsu.com

- ・ 内 容 :
●●●●様
SupportDesk-Webへようこそ!
使用を開始するには、以下のURLにアクセスしてください。
※初めてご利用される場合には、パスワード登録画面が表示されます。

<https://xxxxxxxxxxxxx/xxxxxxxxxxxxx/xxxxxxxxxxxxx>

URL

ユーザー名 : zzzzz.yyyyyy@fujitsu.com.xxxxxxx.fsdk

以上、よろしくお願いいたします。

(2) 本文中のURLにアクセスしてパスワードを設定してください。

(3) 設定完了したら自動で初回ログインされます。

(注) 上記はイメージであり実際のメール本文とは異なります。

※初回ログインでは多要素認証は行われません

6-2. 2回目ログイン時の流れ①

(1) メール本文中のURLにアクセスして、メール本文中のユーザ名（アカウント）とパスワードを入力してログインします。

(2) 以下の画面で「別の方法を選択」をクリックします。

Salesforce Authenticator を接続

セキュリティの都合上、Salesforce Authenticator をアカウントに接続する必要があります。アプリケーションから ID の検証が必要になるときに通知が送信され、1 回のステップのみで検証できます。ロケーションサービスを利用して、信頼できる場所からアプリケーションを使用すると、自動検証することもできます。アプリケーションから、代替検証方法として使用するコードが提供されます。

1. App Store または Google Play からモバイルデバイスに Salesforce Authenticator をインストールします。
2. Salesforce Authenticator を開き、アカウントを追加します。
3. アプリケーションに 2 語の語句が表示されます。ここに語句を入力します。

2 語の語句

キャンセル 接続

別の検証方法を選択

(3) 後者を選択して「次へ」をクリックします。

検証方法を選択してください

ID をどのような方法で検証しますか?

☐ Salesforce Authenticator モバイルアプリケーションを使用

☒ Authenticator アプリケーション (Google Authenticator や Authy など) からの確認コードを使用

次へ

(4) 事前にインストールしてピン止めた Authenticator をクリックします。

サードパーティ Authenticator アプリケーションを Salesforce アカウントに接続して、これを使用して ID を確認できるようにします。

1. Authenticator アプリケーションを開きます。
2. Authenticator アプリケーションを使用してこの QR コードをスキャンします。
3. アプリケーションによって生成されたコードを入力します。

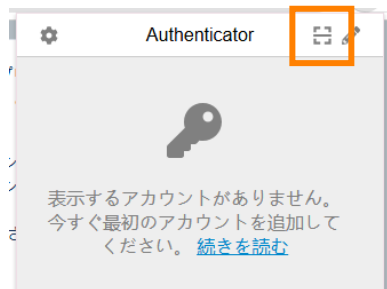
確認コード

戻る 接続

QR コードをスキャンできません
別の検証方法を選択

6-2. 2回目ログイン時の流れ②

(5) 「QRコードをスキャン」のアイコンをクリックします。



(6) ナビゲーションの通りにマウスを左クリックしながらQRコードを囲みます。



(7) ポップアップで「OK」をクリックします。



6-2. 2回目ログイン時の流れ③

(8) 表示された6桁の確認コードを入力し、「接続」をクリックします。

認証アプリケーションを接続

サードパーティ Authenticator アプリケーションを Salesforce アカウントに接続して、これを使用して ID を確認できるようにします。

1. Authenticator アプリケーションを開きます。
2. Authenticator アプリケーションを使用してこの QR コードをスキャンします。
3. アプリケーションによって生成されたコードを入力します。

確認コード

983053

戻る 接続

(9) ログイン完了です。

SupportDesk Web

SupportDeskをご契約のお客様をサポートする専用ホームページです

サポートメニュー

- ご契約確認・製品サポート情報**
お客様ご契約製品の一覧、および各製品に対するセキュリティパッチ/アップグレード等のサポート情報が確認できます。
- ご契約製品に関するお問合せ**
選択した製品から、お問合せ・修理申し込みができます。
- ご利用者情報管理**
ご利用者情報の参照、編集ができます。また、アクセス管理機能をお持ちの場合は、利用者管理（登録/削除/Welcomeメール再送など）ができます。
- サービス全般に関するお問合せ・お申込み**
ご利用方法・ご契約内容・ご利用IDに関するお問合せ・お申込みができます。
- お問合せ履歴**
お問合せ履歴の確認と、未完了のお問合せに対する追加補修/追加資料のアップロードができます。
- 保守サービス報告書の参照**
製品修理や定期保守、障害修正の適用などを実施した際に発行している「保守サービス報告書」をWebで参照できます。作業開始日や対象設備、作業内容などの報告をご確認いただけます。

複数アカウントを登録した場合はアカウントの数だけ確認コードが表示されます。@以前で照合して適切に選出します。

6-3. 3回目以降のログイン

(1) メール本文中のURLにアクセスして、ユーザ名（アカウント）とパスワードを入力してください。

(2) 以下の画面で
Authenticatorをクリックします。



(3) 表示された6桁の確認コードを入力し、
「検証」をクリックします。



(4) ログイン完了です。



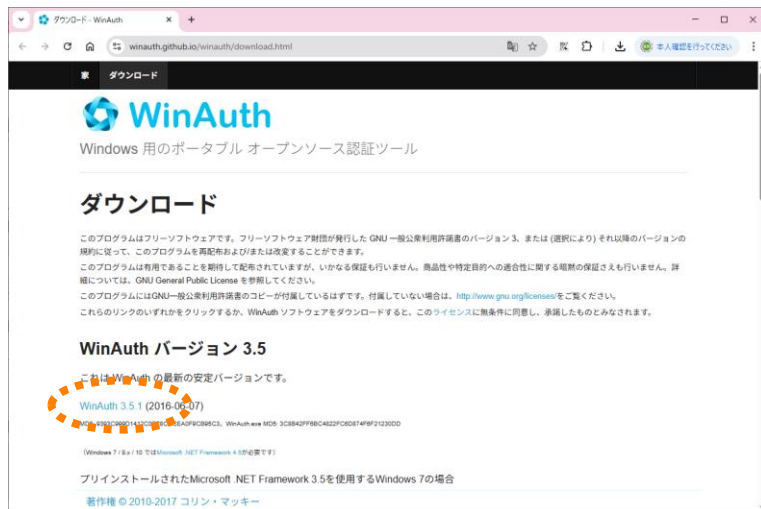
複数アカウントを登録した場合はアカウントの数だけ確認コードが表示されます。
@以前で照合して適切に選出します。

7. WinAuthを使用する場合 (アカウント発行前の準備作業)

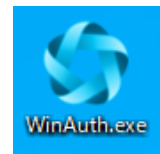
7-1. WinAuthの導入

(1) 以下のサイトよりWinAuthのZipファイルをダウンロードします。

・<https://winauth.github.io/winauth/download.html>



(2) Zipファイルを展開してデスクトップなど
任意の場所にソフトを格納します。



8. WinAuthを使用する場合 (アカウント発行後の設定方法)

8-1. メール受信から初回ログインまでの流れ

(1) アカウントが発行のメールが届きます。

- ・ 件 名 :
【SupportDesk】ご利用開始に関するお知らせ
- ・ 送信元 :
fj-ss-noreply@dl.jp.fujitsu.com

- ・ 内 容 :
●●●● 様
SupportDesk-Webへようこそ!
使用を開始するには、以下のURLにアクセスしてください。
※初めてご利用される場合には、パスワード登録画面が表示されます。

<https://xxxxxxxxxxxxx/xxxxxxxxxxxxx/xxxxxxxxxxxxx>

URL

ユーザー名 : zzzzz.yyyyy@fujitsu.com.xxxxxxx.fsdk

以上、よろしくお願いいたします。

(注) 上記はイメージであり実際のメール本文とは異なります。

(2) 本文中のURLにアクセスしてパスワードを設定してください。

(3) 設定完了したら自動で初回ログインされます。

※初回ログインでは多要素認証は行われません

8-2. 2回目ログイン時の流れ①

(1) メール本文中のURLにアクセスして、メール本文中のユーザ名（アカウント）とパスワードを入力してログインします。

(2) 以下の画面で「別の検証方法を選択」をクリックします。

Salesforce Authenticator を接続

セキュリティの都合上、Salesforce Authenticator をアカウントに接続する必要があります。アプリケーションから ID の検証が必要なときに通知が送信され、1 回のタップのみで検証できます。ロケーションサービスを使用し、接続できる場所からアプリケーションを使用して自動検証することもできます。アプリケーションから、代替検証方法として使用するコードが提供されます。

1. App Store または Google Play からモバイルデバイスに Salesforce Authenticator をインストールします。
2. Salesforce Authenticator を開き、アカウントを追加します。
3. アプリケーションに 2 語の語句が表示されます。ここに語句を入力します。

2 語の語句

|

キャンセル 接続

別の検証方法を選択

(3) 後者を選択して「次へ」をクリックします。

検証方法を選択してください

ID をどのような方法で検証しますか?

☐ Salesforce Authenticator モバイルアプリケーションを使用

☒ Authenticator アプリケーション (Google Authenticator や Authy など) からの確認コードを使用

次へ

(4) 「QRコードをスキャンできません」をクリックします。

認証アプリケーションを接続

サードパーティ Authenticator アプリケーションを Salesforce アカウントに接続して、これを使用して ID を確認できるようにします。

1. Authenticator アプリケーションを開きます。
2. Authenticator アプリケーションを使用してこの QR コードをスキャンします。
3. アプリケーションによって生成されたコードを入力します。



確認コード

戻る 接続

QR コードをスキャンできません

8-2. 2回目ログイン時の流れ②

- (5) 下記の画面が表示されます。
「キー」をコピーします。

認証アプリケーションを接続

モバイルデバイスの認証アプリケーションに移動し、このキーを入力します。

一部のバージョンの Salesforce Authenticator では、手動のキー入力はサポートされていません。別のアプリケーションを使用するか、Salesforce システム管理者にお問い合わせください。

キー

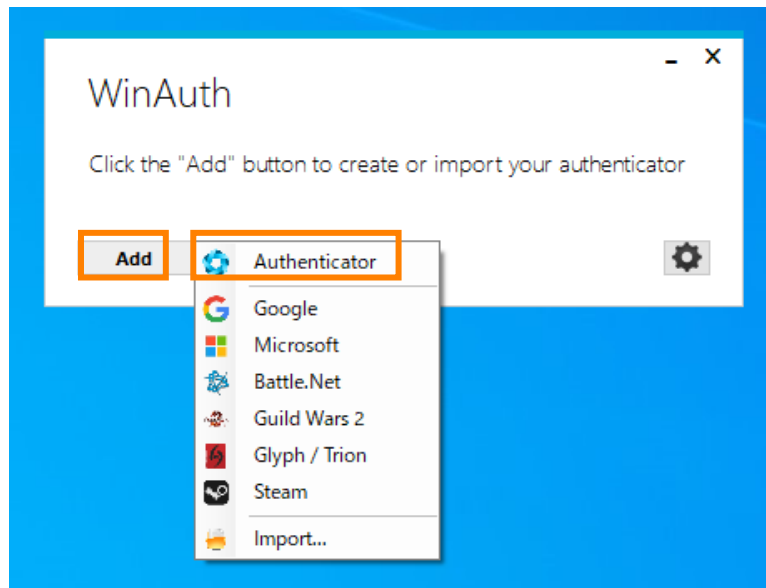
K3V2LYZ5EZOP4BM5BO644D7XYC7YZ5Q6

アプリケーションに表示される確認コードを入力します。

確認コード

戻る 接続

- (6) WinAuthを起動して「Add」をクリックします。
さらに「Authenticator」をクリックします。



8-2. 2回目ログイン時の流れ③

(7) 下記の画面が表示されます。

Add Authenticator

Name: SDKアカウント1

1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.

K3V2LYZSEZOP4BMSBO644D7XVC7YZSQ6

Decode

2. Choose if this is a time-based or a counter-based authenticator. If you don't know, it's likely time-based, so just leave the default choice.

☒ Time-based ☐ Counter-based

3. Click the Verify button to check the first code.

Verify Authenticator

4. Verify the following code matches your service.

OK Cancel



Add Authenticator

Name: SDKアカウント1

1. Enter the Secret Code for your authenticator. Spaces don't matter. If you have a QR code, you can paste the URL of the image instead.

K3V2LYZSEZOP4BMSBO644D7XVC7YZSQ6

Decode

2. Choose if this is a time-based or a counter-based authenticator. If you don't know, it's likely time-based, so just leave the default choice.

☒ Time-based ☐ Counter-based

3. Click the Verify button to check the first code.

Verify Authenticator

4. Verify the following code matches your service.

238 168

OK Cancel

① アカウントを識別できる任意の名称を入力

② 手順（5）でコピーしたものをペースト

③ クリック

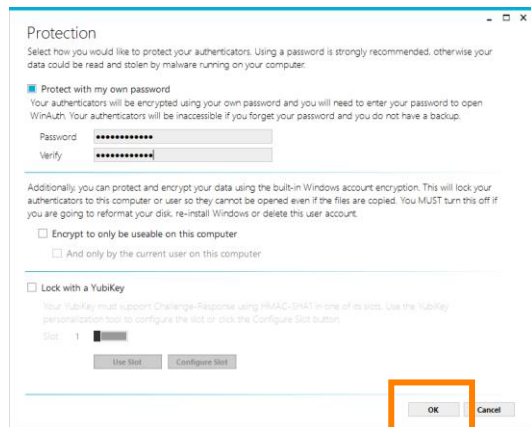
④ デフォルトのまま

⑤ クリック

⑥ クリック

8-2. 2回目ログイン時の流れ④

(8) Win-Auth起動時のパスワードを設定して「OK」をクリックします。



(9) 6桁のCodeが表示されます。



(10) Salesforceの画面に入力して「接続」をクリックします。



ログイン完了です

8-3. 3回目以降のログイン

(1) WinAuthを起動します。



複数アカウントを登録した場合はアカウントの数だけ確認コードが表示されます。

(2) メール本文中のURLにアクセスして、ユーザ名（アカウント）とパスワードを入力してください。

(3) WinAuthに表示されたCodeを入力して「**接続**」をクリックします。

A screenshot of the 'IDを検証' (Verify ID) screen. It says 'SDKWEB にログインしようとしています。アカウントの安全性を確保するために、IDを検証する必要があります。' (Attempting to log in to SDKWEB. To ensure account security, ID verification is required.) and 'モバイルデバイスで認証アプリケーションを使用して、確認コードを生成します。' (Use a mobile device authentication application to generate a verification code.) It shows 'ユーザー名' (Username) as 'SDKアカウント1' and '確認コード' (Verification code) as '064848'. A blue '検証' (Verify) button is highlighted with an orange box.

ログイン完了です

Thank You

