

ご契約者各位



Okta Verifyアプリのセットアップと
オプション管理コンソールへのサインイン手順

株式会社AXSEED

2025年2月25日



1. [はじめに](#)
2. [「Okta Verify」アプリのセットアップ](#)
3. [オプション管理コンソールへのサインイン](#)
4. [「Okta Verify」アプリの設定解除（アカウント削除）](#)
5. [「Okta Verify」アプリの復旧](#)

はじめに

2025年2月26日（水）より SPPM3.0はセキュリティ強化のため、ユーザー管理機能の一つである「オプション管理コンソール」（Okta管理コンソール）へのサインインに2要素認証を導入します。
※SPPM管理画面へのサインインには影響ございません。

以下いずれかのプラン、またはシングルサインオンオプションをご契約のお客様が対象となります。

- SPPM Security One
- Secure SSO（SSO無制限）
- Secure MFA（多要素認証）
- Secure LCM（ライフサイクル管理）

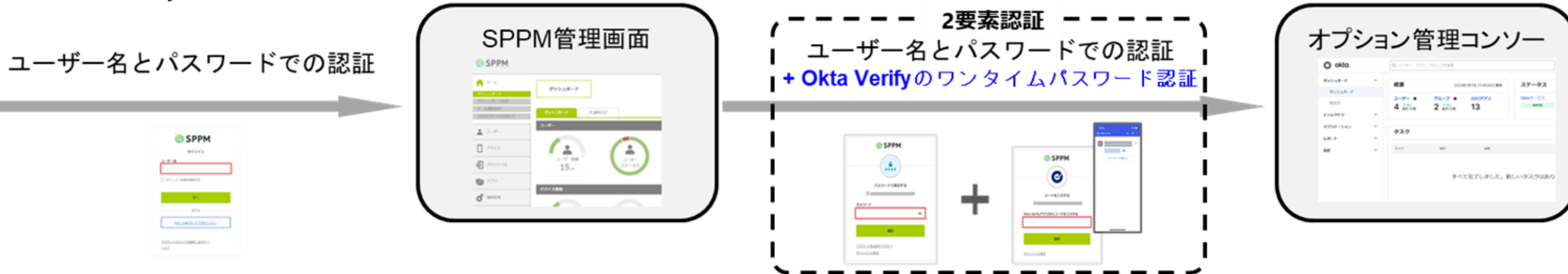
本マニュアルでは2要素認証として利用する「Okta Verify」アプリのセットアップ/設定解除/復旧の手順と「オプション管理コンソール」へのサインイン手順について説明します。

2要素認証とは

知識情報、所持情報、生体情報などの2つを組み合わせる本人認証をする仕組みです。

ユーザー名とパスワードのみでの認証に比べ、セキュリティが強化されます。

SPPMのオプション管理コンソールでは、これまでのユーザー名とパスワードでの認証に加え、Okta Verifyアプリを用いたワンタイムパスワードでの認証が追加されます。



※**デバイス認証を用いてサインインする場合はOkta Verifyアプリでの認証が不要となります。**

（「デバイス認証」と「ユーザー名とパスワードでの認証」により2要素認証の要件を満たすため）

デバイス認証を利用するためには、サインインに利用するデバイスをSPPMの管理デバイスとして登録し、ユーザーに割り当てる必要がございます。詳細は[オンラインマニュアル8.2.1](#)をご確認ください。

Okta Verifyアプリは、Okta社が提供する多要素認証(MFA)アプリです。
Okta Verifyアプリを使用するとオプション管理コンソールへのサインイン時に
本人確認が実施されるため、ユーザーになりすました人物がアカウントに
アクセスできる可能性は低くなります。
SPPMではOkta Verifyアプリのワンタイムパスワード機能を利用します。

注意事項

Okta Verifyの設定にはモバイルデバイス（iOS/Android*）が必要です。
これはSPPMで管理しているデバイスで設定する必要はございませんが
Okta Verifyを設定した状態でデバイスの初期化やアプリの削除を行った場合、
オプション管理コンソールへサインインできなくなる可能性があります。

（詳細は「4.「Okta Verify」アプリの設定解除（アカウント削除）」 および「5.「Okta Verify」アプリの復旧」をご確認ください）

以上ご留意の上デバイスをご選択くださいますようお願いいたします。

*サポートOS

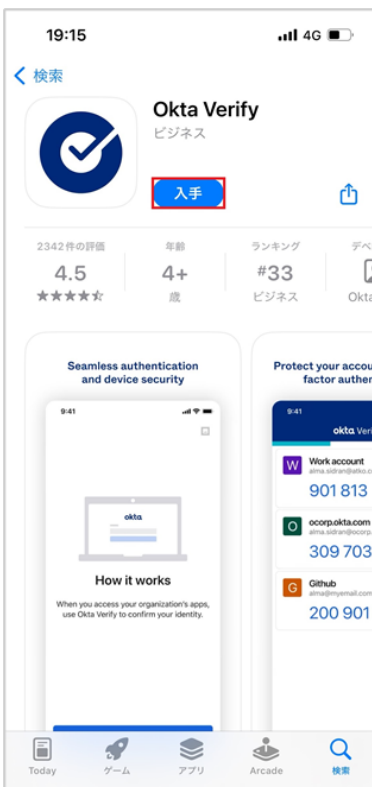
iOS : 過去2年以内に一般向けにリリースされたOSのメジャーバージョン

Android : 過去3年以内に一般向けにリリースされたOSのメジャーバージョン

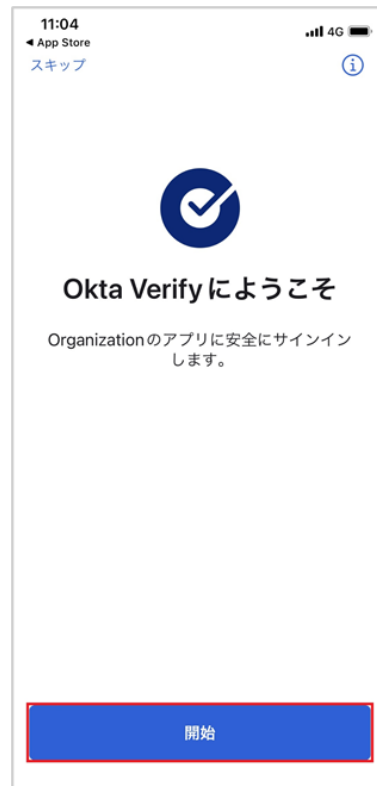


「Okta Verify」アプリのセットアップ

1. iOSまたはAndroidデバイスにOkta Verifyアプリをインストールします。
ここでは、例としてiPhoneの画面を使用します。
※SPPM管理デバイスの場合、アプリを配布してインストールすることも可能です。



2. 「Okta Verify」アイコンをタップし、アプリを起動します。
3. 「Okta Verifyによるこそ」の画面で「開始」ボタンをタップします。
4. 「仕組み」画面で「次へ」をタップします。



5. 「確認方法」画面で「アカウントの追加」をタップします。
6. 「アカウントの種類を選択」画面の「会社名」をタップします。
7. 「別のデバイスからアカウントを追加しますか？」画面の「スキップ」をタップします。



8. 「QRコードをお持ちですか？」画面の「はい、スキャンできます」をタップします。
9. 「QRコードをスキャンする」画面で、「"Okta Verify"がカメラへのアクセスを求めています」の画面が表示されたら、「OK」をタップします。



10. パソコン上でWebブラウザを起動し、SPPM管理画面にアクセスします。

※スマートフォンでの操作からパソコンでの操作に切り替わります。

SPPM管理画面へサインインし、以下いずれかの手順でオプション管理コンソールへアクセスします。

A. ユーザー > オプション設定 > 「オプション管理コンソールへ遷移」 をクリック

B. 設定 > 契約情報 > ユーザー（タブ） > オプション管理コンソール のリンクをクリック

※SPPM管理画面のURLとサインイン情報は、登録通知書の【管理者様情報】

「SPPM管理者サイト」をご確認ください。



11. 「サインイン」画面が表示された場合は、SPPM管理画面へのサインインに用いるユーザー名を入力し「次へ」をクリックします。
12. 「パスワードで確認する」画面でSPPM3.0管理画面で用いるパスワードを入力し、「確認」をクリックします。
13. 「セキュリティ方式の設定」画面でOkta Verifyの「セットアップ」をクリックします。



The image shows a sequence of three screenshots from the SPPM (Security Policy Platform Manager) interface, connected by arrows indicating the flow of the setup process.

Screenshot 1: Sign In (サインイン)

- Header: SPPM
- Section: サインイン
- Form: ユーザー名 (User Name) input field (highlighted with a red border).
- Checkbox: ☐ サインイン状態を維持する (Keep signed in).
- Button: 次へ (Next) (green).
- Text: または (or).
- Link: [PIV / CACカードでサインイン](#) (Sign in with PIV / CAC card) (blue border).
- Footer: [アカウントのロックを解除しますか?](#) (Unlock account?) and [ヘルプ](#) (Help).

Screenshot 2: Password Confirmation (パスワードで確認する)

- Header: SPPM
- Image: Lock icon with **** (password masked).
- Section: パスワードで確認する (Confirm with password).
- Form: Password input field (highlighted with a red border).
- Button: 確認 (Confirm) (green).
- Footer: [パスワードをお忘れですか?](#) (Forgot password?) and [サインインに戻る](#) (Return to sign in).

Screenshot 3: Security Settings (セキュリティ方式の設定)

- Header: SPPM
- Section: セキュリティ方式の設定 (Security settings).
- Form: Selection field (highlighted with a red border).
- Text: セキュリティ方式により、自分だけがアクセス可能なことを保証し、Oktaアカウントを保護できます。 (By using security settings, you can ensure that only you can access and protect your Okta account.)
- Section: セットアップが必要です (Setup required).
- Option: ☒ Okta Verify (Okta Verify is a verification app that can be installed on your mobile phone and used for ID verification. It will be used for access.)
- Button: [セットアップ](#) (Setup) (red border).
- Footer: [サインインに戻ります](#) (Return to sign in).

14. 「Okta Verifyの設定」画面でQRコードが表示されます。
※パソコンでの操作から、スマートフォンの操作に切り替わります。
15. 手順9でセットアップ中のスマートフォンでパソコンの画面に表示されているQRコードを映します。
16. 「プッシュ通知を許可しますか？」画面で「許可する」をタップします。



17. 「"Okta Verify"は通知を送信します。よろしいですか？」画面で「許可」をタップします。
18. 「Face IDによる確認を有効にしますか？」画面で「有効にする」をタップします。
19. 「"Okta Verify"にFace IDの使用を許可しますか？」の画面で「OK」をタップします。

※生体認証の有無や種類によりメッセージが異なる場合がございます。

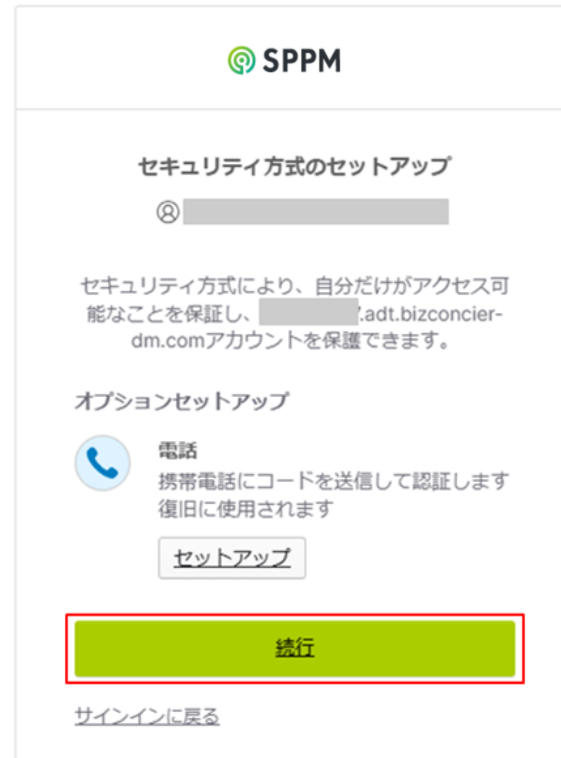
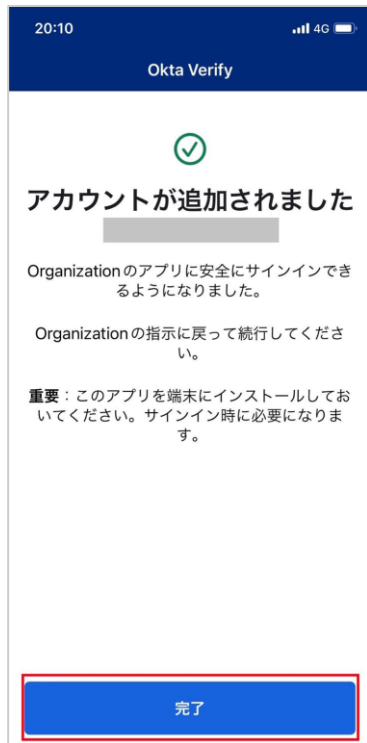


20. 「アカウントが追加されました」画面で「完了」をタップします。

※スマートフォンで完了をタップした後にパソコンの画面が切り替わります。

21. 「セキュリティ方式のセットアップ」画面で「続行」をタップします。

22. 「オプション管理コンソール」画面へ遷移します。セットアップおよび初回サインインが完了です。



オプション管理コンソールへのサインイン

1. SPPM管理画面へサインインし、以下いずれかの手順でオプション管理コンソールへアクセスします。
 - A. ユーザー > オプション設定 > 「オプション管理コンソールへ遷移」 をクリック
 - B. 設定 > 契約情報 > ユーザー（タブ） > オプション管理コンソール のリンクをクリック
2. 「サインイン」画面が表示された場合は、SPPM管理画面へのサインインに用いるユーザー名を入力し「次へ」をクリックします。
3. 「パスワードで確認する」画面でSPPM管理画面で用いるパスワードを入力し、「確認」をクリックします。



4. 「コードを入力する」画面でOkta Verifyアプリの6桁のワンタイムパスワード入力し、「確認」をクリックします。
5. 「オプション管理コンソール」画面へ遷移します。



「Okta Verify」アプリの設定解除 (アカウント削除)

設定解除（アカウント削除）

デバイスの初期化やアプリの削除を実施する場合、必ず事前に以下の手順を実行してください。

1. Okta Verifyアプリを起動し、セットアップしたアカウントを選択します。
2. 「アカウントの詳細」画面で「アカウントを削除する」を選択します。
3. 「アカウントの削除」の画面で「削除」を選択します。
4. アカウントの一覧画面から該当アカウントの表示がなくなっていれば設定解除は完了です。



「Okta Verify」アプリの復旧

Okta Verifyアプリ上でワンタイムパスワードを確認できないなどの理由により
オプション管理コンソールへサインインできなくなった場合、以下手順をお試しください。

1. Okta Verifyアプリを設定した管理者アカウントのデバイス（タブ）を開きます。
ユーザー > ユーザー管理 > ユーザー一覧 > 任意のユーザーIDを選択 > デバイス（タブ）
2. 「認証アプリ導入済みデバイス」でOkta Verifyを設定したデバイスを選択し、「リセット」をクリックします。



3. 「リセット」の画面で、デバイス情報を再度確認し、「OK」をクリックします。
4. 「認証アプリ導入済みデバイス」にデバイスの表示がなくなっていることを確認します。
5. 「2. 「Okta Verify」アプリのセットアップ」をご参考に、Okta Verifyアプリの再設定をお試しく下さい。

※ 「MDM管理デバイス」ではなく、「認証アプリ導入済みデバイス」からご選択ください。
 「認証アプリ導入済みデバイス」のリセットによりSPPM3.0の管理デバイスから削除されることはございません。



AXSEED