



【Microsoft 365】SMS 認証および 音声通話認証の廃止とパスキー移行

2026年09月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年09月30日	初版発行

本書の内容は 2026/09/30 時点のものです。製品のアップデートにより変更となる場合がある旨、ご了承ください。

Agenda

1. 前提情報
 1. 本書の目的
 2. 用語集
2. SMS 認証および音声通話認証が廃止に
 1. SMS 認証および音声通話認証の廃止の背景
 2. 廃止に伴う変更内容
 3. 廃止までのロードマップ
 4. 影響範囲
 5. SMS 認証および音声通話認証を継続利用する場合
3. パスキーとは
 1. パスキーとは
 2. 利用できるパスキー
 3. Microsoft が推奨する認証方式
4. パスキー登録方法
 1. パスキー登録手順
 2. 登録キャンペーンによる登録手順
 3. 登録後の利用方法
5. よくある質問
 1. ユーザー目線でのよくある質問
 2. 管理者目線でのよくある質問



1. 前提情報

1.1. 本書の目的

目的

本書は、Microsoft 365 における SMS 認証および音声通話認証の廃止背景や変更内容、影響範囲を理解するとともに、代替認証方式として推奨されるパスキーの概要や利用方法、今後必要となる対応を理解することを目的としています。

※本書で扱う内容は、2026/09/25 現在の情報となります。
今後仕様や動作が変更される可能性があります。
実際の導入や運用にあたっては、最新の公式ドキュメントをご確認ください。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	認証基盤	ユーザーの本人確認やアクセス制御を実施するためのシステム基盤。
2	Microsoft Entra ID	Microsoft が提供する、ユーザー認証やアクセス制御のためのクラウド型 ID・アクセス管理サービス。
3	Microsoft Entra 管理センター	Microsoft Entra ID の設定や認証ポリシー、ユーザーやグループを管理するための管理ポータル。
4	SMS 認証	SMS で受信した認証コードを利用して本人確認を行う認証方式。
5	音声通話認証	電話による音声案内や確認を利用して本人確認を行う認証方式。
6	多要素認証（MFA）	複数の認証要素を組み合わせる本人確認を行う認証方式。
7	サイバー攻撃	システムやアカウントを不正利用することを目的とした攻撃行為。
8	Microsoft Authenticator	多要素認証やパスキー認証を提供する Microsoft 公式認証アプリ。
9	PIN	デバイス上で本人確認を行うための数字や文字列による認証情報。
10	FIDO2 標準	パスワードレス認証を実現するための国際標準認証規格。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
11	Apple iCloud キーチェーン	Apple デバイス間でパスキーやパスワードを同期する認証情報管理サービス。
12	Google パスワードマネージャー	Google アカウントでパスキーやパスワードを同期・管理するサービス。
13	電子メール OTP	電子メールで受信したワンタイムパスワードを利用する認証方式。
14	リモートフィッシング攻撃	偽の Web サイトやサインイン画面を利用して、認証情報や認証コードを不正に取得するサイバー攻撃。
15	CBA (Certificate-Based Authentication)	デジタル証明書を利用して本人確認を行う認証方式。
16	一時アクセスパス	初回登録や認証方法再設定時に利用する一時的なサインイン用パスコード。
17	テレフォニープロバイダー	SMS や音声通話を配信する通信サービス事業者。
18	セルフサービスパスワードリセット (SSPR)	ユーザー自身でパスワードをリセットできる機能。
19	Microsoft Security Store	SMS 認証や音声通話認証の継続利用に必要なテレフォニープロバイダーを選択できる Microsoft のマーケットプレイス。



2. SMS 認証および音声通話認証が 廃止に

2.1. SMS 認証および音声通話認証の廃止の背景

SMS 認証および音声通話認証は、MFA として広く利用されてきましたが、近年のサイバー攻撃の高度化により十分なセキュリティを確保することが難しくなっています。

そのため、Microsoft は認証基盤のセキュリティ強化を目的に、Microsoft Entra ID で提供する多要素認証（以降、MFA）の SMS 認証および音声通話認証のサポートを終了します。

主なリスク

フィッシング攻撃



偽のサインイン画面を利用して、認証コードを盗み取られる可能性があります。

AI を活用した攻撃



生成 AI や自動化ツールの悪用により、攻撃の規模と頻度が増加しています。

SIM スワップ攻撃



電話番号を不正に乗っ取られ、攻撃者が認証コードを受け取ってしまうリスクがあります。

ソーシャルエンジニアリング



利用者を騙して認証コードを聞き出す手口や、なりすましによる不正利用のリスクがあります。

認証情報の窃取



認証コードの窃取により、アカウント乗っ取りや不正利用のリスクが高まります。

POINT

Microsoft は、SMS 認証および音声通話認証を段階的に廃止し、より安全性の高い認証方式への移行を進めています。

2.2. 廃止に伴う変更内容

SMS 認証および音声通話認証は MFA として利用できなくなるため、パスキーなどの Microsoft 推奨の認証方式への移行が必要です。

変更前

Microsoft が提供する SMS 認証および音声通話認証を MFA として利用可能



SMS 認証



音声通話認証



変更後

Microsoft が提供する SMS 認証および音声通話認証を MFA として**利用不可**
より安全な認証方式（パスキーなど）への移行が必要



SMS 認証



音声通話認証

2027 年 2 月 1 日以降



一般ユーザー
(社内ユーザー)



内部ゲスト
ユーザー

2027 年 7 月 1 日以降



グローバル
管理者



外部ユーザー

2.3. 廃止までのロードマップ

2026 年 9 月からパスキーへの移行が開始され、2027 年 2 月より順次、Microsoft 提供の SMS 認証および音声通話認証が終了します。本ページは[こちら](#)を参考にまとめています。

2026 年 9 月 1 日



1

パスキーが自動で有効化

SMS 認証および音声通話認証を利用しているユーザーは、パスキーの利用対象に自動で追加されます。

サインイン時にパスキー登録を促す案内が表示されます。

2026 年 9 月 18 日



2

テレフォニープロバイダーの一覧公開

SMS 認証および音声通話認証を継続利用する場合に必要な、対応するテレフォニープロバイダーの一覧が公開されます。

価格、サポート、対応するテレフォニープロバイダーを確認できます。

2026 年 10 月 30 日



3

テレフォニープロバイダーの構成開始

Microsoft Security Store を通じて、テレフォニープロバイダーを選択し、構成を行えるようになります。

継続して SMS 認証および音声通話認証を利用する場合は、事前の構成が必要です。

2027 年 2 月 1 日



4

対象ユーザー以外 SMS 認証および音声通話 認証が終了

グローバル管理者と外部ユーザーを除くすべてのユーザーに対して SMS 認証および音声通話認証は利用できなくなります。

SMS 認証および音声通話認証を利用している対象ユーザーはパスキーを含む推奨認証方式への移行が必要です。

2027 年 7 月 1 日



5

全ユーザー SMS 認証および音声通話 認証が終了

全ユーザーに対して SMS 認証および音声通話認証は利用できなくなります。

SMS 認証および音声通話認証を利用しているユーザーはパスキーを含む推奨認証方式への移行が必要です。

2.4. 影響範囲

SMS 認証および音声通話認証を利用しているユーザーは、認証方式を変更する必要があります。なお、パスキーや Microsoft Authenticator での認証方式を利用している場合は、引き続き認証方式を利用することができます。

影響を受けるユーザー

詳細

以下の認証方式を利用しているユーザーは直接的な影響を受けます。

- SMS による認証コードの受信
- 音声通話による認証コード・確認電話の受信
- 既定の認証方式としての SMS 認証または音声通話認証の利用

想定される影響

- SMS または音声通話による認証が利用できなくなります。
- パスキーなど別の認証方式への登録が必要になります。
- 登録キャンペーンなどを通じて認証方式の変更を求められる場合があります。

影響を受けないユーザー

詳細

以下の認証方式を利用しているユーザーは今回の廃止の直接的な影響を受けません。

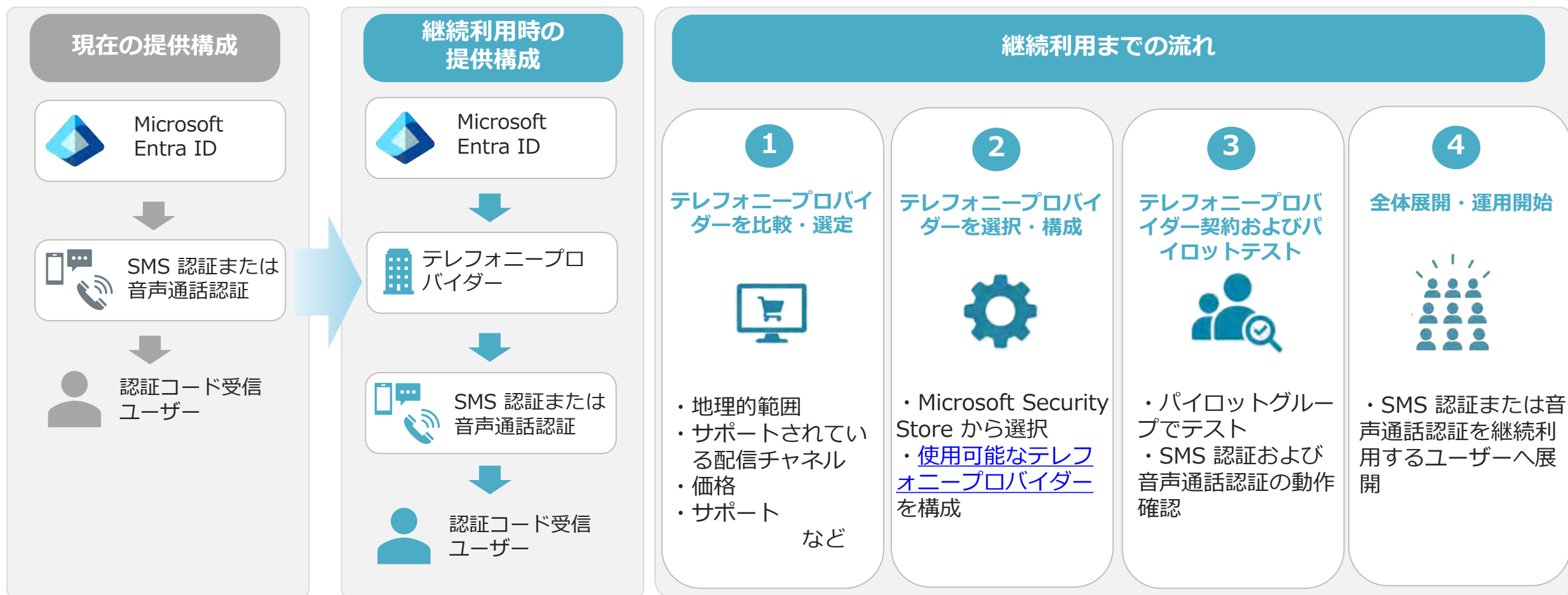
- パスキー
- Windows Hello for Business
- FIDO2 セキュリティキー
- Microsoft Authenticator

補足

- 上記の認証方式は Microsoft が推奨する認証方式として引き続き利用できます。
- 特にパスキー、Windows Hello for Business、FIDO2 セキュリティキーは、フィッシング耐性のある認証方式として Microsoft が推奨しています。

2.5. SMS 認証および音声通話認証を継続利用する場合

規制、技術、業務上の理由で SMS 認証および音声通話認証を維持する必要がある場合は、Microsoft Security Store から対応するテレフォニープロバイダーを選択し、契約・構成する必要があります。



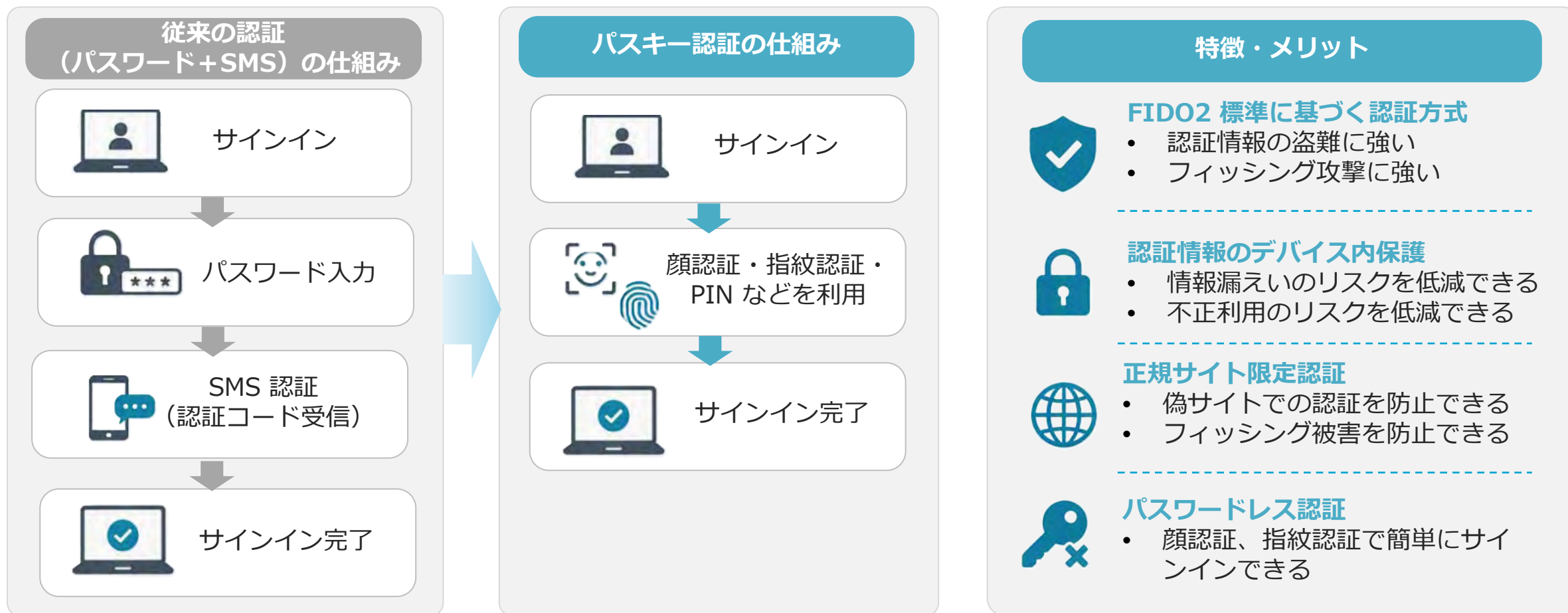
詳細については、[こちら](#)をご確認ください。



3. パスキーとは

3.1. パスキーとは

パスキーは、顔認証・指紋認証・PIN を利用するフィッシング耐性のある認証方式です。認証情報は安全な環境で保護されるため、情報漏えいや不正利用のリスクを低減できます。

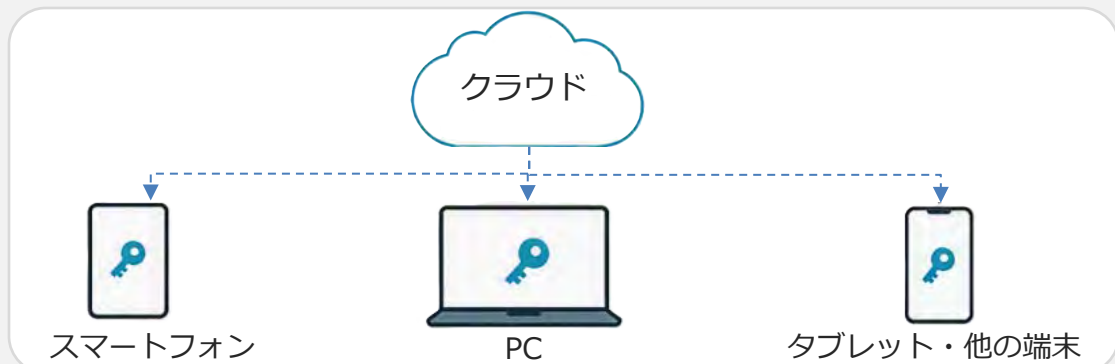


3.2. 利用できるパスキー

Microsoft Entra ID では「同期されたパスキー」と「デバイスバインドキー」の 2 種類のパスキーを利用できます。

同期されたパスキー

同期されたパスキーとは、クラウドを利用して複数のデバイスで共有・利用できるパスキーです。



特徴

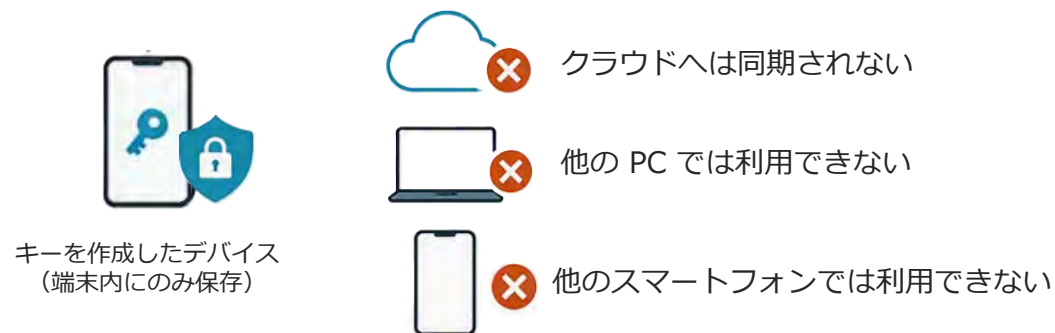
- 顔認証・指紋認証・PIN で利用できる
- 複数のデバイスで利用できる
- 機種変更後も継続利用しやすい

例

- ◆ Apple iCloud キーチェーン
- ◆ Google パスワードマネージャー

デバイスバインドパスキー

デバイスバインドパスキーとは、パスキーを作成したデバイスにのみ保存され、他のデバイスやクラウドには同期されないパスキーです。



特徴

- 作成したデバイスだけで利用できる
- パスキーはデバイス内に保存される
- 機種変更時は再登録が必要になる

例

- ◆ Microsoft Authenticator
- ◆ FIDO2 セキュリティキー

3.3. Microsoft が推奨する認証方式

SMS、電子メール OTP、または認証アプリを使用した従来の MFA では、パスワードのみのシステムよりもセキュリティが大幅に向上しますが、リモートフィッシング攻撃を受けやすくなります。そのため Microsoft では、Windows Hello for Business、パスキー（FIDO2）、FIDO2 セキュリティキー、証明書ベースの認証（CBA）などの以下のフィッシングに強い認証方式を使用することを推奨しています。

Microsoft 推奨の認証方式



同期されたパスキー（FIDO2）

Apple iCloud キーチェーンや Google パスワードマネージャーなどを利用して複数のデバイスで利用できるパスキー



macOS のパスキー

Mac の Touch ID や Face ID に相当する生体認証を利用して、安全にサインインできる認証方式



Windows Hello for Business

Windows デバイスで顔認証・指紋認証・PIN を利用して安全にサインインできるパスワードレス認証方式



FIDO2 セキュリティキー

USB キーなどをパソコンやスマートフォンに接続して安全にサインインする認証方式



Microsoft Authenticator のパスキー

Microsoft Authenticator アプリを利用して顔認証・指紋認証・PIN でサインインできる認証方式



証明書ベースの認証（CBA）

デバイスやスマートカードに格納されたデジタル証明書を利用して本人確認を行う認証方式



4. パスキー登録方法

4.1. パスキー登録手順

認証方法にパスキーを登録する流れは以下となります。各詳細な手順については次のページより説明します。

0

前提条件

パスキーの登録を行う前に必要な前提条件を確認します。

1

セキュリティ情報にアクセス

自身のセキュリティ情報ページにてサインイン方法を追加するため、サインインを実施します。

2

サインイン方法（パスキー）の追加

サインイン方法の追加画面よりパスキーを選択し、指示に従って追加を進めます。

3

サインイン方法の追加完了の確認

自身のセキュリティ情報ページにて、追加したサインイン方法（パスキー）を確認します。

4.1. パスキー登録手順

0 前提条件

自身でパスキーを登録するためには、以下を事前に設定もしくは確認する必要があります。

管理者

パスキー（FIDO2）が有効化されていること

管理者にて Microsoft Entra 管理センターの認証方法ポリシーでパスキー（FIDO2）を有効化し、対象となるユーザーを含める必要があります。

補足

1. 管理者にて [Microsoft Entra 管理センター](#) にサインイン
2. [認証方法] > [ポリシー] > [パスキー (FIDO2)]
3. 対象のユーザーを含め、[有効化]に設定

ユーザー

パスキーの登録先が利用できること

Windows Hello、Microsoft Authenticator、FIDO2 セキュリティキーなど、パスキーを保存する環境が利用可能である必要があります。

補足

- ※Windows の場合
1. [設定] > [アカウント]
 2. [サインインオプション] より利用するサインイン方法が登録されているかを確認します。されていない場合は登録を行います。

ユーザー

ユーザー本人が本人確認できる状態であること

パスキー登録時には本人確認が必要です。そのため、既存の MFA または一時アクセスパスが利用可能である必要があります。

補足

- MFA が登録済み
そのままパスキーの登録が可能です。
- MFA が未登録
一時アクセスパスの発行が必要です。
※詳細は次のページにて記載

4.1. パスキー登録手順

1 セキュリティ情報にアクセス

自身のセキュリティ情報ページにてサインイン方法を追加するため、サインインを実施します。

流れ

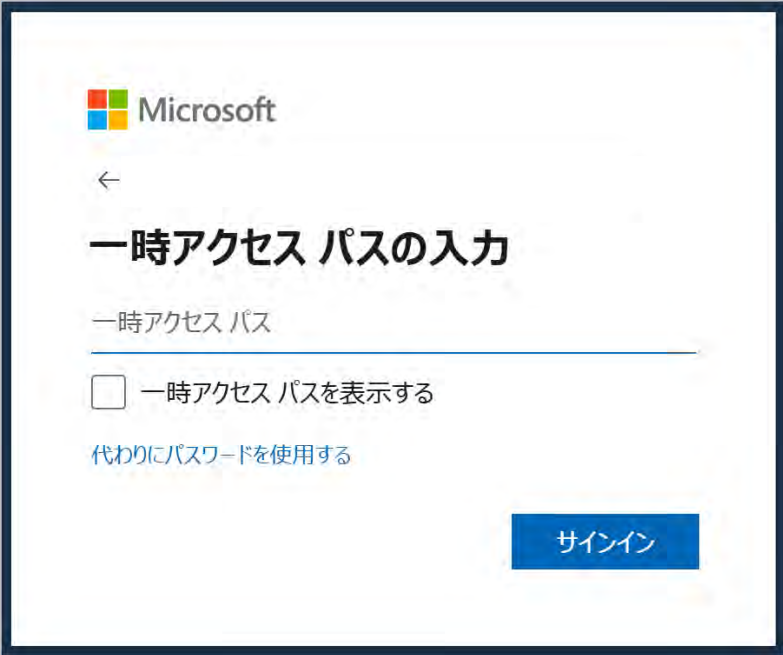
1. 対象ユーザーにて[セキュリティ情報ページ](#)にサインイン

補足

MFA が未設定の場合の事前準備（管理者作業）

1. Microsoft Entra 管理センターにサインイン
2. [Entra ID] > [認証方法] > [ポリシー] に移動
3. 一覧から [一時アクセス パス] を選択
4. [有効にする] を選択し、対象／除外ユーザーを指定
5. [構成] で最大有効期間や長さを変更し [更新] を選択
6. [保存] を選択してポリシーを適用

POINT 設定完了後にサインインすると、右の画面のように一時アクセスパスの入力が求められます。



▲一時アクセスパスの入力画面

※[こちら](#)の記事より引用しています。

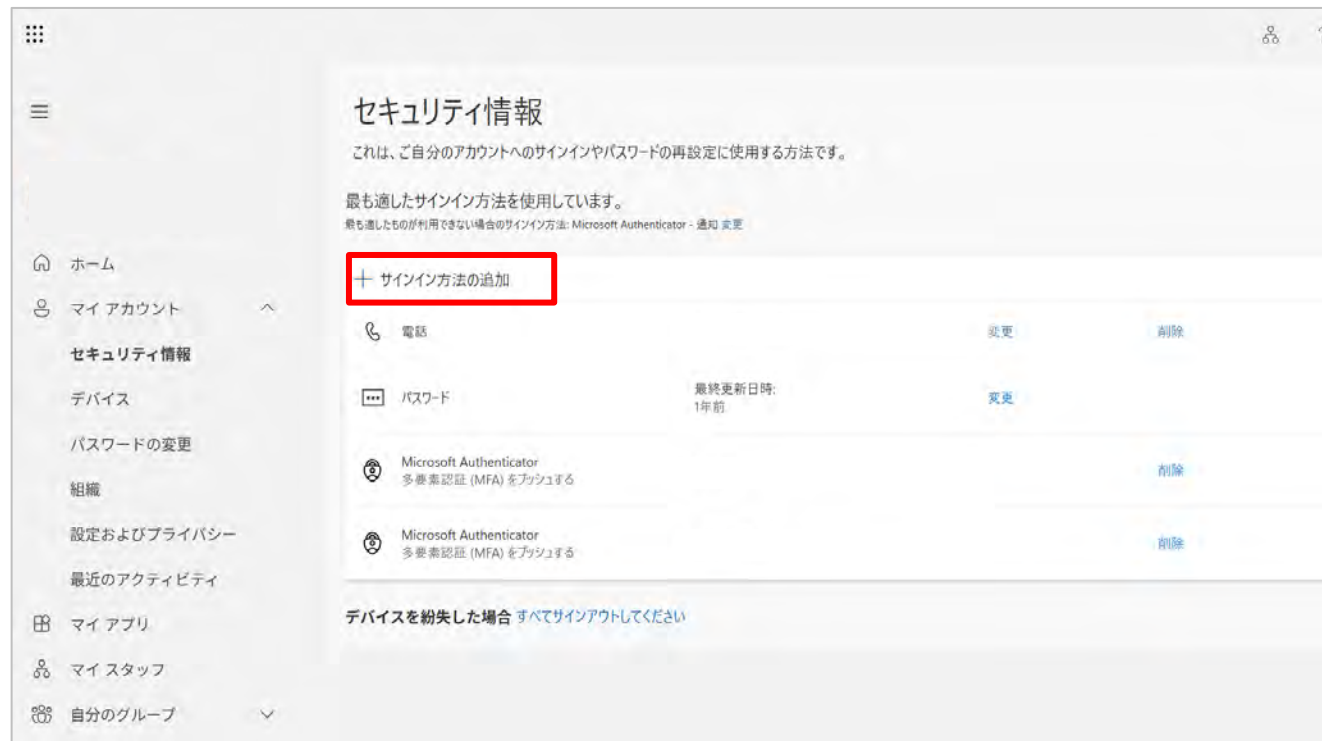
4.1. パスキー登録手順

2 サインイン方法（パスキー）の追加

パスキーを追加するため、パスキーを使える状態にしておきます。

流れ

2. [サインイン方法の追加] をクリック
3. [パスキー] を選択



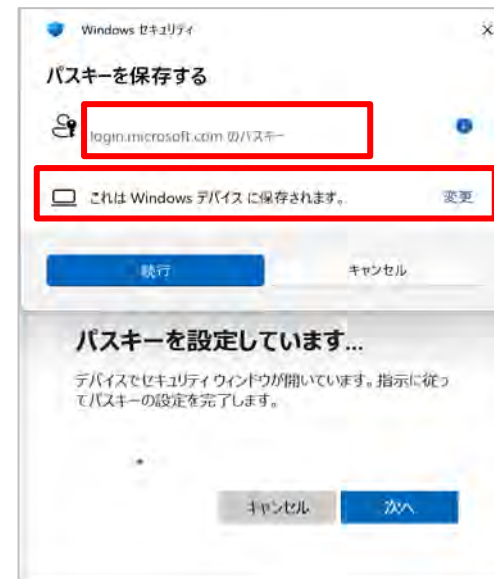
4.1. パスキー登録手順

2 サインイン方法（パスキー）の追加

流れ

4. [次へ] をクリック
5. それぞれの方法でパスキーを保存
※本資料では PIN を採用しています。

6. [続行]をクリック



4.1. パスキー登録手順

2 サインイン方法（パスキー）の追加

流れ

7. セキュリティキーの暗証番号（PIN）を入力して [OK] をクリック

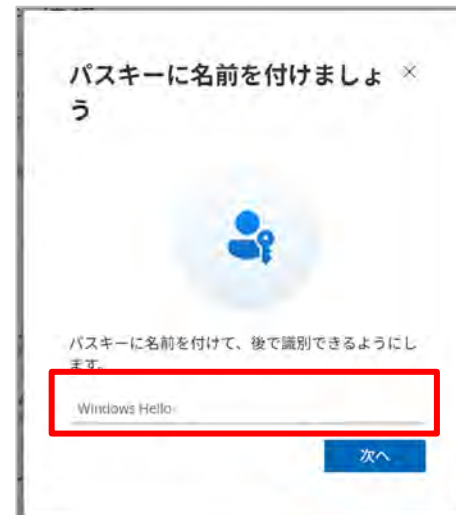


4.1. パスキー登録手順

2 サインイン方法（パスキー）の追加

流れ

- 登録したパスキー（セキュリティキー）をセキュリティ情報のページ上で識別できるように任意の名前を付けて [次へ] をクリック
- 「パスキーが作成されました」と表示されたら [完了] をクリック



4.1. パスキー登録手順

3 サインイン方法の追加完了の確認

流れ

10. セキュリティ情報のページ上でもパスキーが追加されたことを確認できればセットアップ完了

その他の詳細な手順につきましては、[こちら](#)をご参照ください。



4.2. 登録キャンペーンによる登録手順

MFA の認証方法を SMS 認証および音声通話認証からパスキーへ移行する際に、組織内で効率的にパスキー展開を行う「登録キャンペーン」の利用手順を説明します。

登録キャンペーンとは

サインイン時に、ユーザーにパスキーまたは Microsoft Authenticator を設定するよう促すことができます。ユーザーはサインインを実行し、通常どおり MFA を実行した後、対象となる認証方法を設定するように求められます。

ポイント



登録キャンペーンでは「パスキー（FIDO2）」と「Microsoft Authenticator」での認証方法がサポートされています。



※一度に 1 つの認証方法のみを対象にすることができます。

ユーザーが求められた認証方法の登録を延期（一時停止）できる日数を定義することができます。

流れ

1

【管理者作業】登録キャンペーンを設定

Microsoft Entra 管理センターにて登録キャンペーンの詳細設定を行い、展開します。

2

【ユーザー作業】パスキーを設定

サインイン後にパスキー登録の案内が表示されるため、指示に従ってパスキーの登録を行います。

4.2. 登録キャンペーンによる登録手順

1 【管理者作業】登録キャンペーンを設定

流れ

1. 管理者にて [Microsoft Entra 管理センター](#) にサインイン
2. [認証方法]>[ポリシー]>[パスキー (FIDO2)] を有効化
3. 対象のユーザーを含むグループをターゲットに追加

※[パスキー (FIDO2)] の [構成] タブにある [セルフサービス設定を許可] は、既定で有効に設定されています。意図的に無効化している場合は、本手順を実施する前に有効化してください（チェックが入っている場合は有効です）



4.2. 登録キャンペーンによる登録手順

1 【管理者作業】登録キャンペーンを設定

流れ

1. [認証方法]>[登録キャンペーン] にアクセス

2. 以下のように設定し、[保存] をクリック

※反映には時間がかかる場合があります。

項目	設定内容
状態	有効
認証方法	パスキー (FIDO2)
再通知の回数が制限されています	任意に設定。登録キャンペーンによる登録画面が表示される間隔を指定。
含む	登録キャンペーンの対象にするユーザーのグループを指定。
除外	登録キャンペーンから除外したいユーザーを明示的に指定します。



4.2. 登録キャンペーンによる登録手順

2 【ユーザー作業】パスキーを設定

流れ

登録キャンペーンは MFA が完了したタイミングで動作します。

1. ポータルなどにサインインをし、MFA を完了
2. 「アカウントをセキュリティ保護しましょう」という認証方法の登録を誘導する画面より [次へ] をクリック

※「今はしない」を選択すると、認証方法の登録をスキップすることができます。なお、スキップできる回数は、管理者作業の「再通知の回数が制限されています」の設定によって異なります。

3. パスキーの登録が始まる画面が表示
4. [次へ] をクリック



※上記キャプチャは[こちらの](#)記事より引用しております。



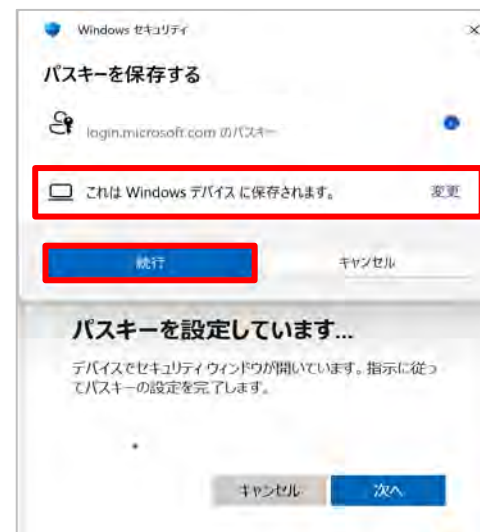
4.2. 登録キャンペーンによる登録手順

2 【ユーザー作業】 パスキーを設定

流れ

5. パスキーの保存先を指定

6. 事前に設定した暗証番号（PIN）の入力が要求されるため、入力してから [OK] をクリック



4.2. 登録キャンペーンによる登録手順

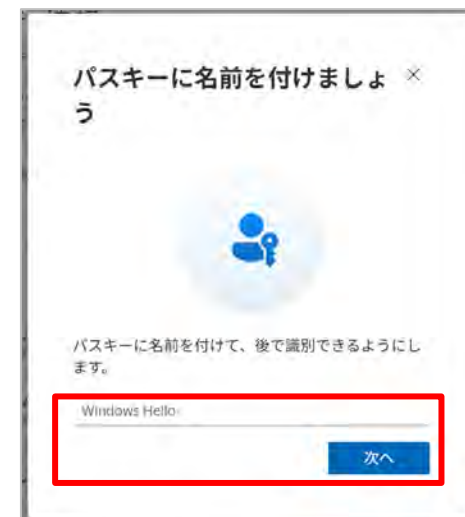
2 【ユーザー作業】 パスキーを設定

流れ

7. 後でセキュリティ情報ページで識別できるよう、パスキーに任意の名前を付けて [次へ] をクリック

8. [完了] を選択してパスキーの登録（セットアップ）を終了

※登録したパスキーは各自のセキュリティ情報のページから確認することができます。



4.3. 登録後の利用方法

1 セットアップ後のサインイン手順

登録後は顔認証・指紋認証・PIN などを利用してサインインできるようになります。

流れ

1. パスキーを使えるように準備
2. サインイン時に Microsoft Entra アカウントの UPN を入力して [次へ] をクリック
3. パスワードの入力画面が表示された場合はパスワードを入力せずに [代わりに顔、指紋、PIN、またはセキュリティキーを使用する] を選択
4. セキュリティキーの暗証番号 (PIN) の入力を求められた場合は入力して [OK] をクリック
5. サインインが完了





5. よくある質問

5.1. ユーザー目線でのよくある質問

本章では、[こちら](#)を参考に、SMS および音声通話認証の提供終了に関してよくある質問をユーザー目線・管理者目線で分けてまとめています。本ページでは、ユーザー目線でのよくある質問をまとめています。

Q1

ユーザーは自動移行されますか、それとも自身で移行を行う必要がありますか？

A

パスキーは自動で登録されません。ただし、登録キャンペーンの対象に自動で追加されます。

登録キャンペーンの設定が [Microsoft マネージド] に更新され、Microsoft Entra 管理センターの認証方法ポリシーで SMS 認証および音声通話認証が有効になっているユーザーは自動的に対象に含まれるようになります。

① サインイン・MFA を完了

② 登録キャンペーンの案内が表示

③ パスキーを登録

④ 次回以降パスキーでサインイン

POINT

対象のユーザーが次にサインインして MFA を完了すると、パスキーの登録案内画面が表示されます。Microsoft マネージドによる登録キャンペーンの案内は、無制限でスキップできます。

Q2

ユーザーは SMS 認証および音声通話認証の提供終了日にアカウントにアクセスできなくなりますか？

A

アクセス可能です。ただし、提供終了日までにパスキー登録、またはテレフォニープロバイダー構成による継続利用の準備が必要です。

該当する提供終了日までにテレフォニープロバイダーを構成しない場合、SMS 認証および音声通話認証を利用するユーザーには、パスキーを登録するためのブロック登録プロンプトが表示されます。

なお、このプロンプトはスキップできなくなります。

① サインイン・MFA を完了

② パスキー登録画面が表示される
(スキップ不可)

③ パスキーを登録

④ 次回以降パスキーでサインイン

POINT

グローバル管理者と外部ユーザーを除くすべてのユーザーは 2027 年 2 月 1 日に提供終了となり、グローバル管理者と外部ユーザーは、2027 年 7 月 1 日に提供終了します。

5.2. 管理者目線でのよくある質問

本ページでは、管理者目線でのよくある質問をまとめています。

Q1

テレフォニープロバイダーを構成した場合、ユーザーへブロックパスキー登録プロンプトは表示されますか？

A

原則として、ブロックパスキー登録プロンプトは表示されません。

なお、構成後に SMS 認証および音声通話認証を引き続き利用する場合、以下を必ず確認します。

- テレフォニープロバイダーが構成されていること
- 影響を受けるすべてのユーザーが該当する提供終了日より前に移行されていること

POINT

テレフォニープロバイダーは、SMS 認証または音声通話認証を引き続き使用するビジネス、規制、または技術的なニーズを持つ組織を対象としています。なお、SMS 認証または音声通話認証を有効にしたままのユーザーは、引き続きパスキー登録要件の対象となります。

Q2

セルフサービス パスワードリセット（以降、SSPR）についてはどうですか？

A

MFA だけでなく、SSPR にも影響します。

SSPR 利用時に、SMS 認証および音声通話認証は利用できなくなります。なお、Microsoft Security Store でテレフォニープロバイダーを構成した場合、引き続き SMS 認証および音声通話認証の利用が可能となります。

POINT

SSPR 利用時に利用する認証方法は、Microsoft Entra 管理センターにて設定することができます。詳細手順は[こちら](#)をご確認ください。