

多要素認証（MFA）の設定方法

Ver.20250918

本資料の内容および画面表示は、2025年9月時点の情報に基づいて作成されています。
Microsoft社の仕様変更や画面構成の変更により、実際の表示と異なる場合がございます。
あらかじめご了承ください。

多要素認証 (MFA) とは

Microsoft における多要素認証 (MFA) は、Microsoft Entra IDの機能の一つで、**無料で利用可能です**。
ユーザーがサインインする際に、パスワードに加えてスマートフォンやワンタイムパスワードなどを使って本人確認を行うことで、不正アクセスのリスクを大幅に低減できます。



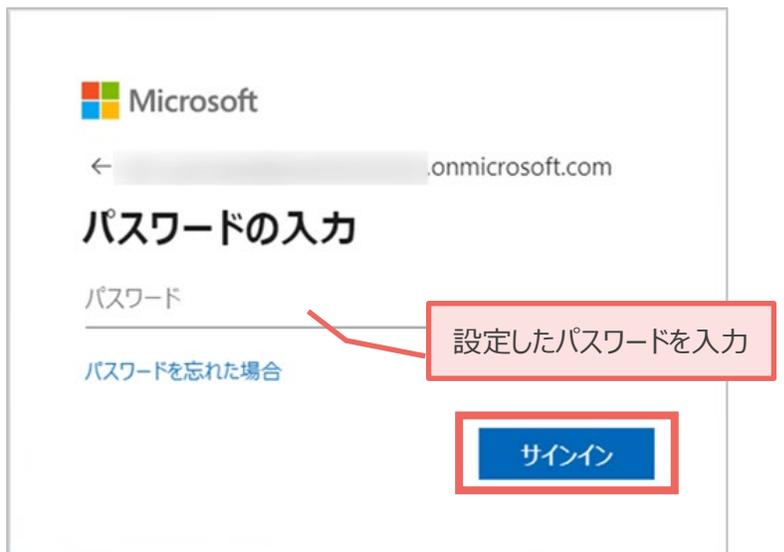
Microsoft Authenticator アプリの設定方法

最初にサインインする管理者 (admin@*.onmicrosoft.com)は
Microsoft Authenticator アプリによる認証設定を完了させる必要があります。
SMS認証を利用したい場合は、Microsoft Authenticator アプリでサインインした後に、
SMS認証の有効化設定を行ってください。
設定手順は本資料の[P12](#)以降をご参照ください。

Microsoft Authenticator アプリの設定方法



1. Microsoft 365 管理センター や Office アプリのサインイン画面でユーザーアカウント（例：*****@*****.onmicrosoft.com）を入力し、「次へ」をクリックします。

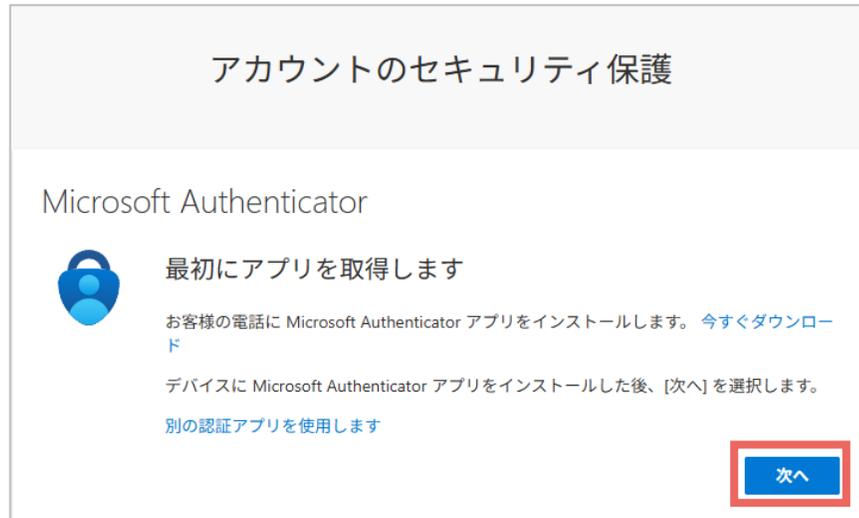


2. パスワードを入力し、「サインイン」をクリックします。

Microsoft Authenticator アプリの設定方法



3. 「アクションが必要」と表示されたら、「次へ」をクリックし、多要素認証（MFA）の設定に進みます。



4. 「最初にアプリを取得します」と表示されたら、「次へ」をクリックします。

Microsoft Authenticator アプリの設定方法



5. 「アカウントのセットアップ」と表示されたら、Microsoft Authenticator アプリの設定を開始します。



6. スマートフォンにMicrosoft Authenticator をインストールしてください。
▼ダウンロードリンク

<https://www.microsoft.com/ja-jp/security/mobile-authenticator-app>

Point : SMS認証を利用するには

管理者1名がMicrosoft Authenticator アプリの設定を完了させてから、本資料13ページ~の手順を参考にSMS設定を行ってください。

Microsoft Authenticator アプリの設定方法

7. Microsoft Authenticator アプリを開き、
「+」→「職場または学校アカウント」→「QRコードをスキャン」を選択し、QRコードのスキャン画面を開きます。



Microsoft Authenticator アプリの設定方法

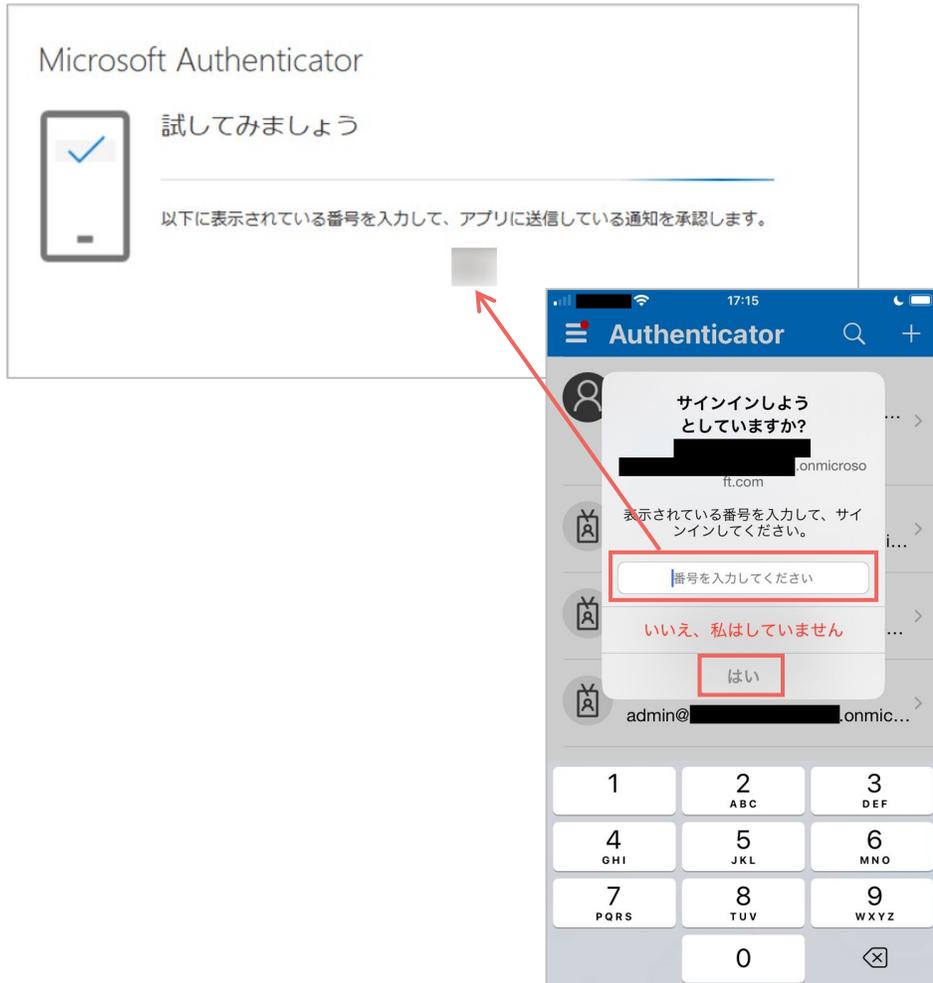


8. アプリの設定が完了したら、「次へ」をクリックします。



9. 画面に表示されたQRコードをアプリで読み取ります。

Microsoft Authenticator アプリの設定方法

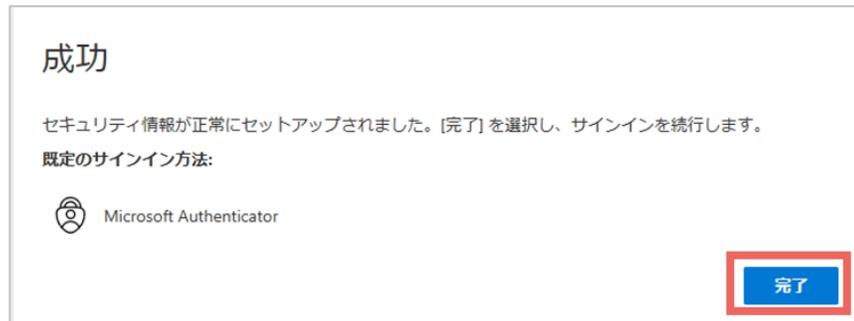


10. 画面に表示されている番号をアプリに入力し、「はい」をタップします。

Microsoft Authenticator アプリの設定方法



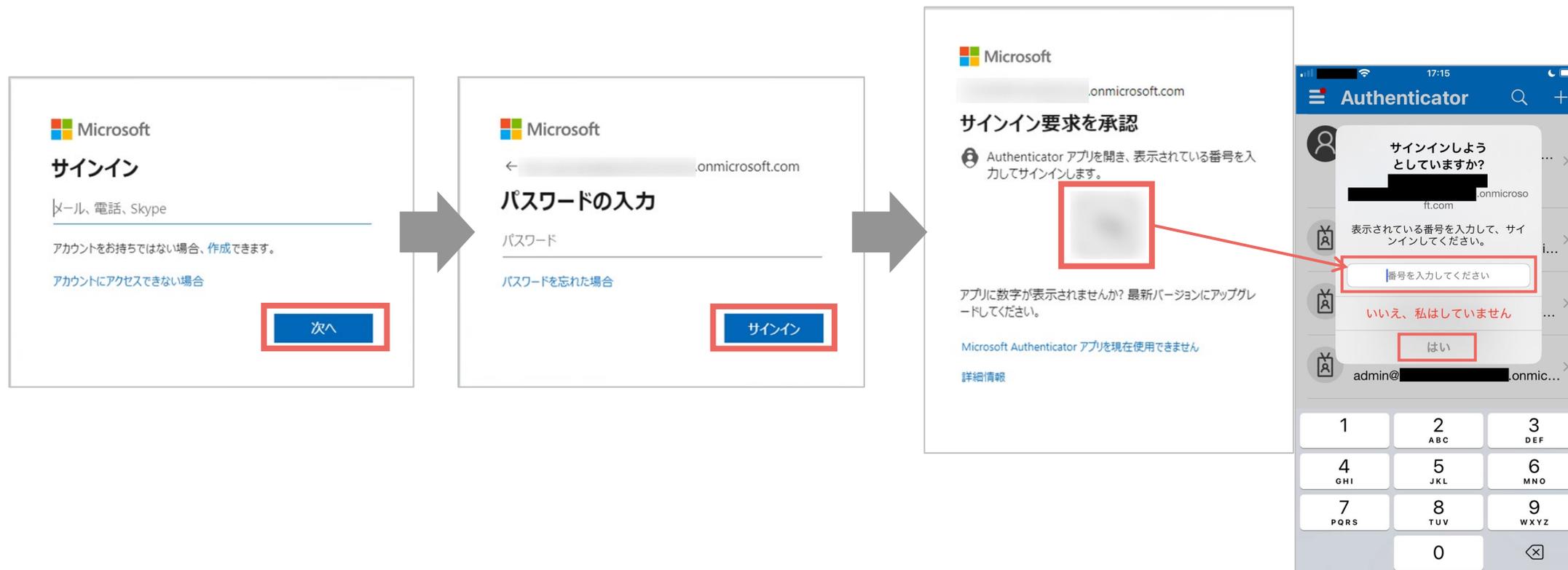
11. 「通知が承認されました」と表示されたら、「次へ」をクリックします。



12. 「完了」をクリックして、MFAの設定が完了します。

【補足】Microsoft Authenticator アプリ設定後のサインイン方法

1. ユーザーアカウントとパスワードを入力して「サインイン」をクリックすると、画面に2桁の番号が表示されます。
2. Microsoft Authenticator アプリを開き、その番号を入力して「はい」をタップすると、サインインが完了します。

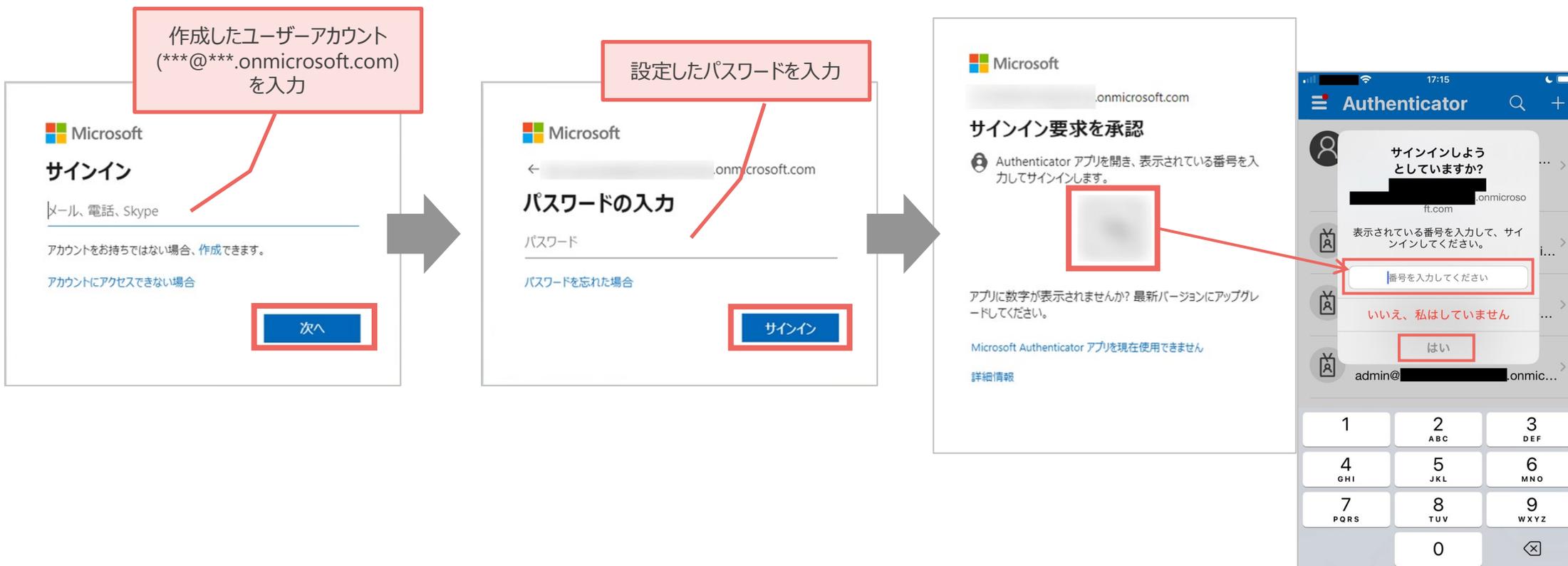


SMS認証の有効化方法

Microsoft では Microsoft Authenticator アプリの利用が推奨されています。
会社の規定等により、アプリの利用が難しい場合は、電話（SMS）による認証をご利用ください。
※ SMS認証を設定するには、**まず管理者1名が Microsoft Authenticator アプリによる
認証設定を完了している必要があります。**

<管理者操作> SMSの設定方法

1. グローバル管理者アカウントで、Microsoft Entra 管理センター（<https://entra.microsoft.com/>）にアクセスします。
PC画面に表示されている番号を、スマートフォンのMicrosoft Authenticatorアプリに入力し、「はい」をタップします。



<管理者操作> SMSの設定方法

2. 左側のメニューから「保護→認証方法」を選択します。

The screenshot displays the Microsoft Entra Management Center interface. The left sidebar contains a navigation menu with the following items: ホーム, 新着情報, 問題の診断と解決, お気に入り, ID, 概要, ユーザー, グループ, デバイス, アプリケーション, 保護, 認証方法 (highlighted with a red box), パスワードリセット, カスタムセキュリティ属性, Identity Governance, External Identities, and さらに表示. The main content area shows the Microsoft Entra tenant overview, including tenant ID, primary domain, user and group counts, and a list of roles. The 'Authentication Methods' menu item is highlighted in the left sidebar.

<管理者操作> SMSの設定方法

- 「SMS」を選択し、SMSの設定画面で「有効にする」をオンにしたうえで、「保存」をクリックしてください。
有効化後は、他のグローバル管理者アカウントにて、初回サインイン時にSMS認証を選択できるようになります。

ホーム > A | 割り当てられたロール >

認証方法 | ポリシー

Microsoft Entra ID セキュリティ

検索

外部メソッドを追加する (プレビュー) 更新 フィードバックがある場合

管理

- ポリシー
- パスワード保護
- 登録キャンペーン
- 認証強度
- 設定

監視

- アクティビティ
- ユーザー登録の詳細
- 登録とリセットのイベント
- 一括操作の結果

認証方法ポリシー

認証方法ポリシーを使用して、ユーザーに登録と使用を可能にする認証方法を構成します。認証とパスワードリセットに使用できます (シナリオによってはサポートされていない方法があります)

メソッド	ターゲット
▼ 組み込み	
パスキー (FIDO2)	
Microsoft Authenticator	すべてのユーザー
SMS	すべてのユーザー
一時アクセス パス	すべてのユーザー
ハードウェア OATH トークン (プレビュー)	
サードパーティ製のソフトウェア OATH トークン	すべてのユーザー
音声通話	
メール OTP	すべてのユーザー
証明書ベースの認証	
QR コード (プレビュー)	



ホーム > 認証方法 | ポリシー >

SMS の設定

この認証方法では、SMS を使用して 1 回限りのコードがユーザーの電話に配信され、ユーザーはそのコードを入力してサインイン。SMS は多要素認証とセルフサービス パスワードリセットに使用できます。さらに、第 1 要素として使用するよう構成することも

有効化およびターゲット

有効にする 「有効にする」をクリック

含める 除外

ターゲット すべてのユーザー グループの選択

名前	種類
すべてのユーザー	グループ

保存 破棄

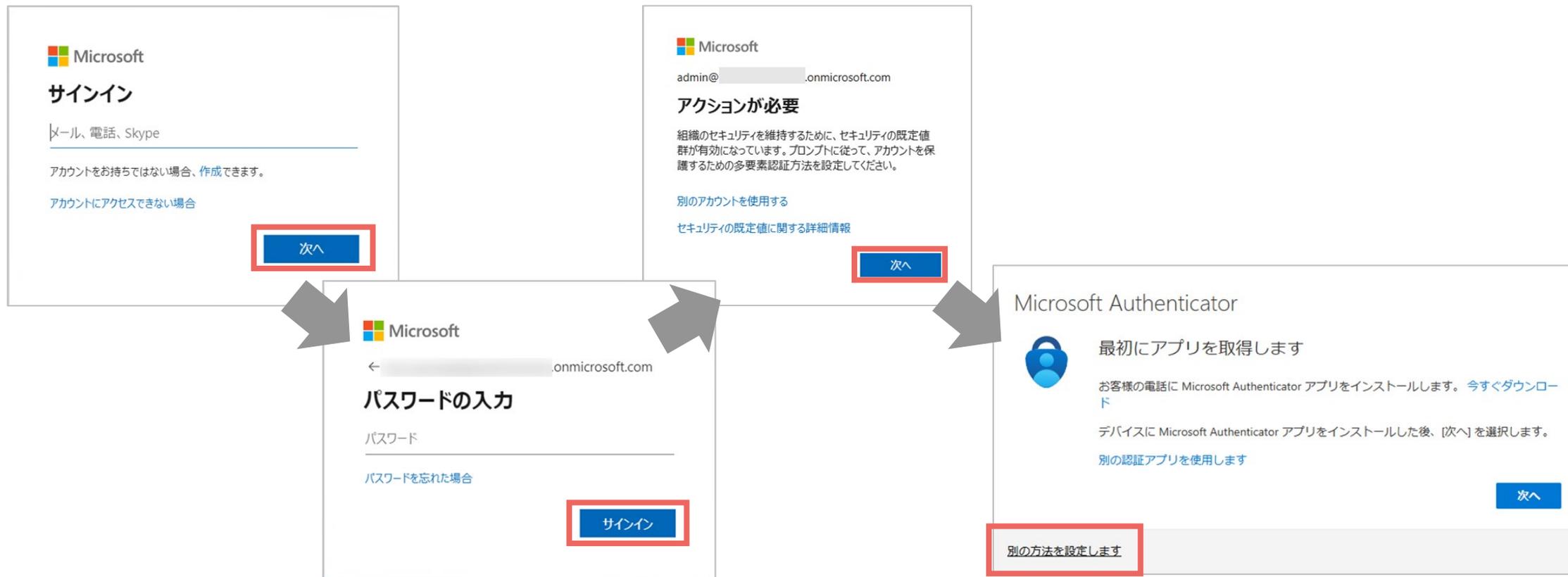
SMS認証設定方法（管理者のみ）

※すでにMicrosoft Authenticator による認証を設定済みの方が、SMS認証を追加したい場合は、詳細をP21にてご確認ください。
初回にサインインした管理者（admin@*.onmicrosoft.com）以外のユーザーは、SMS認証を最初の認証方法として設定することが可能です。
詳細はこの後のページをご参照ください。

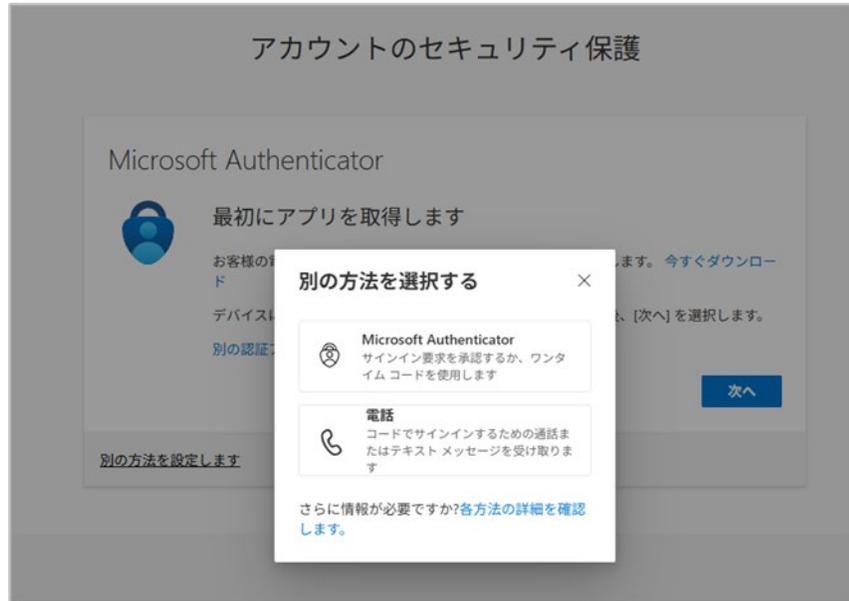
SMSの設定方法

1. グローバル管理者アカウントで、Microsoft Entra 管理センター（<https://entra.microsoft.com/>）にサインインします。
2. 「アクションが必要」と表示されたら、「次へ」をクリックし、多要素認証（MFA）の設定に進みます。
3. 「最初にアプリを取得します」と表示されたら、「別の方法を設定します」をクリックします。

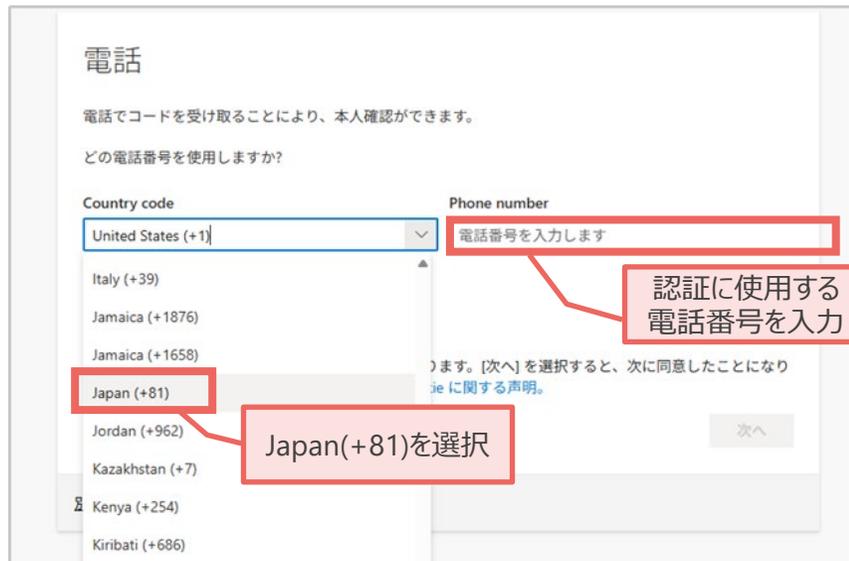
（Microsoft Authenticatorによる認証が始まってしまう場合は、P21をご参照ください。）



SMSの設定方法



4. 「別の方法を選択する」と表示されたら、「電話」をクリックします。



5. プルダウンから「Japan (+81)」を選択し、使用する電話番号を入力後、「次へ」をクリックします。

SMSの設定方法



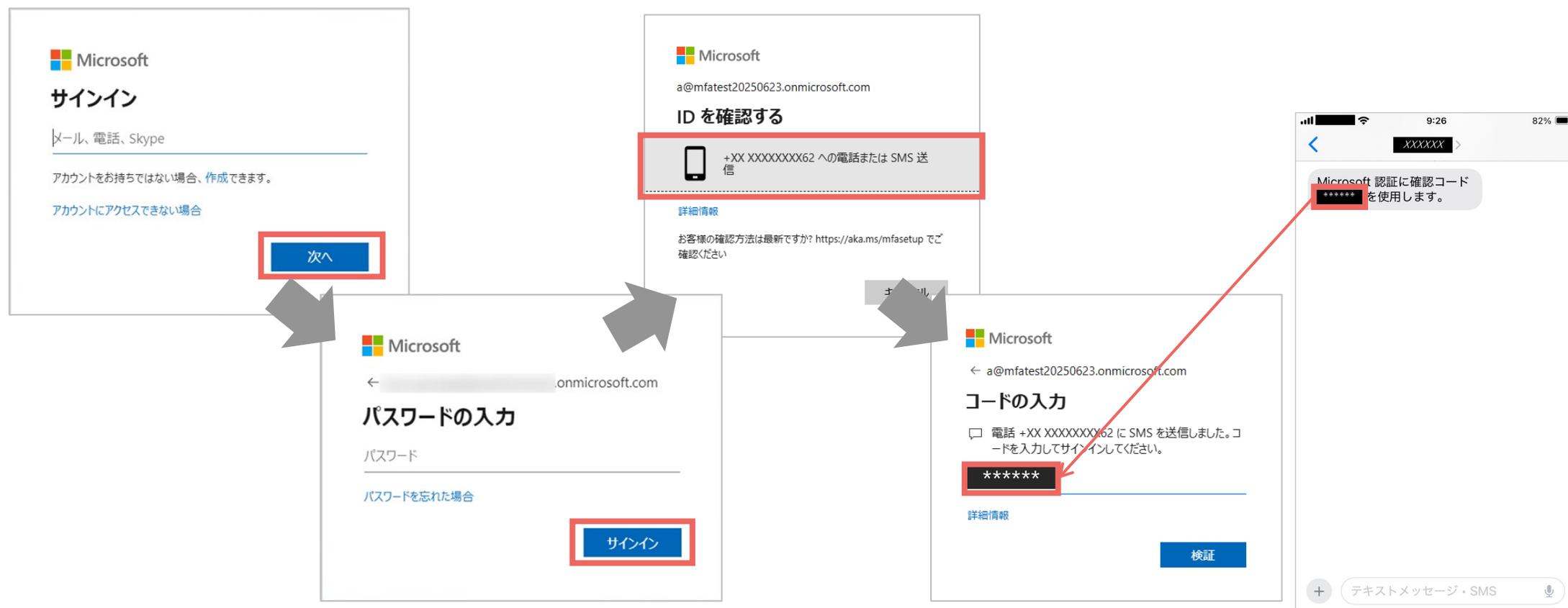
6. 記入した電話番号のSMS宛に送付されたコード（6桁）を入力し、「次へ」をクリック。



7. 「次へ」をクリックして、MFAの設定が完了します。

【参考】SMS認証設定後のサインイン画面

1. Microsoft 365 管理センターや Office アプリ起動時に、ユーザーアカウントとパスワードを入力します。
2. 「+ XXXX（登録した電話）への電話またはSMSを送信」をクリックするとSMSが送信されます。
3. SMSに記載されたコードを入力し、「検証」をクリックすると、サインインが完了します。



自身のアカウントへのSMS認証設定方法（管理者のみ）

<管理者操作> SMSの設定方法

1. マイアカウント (<https://myaccount.microsoft.com/>) にサインインします。
2. 左側のメニュー「セキュリティ情報→サインイン方法の追加」を選択します。

自分のサインイン

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

最も適したサインイン方法を使用しています。
最も適したものが利用できない場合のサインイン方法: [Microsoft Authenticator - 通知 変更](#)

+ サインイン方法の追加

パスワード	変更
Microsoft Authenticator 多要素認証 (MFA) をブッシュする	削除

デバイスを紛失した場合 [すべてサインアウトしてください](#)

<管理者操作> SMSの設定方法

サインイン方法の追加 ×

Microsoft Authenticator
サインイン要求を承認するか、ワンタイム コードを使用します

123 ハードウェア トークン
ハードウェア トークンからのコードを使用してサインインする

電話
コードでサインインするための通話またはテキスト メッセージを受け取ります

電子メール
パスワードをリセットするためのコードを受け取ります

3. 表示された選択肢の中から「電話」を選びます。

電話 ×

電話でコードを受け取ることにより、本人確認ができます。

どの電話番号を使用しますか? **Japan(+81)を選択**

Country code Phone number

日本 (+81) [input field]

Choose how to verify

コードを受け取る

メッセージとデータの通信料が適用される場合があります。[次へ]を選択すると、次に同意したことになります: [サービス使用条件](#) および [プライバシーと Cookie に関する声明](#)。

キャンセル **次へ**

4. 国コード（例：日本の場合は「日本 (+81)」）を選択し、携帯電話番号を入力し、「次へ」をクリックします。

<管理者操作> SMSの設定方法

電話 ×

+81 [redacted] に6桁のコードをお送りしました。コードを以下に入力してください。

[input field]

[コードの再送信](#)

戻る 次へ

5. 入力した電話番号宛にSMSで確認コードが送信されます。受信したコードを画面に入力し、「次へ」をクリックします。

電話 ×

✓ 検証が完了しました。電話が登録されました。

完了

6. 「検証が完了しました。電話が登録されました。」と表示されたら、「完了」をクリックします。これでSMS認証の設定は完了です。

管理者以外のユーザーのMFA設定について

<ユーザー> 一般ユーザーのMFA設定について

セキュリティ強化のため、管理者以外の一般ユーザーにも多要素認証（MFA）の設定が求められる場合があります。以下の仕様をご確認のうえ、設定をお願いいたします。

■仕様について

- ・**一般ユーザーは Microsoft Authenticator アプリの利用が必須です。SMS認証は基本的に利用できません。**

※設定手順については、P3をご参照ください。

- ・SMSによる認証を利用するためには、**対象ユーザー全員に Office 365 ライセンス（Apps for business など）を、割り当てたうえで、管理者にて以下の設定を行う必要があります。**

①認証方法ポリシーでSMSを有効化すること（設定手順：[P12](#)をご参照ください）

②ユーザーごとのMFAを設定すること

③SMS認証をユーザーに対して設定すること

※この設定には、Microsoft が推奨する基本的な**セキュリティ保護を無効化する操作が含まれており、セキュリティリスクが高まる可能性があります。**

上記の内容をご理解のうえで設定を行う場合は、リスクを軽減するために、

テナントに所属するすべてのユーザーに対して、**ユーザーごとの MFA を忘れずに設定してください。**

ユーザーごとのMFAの設定方法

<管理者操作> ②ユーザーごとのMFA設定

1. Microsoft Entra 管理センター (<https://myaccount.microsoft.com/>) にサインインします。
2. 左側のメニュー「概要→プロパティ→セキュリティの規定値群の管理」を選択します。



<管理者操作> ②ユーザーごとのMFA設定

3. 「セキュリティ規定値群」の設定を「無効」に変更します。
4. 表示される「無効にする理由」から任意の理由を選択し、「保存」をクリックします。

Microsoft Entra 管理センター

ホーム > ユーザー > ユーザーごとの多要素認証 >

セキュリティの既定値群

セキュリティの既定値群
無効

無効

多要素認証を使用すると、アカウント侵害の 99.9% を停止させることができます。これは、セキュリティの既定値群によって提供される機能です。

Microsoft のセキュリティ チームによると、セキュリティの既定値群を有効にすることで侵害率が 80% の低下が見られます。

無効にする理由 *

このフィードバックは Microsoft の製品とサービスの改修に使用されます。フィードバックに関する声明の表示

- サインイン情報の多要素認証チャレンジが多くなり過ぎる
- 多要素認証のサインアップ要求が多くなり過ぎる
- 組織では、条件付きアクセスの使用を計画しています
- 自分の組織でアプリまたはデバイスを使用できない

1 条件付きアクセスを使用してアプリケーションを許可するように条件とコントロールを変更します

条件付きアクセス ポリシーを有効にして、セキュリティの既定値群を置き換えます

その他

保存 キャンセル

Microsoft が推奨する基本的なセキュリティ保護を無効にする設定のため、セキュリティリスクが高まる可能性があります。

設定を行う際は、P31以降の手順を参照のうえ、テナントに所属するすべてのユーザーに、ユーザーごとの MFA を忘れずに設定してください。

<管理者操作> ②ユーザーごとのMFA設定

5. 「無効化」をクリックすると、セキュリティ規定値群が無効化されます。



セキュリティの既定値群

セキュリティの既定値群を無効にして、条件付きアクセスを有効にします
セキュリティの既定値群を条件付きアクセス ポリシーに置き換えます。 [詳細情報](#)

無効化 キャンセル

多要素認証を使用すると、アカウント侵害の 99.9% を停止させることができます。これは、セキュリティの既定値群によって提供される機能です。

Microsoft のセキュリティ チームによると、セキュリティの既定値群を有効にすることで侵害率に 80% の低下が見られます。

無効にする理由 *
このフィードバックは Microsoft の製品とサービスの改善に使用されます。 [プライバシーに関する声明の表示](#)

- サインイン情報の多要素認証チャレンジが多くなり過ぎる
- 多要素認証のサインアップ要求が多くなり過ぎる
- 組織では、条件付きアクセスの使用を計画しています
- 自分の組織でアプリまたはデバイスを使用できない

i 条件付きアクセスを使用してアプリケーションを許可するように条件とコントロールを変更します

- 条件付きアクセス ポリシーを有効にして、セキュリティの既定値群を置き換えます
- その他

保存 キャンセル



成功 ✕

セキュリティの既定値群のポリシーが正常に無効になりました。

<管理者操作> ②ユーザーごとのMFA設定

1. 左側のメニュー「ユーザー→ユーザーごとのMFA」を選択します。

The screenshot shows the Microsoft Entra Management Center interface. On the left, the 'ユーザー' (User) menu item is highlighted with a red box. A red arrow points from this menu item to the 'ユーザーごとの MFA' (User-specific MFA) option in the top right corner of the main content area, which is also highlighted with a red box. The main content area displays a list of users with columns for '表示名' (Display Name), 'ユーザー プリンシパル名' (User Principal Name), 'ユーザーの種類' (User Type), 'オンプレミスの...' (On-premises...), 'ID', '会社名' (Company Name), and '作成の種類' (Creation Type). The table contains three rows of user data.

表示名 ↑	ユーザー プリンシパル名 ↑	ユーザーの種類	オンプレミスの...	ID	会社名	作成の種類
[Redacted]	[Redacted]	メンバー	いいえ	[Redacted]		
[Redacted]	[Redacted]	メンバー	いいえ	[Redacted]		
[Redacted]	[Redacted]	メンバー	いいえ	[Redacted]		

<管理者操作> ②ユーザーごとのMFA設定

2. ユーザーのチェックボックスにチェックを入れ、「MFAを有効にする」をクリックします。

Microsoft Entra 管理センター

ホーム > ユーザー > ユーザーごとの多要素認証

Bulk update フィードバックがある場合

ユーザー サービス設定

多要素認証 (MFA) を使用してユーザーとデータを保護します。MFA を適用するための推奨される方法は、アダプティブ条件付きアクセス ポリシーを使用することです。詳細情報

始める前に、多要素認証のデプロイ ガイドを参照してください。

MFA を有効にする MFA を無効にする MFA を適用する ユーザーの MFA 設定

検索

状態: すべて 表示: サインインが許可されたユーザー フィルターのリセット

<input type="checkbox"/>	名前	UPN	状態
<input type="checkbox"/>	[REDACTED]	[REDACTED]	disabled
<input checked="" type="checkbox"/>	[REDACTED]	[REDACTED]	disabled
<input type="checkbox"/>	[REDACTED]	[REDACTED]	disabled

テナントに所属するすべてのユーザーに、ユーザーごとの MFA を設定してください。

<管理者操作> ②ユーザーごとのMFA設定

3. 「有効にする」をクリックすると、ユーザーごとのMFAの設定が完了します。

リソース、サービス、ドキュメントの検索 (G+/)

Copilot

ホーム > ユーザー >

ユーザーごとの多要素認証

Bulk update フィードバックがある場合

ユーザー サービス設定

多要素認証 (MFA) を使用してユーザーとデータを保護します。MFA を適用するための推奨される方法は、アダプティブ条件付きアクセス ポリシーを使用することです。詳細情報

始める前に、多要素認証のデプロイ ガイドを参照してください。

MFA を有効にする MFA を無効にする MFA を適用する ユーザーの MFA 設定

検索 状態: すべて 表示: サインインが許可されたユーザー フィルターのリセット

<input type="checkbox"/>	名前	UPN
<input type="checkbox"/>	[REDACTED]	[REDACTED]
<input checked="" type="checkbox"/>	[REDACTED]	[REDACTED]
<input type="checkbox"/>	[REDACTED]	[REDACTED]

多要素認証を有効にする

ユーザーが通常はブラウザーからサインインしていない場合、多要素認証の登録を行うためのこのリンクをそれらのユーザーに送信することができます: <https://aka.ms/mfasetup>



多要素認証が有効になりました

多要素認証が正常に有効になりました

✕

SMS認証設定方法

<ユーザー操作> ③SMSの設定方法

Microsoft
サインイン

メール、電話、Skype

アカウントをお持ちではない場合、作成できます。

アカウントにアクセスできない場合

次へ

作成したユーザーアカウント
(***@***.onmicrosoft.com)
を入力

1. Microsoft 365 管理センター や Office アプリのサインイン画面でユーザーアカウント（例：*****@*****.onmicrosoft.com）を入力し、「次へ」をクリックします。

Microsoft

← .onmicrosoft.com

パスワードの入力

パスワード

パスワードを忘れた場合

サインイン

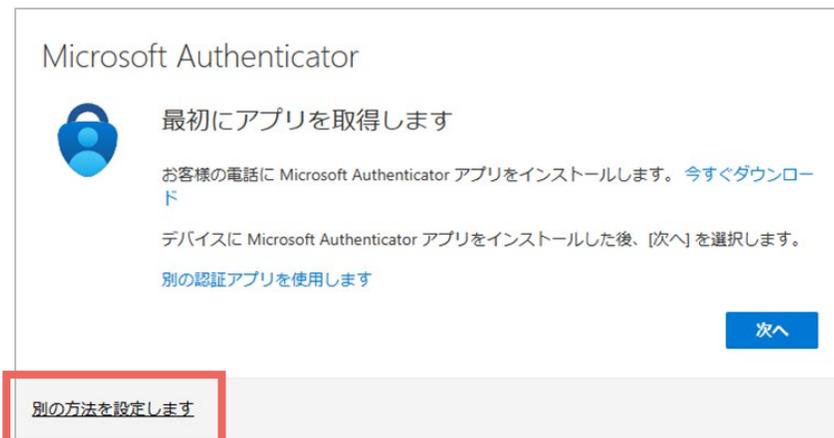
設定したパスワードを入力

2. パスワードを入力し、「サインイン」をクリックします。

<ユーザー操作> ③SMSの設定方法

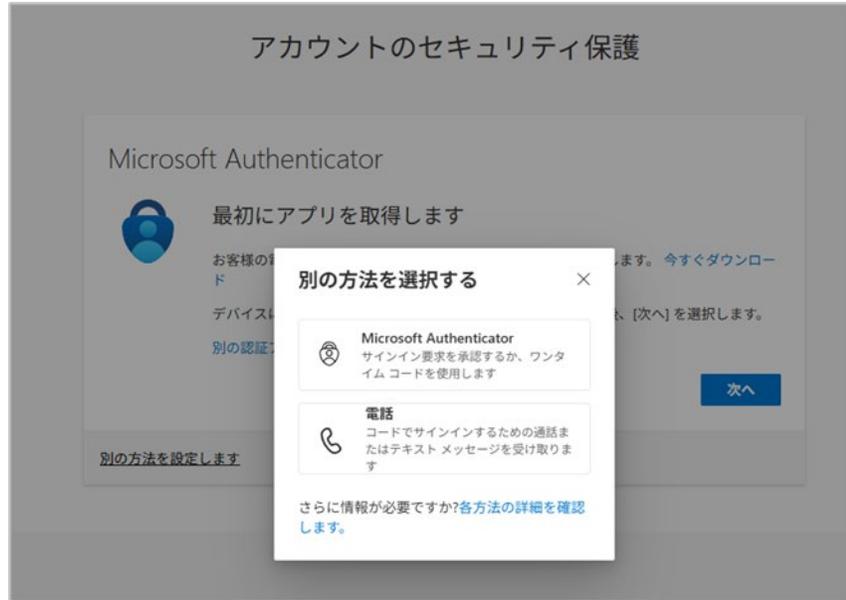


3. 「アクションが必要」と表示されたら、「次へ」をクリックし、多要素認証（MFA）の設定に進みます。

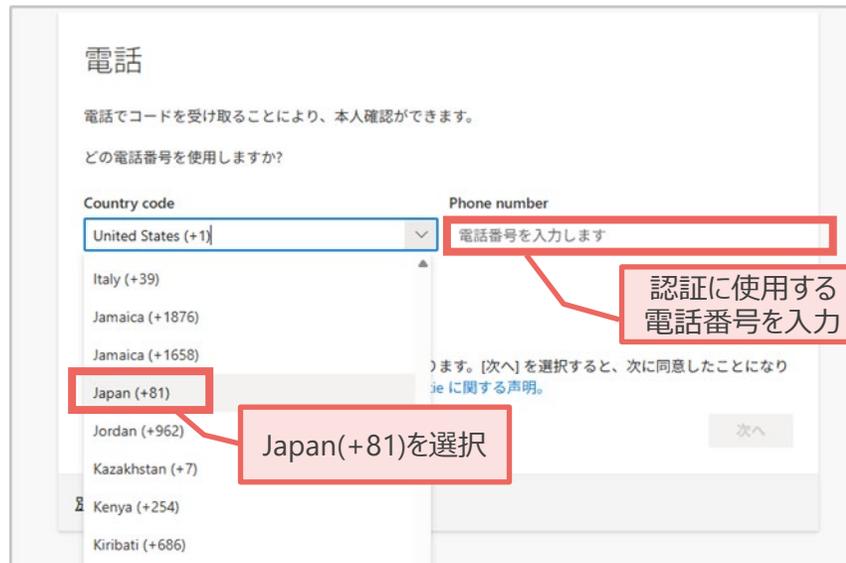


4. 「最初にアプリを取得します」と表示されたら、「別の方法を設定します」をクリックします。

<ユーザー操作> ③SMSの設定方法



5. 「別の方法を選択する」と表示されたら、「電話」をクリックします。



6. プルダウンから「Japan (+81)」を選択し、使用する電話番号を入力後、「次へ」をクリックします。

<ユーザー操作> ③SMSの設定方法



7. 記入した電話番号のSMS宛に送付されたコード（6桁）を入力し、「次へ」をクリック。



8. 「次へ」をクリックして、MFAの設定が完了します。

操作の詳細や不明点などは
クラウドサポートセンターまでお問い合わせください。

<https://www.cloud-all.jp/contact/>

<営業時間>

【平日】 9 : 00 ~ 19 : 00

【土・日・祝日】 9 : 00 ~ 17 : 15 (12 : 00 ~ 13 : 00は除く)

※営業時間外にいただいたお問い合わせは、翌営業日以降の対応となります。