

パスワードルール・二要素認証設定

- 貴校のセキュリティやログインポリシーに合わせて設定を変更してください。
- [パスワードルール・二要素認証設定] 画面で、**セキュリティ**（パスワードルールや認証）に関する設定と、**SSO連携**（GoogleまたはMicrosoftアカウントでのログイン）に関する設定ができます。



初期設定のパスワードルールを確認し、必要に応じて修正をしてください。

パスワードは、初回ログイン時に**先生・子ども本人が設定**します。その際[パスワードルール・二要素認証設定] 画面で設定した、パスワードルールに沿ってパスワードを決定する必要があります。**先生・子どもへログイン情報を配布する前など、事前にパスワードルールをご確認ください。**

- 1 [パスワードルール・二要素認証設定] をクリック



教育委員会管理者の場合

- ①の後に以下の手順で学校を選択します。

複数の学校を一括で設定できます。

- 1 設定する学校に**チェックを入れる**

先頭行（見出し行）のチェックを入れると、すべての学校を選択できます。



- 2 [パスワードルール設定] をクリック

すでに学校ごとに異なるパスワードルールが設定されている場合でも、教育委員会管理者アカウントでログインした場合には**初期値**が表示され、設定すると内容が**上書き**されますのでご注意ください。

2 必要に応じて設定

教育委員会管理者の場合

操作の対象となる学校名を必ず確認してください。

対象外▶ 下記の場合は設定不要です。

- 外部連携（まなびポケット、L-Gate）でミライシードを利用する場合
- SSO連携（Google、Microsoftアカウント）でログインする場合

ミライシードのID※
でログインする場合のみ ※任意IDを含む

セキュリティに関する設定

パスワードルール

先生、子どものパスワードルールを設定できます。

→ p.3

二要素認証

先生がログイン時に、メールまたはSMSで二要素認証できます。

→ p.4

子どもパスワード入力設定

子どもの初回ログインおよびパスワードリセット時に、仮パスワードの入力可否を設定できます。

→ p.5

A小学校

パスワードルール・二要素認証 - 設定

更新

先生パスワードルール設定

パスワードの文字数を制限する * 8 文字以上 32 文字以下

パスワードの有効期限を設定する * 変更後、90 日以上経過したら警告を表示する
☐ 期限を設定しない

前回パスワードとの重複を制限する * ☒ 前回、前々回のパスワードとの重複を禁止する
☐ 前回のパスワードとの重複を禁止する
☐ 重複を許可する

子どもパスワードルール設定

パスワードの文字数を制限する * 8 文字以上 32 文字以下

英数字を強制する * ☐ 強制する ☒ 強制しない

パスワードの有効期限を設定する * 変更後、90 日以上経過したら警告を表示する
☐ 期限を設定しない

前回パスワードとの重複を制限する * ☒ 前回、前々回のパスワードとの重複を禁止する
☐ 前回のパスワードとの重複を禁止する
☐ 重複を許可する

先生二要素認証通称設定

二要素認証通称 * ☒ 任意 ☐ 全員

二要素認証コード情報送付方法 * ☒ メール ☐ SMS

子ども仮パスワード入力設定

初回ログイン * ☒ IDと仮パスワードでログインする
☐ IDのみでのログインを可能にする

パスワードリセット * ☒ IDと仮パスワードでログインする
☐ IDのみでのログインを可能にする

SSO連携利用設定

SSO連携(Google)利用可否設定 ☒ 先生の利用を可能にする ☐ 子どもの利用を可能にする

SSO連携(Microsoft)利用可否設定 ☐ 先生の利用を可能にする ☒ 子どもの利用を可能にする

SSOでログインする場合のみ

SSO連携に関する設定

SSO連携利用設定

SSO連携すると、ミライシードにGoogle、Microsoftアカウントでログインできます。

→ p.6

セキュリティに関する設定

- 先生・子どものパスワードルールや、二要素認証などセキュリティに関する設定ができます。**学校のセキュリティポリシー**に従ってご設定ください。
- これらの設定は、**ミライシードのID（任意IDを含む）でログインする場合のみ**影響します。外部連携（まなびポケット、L-Gate）やSSO連携（Google、Microsoftアカウント）でログインする場合は、この設定の影響を受けません。

1 先生・子どもそれぞれのパスワードルールを設定

利用中にパスワードルールを変更しても、**すでにログインしている先生・子どもは利用を現行ルールで継続できます。**

（「よくあるご質問」マニュアルの「パスワードルールを途中で変更したら子どもや先生は使えなくなりますか？」もご参照ください。）



先生のパスワードルール設定		初期値
パスワードの文字数を制限する	8～32文字の範囲で設定できます。 ※非表示の場合は学校ID、ログインコード受領後に表示されるようになります。	8文字以上 ～32文字以下
パスワードの有効期限を設定する	パスワード変更のお知らせを出す日数を設定します。期限を過ぎると警告が表示されますが、利用中のパスワードが利用できなくなるわけではありません。	90日以上経過したら警告を表示
前回パスワードとの重複を制限する	パスワードを変更する際に、前回もしくは前々回に設定していたパスワードと同一の文字列を設定できないよう制限できます。 従来URLから共通URLに変更した場合※ 、従来URLで使用していた最後のパスワードからチェック対象になります。従来URLでの最後のパスワードより前のものは重複チェックの対象になりません。 ※現在利用中のURLが「共通URL」と「従来URL」のいずれにあたるかを確認する方法は「よくあるご質問」マニュアルを参照	前回、前々回のパスワードとの重複を禁止

子どものパスワードルール設定		初期値
パスワードの文字数を制限する	8～32文字の範囲で設定できます。 ※非表示の場合は学校ID、ログインコード受領後に表示されるようになります。	8文字以上 ～32文字以下
英数混在を強制する	パスワードに英字・数字を含めることを必須とすることができます。	強制しない
パスワードの有効期限を設定する	パスワード変更のお知らせを出す日数を設定します。期限を過ぎると警告が表示されますが、利用中のパスワードが利用できなくなるわけではありません。	90日以上経過したら警告を表示
前回パスワードとの重複を制限する	パスワードを変更する際に、前回もしくは前々回に設定していたパスワードと同一の文字列を設定できないよう制限できます。 従来URLから共通URLに変更した場合※ 、従来URLで使用していた最後のパスワードからチェック対象になります。従来URLでの最後のパスワードより前のものは重複チェックの対象になりません。 ※現在利用中のURLが「共通URL」と「従来URL」のいずれにあたるかを確認する方法は「よくあるご質問」マニュアルを参照	前回、前々回のパスワードとの重複を禁止

2 先生の二要素認証を設定

先生のログイン時に、二要素認証の適用範囲と、認証コードの送信方法（メールまたはSMS）を設定できます。
必要な場合のみご設定ください。

二要素認証とは？

ログイン画面でID、パスワードを入力後、事前に登録しておいたメールアドレスまたはSMSに届いた認証コードを入力しないと、ミライシードにログインできないようにする仕組みです。

▼ ログイン画面でID、パスワードを入力

▼ 認証コードを入力

▼ ポータル画面を表示

！ 二要素認証の適用には、 先生本人による操作が必要です。

- 管理者による「パスワードルール・二要素認証設定」画面での設定だけでなく、**先生本人による操作**（認証コードの送信先の登録など）が必要です。
- 二要素認証を適用するための手順は、「先生情報管理（本人の作業）」のマニュアルを参照してください。

▼ 本人情報設定＞二要素認証

■**最重要事項（認証コード送付先の登録について）**
[パスワードルール・二要素認証設定] 画面で管理者が「**全員**」を選択した場合、先生ご本人による認証コード送付先の登録は**必須**です。登録がない場合、ログイン時に認証コードの登録・入力画面が表示され、**完了するまでログインできません**。

■**管理者とご本人による設定の適用関係**
管理者の設定と、ご本人による設定の組み合わせで、二要素認証が実際に適用されるかどうかが決まります。

▼【参考】

管理者による「パスワードルール・二要素認証設定」での設定と、**本人**による「本人情報設定」での設定の関係

管理者による「パスワードルール・二要素認証設定」での設定

		任意	全員
本人による [本人情報設定] での設定	○ 二要素認証を 適用する	○ 適用 二要素認証が適用されます。	○ 適用 二要素認証が適用されます。
	✕ 二要素認証を 適用しない	✕ 適用しない 二要素認証が適用されません。	○ 適用 二要素認証が適用されます。

3 子どもの仮パスワード入力のルールを設定

※「子ども仮パスワード入力設定」が表示されていない場合は、学校ID、ログインコード受領後に表示されるようになります。

子ども仮パスワード入力設定

初回ログイン時 *

☒ IDと仮パスワードでログインする

☐ IDのみでログインを可能にする

パスワードリセット後ログイン時 *

☒ IDと仮パスワードでログインする

☐ IDのみでログインを可能にする

設定項目		初期値
初回ログイン時	初回ログインの際に、仮パスワードを入力せずIDと学校コードでログインできるよう設定できます。	IDと仮パスワードでログイン
パスワードリセット後ログイン時	パスワードを忘れた子どものパスワードリセット後のログイン時に、仮パスワードを入力せずIDと学校コードでログインできるよう設定できます。	IDと仮パスワードでログイン

4 「更新」をクリック

アカウント管理・認証機能

A小学校

パスワードルール - 要素認証 - 設定

更新

先生パスワードルール設定

パスワードの文字数を制限する *

8 文字以上 32 文字以下

パスワードの有効期限を設定する *

☒ 変更後、90 日以上経過したら警告を表示する

☐ 期限を設定しない

前回パスワードとの重複を制限する *

☒ 前回、前々回のパスワードとの重複を禁止する

☐ 前回のパスワードとの重複を禁止する

☐ 重複を許可する

子どもパスワードルール設定

パスワードの文字数を制限する *

8 文字以上 32 文字以下

英数混在を強制する *

☐ 強制する ☒ 強制しない

SSO連携に関する設定

SSO連携すると、ミライシードにGoogle、Microsoftアカウントでログインできるようになります。

- 1 GoogleまたはMicrosoftの利用可否設定で、SSO連携する対象（先生・子ども）に応じてチェックを入れる

The screenshot shows the 'アカウント管理・認証機能' (Account Management & Authentication) settings page. A callout box highlights the 'SSO連携' (SSO Linkage) section. Below the callout, a table summarizes the settings for Google and Microsoft SSO linkage.

SSO連携	先生	子ども
SSO連携(Google)利用可否設定	<input checked="" type="checkbox"/> 先生の利用を可能にする	<input type="checkbox"/> 子どもの利用を可能にする
SSO連携(Microsoft)利用可否設定	<input type="checkbox"/> 先生の利用を可能にする	<input checked="" type="checkbox"/> 子どもの利用を可能にする

- 2 [更新] をクリック

SSO利用可とした場合でも、SSOログインを利用せず学校コード・ID・パスワードでログインが可能です。

！ 先生・子どもそれぞれ個別に設定・メールアドレス登録が必要です。

先生・子どものアカウントを作成する際に、「SSO連携」の設定でGoogleまたはMicrosoftにチェックを入れ、連携用のメールアドレスを登録すると、SSO連携が完了します。**[パスワードルール・二要素認証設定] 画面での設定だけではSSO連携できませんので、ご注意ください。**

▼ 先生・子どもの個別画面

The screenshot shows the '連携・セキュリティ情報' (Linkage & Security Information) section. It has two rows for Google and Microsoft SSO linkage. Each row has a checkbox and a text input field for the email address.

SSO連携	メールアドレス *
<input checked="" type="checkbox"/> Google	<input type="text"/>
<input type="checkbox"/> Microsoft	<input type="text"/>

⚠ SSO連携設定にあたっての注意点

以下3点が完了していない先生・子どもは、[パスワードルール・二要素認証設定] 画面でチェックが入っていても、SSO連携が適用されません。

- ① パスワードルール・二要素認証 での設定
- ② 個別画面での利用ON
- ③ 個別画面でのメールアドレス

また、GoogleのSSO連携を利用される場合は、①の対応と合わせてp.7以降のGoogle Workspace設定も必要です。MicrosoftのSSO連携を利用される場合は、①の対応と合わせてp.10以降のMicrosoft Entra設定も必要です。

GoogleのSSO連携の設定追加

- SSO連携（Google）を利用される場合は、Google Workspaceの設定追加が必要になります。

Google Workspaceの管理者ID・パスワードをお持ちの先生が作業してください。

※設定しない場合、アクセスブロックのエラーになる可能性があります。

1 Google Workspaceの管理者ID・パスワードでGoogle 管理コンソールにアクセス

URL <https://admin.google.com/ac/appslst/additional>

2 トップページ「アプリのアクセス制御」の「アプリを確認」をクリック

3 「審査待ちのアプリ」に「ベネッセのサービス」があるか確認



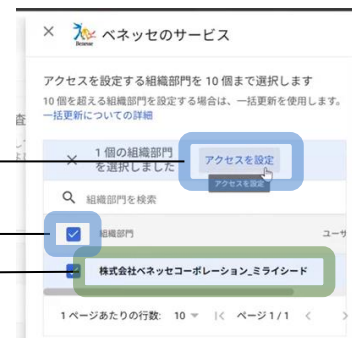
「審査待ちのアプリ」に「ベネッセのサービス」がない場合は、p.8の手順に進んでください。

③で「審査待ちのアプリ」に「ベネッセのサービス」がある場合

4 「アクセスを設定」を押す



組織部門をすべて選択し、「アクセスを設定」を押す



この部分は操作対象の組織名が入ります。

p.9の手順に進んでください。

③で「審査待ちのアプリ」に「ベネッセのサービス」がない場合

4 「設定済みアプリ」の「リストを表示」をクリック



「新しいアプリを設定」をクリック



下記のIDで検索し、「ベネッセのサービス」をクリック

ID 112514126103-r5thgbg4tkm7o63bcscunm42a7vk5h2f.apps.googleusercontent.com

IDを入力して、検索

アプリ名 ベネッセのサービス

クリック



p.9の手順に進んでください。

5 「すべてのユーザー」を選択し、
「続行」をクリック

この部分は操作対象の組織名が入ります。

選択したアプリ: ベネッセのサービス ウェブ 確認済み

範囲: アクセスの設定対象を選択します。10 個を超える組織部門を設定する場合は、一括更新を使用します。
一括更新の詳細
● 株式会社ベネッセコーポレーション、ミライシード 内の全員 (すべてのユーザー)
○ 組織部門を選択
組織を含める +

戻る 続行

6 「信頼できる」を選択し、「続行」をクリック

選択したアプリ: ベネッセのサービス ウェブ 確認済み

Google データへのアクセス: アクセスタイプを選択して、このアプリが Google アカウントでログインしているユーザーにリクエストできるデータを指定します。アプリによる Google データへのアクセスの詳細
● 信頼できる
このアプリは、OAuth 2.0 のスコープを使用して任意の Google サービスのユーザーデータに対するアクセスをリクエストできます。
信頼できるアクセスを使用した場合の挙動
○ 限定
このアプリは、Google サービスで制限なしとマークされている任意の Google サービスのユーザーデータに対するアクセスをリクエストできます。
制限付きアクセスを使用した場合の挙動
○ 特定の Google データ
このアプリは、以下で指定した Google サービスのユーザーデータのみに対するアクセスをリクエストできます。ユーザーが自身の Google アカウントでログインできるようにするには、以下で Google ログインのスコープを含める必要があります。
Google ログイン 3 個のスコープ
Google のサービスまたはスコープを更新
○ ブロック中
ユーザーは Google アカウントでこのアプリにログインすることはできません。また、アプリはどの Google サービスのユーザーデータに対するアクセスもリクエストできません。

戻る 続行

7 「完了」をクリック

1 選択した組織部門については、既存のアクセス設定がその下位組織部門にも適用されます (それらの下位組織部門がすでに設定済みの場合を除く)。設定済みのアプリを表示すると、アクセス設定が済んでいる組織部門を確認できます。 設定済みのアプリを表示
アクセス設定を確認する方法

アプリ: ベネッセのサービス ウェブ 確認済み
アプリを使用している組織の数: 非常に多い (500 超)
クライアント ID: 112514126103-d5hghg48km7o63bcsccum42a7a45... apps.googleusercontent.com

範囲: 組織部門 (1 個)
株式会社ベネッセコーポレーション、ミライシード

Google データへのアクセス: 信頼できる
信頼できるアクセスを使用した場合の挙動

戻る 完了

8 「保護者の同意の確認」について「確認」をクリック

9 「設定済みアプリ」に「ベネッセのサービス」があることを確認

Google サービス: Google サービス API のアクセス設定を選択して、これらサービスへのアクセスをリクエストできるサードパーティアプリの種類を管理します。詳細
リストを表示

審査待ちのアプリ: ユーザーがリクエストしているアプリとクライアント ID のアクセス権を確認および構成します。
リストを表示

4 個の設定済みアプリ: アクセス ポリシーが設定されているアプリとクライアント ID を管理します。詳細
リストを表示

設定済みアプリ: 新しいアプリを設定 リストをダウンロード リストを一括更新
+ フィルタを追加

アプリを	種類	オーナー権限	ID	アクセス
<input type="checkbox"/>	ベネッセのサービス 確認済み	ウェブ	サードパーティ	112514126103-d5hghg48km7o63bcsccum42a7a45... 1 個の組織部門で設定済み

MicrosoftのSSO連携の設定追加

- SSO連携（Microsoft）を利用される場合は、Microsoft Entra管理センターの設定追加が必要になります。
Microsoft Entra管理センターの管理者ID・パスワードをお持ちの先生が作業してください。
※設定しない場合、「管理者の許可が必要」のエラーになる可能性があります。

- 1 ミライシードログイン画面の
「Office365アカウントでログイン」をクリックし、
Microsoft Entraの管理者ID・PWでログイン

The screenshot shows a login interface titled 'ログイン画面'. It has fields for 'ID' and 'パスワード' (password). Below the password field is a checkbox for 'IDを保存する' (Save ID) and a link for 'パスワードを忘れた人はこちら' (Click here if you forgot your password). At the bottom, there are two buttons: 'Google アカウントでログイン' and 'Office365 アカウントでログイン'. The 'Office365 アカウントでログイン' button is highlighted with a red box and a blue border. A line connects this button to step 1 of the instructions.

- 2 「組織の代理として同意する」にチェックを入れる

The screenshot shows a Microsoft consent screen. It displays the Microsoft logo, '管理者メールアドレス', and '要求されているアクセス許可'. Under 'ベネッセのサービス', it says '未確認'. The text states: 'このアプリケーションは、Microsoft またはお客様の組織によって公開されたものではありません。' and 'このアプリに必要なアクセス許可:'. Two permissions are listed: 'Sign in and read user profile' and 'Maintain access to data you have given it access to'. The checkbox '組織の代理として同意する' is checked and highlighted with a blue box. Below this, there is explanatory text about the permissions and a link to '詳細の表示'. At the bottom, there are two buttons: 'キャンセル' and '承諾'. The '承諾' button is highlighted with a blue box and a blue border. A line connects this checkbox to step 2 of the instructions.

- 3 「承諾」をクリック

4 Microsoft Entra管理センターにアクセス

URL <https://entra.microsoft.com>

5 「エンタープライズアプリケーション」 > 「すべてのアプリケーション」に「ベネッセのサービス」が追加されていることを確認

アプリケーションID 3cafe499-4e03-4ae8-a3c3-9e5d8e7fb9bb

Microsoft Entra 管理センター

ホーム > エンタープライズ アプリケーション

エンタープライズ アプリケーション | すべてのアプリケーション

概要

新しいアプリケーション | 更新 | ダウンロード (エクスポート) | プレビューの情報 | 列 | プレビュー機能 | フィードバックがある場合

エージェント ID (プレビュー) はエージェント ID エクスペリエンスに移動されました。エージェント ID を表示します。 →

Microsoft Entra テナントを ID プロバイダーとして使用するように設定されている。ご自身の組織内のアプリケーションを表示、フィルター処理、検索します。

組織で管理されているアプリケーションのリストは、アプリケーションの登録にあります。

アプリケーションの名前またはオブジェクト ID で...

アプリケーションの種類 == エンタープライズ アプリケーション | アプリケーション... 次の値で始まる 3cafe499-4e03-4ae8-a3c3-9e5d8e... | フィルターの追加

1 個のアプリケーションが見つかりました

名前	オブジェクト ID	アプリケーション ID	ホームページ URL	作成日	証明書有効期限...	アクティブな証明書...	識別子 URI (イン...
ベネッセのサービス	f6960bb3-1961-4e...	3cafe499-4e03-4e...	https://www.bene...	2025/12/23			3cafe499-4e03-4e...