

CHleru

InterCLASS[®] Console Support

version 4.1 操作マニュアル(設定編)

目次

はじめに-----	3
InterCLASS® Console Supportの構成-----	3
動作環境-----	4
本書の構成と読み方-----	4
Google Cloud Platform の設定-----	5
Google Workspace でのGoogle Cloud Platform の有効化-----	5
Google Cloud Platform の設定-----	7
ドメイン全体の管理を委任する設定-----	23
Google Classroom のデータアクセスの許可-----	26
QRコードログインの設定-----	28
サードパーティのIDプロバイダを使用したシングルサインオンの設定-----	28
QRコードログインを適用するChrome デバイスを特定の組織部門に移動-----	33
Chrome デバイスの設定の変更-----	36
Chromebook のログイン画面を確認-----	40
デバイスのレポート設定-----	41
InterCLASS® Console Supportの起動と終了-----	44
InterCLASS® Console Supportへログイン-----	44
InterCLASS® Console Supportからログアウト-----	46
システム管理の設定-----	47
システム管理を開く-----	47
サービスアカウント登録-----	48
QRコード情報移行-----	49
権限管理-----	51
権限管理の内部データを移行する-----	51
作成済みの権限情報を移行する-----	52
InterCLASS® Filtering Service連携設定-----	55
InterCLASS® Advance連携設定-----	60
製品間連携 実行結果-----	64
CHIeruサポートについて-----	66

はじめに

InterCLASS[®] Console Supportをご導入いただき、ありがとうございます。
InterCLASS[®] Console SupportはGoogle管理コンソールのユーザー管理機能を拡張し、学校でのユーザー管理業務を効率化するためのGoogle Workspace Marketplace アプリです。本書をよくお読みのうえ、Googleアカウントの運用管理の効率化にお役立てください。

InterCLASS[®] Console Supportの構成

InterCLASS[®] Console Support上で必要な管理権限を割り当てられた管理者は、InterCLASS[®] Console Supportの操作画面を通じてユーザーやグループの管理、Google Classroomの管理ができます。



動作環境

導入前に、あらかじめ以下の動作環境を確認してください。

必要環境

- Google Workspace for Education の利用承認を受けている教育機関であること
- Google 管理コンソールによりお客様のドメインにユーザーが追加され、組織部門が適切に設定されていること
- Chrome Education Upgrade が導入済みであり、学習者用のChromebook がGoogle 管理コンソールに登録されていること

管理画面を使用するコンピュータ

- OS : Windows 11 / 10
最新のChrome OS
- アプリ : 最新のChromeブラウザ
- メモリ : 4GB以上
- その他 : Wi-Fi,Ethernet機能またはLTE通信機能を有すること
インターネットに接続されていること

本書の構成と読み方

本書では、InterCLASS[®] Console Supportの導入と運用にあたり、特権管理者が行うGoogle管理コンソールの設定とInterCLASS[®] Console Supportの設定について記載しています。管理者権限が割り当てられた学校管理者によるユーザー・グループ等の運用管理方法については、別冊「InterCLASS[®] Console Support 操作マニュアル」をご参照ください。

Google Cloud Platform の設定

ドメイン管理者以外のユーザーのご利用には、Google Cloud Platform のご契約とサービスアカウントの発行が必要です。本サービスにおいて、お客様に課金が発生するサービスの利用は求められません。Google 管理コンソールからGoogle Cloud Platform を有効化し、Google Cloud Platform でサービスアカウントを発行します。

⚠️ 注意

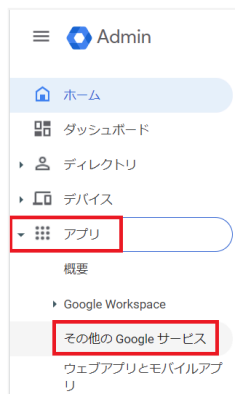
- 2021年9月以降、Google Workspace for Education では、一部のGoogle サービスで年齢に基づくアクセス制御が追加され、規定の設定になっています。Google Cloud Platform も既定の設定では規制されるサービスに含まれるため、事前に設定変更が必要です。詳しくは下記の管理者ヘルプをご参照ください。

Google サービスへのアクセスを年齢別に管理する

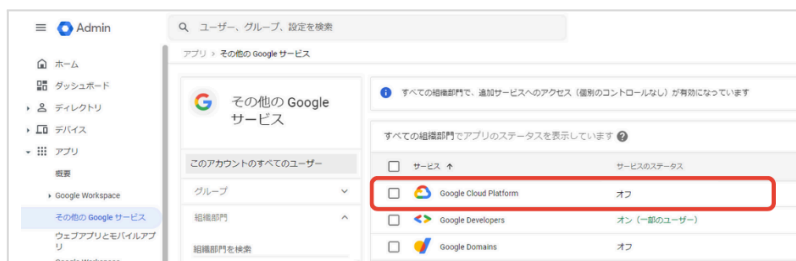
<https://support.google.com/a/answer/10651918>

Google Workspace でのGoogle Cloud Platform の有効化

- Google 管理コンソール(<https://admin.google.com>)へアクセスします。
- メニューからアプリ>その他のGoogleサービスをクリックします。



- Google Cloud Platform をクリックします。



4. Google Cloud Platform の設定画面でサービスのステータスをクリックします。



5. サービスのステータス画面で特権管理者が所属する任意の組織部門を選択し、サービスのステータスをオンにし、オーバーライド(または保存)をクリックします。



6. Google Cloud Platform の設定画面に戻り、プロジェクト作成の設定をクリックします。

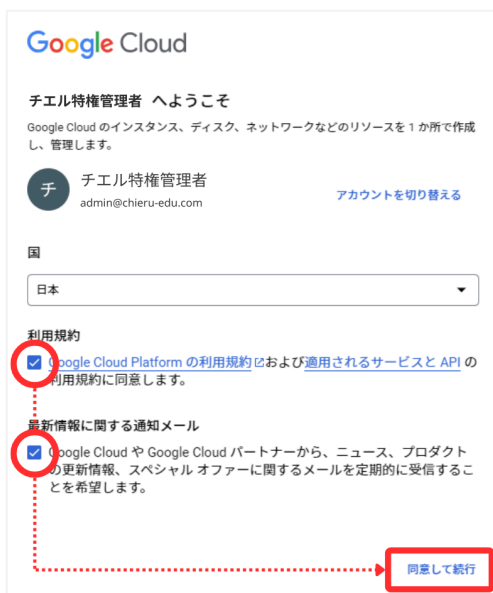


7. Cloud Resource Manager API の設定画面のユーザーにプロジェクトの作成を許可するにチェックを入れ、保存をクリックします。



Google Cloud Platform の設定

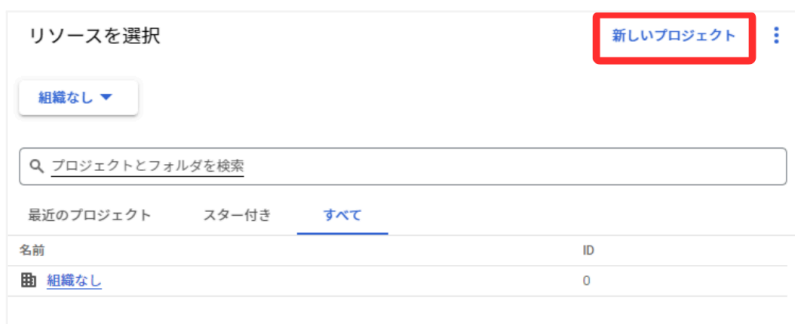
1. Chrome ウェブブラウザでGoogle Cloud Platform (<https://console.cloud.google.com>)にアクセスします。
2. 初回アクセスの場合以下のような画面が表示されます。利用規約にチェックをいれ、同意して続行をクリックします。



3. ページ最上部トッパーのGoogle Cloud 表記の右側にあるプロジェクトの選択をクリックします。



4. リソースを選択ダイアログの新しいプロジェクトをクリックします。



5. 新しいプロジェクト画面のプロジェクト名に任意の名称を入れ、作成ボタンをクリックします。

Google Cloud

新しいプロジェクト

プロジェクト名 *
My Project 500

プロジェクト ID: strong-minutia-391003。後で変更することはできません。 [編集](#)

組織 *
プロジェクトに関連付ける組織を選択します。この選択を後で変更することはできません。

場所 * [参照](#)

親組織またはフォルダ

[作成](#) [キャンセル](#)

6. プロジェクトの作成が終了すると以下のような通知が届きます。プロジェクトを選択をクリックし、プロジェクトのダッシュボードに移動します。



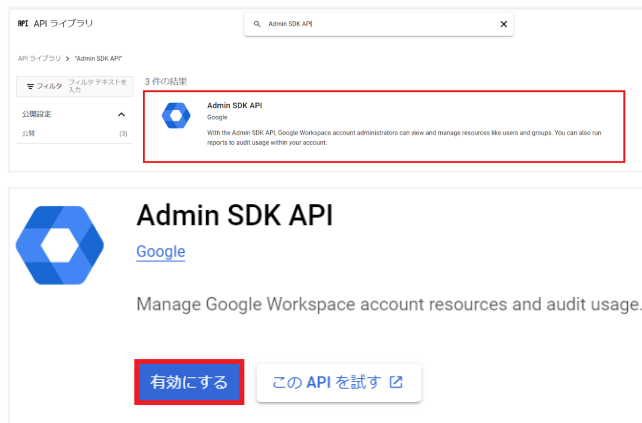
7. メニューからAPI とサービス>ライブラリをクリックします。



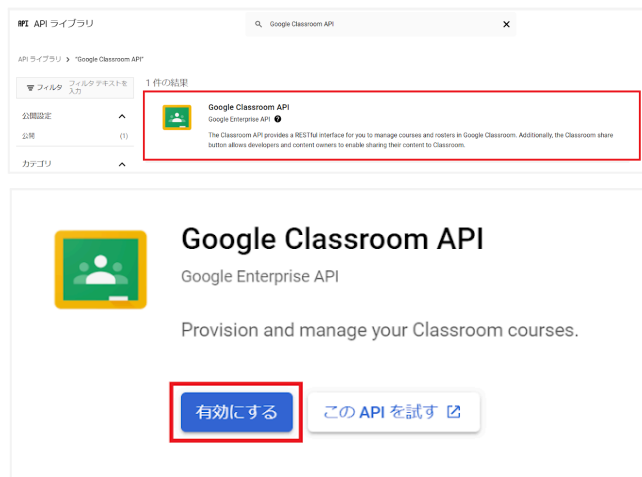
8. API ライブラリ画面のAPI とサービスの検索ボックスに「Admin SDK API」と入力します。



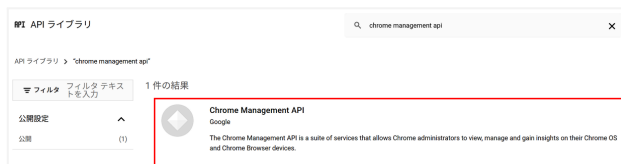
9. 検索結果に表示されたAdmin SDK API をクリックし、有効にするボタンをクリックします。



10. 手順8.9と同じ操作で「Google Classroom API」を検索し、有効にするボタンをクリックします。



11. 手順8.9と同じ操作で「Chrome Management API」を検索し、有効にするボタンをクリックします。



15. プリンシパル別に表示タブ内に管理者ユーザーが存在するか確認します。

a. 管理者ユーザーが存在する場合

i. 編集アイコンをクリックし、ロールを割り当てる画面を開きます。

プリンシパル別に表示		ロール別に表示	
+ アクセスを許可		- アクセス権を削除	
≡ フィルタ プロパティ名または値を入力			
<input type="checkbox"/> タイプ	プリンシパル ↑	名前	ロール
<input type="checkbox"/> 人			プリンシパル アクセス境界ポリシー管理者 
			組織の管理者
			組織ポリシー管理者

ii. 管理者ユーザーが**組織の管理者**ロールを保有していない場合、**ロールを追加**または**別のロールを追加**をクリックします。保有している場合、iv.に進みます。

「 」に対する権限の編集

プリンシパル ● プロジェクト

ロールを割り当てる
ロールは一連の権限で構成され、プリンシパルがこのリソースで実行できることを決定します。 [詳細](#)

+ ロールを追加

保存 変更をテスト ⓘ キャンセル

iii. フィルタに「**組織管理者**」と入力し、表示される以下のロールをクリックします。

ロール IAM の条件 (占拠) ⓘ

検索 組織管理者 ×

組織管理者
IAM ポリシーを管理し、組織、フォルダ、プロジェクトの組織のポリシーを表示するためのアクセス権。

DNS 管理者
DNS リソースへの完全な読み取り / 書き込みアクセス権

Batch 管理者
Batch リソースの管理者

Assured Workloads 管理者
Assured Workloads リソース、CRM リソース (プロジェクト / フォルダ、組織ポリシーの管理) に対する完全アクセス権を付与します。

ロールを管理

- iv. 管理者ユーザーが**組織ポリシー管理者**ロールを保有していない場合、続けて別のロールを追加をクリックします。

ルールを割り当てる

ルールは一連の権限で構成され、プリンシパルがこのリソースで実行できることを決定します。 [詳細](#)

ルール: **組織管理者** IAM の条件 (省略可) ⓘ + IAM の条件を追加

IAM ポリシーを管理し、組織、フォルダ、プロジェクトの組織のポリシーを表示するためのアクセス権。

+ 別のロールを追加

保存 変更をテスト ⓘ キャンセル

- v. フィルタに「**組織ポリシー管理者**」と入力し、表示される以下のロールをクリックします。

ルールを割り当てる

ルールは一連の権限で構成され、プリンシパルがこのリソースで実行できることを決定します。 [詳細](#)

ルール: **組織管理者** IAM の条件 (省略可) ⓘ + IAM の条件を追加

IAM ポリシーを管理し、組織、フォルダ、プロジェクトの組織のポリシーを表示するためのアクセス権。

検索: 組織ポリシー管理者

組織ポリシー管理者
リソースの組織ポリシーを設定する権限。

Dataform 管理者
すべての Dataform リソースに対する完全アクセス権。

Assured Workloads 管理者
Assured Workloads リソース、CRM リソース (プロジェクト/フォルダ、組織ポリシーの管理) に対する完全アクセス権を付与します。

ネットワーク管理者
ネットワーク管理者が、ネットワークと関連する GCP リソースを管理

ロールを管理

- vi. 2つのロールが割り当てられていることを確認し、**保存**ボタンをクリックします。

ルールを割り当てる

ルールは一連の権限で構成され、プリンシパルがこのリソースで実行できることを決定します。 [詳細](#)

ルール: **組織管理者** IAM の条件 (省略可) ⓘ + IAM の条件を追加

IAM ポリシーを管理し、組織、フォルダ、プロジェクトの組織のポリシーを表示するためのアクセス権。

ルール: **組織ポリシー管理者** IAM の条件 (省略可) ⓘ + IAM の条件を追加

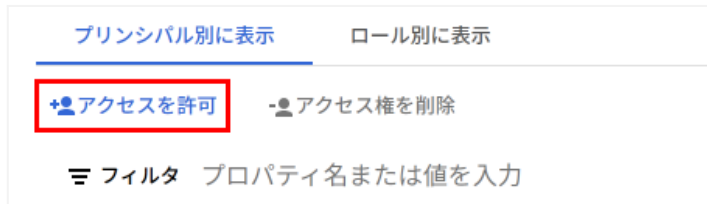
リソースの組織ポリシーを設定する権限。

+ 別のロールを追加

保存 変更をテスト ⓘ キャンセル

b. 管理者となるユーザーが存在しない場合

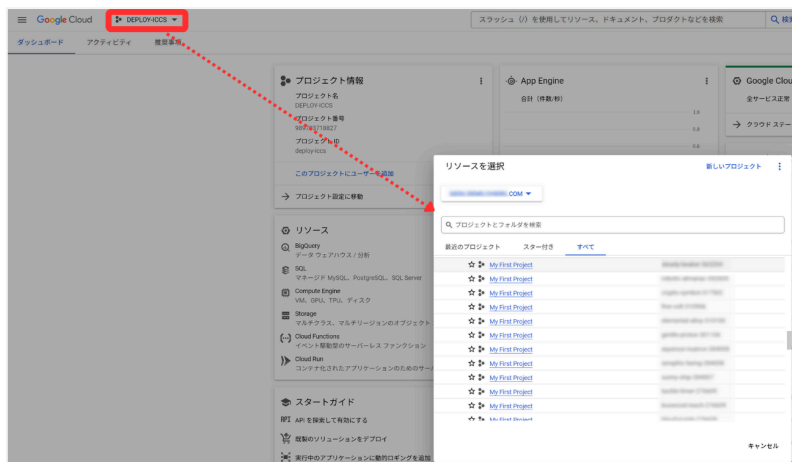
- i. アクセス権を許可をクリックします。



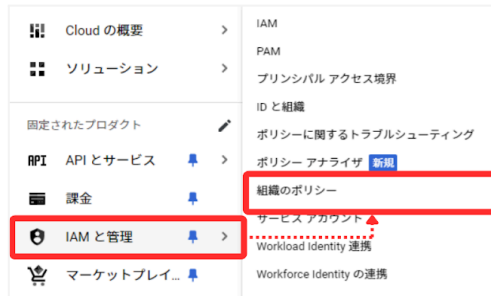
- ii. 管理者ユーザーのメールアドレスを新しいプリンシパルに入力し、a. のii. ~ vi. と同じ手順でロールの割り当てを行います。



16. ヘッダーのプルダウンリストをクリックし、リソースを選択ダイアログでサービスアカウントを発行するプロジェクトを選択します。



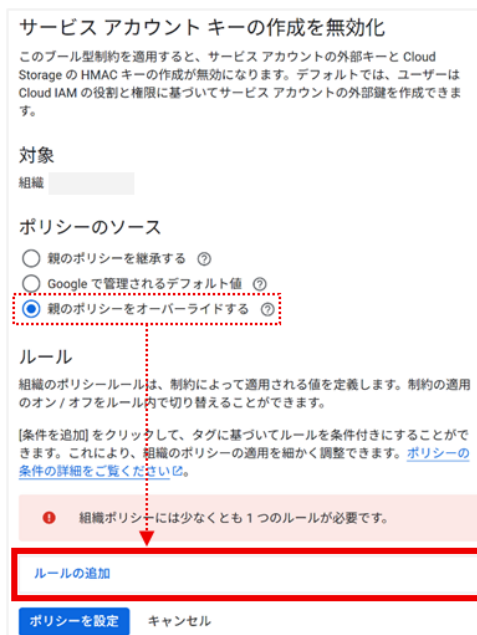
17.メニュー>IAM と管理>組織のポリシーへ移動します。



18.フィルタに「disableServiceAccountKeyCreation」と入力して表示されるものをクリックし、一覧内に表示される **iam.disableServiceAccountKeyCreation** の右側にあるメニューからポリシーの編集をクリックします。



19.ポリシーのソースを親のポリシーをオーバーライドするに変更し、下に表示されるルールを追加をクリックします。



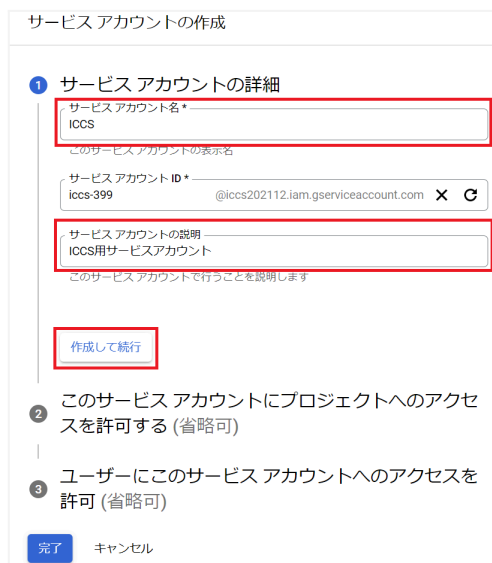
20. 適用をオフを選択した状態で、ポリシーを設定ボタンをクリックします。設定した組織下のプロジェクトでサービスアカウントキーの発行が可能となります。



21. サービスアカウント画面の+サービス アカウントを作成をクリックします。



22. サービスアカウントの作成画面のサービスアカウントの詳細で任意のサービスアカウント名とサービスアカウントの説明を入力し、作成して続行ボタンをクリックします。



23. このサービスアカウントにプロジェクトへのアクセスを許可する>Projectのロールをオーナーに設定し、完了ボタンをクリックします。(※項目3の設定は不要です)

The screenshot shows the 'IAM の条件 (省略可)' dialog box. On the left, the 'Project' role is selected. On the right, the 'オーナー' (Owner) role is selected. A '完了' (Done) button is visible at the bottom left of the dialog. To the right of the dialog, a notification box states: 'ユーザーにこのサービス アカウントへのアクセスを許可 (省略可)' with '完了' and 'キャンセル' buttons.

24. サービスアカウント画面から作成したサービス アカウントのメールのメールアドレスをクリックし、設定画面へ移動します。

The screenshot shows the 'サービス アカウント' (Service Accounts) page. A table lists the service accounts. The email address 'iccs-769@intense-petal-368906.iam.gserviceaccount.com' is highlighted in red.

メール	ステータス	名前 ↑	説明
iccs-769@intense-petal-368906.iam.gserviceaccount.com	✓	ICCS	ICCS用サービス

25. 詳細設定をクリックし、OAuth クライアントを作成するには、OAuth 同意画面を構成する必要があります。の下にある構成をクリックします。

詳細 権限 キー 指標 ログ

サービス アカウントの詳細

保存

保存

メール

一意の ID

サービス アカウントのステータス

アカウントを無効にすることによって、アカウントを削除することなくポリシーを保持できます。

● アカウントは現在アクティブです

サービス アカウントの無効化

詳細設定

ドメイン全体の委任

△ ドメイン全体の委任によって組織のデータへのアクセス権をこのサービス アカウントに付与する場合には、注意深く行う必要があります。元に戻すには、サービス アカウントを無効化または削除するか、Google Workspace 管理コンソールからアクセス権を削除します。

ドメイン全体の委任の詳細は

クライアント ID: 102163024207641961293

Google Workspace 管理コンソールを表示は

Google Workspace Marketplace OAuth クライアント

△ この OAuth クライアントの作成は、ドメインでの Google Workspace Marketplace のインストールをサポートするために必要であり、慎重に使用する必要があります。Google Workspace Marketplace は、プロジェクト内のすべての OAuth クライアントに権限を付与する場合があります。この操作を元に戻すには、サービス アカウントを無効にするか削除するしかありません。

クライアント アクセスの詳細は

○ OAuth クライアントを作成するには、OAuth 同意画面を構成する必要があります。

構成

26. 「Google Auth Platformはまだ構成されていません」表示の下の開始ボタンをクリックします。



27. プロジェクト構成画面のアプリ情報でアプリ名に任意の名称、ユーザーサポートメールに任意のメールアドレスを設定し、次へボタンをクリックします。

プロジェクト構成

1 アプリ情報

アプリ名 *

同量を求めるアプリの名前

ユーザー サポートメール *

同量に同じ問い合わせる際に使用します。 [詳細は](#)

次へ

28. 対象に内部を選択し、次へボタンをクリックします。

プロジェクト構成

1 アプリ情報

2 対象

内部 ⓘ

組織内のユーザーのみが使用できます。確認を受けるためにアプリを送信する必要はありません。[ユーザーの種類の詳細](#)

外部 ⓘ

Google アカウントを持つすべてのテストユーザーが使用できます。アプリはテストモードで起動し、アプリを使用できるのは、テストユーザーのリストに追加されたユーザーに限られます。アプリを本番環境に移す準備ができたなら、アプリの確認が必要となる場合があります。[ユーザーの種類の詳細](#)

次へ

29. 連絡先情報に任意のメールアドレス(例:管理者のメールアドレス)を設定し、次へボタンをクリックします。

プロジェクト構成

1 アプリ情報

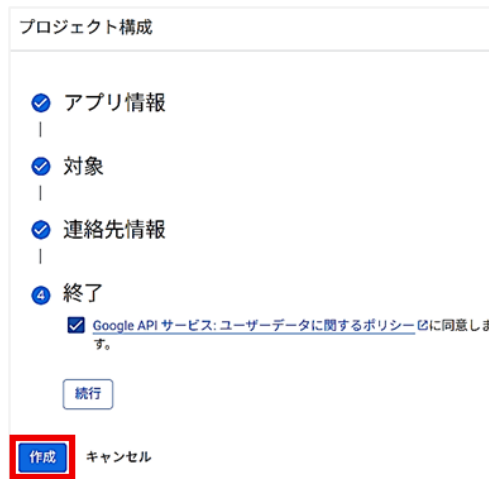
2 対象

3 連絡先情報

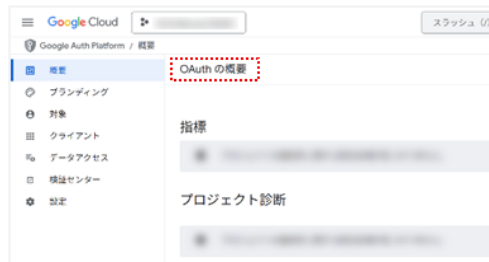
これらのメールアドレスは、プロジェクトの変更について Google からお知らせするために使用します。

次へ

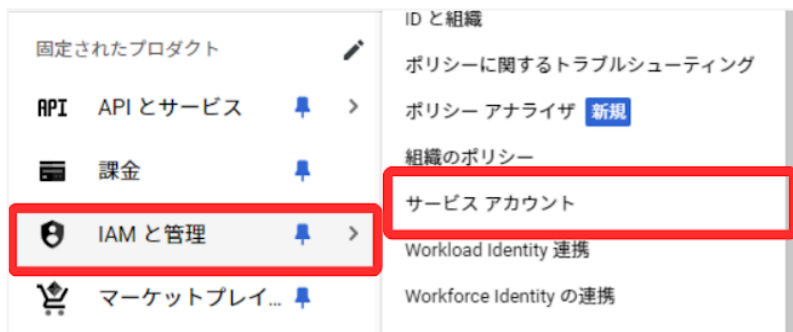
30. 作成をクリックします。



31. OAuth の概要画面が表示されたら、操作は終了です。



32. 再度、メニューからIAM と管理>サービス アカウントをクリックします。



33. サービスアカウント画面のOAuth2クライアントID から操作を選び、鍵を管理をクリックします。



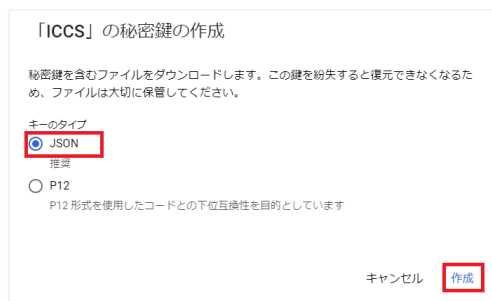
注意

- OAuth2クライアントID の番号は、このあとの工程で使用しますので必ず番号を控えてください。

34. キータブの鍵を追加>新しい鍵を作成をクリックします。



35. 秘密鍵の作成画面のキーのタイプでJSON を選択し、作成をクリックします。



36. JSON形式の秘密鍵がダウンロードされます。

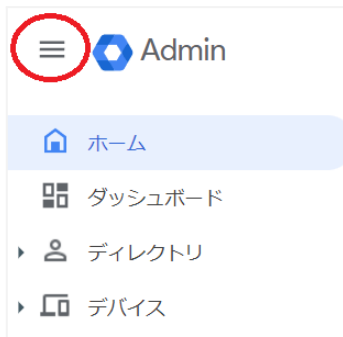


注意

- 生成された秘密鍵は、InterCLASS® Console Supportの秘密鍵を初回ログイン時に登録していただくため、厳重に保管してください。
- 同じ鍵は、1度しかダウンロードできません。紛失した場合は、再作成する必要があります。

ドメイン全体の管理を委任する設定

1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com>)にアクセスします。
2. 特権管理者のアカウントでサインインします。
3. メインメニューをクリックします。



4. セキュリティ>アクセスとデータ管理>API の制御をクリックします。



5. API の制御画面でドメイン全体の委任>ドメイン全体の委任を管理をクリックします。



6. ドメイン全体の委任画面で新しく追加をクリックします。



7. 新しいクライアントID を追加画面が表示されます。

8. クライアントID にGoogle Cloud Platform の設定の手順33.で表示したクライアントID を入力し、OAuth スコープに下記の必要なスコープをカンマ区切りで全て記述します。

■必要なスコープの一覧

```
https://www.googleapis.com/auth/admin.directory.user,  
https://www.googleapis.com/auth/admin.directory.customer.readonly,  
https://www.googleapis.com/auth/admin.directory.group,  
https://www.googleapis.com/auth/admin.directory.orgunit,  
https://www.googleapis.com/auth/admin.directory.userschema,  
https://www.googleapis.com/auth/script.external_request,  
https://www.googleapis.com/auth/classroom.courses,  
https://www.googleapis.com/auth/classroom.rosters,  
https://www.googleapis.com/auth/classroom.profile.emails,  
https://www.googleapis.com/auth/classroom.profile.photos,  
https://www.googleapis.com/auth/sqlservice,  
https://www.googleapis.com/auth/admin.directory.device.chromeos,  
https://www.googleapis.com/auth/chrome.management.telemetry.readonly,  
https://www.googleapis.com/auth/classroom.announcements.readonly,  
https://www.googleapis.com/auth/classroom.student-submissions.students.readonly
```

9. クライアントID とスコープを入力後、承認をクリックします。

新しいクライアント ID を追加

クライアント ID

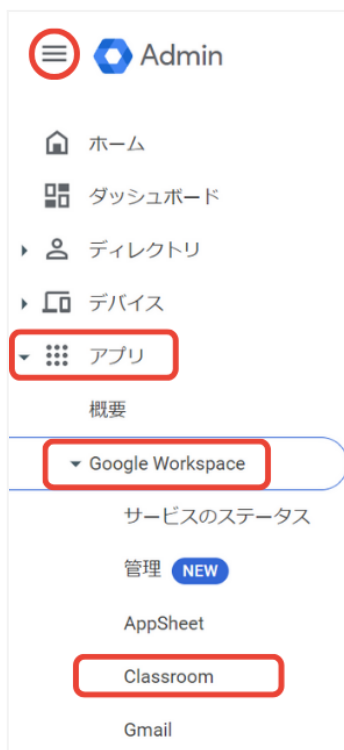
既存のクライアント ID を上書きする ⓘ

OAuth スコープ (カンマ区切り)

キャンセル 承認

Google Classroom のデータアクセスの許可

1. メニュー>アプリ>Google Workspace >Classroom をクリックします。



2. Classroom の設定画面が開きます。



3. データアクセスをクリックします。



4. 適用する組織部門を選択し、ユーザーは、Google Classroom データへのアクセスをアプリに許可することができます。にチェックを入れ、保存をクリックします。



QRコードログインの設定

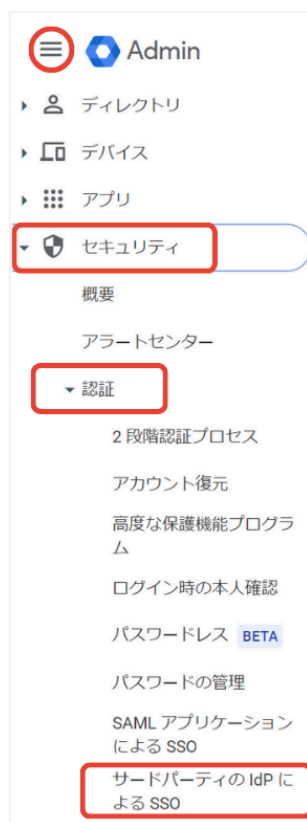
QRコードを使ったChromebook へのログイン機能を有効にする場合は、Google 管理コンソールで以下の設定を適用します。

サードパーティのIDプロバイダを使用したシングルサインオンの設定

QRコードを使用したChromebook へのログインに必要な設定です。

⚠️注意

- 本設定は、特権管理者アカウントで実施してください。
1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com/>)にアクセスします。
 2. 特権管理者のアカウントでサインインします。
 3. メニュー>セキュリティ>認証>サードパーティのIdPによるSSO をクリックします。



4. サードパーティのIDプロバイダ(IdP)によるシングルサインオン(SSO)画面が開きます。

セキュリティ > サードパーティのIDPによるSSO

サードパーティの ID プロバイダ (IdP) によるシングルサインオン (SSO)

SSO を設定すると、ユーザーはサードパーティの IDP でログインして Google Workspace サービスにアクセスできるようになります。 [詳細](#)

サードパーティの SSO プロファイル

組織部門またはグループに割り当てることができる SSO プロファイルは以下のとおりです。 [SSO プロファイルの詳細](#)

[SAML プロファイルを追加](#)

名前	種類	ステータス
Legacy SSO Profile	SAML	有効
Microsoft	OIDC BETA	システム プロファイル ⓘ

SSO プロファイルの割り当ての管理

組織部門またはグループ向けの割り当てを表示、管理します。 [詳細](#)

[管理](#)

名前	種類	SSO プロファイル
テール株式会社	組織部門	以前の SSO プロファイル

5. SAML プロファイルを追加をクリックします。

サードパーティの SSO プロファイル

組織部門またはグループに割り当てることができる SSO プロファイルは以下のとおりです。 [SSO プロファイルの詳細](#)

[SAML プロファイルを追加](#)

6. IdPの詳細ページの下部にある以前のSSOプロファイルの設定に移動をクリックします。

7. 以前の SSO プロファイルを有効にするにチェックを入れ、ログインページの URL と ログアウトページの URL に以下の URL を設定します。

a. ログインページの ID

<https://sso.interclasscloud.com:443/idp/SSORedirect/metaAlias/idp>

b. ログアウトページの ID

<https://sso.interclasscloud.com:443/idp/SSORedirect/metaAlias/idp>

以前の SSO プロファイル

以前の SSO プロファイルを有効にする

すべてのユーザーは、サードパーティの IdP を使用して Google Workspace にログインします（除外した組織部門またはグループを除く）。[SSO プロファイル](#)と[特権管理者 SSO](#) についての記事をご覧ください。

サードパーティの ID プロバイダを使用した管理対象 Google アカウントへのシングルサインオンを設定するには、以下の情報を入力してください。 [詳細](#)

ログインページの URL
<https://sso.interclasscloud.com:443/idp/SSORedirect/metaAlias/idp>

システムと Google Workspace へのログイン用 URL

ログアウト ページの URL
<https://sso.interclasscloud.com:443/idp/SSORedirect/metaAlias/idp>

ユーザーがログアウトするときにリダイレクトする URL

8. ドメイン固有の発行元を使用にチェックを入れ、ネットワークマスクに 1.1.1.1/32 を入力します。

ドメイン固有の発行元を使用

ネットワークマスク
1.1.1.1/32

ネットワーク マスクにより、シングルサインオンが運用されるアドレスが決まります。マスクを指定しない場合、ネットワーク全体に対して SSO 機能が運用されます。マスクの区切りにはセミコロンを使用します（例: 64.233.187.99/8; 72.14.0.0/16）。範囲の指定にはダッシュを使用します（例: 64.233.167-204.99/32）。ネットワーク マスクは CIDR 表記にする必要があります。 [詳細](#)

9. 保存をクリックします。

⚠️ 注意

- 証明書ファイルの登録が必要な場合、Google 管理コンソールで証明書ファイルを登録します。証明書を求められる場合、次の手順で、InterCLASS[®] Console Support から証明書を取得します。

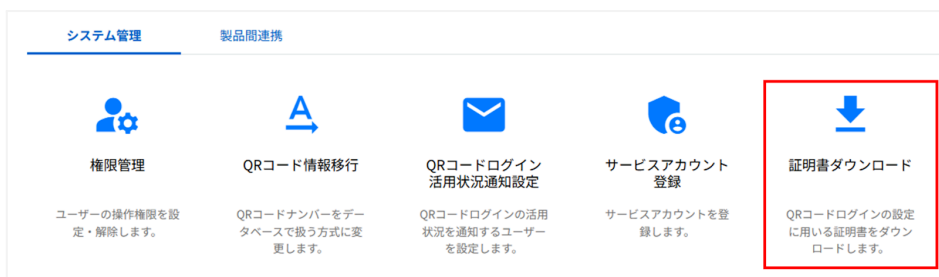
10. Chrome ウェブブラウザでInterCLASS® Console Support

(<https://cs.interclass.jp/>)にアクセスし、特権管理者アカウントでログインします。

11. 左のメニューからシステム管理をクリックします。



12. システム管理画面で証明書ダウンロードをクリックします。

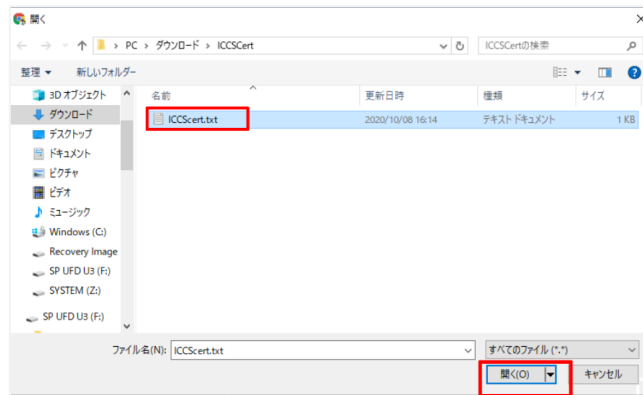


13. ICCSCert.zipがダウンロードされます。

14. Google 管理コンソールに戻り、サードパーティのIDプロバイダを使用したシングルサインオン(SSO)の設定画面で確認用の証明書の証明書をアップロードをクリックします。



15. システムの管理画面からダウンロードしたICCSCert.zipファイルを事前に展開しておき、ICCScert.txtを選択し、開きます。



16. 証明書がアップロードされると下記の表示になります。



17. 未保存の変更の表示で保存をクリックします。

QRコードログインを適用するChrome デバイスを特定の組織部門に移動

特定の組織部門に所属するChrome デバイスに対してのみQRコードログイン機能を有効にする場合は、デバイスの設定を特定の組織部門に適用するため、Google 管理コンソールに登録したChrome デバイスを対象の組織部門に移動します。

⚠注意

- 本設定は、特権管理者アカウントで実施してください。
- 既にChrome デバイスを組織部門にわけて管理している場合は、設定変更の必要はありません。

📌ポイント

- 組織部門はユーザー用とデバイス用に分けて作成することを推奨します。これによりデバイスとユーザーのポリシーを別々に管理することができます。
詳しくは、以下のGoogle Workspace 管理者ヘルプ> [ユーザー別にポリシーを適用する](#)をご参照ください。

(組織部門の作成例)

- ▼ 教育委員会
 - ▼ 教職員ユーザー
 - 教育委員会
 - 管理職
 - 教諭
 - ICT管理者
 - ▼ 教職員デバイス
 - ▼ 児童生徒
 - ▼ チエル第1小学校
 - 児童生徒デバイス
 - ▼ 児童生徒ユーザー
 - 各学年
 - ▼ チエル第2小学校
 - 児童生徒デバイス
 - ▼ 児童生徒ユーザー
 - 各学年

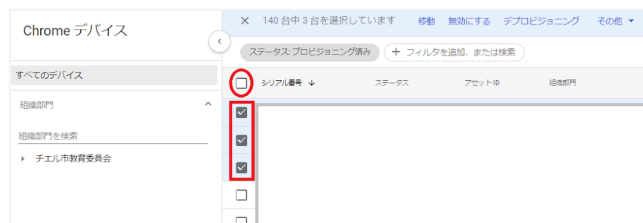
デバイスの組織部門を作成し、
Chromeデバイスを登録する

※最適なユーザー・デバイスの組織部門の構成は、学校や教育委員会の規模や運用方法によって異なります。

1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com/>)にアクセスします。
2. 特権管理者のアカウントでサインインします。
3. メニュー>デバイス>Chrome >デバイスをクリックします。



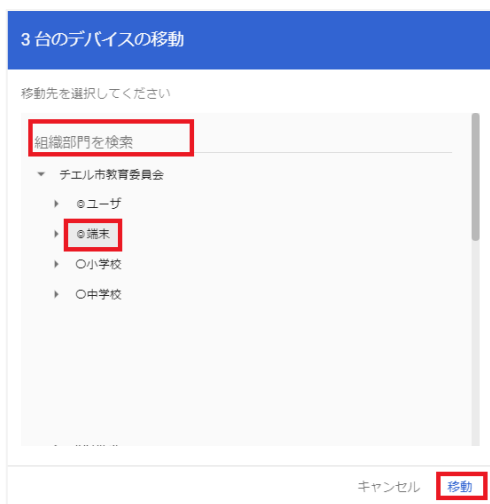
4. Chrome デバイスの一覧画面でQRコードログインを有効にするChrome デバイスにチェックを入れ、選択します。



5. 操作コマンドの移動をクリックします。



6. デバイスの移動画面で移動先の組織部門を選択し、移動をクリックします。



7. 選択したデバイスが移動先の組織部門に移動します。

Chrome デバイスの設定の変更

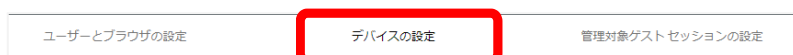
QRコードログイン機能を利用するChrome デバイスが含まれる組織部門のデバイスの設定を変更します。

⚠注意

- 本設定は、特権管理者アカウントで実施してください。
1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com/>)にアクセスします。
 2. 特権管理者のアカウントでサインインします。
 3. メニュー>デバイス>Chrome >設定をクリックします。



4. デバイスの設定タブを選択します。



5. 組織部門のツリーからQRコードログインを有効にするChrome デバイスが含まれる組織部門を選択します。



④ポイント

- QRコードログイン機能を特定のChromebook のみに有効にする場合は、対象のChrome デバイスを特定の組織部門に移動します。詳細は、[QRコードログインを適用するChromeデバイスを特定の組織部門に移動](#)をご参照ください。

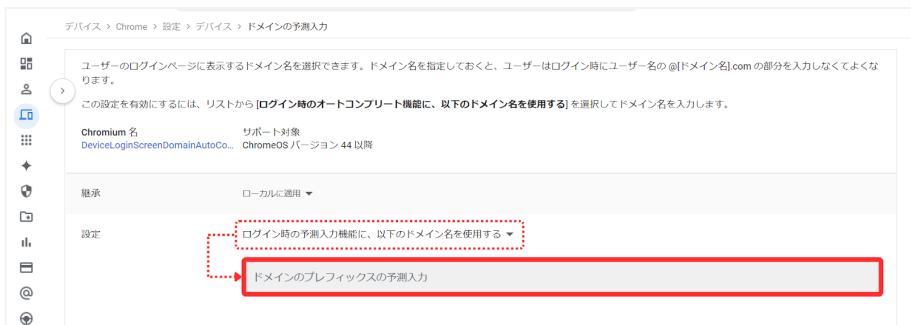
6. ログイン設定の項目に移動します。



7. ゲストモードの設定をゲストモードを無効にするに変更します。



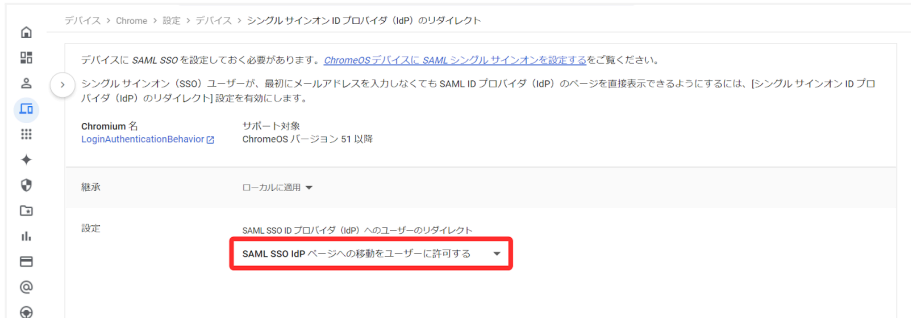
8. ドメインの予測入力の設定をログイン時のオートコンプリート機能に、以下のドメイン名を使用するに変更し、ドメインのプレフィックスの予測入力にお客様のドメイン名を入力します。



9. ログイン画面の設定をユーザー名と写真を表示しないに変更します。



10. シングルサインオン ID プロバイダ(IdP)のリダイレクトの設定をSAML SSO IdP ページへの移動をユーザーに許可するに変更します。



11. シングルサインオンによるカメラへのアクセスの許可の設定に <https://sso.interclasscloud.com> を入力します。



Chromebook のログイン画面を確認

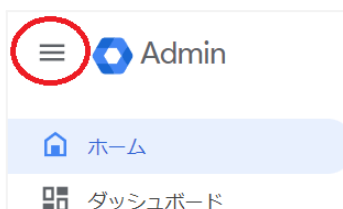
上記の設定が全て正常に適用されると、対象のChromebook のログイン画面が変更され、QRコードを使用したChromebook へのログインができるようになります。
ログイン画面は以下のように変わります。



デバイスのレポート設定

デバイス管理画面でバッテリー状態とネットワークレポートの表示を行う場合は、Google 管理コンソールで以下の設定を適用します。

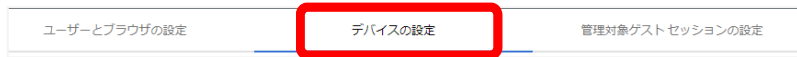
1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com>)にアクセスします。
2. 特権管理者のアカウントでサインインします。
3. メインメニューをクリックします。



4. デバイス>Chrome>設定をクリックします。



5. デバイスの設定タブを選択します。



6. ユーザーとデバイスのレポートに移動し、デバイスのテレメトリーを報告をクリックします。



7. 組織部門のツリーからレポートを取得するChrome デバイスが含まれる組織部門を選択します。



8. 設定からカスタマイズを選択し、ネットワークのステータスと電力のステータスにチェックを入れます。



9. 保存ボタンをクリックします。

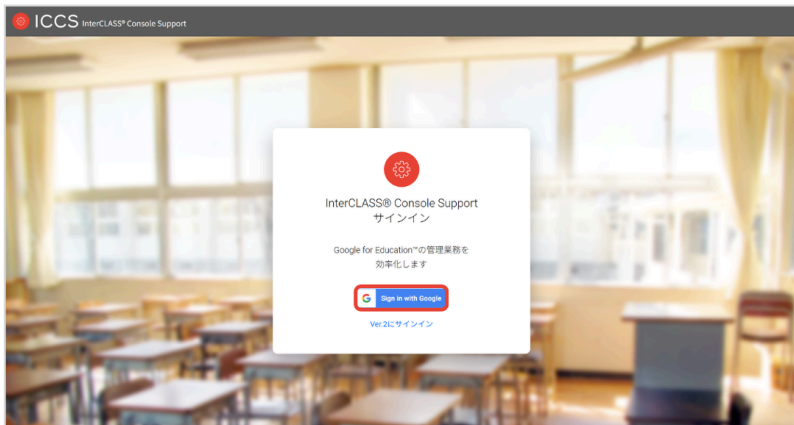


InterCLASS[®] Console Supportの起動と終了

InterCLASS[®] Console Supportへアクセスし、特権管理者アカウントでログインします。

InterCLASS[®] Console Supportへログイン

1. Chrome ウェブブラウザで新しいタブを開き、InterCLASS[®] Console Support(<https://cs.interclass.jp/>)にアクセスします。
2. **Sign in with Google** ボタンをクリックします。



3. **Google** にログイン画面が表示されます。管理者のメールアドレスを入力し、次へボタンをクリックします。



4. パスワードを入力し、次へボタンをクリックします。

Google にログイン

ようこそ

パスワードを入力

パスワードを表示します

続行するにあたり、Google はあなたの名前、メールアドレス、言語設定、プロフィール写真を chierudev.info と共有します。

パスワードをお忘れの場合

次へ

5. InterCLASS® Console Supportのトップページが表示されます。

ICCS InterCLASS® Console Support Ver.4.1.1

管理者沖縄 沖縄

ホーム

Googleユーザー管理

Google Classroom管理

ログイン管理

デバイス管理

組織部門

ユーザー

グループ

組織部門の追加、削除、名前変更を行います

ユーザーを追加、管理します

グループとミーティングリストを作成します

Googleユーザー管理

- 組織部門
- ユーザー
- グループ

Google Classroom管理

- クラス

ログイン管理

- QRコードログイン

デバイス管理

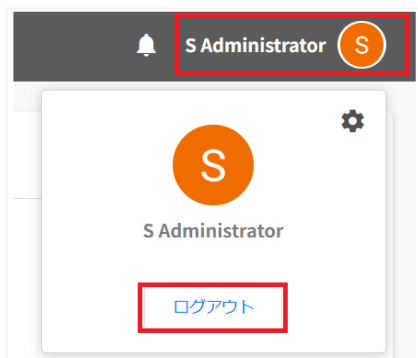
- デバイス
- デバイスレポート

システム関連

- システム管理
- 製品間連携
- 実行ジョブ一覧

InterCLASS® Console Supportからログアウト

InterCLASS® Console Supportからログアウトする際はアカウント名をクリックし、ログアウトをクリックします。



システム管理の設定

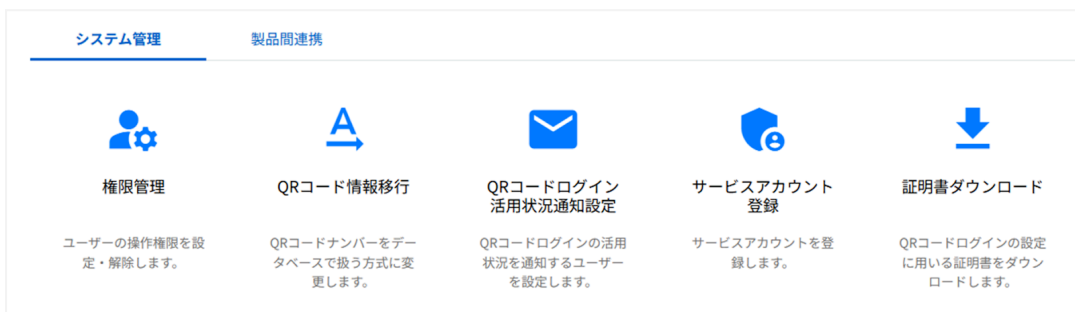
InterCLASS® Console Supportのシステム管理は特権管理者としてログインし、システム管理のため初期設定を行います。システム管理では、権限管理、QRコード情報移行、QRコードログイン活用状況通知設定、サービスアカウント登録、証明書ダウンロードが行えます。

システム管理を開く

1. 左のメニューからシステム管理をクリックします。



2. システム管理画面が開きます。



サービスアカウント登録

GCP(Google Cloud Platform)で作成したサービスアカウントの秘密鍵(.json)をアップロードします。この操作はInterCLASS® Console Supportの利用開始時に行います。

1. システム管理画面のサービスアカウント登録をクリックします。



2. サービスアカウント登録画面が開きます。

サービスアカウント登録

GCPで作成したサービスアカウントの秘密鍵をアップロードします。

登録状態：未登録

インポートファイル: 選択されていません

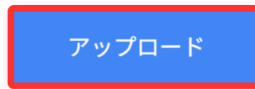
3. インポートファイルのファイルを選択ボタンをクリックします。

インポートファイル:

4. インポートファイルを選択すると次のようにファイル名が表示されます。

インポートファイル:

- アップロードボタンをクリックします。



- サービスアカウント登録画面をもう一度開きます。
- サービスアカウント登録画面の登録状態が登録済みになっていることを確認してください。

サービスアカウント登録

GCPで作成したサービスアカウントの秘密鍵をアップロードします。

登録状態：登録済み

インポートファイル： 選択されていません

QRコード情報移行

InterCLASS[®] Console Supportで作成するQRコード情報の保存場所をGoogle のユーザー情報からシステム内のデータベースに変更します。

- システム管理画面からQRコード情報移行をクリックします。



2. QRコード情報の移行画面で、実行するボタンをクリックします。

QRコード情報の移行

QRコードナンバーのデータベースへの移行を実行しますか？
ドメイン内のユーザー数が多い場合、完了まで時間がかかります。
移行中、新たなQRコードの有効化や、発行済みのQRコードの無効化はできません。

※現在発行済みのQRコードは引き続きご利用いただけます。
移行実行中は他の操作ができません。全ユーザー分の処理が完了するまでお待ちください。

キャンセル 実行する

⚠注意

- 移行実行中は、QRコード利用状況の変更はできません。ただし、発行済みQRコードでのログインは、移行中もご利用いただけます。
- ドメイン内のユーザー数が多い場合、移行に時間がかかる場合があります。

3. QRコードナンバーの移行が完了しました。と表示されたら閉じるボタンをクリックして終了します。

QRコードナンバーの移行が完了しました。

閉じる

📌ポイント

- 移行実行中に再度QRコード情報移行をクリックすると以下のようなダイアログが開き、中止するボタンをクリックすると実行中の移行を中止することができます。

QRコード情報の移行

2023/6/16 16:29に実行したQRコードの移行が完了していません。
新たに移行を実行するため、過去の移行処理を中止しますか？

キャンセル 中止する

- 移行完了後は、QRコード情報移行をクリックしても処理は発生しません。

QRコード情報の移行

QRコード情報は既に移行済みです。

閉じる

権限管理

サービスアカウントを利用する場合、InterCLASS® Console Supportに利用申請時に記載した特権管理者でログインし、権限管理の設定を行います。詳しくは、InterCLASS® Console Support 操作マニュアルをご参照ください。



権限管理の内部データを移行する

InterCLASS® Console Supportをv2.4からご利用いただいている場合は、v4.1のご利用にあたり、権限管理の内部データ移行作業が必要です。

⚠注意

- 最新バージョンへの移行が完了していない場合、「お客様の組織は最新バージョンへの移行が完了していません。上記リンクからVer.2にサインインしてください。」とメッセージが表示されます。

作成済みの権限情報を移行する

⚠️ 注意

- 本設定は、特権管理者アカウントで実施してください。

1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。



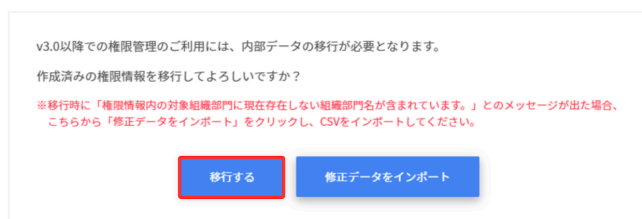
2. 左のメニューから**システム管理**をクリックします。



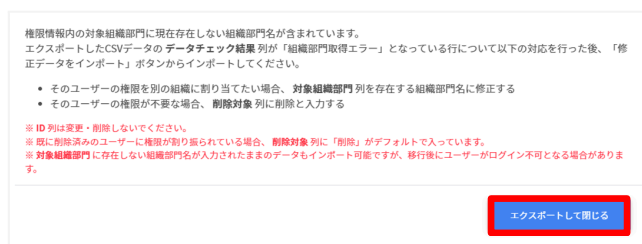
3. システム管理画面を開きます。権限管理をクリックします。



4. 権限管理画面を開くと、次のようなダイアログが開きます。移行するボタンをクリックします。

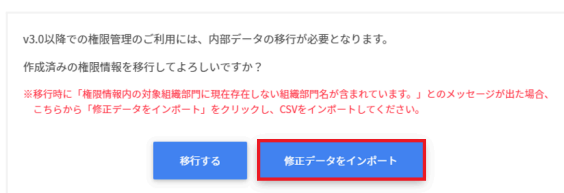


5. InterCLASS® Console Support側に存在している組織名が現在Google Workspace 側に存在しない場合、移行はできません。以下の画面が表示された場合はエクスポートして閉じるボタンをクリックします。「権限管理の移行に成功しました。」が表示された場合は、手順10に進んでください。



6. エクスポートしたCSVファイルをテキストエディタまたは表計算ソフトで編集します。

7. 権限情報のインポートを行います。修正データをインポートボタンをクリックします。



8. 権限情報のインポート画面でインポートファイルのファイルを選択ボタンをクリックし、編集したCSVファイルを選択します。

権限情報のインポート

各ユーザーの権限情報をCSV形式でインポートします。

※一度にインポートできる件数は1000件までとなります。
※実行した操作はジョブに登録されます。実行状況は右上の通知または実行ジョブ一覧画面からご確認ください。

インポートファイル: ファイルを選択 選択されていません

テンプレート キャンセル インポート

9. インポートファイルを選択するとプレビューが表示されます。内容を確認し、インポートボタンをクリックします。

インポートファイル: ファイルを選択 privilege_AllData.csv

表示 10 件

ID	メールアドレス	対象組織部門	削除対象
1		/	
5			
200			
135			
158			
10			削除
11			削除
147			
13			削除
14			

37 件中 1 件から 10 件まで表示 (37 件選択) 前へ 1 2 3 4 次へ

キャンセル インポート

10. 権限情報のインポートが完了すると次の画面が表示されます。システム管理から権限管理をご利用できます。

権限情報の移行に成功しました。権限管理をご利用いただけます。

(警告) データ修正が未完了のデータがあります。
権限管理画面にて、対象組織部門が「削除済み」となっている権限管理情報を修正してください。
※修正されていないユーザーはログインできない可能性があります。

閉じる

④ポイント

- 上記の警告文が表示された場合も、権限管理は利用できます。権限管理画面にて、対象組織部門が「削除済み」となっているユーザーに対し適切な対象組織部門を指定します。

InterCLASS® Filtering Service連携設定

InterCLASS® Filtering Serviceとの連携内容を設定します。

📌ポイント

- 同期が実行された場合、InterCLASS® Filtering Serviceで同期対象となっている組織部門に所属しているユーザーが同期されます。
- 夜間定期同期設定のオン／オフを問わず、操作時の自動同期設定により、InterCLASS® Console Supportでユーザーの追加・編集・削除を行ったタイミングでユーザーの同期を実行することができます。
- 製品間連携機能の利用には、以下のフォームから利用申請をいただく必要があります。
<https://docs.google.com/forms/d/e/1FAIpQLSeHts6rAIKF2Digs-nYnUtX88f3vzIt9vDfBJo84nPuzzYJOW/viewform?>

⚠️注意

- 本設定は、特権管理者アカウントで実施してください。
- 夜間定期同期をオフに設定し、自動同期で行わないを選択した場合、同期は行われません。

1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。



2. 左のメニューから製品間連携をクリックします。



3. InterCLASS Filtering Service連携設定をクリックします。



4. 連携設定を行う InterCLASS Filtering Service 組織の選択ダイアログで対象の組織の設定ボタンをクリックします。

連携設定を行う InterCLASS Filtering Service 組織の選択

表示 10 件

連携先の組織ID	連携先の組織名	連携する組織部門名	
3		/	設定
4		設定なし	設定

2件中1件から2件まで表示

前へ 1 次へ

閉じる

④ポイント

- 連携先が1つしか存在しない場合、このダイアログの表示は省略され、直接手順5のダイアログが開きます。

5. InterCLASS Filtering Service 連携設定ダイアログが表示されます。
連携する組織部門を確認(入力・選択)します。

InterCLASS Filtering Service 連携設定

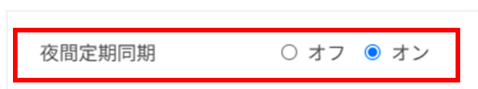
連携先の組織ID	1
連携先の組織名	チエル市教育委員会
	※連携先製品のご契約組織ID・組織名と一致していることをご確認ください。
連携する組織部門	<input type="text" value="/"/>
	※他の連携先に指定されている組織部門と親子関係にある組織部門は選択できません。
夜間定期同期	<input checked="" type="radio"/> オフ <input type="radio"/> オン
操作時の自動同期	<input type="text" value="追加／編集／削除時にユーザーが選択して同期する"/>

キャンセル 保存

④ポイント

- 初期状態では、連携先の組織IDが最も若い連携先の連携する組織部門に、最上位の組織部門(/)が指定されている状態となります。
- 他の連携先の連携する組織部門に指定されている組織部門と親子関係にある組織部門は選択できません。

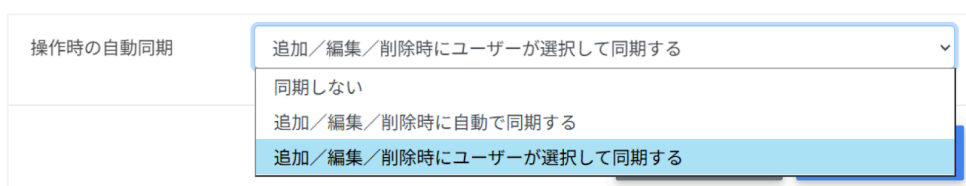
6. 夜間定期同期のオン／オフを設定します。



④ポイント

- 本設定がオンとなっている場合、毎日0:00に同期が実行されます。

7. 操作時の自動同期の動作を設定します。



④ポイント

- 本設定により、夜間定期同期設定のオン／オフを問わず、InterCLASS[®] Console Supportでユーザーの追加や削除を行ったタイミングでユーザーの同期を実行することができます。
- ユーザーの追加・削除時のGoogle Workspaceへの反映時間を考慮し、本設定での同期はユーザーの追加・削除を行った一定時間後に実行されます。
- 重複実行を防ぐため、同期の実行待機中に再度ユーザーの追加・削除が行われた場合は、最後に行われた操作の時間を起点に待機時間が更新されます。
- 自動同期を実行することができるユーザーは、特権管理者または、権限管理画面で権限を付与した対象組織部門に、連携設定の連携する組織部門に指定した組織が含まれているユーザーのみとなります。
- 複数の連携先に異なる自動同期の設定をした場合、追加・編集・削除を行うユーザーが所属している、または新規に所属する組織部門に対応する連携先の設定が優先されます。またユーザーの編集時に組織部門を変更する場合、変更先の組織部門の連携先に追加／編集／削除時にユーザーが選択して同期するが設定されている場合、この設定が優先されます。

8. 保存ボタンをクリックします。



InterCLASS® Advance連携設定

InterCLASS® Advanceとの連携内容を設定します。

⚠注意

- 本設定は、特権管理者アカウントで実施してください。
- 本項目は、InterCLASS® Advance version1.2リリース後に設定可能となります。
- 製品間連携機能の利用には、以下のフォームから利用申請をいただく必要があります。

<https://docs.google.com/forms/d/e/1FAIpQLSeHts6rAIKF2Digs-nYnUtX88f3vzIt9vDfBJo84nPuzzYJOW/viewform?>

1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。



2. 左のメニューから**製品間連携**をクリックします。



3. InterCLASS Advance連携設定をクリックします。



4. 連携設定を行う InterCLASS Advance 組織の選択ダイアログで対象の組織の設定ボタンをクリックします。



④ポイント

- 連携先が1つしか存在しない場合、このダイアログの表示は省略され、直接手順5のダイアログが開きます。

5. InterCLASS Advance 連携設定ダイアログが表示されます。
連携する組織部門を確認(入力・選択)します。

InterCLASS Advance 連携設定

連携先の組織ID 1
連携先の組織名 ██████████

※連携先製品のご契約組織ID・組織名と一致していることをご確認ください。

連携する組織部門

手動同期

キャンセル

④ポイント

- 連携する組織部門名にはこの先の連携設定ダイアログで設定された内容が表示されますが、初期状態では、最も**連携先の組織ID**が若い組織に自動的に「/」組織部門が**連携する組織部門**として設定されます。
- 他の連携先の**連携する組織部門**に指定されている組織部門と親子関係にある組織部門は選択できません。

6. 手動同期機能の利用を設定し、保存ボタンをクリックします。

InterCLASS Advance 連携設定

連携先の組織ID 1

連携先の組織名 XXXXXXXXXX

※連携先製品のご契約組織ID・組織名と一致していることをご確認ください。

連携する組織部門

手動同期

⑨ポイント

- 手動同期を実行することができるユーザーは、特権管理者または、権限管理画面で権限を付与した対象組織部門に、連携設定の連携する組織部門に指定した組織が含まれているユーザーのみとなります。

製品間連携 実行結果

各製品間連携の実行状況を確認できます。

⚠️注意

- 本画面は特権管理者、または権限管理画面で権限を付与した対象組織部門に、連携設定の連携する組織部門に指定した組織部門が含まれているユーザーのみ確認可能です。

1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。本画面を確認可能なアカウントでログインします。



2. 左のメニューから**製品間連携**をクリックします。



3. 製品間連携画面から製品間連携 実行結果をクリックします。



4. 製品間連携の実行結果が一覧で表示されます。

製品間連携 実行結果

検索: 全て | 絞り込み | 部分一致 | 詳細 | リセット

実行日時	終了日時	ステータス	連携製品	連携件数	連携先名	内容	エラー
2025/12/01 00:00:11	2025/12/01 00:00:34	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/30 00:00:11	2025/11/30 00:01:28	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/29 00:00:16	2025/11/29 00:01:26	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/28 00:00:20	2025/11/28 00:01:41	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/27 00:00:12	2025/11/27 00:00:33	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/26 00:00:16	2025/11/26 00:01:32	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/25 00:00:16	2025/11/25 00:01:29	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/24 00:00:12	2025/11/24 00:00:31	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/23 00:00:16	2025/11/23 00:01:27	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	
2025/11/22 00:00:12	2025/11/22 00:01:21	正常終了	InterCLASS Filtering Service	3	Chfiroa QA	連携正常完了	

1,841件中1件から10件まで表示

1 2 3 4 5 ... 185 次へ

CHieruサポートについて

下記サポートセンターまでお問い合わせください。

URL <https://support.chieru.net/>

E-Mail support@chieru.co.jp

TEL 03-5781-8110

FAX 03-6712-9461

【受付時間】

午前10時～正午、午後1時～午後5時

土曜日、日曜日、祝祭日および弊社指定休日は休業させていただきます。

InterCLASS[®] Console Support version4.1 操作マニュアル 設定編

2026年 2月

作成/発行/企画 チエル株式会社

〒140-0002 東京都品川区東品川2-2-24 天王洲セントラルタワー22F

※ 記載されている会社名及び商品名は、各社の商標もしくは登録商標です。

-
- 本書に掲載しているGoogle Workspace for Education 及び弊社製品の画面は、2026年2月時点の画面です。ご利用をいただくタイミングによって、実際の画面とマニュアルの画面が異なる場合があります。
 - 本書の内容は将来予告なしに変更することがあります。
 - 本書の内容の一部、または全部を無断で転載、あるいは複製することを禁じます。
 - プリンターやアプリケーションによって一部違ったフォントで印刷、表示されることがあります。
 - 本書の内容については万全を期して制作致しましたが、万一記載に誤りや不完全な点がありましたらご容赦ください。

Chieruチエル 株式会社

- 本社 〒140-0002 東京都品川区東品川2-2-24 天王洲セントラルタワー22F
TEL: (03)6712-9721 FAX: (03)6712-9461
- 札幌営業所 〒060-0062 北海道札幌市中央区南2条西9丁目1-2 サンケン札幌ビル6F
TEL: (011)804-7170 FAX: (011)804-7171
- 仙台営業所 〒980-0804 宮城県仙台市青葉区大町1-4-1 藤崎芭蕉の辻ビルディング3F
TEL: (022)217-2888 FAX: (022)206-5222
- 首都圏営業所 〒140-0002 東京都品川区東品川2-2-24 天王洲セントラルタワー22F
TEL: (03)6712-9471 FAX: (03)6712-9461
- 名古屋営業所 〒460-0003 愛知県名古屋市中区錦1-18-11 CK21広小路伏見ビル3F
TEL: (052)857-0082 FAX: (052)857-0083
- 大阪営業所 〒550-0001 大阪府大阪市西区土佐堀1-5-11 KDX土佐堀ビル3F
TEL: (06)6441-3677 FAX: (06)6441-3655
- 広島営業所 〒730-0011 広島県広島市中区基町11-10 合人社広島紙屋町ビル 8F-41
TEL: (082)236-6077 FAX: (082)236-6078
- 福岡営業所 〒812-0013 福岡県福岡市博多区博多駅東2-4-17 第6岡部ビル5F
TEL: (092)483-1603 FAX: (092)483-1604
- 沖縄営業所 〒901-2127 沖縄県浦添市屋富祖一丁目6番3号 森ビル
TEL: (098)943-0511 FAX: (098)943-0669

<https://www.chieru.co.jp>