

# InterCLASS Console Support

**InterCLASS Console Support v2.2操作マニュアル（設定編）**

# はじめに

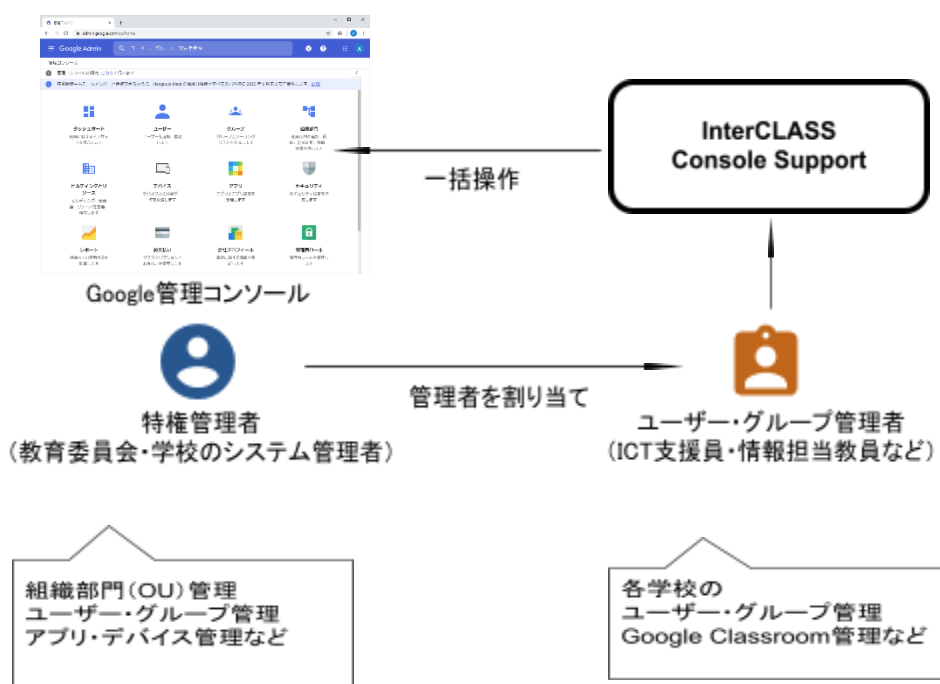
---

InterCLASS Console Supportを導入いただき、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G Suite 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は、Google管理コンソールのユーザー管理機能を拡張するG Suite Marketplaceアプリです。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。



## 本書の構成と読みかた

---

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のインストールと設定について記載しています。また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説明します。

# 目次

---

|   |           |
|---|-----------|
| <b>動作環境</b>                             | <b>3</b>  |
| <b>Google Cloud Platformの設定</b>         | <b>4</b>  |
| Google Cloud Platformの設定                | 4         |
| <b>ドメイン全体の管理を委任の設定</b>                  | <b>13</b> |
| Google Classroomのデータアクセスの許可             | 17        |
| <b>QRコードログインの設定</b>                     | <b>19</b> |
| 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        | 19        |
| 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     | 25        |
| Chromeデバイスの設定の変更                        | 28        |
| Chromebookのログイン画面を確認                    | 31        |
| <b>InterCLASS Console Supportの起動と終了</b> | <b>32</b> |
| InterCLASS Console Supportへログインする       | 32        |
| InterCLASS Console Supportからログアウトする     | 35        |
| <b>システム管理の設定</b>                        | <b>36</b> |
| システム管理を開く                               | 36        |
| サービスアカウント登録                             | 37        |
| サービスアカウント利用設定                           | 38        |
| サービスアカウントを利用しない場合                       | 38        |
| サービスアカウントを利用する場合                        | 38        |
| 権限付与方法の違い                               | 39        |
| 権限管理                                    | 40        |
| <b>CHIeruサポートについて</b>                   | <b>41</b> |

---

# 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 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 10 Pro, Education, Enterprise / 8.1 Pro (32bit版および64bit版)  
Mac OS 10.14 (sierra) 以上  
最新のChrome OS
- アプリ** : Google Chrome v88以上
- 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。

# 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 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. ページ最上部トップバーのGoogle Cloud Platform表記の右側にある、「プロジェクトの選択」ボタンをクリックしてください。




4. ポップアップの右上の「新しいプロジェクト」ボタンからプロジェクトを作成してください。




5. 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てください。




### 新しいプロジェクト

 割り当て内の残りのプロジェクト数は 12 projects 件です。プロジェクトの増加をリクエストするか、プロジェクトを削除してください。[詳細](#)



[MANAGE QUOTAS](#)

プロジェクト名 \*  
ExampleProject 

プロジェクト ID: **exampleproject-302808**。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」をクリックしてプロジェクトのダッシュボードに移動してください。

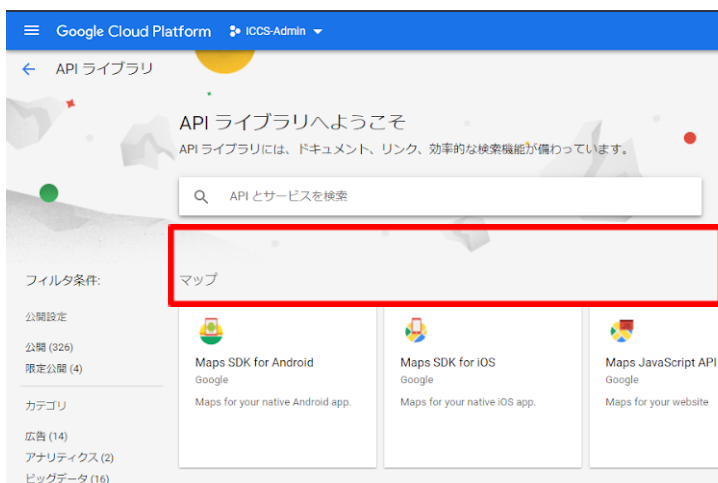
### 通知

 プロジェクト「ExampleProject」を作成 たった今  
[プロジェクトを選択](#)

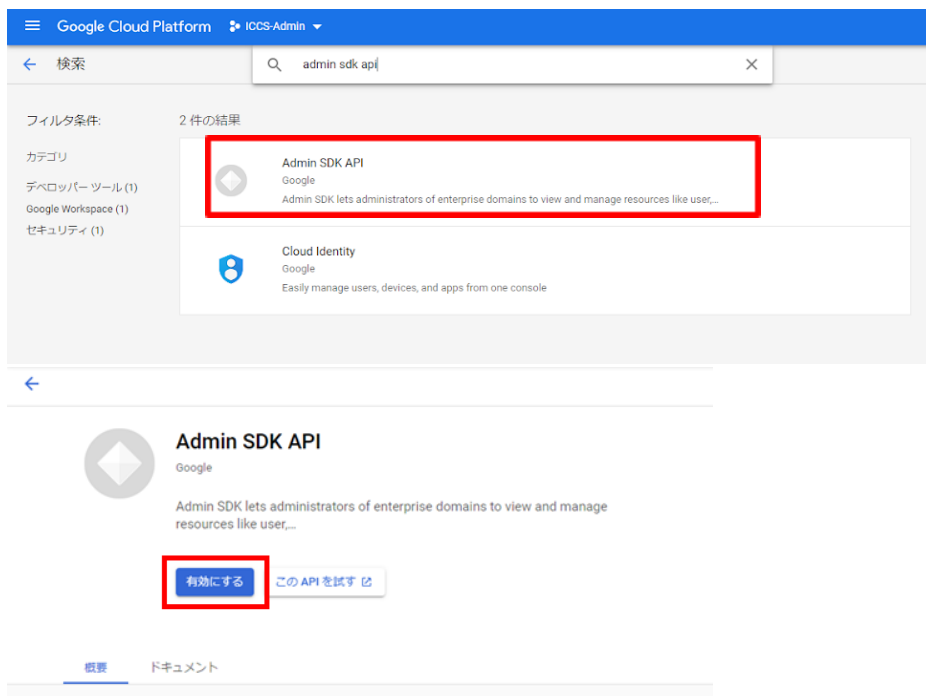
7. メニューの「APIとサービス」から「ライブラリ」を表示します。



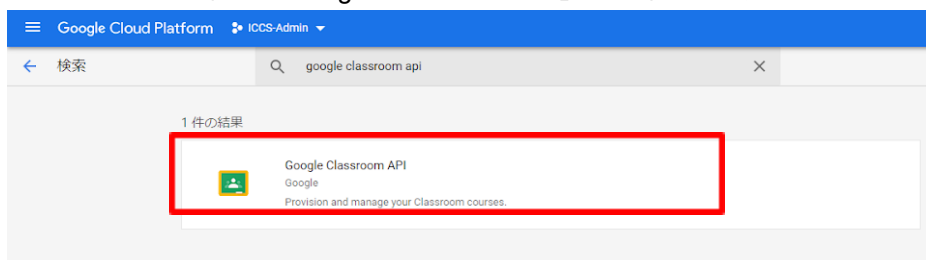
8. 「APIとサービスの検索」ボックスに「Admin SDK API」と入力してください。



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」をクリックします。

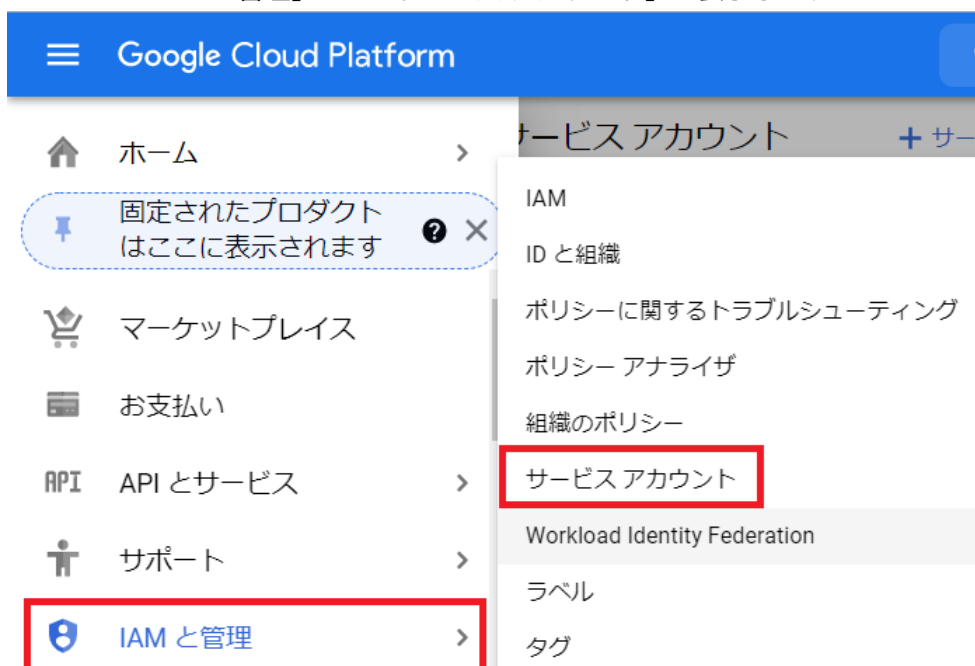


10. 手順7.8.と同じ操作で「Google Classroom API」を検索し、有効化してください。





11. メニューの「IAMと管理」から「サービス アカウント」を表示します。



12. 左上の「+サービス アカウントを作成」をクリックします。



13. 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」をクリックします。

#### サービス アカウントの作成

##### 1 サービス アカウントの詳細

サービス アカウント名

ICCS

このサービス アカウントの表示名

サービス アカウント ID

iccs-181

@iccs-admin.iam.gserviceaccount.com



サービス アカウントの説明

ICCS用サービスアカウント

このサービス アカウントで行うことを説明します

作成

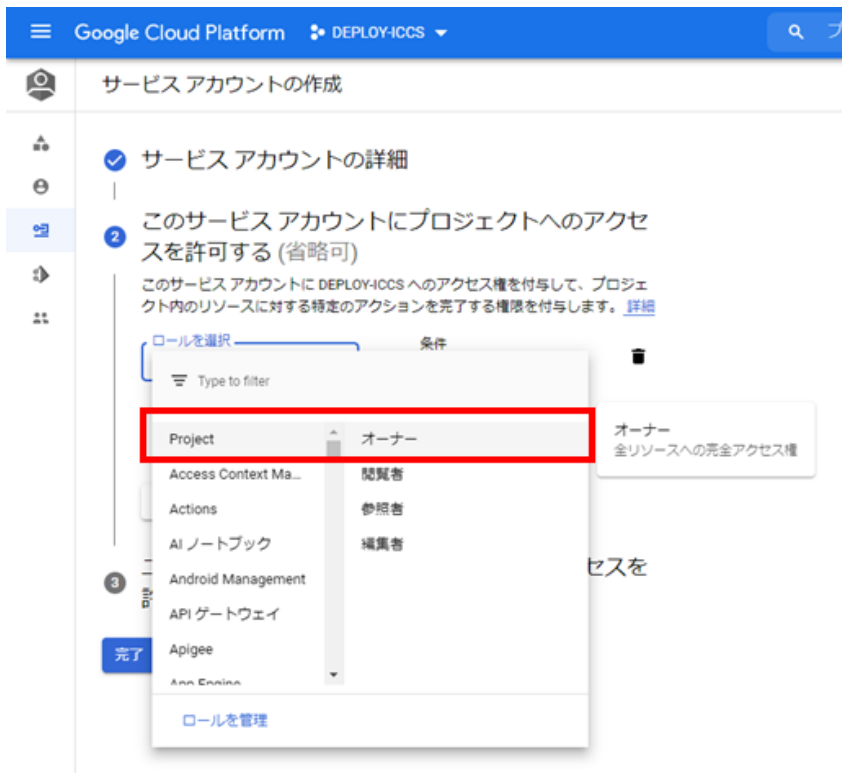
##### 2 このサービス アカウントにプロジェクトへのアクセスを許可する (省略可)

##### 3 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)

完了

キャンセル

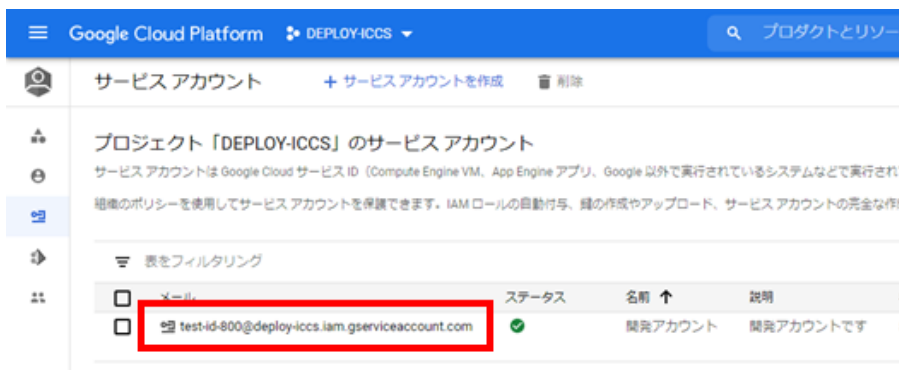
14. 項目 2 で、「Project」→「オーナー」のロールを設定して、一番下の「完了」をクリックしてください。※項目 3 の設定は不要です。



- 3 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)

**完了** キャンセル

15. 一覧画面から、先程作成したサービス アカウントの「メール」部分をクリックし、設定画面へ移動します。



16. 「ドメイン全体の委任の表示」をクリックし、「G Suite ドメイン全体の委任を有効にする」にチェックを入れ「保存」します。保存後に表示されるクライアントIDはこの後の操作で使用するので、控えておいてください。

[← ICCS](#)

[詳細](#) [権限](#) [キー](#) [指標](#) [ログ](#)

### サービス アカウントの詳細

名前  
ICCS

保存

説明  
ICCS用サービスアカウント

保存

メール  
iccs-181@iccs-admin.iam.gserviceaccount.com

一意の ID  
118189969078630904591

### 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 アカウントを無効にする

▼ ドメイン全体の委任の表示

### 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 アカウントを無効にする

☒ G Suite ドメイン全体の委任を有効にする

手動での認証なしで、このサービス アカウントが G Suite ドメインのすべてのユーザーデータにアクセスすることを許可します。 [詳細](#)

保存

ドメイン全体の委任の非表示

17. 続いて「キー」タブの「鍵を追加」から「新しい鍵を作成」をクリックします。



18. 「キーのタイプ」は「JSON」を選択し、「作成」をクリックしてください。

#### 「ICCS」の秘密鍵の作成

秘密鍵を含むファイルをダウンロードします。この鍵を紛失すると復元できなくなるため、ファイルは大切に保管してください。

キーのタイプ

☒ JSON

推奨

☐ P12

P12 形式を使用したコードとの下位互換性を目的としています

キャンセル

作成

19. JSON形式の秘密鍵がダウンロードされます。このICCSの秘密鍵を後ほど初回ログイン時に登録していただくため、確実に保存しておいてください。

#### ⚠ 注意

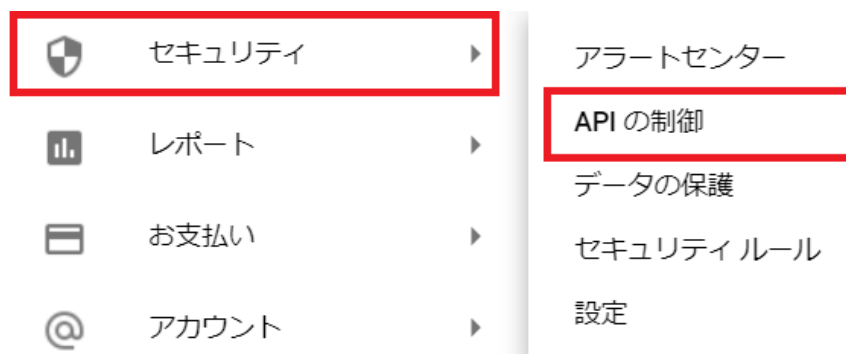
※同じ鍵は2回ダウンロードできません。紛失した場合は再作成する必要があります。

# ドメイン全体の管理を委任の設定

1. Chromeウェブブラウザで、Google Admin (<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。左上のメニューをクリックし、をクリックします。
3. 左上のメインメニューをクリックします。



4. セキュリティのAPI制御をクリックします。



5. APIの制御内のドメイン全体の委任にあるドメイン全体の委任を管理をクリックします。



6. セキュリティ>APIの制御>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. 「新しく追加」をクリックして、「新しいクライアントIDを追加」ポップアップを表示します。



8. 新しいクライアントIDを追加画面が表示されます。

## 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

9. 「クライアントID」には「Google Cloud Platformの設定」の13.で表示したクライアントIDを入力し、「OAuthスコープ」には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

必要なクライアント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

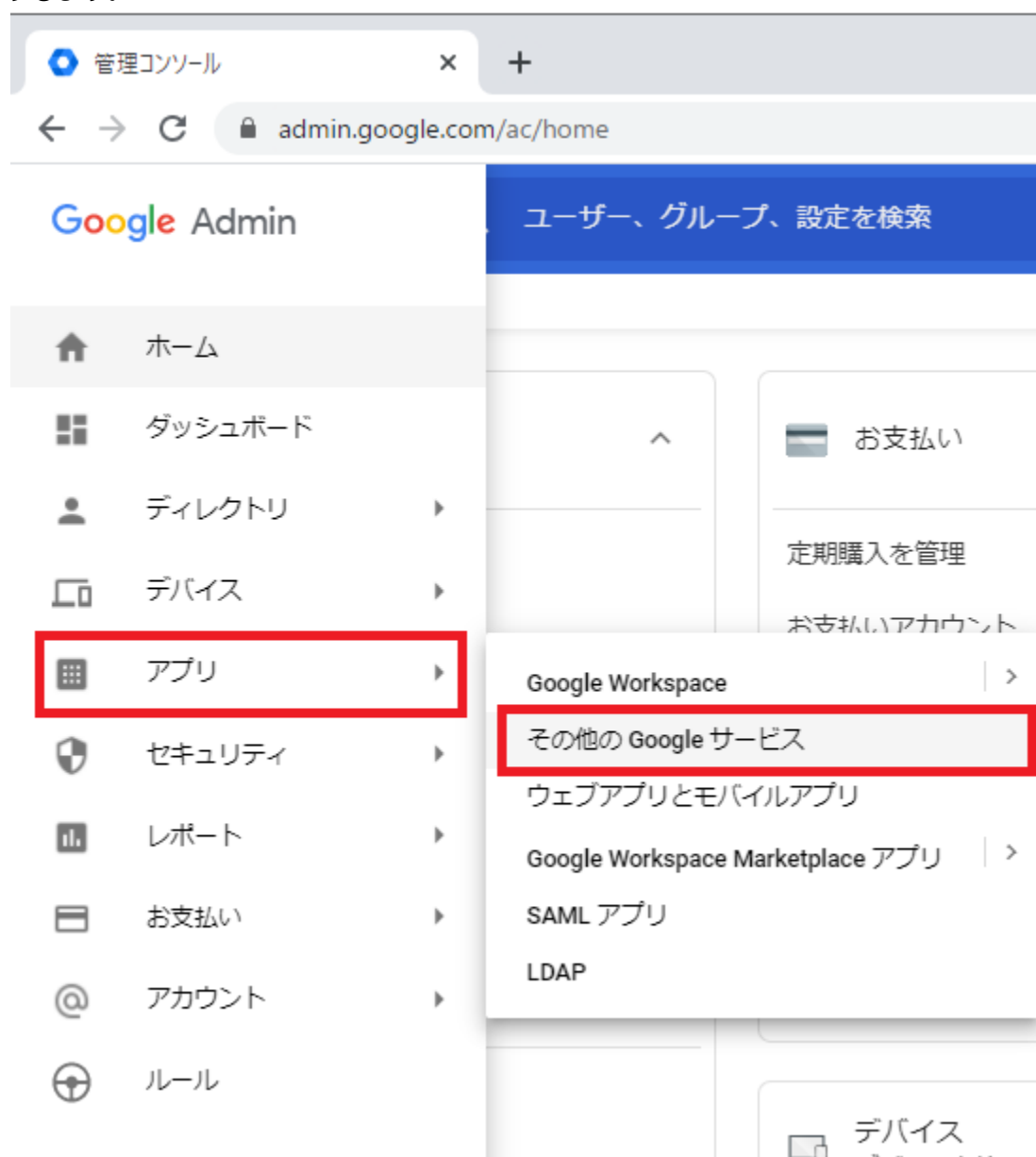
☐ 既存のクライアント ID を上書きする ?

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. 左上のメニューをクリックし、「アプリ」→「その他の Google サービス」をクリックします。



## 2. その他のGoogleサービスの画面で、Classroomをクリックします。



## 3. データアクセスをクリックします。



## 4. 「ユーザーは、アプリからGoogle Classroom のデータへのアクセスを承認することができます。」にチェックを入れ、保存します。



# 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。

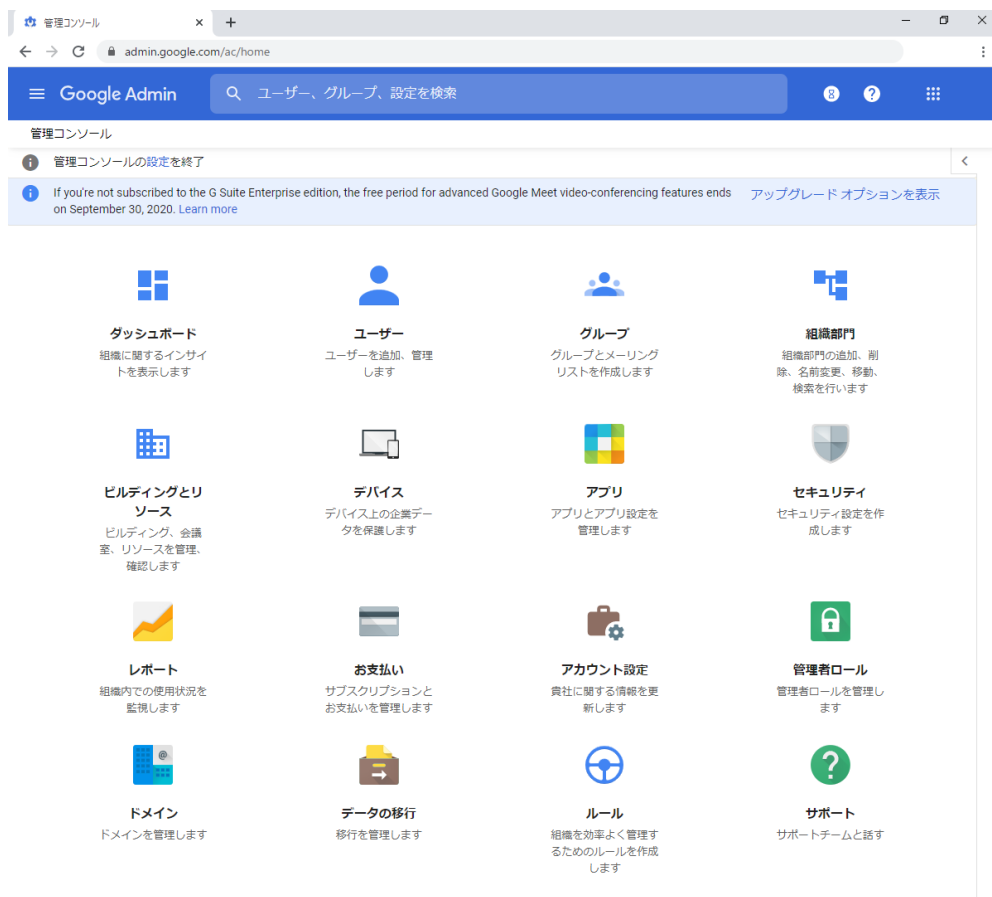
## サードパーティのIDプロバイダを使用したシングルサインオンの設定

QRコードを使用したChromebookへのログインに必要な設定です。

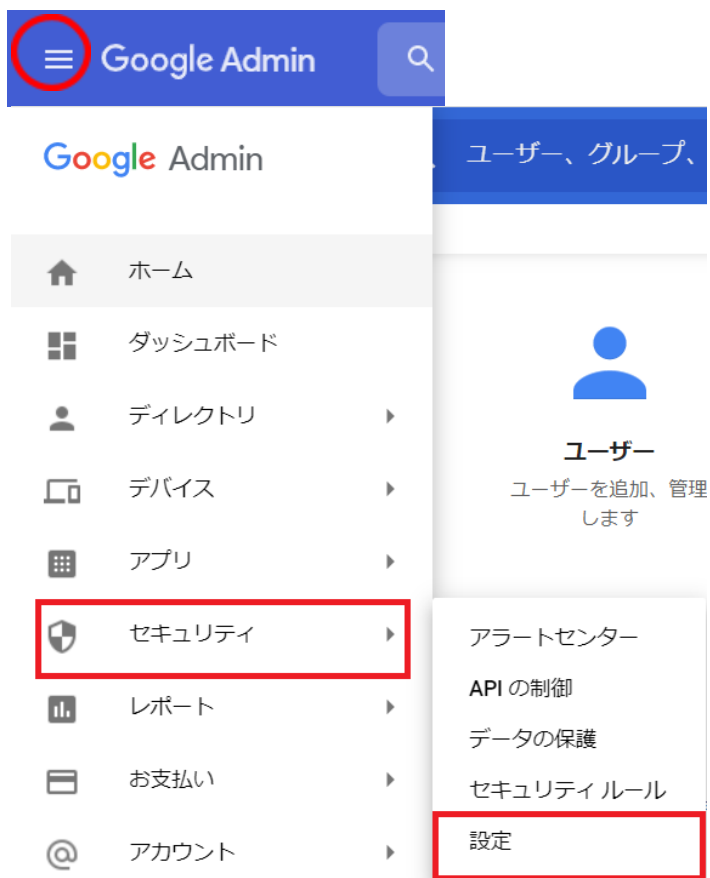
### ④ポイント

設定は特権管理者が行います。

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. 左上のメニューをクリックし、セキュリティ>設定をクリックします。



4. 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）の設定をクリックします。

SAML アプリケーションに対するシングル サインオン（SSO）の設定

ウェブベースのアプリケーション（Gmail やカレンダーなど）のユーザー認証を設定します。

**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（SSO）の設定**

サードパーティの ID プロバイダを使用して、管理対象の Google アカウントに対してシングルサインオンを設定します。

Android 向けの EMM プロバイダの管理

企業向けモバイル管理プロバイダを利用して、会社のデバイスを安全に保護しましょう。

5. サードパーティのIDプロバイダでSSOを設定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の設定項目に以下の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>

- ☒ サードパーティの ID プロバイダで SSO を設定する

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>

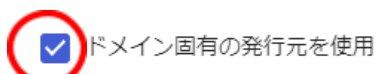
システムと G Suite へのログイン用 URL

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

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



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適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 機能が適用されます。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](#)

7. 右下の**保存**をクリックします。



8. 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InterCLASS Console Supportホーム>ログイン管理>QRコードログインにアクセスし、**証明書をダウンロードする**をクリックします。P30.「[InterCLASS Console Supportへログインする](#)」参照



9. 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）の設定のページで、確認用の証明書欄の「証明書をアップロード」をクリックします。

Google Admin

ユーザー、グループ、設定を検索

8 ?

セキュリティ > シングルサインオン

セキュリティ

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

サードパーティの ID プロバ  
イダ

☒ サードパーティの ID プロバイダで SSO を設定する

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/ldap/SSORedirect/>  
システムと G Suite へのログイン用 URL

ログアウト ページの URL  
<https://sso.interclasscloud.com:443/ldap/SSORedirect/>  
ユーザーがログアウトするときにリダイレクトする URL

確認用の証明書  
証明書ファイルはアップロードされていません。  
[証明書をアップロード](#)  
**必須項目はすべて入力してください**  
証明書ファイルには、Google がログイン リクエストを確認するための  
公開鍵が含まれている必要があります。 [詳細](#)

☒ 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 サインオンが適用されるアドレ  
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 機能が適用されます。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](#)

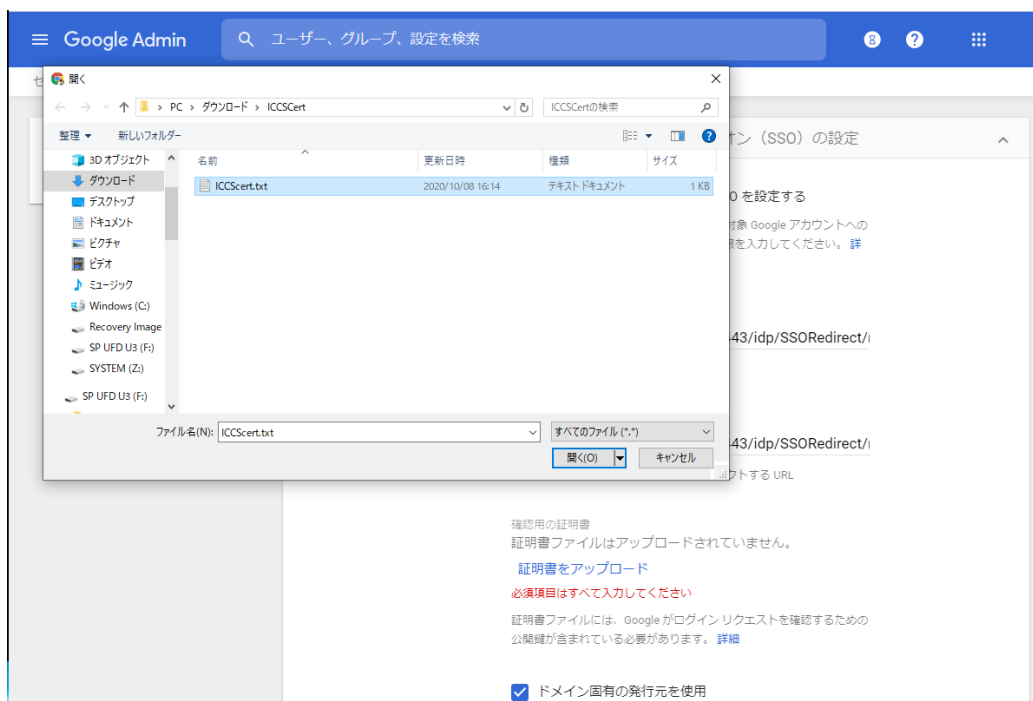
パスワード変更用 URL  
ユーザーがシステムでパスワードを変更する際にアクセスする URL です。  
定義すると、シングルサインオンが有効になっていない場合でもこの URL  
が表示されます

キャンセル

保存



10. QRコードログインからダウンロードした**ICCSert.zip**ファイルを事前に展開しておき、**ICCSert.txt**を選択し開きます。



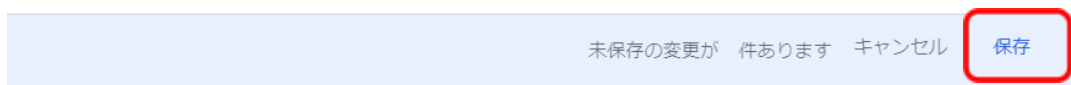
11. 証明書がアップロードされると下記の表示になります。

確認用の証明書

証明書ファイルをアップロードしました。 [証明書を更新](#)

証明書ファイルには、Google がログイン リクエストを確認するための公開鍵が含まれている必要があります。 [詳細](#)

12. ページの最下部へ移動し、変更を保存します。



## 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てください。

### ④ポイント

- 設定は特権管理者が行います。
- 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。

### ⑤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G Suite管理者ヘルプを参照してください：

Google管理者ヘルプ: ユーザー別のポリシーの適用

<https://support.google.com/a/topic/1227584?hl=ja>

(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

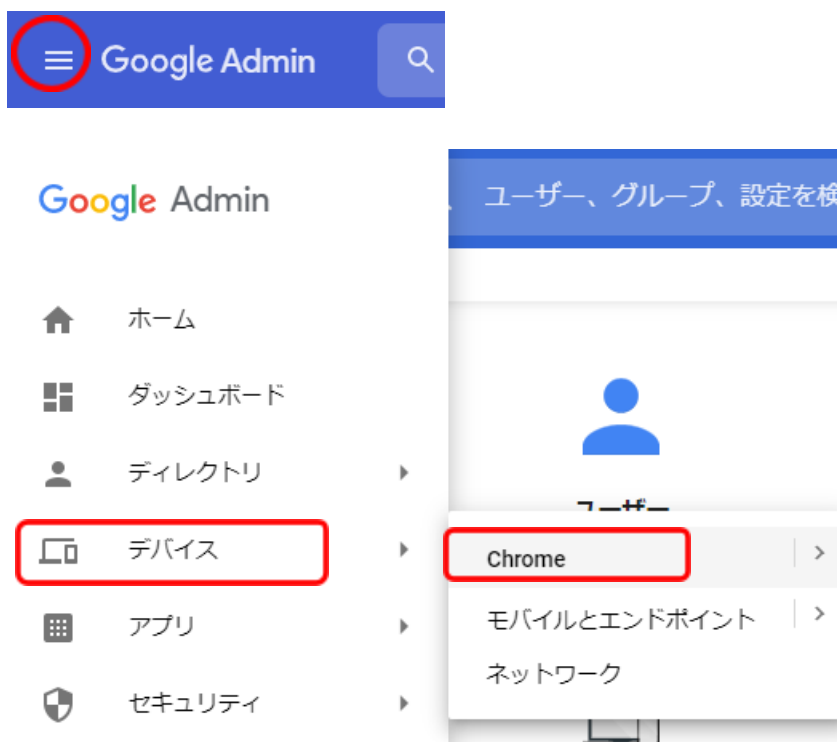
##### ▼ 児童生徒ユーザー

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. 左上のメニューをクリックし、**デバイス> Chrome**をクリックします。



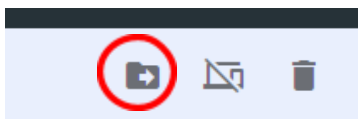
4. Chrome管理で、**デバイス**をクリックします。



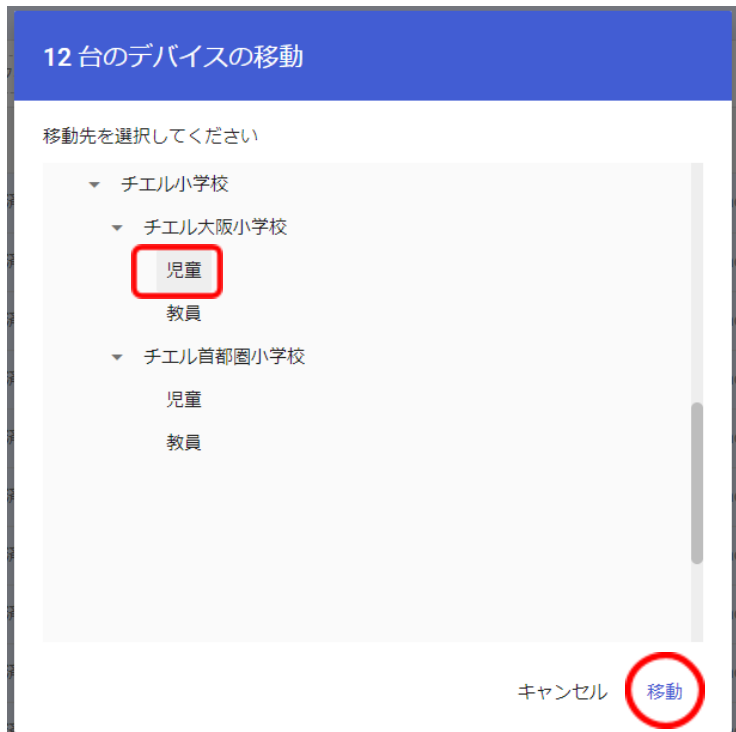
5. Chromeデバイスの一覧画面で、QRコードログインを有効にする**Chromeデバイスにチェック**を入れて選択します。



6. 右上の操作アイコンから**選択したデバイスを移動する**アイコンをクリックします。



7. デバイスの移動画面で、移動先の組織部門を選択して**移動**をクリックします。



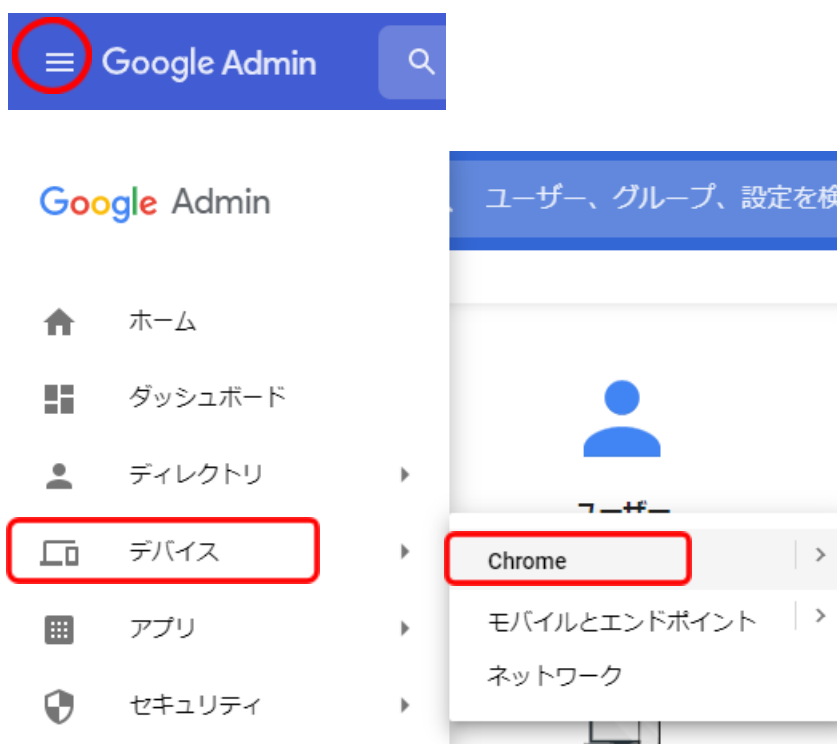
8. 選択したデバイスが、移動先の組織部門に移動します。

## Chromeデバイスの設定の変更

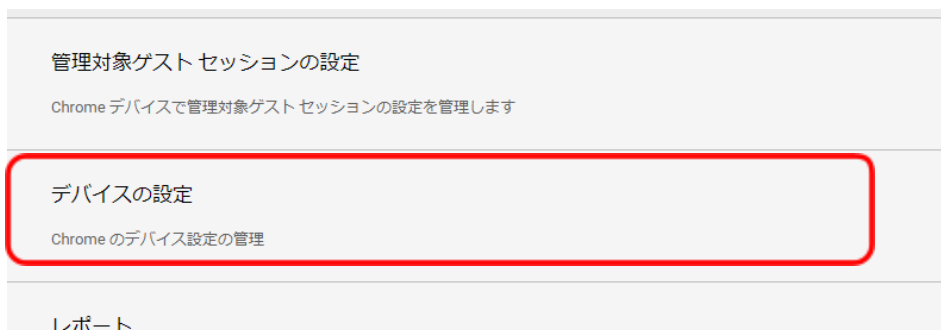
QRコードログイン機能を利用するChromeデバイスが含まれる組織部門のデバイスの設定を変更します。

### ④ポイント

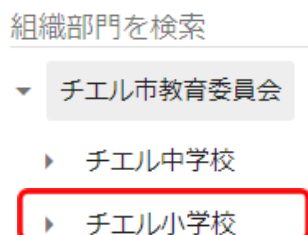
- 設定は特権管理者が行います。
1. Chromeウェブブラウザで**Google管理コンソール** (<https://admin.google.com/>) にアクセスします。
  2. **特権管理者のアカウント**でサインインします。
  3. 左上のメニューをクリックし、**デバイス> Chrome**をクリックします。



4. Chrome管理画面で、**デバイスの設定**をクリックします。



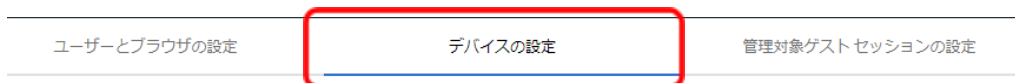
5. 左の組織部門のツリーから、QRコードログインを有効にするChromeデバイスが含まれる組織部門を選択します。



## ④ポイント

- QRコードログイン機能を、特定Chromebookのみに有効する場合は、対象のChromeデバイスを特定の組織部門に移動してください。詳細は、[P23 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する](#)を参照してください。

6. **デバイスの設定**タブが選択されていることを確認します。



7. 画面を下にスクロールし、**ログイン設定**の項目に移動します。



8. 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。

ゲストモード  
ローカルに適用 ▼

ゲストモードを無効にする ▼

9. ドメインのオートコンプリートの設定を、**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オートコンプリート**に、お客様のドメイン名を入力します。

ドメインのオートコンプリート  
ローカルに適用 ▼

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 ▼

ドメインのプレフィックスのオートコンプリート

ユーザー名@ chieru.com (お客様のドメイン)

10. 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。

ログイン画面  
ローカルに適用 ▼

ログイン画面にユーザー名と写真を表示

ユーザー名と写真を表示しない ▼

11. 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。

シングル サインオン ID プロバイダ (IdP) のリダイレクト  
ローカルに適用 ▼

SAML SSO ID プロバイダ (IdP) へのユーザーのリダイレクト

SAML SSO IdP ページへの移動をユーザーに許可する ▼

12. 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。

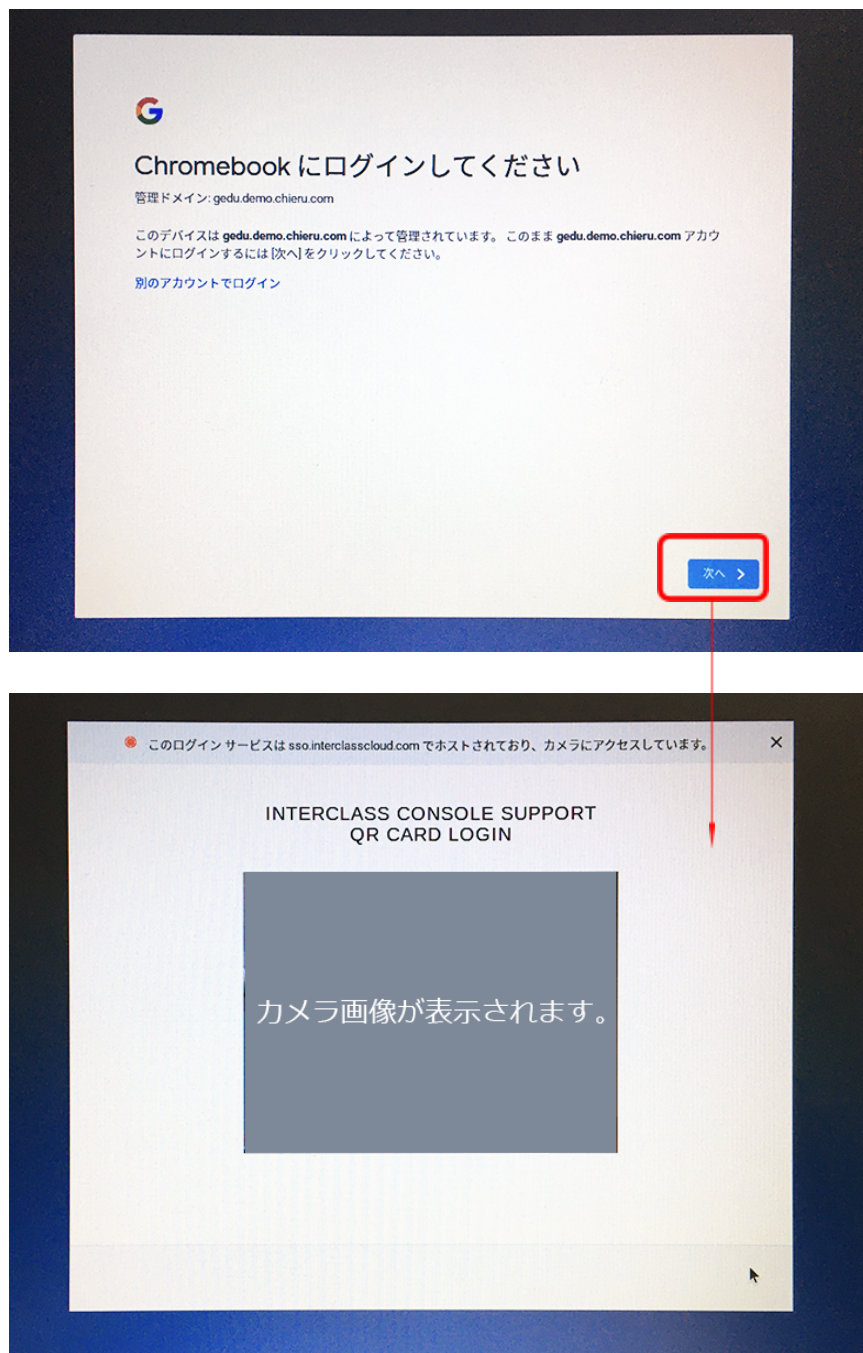
シングル サインオンによるカメラへのアクセスの許可  
ローカルに適用 ▼

シングル サインオンによるカメラへのアクセスを許可するアプリのホワイトリスト  
<https://sso.interclasscloud.com/>

警告: このポリシーを有効にすると、ユーザーのカメラへのアクセスを、ユーザーに代わってサードパーティに許可することになります。シングル サインオンとカメラへのアクセスの許可について詳しくは、ヘルプセンター記事をご覧ください。

## 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。



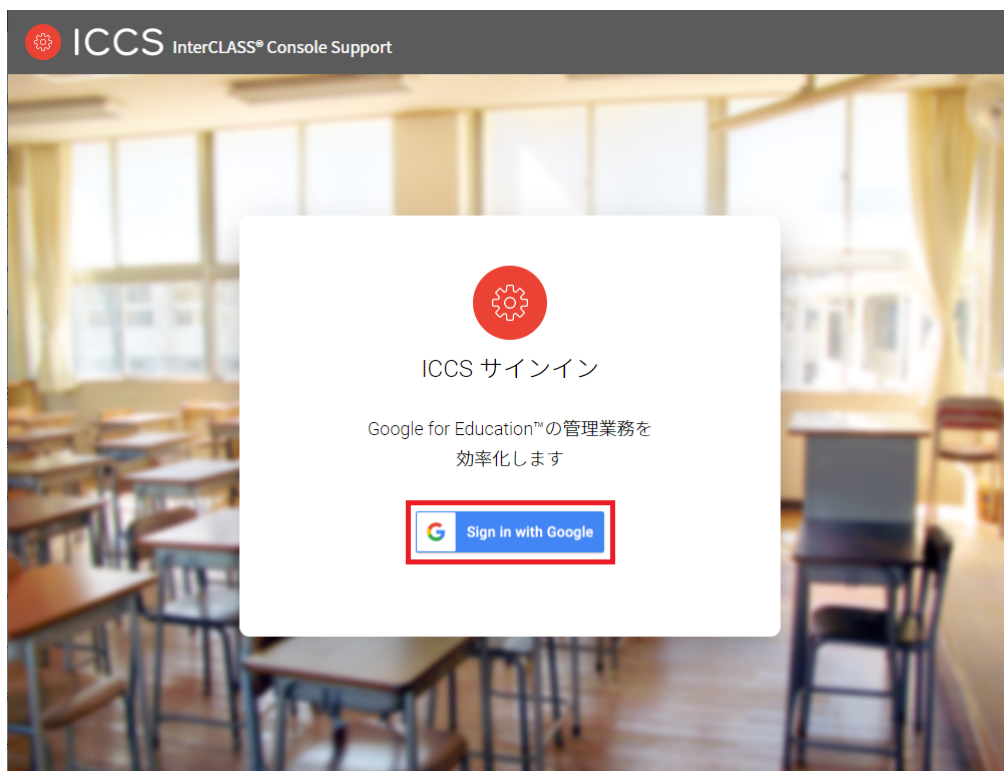


# InterCLASS Console Supportの起動と終了

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へログインする

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. ICCSにログインします。**Sign in with Google**をクリックします。



3. Googleの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**をクリックします。

4. パスワードを入力して次へをクリックします。



ログイン - Google アカウント - Google Chrome

accounts.google.com/signin/v2/challenge/pwd?redirect\_uri=storagerelay%3A%2F%2Fh...

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

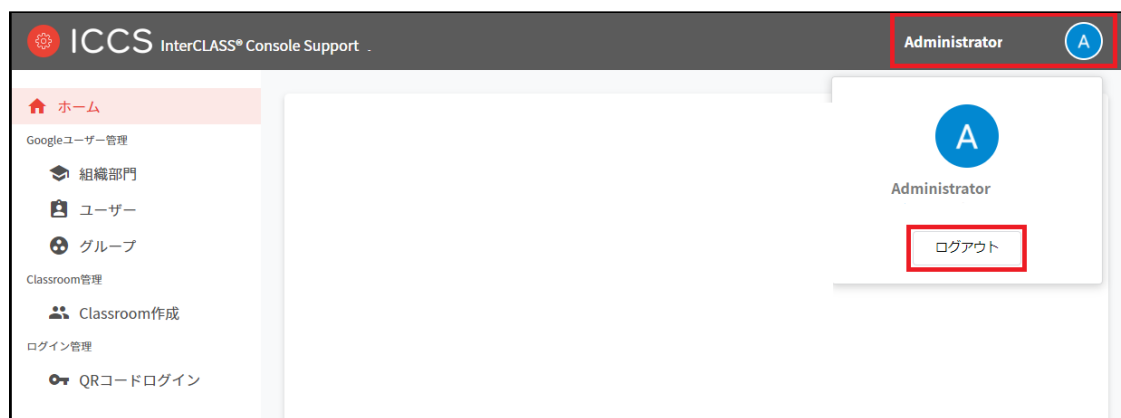
日本語 ヘルプ プライバシー 規約

5. ICCSのトップページが表示されます。



## InterCLASS Console Supportからログアウトする

ICCSからログアウトする際は右上の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。

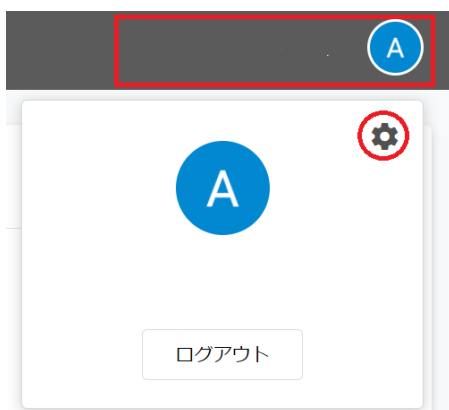


# システム管理の設定

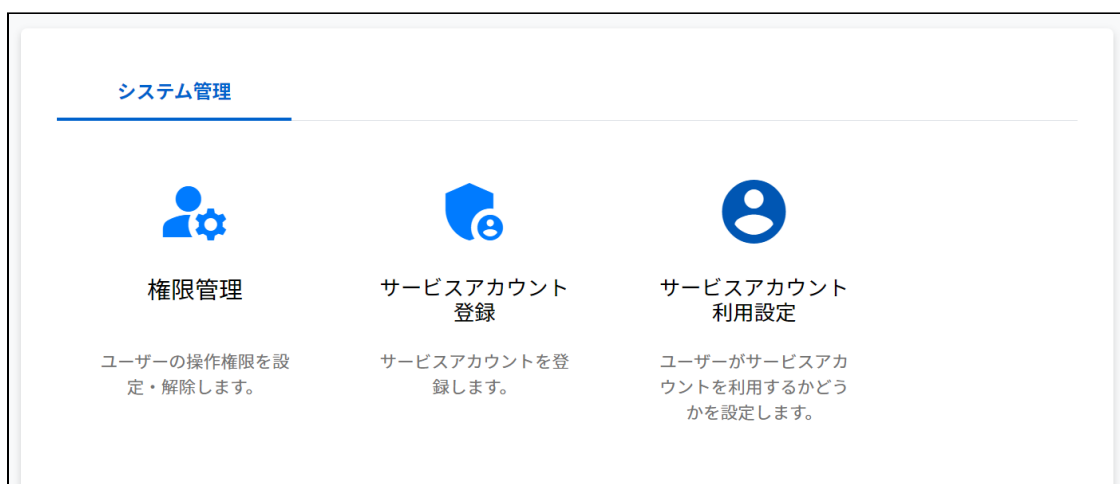
InterCLASS Console Supportのシステム管理は特権管理者としてログインし、システム管理のため初期設定を行います。システム管理では、権限管理、サービスアカウント登録、サービスアカウント利用設定が行えます。

## システム管理を開く

1. InterCLASS Console Supportの右上にあるアイコンをクリックし、歯車マークをクリックします。



2. システム管理が開きます。



## 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. サービスアカウント登録をクリックします。



### サービスアカウント 登録

サービスアカウントを登  
録します。

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: ファイルを選択 選択されていません

キャンセルアップロード

3. インポートファイルからファイルを選択をクリックします。

インポートファイル:

ファイルを選択

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:

ファイルを選択

\_key.json

5. アップロードボタンをクリックします。

アップロード

6. サービスアカウント登録をもう一度開きます。

7. 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: 

ファイルを選択

 選択されていません

キャンセル

アップロード

## サービスアカウント利用設定

InterCLASS Console Supportを操作するサービスアカウントの利用設定を行います。お客様の環境や運用体制によりサービスアカウントの利用有無をご検討ください。

### サービスアカウントを利用しない場合

Google Workspaceの管理ロールを持つユーザーでInterCLASS Console Supportを利用します。Google Workspaceの管理コンソールで設定している特権管理者やカスタムロールが該当します。

### サービスアカウントを利用する場合

InterCLASS Console Support上（内）で有効なサービスアカウントを設定し、権限管理画面でドメイン管理者に操作権限を与えられたユーザーがInterCLASS Console Supportを利用します。

## 権限付与方法の違い

|       | サービスアカウントを利用しない             | サービスアカウントを利用する  |
|-------|-----------------------------|---|
| 設定画面  | Google Workspace<br>管理コンソール | InterCLASS Console Support  |
| 権限の種類 | 特権管理者<br>カスタムロール            | 組織部門権限<br>ユーザー権限<br>グループ権限<br>自Classroom権限<br>全Classroom権限<br>QRコード権限 |

1. サービスアカウント利用設定をクリックします



### サービスアカウント 利用設定

ユーザーがサービスアカウントを利用するかどうかを設定します。

2. サービスアカウント利用設定画面が開きます。

サービスアカウント利用設定

登録したサービスアカウントを利用するか設定します。

サービスアカウントを利用しない場合、権限管理画面でユーザーへ与えた権限は無効となり、特権管理者またはそれと同等の権限を持つユーザーのみが利用可能となります。

現在の状態：サービスアカウントを利用しない

キャンセル

サービスアカウントを利用する



3. 現在の状態を確認します。

現在の状態：サービスアカウントを利用しない

4. サービスアカウントを利用するをクリックします。

サービスアカウントを利用する

5. 現在の状態がサービスアカウントを利用するになっているか確認します。

#### サービスアカウント利用設定

登録したサービスアカウントを利用するか設定します。

サービスアカウントを利用しない場合、権限管理画面でユーザーへ与えた権限は無効となり、特権管理者またはそれと同等の権限を持つユーザーのみが利用可能となります。

現在の状態：サービスアカウントを利用する

キャンセル

サービスアカウントを利用しない

現在の状態：サービスアカウントを利用する

## 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

ユーザーの操作権限を設定・解除します。

# 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 v2.2操作マニュアル（設定編）

---

2021年5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3F

※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。

\*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 千140-0002東京都品川区東品川2-2-24天王洲セントラルタワー3F  
TEL: (03) 6712-9721 FAX: (03) 6712-9461
- 札幌営業所 千060-0062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 千980-0013宮城県仙台市青葉区大町1-4-1 明治安田生命仙台ビル 3F  
TEL: (022) 217-2888 FAX: (022) 206-5222
- 首都圏営業所 千140-0002東京都品川区東品川2-2-24天王洲セントラルタワー3F  
TEL: (03) 6712-9471 FAX: (03) 6712-9461
- 名古屋営業所 千460-0003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 千532-0011大阪府大阪市淀川区西中島7-1-29 新大阪SONEビル5F  
TEL: (06) 6838-3077 FAX: (06) 4806-7056
- 広島営業所 千732-0828広島県広島市南区京橋町1-7アスティ広島京橋ビルディング2F  
TEL: (082) 236-6077 FAX: (082) 236-6078
- 福岡営業所 千812-0013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 千901-2127沖縄県浦添市屋富祖1-6-3 森ビル  
TEL: (098) 943-0511 FAX: (098) 943-0669

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