

InterCLASS Console Support

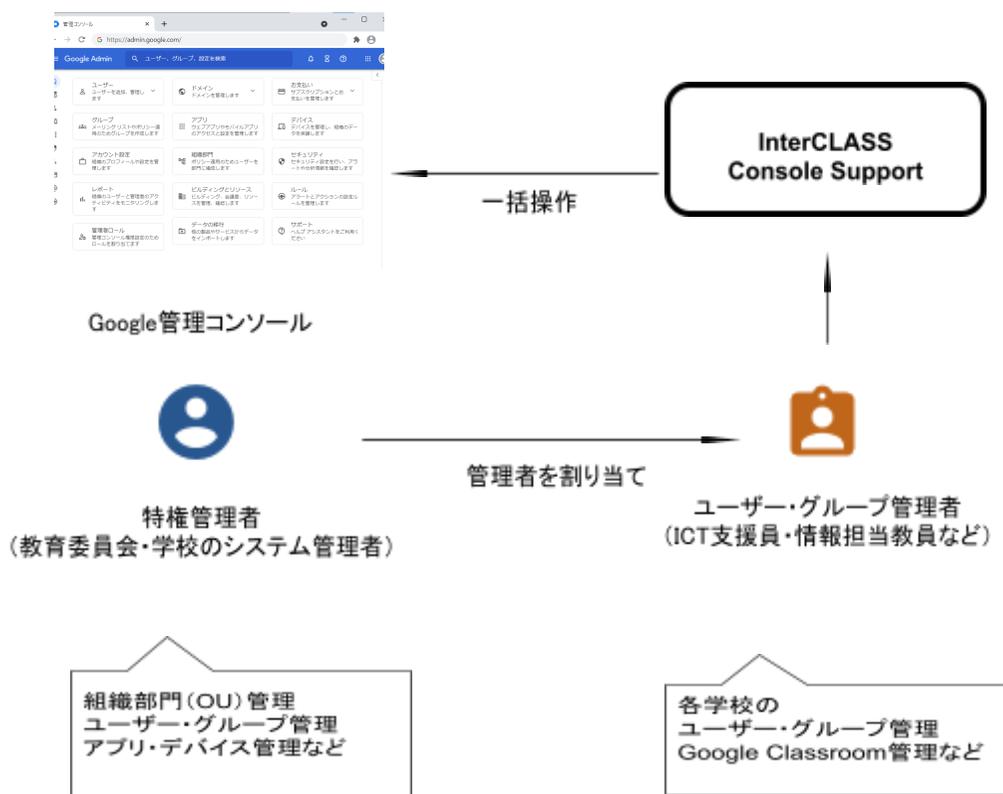
InterCLASS Console Support v3.0操作マニュアル（設定編）

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ご確認ください。

■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

O S : 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 v98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。

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操作マニュアルをご参照ください。

目次

| | |
|---|-----------|
| はじめに | 1 |
| InterCLASS Console Supportの構成 | 1 |
| 動作環境 | 2 |
| 本書の構成と読み方 | 2 |
| Google Cloud Platformの設定 | 4 |
| Google WorkspaceでのGoogle Cloud Platformの有効化 | 4 |
| Google Cloud Platformの設定 | 7 |
| ドメイン全体の管理を委任の設定 | 25 |
| Google Classroomのデータアクセスの許可 | 29 |
| QRコードログインの設定 | 32 |
| 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 | 32 |
| 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 | 38 |
| Chromeデバイスの設定の変更 | 41 |
| Chromebookのログイン画面を確認 | 45 |
| InterCLASS Console Supportの起動と終了 | 46 |
| InterCLASS Console Supportへログインする | 46 |
| InterCLASS Console Supportからログアウトする | 48 |
| システム管理の設定 | 49 |
| システム管理を開く | 49 |
| サービスアカウント登録 | 50 |
| 権限管理 | 52 |
| 権限管理の内部データ移行 | 52 |
| 移行方法 | 53 |
| CHIeruサポートについて | 58 |

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 Admin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で制御する
<https://support.google.com/a/answer/10651918>

Google WorkspaceでのGoogle Cloud Platformの有効化

1. Google Adminコンソール(<https://admin.google.com>)へアクセスします。
2. 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。



3. Google Cloud Platformを選択します。

The screenshot shows the Google Admin console interface. The left sidebar contains navigation options like 'Home', 'Dashboard', 'Directory', 'Devices', 'Apps', and 'Security'. The main content area is titled 'その他の Google サービス' (Other Google Services). A table lists various services and their status for all users. The 'Google Cloud Platform' row is highlighted with a red box. The status for Google Cloud Platform is 'オフ' (Off).

| サービス | サービスのステータス |
|------------------------------|---------------|
| Google AdSense | オフ |
| Google Arts & Culture | オン (すべてのユーザー) |
| Google Bookmarks | オフ |
| Google Cloud Platform | オフ |
| Google Developers | オン (一部のユーザー) |
| Google Domains | オフ |
| Google Earth | オン (すべてのユーザー) |
| Google Fi | オフ |
| Google My Maps | オフ |
| Google Pay | オフ |
| Google Play | オン (一部のユーザー) |

4. Google Cloud Platformの設定内のサービスのステータスをクリックします。

The screenshot shows the 'Google Cloud Platform の設定' (Google Cloud Platform Settings) page. On the left, there's a summary card showing the status as 'オン (すべてのユーザー)'. The main content area contains a warning about Google Workspace contracts and a dropdown menu for 'サービスのステータス' (Service Status), which is currently set to 'オフ (すべてのユーザー)'. Below this, there are sections for 'Cloud Resource Manager API の設定' and 'プロジェクト作成の設定'.

5. 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**で保存をクリックします。

アプリ > その他の Google サービス > Google Cloud Platform の設定 > サービスのステータス

The screenshot shows the Google Cloud Platform settings page. On the left sidebar, the '組織部門' (Organization) dropdown is expanded to show '教育委員会' (Education Commission) and 'ユーザー' (User), with 'ユーザー' selected and highlighted by a red box. The main content area shows 'サービスのステータス' (Service Status) for the selected user. The status is set to 'オン' (On), which is also highlighted by a red box. Below the status, there is a note: 'オーバーライドすると、親組織部門から継承された設定が無効になります。大部分の変更は数分で反映されます。詳細' (Overriding will invalidate settings inherited from the parent organization. Most changes will be reflected within a few minutes. Details). At the bottom right, there are 'キャンセル' (Cancel) and 'オーバーライド' (Override) buttons, with 'オーバーライド' highlighted by a red box.

6. Google Cloud Platformの設定に戻ります。**プロジェクト作成の設定**をクリックします。

アプリ > その他の Google サービス > Google Cloud Platform の設定

The screenshot shows the Google Cloud Platform settings page. The 'プロジェクト作成の設定' (Project Creation Settings) section is expanded and highlighted by a red box. It shows the status 'オン' (On) for 'ユーザーにプロジェクトの作成を許可する' (Allow project creation for users). Below this, there is a red box around the text 'に適用済みです' (Applied to).

7. **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。

アプリ > その他の Google サービス > Google Cloud Platform の設定 > Cloud Resource Manager API の設定

The screenshot shows the Google Cloud Platform settings page. On the left sidebar, the '組織部門' (Organization) dropdown is expanded to show '任意の組織部門' (Any organization), which is highlighted by a red box. The main content area shows 'Cloud Resource Manager API の設定' (Cloud Resource Manager API Settings). The 'プロジェクト作成の設定' (Project Creation Settings) section is expanded, and the checkbox for 'ユーザーにプロジェクトの作成を許可する' (Allow project creation for users) is checked and highlighted by a red box. Below this, there is a note: '大部分の変更は数分で反映されます。詳細' (Most changes will be reflected within a few minutes. Details). At the bottom right, there are '継承' (Inherit), '未保存の変更が 1 件あります' (1 unsaved change), 'キャンセル' (Cancel), and '保存' (Save) buttons, with '保存' highlighted by a red box.

Google Cloud Platformの設定

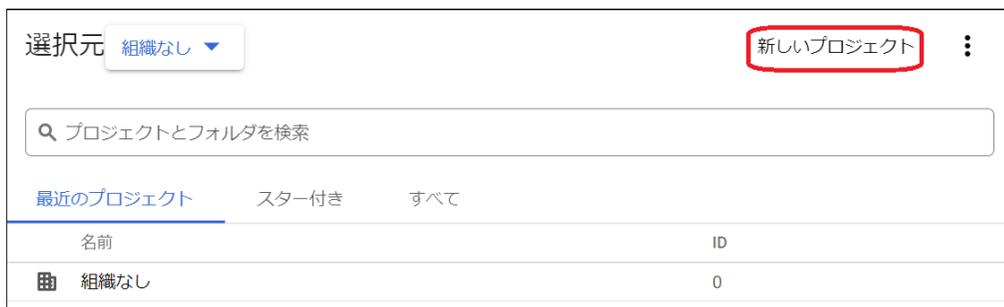
1. ChromeウェブブラウザでGoogle Cloud Platform (<https://console.cloud.google.com>) にアクセスします。
2. 初回アクセスの場合以下のような画面が表示されます。利用規約にチェックをいれ、**同意して続行**をクリックします。



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ます。



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ます。



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ます。



Google Cloud Platform

プロジェクトとリソースの検索

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 27 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 *
ICCS202112

プロジェクト ID: iccs202112。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

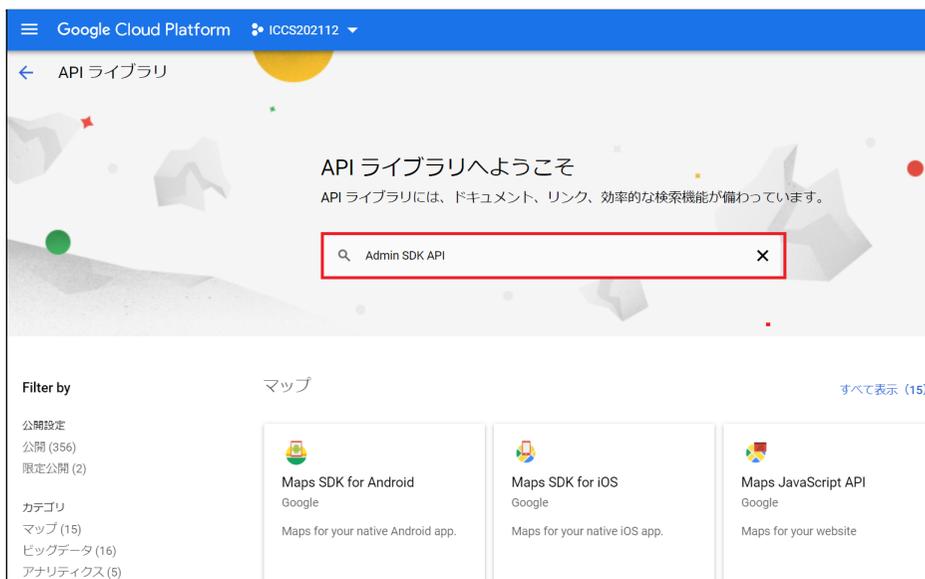
6. プロジェクトの作成が終了すると以下のような通知が届きます。**プロジェクトを選択**をクリックしてプロジェクトのダッシュボードに移動します。



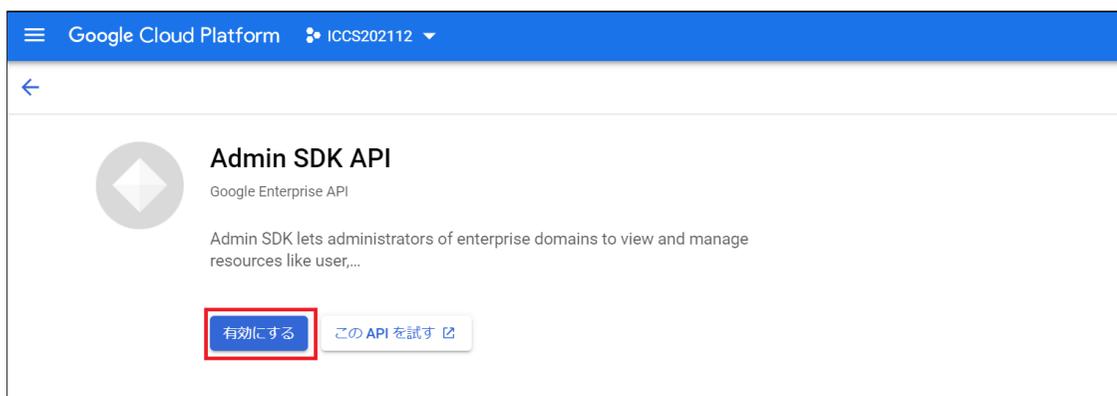
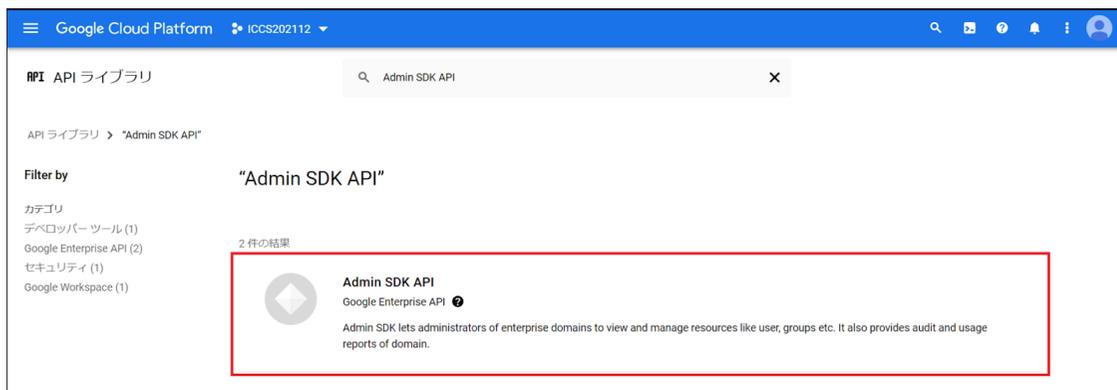
7. メニューのAPIとサービスからライブラリを表示します。



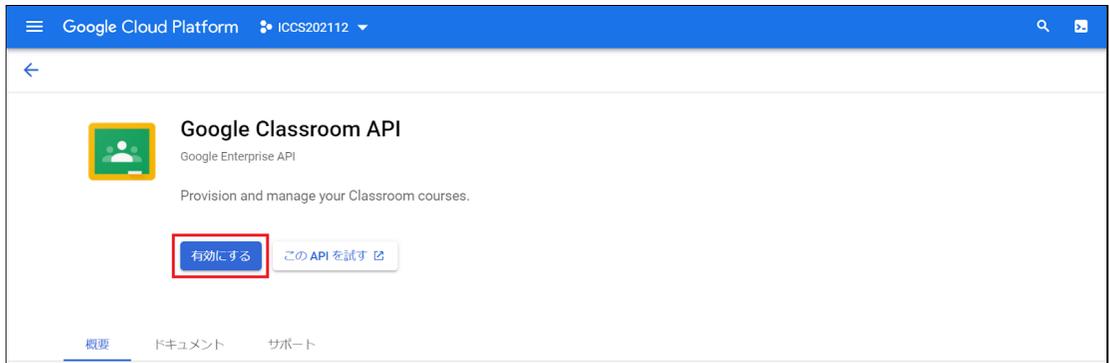
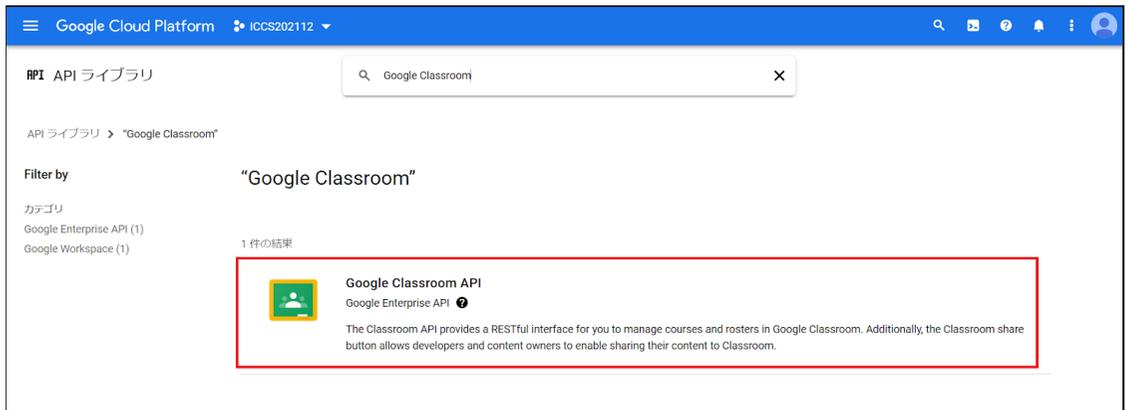
8. APIとサービスの検索ボックスに「Admin SDK API」と入力します。



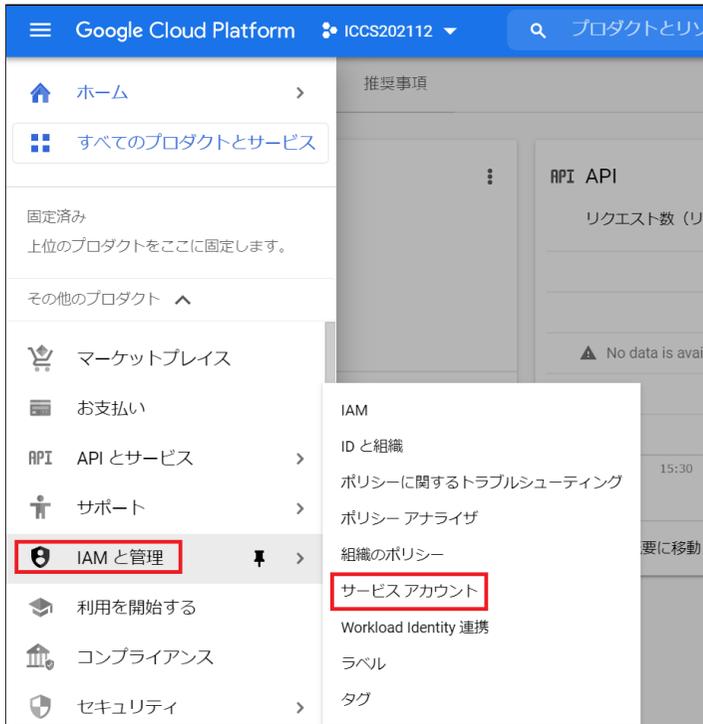
9. 検索結果に表示された**Admin SDK API**をクリックし、**有効にする**をクリックします。



10. 手順7.8.と同じ操作で「**Google Classroom API**」を検索し、**有効にする**をクリックします。



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. +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して続行をクリックします。

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-399 @iccs202112.iam.gserviceaccount.com X ↺

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

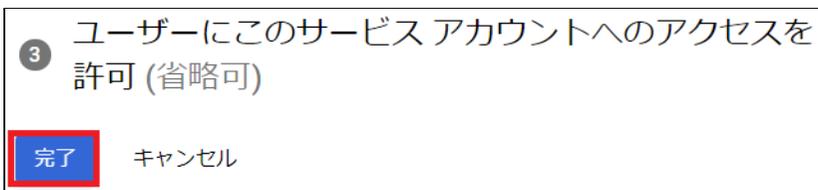
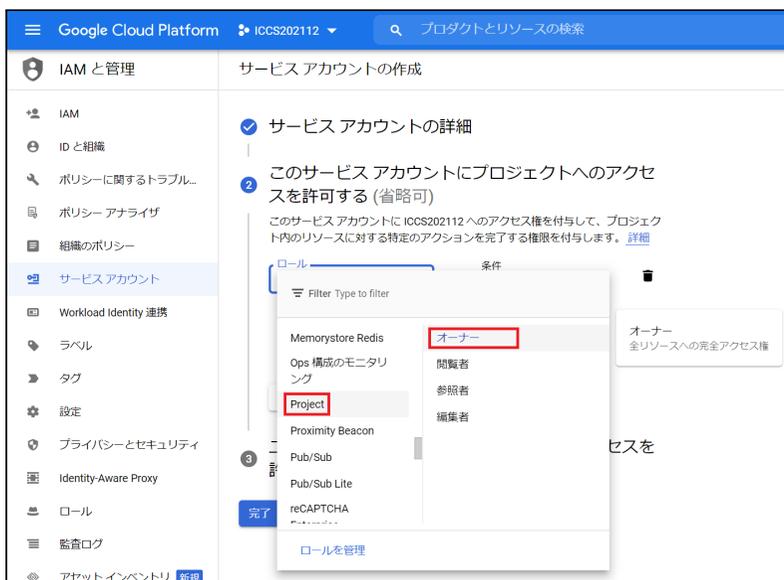
作成して続行

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**をクリックします。※項目 3 の設定は不要です。



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. **詳細設定を表示**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

名前
ICCS 保存

説明
ICCS用サービスアカウント 保存

メール
iccs-399@iccs202112.iam.gserviceaccount.com

一意の ID
110474497649856444661

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 アカウントを無効化

▼ 詳細設定を表示

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。

[詳細](#)

クライアント ID: 110474497649856444661 

GOOGLE WORKSPACE 管理コンソールを表示

Google Workspace Marketplace OAuth クライアント

 この OAuth クライアントの作成は、Google Workspace Marketplace ドメイン全体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。

[詳細](#)

 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

[↑ 詳細設定を非表示](#)

17. User Typeの**内部**を選択し、**作成**をクリックします。

OAuth 同意画面

アプリをどのように構成および登録するか（ターゲット ユーザーを含む）を選択します。プロジェクトに関連付けることができるアプリは1つだけです。

User Type

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](#)

Google の OAuth に関する [ご意見やご要望をお聞かせください](#)。

18. アプリ名に**任意の名称**、ユーザーサポートメール、デベロッパーの連絡先情報に**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、**保存して次へ**をクリックします。

アプリ登録の編集

1 OAuth 同意画面 — 2 スコープ — 3 概要

アプリ情報

この情報は同意画面に表示されるため、デベロッパーのユーザー情報とデベロッパーへの問い合わせ方法をエンドユーザーが把握できます。

アプリ名*
ICCS
同意を求めるアプリの名前

ユーザーサポートメール*
任意のメールアドレス
ユーザーが同意に関して問い合わせるために使用

アプリのロゴ [参照](#)
ユーザーがアプリを認識できるように、同意画面に 1 MB 以下の画像をアップロードします。使用できる画像形式は、JPG、PNG、BMP です。最適な結果を得るには、ロゴを 120 x 120 ピクセルの正方形にすることをおすすめします。

アプリのドメイン

デベロッパーとユーザーを保護するために、Google では、OAuth を使用するアプリのみに認可ドメインの使用を許可しています。同意画面では、次の情報がユーザーに表示されます。

アプリケーションのホームページ
ホームページへのリンクをユーザーに提供します

[アプリケーション プライバシー ポリシー] リンク
一般公開のプライバシー ポリシーへのリンクをユーザーに提供します

[アプリケーション利用規約] リンク
一般公開の利用規約へのリンクをユーザーに提供します

承認済みドメイン [?](#)

同意画面または OAuth クライアントの構成でドメインが使用されている場合は、ここで事前登録する必要があります。アプリの検証が必要な場合は、[Google Search Console](#) にアクセスして、ドメインが承認済みであるかどうかを確認してください。承認済みドメインの上限の[詳細](#)をご覧ください。

[+ ドメインの追加](#)

デベロッパーの連絡先情報

メールアドレス*
任意のメールアドレス

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。

[保存して次へ](#) [キャンセル](#)

19. 保存して次へをクリックします。

アプリ登録の編集

OAuth 同意画面 — 2 スコープ — 3 概要

スコープとは、アプリのユーザーに許可を求める権限を表します。スコープを定めることで、プロジェクトからユーザーの Google アカウントにある特定の種類のプライベートなユーザーデータへのアクセスが可能になります。[詳細](#)

スコープを追加または削除

非機密のスコープ

| API ↑ | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません | | |

🔒 機密性の高いスコープ

機密性の高いスコープとは、プライベート ユーザーデータへのアクセスをリクエストするスコープです。

| API ↑ | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません | | |

🔒 制限付きのスコープ

制限付きのスコープとは、機密性の高いユーザーデータへのアクセスをリクエストするスコープです。

| API ↑ | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません | | |

保存して次へ キャンセル

20. ダッシュボードに戻るをクリックします。

アプリ登録の編集

OAuth 同意画面 — スコープ — 3 概要

OAuth 同意画面 編集

ユーザーの種類
内部

アプリ名
ICCS

サポートメール
任意のメールアドレス

アプリのロゴ
指定されていません

[アプリケーション ホームページ] リンク
指定されていません

[アプリケーション プライバシー ポリシー] リンク
指定されていません

[アプリケーション 利用規約] リンク
指定されていません

承認済みドメイン
指定されていません

連絡先メールアドレス
任意のメールアドレス

スコープ 編集

| API ↑ | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません | | |

[ダッシュボードに戻る](#)

21. OAuth同意画面が表示されたら、操作は終了です。

OAuth 同意画面

ICCS [アプリを編集](#)

ユーザーの種類

内部 [?](#)

[外部へ](#)

OAuth レート上限

トークン付与レート [?](#)

トークン付与レートは、アプリケーションで新規ユーザーを取得できる速度を制限します。

現在の1日あたりのトークン付与レートの上限は10,000件の付与です。1日あたりのトークン付与レートは毎日リセットされます。[1日あたりのトークンの上限を増やす](#)

5分 1日

10,001

10,000

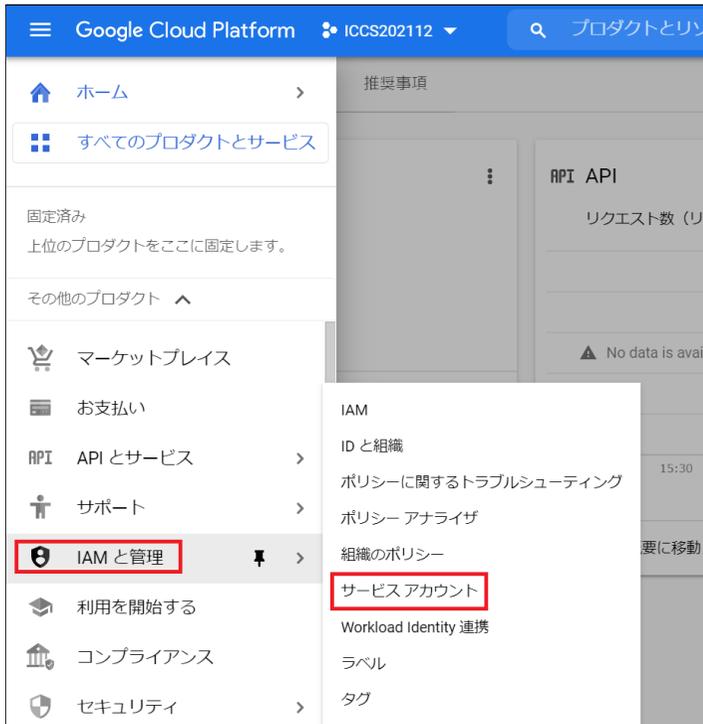
9,999

18:00 21:00 火 14 3:00 6:00 9:00 12:00 15:00

[SHOW LESS](#)

Google の OAuth に関する[ご意見やご要望をお聞かせください](#)。

22. 再度、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。



23. サービスアカウントの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。

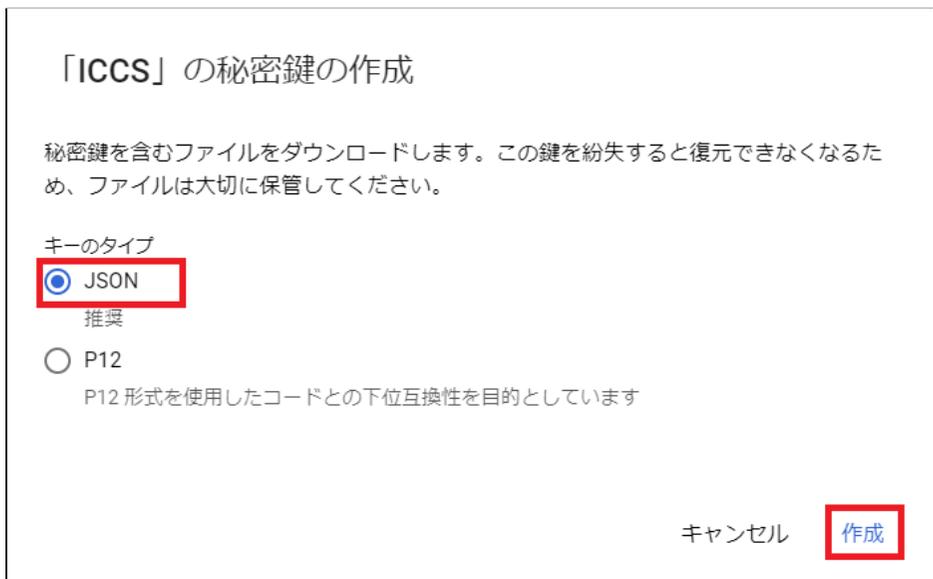
※OAuth2クライアントIDの番号は後ほど使用しますので、番号をお控えください。



24. 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。



25. キーのタイプは**JSON**を選択し、**作成**をクリックします。



26. 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。

秘密鍵がパソコンに保存されました



iccs202112-726632d16c06.json によってクラウド リソースへのアクセスが許可されるため、安全に保存してください。 [詳細](#)

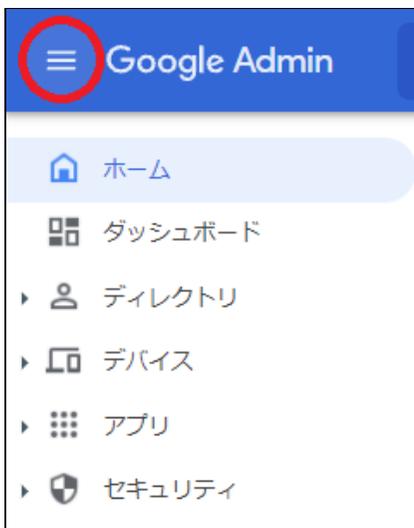
閉じる

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。
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の制御**をクリックします。



- 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。



- 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。

The screenshot shows a dialog box titled '新しいクライアント ID を追加'. It contains a text input field for 'クライアント ID'. Below the input field is a checkbox labeled '既存のクライアント ID を上書きする ?'. Underneath the checkbox is a text input field for 'OAuth スコープ (カンマ区切り)'. At the bottom right of the dialog, there are two buttons: 'キャンセル' and '承認'.

9. **クライアントID**には「**Google Cloud Platformの設定**」の23.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,  
https://www.googleapis.com/auth/admin.directory.device.chromeos
```

10. 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

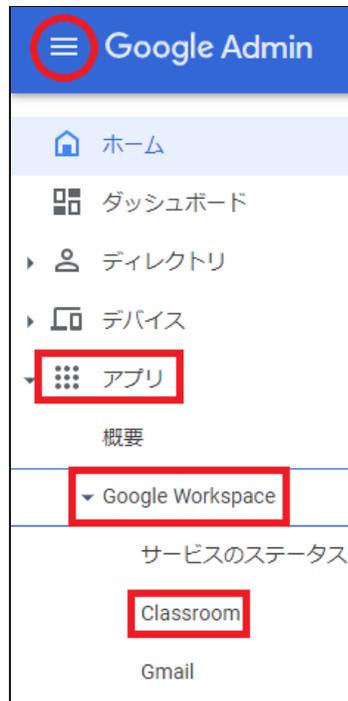
既存のクライアント ID を上書きする ⓘ

OAuth スコープ (カンマ区切り)

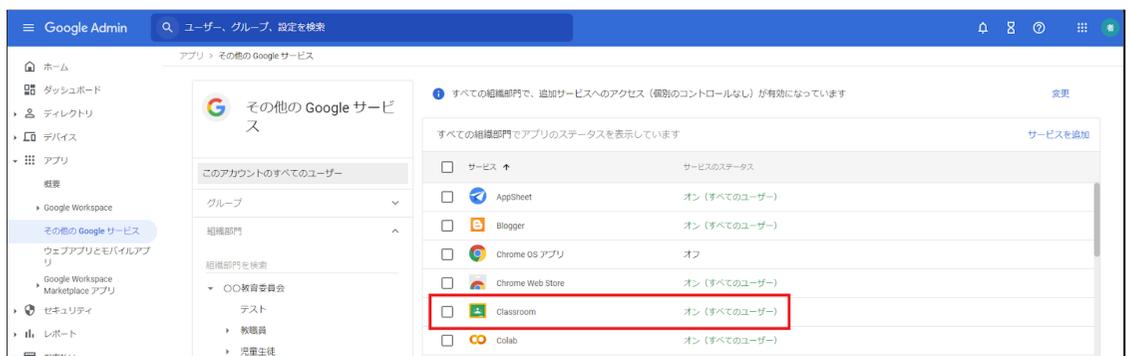
キャンセル 承認

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**>**Google Workspace**>**Classroom**をクリックします。



※上記の場所にて確認できない場合は、**アプリ**>**その他のGoogleサービス**をクリックし、**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、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、保存をクリックします。

The screenshot shows the Google Admin console interface. At the top, the navigation bar includes 'Google Admin', a search bar with the text 'ユーザー、グループ、設定を検索', and utility icons. The breadcrumb trail reads 'アプリ > Google Workspace > Classroom の設定 > データアクセス'. On the left, a sidebar contains navigation icons and a 'Classroom' section with a dropdown menu for '組織部門'. The main content area is titled 'データアクセス' and contains the following information:

- Header: 次の組織部門のユーザー設定を表示しています:
- Section: データアクセス
- Section: Classroom API
「チエル市教育委員会」で適用しました
- Text: ユーザーが Classroom のデータにアクセスする方法を管理します。
- Checklist item: 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。
- Info message: **i** Most changes take effect in a few minutes. [Learn more](#)
監査ログで以前の変更を確認できます
- Buttons: キャンセル and 保存 (circled in red)

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。

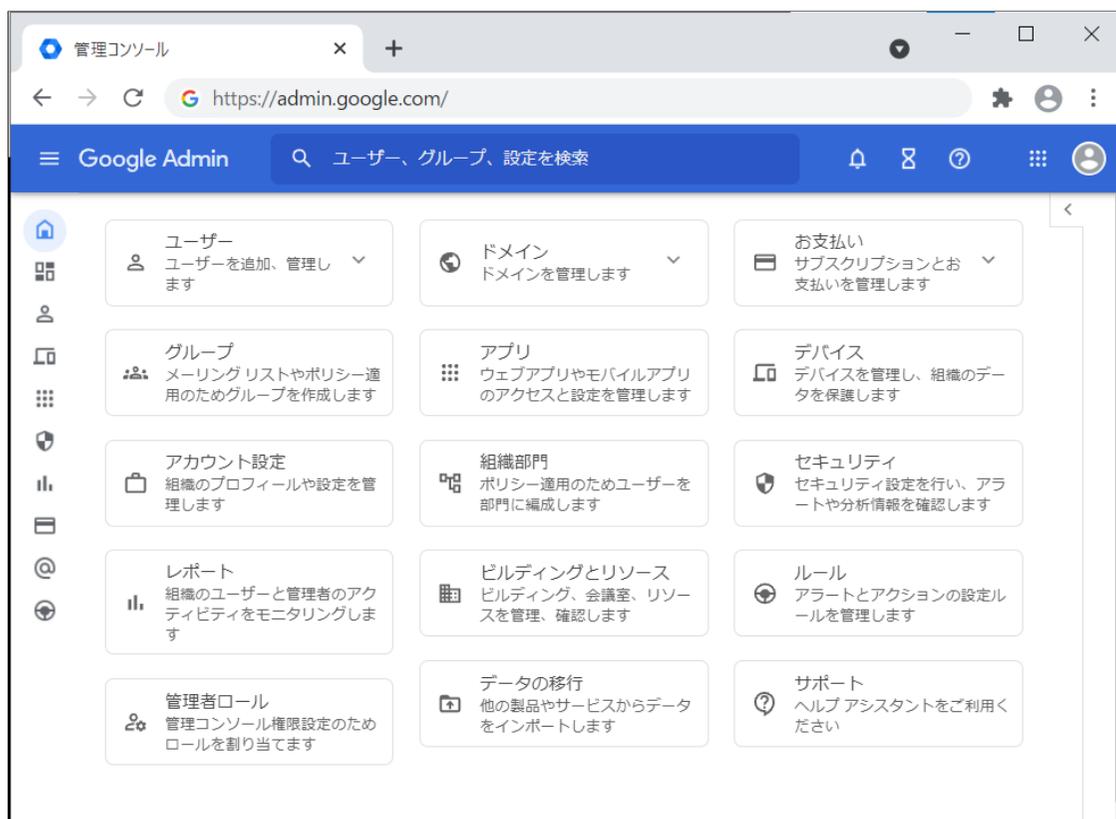
サードパーティのIDプロバイダを使用したシングルサインオンの設定

QRコードを使用したChromebookへのログインに必要な設定です。

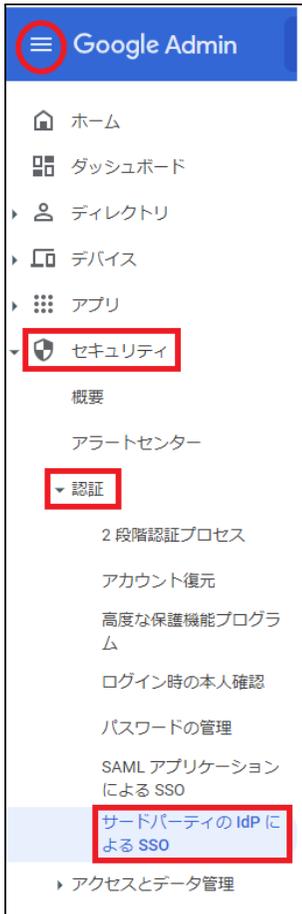
④ポイント

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> 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)の設定が開きます。**



5. 組織向けのサードパーティのSSOプロファイルのパネルを展開するか、組織向けのSSOプロファイルを編集します。

組織向けのサードパーティの SSO プロファイル

すべてのユーザーがこのプロファイルのサードパーティの IdP で Google Workspace にログインします。ただし、このプロファイルを使用しないよう指定した組織部門またはグループは除きます。 [詳細](#)

組織向けの SSO プロファイル オン

パネルを展開

6. 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>

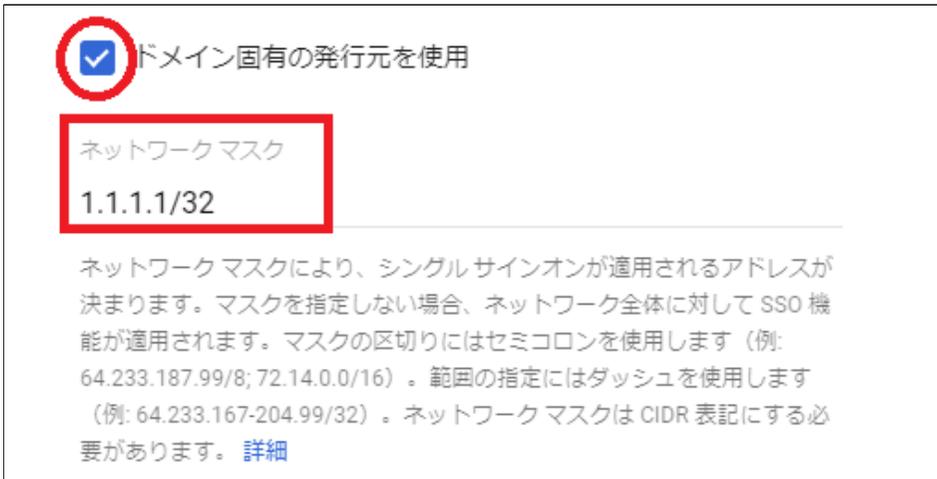
サードパーティの ID プロバイダ サードパーティの ID プロバイダで SSO を設定する

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/met>
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/met>
ユーザーがログアウトするときにリダイレクトする URL

7. **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。



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](#)

8. 右下の**保存**をクリックします。



9. 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。

P46. [InterCLASS Console Supportへログインする参照](#)



10. 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。

The screenshot shows the Google Admin console interface for configuring Single Sign-On (SSO) with a third-party ID provider. The page title is "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".

On the left, there is a navigation menu with "セキュリティ" (Security) selected. The main content area is titled "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".

Under the "サードパーティの ID プロバイダ" (Third-party ID Provider) section, the checkbox "サードパーティの ID プロバイダで SSO を設定する" (Use third-party ID provider for SSO) is checked. Below this, there are fields for "ログインページの URL" (Login page URL) and "ログアウトページの URL" (Logout page URL), both set to "https://sso.interclasscloud.com:443/idp/SSORedirect/".

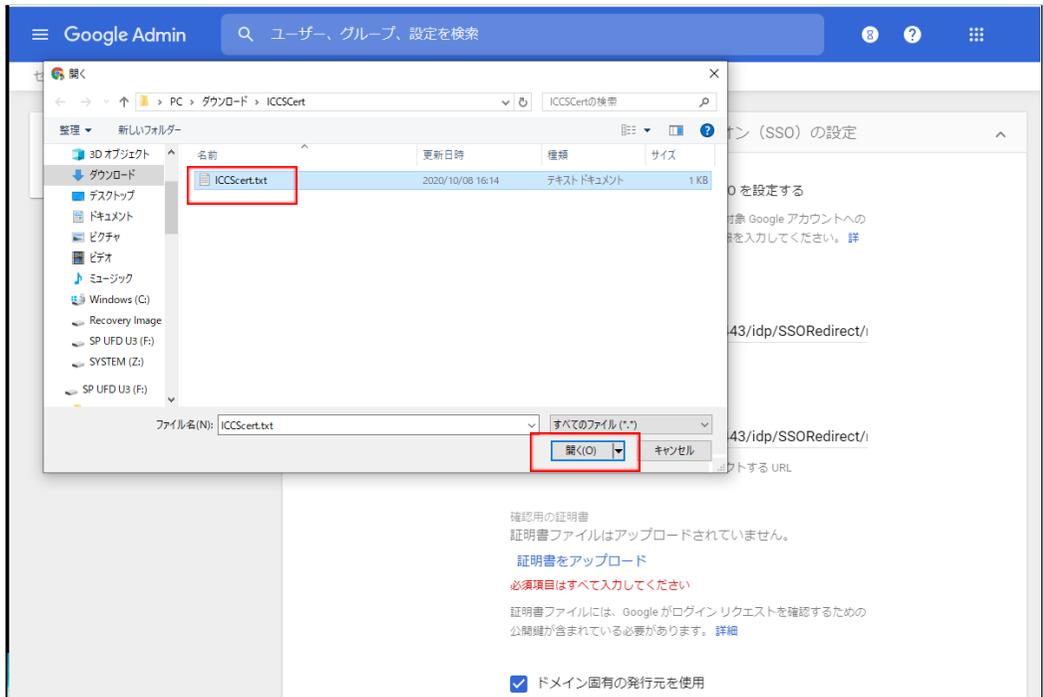
The "確認用の証明書" (Certificate for verification) section contains the text "証明書ファイルはアップロードされていません。" (Certificate file is not uploaded). A red box highlights the "証明書をアップロード" (Upload certificate) button. Below the button, it says "必須項目はすべて入力してください" (Please enter all required items). The text continues: "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。" (The certificate file must contain a public key for Google to verify login requests).

The "ドメイン固有の発行元を使用" (Use domain-unique issuer) checkbox is also checked. Below it, the "ネットワークマスク" (Network mask) is set to "1.1.1.1/32".

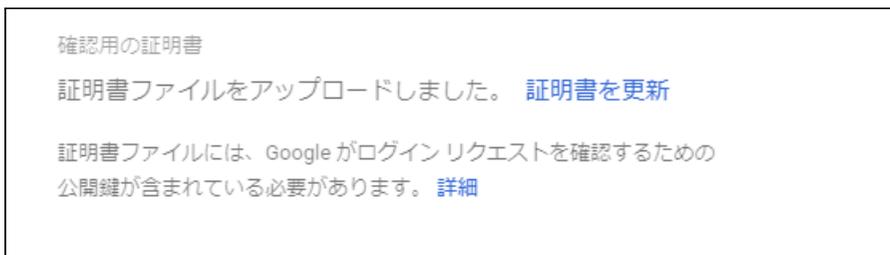
At the bottom, there is a "パスワード変更用 URL" (Password change URL) field.

At the bottom right of the page, there are "キャンセル" (Cancel) and "保存" (Save) buttons.

11. 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。



12. 証明書がアップロードされると下記の表示になります。



13. ページの最下部へ移動し、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。

⑨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。

⑩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管理者ヘルプをご参照ください：

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

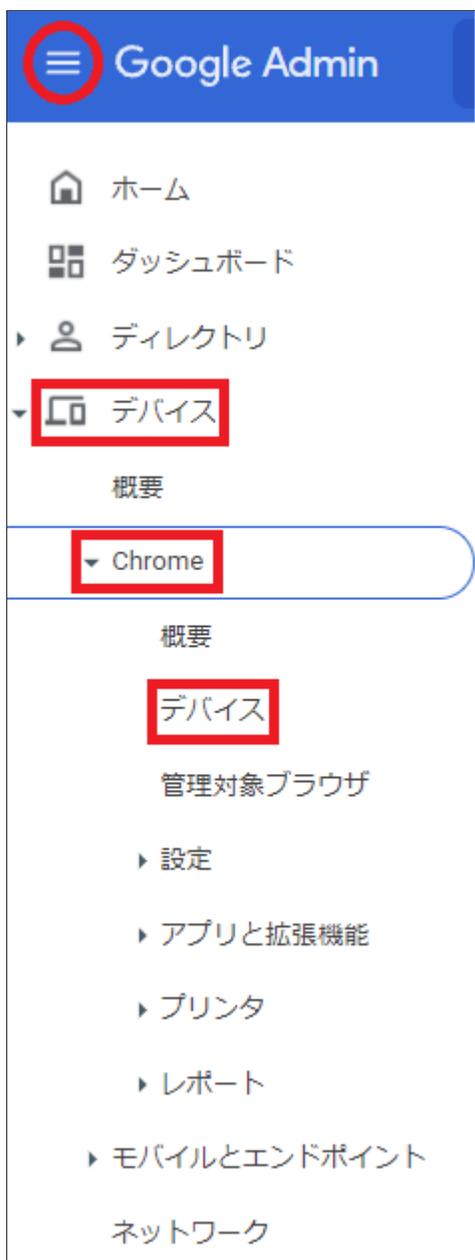
▼ 児童生徒ユーザー

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**>**デバイス**をクリックします。



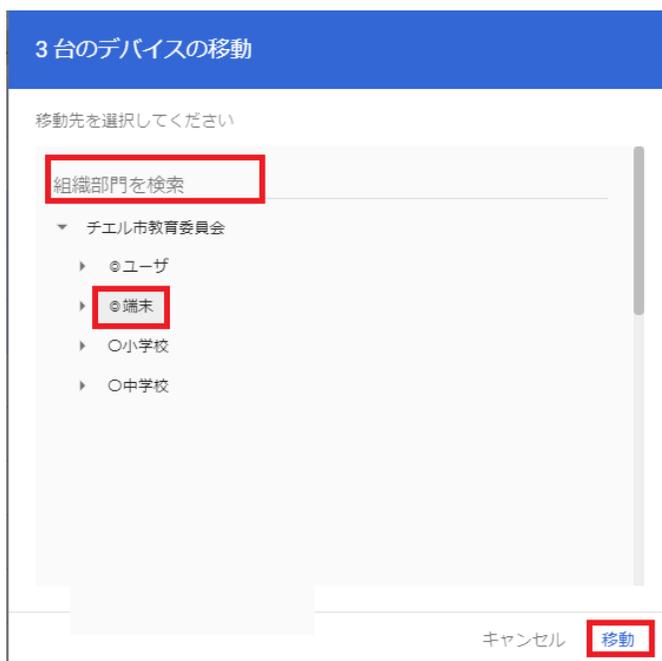
4. Chromeデバイスの一覧画面で、QRコードログインを有効にする**Chromeデバイス**に**チェック**を入れて選択します。



5. 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。



6. 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。



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。

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



4. 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。

組織部門を検索

▼ チエル市教育委員会

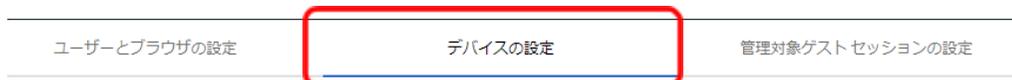
▶ チエル中学校

▶ チエル小学校

📍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、P.38 [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。

5. **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。



6. 画面を下にスクロールし、**ログイン設定**の項目に移動し、**v**を開きます。



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。
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。

| ログイン設定 | |
|--|--|
| 注: ログイン画面アプリページ でスマートカードログインを有効にすることができます。 | |
| 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 ▼ |
| ログインの制限 Google のデフォルトに設定し... | すべてのユーザーにログインを許可する ▼ |
| 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@ domain.com(お客様のドメイン) |
| 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 ▼ 警告: ほとんどの導入環境では、この設定の使用はおすすめできません。詳しくは、 ログイン画面に関するヘルプセンター記事 をご覧ください。 |

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。

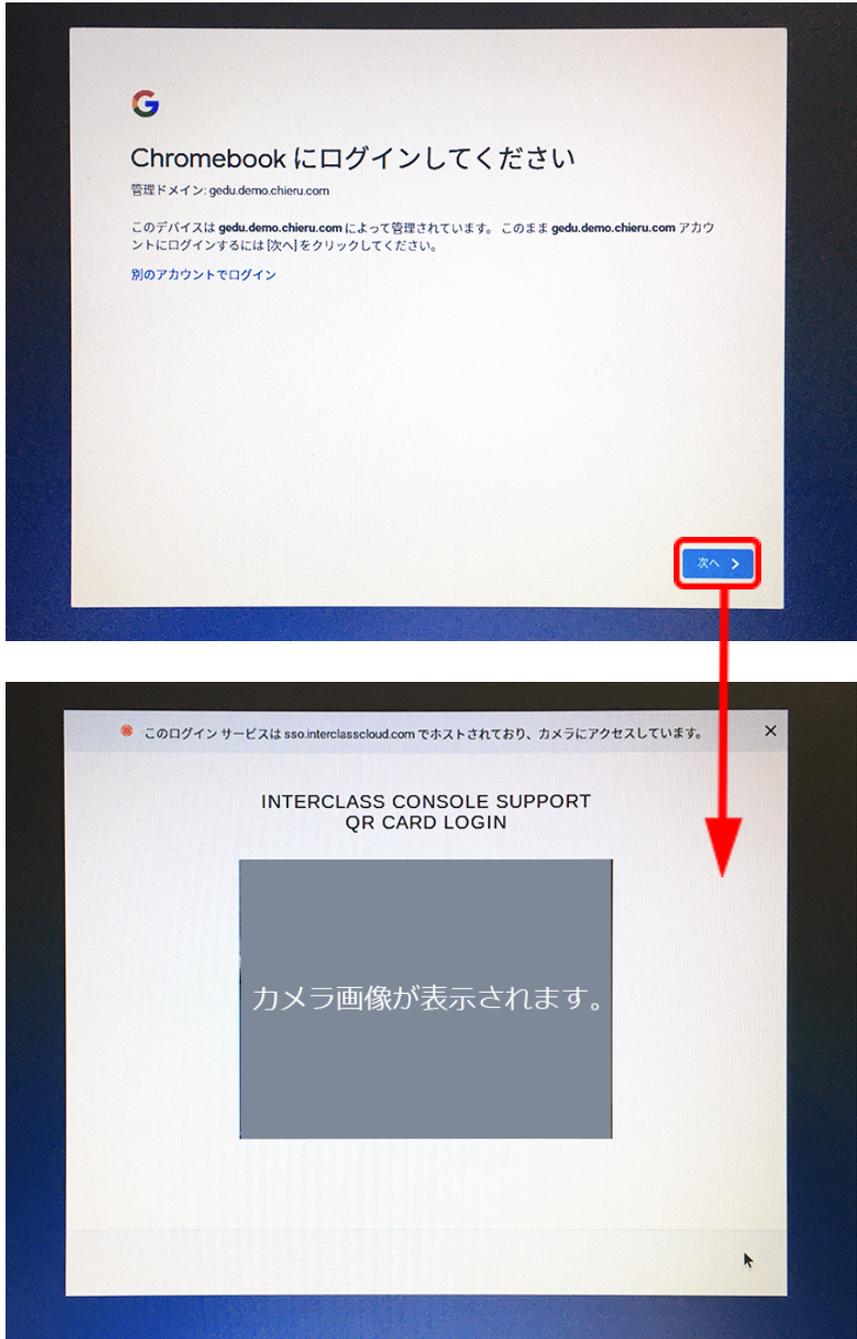
| | |
|---|---|
| シングルサインオン ID プロバイダ (IdP) のリダイレクト ローカルに適用 ▼ | SAML SSO ID プロバイダ (IdP) へのユーザーのリダイレクト SAML SSO IdP ページへの移動をユーザーに許可する ▼ |
| シングルサインオン Cookie の動作 Google のデフォルトに設定し... | ログイン中、ユーザー セッションへの SAML SSO Cookie の転送を無効にする ▼ 警告: このポリシーは、Chrome デバイス向けに SAML SSO が設定されている場合にのみ該当します。 Chrome デバイスでの SAML シングルサインオン設定について |
| 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 ▼ | カメラへのシングルサインオンアクセスが可能な URL 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。 |

12. 画面右上の**保存**をクリックします。

| | | |
|----------------------|--------------|------------------|
| 5 個の設定を変更しました | 元に戻す | 保存 |
| デバイス > Chrome > 設定 ▼ | | |
| 組織部門を検索 | ユーザーとブラウザの設定 | デバイスの設定 |
| | | 管理対象ゲスト セッションの設定 |

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。

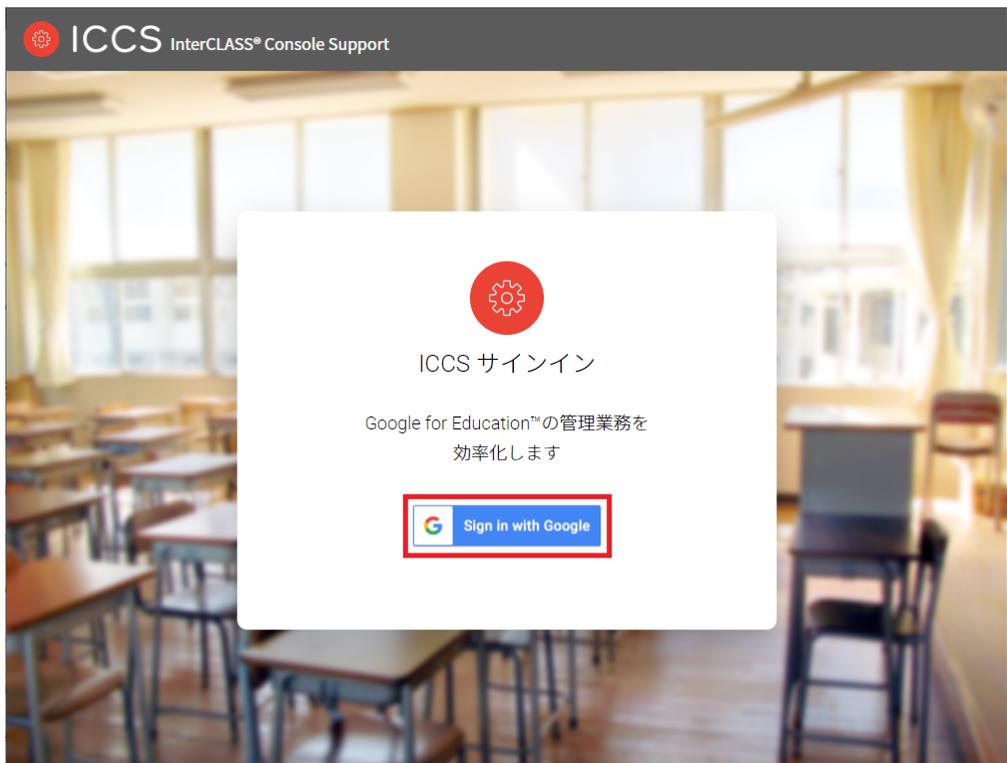


InterCLASS Console Supportの起動と終了

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。



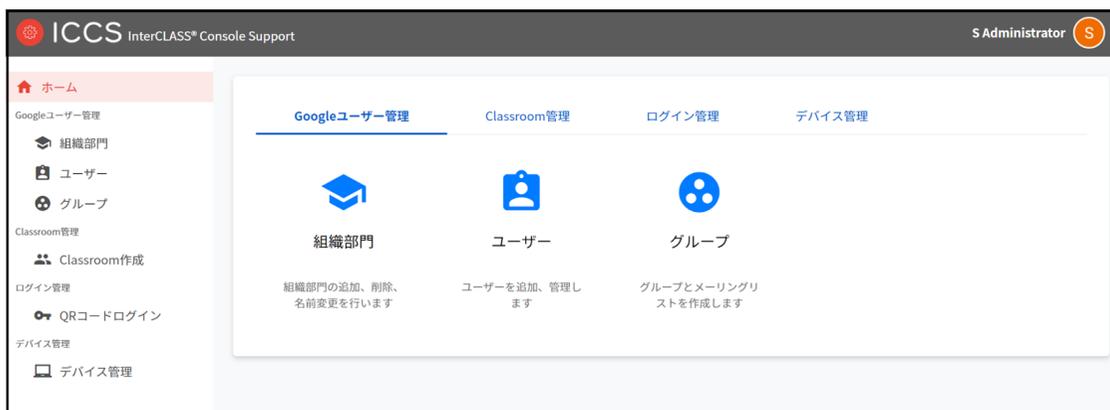
3. Googleのログイン画面が表示されます。管理者のメールアドレスを入力し、**次へ**をクリックします。



4. パスワードを入力して**次へ**をクリックします。

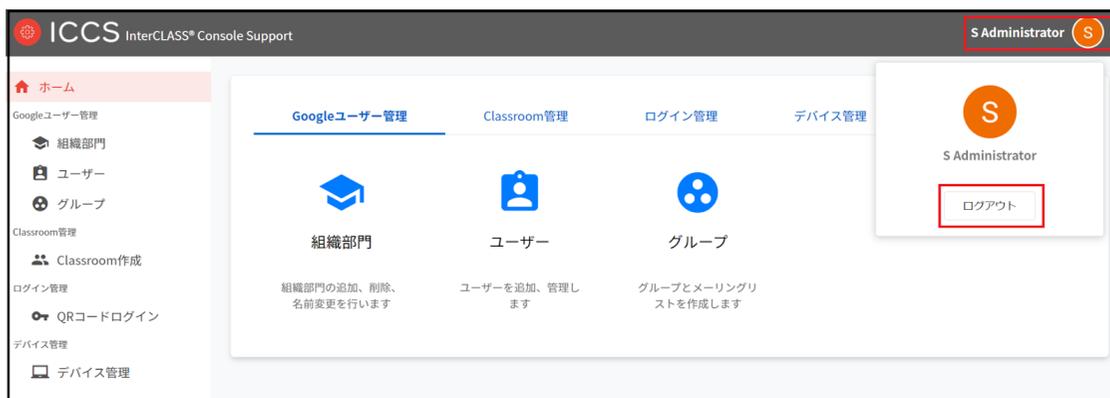


5. ICCSのトップページが表示されます。



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。



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:

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:

5. **アップロード**ボタンをクリックします。



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

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。

権限管理の内部データ移行

InterCLASS Console Supportをv2.4からご利用いただいている場合は、v3.0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。

移行方法

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



2. 画面右上のアイコンをクリックし、**歯車マーク**をクリックします。



3. システム管理が開きます。**権限管理**をクリックします。

システム管理

| | |
|---|---|
|  権限管理 ユーザーの操作権限を設定・解除します。 |  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。 |
|---|---|

4. 権限管理を開くと、次のようなダイアログが開きます。**移行する**をクリックします。

v3.0以降での権限管理のご利用には、内部データの移行が必要となります。

作成済みの権限情報を移行してよろしいですか？

※移行時に「権限情報内の対象組織部門に現在存在しない組織部門名が含まれています。」とのメッセージが出た場合、こちらから「修正データをインポート」をクリックし、CSVをインポートしてください。

移行する

修正データをインポート

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** 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10.に進んでください。

権限情報内の対象組織部門に現在存在しない組織部門名が含まれています。
エクスポートしたCSVデータの **データチェック結果** 列が「組織部門取得エラー」となっている行について以下の対応を行った後、「修正データをインポート」ボタンからインポートしてください。

- そのユーザーの権限を別の組織に割り当てたい場合、**対象組織部門** 列を存在する組織部門名に修正する
- そのユーザーの権限が不要な場合、**削除対象** 列に削除と入力する

※ ID 列は変更・削除しないでください。

※ 既に削除済みのユーザーに権限が割り振られている場合、**削除対象** 列に「削除」がデフォルトで入っています。

※ **対象組織部門** に存在しない組織部門名が入力されたままのデータもインポート可能ですが、移行後にユーザーがログイン不可となる場合があります。

エクスポートして閉じる

⑨ポイント

添付画像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。

6. エクスポートしたCSVファイルはテキストエディタや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**をクリックします。

v3.0以降での権限管理のご利用には、内部データの移行が必要となります。

作成済みの権限情報を移行してよろしいですか？

※移行時に「権限情報内の対象組織部門に現在存在しない組織部門名が含まれています。」とのメッセージが出た場合、こちらから「修正データをインポート」をクリックし、CSVをインポートしてください。

移行する

修正データをインポート

8. エクスポートし編集したCSVファイルを**ファイルを選択**でインポートファイルとして選択します。

権限情報のインポート

内部データ移行のための権限ごとの対象組織部門をCSV形式でインポートします。

※csv内のメールアドレスや各種限の変更は、移行時には反映されません。移行後に権限管理画面での変更をお願いします。
※処理が終了するまでブラウザ・タブを閉じないでください。

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

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。内容を確認のうえ、**インポート**をクリックします。

権限情報のインポート

内部データ移行のための権限ごとの対象組織部門をCSV形式でインポートします。

※csv内のメールアドレスや各種限の変更は、移行時には反映されません。移行後に権限管理画面での変更をお願いします。
※処理が終了するまでブラウザ・タブを閉じないでください。

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

表示 10 件

| <input type="checkbox"/> | ID | メールアドレス | 対象組織部門 | 削除対象 |
|-------------------------------------|-----|---------|--------|------|
| <input checked="" type="checkbox"/> | 1 | | / | |
| <input checked="" type="checkbox"/> | 5 | | | |
| <input checked="" type="checkbox"/> | 200 | | | |
| <input checked="" type="checkbox"/> | 135 | | | |
| <input checked="" type="checkbox"/> | 158 | | | |
| <input checked="" type="checkbox"/> | 10 | | | 削除 |
| <input checked="" type="checkbox"/> | 11 | | | 削除 |
| <input checked="" type="checkbox"/> | 147 | | | |
| <input checked="" type="checkbox"/> | 13 | | | 削除 |
| <input checked="" type="checkbox"/> | 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

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 v3.0操作マニュアル(設定編)

2022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。

