

CHleru

InterCLASS Console Support

InterCLASS Console Support v3.5 操作マニュアル(設定編)

目次

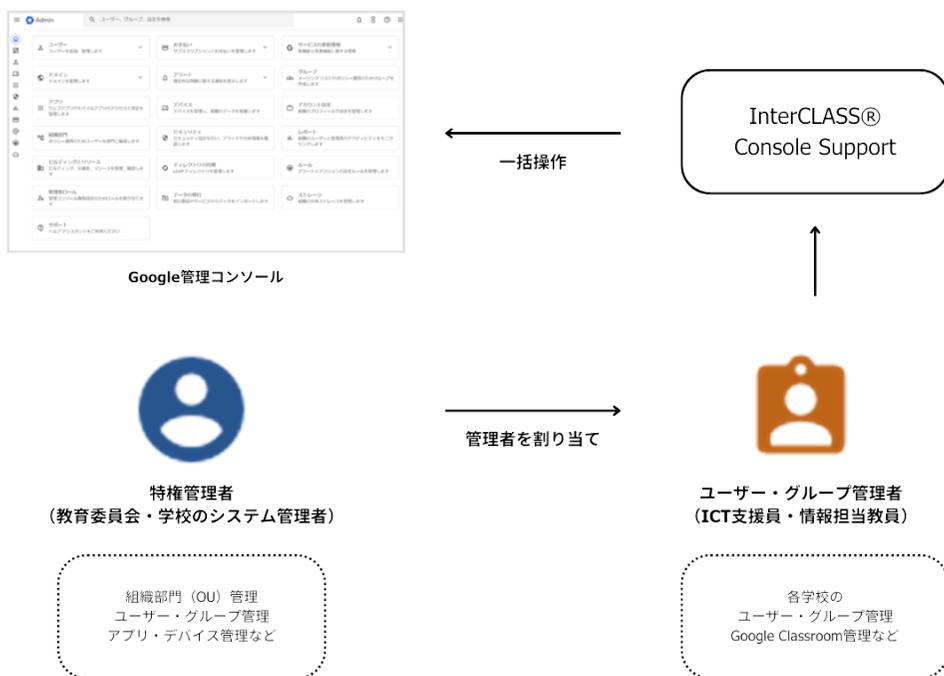
はじめに	2
InterCLASS Console Support の構成	2
動作環境	3
本書の構成と読み方	3
Google Cloud Platform の設定	4
Google WorkspaceでのGoogle Cloud Platformの有効化	5
Google Cloud Platformの設定	8
ドメイン全体の管理を委任する設定	25
Google Classroomのデータアクセスの許可	29
QRコードログイン の設定	31
サードパーティのIDプロバイダを使用したシングルサインオンの設定	31
QRコードログインを適用するChromeデバイスを特定の組織部門に移動	38
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	46
InterCLASS Console Supportからログアウト	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
QRコード情報移行	52
権限管理	54
権限管理の内部データを移行する	54
作成済みの権限情報を移行する	55
CHIeru サポートについて	60

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

- OS** : Windows 11 Pro, SE, Enterprise / Windows 10 Pro, Education, Enterprise /
Mac OS 10.14 (Sierra) 以上
最新のChrome OS
- アプリ** : Google Chrome v104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**InterCLASS Console Support v3.5** 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。

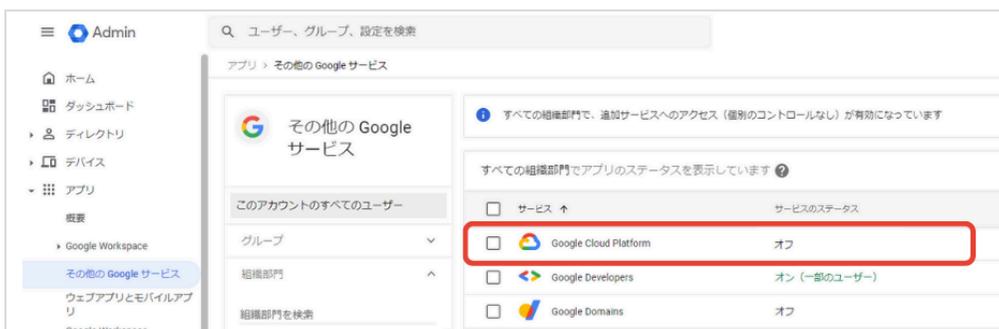
Google サービスへのアクセスを年齢で制御する
<https://support.google.com/a/answer/10651918>

Google WorkspaceでのGoogle Cloud Platformの有効化

1. Google 管理コンソール(<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**をクリックします。



4. Google Cloud Platformの設定画面の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

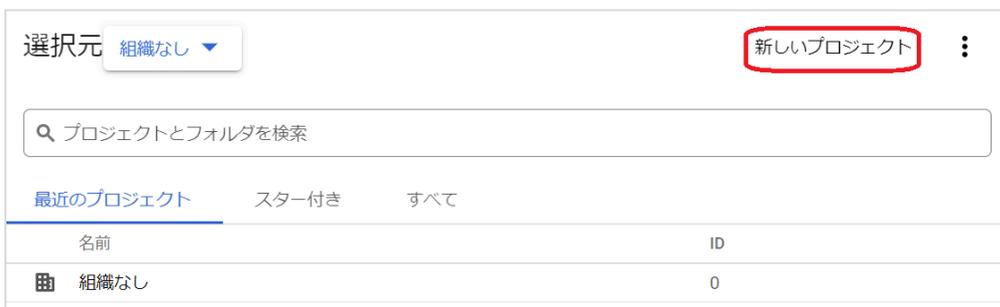
1. ChromeウェブブラウザでGoogle Cloud Platform (<https://console.cloud.google.com>)にアクセスします。
2. 初回アクセスの場合以下のような画面が表示されます。利用規約にチェックをいれ、同意して続行をクリックします。



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. ポップアップの新しいプロジェクトからプロジェクトを作成します。



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、有効にするをクリックします。

API ライブラリ

API ライブラリ > "Admin SDK API"

3 件の結果

Admin SDK API
Google

With the Admin SDK API, Google Workspace account administrators can view and manage resources like users and groups. You can also run reports to audit usage within your account.

 **Admin SDK API**
[Google](#)

Manage Google Workspace account resources and audit usage.

有効にする [この API を試す](#)

10. 手順8.9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。

API ライブラリ

API ライブラリ > "Google Classroom API"

1 件の結果

Google Classroom API
Google Enterprise API

The Classroom API provides a RESTful interface for you to manage courses and rosters in Google Classroom. Additionally, the Classroom share button allows developers and content owners to enable sharing their content to Classroom.

 **Google Classroom API**
Google Enterprise API

Provision and manage your Classroom courses.

有効にする [この API を試す](#)

11. 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。



12. 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。



13. 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. 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で**Project**のロールをオーナーに設定し、完了をクリックします。※項目3の設定は不要です。

✓ サービス アカウントの詳細

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)

このサービス アカウントに My Project 16325 へのアクセス権を付与し、プロジェクト内のリソースに対する特定のアクションを完了する権限を付与し [細](#)

3

完了

ロールを選択 IAM の条件 (省略可) ?

フィルタ フィルタテキストを入力

Monitoring	ロール
Ops 構成のモニタリング	オーナー
Project	閲覧者
Proximity Beacon	参照者
Pub/Sub	編集者
Pub/Sub Lite	
Rapid Migration Assessment	

ロールを管理

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. 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 IAM console interface for a project named 'My Project 16325'. The left sidebar contains navigation options like 'IAM', 'ID と組織', 'ポリシーに関するトピック', 'ポリシー アナライザ', '組織のポリシー', 'サービスアカウント', 'Workload Identity 連携', and 'ラベル'. The main content area is titled 'サービス アカウント' and includes a '+ サービスアカウントを作成' button and links for '削除', 'アクセスを管理', and '更新'. Below this, there is a table of service accounts with columns for 'メール', 'ステータス', '名前', '説明', 'キー ID', 'キーの作成日', 'OAuth 2 クライアント ID', and '操作'. One entry is highlighted with a red box: 'iccs-76@intense-petal-368906.iam.gserviceaccount.com'.

メール	ステータス	名前	説明	キー ID	キーの作成日	OAuth 2 クライアント ID	操作
iccs-76@intense-petal-368906.iam.gserviceaccount.com	有効	ICCS	ICCS用サービスアカウント	キーがありません		102474701619451632628	操作

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。

[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. OAuth同意画面のUser Typeで内部を選択し、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. **OAuth**同意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、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称

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. スコープ画面で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

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. 概要画面で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上限を増やす](#)

5分 1日

10,001

No data is available for the selected time frame

10,000

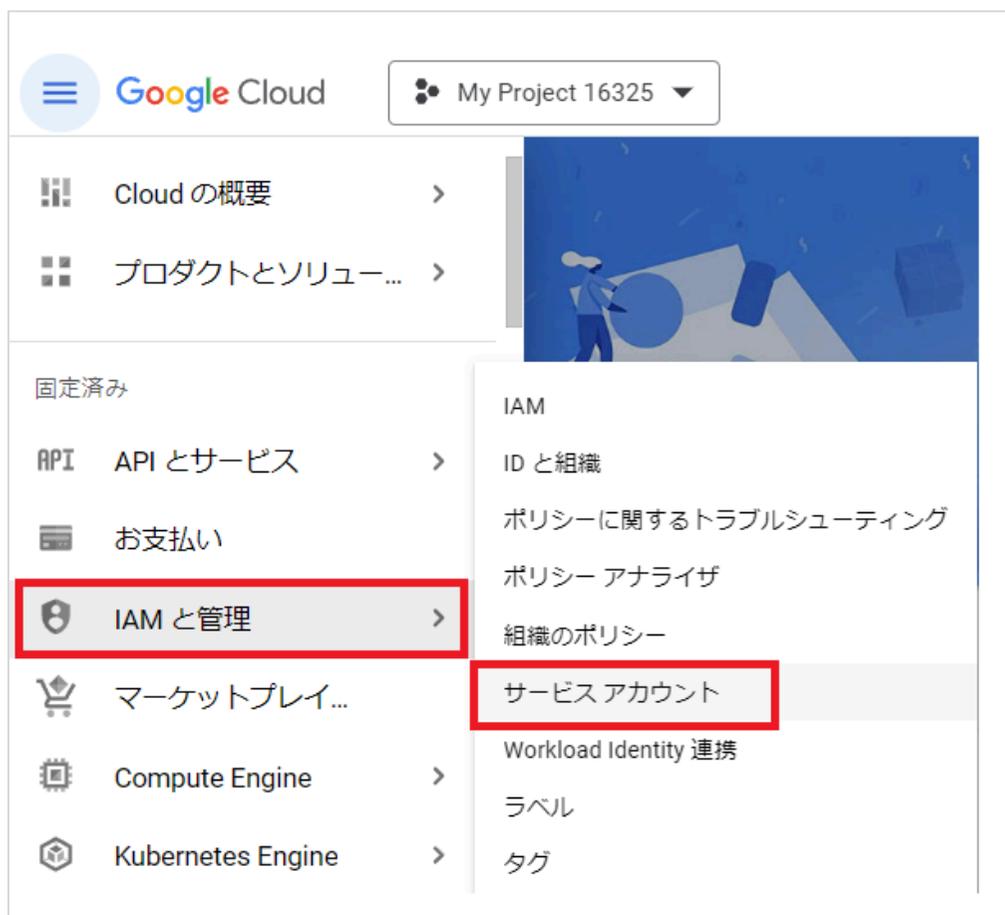
9,999

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、メニューから**IAM**と管理>サービス アカウントをクリックします。



23. 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。

※**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. 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. 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。

「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

26. JSON形式の秘密鍵がダウンロードされます。このInterCLASS Console Support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](#)

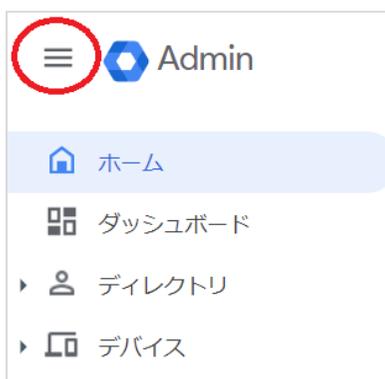
閉じる

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の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

APIの制御

このコントロールを使用して、ユーザーの Google データに対する、内部アプリとサードパーティ製アプリの API アクセスを管理できます。

アプリからのユーザーの Google データへのアクセスを管理します。 [アプリのアクセス制御の詳細](#)

Google Workspace Marketplace の許可リストにあるアプリと、ウェブアプリとモバイルアプリのリストにある Android アプリと iOS アプリは自動的に信頼されます。

概要	0 個の制限付きの Google サービス	1 個のアプリが審査待ち
	18 個の無制限の Google サービス	5 個の設定済みアプリ
	GOOGLE サービスを管理	233 個のアクセス済みアプリ
		サードパーティ製アプリのアクセスを管理

設定 **NEW**

カスタムユーザー メッセージ	未設定のサードパーティ製アプリ	内部アプリ
オン	18 歳以上のユーザー: サードパーティ製アプリへのアクセスをユーザーに許可する 18 歳未満のユーザー: ユーザーにサードパーティ製アプリへのアクセスを許可しない	内部アプリを信頼しない

未設定のアプリへのアクセスに対する 18 歳未満のユーザーのリクエスト
18 歳未満のユーザーにアクセス権のリクエストを許可する

ドメイン全体の委任

デベロッパーは、開発したウェブアプリケーションとその他の API クライアントを Google に登録して、Gmail などの Google サービス内のデータへのアクセスを有効にできます。登録されたこれらのクライアントを管理者が承認すると、個々のユーザーの同意またはパスワードがなくても、クライアントはユーザーデータにアクセスできるようになります。 [詳細](#)

[ドメイン全体の委任を管理](#)

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。

セキュリティ > API の制御 > ドメイン全体の委任

i デベロッパーが Google に登録したウェブアプリケーションや他の API クライアントで、Gmail などデータにアクセスすることを許可できます。

API クライアント	新しく追加	クライアント情報をダウンロード...
------------	-----------------------	------------------------------------

+ フィルタを追加

7. 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

8. クライアントIDにGoogle Cloud Platformの設定の手順23.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>

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

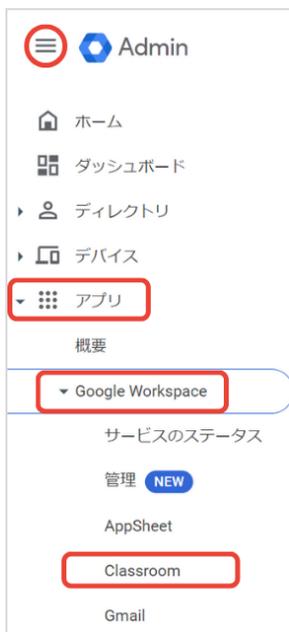
既存のクライアント ID を上書きする ?

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. メニューからアプリ>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。

📍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. メニューからセキュリティ>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。



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プロファイルの編集をクリックします。



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

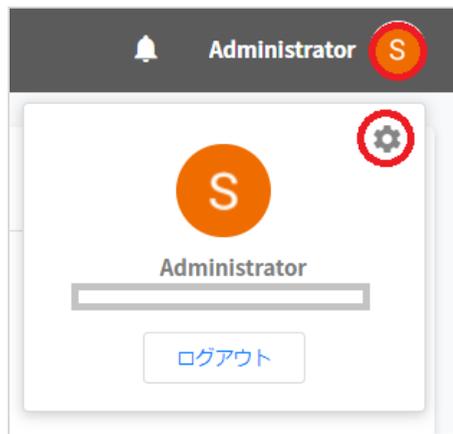
ネットワーク マスク
1.1.1.1/32

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. 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**から取得します。
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. ユーザーアイコンをクリックし、歯車マークをクリックします。



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. 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。

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/

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/

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

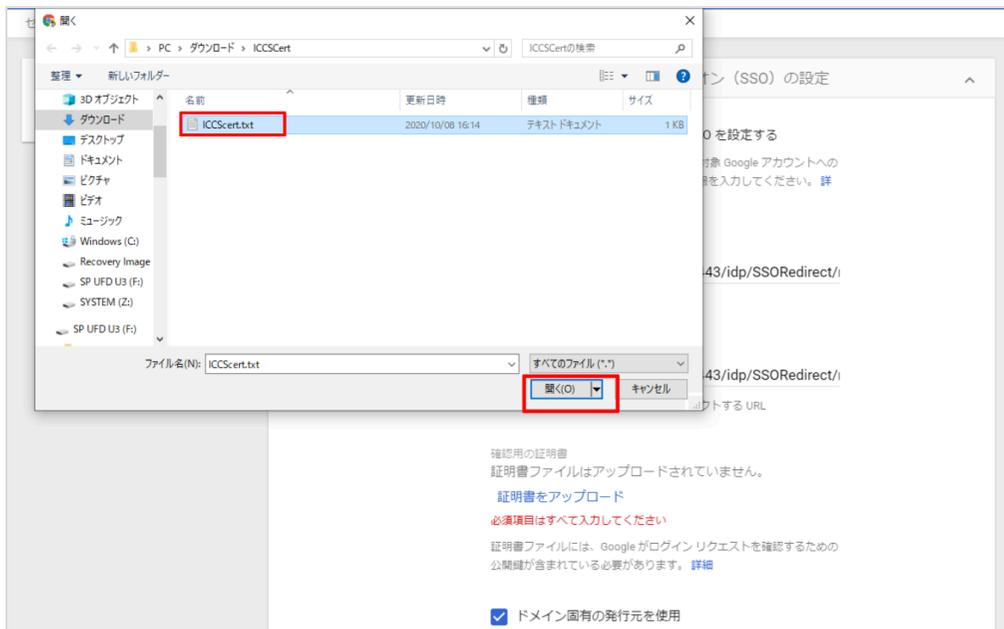
証明書ファイルには、Google がログイン リクエストを確認するための公開鍵が含まれている必要があります。 [詳細](#)

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](#)

15. システムの管理画面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。



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。

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：ユーザー別にポリシーを適用する

<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

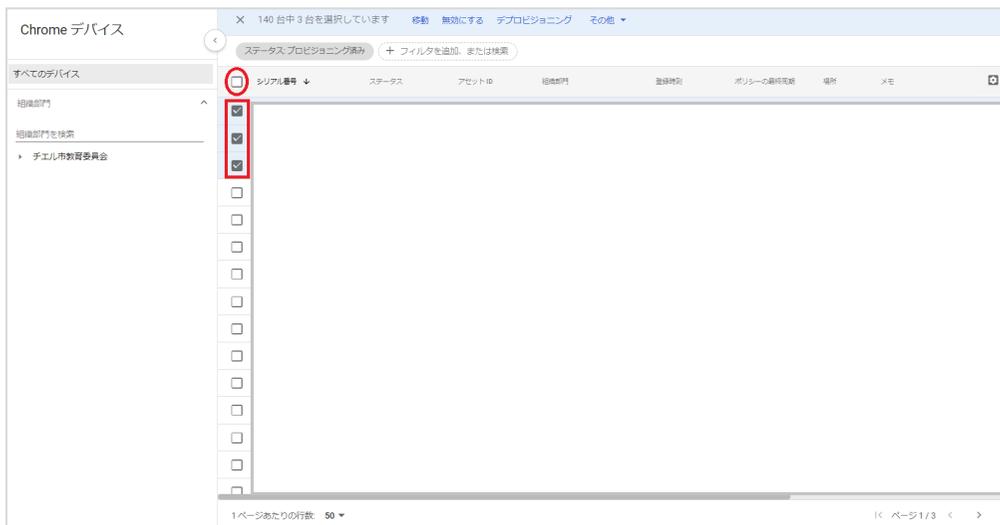
デバイスの組織部門を作成し、**Chrome**デバイスを登録する

※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. メニューからデバイス>**Chrome**>デバイスをクリックします。



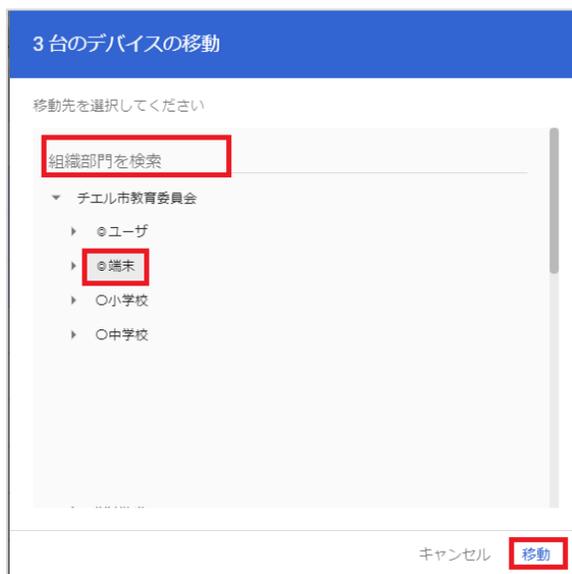
4. **Chrome**デバイスの一覧画面で**QR**コードログインを有効にする**Chrome**デバイスにチェックを入れ、選択します。



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。

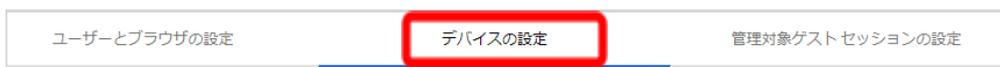
📍ポイント

設定は特権管理者が行います。

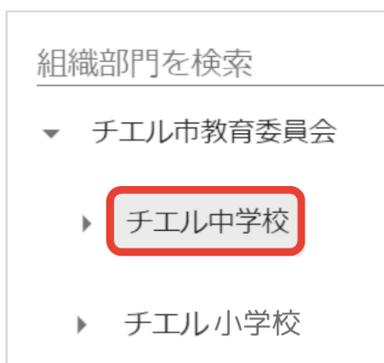
1. Chromeウェブブラウザで**Google 管理コンソール** (<https://admin.google.com/>)にアクセスします。
2. 特権管理者のアカウントでサインインします。
3. メニューからデバイス>**Chrome**>設定をクリックします。



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。



📌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。

6. ログイン設定の項目に移動し、vを開きます。



⚠️注意

一部のお客様環境では、画面が以下のように表示されることがございます。その際は手順7.から11.の各設定項目を選択して変更の上、設定項目ごとに「保存」をクリックして設定してください。（手順12.は不要となります。）

設定	設定	継承	サポート対象
ゲストモード	ゲストモードを許可する	ローカルに適用	📱 🖥️ 📄 iOS
ログインの制限	2件のサブ設定	Googleのデフォルト	📱 🖥️ 📄 iOS
ドメインのオートコンプリート	2件のサブ設定	ローカルに適用	📱 🖥️ 📄 iOS
ログイン画面	ユーザー名と写真を常に表示	ローカルに適用	📱 🖥️ 📄 iOS

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@ <input type="text" value="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. 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。

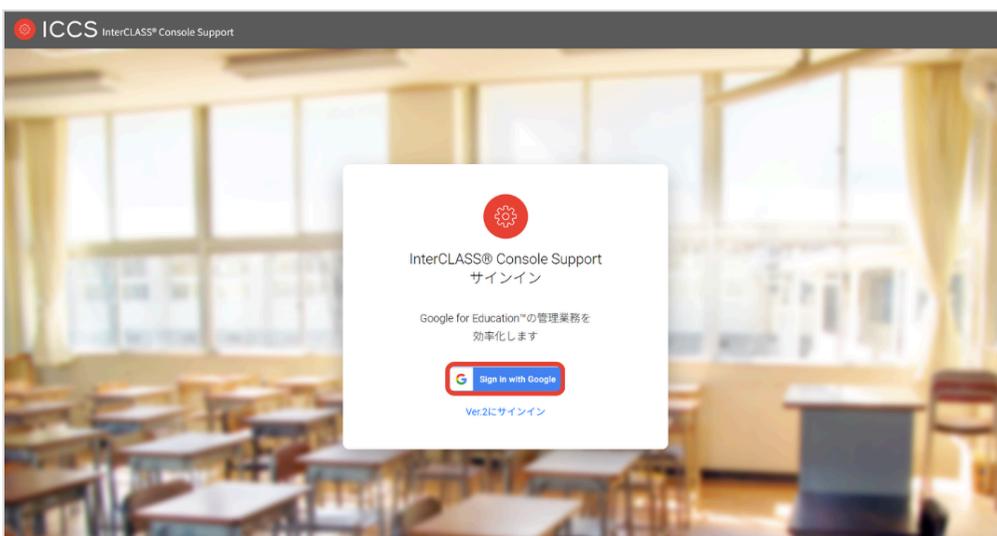


InterCLASS Console Supportの起動と終了

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

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**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、次へをクリックします。



4. パスワードを入力し、次へをクリックします。

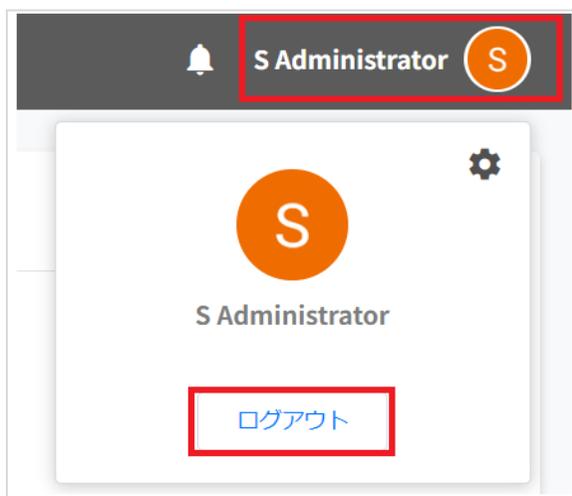


5. InterCLASS Console Supportのトップページが表示されます。



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。

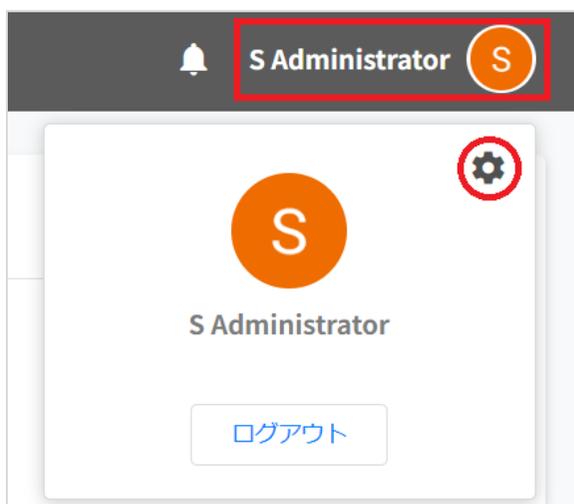


システム管理の設定

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. InterCLASS Console Supportのアカウント名をクリックし、歯車マークをクリックします。



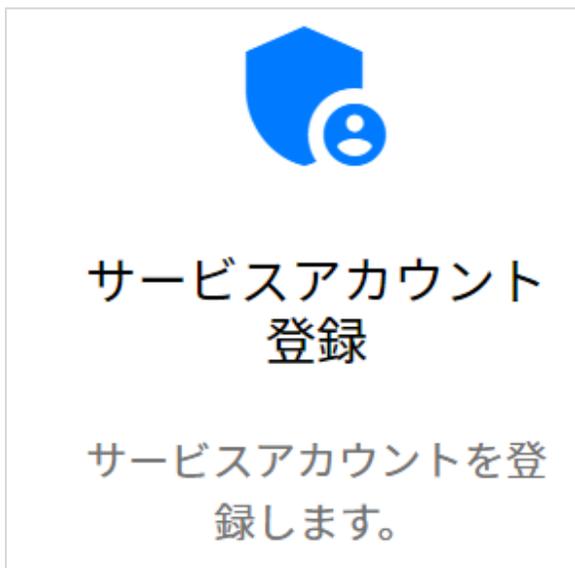
2. システム管理画面が開きます。



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画面をもう一度開きます。
7. 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

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。

1. 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**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**

📌ポイント

- ・移行実行中はQRコード利用状況の変更はできません。
- ・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をクリックして終了します。



④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。



④ポイント

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。



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 v3.5** 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、v3.5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

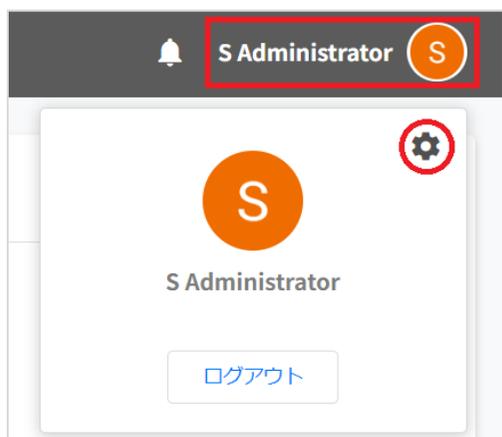
最新バージョンへの移行が完了していない場合、「お客様の組織は最新バージョンへの移行が完了していません。上記リンクからVer.2にサインインしてください。」とメッセージが表示されます。

作成済みの権限情報を移行する

1. InterCLASS Console Supportへアクセスし、**Sign in with Google**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。



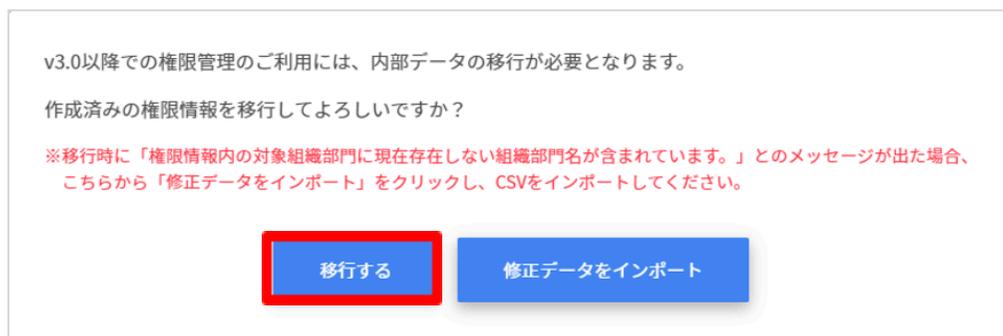
2. アカウント名をクリックし、歯車マークをクリックします。



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 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。

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. 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

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権限の変更は、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。内容を確認し、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権限の変更は、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 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 v3.5 操作マニュアル(設定編)

2024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 〒980-0013 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 〒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1-6-3 森ビル
TEL: (098)943-0511 FAX: (098)943-0669

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