

InterCLASS[®] Console Support

version 4.0 操作マニュアル(設定編)

目次

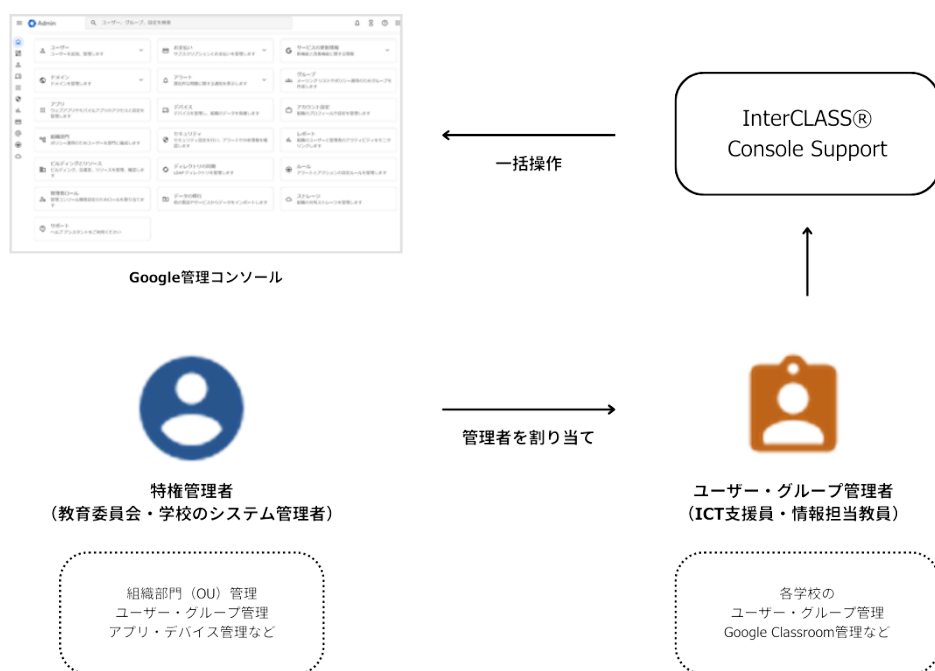
はじめに-----	3
InterCLASS® Console Supportの構成-----	3
動作環境-----	4
本書の構成と読み方-----	4
Google Cloud Platform の設定-----	5
Google Workspace でのGoogle Cloud Platform の有効化-----	5
Google Cloud Platform の設定-----	7
ドメイン全体の管理を委任する設定-----	24
Google Classroom のデータアクセスの許可-----	27
QRコードログインの設定-----	29
サードパーティのIDプロバイダを使用したシングルサインオンの設定-----	29
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-----	34
Chrome デバイスの設定の変更-----	37
Chromebook のログイン画面を確認-----	41
デバイスのレポート設定-----	42
InterCLASS® Console Supportの起動と終了-----	45
InterCLASS® Console Supportへログイン-----	45
InterCLASS® Console Supportからログアウト-----	47
システム管理の設定-----	48
システム管理を開く-----	48
サービスアカウント登録-----	49
QRコード情報移行-----	50
権限管理-----	52
権限管理の内部データを移行する-----	52
作成済みの権限情報を移行する-----	53
InterCLASS® Filtering Service連携設定-----	56
InterCLASS® Advance連携設定-----	59
製品間連携 実行結果-----	61
CHJeruサポートについて-----	63

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 10 Pro, Education, Enterprise(32bit版および64bit版) / 11 Pro, 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、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。

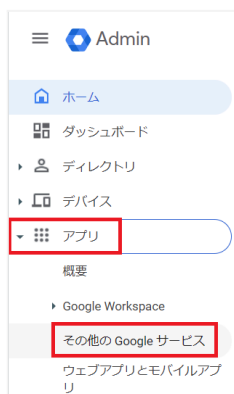
⚠️ 注意

- 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。

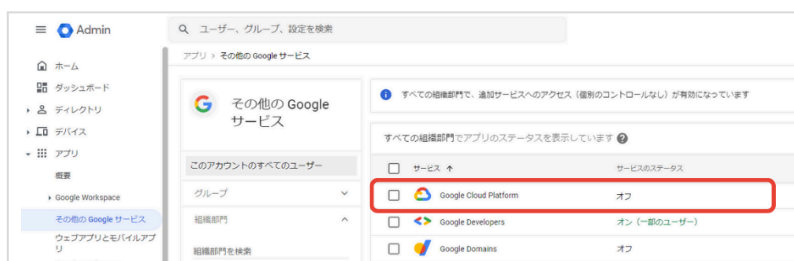
Google サービスへのアクセスを年齢で制御する
<https://support.google.com/a/answer/10651918>

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。



Google Cloud

チエ尔特権管理者へようこそ

Google Cloud のインスタンス、ディスク、ネットワークなどのリソースを 1 か所で作成し、管理します。

 チエ尔特権管理者
admin@chieru-edu.com [アカウントを切り替える](#)

国
日本

利用規約
☒ Google Cloud Platform の利用規約および適用されるサービスと API の利用規約に同意します。

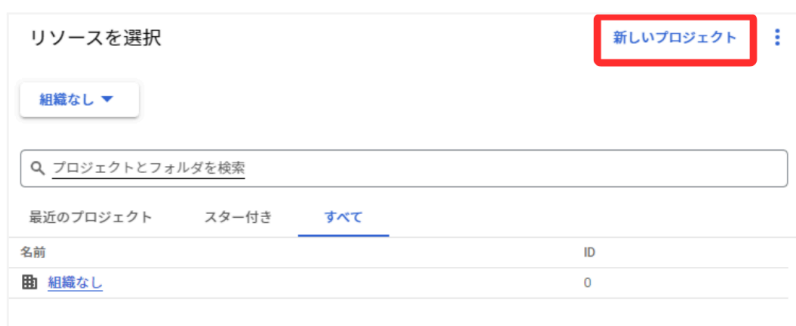
最新情報に関する通知メール
☒ Google Cloud や Google Cloud パートナーから、ニュース、プロダクトの更新情報、スペシャル オファーに関するメールを定期的に受信することを希望します。

[同意して続行](#)

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。



リソースを選択 [新しいプロジェクト](#)

組織なし

プロジェクトとフォルダを検索

最近のプロジェクト スター付き すべて

名前	ID
 組織なし	0

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。



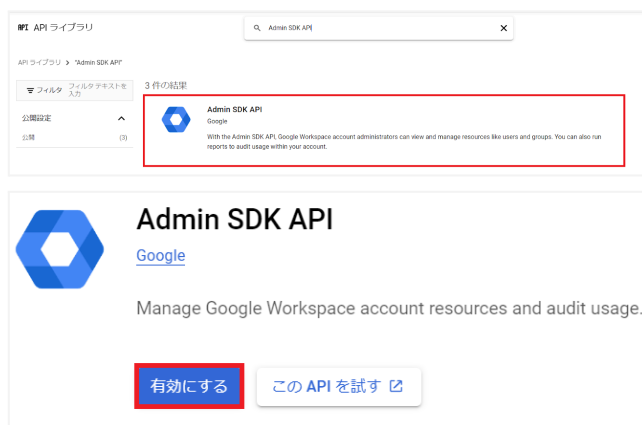
7. メニューからAPI とサービス>ライブラリをクリックします。



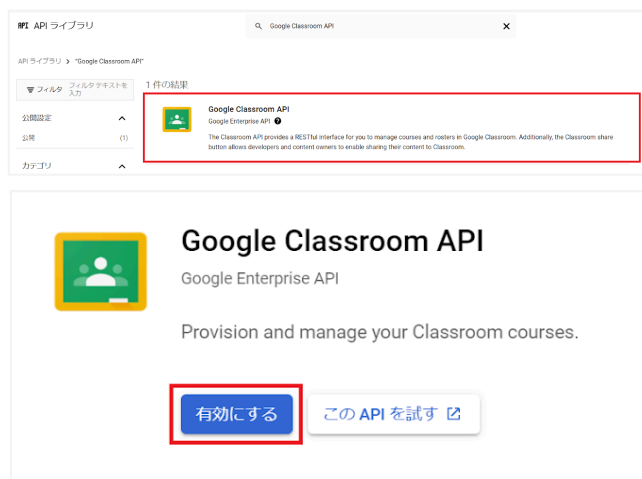
8. API ライブラリ画面のAPI とサービスの検索ボックスに「Admin SDK API」と入力します。



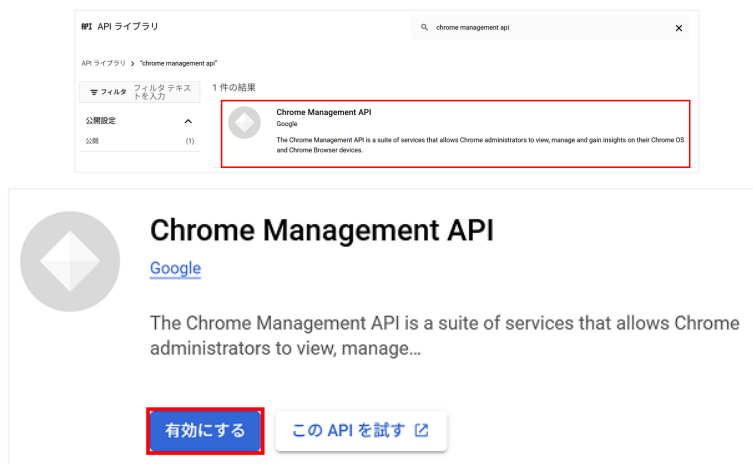
9. 検索結果に表示されたAdmin SDK API をクリックし、有効にするボタンをクリックします。



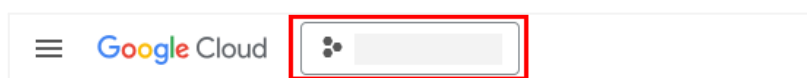
10. 手順8.9と同じ操作で「Google Classroom API」を検索し、有効にするボタンをクリックします。



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



12.ヘッダーのプルダウンリストをクリックします。



13.リソースを選択ダイアログから組織のドメイン名をクリックします。組織のドメイン名が表示されていない場合、項番18.に進んでください。



14.メニュー>IAM と管理>IAM 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

☐ タイプ	プリンシパル ↑	名前	ロール
☐ 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「**組織の管理者**」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 (省略可) ⓘ

≡ フィルタ 組織の管理者 X

組織の管理者
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。

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。

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: **組織の管理者** 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

- 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。

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: **組織の管理者** 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。

フィルタ: **組織ポリシー管理者** X

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。

[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。

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: **組織の管理者** 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。

ロール: **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 ① [キャンセル](#)

- i. アクセス権を許可をクリックします。

プリンシパル別に表示 ロール別に表示

+ 人を許可 - 人をアクセス権を削除

≡ フィルタ プロパティ名または値を入力

- 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。

プリンシパルの追加

プリンシパルは、ユーザー、グループ、ドメイン、またはサービス アカウントです。
[IAM のプリンシパルの詳細](#)

新しいプリンシパル *

① プリンシパルを少なくとも1つ入力してください

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](#)

ロールを選択 *

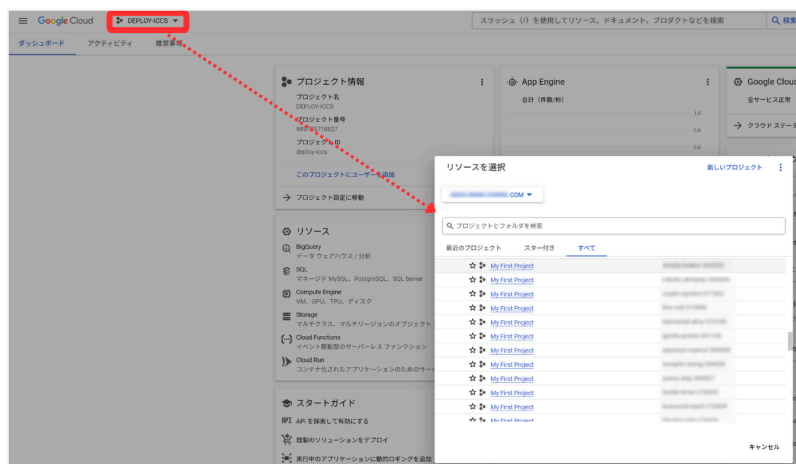
別のロールを追加

IAM の条件 (省略可) ②
+ IAM の条件を追加

保存

キャンセル

13. 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。



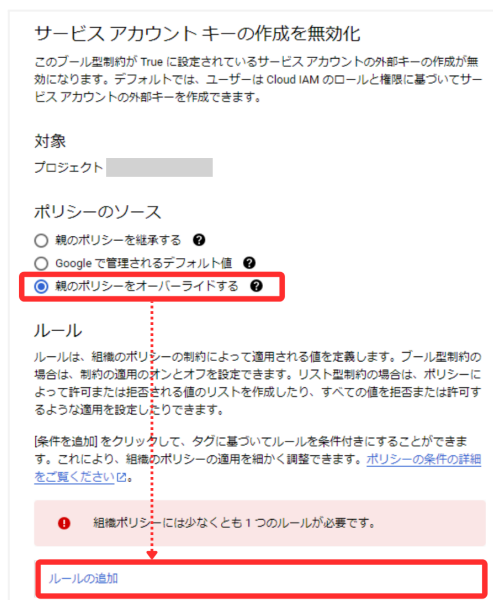
14. メニュー> IAM と管理>組織のポリシーへ移動します。



15. 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**Disable service account key creation**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。



16. 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の追加を押下します。



- 17.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。



18. 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。



19. 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。

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

20. 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)



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

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

21. 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。



IAM と管理

サービス アカウント + サービスアカウントを作成 削除 アksesを管理 更新

プロジェクト「My Project 16325」のサービス アカウント

サービス アカウントは Google Cloud サービス ID (Compute Engine VM、App Engine アプリ、Google 以外で実行されているシステムなど) 組織のポリシーを使用してサービス アカウントを保護できます。IAM ロールの自動付与、鍵の作成やアップロード、サービス アカウントのポリシーの詳細をご覧ください。

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

22. 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。

The screenshot shows the Google Workspace OAuth client setup interface. On the left, under 'サービス アカウントの詳細' (Service Account Details), the '詳細設定' (Detailed Settings) option is highlighted with a red box. The main content area, titled 'ドメイン全体の委任' (Domain-wide delegation), contains a warning about domain-wide delegation and a '構成' (Configure) button, which is also highlighted with a red box.

23. OAuth 同意画面のUser Type で内部を選択し、作成ボタンをクリックします。

The screenshot shows the 'OAuth 同意画面' (OAuth Consent Screen) configuration page. Under the 'User Type' section, the '内部' (Internal) radio button is selected and highlighted with a red box. At the bottom of the page, the '作成' (Create) button is highlighted with a red box.

24. 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、保存して次へボタンをクリックします。

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連して問い合わせるのに使用

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、プロジェクトの歴史について 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

25. 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

OAuth 同意画面 — スコープ — 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

26. 概要画面でダッシュボードに戻るボタンをクリックします。

アプリ登録の編集

OAuth 同意画面 — スコープ — 概要

OAuth 同意画面 [編集](#)

ユーザーの種類

内部

アプリ名

ICONS

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](#)

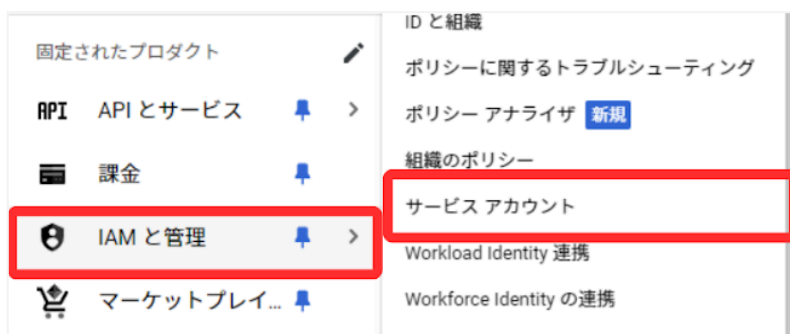
API ↑	範囲	ユーザー向けの説明
表示する行がありません		

[ダッシュボードに戻る](#)

27. OAuth 同意画面が表示されたら、操作は終了です。



28. 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。



29. 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。



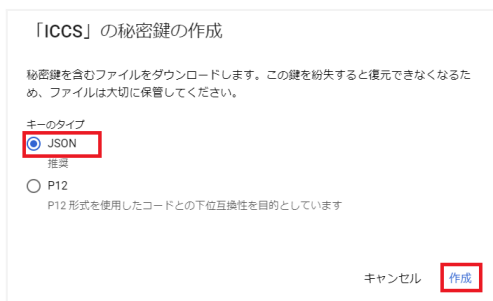
⚠️ 注意

- 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。

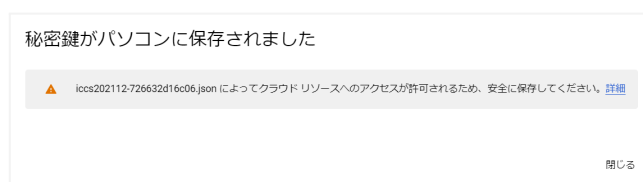
30. キータブの鍵を追加>新しい鍵を作成をクリックします。



31. 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。



32. JSON 形式の秘密鍵がダウンロードされます。

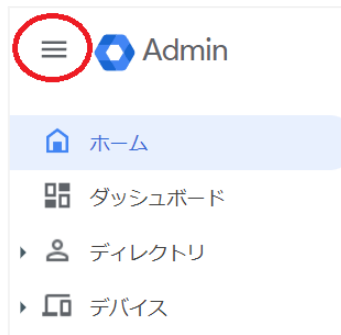


注意

- 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,  
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

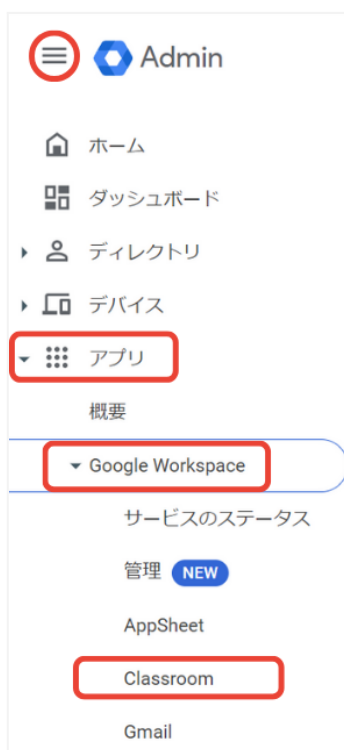
☐ 既存のクライアント ID を上書きする ⓘ

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

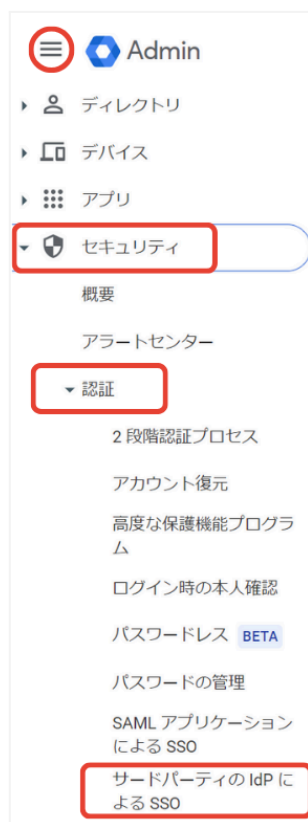
QRコードを使ったChromebook へのログイン機能を有効にする場合は、Google 管理コンソールで以下の設定を適用します。

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
チエル株式会社	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](#)

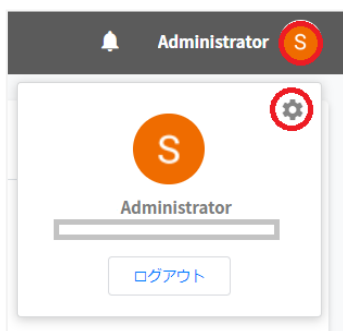
9. 保存をクリックします。

⚠ 注意

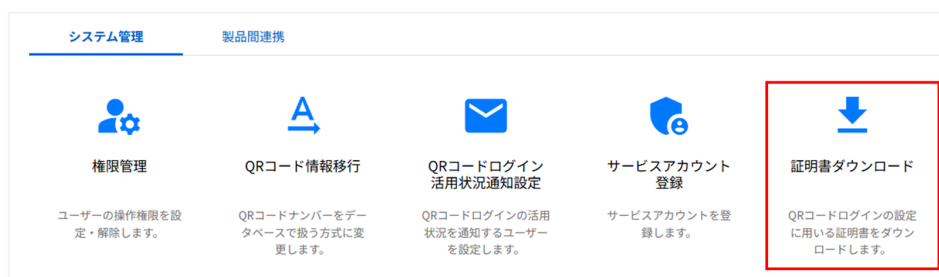
- 証明書ファイルの登録が必要な場合、Google 管理コンソールで証明書ファイルを登録します。証明書を求められる場合、次の手順で、InterCLASS® Console Support から証明書を取得します。

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. アカウント名をクリックし、歯車アイコンをクリックします。



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。

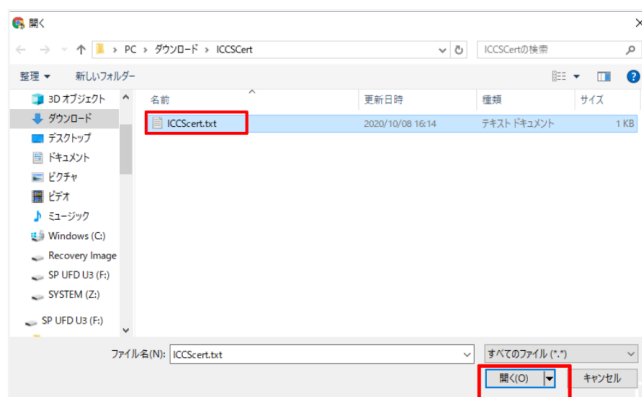


13. ICCSCert.zipがダウンロードされます。

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。

⚠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

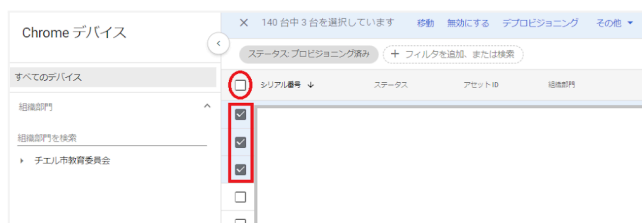
デバイスの組織部門を作成し、
Chromeデバイスを登録する

※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。

3台のデバイスの移動

移動先を選択してください

組織部門を検索

▼ チエル市教育委員会

- ▶ ユーザ
- ▶ 端末
- ▶ 小学校
- ▶ 中学校

キャンセル 移動

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。

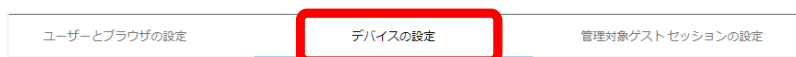
⚠ 注意

- 本設定は、特権管理者アカウントで実施してください。

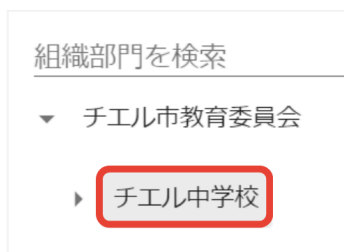
8. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com/>) にアクセスします。
9. 特権管理者のアカウントでサインインします。
10. メニュー > デバイス > Chrome > 設定をクリックします。



11. デバイスの設定タブを選択します。



12. 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。



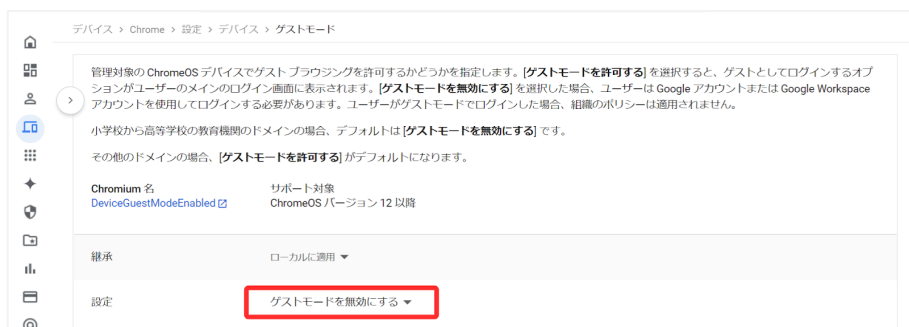
⑨ポイント

- 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。

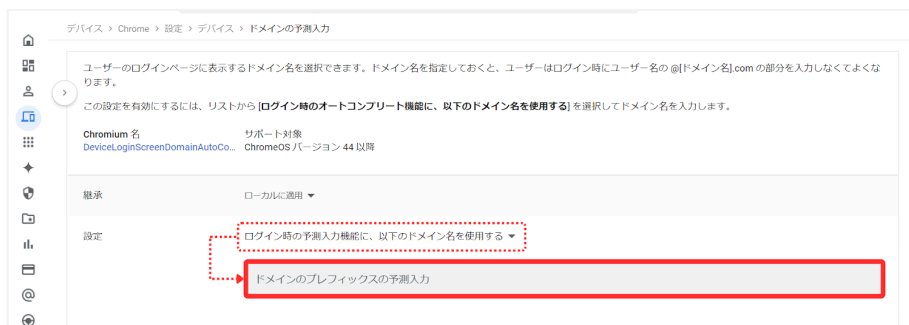
13. ログイン設定の項目に移動します。



14. 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。



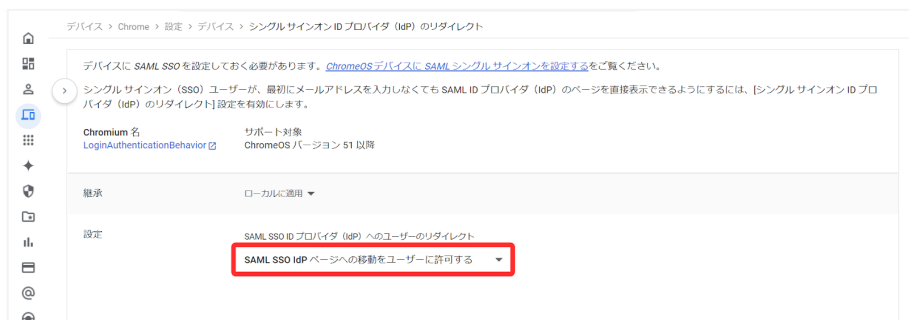
15. ドメインの予測入力の設定をログイン時のオートコンプリート機能に、以下のドメイン名を使用するに変更し、ドメインのプレフィックスの予測入力にお客様のドメイン名を入力します。



16. 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。



17. 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。



18. カメラへのシングルサインオンアクセスが可能なURL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。

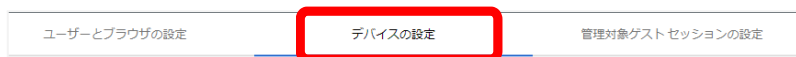
1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com>)にアクセスします。
2. 特権管理者のアカウントでサインインします。
3. メインメニューをクリックします。



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。



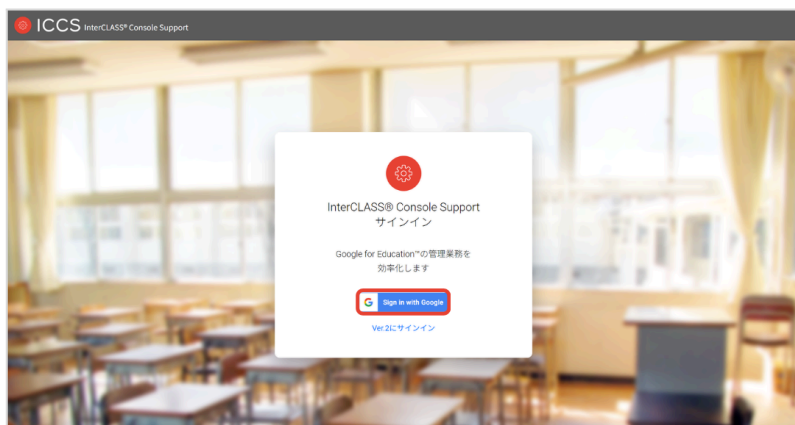
A dialog box with a light gray border. Inside, there are two buttons. The first button is blue with the white text '保存' (Save). It is highlighted with a red rectangular border. The second button is white with the gray text 'キャンセル' (Cancel).

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

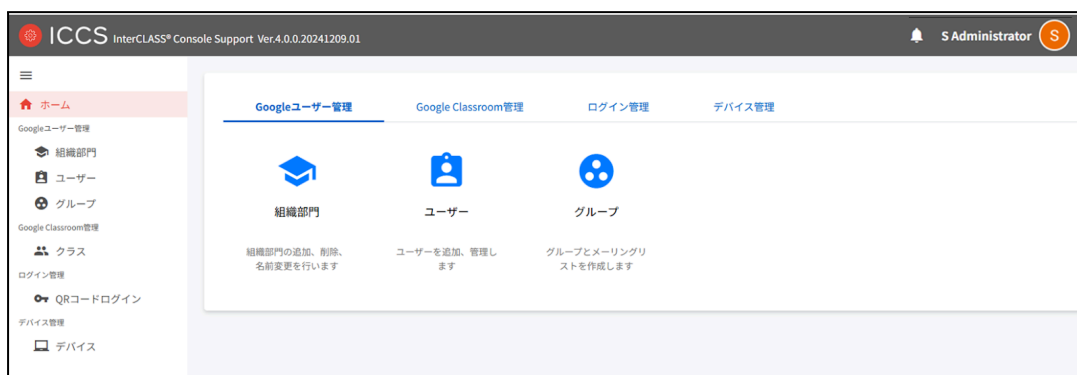
パスワードを表示します

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

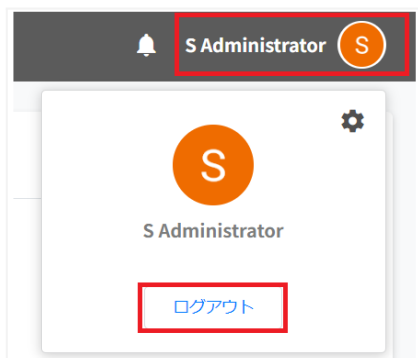
次へ

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



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。

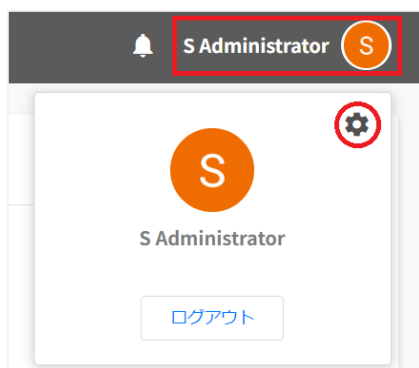


システム管理の設定

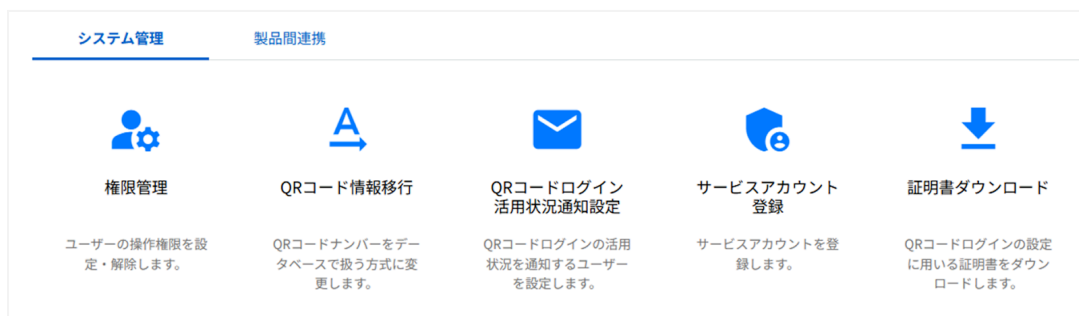
InterCLASS® Console Supportのシステム管理は特権管理者としてログインし、システム管理のため初期設定を行います。システム管理では、権限管理、QRコード情報移行、QRコードログイン活用状況通知設定、サービスアカウント登録、証明書ダウンロードが行えます。

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、設定アイコンをクリックします。



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:

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:

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。



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： 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

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。

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、v4.0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。

作成済みの権限情報を移行する

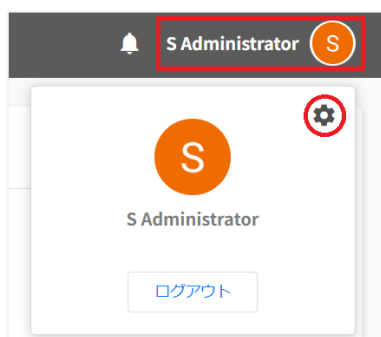
⚠ 注意

- 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. アカウント名をクリックし、**歯車アイコン**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。

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。

権限情報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 列に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

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。

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)

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

⑨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、**新規追加時の自動同期設定**により、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。

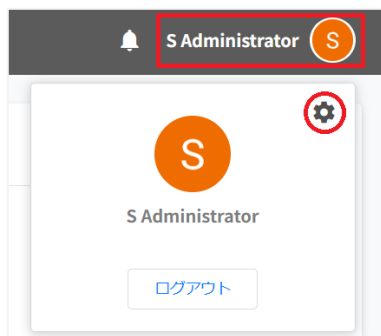
⚠️注意

- 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. アカウント名をクリックし、**歯車アイコン**をクリックします。



3. システム管理画面が開きます。製品間連携タブに切り替え、InterCLASS® Filtering Service連携設定をクリックします。



4. 夜間定期同期のオン／オフを設定します。

夜間定期同期 ☐ オフ ☒ オン

⑨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。

5. 新規追加時の自動同期の動作を設定します。

The screenshot shows a settings interface with a label '操作時の自動同期' (Automatic Sync during operation). A dropdown menu is open, displaying four options: '追加／削除時にユーザーが選択して同期する' (Sync when user selects during add/delete), '同期しない' (Do not sync), '追加／削除時に自動で同期する' (Sync automatically during add/delete), and '追加／削除時にユーザーが選択して同期する' (Sync when user selects during add/delete). The last option is highlighted in blue.

⑨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、ドメイン管理者または、権限管理画面で対象組織部門に最上位の組織部門を設定したユーザーのみとなります。

6. 保存ボタンをクリックします。

The screenshot shows a dialog box with two buttons: 'キャンセル' (Cancel) and '保存' (Save). The '保存' button is highlighted with a red border.

InterCLASS® Advance連携設定

InterCLASS® Advanceとの連携内容を設定します。

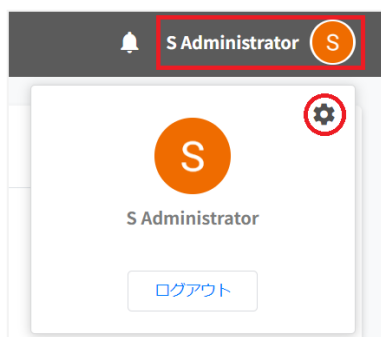
⚠ 注意

- 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。

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. アカウント名をクリックし、歯車アイコンをクリックします。



3. システム管理画面が開きます。製品間連携タブに切り替え、InterCLASS® Advance連携設定をクリックします。



4. 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	78
連携先の組織名	検証用_ICA_
※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。	
手動同期	利用する
キャンセル 保存	

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、ドメイン管理者または、権限管理画面で対象組織部門に最上位の組織部門を設定した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。

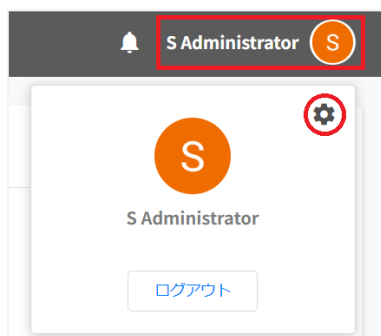
注意

- 本画面は、特権管理者アカウントでのみ確認可能です。

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。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、**歯車アイコン**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

表示 10 件

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	内容	エラー
2025/01/03 00:00:08	2025/01/03 00:00:22	正常終了	InterCLASS Filtering Service	夜間定期同期	
2025/01/02 00:00:08	2025/01/02 00:00:21	正常終了	InterCLASS Filtering Service	夜間定期同期	
2025/01/01 00:00:08	2025/01/01 00:00:21	正常終了	InterCLASS Filtering Service	夜間定期同期	
2024/12/31 00:00:08	2024/12/31 00:00:21	正常終了	InterCLASS Filtering Service	夜間定期同期	
2024/12/30 00:00:08	2024/12/30 00:00:21	正常終了	InterCLASS Filtering Service	夜間定期同期	
2024/12/29 00:00:07	2024/12/29 00:00:20	正常終了	InterCLASS Filtering Service	夜間定期同期	
2024/12/28 16:36:17	2024/12/28 16:36:25	正常終了	InterCLASS Filtering Service	夜間定期同期	
2024/12/28 16:28:38	2024/12/28 16:28:47	正常終了	InterCLASS Filtering Service	自動同期	
2024/12/28 16:17:54	2024/12/28 16:18:06	正常終了	InterCLASS Filtering Service	自動同期	
2024/12/28 16:03:13	2024/12/28 16:03:19	中止	InterCLASS Filtering Service	自動同期	UNEXPECTED_ERROR

106 件中 31 件から 40 件まで表示

前へ 1 2 3 4 5 ... 11 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 version4.0 操作マニュアル 設定編

2025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、2024年8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 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一丁目6番3号 森ビル
TEL: (098)943-0511 FAX: (098)943-0669

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