CHleru

InterCLASS® Console Support

version 4.0 操作マニュアル（設定編）

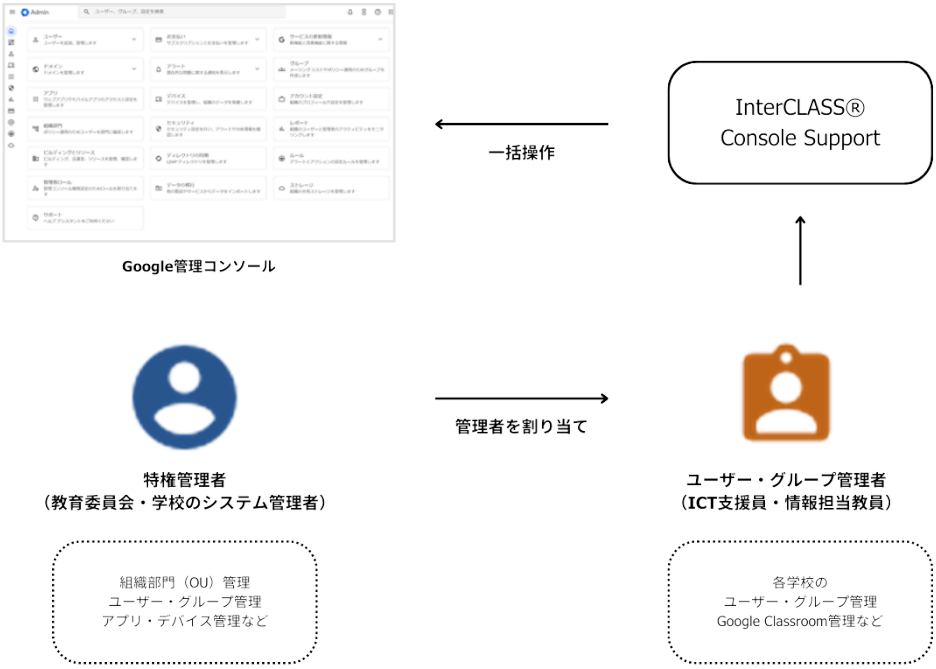
目次

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。

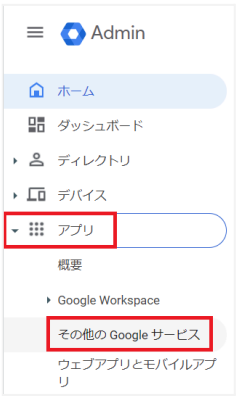
⚠注意

- 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。

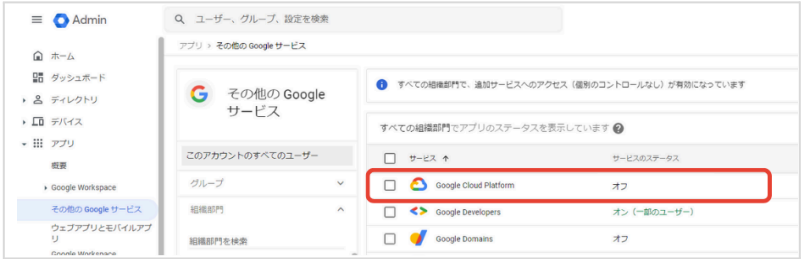
  Google サービスへのアクセスを年齢で制御する
  https://support.google.com/a/answer/10651918

Google Workspace でのGoogle Cloud Platform の有効化

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**画面で**サービスのステータス**をクリックします。

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

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

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

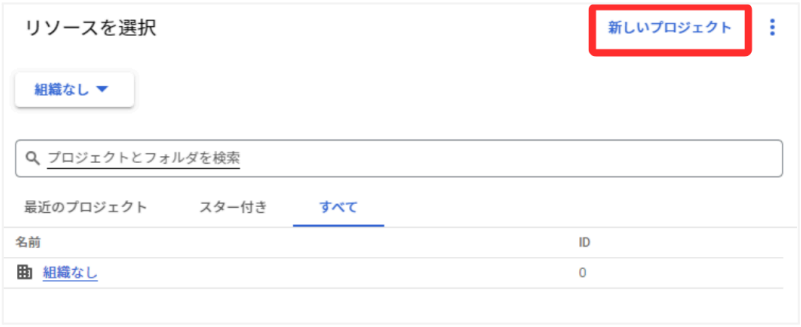
Google Cloud Platform の設定

1. Chrome ウェブブラウザでGoogle Cloud Platform (https://console.cloud.google.com)にアクセスします。

2. 初回アクセスの場合以下のような画面が表示されます。利用規約にチェックをいれ、**同意して続行**をクリックします。

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

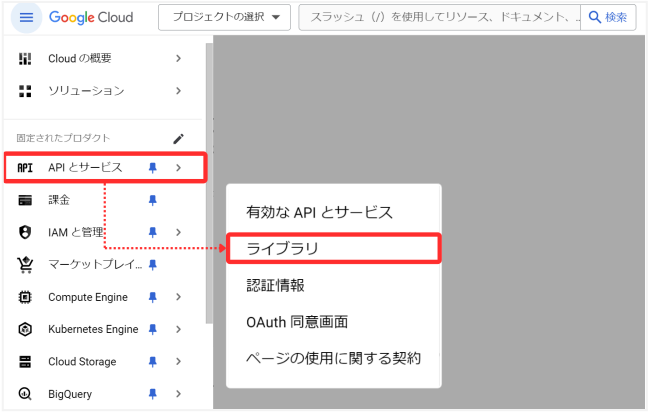
4. **リソースを選択**ダイアログの**新しいプロジェクト**をクリックします。



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

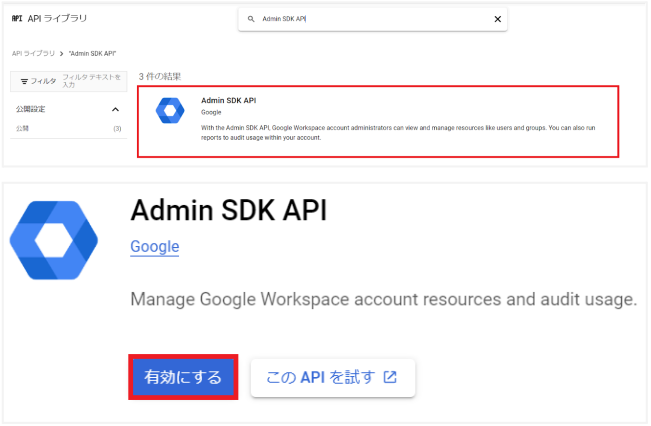
6. プロジェクトの作成が終了すると以下のような通知が届きます。**プロジェクトを選択**をクリックし、プロジェクトのダッシュボードに移動します。

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。

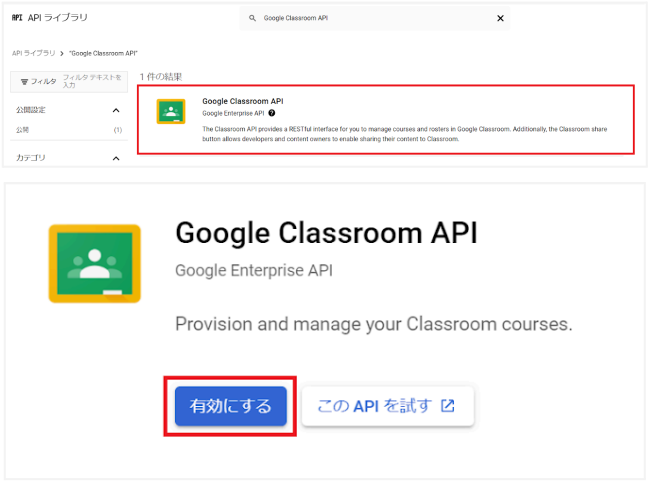


8. **API ライブラリ**画面の**API とサービスの検索ボックス**に「Admin SDK API」と入力します。

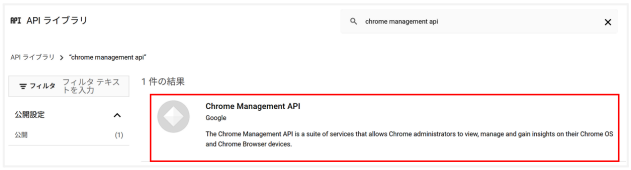
9. 検索結果に表示された**Admin SDK API** をクリックし、**有効にする**ボタンをクリックします。

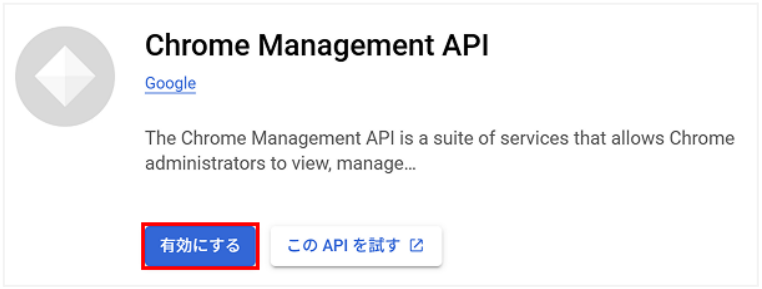


10. 手順8.9と同じ操作で「**Google Classroom API**」を検索し、**有効にする**ボタンをクリックします。



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

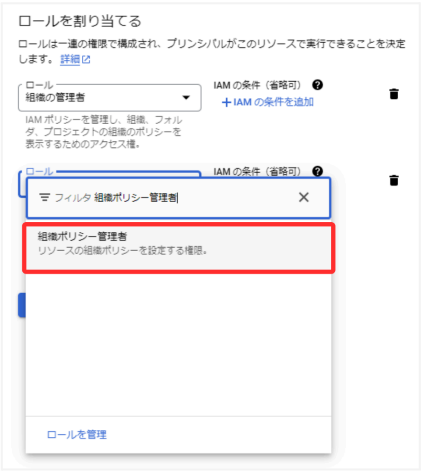
i. **編集**アイコンをクリックし、ロールを割り当てる画面を開きます。

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。

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。

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。

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。



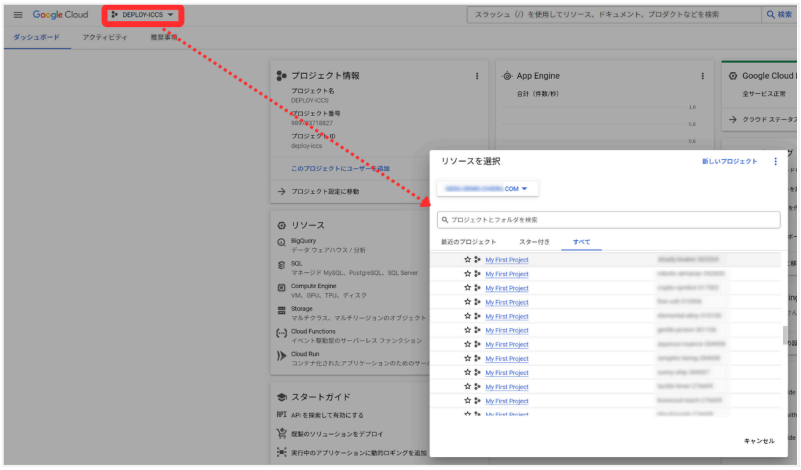
vi. **2つのロールが割り当てられていることを確認し、保存**ボタンをクリックします。

b. 管理者となるユーザーが存在しない場合

i. **アクセス権を許可**をクリックします。

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

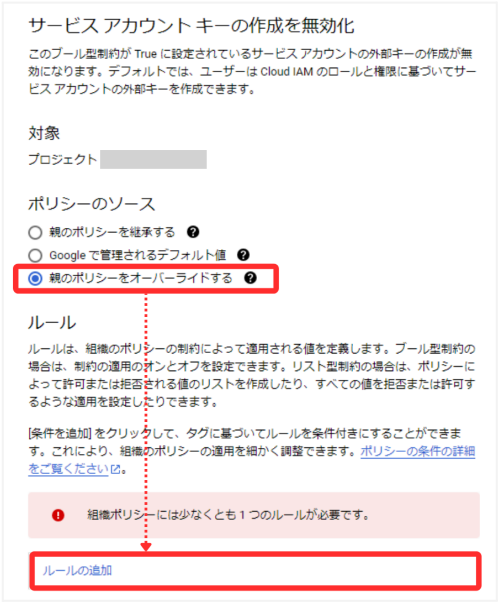
13. **ヘッダーのプルダウンリスト**をクリックし、**リソースを選択**ダイアログでサービスアカウントを発行するプロジェクトを選択します。



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。

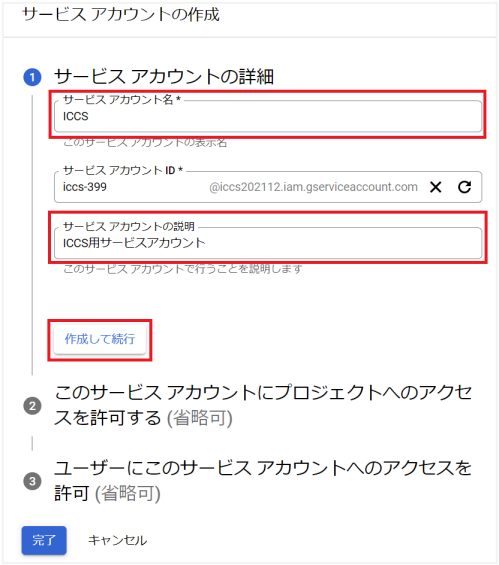
16. **ポリシーのソース**を**親のポリシーをオーバーライドする**に変更し、下に表示される**ルールの追加**を押下します。



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。

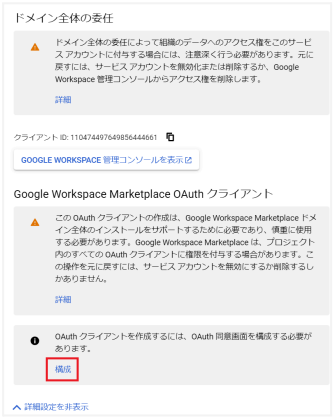
19. **サービスアカウントの作成**画面の**サービスアカウントの詳細**で任意の**サービス アカウント名**と**サービス アカウントの説明**を入力し、**作成して続行**ボタンをクリックします。



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)

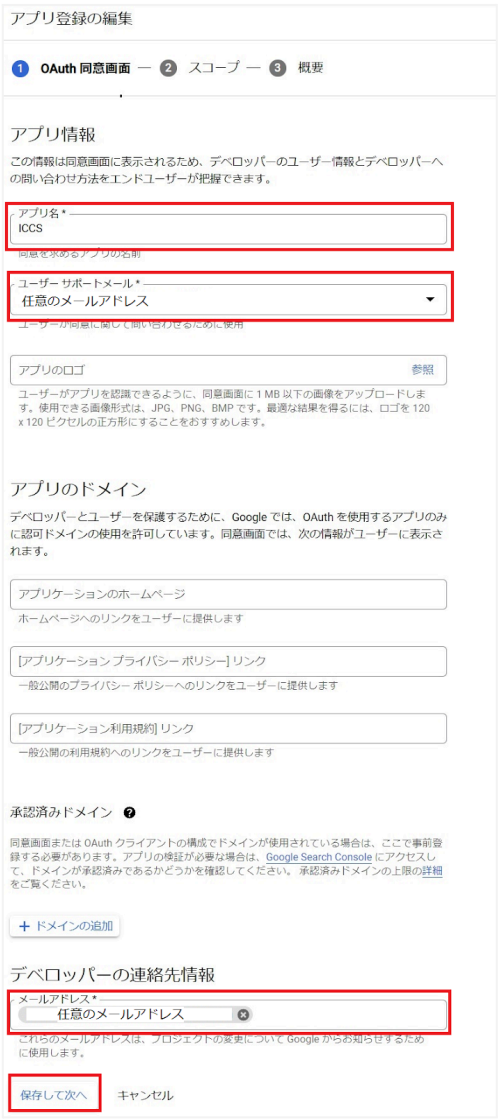
21. **サービスアカウント**画面から作成したサービス アカウントのメールの**メールアドレス**をクリックし、設定画面へ移動します。

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。



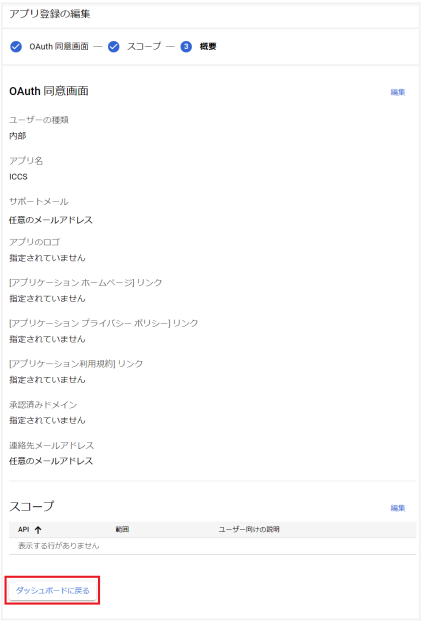
23. **OAuth 同意**画面のUser Type で**内部**を選択し、**作成**ボタンをクリックします。

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。



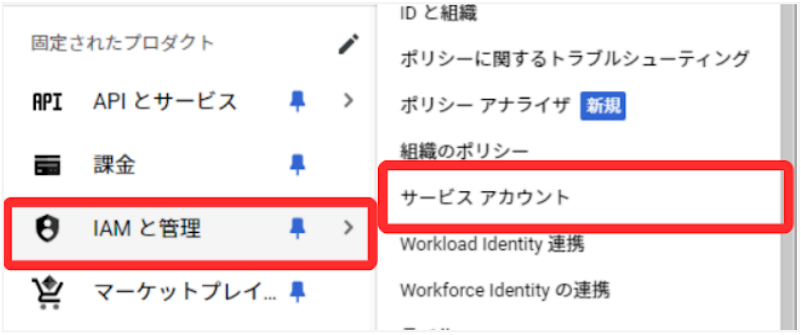
25. **スコープ画面で保存して次へ**をクリックします。

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。



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。



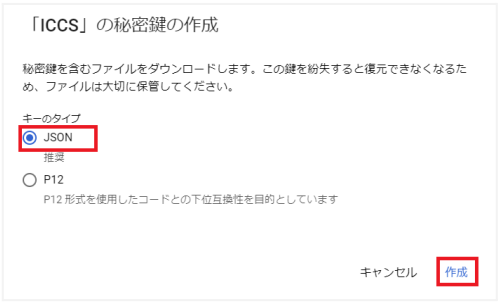
29. **サービスアカウント**画面の**OAuth2クライアントID** から操作を選び、**鍵を管理**をクリックします。

⚠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

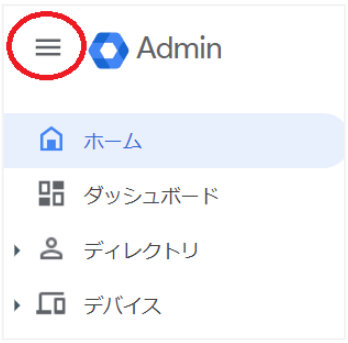
- **生成された秘密鍵は、InterCLASS® Console Supportの秘密鍵を初回ログイン時に登録していただくため、厳重に保管してください。**
- 同じ鍵は、1度しかダウンロードできません。紛失した場合は、再作成する必要があります。

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。

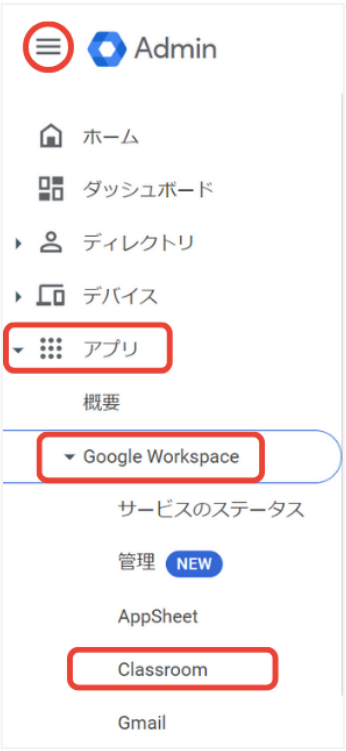
■必要なスコープの一覧

```
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。

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。**

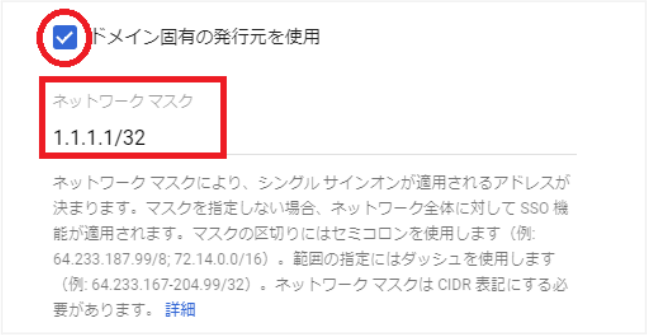
5. **SAML プロファイルを追加**をクリックします。

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

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。



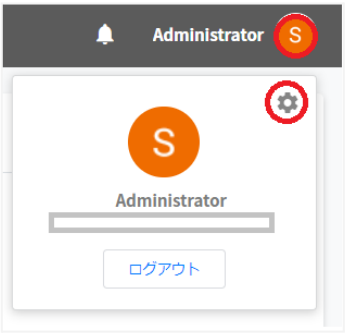
9. **保存**をクリックします。

⚠注意

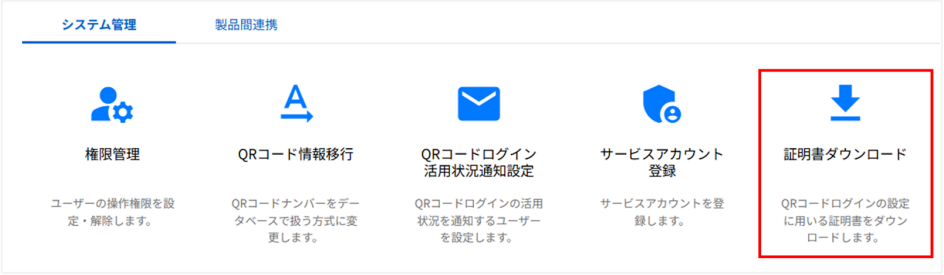
- 証明書ファイルの登録が必要な場合、Google 管理コンソールで証明書ファイルを登録します。証明書を求められる場合、次の手順で、InterCLASS® Console Supportから証明書を取得します。

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。



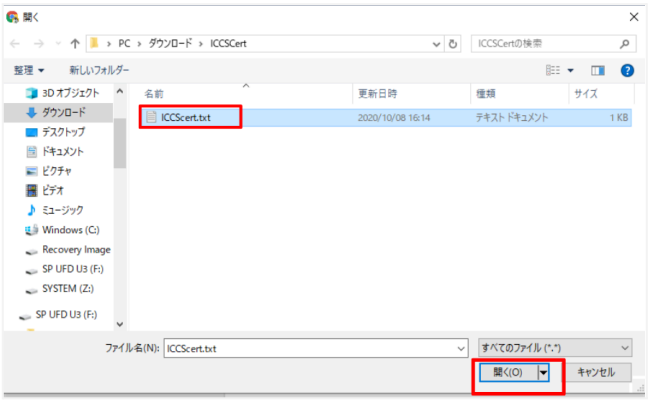
12. **システム管理**画面で**証明書ダウンロード**をクリックします。



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**ICCSCert.zip**ファイルを事前に展開しておき、**ICCScert.txt**を選択し、開きます。



16. 証明書がアップロードされると下記の表示になります。

17. 未保存の変更の表示で**保存**をクリックします。

QRコードログインを適用するChrome デバイスを特定の組織部門に移動

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

⚠注意

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

ポイント

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

（組織部門の作成例）

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

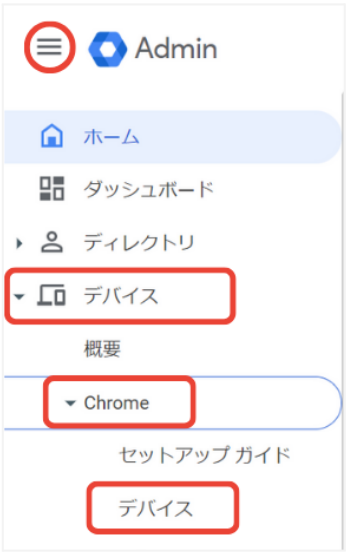
デバイスの組織部門を作成し、Chromeデバイスを登録する

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

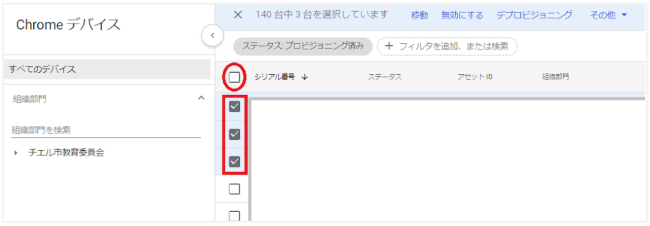
1. Chrome ウェブブラウザでGoogle 管理コンソール（https://admin.google.com/）にアクセスします。

2. 特権管理者のアカウントでサインインします。

3. **メニュー＞デバイス＞Chrome ＞デバイス**をクリックします。



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



5. 操作コマンドの**移動**をクリックします。

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

7. 選択したデバイスが移動先の組織部門に移動します。

Chrome デバイスの設定の変更

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

⚠注意

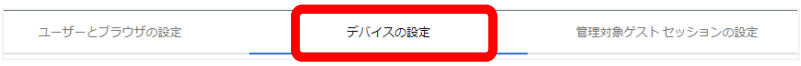
- 本設定は、特権管理者アカウントで実施してください。

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。

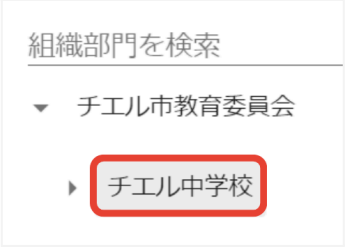
9. **特権管理者のアカウント**でサインインします。

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。



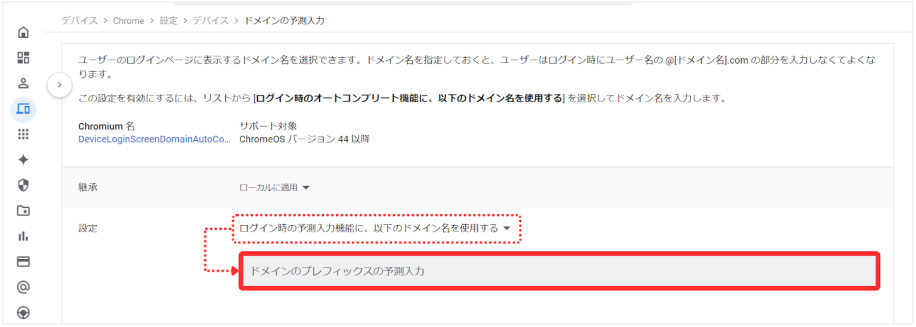
ポイント

- 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。



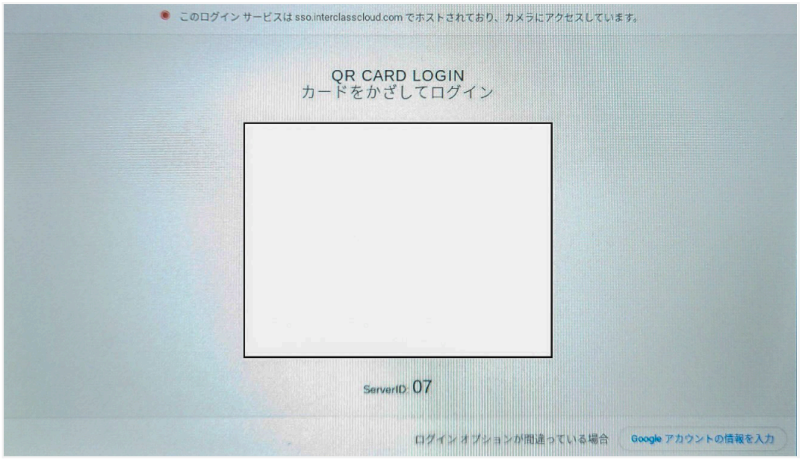
16. **ログイン画面**の設定を**ユーザー名と写真を表示しない**に変更します。

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

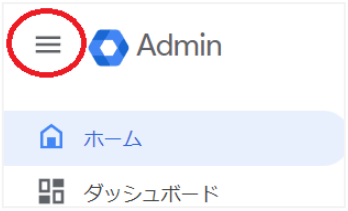
上記の設定が全て正常に適用されると、対象のChromebook の**ログイン**画面が変更され、QRコードを使用したChromebook へのログインができるようになります。
ログイン画面は以下のように変わります。



デバイスのレポート設定

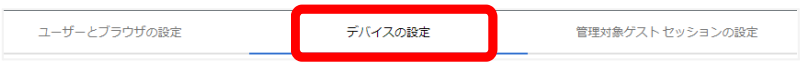
デバイス管理画面でバッテリー状態とネットワークレポートの表示を行う場合は、Google 管理コンソールで以下の設定を適用します。

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。

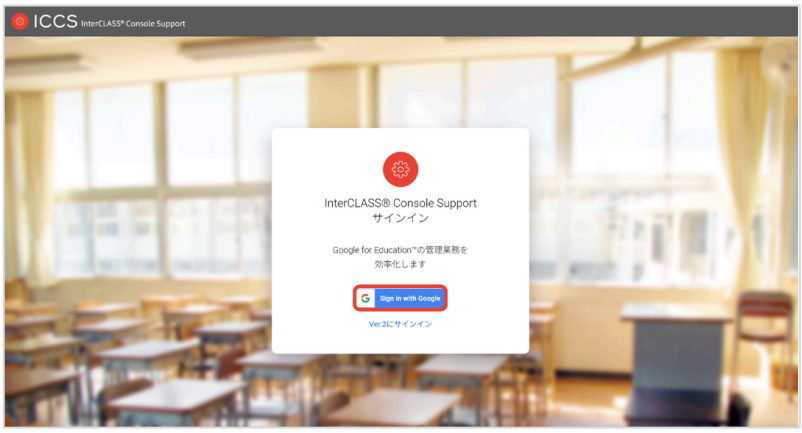
InterCLASS® Console Supportの起動と終了

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

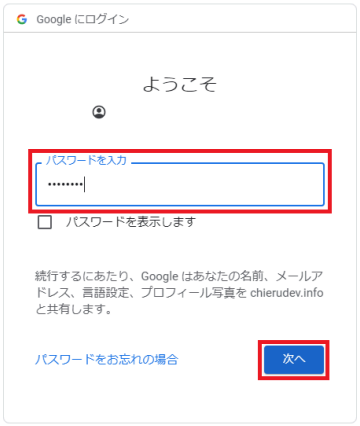
1. Chrome ウェブブラウザで新しいタブを開き、InterCLASS® Console Support(https://cs.interclass.jp/)にアクセスします。

2. **Sign in with Google** ボタンをクリックします。

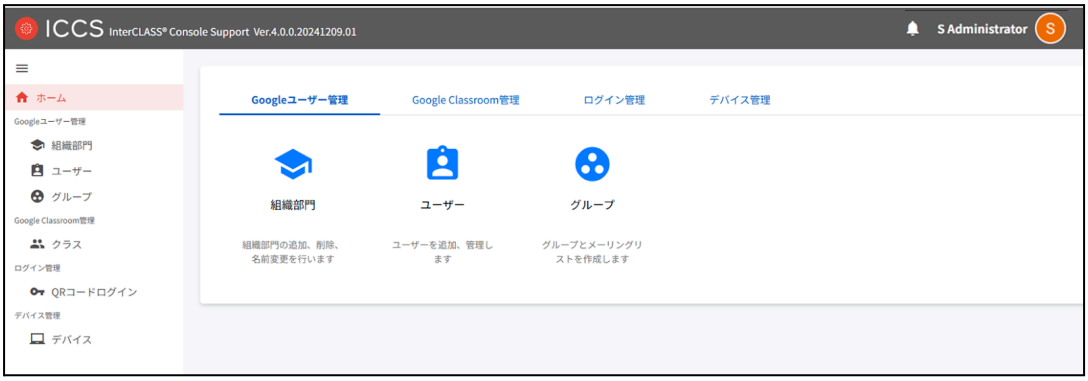


3. **Google にログイン**画面が表示されます。**管理者のメールアドレス**を入力し、**次へ**ボタンをクリックします。

4. **パスワード**を入力し、**次へ**ボタンをクリックします。

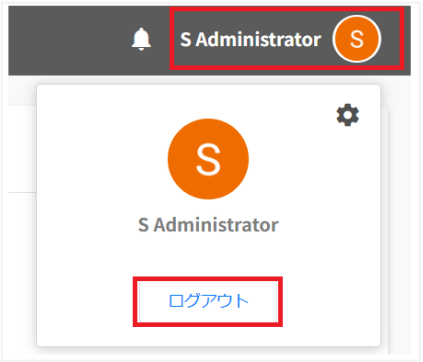


5. InterCLASS® Console Supportのトップページが表示されます。



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。

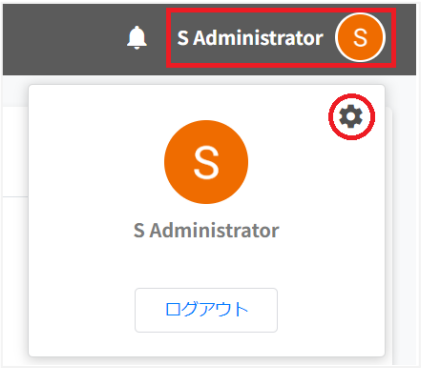


システム管理の設定

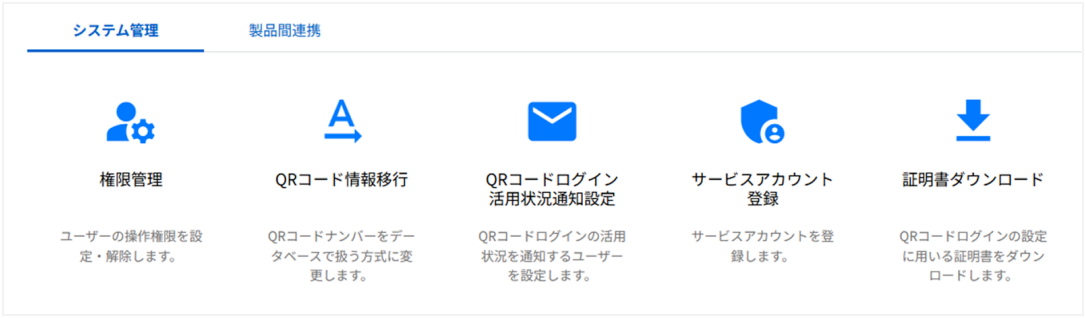
InterCLASS® Console Supportのシステム管理は特権管理者としてログインし、システム管理のため初期設定を行います。システム管理では、権限管理、QRコード情報移行、QRコードログイン活用状況通知設定、サービスアカウント登録、証明書ダウンロードが行えます。

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。

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。

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。

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。

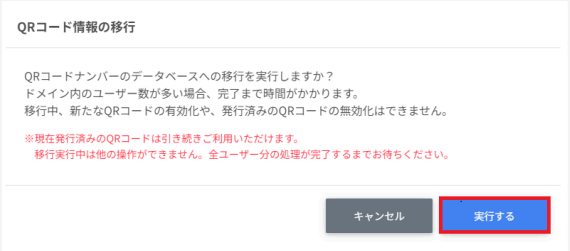
7. **サービスアカウント登録**画面の**登録状態**が**登録済み**になっていることを確認してください。

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。



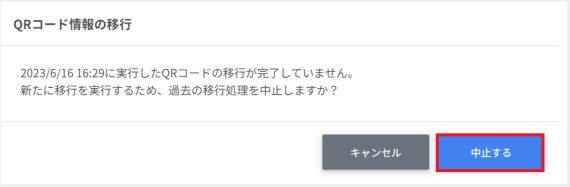
⚠注意

- 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。

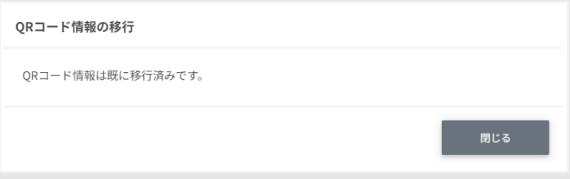
3. **QRコードナンバーの移行が完了しました。**と表示されたら**閉じる**ボタンをクリックして終了します。

🔍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。



- 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 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おりません。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。

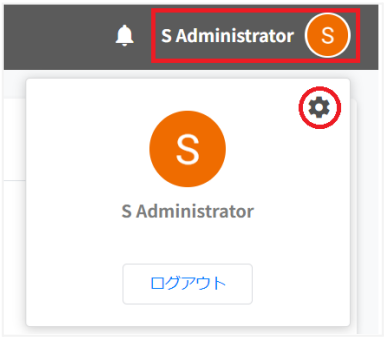
作成済みの権限情報を移行する

⚠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。

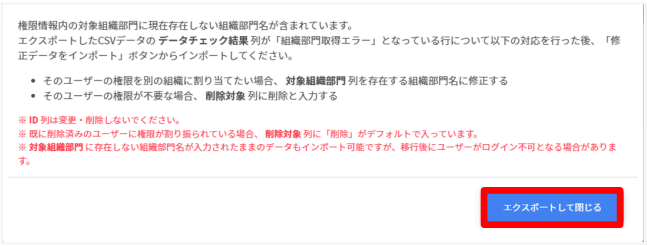
2. **アカウント名**をクリックし、**歯車**アイコンをクリックします。



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。

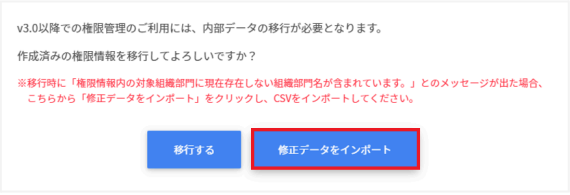
4. **権限管理**画面を開くと、次のようなダイアログが開きます。**移行する**ボタンをクリックします。

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

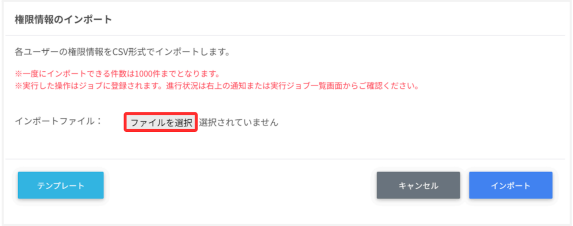


6. エクスポートしたCSVファイルをテキストエディタまたは表計算ソフトで編集します。

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



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



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。

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。

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

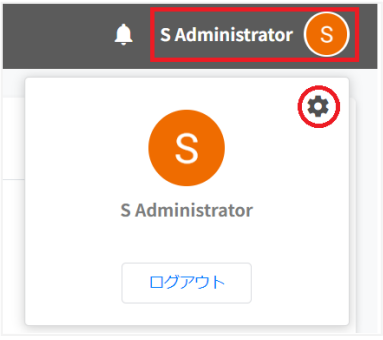
- 同期が実行された場合、InterCLASS® Filterring Serviceで同期対象となっている組織部門に所属しているユーザーが同期されます。
- **夜間定期同期**設定のオン／オフを問わず、**新規追加時の自動同期**設定により、InterCLASS® Console Supportでユーザーの追加や削除を行ったタイミングでユーザーの同期を実行することができます。

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。

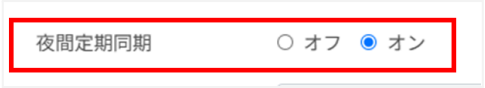
1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。

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。

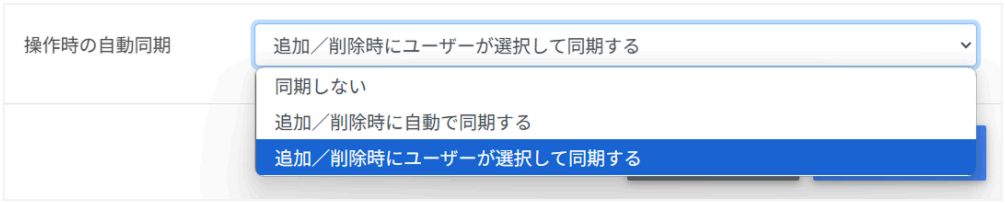
4. **夜間定期同期**のオン／オフを設定します。



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。

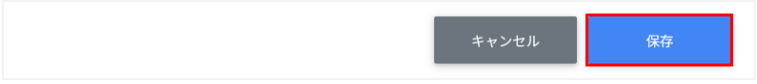
5. **新規追加時の自動同期**の動作を設定します。



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。



InterCLASS® Advance連携設定

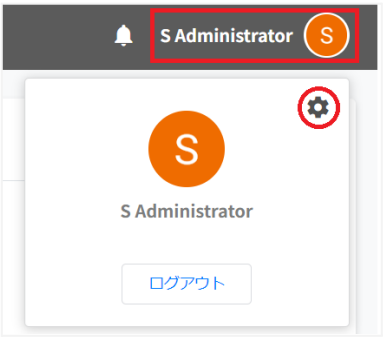
InterCLASS® Advanceとの連携内容を設定します。

⚠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。

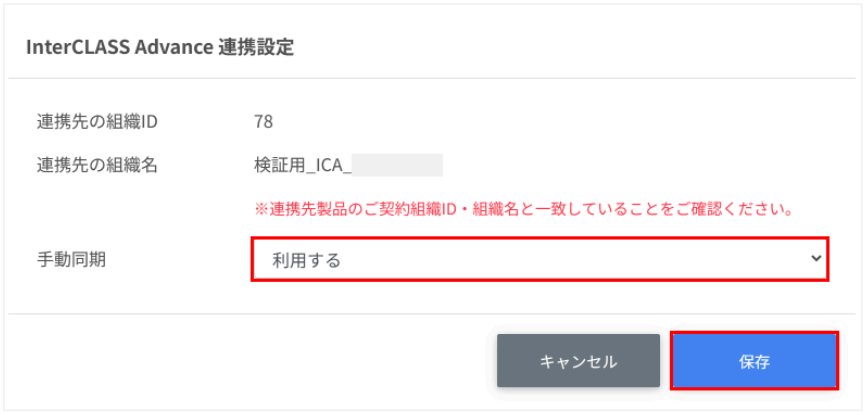
1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。

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。



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

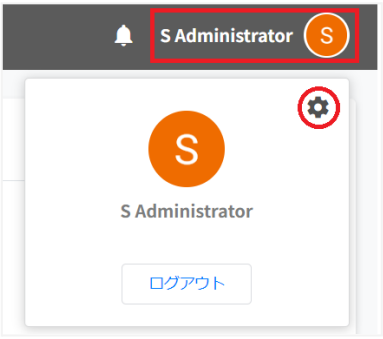
各製品間連携の実行状況を確認できます。

⚠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。

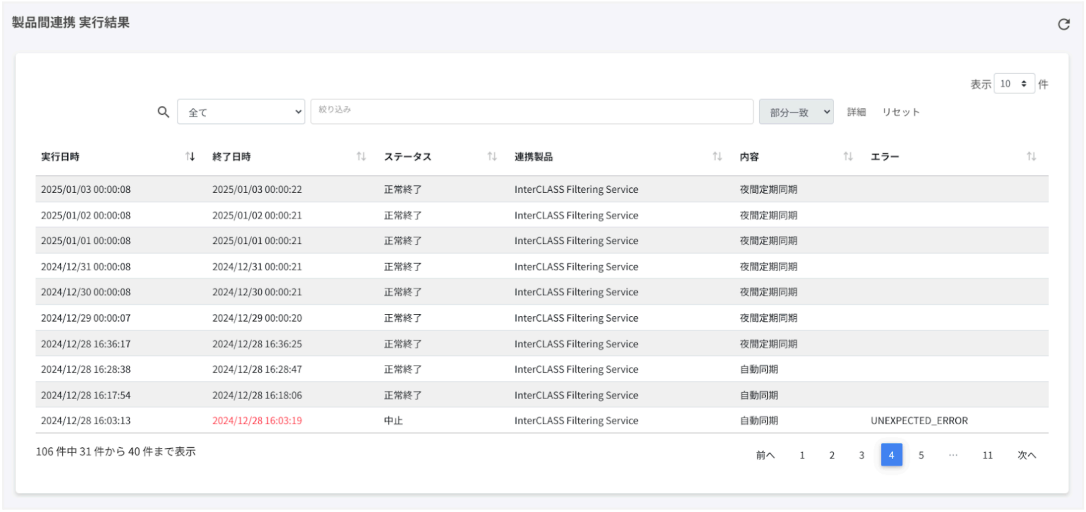
1. InterCLASS® Console Supportへアクセスし、**Sign in with Google** ボタンをクリックします。特権管理者のアカウントでログインします。

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。



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

- 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、あるいは複写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