



InterCLASS[®] Console Support

QRサーバー設定変更マニュアル

目次

はじめに-----	3
QRコードログインの設定-----	4
サードパーティのIDプロバイダを使用したシングルサインオンの設定-----	4
QRコードログインサーバー設定-----	9
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-----	10
Chrome デバイスの設定の変更-----	14
サードパーティの IdP による シングルサインオンの設定-----	19
Chromebook のログイン画面を確認-----	23
CHJeruサポートについて-----	24

はじめに

いつもInterCLASS® Console Support をご利用いただきありがとうございます。
本マニュアルは、v4.1以前から本製品をご利用中かつ、QRコードログイン機能をご利用中
のお客様が、v4.2から追加された最新のQRコードログインサーバーをご利用するための設
定を行うための手順を記したものとなります。

⑨ポイント

- 作業時間の目安は10～20分程度です。
- 作業はすべて「特権管理者アカウント」で行います。

QRコードログインの設定

最新サーバーを利用したQRコードによるChromebook へのログイン機能を有効にするため、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

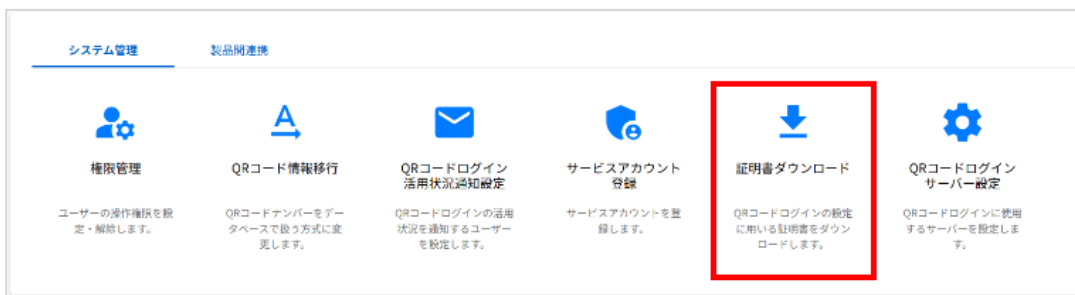
最新サーバーでQRコードを使用したChromebook へのログインを行うためのSAMLプロファイルを作成します。

⚠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。
1. 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。
 2. 左のメニューからシステム管理をクリックします。



3. 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。

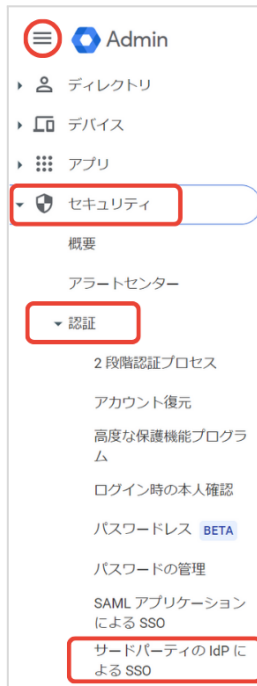


4. ICCSCert.zipがダウンロードされます。

5. 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。

6. 特権管理者のアカウントでサインインします。

7. 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。



8. 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](#)

[OIDC プロファイルを追加](#) [SAML プロファイルを追加](#)

名前	種類	ステータス
...	SAML	有効
...	SAML	完了
...	SAML	完了
...	SAML	完了
...	SAML	完了
...	OIDC	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
...	組織部門	以前の SSO プロファイル

9. 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](#)

[OIDC プロファイルを追加](#) [SAML プロファイルを追加](#)

10. 新しい SAML SSO プロファイルを追加画面に以下の情報を入力します。

設定情報

SSO プロファイル名	ICCS-SAML-SSO
メールアドレスを自動入力	ログインヒントを使用しない
IdP エンティティ ID	https://ssov2.interclasscloud.com/realms/keycloak
ログインページの URL	https://ssov2.interclasscloud.com/realms/keycloak/protocol/saml
確認用の証明書	項番4以降の手順で取得した証明書をアップロード

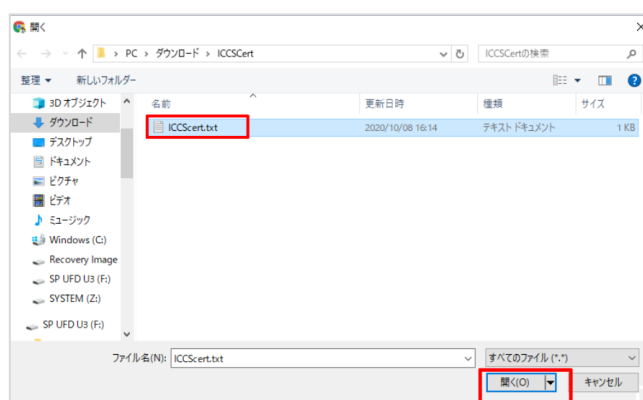
11. 確認用の証明書の証明書をアップロードをクリックします。

確認用の証明書

証明書をアップロードしてください（2 個まで）。証明書は PEM または DER 形式の X.509 証明書で、公開鍵が含まれている必要があります。

[証明書をアップロード](#)

12. 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。



13. 証明書がアップロードされると下記の表示になります。

確認用の証明書

証明書をアップロードしてください（2 個まで）。証明書は PEM または DER 形式の X.509 証明書で、公開鍵が含まれている必要があります。

保留

有効期限:



[別の証明書をアップロード](#)

14. 保存をクリックします。



⚠ 注意

- 保存後に詳細欄に表示されるエンティティIDとACSのURLはこのあとの工程で使用しますので必ずIDとURLを控えてください。

← 戻る

Staging-keycloak-SAML-SSO

この SAML SSO プロファイルは、組織部門またはグループに割り当てることができます。

🗑 削除

SAML SSO プロファイル

名前

Staging-keycloak-SAML-SSO

SP の詳細

IdP で Google を SP として SSO を設定する際には、この詳細情報が必要になります。詳しくは、ご利用の IdP のドキュメントをご覧ください。

エンティティ ID

ACS の URL

SP の証明書

ご利用の IdP でアサーションが暗号化される場合は、IdP が暗号化に使用できる SP 証明書を生成してください。2 つまでの SP 証明書を追加できます。

メールアドレスを自動入力

ログインヒントを使用しない

IdP の詳細

IdP エンティティ ID

ログインページの URL

ログアウト ページの URL

追加

パスワード変更用 URL

追加

確認用の証明書

証明書をアップロードしてください (2 個まで)。証明書は PEM または DER 形式の X.509 証明書で、公開鍵が含まれている必要があります。

K2545871

有効期限: 2036年5月28日 11:22:24 UTC+9

QRコードログインサーバー設定

QRコードによるChromebook へのログインに使用する最新サーバーの設定を行います。

1. システム管理画面からQRコードログインサーバー設定をクリックします。



2. QRコードログインサーバー設定ダイアログが表示されます。最新サーバーを利用するを選択します。
3. エンティティIDとACSのURL欄に、SAML SSO プロファイル作成後に表示されたエンティティIDとACSのURLを入力し、保存をクリックします。

④ポイント

- **レガシーサーバーを利用する設定時に発行していたQRコードは最新サーバーでもご利用いただけます。**ただし設定変更の直前に発行したQRコードは、最新サーバーに反映されるまでに最大1時間かかることがございます。

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。

安全に設定を変更するために

- QRコードログインを利用中のユーザーが所属する組織部門への設定を行う前に、テスト用の組織部門を作成し、テスト用のデバイスをその組織へ移動したのち、以降の設定をテスト用の組織部門に行い、変更が正しく変更されるか確認することを推奨します。

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。

④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

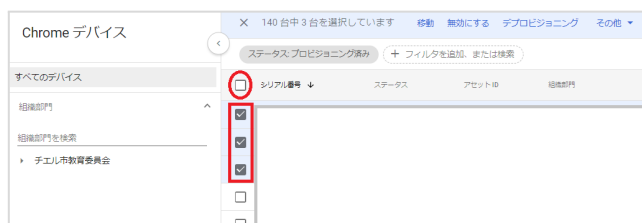
デバイスの組織部門を作成し、
Chromeデバイスを登録する

※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

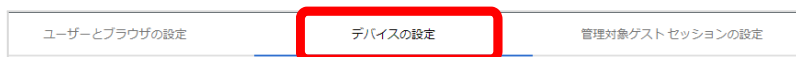
最新サーバーを利用したQRコードログイン機能を利用するChrome デバイスが含まれる組織部門のデバイスの設定を変更します。

⚠ 注意

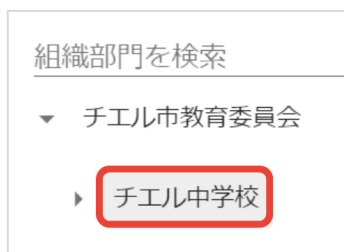
- 本設定は、特権管理者アカウントで実施してください。
1. Chrome ウェブブラウザでGoogle 管理コンソール (<https://admin.google.com/>)にアクセスします。
 2. 特権管理者のアカウントでサインインします。
 3. メニュー>デバイス>Chrome >設定をクリックします。



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。



⚠️安全に設定を変更するために

- 現在QRコードログインを利用しているデバイスが所属する組織部門への設定を行う前に、テスト用の組織部門を選択して以降の設定を行い、正しく変更されるか確認することを推奨します。

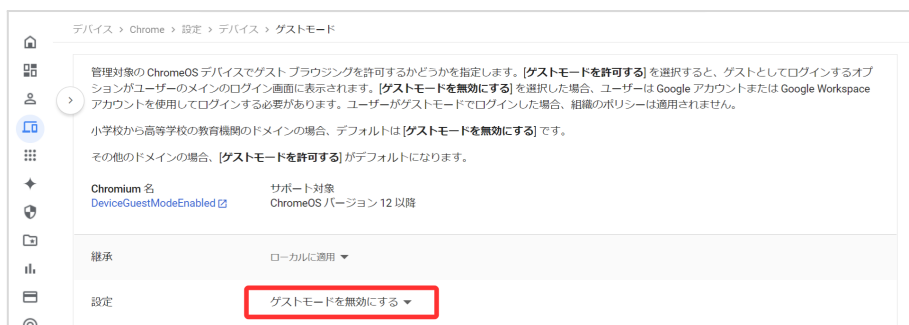
📌ポイント

- 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。

6. ログイン設定の項目に移動します。



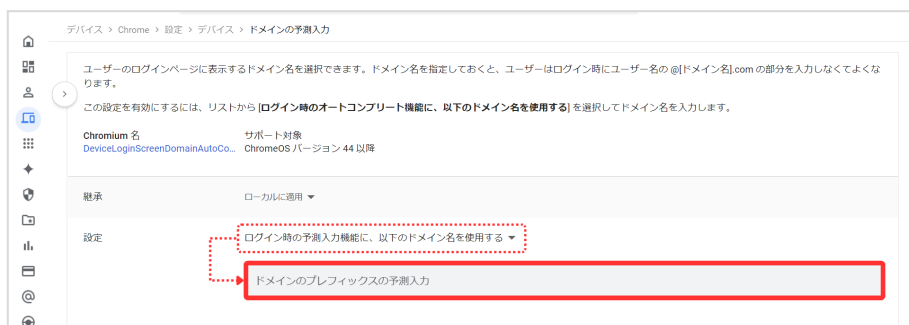
7. ゲストモードの設定をゲストモードを無効にするに変更します。



④ポイント

- 現在QRコードログイン機能をご利用中の組織部門の場合、前回の設定を行った際にすでにこの設定を行っている場合があります。

8. ドメインの予測入力の設定をログイン時の予測入力機能に、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。



④ポイント

- 現在QRコードログイン機能をご利用中の組織部門の場合、前回の設定を行った際にすでにこの設定を行っている場合があります。

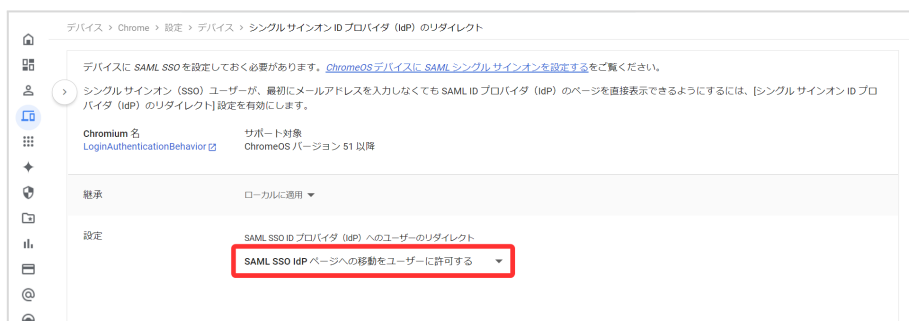
9. ログイン画面の設定をユーザー名と写真を表示しないに変更します。



④ポイント

- 現在QRコードログイン機能をご利用中の組織部門の場合、前回の設定を行った際にすでにこの設定を行っている場合があります。

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。



④ポイント

- 現在QRコードログイン機能をご利用中の組織部門の場合、前回の設定を行った際にすでにこの設定を行っている場合があります。

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://ssov2.interclasscloud.com> を入力します。

この設定について

SAML SSO フローでユーザーのカメラへの直接アクセスが許可されるサードパーティのアプリとサービスを指定します。

重要: 管理者がこのポリシーを有効にすると、ユーザーの代わりにユーザーのカメラへのアクセスをサードパーティに許可することになります。このポリシーでカメラへのアクセスを許可すると、システムからエンドユーザーに対して許可の同意を求めることがないため、管理者は適切な同意書を用意しておく必要があります。

この設定を行うと、サードパーティの ID プロバイダ (IdP) は ChromeOS デバイスに新しい形の認証フローを提供できます。

IdP を許可リストに追加するには、各サービスの URL を 1 行に 1 つずつ入力します。

組織での Clever Badges のセットアップについて詳しくは、[Clever のサポートサイト](#)をご確認ください。

デバイスに SAML SSO が設定されている必要があります。[ChromeOS デバイスに SAML シングルサインオンを設定する](#)をご覧ください。

Chromium 名	サポート対象
LoginVideoCaptureAllowedUrls	ChromeOS バージョン 52 以降

関連設定

[シングルサインオン](#)
ChromeOS デバイスに対して SAML ベースのシングルサインオンを有効または無効にする...

[シングルサインオン Cookie の動作](#)
次回以降のログイン時に、管理対象の ChromeOS デバイスからユーザー セッショ...

[シングルサインオン ID プロバイダ \(IdP\) のリダイレクト](#)
SSO ユーザーがメールアドレスの入力を省略して、SAML ID プロバイダ (IdP) ページに直...

[フィードバックを共有](#)

[一部を表示](#)

継承ローカルに適用 ▼

設定

カメラへのシングルサインオン アクセスが可能な URL

<https://ssov2.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。

サードパーティの IdP による シングルサインオンの設定

最新サーバーを利用したQRコードによる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)画面が表示されます。
5. SSO プロファイルの割り当ての管理の管理から、QRコードログインを行うユーザーが所属する組織部門を選択します。



⚠安全に設定を変更するために

- 現在QRコードログインを利用しているユーザーが所属する組織部門への設定を行う前に、テスト用の組織部門を選択して以降の設定を行い、正しく変更されるか確認することを推奨します。

6. SSO プロファイルの割り当ての管理 > SSO プロファイルの割り当て > SSO プロファイルを選択から、作成したSSOプロファイル (ICCS-SAML-SSO)を選択します。
7. Google でユーザー名の入力を求めた後、このプロファイルの IdP ログインページにリダイレクトするを選択します。

8. 保存をクリックします。

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)

この組織部門またはグループでは、組織向けのサードパーティの SSO プロファイルよりも、以下の SSO プロファイルが優先されます。

次の組織部門のユーザー設定を表示しています: スコープを削除

SSO プロファイルの割り当ての管理

SSO プロファイルの割り当て
上書きされました

SSO プロファイルを選択

この組織部門またはグループのユーザーのログイン方法を選択します。 SSO プロファイルの詳細

ユーザーが最初にこの SSO プロファイルのサードパーティ IdP を使用してログインせずに Google ヤービスに直接アクセスした場合、このように対応するかを選択してください。 SSO プロファイルのパスワード変更も同様。最初のサインオンを選択した場合のみ適用されます。それ以外の場合、パスワードを変更する必要があるユーザーは Google を使用します。 [詳細](#)

☒ Google でユーザー名の入力をもとめた後、このプロファイルの IdP ログインページにリダイレクトする

☐ ユーザーに Google のユーザー名とパスワードを入力してログインするよう求める

[詳細](#)
大部分の変更は数分で反映されます。
以前の変更は数分で適用できます

保存 永保存の変更が 2 件あります キャンセル **保存**

9. 項番5と同様に、SSO プロファイルの割り当ての管理の管理から、QRコードログインを行う**デバイスが所属する組織部門**を選択します。

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)

この組織部門またはグループのユーザーのログイン方法を選択します。 SSO プロファイルの詳細

次の組織部門のユーザー設定を表示しています: チェル市教育委員会

SSO プロファイルの割り当ての管理

SSO プロファイルの割り当て
"チェル市教育委員会" で適用しました

SSO プロファイルを選択

以前の SSO プロファイル

ユーザーはサードパーティの SSO プロファイルでログインする。 Google のログイン時の本人確認を変更するには、SSO 後の本人確認のページに移動します

☒ Google でユーザー名の入力をもとめた後、このプロファイルの IdP ログインページにリダイレクトする

☐ ユーザーに Google のユーザー名とパスワードを入力してログインするよう求める

[詳細](#)
大部分の変更は数分で反映されます。
以前の変更は数分で適用できます

キャンセル 保存

10. SSO プロファイルの割り当ての管理 > SSO プロファイルの割り当て > SSO プロファイルを選択から、作成したSSOプロファイル (ICCS-SAML-SSO)を選択します。

11. Google でユーザー名の入力をもとめた後、このプロファイルの IdP ログインページにリダイレクトするを選択します。

12. 保存をクリックします。



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)

ユーザー



この組織部門またはグループでは、組織向けのサードパーティの SSO プロファイルよりも、以下の SSO プロファイルが優先されます。

次の組織部門のユーザー設定を表示しています: [スコープを削除](#)

SSO プロファイルの割り当ての管理

SSO プロファイルの割り当て
上書きされました

SSO プロファイルを選択

この組織部門またはグループのユーザーのログイン方法を選択します。 SSO プロファイルの詳細

ユーザーが最初にこの SSO プロファイルのサードパーティ IdP を使用してログインせずに Google ワークスペースに直接アクセスした場合、どのように対応するかを選択してください。 SSO プロファイルのパスワード変更周知は、最初のオプションを選択した場合のみ送付されます。 それ以外の場合は、パスワードを変更する必要があるユーザーは Google を使用します。 [詳細](#)

☒ Google でユーザー名の入力を行った後、このプロファイルの IdP ログインページにリダイレクトする

☐ ユーザーに Google のユーザー名とパスワードを入力してログインするよう求める



大部分の変更は数分で反映されます。 [詳細](#)
以前の変更は数分で削除されます

終了

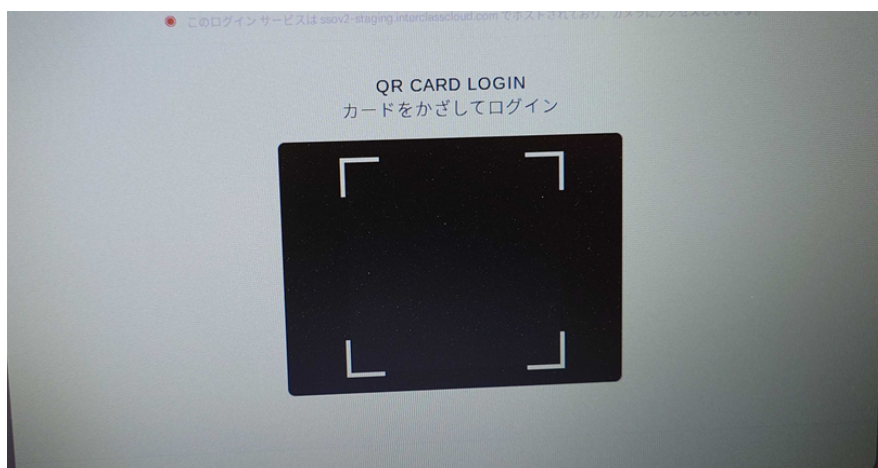
未保存の変更が 2 件あります キャンセル **保存**

22

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、最新サーバーを利用したQRコードによる 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。



④ポイント

- Chrome デバイスの設定やサードパーティの IdP による シングルサインオンの設定で行った内容がChromebookデバイスに適用されることで、ログイン画面の表示が切り替わります。環境により適用まで時間がかかる場合がございますので、ログイン画面が変更されない、カメラが起動しないなどの問題がある場合、**端末を一度再起動してください。**

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 QRサーバー設定変更マニュアル

2026年 8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、2026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 藤崎芭蕉の辻ビルディング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>