D201460

日本 HP Chromebook における多要素認証の利用について

株式会社ディー・ディー・エス
株式会社日本 HP

1. 万能認証基盤 Themis による多要素認証での Chromebook ログイン

Chromebook をはじめとする Chrome デバイスの OS ログインに対して万能認証基盤 Themis を連携することで、Chromebook などに搭載されるウェブカメラを利用した Themis の QR コード認証や顔認証でシームレスなログインが可能となります。これにより、安全かつ便利に Chrome デバイスを利用することができます。

2. 日本 HP の Chromebook について

日本 HP は文部科学省が掲げる GIGA スクール構想に準拠し Chrome OS を搭載した、クラムシェル型の「HP Chromebook 11A G8 EE」と、コンバーチブル型 2in1 の「HP Chromebook x360 11 G3 EE」の 2 モデルを提供しています。いずれも生徒向けのモデルで、長期利用を想定した高耐久バッテリーを採用しています。

Themis と連携した GIGA スクール構想に準拠した文教向けの Chromebook
「HP Chromebook x360 11 G3 EE」と「HP Chromebook 11A G8 EE」

3. 連携イメージ

4. 前提条件とセットアップの流れ

Google Workspace と Themis の SAML 連携を行う前に以下の前提条件をご確認ください。

（ア）前提条件

① Google Workspace と Themis の SAML SSO 設定を行えること

② Chrome サービス ライセンス契約が適用されるサービス（Chrome Enterprise、Chrome Education、Chrome Kiosk 等）であること

（イ）セットアップの流れ

① Google Workspace と Themis の SAML SSO 設定を行う

② Themis の認証要素を登録する

③ Chrome デバイス OS ログインセットアップを行う

④ Chrome デバイスの OS ログインに関する諸設定を行う

⑤ 運用開始

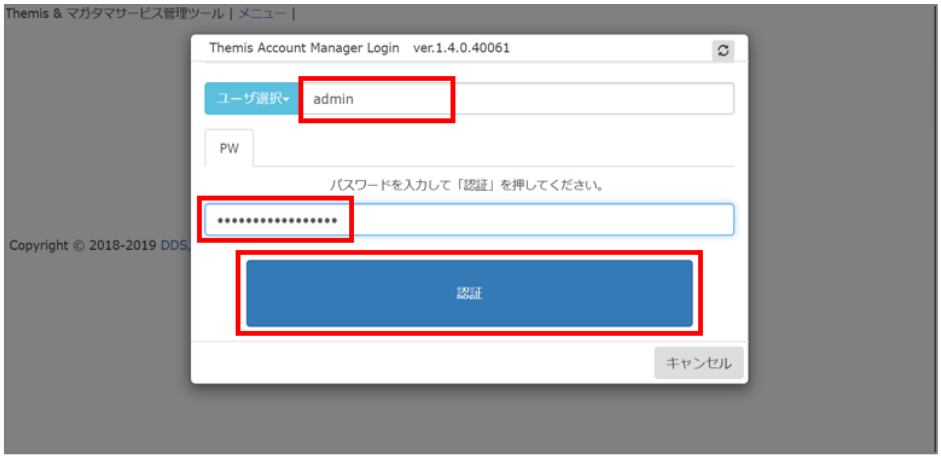
5. Google Workspace と Themis の SAML SSO 設定

（ア）サービスプロバイダ情報（以下SPと記述）の登録

① アプリケーションの登録

Google WorkspaceのSPとしての情報をThemisの管理ツールへ登録します。
ブラウザで管理ツールを開き、「管理ツールにログイン」をクリックします。

管理者用のユーザー名とパスワードを入力して「認証」をクリックし、管理者としてログインします。



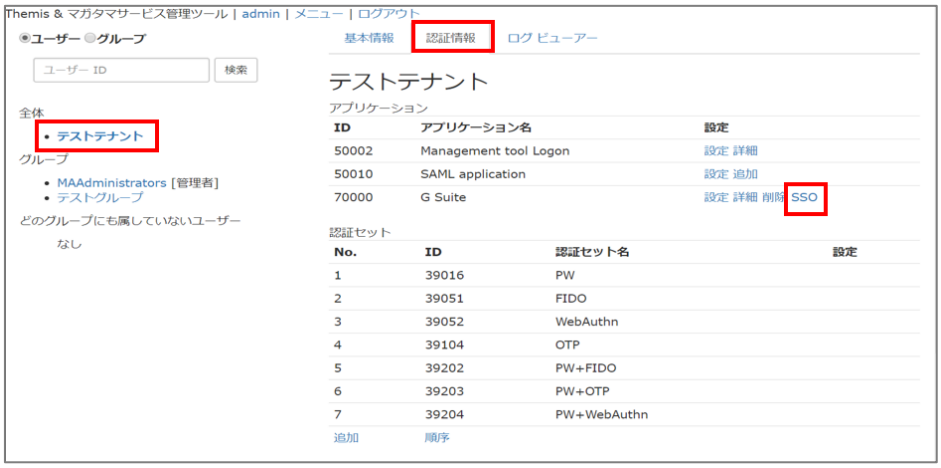
管理ツールの左側「全体」セクションの組織名を選択し、右側ペインの「認証情報」タブの中にある「50010　SAML application」の「追加」をクリックします。

Google Workspaceと分かるアプリケーション名を入力し、認証の際に必要とする利用可能な認証セットのチェックボックスをオンにして「保存」をクリックします。

Google Workspaceの登録が完了すると以下の画面になります。

② ThemisのIdPとしての情報

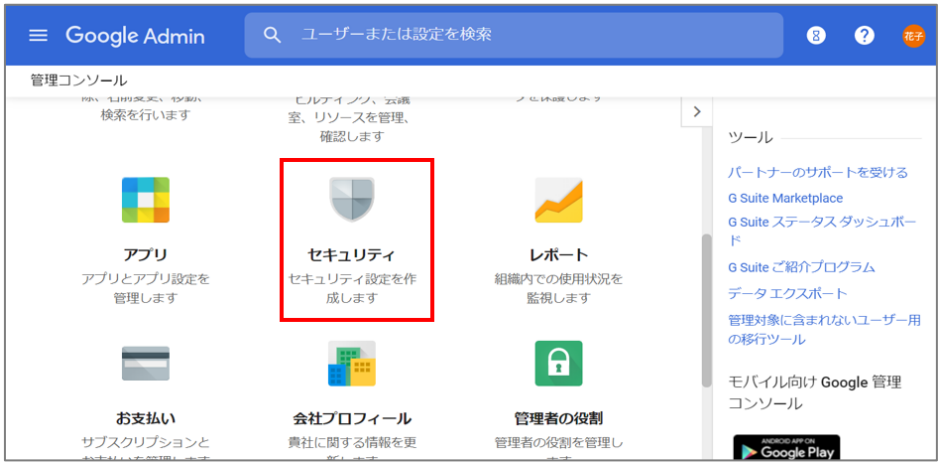
ThemisのIdPとしての情報を確認します。管理ツールの左側「全体」セクションの組織名を選択し、右側ペインの「認証情報」タブの中にあるGoogle Workspace用に作成したアプリケーションの「SSO」をクリックします。



「SSO設定情報」が表示されます。ここで表示される「SSOエンドポイント」、「SLOエンドポイント」、「X.509証明書」の情報を、Google Admin consoleへの登録に利用します。

③ Google WorkspaceにSAML SSO設定を行う

Google Admin consoleにThemisのIdPとしての情報を登録します。Google Admin console（admin.google.com）にアクセスし、管理者としてログインし、「セキュリティ」をクリックします。

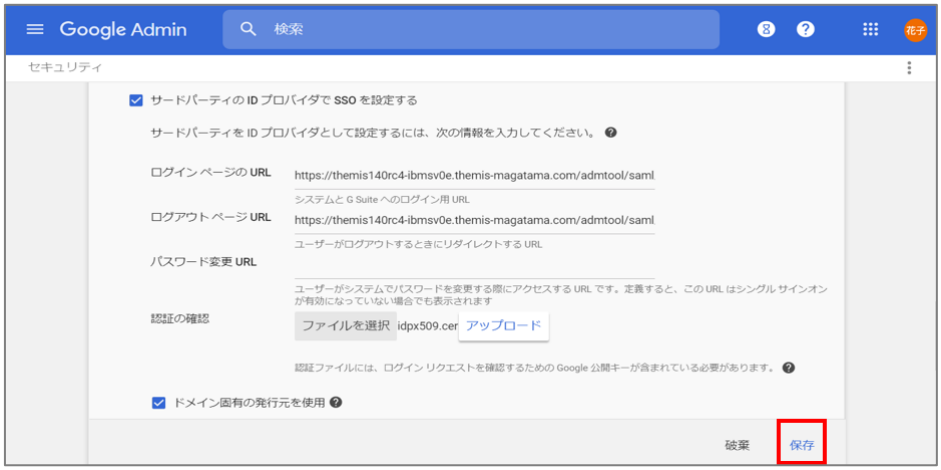


「シングル サインオン（SSO）の設定」をクリックします。

「サードパーティのIDプロバイダでSSOを設定する」のチェックボックスをオンにします。

「ログインページのURL」にThemisのSSOエンドポイントを、「ログアウトページURL」にThemisのSLOエンドポイントを入力し、「認証の確認」の

「ファイルを選択」から保存したThemisのX.509証明書をアップロードし、「ドメイン固有の発行元を使用」のチェックボックスをオンとし、「保存」をクリックし、設定を保存します。



④ Google WorkspaceのSPとしての情報を登録

管理ツールの左側「全体」セクションの組織名を選択し、右側ペインの「認証情報」タブの中にあるGoogle Workspace用に作成したアプリケーションの「詳細」をクリックします。

任意のSPの名前を入力し、「Issuer」に「google.com/a/[Google Workspaceへ設定したドメイン名]」を入力します。ドメイン名はGoogle Workspaceアカウントの「@以降の部分」です。「更新」をクリックし、設定を保存します。

設定が完了すると以下の画面になります。

⑤ Themisでログインさせたいユーザーの登録

管理ツールの左側グループのメンバーリストからユーザーを選択し、右側ペインの「認証情報」タブの中にあるGoogle Workspace用に作成したアプリケーションの「詳細」をクリックします。

ログインユーザー名にThemisで認証を行いたいGoogle Workspaceのユーザー名を入力し、「更新」をクリックします。

設定が完了すると以下の画面になります。以上でGoogle WorkspaceとThemisのSAML SSO設定は完了です。

（イ）ChromeデバイスのOSログインセットアップ

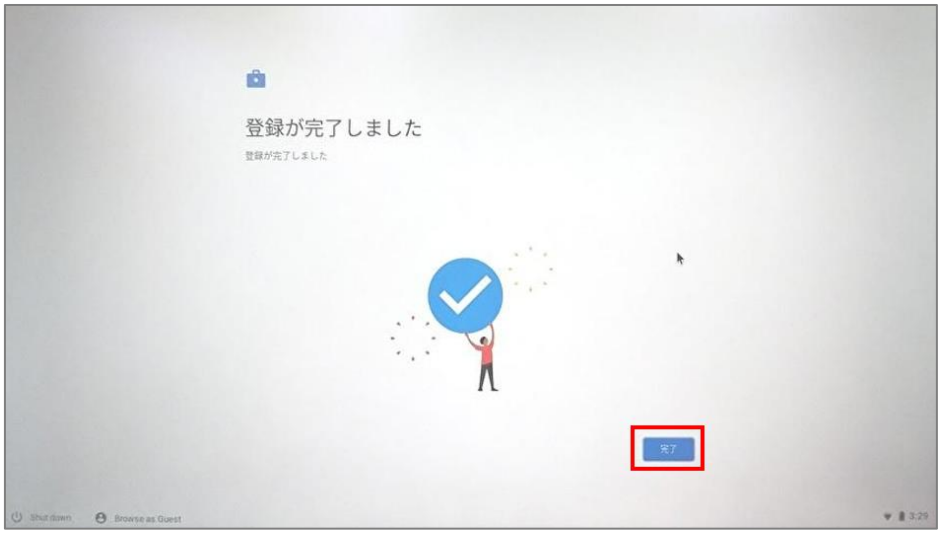
① Chromeデバイスの登録

Chromeデバイスの電源をオンにし、Google Admin console上で設定したデバイスポリシーを適用するために手動でChromeデバイスの登録を行います。

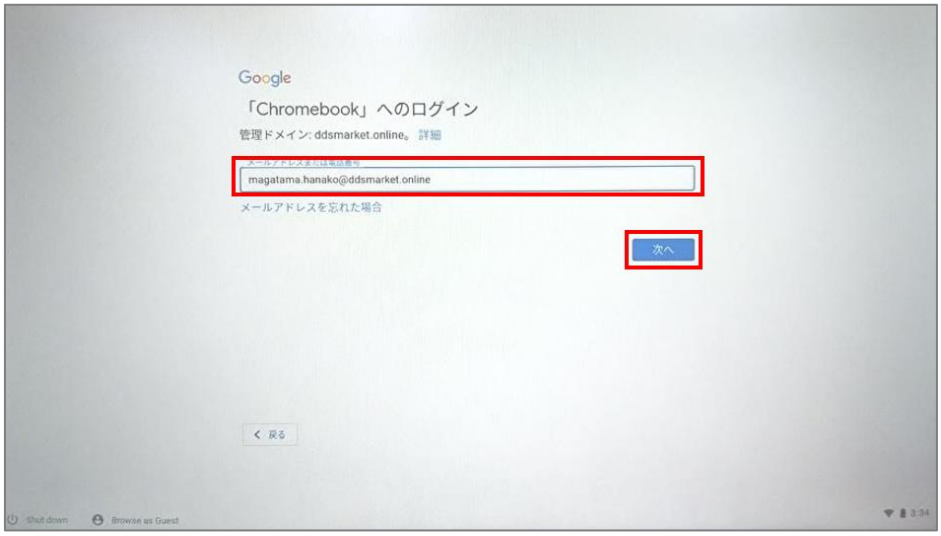
Chromeデバイスの電源をオンにして起動させます。ログイン画面が表示されますがここではログインせず「その他の設定」の「企業の登録」をクリック、またはCtrl + Alt + Eキーを押します。

企業の登録を行います。Google Admin console（admin.google.com）にアクセスできる管理者ユーザーのメールアドレスを入力し「次へ」をクリックし、パスワードを入力し「次へ」をクリックします。

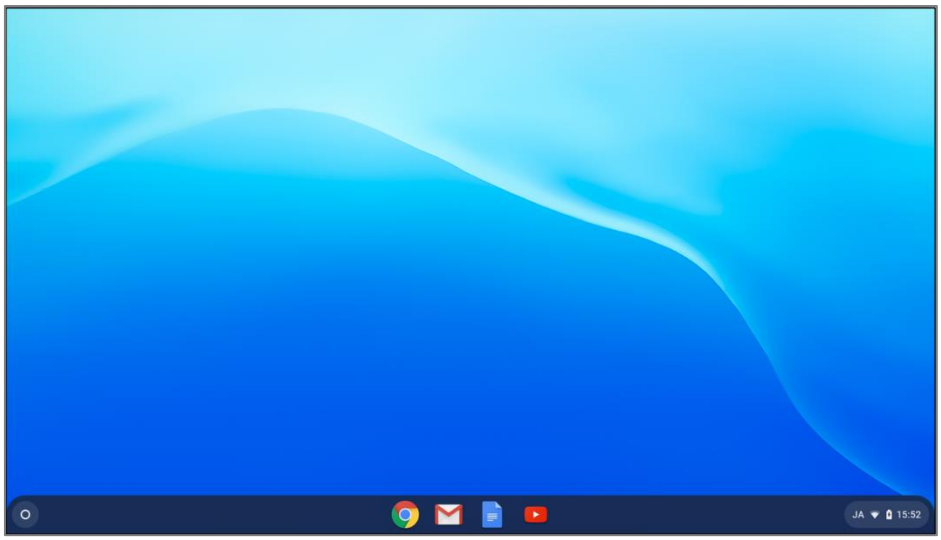
企業の登録が完了したら、「完了」をクリックします。



再度Chrome OSのログインユーザーのメールアドレスを入力し「次へ」をクリックし、パスワードを入力し「次へ」をクリックします。続いて「同意して続行」をクリックします。



Chrome OSへのログインが完了しました。続いてChrome OSログインに関する諸設定を行ってください。



② ChromeデバイスのOSログインに関する諸設定

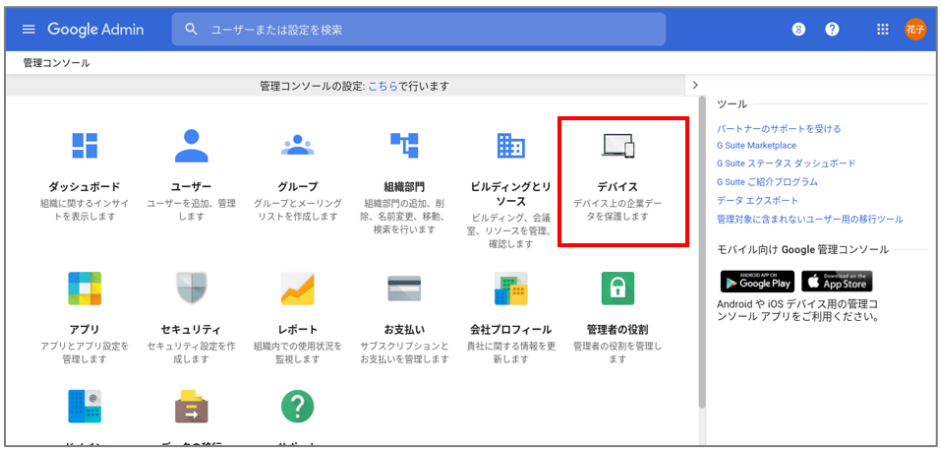
Google Admin consoleの「デバイス管理」 ＞ 「Chrome管理」で、Chromeデバイスのログインに関する諸設定を行うことができます。

設定項目	説明
SAMLによるChromeデバイス OSログインの有効化（必須）	ChromeデバイスのOSログインにThemisの認証を使用するための設定です。
OSログイン時にメールアドレスの入力を省略する	SAMLによるChromeデバイスのOSログイン時にメールアドレスの入力を省略するための設定です。設定を行ってもメールアドレスの入力を要求される場合は、１度メールアドレスを入力してログインすると次回から省略されるようになります。

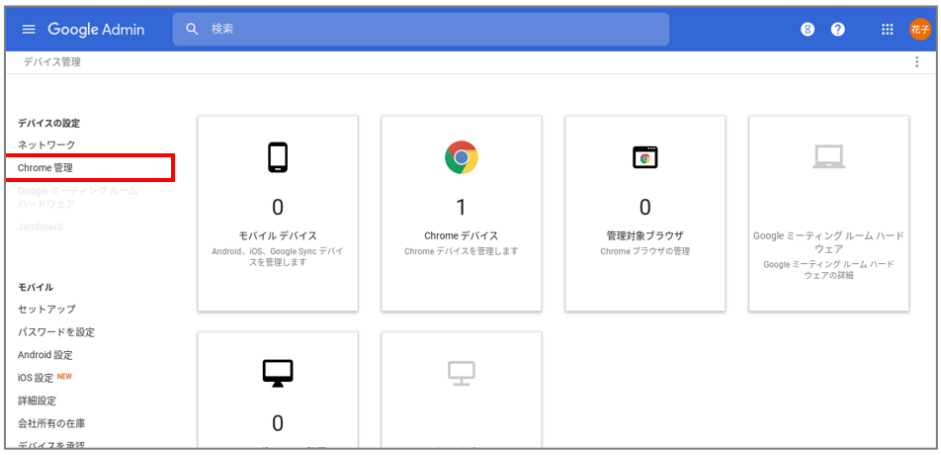
OSログイン後の「以前のパスワードを入力する」ダイアログの表示を抑制する	SAMLによるChromeデバイスのOSログインを行った後に表示される「以前のパスワードを入力する」ダイアログの表示を抑制するための設定です。
OSログイン時のカメラ（顔認証）を有効化する （Themisとの連携が必要）	Chrome デバイスの OS ログイン時にカメラ（顔認証）を使用するための設定です。 ThemisとThemisを連携して使用する場合にこの機能を利用できます。
日本語キーボードを指定する	ChromeデバイスのOSログイン時に日本語キーボードを使用するための設定です。

- SAMLによるChromeデバイス OSログインの有効化

Chrome OSにログインし、Chromeアイコンをクリックしてブラウザを起動し、Google Admin console（https://admin.google.com/）にログインし、デバイスアイコンをクリックします。ここで登録したChromeデバイスの制御を行うことができます。



SAMLによるChromeデバイス OSログインの有効化設定を行います。「デバイス管理」のページで左ペインの「Chrome管理」をクリックします。



「デバイス管理」　＞「Chrome」のページで「ユーザーとブラウザの設

定」をクリックします。

「シングルサインオン」の「Chrome OSデバイス向けのSAMLベースのシングルサインオン」の項目について「Chrome 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にする」を選択し、「保存」をクリックします。

- OSログイン時のメールアドレス入力の省略

SAMLによるChromeデバイス OSログイン後の「以前のパスワードを入力する」ダイアログの表示を抑制します。「デバイス管理」 ＞ 「Chrome」のページを開き、「デバイスの設定」をクリックします。

「デバイス管理」　＞「Chrome」　＞「設定」のページの「デバイスの設定」の「シングルサインオンのIDプロバイダ（IdP）のリダイレクト」の項目について「SAML SSO IdPページへの移動をユーザーに許可する」を選択し、「保存」をクリックします。

● OSログイン後の「以前のパスワードを入力する」ダイアログの表示抑制
SAMLによるChromeデバイス OSログイン後の「以前のパスワードを入力する」ダイアログの表示を抑制します。「デバイス管理」　＞「Chrome」のページを開き、「デバイスの設定」をクリックします。
「ユーザーデータ」の「各ユーザーがログアウトした後に、ローカルユーザー情報、設定、状態をすべて消去する」の項目について「すべてのローカルユーザーデータを消去」を選択し、「保存」をクリックします。

● Chromeデバイス OSログイン時のカメラ（顔認証）を有効化する方法

「デバイス管理」 ＞「Chrome」のページを開き、「デバイスの設定」をクリックします。

「デバイス管理」 ＞「Chrome」 ＞「設定」のページの「デバイスの設定」の「ログイン画面のキーボード」の「ログイン画面で使用するキーボードの順序リストを作成」の項目に表示されるリスト内の「日本語キーボード」を選択し、「保存」をクリックします。

ここまでの登録手順を実施することで、Chromeデバイスへのログインに Themisの多要素認証が利用できるようになります。

以上

※ QRコードは株式会社デンソーウェーブの登録商標です。

※ 本資料に記載されているロゴ、会社名、製品・サービス名は、各社の登録商標または商標です。

※ 導入をご検討の際は、弊社営業までお問い合わせください。