D240790

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. EVECLOUD 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 ログインにクラウド認証サービス EVECLOUD 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顔認証や FIDO2 セキュリティキーを利用した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 スクール構想の第 2 期に準拠し ChromeOS を搭載した、基本パッケージの「HP Fortis Flip G1m 11 Chromebook」と応用パッケージの「HP Fortis x360 G5 Chromebook」の 2 モデルを提供しています。HP の教育向けノート PC は、先生、生徒、学校管理者からの声をもとに開発。耐久性、拡張性、汎用性を兼ね備えた、教育向け専用設計のノート PC です。

https://jp.ext.hp.com/business-solution/education/

EVECLOUD と連携した GIGA スクール構想に準拠した文教向けの Chromebook
「HP Fortis Flip G1m 11 Chromebook」と「HP Fortis x360 G5 Chromebook」

連携イメージ

ChromeOS ログイン

Google Workspace との SAML 連携 をすることで、ユーザーは ChromeOS（Chromebook など）のログインに顔認証などを利用した多要素認証を利用することができます。

3. 前提条件とセットアップの流れ

Google Workspace と EVECLOUD 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 EVECLOUD 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 Upgrade、Chrome Education Upgrade 等）であること

以下の流れでセットアップを行います

（ア）サービスプロバイダ情報の登録

① EVECLOUD へのアプリケーションの登録

② EVECLOUD の IdP としての情報

③ Google Workspace へのシングルサインオン設定

④ EVECLOUD へのシングルサインオン設定

⑤ EVECLOUD ユーザーの SAML ログイン設定

（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 OS ログインに関するデバイスポリシーの設定

② Chrome デバイスの登録

（ウ）運用開始

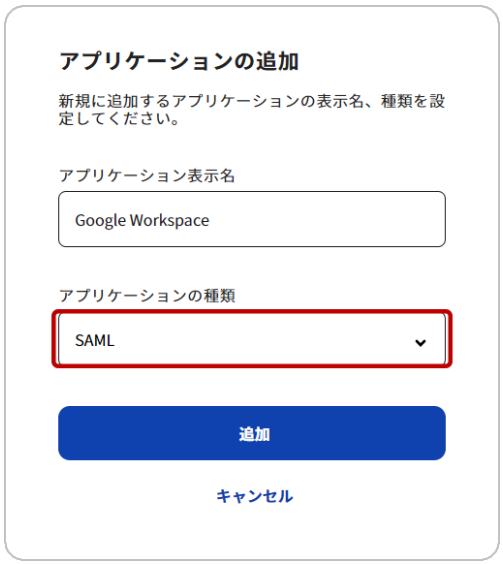
4. Google Workspace と EVECLOUD の SAML SSO 設定

（ア）サービスプロバイダ（以下SPと記述）情報の登録

① EVECLOUDへのアプリケーションの登録

Google WorkspaceのSPとしての情報をEVECLOUD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、管理ツールに管理者用アカウントを用いてログインします。続いて、[アプリケーションの管理]ページにてアプリケーションの登録を行います。登録の際、[アプリケーションの種類]は[SAML]を選択します。



作成したアプリケーション「Google Workspace」をクリックし、設定画面を開きます。

② EVECLOUDのIdPとしての情報

設定画面では、シングルサインオン用のエンドポイントや証明書を確認できます。これらはGoogle Workspace側への登録時に必要になります。

項目	内容
SSO URL	Google Workspaceのログイン時に使用するエンドポイントです。
ログアウトURL	Google Workspaceからのログアウト時に使用するエンドポイントです。
メタデータURL	EVECLOUDのSAML IdPメタデータをダウンロードするURLです。
X.509証明書のダウンロード	Google Workspaceに登録するX.509形式の証明書をダウンロードします。

③ Google Workspaceへのシングルサインオン設定

Google Workspaceの管理コンソールに管理者用アカウントでログインし、「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。

サードパーティのIDプロバイダに以下の情報を設定します。

a) 「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

b) 「ログインページのURL」にEVECLOUDの「SSO URL」を設定

c) 「ログアウトページのURL」に先ほど保存した「ログアウトURL」を設定

d) EVECLOUDの管理ツールからダウンロードしたX.509証明書をアップロード

e) 「ドメイン固有の発行元を使用」にチェック

「保存」をクリックし、設定を保存します。

④　EVECLOUDへのシングルサインオン設定

ブラウザで管理ツールを開き、管理ツールに管理者用アカウントを用いてログインします。アプリケーションの管理にて、作成したアプリケーション「Google Workspace」を選択します。

[サービスプロバイダーの設定情報を直接入力する]にチェックを入れ、以下の箇所に設定を入力します。

項目	内容
Issuer（必須）	「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。
ログアウトURL	ここに以下のURLを入力することで、Googleからのログアウト後にログイン画面に戻ることができます。 https://accounts.google.com/InteractiveLogin/signinchooser? 何も入力しなければ、EVECLOUDのログアウト画面が表示されます。

続いて、必要に応じてSSOに関する設定を行い、すべての設定を終えたら「保存」ボタンをクリックして登録します。

⑤ EVECLOUDユーザーのSAMLログイン設定

EVECLOUD管理ツールにて、「グループの管理」＞「ユーザー管理」からSAMLログイン設定をさせたいユーザーを選択し、「ユーザーの設定」画面を開きます。左メニューの[SAMLログイン設定]を選択し、SAMLアプリケーション一覧から登録済みのSAML「Google Workspace」を選択します。

表示されたダイアログにて、[SAMLログインユーザー]にシングルサインオンを行いたいGoogle Workspaceのユーザー名を入力し、[決定]ボタンをクリックします。

名称	内容
SAMLログインユーザー	SAMLサービスプロバイダーへのログインに使用するIDを入力してください。 必要となるIDの種類はサービスプロバイダーによって異なります。 （例：メールアドレス、ランダムなUUID、一時的に発行されたランダム文字列など）
Chromebookのパスワード	Chromebookを利用する場合の設定項目です。 Chromebookへのログイン時に使用するパスワードを設定します。通常はGoogle Workspaceのパスワード、または以前ログインした際に使用したパスワードを設定します。 設定しない場合、Chromebookへのログイン時に明示的にパスワードの入力を求められることがあります。

[保存]ボタンをクリックし登録内容を保存してシングルサインオンの設定は完了です。

以上で、Google Workspaceへアクセスし一般ユーザーアカウントでログオンを試みると、EVECLOUDへリダイレクトされシングルサインオンを行うことができます。

（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OSログインに関するデバイスポリシーの設定

次回からのChromeデバイスへのログインがスムーズに行えるようログインに関する設定を行う必要があります。設定項目は以下の通りです。

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EVECLOUD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（EVECLOUD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。EVECLOUD と Chrome デバイスを連携して使用する場合にこの機能を利用できます。
OSログイン時の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。

Google Admin console（admin.google.com）にアクセスし、管理者としてログインします。

「デバイス」ページの左カラムメニューから「Chrome」を開き、「設定」＞「ユーザーとブラウザ」を選択し、「ユーザーとブラウザの設定」ページ

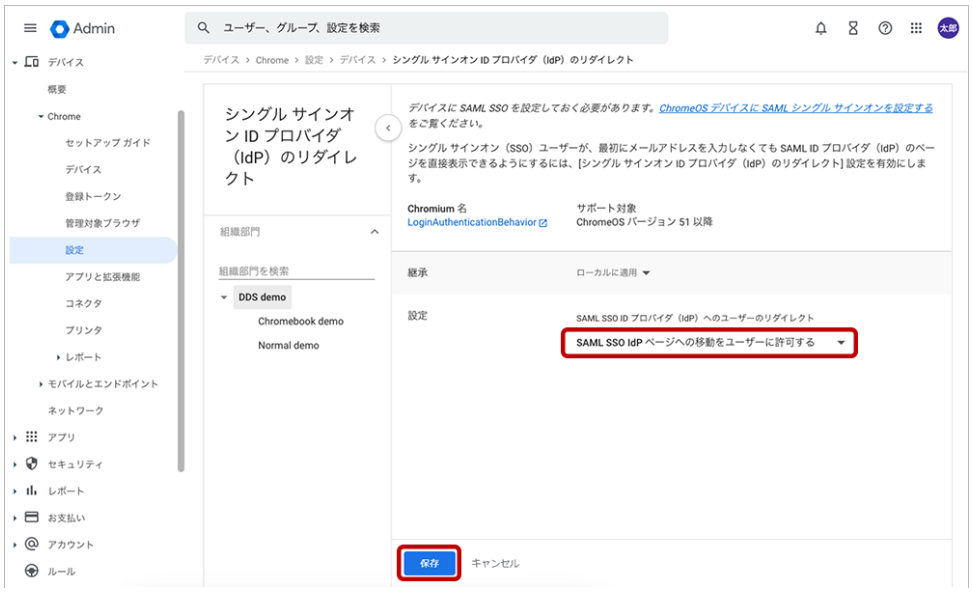
の「シングルサインオン」項目を選択します。

「シングルサインオン」設定ページにある「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。

「デバイスの設定」を行います。「ユーザーとブラウザの設定」ページの上部にある「デバイスの設定」ボタンを選択し、「デバイスの設定」ページへ移動します。

a) 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する設定をしていきます。「デバイスの設定」＞「ユーザーデータ」設定ページを開き、設定項目の「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。

b) SAMLによるChromeデバイス OSログイン時にメールアドレスの入力を省略する設定をしていきます。「デバイスの設定」＞「シングル サインオン ID プロバイダ（IdP）のリダイレクト」設定ページを開き、設定項目の「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。



c) Chromeデバイス OSログイン時のカメラ（顔認証）を有効化する設定をしていきます。「デバイスの設定」＞「シングルサインオンによるカメラへのアクセスの許可」設定ページを開き、設定項目の「カメラへのシングルサインオン アクセスが可能な URL」欄に

「https://saml.dds.click/」と「https://saml.dds-evecloud.com/」を入力し、「保存」をクリックします。

d) Chromeデバイス OSログイン時の日本語キーボードを指定する設定をしていきます。「デバイスの設定」＞「ログイン画面のキーボード」設定ページを開き、設定項目の「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」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。

② Chromeデバイスの登録

Chromeデバイスを起動し、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。

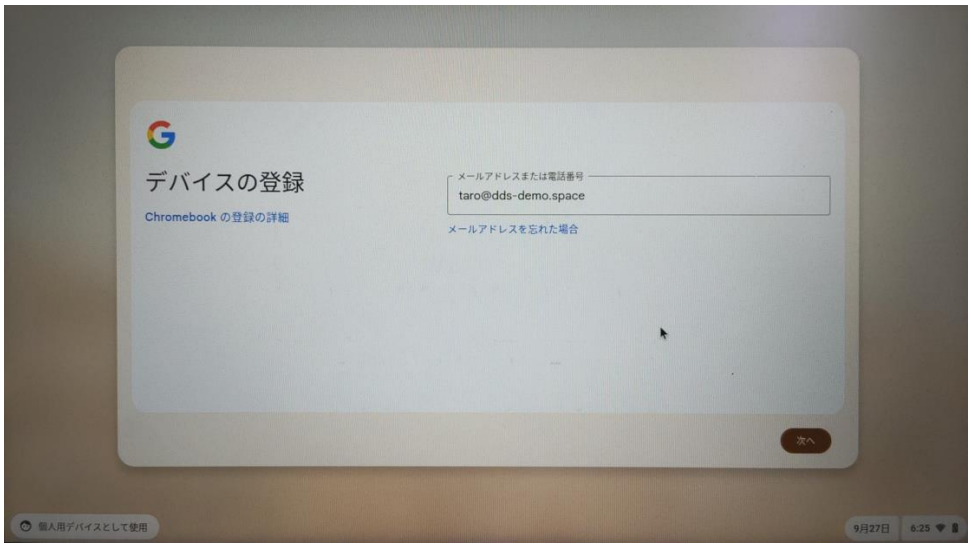
「始める」をクリックします。

ネットワークの設定を行います。接続するネットワークを選択し、表示されたダイアログでパスワードなどの必要事項を入力し、「接続」をクリックします。

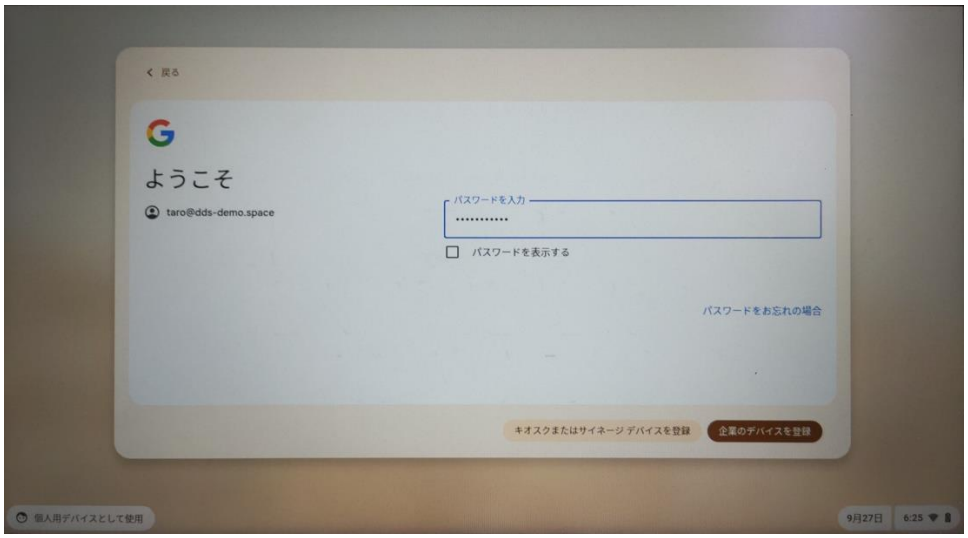
Chromebookの設定の選択画面で、「仕事向け」を選択し「次へ」をクリックします。

デバイスを組織に登録します。「デバイスを登録」をクリックします。

ChromeOSのログインユーザーのメールアドレスを入力し、「次へ」をクリックします。



パスワードを入力し、「次へ」をクリックします。



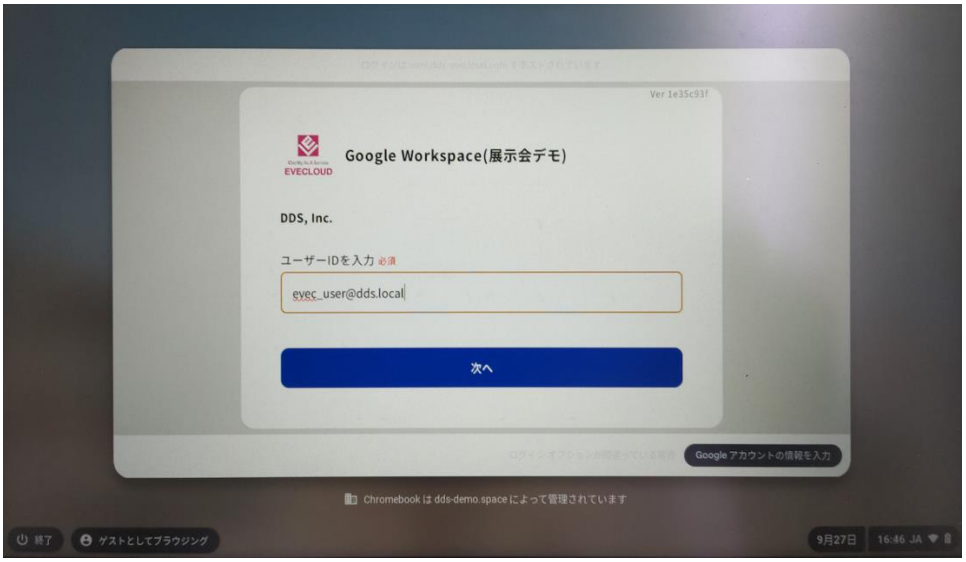
デバイスが正常に登録されたことを示す確認メッセージが表示されたら、「完了」をクリックします。これで、ユーザーはデバイスにログインして使用できるようになりました。

ChromeOSへのログインが完了しました。
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 EVECLOUDの多要素認証が利用できるようになります。

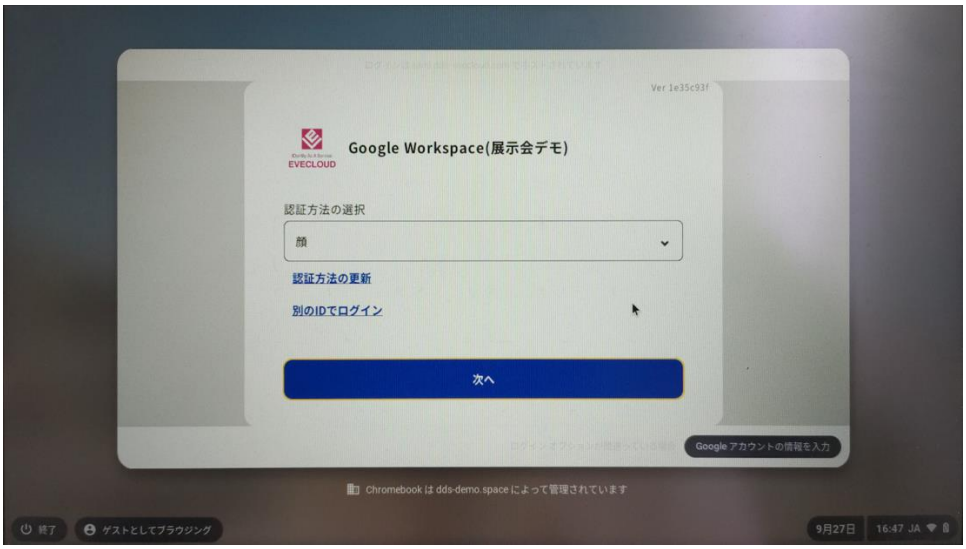
5. Chrome デバイスでの OS ログインの流れ

（ア）ChromebookでのEVECLOUDを利用したOSログイン

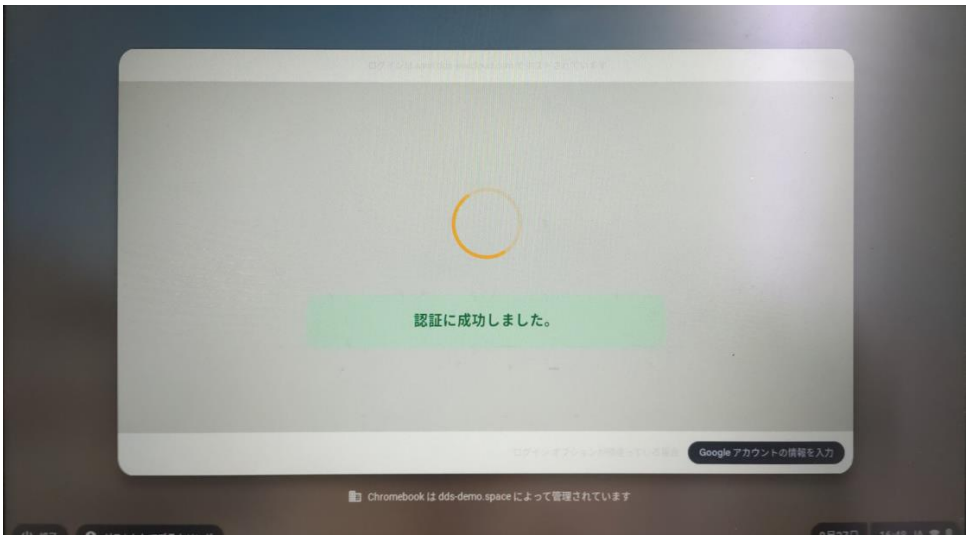
Chromeデバイスの電源を入れます。EVECLOUDの認証画面が表示されます（「Chromebookにログインしてください」と表示された場合（→）をクリックします）。ユーザーIDを入力して「次へ」をクリックします。



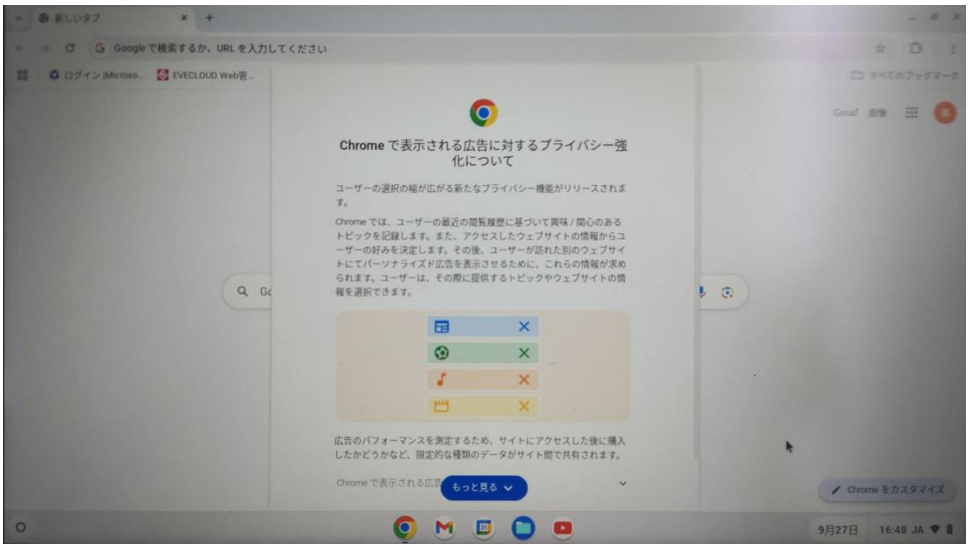
認証方法を選択し「次へ」をクリックします（ここでは顔認証を選択しています）。



顔をカメラに向け、顔認証を行います。



認証に成功すると、Chromebookにログインします。



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。