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



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
- 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

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。

新規に追加す 定してくださ	るアプリケーションの表示名、種類を言 い。
アプリケーシ	ョン表示名
Google Wor	rkspace
アプリケーシ	ョンの種類
SAML	v
SAML	~
SAML	~ 追加

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。

アプリケ-	-ション(の管理			ホーム
					グループの管理
アプリケーションの追加・	・削除が行えます。				アプリケーションの管理
追加または削除したアプリ	リケーションは、すべて	てのグループに反映されます。			認証セットの管理
フィルタ			\oplus	Ū	認証ポリシーの設定
アプリケーションの種類	アプリケーションID	アプリケーション表示名			
DM ID Manager	61000	商品管理システム			組織の管理
	70000	Google Workspace			個人の設定
SAML	10000	ooogie workspace			ログアウト
SAML	70001	chatwork			Ver 9389806

3 Copyright 2024 DDS, Inc. All Rights Reserved.

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。

Google WorkspaceのSAML SSO設定

サービスプロバイダー側に以下の情報を設定してください。

022	LIRI
330	UNL

https://saml.dds.click/saml/dds/sso/70000

ログアウト URL

https://saml.dds.click/saml/dds/slo/70000

メタデータURL

https://saml.dds.click/saml/dds/metadata/70000

X.509証明書のダウンロード

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。

- 😯 セキュリティ
 - 概要
 - アラートセンター
 - ▼ 認証

```
    2 段階認証プロセス
    アカウント復元
    高度な保護機能プログラム
    ログイン時の本人確認
    パスワードレス BETA
    パスワードの管理
    SAML アプリケーション
による SSO
    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



5 Copyright 2024 DDS, Inc. All Rights Reserved. 「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。 ● サービスプロバイダーの設定情報を直接入力する

Issuer

google.com/a/evecloud.com

ACS URL

SAML SSOレスポンスの送信先URLを入力してください

ログアウト URL

https://accounts.google.com/ServiceLogin?hl=ja&passive=true&continue=https://www.google.co.

```
-
SAMLログアウト後のリダイレクト先URLを入力してください
サービスプロバイダーからSAML SLOリクエストが送られた場合、リダイレクトは行わずにこのURLにSLOレスポンスを送信します
```

SPのX.509証明書

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

保存

PEM形式の証明書を入力してください (-----BEGIN CERTIFICATE-----と----END CERTIFICATE-----は入力しなくても問題ありません)

<u>キャンセル</u>

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。

ユーザー基本情報	ユーザーの設定	ホーム
パスワード・PIN設定		グループの管理
TOTP・QRコード設定 Windowsログオン設定	SAMLログイン設定	アプリケーションの管理 認証セットの管理 認証ポリシーの設定
ID Managerログイン設定 <u>SAMLログイン設定</u>	SAMLアプリケーション一覧	組織の管理
WebAuthn設定	SAMLアプリケーショ SAMLログインユーザー ン名	個人の設定
顏認証設定	Google Workspac e	ログアウト
保存		Ver bd1695a

<u>キャンセル</u>

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。

Google wo	rkspaceの編集
アカウント情報	を入力してください。
SAMLログインコ	レーザー
test_user01@	test.co.jp
サービスプロバイダー ールアドレスなどをフ	ーへのSAMLログインに使用するユーザーID、メ い力してください。
Chromebookの	パスワード
	◙
	グイン時の暗号化パスワードを設定します。
ChromebookのOSロ	
ChromebookのOSロ	
ChromebookのOS□	決定

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のバスワード	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。

ユーザー基本情報	ユーザーの設定	ホーム
パスワード・PIN設定		グループの管理
TOTP・ORコード設定		アプリケーションの管理
	CAMI ログイン記中	認証セットの管理
Windowsログオン設定	SAMLロジィン設定	認証ポリシーの設定
ID Managerログイン設定	SAMLアプリケーション一覧	知識の範囲
<u>SAMLログイン設定</u>		組織の官理
WebAuthn設定	SAMLアプリケーショ SAMLログインユーザー ン名	個人の設定
顔認証設定	Google Workspac e	ログアウト
		Ver bd1695a
保存		

キャンセル

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
 - 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「以前のバスワードを入 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

= 🔿 Admin	Q、 ユーザー、グループ、設定を	検索		¢	8 0	·:: 🖈
 「「デバイス」 	デバイス > Chrome > 設定					
概要 ▼ Chrome	設定	ユーザーとブラウザの設定デバ	「イスの設定 管3	聖対象ゲスト セ	ッションの	設定
セットアップ ガイド		+ フィルタを追加、または検索			❹ 最)	丘の変更点
デバイス	組織部門	^ ☑ セキュリティ				
登録トークン	組織部門を検索	設定	設定			継月
管理対象ブラウザ	- DDS demo		Chrome デバイフに対	T SAME OF	-7080-0	911.++
設定	Chromebook demo	シングル サインオン	インオンを有効にする	O C SAME / (-	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	-0
アプリと拡張機能	Normal demo	SAML シングル サインオンによるログインの別	頑度 毎日			0-
コネクタ						0
プリンタ		SAML シンシルサインオンのロック解除の間隔	9			Goc

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。

= 💽 Admin	Q、 ユーザー、グループ、設定を検索					¢	8	0		太郎
 - □ デバイス 	デバイス > Chrome > 設定 > ユーザーと	ニブラウザ > シン	グル サインオン							
概要 ▼ Chrome セットアップ ガイド デバイス	シングル サインオ ン	ChromeOS	デバイスに対して SAMI ポリシーを使用する前に してください。	- ベースのシングル サ ィ 、 <u>ChromeOS デバイス</u>	インオンを有効または無効に に SAML シングル サインオ	すること <i>!</i> ンを設定す	ができま <u>る</u> に記	ミす。 載され ⁻	ている	
登録トークン 管理対象プラウザ	組織部門 ^ 組織部門を検索	継承		ローカルに適用 👻						
設定	- DDS demo	設定		Chrome OS デバイス向	けの SAML ペースのシングル サ	インオン				
アプリと拡張機能	Chromebook demo			Chrome デバイスに	対して SAML ベースのシング	ブル サイン	オンを	有効にす	13	
コネクタ	Normal demo			Chrome デバイス向	けの SAML ベースのシングル	レサインオ	ンを無	効にする	5	
プリンタ										
・ レポート										
▶ モバイルとエンドポイント										
ネットワーク										
▶ Ⅲ アプリ										
▶ 😯 セキュリティ										
→ IL レポート										
▶										
 アカウント 										
⊕ 11-11		保存	キャンセル							

「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。

= 🔿 Admin	Q、 ユーザー、グループ、設定を検索				¢	8	0		大郎
▼ □ デバイス	デバイス > Chrome > 設定 > デバイス >	ユーザー データ							
 敬要 Chrome セットアップガイド デバイス 登録トークン 管理対象ブラウザ 	ユーザーデータ 組織部門 ^ 組織部門を検索 - DDS demo	登録済みの ChromeOS デバイスか +	らユーザーがログアウト 目定します。デバイスか カルユーザーデータを 取得されません。 パイスはすべてのユーキ ウスペリエンスを保証し すすめします。	するたびに、ローカルに保存: 5回開きれたデータはクラウド 割去した設定すると、ユーザーブ 管理対象ゲスト セッションとー 「ーデータを語号化し、複数の となるこの動作はほとんどの環 ます。[すべてのローカルユー	されてい; に残りま が使用で; ・緒に設か ユーザー 増に適し ザー デー	る設定 きした きした で 共お の た オ の た オ	とユー デバイ 春容 く する場合、 (する場う、 デー ((大) (大)	ザーデ イスデシ 合夕 限 定	
設定 アブリと拡張機能 コネクタ	Chromebook demo Normal demo	Chromium 名 DeviceEphemeralUsersEnabled [2	サポート対象 ChromeOS バージョ	ン 19 以降					
プリンタ		継承	ローカルに適用 👻						
 ・レポート ・モバイルとエンドポイント ネットワーク ・ Ⅲ アブリ ・ ② セキュリティ ・ Ⅰ. レポート ・ 一 お支払い 		187E	各ユーザーがログアクト すべてのローカル ユ 警告:ほとんどのデフロ すめしていません。詳し い。 ログアクト時にユーザ- Chrome デバイスで And センターとベスト プラ	した後に、ローカルのユーザー塀 ーザー データを消去 マ イにおいて、ログアウト時にユーザ くくは、ユーザーデータに開するへ ーデータを消去する場合は、セッシ 1001 アブリを許可しないことをお 2 <u>57ィスガイド</u> をご覧ください。	W、設定、 「ーデータ! レ <u>ブセンタ</u> ョンの起動 「すめしま	状態を を消去す <u>一記事</u> を最適 す。詳U	すべて泳 すること をご覧く 化するた いくは、	時去する はおす こださ とめに、 ヘルプ	
 ● アカウント ● ルール 		保存 キャンセル							

 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。

= 🔿 Admin	Q、 ユーザー、グループ、設定を検索				¢	8	0		太郎
- □ デバイス	デバイス > Chrome > 設定 > デバイス >	シングル サインオン ID プロバイダ(IdP) のリダイレクト						
概要 - Chrome セットアップガイド デバイス 登録トークン 管理対象ブラウザ	シングルサインオ ンID プロバイダ (IdP) のリダイレ クト	デ ^ジ (イスに SAML SSO を設定して をご覧ください。 シングル サインオン(SSO)ユー・ ジを直接表示できるようにするに す。 Chromium 名 LoginAuthenticationBehavior [2]	おく必要があります。 ザーが、最初にメールフ は、[シングル サインオ サポート対象 ChromeOS バージョ	<i>ChromeOS デバイスに SA</i> ?ドレスを入力しなくても ン ID プロバイダ(IdP)(ン 51 以降	I <u>ML シングル</u> 5 SAML ID プロ のリダイレク↓	サイン: コバイタ 、] 設定	<u>r (IdP)</u> を有効は	<u>定する</u> のペー こしま	<u>-</u>
設定 アプリと拡張機能 コネクタ プリンタ	組織部門を検索 ▼ DDS demo Chromebook demo	継承 設定	ローカルに適用 マ SAML SSO ID プロバイ	ダ(IdP)へのユーザーのリ	ダイレクト				
▶ レポート ▶ モバイルとエンドポイント ネットワーク > ₩ アブリ	Normal demo		SAML SSO IdP ~-	ジへの移動をユーザーに	許可する	Ľ			
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・									
⊕ <i>n</i> − <i>n</i>		保存 キャンセル							

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。

= O Admin	Q、 ユーザー、グループ、設定を検索				¢	8	0		太郎
 	デバイス > Chrome > 設定 > デバイス > : シングル サインオ	シングル サインオンによるカメラへのア デバイスに SAML SSO が設定されて るをご覧ください。	クセスの許可 てい <i>る必要があります</i> 。	ChromeOS デバイスに SAML :	シングル	・サイン	1726	設定す	t
セットアップ ガイド デバイス 登録トークン	ンによるカメラへの 🕚 アクセスの許可	重要:管理者がこのポリシーを有効 許可することになります。このポリ 許可の同意を求めることがないため	にすると、ユーザーのf リシーでカメラへのアク り、管理者は適切な同意	てわりにユーザーのカメラへの セスを許可すると、システムか 書を用意しておく必要がありま	アクセス トらエン ます。	くをサードユー!	-ドパー ザーにす	ティに すして	5
管理対象ブラウザ	組織部門 ^	SAML シングル サインスク(SSO) サードパーティのアプリまたはサー ChromeOS デバイスに新しい形の説	ラローの処理中にユー -ビスを指定します。こ 8証フローを提供できま	リーのカメラに直接アクセス9 の設定を行うと、サードパーテ す。	-10 ID	プロバ	टगा (तर्ज (IdP) (;	t
設定アプリと拡張機能	組織部門を検索 ・ DDS demo	ldP を許可リストに追加するには、 組織での Clever Badges のセットア	各サービスの URL を 1	行に 1 つずつ入力します。	確認くた	どさい。			
コネクタ プリンタ	Chromebook demo Normal demo	Chromium 名 LoginVideoCaptureAllowedUrls 2	サポート対象 ChromeOS バージョ	ン 52 以降	1000				
 レポート ▶ モバイルとエンドポイント 		継承	ローカルに適用 🔻						
ネットワーク ・ III アプリ		設定	カメラへのシングルサ https://saml.dds	トインオン アクセスが可能な URL .click/					
 ・ ・ ・ ・ ・ ・ ・ ・			管告: このポリシーを ってサードバーティレ スの許可について詳	revectioua.com/ 市効にすると、ユーザーのカメラへ こ許可することになります。シング) しくは、ヘルプセンター記事をご覧	へのアクセ ル サイン ください	zスを、: オンとえ	ユーザー カメラへ	・に代わ のアクヤ	, t
 ・ お支払い ・ ・ ・		保存 キャンセル							

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。

= 💽 Admin	Q、 ユーザー、グループ、設定を検索			¢	8	0		太郎
✓ □□ デバイス	デバイス > Chrome > 設定 > デバイス >	ログイン画面キーボード						
概要								
- Chrome	ログイン画面キーボ	ChromeOS デバイスのログイン画面	iで使用できるキーボード レイアウトを指定します。					
セットアップ ガイド	й — К	Chromium 名 DeviceLoginScreenInputMethods [2	サポート対象 ChromeOS バージョン 58 以降					
デバイス		enteregner ennipetitettete						
登録トークン	組織部門へ	継承	ローカルに適用 🔻					
管理対象ブラウザ	組織部門を検索							1
設定	✓ DDS demo	設定	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					
アプリと拡張機能	Chromebook demo		Q キーボード レイアウトでフィルタ		キーボ	ードレ	イアウ	10
コネクタ	Normal demo		ラテンアメリカ言語キーボード		日本語	キーボ	- 14	1
プリンタ			□ ラトビア語キーボード					-1
・レポート			□ リトアニア語キーボード					
・モバイルとエンドポイント			□ ルーマニア語キーボード					
ネットワーク								
> ## アプリ			レーマニア語標準キーボード	-				
・ ・ ・ セキュリティ			✓ 日本語キーボード					
→ Ih レポート			英国キーボード (南アフリカ)					
 お支払い 			英語 (カナダ) キーボード					
 アカウント 		87 572-771						
⊕ 𝒴−𝒴								

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。

~	-	
÷	Android スマートフォンから Wi-Fi を自動的に移行	
接続して、新しい	Contect-sections	
Chromebookのあらゆ	 harout trippen. 	
る機能をご活用くださ	🗙 multinoimilet	
5	 actor Tell Tellinates 	
次回 Chromebook を使用するときにご利用のネットワークが表示されます。	• CROTHANNAM	
	₽, ==	G
	9, mm	
	₽,	
		24. >

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。

G	
Chromebook の設定の 選択	 個人でのご利用 個人の Google アカウントを使用します
設定後にいつでも別のユーザーをデバイスに追 加できます。ユーザーごとに使用環境をカスタ マイズして、データのプライバシーを確保でき ます。	お子様が使用 お子様の Google アカウントまたは学校用アカウントを使用します。(収損者による使用物限を設定することもできます。)
	● 仕事向け 組織のメールアドレスを使用します
	t (75.)
REAL PROPERTY BUILDING	

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。

G		
デバイスの登録	メールアドレスまたは電話番号 taro@dds-demo.space	
Chromebook の登録の詳細	メールアドレスを忘れた場合	
	*	
		*

< 戻る			
G ようこそ ③ taro®dds-demo.space	/パスワードを入力 		
	רכגאו	ードをお忘れの場合	
	キオスクまたはサイネージデバイスを登録	のデバイスを登録	

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。

	D7 F24 million southed on CEXESCIT	
	Soogle Workspace(展示会デモ)	
	DDS, Inc.	
	ユーザーIDを入力 ion	
	232 ascienzaria	
	<u>*</u> ^	
	ログインボブクシュの行きっているかの Google アカウントの保険モ入力	
◎ 終了 ● ガストとしてブラウジング		16:46 JA 🐨 🛙

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)。

		Ver 1e35c93f	
	Weither Boogle Workspace(展示会デモ)		
	認証方法の選択		
		~	1000
	認証方法の更新 別のIDでログイン	•	
	<u></u> 		
		Google アカウントの情	報e入力
	国 Chromebook は dds-demo space によって管理されて	います	
じ 除了 ● ゲストとしてブラウジング			

```
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。