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
 - 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

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。

Themis & マガタマサービス管理ツール メニュー	
	ログイン先を選択してください
	個人用ポータルにログイン
	智理ツールにログイン
Copyright © 2018-2019 DDS, Inc.	

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。

Themis & マガタマサービス管理ツ	ノール メニュー	
	Themis Account Manager Login ver.1.4.0.40061	
	ユーザ選択・ admin PW パスワードを入力して「認証」を押してください。	
Conversion (2019, 2010, DDC		
Copyright © 2018-2019 DDS,	1250E	
	キャンセル	

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。

Themis & マガタマサービス管理ツール admin メニュー	ログアウト			
◎ユーザー ○グループ	基本情報	i 認証情報 ログビュ	-7-	
ユーザー ID 検索	テスト	テナント		
<u>^</u> #	アブリケー	ション		
王 ¹⁴	ID	アプリケーションネ	5	設定
7×F772F	50002	Management too	Logon	設定 詳細
 MAAdministrators [管理者] テストグループ 	50010	SAML application		1823 <mark>38.50</mark>
どのグループにも厚していないコーザー	認証セット			
*1	No.	ID	認証セット名	設定
20	1	39016	PW	
	2	39066	FACE	
	3	39104	OTP	
	4	39203	PW+OTP	
	5	39205	PW+FACE	
	追加	順序		
	認証要素			
	ID	認証要素名		設定
	16	Password		ツール 設定
	66	Face Authentication		ツール 設定
	104	Time-Based One-Time Pa	ssword	ツール 設定

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。

∮ユーザー ◎グループ	基本情報 認証情報 ログ ビューアー
ユーザー ID 検索	マプリケーションの光坦作成
全体 ・ テストテナント	アプリケーション3 2 00和15元1 FJ以 アプリケーション3 G Suite
ブループ	概要
 MAAdministrators [管理者] テストグループ 	利用可能な認証セット
ビのグループにも属していないユーザー	20056 DW
<i>ъ</i> с	 39104 OTP 39203 PW+OTP 39066 FACE 39205 PW+FACE \$\$\vee\$\$
pyright © 2018-2019 DDS, Inc.	

Google Workspaceの登録が完了すると以下の画面になります。

Themis & マガタマサービス管理ツール admin メニュ	ー ログアウト				
◉ユーザー ○グループ	基本情報	認証情報 ログ ビュー	-7-		
ユーザー ID 検索	アプリケー	ション情報を作成しました。			
全体 • テストテナント	テスト	テナント			
グループ	アフリケーシ ID	ョン アプリケーション名		設定	
 MAAdministrators [管理者] テストグループ 	50002	Management tool Log	on	設定 詳細	
どのグループにも属していないユーザー	50010	SAML application		設定 追加	
なし	70000	G Suite		設定 詳細 削除 SSO	
	認証セット				
	No.	ID	認証セット名	設定	
	1	39016	PW		
	2	39066	FACE		
	3	39104	OTP		
	4	39203	PW+OTP		
	5	39205	PW+FACE		
	追加	順序			
	認証要素				
	ID	認証要素名		設定	

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。

hemis & マガタマサービス管理ツール admin メ	ニュー ログアウ	15			
●ユーザー ◎グループ	基本情報	認証情報 ログ	ビューアー		
ユーザー ID 検索	テストラ	テナント			
全体	アプリケーショ	ョン			
• テストテナント	ID	アプリケーション名		設定	
グループ	50002	Management tool L	ogon	設定 詳細	
• MAAdministrators [管理者]	50010	SAML application		設定 追加	_
• テストグループ	70000	G Suite		設定 詳細 削除 SSC	0
どのグループにも属していないユーザー	認証セット				-
120	No.	ID	認証セット名		設定
	1	39016	PW		
	2	39051	FIDO		
	3	39052	WebAuthn		
	4	39104	OTP		
	5	39202	PW+FIDO		
	6	39203	PW+OTP		
	7	39204	PW+WebAuthn		
	追加	順序			

「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。

◎ユーザー ◎グループ		基本情報	認識正常報	ログビューアー
ユーザー ID	核第	SSO設	定情報	
全体				
• テストテナント		550	ウエンドポイン	https://themis140ro4-ibmsv0e.themis-magatama.com/admtool/sam
グループ				
 MAAdministrators テストグループ 	管理者]	SL	Dエンドボイン	https://themis140rc4-ibmsv0e.themis-magatama.com/admtool/sam Copy
どのグループにも属していた	ミンユーザー			
なし			メタデータ	https://themis140rc4-ibmsv0e.themis-magatama.com/admtool/sam Copy
			X.509証明』	表示
				BEGIN CERTIFICATE MiDDOLCOLMERIFIEGCARE_WAGG2EVGoowDQYIKoZIIWcHAQELBQAXX DELMAG ALUEBMKGIXAEJAQ6gWVMAQMCJ/EPyZpbLUBIgTTMECALUEBWKGTmP DIRILOX0 artEsMIAAA1UECgwJRERTLCBJbmMuMRAwDyTDVQQODAdER/PMgU1NPM BXXDTESMICA CUPYZpLUBIgTTMECALUEBWKGTmPhbJIbLXNoaTESMIBAGA1UECgwJ RERTLCBJ bmMuMRawDgYTDVQQDDAdER/PMgU1NPMIBIJANBjkqNikio9w6BAQEFAA CCAQUAMB CCACUAMB CCACUAMBA CCACUAMBA CCACUAMBA CC
				and the second se
				Copy

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。

≡ Google Admin	Q ユーザーまたは設定を	≥検索	8 ? ಈ
管理コンソール PN、121919&火、19393、 検索を行います	ビルティング、云遠 室、リソースを管理、 確認します	ノに体験したり	> ツール
アブリ ア ブリ アブリとアブリ設定を	セキュリティ セキュリティ セキュリティ設定を作	レポート 組織内での使用状況を	パートナーのサポートを受ける G Suite Marketplace G Suite ステータス ダッシュポー ド G Suite ご紹介プログラム
管理します			データエクスポート 管理対象に含まれないユーザー用 の移行ツール モバイル向け Google 管理 コンソール
お支払い サブスクリプションと	会社プロフィール 責社に関する情報を更	管理者の役割 管理者の役割を管理し	Google Play

「シングル サインオン (SSO) の設定」をクリックします。

≡ Googl	e Admin Q 検索	8	?	767
セキュリティ				
	API リファレンス API を有効にし、独自に作成したアプリケーションやサードパーティ製アプリケーションを介して、プ ロビジョニング、レボート、移行をプログラムで管理します。			
	シングル サインオン(SSO)の設定 ウェブベースのアプリケーション(Gmail やカレンダーなど)のユーザー認証を設定します。			
	高度な保護機能プログラム(ベータ版) ハイレベルの保護を必要とするユーザーのための、最も強固なセキュリティを設定します			
	Context-Aware Access (Beta)			



≡ Google Admin ि	検索	8 ? 👳
セキュリティ		
ヺ゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚	コバイダで SSO を設定する	
サードバーティをIDプI	コバイダとして設定するには、次の情報を入力してください。 🥝	
ログイン ページの URL		
ログアウト ページ URL	システムと G Suite へのログイン用 URL	
パスワード変更 URL	ー ユーザーがログアウトするときにリダイレクトする URL	-
	ユーザーがシステムでパスワードを変更する際にアクセスする URL です。定義す ンが有効になっていない場合でも表示されます	ー すると、この URL はシングル サインオ
認証の確認	ファイルを選択 ファイルが選択されていません アップロード	
		破棄 保存

「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。

≡ Google Admin	续索	8	?	
セキュリティ				:
✓ サードパーティの ID プロ	バイダで SSO を設定する			
サードパーティを ID プロ	バイダとして設定するには、次の情報を入力してください。 🛛			
ログイン ページの URL	https://themis140rc4-ibmsv0e.themis-magatama.com/admtool/saml			
ログアウトページ URL	システムと G Suite へのログイン用 URL https://themis140rc4-ibmsv0e.themis-magatama.com/admtool/saml			
パスワード変更 URL	ユーザーがログアウトするときにリダイレクトする URL			
	ユーザーがシステムでパスワードを変更する際にアクセスする URL です。定義すると、この UR が有効になっていない場合でも表示されます	L はシングルち	オインオン	
認証の確認	ファイルを選択 idpx509.cer アップロード			
	認証ファイルには、ログイン リクエストを確認するための Google 公開キーが含まれている必要	があります。	0	
✓ ドメイン固有の発行;	元を使用 🖉			
		破棄	保存	

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。

nemis & マガタマサービス管理ツール admin メ ● ユーザー ◎グループ	ニュー ログアウト 基本情報	認証情報 ログ ビュー	7-		
ユーザー ID 検索	テスト	テナント			
全体	アプリケーシ	/ヨン			
テストテナント	ID	アプリケーション名		設定	
グループ	50002	Management tool Logo	n	設定 詳細	
 MAAdministrators [管理者] 	50010	SAML application		設定 追加	
 テストグループ 	70000	G Suite		設定 詳細 訓除 \$	sso
どのグループにも属していないユーザー な!	認証セット				
-6.0	No.	ID	認証セット名		設定
	1	39016	PW		
	2	39066	FACE		
	3	39104	OTP		
	4	39203	PW+OTP		
	5	39205	PW+FACE		
	追加	順序			
	認証要素				
	ID	認証要素名			設定
	16	Password			ツール 設定
	66	Face Authentication			ツール 設定

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。

Themis & マカダマサービス管理ツール admin メニ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ユー ロクアウト 基本情報 認証情報	ログ ビューアー
ユーザー ID 検索	Service Provid	er情報の設定
全体 • テストテナント	SPの名前	G Suite
グループ	Issuer	google.com/a/dds-demo.space
 MAAdministrators [管理者] テストグループ どのグループにも属していないユーザー 	SSO エンドポイント	
なし	SLO エンドポイント	
	メタデータURL	
	フィンガープリント	
	RelayState	
	SAMLの設定	
		SAMLリクエストの署名検証を行う

設定が完了すると以下の画面になります。

「hemis & マガタマサービス管理ツール admin メニ:	1-107791				
◉ユーザー ○グループ	基本情報	認証情報 ログビュ	ーアー		
ユーザー ID 検索	SP情報を更	新しました。			
全体 • テストテナント	テスト	テナント			
グループ	ID	アプリケーション名		設定	
 MAAdministrators [管理者] テストグループ 	50002	Management tool Lo	gon	設定 詳細	
どのグループにも属していないユーザー	50010	SAML application		設定 追加	
なし	70000	G Suite		設定 詳細 削除 SSO	
	認証セット				
	No.	ID	認証セット名	8	殳定
	1	39016	PW		
	2	39066	FACE		
	3	39104	OTP		
	4	39203	PW+OTP		
	5	39205	PW+FACE		
	追加	順序			
	認証要素				
	ID	忍証要素名		設定	

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。

ューザー ◎グループ	基本情報	認証情報 ログ ビューアー			
ユーザー ID 検索	テスト	ユーザー			
	アブリケーシ	ョン			
• 77 b7 t > b	ID	アプリケーション名			設定
ブループ	50002	Management tool Logo	n		設定 詳細
MAAdministrators [管理者]	50010	SAML application			設定
・ テストグループ	70000	G Suite			設定詳細
ストグループのメンバー	認証セット				
721-9-	No.	ID	認証セット名		設定
	1	39016	PW		
	2	39066	FACE		
	3	39104	OTP		
	4	39203	PW+OTP		
	5	39205	PW+FACE		
	認証要素				
	ID 認識	正要素名		設定	
	16 Pas	ssword		ツール 設定 登録・更新	所 登録内容
	66 Fac	e Authentication		ツール 設定 登録・更新	析 登録内容

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。

「hemis & マガタマサービス管理ツール admin メニ	ユー ログアウト	
◎ユーザー ◎グループ	基本情報 認証情報 ログ ビューアー	
ユーザー ID 検索	Service Provider情報の設定	
全体 • テストテナント	ログインユーザ名 magatma.hanako@dds-demo.space	
グループ		
 MAAdministrators [管理者] テストグループ 	更新	
どのグループにも属していないユーザー		
なし		
Copyright © 2018-2019 DDS, Inc.		

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。

■¬_#_ ○ #	其木精部	物は特部 ログ	K			
ST-9- S21-2	021011010	BO BLE HIJ TR				
ユーザー ID 検索	SP情報を更	新しました。				
全体	テストコ	ューザー				
•	アプリケーショ	アプリケーション				
<i>ブループ</i>	ID	アプリケーショ	ン名	設定		
 MAAdministrators [管理者] テストグループ 	50002	Management	tool Logon	設定 詳細		
(のグループにも属していないユーザー	50010	SAML applicat	ion	設定		
なし	70000	G Suite		設定 詳細		
	認証セット					
	No.	ID	認証セット名	設定		
	1	39016	PW			
	2	39066	FACE			
	3	39104	OTP			
	4	39203	PW+OTP			
	5	39205	PW+FACE			
	認証要素					
	認証要素 ID 認証	要素名	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。

Google	
「Chromebook」へのログイン	
メールアドレスまたは電話番号	
メールアドレスを忘れた場合	
その他の設定	×^
アカウントを作成	
企業の登録	
< R0	

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。

	Google	
	企業の登録	
	13.88	
	メールアドレスまたは車が巻号 	
	メールアドレスを忘れた場合	
		次へ
	< 現る	
U Shut down		♥ ∰ 5:52

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	ChromeデバイスのOSログインにThemisの認証を使
(必須)	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	SAMLによるChromeデバイスのOSログインを行っ
イアログの表示を抑制する	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	Chrome デバイスの OS ログイン時にカメラ(顔認
(Themisとの連携が必要)	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。

≡ Google Admin	2、検索			8 ? III 77
デバイス管理				:
デバイスの設定				
ネットワーク				
Chrome 管理	U U	V	•	Jacob,
Google ミーディング ルーム ハードウェア	0	1	0	
Jamboard	モバイル デバイス Android、IOS、Google Sync デバイ スを管理します	Chrome デバイス Chrome デバイスを管理します	管理対象 ブラウザ Chrome ブラウザの管理	Google ミーティング ルーム ハード ウェア Google ミーティングルーム ハード
モバイル				ウエアの時間
セットアップ				
パスワードを設定				
Android 設定				
iOS 設定 NEW	T	<u> </u>		
計開設定	0			
デバイフを承辺	0			
「デバイス管理	> Chro	ome のページ	で「ユーザー」	とブラウザの設

¹³ Copyright 2020 DDS, Inc. All Rights Reserved.

定」をクリックします。

≡ Google Admin		8	?	😁
デバイス管理 > Chrome				
	Chrome 管理			
	デバイス Chrome デバイスの表示と管理			
	管理対象ブラウザ Chrome ブラウザを表示、管理します			
	ユーザーとブラウザの設定 Chrome ブラウザや Chrome デバイスでのユーザーベースの設定の管理			

「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。

1				JUICIX J	11 76
デバイス管理 > Chrome > 設定					新機能
組織部門の検索	5	ユーザーとブラウザの設定	デバイスの設定	管理対象ゲスト セッションの設計	2
- ddsmarket.online	29	+ フィルタを追加			
		シングル サインオン ローカルに適用しました マ ロ	Chrome OS デバイス向けの SAML ベースのシングル サインオン 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 このポリシーを使用するには、o Surie に SSO を設定してくださ い		
		TLS の RC4 暗号スイート Google のデフォルトに設定し ロ 🕝 🗣	RC4 を無効にする ~		
		リモート アクセス クライア ント ローカルに適用しました マ	リモート アクセス ホスト クライアントのドメイン		
			リモート アクセスのクライアントで必要なドメイン名を設定します() 行につき のドメイン)。 バージョン 59 以前の Chrome では、必要なドメイン名は 1 つの ボートされており、リストの最初のドメインが使用されます。	10 77	
組織部門を管理する		ローカル トラスト アンカー	ローカル アンカー SHA-1		

● 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。

≡ Google Admin	Q ユーザーまたは設定を検索	8	?	 e 7
デバイス管理 > Chrome				
	アプリと拡張機能 Android アプリと Chrome のアプリおよび拡張機能の管理			
	管理対象ゲスト セッションの設定 Chrome デバイスで管理対象ゲスト セッションの設定を管理します			
	デバイスの設定 Chrome のデバイス設定の管理			
	レポート Chrome デバイスの集計レポートを表示			
	Android アプリのレポート Android アプリのレポートを表示			

「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。

← 1個の設定を変更	Ēしました				元に戻す	保存
デバイス管理 > Chrome >	設定					新機能
組織部門の検索	<u> </u>	ユーザーとブラウザの設定		デバイスの設定	管理対象ゲスト セッションの設定	Ø
 ddsmarket.online 	· · ·	┣ フィルタを追加				
		ユーザー データ ローカルに適用しました マ	各ユーサ ローカル	ーがログアウトした後に、ローカルのユーザー情報、 - ユーザー データを消去しない マ	設定、状態をすべて消去する	
		シングル サインオン ID ブ ロバイダ(IdP)のリダイレ クト ローカルに適用しました マ	SAML SS SAML SS 一に許可	SO ID プロバイダ(IdP)へのユーザーのリダイレクト SO IdP ページへの移動をユーザ マ する		
		シングル サインオン Cookle の動作 ローカルに適用しました マ	ログイン SAML SS 警告: この 定されてい	中、ユーザーセッションへの = SO Cookie の転送を無効にする ポリシーは、Chrome デバイス向けに SAML SSO が設 いる場合にのみ該当します。詳細		
組織専門を範囲する		シングル サインオンによる カメラへのアクセスの許可 ロ−カルに適用しました マ	シングル 警告: この	- サインオンによるカメラへのアクセスを許可するアフ 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、	りのホワイトリ ユーザーに代	

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。

- 1個の設定を変更しました				元に戻9	1未1子
デバイス管理 > Chrome > 設定					新機制
織部門の検索	ユーザーとブラウザの設定		デバイスの設定	管理対象ゲスト セッションの設	定 🗹
ddsmarket.online	+ フィルタを追加	61) 			
	デバイスの壁紙画像	アップロード			
	□−フフルに適用しました ♥	まだどのユーザーもデ イン画面に表示する気 す。JPEG 形式でファイ てください。	バイスにログインしていない場合にログ 低間像を、デバイスレベルで設定しま ルサイズが 16 MB 以下の画像を指定し		
	ユーザー データ ローカルに適用しました マ	各ユーザーがログア すべてのローカル コ 去	ウトした後に、ローカルのユーザー情報、 ザー データを消 マ	股定、状態をすべて消去する	0
	シングル サインオン ID ブ	SAML SSO ID プロ/	(イダ(IdP)へのユーザーのリダイレクト		
	ロバイダ(ldP)のリダイレ クト ローカルに適用しました マ	SAML SSO IdP ペー ーに許可する	ジへの移動をユーザ 👻		
組織部門を管理する	シングル サインオン Cookie の動作	ログイン中、ユーザ SAML SSO Cookie Ø	ー セッションへの マ D転送を無効にする		

 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。

← 1個の設定を変更し:	ました					元に戻す保存
デバイス管理 > Chrome > 設定	}					新機能
組織部門の検索	1	ユーザーとブラウザの設定		デバイスの設定	管理対象ゲスト セッションの設定 🖸	
✓ ddsmarket.online	00	ト フィルタを追加				
		ログイン画面のキーボード ローカルに適用しました マ	ログイン	画面で使用するキーボードの順序リストを	E作成	
			Q	キーボード レイアウトでフィルタす	Order keyboards	
				ポーランド語キーボード	日本語キーボード	×
				マルタ語キーボード		
				ラテンアメリカ言語キーボード		
				ラトビア語キーボード		
				リトアニア語キーボード		
				ルーマニア語キーボード		
				日本語キーボード		
組織部門を管理する			-			

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。

16 Copyright 2020 DDS, Inc. All Rights Reserved. ※ 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。