「地方公共団体情報システム認証機能・ファイル連携機能に関するリファレンスガイド」に関するFAQ　　2024年10月31日更新

#	対象CSP	対象資料	質問	回答	掲載日
1	4CSP共通	リファレンスガイド（ファイル）	ファイル連携機能におけるSSO実装において、なぜOIDCではなくSAML.2.0を使用しているのでしょうか。	各リファレンスのアーキテクチャは「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参考に構成を決定しており、ガイドラインではインターネットへの接続を禁止しております閉域網を前提とした認証を実施するにあたり、OIDC利用時に4CSPの中で機能の仕様上閉域網での接続が難しいCSPがありますそのため、今回は4CSPでのアーキテクチャを統一させ、かつ閉域網での接続要件を満たすためにSAML V2.0を採用しております。	2023-12-20
2	4CSP共通	サンプルソースコード（ファイル）	署名鍵としてKeyCloakのキーのローテーションを実施した際に、IAM-SAMLプロバイダーの更新も実施する必要があるか教えてください。	CSPによって対応要否が異なりますので、以下の内容をご確認ください。 ■AWS レルム キーのローテーションによりレルムの SAML メタデータが変更されるため、IAM Identity Providerの メタデータを更新する必要があります。 ■Azure 現時点では、SAML フェデレーションは Azure に実装されていないため、レルム キーのローテーションは問題を引き起こしません 将来的にカスタム アプリが実装される場合、カスタム アプリの検証処理の実装方式によります。 ■Google Cloud レルム キーのローテーションによりレルムの SAML メタデータが変更されるため、GCP Workload Identity プールの IdP メタデータを更新する必要があります。 ■Oracle Cloud 現時点では、SAML フェデレーションは OCI に実装されていないため、レルム キーのローテーションは問題を引き起こしません 将来的にカスタム アプリが実装される場合、カスタム アプリの検証処理の実装方式によります。	2023-12-20
3	AWS	サンプルソースコード（API）	AWS-API認証において、デプロイ時に次のエラー（ERROR [3/6] RUN apk add libcrypto3=3.0.8-r0 libssl3=3.0.8-r0）が発生した対処法を教えて下さい。	以下のファイルを修正してください。 ■修正ファイル： ./reference-template-for-lg-auth-main/docker/resource-server/Dockerfile ./reference-template-for-lg-auth-main/docker/relyingparty-frontend/Dockerfile ./reference-template-for-lg-auth-main/docker/relyingparty-backend/Dockerfile ■修正対象箇所： 修正前：RUN apk add libcrypto3=3.0.8-r0 libssl3=3.0.8-r0 ↓ 修正後：RUN apk add libcrypto3=3.0.11-r0 libssl3=3.0.11-r0	2023-12-20
4	AWS	サンプルソースコード（API）	AWS-API認証において、dockerfile内の「sh init.sh」をデプロイした際に次のエラー（An image does not exist locally with the tag）が発生した対処法を教えてください。	以下のように修正してください。 ■修正ファイル： 対象ファイル： /reference-template-for-lg-auth-main/init.sh ■修正対象箇所： 修正前：docker build -t $containerName . ↓ 修正後：docker build -t $containerName:latest .	2023-12-20
5	AWS	サンプルソースコード（API）	AWS-API認証において、dockerfile内の「sh init.sh」を実行した際にコマンドエラー（ERROR [3/6] RUN apk add libcrypto3=3.0.8-r0 libssl3=3.0.8-r0）が発生した場合の対処法を教えてください	以下のように修正してください。 ■修正ファイル： docker/relyingparty-backend/Dockerfile、 docker/relyingparty-frontend/Dockerfile、 docker/resource-server/Dockerfile ■修正対象箇所： 修正前　libcrypto3=3.0.8-r0 libssl3=3.0.8-r0 ↓ 修正後　libcrypto3 libssl3	2023-12-20

#	対象CSP	対象資料	質問	回答	掲載日

6	AWS	サンプルソースコード（API）	AWS-API認証デプロイ時に、lg-auth-keycloak でS3バケットが作成できない場合の対処法を教えてください。	以下のように修正してください。
				■修正ファイル:
				lib/primary/keycloak-on-aws-stack.ts
				lib/primary/relying-party-stack.ts
				lib/primary/resource-server-stack.ts
				
				■修正対象箇所：
				修正前：
				// @@ -142,6 +142,7 @@ export class KeycloakOnAwsStack extends cdk.Stack
				const serverLogBucket = new s3.Bucket(this, "ServerAccessLogBucket", {
				// bucketName: 'server-access-log-bucket',
				encryption: s3.BucketEncryption.S3_MANAGED,
				blockPublicAccess: s3.BlockPublicAccess.BLOCK_ALL,
				enforceSSL: true,
				});
				↓
				修正後：
				// @@ -142,6 +142,7 @@ export class KeycloakOnAwsStack extends cdk.Stack
				const serverLogBucket = new s3.Bucket(this, "ServerAccessLogBucket", {
				// bucketName: 'server-access-log-bucket',
				encryption: s3.BucketEncryption.S3_MANAGED,
				objectOwnership: s3.ObjectOwnership.OBJECT_WRITER, //
				blockPublicAccess: s3.BlockPublicAccess.BLOCK_ALL,
				enforceSSL: true,
				});
					2023-12-20

7	AWS	サンプルソースコード（ファイル）	デプロイする際に、npx cdk deployにて以下のエラーが発生した際の対処法を教えてください。 ■エラー内容：Bundling asset lg-file-linkage-server/TriggerLambdaFunction-011002-000101-000201/TriggerLambdaFunction-011002-000101-000201/Code/Stage... esbuild cannot run locally. Switching to Docker bundling. ✗ [ERROR] Could not resolve "axios" asset-input/functions/download-trigger/index.ts:3:18: 3 | import axios from 'axios'; ~~~~~~~ You can mark the path "axios" as external to exclude it from the bundle, which will remove this error an d leave the unresolved path in the bundle.	各function配下で個別に'axios'をインストールする対応を実施してください。 cd functions/download-trigger npm i cd functions/notification-file-creation npm i	2023-12-20
8	AWS	サンプルソースコード（ファイル）	cdk.jsonのauthVpcIdが反映されない場合の対処法を教えてください。	以下のように修正してください。 ■修正ファイル：reference-template-for-lg-file-linkage.ts の56行目 ■修正内容：56行目に記載されているVpcIdの値を、authVpcIdの値に書き換える	2023-12-20
9	AWS	サンプルソースコード（ファイル）	AWS-ファイル連携デプロイ時に、npx cdk bootstrap がエラーになった際の対処法を教えてください。	lib/shared/flowlogs-construct.ts をreference-template-for-lg-auth-mainの同ファイルへのシンボリックリンクに差し替える対応を実施してください。	2023-12-20

#	対象CSP	対象資料	質問	回答	掲載日
10	Azure	サンプルソースコード（API）	Azure-API認証のbastionモジュールのデプロイ時にデプロイ名がかぶっていることが原因となるデプロイエラーが発生した時の対処法を教えてください。	bastionモジュールのdependsOnにssoBicepモジュールとの明示的な依存関係を指定することでエラー回避可能です。 ■修正ファイル： auth/bicep/lib/bastion/main.bicep の87行目 auth/bicep/lib/sso/main.bicep の 89行目 ■修正対象箇所： 修正前： dependsOn: [keycloakBicep relyingPartyBicep resourceServerBicep] ↓ 修正後： dependsOn: [keycloakBicep relyingPartyBicep resourceServerBicep ssoBicep]	2023-12-20
11	OCI	サンプルソースコード（API）	OCI-API認証デプロイ時に、次のエラーが出たときの対処法を教えてください。 ■エラー内容： L113 resource "oci_functions_function" "resource_server-authorizer" { L114　for_each = can(data.oci_artifacts_container_images.resource_server-authorizer.container_image_collection[0].items[0]) ? toset(["authorizer"]) : [] L115 L116	地方公共団体情報システム認証機能・ファイル連携機能に関するリファレンスガイド(OCI編)_令和6年3月版案の項番3.3.2に記載されているデプロイ手順を、以下のように変更して実施してください。 変更前： 1. 依存関係のインストール 2. デプロイ設定ファイルの更新 3. インフラリソースのデプロイ 4. Authorizer Functionsで使用するコンテナイメージをOCI Container Registryにプッシュ 5. SSL証明書情報の設定 6. Authorizer FunctionsのデプロイとSSL証明書情報の反映のためのインフラリソースデプロイ 7. OKEへのコンテナのデプロイ ↓ 変更後： 1. 依存関係のインストール 2. デプロイ設定ファイルの更新 3. 事前にRegistry周りのインフラリソースのデプロイ （oci_artifacts_container_repository と oci_artifacts_container_images） 4. Authorizer Functionsで使用するコンテナイメージをOCI Container Registryにプッシュ 5. インフラリソースのデプロイ 6. SSL証明書情報の設定 7. Authorizer FunctionsのデプロイとSSL証明書情報の反映のためのインフラリソースデプロイ 8. OKEへのコンテナのデプロイ	2023-12-20

12	Azure	サンプルソースコード（API）	Azure-API認証における、要求先システムの認可処理において次のエラーが出たときの対処法を教えてください。
			■エラー内容：
			Data: {
			"statusCode":401,
			"message":"Access denied due to missing subscription key. Make sure to include subscription key when making requests to an API."
			}
				以下のように対応してください。
				■対応内容：
				Azure API Managementのサブスクリプション要件を一時的に無効にし、認可処理を実行する。
					2024-03-14

#	対象CSP	対象資料	質問	回答	掲載日

13	AWS	サンプルソースコード（ファイル）	AWS-ファイル連携デプロイ時に、次のエラーが出たときの対処法を教えてください。
			■エラー内容：
			esbuild cannot run locally. Switching to Docker bundling.
			✗ [ERROR] Could not resolve "axios"
			
			asset-input/functions/download-trigger/index.ts:3:18:
			3 | import axios from 'axios';
				以下のように修正してください。
				■修正ファイル：
				①：/reference-template-for-lg-file-linkage-main/package.json
				②：/reference-template-for-lg-file-linkage-main/package-lock.json
				
				■修正内容
				変更前：
				"dependencies": {
				"aws-cdk-lib": "2.89.0",
				"cdk-nag": "^2.21.46",
				"constructs": "^10.0.0",
				"react": "^18.2.0",
				"source-map-support": "^0.5.21",
				"uuid": "^9.0.1"
				}
				変更後：
				"dependencies": {
				"aws-cdk-lib": "2.89.0",
				"axios": "^1.5.0",
				"cdk-nag": "^2.21.46",
				"constructs": "^10.0.0",
				"react": "^18.2.0",
				"source-map-support": "^0.5.21",
				"uuid": "^9.0.1"
				}
					2024-03-14

14	AWS	サンプルソースコード（ファイル）	AWS-ファイル連携デプロイ時に、次のエラーが出たときの対処法を教えてください。 ■エラー内容： fileLinkageCommonStorageBucket-011002-0001-0002-42d1a1ff33/S3BackupPlan (fileLinkageCommonStorageBucket011002000100024 2d1a1ff33S3BackupPlan820C2A1F) Resource handler returned message: "Insufficient privileges to perform this action. (Service: Backup, Status Code: 403, Request ID: c602f7d8-e2ed-47a1-b6e3-2f24d72dda18)" (RequestToken: 9329bebe-ac83-2c59-75cc-fa9fa3bbeb9e, HandlerErrorCode: GeneralServiceException)	以下のように修正してください。 ■修正ファイル： /reference-template-for-lg-file-linkage-main/lib/shared/common-storage-construct.ts ■修正内容 変更前： backupPlanName: 'aws/s3/custom-backup-plan', ↓ 変更後： backupPlanName: 'aws_s3_custom-backup-plan',	2024-03-14
15	AWS	サンプルソースコード（ファイル）	AWS-ファイル連携デプロイ時に、authVpcIDの値が異なることが原因となるエラーが発生した際の対処法を教えてください。	以下のように対応してください。 ■修正ファイル： /reference-template-for-lg-file-linkage-main/bin/reference-template-for-lg-file-linkage.ts 56行目　authVpcID: envVals.authVpcID ?? 'vpc-0c9983b75ac5d460e', ■対応内容 cdk.jsonのauthVpcIdの値を認証認可サーバが配置されているVPC IDに変更してください。	2024-03-14
16	AWS	サンプルソースコード(ファイル)	AWS-ファイル連携デプロイ時に、次のエラーが出たときの対処法を教えてください ■エラー内容： /home/ubuntu/environment/reference-template-for-lg-file-linkage-main/node_modules/ts-node/src/index.ts:859 return new TSError(diagnosticText, diagnosticCodes, diagnostics); ^ TSError:　Unable to compile TypeScript: lib/primary/file-linkage-server-stack.ts:13:26 - error TS2306: File '/home/ubuntu/environment/reference-template-for-lg-file-linkage-main/lib/shared/flowlogs-construct.ts' is not a module. 13 import { FlowLogs } from '../shared/flowlogs-construct';	以下のように対応してください。 ■対応内容 API認証のファイルから'reference-template-for-lg-file-linkage-main/lib/shared/flowlogs-construct.ts'と同名のファイルをコピーし、コピーしたファイルを利用して再度デプロイを実施してください。	2024-03-14

#	対象CSP	対象資料	質問	回答	掲載日
17	AWS	サンプルソースコード（ファイル）	AWS-API認証において、reference-template-for-lg-file-linkage-main/functions 以下のフォルダにおいて`npm ci`が原因のエラーが発生した際の対処法について教えてください。	以下のように対応してください。 ■対象フォルダ reference-template-for-lg-file-linkage-main/functions/notifcation-file-creation reference-template-for-lg-file-linkage-main/functions/download-trigger ■対応内容 上記の対象ファイルにて、`npm ci`を実行する。	2024-03-14
18	AWS	サンプルソースコード（API）	AWS-API認証デプロイ時に、reference-template-for-lg-file-linkage-main/cdk.jsonに設定したauthVpcIdが反映されない場合の対処法を教えてください。	以下のように修正してください。 ■修正ファイル： reference-template-for-lg-file-linkage-main/bin/reference-template-for-lg-file-linkage.ts ■修正内容 変更前： authVpcID: envVals.authVpcID?? 'vpc-0c9983b75ac5d460e', ↓ 変更後： authVpcID: envVals.authVpc**Id**?? 'vpc-0c9983b75ac5d460e',	2024-03-14

19	OCI	サンプルソースコード（API）	OCI-API認証デプロイ時に、terraform initの実行が失敗した際の対処法を教えてください。	以下のように対応してください。
				対応①
				■対象フォルダ
				auth/terraform/envs/backend.tf
				
				■対応内容
				上記フォルダにおいて、terraform.tfstateを保存するオブジェクトストレージの設定の記述を追加してください
				
				対応②
				■対象フォルダ
				auth/terraform/envs/versions.tf
				
				■対応内容
				上記フォルダにおいて、以下の内容を記述したうえでoci session authenticateを実施してください。
				provider "oci" {
				auth = "SecurityToken"
				config_file_profile = "ucdstorage"
				region = var.region
				}
					2024-03-14

20	OCI	サンプルソースコード（API）	OCI-API認証デプロイ時に、terraform planにおいて以下のエラーが発生した際の対処法を教えてください。 ■エラー内容 ╷ │ Error: Invalid for_each argument │ │ on ../../modules/container/main.resource_server.authorizer.tf line 114, in resource "oci_functions_function" "resource_server-authorizer": │ 114: for_each = can(data.oci_artifacts_container_images.resource_server-authorizer.container_image_collection[0].items[0]) ? toset(["authorizer"]) : [] │ ├──────────────── │ │ data.oci_artifacts_container_images.resource_server-authorizer.container_image_collection[0].items[0] is a object, known only after apply │ │ The "for_each" set includes values derived from resource attributes that cannot be determined until apply, and so │ Terraform cannot determine the full set of keys that will identify the instances of this resource. │ │ When working with unknown values in for_each, it's better to use a map value where the keys are defined statically in │ your configuration and where only the values contain apply-time results. │ │ Alternatively, you could use the -target planning option to first apply only the resources that the for_each value │ depends on, and then apply a second time to fully converge.	以下のように修正してください。 ■修正ファイル： auth/terraform/modules/container/main.resource_server.authorizer.tfの114行目 ■修正内容 変更前： for_each = can(data.oci_artifacts_container_images.resource_server-authorizer.container_image_collection[0].items[0]) ? toset(["authorizer"]) : [] ↓ 変更後： for_each = toset(["authorizer"])	2024-03-14

「地方公共団体情報システム認証機能・ファイル連携機能に関するリファレンスガイド」に関するFAQ　　2024年10月31日更新

#	対象CSP	対象資料	質問	回答	掲載日
21	AWS	サンプルソースコード（ファイル）	AWS-ファイル連携において動作確認実施時に、次のエラーが発生した際の対処法を教えてください。 ■エラー内容： Response signature invalid (service: AWSSecurityTokenService; status code: 400; error code: InvalidIdentityToken)	以下のように対応してください。 ■対応内容 IDプロバイダメタデータを更新してください。以下に実施手順を記載します。 (1) ブラウザからKeyCloakにアクセスし、一般タブからレルムの設定にアクセスしてください。 (2) エンドポイント SAML2.0アイデンティティー・プロバイダー・メタデータと表示されている箇所から、"SAMLMetaData.xml"をダウンロードしてください。 (3) AWSコンソール画面にアクセスしてください。 (4) AWS IAMにアクセスし、IDプロバイダを選択します。 (5) IDプロバイダの中からKeyCloakを選択し、XMLタブを押下します。 (6) XMLタブ内のデータを、2の手順で取得したメタデータ（SAMLMetaData.xml）に置換します。 (7) 再度動作確認を実施してください。	2024-03-14
22	4CSP共通	リファレンスガイド（ファイル）	ファイル連携サーバの共通オブジェクトストレージ内には「rireki」フォルダが含まれています。リファレンスガイド内の「4.6.4.1.データ保全」には、「ファイル連携サーバの共通オブジェクトストレージのバックアップを取得することを推奨する。」との記載がありますが、「rireki」フォルダが含まれている状態でもバックアップを取得する必要があるか教えてください。	「rireki」フォルダ自体は共通オブジェクトストレージ内に入っており、誤作動等でバケットごと削除した際などには「rireki」フォルダごと消えてしまいます。そのため、異なるバケットを用意したうえで、共通オブジェクトストレージのバックアップを取得することを推奨しています。	2024-03-14
23	Azure/OCI	リファレンスガイド（ファイル）	AzureおよびOCIのファイル連携リファレンスガイドにおいて、カスタムアプリ要件は以下のように記載されています。 1.認証認可サーバから発行されたトークンを検証し、CSP認証認可機能から一時的セキュリティ認証情報を受け取る機能（ファイル連携に関する詳細技術仕様書の図2-6における「連携」） 2.認証認可サーバから発行されたトークンの受け取り、CSP認証認可機能から発行された一時的セキュリティ認証情報の送付機能（ファイル連携に関する詳細技術仕様書の図2-6における「③④」） 3.日時的セキュリティ認証情報を利用して行うファイルの取得または格納の機能（ファイル連携に関する詳細技術仕様書の図2-6における「⑤」） カスタムアプリにより、提供側業務システムはCSPからの一時クレデンシャルを受け取ることになるのか、それともカスタムアプリがファイルアップロード/ダウンロードのAPIをもつのか教えてください。	AzureおよびOCIのファイル連携において実装するカスタムアプリについては、要件を満たしていることを前提としたうえで、実装は各自治体ならびに各社にて検討いただくことを想定しております。そのため、ご質問いただいている点につきましては、カスタムアプリケーションの作成方針により、提供側業務システムがCSPからの一時的クレデンシャルを受け取ることも、またカスタムアプリケーションがファイルのアップロード/ダウンロードのAPIを持つことも、どちらも選択肢としてとり得ると考えております。	2024-03-14
24	AWS	サンプルソースコード（API）	職員認証ログインページにおいて、wss://sample.lgauthdemo.local:80/wsに接続していることが原因のエラーが発生しました。対処法を教えてください。	wssで始まるHTTPリクエストは、フロントエンドから、バックエンドへのWebSocketの通信です。WebSockeの通信は発生しているものの、リファレンス実装の機能としてはWebSockeは利用されてなく、機能の実行に支障を及ぼすものではありません。 エラーの解消には、Create React Appを利用した本番用ビルド(https://create-react-app.dev/docs/production-build/)としてリファレンス実装をビルドしてください。ビルドされた静的ファイルをhttpサーバにてホストすること、該当のWebSocket通信は発生しなくなります。	2024-03-14
25	4CSP共通	リファレンスガイド（ファイル）	庁内連携機能におけるファイル連携機能を実装する場合、シングルクラウド構成であればCSP認証認可機能を利用したアカウント間連携を行うことは可能でしょうか。	「ファイル連携に関する詳細技術仕様書」の「2.3.4.連携ファイル格納方法」に記載のとおり可能です。 以下に各CSPにおける設定概要を記載します。 AWS：S3にアクセスする際の認証認可にIAMを利用する。 OCI：オブジェクトストレージにアクセスする際の認証認可にクロステナンシーポリシーを利用する。 Azure：Blob Storageにアクセスする際の認証認可にAzure RBACを利用する。 GCP：Cloud Storageにアクセスする際の認証認可にIAMを利用する。	2024-10-31
26	4CSP共通	リファレンスガイド	リファレンスガイドに記載されている構成に従う必要はありますか。	リファレンスガイドの内容は、推奨指針の位置づけとなるため、遵守を求めるものではなく、あくまで効率的に設計・構築を行うことを目的としたものです。	2024-10-31
27	AWS	リファレンスガイド（ファイル）	格納完了通知ファイルの検知は利用側システムで行う必要があると「ファイル連携に関する詳細技術仕様書」にて規定されていますが、リファレンスガイドAWS編ではS3のイベント通知をLambdaに送信することで検知を行う、またこの仕組みを作るのはオブジェクトストレージを構築する事業者と記載があります。 本記載は仕様書の記載と齟齬があるのではないでしょうか。	「ファイル連携に関する詳細技術仕様書」では、連携ファイル格納途中に提供側業務システムによる連携ファイル格納と利用側業務システムによる取込処理が重複しないよう、利用側システムが連携ファイル格納完了後に処理を行う仕様としています。 また、「地方公共団体情報システム認証機能・ファイル連携機能に関するリファレンスガイド(AWS編)」では、一例としてAWS Lambdaを利用する方式を示しており、当該仕様に沿った実装を妨げるものではありません。	2024-10-31
28	4CSP共通	リファレンスガイド（ファイル）	異なるCSP間でのファイル連携の詳細を整理してリファレンスガイドに追記いただけないでしょうか。	ファイル連携に関する詳細技術仕様書において、異なるCSPまたは対オンプレミスの場合は、認証認可サーバをIDプロバイダーとし、CSPの認証認可機能と連携させ、IdPでオブジェクトストレージの認証を行うことと規定しています。 また、リファレンスガイドの内容は、推奨指針の位置づけとなるため、遵守を求めるものではなく、あくまで効率的に設計・構築を行うことを目的としたものです。	2024-10-31