産業用データ連携基盤
基本設計書
認証・認可
別紙1 画面仕様

第1.0版

変更来歴

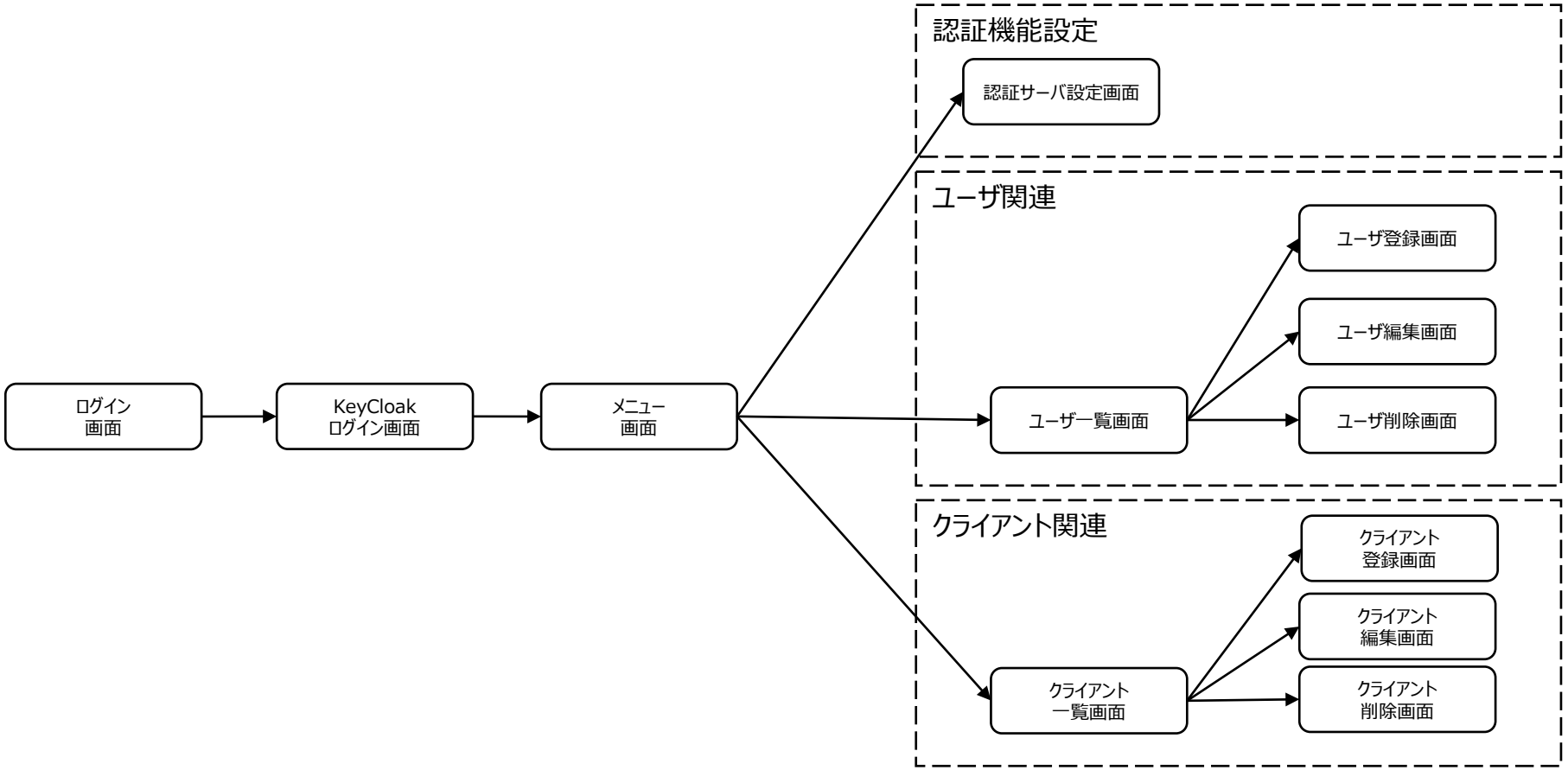
#	版数	発行年月日	変更内容
1	0.9	2023/11/14	・CADDEを活用して、産業用データ連携基盤を開発するにあたり版数0.9として作成 ・CADDEからDATA-EXに文言を修正 ・クライアント認証方式をクライアントID、シークレットから、クライアントID、クライアント証明書に変更 ・クライアント認証にて使用するため、クライアントの登録時に証明書のサブジェクトを登録するように修正 ・外部IdP連携管理機能は対象外のため削除 ・運用管理者を運営事業者に修正
2	1.0	2024/3/21	・基盤名称「DATA-EX」を「産業用データ連携基盤」に変更 ・「利用者」(データ利用者/利用者コネクタ等)を「受領者」に変更

目次

1. 認証機能画面

1. 認証機能画面 > 1.1. 画面遷移図

画面遷移図を以下に示す。



1. 認証機能画面 > 1.2. 入力変数説明

ユーザ新規入力項目の用語説明

#	画面	入力変数名	説明
1	認証サーバ設定	アクセストークン生存期間	アクセストークンが有効な時間の設定
2	認証サーバ設定	リフレッシュトークン生存期間	リフレッシュトークンが有効な時間の設定
3	ユーザ新規登録	DATA-EXユーザID	登録するユーザのDATA-EXユーザID設定
4	ユーザ新規登録	パスワード	登録するユーザのパスワード設定
5	ユーザ新規登録	姓	登録するユーザの姓設定
6	ユーザ新規登録	名	登録するユーザの名設定
7	ユーザ新規登録	Eメールアドレス	登録するユーザのEメールアドレス設定
8	ユーザ新規登録	住所	登録するユーザの住所設定
9	ユーザ新規登録	所属組織	登録するユーザの所属組織設定
10	ユーザ新規登録	その他の属性	登録するユーザのその他の属性設定
11	ユーザ新規登録	ワンタイムパスワード	一度のみ使用できるパスワードを使用するかの設定
12	ユーザ編集	DATA-EXユーザID	登録済みユーザのDATA-EXユーザID編集
13	ユーザ編集	姓	登録済みユーザの姓編集
14	ユーザ編集	名	登録済みユーザの名編集
15	ユーザ編集	Eメールアドレス	登録済みユーザのEメールアドレス編集
16	ユーザ編集	住所	登録済みユーザの住所編集
17	ユーザ編集	所属組織	登録済みユーザの所属組織編集
18	ユーザ編集	その他の属性	登録済みユーザのその他の属性編集
19	ユーザ編集	外部IdP名	外部IdPを使用する際、その外部IdP名の設定
20	ユーザ編集	外部IdPのユーザID	外部IdPを使用する際、その外部IdPユーザIDの設定
21	ユーザ編集	外部IdPのユーザ名	外部IdPを使用する際、その外部IdPユーザ名の設定
22	クライアント登録	クライアントID	登録するクライアントのクライアントID設定
23	クライアント登録	サブジェクト識別子設定	クライアント認証にクライアント証明書を用いるか否かの設定 設定するにした場合、クライアント証明書のサブジェクト（サブジェクト識別子）を設定できる サブジェクトとは国名、組織名、部門名、一般名で構成される識別子の要素

1. 認証機能画面 > 1.3. ログイン画面

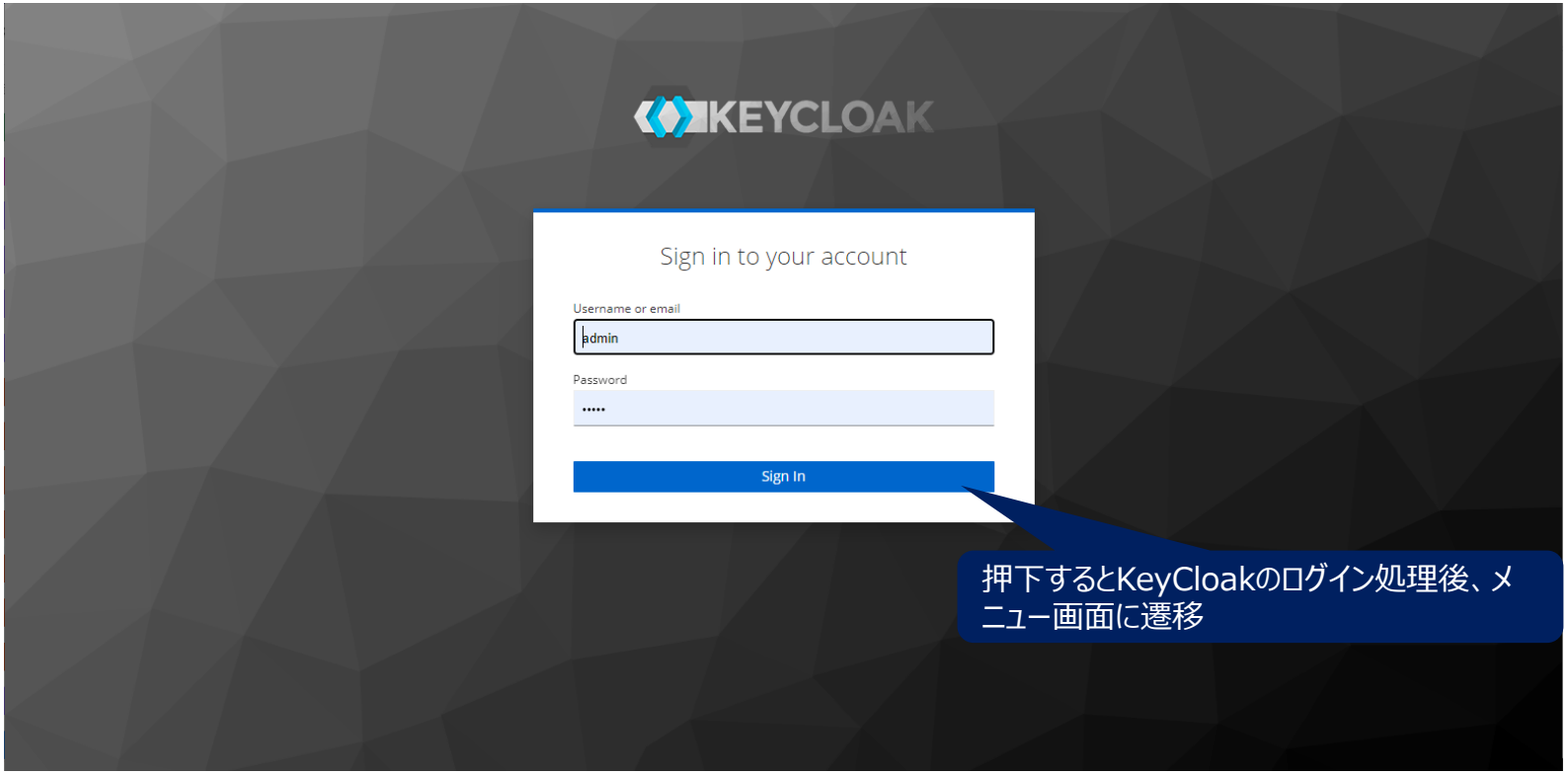
認証機能のデフォルト画面、ログインボタンから、KeyCloakのログインに遷移する

【画面上で使用するAPI】

#	Method	Request URL	Request Parameter	備考
①	POST	/dataex/api/v1/ui/authenticationUrl	url：リダイレクトURL	パラメータにはKeyCloakログイン後に戻ってくる認証機能画面のURLを指定

1. 認証機能画面 > 1.4. Keycloakログイン画面

管理者ログインID、パスワードでログインする



1. 認証機能画面 > 1.5. メニュー画面

ログイン後、左側のメニュー一覧から、①認証サーバ設定画面、②ユーザ画面、③クライアント画面に遷移可能

1. 認証機能画面 > 1.6.認証機能の設定画面

認証サーバの設定画面。アクセストークンの生存期間、リフレッシュトークンの生存期間を更新可能

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	トークン生存期間取得	GET	/dataex/api/v1/settings	-	-
②	トークン生存期間更新	PUT	/dataex/api/v1/settings	access_token_lifespan：アクセストークン生存期間 refresh_token_lifespan：リフレッシュトークン生存期間	-

1. 認証機能画面 > 1.7. ユーザ一覧画面

産業用データ連携基盤に登録されているユーザ一覧を表示する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Parameter	備考
①	ユーザ一覧取得	GET	/dataex/api/v1/users	-	DATA-EXユーザ一覧取得
②	ユーザ詳細取得	GET	/dataex/api/v1/users/{DATA-EXユーザID}	-	DATA-EXユーザ詳細取得

1. 認証機能画面 > 1.8. ユーザ一覧画面(パスワード変更)

産業用データ連携基盤に登録されているユーザのパスワードを変更する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	パスワード変更	PUT	/dataex/api/v1/users/{DATA-EXユーザID}/password	password：パスワード	DATA-EXユーザパスワード更新

1. 認証機能画面 > 1.9. ユーザ登録画面

産業用データ連携基盤にユーザを登録する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	ユーザ登録	POST	/dataex/api/v1/users	DATA-EX_id：DATA-EXユーザID first_name：姓 last_name：名 email：メールアドレス address：住所 organization：所属組織（複数） password:パスワード extras:その他属性 otp:ワンタイムパスワード（オプション）	DATA-EXユーザ登録

1. 認証機能画面 > 1.10. ユーザ編集画面

産業用データ連携基盤のユーザを編集する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	ユーザ編集	PUT	/dataex/api/v1/users/{DATA-EXユーザID}	first_name：姓 last_name：名 email：メールアドレス address：住所 organization：所属組織（複数） extras：その他属性	DATA-EXユーザ更新

1. 認証機能画面 > 1.11. ユーザ削除画面

産業用データ連携基盤のユーザを削除する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	ユーザ削除	DELETE	/dataex/api/v1/users/{DATA-EXユーザID}	-	-

1. 認証機能画面 > 1.12. クライアント一覧画面

産業用データ連携基盤のクライアント一覧を表示する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Parameter	備考
①	クライアント一覧取得	GET	/dataex/api/v1/clients	-	-
②	クライアント詳細取得	GET	/dataex/api/v1/clients/{クライアントID}	URL： client_id：クライアント名	-

1. 認証機能画面 > 1.13. クライアント登録画面

産業用データ連携基盤のクライアントを登録する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Body	備考
①	クライアント登録	POST	/dataex/api/v1/clients	client_id：クライアントID subject_dn：サブジェクト識別子(オプション)	-

1. 認証機能画面 > 1.14. クライアント編集画面

産業用データ連携基盤のクライアントを編集する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Parameter	備考
①	クライアント情報更新	PUT	/dataex/api/v1/clients/{クライアントID}	subject_dn：サブジェクト識別子	-
②	クライアントシークレット更新	PUT	/dataex/api/v1/clients/{クライアント名}/secret	-	-

1. 認証機能画面 > 1.15.クライアント削除画面

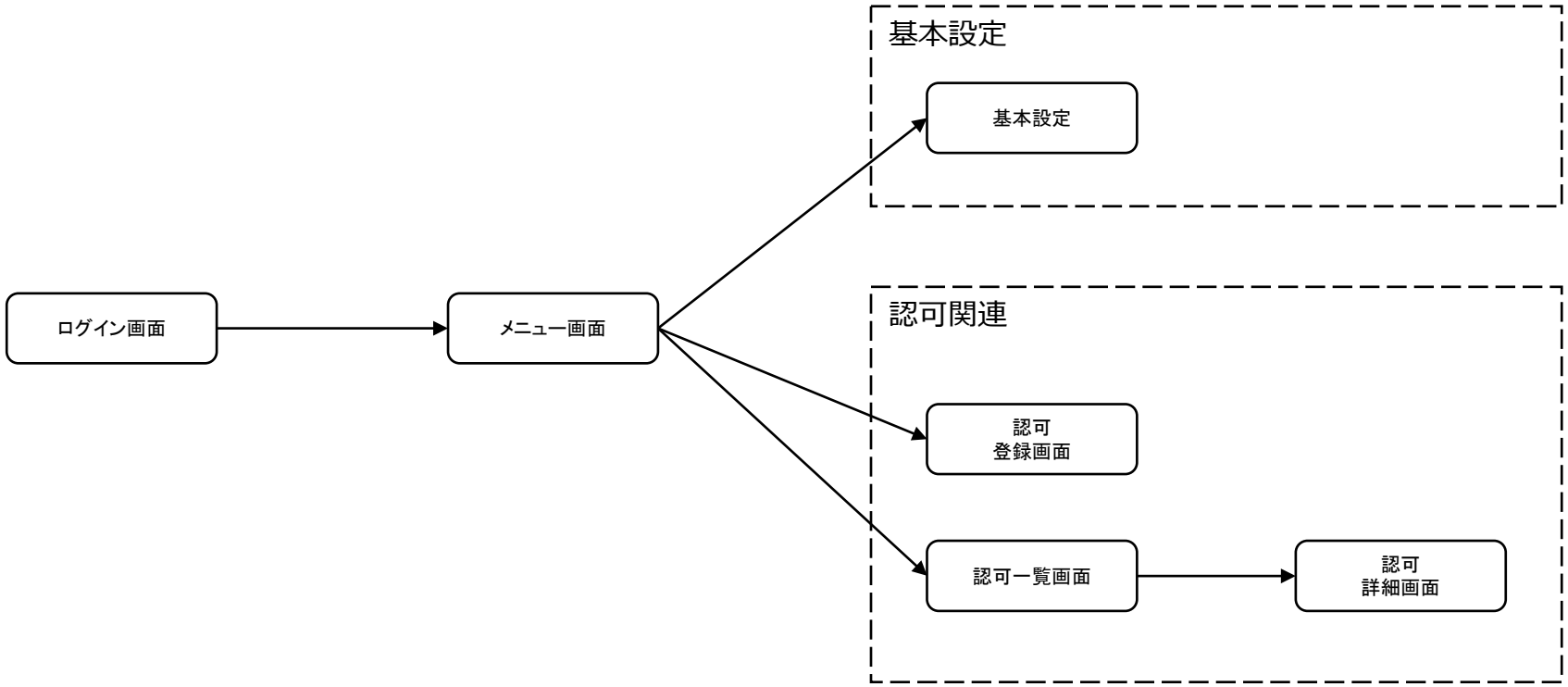
産業用データ連携基盤のクライアントを削除する画面

【画面上で使用するAPI】

#	API名	Method	Request URL	Request Parameter	備考
①	クライアント削除	DELETE	/dataex/api/v1/clients/{クライアントID}	-	-

2. 認可機能画面

画面遷移図を以下に示す。

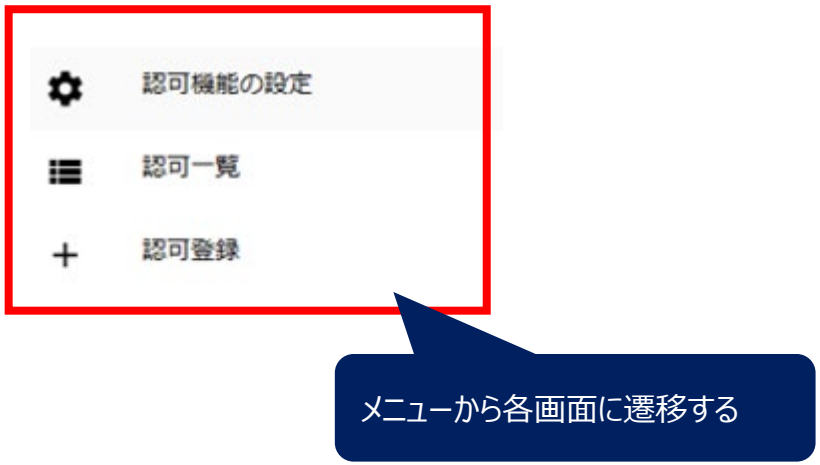


2. 認可機能画面 > 2.2. 入力変数説明

ユーザ新規入力項目の用語説明

#	画面	入力変数名	説明
1	認可の設定	アクセストークン生存期間	アクセストークンが有効な時間の設定
2	認可の設定	UserInfo URL	UserInfo URLの設定
3	認可の登録	配信のURL(使用可能文字は半角英数、ハイフン、アンダーバーのみ)	配信のURLの設定
4	認可の登録	ユーザのDATA-EXユーザID	ユーザに対する認可の設定
5	認可の登録	組織のDATA-EXユーザID	組織に対する認可の設定
6	認可の登録	当人認証レベルに対する認可	当人認証レベルに対する認可の設定
7	認可の登録	契約　(取引ID)	契約管理(取引市場)から発行された取引D
8	認可の登録	契約　(契約管理URL)	契約管理(取引市場)のURL

2. 認可機能画面 > 2.3. ログイン画面


認可機能の設定
認可一覧
認可登録
メニューから各画面に遷移する

2. 認可機能画面 > 2.5. 認可機能の設定画面

2. 認可機能画面 > 2.6. 認可登録画面


認可機能の設定
認可一覧
認可登録
認可機能
Login : xxxxxx
ログアウト
認可一覧
配信のURL
https://example.com
https://example.jp
各URLを押下することで
認可詳細画面に遷移する
表示数 All
2項目中1～2項目を表示中

2. 認可機能画面 > 2.8. 認可詳細画面

2. 認可機能画面 > 2.9. エラーメッセージ一覧

ユーザ側の入力ミスやサーバ側の状態不良などによって発生したエラーに対して画面に表示されるエラーメッセージの一覧を以下に示す。

#	画面	動作	エラー対象	エラーコード	表示されるエラーメッセージ
1	認可機能設定画面	認可設定画面への遷移時	アクセストークン生存期間	403	有効期限切れのためアクセストークン生存期間の取得ができませんでした。ログインしなおしてください。
2	認可機能設定画面	認可設定画面への遷移時	アクセストークン生存期間	403以外	サーバ障害のためアクセストークン生存期間の取得ができませんでした。サーバの状態を確認してください。
3	認可機能設定画面	認可設定画面への遷移時	クライアントシークレット	403	有効期限切れのためクライアントシークレットの取得ができませんでした。ログインしなおしてください。
4	認可機能設定画面	認可設定画面への遷移時	クライアントシークレット	403以外	サーバ障害のためクライアントシークレットの取得ができませんでした。サーバの状態を確認してください。
5	認可機能設定画面	認可設定画面への遷移時	UserInfo URL	403	有効期限切れのためUserInfo URLの取得ができませんでした。ログインしなおしてください。
6	認可機能設定画面	認可設定画面への遷移時	UserInfo URL	403以外	サーバ障害のためUserInfo URLの取得ができませんでした。サーバの状態を確認してください。
7	認可機能設定画面	認可設定の更新時	アクセストークン生存期間	403	有効期限切れのためアクセストークン生存期間の更新ができませんでした。ログインしなおしてください。
8	認可機能設定画面	認可設定の更新時	アクセストークン生存期間	403以外	サーバ障害のためアクセストークン生存期間の更新ができませんでした。サーバの状態を確認してください。
9	認可機能設定画面	認可設定の更新時	クライアントシークレット	403	有効期限切れのためクライアントシークレットの更新ができませんでした。ログインしなおしてください。
10	認可機能設定画面	認可設定の更新時	クライアントシークレット	403以外	サーバ障害のためクライアントシークレットの更新ができませんでした。サーバの状態を確認してください。
11	認可機能設定画面	認可設定の更新時	UserInfo URL	403	有効期限切れのためUserInfo URLの更新ができませんでした。ログインしなおしてください。
12	認可機能設定画面	認可設定の更新時	UserInfo URL	403以外	サーバ障害のためUserInfo URLの更新ができませんでした。サーバの状態を確認してください。
13	認可一覧画面	認可一覧画面への遷移時	認可一覧	403	有効期限切れのため認可一覧の取得ができませんでした。ログインしなおしてください。
14	認可一覧画面	認可一覧画面への遷移時	認可一覧	403以外	サーバ障害のため認可一覧の取得ができませんでした。サーバの状態を確認してください。
15	認可詳細画面	認可詳細画面への遷移時	認可詳細	403	有効期限切れのため認可詳細の取得ができませんでした。ログインしなおしてください。
16	認可詳細画面	認可詳細画面への遷移時	認可詳細	403以外	サーバ障害のため認可詳細の取得ができませんでした。サーバの状態を確認してください。
17	認可詳細画面	認可の削除時	認可削除	403	有効期限切れのため認可削除ができませんでした。ログインしなおしてください。
18	認可詳細画面	認可の削除時	認可削除	403 404以外	サーバ障害のため認可削除ができませんでした。サーバの状態を確認してください。
19	認可登録画面	認可の登録時	認可登録	403	有効期限切れのため認可登録ができませんでした。ログインしなおしてください。
20	認可登録画面	認可の登録時	認可登録	403以外	サーバ障害のため認可登録ができませんでした。サーバの状態を確認してください。