別表第一付表第三（第一条関係）

クライアントアサーションJWT生成方法

本APIのリクエストに必要なクライアントアサーションJWTの生成方法を記載する。

生成方法

1) ヘッダ部分のJSON文字列をbase64urlエンコードする

2) ペイロード部分のJSON文字列をbase64urlエンコードする

3) 1)で作成したbase64urlエンコード後の文字列と2)で作成したbase64urlエンコード後の文字列を"."で接続した文字列を、クライアントシークレットをキーに利用して、HMAC SHA-256アルゴリズムで計算した値をbase64urlエンコードする

4) 1)で作成したbase64urlエンコード後の文字列、2)で作成したbase64urlエンコード後の文字列、3)で作成したbase64urlエンコード後の文字列を"."で接続した値が、クライアントアサーションJWT

※1 【必須】　:「◎」･･･ パラメータまたはオブジェクトが必ず出現する。

ヘッダ (JSON)

| 項番 | パラメータ名 | 項目名 | 項目説明 | 必須<br>※1 | データ型 | 文字種 | データ長<br>桁数 | 検索方法 | 備考 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | alg | アルゴリズム | 署名のアルゴリズム | ◎ | 文字列 | 半角英字記号 | 5 | | "HS256"固定 |

ペイロード (JSON)

| 項番 | パラメータ名 | 項目名 | 項目説明 | 必須<br>※1 | データ型 | 文字種 | データ長<br>桁数 | 検索方法 | 備考 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | iss | 発行者 | クライアントアサーションJWTの発行者 | ◎ | 文字列 | 半角英数字記号 | 32 | | 要求元システムのクライアントIDを指定（32文字） |
| 2 | sub | 主体 | クライアントアサーションJWTの主体 | ◎ | 文字列 | 半角英数字記号 | 32 | | 要求元システムのクライアントIDを指定<br>（32文字） |
| 3 | aud | 対象者 | クライアントアサーションJWTの発行対象者 | ◎ | 文字列 | 半角英数字記号 | - | | 基本的には、認証認可サーバのURL(認証認可サーバのissuerの値)を含むものとする<br>ただし、認証認可サーバを示す識別子の範疇を超えない限り（トークンエンドポイント等）、認証認可サーバ側の判断による変更も可能とする。変更する場合は、RP側に必ずその旨を伝えること。 |
| 4 | jti | JWT ID | JWTのID | ◎ | 文字列 | 半角英数字記号 | - | | 発行者が発行したJWTを一意に識別するためのID<br>データの桁数は、一意に識別するために十分なエントロピーが確保可能な桁数を指定 |
| 5 | exp | 有効期限 | クライアントアサーションJWTの有効期限 | ◎ | 数値 | 半角数字 | 10 | | 発行されたクライアントアサーションJWTの有効期限のUNIX時間 |
| 6 | iat | 発行時刻 | クライアントアサーションJWTの発行時刻 | ◎ | 数値 | 半角数字 | 10 | | 発行されたクライアントアサーションJWTの発行時刻のUNIX時間 |