GMOあおぞらネット銀行

オープンAPI仕様書
認可編（OpenID Connect）

Version : 1.20.0
Last Modified 2025/10/13



GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

変更履歴

版数	内容	区分	更新日
1.0.0	新規作成	新規	2018/08/15
1.1.0	一般提供	変更	2019/01/10
1.2.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2019/03/28
1.2.1	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2019/06/20
1.3.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2019/08/10
1.4.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2020/02/08
1.5.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2020/07/11
1.6.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2021/05/10
1.7.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2021/06/14
1.8.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2021/07/12
1.8.1	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2021/10/11
1.9.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2021/11/15
1.10.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	新規	2022/06/11
1.10.1	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2022/06/11
1.11.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2022/07/11
1.12.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2022/11/14
1.12.1	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2023/01/13
1.13.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2023/03/11
1.14.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2023/05/13
1.15.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2023/10/14
1.16.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2024/07/15
1.17.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2024/09/10
1.18.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2025/05/12
1.19.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2025/09/15
1.20.0	他資料の修正に伴いバージョンアップ(当仕様書に更新なし)	変更	2025/10/13

©GMO Aozora Net Bank, Ltd. All Rights Reserved.

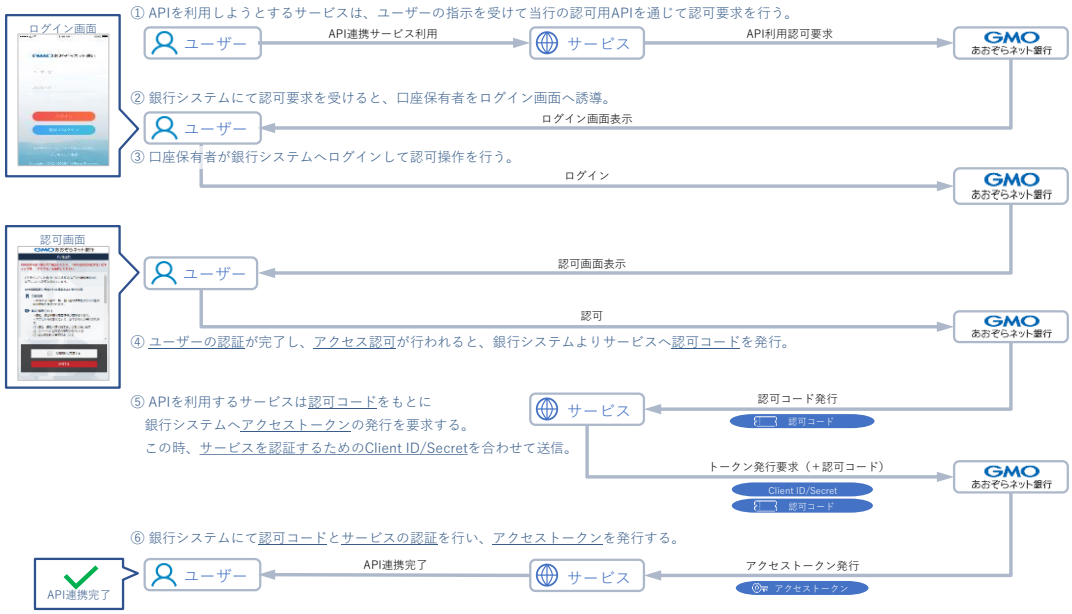
オープンAPI仕様書	エンドポイント一覧

カテゴリ	API種別	スコープ	API	概要
認可	認可系	—	認可エンドポイント	クライアントがユーザーの認証・認可を得るためのエンドポイント
			トークンエンドポイント	認可エンドポイントで取得した認可コードを用いたアクセストークンの取得及びリフレッシュトークンを用いたアクセストークンの更新を行うためのエンドポイント
			ユーザー情報エンドポイント	ユーザーの一意な識別子の取得を行うためのエンドポイント ログインしたユーザーの一意な識別子が必要な場合にのみ利用 （同様の情報はIDトークンに含まれているため、IDトークン検証時に取得可能）

GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

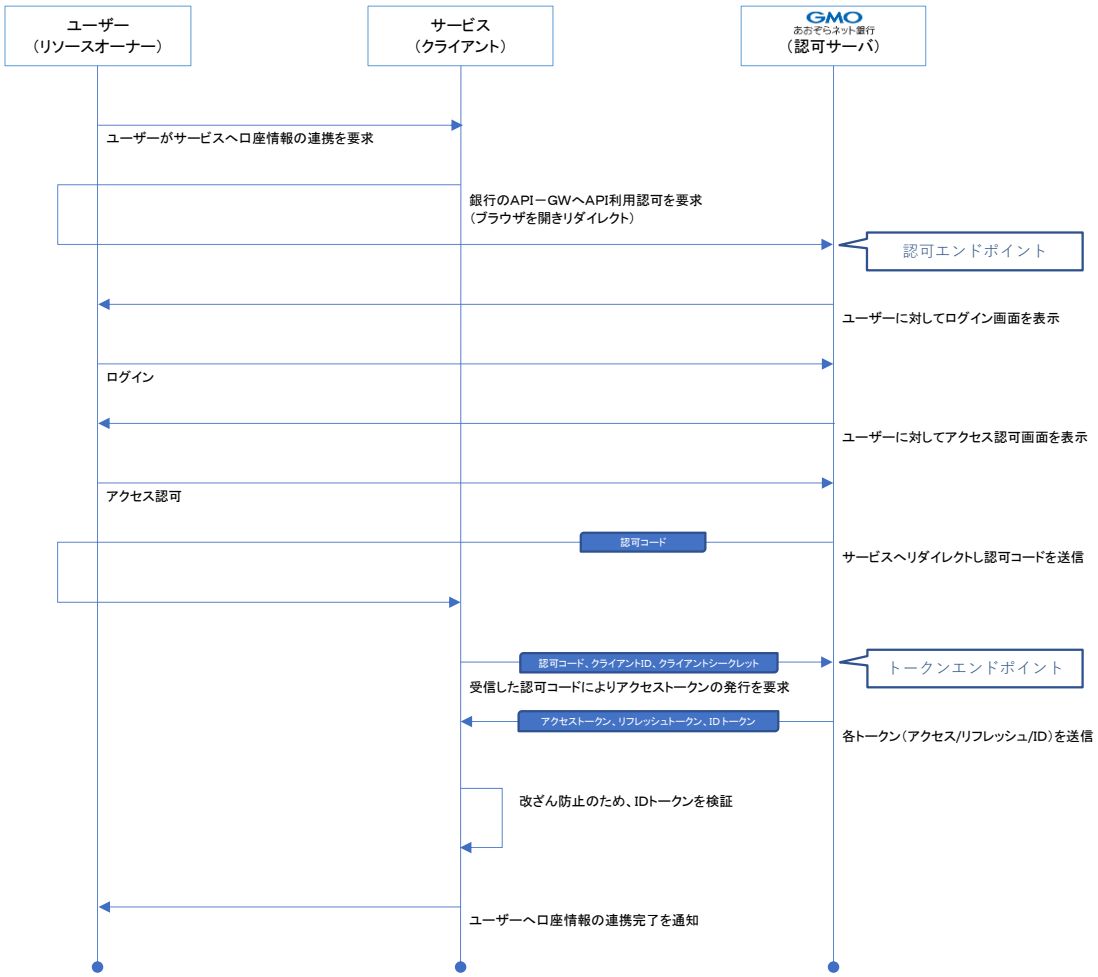
オープンAPI仕様書　認可フロー

API利用認可の流れ



認可フロー

Authorization Code フロー（OpenID Connect）



GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

オープンAPI仕様書	エンドポイント名	認可エンドポイント

要求

URL例

本番環境	https://api.gmo-aozora.com/ganb/api/auth/v1/authorization?response_type=code&scope=[スコープ]&client_id=[クライアントID]&state=[ステート値]&redirect_uri=[リダイレクト用URL]
開発環境	https://stg-api.gmo-aozora.com/ganb/api/auth/v1/authorization?response_type=code&scope=[スコープ]&client_id=[クライアントID]&state=[ステート値]&redirect_uri=[リダイレクト用URL]

プロトコル　HTTPS

HTTPメソッド　GET

クエリ文字列

パラメータ名	必須	説明	最小桁数	最大桁数
client_id	○	クライアントID （当社が事前に発行する貴社向けのID）	1	128
redirect_uri	○	貴社が指定する認可コードをリダイレクトするためのURI 事前に登録済みのリダイレクトURIであることが必要、それ以外の場合はエラーとなります	1	256
response_type	○	認可フロータイプ "code"固定。（Authorization Code Flow）	-	-
scope	○	要求されるアクセス権限を示すスコープID 複数設定する場合は半角スペース区切りにて連結 OpenID Connectの場合"openid" scope値は必須で、存在しない場合はOAuth2.0要求として処理します リフレッシュトークンを発行する場合は "offline_access" scope値が必要 各エンドポイントのスコープはそれぞれのAPI仕様書を参照 （個人向けAPIのスコープと、法人向けAPIのスコープを同時に指定することはできません） 例：openid offline_access private:account private:virtual-account （口座情報照会権限、振込入金口座情報照会権限）	1	256
state	○	貴社にて指定（要求と応答の間で維持されるランダム値） CSRF対策として同一のセッションであることを確認するために利用する項目	1	128
nonce		Client セッションと ID Token を紐づける文字列 設定された場合はそのままの値をID Tokenに含めて返却する リプレイアタック攻撃を防止するため、リクエスト毎にランダム値（十分な不規則性となる値）を設定し、 ID Tokenに含まれるnonce値が認可エンドポイントリクエスト時と同一であることを一度だけ検証するために利用する項目	1	128

リクエスト具体例

```
GET /ganb/api/auth/v1/authorization?
client_id=b3E5hpXFlMbCutYhFiO7
&redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
&response_type=code
&scope=openid%20offline_access%20private%3Aaccount%20private%3Avirtual-account
&state=af0ifjsldkj
&nonce=ef3a091928d5491624c0ac54d697124422705092
HTTP/1.1
Host: api.gmo-aozora.com
```

応答

応答形式　リダイレクト

HTTPボディ

パラメータ名	必須	説明	最小桁数	最大桁数
code	○	エンドユーザにより認可（許諾）された場合に、発行される認可コード	1	128
state	○	要求時に指定された値をそのまま返却する 貴社にて要求時と同一であることを確認	1	128

レスポンス具体例

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?
  code=SplxlOBeZQQYbYS6WxSbIA
  &state=af0ifjsldkj
```

エラー応答形式　Bad Request、またはリダイレクト

HTTPボディ

HTTPステータスコード	パラメータ名	必須	説明	最小桁数	最大桁数
400			クライアント情報が不正、リダイレクトURIが不正		
302			HTTP400時以外のエラーの場合		
	error	○	エラーコード ・invalid_request：要求パラメータが不正（必須パラメータの値が空）※必須パラメータキーの設定がない場合は400 ・access_denied：リソース所有者か認可サーバが要求を否定 ・invalid_scope：要求されたscopeが、無効、未知 ・server error：API-GWサーバにてエラーが発生	-	-
	error_description		エラー内容（ASCIIコード「%x20-21 / %x23-5B / %x5D-7E」の範囲の文字種）	-	-
	error_uri		エラーについての追加情報を含むWebページのURI	-	-
	state	○	要求パラメータのstate	1	128

レスポンス具体例

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?
  error=invalid_request
  &error_description=Unsupported%20response_type%20value
  &state=af0ifjsldkj
```

GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

オープンAPI仕様書	エンドポイント名	トークンエンドポイント（アクセストークン新規発行時）

要求

URL例

本番環境	https://api.gmo-aozora.com/ganb/api/auth/v1/token
開発環境	https://stg-api.gmo-aozora.com/ganb/api/auth/v1/token

プロトコル　HTTPS

HTTPメソッド　POST

HTTPヘッダ

ヘッダ名	必須	説明	最小桁数	最大桁数
Content-Type	○	application/x-www-form-urlencoded	-	-
Authorization		クライアント認証用のBasic認証値 （クライアントIDとクライアントシークレットを":"（コロン）で連結し、Base64エンコードしたものを設定） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は必須 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は設定不要	-	-

HTTPボディ

パラメータ名	必須	説明	最小桁数	最大桁数
grant_type	○	"authorization_code"固定	-	-
code	○	認可エンドポイントにて当社から返却した認可コード	1	128
redirect_uri	○	貴社が指定する認可コードをリダイレクトするためのURI 事前に登録済みのリダイレクトURIであることが必要、それ以外の場合はエラーとする ※認可エンドポイント要求時の「redirect_uri」と同じ値	1	256
client_id		クライアントID（貴社認証用の項目） （当社が事前に発行する貴社向けのID） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は設定不要 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は必須	1	128
client_secret		クライアントシークレット（貴社認証用の項目） （当社が事前に発行する貴社向けのシークレット） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は設定不要 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は必須	1	128

リクエスト具体例

```
POST /ganb/api/auth/v1/token/ HTTP/1.1
Host:api.gmo-aozora.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic YjNFNWhwWEZsTWJDdXRZaEZpMDc6WldidmgwdGpOYjFYam1GQXUxTGh2d2R3VjYzdGM0clp1d3drTWYzbQ==

grant_type=authorization_code
&code=SplxlOBeZQQYbYS6WxSbIA
&redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
```

応答

応答形式　JSON

HTTPヘッダ

ヘッダ名	必須	説明	最小桁数	最大桁数
Content-Type	○	application/json;charset=UTF-8	-	-
Cache-Control	○	no-store	-	-
Pragma	○	no-cache	-	-

HTTPボディ

パラメータ名	必須	説明	最小桁数	最大桁数
access_token	○	アクセストークン 各APIを要求する際「x-access-token」に設定する値	1	128
refresh_token	○	新しいアクセストークンを取得する際に使用するリフレッシュトークン	1	128
scope	○	アクセストークンに紐付く許諾されたスコープ	1	256
token_type	○	発行されたトークンタイプ "Bearer"固定	-	-
expires_in	○	アクセストークンの有効期限（秒単位）	1	20
id_token	○	IDトークン JWT形式で応答します 詳細は、「IDトークン」を参照	-	-

レスポンス具体例

```
HTTP/1.1 200 OK
content-type:application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
 "access_token": "SIAV32hkKG",
 "refresh_token": "8xLOx8tZp8",
 "scope": "private:account private:virtual-account",
 "token_type": "Bearer",
 "expires_in": 2592000,
 "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzcyI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
  NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3FOMyIsCiAibm9uY2UiOiAibiOwUzZfV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
  AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzROEHR9R6jgdqrOOF4daGU96Sr_P6qJp6IcmD3HP990biIPRs-cwh3LO-p146waJ8IhehcwL7FO9JdijmBqkvPeB2T9CJ
  NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSPOaAplt0JIzZwgjxqGByKHiOtX7TpdQyHE5lcMiKPXfEIQILVqOpc_E2DzL7emopWoaoZTF_mO_NOYzFC6g6EJbOEoRoS
  K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4 XUVrWOLrLlOnx7RkKU8NXNHq-rvKMzqg"
}
```

エラー応答形式　HTTPステータスコード400（Bad Request）、application/json形式でレスポンスボディへ含められます。

HTTPボディ

HTTPステータスコード	パラメータ名	必須	説明	最小桁数	最大桁数
400			クライアント情報が不正、リダイレクトURIが不正		
	error	○	エラーコード ・invalid_request:要求パラメータが不正（必須パラメータ：パラメータキー要求なし、パラメータの値が空） ・invalid_client:指定されたクライアント、またはクライアント情報が不正 ・invalid_grant:認可コードが不正、またはリダイレクトURIが不正 ・unauthorized_client:クライアントがグラントタイプauthorization_codeの利用を許可されていない ・unsupported_grant_type:API-GWがサポートしていないグラントタイプが指定された ・invalid_scope:指定されたスコープが不正 ・server_error:OPサーバでエラーが発生	-	-
	error_description		エラー内容（ASCIIコード「%x20-21 / %x23-5B / %x5D-7E」の範囲の文字種）	-	-
	error_uri		エラーについての追加情報を含むWebページのURI	-	-

レスポンス具体例

```
HTTP/1.1 400 Bad Request
content-type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
 "error": "invalid_request",
 "error_description": "Unsupported response_type value"
}
```

GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

オープンAPI仕様書	エンドポイント名	トークンエンドポイント（アクセストークン再発行時）

要求

URL例

本番環境	https://api.gmo-aozora.com/ganb/api/auth/v1/token
開発環境	https://stg-api.gmo-aozora.com/ganb/api/auth/v1/token

プロトコル　HTTPS

HTTPメソッド　POST

HTTPヘッダ

ヘッダ名	必須	説明	最小桁数	最大桁数
Content-Type	○	application/x-www-form-urlencoded	-	-
Authorization		クライアント認証用のBasic認証値 （クライアントIDとクライアントシーレットを":"（コロン）で連結し、Base64エンコードしたものを設定） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は必須 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は設定不要	-	-

HTTPボディ

パラメータ名	必須	説明	最小桁数	最大桁数
grant_type	○	"refresh_token"固定	-	-
refresh_token	○	トークンエンドポイント（新規発行）にて当社から返却したリフレッシュトークン	1	128
client_id		クライアントID（貴社認証用の項目） （当社が事前に発行する貴社向けのID） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は設定不要 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は必須	1	128
client_secret		クライアントシークレット（貴社認証用の項目） （当社が事前に発行する貴社向けのシークレット） 事前に登録する「クライアント認証方式」に"client_secret_basic"（ベーシック認証）を設定した場合は設定不要 「クライアント認証方式」に"client_secret_post"（パラメーター認証）を設定した場合は必須	1	128

リクエスト具体例

```
POST /ganb/api/auth/v1/token/ HTTP/1.1
Host:api.gmo-aozora.com
Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token
&refresh_token=8xLOx8tZp8
&client_id=b3E5hpXFlMbCutYhFiO7
&client_secret=ZWbvhOtjtblXjmFAu1LhvwdwV63tc4rZuwwkMf3m
```

応答

応答形式　「トークン（新規発行）」の応答と同一。

GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.

オープンAPI仕様書	エンドポイント名	ユーザー情報エンドポイント

要求

URL例

本番環境	https://api.gmo-aozora.com/ganb/api/auth/v1/userinfo
開発環境	https://stg-api.gmo-aozora.com/ganb/api/auth/v1/userinfo

プロトコル　HTTPS

HTTPメソッド　GET

HTTPヘッダ

ヘッダ名	必須	説明	最小桁数	最大桁数
Authorization	○	トークンエンドポイントにて当社から返却したアクセストークン 設定例：Authorization:Bearer {アクセストークン}	1	128

リクエスト具体例

```
GET ganb/api/auth/v1/userinfo HTTP/1.1
Host: api.gmo-aozora.com
Authorization: Bearer S1AV32hkKG
```

応答

応答形式　JSON

HTTPヘッダ

ヘッダ名	必須	説明	最小桁数	最大桁数
Content-Type	○	application/json;charset=UTF-8	-	-
Cache-Control	○	no-store	-	-
Pragma	○	no-cache	-	-

HTTPボディ

パラメータ名	必須	説明	最小桁数	最大桁数
sub	○	認証されたエンドユーザを示す識別子。	1	128
iss	○	レスポンスの発行者のための Issuer 識別子。（トークンの発行者） API-GWのIssuer Identifier URLを設定。	1	256
aud	○	このトークンを対象とするAudience。 （エンドユーザが認可したクライアントのクライアントID）	1	128

レスポンス具体例

```
HTTP/1.1200 OK
content-type:application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
"sub": "FDSAHAYT4HDASDY6WHRTE72AGHJGU",
"iss": "https://stg-api.gmo-aozora.com/",
"aud": "b3E5hpXFIMbCutYhFiO7"
}
```

エラー応答形式　HTTPステータスコード400（Bad Request）、application/json形式でレスポンスボディへ含められます。

HTTPボディ

HTTPステータスコード	パラメータ名	必須	説明	最小桁数	最大桁数
400			クライアント情報が不正、リダイレクトURIが不正		
	error	○	エラーコード ・invalid_request:要求パラメータが不正（必須パラメータ：パラメータキー要求なし、パラメータの値が空、パラメータキー重複など） ・server_error:OPサーバでエラーが発生	-	-
	error_description		エラー内容（ASCIIコード「%x20-21 / %x23-5B / %x5D-7E」の範囲の文字種）	-	-
	error_uri		エラーについての追加情報を含むWebページのURI	-	-
401（※1）			Bearerトークンが不正		
	Bearer realm		realm="NC7OOO-3A-OC"	-	-
	Bearer error		error="invalid_token":リクエストにふくまれるaccess_token が存在しないまたは、有効ではない	-	-
	Beareerror _description		エラー内容（ASCIIコード「%x20-21 / %x23-5B / %x5D-7E」の範囲の文字種）	-	-
403			クライアント情報が不正、リダイレクトURIが不正		
	error		error="insufficient scope":アクセス権限が不足している	-	-
	error_description		エラー内容（ASCIIコード「%x20-21 / %x23-5B / %x5D-7E」の範囲の文字種）	-	-

レスポンス具体例

```
HTTP/1.1 400 Bad Request
content-type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
 "error": "invalid_request",
 "error_description": "Unsupported response_type value"
}
```

※1：このエラーの場合はエラー内容を「WWW-Authenticateヘッダ」に設定

レスポンス具体例

```
HTTP/1.1 401 Unauthorized
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
WWW-Authenticate: Bearer realm="NC7OOO-3A-
OC",error="invalid_token",error_description="%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%83%88%E3%83%BC%E3%82%AF%E3%83%B3%E6%A4%9C%E8%A8%BC%E6%9C%89%E5%8A%B9%E6%9C%9F%E9%99%90%E5%88%87%E3%82%8C%E3%82%A8%E3%83%A9%E3%83%BC"
```


©GMO Aozora Net Bank, Ltd. All Rights Reserved.

オープンAPI仕様書	IDトークン

ID Token

JWT形式のセキュリティトークン（JWTの署名アルゴリズムはHS256）

ID Tokenは改ざん検知用の署名付きトークンであり、JWT（JSON Web Token）形式でエンコードされている。
※JWTの詳細な仕様については、以下を参照。
https://tools.ietf.org/html/rfc7519

JWTはピリオド "." 区切りのHeader、Payload、Signatureから構成されている。
各部位はそれぞれBase64URLエンコードされている。

```
Header.Payload.Signature
```

具体例： ID Token

```
ewoidHlwIjogIkpXVCIsCiJhbGciOiAiSFMyNTYiCnO.ewoiaXNzIjogImh0dHBzOlwvXC9zdGctYXBpLmdtbty1hb3pvcmEuY29tXC8iLAoic3ViIjogIkZEUOFIQVIUNEhEQVNEWTZXSFJURTcyQUdISkdVIiwKImF1ZCI6ICJiMOU1aHBYRmxNYkN1dFloRmkwNylsCiJleHAiOiAxNDUzNjE4MDM2LAoiaWFOIjogMTQ1MzI3MjQzNiwKIm5vbmNlIjogImVmM2EwOTE5MjhkNTQ5MTYyNGMwYWM1NGQ2OTcxMjQOMjI3MDUwOTIiLAoiYXpwIjogImIzRTVocFhGbEIiQ3VOWWhGaTA3Igp9.
```

<Header>

```
ewoidHlwIjogIkpXVCIsCiJhbGciOiAiSFMyNTYiCnO
```

<Payload>

```
ewoiaXNzIjogImh0dHBzOlwvXC9zdGctYXBpLmdtbty1hb3pvcmEuY29tXC8iLAoic3ViIjogIkZEUOFIQVIUNEhEQVNEWTZXSFJURTcyQUdISkdVIiwKImF1ZCI6ICJiMOU1aHBYRmxNYkN1dFloRmkwNylsCiJleHAiOiAxNDUzNjE4MDM2LAoiaWFOIjogMTQ1MzI3MjQzNiwKIm5vbmNlIjogImVmM2EwOTE5MjhkNTQ5MTYyNGMwYWM1NGQ2OTcxMjQOMjI3MDUwOTIiLAoiYXpwIjogImIzRTVocFhGbEIiQ3VOWWhGaTA3Igp9
```

<Signature>

```
_sH8PJ-hyOyU6RDJOUg_VRRJL6HZRT9uTutrlcg4yzE
```

Header　JWTを取り扱うために必要な項目が設定されている。

日本語名	パラメータ名	必須	説明
メディアタイプ	typ	○	"JWT" 固定。
暗号化アルゴリズム	alg	○	"HS256" 固定。（HMAC using SHA-256 hash）

具体例：

```
{
"typ": "JWT",
"alg": "HS256"
}
```

Payload　改ざんを検知するために必要な項目が設定されている。

日本語名	パラメータ名	必須	説明
発行者	iss	○	レスポンスの発行者のための Issuer 識別子。（IDトークンの発行者） API-GWのIssuer Identifier URLを設定。
ユーザー識別子	sub	○	認証されたエンドユーザを示す識別子。
対象者	aud	○	このIDトークンを対象とするAudience。（エンドユーザが認可したクライアントのクライアントID）
有効期限	exp	○	ID Tokenの有効期限。 UTCのUNIX時間の秒までを設定する。（例：2014/10/23 15:15:29→1414044929）
発行日時	iat	○	ID Token発行日時。 UTCのUNIX時間の秒までを設定する。（例：2014/10/23 15:15:29→1414044929）
ナンス	nonce		認可エンドポイント要求時に指定された値をそのまま返却する。 （アクセストークンの更新時は未設定）
認可対象者	azp	○	IDトークンを発行されたAuthorized party（認可された対象者のクライアントID）。

具体例：

```
{
"iss": "https:¥/¥/stg-api.gmo-aozora.com¥/",　　（本番環境の場合は"https:¥/¥/api.gmo-aozora.com¥/"）
"sub": "FDSAHAYT4HDASDY6WHRTE72AGHJGU",
"aud": "b3E5hpXFlMbCutYhFiO7",
"exp": 1453618036,
"iat": 1453272436,
"nonce": "ef3a091928d5491624c0ac54d697124422705092",
"azp": "b3E5hpXFlMbCutYhFiO7"
}
```

Signature　HeaderとPayloadから生成されたJWT改ざん防止のための署名。
Base64URLエンコードされたHeader ＋ "." ＋ Payloadを入力値としてクライアントシークレットをキーとし、HS256で署名した結果をさらにBase64URLエンコードした文字列。

ID Token の検証方法

1. 署名の検証

① 取得したJWTをピリオド "." で区切り、Header、Payload、Signatureに分割する。
・前部：Header
・中部：Payload
・後部：Signature

② 分割したHeader、Payloadをそれぞれ Base64URLデコードする。

③ クライアントシークレットをキーとしてHeaderのalg値のアルゴリズムにより、Base64URLエンコードしたままの Header ＋ "." ＋ Payloadのダイジェスト値を取得。
さらにその値にBase64URLエンコードをかける。

キー	クライアントシークレット
アルゴリズム	Base64URLデコードしたHeaderのalg値のアルゴリズム
インプット	Base64URLエンコードされたままの Header ＋ "." ＋ Payload

サンプル：

```
# echo -n '[BASE64URLエンコード状態のままのHeader ＋ "." ＋ Payload]' | openssl dgst -binary -sha256 -hmac '[クライアントシークレット]' | base64 | tr -d '¥n' | tr -d '=' | tr '/+' '_-'
```

④ 「①」で取得した Signature と「③」で取得した値が一致し、正しい署名であることを検証。

2. Payloadの検証

署名の検証が問題ない場合、Base64URLデコードしたPayloadの各項目を判定し、改ざんが行われてないことを確認する。

iss	ID Tokenの発行元の改ざんを防ぐためにこの値が 当社（本番：https://api.gmo-aozora.com、開発：https://stg-api.gmo-aozora.com）であることを確認。
aud	このIDトークンが他のクライアント向けに発行されたものではないことを確認するため、自身のクライアントIDと同一であることを確認。
exp	ID Tokenが有効期限内であることを確認するため、現在時刻（UTC）のUNIX時間よりも大きいことを確認。
iat	ID Token発行から10分以内であることを確認するため、現在時刻（UTC）のUNIX時間 －（600秒）以上であることを確認。
nonce	認可エンドポイント要求時に指定した値と同一であることを確認。リプレイアタック攻撃を防止するため、検証後はnonce値を破棄する。
azp	認可されたクライアントが自身であることを確認するため、自身のクライアントIDと同一であることを確認。

GMOあおぞらネット銀行
©GMO Aozora Net Bank, Ltd. All Rights Reserved.



©GMO Aozora Net Bank, Ltd. All Rights Reserved.