

dアカウント・コネクト マニュアル

〔別紙1〕 パラメータ詳細

～認可利用サービス向け～

第1.10版

2020/11/19

改版履歴

版	項番	種類	修正箇所	修正内容	備考
1.0	1	新規		初版制定	
1.1	1	追記	API-1-1 Authentication Request(認証要求)パラメータ ・項番9「prompt」	・説明に注記を追記	
	2	修正	API-3-2 UserInfo Response(利用者情報取得応答)パラメータ	・API番号の誤記を修正 ・error/パラメータの備考に注記を追記	
1.2	1	—	変更なし	版数のみ変更	
1.3	1	追記	API-1-1 Authentication Request(認証要求)パラメータ ・項番9「prompt」	・説明の「iモードは利用不可」の注記を削除	
	2	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番21「authotp」	・パラメータを追記	
	3	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番22「idauth」	・パラメータを追記	
	4	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番23「authsp」	・パラメータを追記	
	5	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番24「authiden」	・パラメータを追記	
1.4	1	—	変更なし	版数のみ変更	
1.4.1	1	修正	API-2-1 Token Request(トークン払出要求)パラメータ ・項番6「client_id」	・特記事項を記載	
	2	修正	API-2-1 Token Request(トークン払出要求)パラメータ ・項番7「client_secret」	・特記事項を記載	
1.5	1	追記	【補足】ID Tokenについて	ID Tokenのエンコード方式の注記を追記	
	2	修正	【補足】ID Tokenについて	ID TokenのJWS署名検証の例を追記	
1.6	1	—	変更なし	版数のみ変更	
1.6.1	1	追記	API-1-1 Authentication Request(認証要求)パラメータ ・項番22「idauth」	・説明にSSOが行われる条件を追記	
1.7	1	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番20「authif」	・説明のパラメータ省略時の誤記を修正	
1.8	1	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番24「authiden」	・説明に本人確認画面の表示条件を追記	
1.8.1	1	—	変更なし	版数のみ変更	
1.8.2	1	—	【補足】ID Tokenについて	項番2「sub」の「値のとりうる範囲」の説明を追記	
1.8.3	1	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番4「redirect_uri」	・特記事項に注釈を追記	
	2	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番21「authotp」	・説明を補足修正	
1.8.4	1	修正	API-2-1 Token Request(トークン払出要求)パラメータ ・項番3「redirect_uri」	・説明の誤記を修正	
1.8.5	1	—	変更なし	版数のみ変更	
1.9	1	修正	API-1-1 Authentication Request(認証要求)パラメータ ・項番9「prompt」	・説明、値のとりうる範囲、特記事項、Byte数を修正	
1.10	1	追記	API-1-1 Authentication Request(認証要求)パラメータ ・項番9「prompt」	・説明、値のとりうる範囲、特記事項、Byte数を修正	

API-1-1 Authentication Request (認証要求) パラメータ

項番	物理名	論理名	必須	説明	値のとらえる範囲	特記事項	形式	Byte数
1	scope	スコープID	○	認証・認可を要求したいScope名称を設定します。 scope に openid を含む必要があります。openid以外の scope 値が存在していても良いです。	"openid" +(任意のスコープID) ※複数のスコープを指定する場合は、スペース(%20)で連結して指定します。	サーバ側で規定されていない scope についてはエラー応答 (invalid_scope) されます。 ※リフレッシュトークンが必要な場合には、「offline_access」スコープの付与が必要です。	半角英数記	1~1000
2	response_type	応答形式	○	使用される認証処理フローを決定する値を設定します。 ※Authorization Code Flowのみを対応しているため、この値は"code"固定となります。	"code"	Authorization Code Flowのみ対応のため、"code"以外が指定された場合、エラーとなります。	半角英数	4
3	client_id	クライアントID	○	認可サーバに登録されているクライアントIDを設定します。	(本システムが払い出したクライアントID)	利用提携時に本システムより発行されたclient_idを指定します。	半角英数記	1~128
4	redirect_uri	応答先URI	○	認証・認可の結果を受信するURIを設定します。 この URI は、クライアントが、情報連携を行うための事前申請時に通知した Redirection URL のいずれかと完全一致する必要があります。 ※本APIでは、httpsスキームのURIのみ対応します。	([RFC3986] (Simple String Comparison) の Section 6.2.1で規定されたURI形式の値)	利用提携時に提示したURIを指定します。 ※クエリパラメータを付与した値でも設定可能です。("? "がついていても可)ただし、動的なパラメータではなく固定値で設定してください。	半角英数記	1~2048
5	state	セキュア文字列(CSRF/XSRF対策)	○	リクエストとコールバックの間で維持されるランダムな値を設定します。 Cross-Site Request Forgery (CSRF, XSRF) 対策の目的で利用される、ブラウザ Cookie と紐づく暗号論的にセキュアな値を設定します。	(Cookie毎に異なる任意のセキュア文字列)	ドコモ独自仕様として必須項目とします。 サーバ側では形式・サイズチェックは実施しますが、内容のチェックを行いません。設定された値をそのまま応答します。	半角英数記	1~60
6	response_mode	応答様式		未使用	—	—		
7	nonce	セキュア文字列(リプレイアタック対策)	○	Client セッションと ID Token を紐づけるランダムな値を設定する、リプレイアタック対策に用いられます。 この値は ID Token に含まれて応答される、nonce 値には、推測不可能なように十分なエントロピーを持たせる必要があります。	(情報連携の一連のセッション毎に異なる任意のセキュア文字列)	ドコモ独自仕様として必須項目とします。 サーバ側では形式・サイズチェックは実施しますが、内容のチェックを行いません。設定された値をそのまま応答します。	半角英数記	1~60
8	display	画面表示形式		未使用	—	—		
9	prompt	認証・認可動作指定		End-User に再認証および認可を再度要求 (別dアカウントでログイン) する場合、あるいはお客様に異なる画面も表示せずログイン可能であればログインする場合に指定します。 ※本パラメータはオプションのため、必要な場合のみ指定してください。 ※loginを指定した場合はSSO (シングルサインオン) はしません。 ※noneを指定した場合は、処理結果の成否を認証応答にセットして返却します。 ※consentを指定した場合は、強制的に認可画面を表示します。	login End-User を再認証する[SHOULD]。再認証が不可能な場合はエラーを返します[MUST]。 none いかなる認証および認可画面も表示しません[MUST NOT]。 End-User が認証済でない場合、Client が要求する Claim 取得に十分な事前同意を取得済でない場合、またはリクエストを処理するために必要な何らかの条件を満たさない場合には、エラーが返されます。 consent End-User に再認可を要求する[SHOULD]。同意要求が不可能な場合はエラーを返します[MUST]。	ドコモ独自仕様としてlogin (再認証)、none (何も求めない)、consent (再認可) のみに対応します。 select_account (アカウント指定認可)は無視されます。 ※none がその他の値とともに用いられる場合は当該パラメータは無視扱いとします。 ※クライアントタイプが「パブリック」の場合、prompt=login、prompt=consentのみ対応し、それ以外の値は無視扱いとします。	半角英	4~13
10	max_age	有効期限		未使用	—	—		
11	ui_locales	表示言語		未使用	—	—		
12	id_token_hint	ID Token		未使用	—	—		
13	login_hint	利用者識別子		未使用	—	—		
14	acr_values	認証レベル		未使用	—	—		
15	claims_locales	言語		未使用	—	—		
16	claims	クレーム		未使用	—	—		
17	request	要求文字列		未使用	—	—		
18	request_uri	要求参照URI		未使用	—	—		
19	registration	要求参照URI		未使用	—	—		
20	authif	認証/F種別		認証を契約者に限定するか、ドコモ以外のお客様も認証可能とするか指定します。 ※本パラメータを省略した場合、「0: 契約者限定で認証」として扱います。	0: 契約者限定で認証 1: ドコモ以外のお客様も認証可能	認証時に使用するパラメータ ドコモ独自パラメータとなります。	半角数字	1
21	authotp	認証ワンタイムパスワード		アプリで認証を行う場合のワンタイムパスワード (OTP) を指定します。 OTPは、直前にアプリ認証サーバより払い出されたBE5E64文字列の値を付与します。 ※本パラメータが付与された場合、認証済みの状態でもOTPIによる再認証を行います。	(サーバで払い出されたワンタイムパスワードの値)	認証時に使用するパラメータです。 ドコモ独自パラメータとなります。	半角英数記号 (0~21 ~ 0x7E)	1~256
22	idauth	ID認証必須フラグ		dアカウントのIDによる認証を必須で行います。 回線接続している場合でも、回線による認証は行わずdアカウントのIDによる認証を行います。また、回線認証で認証済みの場合でも、SSOは行わずにdアカウントのIDで再認証を行います。 ただし、dアカウントのIDによる認証はSSOが有効となり、すでにdアカウントのIDにより認証済みの場合はSSOが行われます。 ※本パラメータが付与されていない場合は、回線接続であれば回線による認証を行います。	"1"	認証時に使用するパラメータです。 ドコモ独自パラメータとなります。	半角数字	1
23	authsp	spモードパスワード認証要求フラグ		回線による認証を行う場合に、ネットワーク暗証番号ではなくspモードパスワードによる認証を行います。 ※本パラメータが付与されない場合は、ネットワーク暗証番号による認証を行います。 ※本パラメータが付与されているも、回線による認証ができない場合はdアカウントのIDによる認証を行います。	"1"	認証時に使用するパラメータです。 ドコモ独自パラメータとなります。	半角数字	1
24	authiden	本人確認要求フラグ		認可画面 (同意画面) が表示されない場合 (注1)でも、必ず本人確認を行います。ただし、本人確認を行った後の一定期間は「本人確認済み状態」が有効となっているため、その期間に再度、本人確認画面の強制的な表示を要求しても、本人確認画面は省略され表示されません。 (注1) 認可 (同意) が不要なスコープのみを要求した場合や、お客様が認可済み (同意済み) としたスコープを要求した場合。 ※本パラメータが付与されない場合は、必要な場合のみ本人確認を行います。	"1"	認証時に使用するパラメータです。 ドコモ独自パラメータとなります。	半角数字	1

API-1-2 Authentication Response(認証応答)パラメータ

項番	物理名	論理名	説明	値のとりうる範囲	特記事項	形式	Byte数(UTF-8) (エスケープ前)
1	code	認可コード	End-Userからの認可を受けたことを示す認可コードを応答します。 漏洩のリスクを軽減するため、認可コードは発行してから短時間で無効となります。 ※OpenID Connectの規約上は、認可コードの有効期限は最大でも10分です。 認可コードはクライアント識別子とリダイレクトURIに紐づきます。	(セキュアな文字列)	クライアントは2回以上認可コードを使用できません (MUST NOT)。もし、認可コードが2回以上使用された場合は、認可サーバーはリクエストを拒否しなければならず (MUST)。この認可コードを基に発行されたこれまでのすべてのトークンを無効化します (SHOULD)。	半角英数記	1~256
2	error	エラーコード	エラーの内容を示すコードを応答します。 ASCII [USASCII] エラーコードより1つを設定します。	{%x20-21 / %x23-5B / %x5D-7E 以外の文字を含まない値} (エラーコード参照)		半角英数記	—
3	error description	エラー詳細	未使用	—			
4	error uri	エラー情報URI	未使用	—			
5	state	セキュア文字列(CSRF/XSRF対策)	クライアントから受け取ったstate値をそのまま応答します。	(クライアントから受け取った値をそのまま返します)	リクエスト時のstate/パラメータが規定のサイズ超過の場合には応答されません。	半角英数記	1~60

API-2-1 Token Request(トークン払出要求)パラメータ

項番	物理名	論理名	必須		説明	値のとりうる範囲	特記事項	形式	Byte数
			Token Request時	Token refresh時					
1	grant_type	権限形式	○	○	何の権限により、トークンを発行するかを指定します。 ※アクセストークン払出の際は、Authorization Code Flowのみを対応しているため、値は"authorization_code"固定となります。 ※トークンリフレッシュの際は、"refresh_token"を設定します。	"authorization_code" or "refresh_token"	Authorization Code Flowのみ対応のため、アクセストークン払出時、 "authorization_code"以外が指定された場合、エラーとなります。	半角英数	13～18
2	code	認可コード	○	—	認可サーバーから受け取った認可コードを設定します。 アクセストークン要求時に指定します。	(セキュアな文字列)	クライアントは2回以上認可コードを使用できません。 もし、認可コードが2回以上使用された場合、認可サーバーはリクエストを拒否して、この認可コードを基に発行されたこれまでのすべてのトークンを無効化します。	半角英数記	1～256
3	redirect_uri	応答先URI	○	—	認証要求時のredirect_uriを設定します。 認証要求時と同じ値でなければなりません。 アクセストークン要求時に指定します。	([RFC3986] (Simple String Comparison) の Section 6.2.1で規定されたURI形式の値)	認可コードはクライアント識別子とリダイレクトURIに紐づきます。	半角英数記	1～2048
4	refresh_token	リフレッシュトークン	—	○	アクセストークン取得時に同時に払い出されたリフレッシュトークンを設定します。 トークンリフレッシュ要求時に指定します。		リフレッシュトークンについては、アクセストークン要求時に払い出されたリフレッシュトークンの有効期限まで不変となります。 リフレッシュトークン要求を複数回要求する場合には、初回払い出し時のリフレッシュトークン値を要求元にて保持する必要があります。	半角英数記	1～256
5	scope	スコープID	—	△	OP が発行したアクセストークンの範囲を設定します。 トークンリフレッシュ要求時に指定します。 元々許可されていない値を含んではいけません。設定する場合は "openid" スコープは必須となります。 複数設定する場合は半角スペース区切りにて連結します。			半角英数記	1～1000
6	client_id	クライアントID			未使用	—	クライアントIDとクライアントシークレットはHTTPヘッダ部のAuthorizationで指定しますので、本パラメータは利用しません。		
7	client_secret	クライアントシークレット			未使用	—	クライアントIDとクライアントシークレットはHTTPヘッダ部のAuthorizationで指定しますので、本パラメータは利用しません。		

「必須」の凡例
○: 設定する
△: 任意で設定する
—: 設定しない

API-2-2 Token Response(トークン払出応答)パラメータ

項番	物理名	論理名	必須			説明	値のとりうる範囲	特記事項	形式	Byte数
			※1	※2	※3					
1	access_token	アクセストークン	○	○	×	認可サーバーが発行するアクセストークンを応答します。	-		半角英数記	1～256
2	token_type	トークン形式	○	○	×	トークンのタイプを応答する。本システムでは"Bearer"固定となります。	"Bearer"	プロトコルでは値は大文字・小文字を区別しません。	半角英	6
3	expires_in	トークン有効期間	○	○	×	アクセストークンの有効期間を表す秒数を応答します。 例えばこの値が 3600 であれば、そのアクセストークンは発行から1時間後に期限切れとなります。	-		半角数	—
4	refresh_token	リフレッシュトークン	○	×	×	アクセストークン有効期限切れの際にアクセストークンをリフレッシュするためのリフレッシュトークンを応答します。 同じ認可グラントを用いて新しいアクセストークンを取得するのに利用されます。	-	リフレッシュトークンについては、アクセストークン要求時のみ払い出しを行います。	半角英数記	0～256
5	scope	スコープID	○	○	×	発行したアクセストークンのScope範囲を応答します。 ※ 対象の情報がない場合は空で返却されます。 ※ 返却値にopenid, offline_access は含みません。	-		半角英数記	0～1000
6	id_token	IDトークン	○	○	×	クライアントに関連するIDのトークンを応答します。	{サーバーにIDトークンのClaimsとして規定されているClaimsリスト}	{【補足】ID Tokenについて}を参照してください。	—	—
7	error	エラーコード	×	×	○	エラーの内容を示すコードを応答します。 ASCII [USASCII] エラーコードより1つを設定します。	{%x20-21 / %x23-5B / %x5D-7E 以外の文字を含まない値} (エラーコード参照)	WWW-Authenticateヘッダを応答する場合は、WWW-Authenticateヘッダにattributeとして本パラメータを付与します。	半角英数記	—
8	error_description	エラー詳細				未使用	—			
9	error_uri	エラー情報URI				未使用	—			

※1: Authentication Request (認証要求) でscopeに「offline_access」を指定した場合のToken Requestの応答時
※2: Authentication Request (認証要求) でscopeに「offline_access」が指定しなかった場合のToken Requestの応答時
または、Token Refreshの応答時
※3: 準正常の応答時

「必須」の凡例
○: 返却する
△: 要求されていた場合に返却する
×: 返却しない

API-3-1 UserInfo Request (利用者情報取得要求) パラメータ

項番	物理名	論理名	説明	値のとりうる範囲	特記事項	形式	Byte数
1	-	-	-	-	-	-	-

API-3-2 UserInfo Response (利用者情報取得応答)パラメータ

項番	物理名	論理名	必須		説明	値のとりうる範囲	特記事項	形式	Byte数
			正常応答時	準正常応答時					
1	(認可されたScopeに紐付くClaims)	-	○	×	認可されたScopeに紐付くClaimを応答します。 JWT、またはJSON形式で応答します。	-	-	-	-
2	error	エラーコード	×	△	エラーの内容を示すコードを応答します。 ASCII [USASCII] エラーコードより1つを設定します。	(%x20-21 / %x23-5B / %x5D-7E 以外の文字を含まない値) (エラーコード参照)	WWW-Authenticateヘッダを応答する場合(注)は、WWW-Authenticate ヘッダにattributeとして付与して、ボディ部は応答しません。 (注)httpステータス400、401、403応答の場合	半角英数記	-
3	error.description	エラー詳細			未使用	-			
4	error.uri	エラー情報URI			未使用	-			

「必須」の凡例
○:返却する
△:要求されていた場合に返却する
×:返却しない

【補足】ID Tokenについて

Authorization Code Flow では、Token Response にて ID Token が「id_token」項目の値にJWT(JSON Web Token)形式で埋め込まれます。
JWT形式は「ポリゴン」にて区切られた①JWTヘッダ、②JWTクレームセクト、③JWS署名の3つのパートで構成され、それぞれBase64URL(注)でエンコードされています。

(注) エンコード方式の「Base64URL」は「Base64」には異なるエンコード方式なのでご注意ください。

※JWTクレームセット(下記②)はBase64URLエンコードされたJSONテキストオブジェクトが埋め込まれます(暗号化はされません)。
 ※JWS署名(下記③)については署名検証を実施して下さい。

【例：ID Token を含む Token Response (JWS)】

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
```

```
{
    "access_token": "SIW32hKKG",
    "token_type": "Bearer",
    "refresh_token": "8xLoxBtZp8",
    "expires_in": 3600,
    "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInRwIjoiZW9mIGwiLCJpcyI6ImFkbWVudC2vYmlydGVudGIwYXVybm9uZD17IiwiaWF0IjoiMTQ4MjE0ODg1IiwiaXNjaW5lbnZybm9kIjkiLCJibG9ja0IjOiAiZXZGRS3fOmlrLGEoIm9mY2UyMDIuMSBjb2VudC2vYmlydGVudC2vYmlydGVudCI6Im90ZWZ3bW9kIiwiaXNjaW5lbnZybm9kIjoiZW9mIGwiLCJpcyI6ImFkbWVudC2vYmlydGVudC2vYmlydGVudCI6Im90ZWZ3bW9kIiwicmJctcmVhbnBpsTSM-Si-K_U2K18FUBAN6eyjy3T2RIVE"
```

↓

【例: id token 値のJWTを解除 (Base64URLデコード) したJWTクレームセットの状態】

```
{
  "iss": "http://server.example.com",
  "sub": "248289761001",
  "aud": "s6BhdRkqt3",
  "nonce": "n-OS6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970
}
```

以下に埋め込まれる項目を示します。

項番	物理名	論理名	説明	値のとりうる範囲	特記事項	形式	Byte数(UTF-8) (エスケープ前)
1	iss	発行者識別子	レスポンス発行者の識別子。発行者URLを設定します。 クエリやフラグメントの要素を含まないスキーム、ホスト、任意のポート番号とパスからなる https スキームを使用した大文字と小文字を区別するURL です。				
2	sub	利用者識別子(Open ID)	Subject 識別子。OpenIDを設定します。 発行者内で一意であり決して再割り当てされない識別子です。	ASCII で255文字を超えてはならない(MUST NOT)。 大文字と小文字を区別します。 以下のURL形式の値(httpsも含め、すべての文字列が対象です) https://i.mydocomo.com/id/xxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxx部分はお客様固有値(ランダムなユニーク値)			
3	aud	連携先識別子	クライアントIDを設定します。	大文字と小文字を区別する文字列です。	※プロトコル上配列を許容しているが、本システムでは配列の応答は行いません。		
4	exp	IDトークン有効期間	IDトークンの有効期間を設定する。未来の日付となります。	UTC の UNIX 時間の秒までを設定する。1970-01-01T0:0:0Z からの秒数を表します。			
5	iat	IDトークン発行日時	IDトークンのJWT が発行された時刻を設定します。	UTC の UNIX 時間の秒までを設定する。1970-01-01T0:0:0Z からの秒数を表します。			
6	auth time	未使用	未使用	未使用	未使用		
7	nonce	セキュア文字列(リプレイアタック対策)	Client セッションと ID Token を紐づける文字列であり、リプレイアタック対策に用いられます。この値は Authentication Request で指定されたままの値で設定します。	(リクエストされたままの値を設定します。)	Implicit Flow および Hybrid Flowでは必須項目となりますが、Authorization Code Flowのみ対応となるので、任意項目となります。		
8	acr	未使用	未使用	未使用	未使用		
9	amr	未使用	未使用	未使用	未使用		
10	azp		ID トークンを発行された Relying Party を示す値。クライアントIDを設定します。				
11	at hash	未使用	未使用	未使用	未使用		
12	c hash	未使用	未使用	未使用	未使用		
13	(Standard Claims)	未使用	未使用	未使用	未使用		
14	sub iwk	未使用	未使用	未使用	未使用		

【例：JWS署名検証】

① IWTヘッド

② IWT クレーン・セット

③ IWS 署名

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9. ewoglmZcyIGICjodHrW0i8vc2YdmVyLmV4YWlwbGUyZnR1wKtCjzdWIiOiAiMjQAMjg5NzYxMDAxIiwKCjhdWoiOiAic2ZCaGRSa3FOMyIsCiAibm9uZUYuOAIibiOWuzFv3BMk1qIiwKCIJEHAioiAXmxExmjgxOTcwLaoglmdChdCl6I

```
rJctcmxCVhBpsTsM-siK_U2K18F
UB4N6eyjy3T2RIVE
```

- ・署名アルゴリズム: HS256 (HMAC SHA-256)
- ・秘密鍵: クライアントシークレット (例: "sXEqLxbNk5")

生成したJWS署名
"rJctcmxCVhBpsTsm-siK U2K18FUB4N6eviv3T2R1VF"

一致