dアカウント・コネクトマニュアル

spモードコンテンツ決済/d払い/ドコモ払い

第1.22版 2018年11月14日

株式会社NTTドコモ

はじめに

本書は、株式会社NTTドコモ（以下「ドコモ」といいます）が提供するdアカウント・コネクトについて、サービス提供者が導入時に必要とする情報を提供することを目的としています。

なお、本書ではサービス提供者のシステムを「RP（Relying Party）」、ドコモのシステムを「IdP（Identity Provider）」といいます。

本書の関連文書を示します。

文書名	概要	参照先
OpenID Connect Core 1.0	OpenID Connect の主要な機能を定義	http://openid.net/specs/openid-connect-core-1_0.html

商標について

本書に記載されているドコモの商品またはサービスの名称等は、ドコモの商標または登録商標です。

その他、本書に記載された会社名、製品名などは該当する各社の商標または登録商標です。

目次

1. 用語定義

本章で使用する用語を記述します。

1.1 本書における用語定義

本書における用語定義を「表 1.1-1 用語定義」に示します。

表 1.1-1 用語定義

名称	説明
IdP（Identity Provider）	認証・認可を行い、お客様の特定および認可されたお客様情報の提供を行うドコモのシステム。
RP（Relying Party）	IdPに認証・認可を委託し、IdPから提供されたお客様情報を利用してお客様にサービスを提供するシステム。
認証	IdPがdアカウントの ID/パスワードや契約回線などにより、お客様の一人一人を特定すること。
認可	RPが要求するお客様情報の提供について、IdPがお客様から同意を得ること。
お客様情報	ドコモが保有している、RPに提供可能なお客様の情報。 主にお客様の契約情報や、お客様を特定する利用者識別情報など。
認証画面	お客様を特定するために、dアカウントの ID/パスワードやネットワーク暗証番号を入力する画面。
同意画面	お客様に情報の提供に同意していただくために、対象となるお客様情報や提供先のRPの情報を表示する画面。
認可コード	お客様が認可した場合に返却されるユニークな値で、トークンを取得するために一時的に利用されるコード。
IDトークン	お客様を特定する利用者識別情報（OpenId）を含む改ざん検知付きの文字列。
アクセストークン	お客様情報を取得するためのユニークな文字列。
トークン	IdPが払い出すIDトークン、アクセストークンの総称。
クレーム	IdPからRPに提供するお客様情報の個々のデータ項目のこと。
スコープ	IdPが定めた、複数のクレームをまとめたグループのことで、RPにはスコープ単位で情報を提供する。
dアカウントの ID	お客様が認証を行う際に入力する文字列で、ドコモ以外のお客様でも発行できる。 IdPのみで利用され、RPには通知されない。
OpenId	一人一人のお客様を個別に識別するために、IdPからRPに通知されるID。
シングルサインオン（SSO）	お客様がログインした後の一定期間はログイン状態を保持し、ログインを省略してサービスを利用できる機能。
ネットワーク暗証番号	ドコモのお客様が回線のご契約時などにドコモにお申し出いただいた4桁の番号。
契約回線	ドコモのお客様が契約しているFOMA、およびXiの回線。
決済システム	spモードコンテンツ決済、d払い、ドコモ払いの決済システムの総称。

1.2 本書における凡例

本書における必須項目の凡例について、「表 1.2-1 必須項目の凡例」に示します。

表 1.2-1 必須項目の凡例

凡例	内容
○	必須
△	任意
×	設定なし

2. 概要

本章では、概要について説明します。

2.1 サービス概要

dアカウント・コネクトは、IdPが保有しているお客様情報に対して、お客様の特定（認証）とお客様に情報提供の同意（認可）を行い、RP（サービス提供者）にお客様情報を提供する仕組みです。
なお、RPに提供するお客様情報により同意の要否がありますが、本マニュアルでは同意が不要なお客様情報のみを扱うRPを対象としています。

2.1.1 サービスイメージ

認可が不要なお客様情報を提供する場合におけるdアカウント・コネクトの利用イメージを「図 2.1-1 dアカウント・コネクトの利用イメージ」に示します。

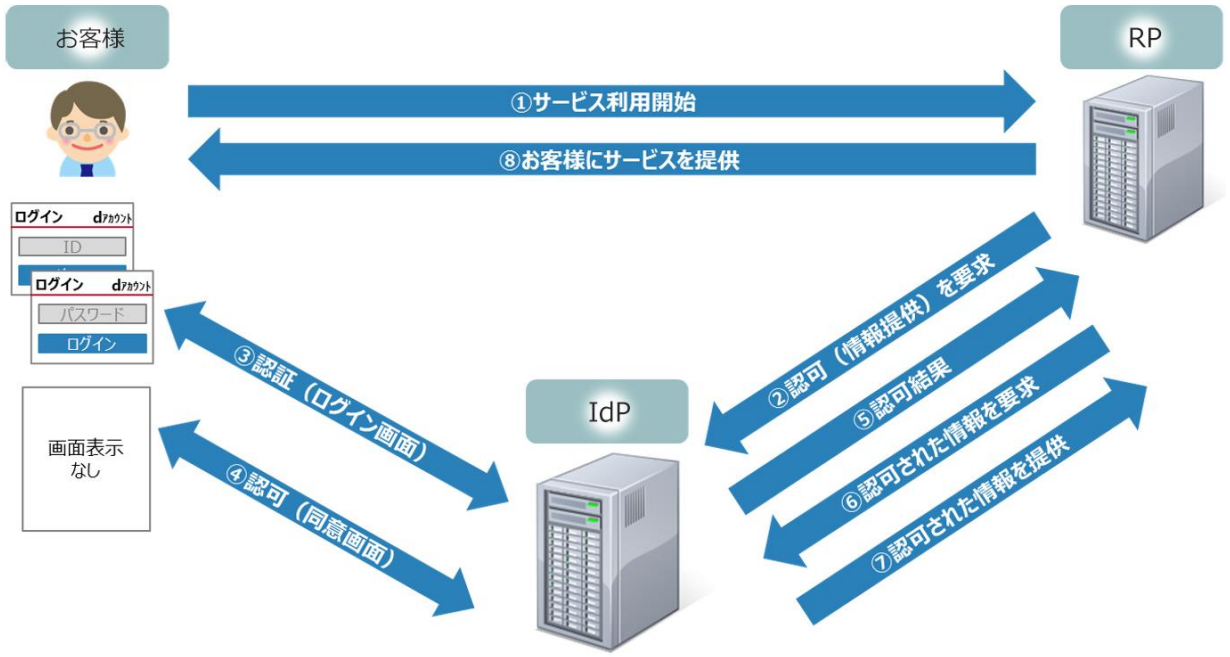


図 2.1-1 dアカウント・コネクトの利用イメージ

(1) お客様はログインボタンを押すなどにより、サービスの利用を開始する。
(2) サービスを提供するRPは認可（お客様情報の提供）をIdPに要求する。
(3) IdPはお客様にログイン画面を表示し、お客様を認証（お客様を特定）する。
(4) 認可が不要なお客様情報の場合、IdPは同意画面を表示せず、認可されたものとして扱う。
(5) IdPはRPに認可結果（同意されたこと）を通知する。
(6) RPは認可されたお客様情報の取得をIdPに要求する。
(7) IdPは認可されたお客様情報をRPに提供する。
(8) RPは提供されたお客様情報を利用し、お客様にサービスを提供する。

2.1.2 スコープとクレームについて

お客様の個々の情報を「クレーム」といいます。利用する目的などによりクレームをグループ化した単位を「スコープ」といい、あらかじめIdPに登録されています。クレームとスコープの関係を「図 2.1-2 クレームとスコープの関係」に示します。

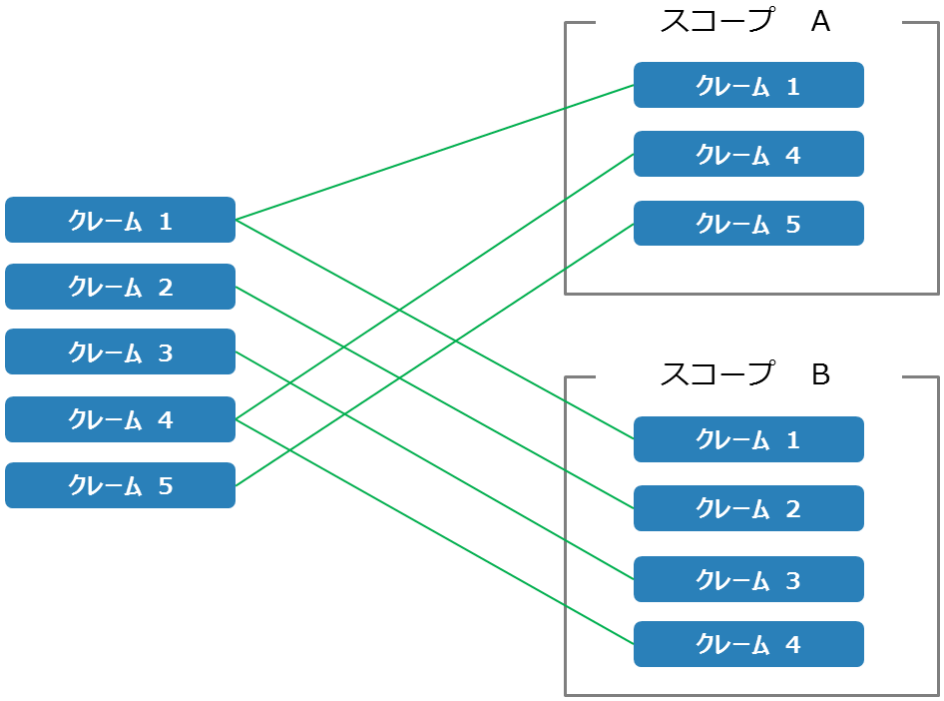


図 2.1-2 クレームとスコープの関係

- RPに提供するお客様情報はスコープ単位で提供し、複数のスコープを組み合わせて提供することが可能です。
- スコープ、およびクレームの詳細については「5.4提供データ」を参照してください。
- RPが利用するスコープは事前に利用申請が必要です。

2.1.3 同意の要否

IdPが保有しているお客様情報には、RPに提供する場合にお客様の同意が必要な情報と不要な情報があります。同意が必要なお客様情報をRPに提供する場合は同意画面が表示され、同意が不要なお客様情報は同意画面が表示されずRPに提供されます。

お客様情報の提供はスコープ単位で行うため、スコープ単位で同意の要否が決まっています。

本マニュアルでは、同意が不要な情報のみを扱うRPを対象としているため、同意不要となるスコープのみ扱うことを前提としています。

2.2　システム概要

OpenID Foundationにて標準化されているOpenID Connect 1.0プロトコルを利用しています。

2.2.1　システム構成

dアカウント・コネクトのシステム構成について「図 2.2-1 dアカウント・コネクトのシステム構成」に示します。

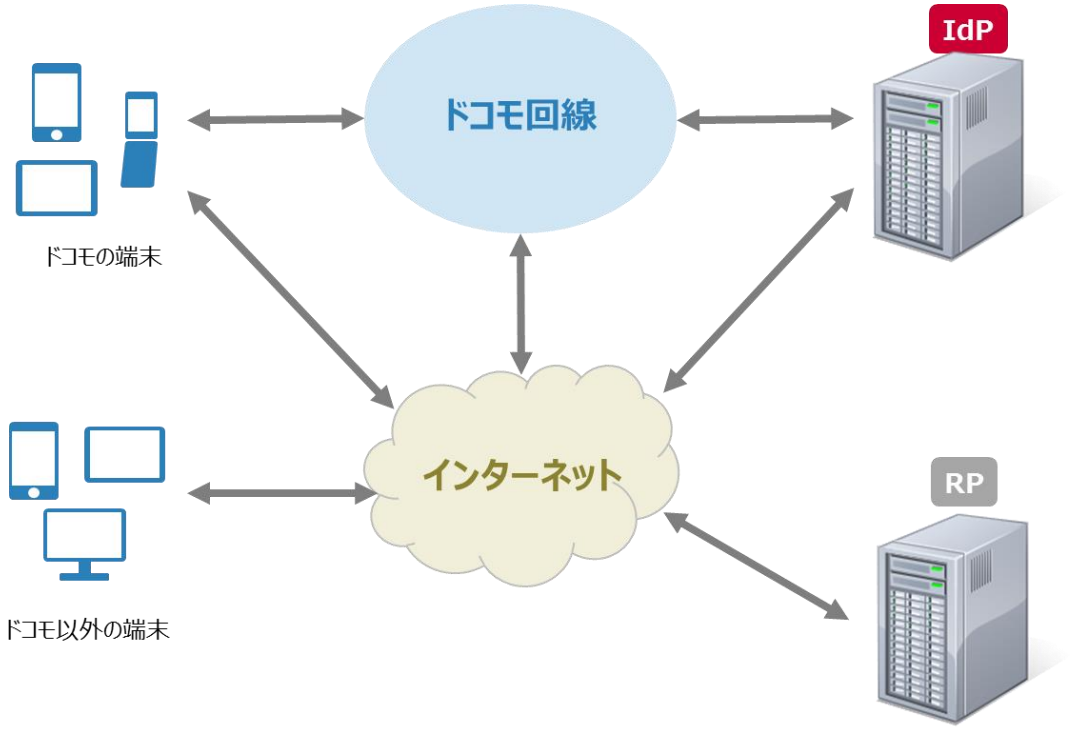


図 2.2-1 dアカウント・コネクトのシステム構成

2.2.2 機能構成

dアカウント・コネクトの機能構成を「図 2.2-2 機能構成」に、機能一覧を「表 2.2-1 機能一覧」に示します。

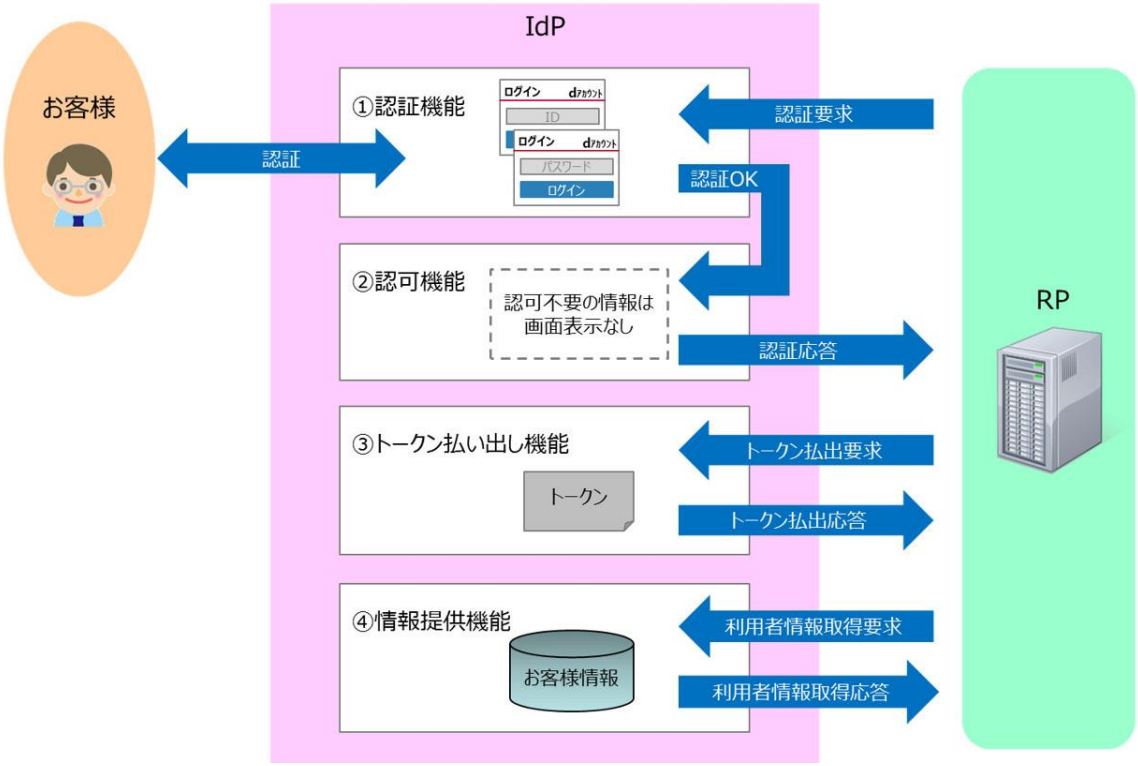


図 2.2-2 機能構成

表 2.2-1 機能一覧

No.	機能名	概要	備考
①	認証機能	RPからの認証の要求を契機に、dアカウントの ID/パスワードなどでお客様の特定を行う機能です。	
②	認可機能	RPが要求するお客様情報について、お客様に情報を提供することの同意を求める機能です。 認可が不要な情報の場合は同意画面が表示されません。 同意した結果を認証応答としてRPに返却します。	本マニュアルは同意画面が表示されない動作が前提です。
③	トークン払い出し機能	RPからのトークン払出要求により、認可されたお客様情報を取得するためのトークンを払い出す機能です。 トークン払出応答にてRPにトークンを返却します。 トークンにはお客様を特定する利用者識別情報のOpenIdが含まれています。	
④	情報提供機能	RPからの利用者情報取得要求により、トークンに対応するお客様情報をRPに提供する機能です。 お客様情報は利用者情報取得応答にてRPに返却します。	OpenIdのみ取得の場合、本機能の利用は不要ですが、suidを取得する場合は本機能の利用が必要です。

2.3 機能概要

2.3.1 認証機能

RPからの認証要求を契機に、dアカウントの ID/パスワードなどでお客様の特定を行う機能です。お客様の特定（認証）が完了後、認可機能に連携します。認証機能における対象のお客様を以下に示します。

- ドコモの携帯電話（FOMAまたはXi）サービスの利用者（個人名義、法人名義）
- ドコモの携帯電話サービス利用にかかわらず、dアカウントの利用者

認証機能のイメージを「図 2.3-1 認証機能のイメージ」に示します。

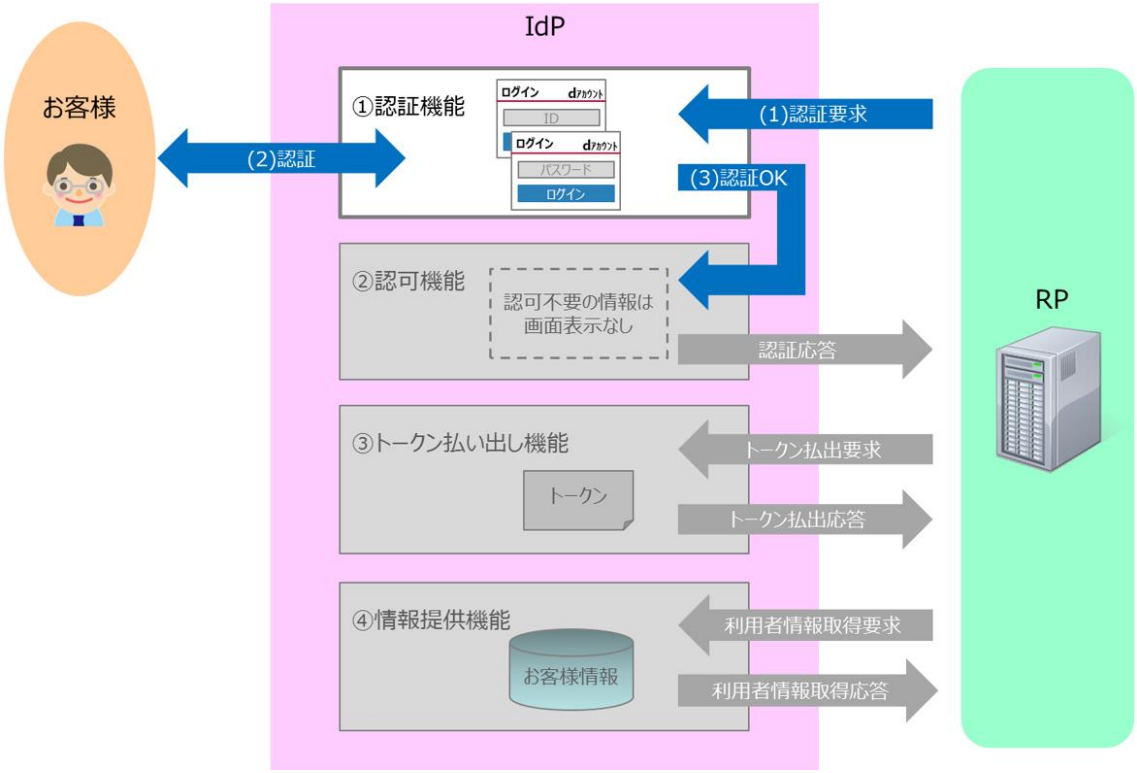


図 2.3-1 認証機能のイメージ

(1) IdPから提供してほしいお客様情報を指定し、RPから認証要求を行う。

(2) IdPはお客様を特定するため、認証を行う。

(3) 認証できた場合、認可機能に連携する。

2.3.1.1 認証要求

IdPから提供してほしいお客様情報について、RPから要求します。RPが要求するお客様情報はスコープ単位で要求します。RPは複数のスコープを指定することができます。

2.3.1.2 認証（ログイン）

お客様が利用する環境に応じて以下の2通りの認証方法を提供します。IdP側で自動的に認証方法を切り替えますので、RP側での指定や対応は不要です。どちらの認証方法を利用しても、同一のお客様として特定します。認証方法について「表 2.3-1 認証方法一覧」に、認証方法のイメージを「図 2.3-2 認証方法のイメージ」に示します。

表 2.3-1 認証方法一覧

認証方法	概要
契約回線による認証	お客様の契約回線によりお客様を特定します。
dアカウントのIDによる認証	dアカウントのIDとパスワードによりお客様を特定します。

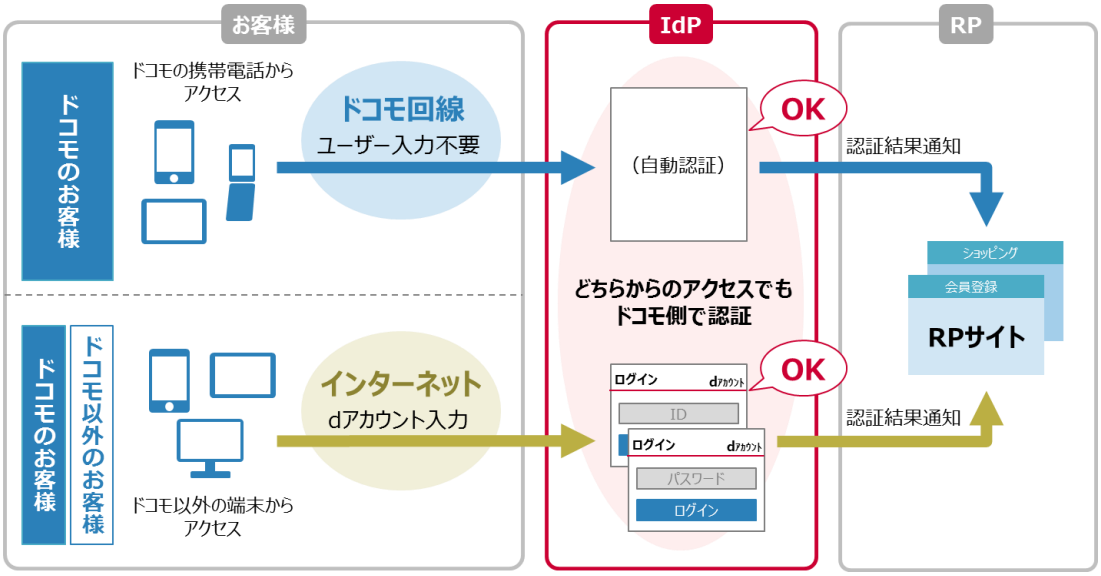


図 2.3-2 認証方法のイメージ

(1) 契約回線による認証

お客様の契約回線によりお客様を特定するため、dアカウントのIDやパスワードなどの入力なしで認証することができます。以下の条件を満たすお客様のみがご利用になれます。

- ドコモの回線契約をされているお客様
- 端末をドコモの回線（FOMAやXi）に接続してご利用の場合

(2)　dアカウントのIDによる認証

dアカウントの IDとパスワードによりお客様を特定します。端末の接続方法(Wi-Fi接続やインターネットなど)に関わらず、利用可能です。dアカウントのIDを発行していれば、ドコモのお客様だけでなく、ドコモ以外のお客様でも利用できる認証方法です。

- 生体認証について

  ドコモの生体認証に対応している端末の場合、dアカウントの IDとパスワードを入力する代わりに指紋認証や虹彩認証により認証することができます。生体認証は、申請不要で利用することができます。

- 生体認証はブラウザでの利用が前提となっているため、アプリでの利用(WebViewの利用も含む)はできません。また、WebViewにブラウザと同一のUserAgentを設定すると誤動作するため、ブラウザとは異なるUserAgentを設定してください。

- iモード利用について

  iモード契約の場合、契約回線による認証のみとなり、dアカウントのIDとパスワードを入力しての認証はできません。

  ただし、「2.3.1.4(1)別のdアカウントでログイン」を認証条件として指定した場合は、dアカウントのIDとパスワードを入力しての認証となります。

2.3.1.3　認証結果

お客様の認証ができた場合は、認可機能に連携します。この時点ではRPには認証結果が通知されず、認可後に「認可コード」が通知されます。

2.3.1.4　認証条件

提供するサービスの目的や提供形態により、お客様を認証する際の条件を指定することができます。認証条件の指定は、RPにて指定することができます。認証条件について「表 2.3-2　認証条件一覧」に示します。

表 2.3-2　認証条件一覧

認証条件	概要
別のdアカウントでログイン	複数のdアカウントをお持ちのお客様など、dアカウントを切り替えて利用するためのログインを行うことができます。 SSO(シングルサインオン)は行わず、強制的にdアカウントのIDとパスワードの入力が求められます。
ドコモのお客様に限定してログイン	ドコモのお客様に限定してサービスを提供することができます(ドコモ以外のお客様はログインできません)。
回線接続時でもID認証でログイン	回線接続をしている場合でも、回線による認証を行わずにdアカウントのIDとパスワードによるログインを必須とすることができます。 SSO(シングルサインオン)は有効であるため、すでにdアカウントのIDとパスワードによりログイン済みの場合は認証画面が省略されます。

(1)　別のdアカウントでログイン

複数の端末（マルチデバイス）をご利用のお客様にサービスを提供する場合など、端末ごとに発行した複数のdアカウントを切り替えて利用するための認証を行うことができます。別のdアカウントでログインするイメージを「図 2.3-3 別のdアカウントでログイン」に示します。

すでに認証済みの状態であってもシングルサインオンせず、強制的にお客様に認証（IDとパスワードの入力）を要求し、入力されたIDとパスワードで再認証をします。

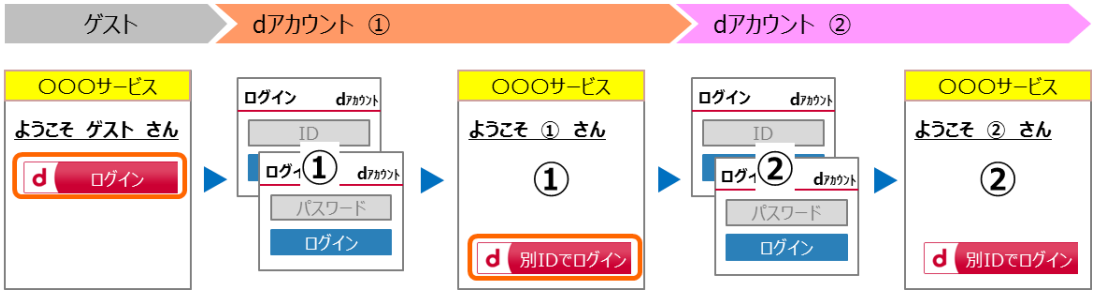


図 2.3-3 別のdアカウントでログイン

(2)　ドコモのお客様に限定してログイン

ドコモのお客様に限定してサービスを提供できます。ドコモ以外のお客様が認証した場合は「このサービスは利用できません」というメッセージを表示し、認証できません。

認証結果は、ドコモのお客様の場合のみに通知され、ドコモ以外のお客様の場合は何も通知されませんので、RP側でドコモ以外のお客様の判定を行う必要はありません。

(3)　回線接続時でもID認証でログイン

回線接続をしている場合でも、回線による認証を行わずにdアカウントのIDとパスワードによるログインを必須とすることができます。回線による認証では、お客様の操作なしにログイン状態となるため、重要な情報を扱うサービスなど、お客様の本人確認をする意味でdアカウントのIDとパスワードを入力していただく場合などに利用します。

- お客様がdアカウントのIDを発行していない場合はログインができませんので、利用する場合はご注意ください。
- シングルサインオンは有効であるため、すでにdアカウントのIDとパスワードによりログイン済みの場合は認証画面が省略されます。

2.3.1.5　ログアウト機能

IdPからログアウトし、シングルサインオンの状態を破棄する機能です。セキュリティ面を考慮し、適宜、ログアウト機能の実装を推奨します。ログアウトのユーザインタフェースについては「3.2ログアウト」、インタフェース詳細については「4.4.7ログアウトCGI [API-4]」を参照してください。

2.3.1.6　シングルサインオン

お客様がログインした後は一定時間ログイン状態を保持し、シングルサインオンに対応するサービス間を移動する際に、ID/パスワードの入力を省略することで便利にサービスをご利用いただくことができる機能を提供しています。シングルサインオンのイメージを「図 2.3-4 シングルサインオン」に示します。

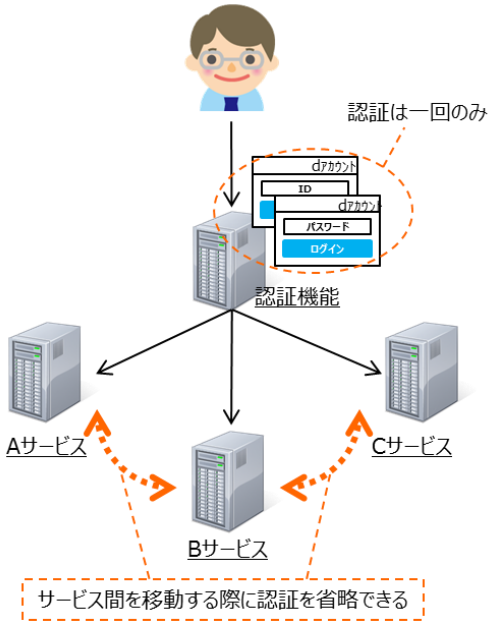


図 2.3-4 シングルサインオン

2.3.1.7　セキュリティ対策機能

セキュリティ対策としてIdPでは以下の機能を提供しています。

(1)　2段階認証

2段階認証は、ID/パスワードの認証に追加して、さらにセキュリティコードによる認証を行うことで、より安全にログインするための機能を提供しています。2段階認証のイメージを「図 2.3-5 2段階認証」に示します。

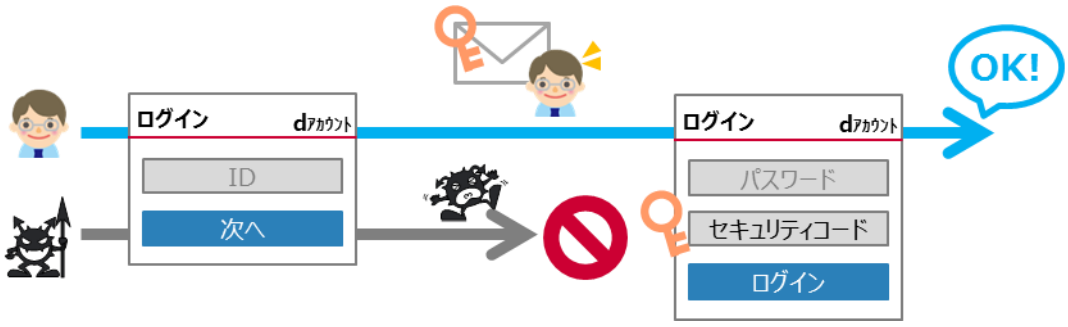


図 2.3-5 2段階認証

(2)　dアカウントのロック

ID/パスワードの入力を一定回数以上間違えた場合、dアカウントをロックすることにより、パスワードの総当たり攻撃などによる不正ログインを防止する機能を提供しています。dアカウントのロックのイメージを「図　2.3-6　dアカウントのロック」に示します。

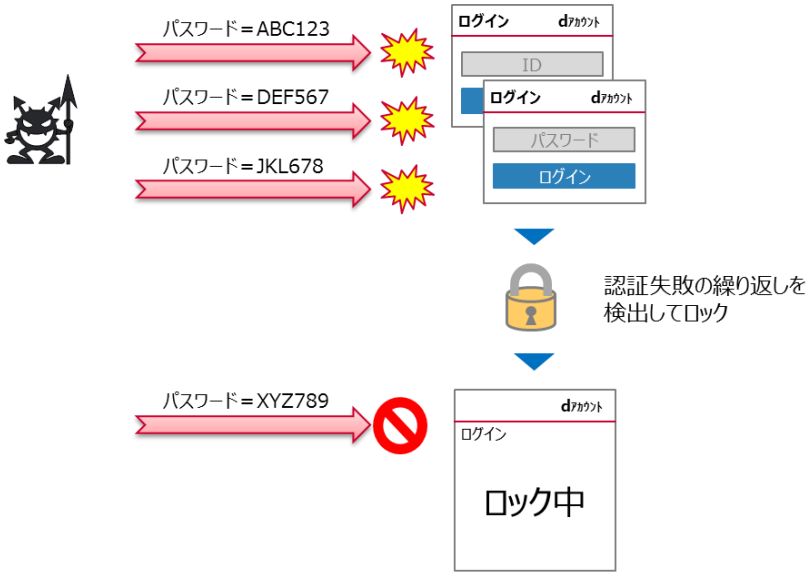


図　2.3-6　dアカウントのロック

(3)　dアカウント利用履歴

dアカウントのID/パスワードによる認証を行った履歴を参照することができ、不正ログインなどが行われたことをお客様が検知できる機能を提供しています。「https://id.smt.docomo.ne.jp/cgi7/id/histview」からdアカウント利用履歴を参照できます。

2.3.2 認可機能

認可機能は、RPが要求したお客様情報に対して、IdPからRPにお客様情報を提供することについてお客様の同意を求める機能です。お客様が情報提供に同意した場合は認可コードがRPに返却されます。

なお、本書では同意画面が表示されない動作を前提としています。認可機能のイメージを「図 2.3-7 認可機能のイメージ」に示します。

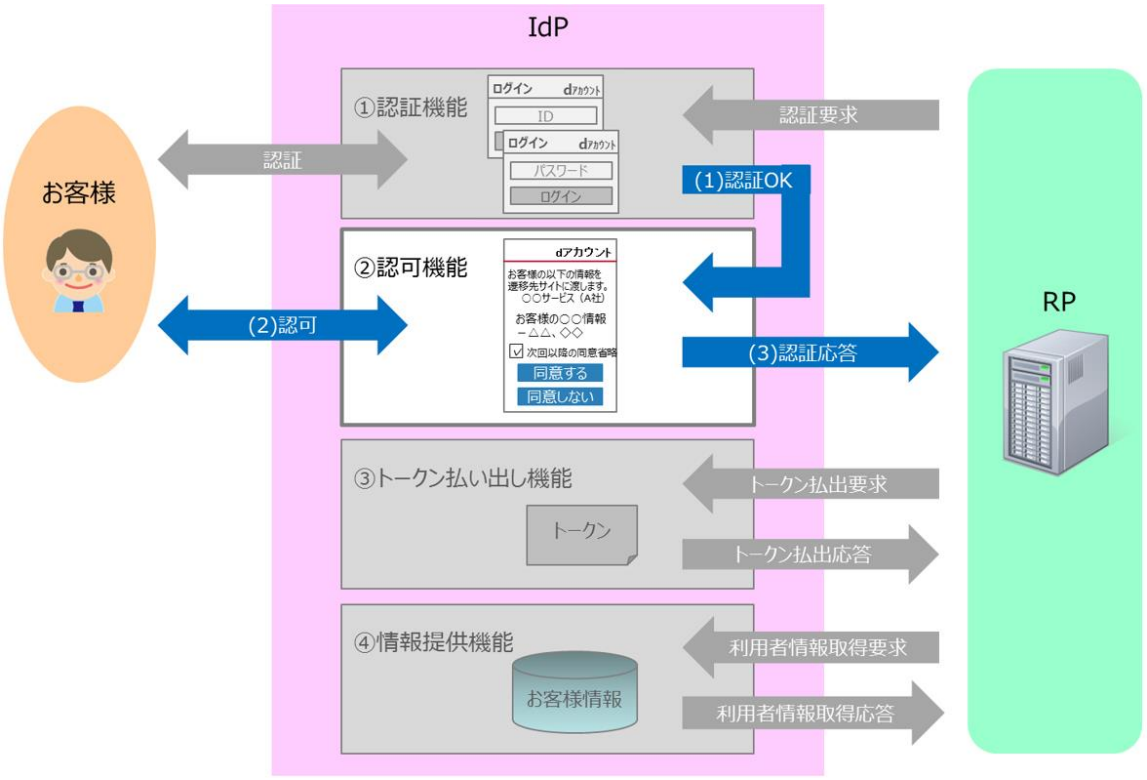


図 2.3-7 認可機能のイメージ

(1) 認証できた場合、認証機能から連携されます。

(2) RPが要求するお客様情報について、お客様に情報を提供することの同意を求めます。

(3) お客様が認可した結果を返却します。

2.3.2.1 お客様同意

RPが要求したスコープが同意を必要とする情報の場合に同意画面を表示し、同意が不要な情報の場合は同意画面が表示されません。本マニュアルでは、同意が不要な情報のみを扱うRPを対象としているため、同意画面が表示されない動作を前提としています。

2.3.2.2 認可結果

同意画面の表示が不要な場合、同意されたものとして扱い、認可の結果として認可コードをRPに返却します。

2.3.3 トークン払い出し機能

認可されたお客様情報を取得するためのトークンを払い出す機能です。

トークン払い出し機能のイメージを「図 2.3-8 トークン払い出し機能のイメージ」に示します。

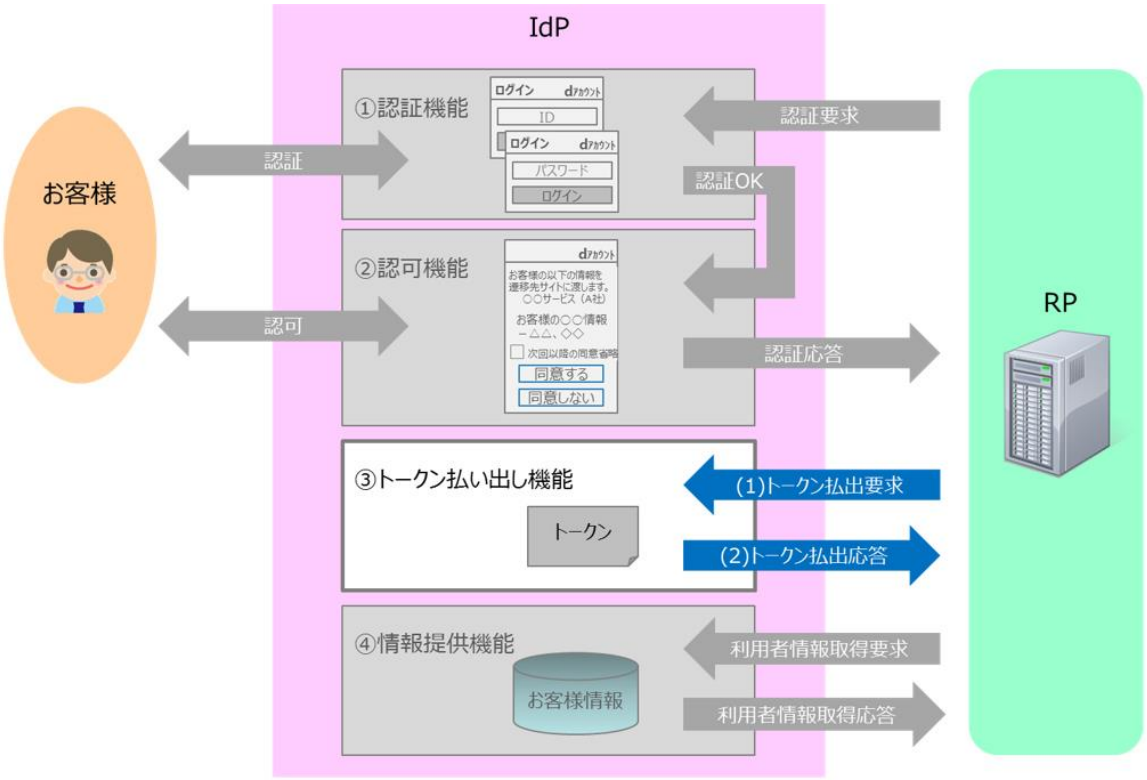


図 2.3-8 トークン払い出し機能のイメージ

(1) 認可されたお客様情報を取得するためのトークン払出要求を行います。

(2) トークン払出応答により、お客様情報を取得するためのトークンを返却します。

2.3.3.1 トークン払い出し

お客様が同意したことを表す認可コードにより、トークンを払い出します。漏洩のリスクを軽減するため、認可コードは発行されてから短期間で無効となり、1回のみ利用ができます。認可コードを取得後は速やかにトークンの払出しを行う必要があります。

トークンについての詳細は「5.3トークン」参照ください。

2.3.4 情報提供機能

お客様が同意した情報をRPに提供する機能です。払い出されたトークンによりお客様の情報が取得できます。

情報提供機能のイメージを「図 2.3-9 情報提供機能のイメージ」に示します。

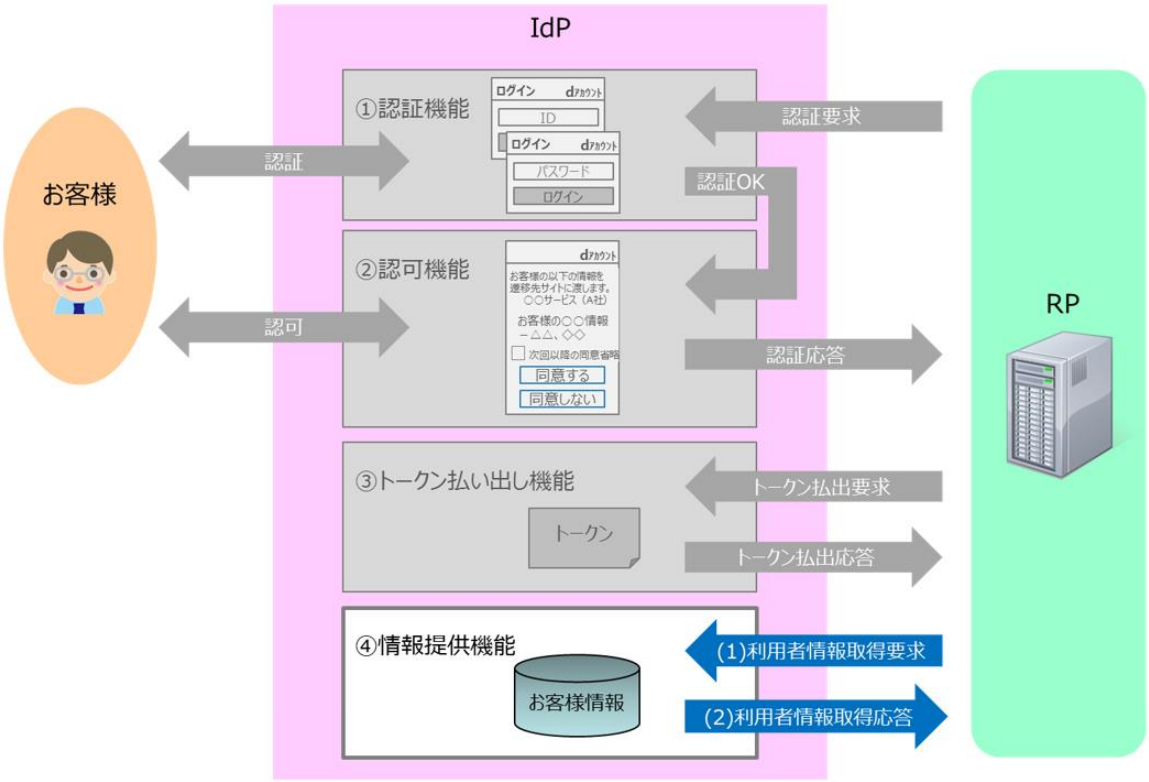


図 2.3-9 情報提供機能のイメージ

(1) 払い出されたトークンにより、お客様情報の取得要求を行います。

(2) トークンに対応したお客様情報を返却します。

2.3.4.1 お客様情報の取得

RPは、IdPから払い出されたトークンにより、お客様情報を取得できます。取得するお客様情報がない場合、情報の取得を行う必要はないため、必要に応じて本機能を利用します。トークンは、認証を行う際にRP側で指定したスコープに対して払い出されるため、指定したスコープの情報のみが取得できます。RPが取得する情報はJSON形式にて提供されます。クレームの出力形式については「4.1.3JSONの形式について」を参照してください。

3. ユーザインタフェース user interface

本章では、dアカウント・コネクトを利用する場合のユーザインタフェースとして、画面遷移について説明します。
Chương này giải thích về di chuyển màn hình như là user interface trong trường hợp dùng daccount-connect manual.

3.1 認証・認可 xác thực - approve

3.1.1 基本シーケンス sequence cơ bản

基本シーケンスについて「図 3.1-1 基本シーケンス」に示します。Về sequence cơ bản thì tham khảo sơ đồ sau

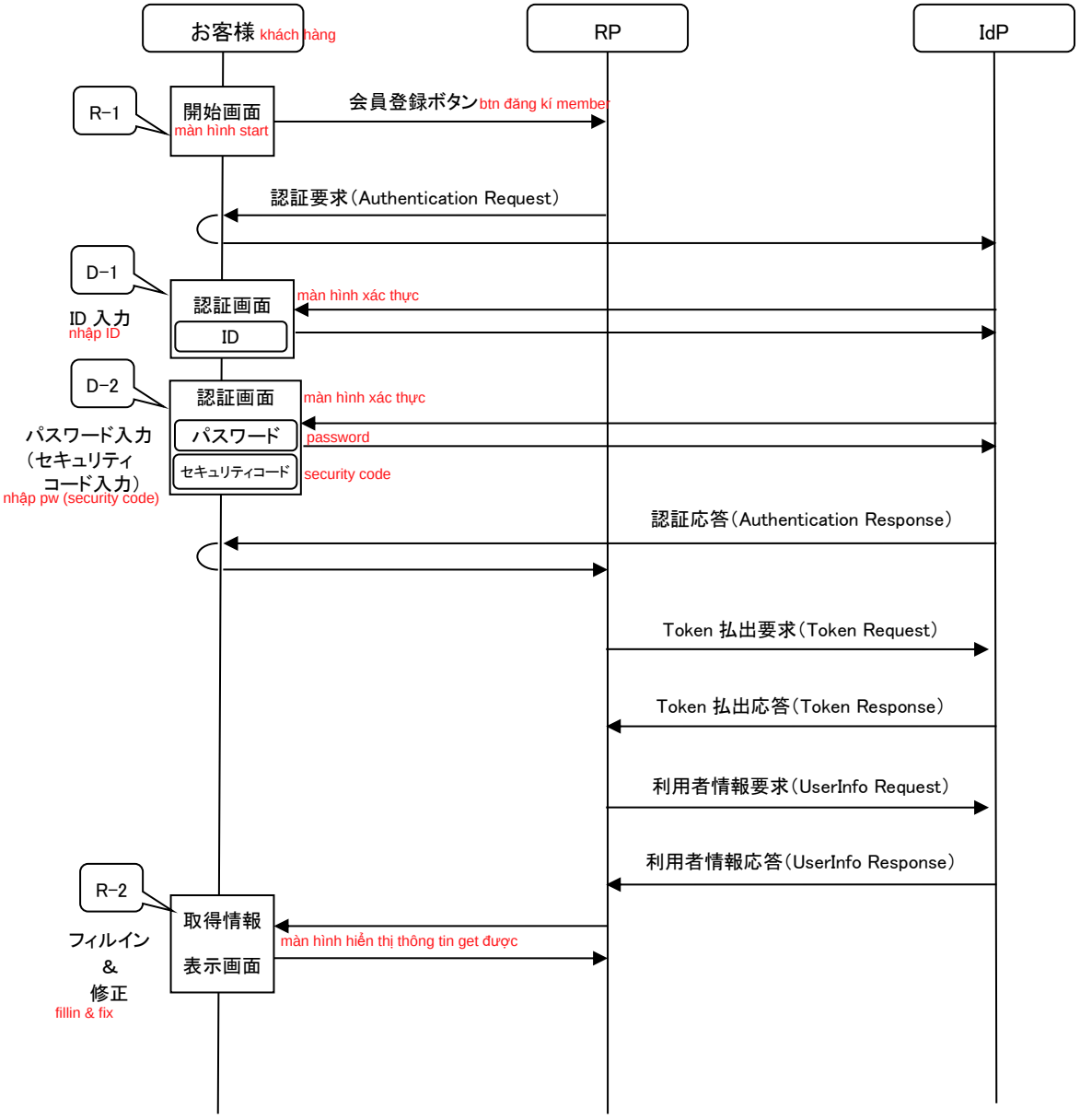


図 3.1-1 基本シーケンス

3.1.2 画面遷移 di chuyển màn hình

契約回線による認証時のイメージを「図 3.1-2 契約回線による認証時の画面遷移」に、dアカウントによる認証時のイメージを「図 3.1-3 dアカウントによる認証時の画面遷移」に示します。
Khi xác thực theo đường dẫn kí kết thì tham khảo sơ đồ 3.1-2, khi xác thực theo d-account thì tham khảo sơ đồ 3.1-3

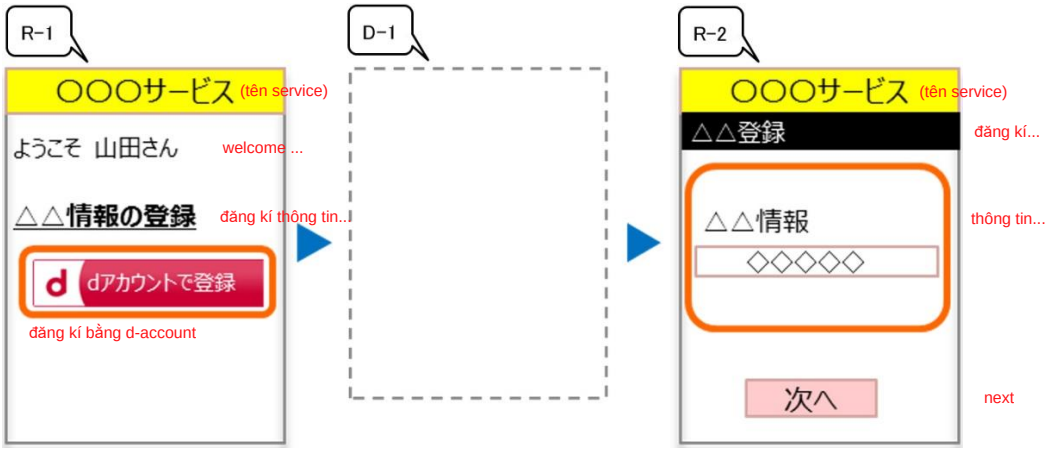


図 3.1-2 契約回線による認証時の画面遷移 di chuyển màn hình khi xác thực theo đường dẫn kí kết

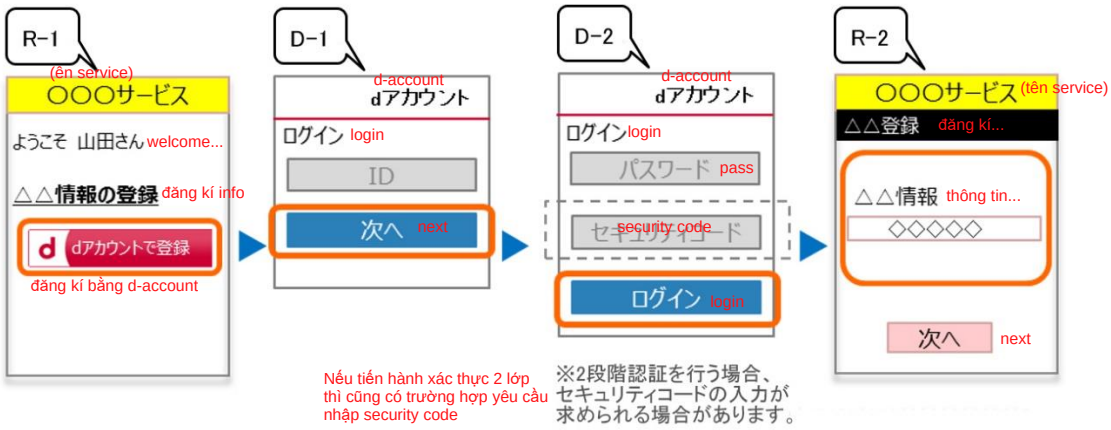


図 3.1-3 dアカウントによる認証時の画面遷移 di chuyển màn hình khi xác thực theo d-account

3.2 ログアウト logout

3.2.1 基本シーケンス sequence cơ bản

ログアウトは、「ログアウト完了画面」の表示有無を指定することができるため、ログアウト完了画面の表示あり/表示なしのシ
Khi logout thì có thể chỉ định có hiển thị màn hình logout hoàn tất hay không, nên sẽ giải thích về sequence hiển thị/không hiển thị màn hình logout hoàn tất.
ーケンスについて説明します。

3.2.1.1 ログアウト完了画面表示なしの場合 TH không hiển thị màn hình logout hoàn tất

ログアウト完了画面表示なしの場合のシーケンスについて、「図 3.2-1 ログアウト完了画面「表示なし」のシーケンス」に示しま
TH không có màn hình logout hoàn tất thì tham khảo sequence sau:
す。

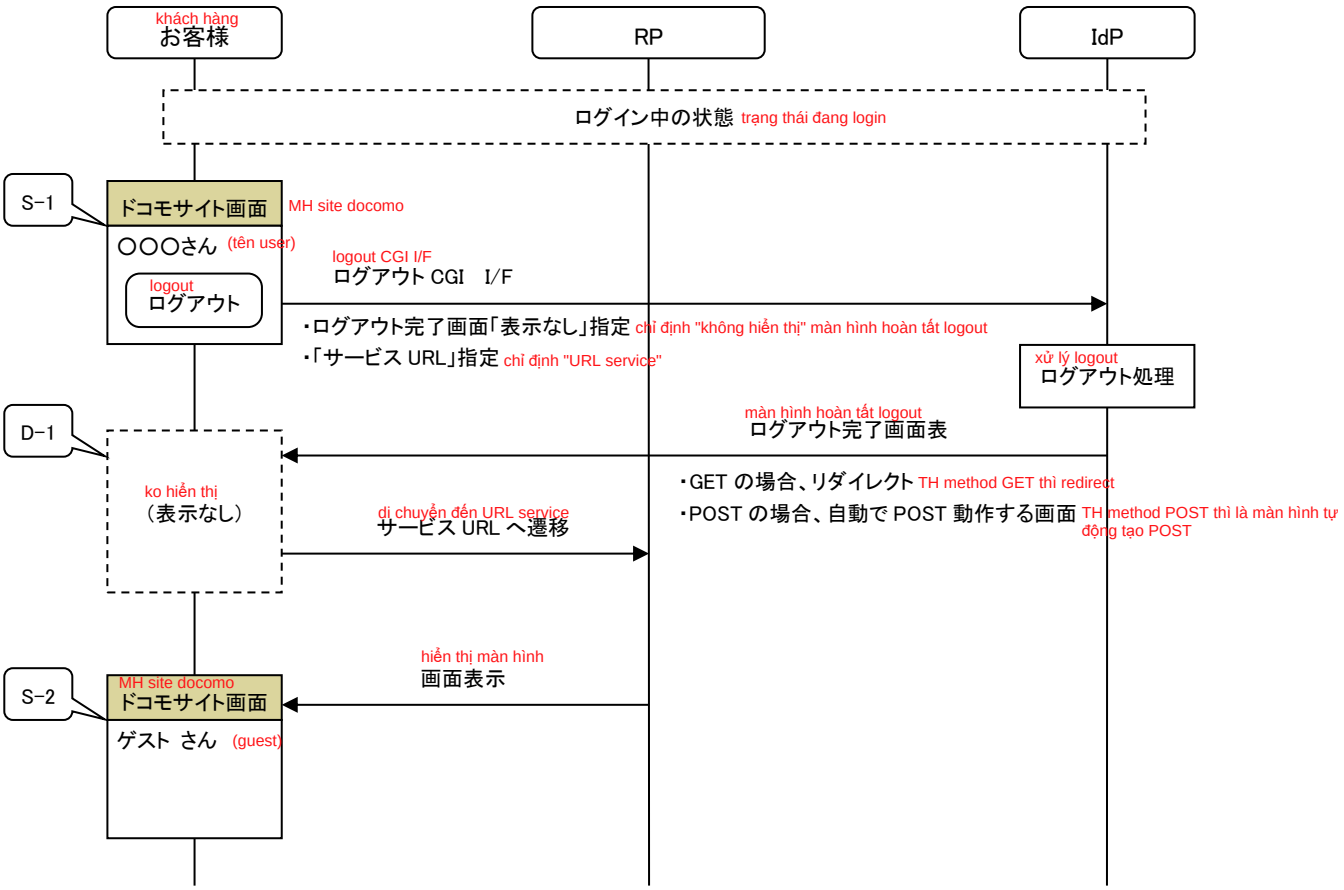


図 3.2-1 ログアウト完了画面「表示なし」のシーケンス seqience không hiển thị màn hình hoàn tất logout

3.2.1.2 ログアウト完了画面表示ありの場合 TH có hiển thị màn hình hoàn tất logout

ログアウト完了画面表示ありの場合のシーケンスについて、「図 3.2-2 ログアウト完了画面「表示あり」のシーケンス」に示します。
TH có hiển thị màn hình hoàn tất logout thì tham khảo sequence sau

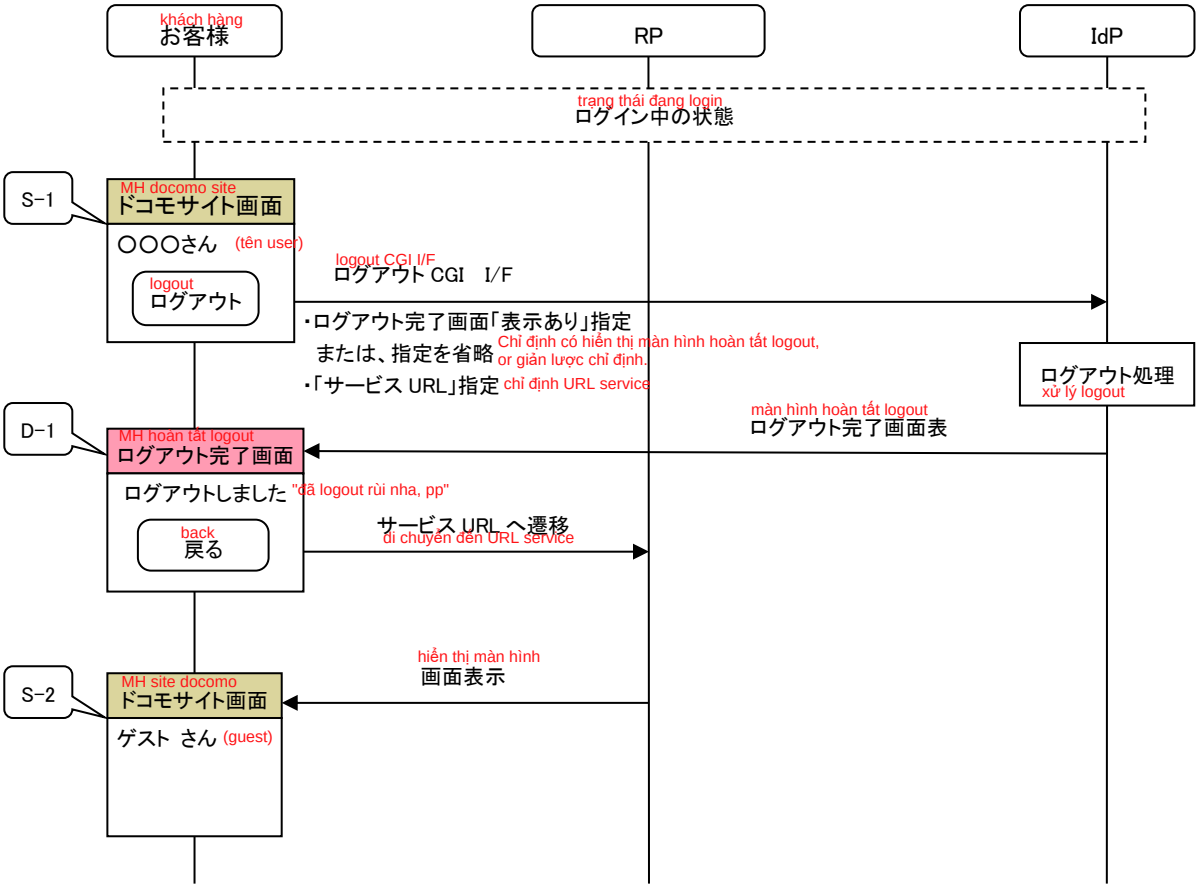


図 3.2-2 ログアウト完了画面「表示あり」のシーケンス
sequence không hiển thị màn hình hoàn tất logout

3.2.2 画面遷移 di chuyển màn hình

3.2.2.1 ログアウト完了画面表示なしの場合 TH không hiển thị màn hình hoàn tất logout

ログアウト完了画面表示なしの場合の画面推移について、「図 3.2-3 画面遷移（ログアウト完了画面表示なし）」に示します。

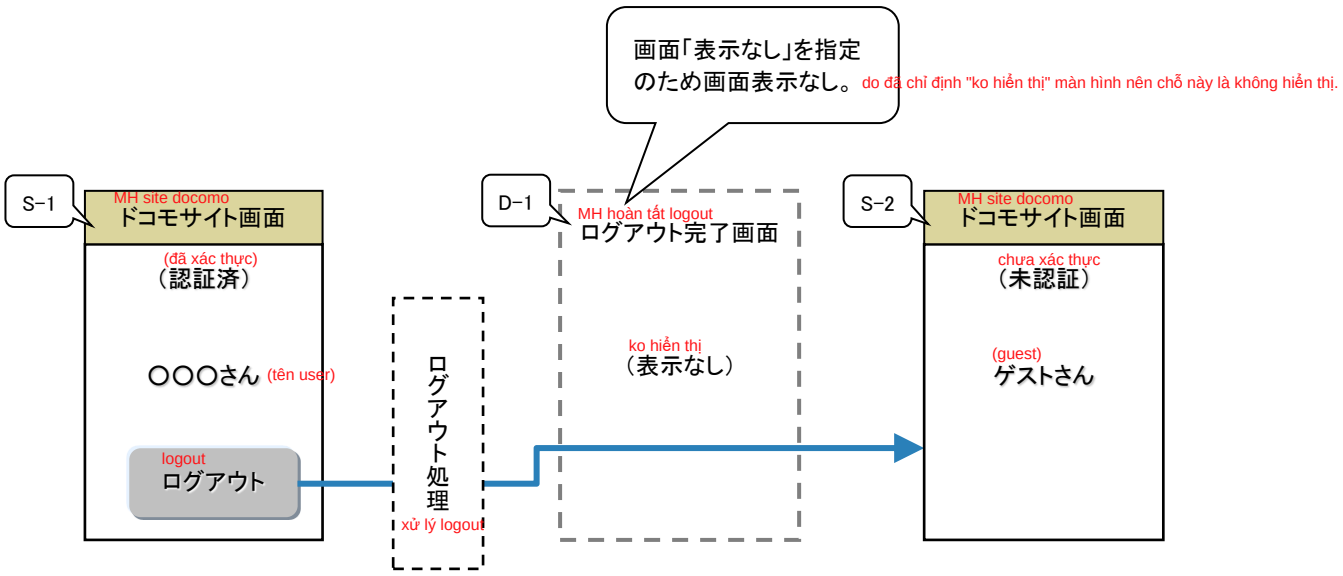


図 3.2-3 画面遷移（ログアウト完了画面表示なし）

- ログアウト完了画面について、ログアウトI/FをPOSTで呼び出した場合、ログアウト完了画面はJavaScriptで自動的にPOST
  Về màn hình hoàn tất logout, TH đã gọi logout I/F bằng POST thì màn hình hoàn tất logout sẽ tự động tiến hành POST bằng JavaScript, theo độ nhanh xử lý và độ nhanh
  を行うため、処理速度や通信速度により一瞬、画面が表示されることがあります。 của giao thức mà màn hình sẽ được hiển thị trong 1 khoảng thời gian ngắn

JavaScriptが動作しないブラウザの場合、「図 3.2-4 JavaScriptが動作しない場合の画面」が表示され、お客様の操作により
TH browser đó JavaScript không thao tác được thì hiển thị màn hình như sơ đồ 3.2-4, di chuyển đến URL service theo thao tác của khách hàng.
サービスURLに遷移します。

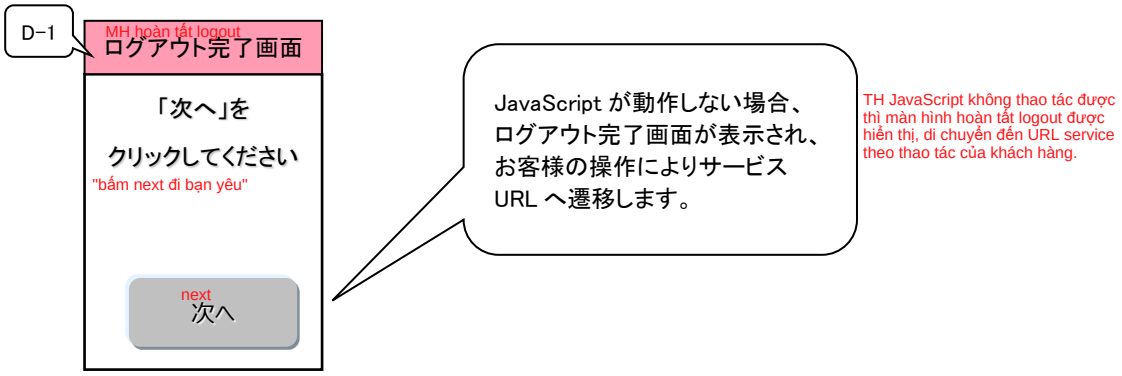


図 3.2-4 JavaScriptが動作しない場合の画面

3.2.2.2 ログアウト完了画面表示ありの場合 TH có hiển thị màn hình hoàn tất logout

ログアウト完了画面表示ありの場合の画面推移について、「図 3.2-5 画面遷移（ログアウト完了画面表示あり）」に示します。

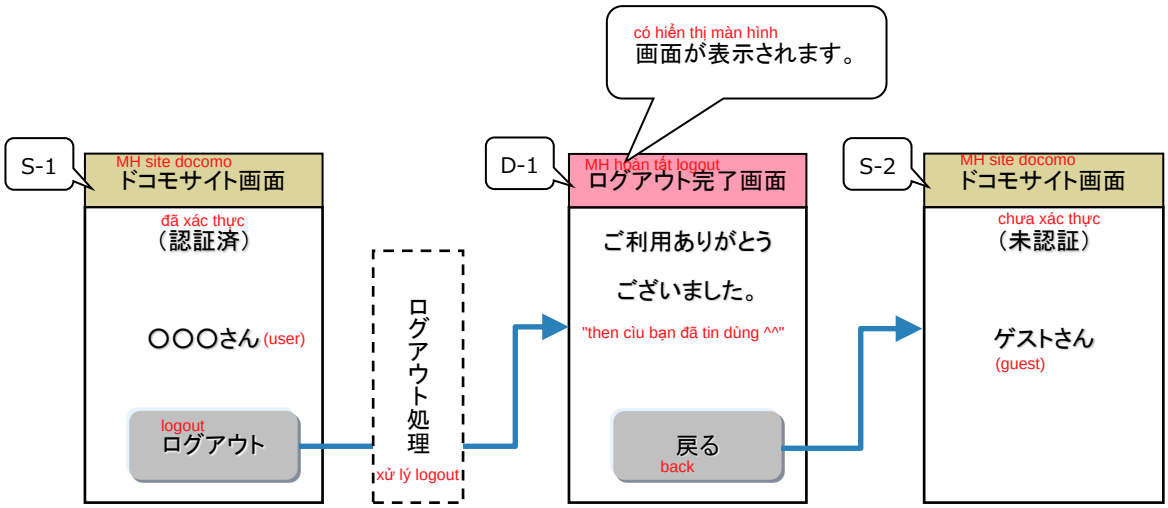


図 3.2-5 画面遷移（ログアウト完了画面表示あり）

3.2.3 ログアウト完了画面 Màn hình hoàn tất logout

ログアウト完了画面は、画面の一部をカスタマイズして表示することができます。MH hoàn tất logout có thể hiển thị sau khi customize 1 phần của màn hình.

カスタマイズするパラメータについては、「4.4.7.3要求パラメータ」を参照ください。Về parameter customize, plz tham khảo 4.4.7.3 (Parameter request)

3.2.3.1 パソコン画面 Màn hình PC

パソコン画面のカスタマイズについて「図 3.2-6 パソコン画面のカスタマイズ」に示します。tham khảo hình dưới nha.

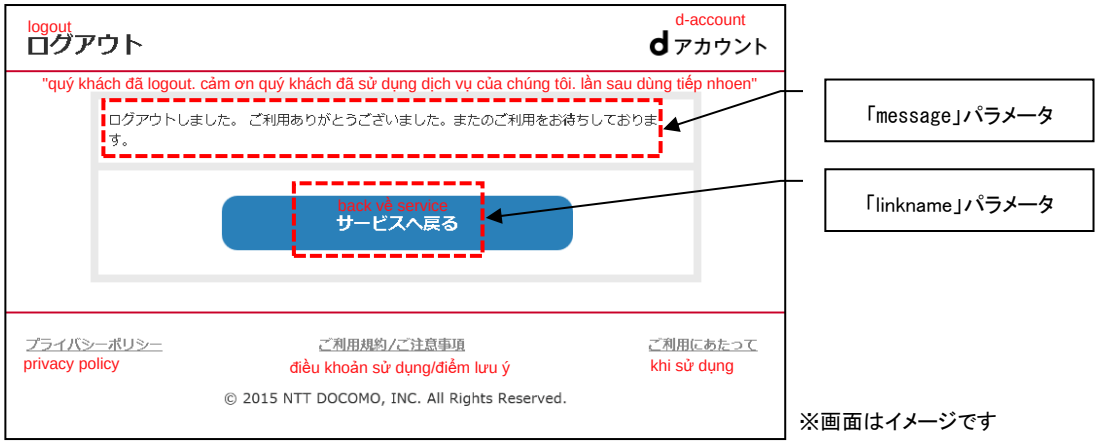


図 3.2-6 パソコン画面のカスタマイズ

3.2.3.2 スマートフォン画面 Màn hình SP

スマートフォン画面のカスタマイズについて「図 3.2-7 スマートフォン画面のカスタマイズ」に示します。 tham khảo hình dưới

item giống PC nên em ko dịch nha

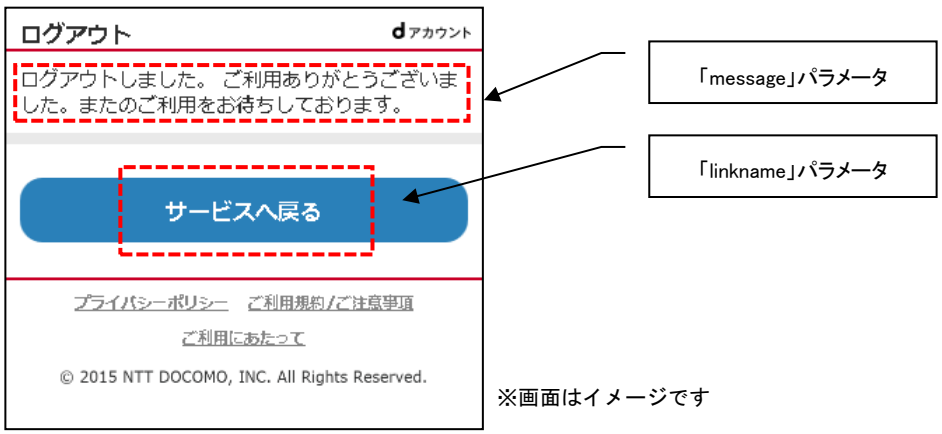


図 3.2-7 スマートフォン画面のカスタマイズ

3.2.3.3 デフォルト画面 Màn hình default

パラメータの指定がない場合や、パラメータにエラーがある場合は、デフォルト画面が表示されます。
TH không có parameter chỉ định or parameter bị lỗi thì hiển thị màn hình default.

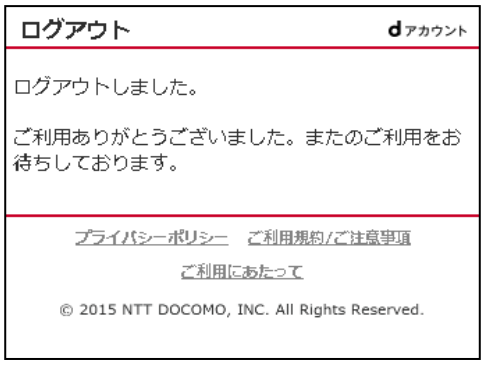
デフォルト画面は固定表示となり、カスタマイズはできません。
Màn hình default được hiển thị cố định, không customize.

デフォルト（パソコン、スマートフォン）画面イメージを「図 3.2-8 デフォルト画面」に示します。
Tham khảo hình dưới

パソコン画面 Màn hình trên PC

※画面はイメージです

スマートフォン画面 màn hình trên SP



※画面はイメージです

図 3.2-8 デフォルト画面

4. システムインタフェース sequence system

本章では、dアカウント・コネクトのシステムインタフェースについて説明します。

4.1 共通事項 mục common

4.1.1 利用プロトコル protocol sử dụng

HTTPプロトコルを利用する。HTTP

4.1.2 HTTP利用規定 quy định sử dụng HTTP

4.1.2.1 HTTPリクエスト規定 quy định request HTTP

(1) リクエストURIのホスト部については、英字大/小文字を区別しない。phần host của URI request thì không phân biệt chữ hoa thường

(2) リクエストURIのパス、CGI名については英字大/小文字を区別する。path của URI request không phân biệt hoa thường.

(3) リクエストヘッダ名については、英字大/小文字を区別しない。tên header request không phân biệt hoa thường.

(4) リクエストヘッダの値については、英字大/小文字を区別する。giá trị của header request CÓ phân biệt hoa thường.

(5) リクエストヘッダの並び順については規定しない。không quy định chiều sort của header request.

(6) リクエストの行末と認識するのは、<CR><LF>のみである。Nhận thức về cuối line của request chỉ có <CR>, <LF>

(7) <CR> :0x0d (CarriageReturn)

(8) <LF> :0x0a (LineFeed)

(9) チャンク形式は対応しない。không đối ứng format chunk

(10) HTTPリクエスト各部の制限長は以下の通りとする。 độ dài giới hạn cảu từng phần request HTTP:

- リクエストライン:2048byte request line
- リクエストヘッダ部:8192byte phần header request
- ボディ部:40960byte phần body

4.1.2.2 HTTPレスポンス規定 quy định response request

(1) レスポンスヘッダの並び順については、規定しない。 không quy định chiều sort của header request

4.1.3 JSONの形式について về format JSON

4.1.3.1 出力規則 quy tắc output

APIのレスポンスデータがJSON形式の場合、応答データの各データ型に従い、「表 4.1-1 JSONの出力規則」に示す規則にしたがって出力されます。
TH data response của API là format JSON thì theo từng data của data đối ứng để output dựa theo bảng sau:

表 4.1-1 JSONの出力規則

No.	データ型	出力形式	備考
1	Object	半角中括弧「{ ～ }」の内部に包含するデータを、data chứa trong phần ngoặc {} halfsize (項目名):(データ) (tên item):(data) の形式で繰り返し出力する。thì output lặp lại theo định dạng. (項目名):(データ)は、″,″(半角カンマ)で区切られる。phân cách bằng dấu "," (データ)は、Object、Array、String、Number、Booleanがある。 例：{ ″name1″:value1, ″name2″: value2, … ″nameN″:valueN }	※JSONレスポンスは1つのObjectで全体を包括している。 Response JSON chứa toàn bộ trong 1 Object.
2	Array	半角大括弧「[～]」の内部に複数のデータを繰り返し出力する。lặp lại nhiều data trong phần [] [(データ), (データ)…] [(data), (data),...] (データ)は、″,″(半角カンマ)で区切られる。 phân cách bằng "," (データ)は、Object、Array、String、Number、Booleanがある。 (data) có thể là object, array, string, number, boolean 例： [value1, value2, … , valueN]	
3	String	前後を「″」(半角ダブルクォーテーション)で括り、対象データの文字列として出力する。bỏ trong dấu ngoặc kép "", output dưới dạng chuỗi kí tự của data đối tượng. また、対象の文字列は次の規則によりエスケープ処理が行なわれる。Ngoài ra, chuỗi kí tự đó phải xử lý escape theo quy tắc: ①¥によるエスケープ 1. Escape theo ¥ 「″」(半角ダブルクォーテーション) ⇒「¥″」 「"」→「¥ "」 「¥」(エンマーク) ⇒「¥¥」 「¥」(enmark)→「¥¥」 「/」(スラッシュ) ⇒「¥/」 「/」→「¥/」 水平タブ(HT) ⇒「¥t」 復帰(CR) ⇒「¥r」 改行(LF) ⇒「¥n」 後退(BS) ⇒「¥b」 改頁(FF) ⇒「¥f」 ②Unicodeエスケープ 「<」⇒「¥u003C」 「>」⇒「¥u003E」 例： ″string-value″	※インタフェース詳細仕様に記載されているパラメータ長については、エスケープ処理による文字数増を含めない標記となります。 エスケープ対象の文字が含まれる項目については、各インタフェース詳細仕様の形式欄を参照してください。
4	Number	対象のデータを10進数値としてそのまま出力する。 エスケープ処理は行なわない。 例： 2	※項目によっては、負数もあります。
5	Boolean	ブール値対象のデータをそのまま出力する。 ・ブール値のtrue： true ・ブール値のfalse： false	

4.1.3.2 クレームの返却の有無

クレームに値が存在しない場合、クレームそのものを返却しません。(空白やnullなどの返却はしません)

4.1.4 インタフェース接続条件

4.1.4.1 対象ブラウザ

動作確認を行ったブラウザを「表 4.1-2 動作確認を行ったブラウザー覧」に示します。なお、動作確認を行ったブラウザについても動作を保障するものではなく、バージョンなどにより動作しない可能性がありますので、あらかじめご了承ください。

表 4.1-2 動作確認を行ったブラウザー覧

デバイス	ブラウザ
パソコン	Internet Explorer 11.0 Microsoft Edge Chrome Firefox
スマートフォン・iPhone	ドコモが発売しているスマートフォン（Android2.3以降）の標準ブラウザ ドコモが発売しているiPhoneの標準ブラウザ
タブレット・iPad	ドコモが発売しているタブレット（Android4.0以降）の標準ブラウザ ドコモが発売しているiPadの標準ブラウザ
フィーチャーフォン	ドコモが発売しているiモード端末のiモードブラウザ2.0以降 （iモードブラウザ1.0の端末はご利用になれません）

4.1.4.2 対象RP

ドコモが認めたRPに限定します。ご利用になる前に利用申請されている必要があります。

4.1.4.3 ネットワーク条件

(1) SSL通信

- RPからIdPへの接続はSSL通信が必須です。
- SHA-2のSSLサーバ証明書に対応している必要があります。
- IdPのSSLサーバ証明書に対応する以下のルート証明書がRPに導入されている必要があります。

  DigiCert Global Root CA

(2) IPアドレス

- IPアドレスは固定である必要があります。
- 固定IPアドレスの対象は、トークン払出要求、利用者情報取得要求を行うサーバのIPアドレスです。（認証要求を行うサーバは対象外です）
- 固定IPアドレスであれば、複数のIPアドレスの利用も可能です。（負荷分散などで複数台のサーバから要求を行う場合、要求を行うすべてのIPアドレスの利用申請が必要です）
- 複数IPアドレスを利用する場合、各要求（トークン払出要求、利用者情報取得要求）が異なるIPアドレスから要求されても利用可能です。

4.1.4.4　文字コード

UTF-8を使用します。

4.1.4.5　制限事項

(1)　HTTPリダイレクト連続回数制限

認証要求から認証応答までのリダイレクト連続回数は最大で3回です。

(2)　Cookie

Cookieが利用できる必要があります。

4.1.5　共通エラー

エラー応答は、個別の要求に対するエラー応答の他に共通的に応答するエラー応答が存在します。

- 共通エラーでは、エラーコードは応答しません。
- Authentication Request（認証要求）固有のエラーは、RP（クライアント）に「302 : Found」にて応答しますが、共通エラーの発生時は応答を行いません。

共通的に応答する可能性のあるエラー応答を「表 4.1-3　共通エラー応答」に示します。

表 4.1-3 共通エラー応答

No.	ステータスコード		事象	詳細
1	400	Bad Request	リクエスト構文にエラーがある。	リクエストライン形式不正
2				Method不正(POST/GETでない)
3				リクエストHTTPバージョン形式不正
4				リクエストヘッダ解析エラー
5				リクエストヘッダが重複している場合
6				リクエストラインサイズ不正
7				リクエストラインに2048byteを超える長さの値が設定された場合 ※iモードアクセスの場合、2048byteが制限。 ※iモードアクセス以外の場合、4096byteが制限
8				Content-Typeヘッダに誤りがある
9				リクエストヘッダサイズ不正
10				受信したリクエストヘッダのサイズ合計が8192byteを超える場合
11				リクエスト不正
12				Content-Lengthヘッダ値に40960を超える値が設定された場合
13				リクエスト受信エラー
14	404	Not Found	リクエストURLかHostヘッダに誤りがある。	URLに対するCGIがない
15				URLがWCのサービスサイト向け透過I/F許容IPアドレステーブルに存在しない
16	408	Request Time-out	リクエストの受信に時間がかかった。	リクエストタイムアウト
17				レスポンス送信タイムアウト
18				Content-lengthヘッダに誤りがある
19	413	Request Entity Too Large	リクエストのContent-Lengthヘッダの設定値に誤りがある。	リクエストボディサイズ不正
20	500	Internal Server Error	システム内で障害、エラーが発生した。	センタ切替折り返しエラー
21				強制折り返しエラー
22				コンテナ折返し
23				GI/GX付加リクエストヘッダ不正
24				自サーバの内部矛盾
25				下位CP異常検知など。
26	501	Not Implemented	未対応のメソッドでリクエストされた。	Method不正
27	503	Service Unavailable	システムで輻輳が発生した。	FWグレイン 流量規制
28				FWグレイン アクティブスレッド数規制
29				APグレイン 流量規制
30				APグレイン アクティブスレッド数規制
31				リソース不足
32				CGI折返し

4.2 基本シーケンス SEQUENCE CƠ BẢN

4.2.1 認証・認可 Xác thực - cho phép

dアカウント・コネクトの基本シーケンスを「図 4.2-1 認証・認可の基本シーケンス」に示します。
sơ đồ 4.2-1 là sequence cơ bản của d-account - connect

吹き出しの数字はインタフェース一覧（表 4.3-1 インタフェース一覧）の「API番号」に対応します。
Những chữ như API-1-1 thì tham khảo bảng 4.3-1 với mã số API

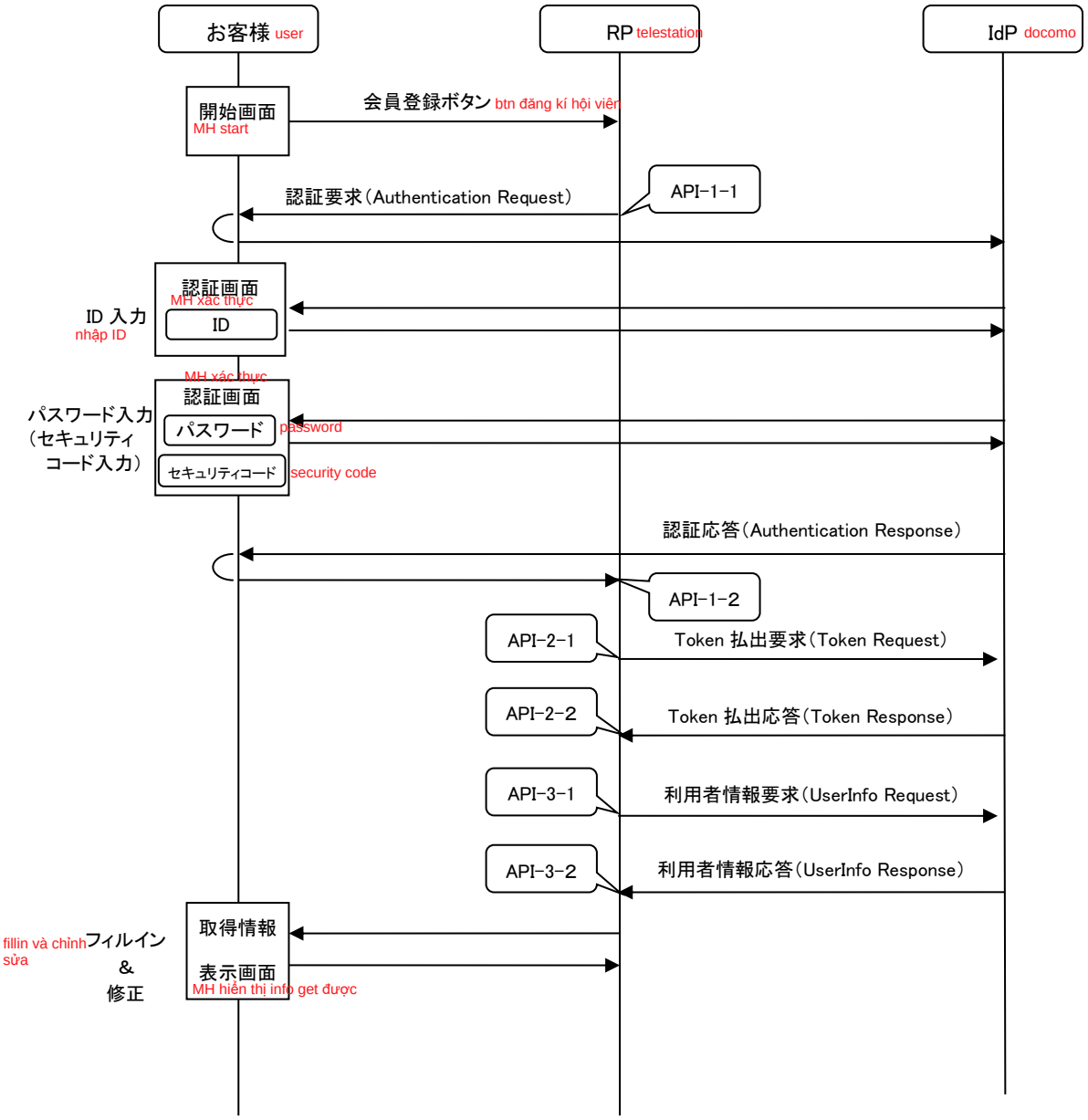


図 4.2-1 認証・認可の基本シーケンス

logout không cần nên ko dịch

4.2.2 ログアウト

ログアウトの基本シーケンスを「図 4.2-2 ログアウトの基本シーケンス」に示します。

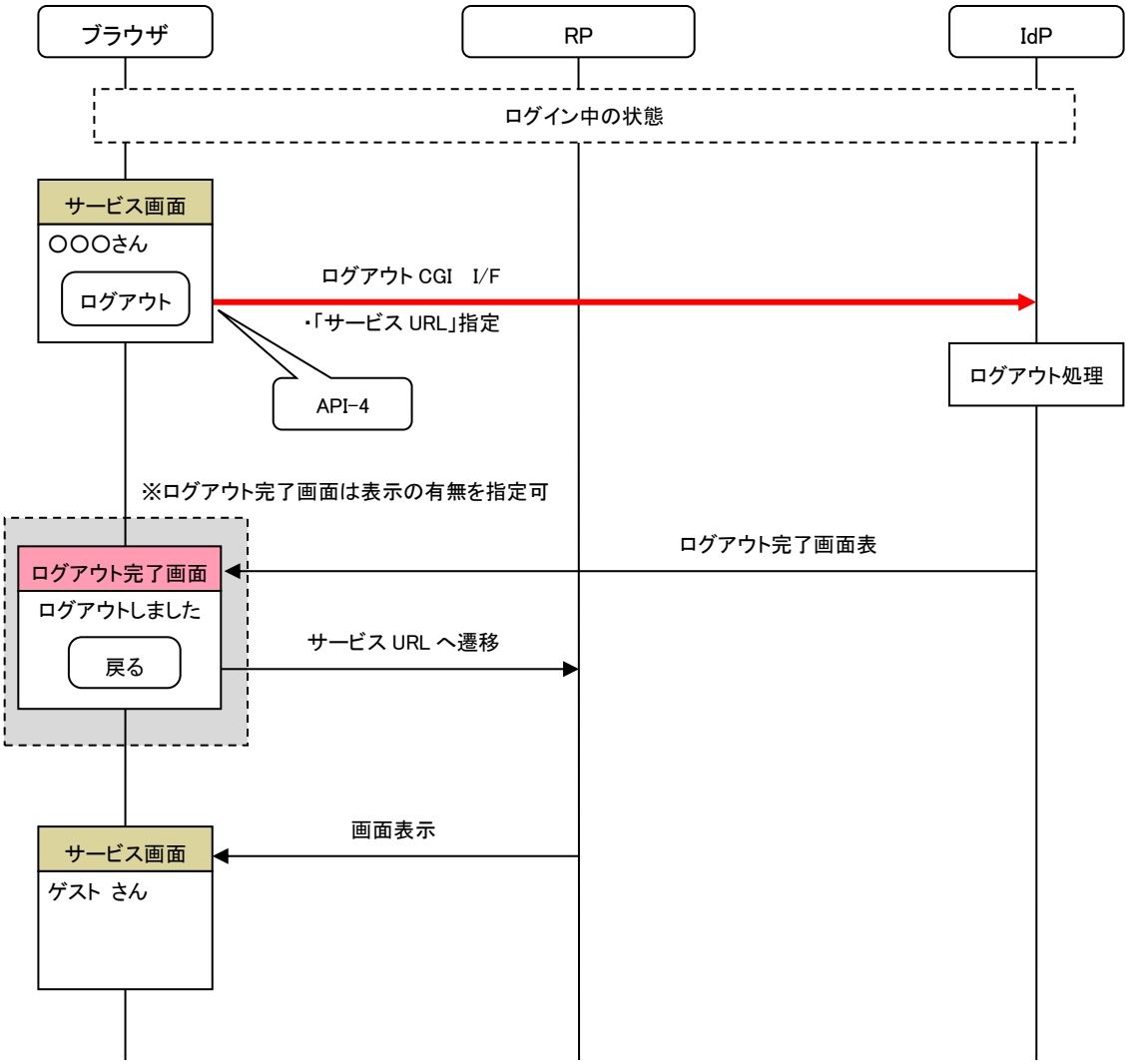


図 4.2-2 ログアウトの基本シーケンス

4.3 インタフェース一覧 LIST INTERFACE

dアカウント・コネクトが提供するインタフェースの一覧を「表 4.3-1 インタフェース一覧」に示します。

List interface
表 4.3-1 インタフェース一覧

API番号 mã số API	API名 tên API	概要 khái quát	URL
API-1-1	Authentication Request （認証要求）	お客様の認証、およびスコープで指定した情報に対する認可の要求を行います。 tiến hành request xác thực cho thông tin đã chỉ định bằng scope và xác thực user.	https://id.smt.docomo.ne.jp/cgi8/oidc/authorize ※i-mode時のスキームは「http」、他キャリアのフィーチャーフォン時のスキームは「https」 khi i-mode thì schem là http, lúc khác thì là https.
API-1-2	Authentication Response （認証応答）	Authentication Request（認証要求）に対する応答です。 trả về response của API-1-1 お客様による認可が行われたことを「認可コード」として返却します。 trả về "code cho phép"	（なし） không có
API-2-1	Token Request （トークン払出要求）	認可コードに対応するトークンの払い出しを要求します。 yêu cầu gọi token đối với "code cho phép"	https://conf.uw.docomo.ne.jp/token
API-2-2	Token Response （トークン払出応答）	Token Request（Token払出要求）に対する応答です。 response của API-2-1 払い出したトークンを返却します。 trả về token đã gọi	（なし） không có
API-3-1	UserInfo Request （利用者情報取得要求）	アクセストークンに紐付く利用者が認可したスコープの情報を要求します。 request thông tin của scope mà user đã cho phép, gắn với token truy cập	https://conf.uw.docomo.ne.jp/userinfo
API-3-2	UserInfo Response （利用者情報取得応答）	UserInfo Request（利用者情報取得要求）に対する応答です。 response của API-3-1 要求されたお客様のスコープの情報を返却します。 trả về thông tin của scope của user đã yêu cầu	（なし） không có
API-4	ログアウトCGI ko cần	IdPからログアウトを行い、指定されたURLに遷移します。 ※iモード端末での利用はできません。	https://id.smt.docomo.ne.jp/cgi8/id/relogin

4.4 インタフェース詳細 chi tiết interface

4.4.1 Authentication Request （認証要求）[API-1-1]

4.4.1.1 動作概要

お客様が設定した情報連携の認可に対する認可コードを取得します。お客様のブラウザを経由したリダイレクトにより、RPから
Get "code cho phép" ứng với xác thực của liên kết thông tin mà user đã chỉ định. Được request từ RP (client) bằng redirect thông qua browser của user.
要求されます。

4.4.1.2 リクエストライン request line

認証要求のリクエストラインについて、「表 4.4-1 認証要求のリクエストライン」に示します。

request line của request authentication
表 4.4-1 認証要求のリクエストライン

No.	ヘッダ名tên header	必須 bắt buộc	概要 khái quát
1	メソッド method	○	メソッドはGET、POSTの受付が可能です。 method thì có thể tiếp nhận GET, POST
2	URL	○	https://id.smt.docomo.ne.jp/cgi8/oidc/authorize ※iモードの場合、スキーマは"http://"となります nếu là i-mode thì schema là https://
3	HTTPバージョン http version	○	HTTP/1.1とします。set là HTTP/1.1

4.4.1.3 ヘッダ部 phần header

認証要求のヘッダ部について、「表 4.4-2 認証要求のヘッダ部」に示します。

phần header của authentication request
表 4.4-2 認証要求のヘッダ部

No.	ヘッダ名tên header	必須 bắt buộc	概要 khái quát
1	Host	○	ホスト名を設定する。setting tên host. ・ リクエストラインまたは、Hostヘッダの少なくともどちらか一方に、有効なホスト名が指定されていること。Phải chỉ định tên host hiệu lực, ít nhất cũng phải có trên request line, host header. ・ 両方とも設定されている場合、一致していること。TH setting ở cả 2 thì phải giống nhau.
2	Content-Type	○	application/x-www-form-urlencoded
3	Content-Length	○	POST時必須。 bắt buộc khi post

4.4.1.4 要求パラメータ parameter request

認証要求のパラメータ詳細について、「表 4.4-3 認証要求のパラメータ詳細」に示します。

表 4.4-3 認証要求のパラメータ詳細

No.	パラメータ名	和名	必須	値	形式	Byte数
1	scope	スコープID	○	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。	半角英数記	1～1000
2	response_type	応答形式	○	code(固定値)	半角英数	4
3	client_id	クライアントID	○	(本システムが払い出したクライアントID)	半角英数記	1～128
4	redirect_uri	応答先URI	○	([RFC3986] (Simple String Comparison) の Section 6.2.1で規定されたURI形式の値)	半角英数記	1～2048
5	state	セキュア文字列 (CSRF/XSRF対策)	○	(Cookieごとに異なる任意のセキュア文字列)	半角英数記	1～60
6	nonce	セキュア文字列 (リプレイアタック対策)	○	(情報連携の一連のセッションごとに異なる任意のセキュア文字列)	半角英数記	1～60
7	prompt	認証・認可動作指定	△	login(固定値) お客様を再認証します。再認証が不可能な場合はエラーを返します。	半角英	5
8	authif	認証I/F種別	△	0:契約者限定で認証 1:ドコモ以外のお客様も認証可能	半角数字	1
9	idauth	ID認証必須フラグ	△	1:IDによる認証を必須	半角数字	1

認証要求のパラメータ設定内容について、「表 4.4-4 認証要求のパラメータ設定内容」に示します。

表 4.4-4 認証要求のパラメータ設定内容

No.	パラメータ名	設定内容	特記事項
1	scope	認証・認可を要求したいScope名称を設定します。scopeにはopenidを含む必要があります。またopenid以外のscope値を含むことができます。	IdP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。
2	response_type	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のみに対応しているため、この値は”code”固定となります。	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。
3	client_id	IdPに登録されているクライアントIDを設定します。	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。
4	redirect_uri	認証・認可の結果を受信するURIを設定します。 このURIは、RPが、情報連携を行うための事前申請時に通知した Redirection URI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。	利用提携時に提示したURIを指定します。
5	state	リクエストとレスポンス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。	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。
6	nonce	ClientセッションとID Tokenを紐づけるランダムな値を設定します。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ます。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。	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。
7	prompt	お客様に対して再認証を要求（別dアカウントでログイン）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。 ※本パラメータを指定した場合はSSO（シングルサインオン）はしません。 ※ドコモ独自仕様としてlogin（別のdアカウントでログイン）のみに対応します。 ※iモード接続の場合は利用できません。	ドコモ独自仕様としてlogin（別dアカウントでログイン）のみに対応します。 none（何も求めない）、consent（再認可）、select_account（アカウント指定認可）は無視されます。 ※prompt=loginのみ対応し、valueに複数指定された場合には、当該パラメータは無視扱いとします。
8	authif	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する。 ※値を省略した場合、「0：契約者限定で認証」として扱う。 ※ドコモの独自パラメータです。	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。
9	idauth	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。 ※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。 ※ドコモの独自パラメータです。	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。

4.4.1.5 電文例 ví dụ

(1) GET時 Khi GET

GET時の例を「サンプルコード 4.4-1 GET時の電文例」に示します。

サンプルコード 4.4-1 GET時の電文例

```
GET /cgi8/oidc/authorize?response_type=code&scope=openid%20suid&client_id=s6BhdRkqt3&state=af0ifjsldkj&redirec
t_uri=https%3A%2F%2Fclient.example.org%2Fcb&nonce=xxxxxxxxxx HTTP/1.1
Host: id.smt.docomo.ne.jp
```

(2) POST時 Khi POST

POST時の例を「サンプルコード 4.4-2 POST時の電文例」に示します。

サンプルコード 4.4-2 POST時の電文例

```
POST /cgi8/oidc/authorize HTTP/1.1
Host: id.smt.docomo.ne.jp
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: xxx

response_type=code&scope=openid%20suid&client_id=s6BhdRkqt3&state=af0ifjsldkj&redirect_uri=https%3A%2F%2Fclient.
example.org%2Fcb&nonce=xxxxxxxxxx
```

4.4.1.6 制限事項 giới hạn

認証要求に独自のパラメータを付与しても、リダイレクトURIには独自パラメータは付与されません。(規定されたパラメータ以外
dù có gán parameter khi authentication request thì trên uri redirect cũng không gán parameter độc lập (ngoài những parameter được quy định thì hủy).
は破棄されます)

4.4.2 Authentication Response （認証応答）[API-1-2]

4.4.2.1 動作概要 khái quát thao tác

Authentication Requestに対する応答を行います。パラメータに認可コードを設定し、要求元にリダイレクトを行います。
tiến hành response đối với authentication request. setting "code cho phép" lên parameter, tiến hành rdirect lên nguồn request.

4.4.2.2 ヘッダ部 phần header

ヘッダはありません。ko có header

4.4.2.3 応答パラメータ parameter response

認証応答のパラメータ詳細について、「表 4.4-5 認証応答のパラメータ詳細」に、パラメータ設定内容について、「表 4.4-6 認証応答のパラメータ設定内容」に示します。

chi tiết parameter response xác thực

表 4.4-5 認証応答のパラメータ詳細

No.	tên parameter パラメータ名	tên tiếng nhật 和名	giá trị 値	hình thức 形式	Byte数(UTF-8)（エスケープ前） số byte trước escape
1	code	認可コード	（任意の文字列）chuỗi tùy ý	半角英数記	1～256
2	error	エラーコード	(%x20-21 / %x23-5B / %x5D-7E 以外の文字を含まない値)giá trị bao gồm kí tự trên（エラーコード参照）tham khảo error code	半角英数記 chữ, số halfsize	ー
3	state	セキュア文字列（CSRF/XSRF対策）	（RPから受け取った値をそのまま返します）trả về nguyên giá trị đã nhận từ RP	半角英数記 chữ, số halfsize	1～60

表 4.4-6 認証応答のパラメータ設定内容 nội dung setting parameter response xác thực

No.	tên parameter パラメータ名	設定内容 nội dung setting	特記事項 mục ghi chú đặc biệt
1	code	お客様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。trả về "code cho phép", chỉ việc đã nhận xác thực từ user. 漏洩のリスクを軽減するため、認可コードは発行されてから短期間で無効となります。để giảm khả năng bị lack, thì sau khi phát hành "code cho phép" thì sẽ vô hiệu hóa trong thời gian ngắn. ※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。Theo quy ước của openID connect thì tối đa sẽ có hiệu lực trong 10 phút. ※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。"code cho phép" gắn với uri redirect và tên định danh client.	RPは2回以上認可コードを使用できません。RP ko thể dùng "code cho phép" từ 2 lần trở lên. もし、認可コードが2回以上使用された場合、IdPはリクエストを拒否して、このnếu mà dùng từ 2 lần trở lên thì ko chấp nhận request, toàn bộ những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。token được phát hành dựa vào "code cho phép" này từ trước đến nay thì vô hiệu hóa chúng đi.
2	error	エラーの内容を示すコードを応答します。response code chỉ ra nội dung lỗi. ASCII [USASCII] エラーコードより1つを設定します。setting 1 cái theo error code ASCII [USASCII]	
3	state	RPから受け取ったstate値をそのまま応答します。response nguyên giá trị state đã nhận từ RP	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。TH parameter state khi request vượt quá size quy định thì không response.

4.4.2.4 エラー lỗi

認証応答のエラーについて、「表 4.4-7 認証応答のエラー」に示します。

表 4.4-7 認証応答のエラー (lỗi response xác thực)

No.	ステータスコード (status code)	エラーコード (error code)	事象 (hiện tượng)	復旧手段 (cách phục hồi)
1	302	invalid_request	リクエストに必須パラメータが含まれていない/サポート外のパラメータが付与されている/同一のパラメータが複数含まれる場合、その他不正な形式である。 (lỗi khi không có parameter bắt buộc khi request/ gán parameter không support/ nhiều parameter giống nhau.)	xác nhận việc request theo spec API trên RP. API仕様に基づいたリクエストであることを、RPにて確認。
2		access_denied	お客様が同意しなかった。 (user không đồng ý) ※同意画面を表示しないため発生しない (không phát sinh do không hiển thị màn hình đồng ý)	
3		invalid_auth	認証情報の不一致を検知した。 (phát hiện thông tin xác thực không đồng nhất)	API仕様に基づいた、リクエストを再送。 (gửi lại request dựa theo spec API)
4		timestamp_refused	認証セッションの有効期限切れを検知した。 (phát hiện hết hạn session xác thực)	API仕様に基づいた、リクエストを再送。 (gửi lại request dựa theo spec API)
5		unsupported_response_type	IdPは現在の方法による認可コード取得をサポートしていない。 (IdP không support việc get "code cho phép" theo cách hiện tại)	API仕様に基づいたリクエストであることを、RPにて確認。 (xác nhận việc request theo spec API trên RP.)
6		invalid_scope	リクエストスコープが不正/未知/もしくはその他の不当な形式である。 (scope request không đúng/chưa biết/ hoặc format những cái khác bị sai)	API仕様に基づいたリクエストであることを、RPにて確認。 (xác nhận việc request theo spec API trên RP.)
7		server_error	IdPがリクエストの処理ができないような予期しない状況に遭遇した。 (gặp phải tình trạng không dự đoán được làm cho IdP ko xử lý request được.) ※500 Internal Server Error のHTTPステータスコードをHTTPのリダイレクトでクライアントに返すことができないため、本エラーコードで応答する。 (do không trả về HTTP status code của 500 internal server error trên client bằng redirect của HTTP được nên response bằng chính error code.)	hỏi lên site quản lý cửa hàng liên kết or docomo@. tiến hành phân tích log ở phía IdP. 加盟店管理者サイトまたはdocomo@に問合せする。 IdP側でログ解析を実施する。
8		request_not_supported	request パラメータをサポートしていない。 (ko support param request)	左記パラメータを除外して、リクエストを再送。 (bỏ param bên trái ra rồi gửi request lại.)
9		request_uri_not_supported	request_uri パラメータをサポートしていない。 (ko support param request_uri)	左記パラメータを除外して、リクエストを再送。 (bỏ param bên trái ra rồi gửi request lại.)
10		registration_not_supported	registration パラメータをサポートしていない。 (ko support param registration)	左記パラメータを除外して、リクエストを再送。 (bỏ param bên trái ra rồi gửi request lại.)
11	400	–	クライアント情報が不正、リダイレクトURIが不正。 (thông tin client ko đúng, redirect_uri ko đúng)	RPには応答されないため検知不可（ブラウザへの表示のみ） (ko biết được do không response lên RP (chỉ hiển thị ở browser)) ※OpenID Connectの規定 (quy định của openID connect)

4.4.2.5 電文例 vd

(1) 正常応答時 khi bình thường

正常応答時の例を「サンプルコード 4.4-3 正常時の電文例」に示します。

サンプルコード 4.4-3 正常時の電文例

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

(2) 準正常応答時 khi bất thường

準正常応答時の例を「サンプルコード 4.4-4 準正常時の電文例」に示します。

サンプルコード 4.4-4 準正常時の電文例

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

4.4.3 Token Request(トークン払出要求)[API-2-1]

4.4.3.1 動作概要 khái quát thao tác

RPから認可コードを受領することで、RPにトークン(IDトークン、アクセストークン)を払い出します。
nhận "code cho phép" từ RP, xuất token lên RP (id token, access token)

4.4.3.2 リクエストライン request line

リクエストラインについて「表 4.4-8 トークン払出要求のリクエストライン」に示します。

表 4.4-8 トークン払出要求のリクエストライン
request line của request token

No.	ヘッダ名 tên header	必須 bắt buộc	概要 khái quát
1	メソッド method	○	メソッドはPOSTのみ受付が可能です。method chỉ có POST
2	URL	○	https://conf.uw.docomo.ne.jp/token
3	HTTPバージョン HTTP version	○	HTTP/1.1とします。

4.4.3.3 ヘッダ部 phần header

ヘッダ部について「表 4.4-9 トークン払出要求のヘッダ部」に示します。

表 4.4-9 トークン払出要求のヘッダ部
phần header request token

No.	ヘッダ名 tên header	必須 bắt buộc	概要 khái quát
1	Host	○	ホスト名を設定する。setting tên host. ・ リクエストラインまたは、Hostヘッダの少なくともどちらか一方に、有効なホスト名が指定されていること。Phải chỉ định tên host hiệu lực, ít nhất cũng phải có trên request line, host header. ・ 両方とも設定されている場合、一致していること。TH setting ở cả 2 thì phải giống nhau.
2	Content-Type	○	application/x-www-form-urlencoded
3	Content-Length	○	POST時必須。bắt buộc khi POST
4	Authorization	○	Basic クレデンシャルを設定する。setting credential Basic. ※本APIでは、Basic認証固定とするため、必須 cần thiết ở API này, do setting cố định basic authentication. ※クライアント申請時に登録したクライアントIDとクライアントシークレットを":"でつなぎ、Base64エンコードした値を付与する。 hình thức: client id (đã đăng kí khi đăng kí client) + ":" + client secret, encode bằng Base64

4.4.3.4 要求パラメータ parameter request

トークン払出要求のパラメータ詳細について「表 4.4-10 トークン払出要求のパラメータ詳細」に示します。

表 4.4-10 トークン払出要求のパラメータ詳細 chi tiết parameter request token

No.	パラメータ名 tên parameter	和名 tên tiếng nhật	必須 bắt buộc	値 giá trị	形式 hình thức	Byte数 số byte
1	grant_type	権限形式	○	authorization_code(固定値) giá trị cố định	半角英数 chữ halfsize	13～18
2	code	認可コード	○	(認可コードの文字列) chuỗi kí tự của "code cho phép"	半角英数記 chữ, số halfsize	1～256
3	redirect_uri	応答先URI	○	([RFC3986] (Simple String Comparison) の Section 6.2.1で規定されたURI形式の値) giá trị của hình thức uri đã quy định ở Section 6.2.1 của cái trong ngoặc đơn á	半角英数記 chữ, số halfsize	1～2048

トークン払出要求のパラメータ設定内容について「表 4.4-11 トークン払出要求のパラメータ設定内容」に示します。

表 4.4-11 トークン払出要求のパラメータ設定内容 nội dung setting parameter của request token

No.	パラメータ名 tên parameter	設定内容 nội dung setting	特記事項 mục gi chú đặc biệt
1	grant_type	トークンを発行するときに使用する権限形式を指定します。 chỉ định hình thức quyền hạn dùng khi phát hành token ※Authorization Code Flowのみに対応しているため、値は"authorization_code"固定となります。 do chỉ dùng để đối ứng authorization code flow nên có giá trị cố định là "authorization_code"	Authorization Code Flowのみ対応のため、"authorization_code"以外が指定された場合、エラーとなります。 nếu giá trị khác "authorization_code" thì lỗi
2	code	IdPから受け取った認可コードを設定します。 setting "code cho phép" get từ IdP.	RPは2回以上認可コードを使用できません。 ko thể dùng "code cho phép" từ 2 lần trở lên. もし、認可コードが2回以上使用された場合、IdP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。 nếu đã dùng từ 2 lần trở lên thì những token được phát hành dựa theo "code cho phép" từ trước tới nay sẽ vô hiệu hoá. IdP sẽ không chấp nhận request.
3	redirect_uri	トークンを受信するURIを設定します。 認証・認可要求時と同じ値でなければなりません。 setting URI nhận token giá trị phải giống với khi request authentication.	認可コードはクライアント利用者識別情報とリダイレクトURIに紐つきます。 "code cho phép" gắn với URI redirect và thông tin định danh user client.

4.4.3.5 電文例 ví dụ

トークン払出要求の電文例を「サンプルコード 4.4-5 トークン払出要求の電文例」に示します。

サンプルコード 4.4-5 トークン払出要求の電文例

```
POST /token HTTP/1.1
Host: conf.uw.docomo.ne.jp
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Content-Length: xxx
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

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

4.4.4 Token Response（トークン払出応答）[API-2-2]

4.4.4.1 動作概要 khái quát thao tác

Token Request（Token払出要求）に対する応答を行います。
tiến hành response đối với token request.
クライアントから指定された認可コードに対応するアクセストークンを払い出します。
xuất access token đối ứng cho "code cho phép" mà client đã chỉ định.

4.4.4.2 ヘッダ部 phần header

トークン払出応答のヘッダ部について「表 4.4-12 トークン払出応答のヘッダ部」に示します。

表 4.4-12 トークン払出応答のヘッダ部

No.	ヘッダ名 tên header	必須 bắt buộc	概要 khái quát
1	Content-Length	○	ボディ部のバイト長を半角数字で設定。setting chiều dài byte của phần body bằng số halfsize.
2	Content-Type	△	application/json
3	Date	○	サーバ処理日付をGMTで設定。 setting ngày tháng xử lý server bằng GMT
4	Pragma	△	「no-cache」固定。 cố định
5	Cache-Control	△	「no-store」固定。cố định
6	WWW-Authenticate	△	httpステータス401応答の場合に設定 setting khi response HTTP status 401 (例)WWW-Authenticate: Bearer realm=″Connect″
7	Connection	○	「close」固定cố định

4.4.4.3 応答パラメータ parameter đối ứng

トークン払出応答のパラメータ詳細について「表 4.4-13 トークン払出応答のパラメータ詳細」に示します。

表 4.4-13 トークン払出応答のパラメータ詳細

No.	パラメータ名	和名	必須		値	形式	Byte数
			正常	準正常			
1	access_token	アクセストークン	○	×	-	半角英数記	1～256
2	token_type	トークン形式	○	×	"Bearer"(固定値)	半角英	6
3	expires_in	トークン有効期間	○	×	-	半角英	ー
4	scope	スコープID	○	×	-	半角英数記	1～1000
5	id_token	IDトークン	○	×	(IdPにIDトークンのClaimsとして規定されているClaimsリスト)	ー	ー
6	error	エラーコード	×	○	(%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	ー

トークン払出応答のパラメータ設定内容について「表 4.4-14 トークン払出応答のパラメータ設定内容」に示します。

表 4.4-14 トークン払出応答のパラメータ設定内容

No.	パラメータ名	設定内容	特記事項
1	access_token	IdPが発行するアクセストークンを応答します。	
2	token_type	トークンのタイプを応答します。本システムでは"Bearer"固定となります。	プロトコルでは値は大文字・小文字を区別しません。
3	expires_in	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 300 であれば、そのアクセストークンは発行から5分後に期限切れとなります。	
4	scope	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は含みません。	
5	id_token	お客様に関連するIDのトークンを応答します。 ※ id_tokenは「署名あり」「暗号化なし」で返却されます。	「5.3.1. IDトークン」を参照してください。
6	error	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。	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。

4.4.4.4 エラー lỗi

トークン払出応答のエラーについて「表 4.4-15 トークン払出応答のエラー」に示します。

lỗi response token

表 4.4-15 トークン払出応答のエラー

No.	ステータスコード status code	エラーコード error code	事象 hiện tượng	復旧手段 cách phục hồi
1	400	invalid_request	リクエスト形式またはパラメータが解析不可能な状態を示す。 chỉ trạng thái không thể phân tích parameter or hình thức request. リクエストに必要なパラメータが含まれていない。 không bao gồm parameter cần cho request. (認証方式(grant type))以外のパラメータについて、サポートされないパラメータ値が含まれている。 về parameter khác grant_type thì lại chứa giá trị param không được support. パラメータが重複している。 param bị trùng lặp or được setting giá trị khác thường. その他、異常値が設定されている。	API仕様に基づいたリクエストであることを、RPにて確認。 xác nhận trên RP việc request dựa theo spec API.
2	401	invalid_client*	クライアント認証に失敗した状態を示す。 chỉ trạng thái đã xác thực client thất bại 利用申請されていないIPアドレスからアクセスされている。 truy cập từ địa chỉ IP không được đăng kí sử dụng. 未知のクライアントである。 client không xác định. クライアント認証情報が含まれていない。 không chứa thông tin xác thực client. サポートされない認証方式が利用されている。 dùng cách xác thực không được support. HTTP Basic認証(RFC2617)に失敗した。 xác thực Basic HTTP (RFC2617) bị thất bại. その他、上記以外の要因により認証に失敗した。 ngoài ra, xác thực thất bại do những nguyên nhân khác.	API仕様に基づいたリクエストであることを、RPにて確認。 xác nhận trên RP việc request dựa theo spec API. 加盟店管理者サイトまたはdocomo@に問合せ、クライアントの設定が妥当か確認する。 hỏi đến site admin của hàng liên kết or docomo@, xác nhận setting của client có đúng không.
3	400	invalid_grant	クライアントが正当な認可を受けていないことを示す。 chỉ việc client không nhận đúng xác thực. 提供された認可を得ていることを示す値(認可コード、エンドユーザを示す値)が不正/有効期限切れ/失効している。 giá trị chỉ việc nhận được xác thực được cung cấp ("code cho nhận", end user) thì không đúng/hết hạn/thất bại. エンドユーザの契約が認可時から更新されている。 Hợp đồng của end user bị update từ khi xác thực. 認可リクエストで用いられたリダイレクトURIとマッチしていない。 không match với redirect uri được dùng ở request authentication. 他のクライアントに対して発行されたものである。 cũng được phát hành cho client khác.	Authentication Requestから再実施 thực hiện lại từ request authentication
4		unsupported_grant_type	クライアントが指定した認証方式(grant type)がサポートされていないことを示す。 chỉ việc không support grant_type mà client đã chỉ định. grant_type に "authorization_code"以外が指定されている。 setting khác "authorization_code" trên grant_type.	API仕様に基づいた、リクエストを再送。 gửi request lại dựa theo spec API
5		invalid_scope	要求されたスコープが不正であることを示す。 chỉ việc scope được request là không đúng. 要求されたスコープが不正/未知/異常である。 scope được request là không đúng/không xác định/bất thường. 要求されたスコープが利用者によって認可された範囲を超えている。 scope được request vượt quá phạm vi được xác thực theo user	Authentication Requestで指定したスコープと、本APIのリクエストスコープが一致しているかをRPにて確認。 xác nhận trên RP xem scope đã chỉ định trên Authentication Request có khớp với scope request của API này không.
6	500	server_error	サーバでエラーが発生。 phát sinh lỗi ở server. 内部矛盾、下位CP通信異常によるエラー発生。 mâu thuẫn nội bộ, lỗi do truyền tin bất thường CP.	加盟店管理者サイトまたはdocomo@に問い合わせしてください。 hãy liên hệ đến admin của hàng liên kết or docomo@

*httpステータス 401応答の場合、エラーコードはヘッダ部のWWW-Authenticateに設定します。

4.4.4.5 電文例 ví dụ

(1) 正常応答時 khi bình thường

正常応答時の電文例を「サンプルコード 4.4-6 正常応答時の電文例」に示します。

id_tokenについては、「署名あり」、「暗号化なし」の例です。
về id_token thì có vd "có chữ kí", "không encode"

vd khi response OK
サンプルコード 4.4-6 正常応答時の電文例

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Date: Mon, 13 Apr 2015 04:26:04 GMT
Cache-Control: no-store
Pragma: no-cache
Connection: close

{
"access_token": "DWMvUUcuZ8IuhkSDURznnArCkQfOt0Pv",
"token_type": "Bearer",
"expires_in": 300,
"scope":"suid",
"id_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE0Mzc1NTA1NjMsImF6cCI6IlJQLVRFU1QwMDEiLC
JzdWIiOiJodHRwczpcL1wvaS5teWRvY29tby5jb21cL2lkXC8xMjM0NTY3ODkwYWJjZGVmZ2hpamtsbW5cLzIwMTVcLzA
3XC8yMn4xNS4zNi4wMyIsIm5vbmNlIjoicmVxdWVzdF9ub25jZSIsImF1ZCI6IlJQLVRFU1QwMDEiLCJpc3MiOiJodHRwczp
cL1wvY29uZi51dy5kb2NvbW8ubmUuanBcLyIsImlhdCI6MTQzNzU0Njk2M30.MgcM35JpVRKZyJnIprcTfMGqqmaUapZ7Bl
vQrVYNVh"
}
```

(2)　準正常応答時 khi bất thường

準正常応答時の電文例を「サンプルコード 4.4-7 準正常応答時の電文例①」、「サンプルコード 4.4-8 準正常応答時の電文例②」に示します。

vd 1 khi response bất thường

サンプルコード 4.4-7 準正常応答時の電文例①

```
HTTP/1.1 400 Bad Request
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Date: Mon, 13 Apr 2015 04:26:04 GMT
Connection: close

{
  "error":"invalid_request"
}
```

vd 2 khi response bất thường

サンプルコード 4.4-8 準正常応答時の電文例②

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="Connect", error="invalid_client"
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Cache-Control: no-store
Pragma: no-cache
Connection: close
```

4.4.5 UserInfo Request（利用者情報取得要求）[API-3-1]

4.4.5.1 動作概要 khái quát thao tác

アクセストークンに紐付く利用者が認可したスコープの情報を要求します。
request thông tin scope mà user đã xác thực gắn với access token.
取得する情報がない場合、本要求の省略が可能です。
TH không có thông tin get được thì có thể bỏ request này.

4.4.5.2 リクエストライン request line

利用者情報取得要求のリクエストラインについて「表 4.4-16 利用者情報取得要求のリクエストライン」に示します。

request line của request user info
表 4.4-16 利用者情報取得要求のリクエストライン

No.	ヘッダ名 tên header	必須 bắt buộc	概要 khái quát
1	メソッド method	○	メソッドはGET、POSTの受付が可能です。GET, POST đều được ※OpenID Connect Coreの規定に従い、GETでの要求を推奨する。Tuân theo quy định của OpenID Connect Core, khuyến khích request bằng GET
2	URL	○	https://conf.uw.docomo.ne.jp/userinfo
3	HTTPバージョン HTTP version	○	HTTP/1.1とします。

4.4.5.3 ヘッダ部 phần header

利用者情報取得要求のヘッダ部について「表 4.4-17 利用者情報取得要求のヘッダ部」に示します。

phần header của request user info
表 4.4-17 利用者情報取得要求のヘッダ部

No.	ヘッダ名 tên header	必須 bắt buộc	概要 khái quát
1	Host	○	ホスト名を設定する。setting tên host ・ リクエストラインまたは、Hostヘッダの少なくともどちらか一方に、有効なホスト名が指定されていること。ít nhất phải setting tên host hiệu lực trên 1 trong 2 là request line or host header. ・ 両方とも設定されている場合、一致していること。nếu setting trên cả 2 thì phải thống nhất.
2	Content-Type	○	application/x-www-form-urlencoded
3	Content-Length	○	POST時必須。bắt buộc khi POST
4	Authorization	○	Bearer Tokenを設定する。setting Bearer Token. Tokenの値は、Token Responseで得たAccess Tokenの値を設定する。 giá trị của token thì setting giá trị của Access Token đã có trên Token response

4.4.5.4 要求パラメータ param request

要求パラメータはありません。ko có param request

4.4.5.5 電文例 ví dụ

利用者情報取得要求の電文例を「サンプルコード 4.4-9 利用者情報取得要求の電文例」に示します。

ví dụ của request user info
サンプルコード 4.4-9 利用者情報取得要求の電文例

```
GET /userinfo HTTP/1.1
Host: conf.uw.docomo.ne.jp
Authorization: Bearer DWMvUUcuZ8IuhkSDURznnArCkQfOt0Pv
```

4.4.6 UserInfo Response （利用者情報取得応答）[API-3-2]

4.4.6.1 動作概要 khái quát thao tác

UserInfo Request （利用者情報取得要求）に対する応答です。要求された利用者のスコープの情報を返却します。
response của UserInfo Request. Trả về thông tin của scope của user đã request.

4.4.6.2 ヘッダ部 phần header.

利用者情報取得応答のヘッダ部について「表 4.4-18 利用者情報取得応答のヘッダ部」に示します。

表 4.4-18 利用者情報取得応答のヘッダ部

項番	ヘッダ名 (tên header)	必須 (bắt buộc)	概要 khái quát
1	Content-Length	○	ボディ部のバイト長を半角数字で設定。setting chiều dài byte của phần body bằng số halfsize.
2	Content-Type	△	application/json
3	Date	○	サーバ処理日付をGMTで設定。setting ngày tháng năm xử lý server bằng GMT
4	Pragma	△	「no-cache」固定。 cố định
5	Cache-Control	△	「no-store」固定。 cố định
6	WWW-Authenticate	△	httpステータス400、401、403応答の場合に設定します。setting trong trường hợp trả về HTTP status code 400, 401, 403 (例)WWW-Authenticate: Bearer realm=″Connect″
7	Connection	○	「close」固定 cố định

4.4.6.3 応答パラメータ param response

利用者情報取得応答のパラメータ詳細について「表 4.4-19 利用者情報取得応答のパラメータ詳細」に示します。

表 4.4-19 利用者情報取得応答のパラメータ詳細
chi tiết param

No.	パラメータ名 (tên param)	和名 (tên tiếng nhật)	必須 (bắt buộc)		値 (giá trị)	形式 (hình thức)	Byte数 (số byte)
			正常 (bình thường)	準正常 (bất thường)			
1	(認可されたScopeに紐付くClaims)	-	○	×	(Claimの値) giá trị của Claim	ー	ー
2	error (claims gắn với scope được xác thực)	エラーコード	×	△	(%x20-21 / %x23-5B / %x5D-7E 以外の文字を含まない値) giá trị chỉ chứa những kí tự trên (エラーコード参照) tham khảo error code	半角英数記 chữ, số, kí hiệu halfsize	ー

利用者情報取得応答のパラメータ設定内容について「表 4.4-20 利用者情報取得応答のパラメータ設定内容」に示します。

表 4.4-20 利用者情報取得応答のパラメータ設定内容
nội dung setting param

No.	パラメータ名	設定内容	特記事項
1	(認可されたScopeに紐付くClaims) Claims gắn với Scope được xác thực	認可されたScopeに紐付くClaimを応答します。 response Claims gắn với Scope được xác thực. JWT、またはJSON形式で応答します。 response ở hình thức JWT or JSON	-
2	error	エラーの内容を示すコードを応答します。 response code chỉ ra nội dung lỗi. ASCII [USASCII] エラーコードより1つを設定します。 setting 1 cái theo error code ASCII [USASCII] (注)httpステータス400、401、403応答の場合はヘッダ部のWWW-Authenticateに設定します。 (Chú ý) TH trả về http status là 400, 401, 403 thì setting lên WWW-Authenticate của phần header.	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。 TH response header WWW-Authenticate thì gán lên WWW-Authenticate như là attribute, không response phần body. (注)httpステータス400、401、403応答の場合 (chú ý) TH trả về http status 400, 401, 403

(1) Claim取得の仕様 spec của get Claim

Claimが取得できないときは、項目名と値の両方とも返却しません。値なし、空白、nullなどでの返却はしません。
Khi không get được Claim thì không trả về cả tên item và giá trị luôn. Không trả về chẳng hạn hạn không có giá trị, rỗng, null.

4.4.6.4 エラー Lỗi

利用者情報取得応答のエラーについて「表 4.4-21 利用者情報取得応答のエラー」に示します。

表 4.4-21 利用者情報取得応答のエラー

No.	ステータスコード	エラーコード	事象	復旧手段
1	400	invalid_request*	リクエスト形式またはパラメータが解析不可能な状態を示します。 chỉ trạng thái không thể phân tích param or hình thức request	API仕様に基づいたリクエストであることを、RPにて確認してください。 xác nhận trên RP việc request dựa theo spec API.
2	401	invalid_token*	提供されたアクセストークンが無効です。 acccess token đã cung cấp bị vô hiệu	Authentication Requestから再実施してください。 thực hiện lại Authentication Request.
3		invalid_client*	クライアント認証に失敗した状態を示します。 chỉ việc xác thực client thất bại	API仕様に基づいたリクエストであることを、RPにて確認してください。 xác nhận trên RP việc request dựa theo spec API. 加盟店管理者サイトまたはdocomo@に問合せ、RPの設定が妥当か確認してください。 liên hệ đến site admin cửa hàng liên kết or docomo@, xác nhận setting của RP có tương ứng không.
4	403	insufficient_scope*	リクエストにはアクセストークンにより提供されるよりも高い権限が必要です。 khi request thì cần quyền cao hơn quyền được cung cấp theo access token.	Authentication Requestから再実施してください。 thực hiện lại Authentication Request.
5	500	server_error	サーバでエラーが発生しました。 phát sinh lỗi ở server	加盟店管理者サイトまたはdocomo@に問合せてください。 liên hệ đến site admin cửa hàng liên kết or docomo@,

*httpステータス 400、401、403応答の場合、エラーコードはヘッダ部のWWW-Authenticateに設定します。
なお、エラーコードが"invalid_client"の場合、RFC6750に則りエラー情報は応答しないため、error="invalid_client"は設定しません。

4.4.6.5 電文例 ví dụ

(1) 正常応答(JSONで応答)時 khi bình thường

正常応答(JSONで応答)時の電文例を「サンプルコード 4.4-10 正常応答(JSONで応答)時の電文例」に示します。

サンプルコード 4.4-10 正常応答(JSONで応答)時の電文例

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Date: Mon, 13 Apr 2015 04:26:04 GMT
Cache-Control: no-store
Pragma: no-cache
Connection: close

{
  "sub": "https://i.mydocomo.com/id/xxxxxxxxxxxxxxxxxxxx",
  "suid": "9999Abc9EFghIJK9LmnOpqr9s99TU"
}
```

(2)　準正常応答時 khi bất thường

準正常応答時の電文例を「サンプルコード 4.4-11 準正常応答時の電文例①」、「サンプルコード 4.4-12 準正常応答時の電文例②」に示します。

ví dụ 1

サンプルコード 4.4-11 準正常応答時の電文例①

```
HTTP/1.1 500 Internal Server Error
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Date: Mon, 13 Apr 2015 04:26:04 GMT
Connection: close

{
  "error":"server_error"
}
```

ví dụ 2

サンプルコード 4.4-12 準正常応答時の電文例②

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Bearer realm="Connect", error="invalid_token"
Content-Type: application/json;charset=UTF-8
Content-Length: xxx
Cache-Control: no-store
Pragma: no-cache
Connection: close
```

4.4.7 ログアウトCGI [API-4] logout, không làm, ko cần dịch

4.4.7.1 動作概要

IdPからログアウトを行い、指定されたURLに遷移します。ログアウト実行後に、ログアウト完了画面を表示する/表示しないの指定をすることが可能です。

- ログアウトCGIはiモード端末での利用はできません。

4.4.7.2 リクエストライン

ログアウトCGIのリクエストラインについて「表 4.4-22 ログアウトCGIのリクエストライン」に示します。

表 4.4-22 ログアウトCGIのリクエストライン

No.	ヘッダ名	必須	概要
1	メソッド	○	メソッドはGET、POSTの受付が可能。
2	URL	○	https://id.smt.docomo.ne.jp/cgi8/id/relogin
3	HTTPバージョン	○	HTTP/1.1

4.4.7.3 要求パラメータ

ログアウトCGIの要求パラメータの一覧を「表 4.4-23 ログアウトCGIのパラメーター覧」に示します。

表 4.4-23 ログアウトCGIのパラメーター覧

No.	パラメータ名		必須	概要
1	serviceurl	サービスURL	△	ログアウト後に遷移するサービスのURL
2	rbody	遷移先Body情報	△	ログアウト後のサービスへPOSTで遷移する際に付与するボディ部情報
3	linkname	リンク文字列	△	ログアウト完了画面の「サービスへ遷移」ボタンに表示するラベル文字列
4	message	任意メッセージ	△	ログアウト完了画面に表示するメッセージの文字列
5	dispflg	画面表示有無	△	ログアウト完了画面の表示有無の指定

(1) serviceurl(サービスURL)

サービスURLのパラメータ詳細について「表 4.4-24 サービスURLのパラメータ詳細」に示します。

表 4.4-24 サービスURLのパラメータ詳細

項目	詳細
パラメータ値	ログアウト後に遷移するサービスのURL。 パラメータ付きのURLも指定可能。 本パラメータ全体をURLエンコードして設定する。 ※URLエンコード方法は「4.4.7.5(1)URLエンコード方法」を参照。
パラメータ値のチェック条件	①スキームが"http://" または "https://"であること。 ②サービスURLのドメインが、申請されているリダイレクトURIのドメインと一致すること。 ※URLエンコード後のサイズが1900バイトを超えた場合は、1900バイト(泣き別れ文字は削除)でURLを切って使用する。
パラメータエラー時の動作	①パラメータが取得できなかった場合 画面表示有無フラグ指定が「表示」の場合 ログアウト画面に遷移する 画面表示有無フラグ指定が「非表示」の場合 パラメータエラー画面に遷移する ②パラメータ値のチェック条件でNGとなった場合 画面表示有無フラグ指定が「表示」の場合 ログアウト画面に遷移する 画面表示有無フラグ指定が「非表示」の場合 ホワイトリストエラー画面に遷移する ※サービスURLが実在しないURL(404エラーとなるURLなど)であったとしても、妥当性チェックは行わず、動作保証しない。

(2) rbody(遷移先Body情報)

遷移先Body情報のパラメータ詳細について「表 4.4-25 遷移先Body情報のパラメータ詳細」に示します。

表 4.4-25 遷移先Body情報のパラメータ詳細

項目	詳細
パラメータ値	ログアウト後のサービスへPOSTで遷移する際に付与するボディ部情報。 ※ログアウト後のサービスへGETで遷移する場合は、本パラメータの指定は不要(GETの場合はserviceurlにパラメータ付与のこと)
パラメータ値のチェック条件	※URLエンコード後のサイズが10240バイトを超えた場合は、使用しない。(取得できなかったものとする) ※「rbody=」も許容する。 ※以下の形式でない場合は、使用しない(取得できなかったものとする)。 各パラメータがName=Value形式で記述されていること。 各パラメータの結合部は"&"で記述されていること。
パラメータエラー時の動作	①パラメータを取得できなかった場合 サービスURLがある場合、遷移先にGETで遷移させる様動作する。 ②パラメータ値のチェック条件でNGとなった場合 パラメータ内容を破棄する(取得できなかったものとする)。

(3) linkname(リンク文字列)

リンク文字列のパラメータ詳細について「表 4.4-26 リンク文字列のパラメータ詳細」に示します。

表 4.4-26 リンク文字列のパラメータ詳細

項目	詳細
パラメータ値	ログアウト完了画面の「サービスへ遷移」ボタンに表示するラベル文字列
パラメータ値のチェック条件	バイト数: 60bytes以下であること 文字種: 全角半角すべて(端末に合わせた文字コードで設定する) 他キャリアFP向け画面の場合「SJIS」 スマートフォン、パソコン向け画面の場合「UTF-8」
パラメータエラー時の動作	①パラメータを取得できなかった場合 ログアウト完了画面の「サービスへ遷移」ボタンのラベルに文字列の埋め込みを行わない。 ②パラメータ値のチェック条件でNGとなった場合 パラメータ内容を破棄する(取得できなかったものとする)。

(4) message(任意メッセージ)

任意メッセージのパラメータ詳細について「表 4.4-27 任意メッセージのパラメータ詳細」に示します。

表 4.4-27 任意メッセージのパラメータ詳細

項目	詳細
パラメータ値	ログアウト完了画面に表示するメッセージの文字列
パラメータ値のチェック条件	バイト数: 450bytes以下であること 文字種: 全角半角すべて(端末に合わせた文字コードで設定する) 他キャリアFP向け画面の場合「SJIS」 スマートフォン、パソコン向け画面の場合「UTF-8」
パラメータエラー時の動作	①パラメータを取得できなかった場合 ログアウト完了画面に任意メッセージの埋め込みを行わない。 ②パラメータ値のチェック条件でNGとなった場合 パラメータ内容を破棄する(取得できなかったものとする)。

(5) dispflg(画面表示有無)

画面表示有無のパラメータ詳細について「表 4.4-28 画面表示有無のパラメータ詳細」に示します。

表 4.4-28 画面表示有無のパラメータ詳細

項目	詳細
パラメータ値	ログアウト完了画面の表示有無を指定する '0':表示しない '1':表示する ※パラメータを省略した場合は「'1':表示」として扱う。
パラメータ値のチェック条件	バイト数: 1bytes 文字種: 半角数字 値が'0'または'1'であること
パラメータエラー時の動作	①パラメータを取得できなかった場合 ログアウト完了画面の表示有無を「'1':表示」として扱う。 ②パラメータ値のチェック条件でNGとなった場合 パラメータエラー画面を返却する。

4.4.7.4　電文例

ログアウトCGIの電文例を「サンプルコード 4.4-13 ログアウトCGIの電文例」に示します。

サンプルコード 4.4-13 ログアウトCGIの電文例

```
https://id.smt.docomo.ne.jp/cgi8/id/relogin?serviceurl=http%3A%2F%2Fsmt%2Edocomo%2Ene%2Ejp%2Fportal%2Fsuppor
t%2Fsrc%2Fsupport%5Findex%2Ehtml%3Fd%5Fand%5Fhead&rbody=a%3D1%26b%3D2&linkname=%E3%83%AA%E3%83%B3%E
3%82%AF&message=%E3%83%A1%E3%83%83%E3%82%BB%E3%83%BC%E3%82%B8%E3%81%A7%E3%81%99&dispflg=1
```

4.4.7.5　補足事項　mục bổ sung

(1)　URLエンコード方法 cách encode url

パラメータ付きのURLをリクエストパラメータに付与する方法について説明します。
gaiir thích cách gán url có param lên param request

- <form></form>タグ内の<input type="hidden">タグにて「URLパラメータ」を指定する場合は【手順①】を行い、パラメータ部がエンコードされたものを「value」として指定してください。
  trên tag <input type = "hidden"> của tag <form></form> có chỉ định param url thì tiến hành "quy trình 1", lấy phần param đã encode làm value.
- <a>タグに指定するURLのクエリ部に「URLパラメータ」を指定する場合は【手順①】および【手順②】を行い、パラメータ部が2重エンコードされたものを「value」として指定してください。
  nếu chỉ định param url trên phần query của url chỉ định trên tag <a> thì tiến hành "quy trình 1" và "quy trình 2", lấy phần param đã encode 2 lần làm value.

quy trình 1. encode url phần giá trị param gắn trên url của param url.
【手順①】「URLパラメータ」のURLに付加するパラメータの値の部分をURLエンコードする。

表 4.4-29 【手順①】URLエンコード例

状態 trạng thái	内容 nội dung
エンコード前 trước	http://aaaa.bb.ccc/xxx/yy/zzzz?para1=ぱら1&para2=ぱら2
エンコード後 sau	http://aaaa.bb.ccc/xxx/yy/zzzz?para1=%82%CF%82%E7%82P&para2=%82%CF%82%E7%82Q

quy trình 2: encode url toàn bộ
【手順②】更に全体をURLエンコードする。

表 4.4-30 【手順②】URLエンコード例

状態 trạng thái	内容 nội dung
エンコード前 trước	http://aaaa.bb.ccc/xxx/yy/zzzz?para1=%82%CF%82%E7%82P&para2=%82%CF%82%E7%82Q
エンコード後 sau	http%3A%2F%2Faaaa.bb.ccc%2Fxxx%2Fyy%2Fzzzz%3Fpara1%3D%2582%25CF%2582%25E7%2582P%26para2%3D%2582%25CF%2582%25E7%2582Q

5. データ

dアカウント・コネクトにて、IdPから取得できるデータについて説明します。

データの一覧を「表 5-1　IdPから取得できるデーター覧」に示します。

表 5-1　IdPから取得できるデーター覧

No.	分類	データ名	概要
1	認可結果	認可コード	お客様が認可を受けたことを示す。 トークンを取得するために利用する。
2	利用者識別情報	OpenId	お客様を一意に識別するためのIDで、 Open ID Connectの仕様として必須で払い出される。 全てのお客様に払い出されるため、基本的に本IDでお客様の識別を行います。
3	トークン	IDトークン	OpenIdを含むIDのトークン。
4		アクセストークン	提供データを取得するためのトークン。
5	提供データ	（「5.4. 提供データ」参照）	（「5.4. 提供データ」参照）

5.1　認可結果

お客様による認可結果を表すデータです。

5.1.1　認可コード

5.1.1.1　詳細

お客様が認可した情報に紐づく一意のコードです。認可コードでは直接、お客様情報が取得できないことから、お客様情報を取得するトークンを払い出します。漏洩のリスクを軽減するため、認可コードは発行されてから短期間で無効となります。取得後は速やかに利用してください。

5.1.1.2　ライフサイクル

認可コードのライフサイクルについて「表 5.1-1　認可コードのライフサイクル」に示します。

表 5.1-1　認可コードのライフサイクル

No.	ライフサイクル	概要
1	生成	お客様が認可をした時
2	更新	なし
3	削除	一定期間を経過したとき（無効化されます）

5.1.1.3　制限事項

認可コードは2回以上使用できません。もし、認可コードが2回以上使用された場合、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が無効化されます。

5.2 利用者識別情報

認証・認可を行ったお客様を識別するために利用するデータです。

5.2.1 OpenId

5.2.1.1 詳細

IdPがRPに提供する、お客様を一意に識別するための利用者識別情報です。OpenIdは、IDトークン内、および提供データの両方に設定されます。ドコモのお客様かどうか、各種契約があるかどうか、などの条件に関係なく、全てのお客様に払い出されるため、基本的に本利用者識別情報でお客様の識別を行います。以下のOpenID仕様の形式で払い出します。

【形式】URL形式（以下）のユニークな値

- https://i.mydocomo.com/id/[お客様固有値]

  [お客様固有値]:半角英数をランダムに組み合わせたユニークな値

5.2.1.2 ライフサイクル

OpenIdのライフサイクルについて「表 5.2-1OpenIdのライフサイクル」に示します。

表 5.2-1OpenIdのライフサイクル

No.	ライフサイクル	概要
1	生成	①ドコモのお客様の場合、ドコモの回線契約をした時 ②ドコモのお客様が名義変更した時 ③ドコモ以外のお客様の場合、dアカウントを発行、および再発行した時
2	更新	なし
3	削除	①ドコモのお客様の場合、ドコモの回線を解約後、dアカウントを廃止した時 ②ドコモ以外のお客様の場合、dアカウントを廃止した時

5.2.1.3 制限事項

同一のお客様でも、RPサイトが異なると別のIDが払い出されます(RPサイトのレルム(realm)の値が異なると別のIDとなります）。複数のサービスで同じopenidを利用する場合は、同じレルム(realm)の値で申請してください。レルムの詳細について「5.5レルム」を参照してください。

5.3 トークン

OpenID Connectの仕様で規定されたデータです。

5.3.1 IDトークン

5.3.1.1 詳細

OpenIdを含むIDのトークンをIDトークン（以下、「IDトークン」）といいます。トークン取得要求にて認可コードを指定することにより、認可したお客様のIDトークンを取得します。IDトークンには複数の項目（発行日時、有効期限、利用者識別情報、など）があり、OpenIdは「sub（利用者識別情報）」に設定されます。

【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形式はピリオド"."で区切られた①JWTヘッダ、②JWTクレームセット、③JWS(JSON Web Signature)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。

- エンコード方式の「Base64URL」は「Base64」とは異なるエンコード方式であるため、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ください。

詳細を「サンプルコード 5.3-1 ID Token を含む Token Response（JWS）（例）」「サンプルコード 5.3-2 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（例）」「図 5.3-1 JWS署名検証（例）」、設定の詳細を「表 5.3-1 設定の詳細」、「表 5.3-2 設定の内容」に示します。

サンプルコード 5.3-1 ID Token を含む Token Response（JWS）（例）

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

 {
   "access_token": "SIAV32hkKG",
   "token_type": "Bearer",
   "expires_in": 3600,
   "id_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ewogImlzcyI6I
     CJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5Nz
     YxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
     fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5
     NzAKfQ.rJctcmxCVhBpsTsM-siK_U2KI8FUB4N6eyjy3T2RIVE"
 }
```

①JWT ヘッダ

②JWT クレームセット

③JWS 署名

サンプルコード 5.3-2 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（例）

```
{
   "iss": "http://server.example.com",
   "sub": "248289761001",
   "aud": "s6BhdRkqt3",
   "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970,
   "iat": 1311280970
 }
```

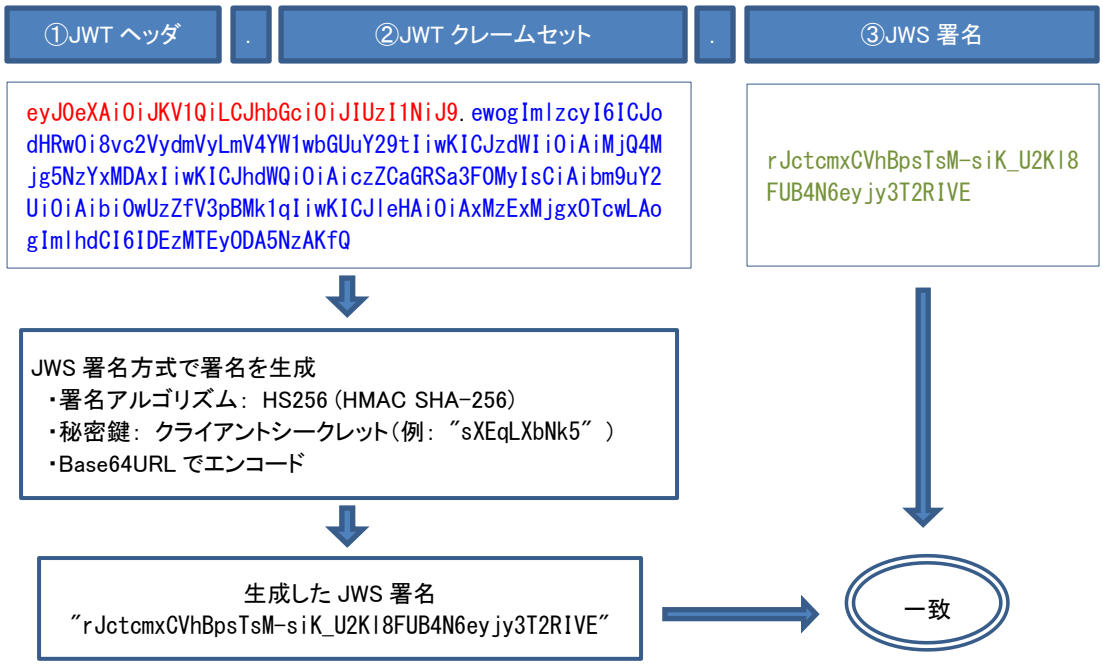


図 5.3-1 JWS署名検証（例）

表 5.3-1 設定の詳細

No.	物理名	論理名	値のとりうる範囲	形式	Byte数(UTF-8) (エスケープ前)
1	iss	発行者識別情報			
2	sub	利用者識別情報 (Open ID)	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。		
3	aud	連携先識別情報	大文字と小文字を区別する文字列です。		
4	exp	IDトークン有効期間	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	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	nonce	セキュア文字列 (リプレイアタック対策)	(リクエストされたままの値を設定します。)		
7	azp				

表 5.3-2 設定の内容

No.	物理名	論理名	説明	特記事項
1	iss	発行者識別情報	レスポンス発行者の識別情報。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	利用者識別情報(Open ID)	Subject 識別情報。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情報です。	
3	aud	連携先識別情報	クライアントIDを設定します。	※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。	
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。	
6	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。	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。
7	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。	

5.3.1.2 ライフサイクル

IDトークンのライフサイクルについて「表 5.3-3 IDトークンのライフサイクル」に示します。

表 5.3-3 IDトークンのライフサイクル

No.	ライフサイクル	概要
1	生成	お客様が認可を行った時。
2	更新	なし
3	削除	一定期間を経過した時（無効化されます）。

5.3.1.3 制限事項

IDトークンとIDトークンの署名（JWS署名）の仕様について「表 5.3-4 IDトークンの仕様」に示します。

表 5.3-4 IDトークンの仕様

項目	仕様		備考
IDトークン	「署名あり」、「暗号化なし」で通知		システム要件上、暗号化が必須の場合はご相談ください
IDトークンの署名（JWS署名）	署名アルゴリズム	HS256（HMAC SHA-256）	システム要件上、署名アルゴリズムがRS256必須の場合はご相談ください
	秘密鍵	クライアントシークレットの値	-

5.3.2 アクセストークン

5.3.2.1 詳細

お客様の提供情報を取得するためのトークンをアクセストークン（以下、「アクセストークン」）といいます。

トークン取得要求にて認可コードを指定することにより、認可したユーザのアクセストークンを取得します。

5.3.2.2 ライフサイクル

アクセストークンのライフサイクルについて「表 5.3-5 アクセストークンのライフサイクル」に示します。

表 5.3-5 アクセストークンのライフサイクル

No.	ライフサイクル	概要	備考
1	生成	お客様が認可を行った時	
2	更新	なし	
3	削除	一定期間を経過した時（無効化されます）	有効期間は5分 （ドコモの都合で変更する場合があります）

5.3.2.3 制限事項

アクセストークンはお客様ごとに最新の1つのみが有効となります。異なるスコープで認可した場合はアクセストークンが上書きされ、それまでのアクセストークンは無効になります。

5.4 提供データ

お客様の個人情報をRPに提供するデータについて説明します。

5.4.1 クレーム

5.4.1.1 利用者識別情報

ドコモで管理しているお客様を識別するための情報を利用者識別情報（以下、「利用者識別情報」）といいます。

(1) 詳細

利用者識別情報の詳細データー覧について「表 5.4-1 利用者識別情報の詳細データー覧」に示します。

表 5.4-1 利用者識別情報の詳細データー覧

クレーム名	クレーム名（日本語）	データ型(byte)	値の取り得る範囲
sub	OpenId	URL形式(256)	https://i.mydocomo.com/id/[お客様固有値] [お客様固有値]:半角英数をランダムに組み合わせたユニークな値

(2) 制限事項

なし

5.4.1.2 提供情報

サービスごとに提供情報が異なります。

5.4.2 スコープ

各クレームはスコープの単位で取得できます。

利用できるスコープの詳細を「表 5.4-2 スコープ詳細」に示します。

表 5.4-2 スコープ詳細

スコープ名	クレーム名	クレーム名（日本語）	データ型（byte）	値の取り得る範囲
openid	sub	OpenId	URL形式(256)	https://i.mydocomo.com/id/[お客様固有値] [お客様固有値]:半角英数をランダムに組み合わせたユニークな値
suid	SUID	SUID	半角英数(29)	ランダムの文字列
guid	GUID	GUID	半角英数(7)	ランダムの文字列
sbscrbsts_n	sbscrbsts	回線契約種別	半角数(1)	0：回線未契約 1：回線契約中
sbscrbsts2	sbscrbsts2	回線契約種別2	半角数(1)	0：iモード契約 1：spモード契約 2：重畳契約 3：i/spモード契約以外 4：docomo契約以外
CXIch	CXIch	iチャネル契約状態(xモード)	半角数(1)	0：契約なし 1：契約あり 9：公開不可
CXIco	CXIco	iコンシェル契約状態(xモード)	半角数(1)	0：契約なし 1：契約あり 2：お試し（初期設定完了） ※お試しの場合で、初期設定未完了であれば「契約なし」 9：公開不可

利用用途を「表 5.4-3 スコープ利用用途」に示します。サービスごとに利用できるスコープが異なります。

表 5.4-3 スコープ利用用途

スコープ名	クレーム名	利用用途	サービス別利用可否	
			spモード コンテンツ決済	d払い/ドコモ払い
openid	sub	回線契約や各種サービス契約の有無にかかわらず、すべてのお客様を個別に識別するために利用します。	利用可能	利用可能
suid	SUID	spモード契約をしているお客様にサービスを提供する場合に、お客様の識別をするために利用します。	利用可能	条件付き 利用可能*
guid	GUID	iモード契約をしているお客様にサービスを提供する場合に、お客様の識別をするために利用します。	利用可能	利用可能
sbscrbsts_n	sbscrbsts	お客様がドコモの契約者かどうかを取得する場合に利用します。	利用可能	利用可能
sbscrbsts2	sbscrbsts2	お客様がドコモの契約者かどうか、およびISP契約の種別（お客様がドコモ契約者の場合）を取得する場合に利用します。	利用可能	利用可能
CXIch	CXIch	お客様のspモード用iチャネル契約状態を取得するために利用します。	利用可能	×
CXIco	CXIco	お客様のspモード用iコンシェル契約状態を取得するために利用します。	利用可能	×

＊ dメニューのメニューリストにサイトを掲載するspモードコンテンツ決済契約加盟店のみ利用可能です。

5.5 レルム

OpenID Connectの仕様ではレルムは利用しませんが、ドコモの独自仕様としてopenid識別子の生成に利用しています。レルムは、同一の認証ポリシーを適用するURLの範囲を指定するため、同一のレルムをもつサービス間ではopenid識別子が同一となります。通常はセキュリティを考慮してサービス毎に異なるレルムを指定します。ただし、以下に該当する場合は、対応するレルムの指定が必要となります。

5.5.1 認証方式を「docomo ログイン」から「dアカウント・コネクト」に移行

すでにOpenID認証 2.0プロトコルの「docomo ログイン」を利用したサービスを提供し、openidをユーザ識別子として利用している場合、OpenID認証 2.0プロトコルで指定していたレルムを指定してください。

- レルムが異なると、同一のお客様でも異なるopenid識別子の値となり、別のお客様と認識されるため、お客様の移行ができません。

5.5.2 複数サービスを提供、お客様を同一のopenid識別子で管理

複数のサービスを提供し、サービスを利用する同一のお客様を同一のopenid識別子で管理する場合は、代表サービスのレルムなど全サービスで同じレルムを指定してください。

- dアカウント・コネクトでは、サービス提供者が管理するドメイン配下のレルム値であれば、必ずしもサービスURLに一致するレルムを指定する必要はありません。

5.5.3 ログインは「dアカウント・コネクト」、決済システムは「docomo ログイン」を利用

ログインは「dアカウント・コネクト」、決済システムは「docomo ログイン」を利用する場合、docomo ログインで指定したレルムと同一のレルムを、dアカウント・コネクト側にも指定してください。決済代行事業者の決済システムを利用する場合は「5.5.4」を参照ください。

- ユーザずれ防止のため、決済処理を行う際、ログイン時に取得したopenidと決済前の認証で取得したopenidの値が同一かチェック処理を行うことを推奨します。

5.5.4 ログインは「dアカウント・コネクト」、決済システムは決済代行事業者を利用

認証システムは加盟店で構築し、決済システムは決済代行事業者を利用する場合、dアカウント・コネクトのレルムは認証システムにて利用しているレルムと同一のレルムを指定してください。

- 決済代行事業者を利用する場合は、ユーザずれ防止のチェックはできません。

改版履歴

日付	版数	変更箇所	変更内容
2017年7月7日	第1.0版	–	初版
2018年1月23日	第1.1版	5.4.2	（追記）利用できるスコープに「guid」「sbscrbsts2」「CXIch」「CXIco」を追記。
2018年4月20日	第1.2版	5.2	（追記）利用者識別情報の制限事項を追記。
		5.5	（追記）レルムについての説明を追記。
2018年6月22日	第1.21版	4.1.4.3	（変更）RPに導入が必要なルート証明書を「VeriSign Class 3 Public Primary Certification Authority – G5」→「DigiCert Global Root CA」に変更。
2018年11月14日	第1.22版	全体	（変更）dアカウントのログイン画面にて表示される「ID/パスワード入力画面」を「ID入力画面」、「パスワード入力画面」に変更。
		5.5.4	（変更）認証システムにて利用しているレルムと、dアカウント・コネクトのレルムを同一のレルムに指定する内容に変更。