

Sandboxを利用した OAuth認証付きAPI利用方法

@2020/12/05 医療情報学会課題研究会セミナー

木村映善

愛媛大学医学部医療情報学講座



正確な内容を心がけていますが、間違いがあったら済みません。その場合は煽らずにご指摘頂ければ幸いです。

目的

- HEART WGの紹介
 - CMSが提供しているBlue Button 2.0の開発者向けサイトを用いて疑似演習・理解
 - 認可プロセスを体験
 - OAuthのフロー
 - FHIR Resourceの認可要求
 - 実際の処理
 - PHRにおける認可プロセスの仕様の検討に参加できるようになること
-

情報共有に関する問題意識

- 新患の記録へのアクセス
- かかりつけ医以外での専門医の受診が必要
- 配偶者やadult childと健康データを共有
- 研究機関と医療保健データを共有する
- 代理人や委任状による意志決定
- 緊急時のアクセス
- データ公開範囲の制限



情報へのアクセス認可を制御



- 何の情報を
- どのように
- いつ
- だれに



患者が主役

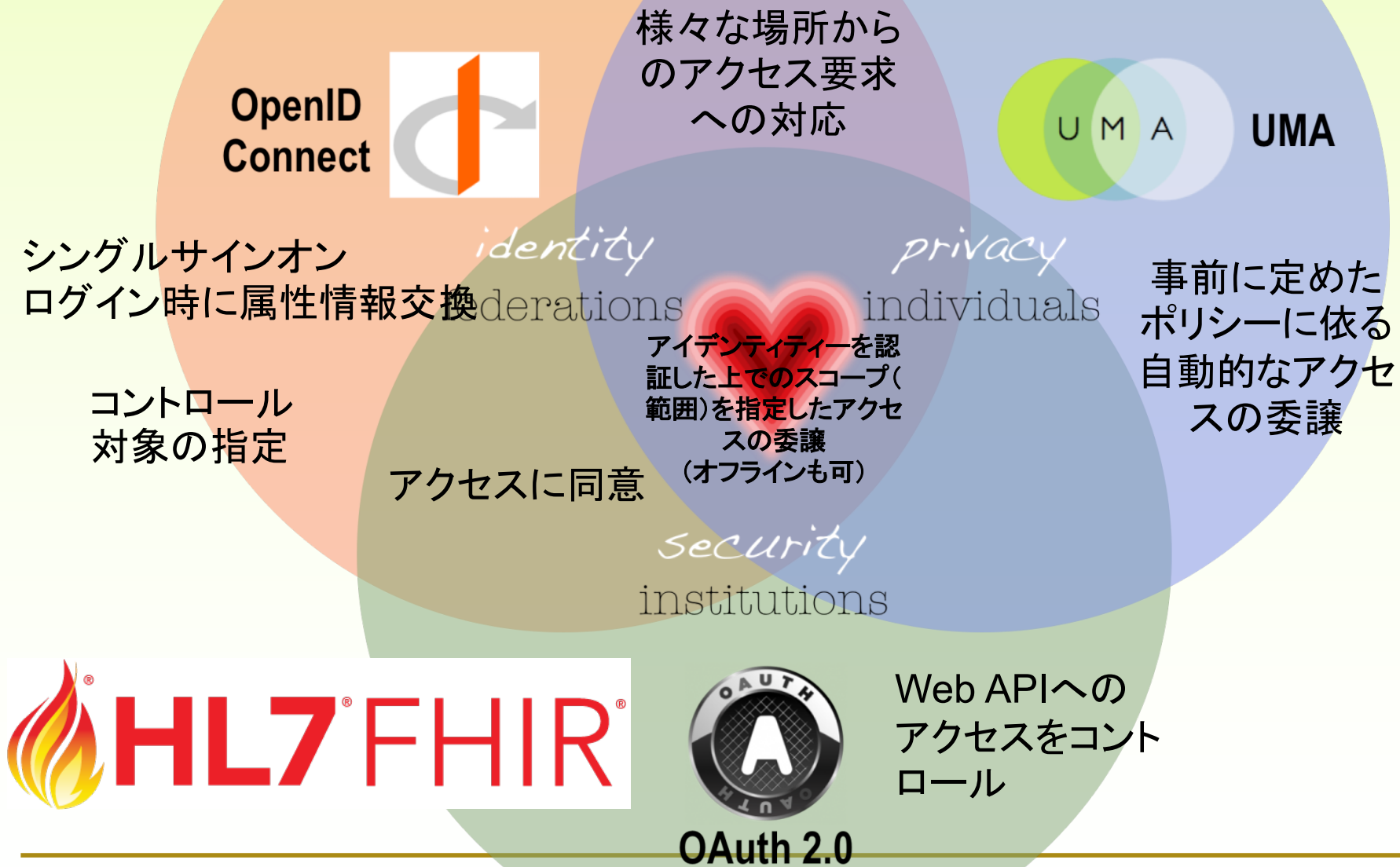
認可に関するプロファイルが必要

- FHIRの規格自体はOAuthを認可手段として推奨。どう使うかは細かく定めていない。
 - OAuthの使い方はバリエーションがある。ステークホルダーで合意しておかないと計画なしのOAuth採用が相互運用性を損なう可能性がある。
 - かかりつけ医、地域医療連携、PHR、調剤薬局、eコマース、etc…
-

医療分野向けに OpenID Connectのプロファイル

要配慮個人情報を含む医療情報交換のために、Open ID Connectの様々なユースケースの中でもセキュリティが高い方法（ベストプラクティス）を採用

HEART (Health Relationship Trust) Profile



What is the HEART WG? <https://openid.net/wg/heart/>

<http://www.findthomas.net/blog/2012/03/10/uma-openid-connect-oauth2-0/> を元に構成

OAuth



リソース所有者



認可サーバ

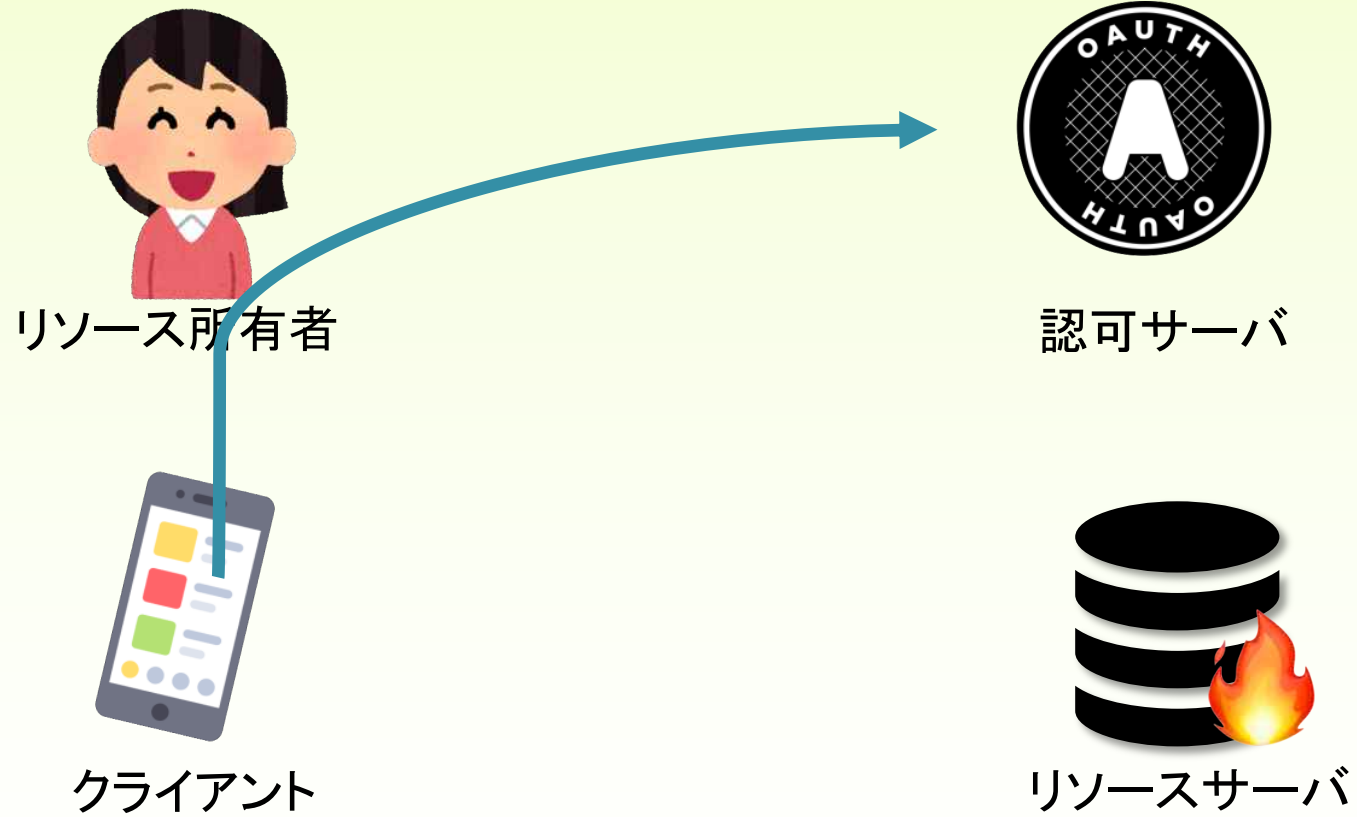


クライアント

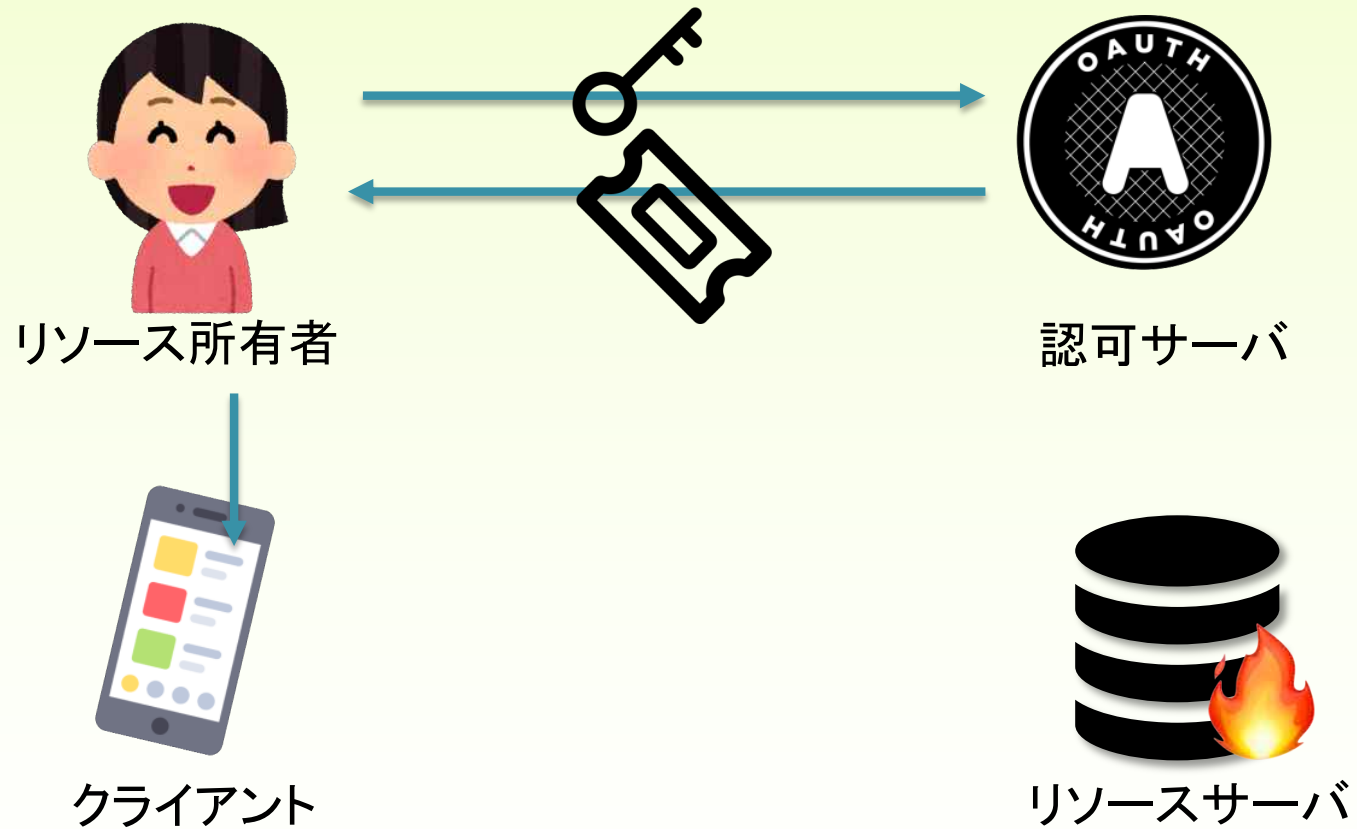


リソースサーバ

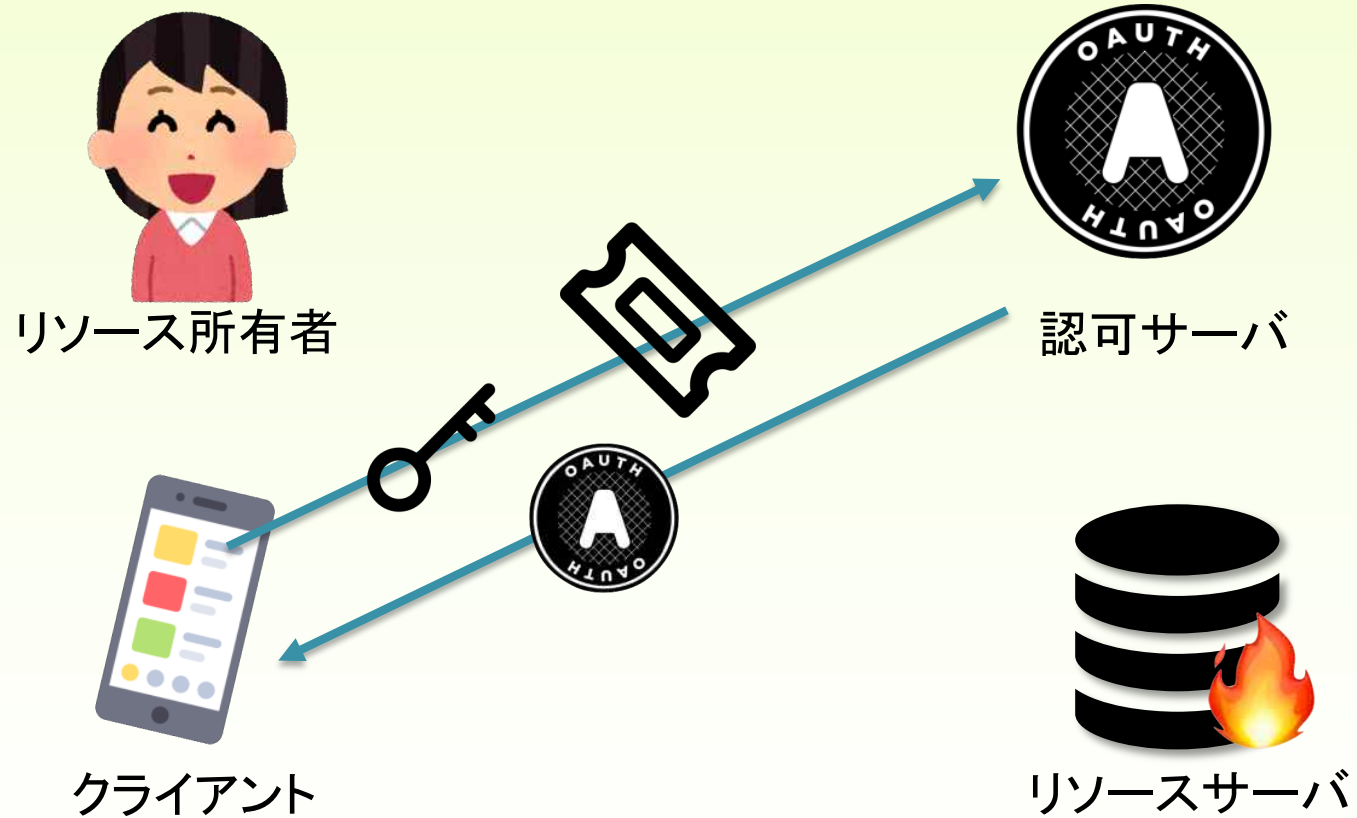
OAuth



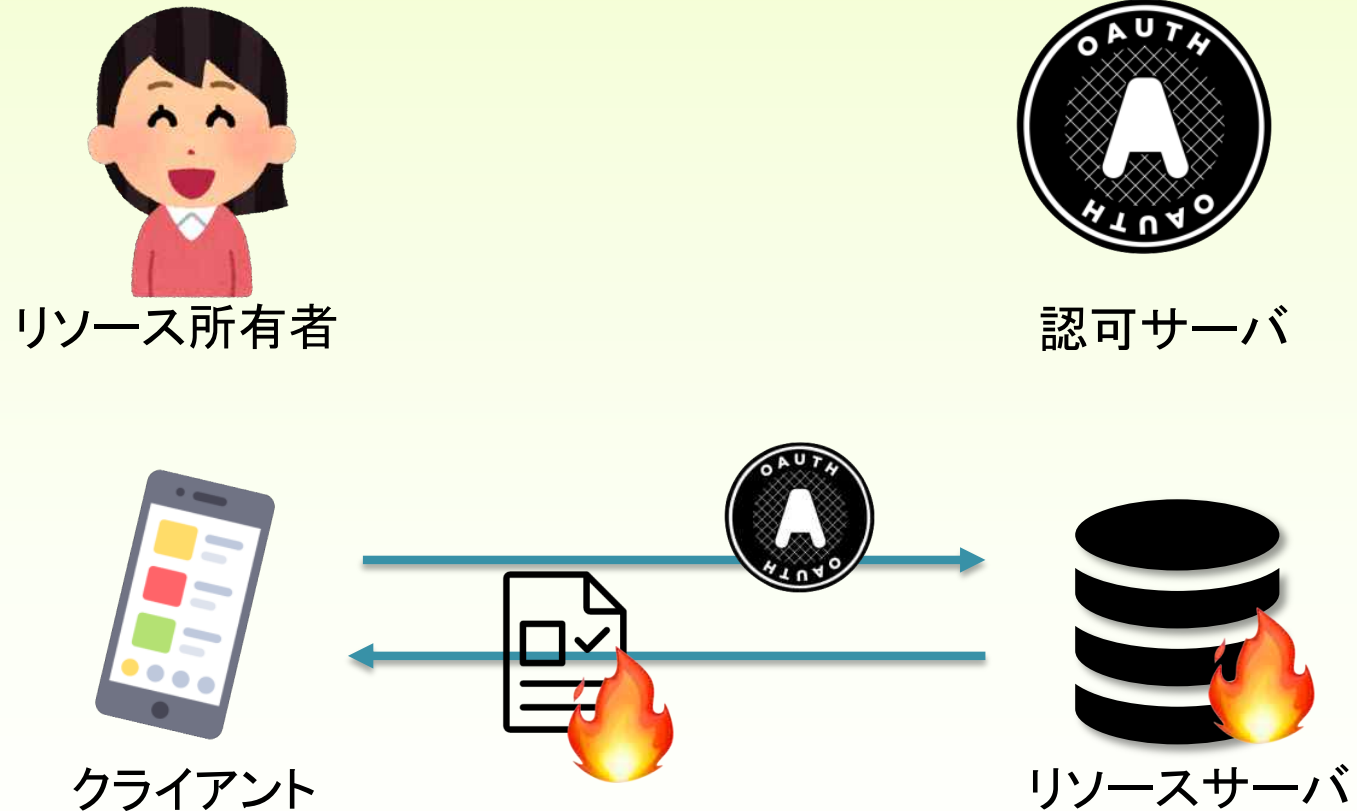
OAuth



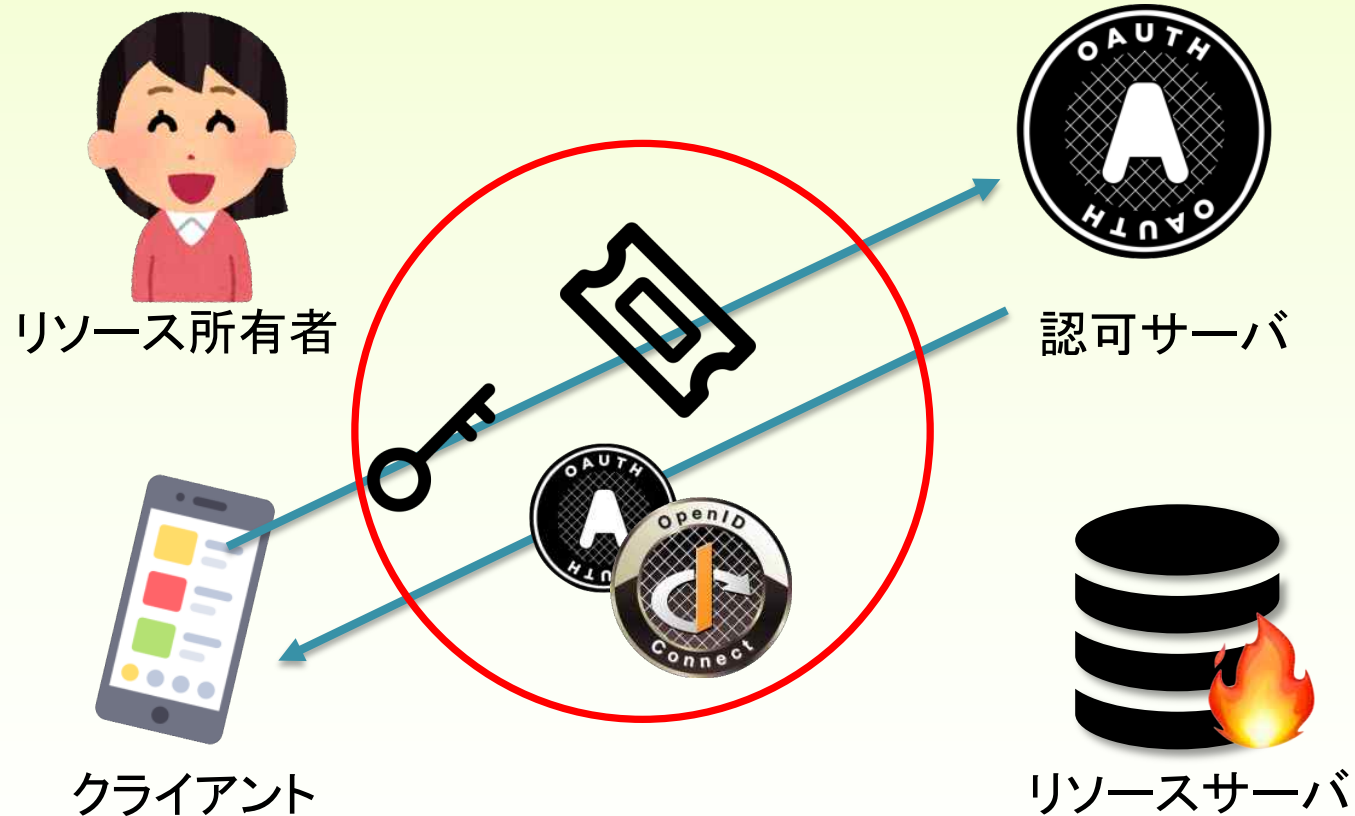
OAuth



OAuth



OAuthと Open ID Connect



OAuthは本人まわりのみ



リソース所有者



クライアント



認可サーバ



リソースサーバ

医療のユースケース



リソース所有者
(患者)



クライアント



認可サーバ



リソースサーバ



医師



パソコン

User-Managed Access (UMA) の考え方



医療のユースケース



リソース所有者
(患者)



認可サーバ



医師



クライアント

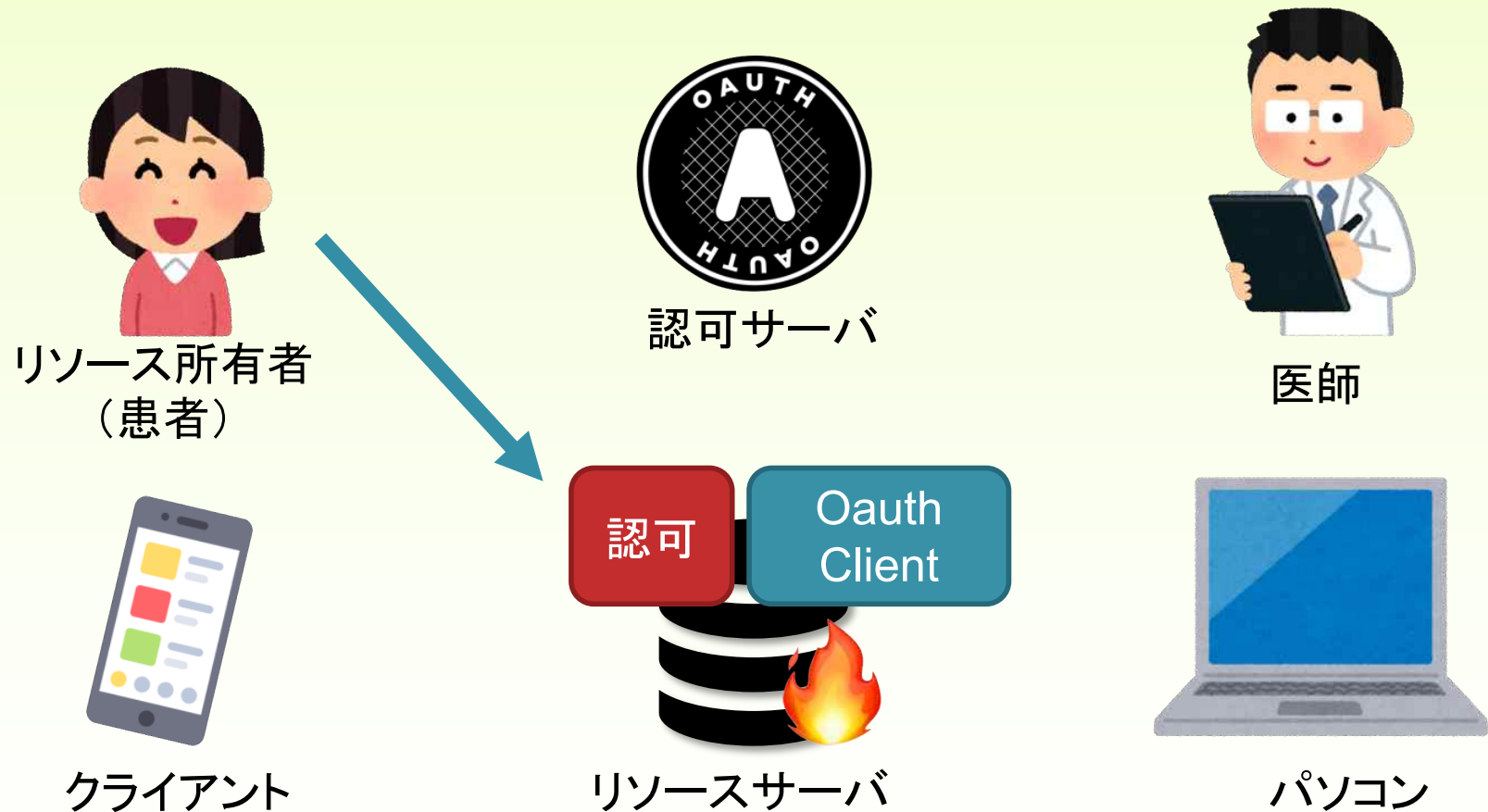


リソースサーバ



パソコン

医療のユースケース



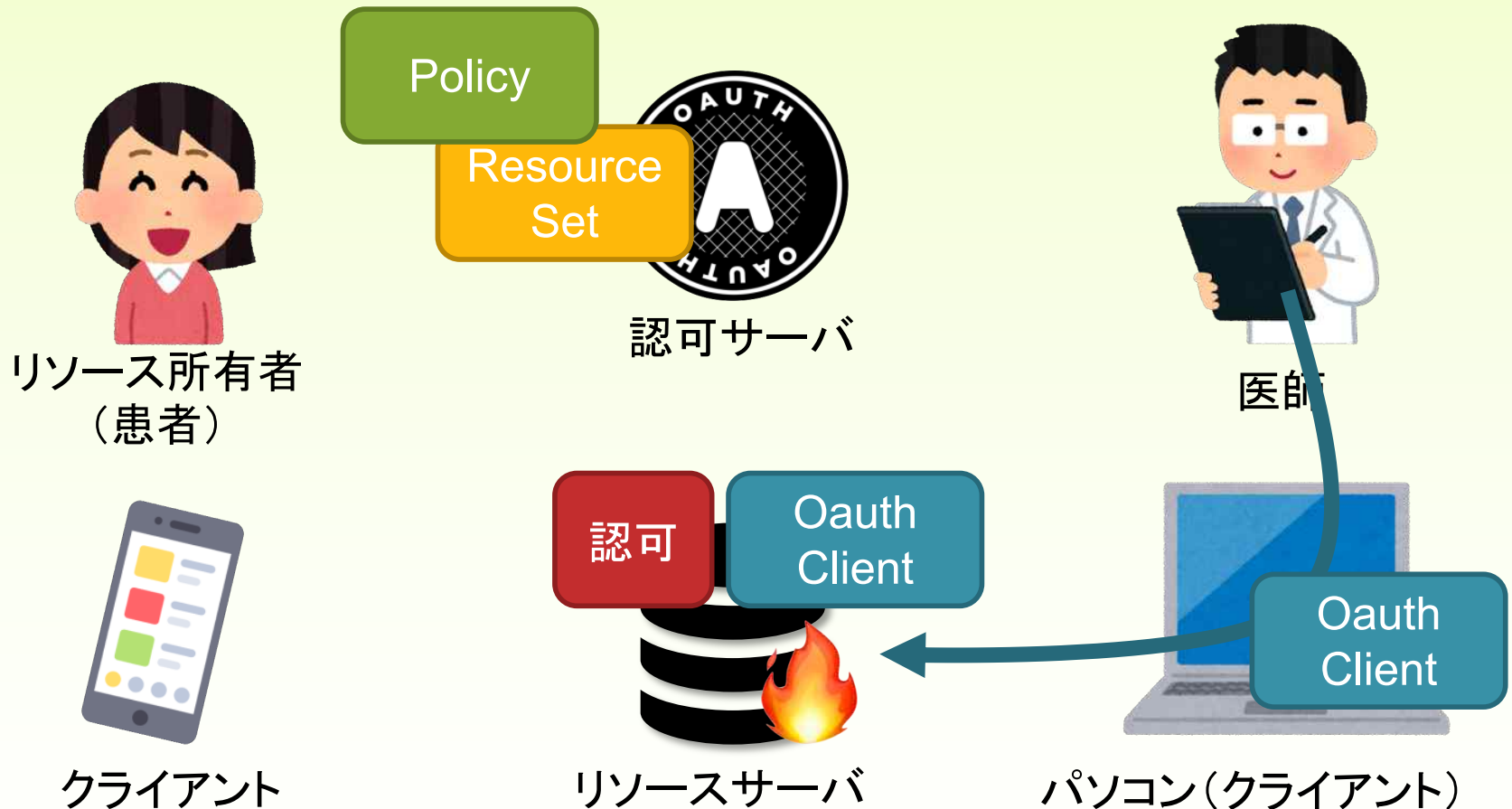
医療のユースケース



医療のユースケース



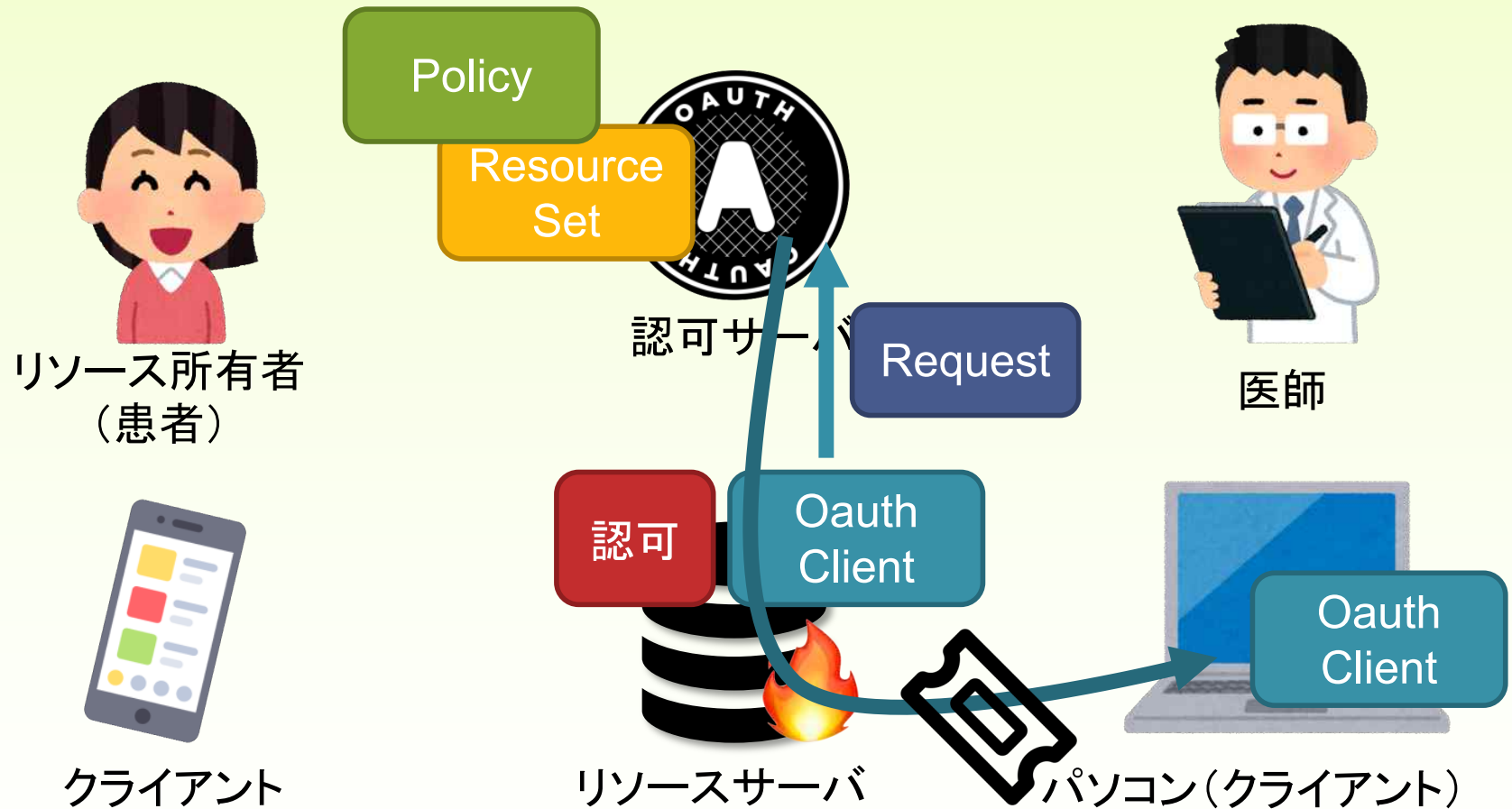
医療のユースケース



医療のユースケース



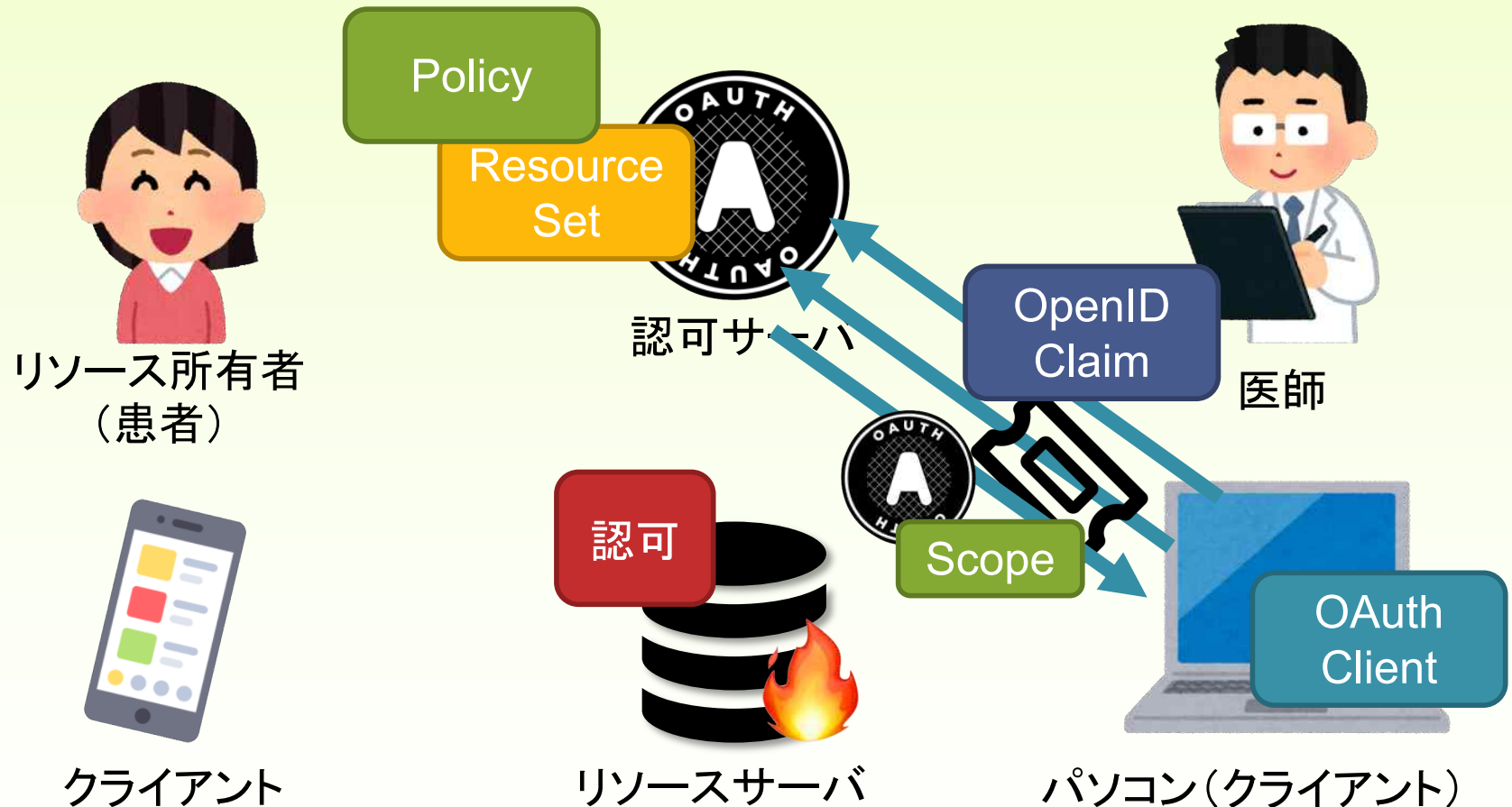
医療のユースケース



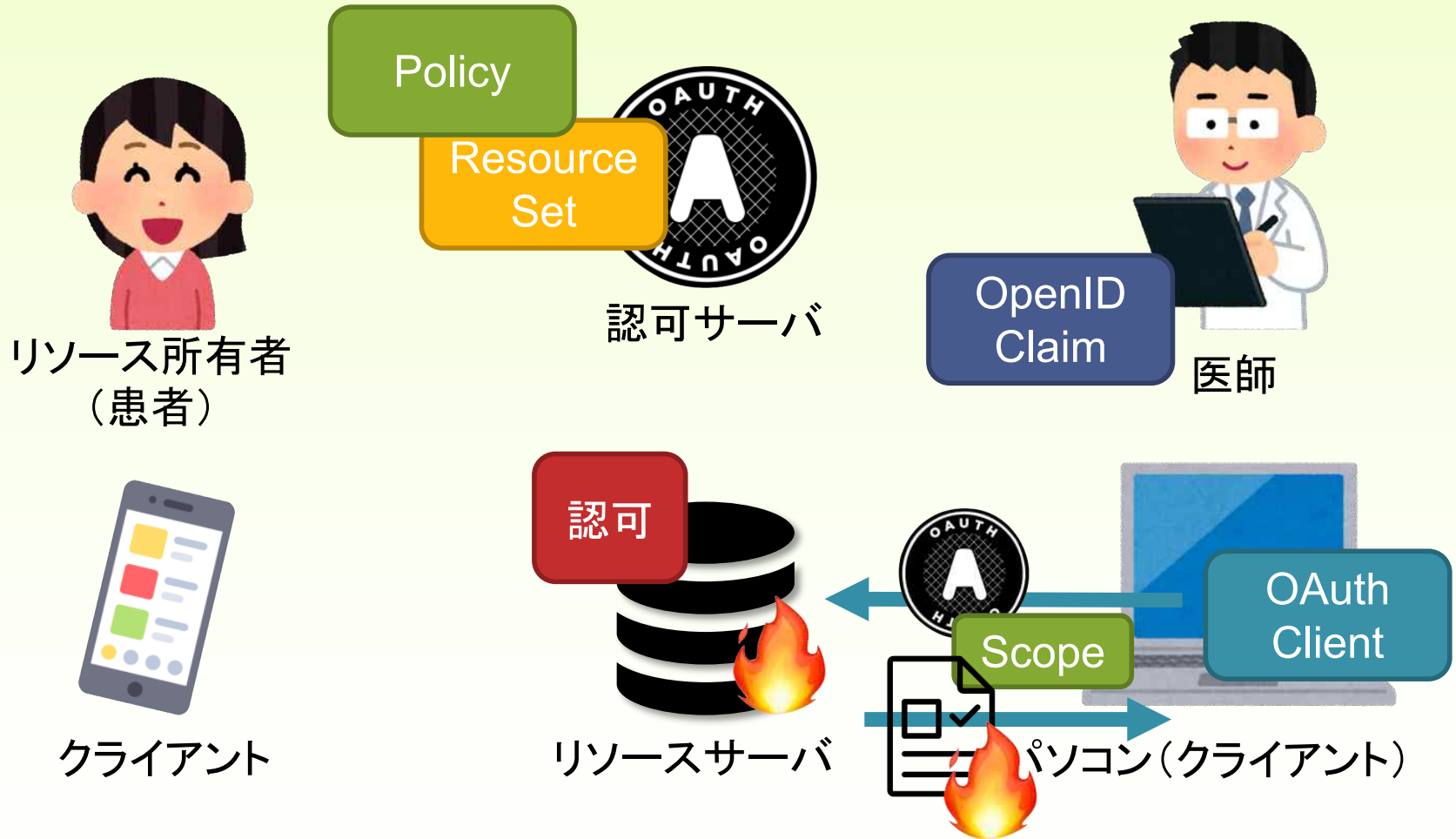
医療のユースケース



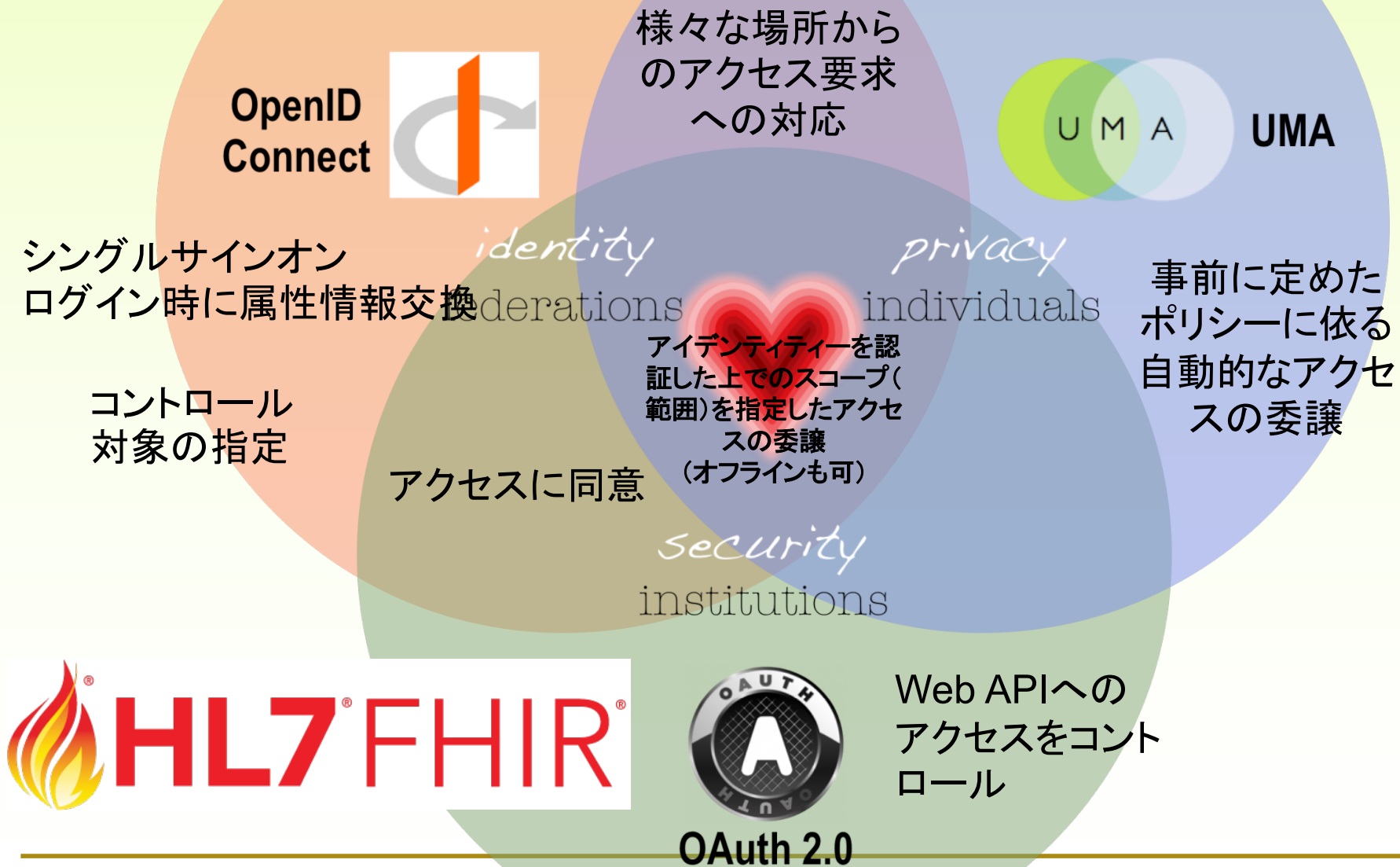
医療のユースケース



医療のユースケース



HEART (Health Relationship Trust) Profile



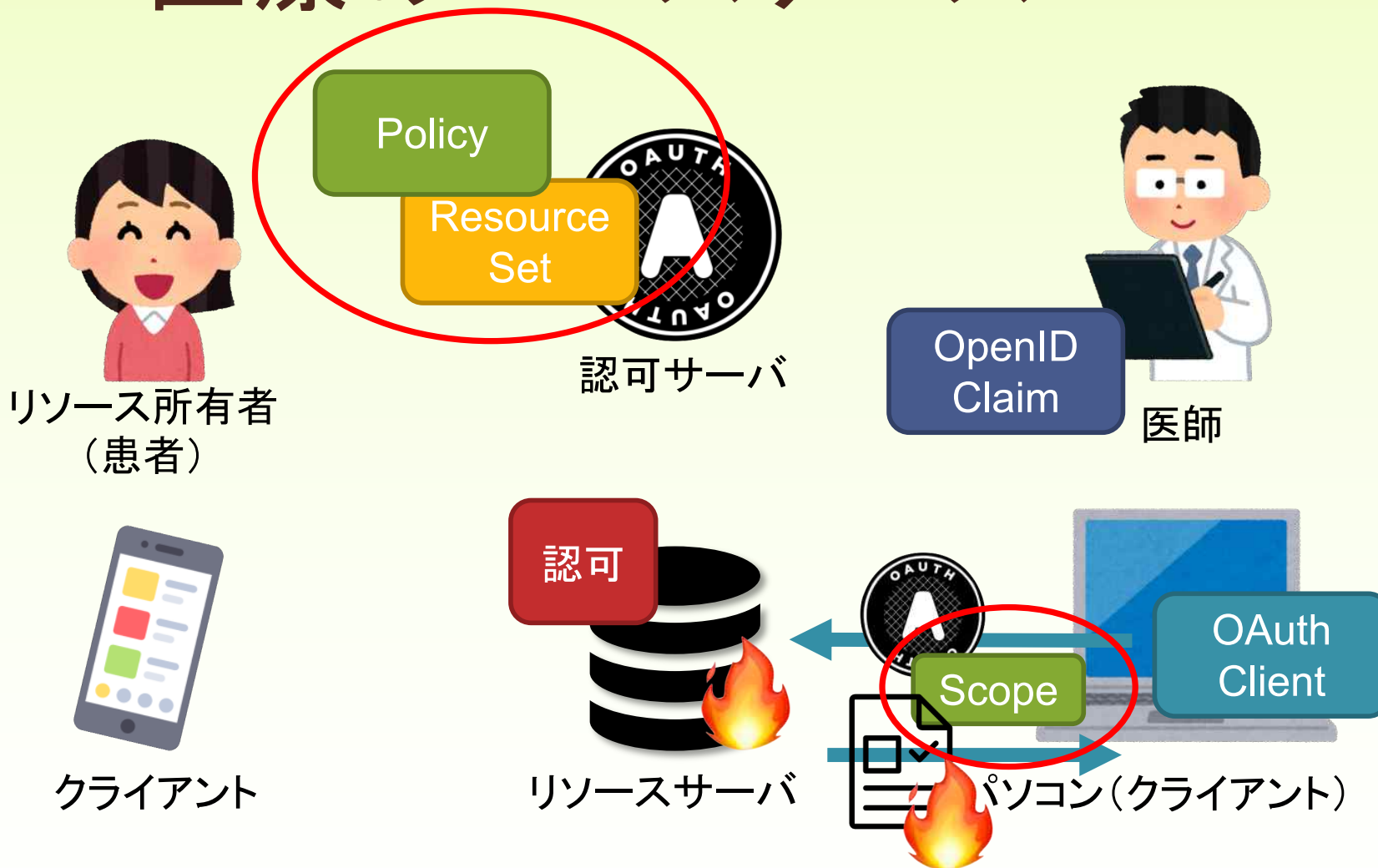
What is the HEART WG? <https://openid.net/wg/heart/>

<http://www.findthomas.net/blog/2012/03/10/uma-openid-connect-oauth2-0/> を元に構成

HEART

- OAuth, Open ID Connect、UMAに関して医療分野向けプロファイルを作成
 - 任意要素を必須に
 - 既存の拡張ポイントを利用した拡張
- HEARTの構成
 - メカニクス（仕組み）
 - HEART OAuth Profile
 - HEART OpenID Connect Profile
 - HEART UMA Profile
 - セマンティクス（意味）
 - HEART OAuth Profile for FHIR
 - HEART UMA Profile for FHIR

医療のユースケース



Health Relationship Trust Profile for Fast Healthcare Interoperability Resources (FHIR) UMA 2 Resources openid-heart-fhir-uma-2_0

Table of Contents

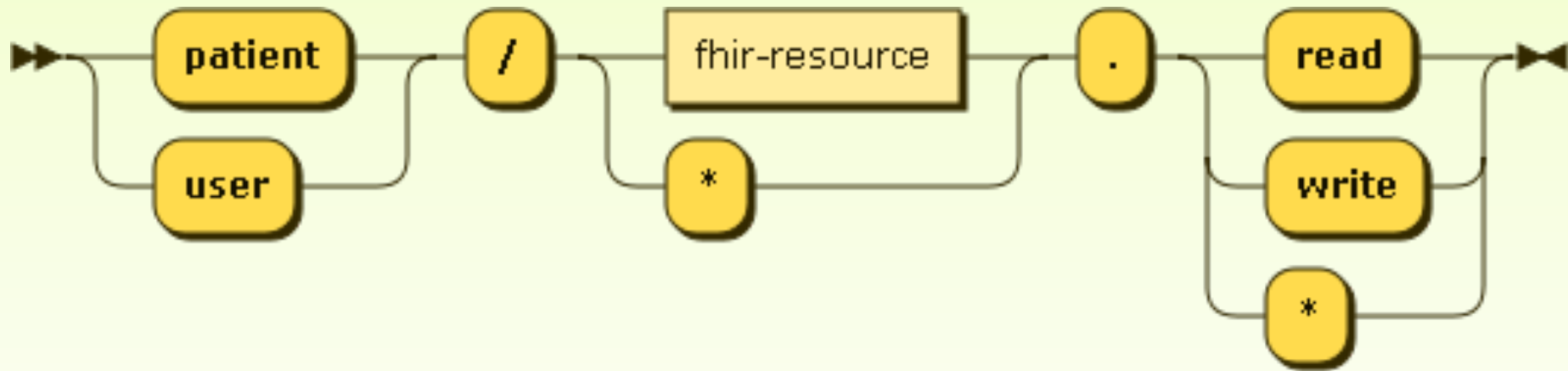
- 1. Introduction
 - 1.1. Requirements Notation and Conventions
 - 1.2. Terminology
- 2. Resource Registration
 - 2.1. Resource Types
 - 2.2. Scopes
- 3. Claims Presentation
 - 3.1. Membership in an organization
 - 3.2. Professional credentialing status
 - 3.3. Specific identification of parties
 - 3.4. Emergency access
- 4. Policy Development
 - 4.1. "Break the glass" emergency access policies
- 5. Security considerations
- 6. Privacy considerations
- 7. Normative References
- Appendix A. Acknowledgements
- Appendix B. Notices
- Appendix C. Purpose of Use
- Appendix D. Document History
- Author's Address

FHIRのリソースの定義、スコープ

アクセスするステークホルダーに関する
取り決め

Break the glassへの対応

Scopeの例



user/Appointment.*

利用者は予約に関するリソースを読み書き可能

patient/Observation.read

患者は自身のObservationリソースを読み込みのみできる

EBNFは <http://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context/> より引用

https://openid.net/specs/openid-heart-fhir-oauth2-1_0.html#rfc.section.2

Claimの例

3.2. Professional credentialing status

To reference licenses, accreditations, or other professional credentials held by the current user, include the `pro` claim. These are generally for things such as specific medical licenses or degrees.

`pro` 機械読み取り可能な医療従事者の資格情報
Array of machine-readable values representing the professional credential held by the current user.

Each `pro` value consists of a JSON object with the following members:

`src` 資格の管理者を表すURL
URI representing the authority conveying the professional credential on the user, such as a state or regulatory group

`val` 資格名(文字列)
String value representing the nature of the professional credential held.

The value of the professional credential is dependent on and potentially defined in the context of the authoritative source. An example list of professional values can be found at <http://www.hl7.org/fhir/v2/0360/2.7/index.html>.

The means by which a given organization is trusted to convey a given professional status of an organization is outside the scope of this document. Note that the `src` claim here is likely to be different from the `iss` of the ID token, and the means by which an issuer is trusted to assert a claim of accreditation from a particular source is outside the scope of this specification.



こういう風にやればいいよ、というレベルの定義。
日本でやるとしたら？ HPKIと証明書・属性を活用する？

https://openid.net/specs/openid-heart-fhir-uma2-1_0.html

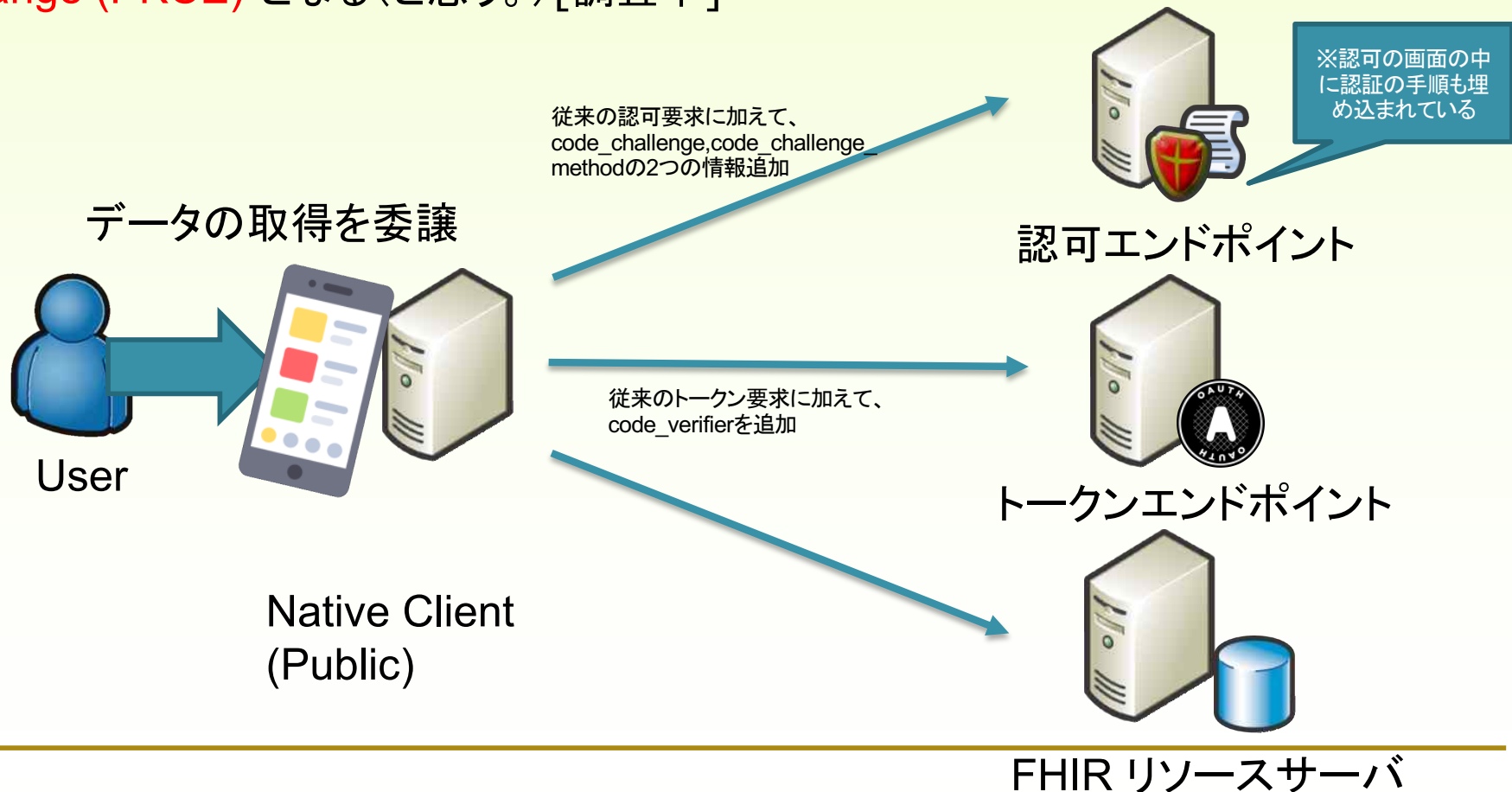
HEARTの要求事項

- Client Secretを取り除き、公開鍵を認可サーバへの登録を要求
 - 鍵フォーマット JOSE JWK
- Grant Typeの制約
 - Implicit Grant Type利用への制約
 - ブラウザ内のクライアントに使う場合のみ
 - Client Credential Grant Type
 - バックチャネルを使って一括処理を行うサーバアプリケーションのみ
- OAuth認可サーバのサポート要求
 - Token Introspection, Token Revocation
 - サービス検出エンドポイント
 - トークンは非対称暗号方式で署名されたJWT
 - 動的クライアント登録の要求
- OAuthクライアントへの要求
 - 最低限の乱雑さをもったstateパラメータの毎回使用
 - 完全なリダイレクトURI 文字列の完全一致ベースの比較検証

セキュリティの
底上げ

PHR クライアントの種類

2.1.2. Native Client with User Delegation [Public]、いわゆる Authorization Code Flow with Proof Key for Code Exchange (PKCE) となる(と思う。)[調査中]



参考:フローについてはここが分かりやすいと思います。

<https://qiita.com/TakahikoKawasaki/items/200951e5b5929f840a1f>

Public Native Clientの要件

Specs	2.1.2 b Public Native Client
OAuthの認可コードフロー	MUST
認証エンドポイントにおける認証	MUST
公開鍵への関連付け	MUST
リフレッシュトークン発行	MAY
別個のWebブラウザアプリケーションとの相互作用	○
ダイナミッククライアント登録	MUST
公開鍵の認可サーバへの登録	SHOULD
登録プロセスにおける認証サーバによる公開鍵と秘密鍵の発行	MAY
S256コードチャレンジとともにPKCEを利用する	MUST
アクセストークンの短命化	--

HEARTは厚生労働省の医療情報システムの安全管理に関するガイドラインで想定されている水準をクリアしている

我が国での取り組みの方向性

- FHIRの日本版標準プロファイル策定
 - NeXEHRs WGで進行中
 - 情報交換時の認証・認可のプロファイル策定
 - 未定
 - マイナポータル、PHR、地域医療連携システムで使えるようなProfileを
 - 調査 中山雅晴先生 厚労科学研究班
 - HEART WGを中心に日本のガイドラインやPHR、地域医療連携のユースケースとの整合性を取りながら検討
-

OAuthを用いたアプリケーション例

前提

- OAuthに関する基本的な知識
 - Postmanをインストールしていること
 - Application Registration
 - Blue Button 2.0 Developer Guide
 - Sample Beneficiaries CSV Data
-

Blue Button 2.0

- トランプ大統領による“MyHealthEData”イニシアチブ（2018年3月）の一環で開発^[1]
 - 患者によるデータのアクセスとコントロール能力の拡大
 - 十分な情報にもとづいた意志決定を支援
 - 4年間のMedical Part A,B,D 償還請求データ
 - 処方箋、プライマリーケア等
 - **FHIR**（標準医療情報規格）, **OAuth2.0**（認可）^[2]

[1] <https://royaljay.com/healthcare/cms-announces-first-ever-blue-button-2-0-developer-conference/>

[2] CMS Blue Button 2.0 <https://bluebutton.cms.gov/developers/>

Blue Button 2.0 Developer

- CMSはBlue Button 2.0で採用されたFHIR REST API/Oauthに対応する開発者の為に **Sandbox**とDocumentを公開
 - 登録すれば米国以外の方でも利用可能
 - ダミーのBeneficiary 100名分のアカウントとデータを用意 → リアルな環境で検証可能
-

Sandbox

- 開発者ごとに割り当てられる仮想環境
 - FHIR関連サービスで実環境に近いSandboxを提供 → 従来の医療情報システムと比べて開発スピードが劇的に向上
 - 単なる公開テスト用サーバとの違い
 - 開発者ごとに独自のインスタンス
 - テストシナリオが準備されていることが多い
 - 実際のユーザー認証(OAuth)、権限が設定
 - リアルな医療情報
 - サービス提供者が採用しているProfileに準じた稼働
-

This wiki has undergone a migration to Confluence found [Here](#)

Publicly Available FHIR Servers for testing

Content on this page has been migrated to Confluence here: <https://confluence.hl7.org/display/FHIR/Public+Test+Servers>

Back to [FHIR](#) home page

Introduction

This page lists FHIR servers that are publicly available for testing. These are public services provided by volunteers and HL7 members. In order to avoid spam etc, the servers are generally password protected. A contact is provided to get a password.

BTW: List of publically available test data (some of these test servers preload some of this data):

- [\[Base: What is in the specification\]](#)
- [\[Smart on FHIR test data\]](#)

Status

The status of publicly available FHIR servers is monitored using UptimeRobot at <https://stats.uptimerobot.com/9DARdu1Jo>. If you want to see the UptimeRobot status page, email [\[Sean McIlvenna\]](mailto:Sean.McIlvenna@hl7.org).

Servers

Note that these servers are testing servers. They may be sporadically unavailable, and as the FHIR specification is a moving target, they may not be implemented correctly.

- <http://test.fhir.org/r2>, <http://test.fhir.org/r3> and <http://test.fhir.org/r4> - Grahame's test server
 - Supports all resource types, all operations, xml + json
 - implementation details: open source - see [\[\[2\]\]](#)
 - supports Smart on FHIR

FHIR Server

This is an implementation of the FHIR standard using the [US Core Implementation guide](#). We expect client developers to use the server as part of their development activities to work with different data sets.

DSTU2

STU3

R4

Instructions and Guidelines to use the FHIR Server:

The FHIR Server can be used in two modes. An open mode (No OAuth token required) and a secure mode (OAuth tokens required).

1. The server URI for R4 open mode is : <https://fhir.sitenv.org/open/r4/fhir>
2. The server URI for R4 secure mode is : <https://fhir.sitenv.org/secure/r4/fhir>

Register

Login

Using the Open FHIR Server For R4:

A client can use the open server by making a FHIR request using a FHIR READ or SEARCH operation.

1. For example a simple READ can be executed as follows:
 - GET <https://fhir.sitenv.org/open/r4/fhir/Patient/1> - XML format.
 - GET https://fhir.sitenv.org/open/r4/fhir/Patient/1?_format=json - JSON format.
2. For example a simple SEARCH can be executed as follows:
 - GET https://fhir.sitenv.org/open/r4/fhir/Patient/?_id=1 - XML format.
 - GET https://fhir.sitenv.org/open/r4/fhir/Patient/?_id=1_format=json - JSON format.
3. Click [here](#) for more details on [FHIR Search](#).
4. For a list of Patients [Click here](#).

Using the Secure FHIR Server For R4:

1. The Secure FHIR server follows the implementation of Smart On FHIR specifications.
2. In order to use the FHIR Server with the appropriate tokens the following steps need to be followed
 - Create a user account in the FHIR Authorization Server: Follow instructions [here](#) for user creation.
 - Login and Register a client so that you can get the Client Id and Client Secret. Follow instructions [here](#) for client registration.
 - Once you have a Client Id and Client Secret follow the guidelines according to the Smart On FHIR to request resources.

API

CMS Blue Button 2.0

Blue Button 2.0 is a standards-based application programming interface (API) that delivers Medicare Part A, B, and D data for over 60 million Medicare beneficiaries.

[VIEW THE DOCUMENTATION →](#)

[SIGN UP FOR THE DEVELOPER SANDBOX →](#)

Overview

Getting started

Value and Use Cases

Support

Overview

Blue Button 2.0 is a standards-based application programming interface (API) that delivers Medicare Part A, B, and D data for over 60 million Medicare beneficiaries. Claims and enrollment data is available from May 2014.

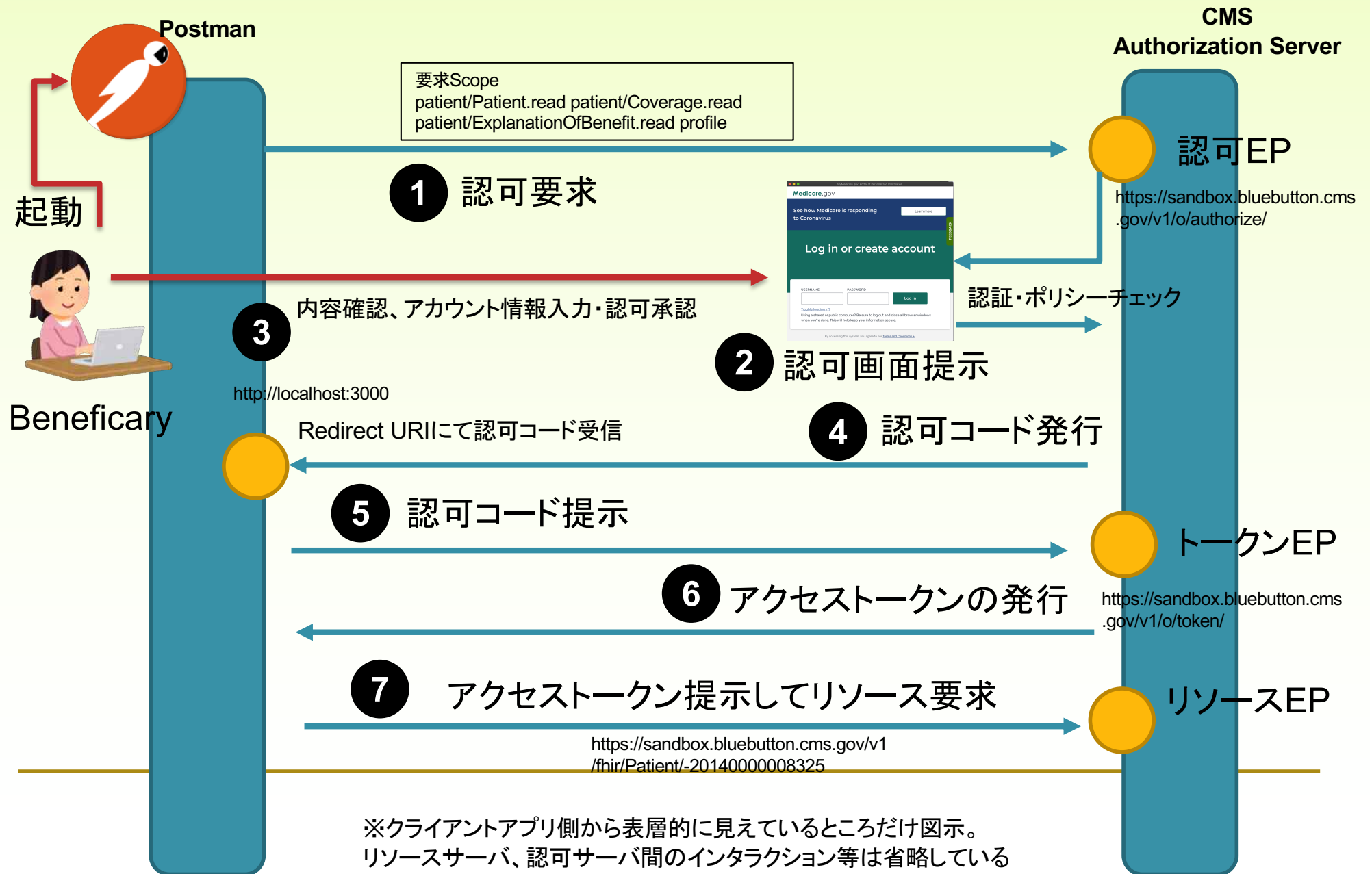
The Blue Button 2.0 API uses the [HL7 FHIR standard](#) for beneficiary data and the [OAuth 2.0 standard](#) for beneficiary authorization.

<https://bluebutton.cms.gov/>

CMS Blue Button 2.0 APIについて

- Blue Button 2.0のプロファイルで定められているOAuthは2種類のFlowをサポート
 - Authorization Code Flow
 - Webアプリケーションのサーバとの連携
 - Native Apps Authentication Flow
 - 患者PHRクライアントアプリとの連携
 - 今回はAuthorization Code Flowを説明
-

Authorization Code Flow



Developer Dashboard

The Developer Sandbox lets you register applications to get credentials to access our synthetic (or sample) beneficiary data. You can use that data to build and test your application to get it ready for production!

ADD AN APPLICATION →

READ OUR DOCUMENTATION →

My Sandbox Apps

jp.ac.ehime-u.m.test

Last Updated: July 12, 2020, 8:25 a.m.



Client ID

Show/Hide Credentials

.....

Client Secret

.....

View/Edit App →

+ Add an Application

事前準備として、Blue Button 2.0 REST APIにアクセスするアプリケーションの情報を登録する

Register a New Application

App Details - Required Info

Application Name

reverse domain name notation.

ex. `jp.ac.ehime-u.m.client`

OAuth - Client Type

Confidential

Web Application Flow
での設定

Authorization Grant Type*

Authorization code

Callback URLs / Redirect URIs

`http://localhost:3000` 等

Web Application Flowの場合
OAuth Client TypeはConfidential,
Grant TypeはAuthorization Code

Optional App Information

Yes I have read and agree to the [API Terms of Service Agreement](#)*

Save Application

App Credentials

Client ID	Show/Hide Credentials
<input type="text" value="....."/>	
Client Secret	
<input type="text" value="....."/>	

App Details - Required Information

OAuth - Client Type	<input type="text" value="confidential"/>
OAuth - Grant Type	<input type="text" value="authorization-code"/>
Callback URLs / Redirect Uris	<input type="text" value="http://localhost:3000"/>

登録されたら、このような詳細情報が表示されるので確認すること。なお、属性値は小文字での記述

App Details - Optional Information

This information can be used to more fully emulate elements of having an application in production. **This information is only used for sample purposes.** For example, you can enter your website or privacy policy to simulate what a Medicare beneficiary would see when authorizing your application.

Sample Beneficiariesのデータ入手

FHIRのPatient ResourceのIDとBeneficarie Accountの対応については、下記のWebサイトでCSVデータで公開されているのでダウンロードの上お手元においてください。

<https://bluebutton.cms.gov/developers/#try-the-api>

Sample Beneficiaries

[CSV of 100 sample beneficiaries with rich claims data](#)

When getting started with the Blue Button API, it can be overwhelming to understand all of the coding systems and types of data that can be found in the Explanation of Benefit FHIR resource.

Below are some hypothetical Beneficiaries in the sense of what is found in claims data

検証用REST APIに登録されているデモデータをCSVでも提供されているので、結果を照合・確認するために手元に置くと便利です。

OAuthのAccess Token取得

The screenshot shows a REST client interface with the following elements:

- Request Bar:** Method: GET, URL: `https://sandbox.bluebutton.cms.gov/v1/fhir/Patient/-20140001`, Buttons: Send, Save.
- Auth Tab:** Selected, showing OAuth 2.0 configuration.
- Auth Configuration:** TYPE: OAuth 2.0, Header Prefix: Bearer, Access Token field.
- Buttons:** Get New Access Token (highlighted in orange).

Three callout boxes provide instructions:

- ①リソースEPへの要求URLを入力するが、そのまま”Send”は押さずに
- ②Authタブを開き、認証タイプにOAuth2.0を選択、認可データはRequest Headerを指定
- ③アクセストークン要求ボタンを押す。

GET NEW ACCESS TOKEN



Token Name

jp.ac.ehime-u.m.client

Grant Type

Authorization Code

Callback URL ⓘ

http://localhost:3000

Authorize using browser

Auth URL ⓘ

https://sandbox.bluebutton.cms.gov/v1/o/authorize/

Access Token URL ⓘ

https://sandbox.bluebutton.cms.gov/v1/o/token/

Client ID ⓘ

[Redacted]

Client Secret ⓘ

[Redacted]

Scope ⓘ

patient/Patient.read patient/Coverage.read patient/ExplanationOfBen ...

State ⓘ

State

Client Authentication

Send as Basic Auth header

CMSに登録したアプリケーション情報を記入する。
Token Name == Application Nameである。

CMSが提示しているSandboxのEPの
URLを入れる。

アプリケーションを登録した時にCMS
から提供された認証情報を入れる

欲しいリソースを要求スコープに入れる。
patient/Patient.read
patient/Coverage.read
patient/ExplanationOfBenefit.read
profile

必要な情報を入力し終わったら、トークン
要求をする

Cancel

Request Token

Medicare.gov

See how Medicare is responding
to Coronavirus

Learn more

FEEDBACK

Log in or create account

認証画面に遷移するので、ダミーBeneficiaryのアカウントをどれか選んで入力する。(このアカウントは、最初に入力した要求リソースに対応するBeneficiaryのものにしないと、認可が下りても、権限のないリソースの要求をすることになるので、認可を貰っても何もリソースが得られないという結果になる。)

USERNAME

PASSWORD

Log in

[Trouble logging in?](#)

Using a shared or public computer? Be sure to log out and close all browser windows when you're done. This will help keep your information secure.

Patient Resourceと Beneficiarie Accountの対応

synthetic_users_by_

	A	B	C	D	E	
	BENE_ID	FRONTEND_USER_NAME	FRONTEND_USER_PASSWORD	total_claim_count	total_claim_line_count	carri
1	20140000001827	BBUser21826	PW21826!	592	635	
2	20140000004807	BBUser24806	[被保険者のIDとPass	510	591	
3	20140000005499	BBUser25498	PW25498!	509	568	
4	20140000004547	BBUser24546	PW24546!	503	524	
5	20140000008953	BBUser28952	PW28952!	474	509	
6	20140000000183	BBUser20182	PW20182!	452	517	
7	20140000006105	BBUser26104	PW26104!	445	532	
8	20140000005798	BBUser25797	PW25797!	439	473	
9						

Annotations:
- Red arrow pointing to BENE_ID in row 2: **これがPatient Resourceを指定する時のID**
- Red arrow pointing to FRONTEND_USER_NAME in row 3: **被保険者のIDとPass**

Medicare.gov

jp.ac.ehime-u.m.test has asked for some of your data.

Information about your doctor/hospital visits

Information about the prescription medications you

Personal Information like your name, address, date of birth

Beneficiaryに対して、アプリケーションがデータへアクセスしようとしていること、その為の許可を求めたいことを、この画面で説明しています。それに対して、全てのデータを渡すか、個人に関する情報以外のデータのみ認めるかを選択できるオプションを提示しています。

Privacy Options



Share all of your data

This app will have access to both your healthcare data and some personal information



Share healthcare data, but not your personal info

Block some of your personal data like name, address, date of birth, race, and gender

Understand how your data is being used

To understand fully how jp.ac.ehime-u.m.test will use your data, please read the app's [Privacy Policy](#) and [Terms and Conditions](#).

この認可要求時の選択、要求スコープ、サーバ側の要求スコープに関する各ポリシー等を統合して判断して、最終的に認可されるスコープが決定されます。

Allow

[Deny](#)

アクセストークンの取得

The screenshot displays a web interface for managing access tokens. The main title is 'MANAGE ACCESS TOKENS'. On the left, there is a sidebar with 'All Tokens' and a 'Delete' button. The selected token is 'jp.ac.ehime-u.m.client'. The main area shows 'Token Details' for this token, including its name, access token, type, expiration, scope, refresh token, and patient ID. A 'Use Token' button is visible in the top right corner of the details panel.

Token Details	
Token Name	jp.ac.ehime-u.m.client
Access Token	xQBCAlbtBmFCsI2UXnfDCCTWLLrTz
Token Type	Bearer
expires_in	36000
scope	patient/Patient.read patient/Coverage.read patient/ExplanationOfBenefit.read profile
refresh_token	LzI2Tuwn0cTpBixHkHqFIVIsd1Y6XJ
patient	-19990000000001

Patientリソースへのアクセス

The screenshot displays a REST client interface with the following elements:

- Request Bar:** Method: GET, URL: `https://sandbox.bluebutton.cms.gov/v1/fhir/Patient/-20140000`, Buttons: Send, Save.
- Auth Tab:** Selected, showing OAuth 2.0 configuration.
- Access Token:** Field containing `xQBCAlbtBmFCsI2UXnfl`.
- Header Prefix:** Field containing `Bearer`.
- Warning:** A yellow circle highlights a warning message: "Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)".
- Buttons:** "Get New Access Token" button is visible below the token field.
- Other Tabs:** Params, Headers (8), Body, Pre-req., Tests, Settings, Cookies, Code.

```
{
  "resourceType": "Patient",
  "id": "-19990000000001",
  "meta": {
    "lastUpdated": "2020-07-07T20:39:31.478+00:00"
  },
  "extension": [...],
  "identifier": [
    {
      "system": "https://bluebutton.cms.gov/resources/variables/bene_id",
      "value": "-19990000000001"
    },
    {
      "system": "https://bluebutton.cms.gov/resources/identifier/mbi-hash",
      "value": "37c37d08d239f7f1da60e949674c8e4b5bb2106077cb0671d3dfcbf510ec3248"
    }
  ],
  "name": [
    {
      "use": "usual",
      "family": "Doe",
      "given": [
        "Jane",
        "X"
      ]
    }
  ],
  "gender": "female",
  "birthDate": "1999-06-01",
  "address": [
    {
      "district": "999",
```



Medicare Beneficiary Identifier (MBI)

```
},
"extension": [
  {
    "url": "https://bluebutton.cms.gov/resources/variables/race",
    "valueCoding": {
      "system": "https://bluebutton.cms.gov/resources/variables/race",
      "code": "1",
      "display": "White"
    }
  },
  {
    "url": "https://bluebutton.cms.gov/resources/variables/rfrnc_yr",
    "valueDate": "0003"
  },
  {
    "url": "https://bluebutton.cms.gov/resources/variables/dual_01",
    "valueCoding": {
      "system": "https://bluebutton.cms.gov/resources/variables/dual_01",
      "code": "AA"
    }
  },
  {
    "url": "https://bluebutton.cms.gov/resources/variables/dual_02",
    "valueCoding": {
      "system": "https://bluebutton.cms.gov/resources/variables/dual_02",
      "code": "AA"
    }
  },
  {
    "url": "https://bluebutton.cms.gov/resources/variables/dual_03",
    "valueCoding": {
      "system": "https://bluebutton.cms.gov/resources/variables/dual_03",
      "code": "AA"
    }
  }
]
```

https://bluebutton.cms.gov/resources/variables/dual_01/

Variable: DUAL_01

Monthly Medicare-Medicaid dual eligibility code - January

メディケイドとメディケアの両方への加入資格がある「二重資格者」に該当するかの情報

Description

This variable indicates whether the beneficiary was eligible for both Medicare and Medicaid in a given month (January).

Comment

The original source for this variable is the State Medicare Modernization Act (MMA) files that states submit to CMS. Those files are considered the **gold standard** for identifying dual eligibles because the information in them is used to determine the level of Medicare Part D low-income subsidies. Dual eligibles are often divided into **full duals** and **partial duals** based on the level of Medicaid benefits they receive. CMS generally considers beneficiaries to be full duals if they have values of 02, 04, or 08, and to be partial duals if they have values of 01, 03, 05, or 06. Partial duals sometimes divided into the QMB-only population (01) and all other partial duals (03, 05, or 06). There are different ways to classify dually eligible beneficiaries. Additional information regarding various ways to identify dually enrolled populations, refer to a CCW Technical Guidance document entitled: "Options in Determining Dual Eligibles". There are 12 monthly variables - where the 01 through 12 at the end of the variable name correspond with the month (e.g., 01 is January and 12 is December).

Values

This variable is coded, and will contain one of the following values.

Values for Codeset

Value	Description
NA	Non-Medicaid
00	Not enrolled in Medicare for the month
01	Qualified Medicare Beneficiary (QMB)-only
02	QMB and full Medicaid coverage, including prescription drugs
03	Specified Low-Income Medicare Beneficiary (SLMB)-only

Take Home Message

- FHIRで情報交換する際の認証・認可はOAuthだけでは不足。また使い方も決める必要がある。
 - OpenID Connectで医療分野向けのProfileをHEART WGが策定している。
 - OpenID Connect、OAuth、UMA、FHIRの規格を理解し、PHR、地域医療連携、研究用のデータ提供の各ユースケースに即した日本版プロファイルの策定が必要
 - FHIRを利用したアプリケーションを開発者が実地に使える環境 = Sandbox
 - Sandboxを実際に使うことがFHIRとOAuthの理解の早道
-

出席用クイズ

- BlueButton 2.0を策定した時の米国大統領は？
 - クリントン大統領
 - オバマ大統領
 - トランプ大統領
-