FHIR研究会 Webセミナー　2020.12.05 SAT

IHE on FHIR
～ OAuth を利用した IUAプロファイル ～

一般社団法人 日本IHE協会
理事 放射線技術委員長 接続検証委員長
塩川　康成

キヤノンメディカルシステムズ株式会社
日本HL7協会 適合性認定委員長
上級医療情報技師 S2007007
上級医療情報技師育成指導者

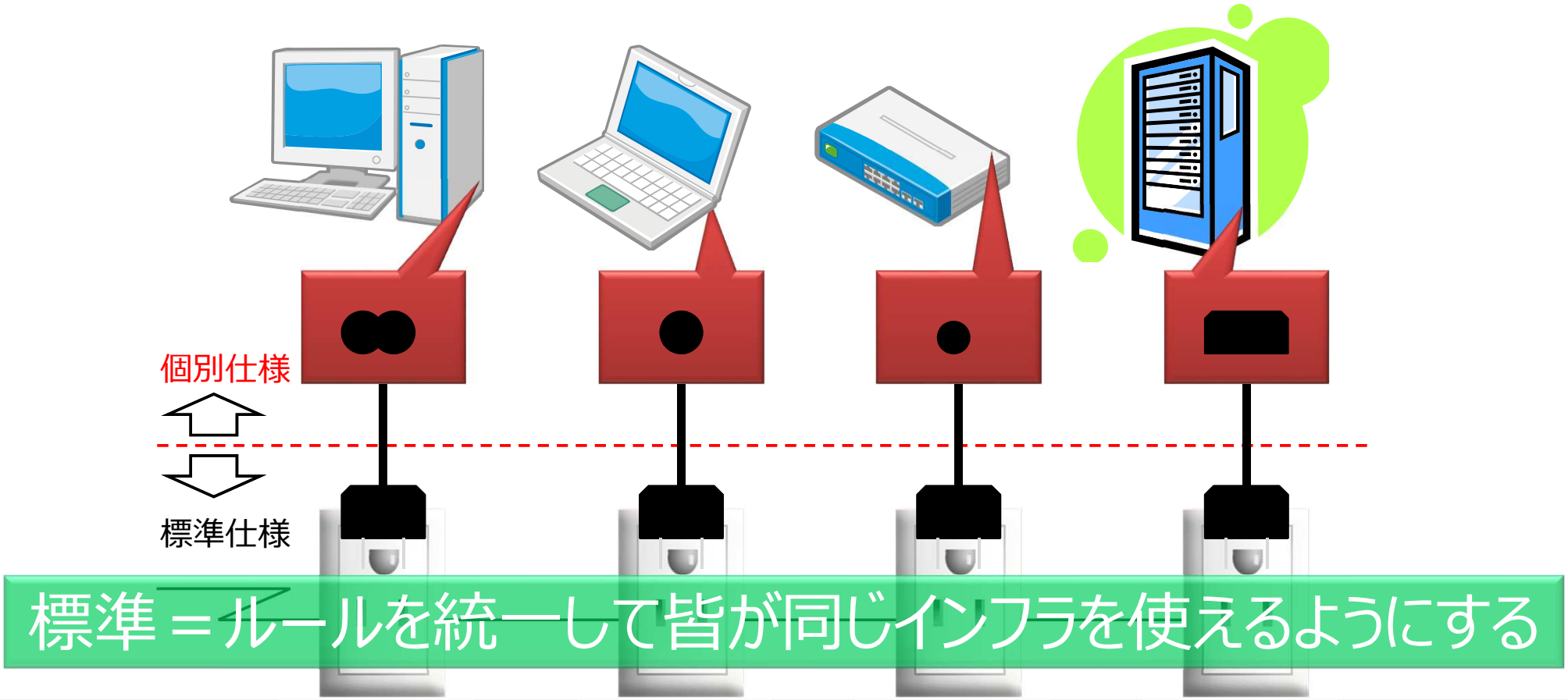
IHE とは

https://www.ihe.net/

標準とはなにか？

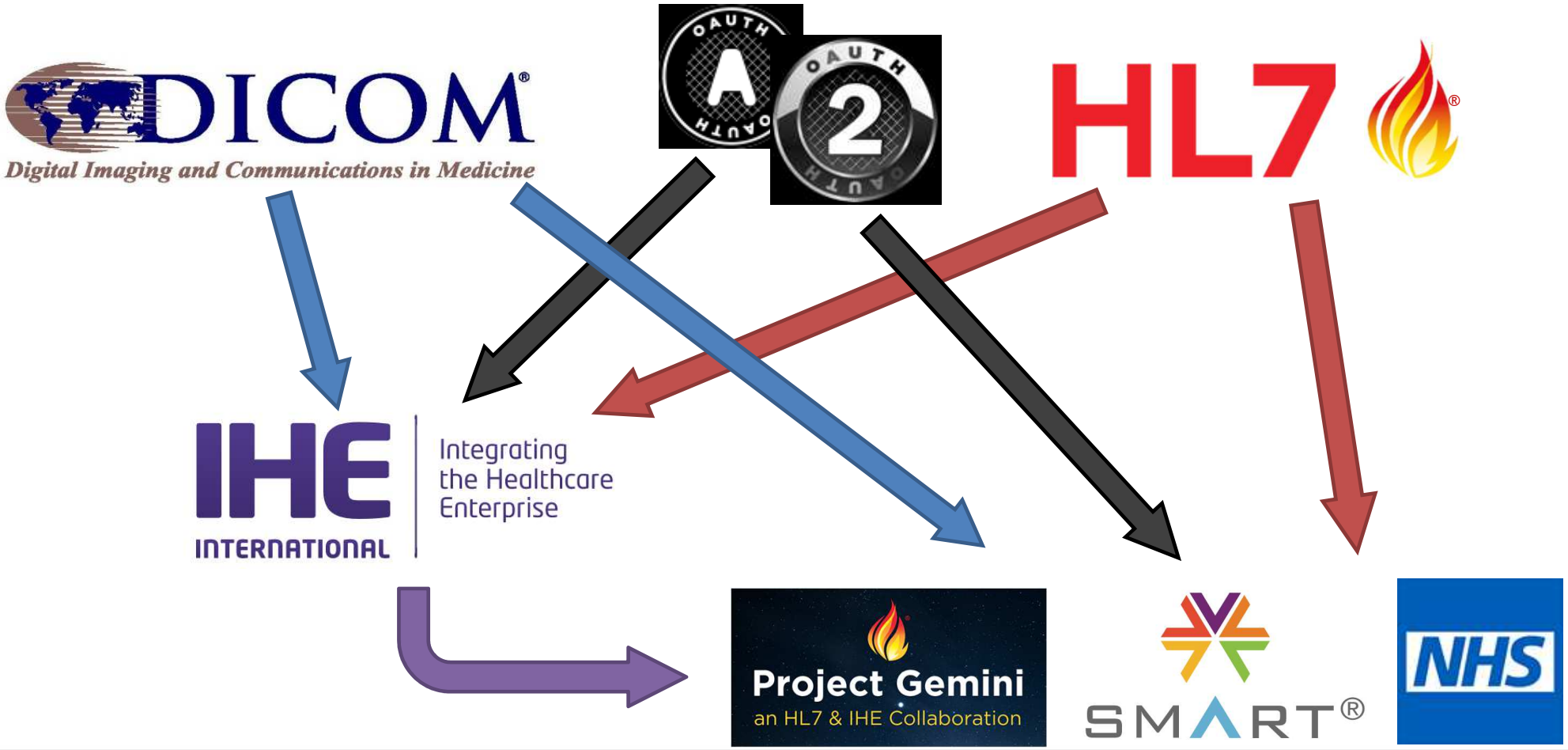
IHE JAPAN Integrating the Healthcare Enterprise

➢ 電源ケーブルを考えてみよう！



標準＝ルールを統一して皆が同じインフラを使えるようにする

OAuthも含め、規格は単独で使うだけではない



本日の Agenda

1. IHE活動と、IHE on FHIRについて
2. OAuth について（超概要）
3. OAuth を利用した IUAプロファイル

IHE活動と、IHE on FHIRについて

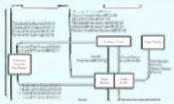
IHE とは： 活動概要（IHEサイクル）

IHE INTERNATIONAL Integrating the Healthcare Enterprise

IHE JAPAN Integrating the Healthcare Enterprise

複数システムや複数メーカの装置間で医療情報を連携し、機能を統合し、相互運用性の向上を図るシステムの実現方法を提供する。

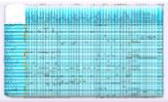
各分野での業務シナリオの作成



既存の規格を利用してシナリオの実現（統合プロファイル）

統合プロファイルの実装（ベンダ）

コネクタソン(接続テスト)

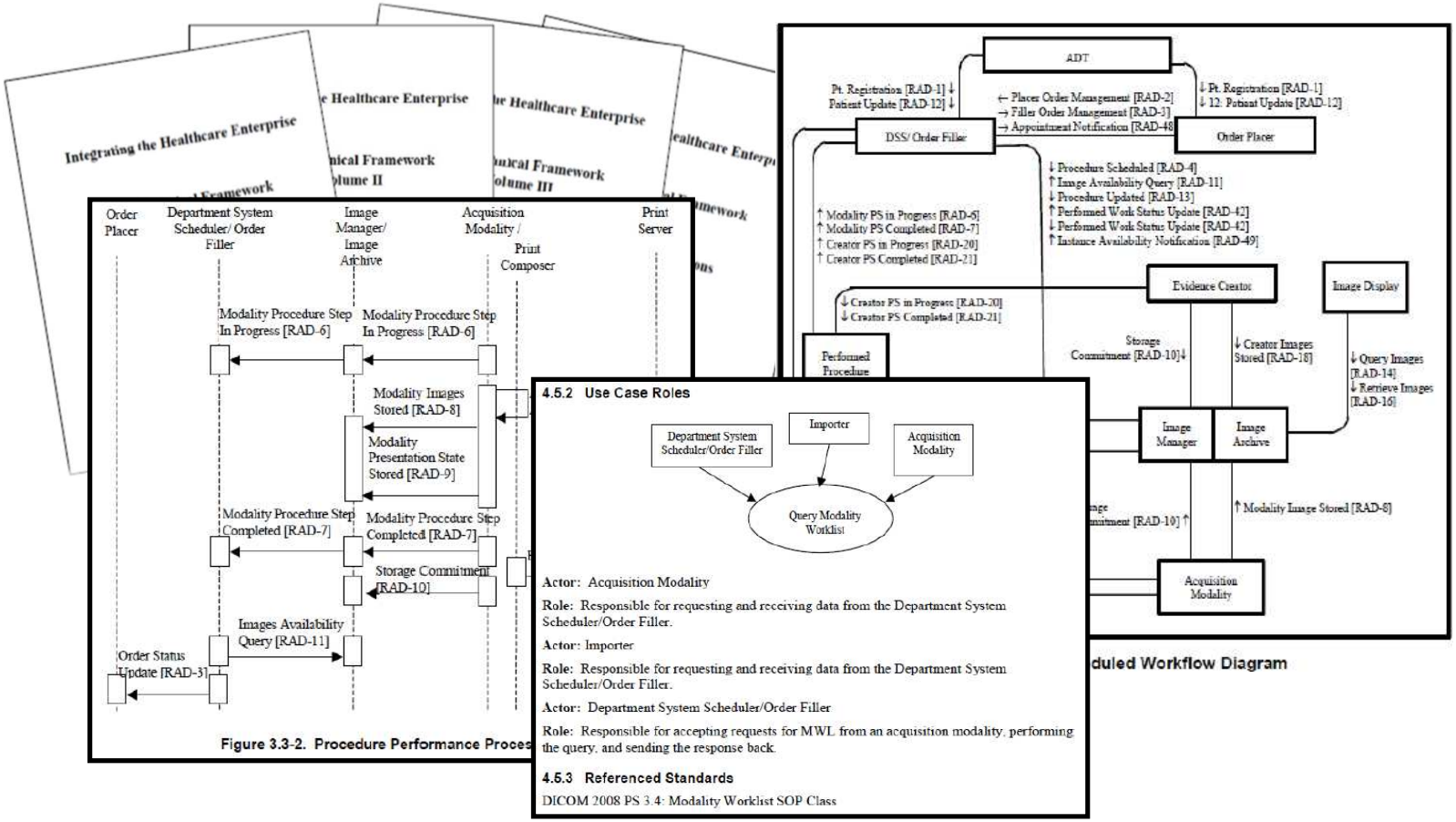


結果の公開・活動の広報

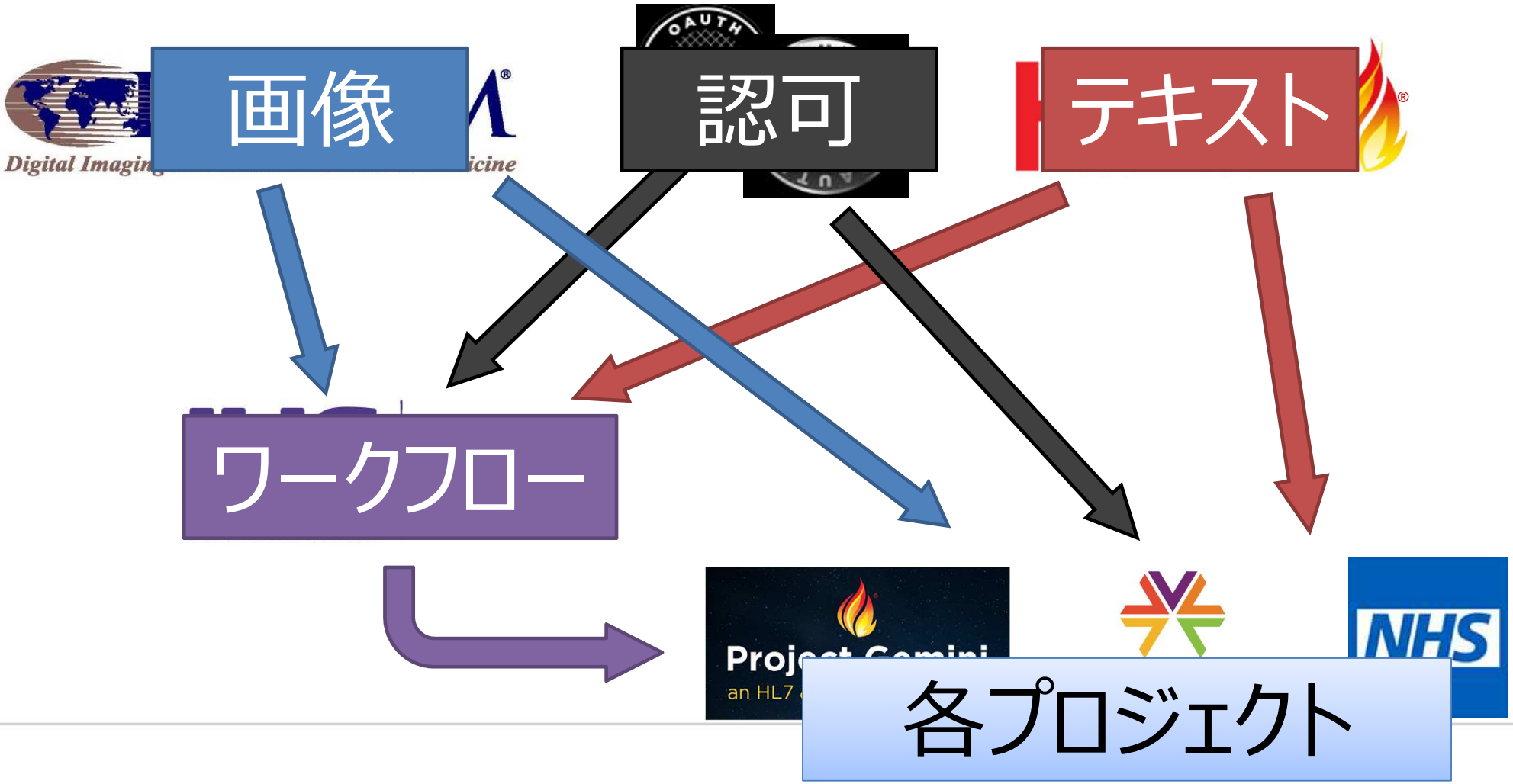
国際的な標準化活動(ISO）、国際協調　など

【引用】 IHE活動の概要　細羽 実, 日本IHE協会 副理事長, JCMI40 2020

IHEとは： テクニカルフレームワークの発行



IHEは各規格を使った医療ワークフローを定義



IHE on FHIR

- 2018年の Project Gemini 立上げより、HL7 FHIR と IHE のコラボレーションが加速し、「IHE on FHIR」として広報されるようになった。
- Project Gemini は HIMSS18の場で立ち上がり、HL7 と IHE それぞれの特徴を調和し、より医療現場での FHIR を活用したワークフローの追求と、整備を行っている。
- IHEではこれに伴い、PCC（Patient Care Coordination）、QRPH（Quality, Research, and Public Health）の各ドメインで FHIRプロファイルの整備を実施。
- また、Radiology、ITI（IT Infrastructure）、Pharmacy、Devices では、モバイルデバイス対応や、医療現場の REST通信環境の整備促進に伴い、FHIRプロファイルを独自に整備している。

IHE on FHIR Profiles (1/2)

- Devices（旧 PCD: Patient Care Device）
  - POU Personal Health Device Observation Upload
- ITI (IT Infrastructure)
  - ATNA Audit Trail and Node Authentication
  - IUA Internet User Authorization
  - mACM Mobile Alert Communication Management
  - MHD Mobile access to Health Document
  - MHDS Mobile Health Document Sharing
  - mCSD Mobile Care Service Discovery
  - mXDE Mobile Cross-enterprise Document Data Element Extraction
  - NPFS Non-Patient File Sharing
  - PDQm Patient Demographics Query for Mobile
  - PIXm Patient Identifier Cross-reference for Mobile
  - PMIR Patient Master Identity Registry
  - SVCM Sharing Valuesets, Codes and Maps
- PCC (Patient Care Coordination)
  - ACDC Assessment Curation and Data Collection
  - DCP Dynamic Care Planning
  - DCTM Dynamic Care Team Management
  - GAO Guideline Appropriate Ordering
  - IPS International Patient Summary
  - PCS Paramedicine Care Summary
  - PMDT Point-of-care Medical Device Tracking
  - QEDm Query for Existing Data for Mobile
  - RECON Reconciliation of Clinical Content and care providers
  - RIPT Routine Interfacility Patient Transport
  - CMAP Clinical Mapping
- Pharmacy
  - MMA Mobile Medication Administration
  - UBP Uniform Barcode Proccessing

https://wiki.ihe.net/index.php/Profiles より FHIRマーク付きプロファイル抜粋

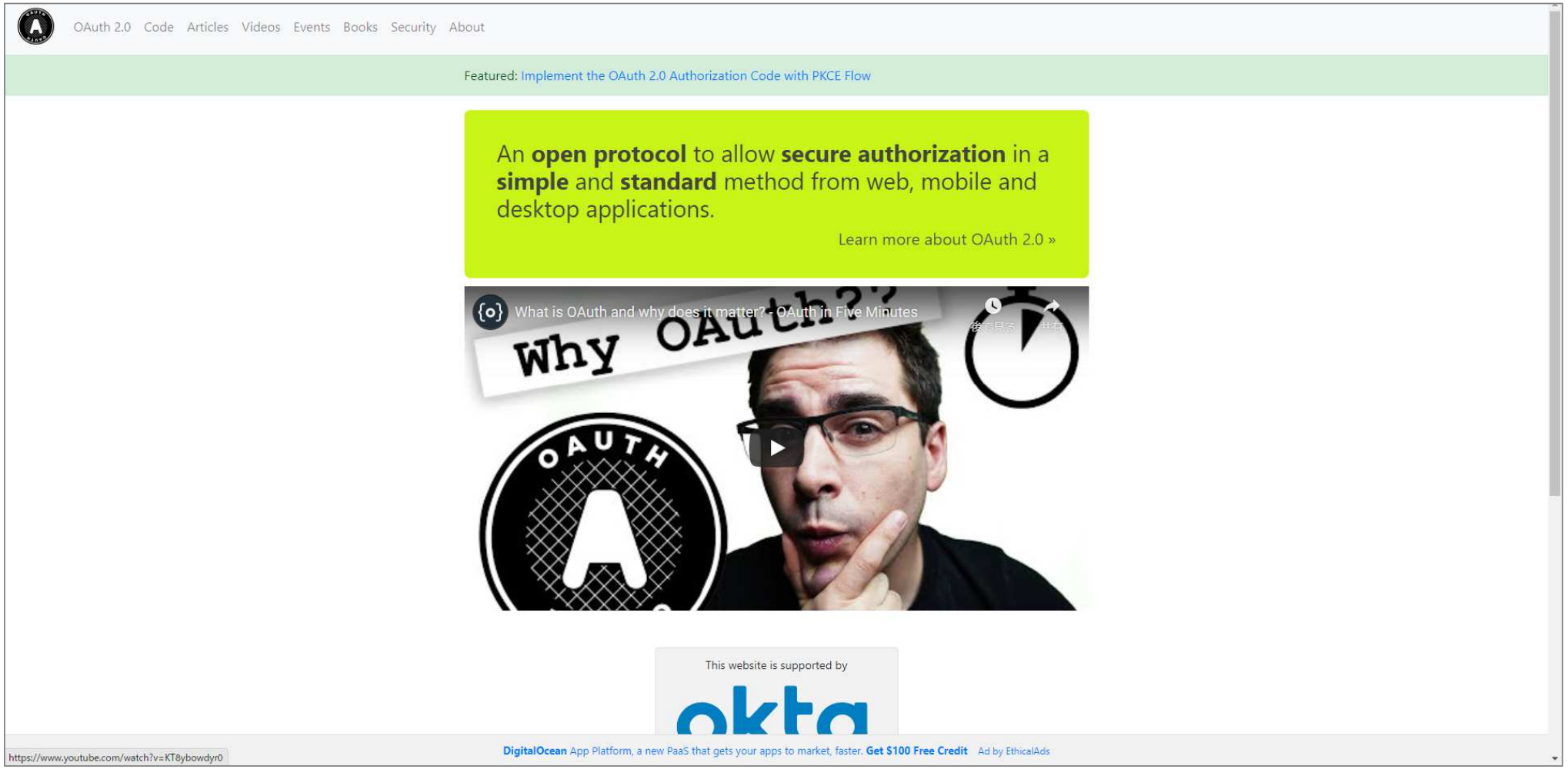
IHE on FHIR Profiles (2/2)

- QRPH (Quality, Research, and Public Health)
  - BFDR-E Birth and Fetal Death Reporting Enhanced Profile
  - CCG Computable Care Guidelines
  - mADX Mobile Aggregate Data Exchange
  - mRFD Mobile Retrieve Form for Data capture
  - PRQ Prescription Repository Query
  - QORE Quality Outcome Reporting for EMS
  - VRDR Vital Records Death Reporting
- Radiology
  - IDEP Import and Display of External Priors
  - SOLE Standardized Operational Log and Events

https://wiki.ihe.net/index.php/Profiles より FHIRマーク付きプロファイル抜粋

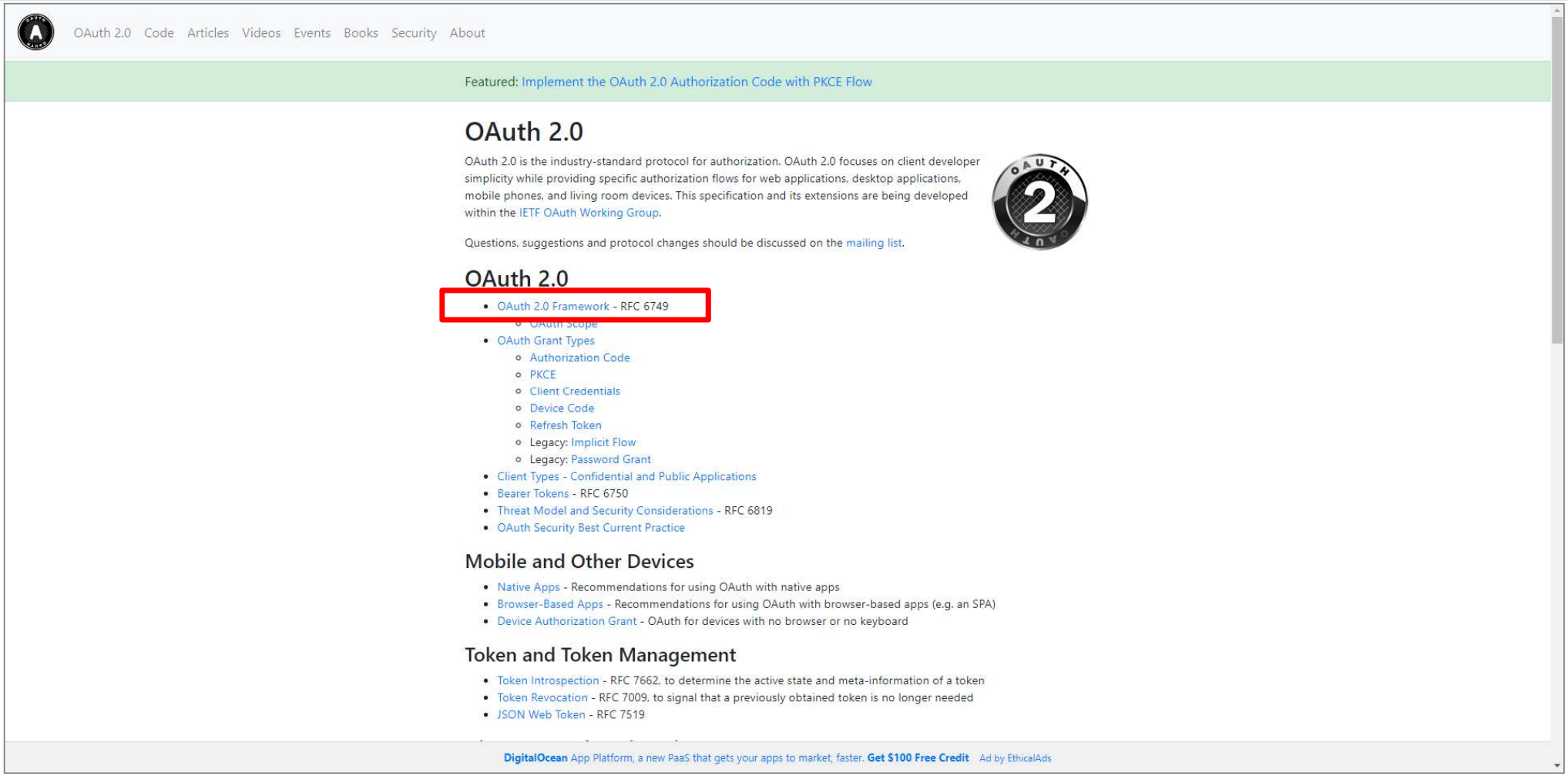
OAuth について（超概要）

OAuth とは



https://oauth.net/

OAuth とは



https://oauth.net/2/

RFC 6749 The OAuth 2.0 Authorization Framework

[Docs] [txt|pdf] [draft-ietf-oaut...] [Tracker] [Diff1] [Diff2] [IPR] [Errata]

Updated by: 8252 PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 6749
Obsoletes: 5849
Category: Standards Track
ISSN: 2070-1721

The OAuth 2.0 Authorization Fr

Abstract

The OAuth 2.0 authorization framework enables a application to obtain limited access to an HTTP behalf of a resource owner by orchestrating an between the resource owner and the HTTP service third-party application to obtain access on its specification replaces and obsoletes the OAuth in RFC 5849.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engi (IETF). It represents the consensus of the IET received public review and has been approved fo Internet Engineering Steering Group (IESG). Fu Internet Standards is available in Section 2 of

Information about the current status of this do and how to provide feedback on it may be obtain http://www.rfc-editor.org/info/rfc6749.

Copyright Notice

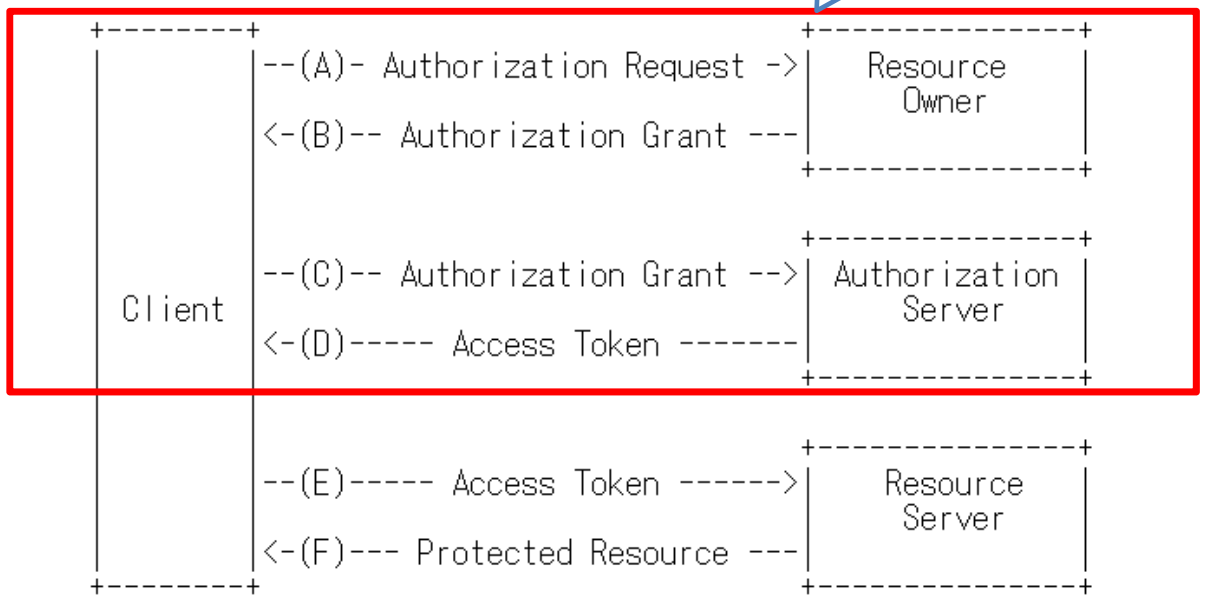
Copyright (c) 2012 IETF Trust and the persons i document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of

RFC 6749 OAuth 2.0

1.2. Protocol Flow

この認可トークンを得るまでの手順について、４種類の方法がある。



https://tools.ietf.org/html/rfc6749

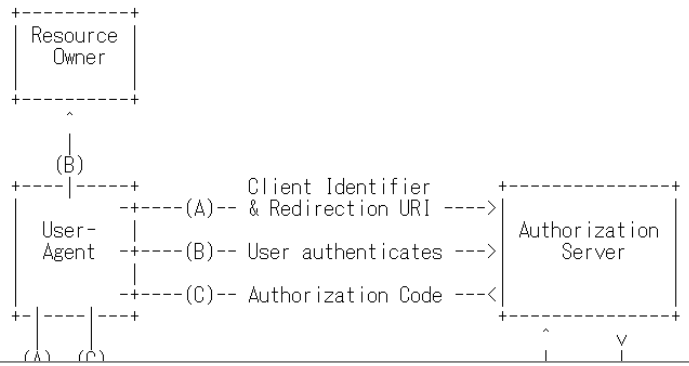
RFC 6749 The OAuth 2.0 Authorization Framework

4. Obtaining Authorization

To request an access token, the client obtains authorization from the resource owner. The authorization is expressed in the form of an authorization grant, which the client uses to request the access token. OAuth defines four grant types: authorization code, implicit, resource owner password credentials, and client credentials. It also provides an extension mechanism for defining additional grant types.

4.1. Authorization Code Grant

The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. Since this is a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.



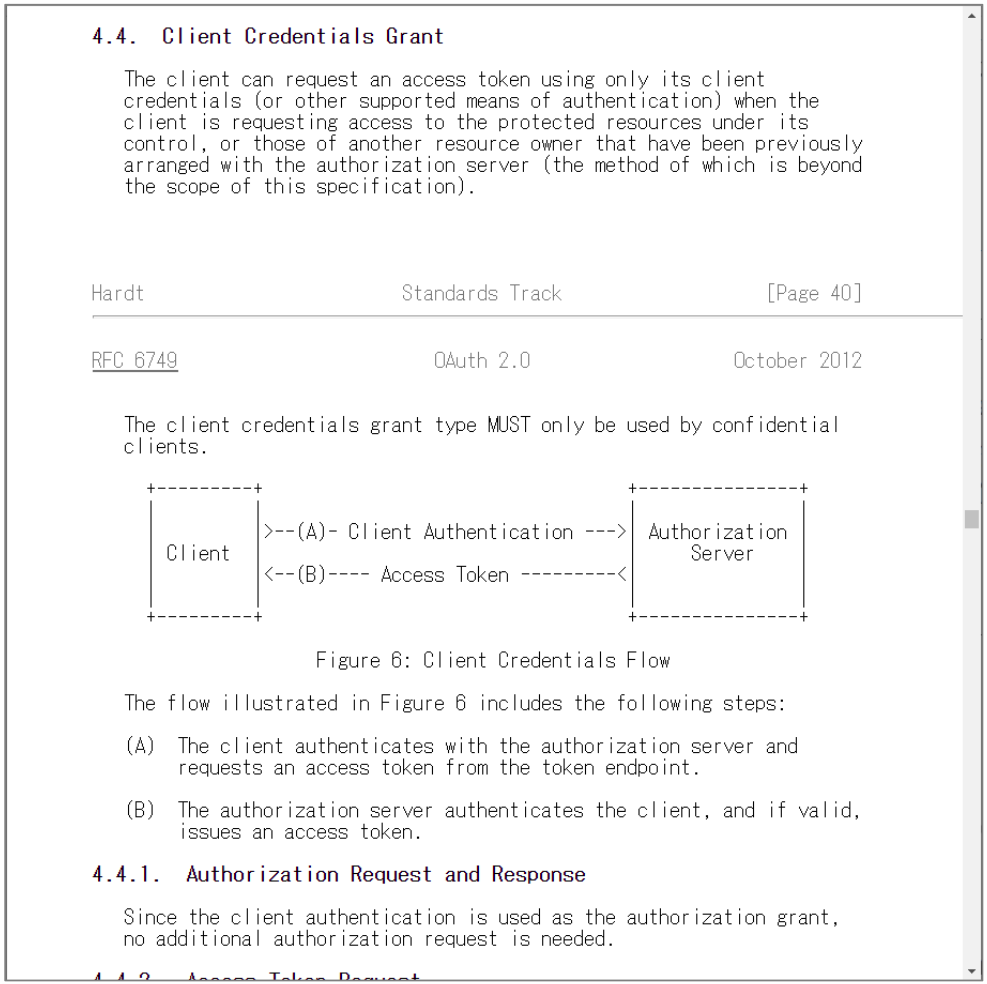
第４章に認可取得手順が解説されている。

1. 認可コード付与
2. インプリシット（暗黙的）付与
3. リソースオーナー パスワード クレデンシャルズ付与
4. クライアント クレデンシャルズ付与

IUAプロファイルの解説では一番単純な「手順４」を引き合いに出したいと思います。

https://tools.ietf.org/html/rfc6749

RFC 6749 The OAuth 2.0 Authorization Framework



4.4. Client Credentials Grant

The client can request an access token using only its client credentials (or other supported means of authentication) when the client is requesting access to the protected resources under its control, or those of another resource owner that have been previously arranged with the authorization server (the method of which is beyond the scope of this specification).

Hardt Standards Track [Page 40]

RFC 6749 OAuth 2.0 October 2012

The client credentials grant type MUST only be used by confidential clients.

Figure 6: Client Credentials Flow

The flow illustrated in Figure 6 includes the following steps:

(A) The client authenticates with the authorization server and requests an access token from the token endpoint.

(B) The authorization server authenticates the client, and if valid, issues an access token.

4.4.1. Authorization Request and Response

Since the client authentication is used as the authorization grant, no additional authorization request is needed.

4.4章 クライアント クレデンシャルズ付与
Clientが自身の制御化にある保護リソースに対しアクセスする、あるいは他のリソースオーナーが、認可サーバーを用いて事前にアクセスを実行しているような場合に、Client は自身の信頼性（または他の認証手段を伴い）トークン取得を依頼する。

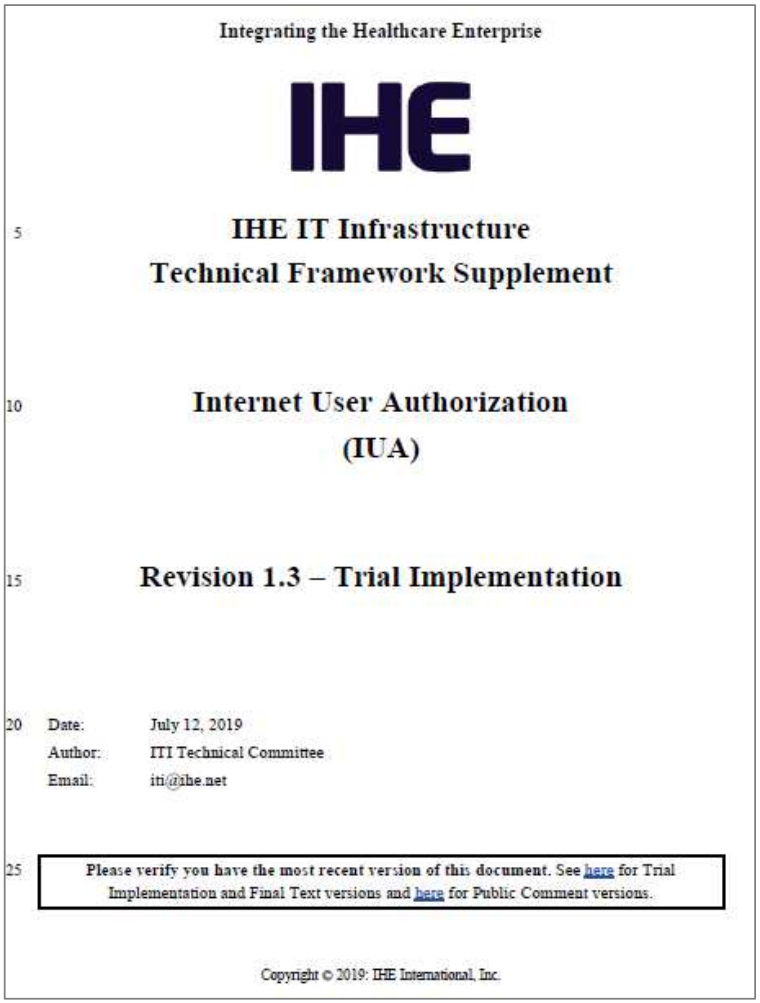
Qiita の OAuth の記事に４種類の認可取得手順について解説しているページがある。
「OAuth 2.0 全フローの図解と動画」
（URLはページ下部に記載）

手順４（クライアント クレデンシャルズ フロー）
については、
①アプリから認可サーバーに対するトークン取得要求
②認可サーバよりアプリにアクセストークンが付与
の流れが示されている。

https://tools.ietf.org/html/rfc6749 → https://qiita.com/TakahikoKawasaki/items/200951e5b5929f840a1f

OAuth を利用した IUAプロファイル

IUA (Internet User Authorization) Profile



Integrating the Healthcare Enterprise

IHE

IHE IT Infrastructure
Technical Framework Supplement

Internet User Authorization
(IUA)

Revision 1.3 – Trial Implementation

Date: July 12, 2019
Author: ITI Technical Committee
Email: iti@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Copyright © 2019: IHE International, Inc.

Volume 1- 34章 IUAプロファイル概要の記載

IUA プロファイルは HTTP RESTful 通信に対して認可情報を付与する。IUA の実装は、認可情報を必要とする他のプロファイルや通信に対して行われる（単独では実装されない）。

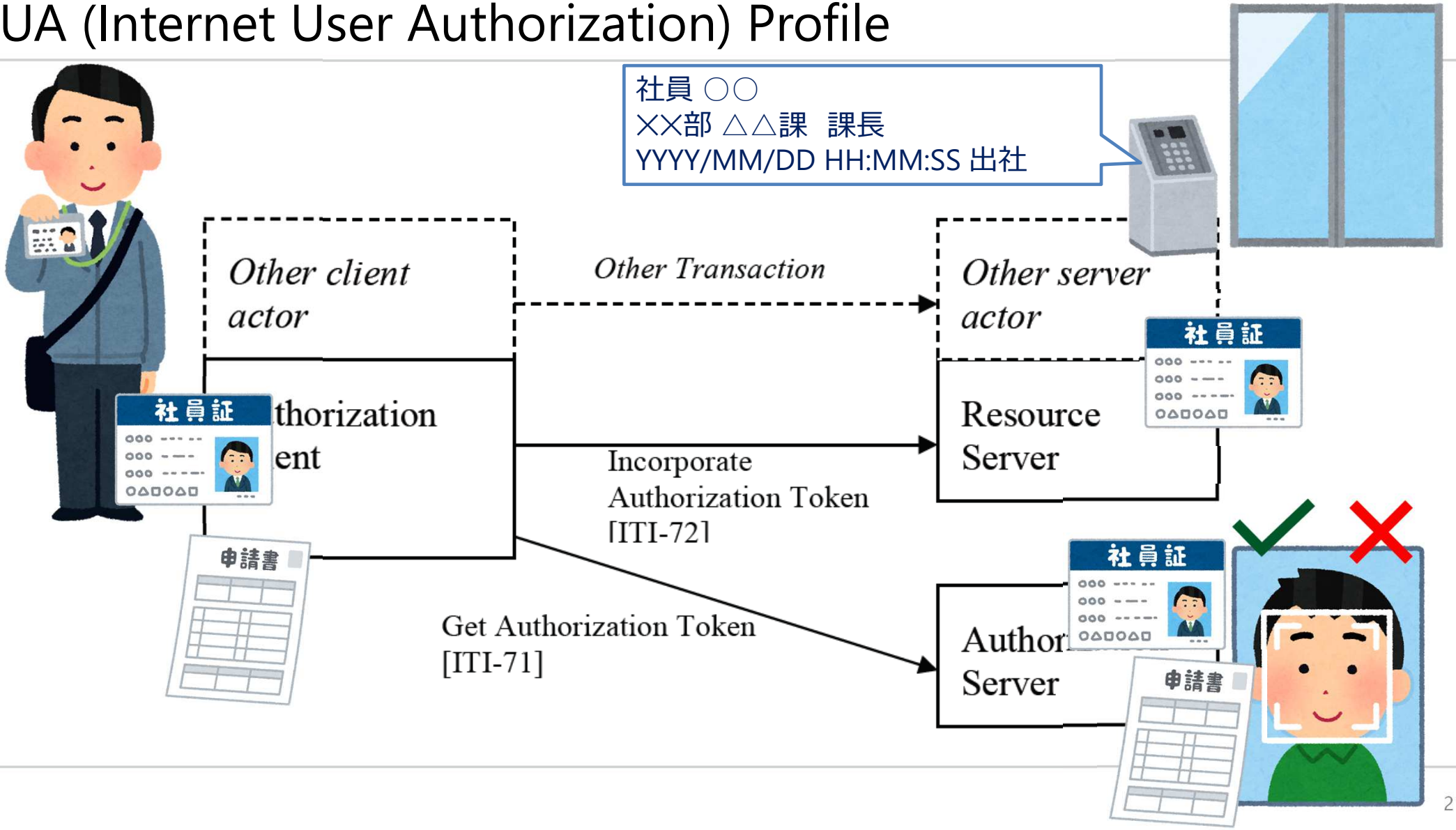
IUA では HTTP RESTful 通信上での認可情報として用いられるトークンを管理する。

クライアント側は HTTP RESTful通信に認可トークンを載せ、この通信は認可されている、ということを示す。また、認可トークンを獲得するため、認可サーバとの通信管理を行っている。

サービスサーバ側は HTTP RESTful要求が認可されているかを確認するための、サーバ側としての通信手順を提供し、無認可の通信要求をブロックする。認可された通信の場合、サービスサーバ側へのアクセス制御に用いるための情報を、認可トークンから提供する。

https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf

IUA (Internet User Authorization) Profile



RFC 6749 The OAuth 2.0 Authorization Framework

[Docs] [txt|pdf] [draft-ietf-oaut...] [Tracker] [Diff1] [Diff2] [IPR] [Errata]

Updated by: 8252 PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 6749
Obsoletes: 5849
Category: Standards Track
ISSN: 2070-1721

The OAuth 2.0 Authorization Fr

Abstract

The OAuth 2.0 authorization framework enables a application to obtain limited access to an HTTP behalf of a resource owner by orchestrating an between the resource owner and the HTTP service third-party application to obtain access on its specification replaces and obsoletes the OAuth in RFC 5849.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engi (IETF). It represents the consensus of the IET received public review and has been approved fo Internet Engineering Steering Group (IESG). Fu Internet Standards is available in Section 2 of

Information about the current status of this do and how to provide feedback on it may be obtain http://www.rfc-editor.org/info/rfc6749.

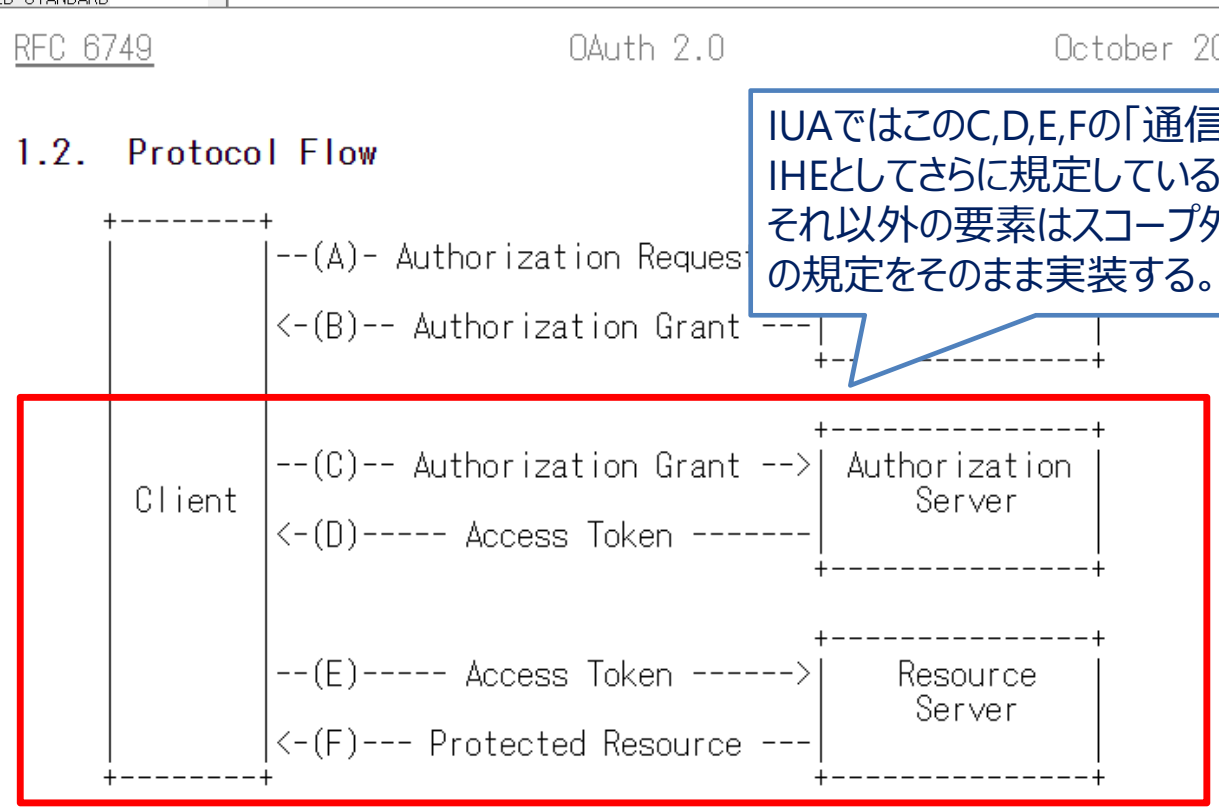
Copyright Notice

Copyright (c) 2012 IETF Trust and the persons i document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of

RFC 6749 OAuth 2.0 October 2012

1.2. Protocol Flow



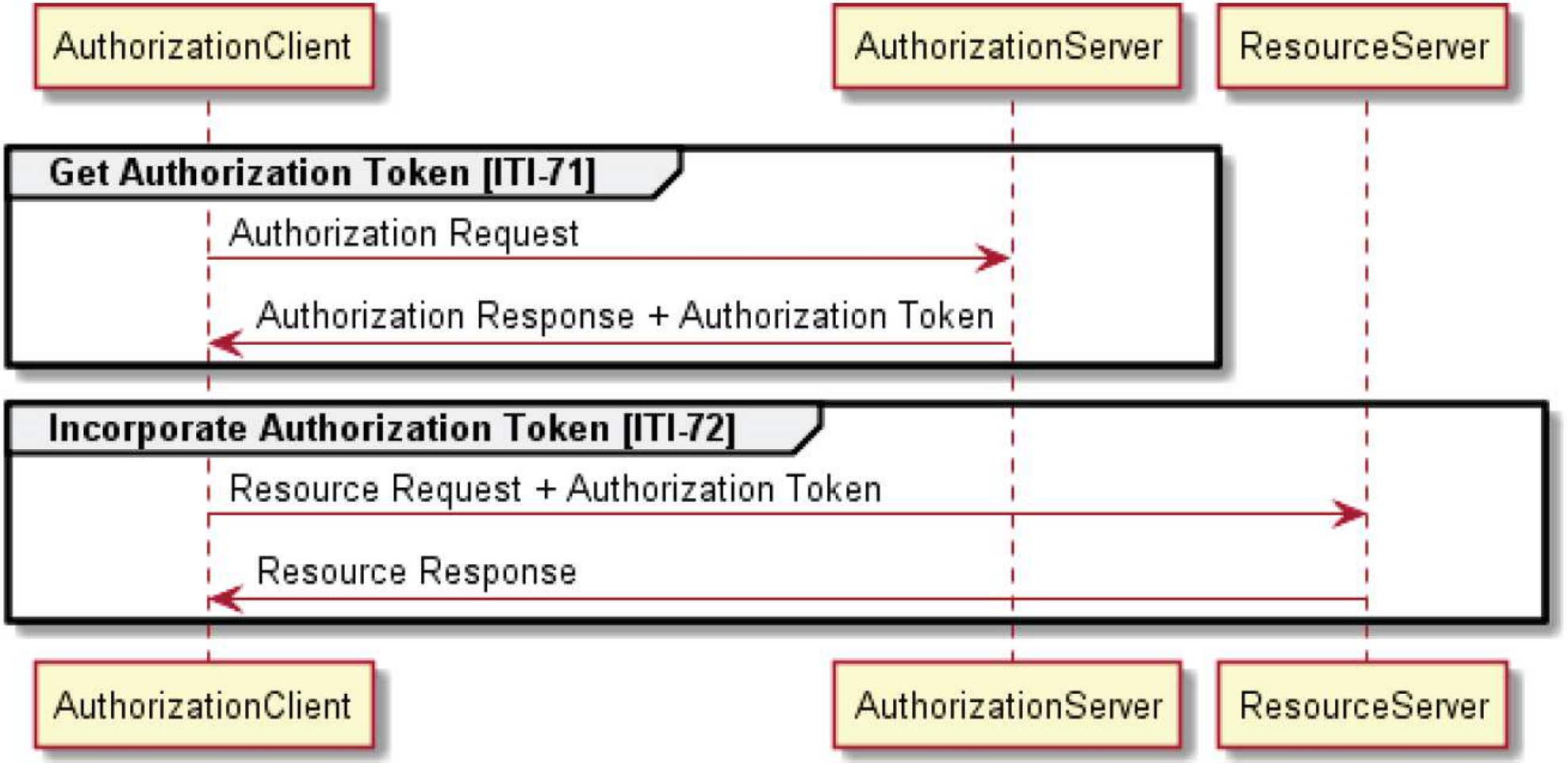
IUAではこのC,D,E,Fの「通信要件」を
IHEとしてさらに規定している。
それ以外の要素はスコープ外＝OAuth
の規定をそのまま実装する。

https://tools.ietf.org/html/rfc6749

IUA (Internet User Authorization) Profile

- HTTP RESTful 通信を行い、Authorization Client は内部トークンか、Authorization Server から得たトークンを、Resource Server にリクエストに付与して通知する。
- ユースケース：認可トークンを用いた Resource Serverへのリクエスト、認可の移譲（アプリ→装置、中継機能、上位組織など）、Authorization Server から認可トークンの取得。
- JWT（JSON Web Token）format は必須。その上で、SAML Token、あるいはOAuth Bearer Token（OAuth 2.0 framework）をオプションとして実装できる。
- 基本コンセプトは「認可」と「通信制御」で、権限付与、移譲、認証、認可、通信制御を含む。ただし、あくまで通信手順のみで、内部的な権限制御ロジックは対象外。
- Resourceサービスは Authorizationサービスを認識していることが前提。これらは一連のサービスとしてか、それぞれ別のサービスとして提供されているかは問わない。
- OAuth と OAuth RFCを機密性分析に用いる。ただし、OAuth 2.0の要である、client_id の管理を IUAでは規定しない。各アクターが独自にその機構を実装する。

IUA (Internet User Authorization) Profile Implementation



ITI-71 Get Authorization Token transaction

- Clientが必要時に HTTP GET で認可トークンを要求し、RESTful の応答で取得する。
- OAuth 2.0 RFC 6749 対応が必須。
- トークンは JWTを基礎とし、SAML または OAuth Bearerトークンをオプションで実装できる。JWS signed（draft-ietf-oauth-json-web-token, draft-ietf-oauth-jwt-bearer）／JWE unsigned but encrypted alternative を JWTとして実装する。
- JWTトークンの細かな要件は TFを参照のこと。ITI-40（XUAプロファイル）と基本は同じ。
- SAMLトークンオプションは、SAML 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants (RFC-draft-ietf-oauth-saml2-bearer) ルールに従う。
- OAuth Bearerトークンオプションは、RFC 6750 OAuth 2.0 Authorization Framework: Bearer Token Usage に従う。
- Client は OAuth confidential clientであることが、機密上求められる。Clientは別途 ATNA Secure Nodeか Secure Applicationを同時に実装が求められる場合がある。Server側のフォームはIHEでは規定しない。Client側は規定はするが必須ではない。

ITI-71 JSON Web Token (JWT) の要件

IHE JAPAN Integrating the Healthcare Enterprise

Table 3.71.4.1.2.1-1: JWT Token requirements

Parameter	Optionality	Definition	RFC Reference
iss	R	Issuer of token	Draft json-web-token Section 4
sub	R	Subject of token (e.g., user)	Draft json-web-token Section 4
aud	R	Audience of token	Draft json-web-token Section 4
exp	R	Expiration time	Draft json-web-token Section 4
nbf	O	Not before time	Draft json-web-token Section 4
iat	O	Issued at time	Draft json-web-token Section 4
typ	O	Type	Draft json-web-token Section 4
jti	R	JWT ID	Draft json-web-token Section 4

Table 3.71.4.1.2.1-2: Extensions to JWT Parameters

XUA Attribute	XUA Definition	JSON type	JWT Parameter
SubjectID	Plain text user's name	string	SubjectID
SubjectOrganization	Plain text description of the Organization	array of string	SubjectOrganization
SubjectOrganizationID		array of string	SubjectOrganizationID
HomeCommunityID	Home Community ID where request originated	string	HomeCommunityID
NationalProviderIdentifier		string	NationalProviderIdentifier
Provider-identifier	Other Provider Identifier Attribute	array of Instance Identifier objects	ProviderID
Subject:Role		array of Code objects	SubjectRole
docid	Patient Privacy Policy Acknowledgement Document ID	string	docid
acp	Patient Privacy Policy Identifier	string	acp
PurposeOfUse	Purpose of Use for the request	Code object	PurposeOfUse
Resource-ID	Patient ID related to the Patient Privacy Policy Identifier	string	resourceID
	Patient ID, Citizen ID, or other similar public ID used for health identification purposes.	string	personID

Table 3.71.4.1.2.1-3: JSON "Code" object definition

JSON attribute	Attribute type	Description
code	string	Mandatory. Code attribute shall contain the role code from the identified Value-Set that represents the role that the user is playing when making the request.
codeSystem	string	Mandatory. Specifies the code system (OID format) that defines the code.

Table 3.71.4.1.2.1-4: JSON "Instance Identifier" object definition

JSON attribute	Attribute type	Description
root	string	Mandatory. The "root" attribute shall contain an OID identifying the authority issuing the provider identifier.
extension	string	Mandatory. The "extension" attribute shall contain the provider identifier itself.

The following XUA subject role

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
 <saml:AttributeValue>
  <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001"
   codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT"
   displayName="Pharmacist"/>
 </saml:AttributeValue>
</saml:Attribute>
```

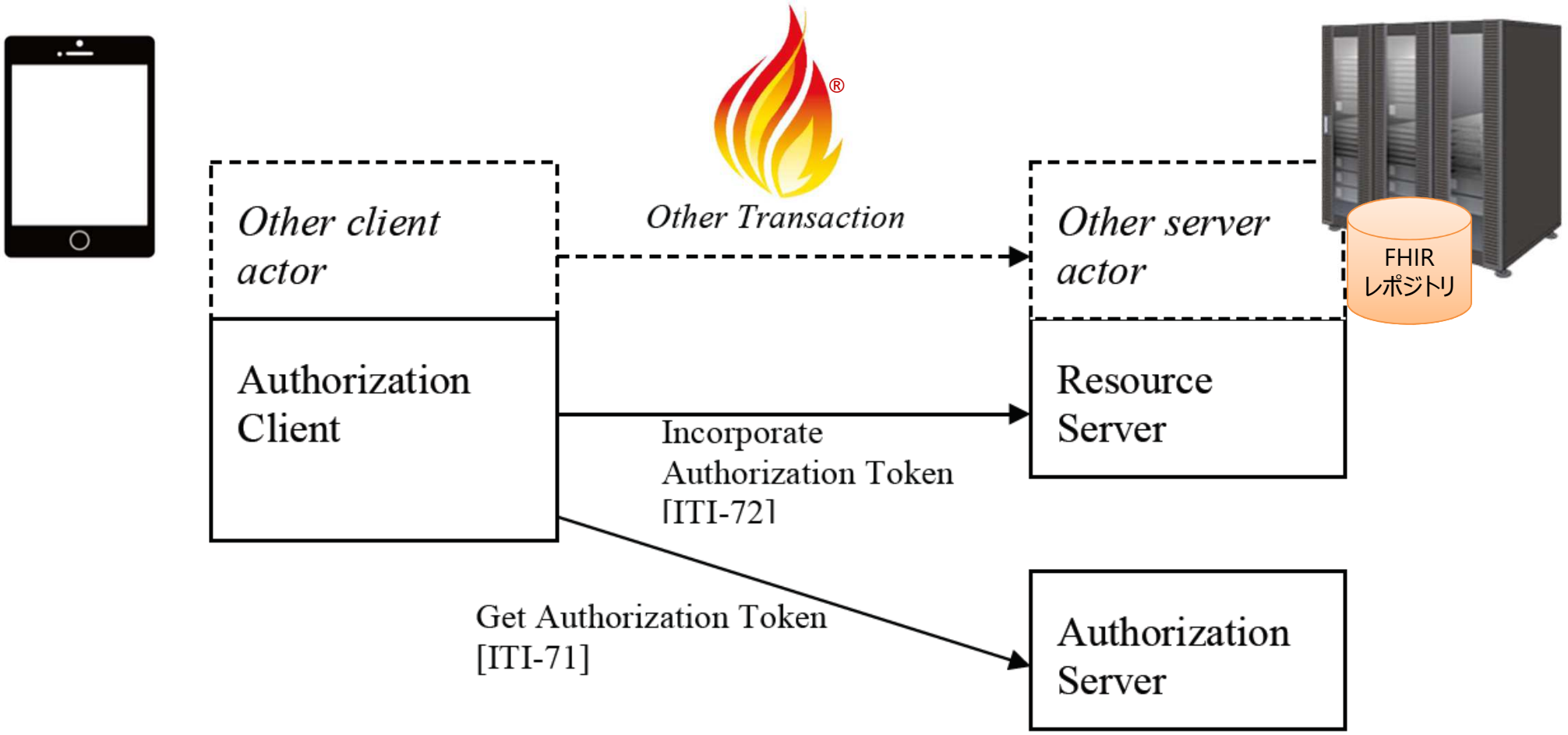
is expressed in a JWT token as an JSON array of Code objects:

```
"Subject:Role": [
      {
        "code": "46255001",
        "codeSystem": "2.16.840.1.113883.6.96"
      }
  ]
```

ITI-72 Incorporate Authorization Token

- Clientが必要時に HTTP RESTful 通信を認可トークン付きでリクエストし、認可確認をServer側に依頼する。確認後、本来の目的の通信を行うか、HTTP 401エラーを返す。
- トークンの有効性を先ず確認する。HTTPの Authorization: ヘッダーにトークン値を設定（RFC6750 Section 2.1）、それ以外のフィールド要件はトークンオプションに依存。
- SAMLトークンオプションの場合、XUAプロファイル要件と供にSAML要件の実装が必要。エンコードとして SAML 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants (RFC-draft-ietf-oauth-saml2-bearer) ルールに従う。
- OAuth Bearerトークンオプションは、RFC 6750 OAuth 2.0 Authorization Framework: Bearer Token Usage に従う。
- Client は OAuth confidential clientであることが、機密上求められる。Clientは別途ATNA Secure Nodeか Secure Applicationを同時に実装が求められる場合がある。
- Serverは JWTの確認をした際、ATNA監査通知上の alias”<“user”@”issuer”>” のコードが「UserName」に必要。JWT Tokenか SAML Tokenかによって設定値は異なる。

ところで、IUA Profile と FHIRとの関係性は？



IUA Profile の コネクタソン合格企業

		Authorization Client	Authorization Server	Resource Server
AGFA Healthcare				*
Epic Systems Corporation			*	*
Forcare BV		*	*	*
Hyland		*	*	*
INFINITT		*	*	*
INSIEL S.p.A		*		
InterSystems Corporation		*	*	*
IOD Incorporated		*		
IRM, Inc.		*	*	*
ITH icoserve technology for healthcare GmbH		*	*	*
Meddex		*	*	*
Parsek, d.o.o.		*	*	*
Siemens Healthineers		*	*	*
Systelab Technologies S.A.		*		
Thieme Compliance GmbH		*		
Tiani-Spirit Gmbh		*	*	*
Tiani "Spirit" GmbH - Cisco Systems Inc.		*	*	*
Tiani-Spirit Gmbh - Cisco Systems Inc.		*	*	*
VANAD Enovation			*	*
VISUS Health IT GmbH			*	*
Vital Images, Inc;		*		
x-tention/soffico			*	*

https://connectathon-results.ihe.net/view_result.php?rows=company&columns=actor&title=integration_profile

認証、認可、監査証跡に関する IHE プロファイル

CT（Consistency Time）

サーバーの時刻同期。認証、認可、監査証跡関連プロファイルの前提として必ず実装が必要。

ATNA（Audit Trail and Node Authentication）

患者情報や診療情報を取り扱う上での基本的なセキュリティ環境を提供する。

ユーザ認証や、接続認証、監査証跡情報に関するワークフローを規定する。

FHIRサポートのため、RESTful Query and Feed を追加。（Trial Implementation中）

EUA（Audit Trail and Node Authentication）

１ユーザ情報で複数のサーバやデバイスの認証を行う（シングルサインオン）。

Kerberos（RFC1510）、HL7 CCOWを使う。

XUA（Cross-Enterprise User Assertion）

別のシステムに対してアクセスする際に、認可されていることを示す情報を付与し、アクセス許可を判断してもらう。SAML 2.0 Identity Assertion を用いる。

IUA（Internet User Assertion）

トークンを用いた、HTTP RESTful通信上のアクセス許可確認のための手順。

最後に

医療情報 … 共有し活用してますか？

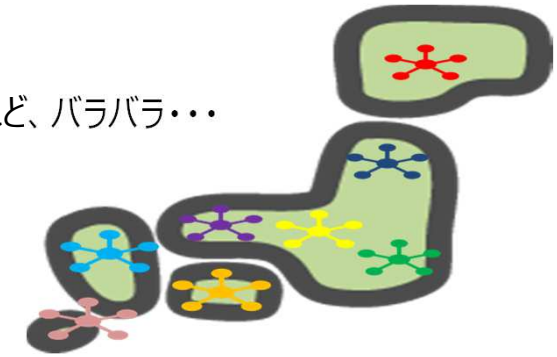
地域連携の仕組みは、全国で270箇所（2016年）存在*する！

* 厚生労働省　地域医療情報連携ネットワークの構築状況等調査結果（H28年度調査）より

では、それらを連携して情報共有したら、すごいことができる！？

⇒「医療IT」かけ声倒れ　診療データ共有、登録1%どまり **

** 日本経済新聞 電子版 2019年3月14日



令和の時代で医療情報の「調和」を実現しよう！

令和（れいわ）【意味】

人々が美しく心 化が生まれ育つ（首相官邸）

beautiful harmo 美しい調和：外務省）

医療情報の
高度な利活用

調和

既存の医療
情報システム

新たなニーズ
未達なニーズ

IHE JAPAN
Integrating the Healthcare Enterprise

ご清聴ありがとうございました。

参考情報（スライド作成に当り、要素、図等一部引用）

IHE International Official Site
https://www.ihe.net/

HL7 International Official Site
https://www.hl7.org/

OAuth 2.0 Official Site
https://oauth.net/2/

HL7 Project Gemini page
http://blog.hl7.org/another_type_of_moonshotproject_gemini

SMART on FHIR Official Site
https://docs.smarthealthit.org/

The NHS Website
https://www.nhs.uk/

HL7 FHIR Official Site
http://hl7.org/fhir/

参考情報（スライド作成に当り、要素、図等一部引用）

IHE Wiki - Profiles
https://wiki.ihe.net/index.php/Profiles

IHE IUA Profile Supplement Trial Implementation document
https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf

IHE Connectathon Results Browsing
https://connectathon-results.ihe.net/

Qiita OAuth OAuth 2.0 全フローの図解と動画（Authlete 社　川崎貴彦 様）
https://qiita.com/TakahikoKawasaki/items/200951e5b5929f840a1f

IHE活動の概要（スライド）
細羽 実, 日本IHE協会 副理事長, JCMI40 2020

IHE on FHIR（スライド）
Tone Southerland, Program Director, IQVIA; RSNA 2019

PULSE The Human Side of Innovation（スライド）
Eric Heflin, CTO/CISO Sequoia Project; NA Connectathon Conference 2019.01.23

参考情報（IUA 実装にあたってのサンプル、他）

4S - IHE-IUA Architecture

http://4s-online.dk/wiki/doku.php?id=net4care:security-component:ihe-iua

デンマークの団体サイト。IUAに関する概説をサンプル付きで紹介。

IHE Wiki - Guidance on writing Profiles of FHIR

https://wiki.ihe.net/index.php/Guidance_on_writing_Profiles_of_FHIR

FHIRを IHEプロファイルの規定で扱う際の内部的なガイドライン。考え方やツール類は使えるかもしれない。

※その他、IUAプロファイル系のサンプルは見つかりませんでした。基本的には実装は OAuthで提供しているモジュールを用いる形になりますので、OAuthの実装サンプル等を Qiita等でご確認くだされればと思います。