



トークンを用いた クラウド型情報交換技術仕様

文書番号： IHE-J-A-G0007

版番号： **2.2**

2024年8月20日

一般社団法人 日本 IHE 協会

改定履歴		
日付	バージョン	改定概要
2022/4/26	Draft	Draft 版作成
2022/5/19	1.0	初版発行
2022/7/6	1.1	タイトルを変更 9.2.に厚生労働省ガイドラインへの参照を追加 C.2.1.に施設コードに関する記述を追加
2023/4/17	2.0	タイトルおよび通称を変更 通信方式を変更等
2024/5/24	2.1	3 の引用規格を更新 7.2.3.2 にパスワードに関する記述を追加 8.1.2.2 の暗号化・復号に関する記述を変更 8.1.6.2 の Bundle リソースの定義を変更 Appendix D の Bundle リソース例を変更 Appendix E を追加 その他、表現の見直し及び記述の改善等
2024/8/20	2.2	4 の用語及び定義を更新 7.3 の表現の見直しおよび記述の改善 9.4 に参考資料を追加

目次

1	はじめに	4
2	適用範囲	4
3	引用規格	4
4	用語及び定義	5
5	略語	6
6	cloudPDI の概要	7
7	cloudPDI アクタとトランザクション	7
7.1	施設間の医療等情報転送サービス	7
7.2	アクタ	9
7.3	トランザクション	11
7.4	ユースケースとプロセスフロー	14
8	cloudPDI データ内容	15
8.1	交換データ	15
8.2	トークン	23
9	セキュリティに関する配慮事項	24
9.1	認証	24
9.2	通信路	24
9.3	トークン	24
9.4	監査証跡	24
Appendix A	PDI 形式データセットの概要	25
Appendix B	HI-TOKEN の例	26
Appendix C	アウトラインの例	27
Appendix D	cloudPDI FHIR Bundle の例	30
Appendix E	Repository への要求・応答の例	32
E.1.	Binary 提出時の要求・応答の例	32
E.2.	Bundle 提出時の要求・応答の例	32
E.3.	Bundle 取得時の要求・応答の例	33
E.4.	Binary 取得時の要求・応答の例	33

1 はじめに

地域医療連携情報システムの必要性がうたわれて久しいが、未だそれらのシステムが十分に普及したとは言えない状況である。特に交換する情報に画像を含む場合にはその大容量に由来する困難もある。そこで、導入のためのコストが低く利用しやすい情報連携基盤としてトークンを用いたクラウド型情報交換技術仕様（cloudPDI）を定める。

cloudPDIは、従来のCD・DVDを使った運用との併用が可能で業務の流れもほとんど変わらずに低コストで導入・運用ができ、PACS内の検査画像、SS-MIX2標準化ストレージ内の検査結果データ、処方データFHIR形式の厚生労働省標準化されたBundle文書等を送ることができる。また、平成28年度診療報酬改定の算定条件を満たしている。

交換する医療情報はリポジトリに一時格納するが、トークン（HI-TOKEN）を使用することでリポジトリの中からデータを一意に特定できるため、検索が不要であることを特長としている。

また、従来から画像等の大容量データを交換する際に標準的に使用されているPDIフォーマットを元データとして送信するため、既存システムとの互換性が高い。

通信には医療情報において国際的な標準となっているFHIRを用いる。

2 適用範囲

本技術仕様は、参加施設の情報システム間で患者の医療情報等を交換するのに必要な情報連携基盤の仕様を定めたものである。

3 引用規格

この技術仕様では以下の規格を参照する。

IHE Radiology (RAD) Technical Framework, Volume 1 Revision 21.0

IHE Radiology (RAD) Technical Framework, Volume 1x Revision 21.0

IHE Radiology (RAD) Technical Framework, Volume 2 Revision 21.0

IHE Radiology (RAD) Technical Framework, Volume 2x Revision 21.0

IHE 統合プロファイル「可搬型医用画像」およびその運用指針第一版（HELICS HS009 IHE 統合プロファイル「可搬型医用画像」およびその運用指針）

IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 20.0

IHE IT Infrastructure (ITI) Technical Framework, Volume 2 Revision 20.0

IHE IT Infrastructure (ITI) Technical Framework, Volume 3 Revision 20.0

ISO/TS 22691-2021 Health informatics —Token-based health information sharing

HL7 FHIR Release 4 (v4.0.1)

HL7J-CDA-005 診療情報提供書規格（医療機関への紹介状）1.00 （HELICS HS008 診療情報提供書（電子紹介状））

HL7J-CDA-007 HL7 CDAに基づく退院時サマリー規約 1.52(HELICS HS032 HL7 CDAに基づく退院時サマリー規約)

診療情報提供書 HL7 FHIR 記述仕様 1.01 （HELICS HS038 診療情報提供書 HL7 FHIR 記述

仕様)

退院時サマリー HL7 FHIR 記述仕様 1.01 (HELICS HS039 退院時サマリー HL7 FHIR 記述仕様)

HL7J-CDA-003 CDA 文書暗号化規格 ver. 1.02

RFC 4648 The Base16, Base32, and Base64 Data Encodings

RFC 6749 The OAuth 2.0 Authorization Framework

RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage

RFC 7519 JSON Web Token (JWT)

RFC 7591 OAuth 2.0 Dynamic Client Registration Protocol

RFC 7636 Proof Key for Code Exchange by OAuth Public Clients

RFC 8252 OAuth 2.0 for Native Apps

RFC 8259 The JavaScript Object Notation (JSON) Data Interchange Format

RFC 9068 JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

draft-ietf-oauth-security-topics-22 OAuth 2.0 Security Best Current Practice

FIPS PUB 180-4 Secure Hash Standard (SHS)

OpenID Connect 1.0

医療情報システムの安全管理に関するガイドライン 第 6.0 版

4 用語及び定義

4.1 交換データ

cloudPDI で交換できる医療情報のセット。検査結果、処方、画像、その他の FHIR ドキュメント等を含む。

4.2 PDI 形式データセット

交換データに含まれる複数のファイルを IHE PDI の規約にのっとり配置したもの。

4.3 cloudPDI データセット

PDI 形式データセットをアーカイブしさらに暗号化したもの。

4.4 cloudPDI データセット断片

cloudPDI データセットを分割したもの。

4.5 アウトライン

PDI 形式データセットの概要を一時的に表示するためのデータ。

4.6 暗号化済みアウトライン

アウトラインを暗号化したもの。

4.7 cloudPDI FHIR リソース

交換データをリポジトリに登録するための FHIR リソース。cloudPDI FHIR Binary と登録用 FHIR Bundle からなる。

4.8 cloudPDI FHIR Binary

交換データをリポジトリに登録するための FHIR リソース。cloudPDI データセット断片と

暗号化済みアウトラインからなる。

4.9 cloudPDI FHIR Bundle

交換データをリポジトリに登録するための FHIR リソース。cloudPDI FHIR Binary への参照を含む。

4.10 ドキュメント ID

cloudPDI データセットを一意に特定する識別子(OID)。

4.11 コミュニティ

同一のリポジトリを共有するサービスの単位。

4.12 コミュニティ ID

コミュニティを一意に特定する識別子(OID)。

4.13 HI-TOKEN

ドキュメント ID や、パスワード等を含む情報のセット。ISO/TS 22691 『Health informatics —Token-based health information sharing』 で定義されている。

4.14 Access Token

保護されたリソースへのアクセスに利用される資格情報。OAuth 2.0 で定義されている。

4.15 base64

データを印字可能な 64 種類の文字のみで表現するエンコード方式。RFC 4648 『The Base16, Base32, and Base64 Data Encodings』 で定義されている。

5 略語

IHE	Integrating the Healthcare Enterprise
ITI	Information Technology Infrastructure
TF	Technical Framework
HL7	Health Level 7
FHIR	Fast Healthcare Interoperability Resources
DICOM	Digital Imaging and Communications in Medicine
CDA	Clinical Document Architecture
ISO/TS	International Organization for Standardization/ Technical Specifications
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
PDI	Portable Data for Imaging
JSON	JavaScript Object Notation
JWT	JSON Web Token
PKCE	Proof Key for Code Exchange by OAuth Public Clients
PNG	Portable Network Graphics
JPEG	Joint Photographic Experts Group

6 cloudPDI の概要

cloudPDI とは、医療情報をインターネットで他施設に提供するサービスである。患者紹介・臨床検査などで必要な情報（診療情報提供書・画像・検査結果・処方（FHIR ドキュメント含む）など）を送受することができる。IHE PDI のファイルシステムを受領情報のコンテナとし、コンテナ受領用トークンは ISO/TS 22691-2021 『Health informatics —Token-based health information sharing』 で定められた HI-TOKEN を使用する。

提供する情報は、暗号化された上でリポジトリにアップロードされ、受信側は受領した HI-TOKEN に含まれるドキュメント ID とパスワードを用いてダウンロードおよび復号して利用する。パスワードは HI-TOKEN によってのみ保持伝達され、リポジトリには知らされない。

診療情報提供書に画像や検査結果を関連付けて提供することができる。

大量の DICOM 画像を送受することを考慮し、IHE PDI プロファイルに定めるファイル構造を採用しているが、画像は必須ではなく、診療情報提供書などの文書のみ、あるいはそれと検査結果のみといった運用も可能である。

データは新規登録のみであり、登録済みデータの変更はできない。またこの仕様では削除は規定しない。

7 cloudPDI アクタとトランザクション

7.1 施設間の医療等情報転送サービス

Figure 1 に施設間の医療等情報転送サービスのアクタとトランザクションを示す。

XDS レジストリ／リポジトリがまだ実装されていないか、情報交換に利用できない場合にも利用することが可能である。

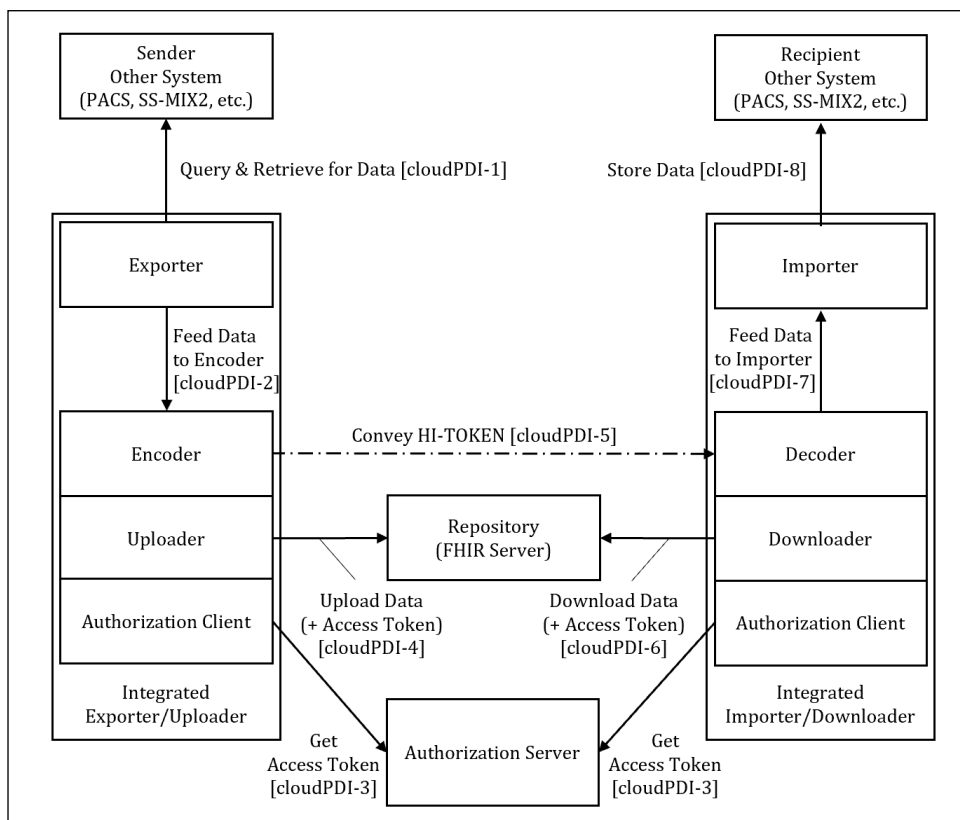


Figure 1 - 施設間の医療等情報転送サービスのアクタとトランザクション

標準的な利用方法は概略次のようなものである。

まず、送信施設では、ユーザーが **Exporter** の UI を使って施設内の PACS や SS-MIX2 標準化ストレージ、カルテなどの **Sender Other System** から提供したい情報を検索して指定する。**Exporter** は **Sender Other System** から指定された情報を取り出し、PDI 形式データセットを作成して **Uploader** に渡す。

Uploader は、ドキュメント ID とパスワードが含まれた **HI-TOKEN** を発行する。**HI-TOKEN** は患者に渡される。

Uploader はまた **Exporter** から受け取った PDI 形式データセットをアーカイブしたうえでパスワードで暗号化して **HI-TOKEN** に記載されたドキュメント ID で **Repository** に登録する。

患者が紹介先に **HI-TOKEN** を持って行くと、紹介先施設では **Downloader** で **HI-TOKEN** を読み取り、この中に書かれたドキュメント ID で **Repository** からデータを取得し、またパスワードで復号して **Importer** に渡す。

インポーターはデータを適合化（患者 ID の付け替えなど）を行った後、施設内の PACS、SS-MIX2 標準化ストレージ、カルテなどの **Recipient Other System** に格納する。

7.2 アクタ

Table 1 に、cloudPDI の仕様に含まれるアクタのそれぞれに対するトランザクション ("R"は必須、"O"はオプション) を示す。

Table 1 - cloudPDI アクタ/トランザクション

Actors	Transactions	Initiator or Responder	Optionality	Reference
Sender Other System	Query & Retrieve for Data [cloudPDI-1]	Responder	R	7.3.1
Exporter	Query & Retrieve for Data [cloudPDI-1]	Initiator	R	7.3.1
	Feed Data to Uploader [cloudPDI-2]	Initiator	R	7.3.2
Uploader	Feed Data to Uploader [cloudPDI-2]	Responder	R	7.3.2
	Convey HI-TOKEN [cloudPDI-5]	Initiator	R	7.3.5
	Get Access Token [cloudPDI-3]	Initiator	R	7.3.3
	Upload Data [cloudPDI-4]	Initiator	R	7.3.4
Repository	Upload Data [cloudPDI-4]	Responder	R	7.3.4
	Download Data [cloudPDI-6]	Responder	R	7.3.6
Downloader	Convey HI-TOKEN [cloudPDI-5]	Responder	R	7.3.5
	Get Access Token [cloudPDI-3]	Initiator	R	7.3.3
	Download Data [cloudPDI-6]	Initiator	R	7.3.6
	Feed Data to Importer [cloudPDI-7]	Initiator	O	7.3.7
Importer	Feed Data to Importer [cloudPDI-7]	Responder	R	7.3.7
	Store Data [cloudPDI-8]	Initiator	R	7.3.8
Recipient Other System	Store Data [cloudPDI-8]	Responder	R	7.3.8
Integrated Exporter/Uploader	Query & Retrieve for Data [cloudPDI-1]	Initiator	R	7.3.1
	Convey HI-TOKEN [cloudPDI-5]	Initiator	R	7.3.5
	Get Access Token [cloudPDI-3]	Initiator	R	7.3.3
	Upload Data [cloudPDI-4]	Responder	R	7.3.4
Integrated Importer/Downloader	Convey HI-TOKEN [cloudPDI-5]	Responder	R	7.3.5
	Get Access Token [cloudPDI-3]	Initiator	R	7.3.3
	Download Data [cloudPDI-6]	Initiator	R	7.3.6
	Store Data [cloudPDI-8]	Initiator	O	7.3.8
Authorization Server	Get Access Token [cloudPDI-3]	Responder	R	7.3.3

以下の項でアクタについて説明する。

7.2.1 Sender Other System

提供施設の医療情報を格納するシステムである。たとえば PACS, SS-MIX2 標準化ストレージ、電子カルテシステムなどがこれに相当する。

7.2.2 Exporter

Exporter は通常、ユーザーが提供したい医療情報を Sender Other System から検索・指定する UI を持つ。Exporter はユーザーが指定した情報を Sender Other System から取り出し、PDI 形式データセットとして整形する。また PDI 形式データセットの内容の概要を示すアウトラインを生成し、PDI 形式データセットと合わせて Uploader に与える。

7.2.3 Uploader

PDI 形式データセットを Exporter から受け取ると、交換データを暗号化し Repository に提出する。また交換データに対応する HI-TOKEN を生成する。

7.2.3.1 ドキュメント ID の生成

cloudPDI データセットを一意に特定する id であるドキュメント ID を生成する。

7.2.3.2 パスワードの生成

交換データを暗号化・復号するパスワードを生成する。

パスワードは固定値"01."と 36 種の文字 (0~9, A~Z) による 25~61 桁からなる任意の文字列を順に連結した計 28~64 桁の文字列とする。

固定値を除いた任意の文字列は、使い回しをしない乱数等を用いて生成する。

パスワード例: 01.RV81OC9QCYUUC6VPEPQRLCK9YOVTTBWKTGW

7.2.3.3 HI-TOKEN の生成

ドキュメント ID とパスワードを、コミュニティ ID と合わせてトークン (HI-TOKEN) を生成する。

7.2.3.4 cloudPDI データセットと暗号化済みアウトラインの生成

Exporter から与えられた PDI 形式データセットをアーカイブしたうえパスワードで暗号化し cloudPDI データセットを生成する。またアウトラインをパスワードで暗号化して暗号化済みアウトラインを生成する。

7.2.3.5 cloudPDI FHIR リソースの生成と提出

cloudPDI データセットおよび暗号化済みアウトラインから cloudPDI FHIR Binary を生成し、またそれらを統合する cloudPDI FHIR Bundle を生成したうえ、それらを Repository に提出する。

Uploader は、提出先となる Repository が指定する一度の HTTP リクエストで受信できるデータの最大サイズを超えないように留意して cloudPDI データセット断片および cloudPDI FHIR Binary を生成する必要がある。

cloudPDI FHIR リソースの内容は 8.1.6 cloudPDI FHIR リソースに示す。

7.2.4 Repository

提供するデータを一時的に保管する FHIR サーバー。

Uploader から送られる cloudPDI FHIR リソースを受信して保存する。また、Downloader の求

めに応じてドキュメント ID によって特定された cloudPDI FHIR リソースを送信する。一度の HTTP リクエストで受信できるデータの最大サイズは Uploader に対して通知する。通知の方法はこの仕様では規定しない。

7.2.5 Downloader

HI-TOKEN を読み取り（たとえば QR コードをスキャンするなどの方法で）、HI-TOKEN から取り出したドキュメント ID およびパスワードを使って Repository から交換データを取得する。

7.2.5.1 cloudPDI FHIR リソースの取得

受領した HI-TOKEN から取り出したドキュメント ID を使って Repository から cloudPDI FHIR リソースを取得する。

7.2.5.2 cloudPDI データセットと暗号化済みアウトラインの生成

取得した cloudPDI FHIR Bundle、cloudPDI FHIR Binary から cloudPDI データセットおよび暗号化済みアウトラインを生成する。

cloudPDI FHIR リソースの内容は 8.1.6 cloudPDI FHIR リソースに示す。

7.2.5.3 cloudPDI データセットおよび暗号化済みアウトラインの復号

受領した HI-TOKEN から取り出したパスワードを使って cloudPDI データセットおよび暗号化済みアウトラインを復号して、それぞれ PDI 形式データセットとアウトラインを得る。また得られた PDI 形式データセットを Importer に与える。

7.2.6 Importer

Downloader から与えられた PDI 形式データセットを適合化（患者 ID を自施設のものに書き換えるなど）したうえで Recipient Other System にそれぞれの方法で登録する。

7.2.7 Recipient Other System

受領施設の医療情報を格納するシステム。たとえば PACS, SS-MIX2 標準化ストレージ、電子カルテシステムなどがこれに相当する。

7.2.8 Integrated Exporter/Uploader

Exporter と Uploader は統合してよい。その場合その間の Transaction は任意の方法で置き換えてよい。

7.2.9 Integrated Importer/Downloader

Importer と Downloader は統合してよい。その場合その間の Transaction は任意の方法で置き換えてよい。

7.2.10 Authorization Server

Uploader、Downloader からの求めに応じて RFC 6749 『The OAuth 2.0 Authorization Framework』の定める Authorization Server として操作者を認証し、Repository へのアクセス時に使用する Access Token を発行し送信する。Access Token の形式は RFC 9068 『JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens』に従う。

7.3 トランザクション

以下の項で各トランザクションのプロトコルとコンテンツを説明する。

7.3.1 Query & Retrieve for Data [cloudPDI-1]

Sender Other System から検査結果、処方、画像その他のデータを取得する。

DICOM Query/Retrieve や SS-MIX2 標準化ストレージが利用可能である。他の方法で実現してもよい。

7.3.2 Feed Data to Uploader [cloudPDI-2]

USB 等の可搬媒体、ローカルエリアネットワーク等によって PDI 形式データセットおよびアウトラインを転送する。

転送方法はファイル共有が利用可能である。他の方法で実現してもよい。

7.3.3 Get Access Token [cloudPDI-3]

RFC 6749 『The OAuth 2.0 Authorization Framework』の仕様に従い、Uploader、Downloader からの求めに応じて Authorization Server が Access Token を送信する。

7.3.3.1 Authorization Code Flow の利用

Authorization Code Flow を利用し Repository の利用認可を得る。

Access Token のリクエストのパラメータには以下の内容を含める。

response_type: code

Authorization Server は利用認可を発行するにあたって利用者を認証する。

7.3.3.2 PKCE の利用

RFC 7636 『Proof Key for Code Exchange by OAuth Public Clients』の仕様に従って、PKCE を利用する。

7.3.3.3 JWT 形式 Access Token の利用

Authorization Server は RFC 9068 『JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens』の仕様に従って、JWT 形式の Access Token を発行する。

7.3.3.4 認可付与のポリシー

Access Token のリクエストにおける scope の内容および、各利用者にとどのようなアクセス権を与えるかのポリシーについてはこの仕様では規定しない。

7.3.4 Upload Data [cloudPDI-4]

安全管理ガイドライン^{※1}に適合したネットワークのセキュアな通信により cloudPDI FHIR リソースを提出する。

cloudPDI FHIR リソースのそれぞれのサイズが提出先の Repository が一度の HTTP リクエストで受信できるデータの最大サイズを超える時には、cloudPDI データセットを分割して提出する。分割の方法は 7.3.4.2 cloudPDI FHIR Binary の生成および 8.1.3 cloudPDI データセット断片に示す。

※1 安全管理ガイドライン: 厚生労働省『医療情報システムの安全管理に関するガイドライン 第 6.0 版』「システム運用編 1.3. ネットワークに関する安全管理措置 [I、III]」

7.3.4.1 Access Token の利用

Uploader は cloudPDI FHIR リソースを Repository に提出するにあたって、Get Access Token[cloudPDI-3]により Authorization Server から Access Token を取得する。以降の FHIR に

よる通信の際には RFC 6750 『The OAuth 2.0 Authorization Framework: Bearer Token Usage』に従いこの Access Token を送信する。

この Access Token を受け取った Repository は RFC 9068 『JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens』 4.Validating JWT Access Tokens に従い Access Token を検証する。また Access Token に含まれる各 claim から認証情報を取得する。

7.3.4.2 cloudPDI FHIR Binary の生成

cloudPDI データセットを任意の数に分割したものおよび暗号化済みアウトラインをそれぞれその内容とする cloudPDI FHIR Binary を生成する。

cloudPDI データセットを分割するときには、生成された cloudPDI FHIR Binary のサイズがそれぞれ提出先となる Repository が指定する一度の HTTP リクエストで受信できるデータの最大サイズを超えないようにする必要がある。

cloudPDI FHIR Binary の内容は 8.1.6.1 cloudPDI FHIR Binary に示す。

7.3.4.3 cloudPDI FHIR Binary の提出

cloudPDI FHIR Binary として生成されたものをすべて FHIR の create インタラクションで Repository に提出しそれぞれの URL を取得する。

update インタラクションは使用しない。

Appendix E E.1 に Binary 提出時の要求・応答の例を示す。

7.3.4.4 cloudPDI FHIR Bundle の生成

7.3.4.3 で得られた URL をリストとして列挙し cloudPDI FHIR Bundle を生成する。cloudPDI FHIR Bundle の内容は 8.1.6.2 cloudPDI FHIR Bundle に示す。

7.3.4.5 cloudPDI FHIR Bundle の提出

7.3.4.4 で得られた cloudPDI FHIR Bundle を FHIR の update インタラクションで Repository に提出する。この際の id にはドキュメント ID を使用する。

登録済みドキュメント ID に対する update インタラクションは使用しない。Repository は登録済みドキュメント ID に対する update インタラクションの要求には応じない。

この要求を受けた Repository は、cloudPDI FHIR Bundle に含まれる要素を検証し、不正や参照先の cloudPDI FHIR Binary が存在しない等の不整合がある場合は要求に応じない。

Appendix E E.2 に Bundle 提出時の要求・応答の例を示す。

7.3.5 Convey HI-TOKEN [cloudPDI-5]

コンテンツは ISO/TS 22691 『Health informatics —Token-based health information sharing』に準じたトークン。

運搬は紙媒体、可搬型媒体、モバイルデバイス、あるいはセキュアなネットワークによる。他の方法で実現してもよい。

7.3.6 Download Data [cloudPDI-6]

安全管理ガイドライン^{※1}に適合したネットワークのセキュアな通信により cloudPDI FHIR リソースを取得する。

※1 安全管理ガイドライン: 厚生労働省『医療情報システムの安全管理に関するガイドライン 第 6.0 版』「システム運用編

1.3. ネットワークに関する安全管理措置 [I、III]

7.3.6.1 Access Token の利用

Downloader は cloudPDI FHIR リソースを Repository から取得するにあたって、Get Access Token [cloudPDI-3]により Access Token を取得する。以降の FHIR による通信の際には RFC 6750 『The OAuth 2.0 Authorization Framework: Bearer Token Usage』に従いこの Access Token を送信する。

この Access Token を受け取った Repository は RFC 9068 『JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens』 4.Validating JWT Access Tokens に従い Access Token を検証する。また Access Token に含まれる各 claim から認証情報を取得する。

7.3.6.2 cloudPDI FHIR Bundle の取得

Convey HI-TOKEN [cloudPDI-5]により受領したトークンから取得したドキュメント ID を id として FHIR の read インタラクションで Repository から cloudPDI FHIR Bundle を取得する。search インタラクションは使用しない。

Appendix E E.3 に Bundle 取得時の要求・応答の例を示す。

7.3.6.3 cloudPDI FHIR Binary の取得

7.3.6.2 で取得した cloudPDI FHIR Bundle の内容から cloudPDI データセット断片および暗号化済みアウトラインを構成する cloudPDI FHIR Binary の URL を取得し、それぞれを FHIR の read インタラクションで取得する。

cloudPDI FHIR Bundle の構造は 8.1.6.2 cloudPDI FHIR Bundle に示す。

Appendix E E.4 に Binary 取得時の要求・応答の例を示す。

7.3.6.4 cloudPDI データセットの再構成

7.3.6.3 で得られた cloudPDI FHIR Binary 中の cloudPDI データセット断片を結合し cloudPDI データセットを再構成する。cloudPDI データセットの再構成の手順は 8.1.3.2 cloudPDI データセットへの復元方法に示す。

7.3.7 Feed Data to Importer [cloudPDI-7]

USB 等の可搬媒体、ファイアウォール等を介したセキュアな通信により PDI 形式データセットを転送する。

転送方法はファイル共有が利用可能である。他の方法で実現してもよい。

7.3.8 Store Data [cloudPDI-8]

Recipient Other System へ検査結果、処方、画像その他の医療情報を登録する。

DICOM Store や SS-MIX2 標準化ストレージが利用可能である。他の方法で実現してもよい。

7.4 ユースケースとプロセスフロー

7.4.1 施設間の医療等情報転送サービス

Figure 2 に施設間の医療等情報転送サービスにおける処理の流れを示す。

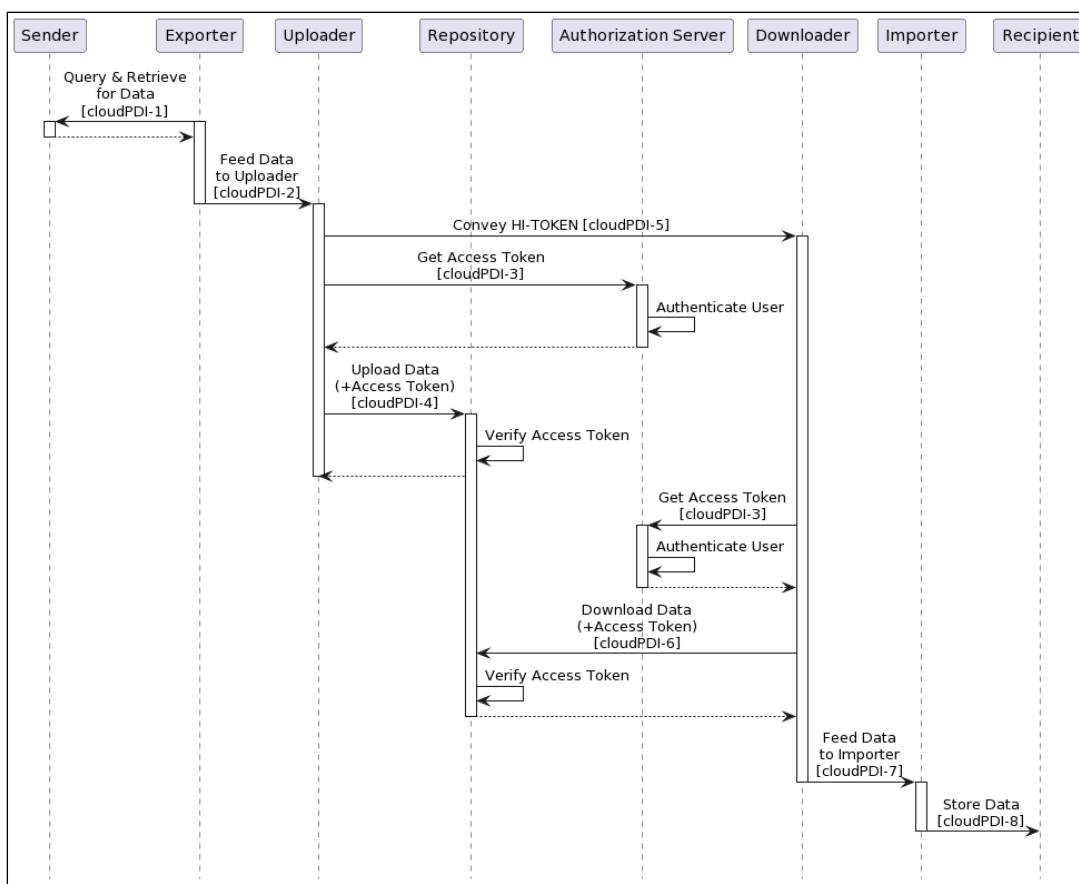


Figure 2 - 施設間の医療等情報転送サービスのプロセスフロー

note: [cloudPDI-5]は [cloudPDI-4]の後に実行してもよい

以下のようなケースで利用できる。

- ・ 紹介元から診療情報提供書に付帯する画像と検査データを送る
- ・ 医療機関から退院時に紹介先に診療情報提供書や退院時サマリー等を送る
- ・ 医療機関が画像検査センターへ検査依頼した画像撮影結果を依頼元医療機関に送る

8 cloudPDI データ内容

8.1 交換データ

8.1.1 PDI形式データセット

交換データは一般に複数のファイルから構成されるが、そのファイル群はPDI形式データセットとして配置する。

PDI形式データセットは、『HELICS HS009 IHE 統合プロファイル「可搬型医用画像」およびその運用指針』に定義される仕様に準拠して構成する。

ただし、検体検査結果、処方、診療情報提供書などの文書(FHIR ドキュメントも含む)、DICOM以外の画像などは、Other Files の部分に格納する。DICOM 画像がない場合は、DICOMDIR, Directory of DICOM files が存在しなくてもよい。

Appendix A に PDI 形式データセットの概要を示す。

8.1.2 cloudPDI データセット

PDI 形式データセットとして配置された複数のサブフォルダー・ファイルを一つのファイルに圧縮してまとめ、これを暗号化する。

圧縮および暗号化・復号の方法を以下に示す。

8.1.2.1 圧縮の方法

PDI 形式データセットを構成するファイル群を、ZIP 圧縮アルゴリズムを用いて 1 つのファイルにする。ZIP 圧縮の対象として PDI 形式データセットを配置した際のルートフォルダは含めない。

ZIP 圧縮アルゴリズムは「無圧縮」または「DEFLATE」とし、どちらを利用するかは各システムで任意に決定してよい。但し、受信側はどちらの ZIP 圧縮アルゴリズムであっても展開できなければならない。

8.1.2.2 暗号化・復号の方法

PDI 形式データセットを圧縮して 1 ファイル化したものを暗号化する。

暗号技術は『電子政府における調達のために参照すべき暗号のリスト (CRYPTTEC 暗号リスト)』における「共通鍵暗号、128 ビットブロック暗号」の AES 暗号アルゴリズムを用いて暗号化する。

CRYPTREC 暗号リスト: <https://www.cryptrec.go.jp/list.html>

AES 暗号アルゴリズムの設定について、暗号モードは「CBC」、キー長は「256bit」、ブロックパディング方式は「PKCS7」を用いる。

暗号キー、初期ベクトルの導出方法を以下に示す。

暗号キーはパスワードを SHA-256^{*1} でハッシュ化して生成する。

※1: 『FIPS PUB 180-4 Secure Hash Standard (SHS)』

初期ベクトルは暗号キーを SHA-256 でハッシュ化して生成されたハッシュ値の先頭 128bit を取得した値とする。

パスワードから導出した暗号キー、初期ベクトルの例 (それぞれ bit 列を 16 進法で表現したもの) を示す。

パスワード例: 01.0123456789ABCDEFGHIJKLMNOPQRS

暗号キー: 91ddf4c90a403a086ab195242bc398dac8814d4679976b03bb0286ce88adfa66

初期ベクトル: 264c43e44bec0d3c5418ffbb08df85f9

暗号化処理ロジックのイメージを Figure 3 に示す。

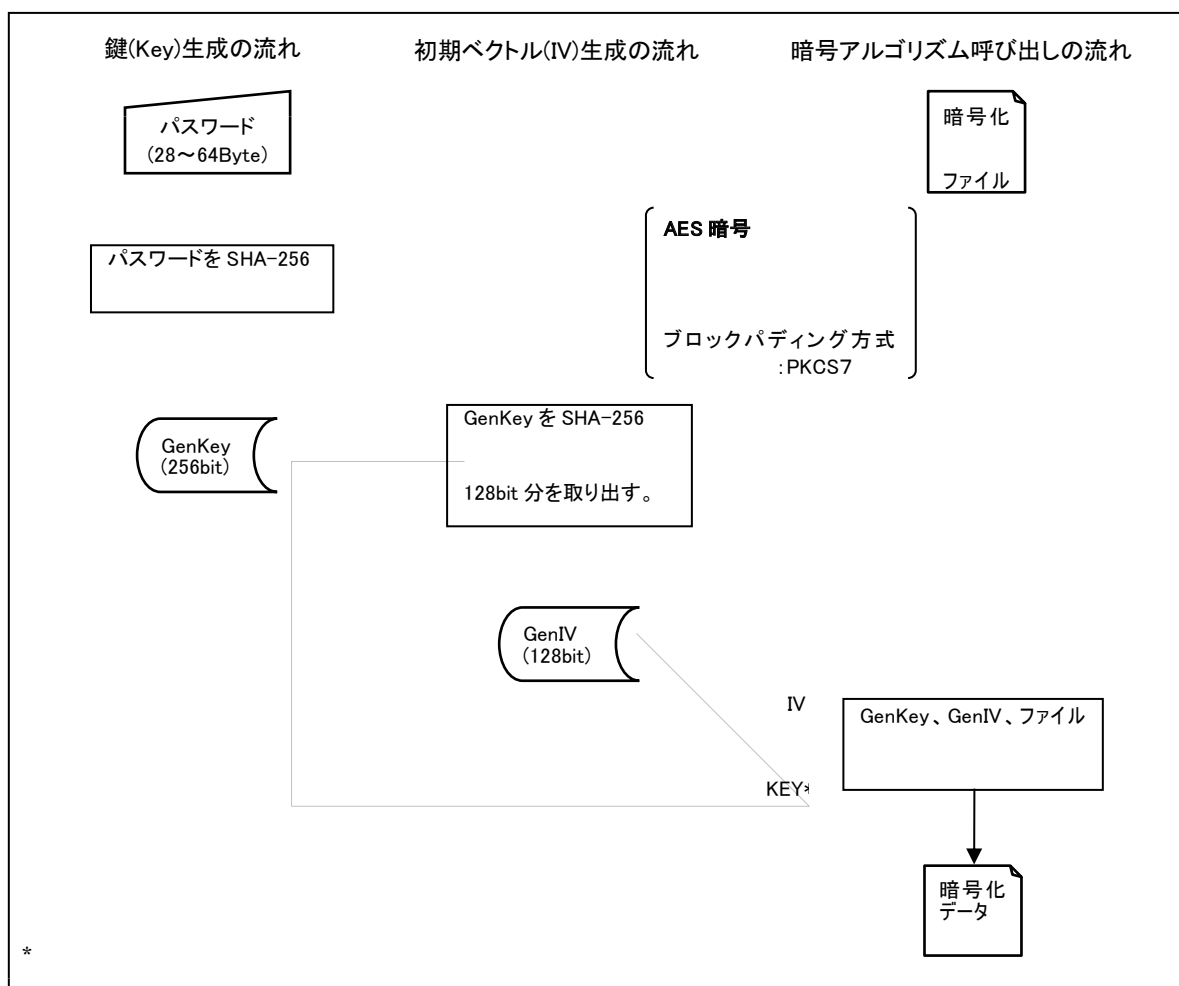


Figure 3 - 暗号化処理ロジックのイメージ

復号処理は、暗号化と逆の処理ロジックで元の PDI 形式データセットに展開する。

8.1.3 cloudPDI データセット断片

cloudPDI データセットは任意の長さの一つ以上の部分に分割して cloudPDI データセット断片とする。

8.1.3.1 cloudPDI データセット断片の生成方法

cloudPDI データセットを先頭から順に任意の長さで切り出して各断片を生成する。各断片の長さおよび断片間の順序その他の情報は各断片内には付加しない。

8.1.3.2 cloudPDI データセットへの復元方法

各断片の長さおよび断片間の順序に従って、各断片を結合して cloudPDI データセットを生成する。

各断片の長さは cloudPDI FHIR Binary の長さを、断片間の順序は cloudPDI FHIR Bundle の該当する entry 内に配置されている順序を利用する。

8.1.4 アウトライン

PDI 形式データセットの内容の概要を記述したファイル。JSON 形式で記述する。文字符号化形

式は UTF-8 とする。バイト順マーク (BOM) は付与しない。
各要素の要素名、多重度、型、値および説明を以下の表に示す。

Table 2 - アウトラインの要素

要素	多重度	型	値	説明
Version	1..1	文字列	"1"	アウトラインの定義のバージョン
Creator	1..1	Creator オブジェクト		交換データ作成施設の情報
CreationInformation	1..1	CreationInformation オブジェクト		交換データ作成情報
Patient	1..1	Patient オブジェクト		交換データに含まれる患者情報
Contents	0..*	Contents オブジェクト		交換データに含まれる内容のリスト

Table 3 - Creator オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Code	1..1	文字列		作成施設の医療機関コード 必要に応じて他のコードを利用してもよい
Name	1..1	文字列		施設名
Contact	1..1	文字列		連絡先 形式は任意
Logo	0..1	文字列		作成施設のロゴ画像 ロゴ画像の PNG ファイルの内容全体を base64 でエンコードして格納する

Table 4 - CreationInformation オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
DateTime	1..1	文字列		交換データを作成した日時 YYYY-MM-DDThh:mm:ss+zz:zz の形式で 表現する 例: 2020-06-10T17:07:00+09:00 この例は西暦 2020 年 6 月 10 日午後 5 時 7 分 0 秒 (日本標準時) をあらわす
DataSize	0..1	数値		圧縮前の PDI 形式データセットの Byte 単位の合計サイズ

Table 5 - Patient オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
PatientID	0..1	文字列		提供施設における患者 ID
Name	0..1	文字列		患者の氏名 形式は任意

要素	多重度	型	値	説明
Name(ABC)	0..1	文字列		患者の氏名 ローマ字で表現する
Name(IDE)	0..1	文字列		患者の氏名 漢字で表現する
Name(SYL)	0..1	文字列		患者の氏名 カナで表現する
Sex	0..1	文字列	“male”, “female”, “other”, “unknown” のいずれか、または コミュニティで定義 した文字列	患者の性別
BirthDate	0..1	文字列		患者の生年月日 YYYY-MM-DD の形式で表現する 例: 2020-06-10 この例は西暦 2020 年 6 月 10 日をあら わす
Description	0..1	文字列		患者が特定されていない等、患者に関 するその他の情報を記述する

Table 6 - Contents オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Type	1..1	文字列	“Referral”, “Observation”, “ImagingStudy”, “MedicationRequest”, “DischargeSummary”, “Other” のいずれか、または “Other.”で始まる任意の 文字列	内容の種別
TypeDisplayName	1..1	文字列		種別を表すタイトル
Description	0..1	文字列		内容の概要 形式は任意
Date(注 1)	0..1	文字列		内容の日付 YYYY-MM-DD の形式で 表現する
Period(注 1)	0..1	Period オブ ジェクト		内容の期間
Detail	0..*	Detail オブ ジェクト		内容の概要の明細 内容の概要の内訳を記述 する
Study	0..*	DICOMStu dy オブジェ クト		内容が DICOM の Study であるときに使用する

要素	多重度	型	値	説明
Count	0..1	数値		内容に含まれる情報の件数
CountUnit	0..1	文字列		内容に含まれる情報の件数の単位

(注 1): 内容の性質に応じて Period または Date のいずれかを使う

Table 7 - Detail オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Description	1..1	文字列		内容の概要 形式は任意
Date(注 2)	0..1	文字列		内容の日付 YYYY-MM-DD の形式で 表現する
Period(注 2)	0..1	Period オブ ジェクト		内容の期間

(注 2): 内容の性質に応じて Period または Date のいずれかを使う

Table 8 - DICOMStudy オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Description	0..1	文字列		内容の概要 形式は任意
Date	0..1	文字列		検査の日付 YYYY-MM-DD の形式で 表現する
Thumbnail	0..1	文字列		検査を代表する画像のサム ネイル サムネイル画像の JPEG フ ァイルの内容全体を base64 でエンコードして 格納する
NumberOfSeries	0..1	数値		検査に含まれるシリーズ 数
NumberOfInstance	0..1	数値		検査に含まれるインスタ ンス総数
Series	0..*	DICOMSeries オブジェクト		検査に含まれるシリーズ の情報

Table 9 - DICOMSeries オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Modality	0..1	文字列		モダリティタイプ
BodyPartExamined	0..1	文字列		検査部位
Description	0..1	文字列		内容の概要 形式は任意

要素	多重度	型	値	説明
Date	0..1	文字列		シリーズの日付 YYYY-MM-DD の形式で 表現する
Thumbnail	0..1	文字列		シリーズを代表する画像 のサムネイル サムネイル画像の JPEG フ ァイルの内容全体を base64 でエンコードして 格納する
NumberOfInstance	0..1	数値		シリーズに含まれるイン スタンス数

Table 10 - Period オブジェクト (アウトライン) の要素

要素	多重度	型	値	説明
Start	1..1	文字列		期間の開始日 YYYY-MM-DD の形式で 表現する
End	0..1	文字列		期間の終了日 YYYY-MM-DD の形式で 表現する 開始日と終了日が同じ日 になるときは開始日と同 じ値を指定する 期間が終了していない場 合この要素は省略する

Appendix C にアウトラインの記述例を示す。

8.1.5 暗号化済みアウトライン

アウトラインを暗号化したもの。

暗号化・復号の方法は 8.1.2.2 と同様とする。

8.1.6 cloudPDI FHIR リソース

8.1.6.1 cloudPDI FHIR Binary

cloudPDI データセット断片はそれぞれ cloudPDI FHIR Binary とする。

暗号化済みアウトラインは一つの cloudPDI FHIR Binary とする。

各要素の要素名、多重度、型、値および説明を以下の表に示す。

Table 11 - Binary リソース (cloudPDI FHIR Binary)

要素 Lv1	要素 Lv2	多重度	型	値	説明
resourceType				“Binary”	Binary リソース
contentType		1..1	code	“application/octet-stream”	内容の種類 “application/octet-stream”を指定する
data		1..1	base64Binary		base64 でエンコードされた内容

8.1.6.2 cloudPDI FHIR Bundle

cloudPDI FHIR Binary を含む FHIR 文書。

各要素の要素名、多重度、型、値および説明を以下の表に示す。

またこの文書には患者情報その他の交換データに関する情報の記載はしない。

Table 12 - Bundle リソース (cloudPDI FHIR Bundle)

要素 Lv1	要素 Lv2	多重度	型	値	説明
resourceType				“Bundle”	Bundle リソース
identifier		1..1	identifier		
	system	1..1	uri	“urn:ietf:rfc:3986”	常に“urn:ietf:rfc:3986”を指定する
	value	1..1	Codeable Concept		“urn:oid:<ドキュメント ID>”の形で指定する
type		1..1	code	“document”	Document タイプの Bundle 常に“document”を指定する
timestamp		1..1	instant		この Bundle を生成した日時
entry		1..1	Backbone Element		
	Resource		Resource	Composition リソース	この Bundle が含むリソースのリスト

Table 13 - Composition リソース (cloudPDI FHIR Bundle)

要素 Lv1	要素 Lv2 /要素 Lv3	多重度	型	値	説明
resourceType				“Composition”	Composition リソース
status		1..1	code	“final”	常に“final”を指定する
type		1..1	Codeable Concept		
	Coding	1..1	Coding		
	Coding /system	1..1	uri	“http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-type”	常に“http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-type”を指定する
	Coding /code	1..1	code	“cloudPDI-Document-Set”	常に“cloudPDI-Document-Set”を指定する
	Coding /display	1..1	string	“cloudPDI Document Set”	常に“cloudPDI Document Set”を指定する
category		1..1	Codeable Concept		
	Coding	1..1	Coding		
	Coding /system	1..1	uri	“http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-category”	常に“http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-category”を指定する

要素 Lv1	要素 Lv2 /要素 Lv3	多重度	型	値	説明
	Coding /code	1..1	code	“cloudPDI-Document-Set”	常に“cloudPDI-Document-Set”を指定する
	Coding /display	1..1	string	“cloudPDI Document Set”	常に“cloudPDI Document Set”を指定する
title		1..1	string	“cloudPDI Document Set”	常に“cloudPDI Document Set”を指定する
date		1..1	dateTime		この Composition を生成した日時
author		1..1	Reference		
	type	1..1	uri	“Device”	常に“Device”を指定する
	display	1..1	string		この Composition を生成したアプリケーション名を記述する
section		1..1			
	title	1..1	string	“Dataset Chunks”	cloudPDI データセット断片
	entry	1..*	Reference		cloudPDI データセット断片への参照のリスト。cloudPDI データセットの前方の内容を保持する cloudPDI データセット断片から順に配置する
section		1..1			
	title	1..1	string	“Outline”	暗号化済みアウトライン
	entry	1..1	Reference		暗号化済みアウトラインへの参照

Appendix D に cloudPDI FHIR Bundle の例を示す。

8.2 トークン

医療情報の交換には、交換する医療情報を特定するドキュメント ID や cloudPDI データセットを復号するためのパスワードを含むトークン (HI-TOKEN) を使用する。

HI-TOKEN は ISO/TS 22691 『Health informatics —Token-based health information sharing』に定義される。

HI-TOKEN のデータ項目のうち community.identifier にコミュニティ ID を、document.identifier にドキュメント ID を、decryption.password にパスワードをアサインする。その他のデータ項目は任意である。

Appendix B に HI-TOKEN の例を示す。

9 セキュリティに関する配慮事項

9.1 認証

9.1.1 システムの利用者認証

Exporter、Uploader、Downloader、Importer の利用にあたっては、利用者認証をする。Uploader、Downloader が院内システムのネットワークと接続されていないときには OpenID Connect 1.0 を利用して利用者認証をすることが考えられる。

9.1.2 通信の認証

Upload Data [cloudPDI-4]、Download Data [cloudPDI-6]においては、サーバーの利用認可および利用者認証を確実にする。RFC 8252 『OAuth 2.0 for Native Apps』、RFC 7591 『OAuth 2.0 Dynamic Client Registration Protocol』、draft-ietf-oauth-security-topics-22 『OAuth 2.0 Security Best Current Practice』等を参照し、OAuth2.0 を適切に使用する。

9.2 通信路

Upload Data [cloudPDI-4]、Download Data [cloudPDI-6]では、『医療情報システムの安全管理に関するガイドライン 第 6.0 版』の「システム運用編 13. ネットワークに関する安全管理措置 [I、III]」に従って保護が確保された通信路を利用する。

9.3 トークン

トークンには復号のためのパスワードを含む秘密情報が保持されており、トークンの内容が意図せず暴露されることは避ける必要がある。特に患者がトークンを運ぶケースでは、トークンの内容を秘密に保つ必要があることを患者に説明することを考慮する。

9.4 監査証跡

監査証跡を記録する。記録する内容や記録の方法についてはこの技術仕様では規定しない。システムを構築するにあたっては、以下の資料が参考になる。

IHE ATNA Profile^{※1}

JAHIS ヘルスケア分野における監査証跡のメッセージ標準規約 Ver2.1^{※2}

個人情報保護に役立つ監査証跡ガイド —あなたの病院の個人情報を守るために—^{※3}

※1 <https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html>

※2 <https://www.jahis.jp/standard/detail/id=803>

※3 https://www.medis.or.jp/7_kikaku/hanbai/file/DL_P200703.pdf

Appendix A PDI 形式データセットの概要

実装を容易にするため、以下に PDI 形式データセットの概要を表す図を示す。

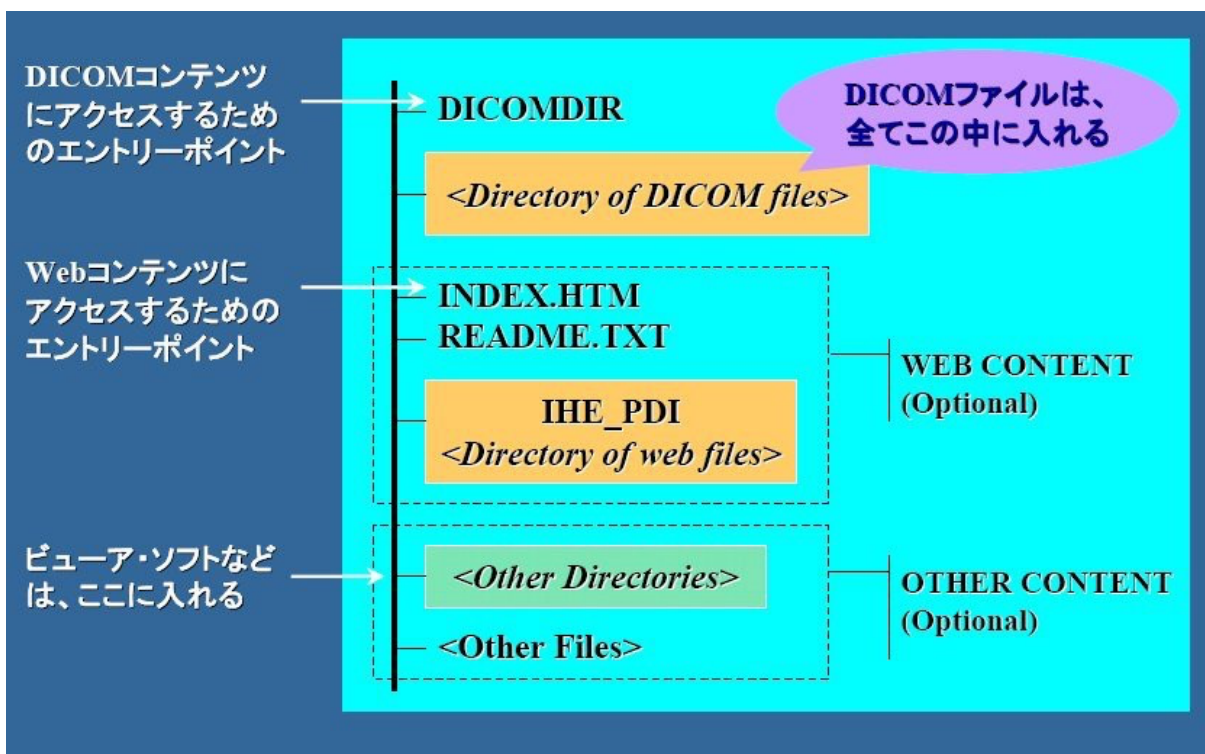


Figure A.1 - PDI 形式データセットの概要

日本医療情報学会『IHE 統合プロフィール「可搬型医用画像」の運用指針第1版』より

検体検査結果、処方、診療情報提供書などの文書(HL7 CDA, FHIR と)、DICOM 以外の画像などは、Other Files の部分に格納する。DICOM 画像がない場合は、DICOMDIR, Directory of DICOM files が存在しなくてもよい。

Appendix B HI-TOKEN の例

以下にデータ受領用の HI-TOKEN の例を示す。

この例では、トークンの内容の表現に QR コードを利用し、紙媒体に印刷している。

cloudPDI トークンシート	
提供施設	HI-TOKEN 病院
	電話番号 : 000-000-0000 医療機関コード : 00000000
お預かり日	2020年06月03日
有効期限	2020年09月03日
	必ず期限までにダウンロードしてください
	
フリガナ:	
氏名	提供施設患者ID : 20190407-CRC-000011
性別 男 生年月日	受領施設患者ID : _____ ↑ 記入してお使いください
検査結果	処方データ
なし	なし
検査画像	
2019年04月07日 CR 1 画像	
発行日時 2020年06月03日 22時05分	

Figure B.1 - HI-TOKEN の例

Appendix C アウトラインの例

以下にアウトラインの例を示す。

```
{
  "Version": "1",
  "Creator":
    {
      "Code": "00000000",
      "Name": "HI-TOKEN 病院",
      "Contact": "000-000-0000"
    },
  "CreationInformation":
    {
      "DateTime": "2020-06-03T10:00:00+09:00"
    },
  "Patient":
    {
      "PatientID": "00000000",
      "Name": "患者 氏名",
      "Name(IDE)": "患者 氏名",
      "Name(SYL)": "カンジヤ シメイ",
      "Sex": "unknown",
      "BirthDate": "1970-01-01"
    },
  "Contents":
    [
      {
        "Type": "Referral",
        "TypeDisplayName": "診療情報提供書",
        "Description": "診療情報提供書",
        "Date": "2020-06-03"
      },
      {
        "Type": "Observation",
        "TypeDisplayName": "検査結果",
        "Description": "検査結果 2 件",

```

(続く)

(続き)

```
"Period":
  {
    "Start": "2020-05-10",
    "End": "2020-05-25"
  },
"Detail":
  [
    {
      "Description": "検査結果",
      "Date": "2020-05-10"
    },
    {
      "Description": "検査結果",
      "Date": "2020-05-25"
    }
  ],
{
  "Type": "ImagingStudy",
  "TypeDisplayName": "検査画像",
  "Description": "CT 1 検査 130 画像",
  "Period":
    {
      "Start": "2020-05-10",
      "End": "2020-05-10"
    },
  "Study":
    [
      {
        "Date": "2020-05-10",
        "NumberOfSeries": 1,
```

(続く)

(続き)

```
        "Series":
            [
                {
                    "Modality": "CT",
                    "Date": "2020-05-10",
                    "NumberOfInstance": 130
                }
            ]
    }
]
```

Appendix D cloudPDI FHIR Bundle の例

以下に cloudPDI FHIR Bundle の例を示す。

```
{
  "resourceType": "Bundle",
  "id": "2.999",
  "identifier": {
    "system": "urn:ietf:rhc:3986",
    "value": "urn:oid:2.999"
  },
  "type": "document",
  "timestamp": "2020-06-03T10:10:00+09:00",
  "entry": [
    {
      "resource": {
        "resourceType": "Composition",
        "status": "final",
        "type": {
          "coding": [
            {
              "system": "http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-type",
              "code": "cloudPDI-Document-Set",
              "display": "cloudPDI Document Set"
            }
          ]
        },
        "category": {
          "coding": [
            {
              "system": "http://ihe-j.org/cloudPDI/fhir/CodeSystem/document-category",
              "code": "cloudPDI-Document-Set",
              "display": "cloudPDI Document Set"
            }
          ]
        },
        "title": "cloudPDI Document Set",

```

(続く)

(続き)

```
"date": "2020-06-03T10:10:00+09:00",
"author": [
  {
    "type": "Device",
    "display": "cloudPDI Uploader"
  }
],
"section": [
  {
    "title": "Dataset Chunks",
    "entry": [
      {
        "reference": "https://fhir.example.com/Binary/c1"
      },
      {
        "reference": "https://fhir.example.com/Binary/c2"
      },
      {
        "reference": "https://fhir.example.com/Binary/c3"
      }
    ]
  },
  {
    "title": "Outline",
    "entry": [
      {
        "reference": "https://fhir.example.com/Binary/o1"
      }
    ]
  }
]
}
```

Appendix E Repository への要求・応答の例

E.1. Binary 提出時の要求・応答の例

Binary (cloud PDI データセット断片の場合) 提出時の HTTP 要求の例を示す

```
POST https://fhir.example.com/Binary
Authorization: Bearer eyJ0eX<略>wZU6Q
Content-type: application/fhir+json

{
  "resourceType": "Binary",
  "contentType": "application/octet-stream",
  "data": <cloud PDI データセット断片>
}
```

```
HTTP/1.1 201 Created
Content-Type: application/fhir+json;
Location: https://fhir.example.com/Binary/c1
```

E.2. Bundle 提出時の要求・応答の例

Bundle (ドキュメント ID が 2.999 の場合) 提出時の HTTP 要求の例を示す

```
PUT https://fhir.example.com/Bundle/2.999
Authorization: Bearer eyJ0eX<略>wZU6Q
Content-type: application/fhir+json

{
  "resourceType": "Bundle",
  "id": "2.999",
  "identifier": {
    "system": "urn:ietf:rhc:3986",
    "value": "urn:oid:2.999"
  },
  "type": "document",
  <Bundle リソースの詳細な内容は省略する。Appendix D を参照>
}
```

Bundle (ドキュメント ID が 2.999 の場合) 提出時の HTTP 応答の例を示す。


```
HTTP/1.1 201 Created
Content-Type: application/fhir+json
Location: https://fhir.example.com/Bundle/2.999
```

E.3. Bundle 取得時の要求・応答の例

```
GET https://fhir.example.com/Bundle/2.999
Authorization: Bearer eyJ0eX<略>wZU6Q
```

Bundle（ドキュメント ID が 2.999 の場合）取得時の HTTP 応答の例を示す。

```
HTTP/1.1 200 OK
Content-Type: application/fhir+json

<Bundle リソースの内容は省略する。Appendix D を参照>
```

E.4. Binary 取得時の要求・応答の例

Binary（cloud PDI データセット断片の場合）取得時の HTTP 要求の例を示す。

```
GET https://fhir.example.com/Binary/c1
Authorization: Bearer eyJ0eX<略>wZU6Q
```

```
HTTP/1.1 200 OK
Content-type: application/fhir+json

{
  "resourceType": "Binary"
  "id": "c1",
  "contentType": "application/octet-stream",
  "data": <cloud PDI データセット断片>
}
```