IHE IT
インフラストラクチャの概要

IHE-J ベンダワークショップ2009

（2009･05･21）

接続検証委員会

IHE統合プロファイルーモデル

- アクタ、正確に定義された役割
  - 情報システムの特定の機能を抽象化
- …精緻に定義されたトランザクションの実施
  - 既存の標準を利用
- ……現実世界の相互運用性の問題を解決
  - 統合プロファイルの明確化

テクニカルフレームワークの構成

- **Volume 1: 統合とコンテンツのプロファイル**
  - 臨床ニーズとユースケースの記述
  - 明確化:
    - アクターとトランザクション、あるいは
    - コンテンツ・モジュール
- **Volume 2:**
  - トランザクションまたはコンテンツモジュールの実装仕様を提供

IHE IT インフラストラクチャ(1)

- **Profiles – 医療情報**
  - Document Sharing（ドキュメント共有）
    - XDS – Cross-Enterprise Document Sharing
    - ★ XDS Stored Query
    - ★ XDS-SD – XDS Scanned Documents
    - ★ XDP – Cross-Enterprise Document Interchange
    - NAV – Notification of Document Availability
    - RID – Retrieve Information for Display
  - Patient Management（患者情報管理）
    - PAM – Patient Administration Management
    - PDQ – Patient Demographics Query
    - PIX – Patient Identifier Cross-referencing
    - PSA – Patient Synchronized Applications
  - ★ RFD – Retrieve Form for Data Capture

IHE IT インフラストラクチャ(2)

- **Profiles – セキュリティ**
  - ATNA – Audit Trial and Node Authentication
  - CT – Consistent Time
  - DSG – Document Digital Signature
  - EUA – Enterprise User Authentication
  - PWP – Personnel White Pages

IHE Transactions

- 3.1 Maintain Time
- 3.2 Get User Authentication
- 3.3 Get Service Ticket
- 3.4 Kerberized Communication
- 3.5 Join Context
- 3.6 Change Context
- 3.7 Leave Context
- 3.8 Patient Identity Feed
- 3.9 PIX Query
- 3.10 PIX Update Notification
- 3.11 Retrieve Specific Information for Display
- 3.12 Retrieve Document for Display
- 3.13 Follow Context
- 3.14 Register Document Set
- 3.16 Query Registry
- 3.17 Retrieve Document
- 3.18 Registry Stored Query
- 3.19 Authenticate Node
- 3.20 Record Audit Event
- 3.21 Patient Demographics Query
- 3.22 Patient Demographics and Visit Query
- 3.23 Find Personnel White Pages
- 3.24 Query Personnel White Pages
- 3.30 Patient Identity Management
- 3.31 Patient Encounter Management
- 3.32 Distribute Document Set on Media
- 3.40 Provide X-User Assertion
- 3.41 Provide and Register Document Set-b
- 3.42 Register Document Set-b
- 3.43 Retrieve Document Set

IHE IT インフラストラクチャ(3)

- **最近のprofiles**
  - XDS Federation
  - PIX and PDQ using HL7 v3
  - Web Services Transport for IHE Transactions
  - XUA – Cross-Enterprise User Authentication
  - Risk Management Planning White Paper
  - IHE XDS Publish/Subscribe Profile
  - Emergency Contact Registry (ECON)
  - Sharing of Terminology Value Sets (SVS)
  - Cross-Enterprise Service Bus (XSB)
  - Asynch XDS.b Profile
  - Referral Request/ Referral Order
  - Extended Patient Demografics Query PDQ

IHE IT インフラストラクチャ(4)

PIX / PDQ

Patient Demographics Query

Patient Identifier Cross-referencing

Map patient identifiers across independent identification domains

Emergency Referrals
Patient Created Summaries
ECG Report Document
Lab Results Document
Scanned Documents
Imaging Information
Medical Summary
(Meds, Allergies, Pbs)
Format of the Document Content and associated coded vocabulary

Patient Consent

DSG

Document Digital Signature
Attesting "true-copy and origin

Notice of Document Availability
Know about new information

ATNA / CT

Audit Trail & Node Authentication

Centralized privacy audit trail and node to node authentication to create a secured domain.

Cross-Enterprise Document Sharing
Registration, distribution and access across health enterprises of clinical documents forming a patient electronic health record

NAV

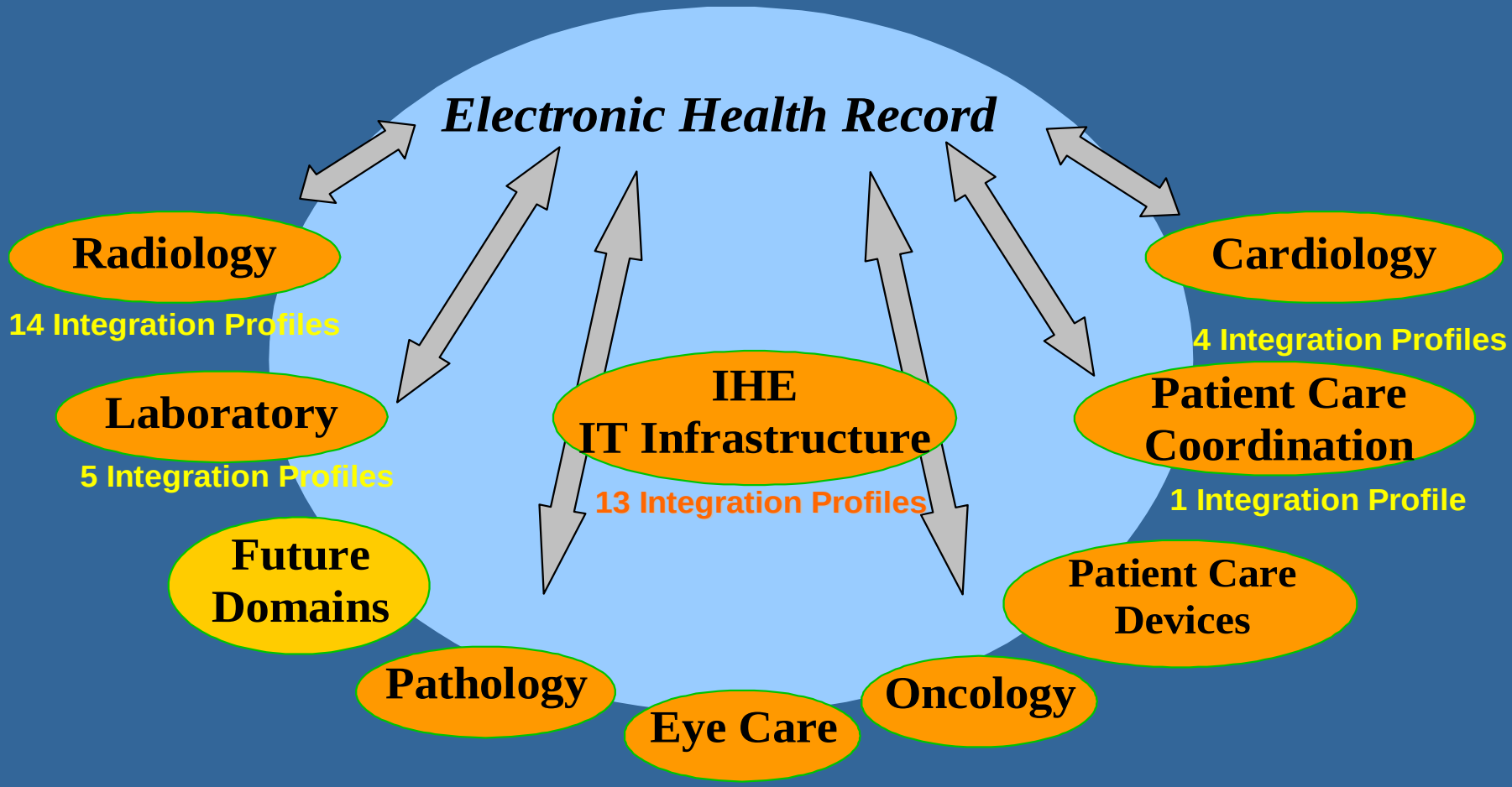
RHIOの構築を支援

Cross-enterprise Document Point-to-Point Interchange
Media-CD/USB & e-mail push

XDS / XDP

Consistent Time
Coordinate time across networked systems

IHE IT インフラストラクチャ(5)



IHE IT インフラストラクチャ情報の入手

- **調査研究: テクニカルフレームワーク**
  - www.ihe.net/Technical_Framework/index.cfm
    - Volume 1 – Profiles
    - Volume 2 – Transaction
  - www.ihe.net – New profiles and transactions
- **実践段階: コネクタソン接続テスト**
  - www.ihe.net and www.connectathon.net
- **流通段階:**
  - ヘルスケア IT ベンダのインフラストラクチャ専門家
  - 他のITベンダとの協業

詳細情報

- IHE Web Site - http://www.ihe.net
  - Technical Frameworks
  - Technical Framework Supplements – Trial Implementation
  - Calls for Participation
  - IHE Fact Sheet and FAQ
  - IHE Integration Profiles: Guidelines for Buyers
  - IHE Connectathon Results
  - Vendors' Product Integration Statements
- Sponsors' IHE sites
  - http://www.himss.org/IHE
  - http://www.rsna.org/IHE
  - http://www.acc.org/quality/ihe.htm

IHE : XDS (Cross-Enterprise Document Sharing)

IHE-J ベンダワークショップ2009

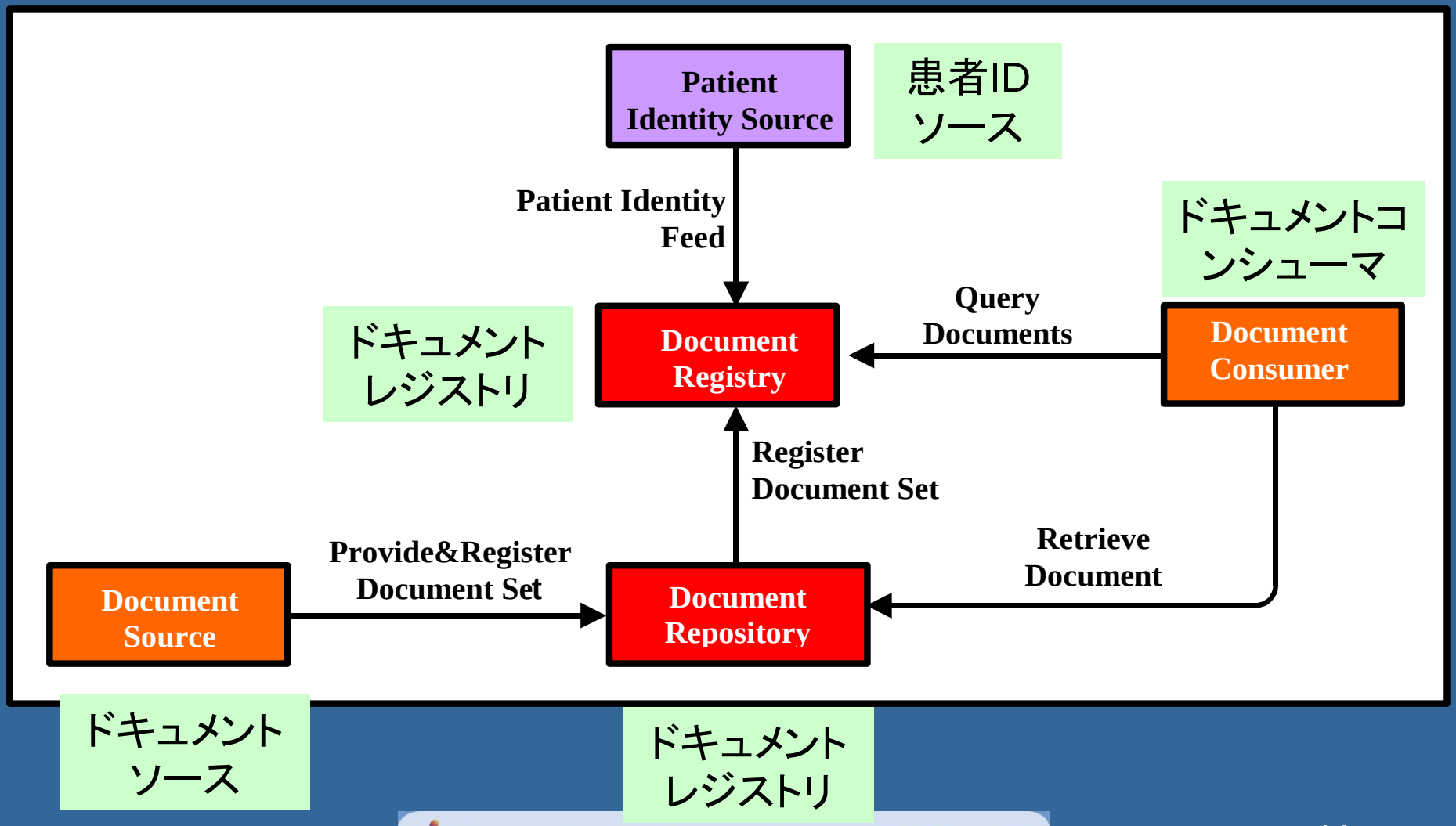
（2008･05･21）

接続検証委員会

内容

- アーキテクチャ
- 関連プロファイル
- メタデータ
- インフラストラクチャ
- テストおよびリソース
- 課題

XDS.a トランザクション

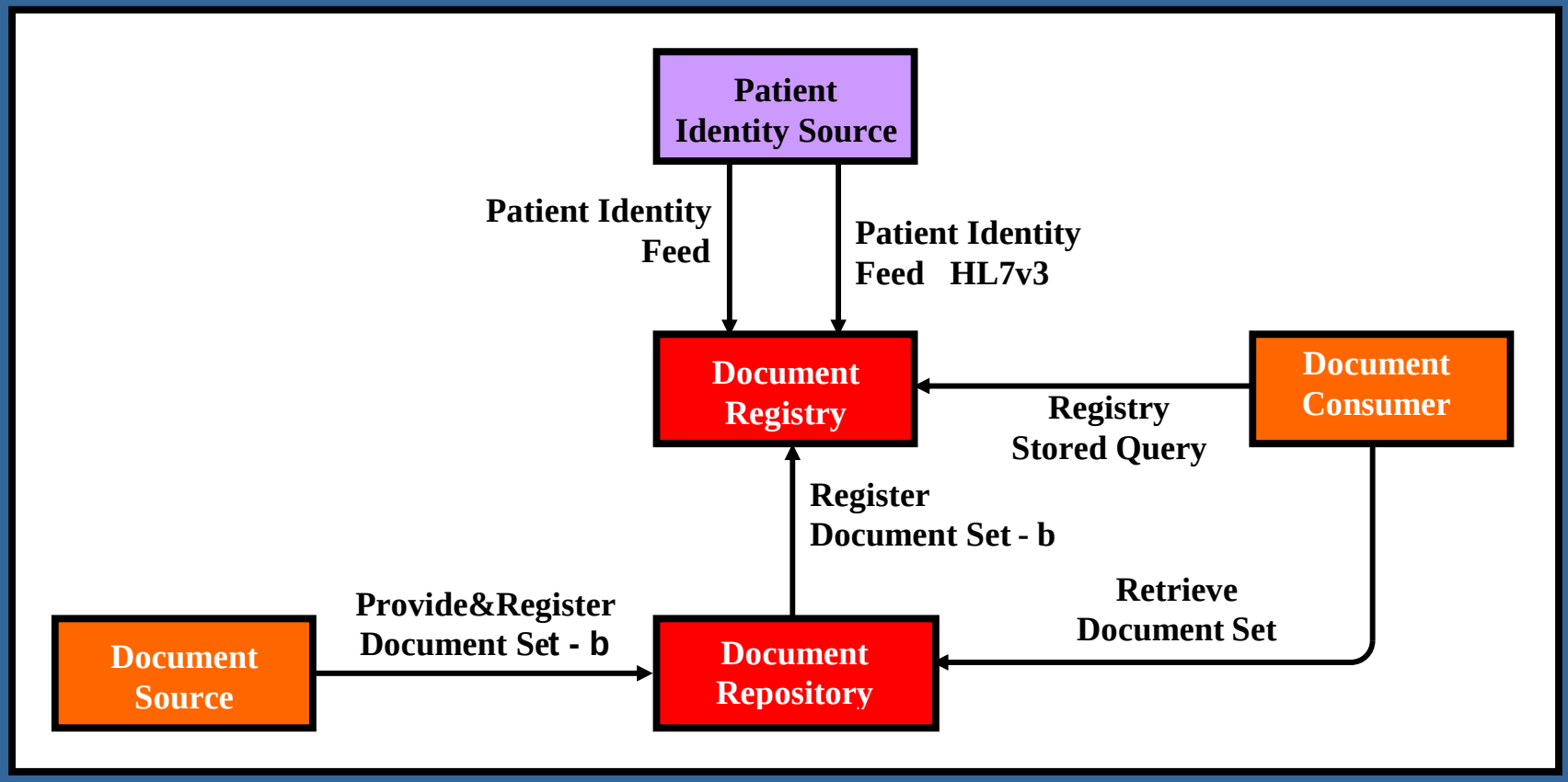


XDS.a とXDS.bの比較

- **XDS.a**
  - 従来のXDS profile, 2007年版以前
  - ebXML Reg/Rep 2.1をベース
  - SOAP with attachments を基にした Provide and Register
  - Retrieve は、HTTP GET
- **XDS.b**
  - Web Services およびebXML Reg/Regなど、現在のベンダによる開発状況に合わせた標準を採用。
  - ebXML Reg/Rep 3.0
  - MTOM、MTOM /XOPを基にしたProvide and Register
  - MTOM /XOPを基にしたRetrieve
  - HL7 V3 を採用したPatient Identity Feed
- **XDS.a とXDS.bでアクアは、共通**
- **メタデータも、XDS.a とXDS.bで共通**

（MTOM： Message Transaction Optimization Mechanism）
（XOP： XML-binary Optimized Packaging）

XDS.b トランザクション



XDS アフィニティドメインのタイプ

- **XDS.a 対応**
  - すべてのアクタは、XDS.a トランザクションをサポート
- **XDS.b 対応**
  - すべてのアクタは、XDS.b トランザクションをサポート
- **XDS.a 及びXDS.b対応**
  - Document Repository とDocument Registry は、XDS.a およびXDS.b の両方のトランザクションに対応
  - Document Source とDocument Consumer は、一方、または、両方をサポートできる

関連プロファイル

- CT (Consistent Time)
  - ネット上の時刻の同期、整合性維持
- ATNA (Audit Trail and Node Authentication
  - ノード認証
  - イベントログ（監査証跡）
- PIX（Patient Identifier Cross-referencing for MPI)
  - 患者IDドメイン（施設ごとに管理される患者ID）
  - アフィニティ･ドメイン（参加施設全体で管理される患者ID）
  - PIXマネジャ
- PDQ (Patient Demographics Query)
  - 患者基本情報を基にした患者IDの問合わせ
- XUA (Cross-Enterprise User Authentication)
  - 施設間にまたがる利用者認証
- NAV (Notification of Document Availability)
  - ドキュメントの利用可能通知
- PAM (Patient Administration/Management)
  - 患者の入院･退院情報の管理

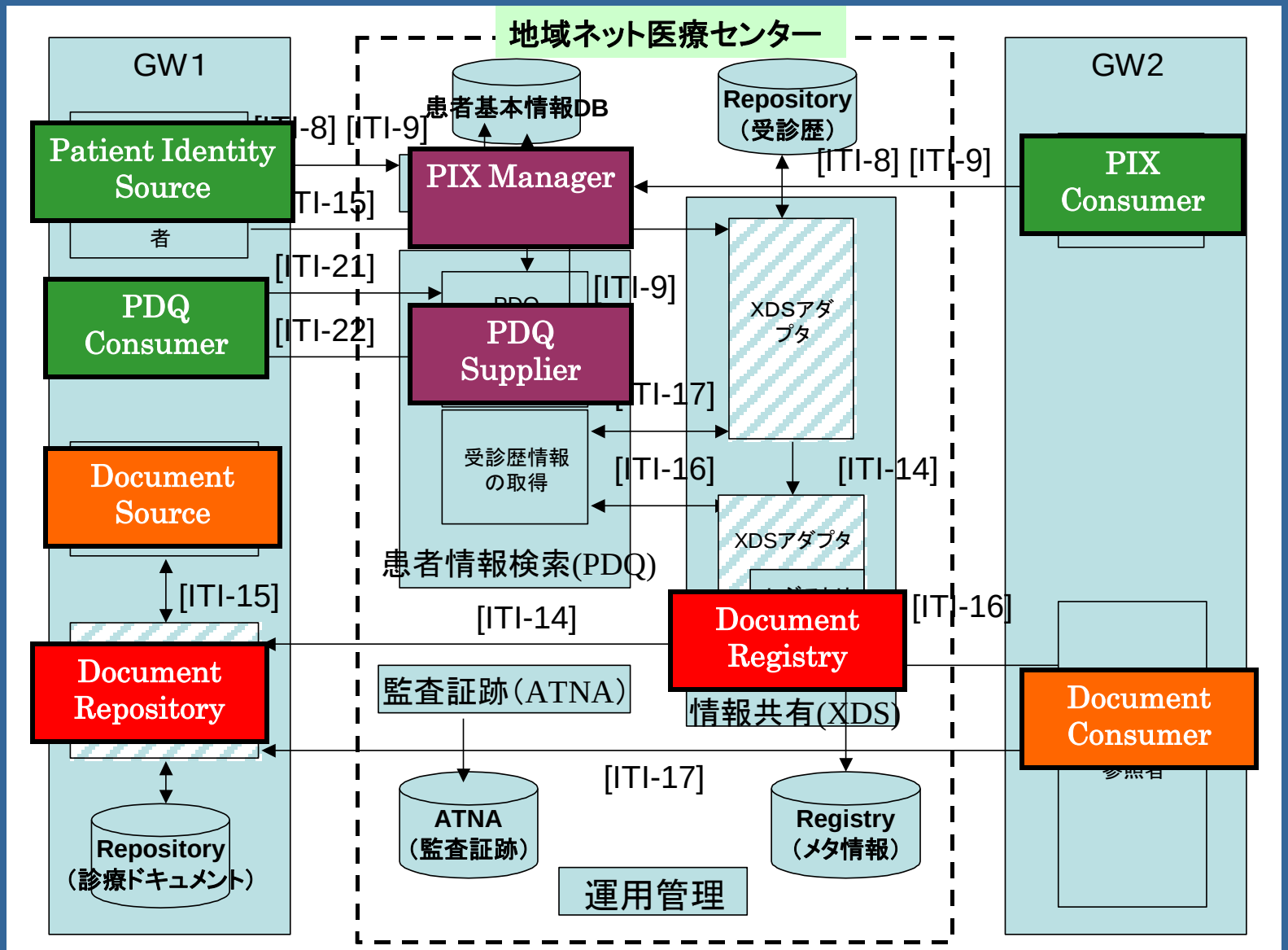
関連プロファイル（トランザクション例）

- [ITI-14] Register Document Set（ドキュメントの登録）
- [ITI-15] Provide and Register Document Set（ドキュメントの提出、登録）
- [ITI-16] Query Registry（ドキュメントの問合せ）
- [ITI-17] Retrieve Document（ドキュメントの取り出し）
- [ITI-9] PIX Query（地域患者IDの問い合わせ）
- [ITI-8] Patient Identity Feed（地域患者IDの登録）
- [ITI-21] Patient Demographics Query（患者基本情報の問合せ）
- [ITI-22] Patient Demographics and Visit Query（受診歴、入退院歴の問合せ）

  - アフィニティドメイン（Affinity Domain ）：共通のポリシーで運営することを合意したヘルスケア関連施設のグループ。レジストリ及びリポジトリの共通のインフラストラクチャを共有する。

参考になる実装例

実装例(Nagoya-RHIE)

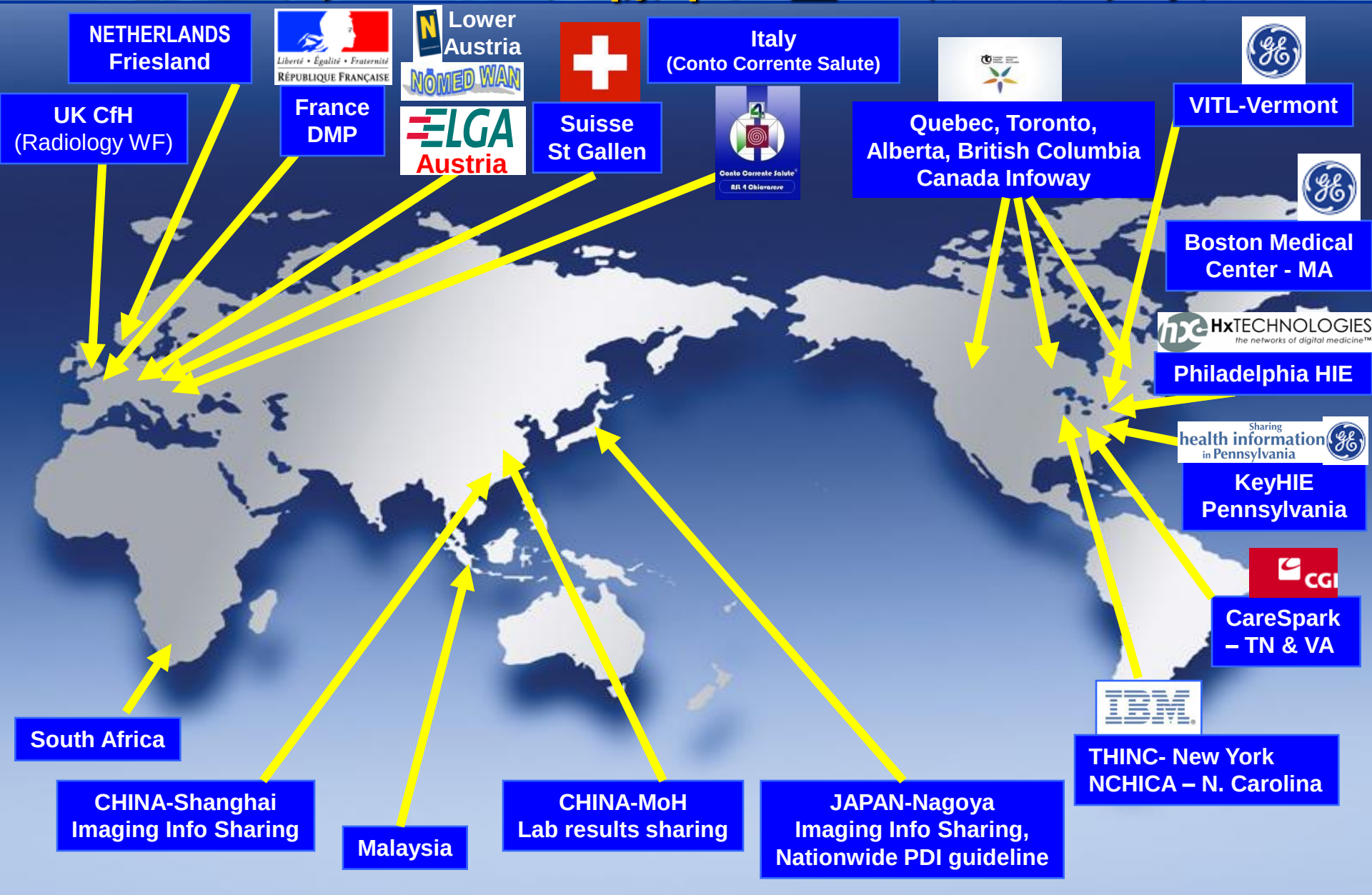


参考情報

- **東海ネット医療フォーラム・NPO**
  - 平成18年度　地域医療情報連携システムの標準化及び実証事業　事業報告書
- **JAHIS技術文書**
  - ・地域医療情報連携システム　診療情報共有化のためのIHE XDS 適用ガイド
  - ・地域医療情報連携システム　患者情報管理のためのIHE PIX/PDQ 適用ガイド
  - ・地域医療情報連携システム　運用管理システムのサービス機能

http://www.jahis.jp/standard/seitei/index.html
（ページ下部の「制定済み技術文書一覧」に掲載されています。）

国、地域のプロジェクトで採用された IHEのグローバル標準に基づくプロファイル



ebXML レジストリ

XDSとの対応

ebXML レジストリ vs XDS

- XDS は、ebXMLレジストリ（標準）の1つのプロファイル
- ebXML レジストリは、2つの標準からなる
  - ebRIM (Registry Info Model)
  - ebRS (Registry Services - protocols)
- XDSは、ebRIM およびebRSの全部ではなく、一部の機能を使用

ebRIM

- ebRIM は、対象のドキュメントについて記述する言語を定義している
- この言語は、オブジェクトとその属性から構成されている
- それらは、XMLで表現される
- メタデータの表現形式である

サブミッション

- ドキュメントソースからリポジトリへ提出する
- 内容:
  - メタデータ
  - 0個以上のドキュメント
- 「MIMEアタッチメント付きSOAP」によるコード化

クエリ

- ebRIM は、メタデータの関係データモデルでのビューを定義している
- クエリは、SQLのサブセットで記述される
- XDSでは、以下のようなクエリを定義している
  - FindDocuments
  - FindSubmissionSets
  - FindFolders
  - GetAll
  - GetDocument
  - GetSubmissionSetContents
  - GetFolderContents など

主要なebRS メソッド

ドキュメントソース

- **SubmitObjectsRequest**

ドキュメントコンシューマ

- **AdhocQueryRequst**

レジストリアダプタ

- **ApproveObjectsRequest**
- **DeprecateObjectsRequest**

メタデータの構成

レジストリとの対応

主要なebRIM オブジェクト

ebRIM 要素	用途
ExtrinsicObject	**リポジトリ内でドキュメントを表現**
RegistryPackage	**フォルダの機構**
Association	**オブジェクト間のリンク**

XDS基本オブジェクト

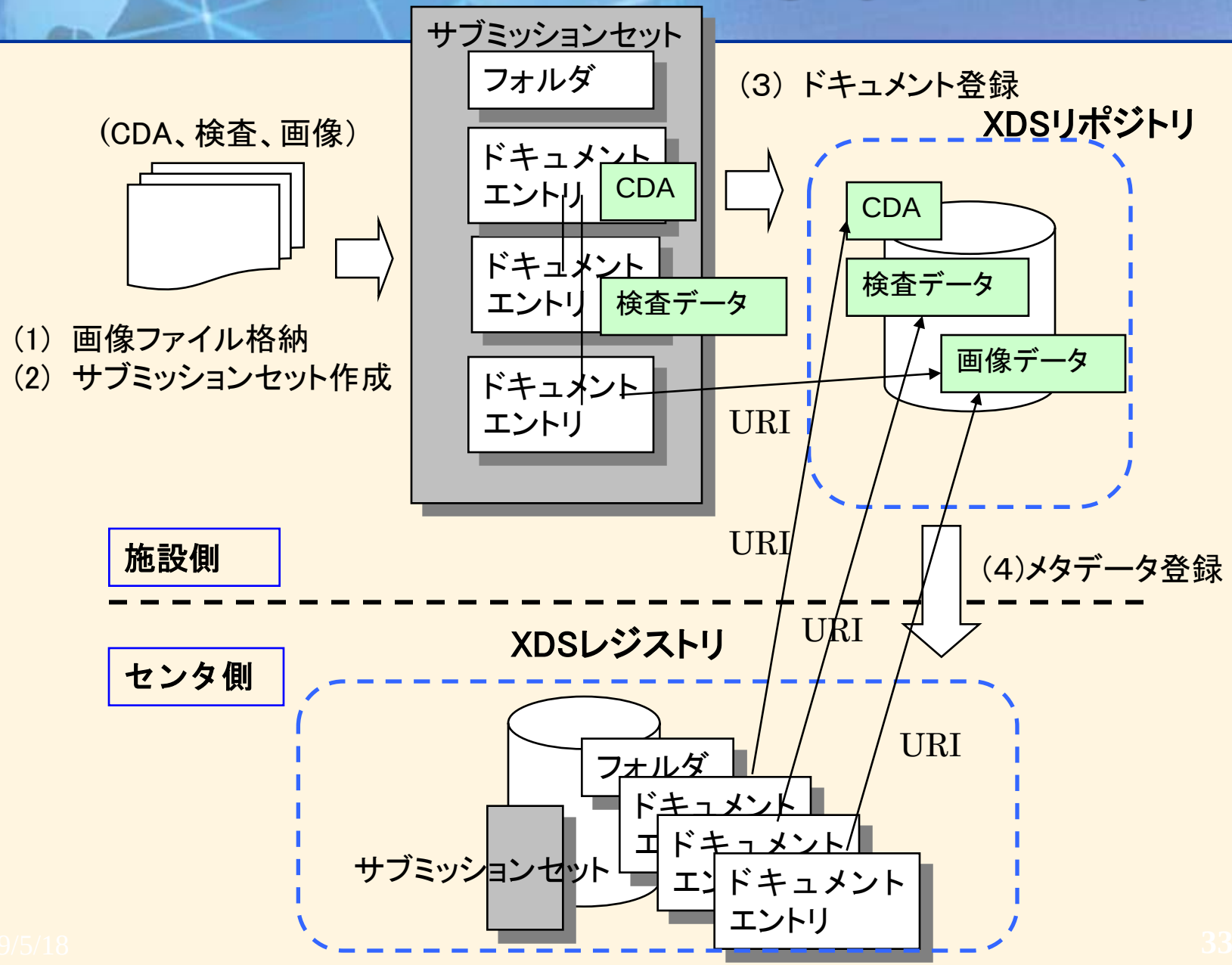
XDSDocumentEntry **(ExtrinsicObject)**

- **リポジトリ内のドキュメントを表現する**
- **さらに詳しい属性をもつ**

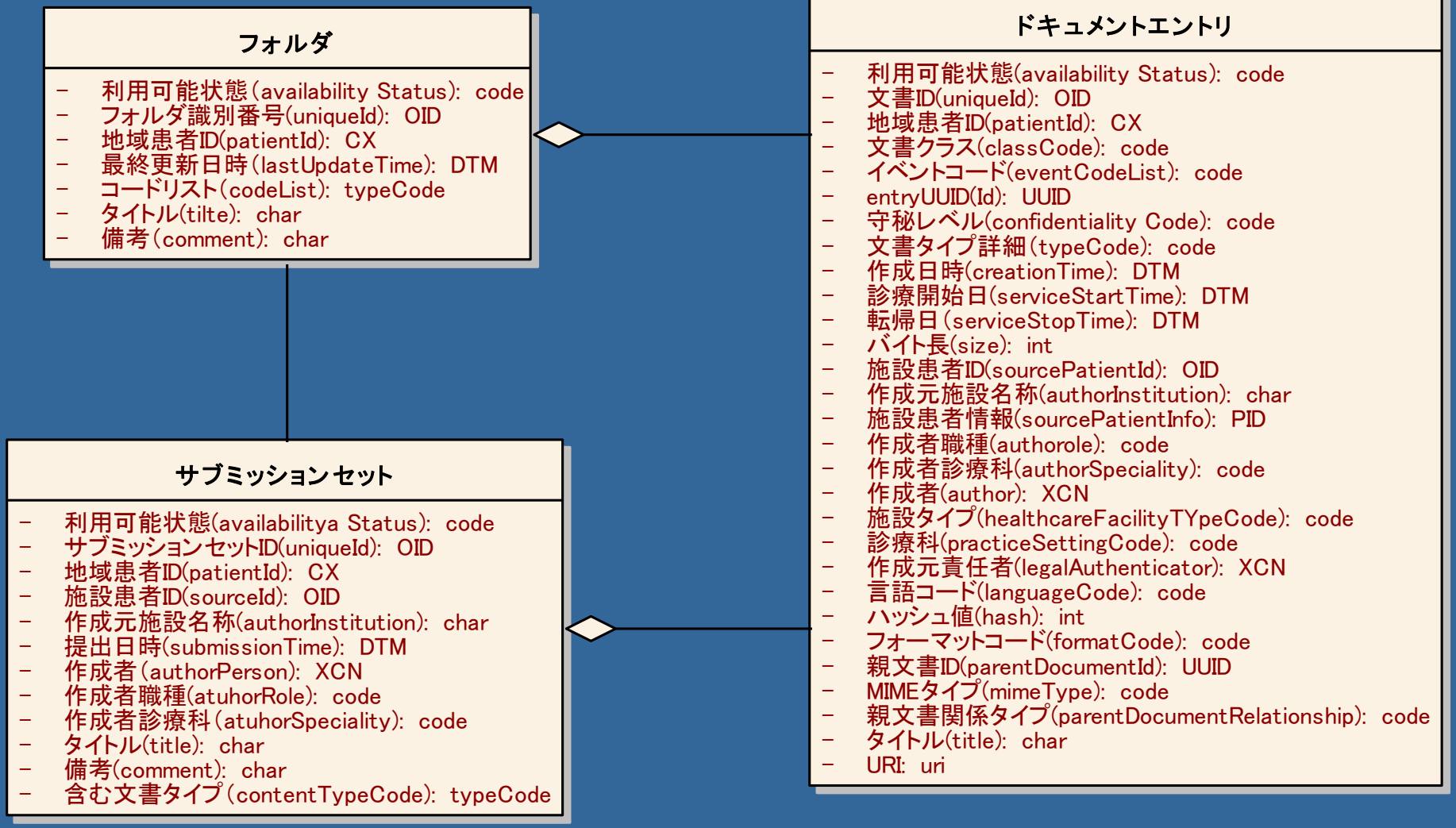
XDSSubmissionSet **(RegistryPackage)**

- **サブミッションの記録**
  - 提出されたドキュメント
  - 意味のある診療上のイベント
- **さらに詳しい属性をもつ**

サブミッションの例（Nagoya-RHIE）



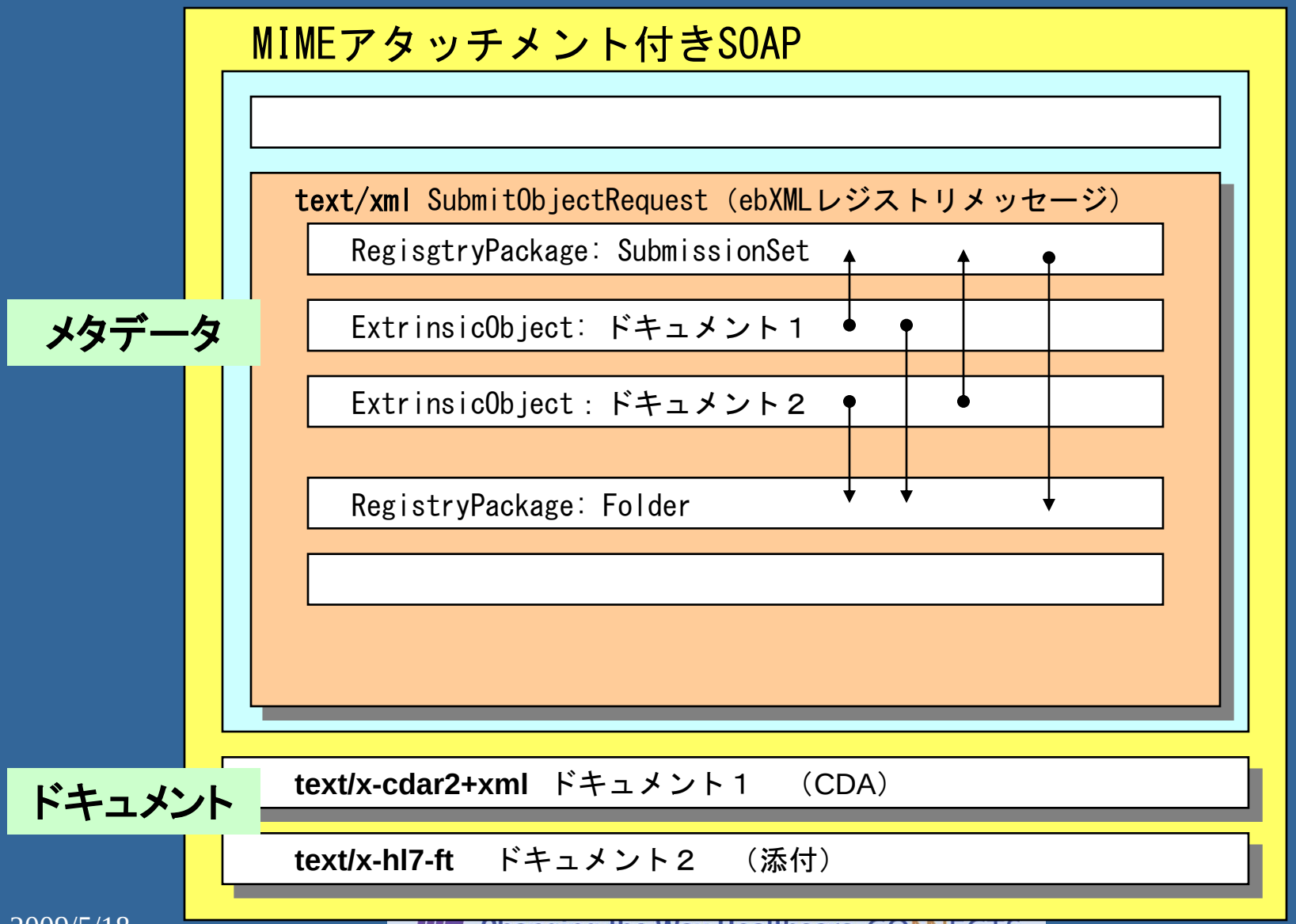
メタデータ項目


フォルダ
- 利用可能状態(availability Status): code
- フォルダ識別番号(uniqueId): OID
- 地域患者ID(patientId): CX
- 最終更新日時(lastUpdateTime): DTM
- コードリスト(codeList): typeCode
- タイトル(tilte): char
- 備考(comment): char
ドキュメントエントリ
- 利用可能状態(availability Status): code
- 文書ID(uniqueId): OID
- 地域患者ID(patientId): CX
- 文書クラス(classCode): code
- イベントコード(eventCodeList): code
- entryUUID(Id): UUID
- 守秘レベル(confidentiality Code): code
- 文書タイプ詳細(typeCode): code
- 作成日時(creationTime): DTM
- 診療開始日(serviceStartTime): DTM
- 転帰日(serviceStopTime): DTM
- バイト長(size): int
- 施設患者ID(sourcePatientId): OID
- 作成元施設名称(authorInstitution): char
- 施設患者情報(sourcePatientInfo): PID
- 作成者職種(authorole): code
- 作成者診療科(authorSpeciality): code
- 作成者(author): XCN
- 施設タイプ(healthcareFacilityTYpeCode): code
- 診療科(practiceSettingCode): code
- 作成元責任者(legalAuthenticator): XCN
- 言語コード(languageCode): code
- ハッシュ値(hash): int
- フォーマットコード(formatCode): code
- 親文書ID(parentDocumentId): UUID
- MIMEタイプ(mimeType): code
- 親文書関係タイプ(parentDocumentRelationship): code
- タイトル(title): char
- URI: uri
サブミッションセット
- 利用可能状態(availabilitya Status): code
- サブミッションセットID(uniqueId): OID
- 地域患者ID(patientId): CX
- 施設患者ID(sourceId): OID
- 作成元施設名称(authorInstitution): char
- 提出日時(submissionTime): DTM
- 作成者(authorPerson): XCN
- 作成者職種(atuhorRole): code
- 作成者診療科(atuhorSpeciality): code
- タイトル(title): char
- 備考(comment): char
- 含む文書タイプ(contentTypeCode): typeCode

メタデータのXML形式

ebXML レジストリとの対応

サブミッション（HTTP Post）



XML - XDSDocumentEntry

```
<rim:ObjectRef id="urn:uuid:7edca82f-054d-47f2-a032-
    9b2a5b5186c1" />
<rim:ExtrinsicObject
  objectType="urn:uuid:7edca82f-054d-47f2-a032-
    9b2a5b5186c1" >
    …
<rim:/ExtrinsicObject>
```

レジストリ内での識別子を宣言

XML - XDSSubmissionSet

```
<rim:RegistryPackage id="ss">
…
</rim:RegistryPackage>
<rim:Classification
   classifiedObject="ss"
  classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
    b4633d873bdd"/>
<rim:ObjectRef id="urn:uuid:a54d6aa5-d40d-43f9-88c5-
    b4633d873bdd"/>
```

サブミッションセットを定義

XML – SubmissionSetにdocumentEntryを追加

```
<rim:ExtrinsicObject id=“doc”>
…
</rim:ExtrinsicObject>
<rim:RegistryPackage id=“ss”
…
</rim:RegistryPackage>
<rim:Association
    associationType="HasMember"
    sourceObject=”ss"
    targetObject=”doc">
```

XML - Submission

```
<rs:SubmitObjectsRequest>
  <rs:LeafRegistryObjectList>
        <rim:ExtrinsicObject>
              …
        </rim:ExtrinsicObject>
        <rim:RegistryPackage>
              …
        </rim:RegistryPackage>
        …
  </rs:LeafRegistryObjectList>
</rs:SubmitObjectsRequest>
```

XML – 属性のタイプ

- Main
- Slot
- Classification
- External Identifier

XML – 主な属性のタイプ

- **main要素の属性**

```
<rim:ExtrinsicObject
    objectType=“”
   mimeType=“text/xml”>
```

- **Name 及びDescription 要素**

```
<rim:Name>
    <rim:LocalizedString value = "test 11731"/>
</rim:Name>
```

- **（SubmissionSetに対しても同様）**

XML - Slot で表現された属性のタイプ

- 名前と値のペア
- (XDSで規定されている) 順不同の複数の値をもつことができる

```
<rim:Slot name="authorPerson">
 <rim:ValueList>
    <rim:Value>^Welby^Marcus^^^Dr^MD</rim:Value>
  <rim:Value>^Jones^Barnaby^^^Dr^MD</rim:Value>
 </rim:ValueList>
</rim:Slot>
```

XML – Classification（コード化された属性値）

- コード化された属性（値）は、3つの要素で表現

(コードスキーマ, コード値, コード値の表示名)

- **classCode, eventCode, healthcareFacilityTypeCode, など**

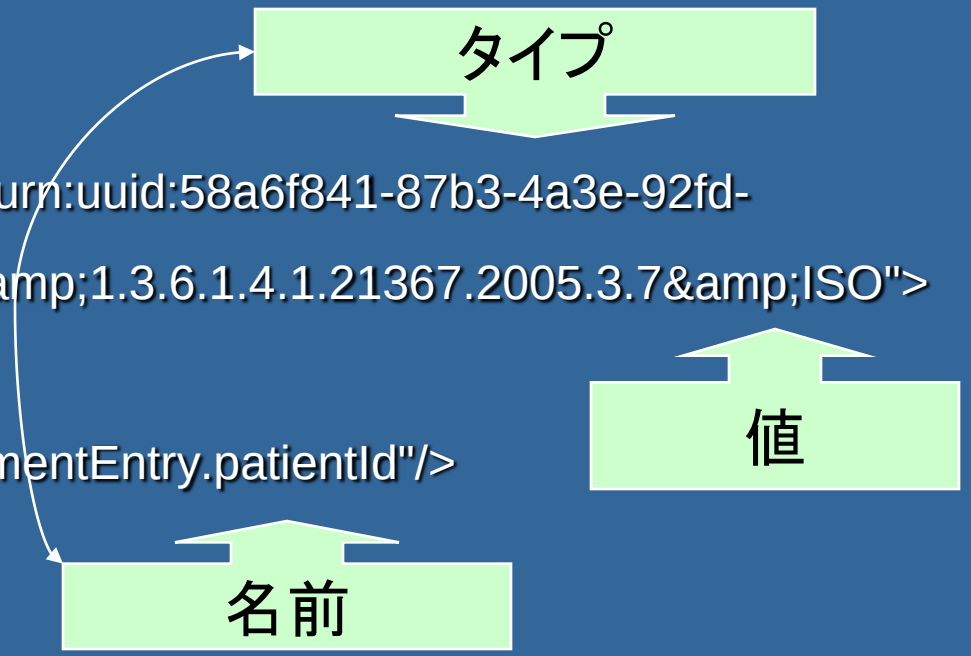
```
<rim:Classification   classificationScheme= "urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
      classifiedObject="theDocument"      nodeRepresentation=″code_value" >
   <rim:Name>
      <rim:LocalizedString value=″code value display name"/>
   </rim:Name>
   <rim:Slot name="codingScheme">
    <rim:ValueList>
      <rim:Value>Coding scheme name</rim:Value>
    </rim:ValueList>
   </rim:Slot>
</rim:Classification>
```

どのコード化された属性かを識別

XML - External Identifiers（外部で定義された識別子）

タイプ、値、名前で表現される

```
<rim:ExternalIdentifier
      identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-
          a8ffeff98427"
      value= “6578946^^^&amp;amp;1.3.6.1.4.1.21367.2005.3.7&amp;amp;ISO">
   <rim:Name>
      <rim:LocalizedString
            value = "XdsDocumentEntry.patientId"/>
   </rim:Name>
</rim:ExternalIdentifier>
```



属性の記述順

属性は、以下の順に記述（制約）

- Main (element attributes 及び title/description)
- Slots
- Classifications
- External Identifiers

サブミッションの応答 Submission Response

<RegistryResponse

codeContext="Test 11710"
status="Success" >

</RegistryResponse>

SOAP

HTTP Header

---blank line---

HTTP Body - SOAP encoded

HTTP/SOAP Header

POST /ebxmlrr/registry/soap HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://sst138.ncsl.nist.gov/web/soap/soap-diag-client.htm
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: gunshot.ncsl.nist.gov:8080
Connection: Keep-Alive
Cache-Control: no-cache
Content-Length: 851

HTTP/SOAP Body

```
<?xml version="1.0" ?>
<SOAP-ENV:Envelope xmlns:SOAP-
    ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <rs:SubmitObjectsRequest>
            …
        </rs:SubmitObjectsRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SOAP with Attachments

```
POST /ebxmlrr/registry/soap HTTP/1.1
Content-Type: multipart/related; type="text/xml"; boundary=----------------------------7d4285f14803b8
SOAPAction: ""

----------------------------7d4285f14803b8
Content-Type: text/xml

<?xml version="1.0" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <rs:SubmitObjectsRequest>
        <rs:LeafRegistryObjectList>
        <rim:ExtrinsicObject id="doc_1"/>
      </rs:LeafRegistryObjectList>
    </rs:SubmitObjectsRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
----------------------------7d4285f14803b8
Content-Type: text/xml
Content-Id: <doc_1>

<books>
  <book isbn="0345374827"><title>The Great Shark Hunt</title>
  <author>Hunter S. Thompson</author></book>
  <book><title>Life with Father</title><author>Clarence Day</author></book>
</books>

----------------------------7d4285f14803b8--
```

ヘッダ

メタデータ

ドキュメント

Note extra dashes

主要リソース

- Tomcat (assuming Java)
- Apache
  - 双方向の認証をサポート (ATNAのノード認証部分)
- ebxmlrr - Source Forge project
- Iheos - Source Forge project

テスト及び関連リソース

関連リソース

- **ihe.net**
  - スキーマ、例、レジストリの初期化用のメタデータ
- **Test Kit (NIST)**
  - XDSトランザクションに対するすべてのテストを定義
  - ソースコード及びメタデータの例を含む
- **Metadata Cookbook**
- **NIST Public Registry**
  - レジストリ及びリポジトリ･アクタの実装
  - すべてのイベントの捕捉のツール
  - 試験者が確認可能なログのビューア
  - テストのための患者IDの登録用Webページ
- **Test Result Reporting**

IHE : ATNA (Audit Trial and Node Authentication)

IHE-J ベンダワークショップ2009

（2008･05･21）

接続検証委員会

IHE での PHI（患者情報）保護

- User Identity（ユーザ識別）→ PWP, EUA
- User Authentication（ユーザ認証）→ EUA, XUA
- Node Authentication（ノード認証）→ ATNA
- Security Audit Trails（監査証跡）→ ATNA
- Data Integrity Controls（データ完全性）→ CT, ATNA TLS option
- Data Confidentiality（データ機密性）→ ATNA TLS option
- Access Controls（アクセス制御）→ IHEロードマップの今後の作業項目

ATNA：概要、スコープ

- 各システムに対する基本的なセキュリティ特性を定義。セキュリティおよびプライバシー環境の一部として使用される。
- IHE放射線部門の基本セキュリティプロファイル（2002年に制定）を、他の場面に適用できるように拡張。
- ホストレベルの認証を提供する。EUAおよびXUAによるユーザ認証と連係して使用される。

ATNA：価値に関する命題

- **患者のプライバシーおよびシステムセキュリティの保護：**
  - 倫理および法規上の要求を満たす
- **施設管理上の利便性：**
  - 統一された同一の監査システム
  - 複数ベンダの共通のアプローチで、施設間のポリシーおよびプロトコル定義が単純化される
  - 共通のアプローチで管理が簡素化される
- **コードの再利用で、開発及び保守コストが削減できる：**
  - ベンダは、一回の開発の手間で、複数のアクタをサポートすることができる。
  - 一回の開発の手間で、さまざまなセキュリティポリシー及び法規的な環境のニーズをサポートできる

ATNA：セキュリティ要件

- **動機：診療での利用とプライバシー**
  - 許可された人のみ、患者の臨床データにアクセスで、その情報は、他には開示されてはならない
  - 不許可の人が操作の妨害やデータの改ざんをできないようにすべきである
- **手続きとセキュリティ機構により、以下を保証する**
  - Confidentiality（機密性）
  - Integrity（完全性）
  - Availability（利用可能性）
  - Authenticity（真正性）

ATNA：セキュリティ対策

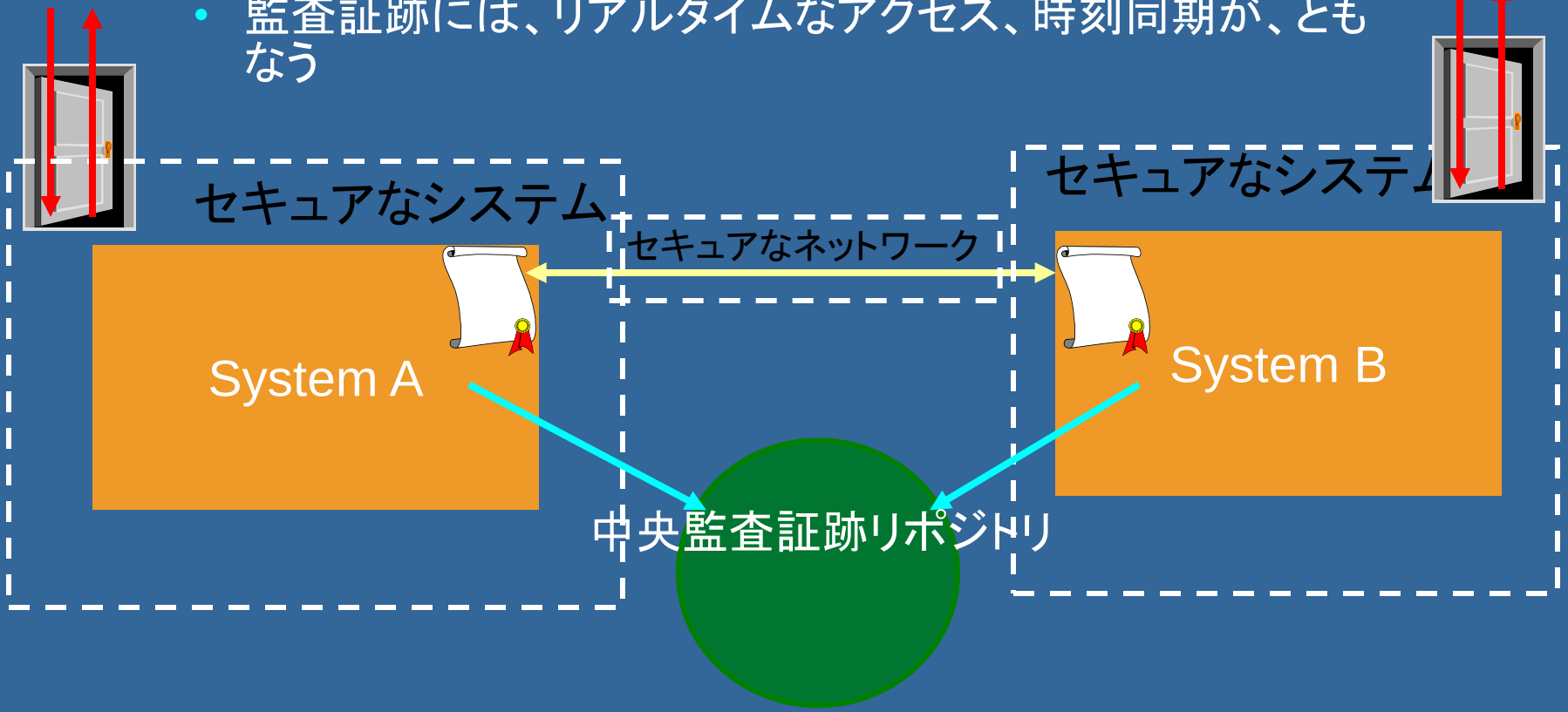
- **認証（Authentication）：**
- *ユーザ及びシステムの識別の確立、「あなたはだれか？」に答える*
  - ATNAは、ネットワーク接続の認証方法を定義する
  - ATNAは、認証機構をサポートする。例えば、EUA（Enterprise User Authentication ）、またはXUA（Cross Enterprise User Authentication ）。
- **許可及びアクセス制御（Authorization and Access control）**
- *ユーザのできる行為を確立する。例えば、データへのアクセスで、「あなたがだれかは分かったが、できることは何か？」に答える*
  - ATNAは、ネットワーク接続の認証方法を定義する
  - ATNAは、、ローカル及びネットワークアクセスの両方に対するシステムの内部機構を要求する。
- **説明責任及び監査証跡（Accountability and Audit trail）**
- *ある期間中の、ユーザ又はシステムの動作の履歴を確定する。「何を行なったか？」に答える。*
  - ATNAは、監査証跡のメッセージ形式及び転送プロトコルを定義する

ATNA：IHE の目標

- **IHEは、ノード間のセキュリティ管理を容易にする**
  - より洗練されたシステムも利用可能であるが、単純な人手による証明書の取り付けだけを必要とする
  - さまざまなアプローチのニーズに応えるために、認証、許可、説明責任の機能を分離する
  - 「事後監査」及び実行時の視認性により、誘導された運用

ATNA：信頼できるノードの統合

- ローカルアクセス制御（ユーザ認証）
- リモートノードの強力な認証（デジタル証明書）
- ネットワーク上の暗号化は、必須ではない。オプション
- 監査証跡には、リアルタイムなアクセス、時刻同期が、ともなう



ATNA：適切なネットワーク環境

- **物理的にセキュアなネットワーク**
  - 他のノードからのアクセスを防止できる物理的に明確に安全か、
  - 又は、同等なネットワークを隔離するVPN及びVLAN技術。
- **保護されたネットワーク**
  - 不許可の機器の変更、取り付けを防止する物理的なセキュリティがある
  - ネットワークは、患者情報への制限なしのアクセスを許さない施設内では、他の認証されたノードと共用される。
- **保護されたないネットワーク**
  - 十分なノードレベルセキュリティがあり、暗号化を用いたノードは、安全であるかもしれないが、一般にはサポートしない。

ATNA：ノードセキュリティ

- ATNAは、アクセス制御などの必要な機能の一部を指定する
- ATNAはポリシーを指定しない
- EUAなどの他のIHEプロトコルが、候補であるが、ATNAは、メカニズムは指定しない
- ベンダと施設は、ノードセキュリティにより、ATNAプロファイルに矛盾することなく、独自の適合する技術とポリシーを選択可能

ATNA：ノード認証

- X.509証明書をノードの識別及びキーとして使用する
- TCP/IPトランスポート層セキュリティプロトコル（TLS)をノード認証、及びオプショナルな暗号化に使用する
- アソシエーション確立時に、両者のセキュアハンドシェ - クプロトコルが、つぎを行なう。
  - 暗号プロトコルの識別
  - セッションキーの交換
- アクタは、許可されたノードの証明書リストを構成できなければならない
- ATNAは、現在、HTTP,DICOM,HL7に対するメカニズムを規定している。

なぜ、ノード認証なのか？

- CTシステムなどのように、多くのシステムで、そのアクセスが共有されている。マシンの識別は、操作者の識別よりも、セキュリティのためには、より重要である。
  - 1つのCTの操作は、CTシステムからのCT記録を更新だけがゆるされる
- PACSアーカイブなど、自律的に動作するシステムもある
  - PACSの活動をモニタする際は、、PACSの従事している管理責任者を識別することは、できないこともありうる。だれも、ログインしてないかもしれない。
- マシンのアクセスは、通常、サイト管理者により制御される。
  - 許可されたユーザであっても、個人のマシンを使用してことは禁止される

ATNA:監査システム

- use.法的な用途ではなく、監視の目的で設計されている
- 2種類の監査メッセージ形式
  - IHE放射線部門用の暫定形式。放射線部門との下位互換性がある
  - IETF/DICOM/HL7/ASTM形式。将来、さらに拡張される。
    - DICOM Supplement 95
    - IETF Draft for Common Audit Message
    - ASTM E.214
    - HL7 Audit Informative documents
- 両方の形式は、XMLでコード化されたメッセージであり、XML標準を用いて、拡張が可能。

ATNA：監査イベント(1)

Actor-start-stop	*The starting or stopping of any application or actor.*
Audit-log-used	*Reading or modification of any stored audit log*
Begin-storing-instances	*The storage of any persistent object, e.g. DICOM instances, is begun*
Health-service-event	*Other health service related auditable event.*
Images-availability-query	*The query for instances of persistent objects.*
Instances-deleted	*The deletion of persistent objects.*
Instances-stored	*The storage of persistent objects is completed.*

Medication	*Medication is prescribed, delivered, etc.*
Mobile-machine-event	*Mobile equipment is relocated, leaves the network, rejoins the network*
Node-authentication-failure	*An unauthorized or improperly authenticated node attempts communication*
Order-record-event	*An order is created, modified, completed.*
Patient-care-assignment	*Patient care assignments are created, modified, deleted.*
Patient-care-episode	*Auditable patient care episode event that is not specified elsewhere.*
Patient-record-event	*Patient care records are created, modified, deleted.*

ATNA：監査イベント(2)

PHI-export	*Patient information is exported outside the enterprise, either on media or electronically*
PHI-import	*Patient information is imported into the enterprise, either on media or electronically*
Procedure-record-event	*The patient record is created, modified, or deleted.*
Query-information	*Any auditable query not otherwise specified.*
Security-administration	*Security alerts, configuration changes, etc.*
Study-object-event	*A study is created, modified, or deleted.*
Study-used	*A study is viewed, read, or similarly used.*

ATNA: 監査イベントの記録

- 監査記録のトランスポートには、Reliable Syslog (RFC 3195) が、優先されるが、BSD Syslog protocol (RFC 3164) も、放射線部門基本セキュリティとの下位互換性のため使用可能である
- 監査証跡イベントの内容は、IETF, DICOM, HL7, 及び ASTM 標準に準拠する。放射線部門基本セキュリティの監査イベント形式も下位互換性があるため使用可能である

セキュアノードにするために(1)

- 各アクタだけでなく、ホスト全体が安全でなければならない
- ホスト全体は、識別、認証、及び許可のために、適切なユーザアクセス制御がなされなければならない
- 保護情報を転送する通信は、すべて認証され、傍受から保護されなければならない。これは、IHEトランザクションだけでなく、あらゆるプロトコルが該当する
- IHEアクタだけでなく、すべての医療情報活動は、監査証跡を生成すべきである

セキュアノードにするために(2)

- セキュアノードは、監査機能を単純に追加するだけでなく、完全にするには、以下の作業を含む。
  - すべてのアプリケーションを監査証跡イベントを検知し、監査証跡メッセージを生成するように設定する
  - すべての通信接続が、保護されていることを保証する
  - すべてのローカルリソースを保護するために、ローカルなセキュリティ機構を確立する
  - 以下の構成機構を確立する。
    - 時刻の整合性(CT)プロファイルを利用した時刻同期
    - 証明書の管理
    - ネットワークの構成
- 監査証跡ログ機能を実装する

CT (Consistent Time)

- 時刻の同期には、ネットワークタイムプロトコル（NTP）V3（RFC1305）を使用
- アクタは手動による構成調節をサポートしなければならない
- 要求される精度：1秒
- オプショナルとして、セキュアNTPを使用できる
- ATNA,EUA,XUAでは、CTが必要になる

詳細情報

- IHE Web sites: www.ihe.net
- Technical Frameworks, Supplements
  - ITI V1.0, RAD V5.5, LAB V1.0
- Non-Technical Brochures :
  - Calls for Participation
  - IHE Fact Sheet and FAQ
  - IHE Integration Profiles: Guidelines for Buyers
  - IHE Connect-a-thon Results
  - Vendor Products Integration Statements

IHE：PIX/PDQ
（PIX – Patient Identifier Cross-referencing
PDQ – Patient Demographics Query）

IHE-J ベンダワークショップ2009

（2009･05･21）

接続検証委員会

PIX/PDQ：XDS環境での患者IDサービス

- すべての施設（参加医療機関）に対して、ドメイン内の患者に付与されたIDを登録する
- 施設は、関係する患者インデックスを継続して管理する
- 他のシステムの患者IDについて、ドメインシステムの問い合わせをサポートする
- 他のシステムが患者IDを更新したとき、ドメインのシステムに通知する（オプション）

PIX/PDQ：価値

- 一定の場所に住んでいる患者に対して、すべてのシステムの患者IDを維持する
- 異なるIDドメインを越えて患者をマッチングするアルゴリズムを用いる
- システム間でデータをつき合わせるコストを下げる
  - 既存のシステムにおいてIDをつけたり、形式を変換する必要がなくなる
- IHEで、すでに使われている規格やトランザクションを用いる

PIX：効果

- マスタ患者IDを必要としない（分散的に対応可能）
- PIXマネジャは、統合した患者情報を生成する必要がない（患者情報そのものは各ドメインで管理）
- どの患者IDドメインもマスタ患者IDを生成しているとみなすことができる
- 患者情報は、ADTアクタが責任をもつ。患者登録が分散化する場合は、患者情報問合わせ統合プロファイル（PDQ）を用いる

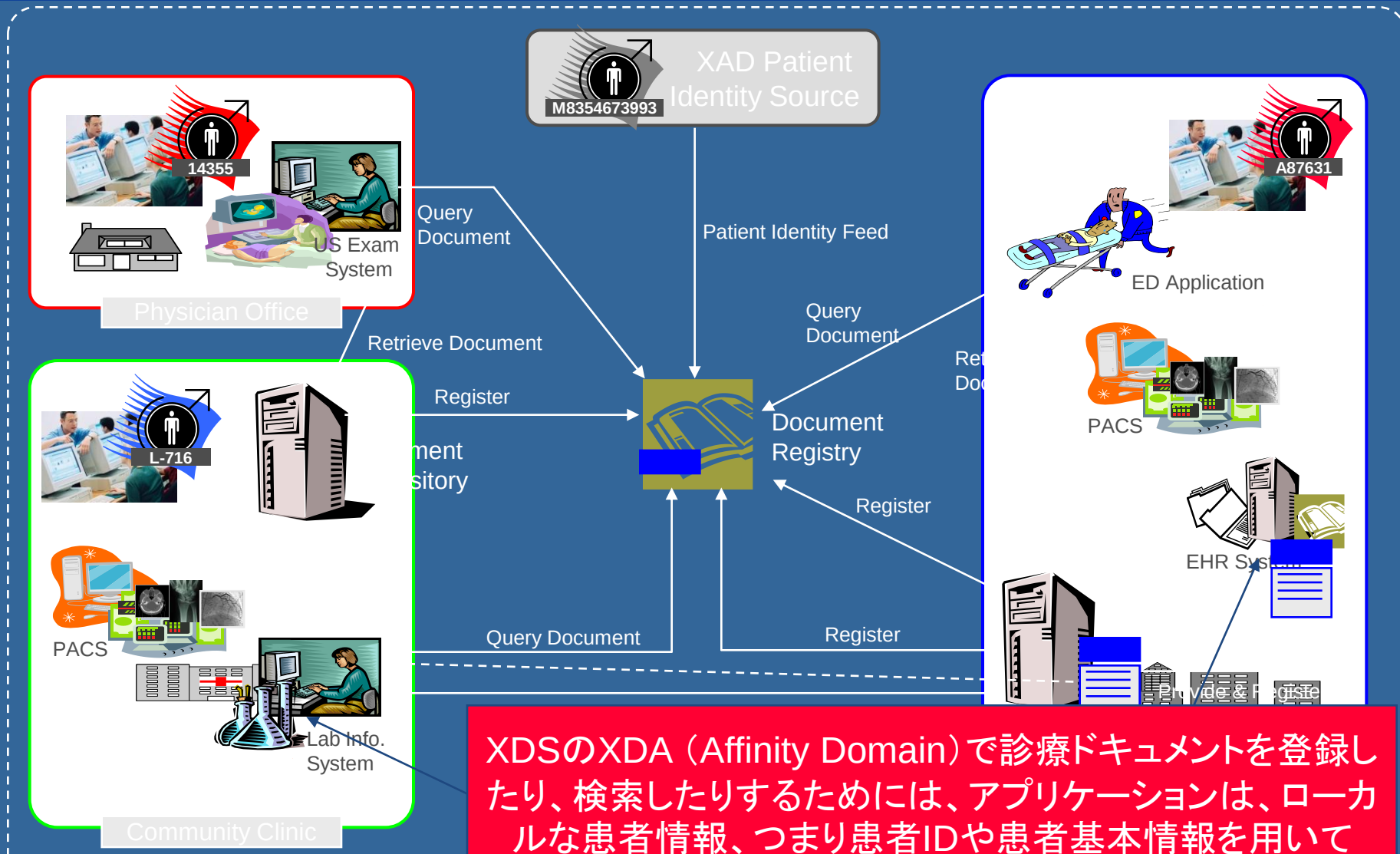
PDQ：効果

- 共通の患者名、識別子、関係、および来院情報を含む
- 患者リストの迅速な検索を可能とする
- 完全な識別データを得ることができないとき、正しい患者の選択を可能とする
- 患者情報と来院情報の部分的なものだけに制限する

HL7Queryの採用
HI7V2,又はV3メッセージ

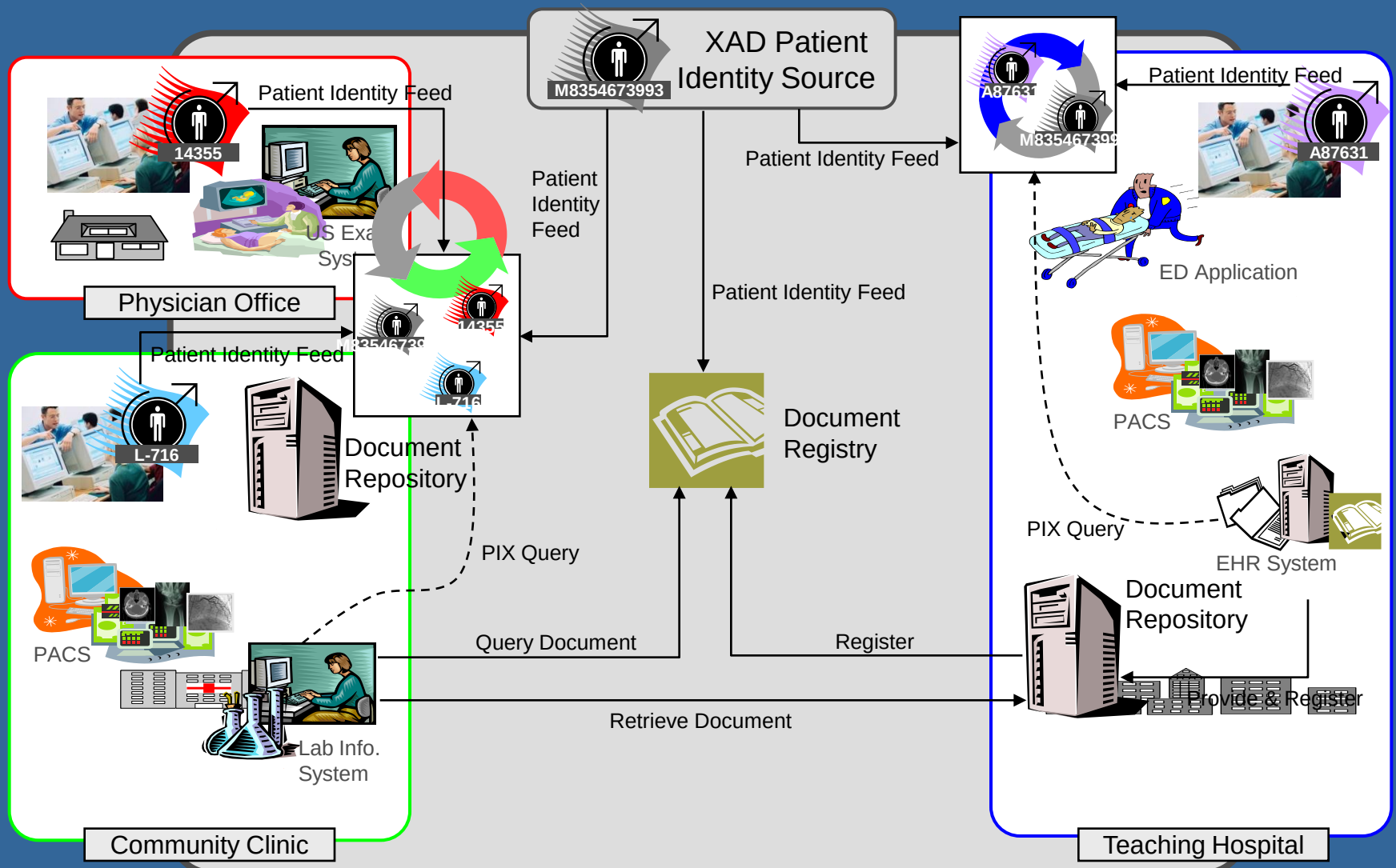
- **最初は、ADTトランザクションに対しては、HL7V2メッセージをサポート。**
  - A01 Admit Patient, A04 Register Patient, A08 Update Patient Info, など
  - “I” ベースにした形式の、すべてのHL7 V2 ADTメッセージが、定義され、サポートされる。
- **HL7V3RIM (Reference Information Model) をサポートを開始**
  - HL7 V3標準バージョン7. 5のサポートを開始
  - HL7V3Queryメッセージのみが、テストされている
  - 現在、カナダのHealth Infoway、およびIHEで、新規のサポート要求が議論されている
- **HL7Query Adaptorとして、バージョン7.0を公式にサポート開始**
  - HL7 Q (Query) および K (Response) メッセージをサポート
  - IHEで利用する主要なサポートは、以下のメッセージ
    - Q22 (Find Candidates)
    - Q23 (Get Corresponding Identifiers)
  - 他のQベースのメッセージもサポートできる

XDS: RHIOにおける診療情報の共有



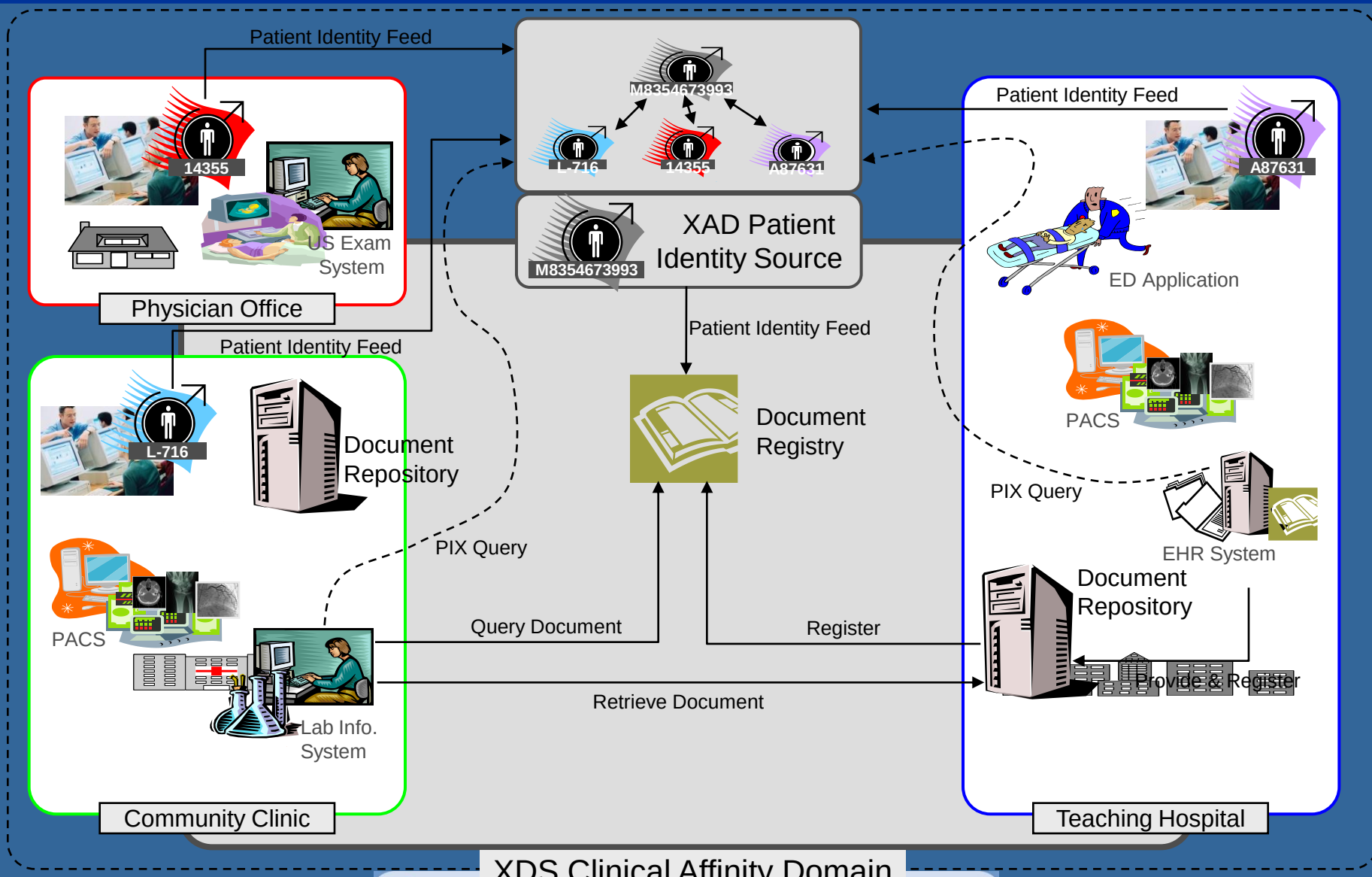
XDSのXDA（Affinity Domain）で診療ドキュメントを登録したり、検索したりするためには、アプリケーションは、ローカルな患者情報、つまり患者IDや患者基本情報を用いてXADの患者IDを調べる必要がある。

ローカルなPIX Serviceを用いた、XDSアフィニティドメインの患者IDの調査

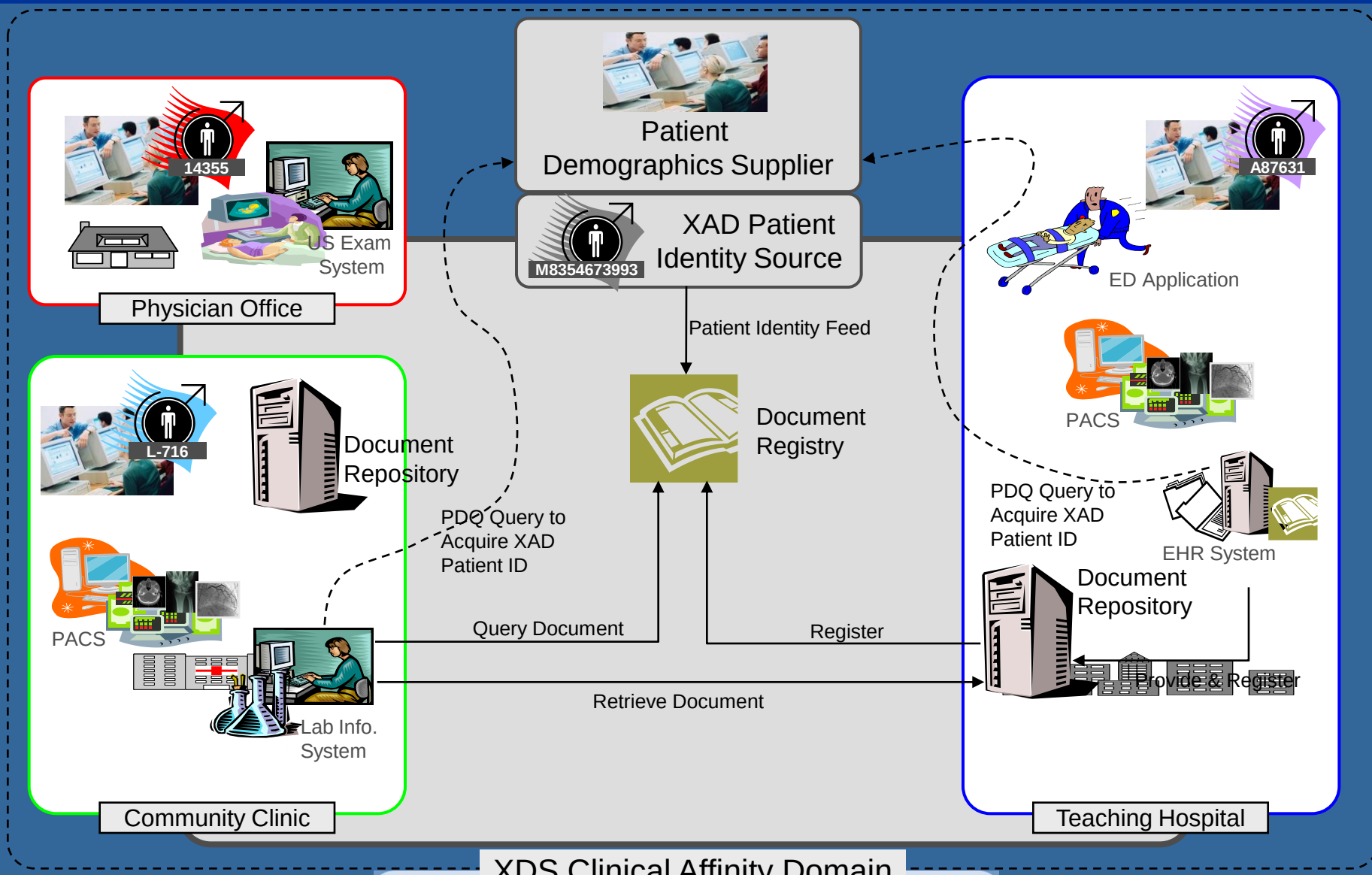


XDS Clinical Affinity Domain

XDSアフィニティドメインのPIX Serviceを用いた、XDSアフィニティドメインの患者IDの調査



XDSアフィニティドメインの患者IDの検索のための、XDSアフィニティドメインのPDQ Serviceへのクエリ



IHE：ITIプロファイル
EHR運営のための強固な基礎を提供

患者ヘルス情報（PHI：Patient Health Information ）施設間の管理原則：

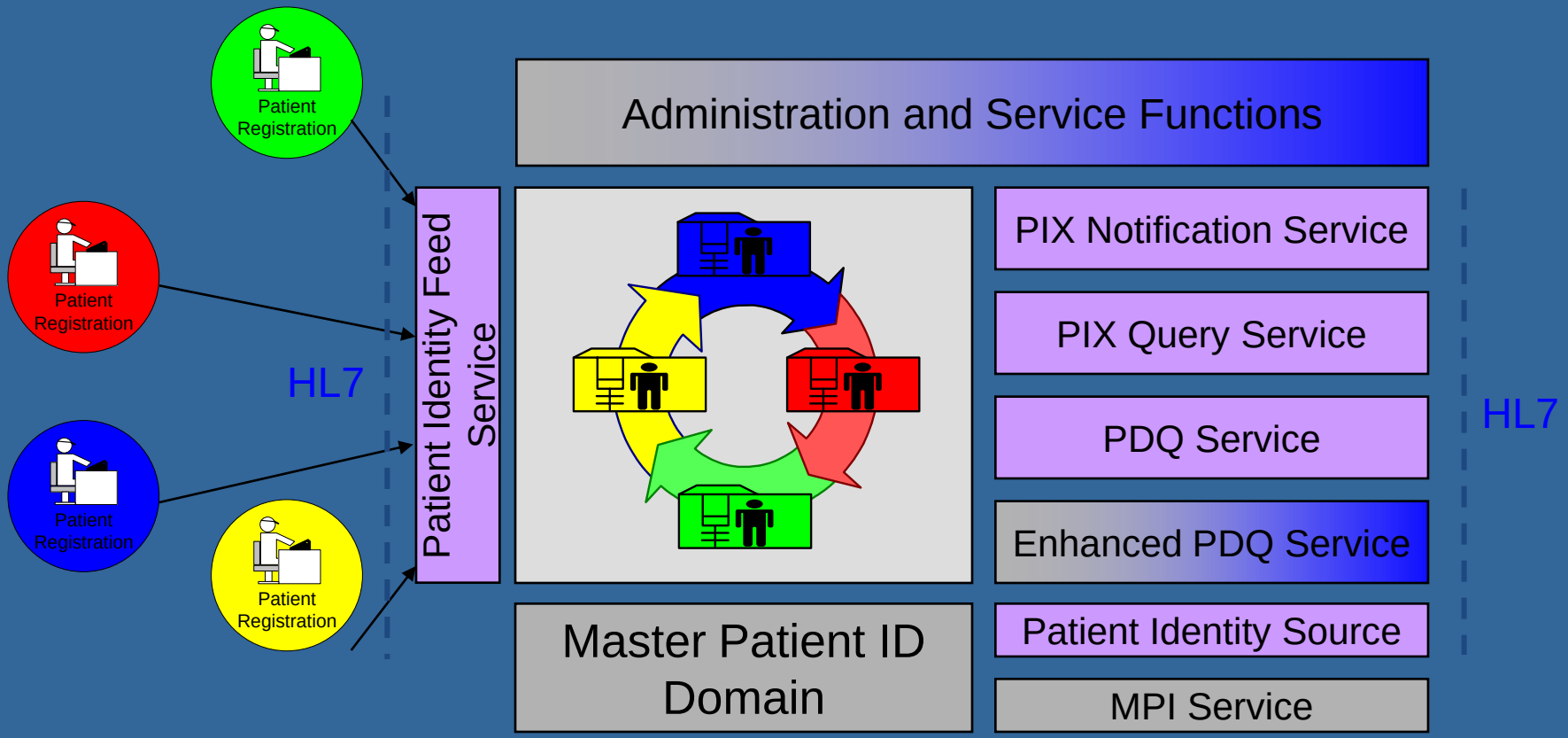
- 患者情報ソースが、患者記録（基本情報）を管理、そのドメインでのそれらの患者の記録を識別するため、患者IDドメインを管理する患者IDは、管理された患者IDドメイン内で、割当てられ、維持される
- （患者情報ソース内の）患者記録を検索

  → PDQ Integration Profile連係ドメインで、患者IDを調査

  → PIX Integration Profile
- ヘルスケア情報(ドキュメントまたはサービス）を格納する

  → XDS Integration Profile

IHE PIX / PDQ プロファイルの実装



Service defined in IHE Technical Framework

Service out of IHE scope

IHE : PWP
（ Personnel White Pages ）

IHE-J ベンダワークショップ2009

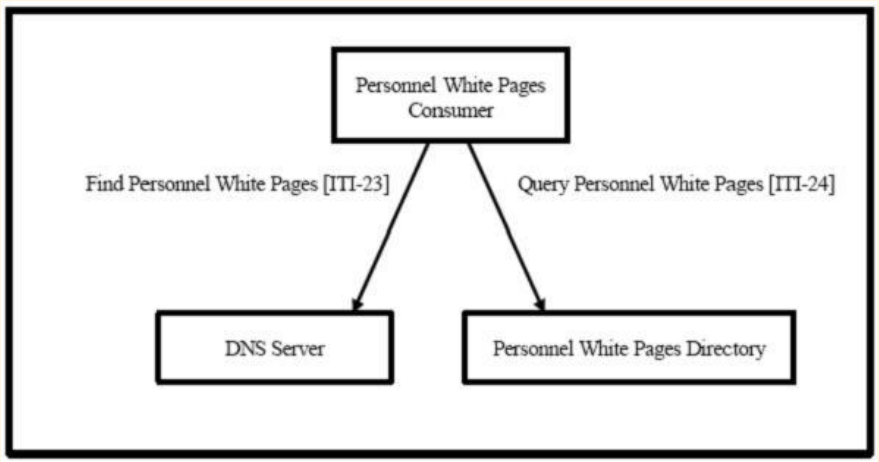
（2009･05･21）

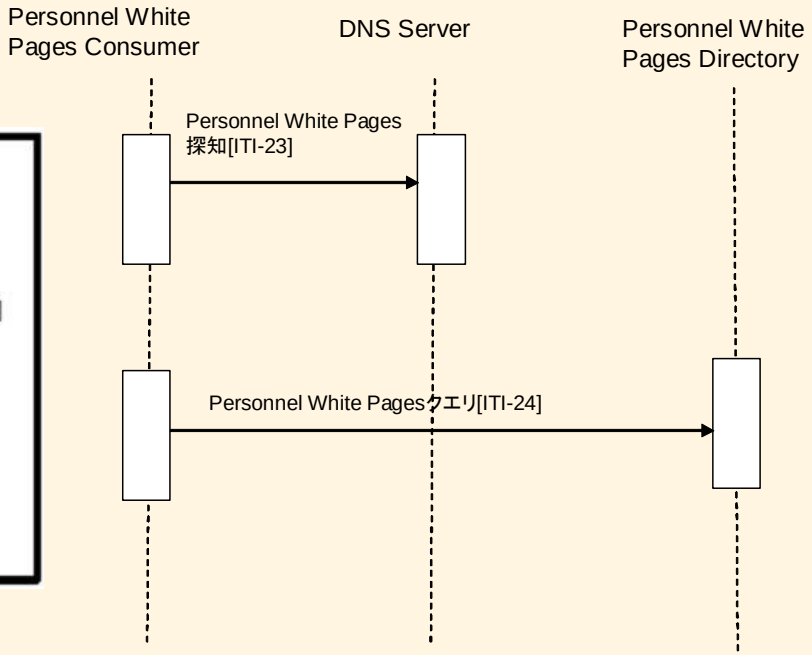
接続検証委員会

PWP: Personnel White Pages

- **PWP: 職員登録簿**
- **Domain Naming System (DNS)**
- **Light Weight Directory Access Protocol (LDAP)**
  - LDAP Query/Response
  - RFC2798 DefinetOrgPerson Object Class
- **LDAP は、EUAシングルサインオンの基盤**

PWP:トランザクション





アクタ	トランザクション	必須(R)／オプショナル(O)	Vol.2内の節
Personnel White Pages Consumer	Find Personal White Pages (ホワイトページ探知)	O	ITI TF-2:3.23
	Query Personal White Pages (ホワイトページクエリ)	R	ITI TF-2:3.24
DNS Server	Find Personal White Pages (ホワイトページ探知)	R	ITI TF-2:3.23
Personnel White Pages Directory	Query Personal White Pages (ホワイトページクエリ)	R	ITI TF-2:3.24

メンバ属性一覧

属性	定義	必要性	備考
description	説明	O	
dn	識別名	R	
facsimileTelephoneNumber	FAX番号	R2	組織部署の代表FAX番号 属性名は「fax」としても可
l	地域名	O	
labeledURI	URI	O	組織・部署へのアクセスURI 定義する場合、objectClassとしてlabeledURIObjectを設定する
o	組織	R2	objectClassとして「organization」を指定した場合は必須（R）
objectClass	オブジェクトクラス	R	組織の場合はorganizationを必ず指定し、o属性を必ず設定する。 組織部署の場合はorganizationalUnitを必ず指定し、ou属性を必ず指定する。
ou	組織内の部署名	R2	objectClassとして「organizationalUnit」を指定した場合は必須（R）
physicalDeliveryOfficeName	郵便局名	R2	
postalAddress	住所	R2	
postalCode	郵便番号	R2	
postOfficeBox	郵便局の私書箱	R2	
preferredDeliveryMethod	配達方法	O	
registeredAddress	配達証明が必要な場合、書類の受け取りに使用する住所	O	
seeAlso	参照	O	
st	州、あるいは郡	R2	
street	ストリートアドレス	R2	
telephoneNumber	電話番号	R2	部署の代表電話番号

組織属性一覧(1)

属性	定義	必要性(IHE)	備考
aliasdObjectName	エイリアスオブジェクト名	O	複数定義不可 定義する場合、objectClassにaliasを必ず定義する
audio	音声	D	
businessCategory	ビジネスカテゴリ	D	
carLicence	自動車免許IDあるいは自動車のナンバープレート	O	
cn	氏名	R	
departmentNumber	所属部署コード	O	
description	説明	D	
destinationIndicator	伝送先インジケータ	D	
displayName	表示名	R	複数定義不可
employeeNumber	従業員番号	O	複数定義不可
employeeType	雇用形態	O	
facsimileTelephoneNumber	FAX番号	R2	
givenName	名前(ファーストネーム)	R2	
homePhone	自宅電話番号	O	
homePostalAddress	自宅住所	O	
Initials	イニシャル	R2	
internationalISDNNumber	国際ISDN番号	D	
jpegPhoto	JPEG形式の写真	O	
l	地域名	O	
labeledURI	URI	O	
mail	電子メールアドレス	R2	
manager	マネージャ	O	
mobile	携帯電話番号	R2	
o	組織	R2	
objectClass	オブジェクトクラス	R	最低限、Person、organizationalPersonとinetOrgPersonを指定する(属性設定例参照) cf: objectClass: Person objectClass: organizationalPerson objectClass: inetOrgPerson

属性	説明	必要性	備考
dn	識別名	R	
c	国名	O	複数定義不可

組織属性一覧(2)

属性	定義	必要性(IHE)	備考
ou	組織内の部署名	R2	
pager	ページャー電話番号	R2	
photo	写真	D	
physicalDeliveryOfficeName	郵便局名	R2	
postalAddress	住所	R2	
postalCode	郵便番号	R2	
postOfficeBox	郵便局の私書箱	R2	
preferredDeliveryMethod	配達方法	O	複数定義不可
preferedLanguage	登録メンバーが読み書きするのに好ましい言語	R2	複数定義不可
registeredAddress	配達証明が必要な場合、書類の受け取りに使用する住所	O	
roomNumber	居室番号	O	
secretary	秘書	O	
seeAlso	参照	D	
sn	苗字(Surname)	R	
st	州、あるいは郡	R2	
street	ストリートアドレス	R2	
telephoneNumber	電話番号	R2	
teletexTerminalIdentifier	テレテックス端子識別子	D	
telexNumber	テレックス番号	D	
title	肩書き、役職名	R2	
uid	ユーザID	R	
userCertificate	ユーザID証明書	D	
userPassword	ユーザパスワード	D	ITI-TF-2では「Generally Not Accessible」とある。しかし各自のデータを自分で管理する場合、および何らかのアクセス制限をかける場合は必要
userPKCS12	ユーザPKCS#12	D	
userSMIMECertificate	ユーザSMIME証明書	O	
x121Address	X121のアドレス	D	
X500uniqueIdentifier	ユニーク識別子。識別名dnが再利用されたときに、オブジェクト間で区別するために使用する。	R	

LDAP V3　関連参考サイト

- 第1回　OpenLDAPの設計
  http://www.atmarkit.co.jp/flinux/rensai/openldap01/openldap01a.html
- 2 標準的なLDAP APIを使用したアプリケーションの開発
  http://otndnld.oracle.co.jp/document/products/id_mgmt/101401/doc_cd/idmanage.1014/B31464-01/concepts.htm#141577
- LDAPによるHP-UXアカウントの管理
  http://h50146.www5.hp.com/products/software/oe/hpux/developer/tips/ldap/ldap_06.html
- Solarisネーミングサービス/ディレクトリサービス
  http://jp.sun.com/practice/software/solaris/jp/8/ds/ds-namingdirectory/

IHE : PAM
（Patient Administration Management）

IHE-J ベンダワークショップ2009

（2009･05･21）

接続検証委員会

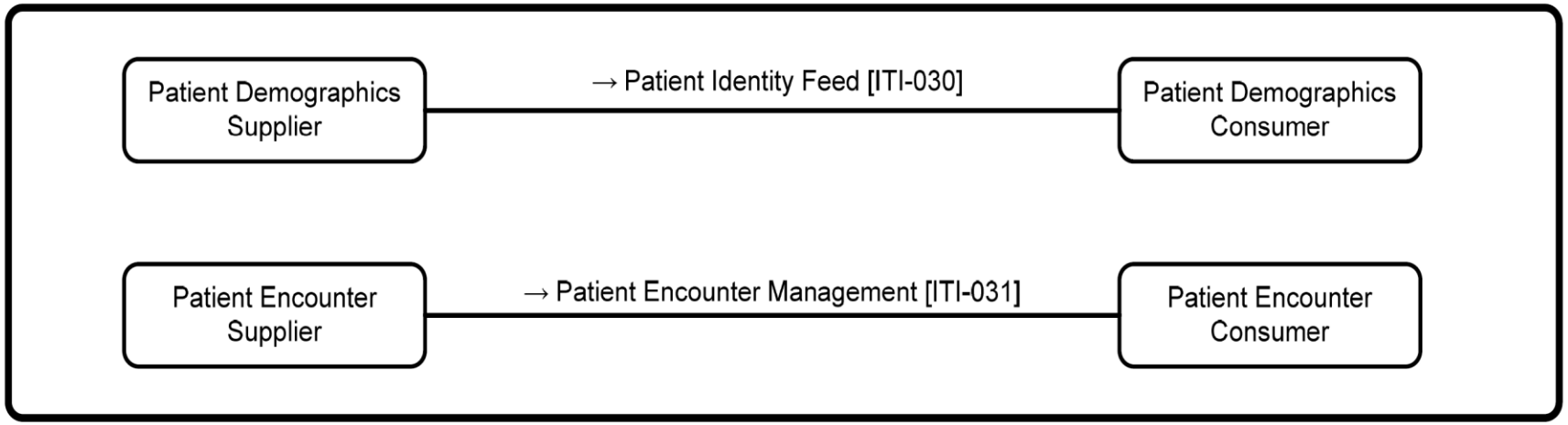
PAM: 患者ID、入院・受診管理

- 患者ID、診察情報、緊急治療内の移動等に連動した情報の変更をサポート
- メッセージ交換に基づくトランザクションを定義
- ユースケース
  - 患者ID管理ユースケース
  - 患者受診管理のユースケース

ユースケース例

イベント	内容
Patient Registration (患者登録):	患者が年次定期健診のためクリニックへ到着。患者記録は前もってPatient Demographics Supplierが作成し、Patient Demographics Supplierアクタとのグループ化を通じ、クリニックの登録システムに存在する。医院患者登録システムにより、Patient Registrationメッセージが、ローカルなAncillary System（補助的システム）と提携病院のADTシステムに送信される。
Change Outpatient to Inpatient (外来から入院への変更):	健診で、患者の深刻な病状が発見され、即時入院が勧められる。患者は入院のため、提携病院へ紹介される。Change Outpatient to Inpatientメッセージが、病院のADT Systemへ送信される。
Pre-admit Patient for Hospitalization (入院のための予備入院):	患者は関連する検査のため、病院へ予備入院する。病院のADTシステムから、病院のAncillary Systemへ、Patient Pre-Admitメッセージが送信される。
Patient Admitted Notification (患者入院通知):	検査で病状が確認され、患者は病院のICUへ入院。病院のADTシステムからAncillary Systemへ、Admission Notificationメッセージが送信される。
Patient Insurance Information Update (患者保険情報更新):	ICUへ入院中、患者の保険について確認が行われ、病院のADTから病院のAncillary System へ更新情報が送信される。
Patient Location Transfer (患者移送):	1日ICUに入院した後、患者の病状は改善し、一般病室へ転送される。病院のADTシステムから病院のAncillary Systemへ、Patient Transferメッセージが送信される。
Patient Location Transfer Error Reconciliation (患者移送エラーの調整):	転送について記録する看護師がミスを犯し、間違った病室とベッドが入力される。エラーが発見されたあと、病院のADTシステムから Hospital Ancillary System へ、Cancel Patient Transferメッセージが送信され、続いて新しいPatient Transferメッセージが送信される。
Patient Pending Discharge (患者退院手続中):	患者は回復し、退院しようとしている。ADTシステムからAncillary System へ、Patient Pending Dischargeメッセージが送信される。
Change Inpatient to Outpatient (入院から外来への変更):	病院の手順にしたがって、患者はフォローアップ検査の管理のため外来患者用のユニットへ転送される。ADTシステムから、Hospital Outpatient Registration Systemへ、Change Inpatient to Outpatientメッセージが送信される。
Register Patient as Outpatient (外来患者として登録):	患者は、Hospital Outpatient Registration Systemに登録し、そこから病院のADTシステムとAncillary System に、Patient Registrationメッセージが送信される。
Patient Discharged from Outpatient System (外来患者システムからの退院):	外来診察が終了する。Patient Dischargeメッセージが、病院ADT SystemとHospital Ancillary Systemへ送信される。
Patient discharged from Hospital ADT System (病院ADTシステムからの退院):	患者は十分な検査結果に基づき退院する。病院のADTシステムからAncillary Systemへ、Patient Dischargeメッセージが送信される。

PAM:トランザクション



アクタ	トランザクション	必須（R）／オプショナル（O）	Vol.2内の節
Patient Demographic Supplier	Patient Identity Feed	R	ITI TF-2:3.30
Patient Demographic Consumer	Patient Identity Feed	R	ITI TF-2:3.30
Patient Encounter Supplier	Patient Encounter Management	R	ITI TF-2:3.31
Patient Encounter Consumer	Patient Encounter Management	R	ITI TF-2:3.31

PAM: オプション

- Marge（統合）オプション
- Link／Unlink（リンク／リンク削除）オプション
- Inpatient／Outpatient Encounter Management（入院／外来患者診察管理）オプション
- Pending Event Management（中断イベント管理）オプション
- Advanced Encounter Management（高度診察管理）オプション
- Temporary Patient Transfer Tracking（一時的患者移動証跡）オプション
- Historic Movement（履歴移動）オプション

PAM: オプション

アクタ	オプション	Vol.＆セクション
Patient Demographic Supplier	統合	ITI TF-2: 3.30
	リンク／リンク削除	ITI TF-2: 3.30
Patient Demographic Consumer	Marge (統合)	ITI TF-2: 3.30
	Link／Unlink(リンク／リンク削除)	ITI TF-2: 3.30
Patient Encounter Supplier	Inpatient/Outpatient Encounter Management	ITI TF-2: 3.31
	Pending Event Management	ITI TF-2: 3.31
	Advanced Encounter Management	ITI TF-2: 3.31
	Temporary Patient Transfer Tracking	ITI TF-2: 3.31
	Historic Movement	ITI TF-2: 3.31
Patient Encounter Consumer	Inpatient/Outpatient Encounter Management	ITI TF-2: 3.31
	Pending Event Management	ITI TF-2: 3.31
	Advanced Encounter Management	ITI TF-2: 3.31
	Temporary Patient Transfer Tracking	ITI TF-2: 3.31
	Historic Movement	ITI TF-2: 3.31


Questions?


Thank You.