# IT Infrastructure（IT基盤）2
# 具体説明

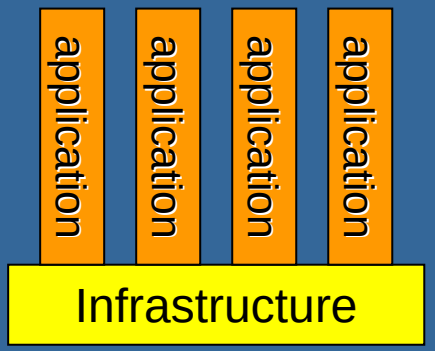
IHE-J ベンダーワークショップ 2006
大島　義光
（株）日立製作所 医療事業統括本部

# 目次

- IHE IT Infrastructureとは?
- 個別統合プロファイルの紹介
- 関連臨床部門でのXDSの応用
  - XDS-I、患者ケア連携（PCC）、XDS-LAB
- 関連、実装状況（IHE ITI オープンソース等）
- ロードマップ

# IHE IT Infrastructureとは?

- **IT Infrastructureとは...**
  - コンピュータ・アプリケーションの実行を可能にする
    - オペレーティング・システム
    - コンピュータ言語
    - ハードウェア
    - ネットワーク
  - 多種のアプリに役立つ
    - セキュリティ
    - データベース
    - インタフェース



# IHE IT Infrastructureとは?

- **IHE IT Infrastructureとは...**
  - 標準をベースにした IT infrastructure の実装ガイド、テクニカルフレームワークの一つ
  - 関係委員会
    - 企画委員会(Planning)– 各年の作業の承認と今後のロードマップ作成
    - 技術委員会(Technical)– テクニカルフレームワークの執筆とメンテナンス
  - 提供サービス
    - 関係者への教育活動
    - 各種の標準化機関やコンソーシアムとの協力
    - IHE内の各分野委員会との協力

# IHE IT Infrastructureとは?

- **IHE IT Infrastructure 部門で生成されるもの...**
  - IHEの各臨床部門に依存しない（つまり共通の）ワークフロー記述に用いられるプロファイル
    - 例：セキュリティ、記録の保存、患者管理
  - 基礎的な実装仕様の基盤。これは臨床部門で拡張される
    - 例：文書コンテンツの基本仕様、データ収集のための取り出し形式
  - 現在の作業項目に対する白書
    - 例：施設間利用者認証、Webサービス、リスク管理

# IHE IT Infrastructureとは?

- **統合プロファイル – 診療情報 1**
  - Document Sharing（文書共有）
    - XDS – Cross-Enterprise Document Sharing
      （施設間文書共有）
    - ★ XDS Stored Query – XDSへの追加統合プロファイル
    - ★ XDS-SD – XDS Scanned Documents
      （XDSスキャン文書）
    - ★ XDP – Cross-Enterprise Document Interchange
      （施設間文書交換）
    - NAV – Notification of Document Availability
      （文書入手可能通知）
    - RID – Retrieve Information for Display
    - （表示のための情報検索）

注）「★」は2006年新規追加

# IHE IT Infrastructureとは?

- **統合プロファイル – 診療情報 2**
  - 患者管理
    - PAM – Patient Administration Management
      （患者情報管理）
    - PDQ – Patient Demographics Query
      （患者基本情報の問合せ）
    - PIX – Patient Identifier Cross-referencing
      （患者IDの相互参照）
    - PSA – Patient Synchronized Applications
      （患者アプリケーション同期）
  - ★RFD – Retrieve Form for Data Capture
    （データ収集のための取り出し形式）

注）「★」は2006年新規追加

# IHE IT Infrastructureとは?

- 統合プロファイル – セキュリティ
  - ATNA – Audit Trial and Node Authentication
    （監査証跡とノード認証）
  - CT – Consistent Time
    （統一時刻）
  - DSG – Document Digital Signature
    （文書電子署名）
  - EUA – Enterprise Use Authentication
    （施設内利用者認証）
  - PWP – Personnel White Pages
    （職員登録簿）

# IHE IT Infrastructureとは?

- 次のステップ
  - XDS 連合化（地域間連携）
  - PIX、PDQ のHL7V3化
  - トランスポートレイヤーでのWebサービスの利用
  - XUA – Cross-Enterprise User Authentication（施設間利用者認証）
  - リスク管理計画の白書

# IHE IT Infrastructureとは?

救急時紹介状
患者作成のサマリ
心電図報告
検査結果文書コンテンツ
スキャン文書
画像情報
診療サマリ
(投薬, アレルギー, 問題)
文書コンテンツの書式と
関連する語彙コード

患者同意

文書電子署名
真正コピーまたは原本の証明

文書入手可能通知
新情報について知る

患者基本情報の問合せ

患者IDの相互参照
独立した複数のID領域にわたって
患者IDを対応付ける

施設間文書共有
(XDS)
患者EHRを構成する診療文書の、医療機
関間の登録、配布及びアクセス

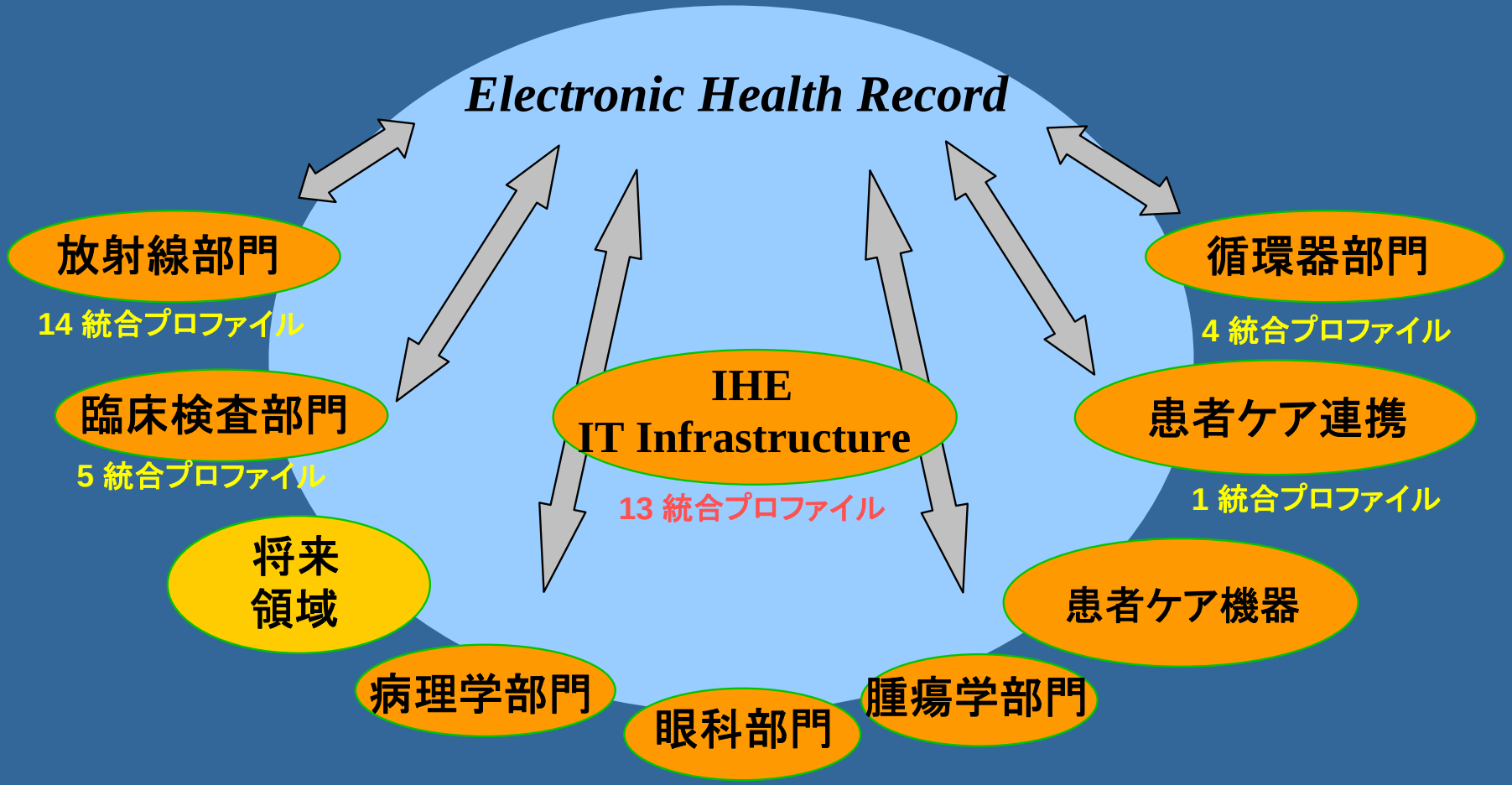
施設間文書交換
CD/USBメディア、及び電子メール送付

RHIOの
支援

監査証跡とノード認証
セキュアなドメインを形成するための
集中化した個人情報監査証跡と
ノード間認証

統一時刻
複数のネットワークシステムにわた
り、時刻を合わせる

# IHE IT Infrastructureとは?



# 個別統合プロファイルの紹介

- **文書共有**
  - XDS – 施設間文書共有
  - ★ XDS Stored Query
  - ★ XDS-SD – スキャン文書
  - ★ XDP – 施設間文書交換
  - NAV – 文書入手可能通知
  - RID – 表示のための情報検索
- **患者管理**
  - PAM – 患者情報管理
  - PDQ – 患者基本情報の問合せ
  - PIX – 患者IDの相互参照
  - PSA – 患者アプリケーション同期
- ★ **RFD – データ収集のための取り出し形式**
- **セキュリティ**
  - ATNA – 監査証跡とノード認証
  - CT – 統一時刻
  - DSG – 文書電子署名
  - EUA – 施設内利用者認証
  - XUA – 施設間利用者認証
  - PWP – 職員登録簿

注）「★」は2006年新規追加

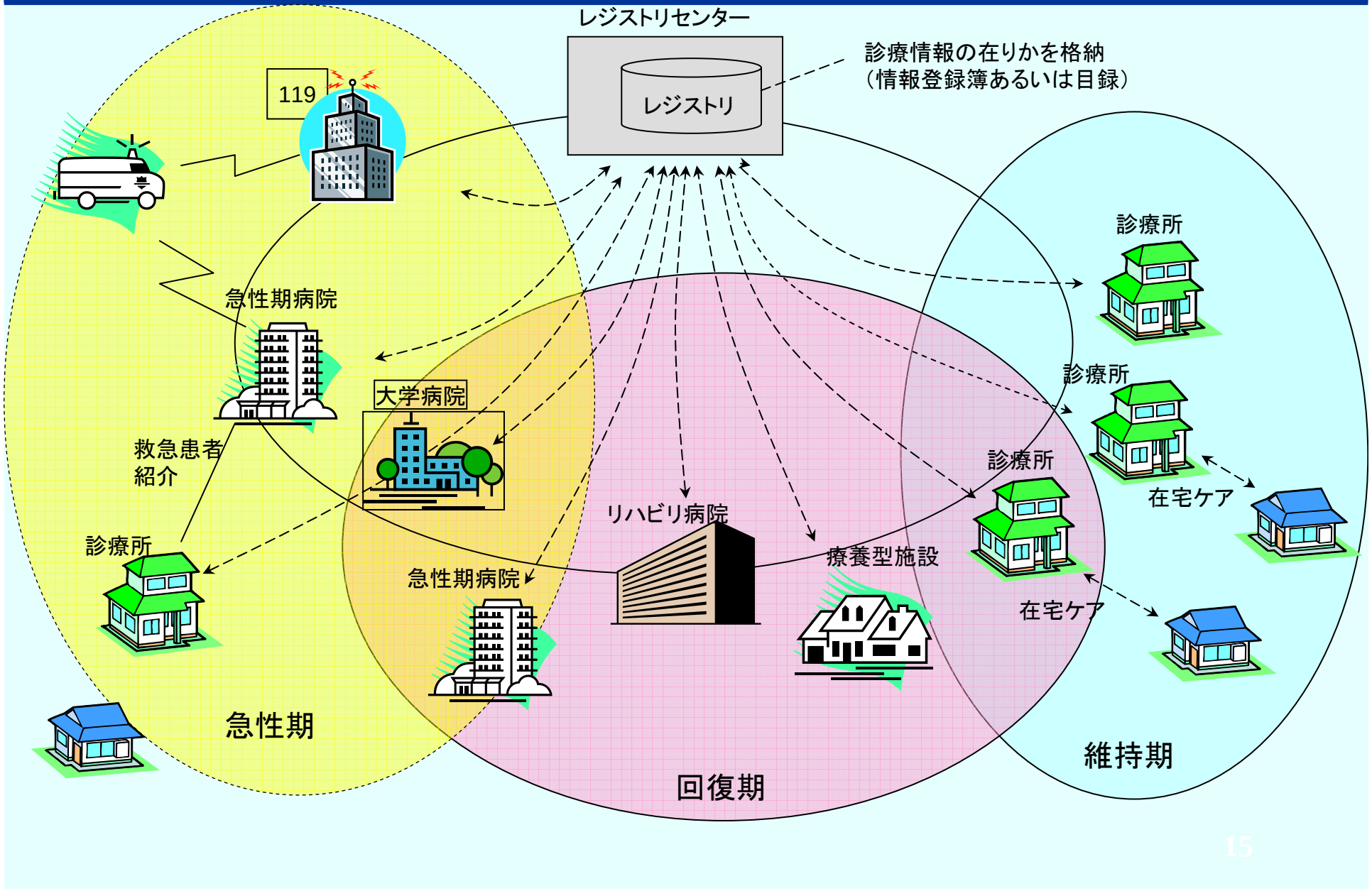
# 施設間文書共有（XDS）

- 異なる医療施設間にわたる診療文書の共有（登録、配布とアクセス）のサポート
- IHE IT Infrastructureで、施設間用の中心となる統合プロファイル
- 文書トレジストリ（診療録登録簿）と、文書リポジトリ（診療録保管庫）を中心に構成
- レジストリの実現には ebXML の Registry 規格を利用（ebXML RIM, RS）
- 適用中の国: イタリー、フランス、カナダ、オーストリア、近いうちに米国?

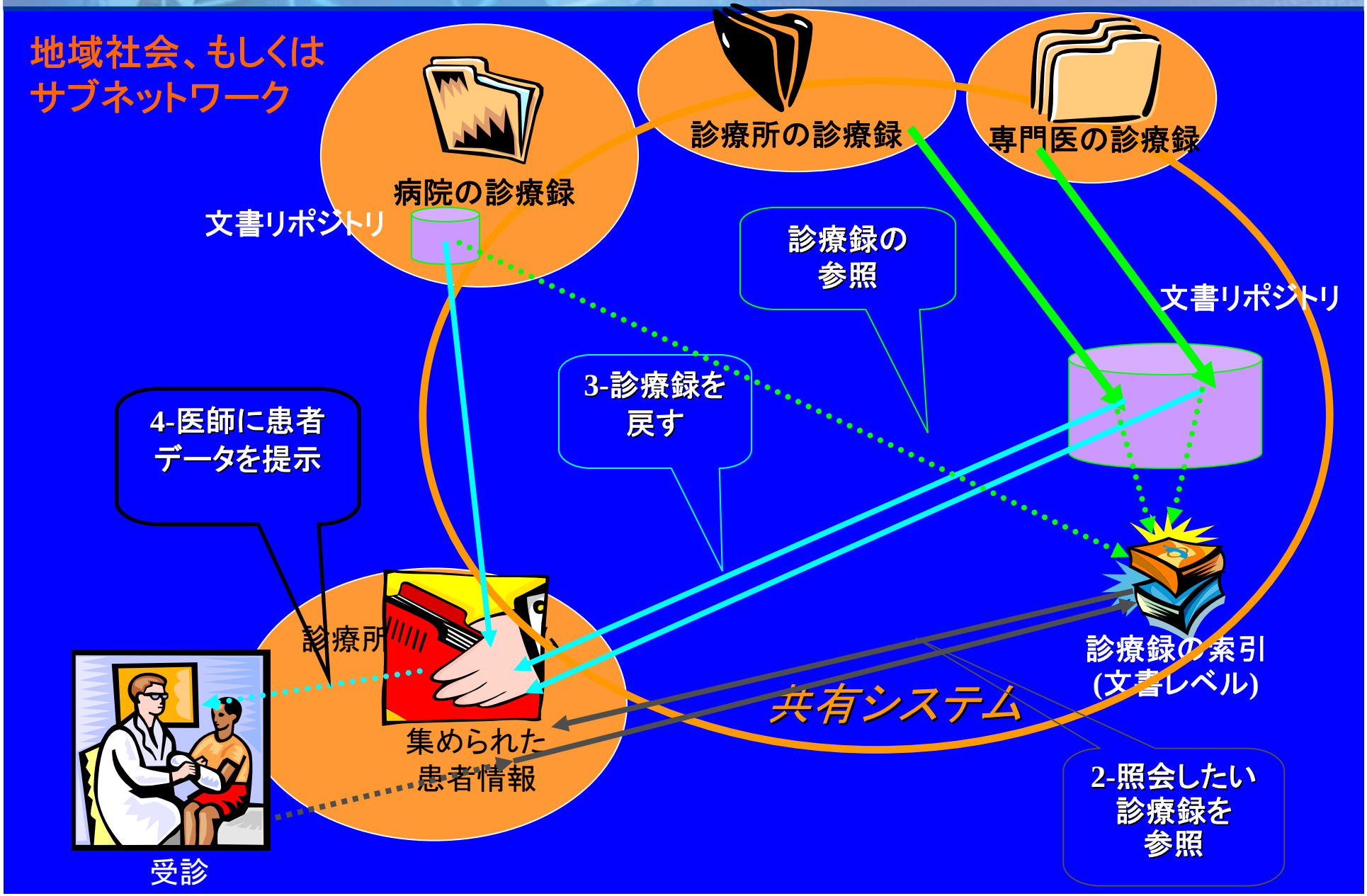
# ebXML

- XMLをベースとした電子商取引の標準仕様を提供することを目的とした団体。また同団体によって規定される技術標準。
- XMLによる取引情報のフォーマットだけでなく、ビジネスプロセスや通信プロトコル、取引先検索のためのレジストリやリポジトリなど幅広い内容を定義している。
- **制定規格：RIM, RS, MSG, CPPA, BPSS, 等**
- http://www.ebxml.org/

# 地域医療情報連携システムのイメージ



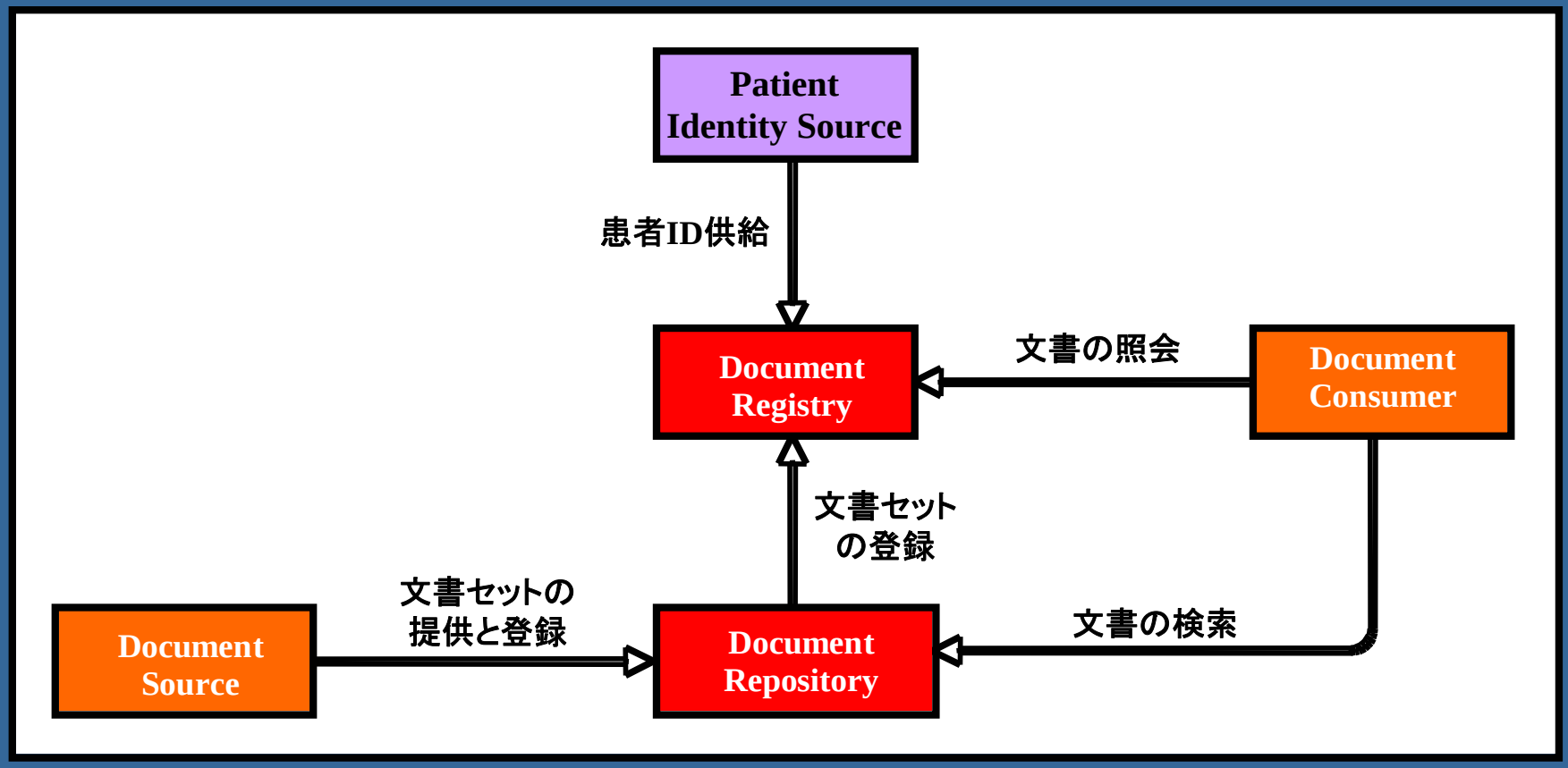
# IHE-XDS：2005年のHIMSSで紹介



# 医療情報交換の相互運用性:
# 施設間文書共有

- 施設間文書共有は、IT基盤による臨床データ管理の負担を減らす。
  *透明性 = 発展の容易性*
- 患者にとってデータの持ち運びが可能となり、医療提供者にとってはデータ収集のエラーを気にせず情報共有が可能となる。
  *電子文書 = 患者と医療提供者 双方の 能力向上*
- 集中、非集中、両方式のリポジトリ・アーキテクチャのサポート。国レベルでのネットワーク連結の容易化。
  **柔軟な個人情報保護、システム構成の柔軟性**
- 次のステップではより簡便な方法でワークフローに取り組んでいる。
  *ワークフロー管理に適した2地点間のメッセージ交換*

# 施設間文書共有 (XDS)
## *トランザクション図*



# 施設間文書共有 (XDS)
## *アクタ*

**Document Source**

文書に関するメタデータと文書のソース

**Document Repository**

文書の格納、Document Registry（診療録登録簿）へ索引付けを要求、検索の支援

**Document Registry**

文書の索引付け、探索の支援

**Patient Identity Source**

既知の患者のIDをDocument Registryに供給する

**Document Consumer**

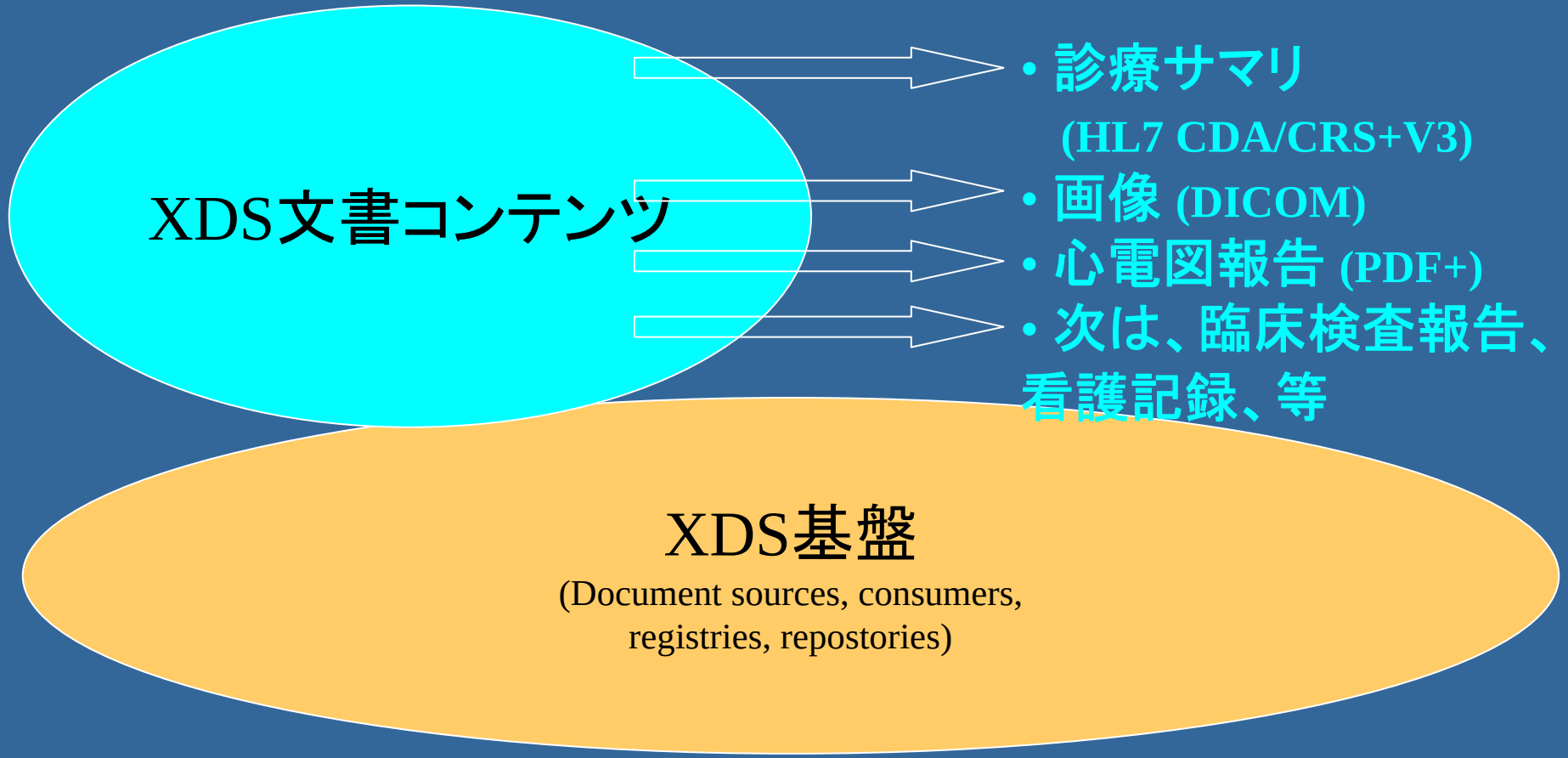
探索の開始と、利用者の文書の検索

# 施設間文書共有 (XDS)
## *使用規格*


- *世界で30以上のベンダーIオープンソースで実装されている。*
  *最新版は2005年8月発行*
- *いくつかの国家プロジェクトないし地域プロジェクトで採用*
  *（イタリア、フランス、カナダ、オーストリア、米国、等）*
  *米国のEHR Vendor Associationの相互運用性ロードマップで利用*
- *IHE XDS: 40,000 “Google” ヒット (2006年6月)*

# 施設間文書共有 (XDS)
## *使用規格*

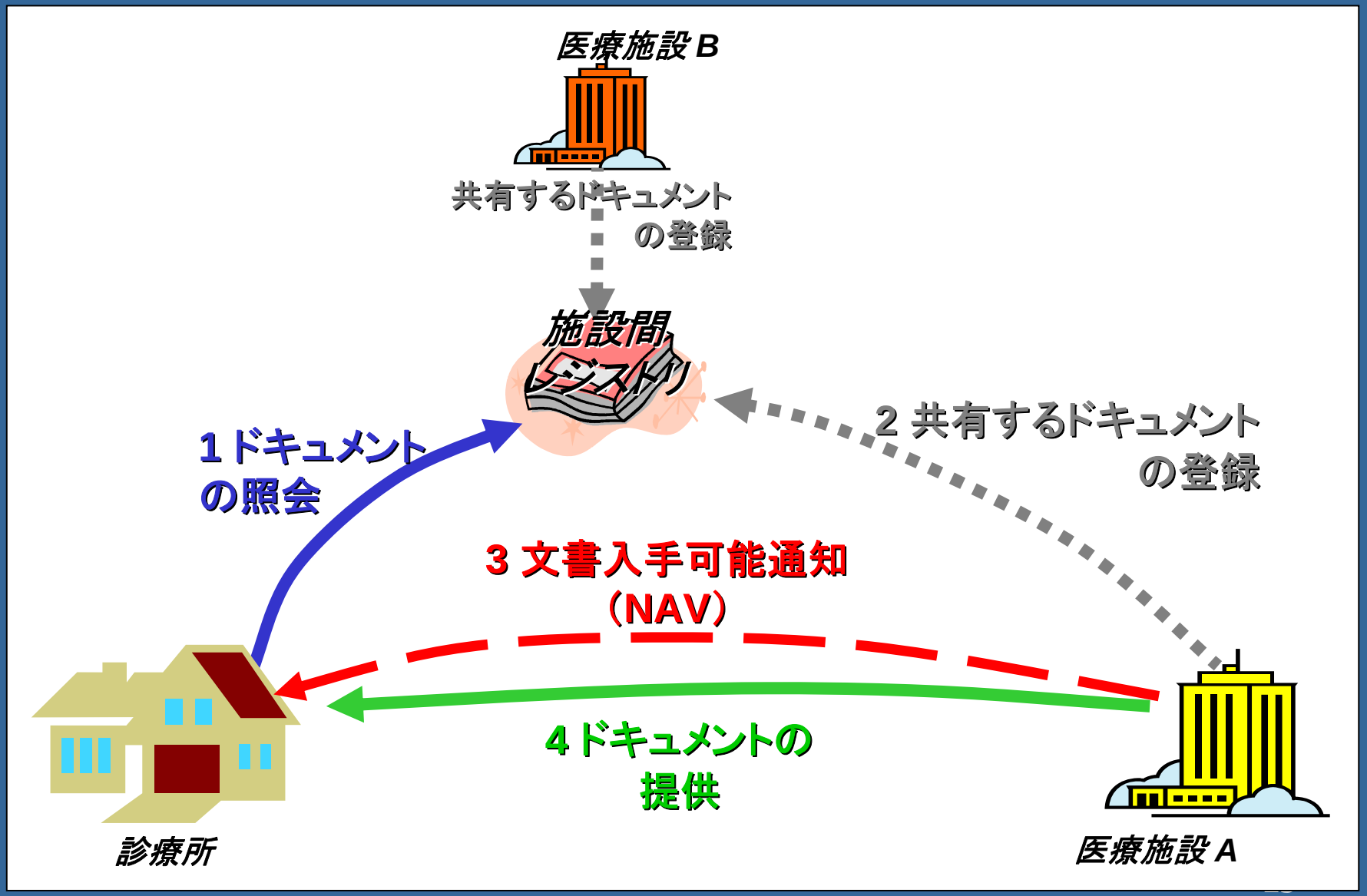
二つの”範疇”の規格が使用されている



# 文書入手可能通知（NAV）

- XDSの利用地域で、所望の文書がリポジトリに登録され、利用可能となったことを自動的に通知する
- 電子メールの仕掛け（SMTP）を利用

# 施設間文書共有（XDS）で機能する文書入手可能通知（NAV）



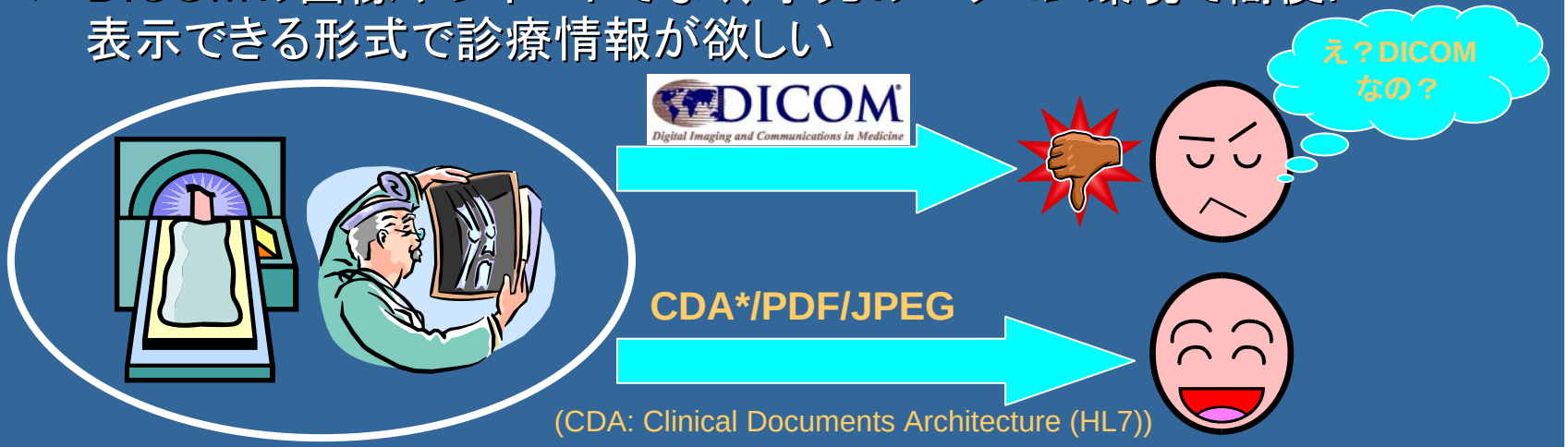
# 表示のための情報検索（RID）

- 簡便かつ迅速な、しかし読み出し専用の患者情報アクセス手段の提供
  - 専用のアプリがない場合の補完
- 現在使用中のアプリ中で、しかしそのアプリの外にある患者情報を見られるようにする。
  - 例：放射線部門から臨床検査結果をアクセス
- 二つのアクセス機能

1. 保存文書の検索と表示
   - CDA、PDF、JPEG等、ポピュラーな形式で表示
     … 概ね任意の端末で表示可能
2. 特定情報の検索と表示
   - アレルギー、処方情報、診療サマリ、など

# RIDの背景は？

- 例えば、
  - 診療科で放射線検査画像や読影レポートを参照したいとしても、DICOM環境を用意するのは負担が大きい
  - DICOMの画像やレポートでなく、手元のパソコン環境で簡便に表示できる形式で診療情報が欲しい

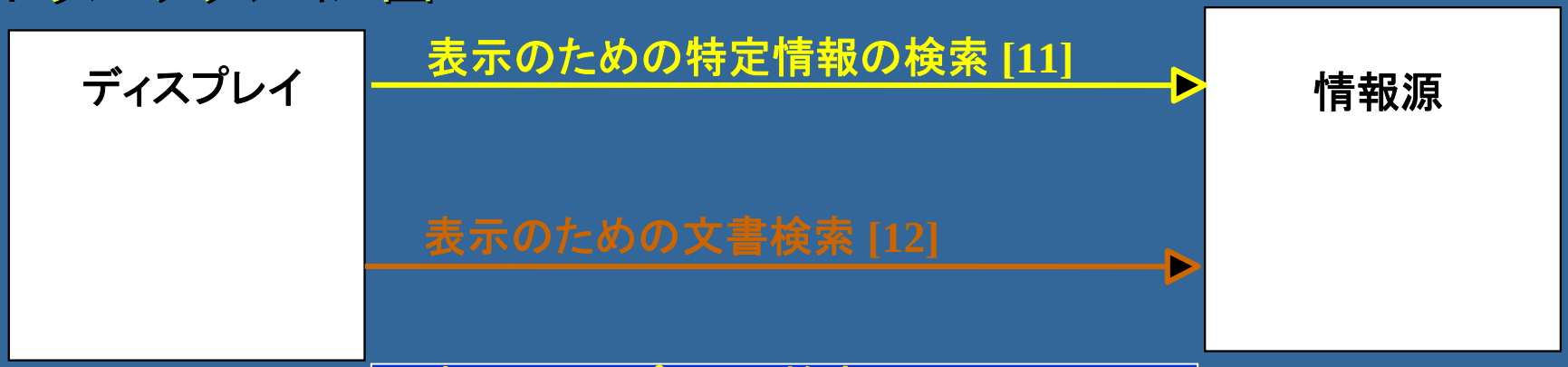



- より簡便な方法で、他部門の情報を「一時的に」参照したいというニーズがある

# 表示のための情報検索（RID）

## トランザクション図




リクエストのタイプ

- すべてのリポートの検索
- 臨床検査リポート・サマリ
- 処方サマリ
- 放射線リポート・サマリ
- 循環器リポート・サマリ
- 手術リポート・サマリ
- 集中治療リポート・サマリ
- 救急リポート・サマリ
- 退院リポート・サマリ
- アレルギー・リスト
- 投薬リスト

保存文書

# 表示のための情報検索（RID）

- **使用規格：**
  - Webサービス(WSDL for HTTP Get).
  - 汎用のIT表現形式：XHTML, PDF, JPEG, CDA L1 (HL7)
  - クライアントソフトは市販のブラウザかディスプレイ・アプリケーション

# 患者情報管理(PAM)

- 全臨床部門での、患者の登録、更新、移動に関する情報交換の調整
- 情報は、各臨床部門の利用アプリケーションで受信ないし処理可能
- 入院と外来の両方の個人情報/受診情報の追跡調査
- 患者の受診状況や居場所も管理
- 患者だけでなく、身元保証人の情報も管理する
- 既存の数種のIHE統合プロファイルの患者管理プロファイルを発展
  - 放射線SWF、カテーテル検査SWF、エコーSWF、臨床検査SWF、PIX

# 患者情報の問合せ（PAM）ユースケース

患者情報Source

ICUの看護師が、現在のベッド番号を検索キーとして患者IDと氏名を問合せ

診察室の医師が、一部の患者情報を検索キーとしてカルテの一覧を問合せ

検査技師が、患者情報を問合せ、および、他ドメインの患者IDを問合せ

ICU ベッドサイドシステム

診察室システム

臨床検査システム

# 患者情報管理(PAM)

## 使用規格

- **HL7 Version 2.5**
  - ADT 登録、更新、患者移動トリガーイベント
    - 入院/登録
    - マージ、更新、関連付け/関連付け解除
    - 移動管理

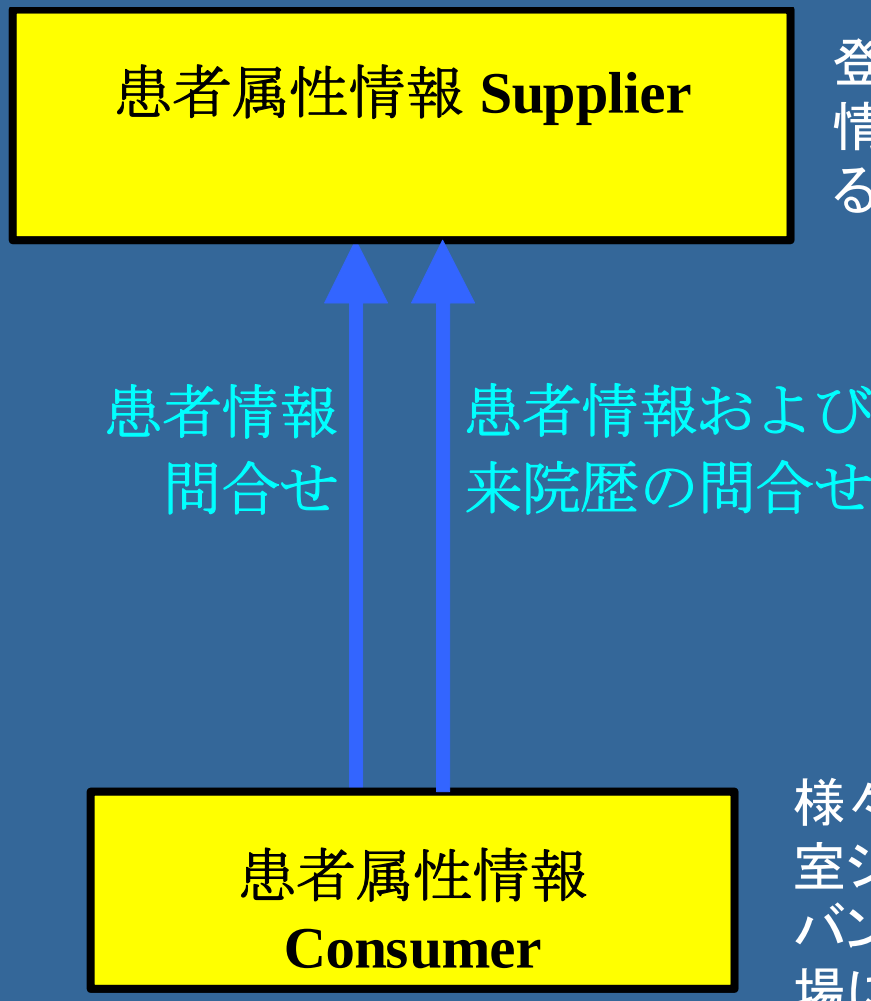
# 患者基本情報の問合せ（PDQ）

- 患者基本情報とは：
  - 患者ID情報
  - 患者氏名、住所、電話番号、生年月日、受診歴(オプション)

# 患者基本情報の問合せ（PDQ）

- 特長
  - 患者氏名、ID、連絡先および受診歴(オプション)を含む患者一覧を素早く検索することが可能
  - 完全なID情報が利用できないときも、正しい患者を選択することが可能
  - 全てあるいは一部のデータの検索可
  - クライアントは検索要求に（対応する患者IDドメインにより）情報ソースを指定可
  - 類似探索に照合アルゴリズム (例：Soundex) を使用可
    - アルゴリズムや操作の詳細はIHEテクニカルフレームワークの範囲外

# 患者基本情報の問合せ（PDQ）
## *トランザクション図*




登録システムで管理されている患者情報レポジトリへのアクセスができるシステム

様々なシステム：ベッドサイドモニタ、診察室システム、検査システム、モバイル血液バンク登録システム等々を含む(診療現場における如何なるシステムでも良い)

# 患者基本情報の問合せ(PDQ)

## 使用規格

- **HL7 Version 2.5**
  - 2章 – コントロール
  - 3章 – 患者管理
  - 5章 – 照会

# 患者IDの相互参照（PIX）

- 部門ごとに異なるIDを持つ同一患者の情報を検索する。
- 同一患者の複数のIDを「Patient Identifier Cross-reference Manager」が対応させる

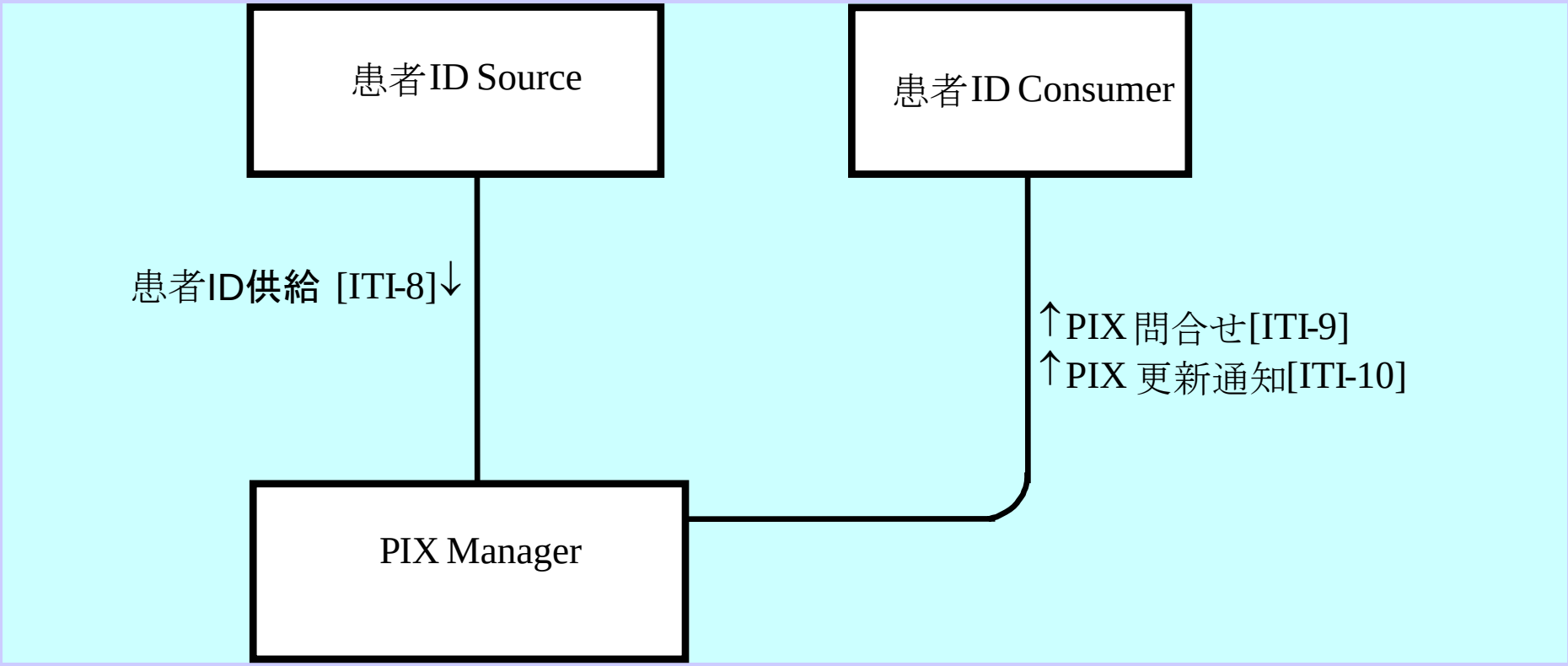
  - 部門毎に患者IDを管理する米国の環境をベースに作られた統合プロファイル
    - 日本では院内の用途はほとんどない
  - IT Infrastructureの守備範囲が地域に広がったので、拡張して利用されている

# 患者IDの相互参照(PIX)

- **特長**
  - 施設の全職員はおのおのの部門内で使用している患者IDで登録可能
  - 各部門で維持している一つ以上の患者インデックスを継続して使用可能
  - 患者の他システムでのIDの問合せを部門システムの問合せとしてサポート
  - オプションとして、他システムで患者のIDが更新されたとき、部門システムに通知する機能を持つ
  - 1患者に対する全システムでの識別子を1ヶ所でメンテする
  - 異なるIDドメイン間での合致する患者の探索に、(カプセル化されている)任意のアルゴリズムを使用可
  - 複数システムにわたるデータ同期のコストを削減
    - 既存システムのIDや書式の変更を強いる必要なし
  - IHEで使用中の標準とトランザクションを活用する

# 患者IDの相互参照（PIX）

## トランザクション図



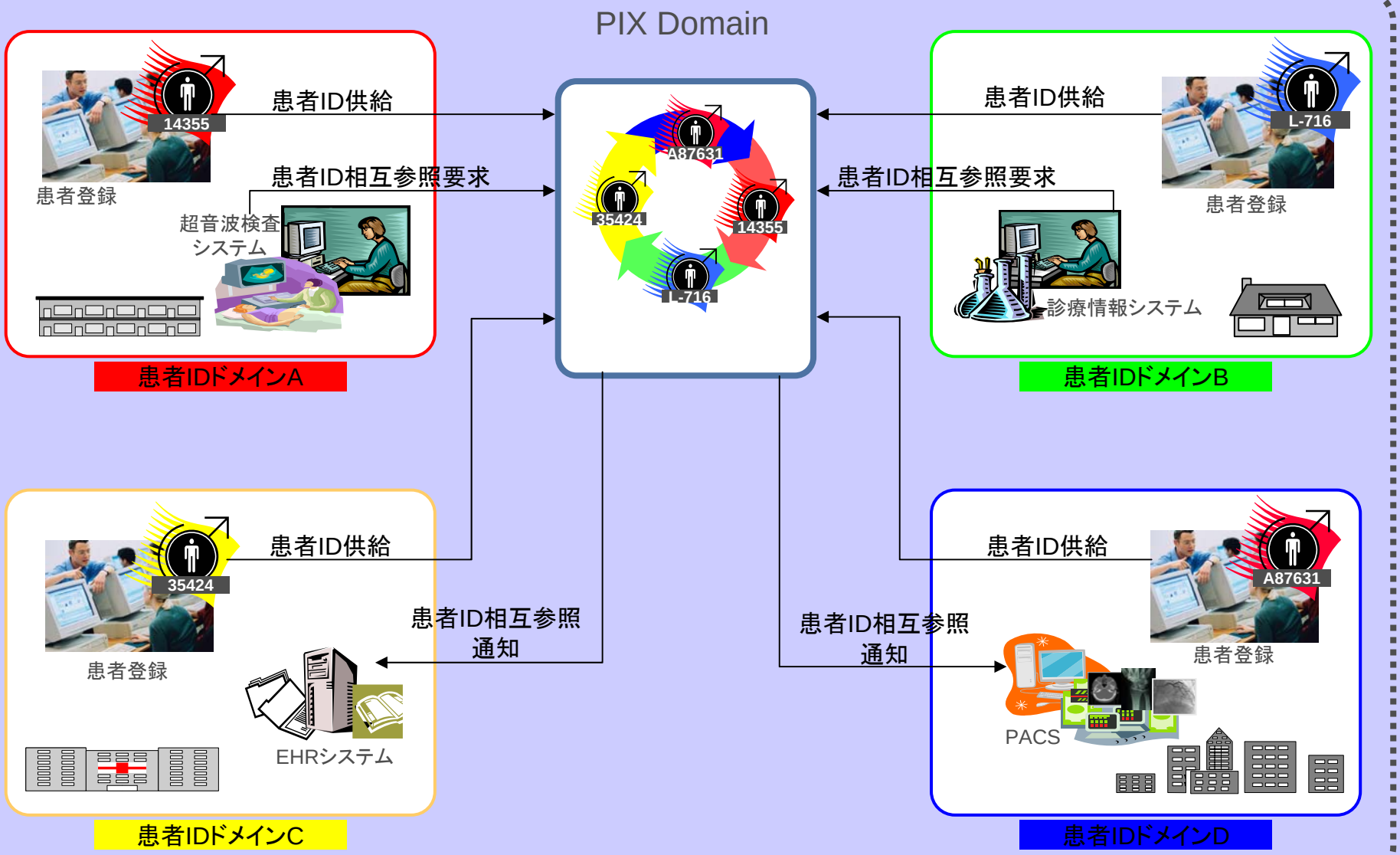
# 患者IDの相互参照(PIX)

**使用規格**

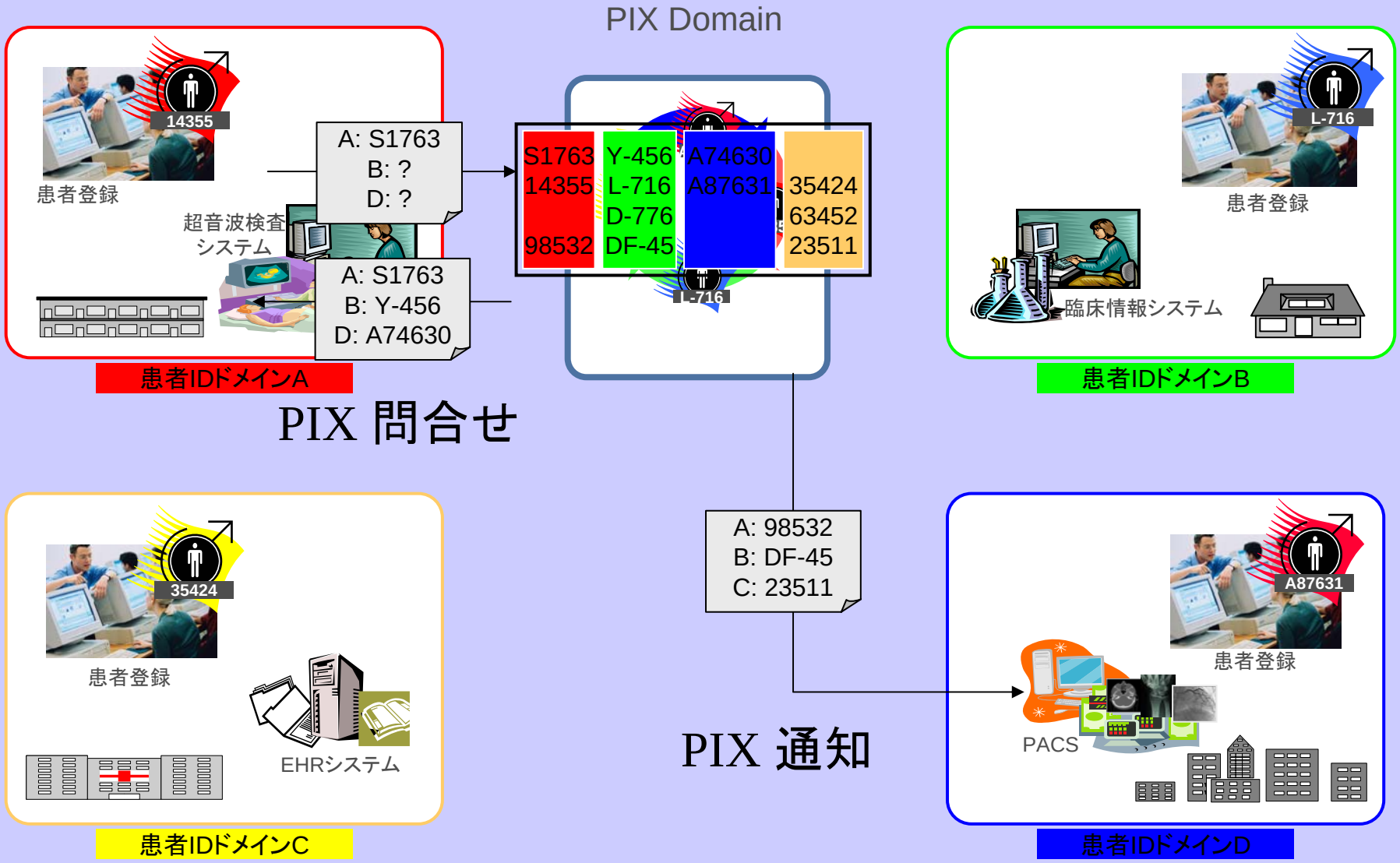
- トランザクション:患者ID供給 [ITI-8]
  HL7 Version 2.3.1
  - 2章 – コントロール
  - 3章 – 患者管理
- トランザクション:PIX問合せ [ITI-9]、
  PIX更新通知 [ITI-10]
  HL7 Version 2.5
  - 2章 – コントロール
  - 3章 – 患者管理
  - 5章 – 照会

# 患者IDの相互参照（PIX）

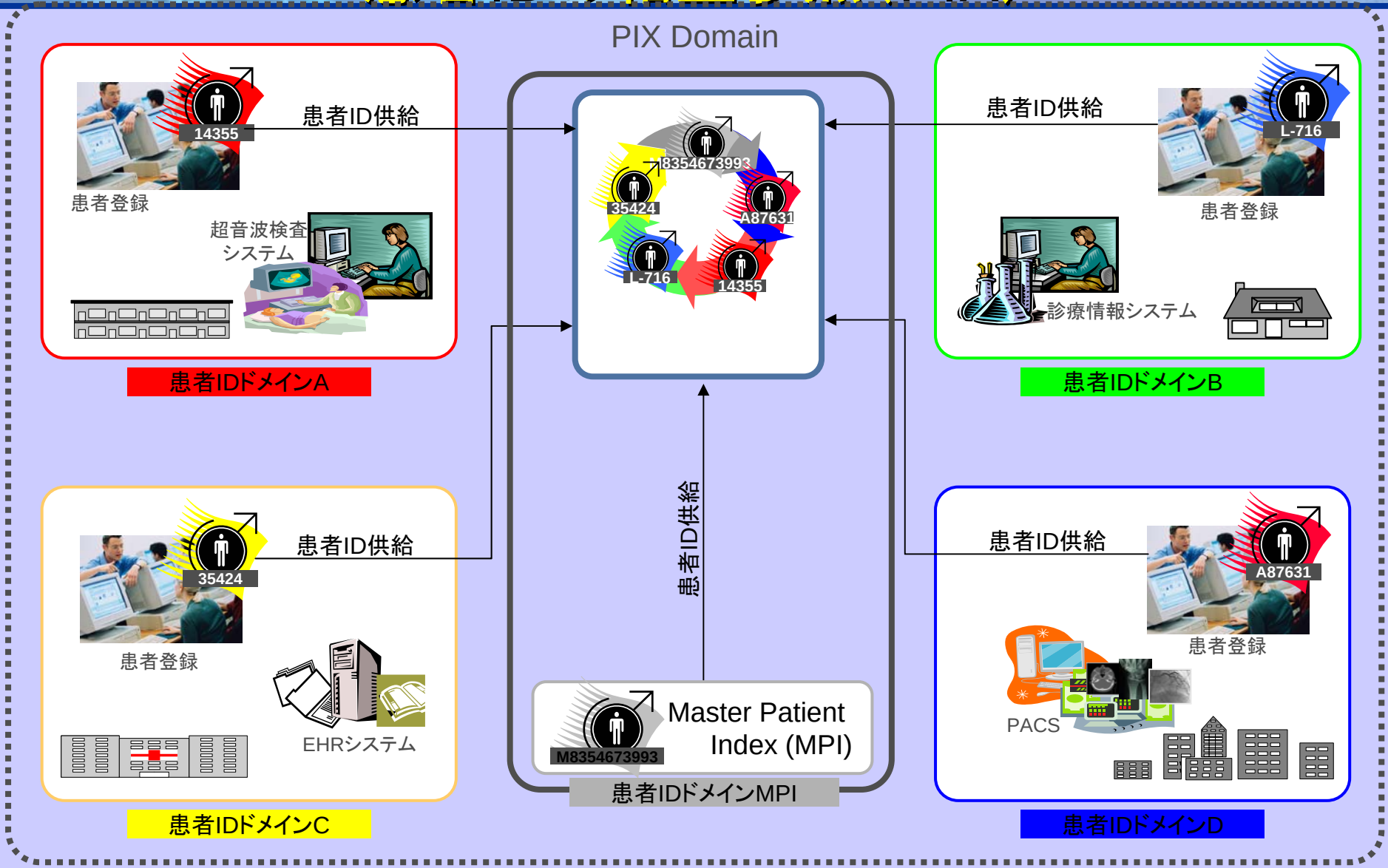
## *IDドメインとトランザクションを示すプロセスフロー図*



# 患者IDの相互参照(PIX)
## サービス: PIX問合せと通知



# MPI(マスター患者索引)を使用した患者IDの相互参照(PIX)

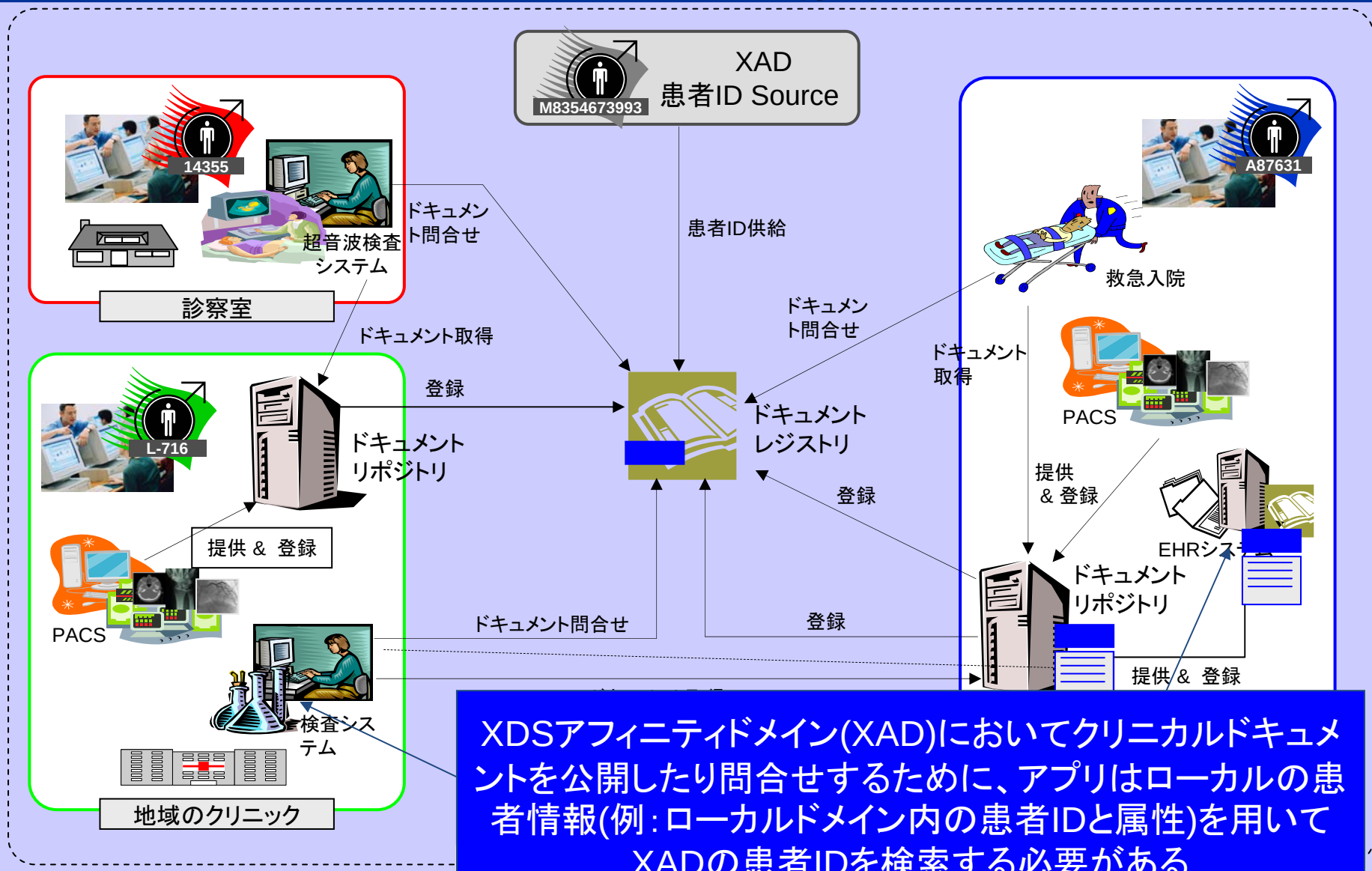


# XDS環境で患者識別サービスを提供する PIX / PDQアプリケーション

## 用語

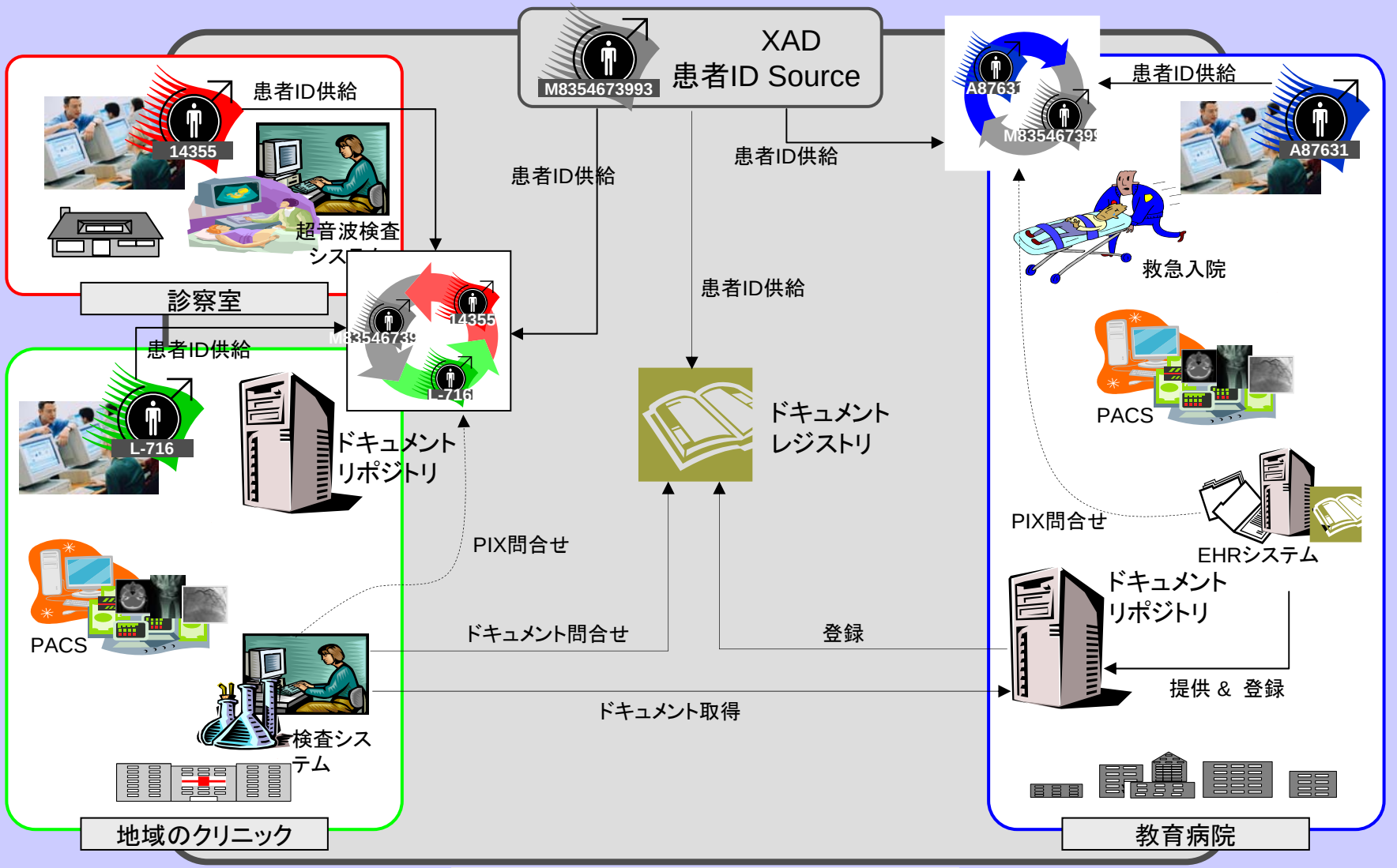
- XDS: 施設間文書共有
- アフィニティドメイン: 共通のポリシーセットで連携したり、リポジトリやレジストリの共通インフラを共有するのを合意した医療機関のグループ

# IHE ITI 統合プロファイル XDS: RHIOにおける臨床情報の共有

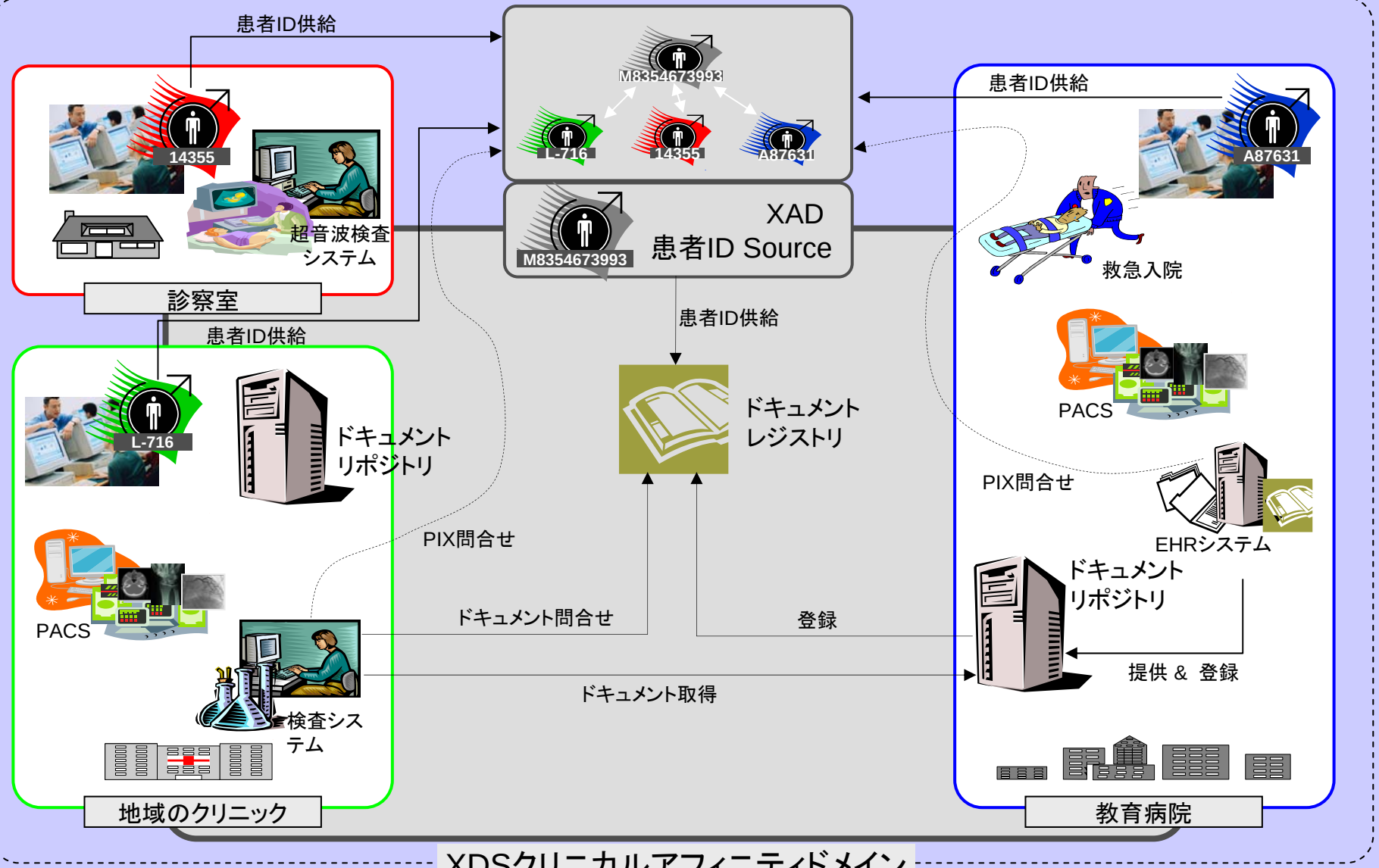



XDSアフィニティドメイン(XAD)においてクリニカルドキュメントを公開したり問合せするために、アプリはローカルの患者情報(例：ローカルドメイン内の患者IDと属性)を用いてXADの患者IDを検索する必要がある

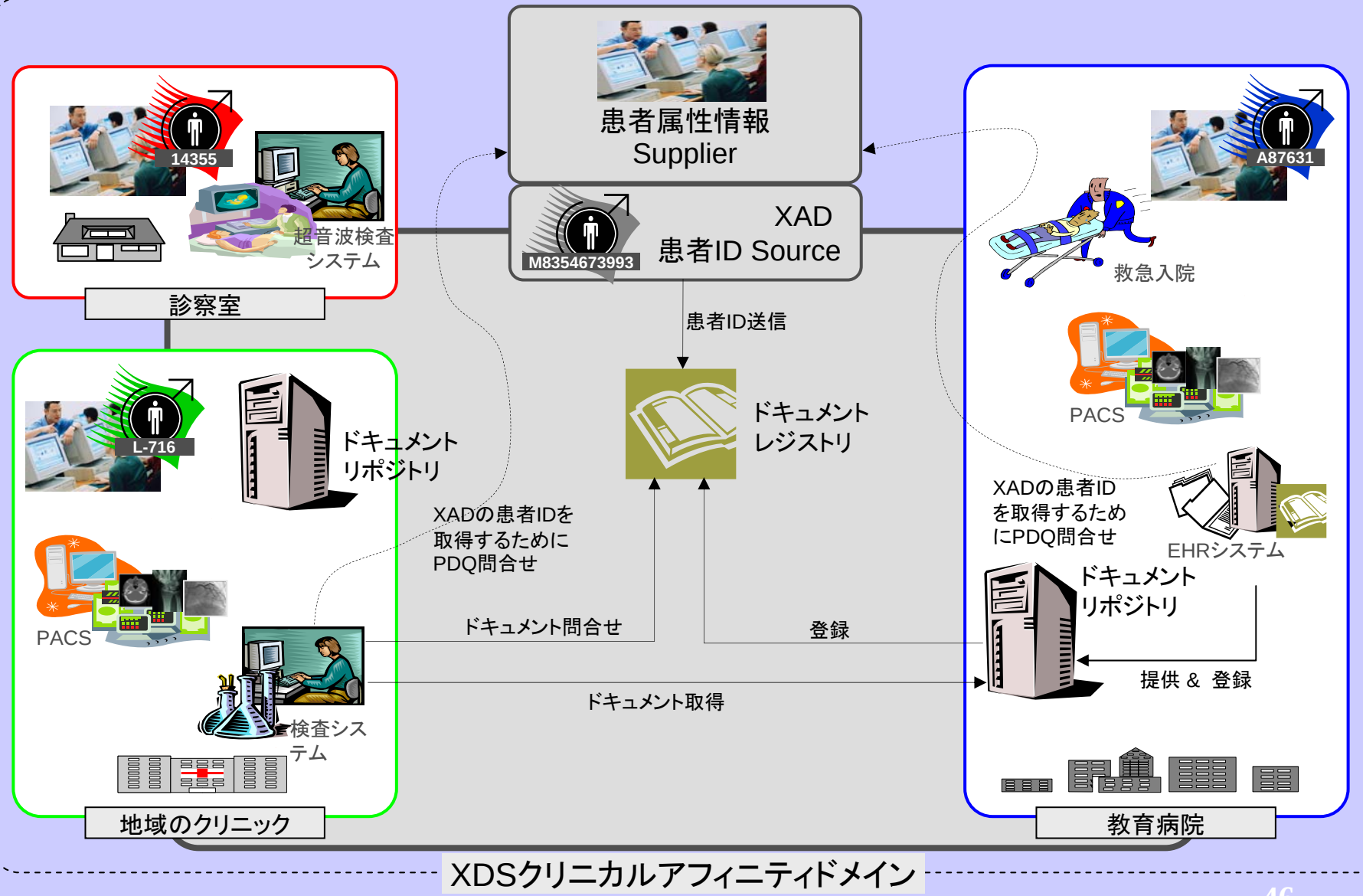
# ローカルPIXサービスによる XDSアフィニティドメインの患者ID検索



# アフィニティドメインPIXサービスによる XDS アフィニティドメインの患者ID検索



# XDSアフィニティドメイン患者ID問合せのための アフィニティドメインPDQサービス



# 患者アプリケーション同期（PSA）

- デスクトップ上の複数の異なるアプリケーションの対象データを同一患者に維持する
- PIXプロファイルとつなぐと、複数患者IDドメインにわたる患者アプリ同期が可能となる
- EUAプロファイルとつなぐと、シングルサインオン（SSO）機能を提供する

# 患者アプリケーション同期（PSA）

**利点**

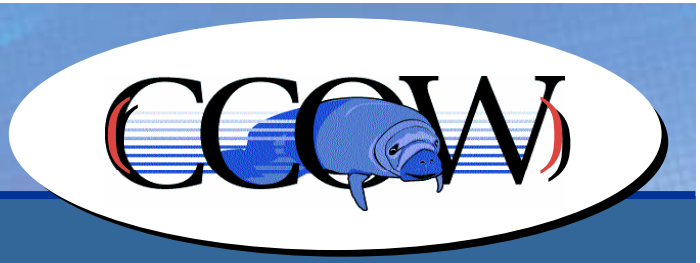
- **利用者の便宜:**
  - アプリケーションごとに繰り返し行う患者選択作業の省略
  - なじみの、また対象の臨床ワークフローに適したアプリケーションで患者を選択することを可能にする
- **患者安全:**
  - 複数アプリケーションにわたって見ているすべてのデータが同一患者のものであることを保証する
- **単一開発環境の利用:**
  - ベンダーに対して、複数アクタをサポートするために単一のCCOW環境を利用可能にする
    - 患者関係のアプリ (PSA)
    - 利用者関係のアプリ (EUA)

# 患者アプリケーション同期（PSA）

## 使用規格

- **HL7 Context Management “CCOW” Standard, Version 1.4:**
  - CCOW : もともとは “Clinical Context Object Workgroup” の略だが、今は単にCCOWと言う
- **Support for both Windows and Web Technology**
- **Support of “Patient Subject”**

# CCOW（シーカウ）とは




※Sea cow : ジュゴン

- The Clinical Context Object Workgroup
- Visual Integration の規格としてHL7で検討され、ANSI標準としても承認されている
- Visual Integration とは
  - サーバ間で情報のやり取りをするのではなく、操作端末のデスクトップ上で見掛けの情報の統合・連携を行う
  - 画面上の独立したアプリケーションウィンドウの中に表示あるいは入力される情報を連携させる
  - 解決すべき問題点は、情報の連携を管理する仕組みと、ユーザ操作の通知とそれに伴う同期の管理である
  - CCOWではその仕組みを標準規格化している

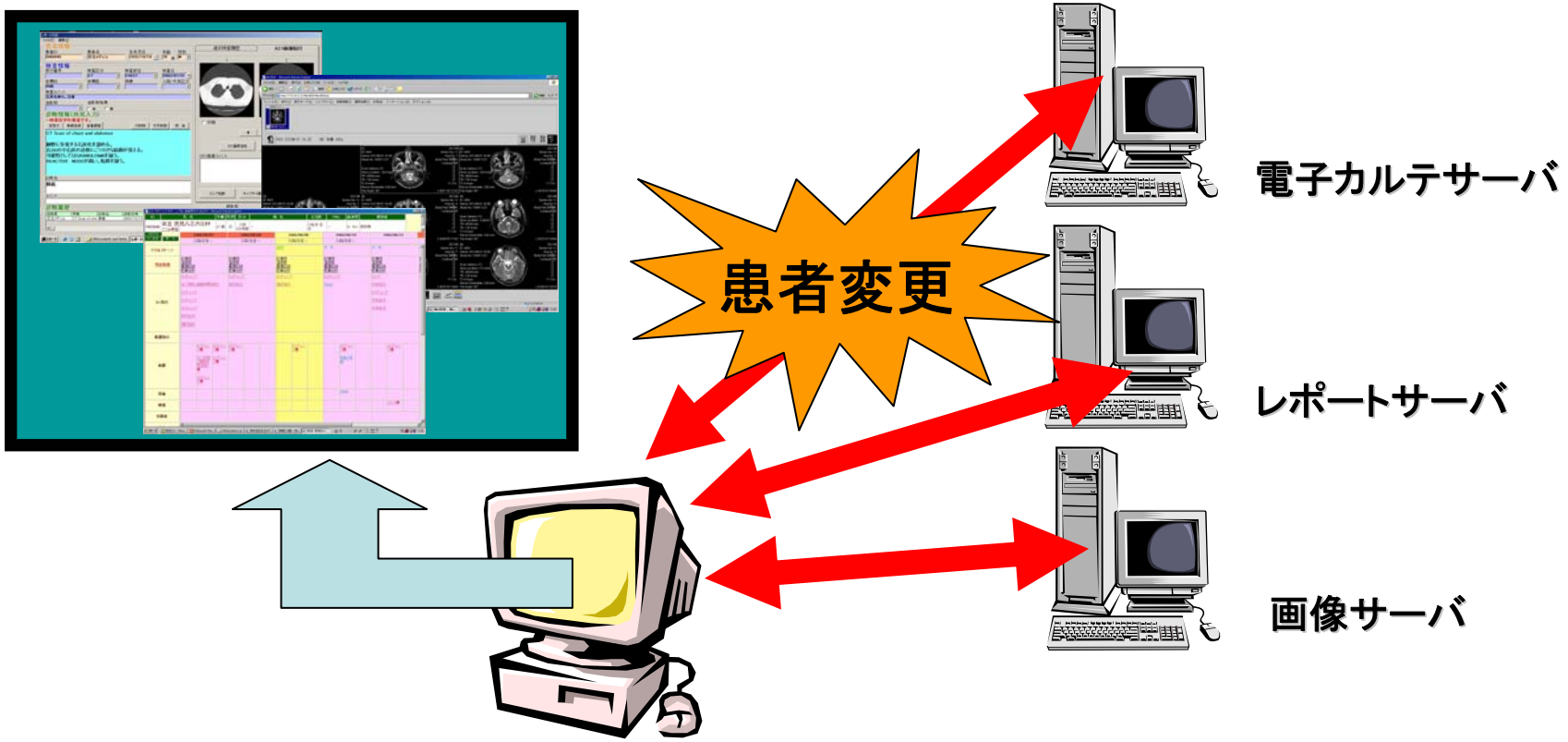
☆ IHE－Jベンダーワークショップ 2005/9/8 

# PSAでのCCOWとは...

- 同一デスクトップ画面上で、独立したアプリケーションに対して、同一患者に同期させる

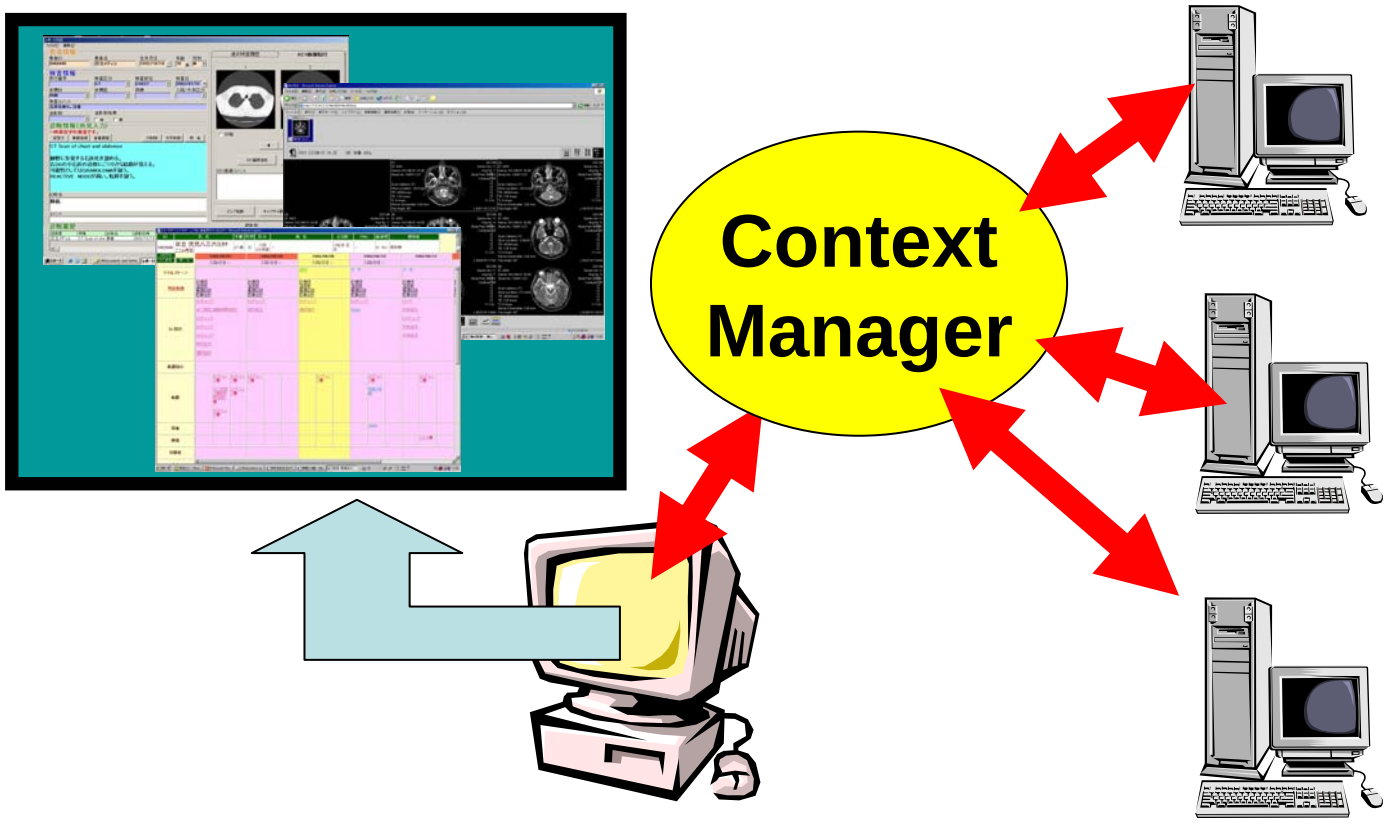
# 解決しようとする問題

従来の方法では、あるアプリケーションが表示するウィンドウの
患者を変更しても、他のウィンドウが表示する情報は以前のまま



# 患者アプリケーション同期

ひとつのウィンドウで患者を変更したら、他のウィンドウでもその患者の情報を表示する



# IHE IT Infrastructureの
# セキュリティ関係統合プロファイル

- ユーザー識別 → PWP、EUA
- ユーザー認証 → EUA
- ノード認証 → ATNA
- セキュリティ監査証跡 → ATNA
- データ完全性管理 → CT、ATNA TLSオプション
- データ機密性 → ATNA TLSオプション
- アクセス制御 →（RBAC）

# セキュリティ要件

- 理由：臨床での使用と個人情報保護
  - 医療従事者は患者の診療情報にアクセスしなくてはならないが、その情報を他に開示してはならない
  - 許可されていない人が業務の邪魔をしたり、データを変更したりすることができないようにすべきである
- 運用とセキュリティ機構により、以下を保証する
  - 機密性（Confidentiality）
  - 完全性（Integrity）
  - 可用性（Availability）
  - 信頼性（Authenticity）

# セキュリティ施策

- 認証：*ユーザとシステムのアイデンティティを確立する。「あなたは誰？」という質問に答える*
  - ATNAの規定：ネットワーク接続をどのように認証するか
  - ATNAのサポート：認証メカニズム　例：施設内利用者認証（EUA）または施設間両者認証（XUA）. .
- 権限付与とアクセス制御：
  *ユーザのできることを明確にする。たとえばデータへのアクセスで、「あなたが誰かは知っているけど、何をしていいの？」という質問に答える*
  - ATNAの規定：どのようにネットワーク接続を許可するか
  - ATNAの要求：ローカルとネットワーク双方からのアクセスに対応するシステム内部メカニズム

# セキュリティ施策

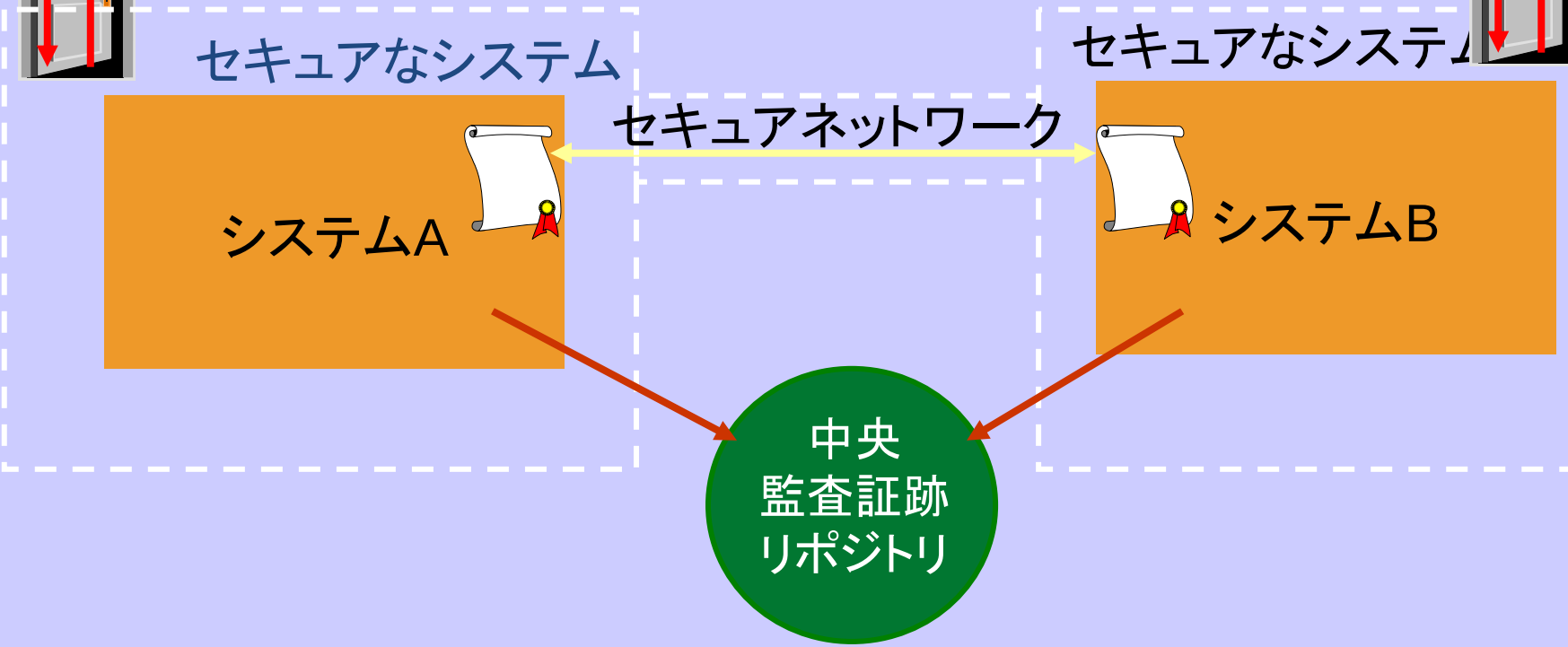
- 説明責任と監査証跡：
  *ユーザまたはシステムの一定期間の動作履歴を確定させる。「あんた、何をしたの？」という質問に答える*
  - ATNAの規定：監査メッセージ形式とト通信のプロトコル

# 監査証跡とノード認証（ATNA）

- 集中監査証跡とノード間認証によりセキュアなドメインを形成する
- 医療機関のセキュリティ環境と個人情報保護環境の一部として使用する個々のシステムについて、基本的なセキュリティ機能を定義する
- IHE放射線部門用の基本セキュリティプロファイル（2002年に定義）を他の医療部門に適用できるように拡張した
- ホストレベルの認証を実施する。この認証は、EUAとXUAによるユーザー認証と連携して使用する

# 監査証跡とノード認証（ATNA）
## 信頼できるノードの構築

- ローカルアクセス制御（利用者認証）
- リモートノードの強力な認証（デジタル証明書）
  - ネットワーク通信時の暗号化はオプション、必須ではない
- 監査証跡：
  - リアルタイムアクセス
  - 時間的同期



# ATNA
## ノード認証

- X.509証明書をノードの識別と鍵として使用する
- TCP/IPトランスポート層セキュリティプロトコル（TLS）をノード認証と、オプションとして暗号化に使用する
- アソシエーションの確立時に双方のセキュア・ハンドシェイク・プロトコルを使用する
  - 暗号化プロトコルの識別
  - セッション鍵の交換
- アクタは許可されたノードの証明書リストを作れなければならない
- ATNAは現時点では、HTTP、DICOM、HL7に対するメカニズムを指定する

# なぜ、ノード認証なのか？

- CTシステムなど、多くのシステムはアクセスを共用しており、セキュリティ目的としてはオペレータの識別よりマシンの識別の方が重要である
  - CTの操作者に許されているのは、CTシステムからCT記録を更新することだけである
- PACSアーカイブなど、自律的に動作するシステムもある
  - PACSの動作内容をモニターするとき、勤務中のPACS管理者を知っても意味はない。たいてい誰もログインしていない。
- 機器のアクセスは通常、施設全体管理者によって管理されている
  - 許可されたユーザーであっても、個人のマシンを使用してアクセスすることは許されない

# ATNA
## *監査システム*

- 法的な利用よりも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放射線部門用暫定形式。放射線部門用と下位互換
  - IETF/DICOM/HL7/ASTM形式。将来拡張可能
    - DICOM Supplement 95
    - IETF Draft for Common Audit Message
    - ASTM E.214
    - HL7 Audit Informative documents
- 両形式ともXMLメッセージであり、XML規格の拡張メカニズムを使用して拡張可能である

# 監査証跡

- 関連する国内･海外状況
  - 相互運用性実証事業
    - 監査証跡のフレームワークについて検討
  - JAHIS/JIRA合同 監査証跡WG
    - 監査証跡メッセージ標準規約を策定中
  - ISO TC215
    - 韓国済州島会議（2006.4）で新しいタスクグループを立上げ “Audit trails for electronic health records”

# 時刻の整合性(CT)

- ネットワークタイムプロトコル(NTP)バージョン3(RFC 1305)を時刻の同期に使用する
- アクタは手動での調整をサポートすること
- 要求精度:1秒
- オプションとしてセキュアNTPを使用できる
- ATNA、EUA、XUAを使用する場合はCTが必須である

# 文書電子署名（DSG）

- 電子署名の目的
  - 説明責任（Accountability）
  - 文書の完全性（Document Integrity）
  - 否認防止（non-repudiation）
  - 著作者、承認、レビュー、認証に対する十分なエビデンスの提供

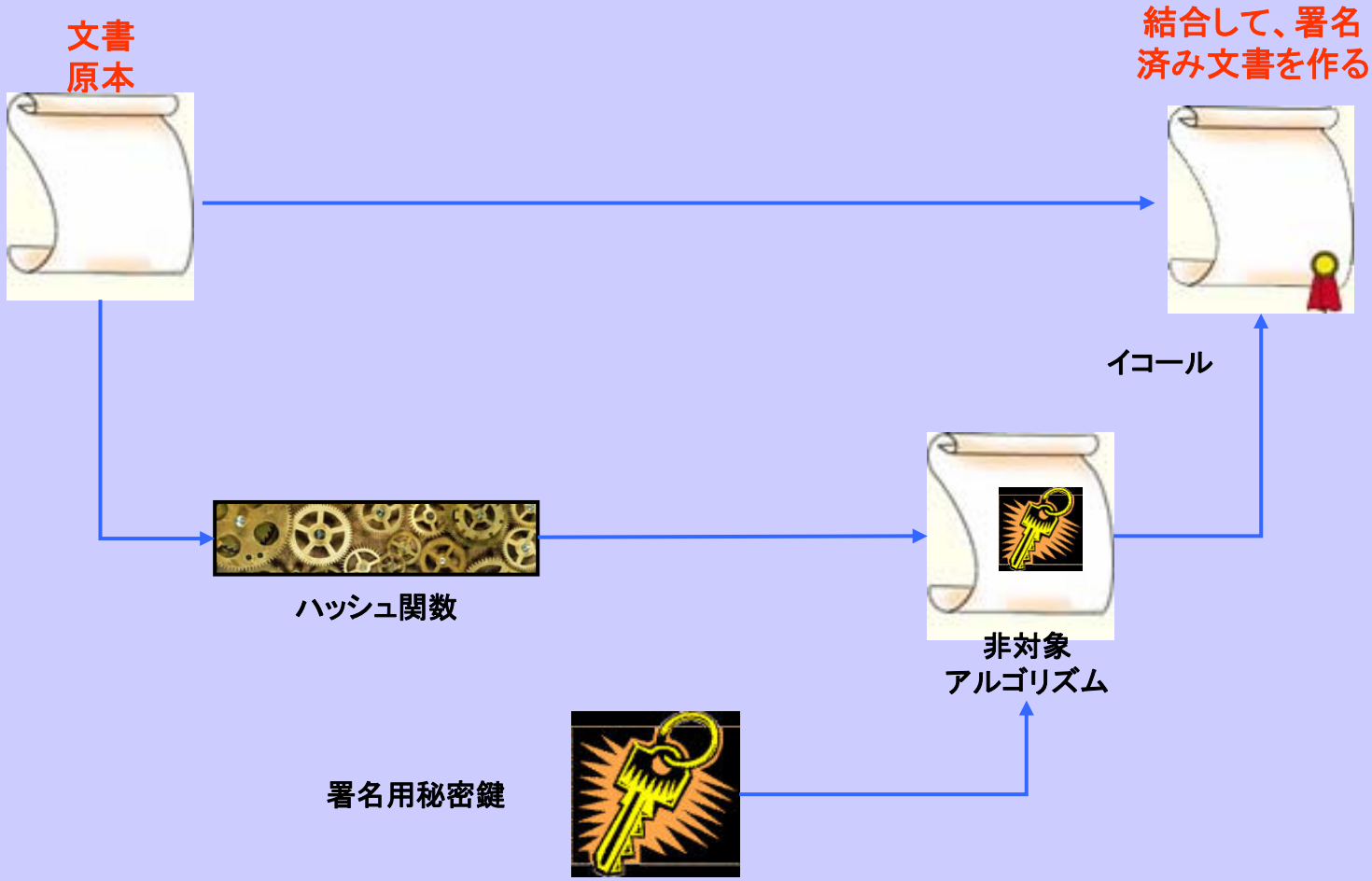
# 文書電子署名(DSG)

- **IHE DSGの特長**
  - XDS文書基盤の利用
  - XDSレジストリを使用しない他の分野での活用
    - 電子処方箋、電子紹介状

# 文書電子署名（DSG）

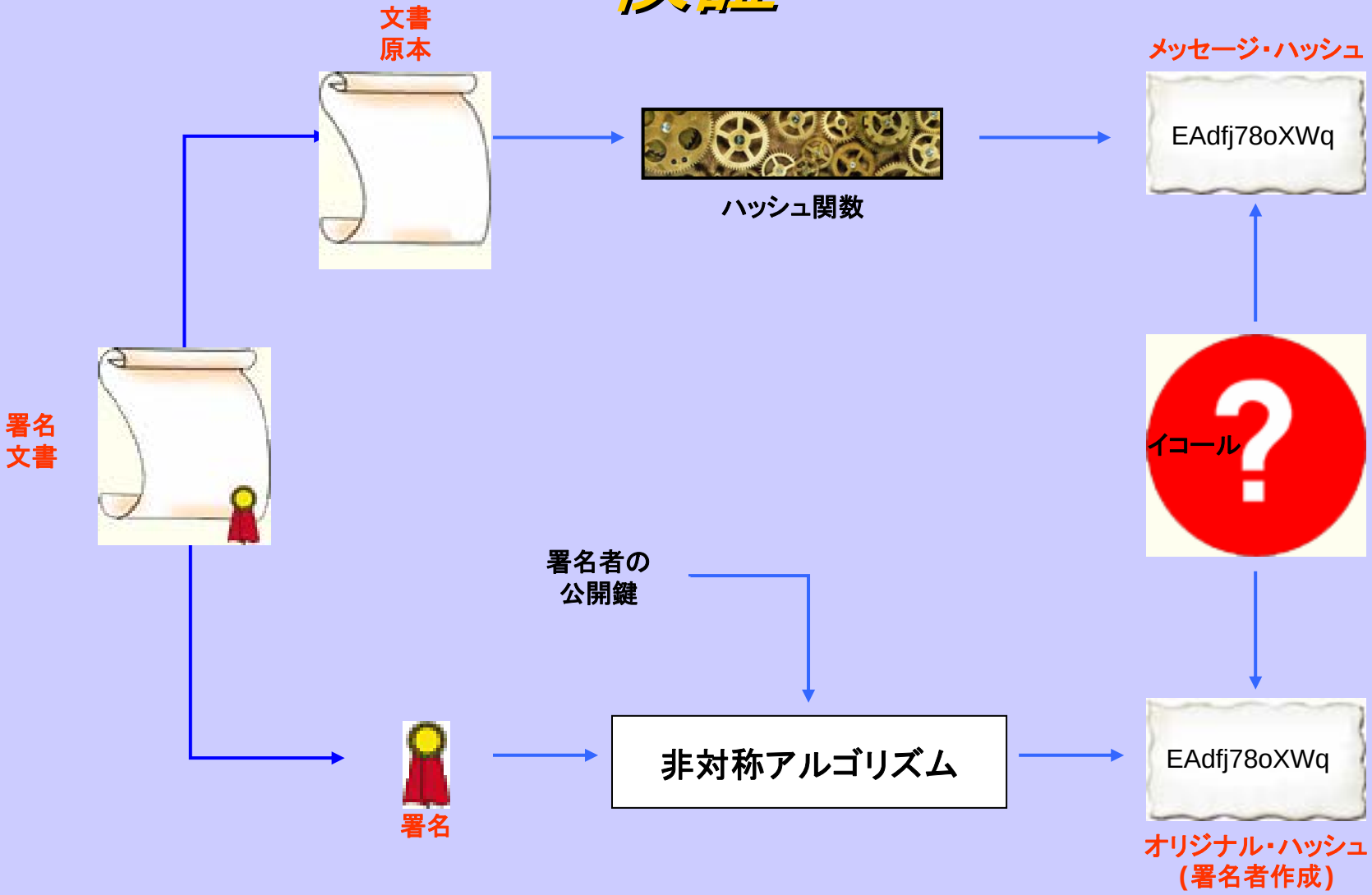
- 電子署名の原理
  - PKI（Public Key Infrastructure：公開鍵基盤）の利用
    - 非対称アルゴリズムによる暗号化技術の利用
      - 暗号化は簡単だが、鍵がないと復号は困難（実用的時間内に解けない）。
      - 素数を利用した方式、楕円関数を利用した方式、など
    - 公開鍵方式
      - 公開鍵と秘密鍵
      - 公開鍵を相手に渡し、秘密鍵は自分で保持する
      - 秘密鍵で暗号化、公開鍵で復号
    - PKIは、VPN（Virtual Private Network）やSSL（Secure Socket Layer）など、通常のインターネット通信でも広く使われている。

# 文書電子署名(DSG)
## *署名の実施*



# 文書電子署名（DSG）

## *検証*



# 文書電子署名（DSG）

- 一般用電子署名
  - ITUの勧告X.509V3による公開証明書、それに基づくIETFのRFC3280基本プロファイルにより規定
  - 認証局（CA）が発行する公開鍵証明書により署名の真正性を保証する
- **ISO TS17090 (Health Informatics - Public key infrastructure)**
  - 一般用電子署名を拡張。医療分野における役割を規定するエクステンション（hcrole）を定義している
  - IS（国際標準）化見込み
- **IHE DSG（Digital Signature）**
  - ISO TS17090準拠
  - W3C XML署名
  - XML長期署名規格（XaDES）に対応

# 文書電子署名(DSG)
## *主要技術*

- W3C XML 証明の構成
  - 証明書、タイムスタンプ、その他の署名属性(署名の目的など)
- XDSに格納された文書の参照
- ISO TS17090 準拠デジタル証明書
- メッセージの完全性を保証
- 署名済み文書の有効性の検証
- 多重署名機能の提供

# 文書電子署名（DSG）

- 日本における医療用電子署名の状況
  - H13.4 電子署名法施行
  - H15年度、MEDIS-DCでTS17090に基づくHPKIの実証実験を実施
  - 厚労省医療情報ネットワーク基盤検討会で「HPKI認証局 証明書ポリシ」を作成（H17.4）
  - その後「HPKI認証局の整備と運営に関する専門家会議」を開催（H18.3までに2回）
  - H18年度、厚労省ルートCA局及び日医CA局、MEDIS CA局を構築、認証業務のフィージビリティ検証を行う

# タイムスタンプ

- **タイムスタンプ**
  - あるアクションが正しい時間に実施されたことを証明するために必要。特に電子署名文書では必須
  - 正しい時間を保証するためには、ネットワークに散在するマシンの時間の同期をとる必要がある
- **国際規格**
  - IETF RFC3161（PKI Time-Stamp Protocol）
  - IETF RFC1305（Network Time Protocol）、等
- **IHE**
  - CT（Consistent Time）： RFC1305によるネットワーク上の時刻一貫性維持
- **日本における状況**
  - H16.11 総務省「タイムビジネスに係る指針（ネットワークの安心な利用と電子データの 安全な長期保存のために）」
  - H17.2 (財)日本データ通信協会が「タイムビジネス信頼・安心認定制度」創設
  - 現在、アマノ、セイコーインスツルメンツ、PFUなど数社がサービス提供中

# 利用者認証

- 現状は個別の医療情報システムベンダーが、ID＋パスワードやカード等のデバイス、生体認証などによる独自の認証手段を提供している
- 一つの施設内でもマルチベンダーシステムを導入している施設は、ログインの手間を省くため（SSO：シングルサインオン）共通の認証手段が必要となる
- 地域連携では当然共通の認証手段が必要
- IHE IT Infrastructureテクニカルフレームワークでは、以下の二つの統合プロファイルを提供している
  - EUA（Enterprise User Authentication）：施設内利用者認証
  - XUA（Cross-Enterprise User Authentication）：施設間利用者認証

# 施設内利用者認証（EUA）

- 施設内の一元的利用者認証
  - 単一のセキュリティポリシィ、共通のネットワークドメインが前提
- シングルサインオンをサポート
- 認証Kerberos＋利用者アプリ同期CCOWを利用
  - Kerberos：MITで開発された分散環境向け利用者認証方式。利用者はKerberosサーバに問い合わせることにより認証を得る。このときチケットと呼ばれる信用証明書が与えられる。以後この証明書を使用してネットワーク上のリソースを利用する。
    DCE及びWindows 2000 Server標準装備
  - CCOW：HL7 コンテキスト管理規格

# Kerberos（ケルベロス）とは

- **Athenaプロジェクトで、MIT、IBM、DECが研究開発したネットワーク認証システムである (1983)**
- **「信頼された第3者機関による認証方式」**

  (Trusted Third Party Authentication)
- **IETF（Internet Engineering Task Force）認定のオープン標準**
- **設計方針**
  - 双方向認証

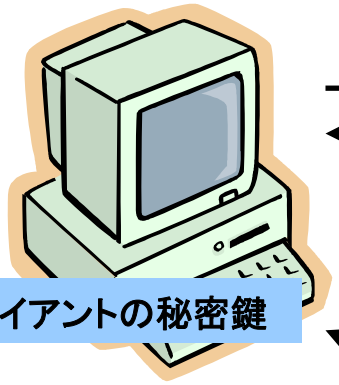
    サーバによるクライアント認証、または、その逆
  - パスワードは認証後消失
  - 暗号の鍵は寿命あり

# Kerberosの基本概念･用語

- 発行局 KDC　　Key Distribution Center
- 王国（領域）Realm（レルム）
  - KDC が支配する複数のクライアントとサーバを含む領域
- 秘密鍵　　共有鍵という表現が適切か？
- チケット　　サービス供給元へのアクセス許可証
- セッション鍵　一時的な通信暗号鍵
- 証明書　　チケットとセッション鍵がセットになったもの

# 基本的な認証の手順

Client

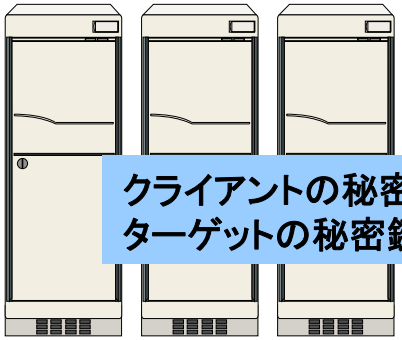


クライアントの秘密鍵

1）ターゲットに対する
チケットを要求する

2）チケットを含んだ
証明書を返す

KDC
(Key Distribution Server)



クライアントの秘密鍵
ターゲットの秘密鍵

3）チケットを送信する

4）認証完了

Application Server
(Target)

ターゲットの秘密鍵

証明書

クライアントの秘密鍵で暗号化

セッション鍵（一時的な暗号鍵）

チケット

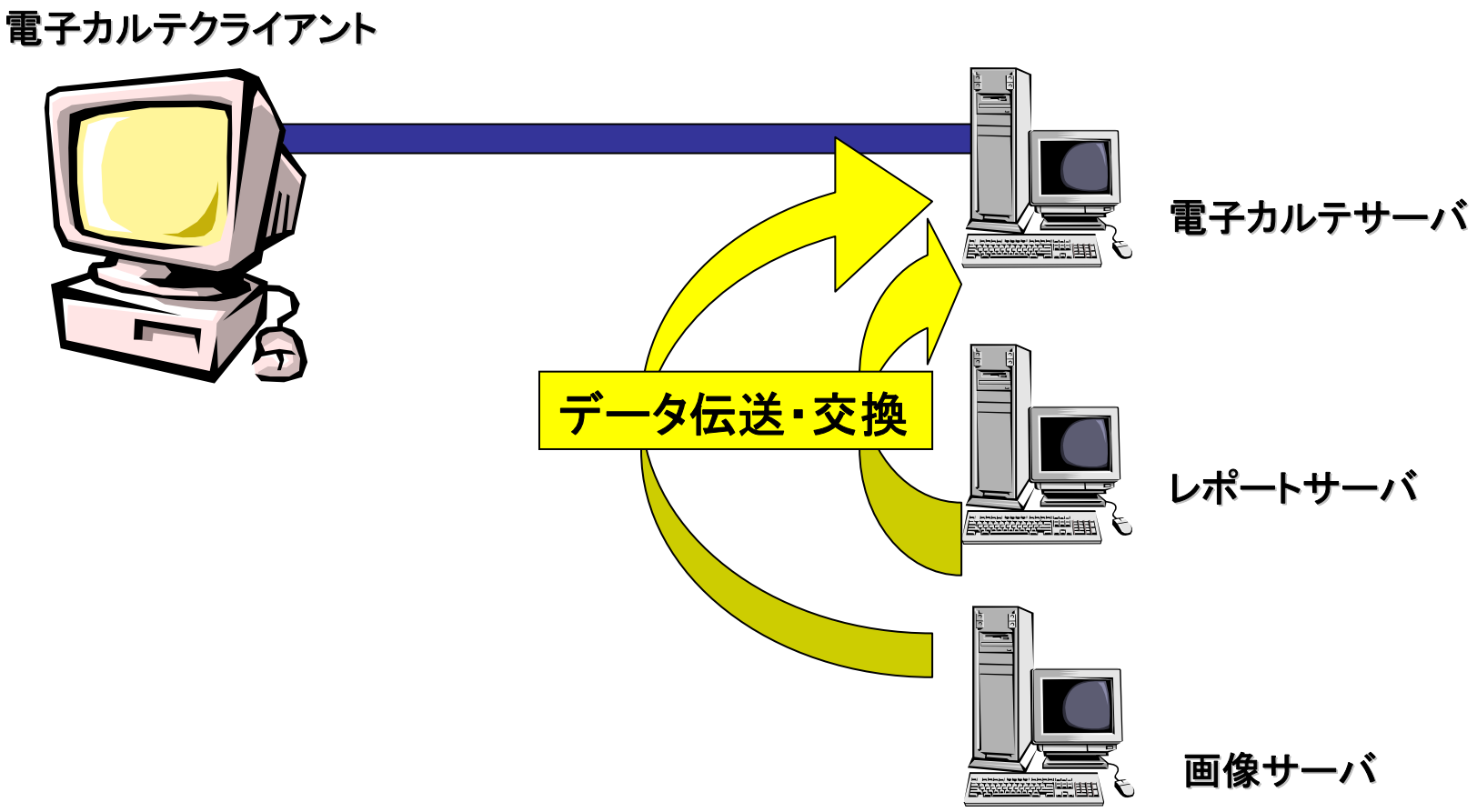
ターゲットの秘密鍵で暗号化

サーバー名、クライアント名、クライアントのIPアドレス、タイムスタンプ、
有効期限、ランダムなセッション鍵（一時的な暗号鍵）

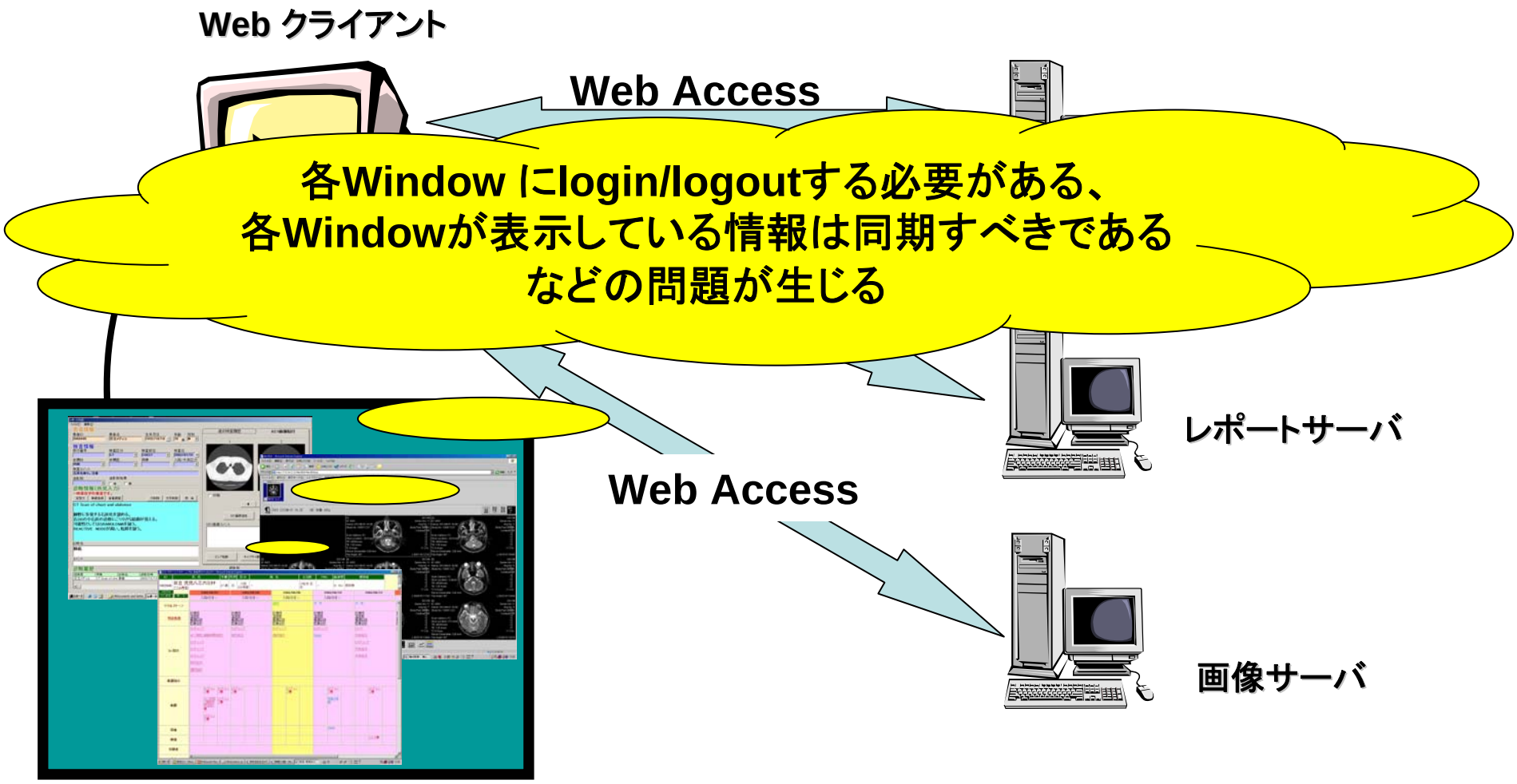


☆ IHE－Jベンダーワークショップ 2005/9/8 

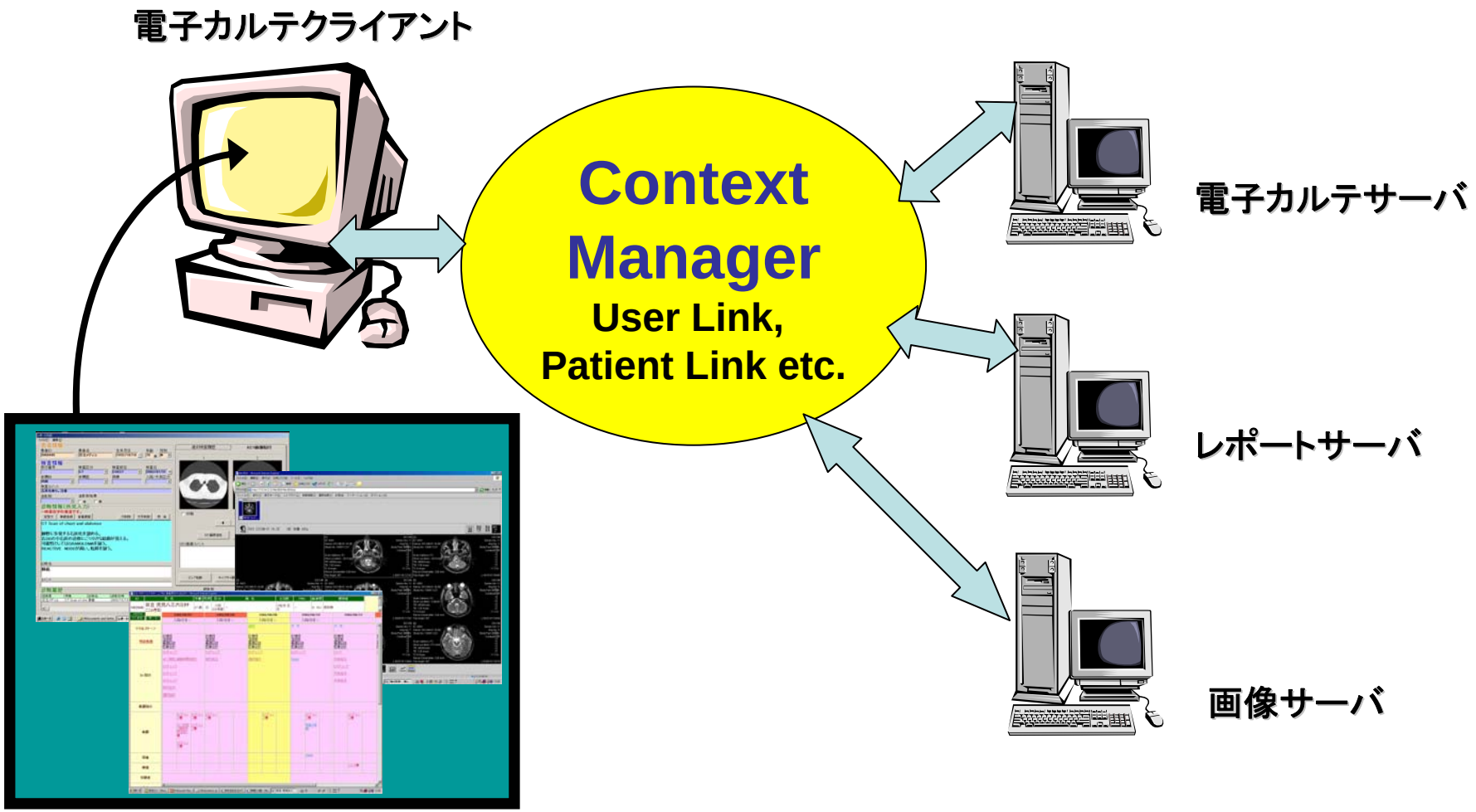
# 従来の情報システムの例



# Web版情報システム



# CCOW が解決しようとする方式

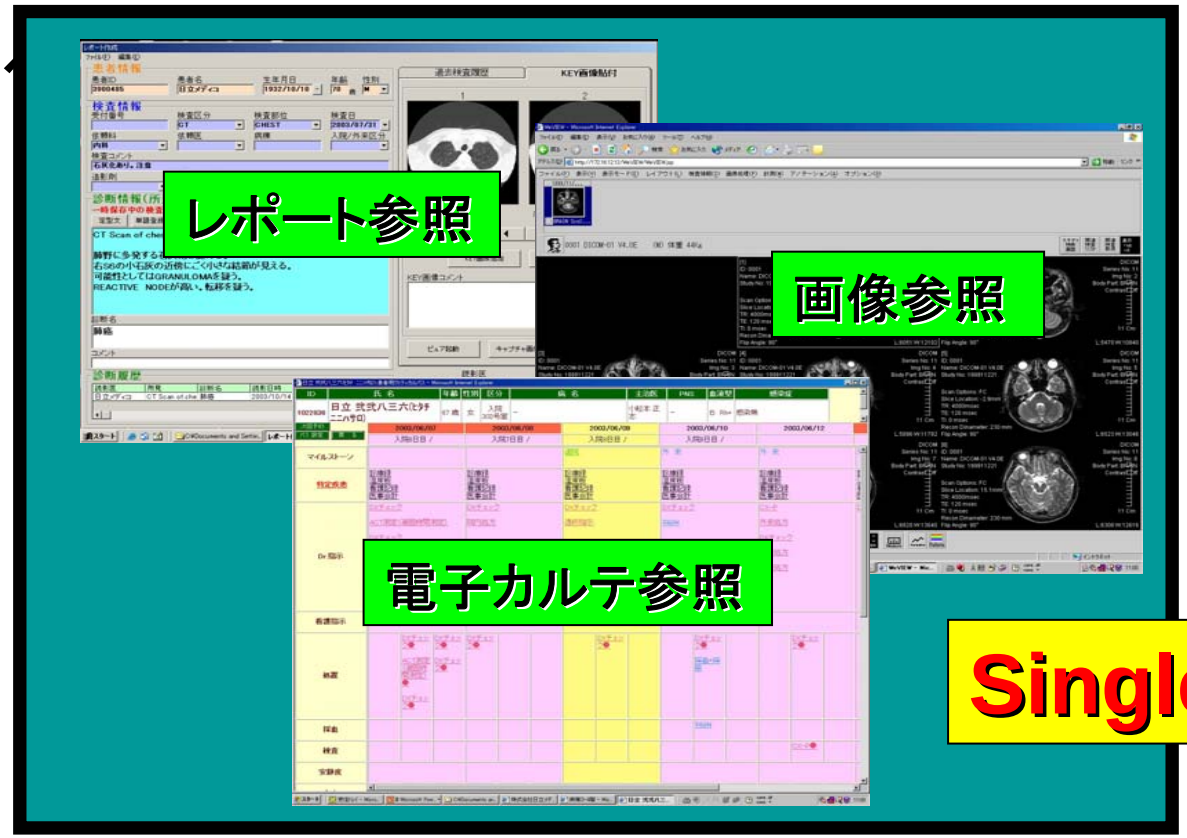





☆ IHE－Jベンダーワークショップ 2005/9/8 

# EUAでのCCOWとは...

- 同一デスクトップ画面上で、独立したアプリケーションに対して、同一ユーザに同期させ

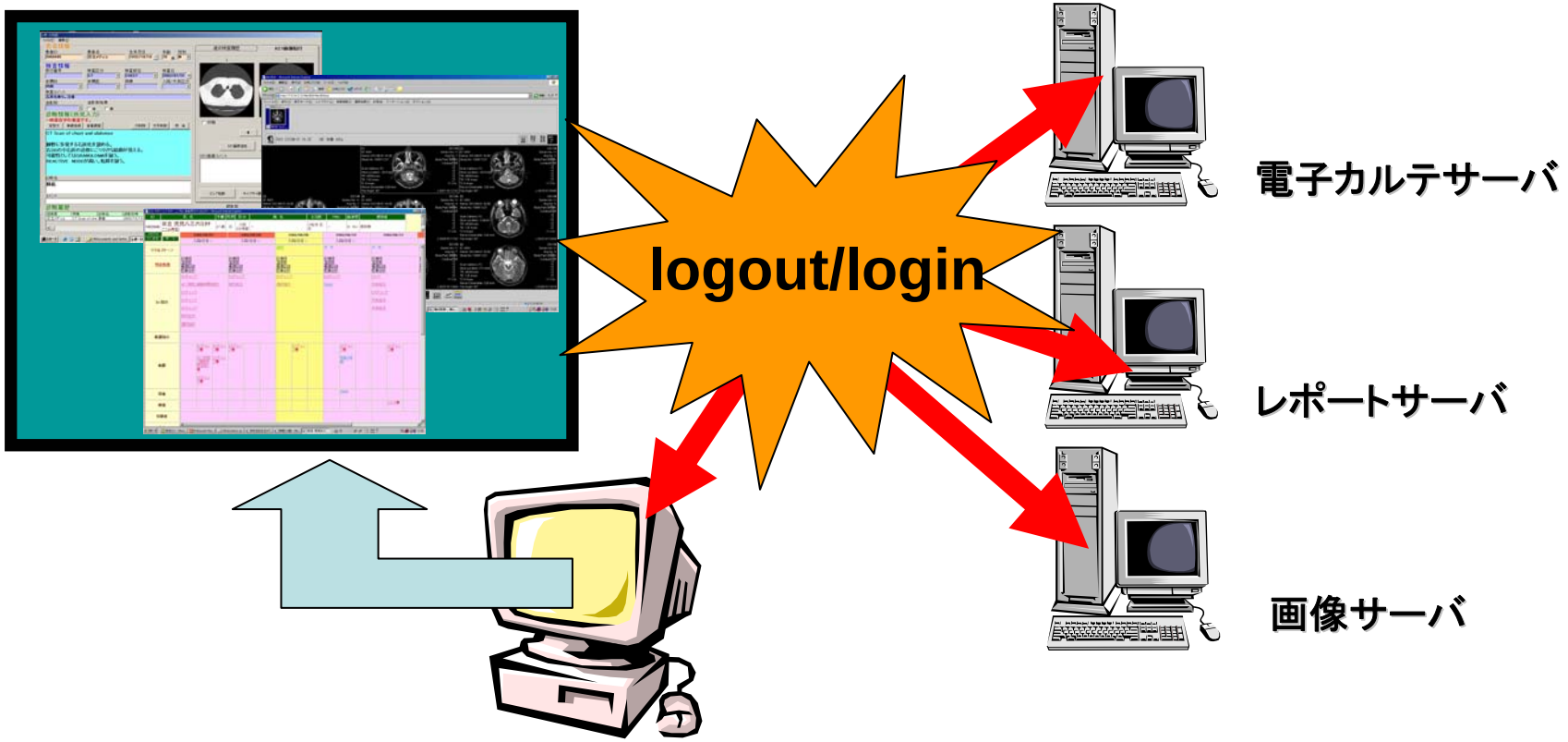





☆ IHE－Jベンダーワークショップ 2005/9/8  から引用

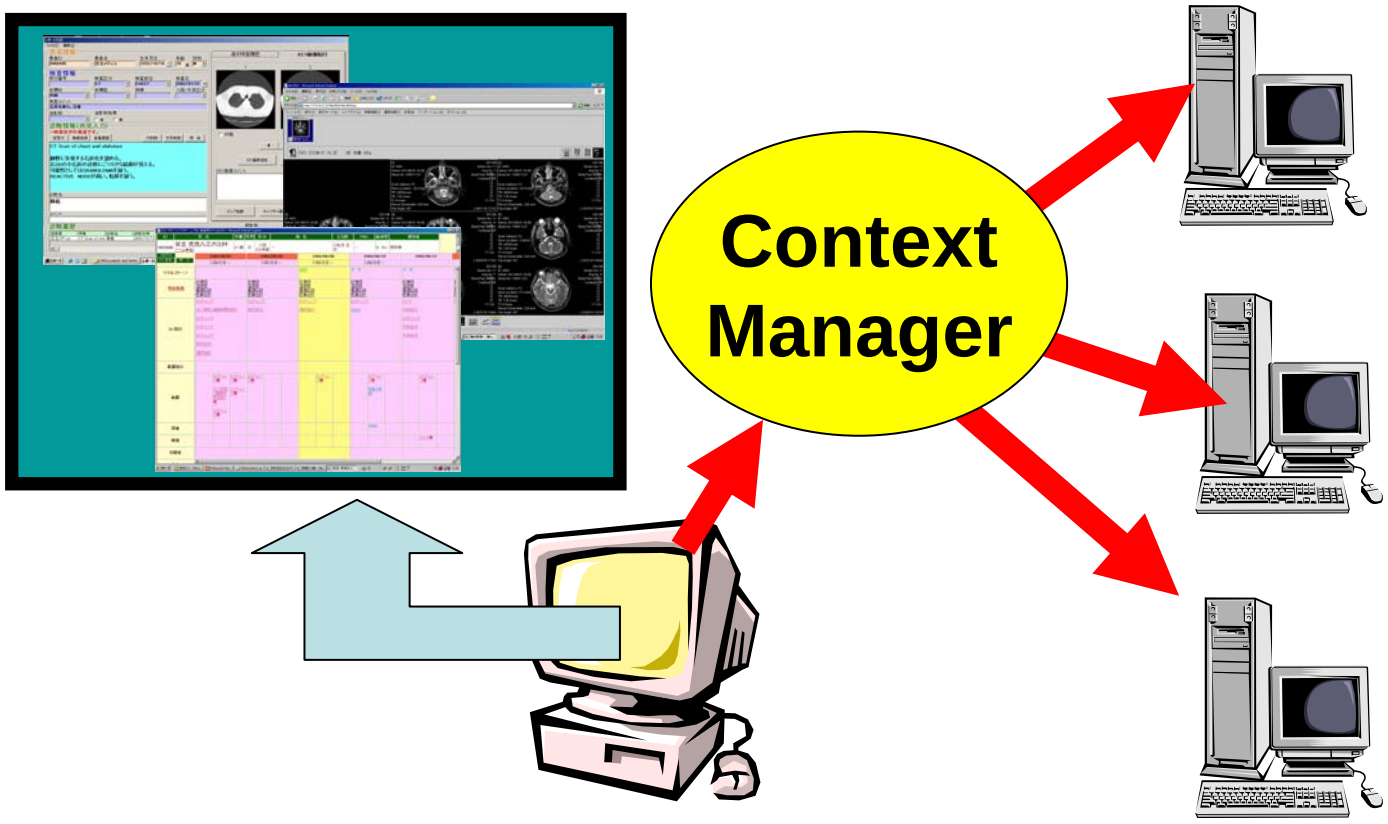
# 解決しようとする問題

従来の方法では、この端末のユーザが代わる時には全ての
アプリケーションとPCに対してlogoutとloginが必要であった



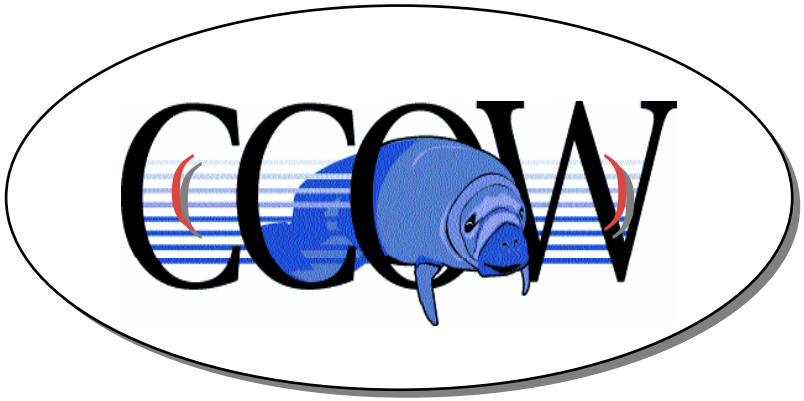
# ユーザアプリケーション同期

一度loginすれば全てのWindowに同一ユーザでloginできる
login後に起動するWindowも同一ユーザで自動的にloginされる



# 施設内利用者認証（EUA）

EUA = Kerberos + CCOW



# 施設間利用者認証（XUA）

## *概要と範囲*

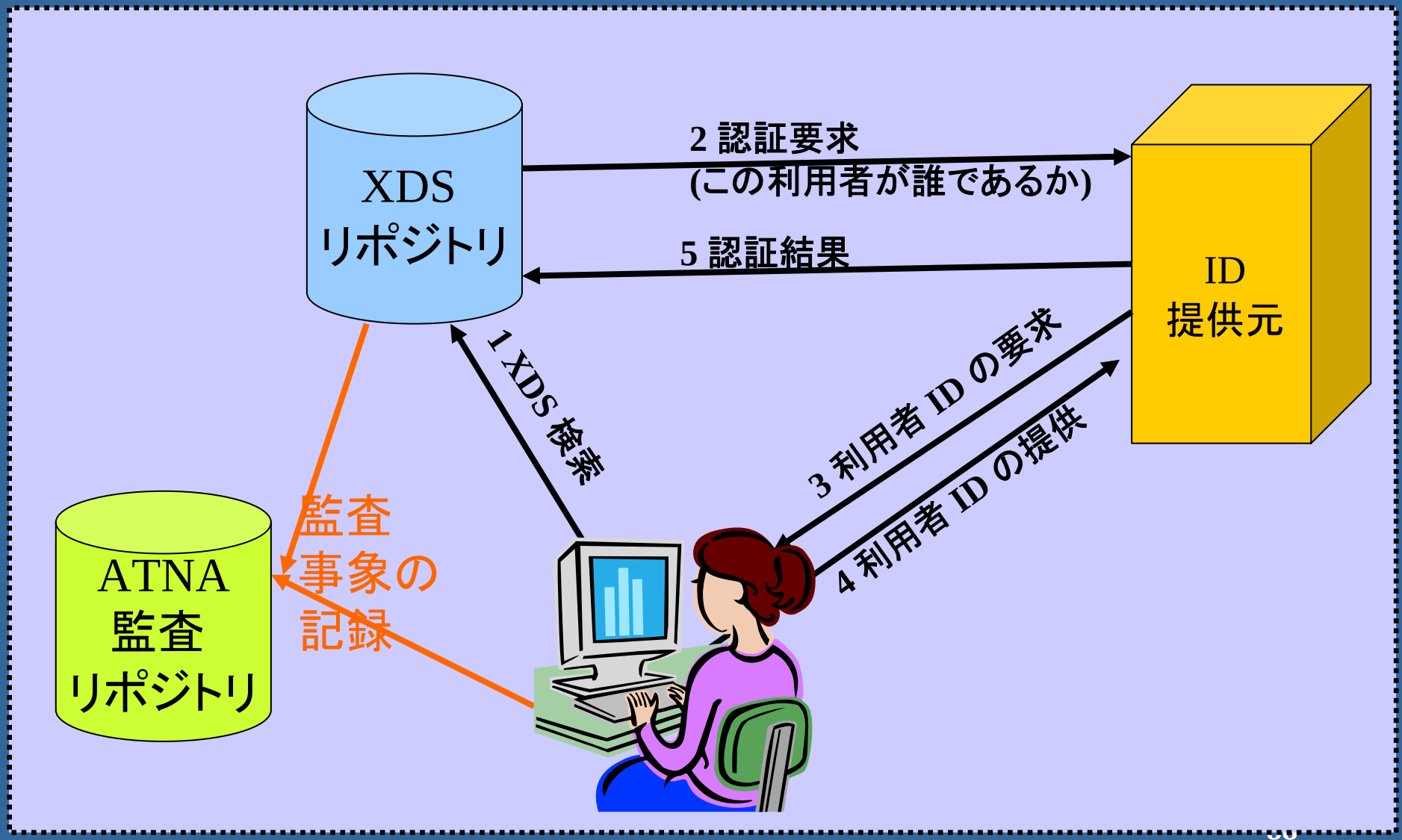
- 施設間にまたがるユーザー認証の提供
- 認証強度情報の提供
- オプションとして連絡先情報の提供
- 利用者IDの開示メカニズムはIHEのプロファイルで指定される。また地域ドメインのポリシーにより制約を受ける。

# 施設間利用者認証（XUA）

## *特長*

- 利用者IDの地域ドメインへの拡張
  - 任意の施設間トランザクションをサポート
  - 連携型、または集中型
- 必要な情報を提供し、XDSアクタがアクセス制御の決定を行えるようにする
  - アクセス制御のメカニズムは含まない
- 必要な情報を提供し、XDSアクタが詳細かつ正確なセキュリティ監査証跡を生成できるようにする

# 施設間利用者認証（XUA）



# 施設間利用者認証（XUA）

## *使用規格*

- SAML2.0プロファイルを採用
- SAMLブラウザのSSOプロファイルの利用を指定、クライアント/プロキシ・プロファイルを拡張した
- SAMLプロファイルをXDS（すなわちebXMLレジストリ）と一緒に使用することを指定
  - SAMLの使用がebXML 3.0 と両立すること
- SAML2.0の仕組みを拡張してHL7に合わせる
  - 将来はDICOMも

# SAML

- SAML: Security Assertion Markup Language
- 標準化団体OASISによって策定された、IDやパスワードなどの認証情報を安全に交換するためのXML仕様。一度の認証で複数のWebサイトやサービスが利用できるSingle Sign-On（SSO）を実現。
  - OASIS:ビジネスにおける情報交換用技術標準を作成する国際団体。XMLやSGMLなどの標準技術をベースに活動。
- 従来のSSOと異なり認証クッキーを使用しないので、クッキードメインの制限がなく、グローバルなSSOを実現できる。
- 現行版はSAML 2.0

# 施設間利用者認証(XUA)

## アクタ

利用者認証提供者 – 仕様にはないが必要である。EUAないし他の認証システムでよい

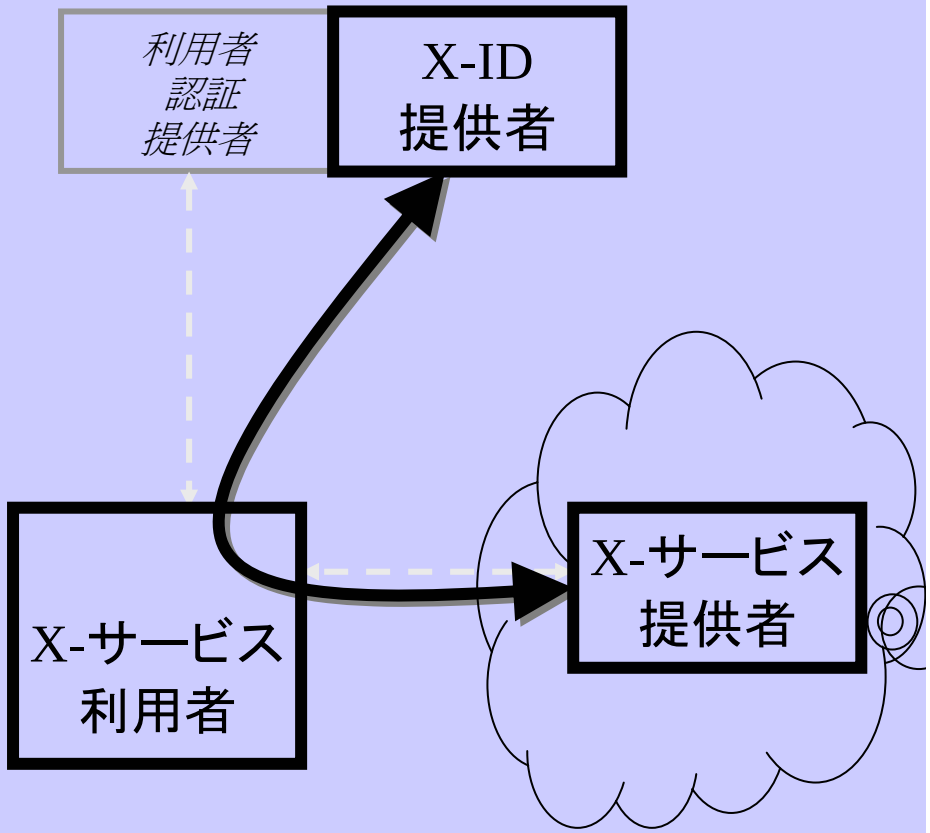
X-ID提供者 – SAML ID 提供者

X-サービス利用者 – 利用者と相互作用する任意のIHE アクタで、“利用者認証提供者”を用いて利用者の認証を行った

X-サービス提供者 – XUAを要求する任意のIHEアクタ

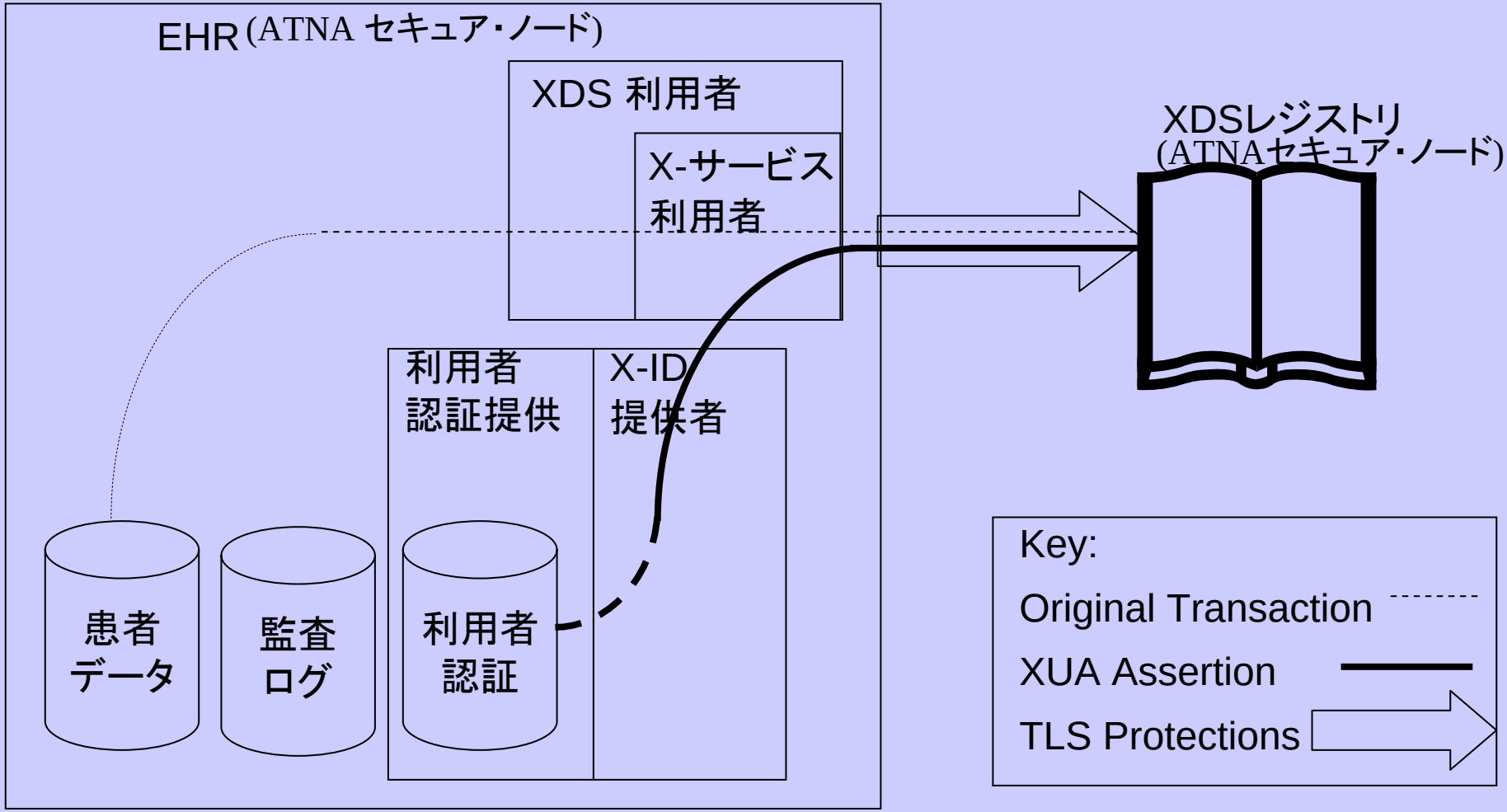
破線 – 既存のトランザクション

実線 – XUA



# 施設間利用者認証(XUA)

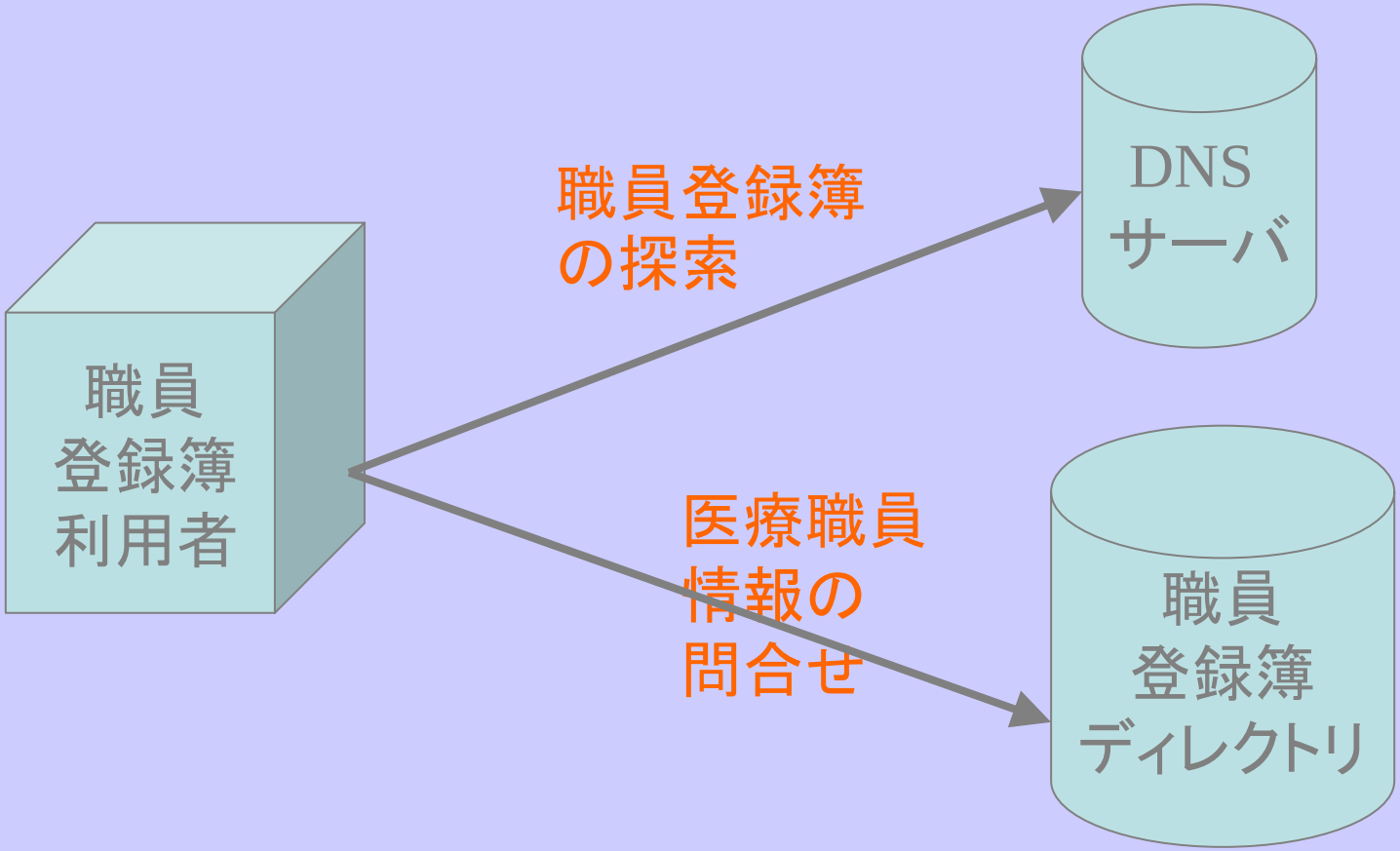
## *実装例*



# 職員登録簿(PWP)

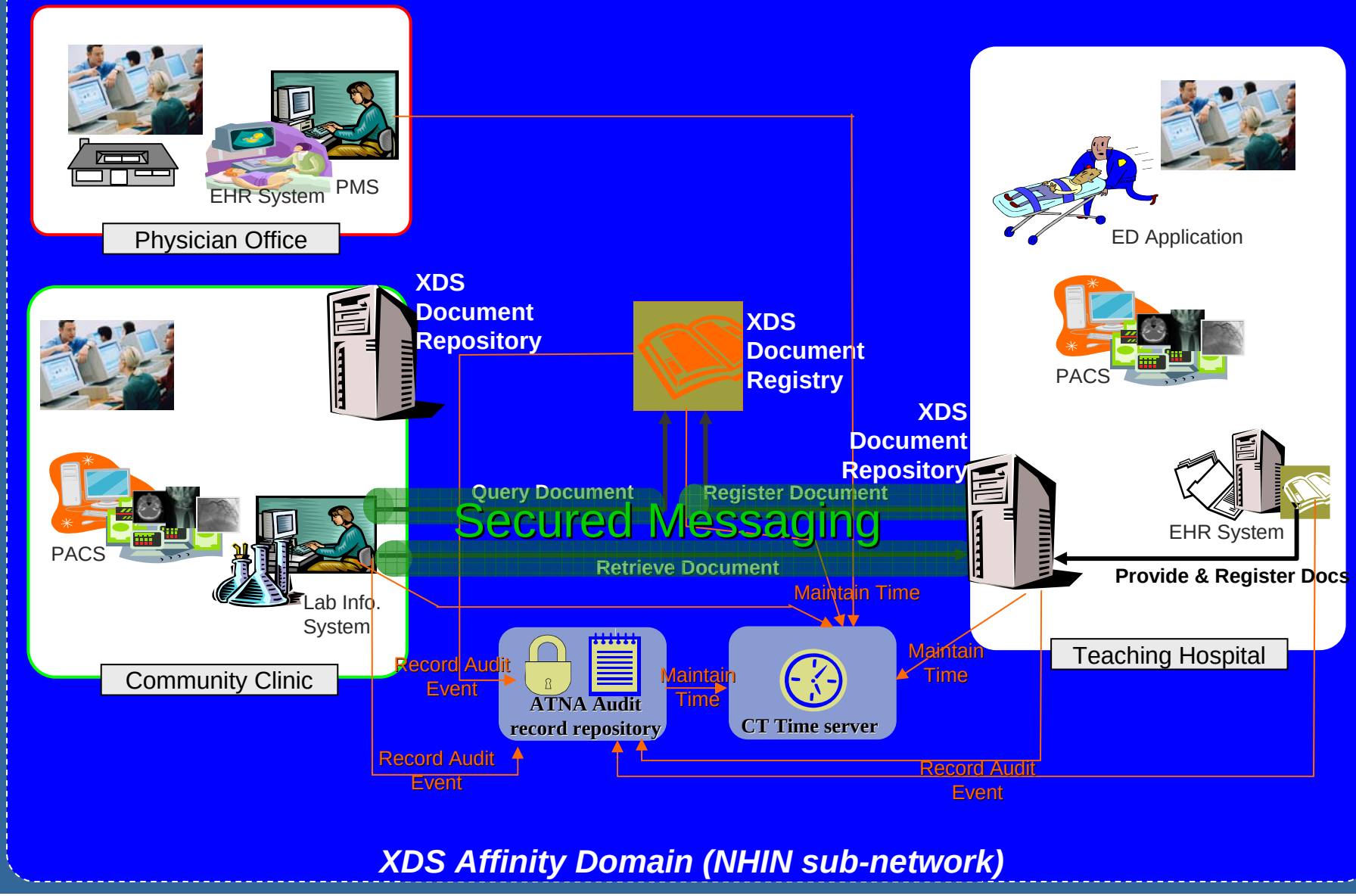
- White Page:個人別電話帳
  ⇔　Yellow Pages :職業別電話帳
- 病院スタッフの基本情報へのアクセス手段を提供する
- PWP(職員登録簿)を見つける方法を定義
- 問合せとアクセス方法の定義

# PWP – トランザクション

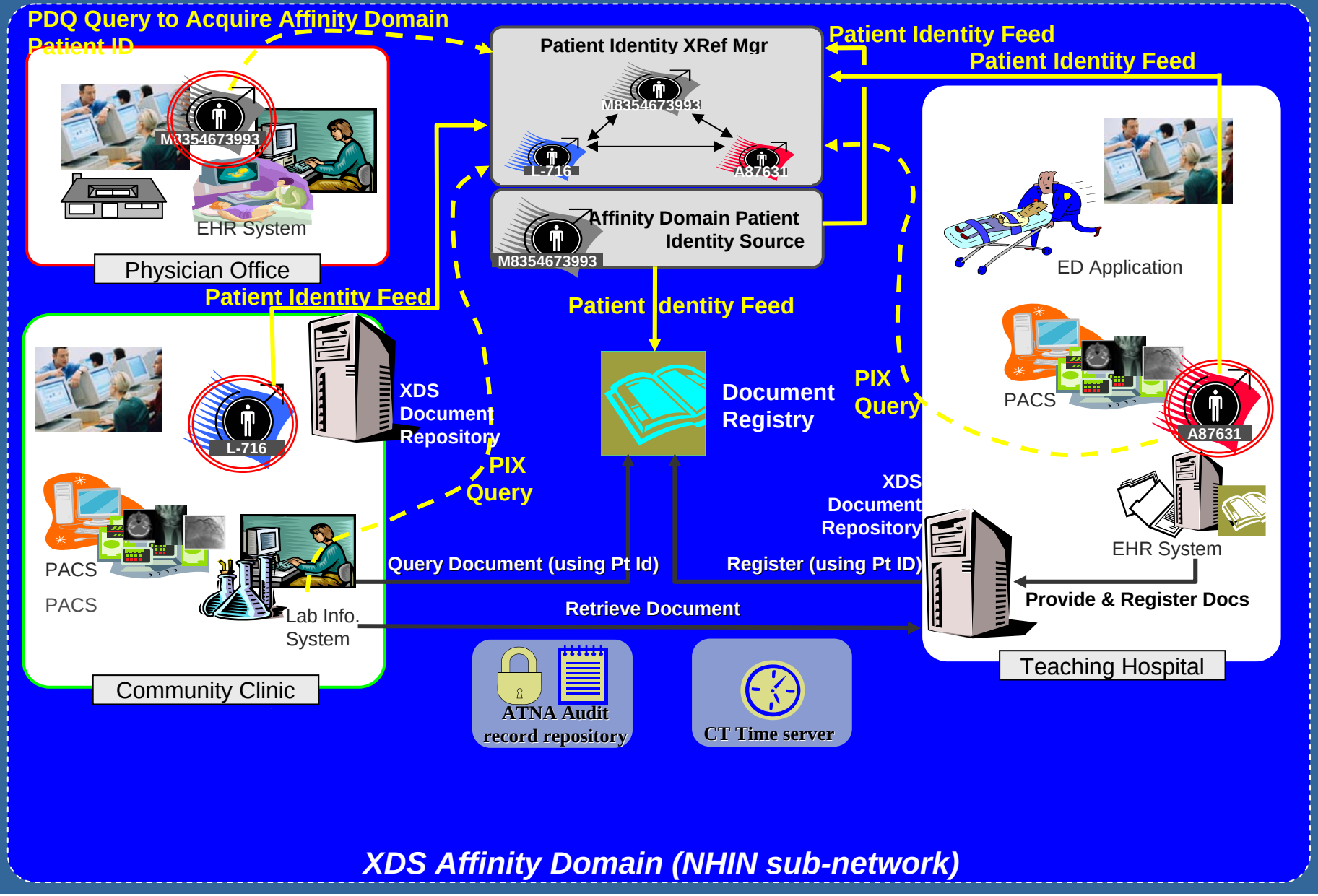



***標準の方法でシステムに医療職員情報をアクセスする手段の提供***

# XDS シナリオ + ATNA と CT の利用

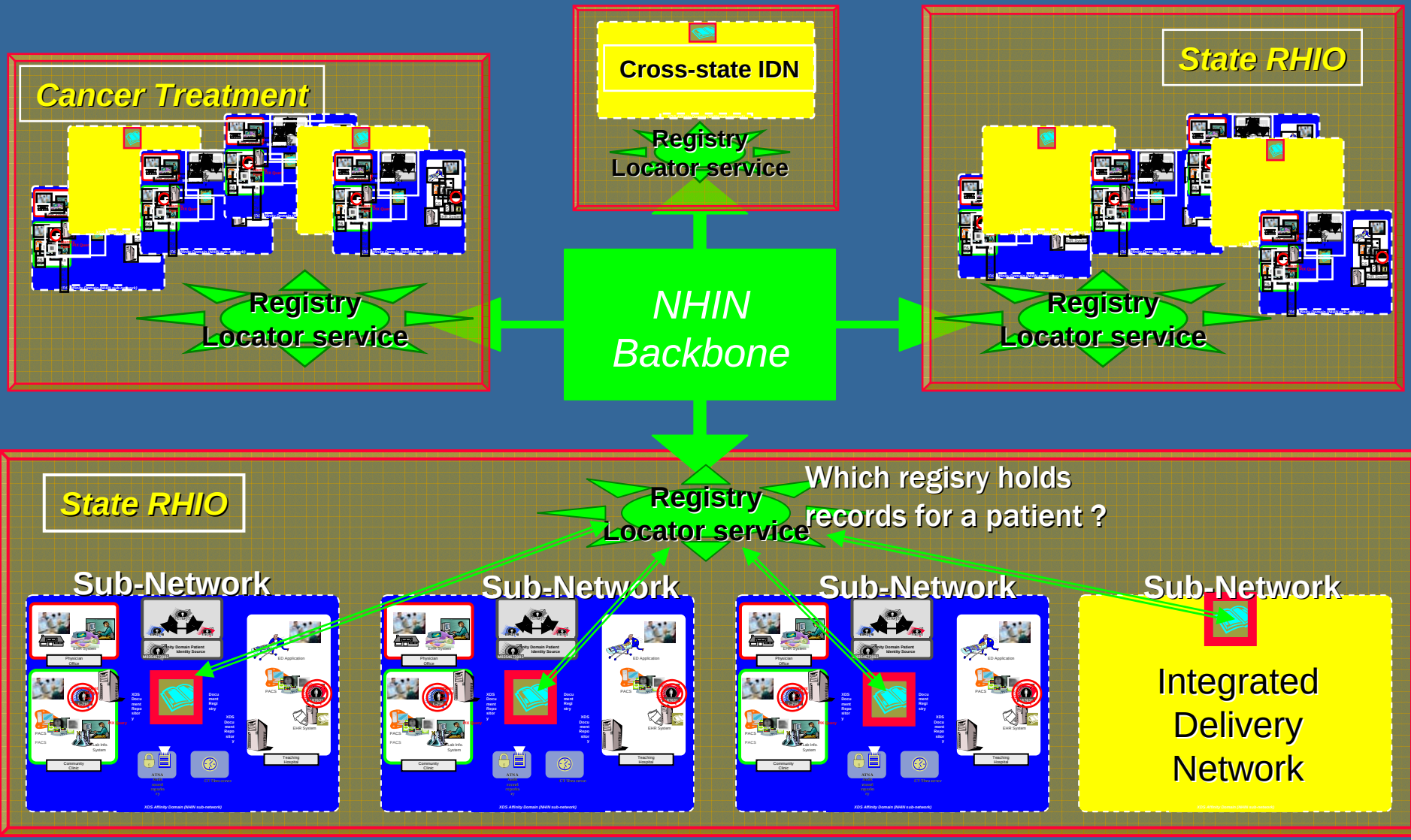


# XDS シナリオ + PIX と PDQ の利用



# XDSドメインと非XDSドメインの連結

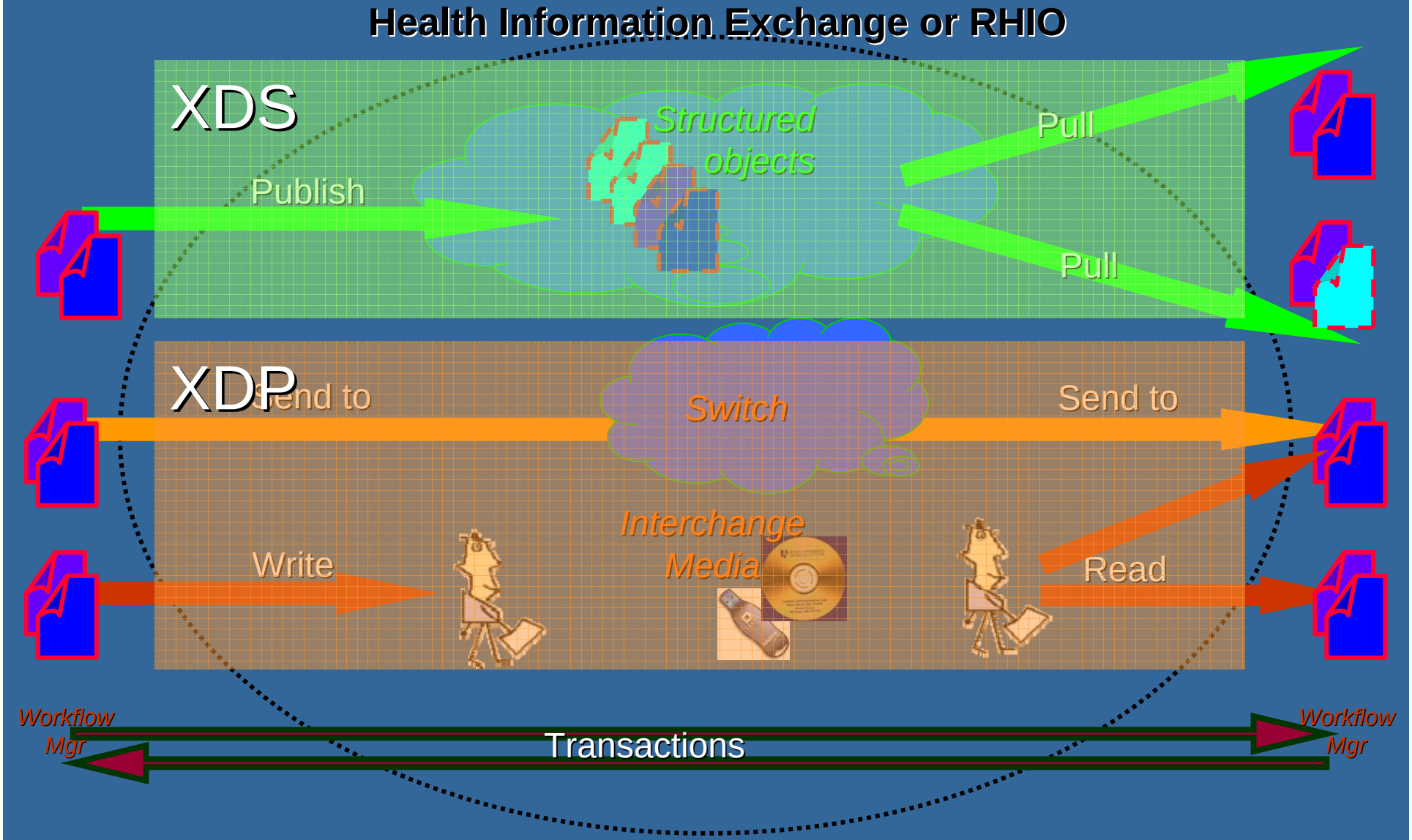
## Leverage Connecting for Health RLS – 2006-2007 Development



# 2006-2007の新プロファイル Supplements

- **パブコメ締め切り: 2006年7月5日**
  - XDS Stored Query
  - XDS-SD – スキャン文書
  - XDP – 施設間文書交換

# Flexible Infrastructure:
# 共有、送付、交換



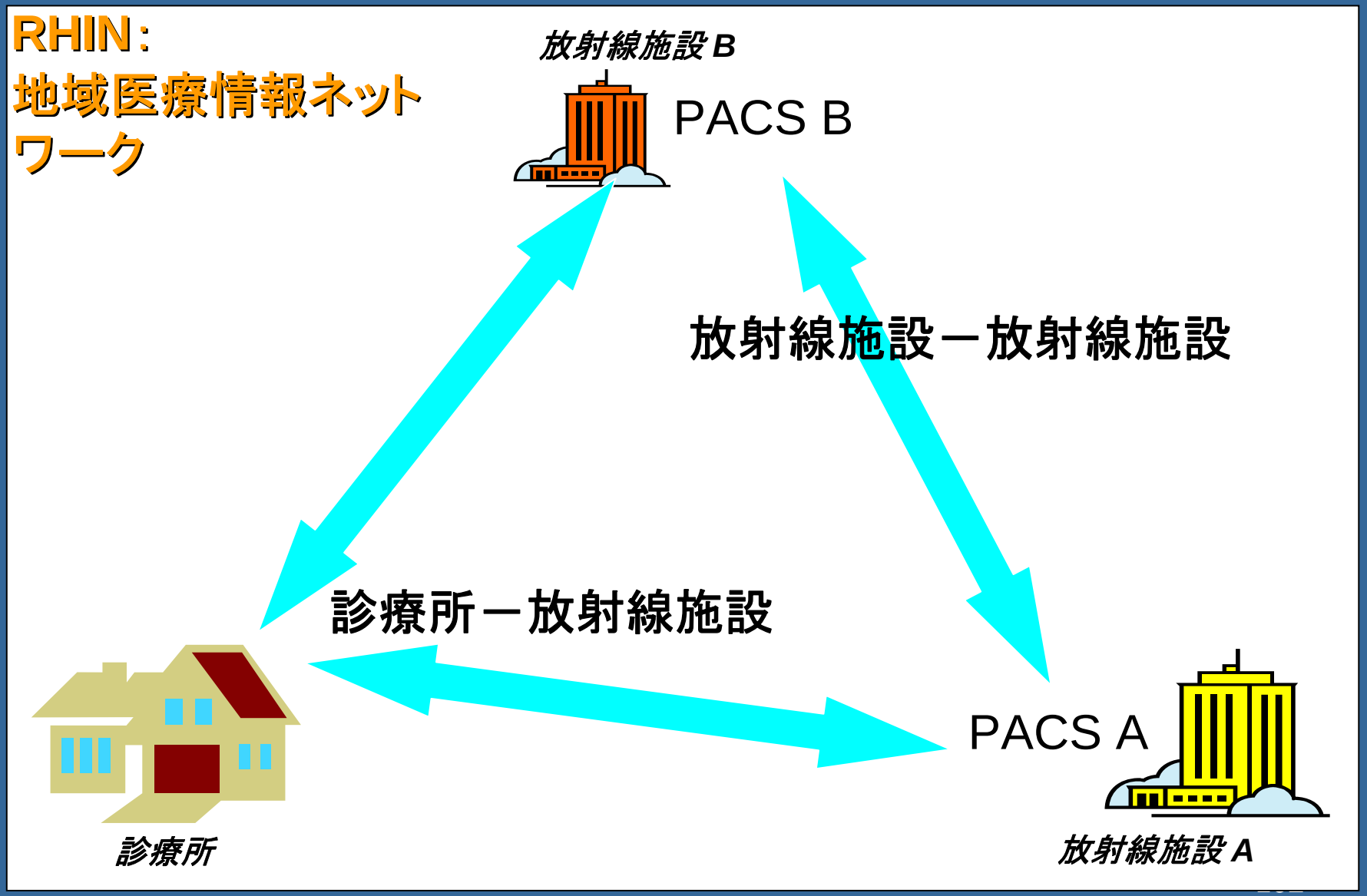
# XDSの応用

- XDS-I
- PCC
- XDS-LAB

# 施設間画像情報共有（XDS-I）

- 施設間で画像情報を共有する
- 画像情報とは以下のものを含む
  - 広義のDICOMインスタンス
    画像、evidence　documents、presentation states
  - （表示用の）読影レポート
  - レポートに関連したキー画像

# RHINにおける放射線レポート・画像の共有



# RHINにおける放射線レポート・画像の共有

**RHIN：**
**地域医療情報ネットワーク**

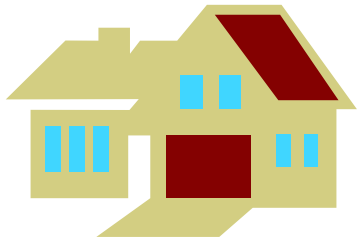
*放射線施設 B*

PACS B

*施設間*
*レジストリ*

*患者Id= 3547F45*

- レポート 5/21/1998 : CT頭部 ➔B
- 検査画像 5/21/1998 : CT頭部 ➔B
- レポート 2/18/2005 : 胸部X線 ➔A
- 検査画像 2/18/2005 : 胸部X線 ➔A

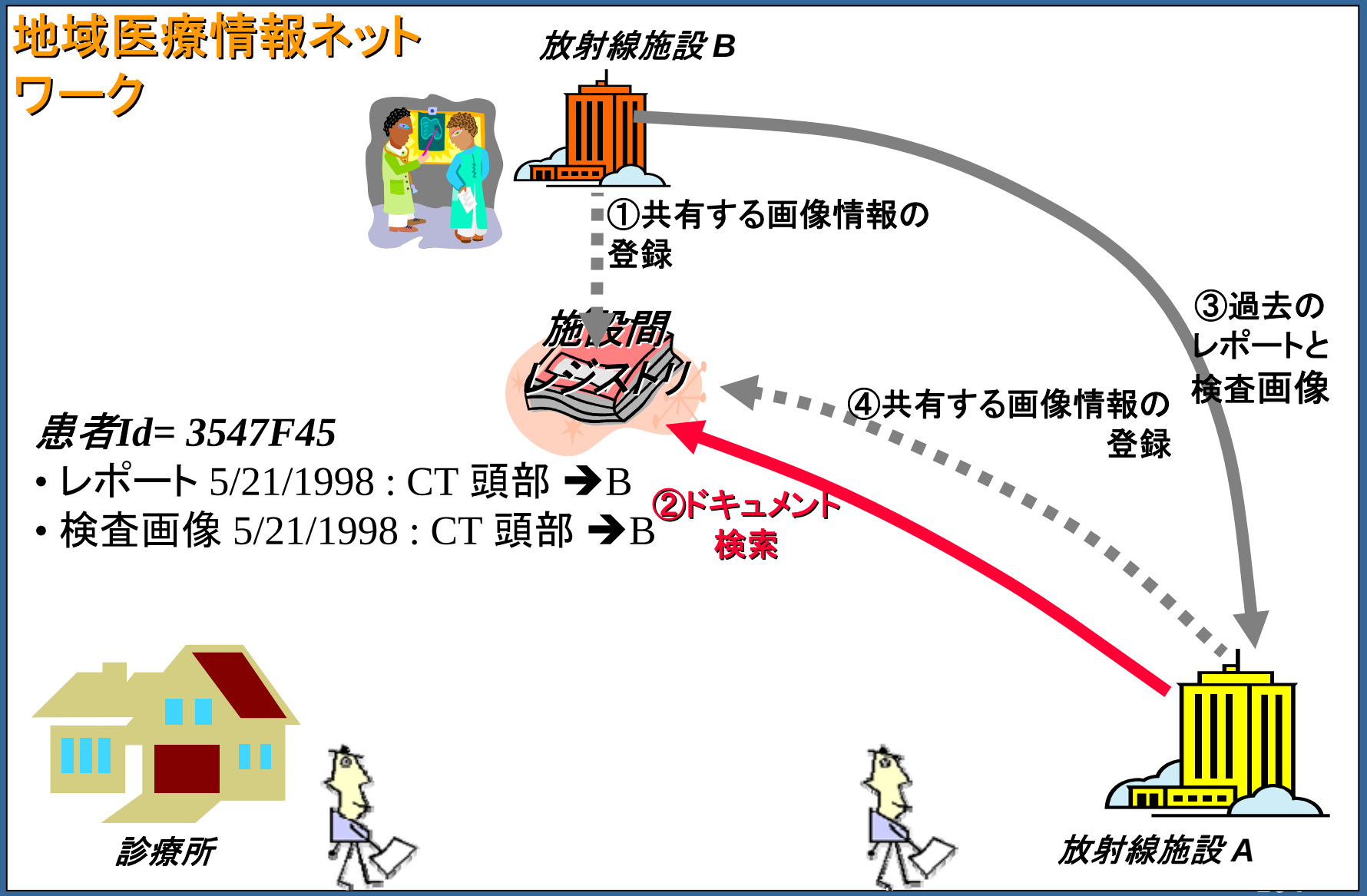


*診療所*

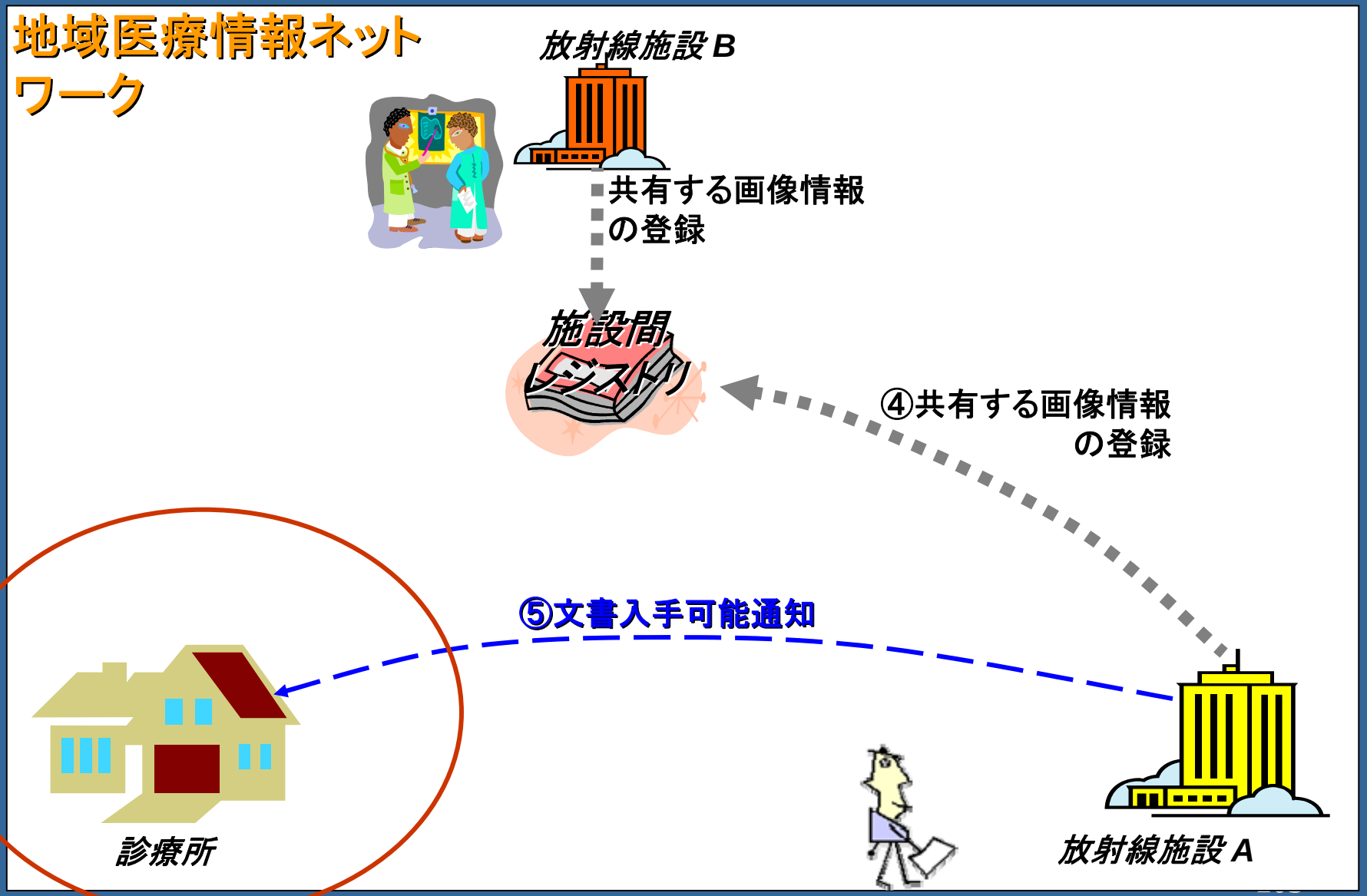
PACS A

*放射線施設 A*

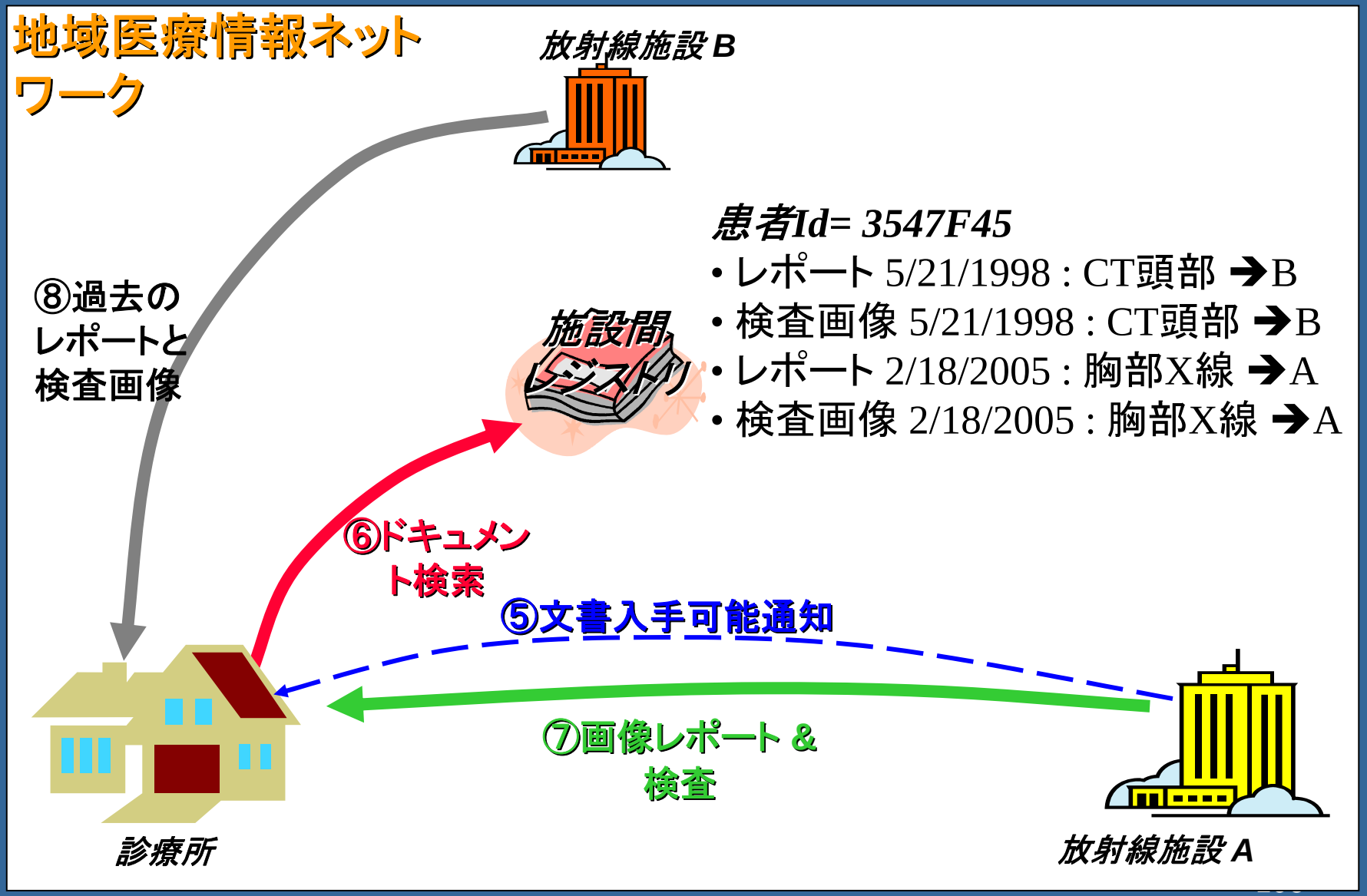
# 通常の画像検査の紹介ケース
## ～ RHINにおける診療医と医療のしくみ～



# 通常の画像検査の紹介ケース
## ～ RHINにおける診療医と医療のしくみ～



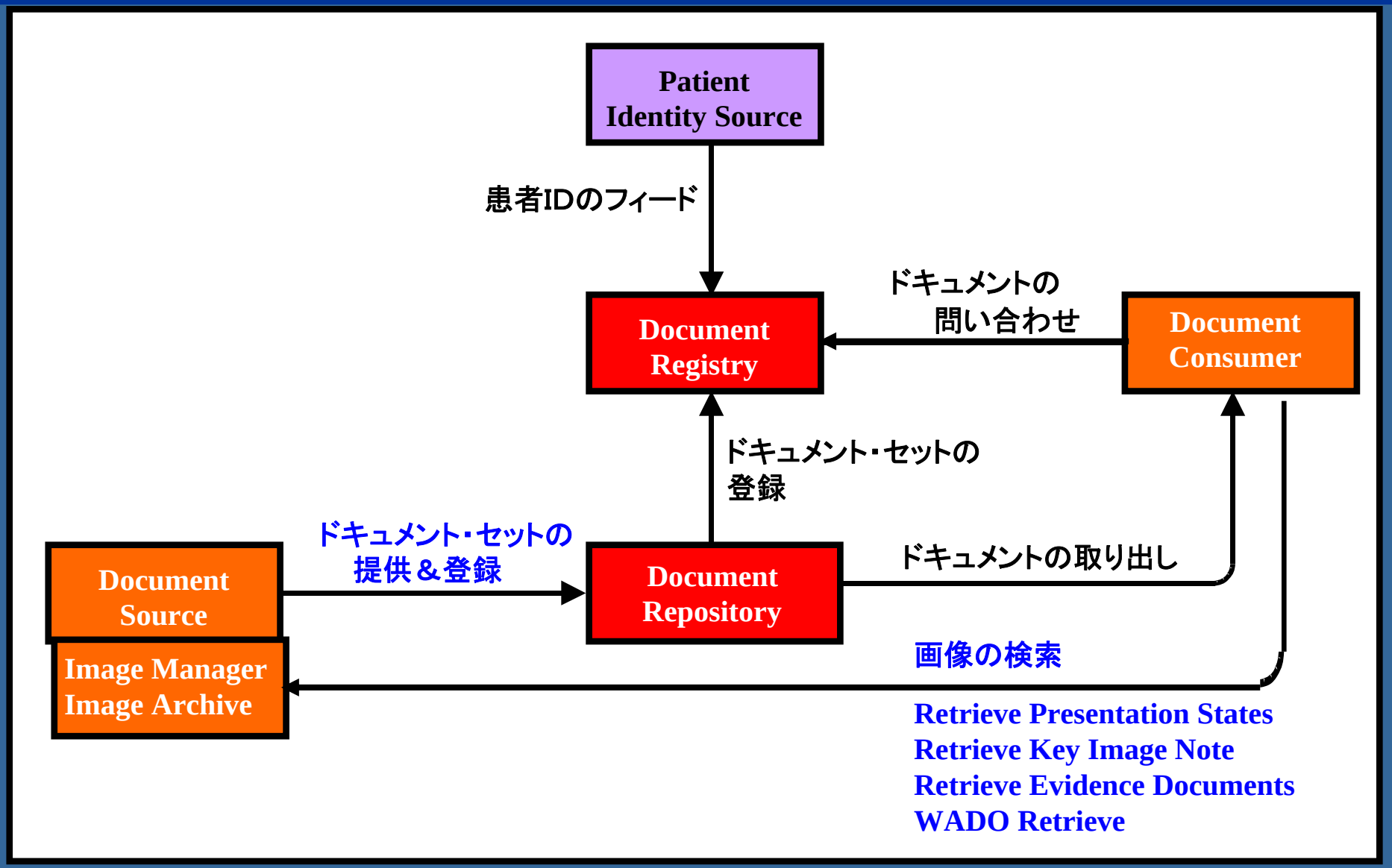
# 通常の画像検査の紹介ケース
## ～ RHINにおける診療医と医療のしくみ～



# XDS-I とXDSの関係

- XDS-I はXDSをベースにしている。
- アクターはXDSと同じ
  - Document Source
  - Document Consumer
  - Document Registry
  - Document Repository
- 画像検査データ（画像とレポート）のサポートを追加している

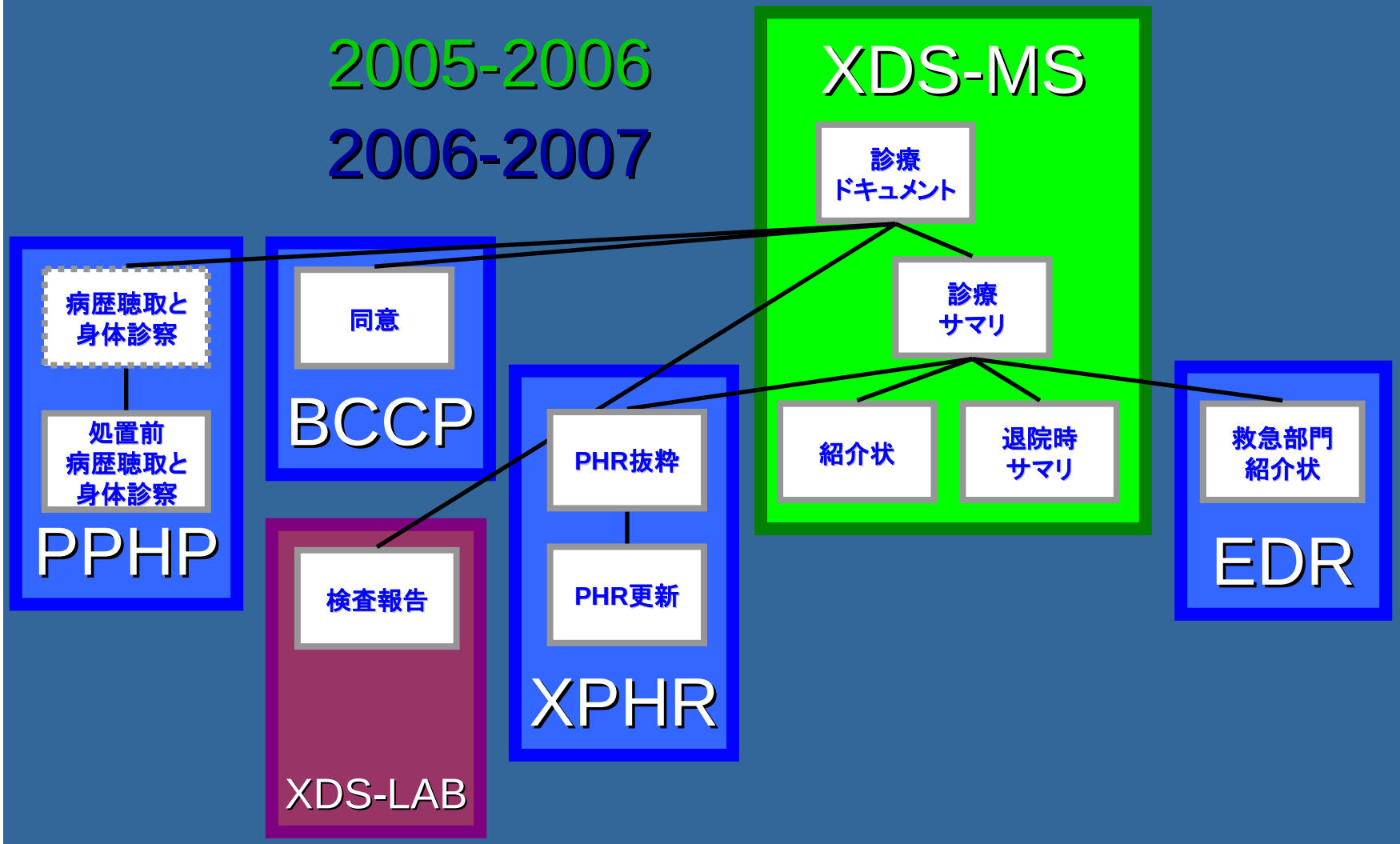
# XDS-I アクタとトランザクション



# 患者ケア連携(PCC)

- 2005年に導入された新しいテクニカルフレームワーク
- ケアの連携
  - 医療提供者間で
  - 患者の複数の問題にわたって
  - 時間を越えて
- XDSの成功の上に構築
- データ型の混在
  - 現状は構造化されていないテキストが主
  - +/- 構造化されたデータの混在

# 患者ケア連携（PCC）
## コンテンツ統合プロファイル



# 患者ケア連携(PCC)
# 統合プロファイルロードマップ

- **Year 2005-2006 (試行実装)**
  - 診療サマリ [MS] – 急性期医療からかかりつけ医への退院時サマリ、かかりつけ医から専門医への紹介状
  - 非構造化文書 – CDAで包んだPDF
- **Year 2006-2007 (開発と試験)**
  - 診療サマリ [MS] – 救急部門紹介状 [EDR]
  - 手術前の病歴聴取と身体診察 [PPHP]
  - 基本的な患者プライバシー同意 [BPPC]
  - 患者カルテ交換 [XPHR]
  - 検査部門との連携 [XDS-LAB]
- **将来 (プロファイル文書 / 白書)**
  - 診療サマリ [MS] – LTCに向けての退院時サマリ
  - データ取得の書式表示 (例 臨床研究)

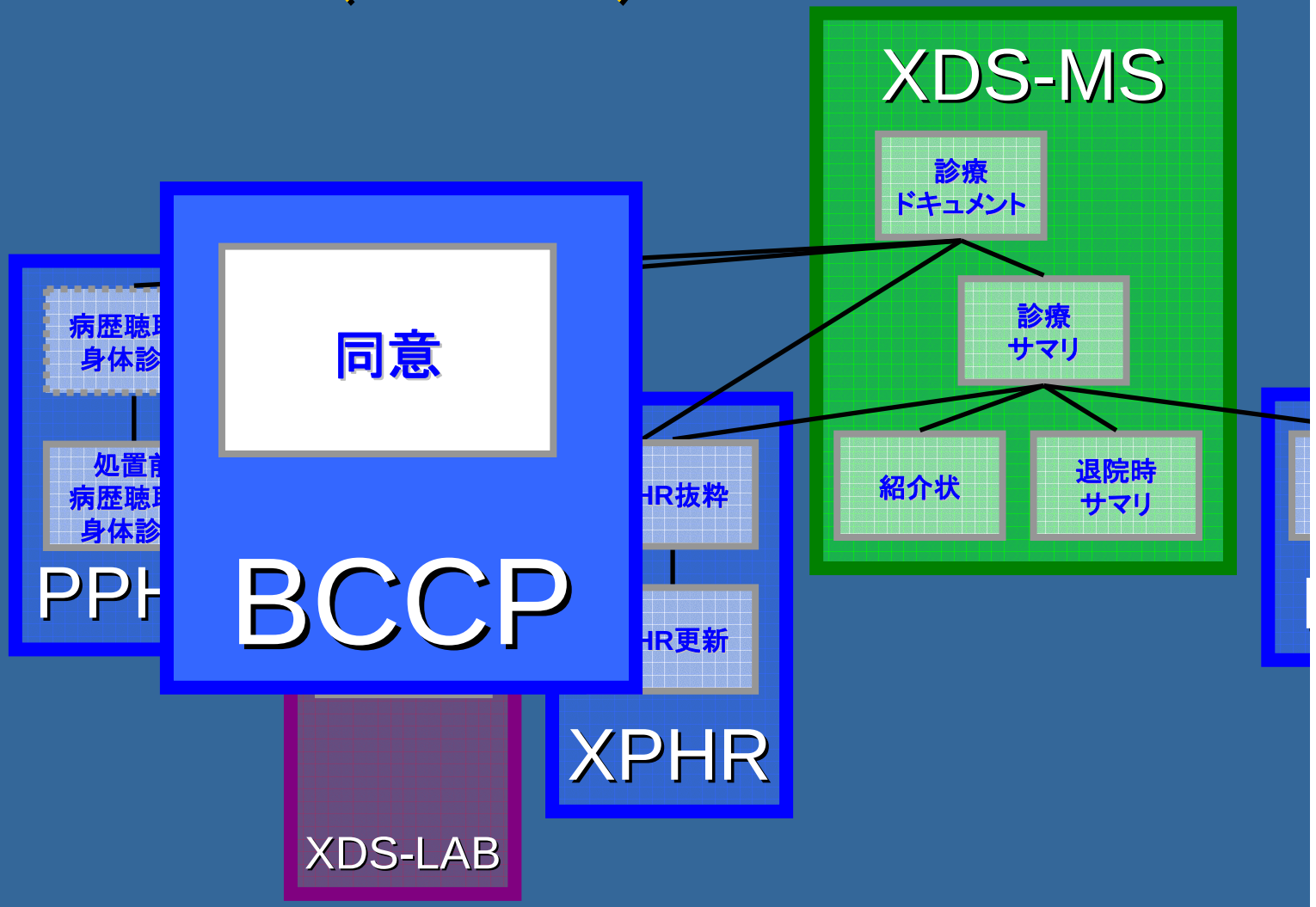
# 患者ケア連携(PCC)
## 診療サマリ・プロファイル

- **文書移送 (統合プロファイル)**
  - XDS/XDP 文書共有用.
  - NAV 通知用.
  - 組織をサポートするXDS フォルダ.
  - パッケージ化をサポートするXDS 登録セット.
  - 「主要」文書もしくは目録の同定
- **文書コンテンツ (コンテンツプロファイル)**
  - CDA Release 2.0
  - Care Record Summaries 実装ガイド

# 患者ケア連携(PCC)
# コンテンツ統合プロファイル

- 特定の標準を使用するコンテンツ
  - CDA Release 2.0
  - HL7 Care Record Summary (CRS)
  - ASTM/HL7 Continuity of Care Document (CCD)
  - 必要に応じて他も (e.g., ASTM CCR, DICOM …)
- 再利用可能な部品のライブラリ
  - 文書タイプ
  - セクション
  - 入力

# 患者プライバシーの基本同意（BPPC）



# 患者プライバシーの基本同意（BPPC）

- 患者プライバシーの基本同意 (BPPC) プロファイルは、以下の機構を提供する:
  - 患者プライバシー同意の記録、
  - 公開を許可するのに用いられる患者プライバシー同意付きでXDSへ公開された文書の印付け、
  - 使用に適切なプライバシー同意の強制

# IHE IT Infrastructure ロードマップ

| | | EHR サポート | セキュリティ | 共通データ |
|---|---|---|---|---|
| ステージ0 | 2004年コネクタソンに向けた2003年プロファイル開発成果 | ・表示のための情報検索 (RID)<br>・患者IDの相互参照 (PIX)<br>・患者同期アプリケーション (PSA) | ・施設内利用者認証 (EUA)<br>・統一時刻 (CT) | |
| ステージ1 | 2005年コネクタソンに向けた2004年プロファイル開発成果 | ・施設間ドキュメント共有 (XDS)<br>・患者情報の問合せ (PDQ) | ・監査証跡とノード認証 (ATNA)<br>・職員登録簿 (PWP) | |
| ステージ2 | 2006年コネクタソンに向けた2005年プロファイル開発成果 | ・ドキュメント入手可能通知 (NAV)<br>・患者情報管理 (PAM) | ・施設間利用者認証 (XUA)<br>・ドキュメント電子署名 (DSG) | |
| ステージ3 | 2007年コネクタソンに向けた2006年プロファイル候補 | – 2005年11月に決定<br>・テンプレート・レジストリ<br>・患者情報の問合せ - 複数施設<br>・連合XDSレジストリ<br>・XDSとRIDのドキュメント検索能力整合<br><br>IHE PCC (患者ケア連携) 分野関連<br>・診療計画作成 – 施設内適用<br>・EHRの動的データ | – 2005年11月に決定<br>・RBAC (Role Based Access Control) – 施設内適用<br><br>IHE PCC (患者ケア連携) 分野関連<br>・患者同意 | – 2005年11月に決定<br>・LDAP 情報源の拡張<br>・処理誤りの管理 (TFM)<br>・RID 構成調整情報のディレクトリ<br>・サービス発掘<br><br>他のIHE分野ニーズに依存する項目<br>・マスターファイルのメンテナンス<br>・参照コードセットのメンテナンス |
| ステージ4 | 2008年コネクタソンに向けた2007年プロファイル候補 | ・診療計画作成 - 複数施設適用<br>・国家／地域EHRの指令書および計画への対応 (今後決定) | ・RBAC – 複数施設適用<br>・広域患者アクセス<br>・モバイルアプリケーション<br>・患者を個別識別したセキュリティ | ・ワークフロー管理の選好性<br>・SNMP MIBS (Simple Network Management Protocol, Management Informations Bases)<br>・LDAP機器ディレクトリのサポート |
| ステージ5 | 2009+年コネクタソンに向けた2008+年プロファイル候補 | ・複数診療領域の要素からなるXDS複合ドキュメント | ・遠隔サービスアクセス<br>・匿名化 (anonymization)<br>・仮名化 (pseudoanonymization)<br>・患者主導のアクセス | ・機器の自動認識と自動装備<br>・自動構成可能なRIDとXDS |

☆ 2005年6月時点の計画

# IHE IT Infrastructure
# 開発、実装状況

- オープンソース
  - IHE XDSのオープンソース公開中。他の統合プロファイルも予定
    - NIST（米国国立標準技術局）とSourceForge.net（オープンソース開発のサイト）から公開
    - JavaとJSP（Java Server Pages）で記述
    - 関連URL:
      - http://hcxw2k1.nist.gov/wiki/index.php/IheOs、http://sourceforge.net/projects/iheos/
  - NISTはXDSのテスト仕様／ツールも公開
    - 関連URL:
      - http://hcxw2k1.nist.gov/wiki/index.php/XDS_-_Cross-Enterprise_Document_Sharing
- テスト実装
  - HIMSS（米国医療情報管理システム協会）展示会（毎年2月開催）
  - Eclipse（米国ソフトウェアベンダによるオープンソース団体）のOHF（Open Healthcare Framework）プロジェクト
    - 関連URL:
      - http://hssp.wikispaces.com/、http://www.eclipse.org/ohf/


ご清聴
ありがとうございました