セキュリティ基盤の構築（ATNA）

ATNAの概要～目的

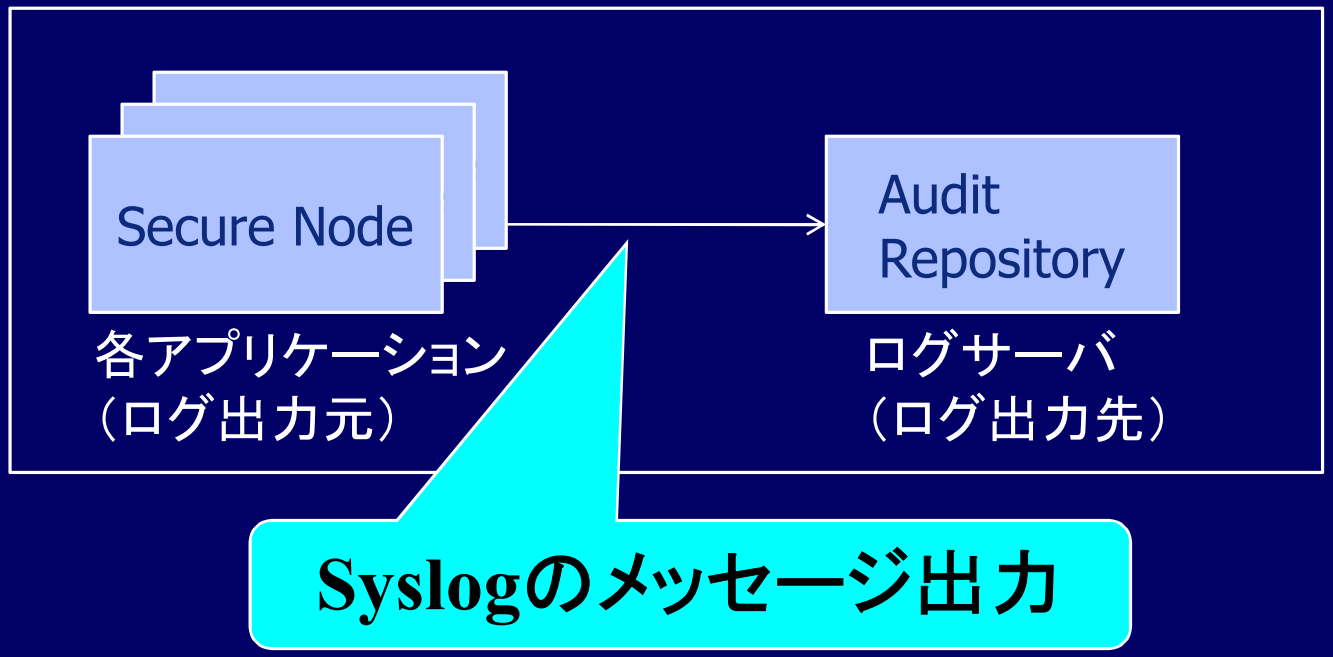
- ユーザへの説明責任（監査証跡）
  - 組織のセキュリティ管理者による監査に基づく、安全性に関する領域内のポリシーの遵守の評価
  - 保護すべきPHI(健康情報）に対する不適切な生成、アクセス、修正、削除の発見
- アクセス制御
  - ネットワークアクセスをノード間に制限し、各ノードに対して認可されたユーザにアクセスを制限する方法でのアクセス制御
- 集中監査記録レポジトリ
  - 全てのIHEアクタから、監査証跡レポジトリへ集中して記録する

ATNAの概要～監査証跡(AT)

- 1つのSecure Domain(院内システム)のシステムはIHEのアクタを実装している/いないにかかわらず、監査証跡ログを出力すること。
- 監査記録メッセージは、集中監査レポジトリへログ採取が行われる。
- 監査ログ取得の仕組みは、Reliable Syslog Cooked Profile(RFC-3195)を採用。
- 監査ログ取得すべきイベントが提案されている。

監査証跡の取得方法

- ATNAのAT(Audit Trail)は、監査証跡用ログ取得方法を検討。



監査証跡で取得するevent(例)

- システム/アプリケーションの開始/終了時
- ユーザログイン時
- ユーザ認証失敗時
- オーダ発行時
- 患者情報の出力export時
- 患者情報の取り込みimport時
- 画像格納時
- データ削除時

など

ATNAの概要～接続認証(NA)

- 各ノードの接続に対して、双方向の証明書ベースのノード認証を行う。
- DICOM,HL7,HTTPの各プロトコルは全て証明書ベースの決まった認証機構を持っている。
- ユーザではなく、ノード（システムや機器）を認証している。
- 双方向のノード認証ができない機器の接続は禁止されるか、PHIアクセスを防ぐようにする。

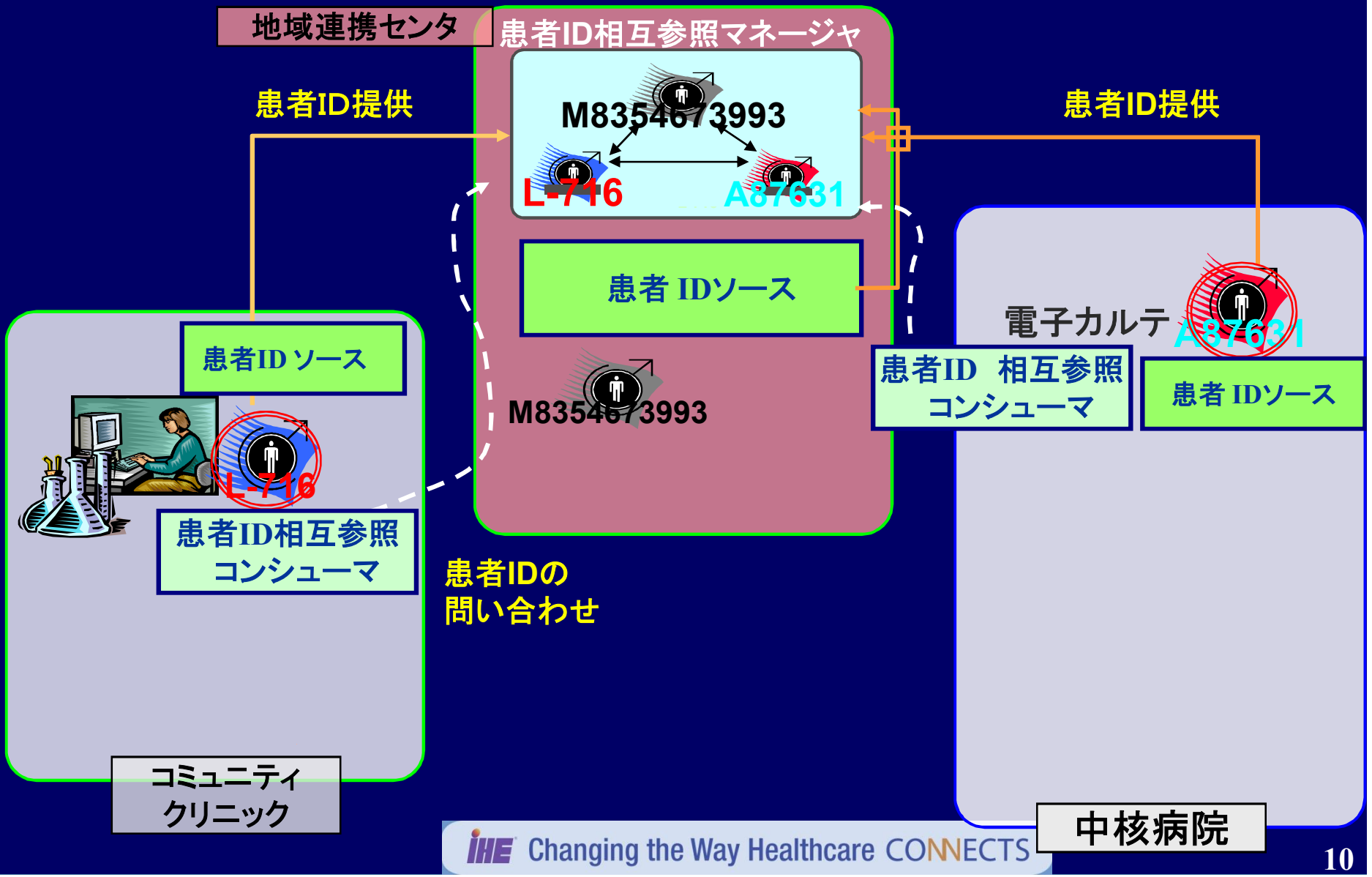
ATNAの概要～接続認証(NA)

- 利用している規格
  - DICOM及びHL7：TLSプロトコルを使用。
    - TLS_RSA_WITH_NULL_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA（ATNA暗号化オプション）
  - HTTP：一般的なブラウザはTLSによる相互認証をサポートしない＝拡張したブラウザを使用する。

    ※セキュアノードが物理的なセキュリティを守られた形で構成された場合は、通常のHTTP利用可。

患者IDの参照基盤（PIX/PDQ）

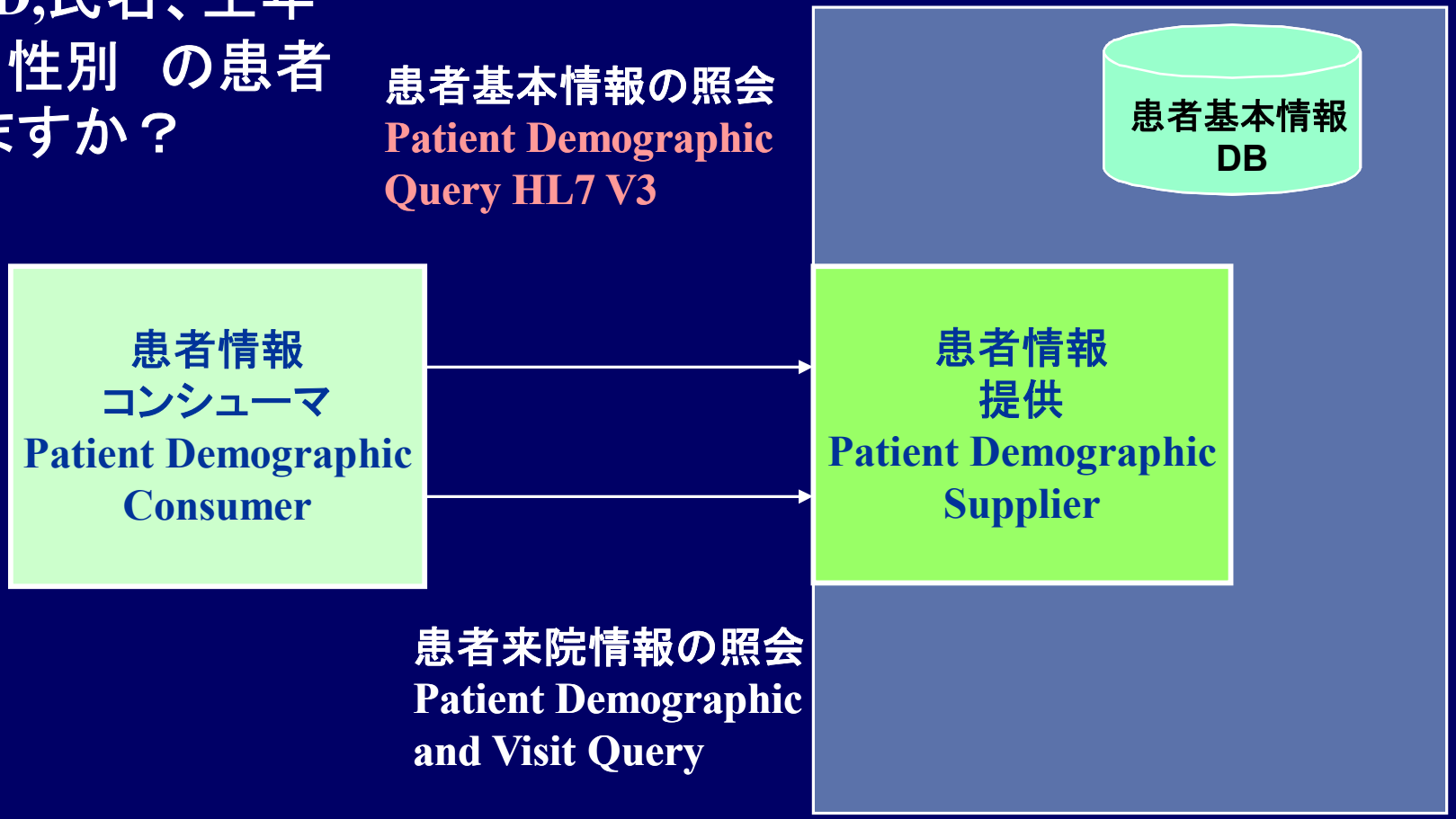
患者ID相互参照
PIX （Patient ID Cross Referencing）



患者基本情報の問い合わせ
Patient Demographic Query（PDQV3）

患者ID,氏名、生年月日、性別　の患者はいますか？

患者基本情報の照会
Patient Demographic Query HL7 V3



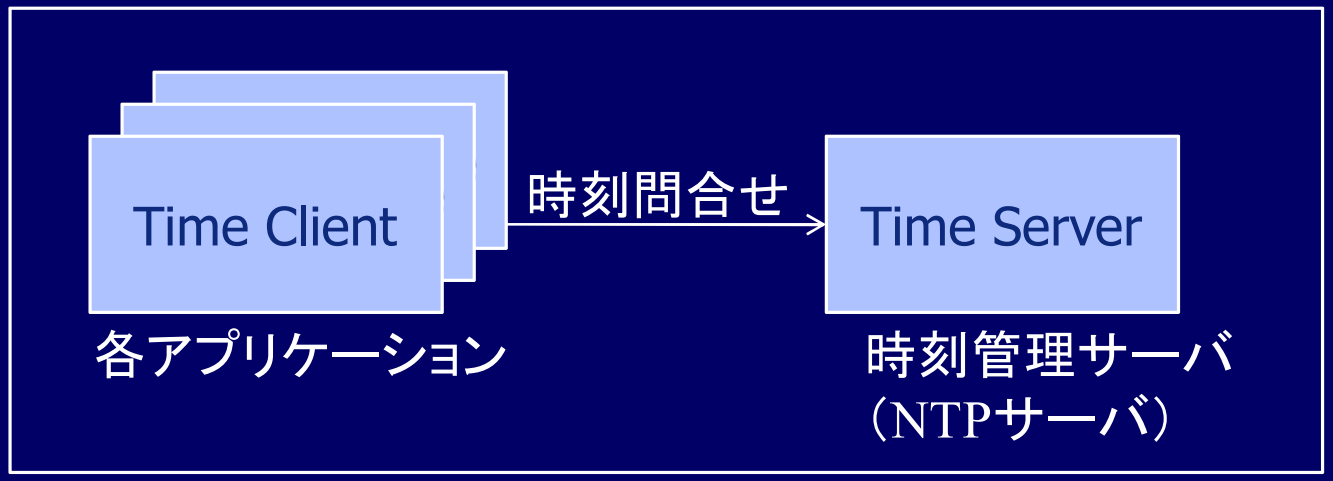
患者来院情報の照会
Patient Demographic and Visit Query

旧バージョンPDQも使用可能

セキュリティ基盤の構築（CT）

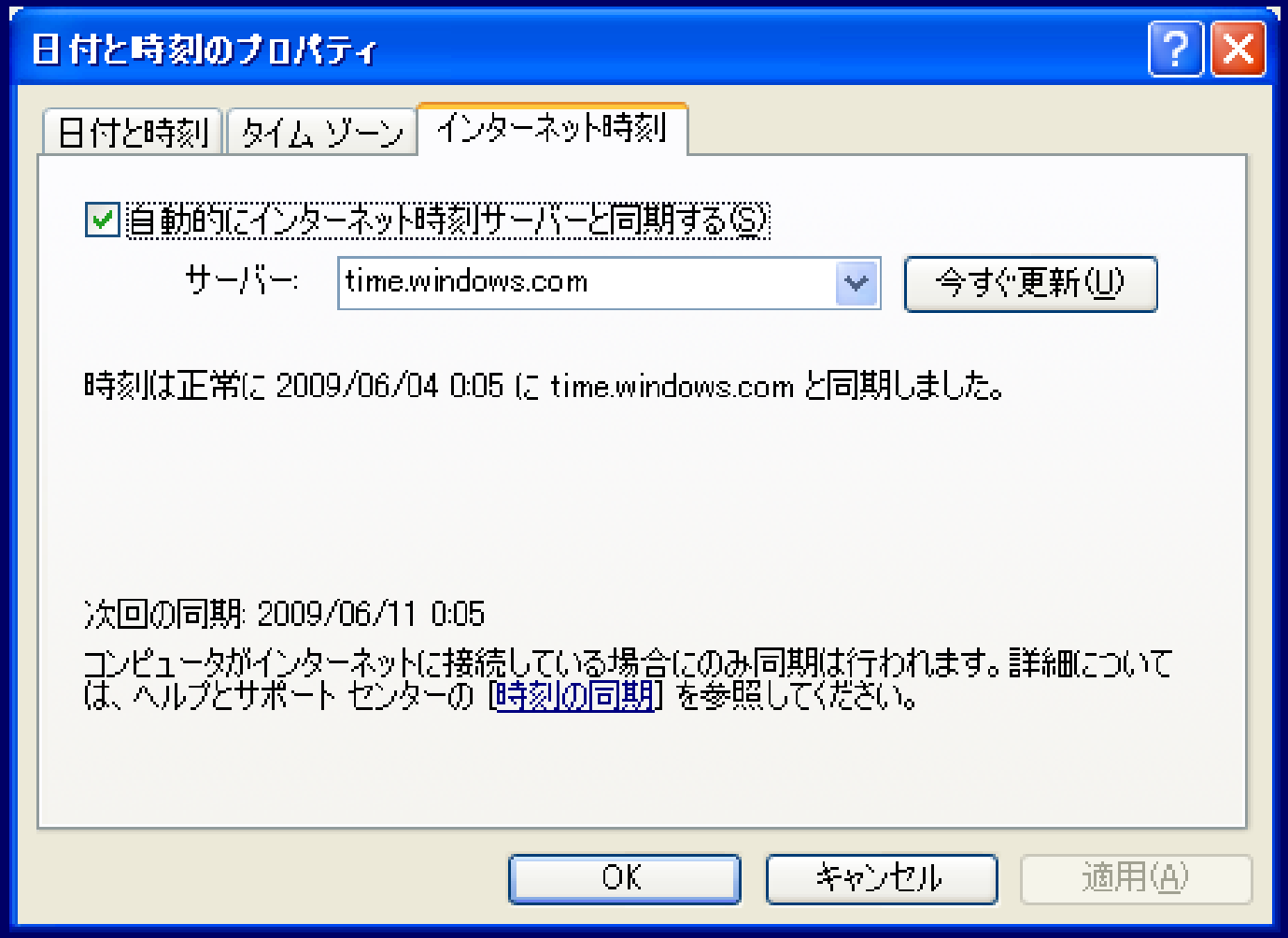
CTの概要

- CT(Consistent Time)は、時刻同期を行うための仕組みを検討。



- 正しいログを取得して監査を実現するためには全てのアプリケーションが同じ時刻を保持しておかなければいけない。

Windows PCで時刻同期



IHEによるセキュリティ確保

- 正しいユーザか
  - ユーザのID → PWP(職員の登録)
  - ユーザ認証 → EUA/XUA(ユーザ認証)
  - アクタ(機器、ノード)認証 → ATNA(監査証跡とノード認証)
  - アクセス制御 → 今後の作業
- 誰がアクセスしたか
  - 監査証跡 → ATNA (監査証跡とノード認証)
- 改ざんはないか
  - データ完全性
    → CT(時刻の整合), ATNA(TLS option), DSG(ディジタル署名)
- 秘匿されているか
  - データ秘匿 → ATNA(TLS option)

複数アプリ間のユーザID,患者IDの共有（EUA/PSA）

EUA/PSAの必要性

- 稼動システム＝マルチベンダ/マルチシステム
- ユーザは、複数のアプリケーションを同時に利用
  - カルテで今参照している患者さんの画像情報をPACSで見たい。
  - この治療を受けた全ての患者さんの経過をまとめてみるには別システムにログインしなくちゃ、、、。

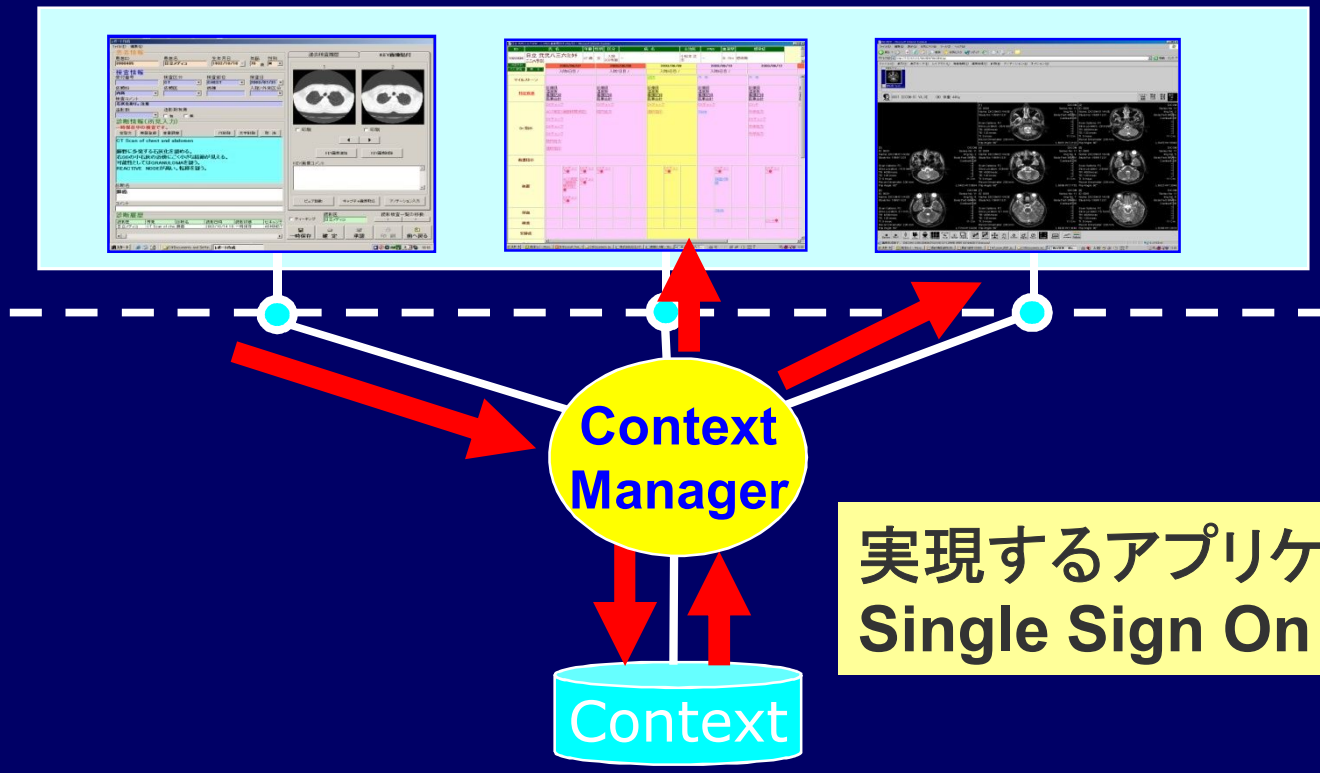
↓

- 様々なシステムの情報を端末上で同期させて表示する方法が開発されている

HL7/CCOW(Clinical Context Object Workgroup)

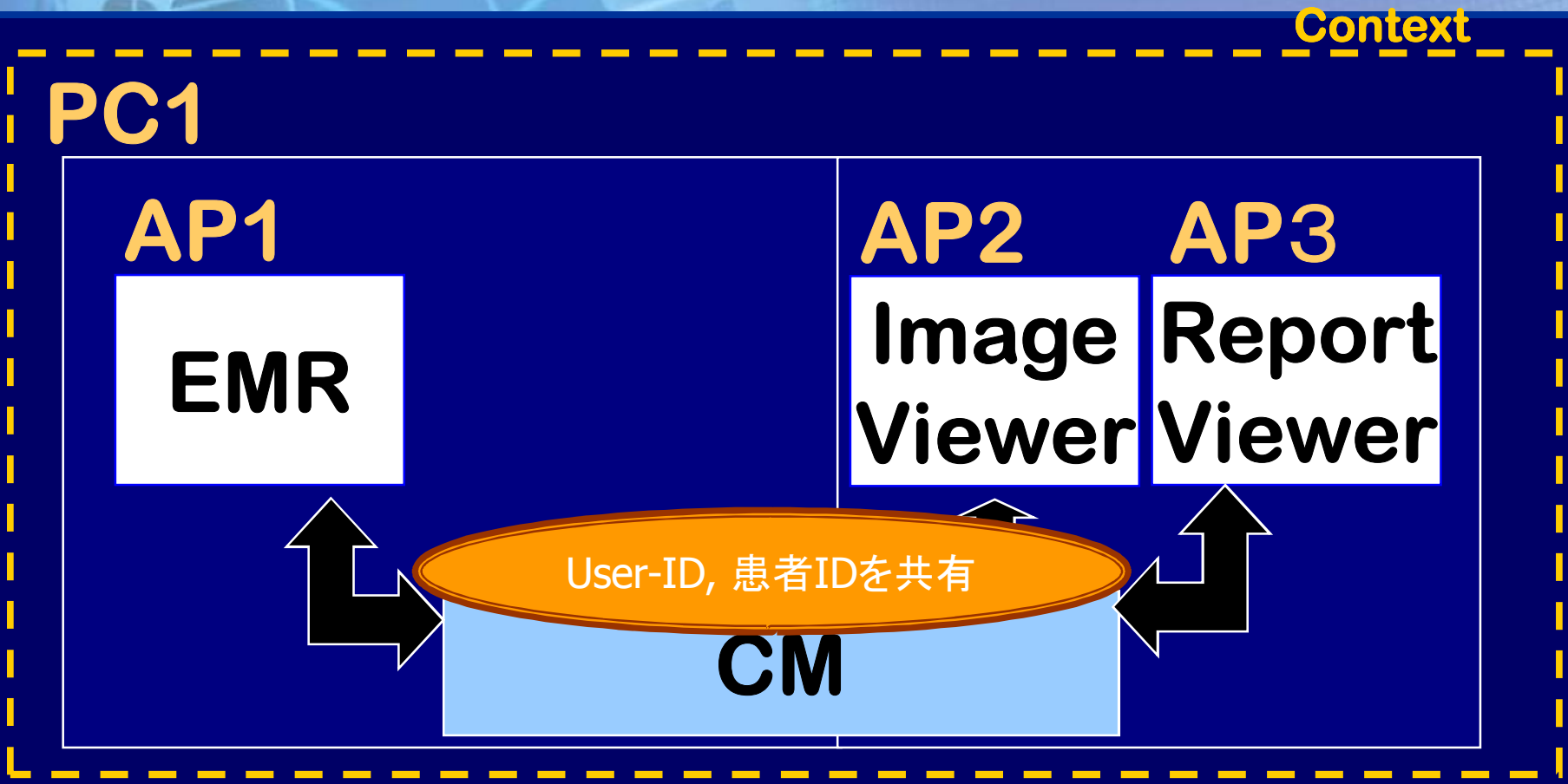
CCOWが定義する仕組み

(1)共有する情報（Context）の定義
(2)Contextの同期を管理するプロセス（Context　Manager）の定義
(3)Context Manager とアプリケーション間のトランザクション仕様



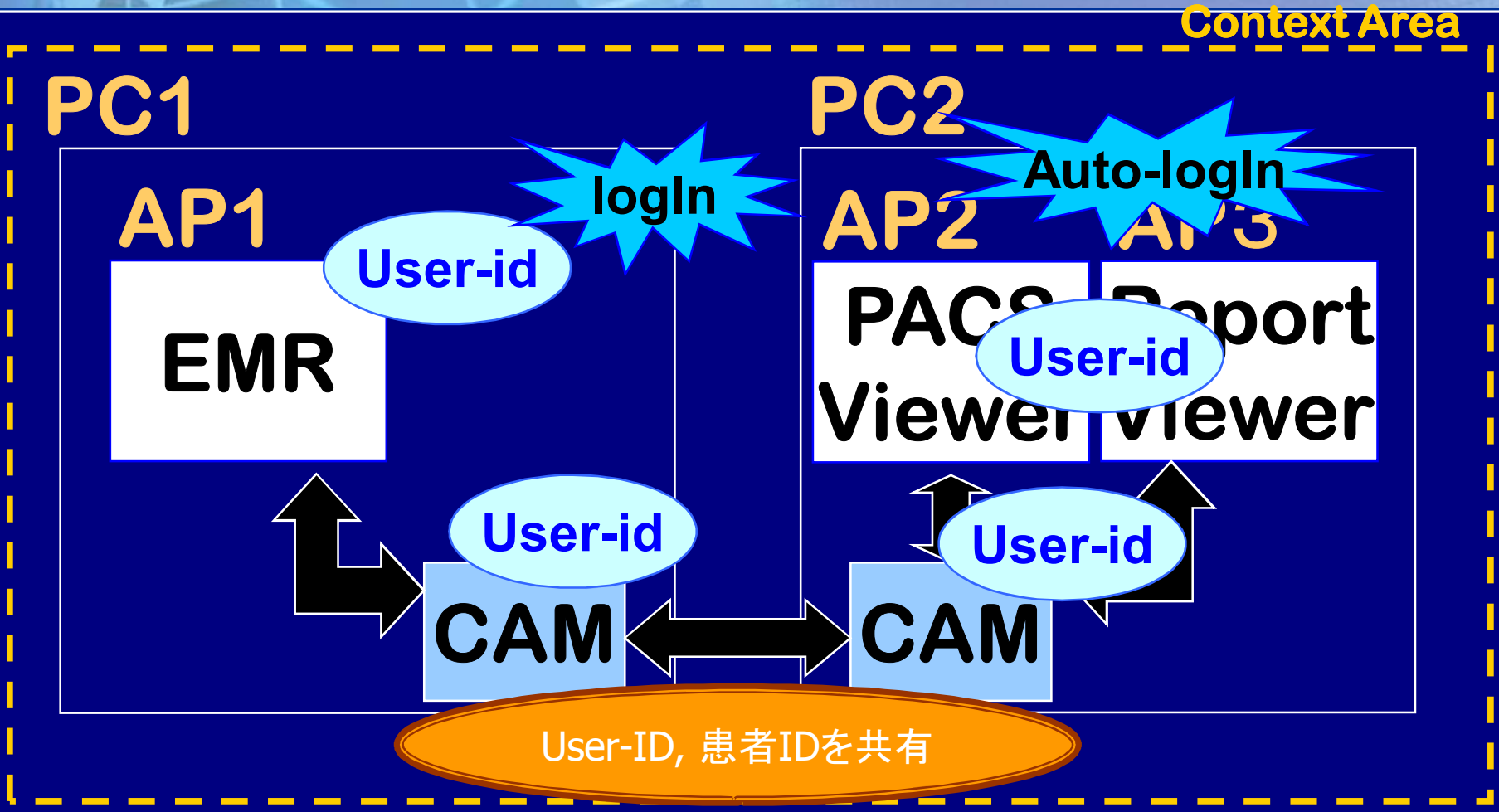
実現するアプリケーションの機能は
Single Sign On と患者同期

IDが連動する仕組み



CM: Context Manager
AP: Application 1,2 …
PC: Personal Computer 1,2 …

IDが連動する仕組み



CAM: Context Area Manager
AP: Application 1,2 …
PC: Personal Computer 1,2 …

EUA（シングルサインオン）

- EMRにユーザAがログイン
- PACSに同一ユーザで参加（ログイン不要）

  ……
- EMRからユーザAがログアウト
- PACSも連動して、ログアウト
- EMRにユーザBがログイン
- PACSに同一ユーザで参加（ログイン不要）

PSA（患者選択連動機能）

- EMRにログインしている
- EMRで患者Aを選択
- PACSにログイン
- PACSは患者Aで連動（患者選択が不要）
- PACSで患者Bに変更
- EMRは、連動して患者Bに切り替わる
- 他のアプリケーションにログイン
- このアプリケーションでも患者が連動する

最新情報はこちらから

- **日本IHE協会**

  http://www.ihe-j.org

- **IHE（北米）**

  http://www.ihe.net

ご清聴ありがとうございました

END