

JPACS/ePHDS 勉強会

「施設間ヘルスケア連携のデータベースのあり方とセキュリティ」 — XDS、HPKI、オンデマンド VPN を含めて —

日本 PACS 研究会/ePHDS 委員会

IT 戦略本部の「重点計画-2006(案)」(2006年6月1日)において、健康・医療・福祉分野の IT による構造改革が掲げられており、施設間情報連携の促進や生涯健康管理の基盤作りが重要なテーマとなっています。日本 PACS 研究会では 2005 年 5 月より ePHDS (enhanced Personal Health Document Sharing system) 委員会を設置し、医療機関間および個人の健康・医療情報の統合を主なテーマとして活動を行っています。

今回は、施設間ヘルスケア連携の課題解決に向けて、医療現場におけるニーズの具体例と、必須となる要素技術の動向について紹介します。

日 時： 2006 年 11 月 14 日 (火) 13:20-17:20 (13:00 受付開始)
場 所： 医科器械会館 セミナーホール
(東京都文京区本郷 3-39-15 Tel 03-3811-6761 URL: <http://www.t-mia.org>)

プログラム

| No. | 時間 | タイトル | (分) | 講師 |
|-----|-------|---|-----|---|
| 1 | 13:20 | (1) HPKI の概要と活用方法 ・保健医療分野における PKI 認証について ・MEDIS-DC における取り組みと利用手順 | 20 | 医療情報システム開発センター 主任研究員 町田 悦郎 |
| 2 | 13:40 | (2) 公立富岡総合病院における実証実験の紹介 ・診療情報の施設間交換への適用モデル ・実証実験の紹介 | 20 | |
| | 14:00 | Q&A | 10 | |
| 3 | 14:10 | 周産期医療情報ネットワークによる医療機関相互連携 ・周産期医療における医療機関相互連携 ・周産期医療情報ネットワークの今後の展開 | 40 | 香川大学医学部附属病院 医療情報部教授 原 量宏 |
| | 14:50 | Q&A | 10 | |
| 4 | 15:00 | 粒子線治療における医療情報連携モデルと課題 ・粒子線治療における情報連携の必要性 ・情報連携モデルとシステム構築の課題 | 30 | 放射線医学総合研究所 重粒子医科学センター病院 医療情報課長 安藤 裕 |
| | 15:30 | Q&A | 10 | |
| 休 憩 | | | | 20 |
| 5 | 16:00 | IHE による施設間医療情報交換の課題と解決策 ・XDS による施設間医療情報連携モデル ・IHE の現状と最新動向/今後の展開 | 30 | 京都医療技術短期大学 教授 細羽 実 |
| | 16:30 | Q&A | 10 | |
| 6 | 16:40 | 個人健康管理システムとオンデマンドVPNによるセキュリティ確保 ・個人健康管理システムとリモートアクセスの課題 ・オンデマンドVPNによるセキュリティ確保 | 30 | 東京工業大学 特任教授 喜多 紘一 |
| | 17:10 | Q&A | 10 | |

お問合せ先：

日本 PACS 研究会事務局

TEL: 03-5684-1636 FAX: 03-5684-1650 E-mail: jpacs@quantum-inc.jp

* 写真・ビデオ撮影は事務局・講演者の許諾がある場合を除いて禁止致します。

JPACS,ePHDS勉強会
HPKIの概要と活用方法
公立富岡総合病院における実証実験



(財)医療情報システム開発センター
研究開発部
町田 悦郎

2006/11/14

(c) MEDIS-DC All Rights Reserved

1

概要



- 1. HPKIの概要と活用方法
 - (1) 保健医療福祉分野におけるPKI
 - (2) MEDIS HPKI認証局サービス
- 2. 公立富岡総合病院における実証実験
 - (1) 電子診療情報提供書
 - (2) 実証実験

2006/11/14

(c) MEDIS-DC All Rights Reserved

2

概要

- 1. HPKIの概要と活用方法
 - (1) 保健医療福祉分野におけるPKI
 - (2) MEDIS HPKI認証局サービス
- 2. 公立富岡総合病院における実証実験
 - (1) 電子診療情報提供書
 - (2) 実証実験

ISO17090

- 保険医療分野におけるPKIの利用法を規定
- Health informatics
 - Public key infrastructure --
 - Part 1: Framework and overview
 - Part 2: Certificate profile
 - Part 3: Policy management of certification authority
- まもなくISとして発行(現状はTS,2002年発行)
- Part2でhc Role (healthcare role)を規定
 - 医療従事者の役割を現すための属性
 - Subject directory attributeに設定



保健医療福祉分野PKI認証局証明書ポリシー

- ISO17090に準拠し、厚生労働省が作成
- 署名目的のみを規定。認証は範囲外
- 厳格な本人確認を規定
- hcRoleに医師などの25の国家資格と病院長などの4つの管理者資格を入れられる。
- 下記URLから参照可能
<http://www.medical-it-link.jp/lib/index.shtml#sk>
- 以下「共通ポリシー」と呼ぶ

2006/11/14

(c) MEDIS-DC All Rights Reserved

5



MEDIS-HPKI認証局

- 共通ポリシーに完全準拠
- MEDIS-HPKI認証局は署名用証明書に加え認証用証明書も発行
- 下位認証局証明書も発行予定

2006/11/14

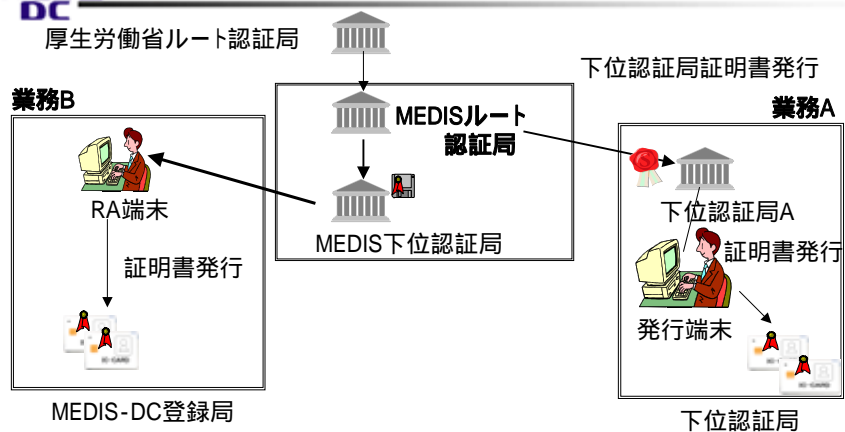
(c) MEDIS-DC All Rights Reserved

6

署名と認証

- どちらも私有鍵で署名し、公開鍵で検証
差異は？
- 署名:人が確認して、押印
実世界の印鑑による押印と同じ
- 認証:機器が相手を確認
SSLのサーバ認証など

MEDIS-HPKI認証局の概要



厚生労働省ルート認証局

- 18年度に厚生労働省HPKIルート認証局を構築
- 18年度は、実証実験として、日本医師会とMEDISの認証局のみの共通ポリシへの準拠性確認を行い、厚生労働省ホームページで公開
- 19年度以降は他の下位認証局の準拠性確認を行う予定

MEDIS-HPKI認証局(業務A)

下位認証局の確認作業

- 下位認証局のCPSと共通ポリシとの齟齬を確認
- 運用環境、運用管理について、現地確認作業を実施
- 確認作業を毎年継続

署名用と認証用の
認証局で認証基準
に差異をつけない。

MEDIS-HPKI認証局(業務B)

署名用証明書の発行

- 共通ポリシー記載の直接申請、オンライン申請は行わない。郵送申請のみとする。
- 他は、共通ポリシーに完全準拠
- 証明書は、ICカードに書き込み本人限定郵便で郵送

MEDIS-HPKI認証局(業務B)

認証用証明書の発行

- クラス2相当の本人認証
- 一括発行を行う。
- 証明書は、ICカードまたはPKCS#12形式で発行
- 他は、共通ポリシーに原則準拠
- 1枚からでも発行

電子証明書の取得法

- 共通ポリシーで詳細を規定
- 以下の書類の提出が必要

電子証明書申請書 (実印押印)

医師免許証のコピー (空いたところに実印押印)

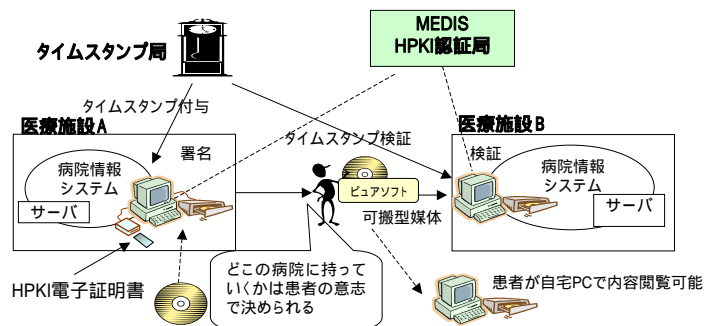
運転免許証のコピー (空いたところに実印押印)

住民票の写し

印鑑登録書

HPKI電子証明書の利用例

電子診療情報提供書



概要

- 1. HPKIの概要と活用方法
 - (1) 保健医療福祉分野におけるPKI
 - (2) MEDIS HPKI認証局サービス
- 2. 公立富岡総合病院における実証実験
 - (1) 電子診療情報提供書
 - (2) 実証実験

電子診療情報提供書

- 患者基本情報、現病歴などの紙の紹介状と同じ情報に加えて処方・検査・画像データを付加
- CD-Rに閲覧用ビューと共に書き込む
- 診療情報提供書本文: MERIT9-V2
処方・検査: HL7 V2.5 画像: DICOM V3
- 診療情報提供書本文に処方・検査データのハッシュ値、ハッシュアルゴリズム、URIを要素とした local_markupタグを追加
本文から処方・検査データへリンクをたどれる。

電子診療情報提供書ビューア

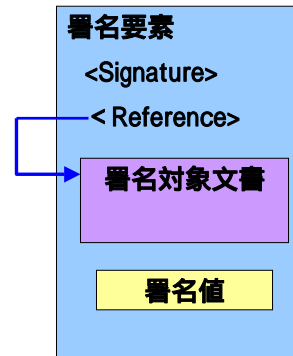
- 診療情報提供書 (XML) とXMLに整形した処方・検査をスタイルシートと共にInternet Explorer V6で表示
 - 表示フォーマット変更容易
 - 広く利用されているIEのGUI利用のため操作容易
- DICOMは専用アプリケーション使用
- ビュア起動時に電子署名検証実行
ユーザ意識しなくとも安全性確保

電子署名とタイムスタンプ

- 電子診療情報提供書に電子署名を付与し、「真正性」(非改ざん性)、保存性(法的条件)を担保
- 医師資格を確認できるMEDIS HPKI電子証明書を利用
- 電子証明書の有効期間が2年と短いため、長期の署名有効性確認のためタイムスタンプ(有効期間10年)を付加

署名フォーマット

- 本文がXMLのため、親和性のよいXML電子署名を採用
- Enveloping署名を採用
最初の医師が署名したデータに他の医師が追記した部分のみにも署名ができる。



暗号化

- 電子診療情報提供書CD-Rには多くの診療データが入り、患者が持ち運ぶ
紛失や盗難の恐れ



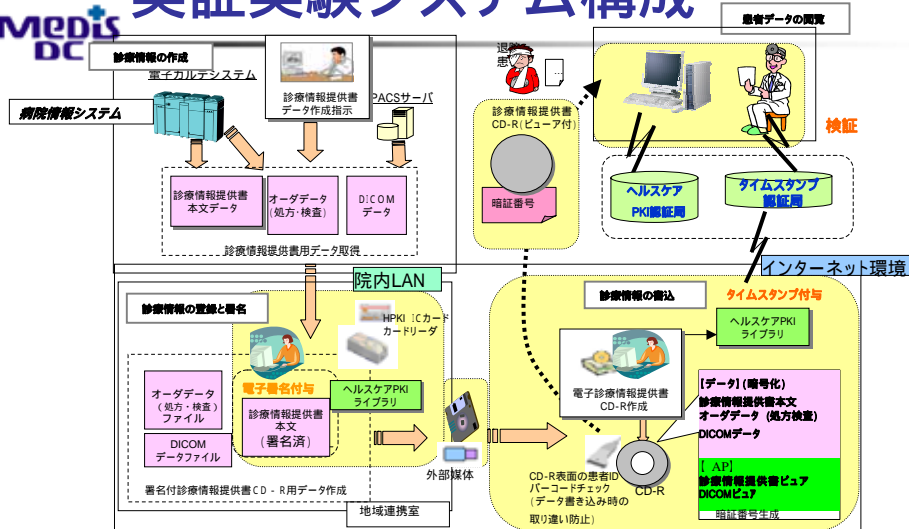
- 暗号アルゴリズムにはAES-128を採用
ランダムな16文字もの鍵長
記憶困難
4～16文字の鍵長を設定できる
パディングアルゴリズム

実証実験

- 2006年1～2月に公立富岡総合病院(359床 群馬県富岡市)で実証実験
- 26名の患者(平均59.5歳)の逆紹介に利用
- 19医療機関へ紹介



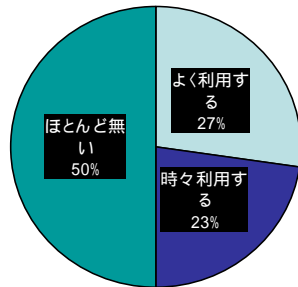
実証実験システム構成



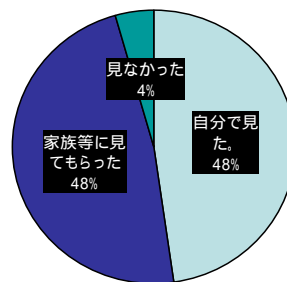
運用評価(患者)



患者のパソコン利用頻度・経験



診療情報CD-Rの内容の確認



- 回答数23名、平均年齢59.5才
- 重複検査回避、治療内容の理解促進など高評価

2006/11/14

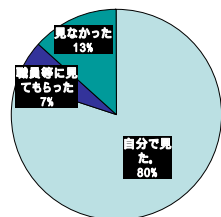
(c) MEDIS-DC All Rights Reserved

23

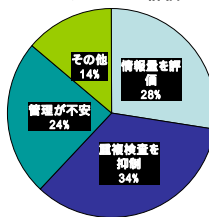
運用評価(紹介先医療機関)



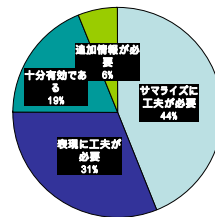
診療情報CD-Rの内容の確認



診療情報提供書への電子媒体利用についての評価



電子診療情報提供書への改善要望



- 紙の紹介状に比べ情報量が多く、診療経過が良く理解でき、重複検査も抑制
- 多量のDICOMデータにおけるキー画像の指定や所見登録などデータ要約簡素化への要望
- 暗証番号やCD-R管理への不安と個人情報漏洩への懸念

2006/11/14

(c) MEDIS-DC All Rights Reserved

24

課題(運用体制)

- CD-R作成・発行に要する時間と要員の確保
 - ・診療情報の収集
 - ・暗証番号発行、CD-Rラベル作成、バーコードチェック、CD-R書込み
 - 院内組織の新たな連携
 - ・DICOM画像の選択連絡、書込みの確認等院内組織間連携の円滑化
 - 患者対応
 - ・CD-R作成時間(患者待ち時間)の有効活用
 - ・患者へのCD-R取扱説明およびビューア操作に関するフォローアップ
 - 提供先医療機関対応
 - ・電子診療情報提供書への理解協力とりつけ
 - ・ビューア操作に関するフォローアップ
- 慣れや業務の見直しで解消可能なものと新たな追加業務となるものの分析整理が必要**

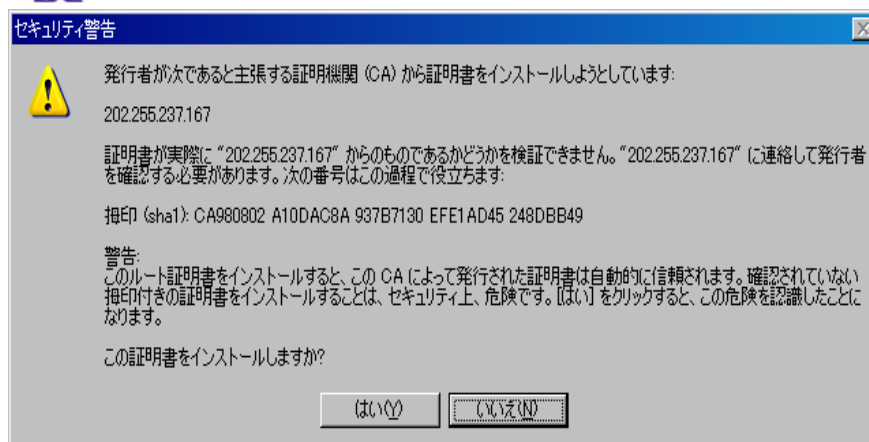
課題(タイムスタンプ)

- 院内電子カルテネットワークはインターネットに接続されていない。
タイムスタンプ付与不可能
- セキュリティポリシーの変更は、十分なリスクアセスメントを行い慎重に行う必要
- 電子カルテネットワークからインターネット環境にオフラインでデータ移動
- 人手介在 非効率・間違いの可能性

課題(ルート証明書)

- 一般にPKIでは、信頼点であるルート証明書は利用者が意識してインストール
- 今回もルート証明書がインストールされていることを前提に開発
- 実際にインストールはかなり困難

セキュリティ警告画面



対策

- データ移行時のとりちがえ防止策
- 院内電子カルテネットワーク上で電子署名付与時に失効確認を行うProxy Server
- CD-Rにルート証明書も同時に焼き込む。
- 署名・暗号ツールはDLLで提供したが、より簡単に利用できるようにアプリケーションとしてまとめる。

おわりに

ご清聴ありがとうございました。
ご質問・お問い合わせは、
machida@medis.or.jp
まで！