資料２

医療分野における公開鍵基盤の実証試験について

2003年10月6日

喜多　紘一
（財）医療情報システム開発センター
審議役・プライバシーマーク付与認定審査室長
第4回医療情報ネットワーク基盤検討会

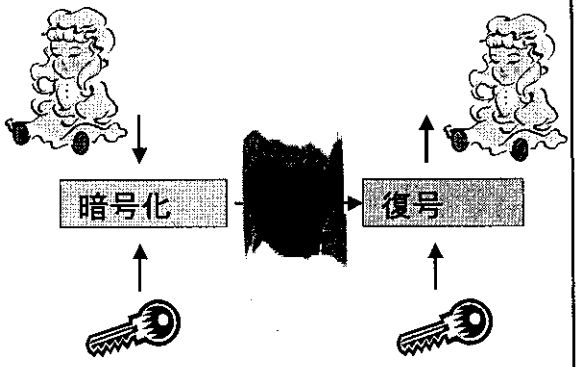
公開鍵基盤とは

- 私有鍵（秘密鍵）は本人が所有し、対応する鍵（公開鍵）が本人の所有する鍵に対応するものであることを第三者が証明し（公開鍵証明書を発行）、それを当事者どうしが検証することによりセキュリティを確保するための基盤である。
- 従って登場人物として3者が登場し、3者のポリシーの確認と検証プロトコルにより成り立つ基盤である。

類似

- 印鑑証明
  - 一度に一回
  - 公開鍵証明書は有効期限の間コピー可
- クレジットカード
  - 支払能力を証明
  - カードは支払可の間は何度でも

暗号技術



- **秘密共有鍵方式（対称鍵方式）**
- **公開鍵方式（非対称鍵方式）**
  - **公開鍵・秘密鍵(私有鍵)**
  - **公開鍵証明書(電子証明書)・公開鍵認証局(CA局)**

セキュリティの5つの観点

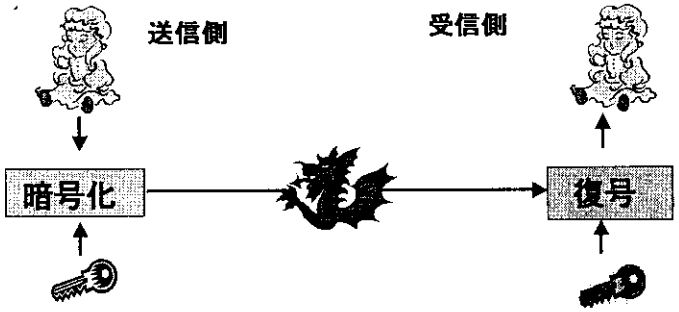
- 物理的安全
- 電子保存(電子媒体による原本性保証)
- 通信のセキュリティ
- 事後否認(電子署名)
- 個人情報の保護

鍵の利用目的
(サイバースペース)

- 平文・共通鍵の秘匿
- 相手認証
- 改ざん検知
- 意思確認(電子印鑑)

秘匿化（一般に暗号化と言う）

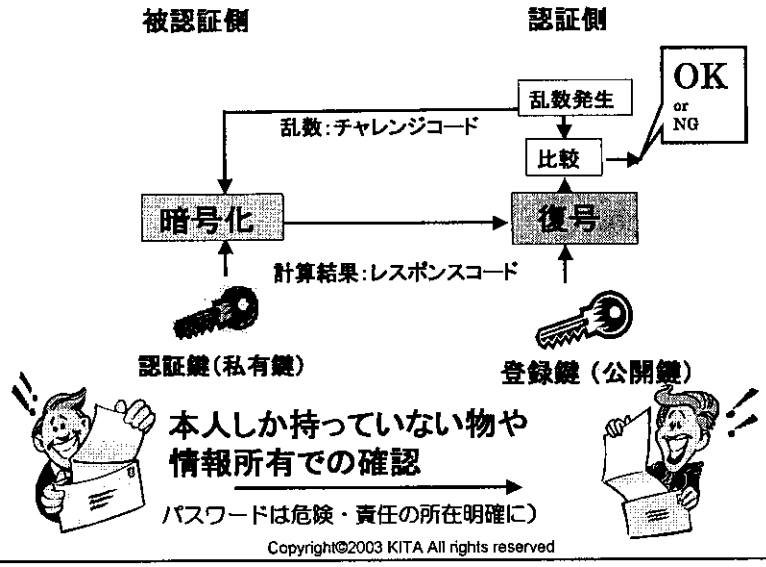
- 非対称鍵の場合



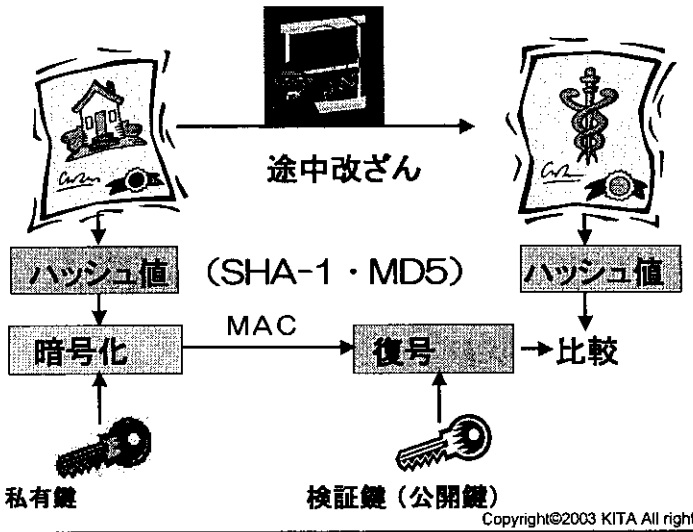
公開鍵（関係者また不特定に登録等により周知させる）

私有鍵（第三者に絶対開示しない）

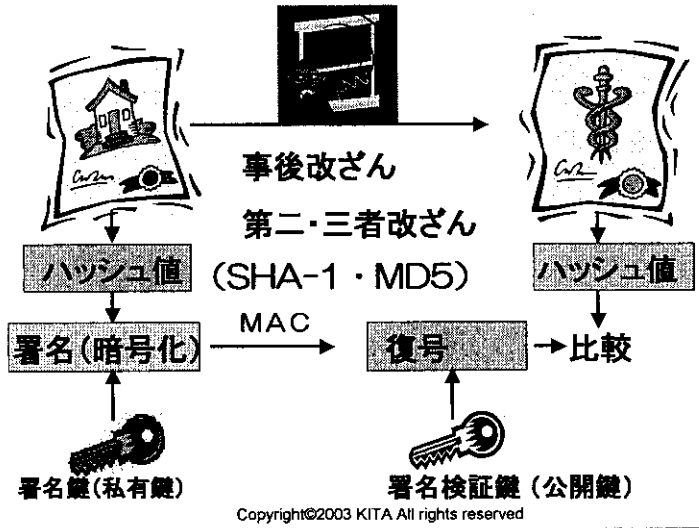
相手認証



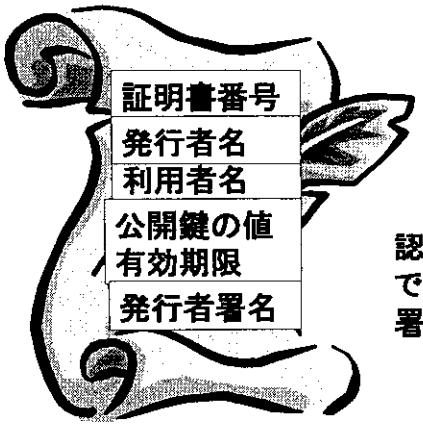
改ざん検知



意思確認(事後否認・電子印鑑)



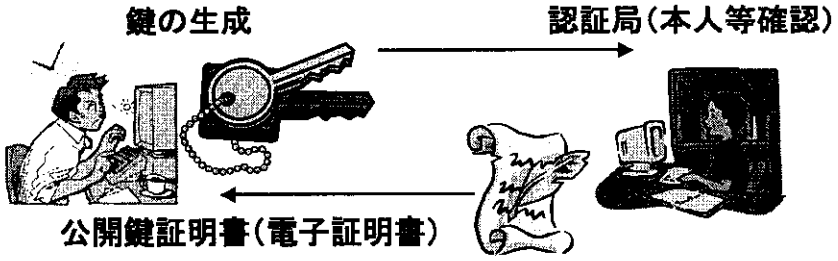
公開鍵証明書(電子証明書)



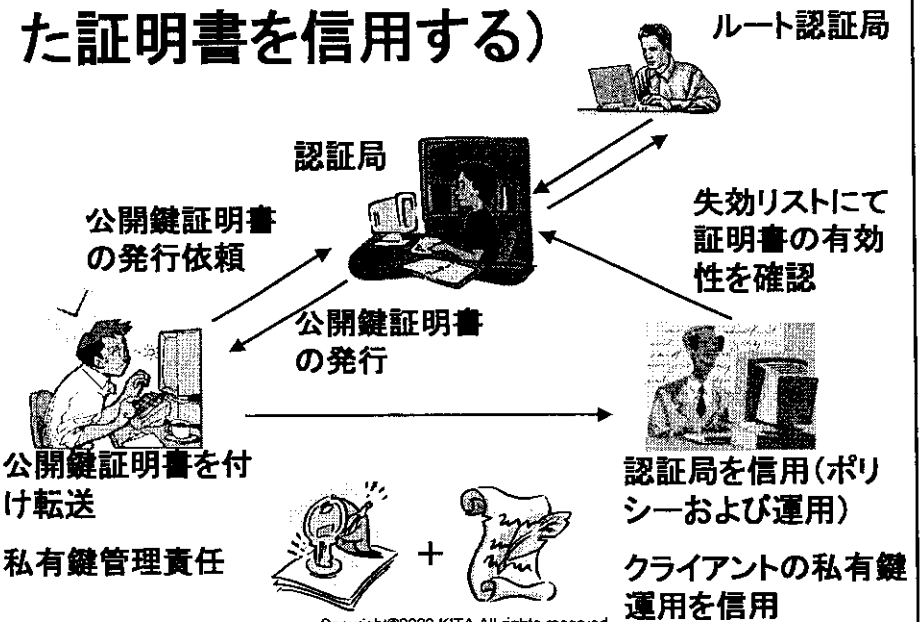
認証局(発行者)の秘密鍵で証明内容のハッシュ値に署名

公開鍵証明書(電子証明書)の入手

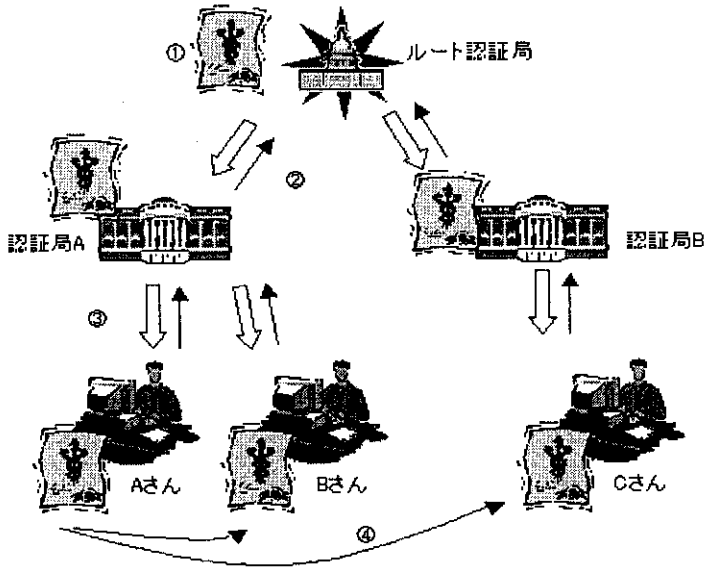
- 秘密鍵と公開鍵を生成
- 公開鍵をCA局(認証局)へ送り、公開鍵証明書(電子証明書)を入手



PKIの前提条件(第三者の発行した証明書を信用する)



認証局の階層化 ポリシーのマッピングが重要



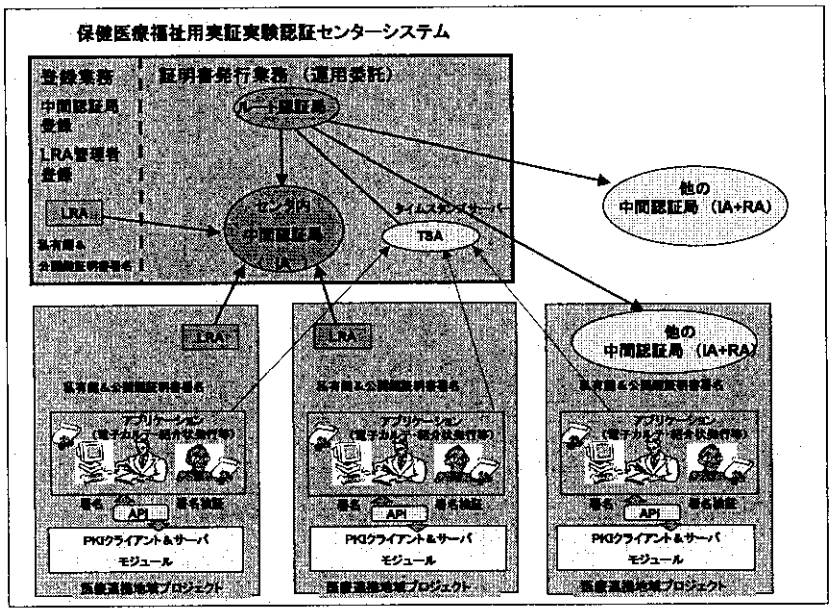
IPA 「電子メールのセキュリティ」より引用

保健医療福祉情報セキュリティ推進事業

ヘルスケア情報の共有と活用のために
電子署名／データベースへの安全なアクセスを
PKIにより実現する為のHPKIの実証実験を行う。

- ヘルスケアPKIドメインの実証
- 公開鍵証明書の発行
- タイムスタンプの実装
- 医療施設での公開鍵証明書利用（登録局と発行局の分離）
- 異なった発行局で発行された公開鍵証明書間での互換性テスト

保健医療福祉情報セキュリティ推進事業概念図



HPKIは何を目的としているか

MEDIS DC

- サイバースペースでヘルスケアサービスを行うために、対面と本人確認および署名、記名捺印と同等な機能をもたせること。
  - MD-HPKI-01-YYYYYY で区別
- 以下と同等な資格のサイバー区間での確認
  - 三師免許等(公的免許)・・・hcRoleで表示
  - 医療施設開設
  - 公的認証サービス・電子署名法における特定認証業務相当
  (パスポート、運転免許証・銀行の口座開設)
- 同等な全国で共通に使用できる証明書を対象
  - 一つの医療機関にのみ通用する証明書ではない。
  - 一箇所が脆弱になるとシステム全体の信頼性がなくなる。

MEDIS発行局の特徴

- Issuer CN
  - 署名用 CN=MD-HPKI-01-nonRepudiation
  - 認証用 CN=MD-HPKI-01-Authentication-and-keyEncipherment
- 本人確認はCPに従いレベル3

本人確認のレベル

- （レベル1）（rudimentary assurance）
  - 申請者から提出された電子メールのアドレスが当該申請者に対して正しく送信できるものであることだけを確認する。本人の同一性確認は行わない。
- （レベル2）（basic assurance）
  - オンラインにより申請者から提出された申請書の内容について、住民基本台帳等の記載内容と照合する。
- （レベル3）（medium assurance）
  - 認証機関の窓口において申請者から提出された申請書の内容を住民基本台帳等と照合するとともに、官公署の発行した身分証明書等の本人確認を行うための書類の提示を求める。
- （レベル4）（high assurance）
  - 申請者から提出された申請書の内容を住民基本台帳等と照合した上で、申請者が申請を行った事実を認証機関が郵送その他の方法により当該申請者に対して文書で照会し、その回答書を認証機関に持参してもらう。

【新規発行時での所有者の本人確認方法 】　～個人の認証 ～

（1）申請者が実在すること（実在性）の確認

申請書に記載された申請者の「氏名、出生の年月日、男女の別、住所」と住民票に記録されている情報を照合することにより、申請者が実在すること（住民基本台帳に記録されていること）を確認する。

（2）申請者が本人であること（本人性）の確認

次の方法のいずれかのものにより、申請者と称する者が実在性の確認された申請者本人であること（住民基本台帳に記録されている者であること）を確認する。

①官公署の発行した資格証明書、運転免許証、旅券その他本人であることを証明できる書面であって、本人の写真を貼付してあるものの提示を求める方法

②本人であることを証明できる①以外の官公庁の発行した書面（各種健康保険の被保険者証、各種年金の年金手帳等）の２種類以上の提示を求める。

【国家資格保有の確認方法 】　～資格の認証 ～

医療専門家の国家資格免許を認証するためには，関係官庁によって発行された職業上の国家資格免許状や身分証明書またはその写しをRAに提示するものとする。

上記の手続で脆弱性を生じない範囲およびその主旨を変更しない範囲で「商業登記に基礎を置く電子認証制度」および「公的個人認証サービス制度」を利用することに置き換えても良い。また、公開されたアクセス可能な公的資格台帳がある場合はこれを利用することを妨げない。

【新規発行時での組織の確認方法 】　～組織の認証 ～

（1）組織もしくは団体が実在していること、および、その組織が保健医療福祉機関であること（実在性および有資格性）の識別

法人組織の場合：登記簿謄本、法人印鑑証明書等により実在確認を行う。また、「保健医療福祉機関であることを証明する書類（開業届けおよび受理等の写し）により行う。

個人事業者の場合：個人事業者であることを証明する書類（開業届け、受理、保険事業者の「指定書」等の写し）等により確認を行う。申請書に記載された申請者の「氏名、出生の年月日、男女の別、住所」と住民票に記録されている情報を照合することにより、申請者が実在すること（住民基本台帳に記録されていること）を確認する。

（2）組織もしくは団体の名前に於いて正当に代表者として認可されている者が、証明書発行の申請に署名（自署）、押印を行っていることの確認

法人組織の場合：法人印鑑証明書等により確認を行う

個人事業者の場合：代表者個人の印鑑証明書等により確認を行う

証明書の申請書に記載された情報に虚偽が無いこと。

（3）申請者の本人確認

個人の認証と同様な方法による。

上記の手続で脆弱性を生じない範囲およびその主旨を変更しない範囲で「商業登記に基礎を置く電子認証制度」および「公的個人認証サービス制度」を利用することに置き換えても良い。また、公開されたアクセス可能な公的資格台帳がある場合はこれを利用することを妨げない。

【エンドエンティティ (End Entity) 】

エンドエンティティは、証明書所有者と署名検証者から構成される。

証明書所有者とは、証明書発行申請を行い、自ら鍵を生成し、CAにより証明書を発行される個人あるいは組織をさす。

証明書所有者の範囲は次のとおりとする。

- 医療従事者等のサービス供給者
- 医療機関、および、保健医療福祉サービス供給組織
- 患者／保健医療福祉サービス利用者

【鍵の使用目的】

認証鍵は身元確認、電子署名鍵は否認防止目的のためだけに使用されるものとする。データの暗号化目的には別個の鍵ペアがあるものとするが本CPでは扱わない。認証用鍵を否認防止目的のための署名に使用、あるいは否認防止用鍵を認証に使用しないように運用管理すべきである。あやまって共用した場合は認証プロトコルで用いられるデジタル署名機能によっては、悪意により、否認防止対象文書のハッシュ値に電子署名を行わせるかもしれない脆弱性を持つ場合があることを留意すべきである。

従って、保健・医療・福祉分野で、Subjectが人や組織の場合で法的に有効な署名に用いる場合は証明書プロファイルのkeyUsageのビットの内、nonRepudation 以外のビットをオンにしないこととする。また認証に用いる場合はdigitalSignatureとkeyEnciphermentの以外のビットをオンにしないこととする。公開鍵証明書申請時に秘密鍵をどちらの鍵として持ちいるか使用目的を明確にする必要がある。

【鍵のサイズ】

CA証明書の鍵の最小サイズは，RSAアルゴリズムの場合，2048ビットとする 。CA以外の証明書の鍵の最小サイズは，RSAアルゴリズムまたは技術的に同等のアルゴリズムの場合，1024ビットとする 。

【私有鍵と公開鍵の有効期間】

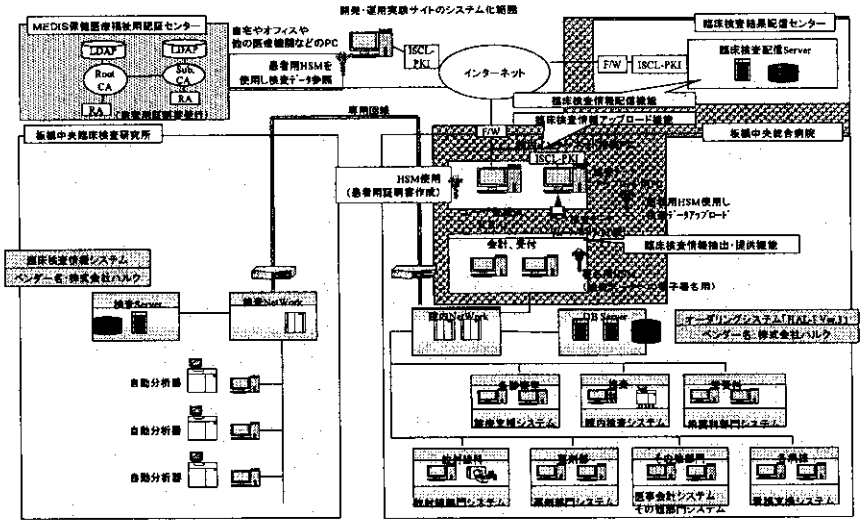
CA以外の公開鍵と私有鍵の使用は，3年を超えないものとし，その後に新しい鍵ペアが発行されるものとする。属性証明書は業務上の必要性により、より短い期間でも良い。CAの公開鍵と私有鍵の使用は，10年を超えないものとし，その後に新しい鍵ペアが発行されるものとする 。

ポリシードキュメントの作成

- HPKIガイドライン
- 証明書ポリシー(CP)
- 認証実施規定(CPS)
- LRA運用規程

板橋中央病院システム概要

署名とセキュア通信



島根県立中央病院開発システム概要

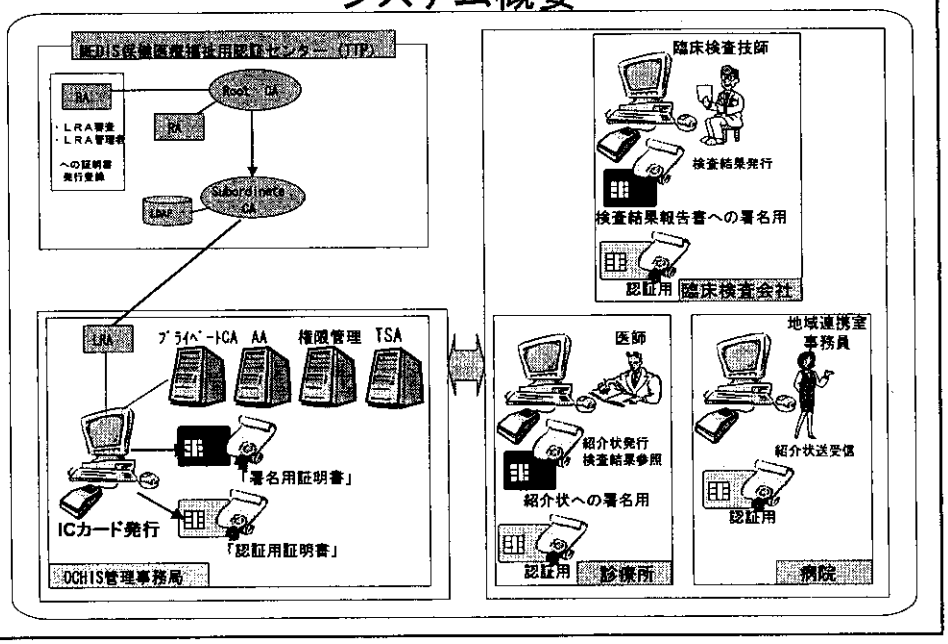
公開鍵基盤を用いて、本事業での保健医療福祉情報セキュリティガイドラインに沿って、以下について署名およびタイムスタンプを利用するものである。

(1)地域医療情報ネットワーク管理システムのクライアントからの紹介状送信

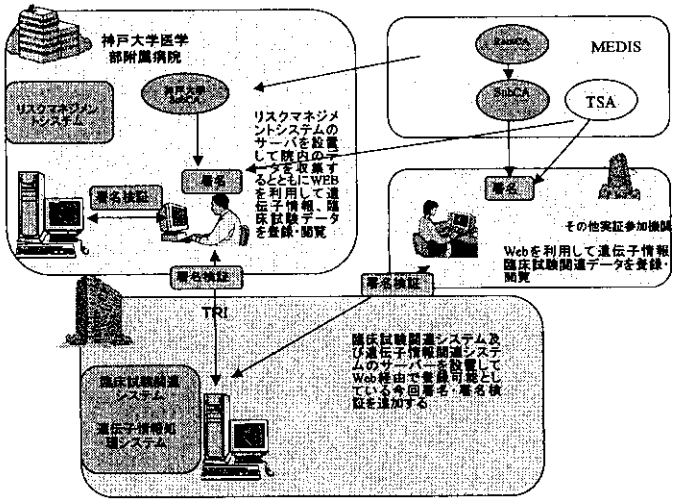
(2)診療所用インターネット対応電子カルテシステムからの紹介状送信

(3)隠岐島遠隔医療支援システムにおける読影レポートの送信・参照

大阪ヘルスケアネットワーク普及推進機構 システム概要



「神戸市における公開鍵基盤の実証」システム概要



HPKIの位置付け

法律・施行規則の整備
何の情報をどう保護するか
セキュリティ基準を明示

⇩

医療情報セキュリティポリシーガイドライン
医療機関での情報セキュリティ対策の全体整合性を検討し対策基準を明示

⇩

医療用公開鍵基盤ガイドライン
保健医療福祉分野に於ける全国規模でのPKIの互換性確保のための標準ガイドライン

⇩

ヘルスケアPKI認証局証明書ポリシ
保健医療福祉分野に於ける電子証明書の発行基準