Challenge PKIプロジェクトと PKI技術最新事情

セコム株式会社 IS研究所/
JNSA PKI相互運用技術WGリーダー
松本　泰

2005 年 10月 28日

Challenge PKIプロジェクトと PKI技術最新事情

- PKI相互運用技術WGでは、年3回行なわれるIETFの参加、IPA等に公募に応募し採択されたプロジェクト（Challenge PKIプロジェクト）の活動、これらの成果物の発表などを行ってきました。
- ここ数年は、PKIの相互運用技術を中心に、PKIの展開、ベストプラクティスを示すと言ったこと念頭に活動を行っており、本セミナーもこれらの活動の一環になります。
- ここでは、 Challenge PKIプロジェクトのご紹介と、最近のPKIに関連するトピックと今後の課題について説明します。

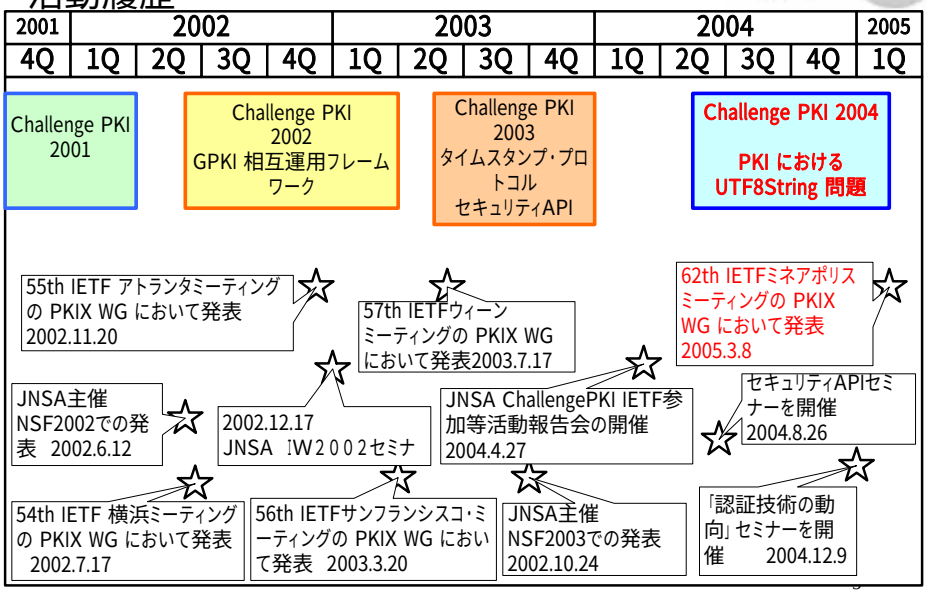
Challenge PKIプロジェクトとPKI技術最新事情

- Challenge PKIプロジェクトの活動
- PKI技術最新事情と今後の課題
  - SHA-1問題
  - 電子署名法の改正の検討??
  - 医療PKI

Challenge PKIプロジェクトの活動
プロジェクトの目標と課題

- プロジェクトの今後の目標
  - 実際に幅広く展開可能なセキュリティインフラの構築(= 幅広く相互運用可能なPKIの展開)
- 標準化の課題 (標準・実装から展開)
  - アイディアから仕様へ -> 多くの研究者が行っている
  - 仕様から標準、標準から実装 -> 学術系＆ベンダーなど
  - 標準・実装から展開 (相互運用) -> 誰が担うか
    - 標準と呼ばれる文書は山のようにある。しかし相互運用可能なものは極わずか…. これを解決して行かなければならない。
    - -> ベストプラクティスが重要。。。。ここに注力する。
- セキュリティフレームワークやミドルウェア重要性
  - 実際のアプリケーションにおいて、セキュリティ・ミドルウェアが、実行時のネットワーク上の信頼と複雑な相互運用の問題を吸収する

Challenge PKIプロジェクトの活動
活動履歴

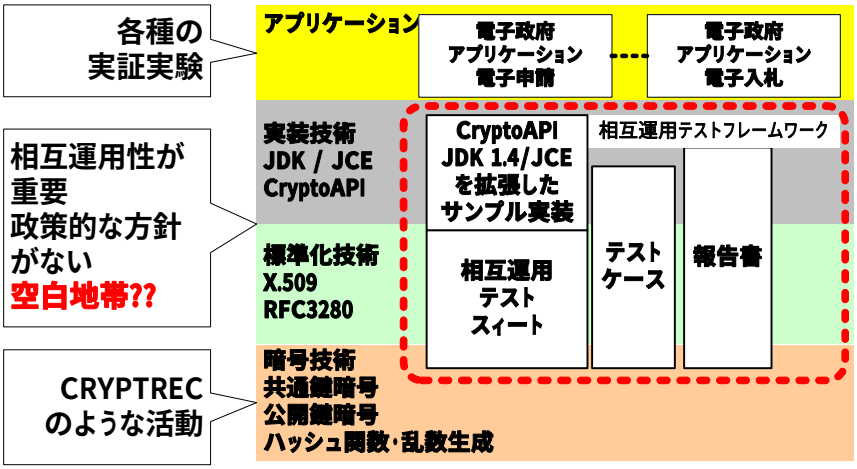


JNSA Challenge PKIプロジェクト
Challenge PKI 2001 - 参加団体
(と今日のセミナーの講演者)

実験参加企業(団体)	製品	
セコムトラストネット/エントラストジャパン	Entrust PKI 6.0	島岡、松本
SSH	SSH Certifier 2.0	
NECソフト	NEC Carassuit電子政府版Ver1.1	
RSAセキュリティ	Keon Cerficate Authority 6.0	
富士ゼロックス/富士ゼロックス情報システム	未発表製品	稲田さん
マイクロソフト プロダクトディベロップメント リミテッド	Microsoft Windows Server	及川さん
日本ベリサイン	(非公開)	
名古屋工業大学	Easy Cert(開発 奥野 琢人氏)	奥野さん
WIDEプロジェクト	ICAP v2.51(ICAT)	木村さん

6

Challenge PKIプロジェクトの活動
プロジェクトの目標と課題(2) – Challenge PKI 2002

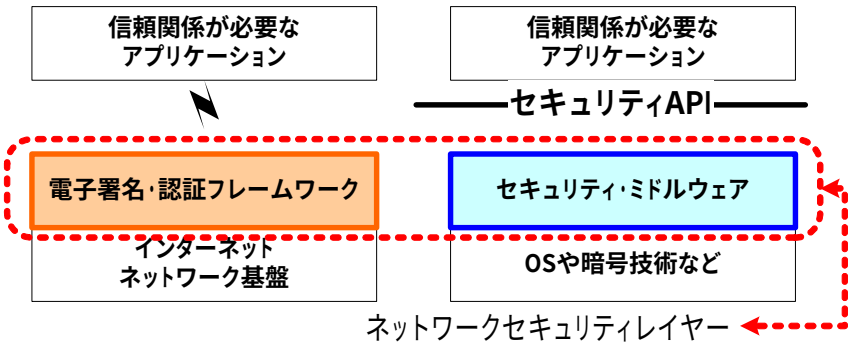


複雑さを隠蔽するためどんどん階層化されていく。。

このことが、問題の本質を分かり辛くしている！！

7

Challenge PKIプロジェクトの活動
セキュリティフレームワークやミドルウェア重要性 Challenge PKI 2003



- 何処でも、何時でも、誰にでもつながるユビキタスネットワークにおいて信頼の拠りどころが求められる。。。。
- ネットワーク上の信頼を実現するセキュリティ・レイヤーの必然性
  - これらは、古典的なOSI参照モデルなどでは説明がつかない。。

8

Challenge PKIプロジェクトの活動

セコムIS研究所 Intelligent Systems Laboratory

セキュリティフレームワークやミドルウェア重要性 Challenge PKI 2003

標準化、相互運用の課題

非常に複雑なセキュリティプロトコルの要求

セキュリティに対応し切れていない標準化＆標準化組織

テスト環境、テストケース、相互運用テストが非常に重要だが、整備ができていない

信頼関係が必要なアプリケーション

セキュリティAPI

セキュリティ・ミドルウェア

OS

実装上の課題

暗号技術等、基礎技術が、セキュリティ・フレームワーク＆ミドルウェアに組み込まれていかない（日本の話し。。。。）

多くのバグが内在する可能性（OpenSSLなどは典型的）

標準と実装のギャップ。何がどこまで正しく実装されているのか分からない。

複雑さを隠蔽するために、どんどん階層化されていく。そのことにより本質的な問題点も隠蔽されていく??

複雑さと問題点が集約されていく

9

Challenge PKIプロジェクトの活動

セコムIS研究所 Intelligent Systems Laboratory

PKI における UTF8String 問題　Challenge PKI 2004

- 調査報告書の概要
  - 問題の公知化と論点の整理
    - 対象とする読者
      - **標準化団体に参画しているエンジニア**
      - **PKI 利用ソフトウェア開発者**
      - **認証局を運用管理している主体**
      - **IT政策当局**
  - PKI利用S/W製品におけるUTF8String項目処理の現状
  - 東アジア圏で発行されている証明書の項目の状況
  - IETFにおける標準化動向
  - 開発者向けのテスト仕様設計
  - 認証局向け移行指針の提言
- 調査報告書URL
  - http://www.ipa.go.jp/security/fy16/reports/pki-utf8string/pki-utf8string.html
- 「PKI における UTF8String 問題」の解決はこれから
  - なぜ問題が認知されていないか？
    - これは、多くの場合、マルチドメインPKIの問題だから。。。

標準化活動に反映する基礎
あるべき仕様の提案
IETFへのフィードバック

10

Challenge PKIプロジェクトの活動
PKI における UTF8String 問題　Challenge PKI 2004
標準の問題 - RFC 3280

セコムIS研究所 Intelligent Systems Laboratory

RFC 3280

UTF8String への移行

2003年12月31日以降に発行する証明書は全てUTF8Stringで
エンコードされなければならない(**とされていた。。。しかし現実には移行されなかった。。**)

*RFC 2459の遺産
*3280bisでは削除

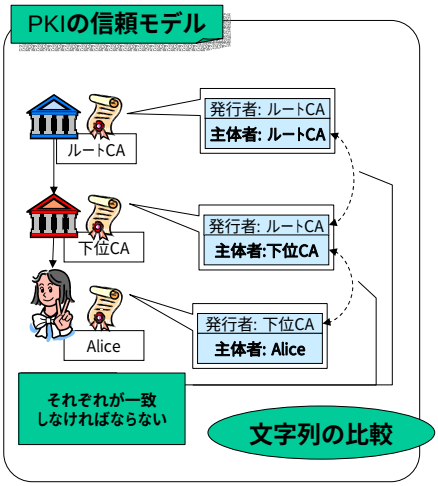
要件定義

曖昧な記述、あるいは記述の欠如
文字列比較、移行、証明書発行、アプリケーション

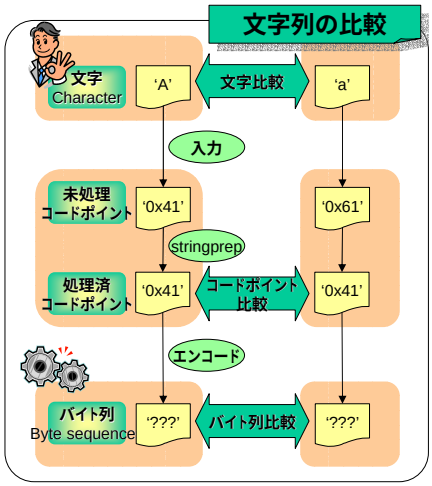
Challenge PKIプロジェクトの活動
PKI における UTF8String 問題　Challenge PKI 2004
PKIの信頼モデルとDNの比較

セコムIS研究所 Intelligent Systems Laboratory

PKIの信頼モデル



文字列の比較



Challenge PKIプロジェクトの活動
PKI における UTF8String 問題　Challenge PKI 2004
様々な関係者　-　様々な悩み

- **標準仕様の策定者**の悩み
  - 「PKIの信頼モデルとDNの比較」の仕様の曖昧さを解消できていない
  - マイグレーションに対する指針を示せていない　– 意見が集約できない。。。
- **CA（認証局）運営者**の悩み
  - CAは、アプリェーションが対応しない限り、 UTF8Stringに対応した証明書を発行できない。。。移行できない。
- **PKIミドルウェア開発者**の悩み
  - 標準が曖昧で、マイグレーションを考えると複雑な実装になってしまう。
  - テストケースの不在
- **アプリケーションベンダー**の悩み
  - **PKIミドルウェア**頼み。悩みがないわけでもないが分からない。。。
- （電子政府などの)??の悩み
  - #理解していないので悩みはない。。。。???

13

Challenge PKIプロジェクトの活動
PKI における UTF8String 問題　Challenge PKI 2004
62nd IETF Meeting, ミネアポリス 2005.3.8

発表シーン

Tim Polk（NIST）

Steve Kent（BBN Tech.）

14

PKI技術最新事情と今後の課題
今後取り上げたいテーマでもある。。。

- SHA-1問題
  - 「PKI における UTF8String 問題」と似た課題を抱える？
  - どうやって移行するのか??誰が全体を取りまとめるか??
- 電子署名法の改正の検討??
  - 技術の問題ではないかもしれない。。
  - しかし技術と政策の乖離が様々な問題を引き起こしているのではないか？
- 医療PKI
  - 医療のIT化等による、医療の効率化、質の向上、利便性向上等の要求
  - これらを実現するセキュリティ基盤としてのPKI
- その他注目すべき動向
  - e文書法に対応した動向
    - ECOMの「長期署名フォーマットのプロファイルの相互運用性テスト」など
  - PKI＆アイデンティティマネージメント
    - 大規模なPKIは、連携アイデンティティ・マネージメントへと進化していく。
  - グリッドコンピュータとPKI
  - 学術系認証基盤の動向
  - 機器認証、プラットフォーム認証　TPM/TCG等

普及といった観点からは、ライトウェイトなPKIの重要性も認識されるべき

15

SHA-1問題

- CRYPTRECの見解　　平成16年9月8日
  - ハッシュ関数SHA-1及びRIPEMD-160の安全性について
    - 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
- 現実の世界
  - IEの証明書リストにある107個の自己署名証明書
    - MD5(46個)、MD2(11個)、SHA1(50個)
  - 自己署名証明書の有効期間は、10年から20年
  - これらは「信頼できる認証局の信頼点」になり得るのか？
- どうやって移行するのか??誰が全体を取りまとめるか??
  - 政策担当者(電子政府など)、暗号関係者、アプリケーション開発ベンダー、認証局、PKI標準化関係者。。。これらの2者以上で会話することは極めて稀（3者となると皆無??)

16

SHA-1からの移行
IETFでの議論 - CRYPTREC等とのレイヤーとの違いがある

- SHA-256などSHA-2ファミリーへの移行
  - 移行負荷が大きい。時間もかかる。
  - 運用だけでなく関連アプリとの相互運用性についても配慮の必要あり。
- SHA-1互換の安全な実装検討
  - 上記のような関連アプリとの相互運用性問題を回避するため、現行SHA-1とできるだけ互換性の高い改善案の検討。
    - Hash BOFの3つの提案
- 新しいハッシュ関数を組み込んだTLS 1.2の検討
  - Eric Rescorla(TLS WG Chair)とSteve Bellovin（IETFセキュリティエリアの元ディレクタ）の見解
  - RFC化に2年、ベンダが設計・開発・テストするのにもう1,2年、展開に3～5年

SHA-1問題
SHA-1からの移行 – 想定される問題
- 「PKI における UTF8String 問題」と似た課題

- 暗号関係者 – CRYPTREC等
  - SHA2ファミリーに移行してね。。。
- **(PKIなどの)標準仕様の策定者**の悩み - IETFでの議論
  - 現実として展開されているプロトコルやフォーマットとの整合やマイグレーション
- **PKIミドルウェア開発者**の悩み
  - 標準が曖昧で、マイグレーションを考えると複雑な実装になってしまう。
  - テストケースの不在
  - #最新のバージョンのOS対応だけでいいよね？。。。。。
- **アプリケーションベンダー**の悩み
  - **PKIミドルウェア**頼み。悩みがないわけでもないが分からない。。。
  - #そもそも、そんな費用誰が負担するの??
- **CA（認証局）運営者**の悩み
  - CAは、アプリケーションが対応しない限り、 SHA2ファミリに対応した証明書を発行できない。。。移行できない。
- (電子政府などの)??の悩み
  - #理解していないので悩みはない。。。。???

電子署名法改正の議論

- 正式名称
  - 「電子署名及び認証業務に関する法律」
- 主な内容
  - 電磁的記録の真正な成立の推定
  - 認証業務に関する任意的認定制度の導入
    - 「特定認証業務」の認定 – 2005年10月時点で17件の認定
- 対象
  - 自然人の電子署名が対象
- 対象外
  - 法人、サーバ、エージェント。。。。の署名
  - 電子認証(Authentication)??、暗号
- 電子署名法の施行　2001年4月1日に施行　（来年で5年)
  - 政府は、この法律の施行後五年を経過した場合において、この**法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずる**ものとする」(附 則　第三条)
    - 5年前、当初目指していた社会との齟齬はたくさんあるはず。

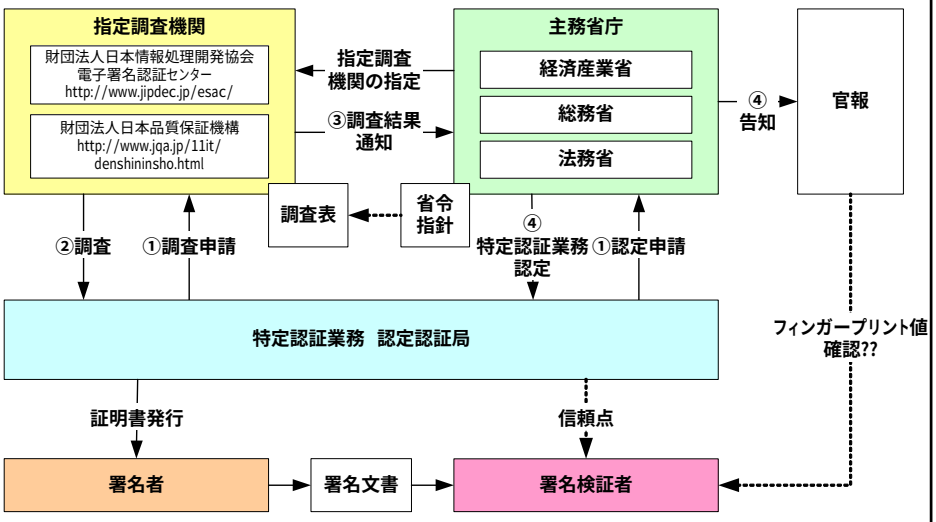
19

電子署名法改正の議論
電子署名法特定認証業務認定制度の問題

- 非常に認定基準が厳しい
  - 結果、高コスト
  - 「認定基準が厳しい」ことは悪いことではない。問題は「認証事業者」以外がそのことを知らないこと。
- 非常に制約が厳しい　#技術の不理解が融通の利かない制度を作っている??
  - 結果、柔軟なPKIが構築できない
  - 自然人にしか証明書が発行できない
    - 「電子署名法」の範疇は、人と人の関係だけで、人と物、物と物の信頼関係を築けない。もしくは、人と物、物と物の信頼関係を分断しているかもしれない　-　いわゆる「オレオレ証明書」問題も関係あるかも。。。。
- 民間における電子署名法特定認証業務認定認証局の問題
  - 「非常に認定基準が厳しい」+「非常に制約が厳しい」=民間におけるビジネスの創造を阻害している可能性がある。現実に純粋に民間向けの認証局は少ないし減少傾向にある。これは本来の制度の目的を満たしていない。また、普及しないのであれば「制度」自体の意味をなさない。

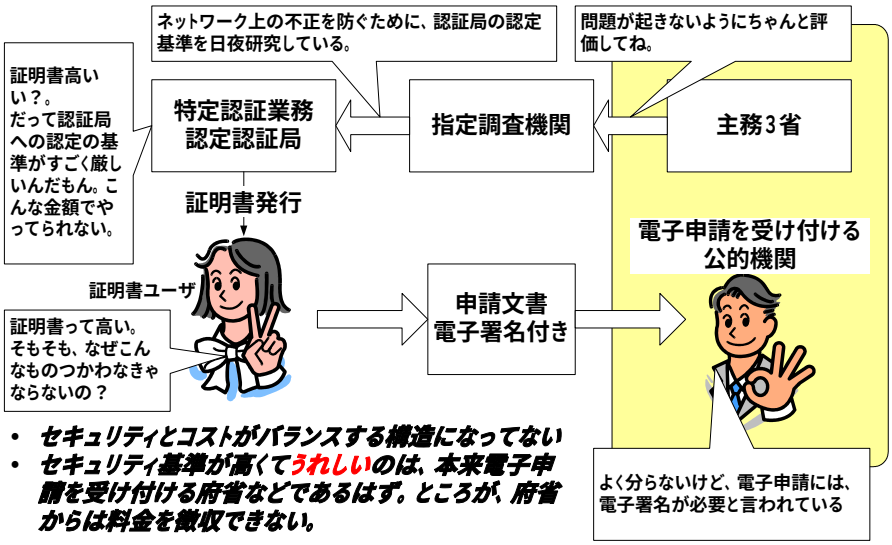
20

電子署名法改正の議論
電子署名法特定認証業務認定のスキーム



21

電子署名法改正の議論
非常に認定基準が厳しい　- 結果、高コスト



- ***セキュリティとコストがバランスする構造になってない***
- ***セキュリティ基準が高くて<u>うれしい</u>のは、本来電子申請を受け付ける府省などであるはず。ところが、府省からは料金を徴収できない。***

**公的個人認証サービスは、証明書検証者からお金を取ってる。

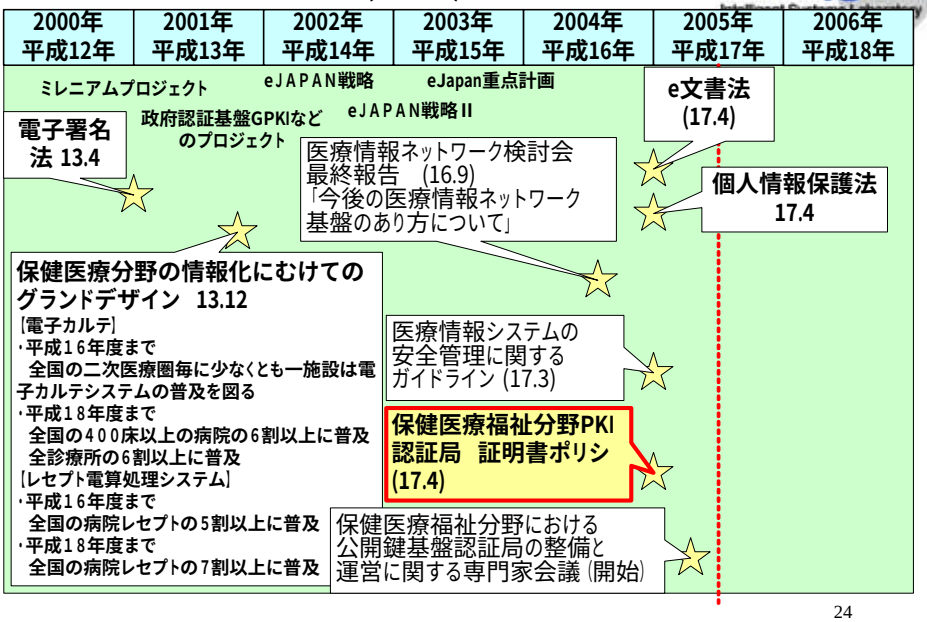
22

保健医療福祉分野PKI(HPKI)の動向

- 医療情報の電子化、ネットワーク化　ー　必須の流れ
  - IT化による医療情報の有効利用促進
  - 患者へのサービス向上
  - 病診連携、病病連携、遠隔医療
- セキュリティ基盤の整備の要求
  - 連携、情報共有+「患者の視点」を行なうためには、セキュリティ基盤が重要
    - 単なるIT化ではない。
  - セキュリティ基盤のひとつに**医師による電子署名**を行うための**保健医療福祉分野PKI(HPKI)**がある
- 電子カルテ等への医師による電子署名
  - 診療記録の電子化データの証拠能力のために必須
  - 医師の署名　－　カルテへの署名など
    - 医師という資格を持った人間が、その責任において文書に署名を施す。法令遵守などを示すためには、この署名文書が保存される必要がある
- 電子署名対象
  - 診療録、処方箋、放射線記録、紹介状・・・

23

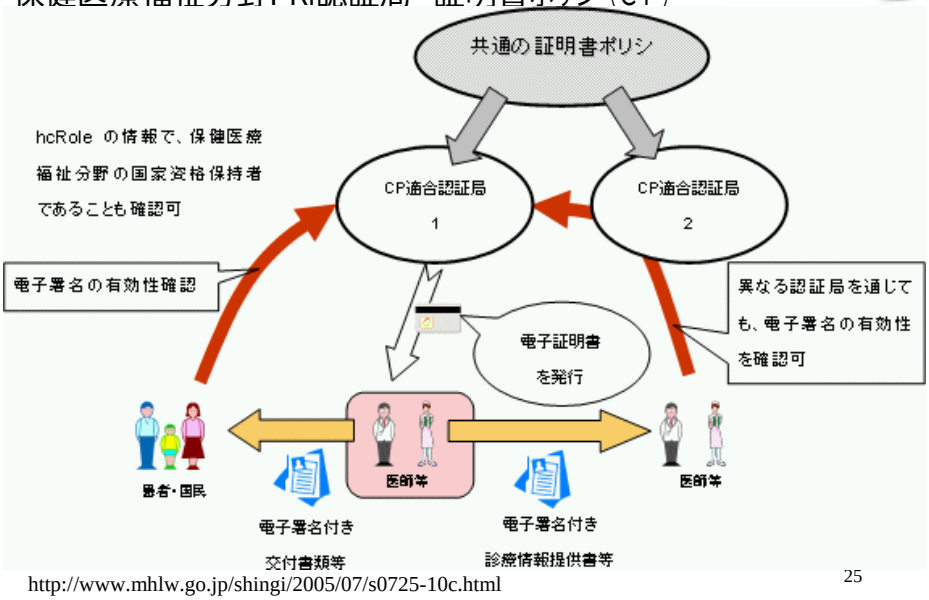
保健医療福祉分野PKI(HPKI)の動向 － 続き



24

保健医療福祉分野PKI(HPKI)の動向 － 続き

保健医療福祉分野PKI認証局　証明書ポリシ（ＣＰ）



http://www.mhlw.go.jp/shingi/2005/07/s0725-10c.html

25

まとめ

- PKIは、情報社会の様々なインフラとなるべき技術ですが、その技術の幅は非常に幅広く、また、奥深いものがあります。
- 様々な技術の課題がありますが、やはり一番大きな課題は、相互運用性に関する問題を克服することでしょう。
- PKIは、社会インフラとの視点から考えた場合、社会の「信頼」を築くための技術と言えます。IT技術が社会に浸透するほどに、幅広いPKIの相互運用性は、その重要性は深まっていくでしょう。

26

参考

- NPO JNSA Challenge PKIプロジェクトのホームページ
  - http://www.jnsa.org/mpki/index_j.html
- これまでのNPO JNSA相互運用技術WG主催セミナー
  - セキュリティAPIセミナー
    - http://www.jnsa.org/seminar/2004/seminar_20040826.html
    - 2004年8月26日(木)
  - 「認証技術の動向」セミナー
    - http://www.jnsa.org/seminar/2004/seminar_20041209.html
    - 2004年12月9日(木)