平成 19 年 1 月 24 日

国立大学病院医療情報企画関連部長会
情報関連法規と国立大学附属病院の情報管理に係る
検討ワーキンググループ長
廣瀬康行＠琉球大学

情報関連法規と国立大学附属病院の情報管理に係る検討ワーキンググループ
第４四半期　報告書

本WGの第１四半期報告書に引き続いて第４四半期報告書として若干の解説等を報告する.

別　添

- いわゆる「電子カルテシステム」等における診療録等の
  電子文書の調整と運用等

参　照

- 情報関連法規と国立大学附属病院の情報管理に係る検討
  ワーキンググループ第１四半期報告書
  - 医療情報システムの安全管理に関するガイドライン
    （厚生労働省医政局長通達 H17.3）に係わる提言（案）
  - いわゆる「電子カルテシステム」等における診療録等の
    電子保存について ～若干の解説～
  - 情報関連法規と国立大学附属病院の情報管理に係る検討
    ワーキンググループ 設立趣意書

以上

平成 19 年 1 月 24 日
国立大学病院医療情報企画関連部長会
情報関連法規と国立大学附属病院の情報管理に係る検討ワーキンググループ

いわゆる「電子カルテシステム」等における
診療録等の電子文書の調整と運用等

１．電子文書の調整に際して法で定める電子認証や電子署名が適用される診療記録等

いわゆる「電子カルテシステム」等において調整される各種文書を次のように区分する：
(1)　法令等で「記載すべき事項とされた記名押印」が規定されている書面の電子文書
(2)　上記以外の書面の電子文書
(3)　電子文書を調整した後には当初は原本であった当該の紙の文書を法令で規定された保存期間内であるにも関わらず破棄することを前提して調整するような電子文書

関係法令が規定するところとは，(1) と (3) については，いわゆる電子署名法 ならびに e-文書法に則って特定認証業務を行う認証事業者の認証および時刻認証業務認定事業者の時刻認証を用いること，である．

さて (1) は厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令（平成 17 年 3 月 25 日厚生労働省令第 44 号）によって規定されおり，そのうち通常の診療業務において診療従事者が作成閲覧する診療文書とされるものは僅かに，放射線の照射録，臨床修練外国医師の診療録，および様々な制度の下に交付運用される診断書等，のみである．

事由１：上記省令の第七条には「別表第二の下欄に掲げる書面の作成において記載すべき事項とされた記名押印に代わるものであって、法第四条第三項に規定する主務省令で定めるもの（抜粋)」とある．

事由２：厚生労働省「医療情報ネットワーク基盤検討会」最終報告（平成 16 年 9 月 30 日）
III. 医療に係る文書の電子化

したがってその他の多くの診療文書は (1) には該当せず (2) の範疇に属するものと解釈される．ただし上述の最終報告が言明しているように，院内業務で用いられている連絡票的ないわゆる院内処方箋ではなくて，通常云うところの（院外）処方箋については，そもそも電子文書化の対象外とされている．

次に (2) については，法令においては特定認証業務を行う認証事業者の認証ならびに時刻認証業務認定事業者の時刻認証を用いることを求めてはいない．ただし法令の趣旨や社会的な要請を基として関係ガイドラインそのほかは，上記関係法令等に準じた機構や管理に

よって当該医療機関としての自己責任（管理責任，説明責任，結果責任）を全うすることについては，これを求めている．よってその実現にあたっては，必ずしも院内認証や院内時刻認証による運用を妨げるものではない．

そして（3）については，紙媒体から電子媒体へと原本性を移転することを意味するので，相当の厳格さが要求されることには論を待たない．
ただし，日常業務においては電子文書を参照し，紙媒体については少なくとも規定された保存期間内は保管しておき・必要に応じて遅滞なく参照しうるし参照する，というような運用であるならば，必ずしも特定認証業務を行う認証事業者の認証ならびに時刻認証業務認定事業者の時刻認証を用いることを要さない．

２．いわゆる「電子カルテシステム」等における電子文書の調整と運用

先ず（2）については，前節１に記した要件を満たす限りにおいては，これまでのシステムデザインやシステム運用の改変を要するものではなかろう．

次に（3）については，たとえば「スキャニングセンター」なるものを設置して，その部署は Internet に接続し・しかしながら診療情報システム用ネットワークとは切り離す，というネットワークトポロジーにて運用可能であろう．したがって調整された電子診療録を診療情報システムに複写する際には外部記憶媒体に拠ることとなる．

当然ながらスキャニングセンターの端末やサーバは相当の（しかし通常の）セキュリティ機能の保護下にある必要があり，また外部記憶媒体による複写においては機関内（事業者内）の局所的にではあっても厳密には「持出・持込」が発生するのであるから，責任所在追跡性に関わる相当の機構が用意されて然るべきであろう．
よって必ずしも甚大なる費用が必要になるとは思われない．

(1) については場合分けしながら述べる．
法令によって特定認証業務を行う認証事業者の認証および時刻認証業務認定事業者の時刻認証を用いることが定められているので，以下のような運用形態となる．

(a) 署名された診療文書を閲覧するのみであれば，Internet への接続は要するけれども，CRL を「見にいく」だけである．
(b) 署名するのみであれば，Internet に接続する必要はない．
(c) 署名の際に時刻認証を含む場合には，Internet に接続して「要求を出す」とともに「返答を受ける」必要がある．

いずれにせよ特定の（あるいは極めて限られた）サイトとの交信のみである．
逆にもし院内認証局や院内時刻認証局を設置した場合には，むしろ交信サイトを限定することができなくなる．

さて（a）については，たとえば代替サーバのみが RC232 を介して定期接続して CRL を確認し，その情報を院内診療情報システム内の端末等からの要求に応じて返答する，などの機構が考えられる．もちろんファイアウォールを用いて，限られたサイトのみと限られたポートならびにプロトコルのみで交信することも現実的であるし，膨大な通信量とはならないと推測されるため，ファイアウォール等のハードウエアやソフトウエアに要する各種費用等も比較的廉価に調達することも可能であると思われる．
この事情は，基本的には（c）においても同様である．

そもそも（1）については，現況のところ，或る医療機関の内外で交信される文書には「様々な制度の下に交付運用される診断書等」しか想定されえない．
然るに，そのような電子文書を処理しうる各種の社会基盤（行政側の準備）は未だ整っているとは云い難い．ゆえに相当に広汎の実現環境が無い段階で実現準備にコストを掛けることは，個々の機関の経営判断に委ねるべきことと思われる．

なお，いわゆる地域連携システムによって，既に「記載すべき事項とされた記名押印」が規定されている診療文書等を真正なる電子文書として交換している事例においては，その真正性を法的に主張するためには，法令に則る必要を回避しえないことは無論である．

３．真正であることなど（技術・標準・法令・指針）

本当 って なんだろう ？

- 現実世界
  - 本当か そうでないかは 見れば 触れば 判る？
  - そう かな..
    - では，紙に名前を書いて，その紙をコピーしたら，その紙と，そのコピーは，どちらが『本当』なの？
    - どうして？　ホンモノ とは 云ってはいない
- 情報技術（IT）の世界
  - そのファイルと，そのファイルのコピーとでは，どちらが『本当』なの？

08-SEP-2006 ©1997-2006 Y.Hirose 5

考えるための準備

WHO	ダレ	が
WHEN	イツ	
WHERE	ドコ	で
WHOSE	ダレ	の
WHAT	ナニ	を
content		
WHY	ナゼ	
HOW	ドユ	ふに
DO WHAT	ナニ	した

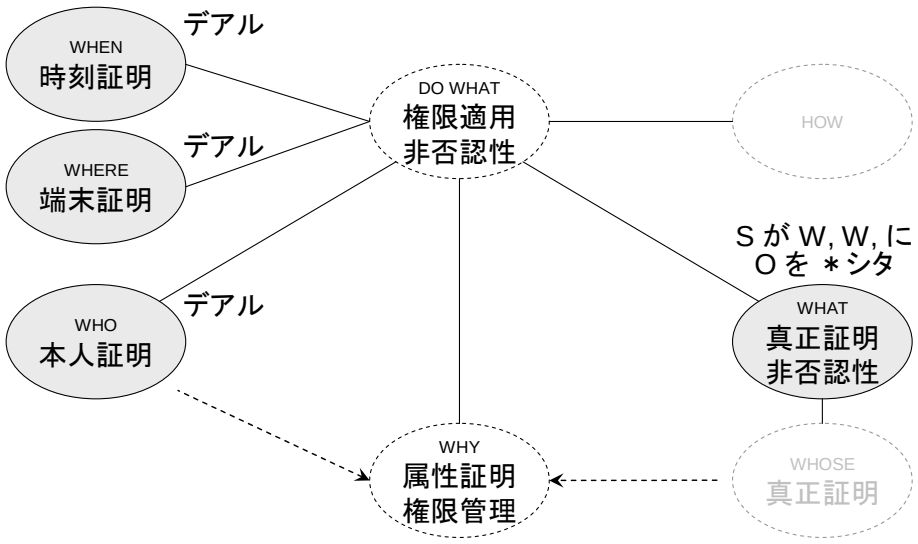
08-SEP-2006 ©1997-2006 Y.Hirose 6

情報技術の世界

- WHO　本人証明
- WHEN　時刻証明
- WHERE　端末証明
- WHOSE　真正証明
- WHAT　真正証明 と 非否認性
  - content　要約
- WHY　属性証明 と 権限管理
- HOW
- DO WHAT　権限適用 と 非否認性

08-SEP-2006 ©1997-2006 Y.Hirose 9

どこから 押さえて いくか



08-SEP-2006 ©1997-2006 Y.Hirose 25

どのように 押さえて いくか

- WHO　認証
- WHEN　認証
- WHERE　認証
- WHOSE
- WHAT　署名
  - content　要約の比較（ハッシュ値で）
- WHY　属性証明 と 権限管理
- HOW
- DO WHAT　権限適用 と 非否認性

08-SEP-2006 ©1997-2006 Y.Hirose 26

基礎となる技術

- ハッシュ（hash）
  - 与えられた原文から固定長の疑似乱数を生成する演算
  - 同一のハッシュ値を生成しない性質（collision proof）
    - 同じビットパタンが得られるような2つの原文の発見は困難
    - あるビットパタンが生成されるような原文の発見は困難
    - この意味において 通常の チェック･サム とは異なる
- 暗号（ここでは cipher）
  - 特定の規則によって原文（平分）を暗号文に変換すること
    - 暗号とは平分空間と暗号空間の一意写像
    - その変換函数 F(x,y ..) の変数が『鍵』として用いられる
    - 暗号化（encrypt）と 復号化（decrypt）の際に『鍵』が必要
  - 秘匿通信技術には 他に code や steganography がある

08-SEP-2006 ©1997-2006 Y.Hirose 28

ハッシュ

MD, RIPEMD, SHA, Tiger などあるが通常に用いられるのは MD5, SHA-1

4918DD8442E95DCFCFAF13072A61996B13263E55

観自在菩薩　行深般若波羅蜜多時　照見五蘊皆空　度一切苦厄　舎利子
色不異空　空不異色　色即是空　空即是色　受想行識　亦復如是　舎利子
是諸法空相　不生不滅　不垢不浄　不増不減　是故空中　無色無受想行識
無眼耳鼻舌身意　無色声香味触法　無眼界乃至無意識界　無無明亦無無明尽
乃至無老死　亦無老死尽　無苦集滅道　無智亦無得　以無所得故菩提薩捶
依般若波羅蜜多故　心無圭礙無圭礙故　無有恐怖遠離一切顛倒夢想
究竟涅槃　三世諸仏　依般若波羅蜜多故　得阿耨多羅三藐三菩提　故知般若波羅蜜多
是大神咒　是無上咒　是無等等咒　能除一切苦　真実不虚　故説般若波羅蜜多咒
即説咒曰　羯諦羯諦　波羅羯諦　波羅僧羯諦　菩提娑婆訶　般若心經

本当 を確認するため
全部を読むのなら，
もはや確認ではなく，
2回読むということ．
1000ページの本は？
高密精細な画像は？

AFE875865851D05B67B2AE0D650A3A85E630DE92

観自在菩薩　行深般若波羅蜜多時　照見五蘊皆空　度一切苦厄　舎利子
色不異空　空不異色　色即是空　空即是色　受想行識　亦復如是　舎利子
是諸法空相　不生不滅　不垢不浄　不増不減　是故空中　無色無受想行識
無眼耳鼻舌身意　無色声香味触法　無眼界乃至無意識界　無無明亦無無明尽
乃至無老死　亦無老死尽　無苦集滅道　無智亦無得　以無所得故菩提薩唾
依般若波羅蜜多故　心無圭礙無圭礙故　無有恐怖遠離一切顛倒夢想
究竟涅槃　三世諸仏　依般若波羅蜜多故　得阿耨多羅三藐三菩提　故知般若波羅蜜多
是大神咒　是無上咒　是無等等咒　能除一切苦　真実不虚　故説般若波羅蜜多咒
即説咒曰　羯諦羯諦　波羅羯諦　波羅僧羯諦　菩提娑婆訶　般若心經

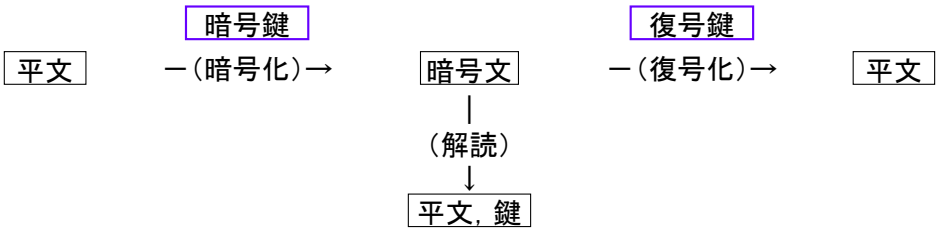
一文字 異なるだけで
全く異なる ハッシュ値

ハッシュ値を較べる
だけで よい

08-SEP-2006　©1997-2006 Y.Hirose　29

暗号（cipher）

昔から よく 使われてきた：　恋人同士，外交，軍隊　（置換 or 換字，転置）



赤田首里殿内　黄金灯篭 下ぎてぃ
うりが明がりば　弥勒迎い

大黒のぅ弥勒　我が島に居もち
うかきぶせみしょり　弥勒世果報

弥勒代のぅ昔　くいむどぅちなまに
うまんちゅのぅ交り　遊ぶ嬉しや

aaa

```
3E C6 07 0B 9D E8 13 DD 82
D5 71 2D 83 84 E0 E7 94 75
02 78 A5 5A 69 1D DB 91 5D
F9 55 8F 0F 48 71 AF 61 23
C6 9E 33 E9 69 C2 D4 F3 4C
7B F3 51 DD D9 AC 78 17 EB
0D 0A 53 8F EB 14 8A 9A 67
..
```

08-SEP-2006　©1997-2006 Y.Hirose　30

安全性と 計算経済性

- 暗号（cipher）とは平分空間 2^N と暗号空間 2^N の一意写像
- 変換函数 F(x,y ..) の変数が『鍵』として用いられる

- 解読とは 平分空間と暗号空間との 写像パターン の発見
  - 鍵を長くすると「組合せ」は 指数函数的に増加する $(2^N)!$
  - 鍵を 1 ビット 長くすると 計算コストは 2 倍となる
- 安全性は，解読に要するコストを大きくして 解読によって得られる利益を相対的に減殺すること，に依存している
  - 計算的安全性（computational security）
  - 無条件安全性（unconditional security）
- 暗号の安全性は 鍵の安全性 に依っている
  - 長い鍵
  - 鍵の管理

Public key distribution という アイデア

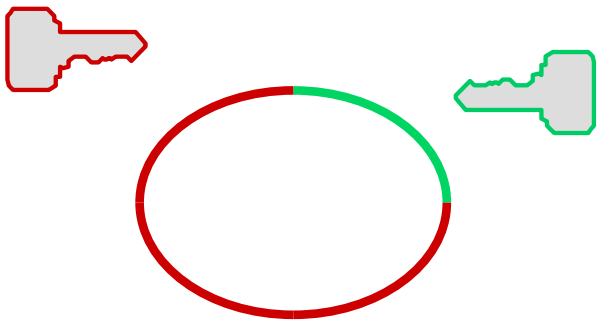
- 対称鍵 の不都合
  - 鍵の保管 vs 鍵の交換 という矛盾する状況
  - 関係者が増えると 鍵の数も急激に増加 $(N^2 – N)/2$
    - 鍵 が増えれば 管理も杜撰と なりがち
- アイデアの原型
  - ペア鍵 (K, P) を用意する
  - Aの秘密鍵 K_A と B の公開鍵 P_B を使って暗号化
  - Bの秘密鍵 K_B と A の公開鍵 P_A を使って復号化
  - もし これを実現できるなら
    公開鍵 P_X を insecure な場所に公開しておいてよい

一方向性函数（one-way function）

- 逆元の導出が極めて困難
  - 逆函数計算が極めて困難（離散対数 や 楕円函数）
  - 離散対数
    - 素数 q の modulo の基で 整数 a,x,y が　$y = a^x \pmod q$
      のとき，逆に a,q,y から x を求める際，
      x は a を底とする y の離散対数となる.　$x = \log_a y \bmod q$
    - 計算困難性は素因数分解に起因
- 計算コスト
  - 順方向　$O(2 \log_2 q)$　　q=2 200 なら 400 回の演算
  - 逆方向　$O(q^{1/2})$　　q=2 200 なら 10 30 回の演算
    - 256 bit なら 10進数で 77桁程度
    - 10進数で 100桁を超えると因数分解は通常困難
      10進数で 200桁となると素因数分解は極めて困難

非対称鍵暗号　Asymmetric key cryptography

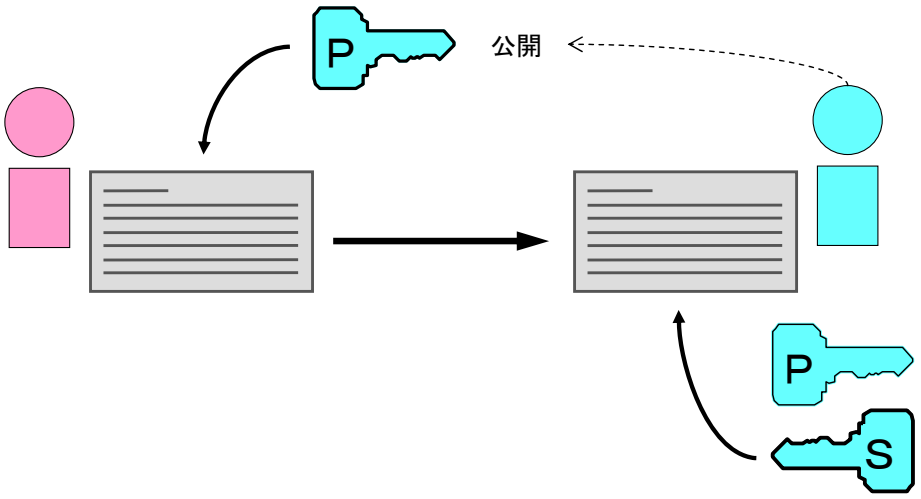
片方の鍵 で 暗号 した 原文 は
他方の鍵 でなければ 復号 できない



秘密鍵 での 暗号化
公開鍵 での 復号化

Yamamoto R, Tokyo Univ

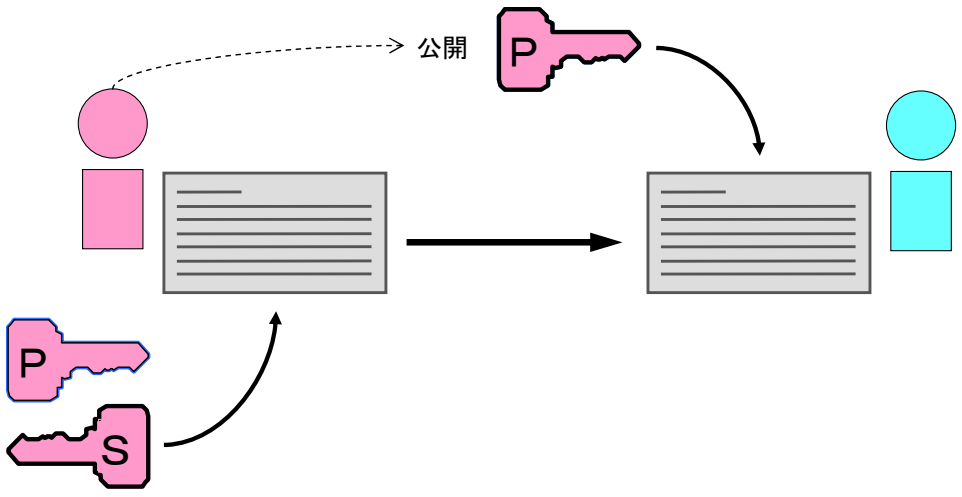
公開鍵暗号（相手P鍵で暗号：相手の特定）



08-SEP-2006 ©1997-2006 Y.Hirose 37

Yamamoto R, Tokyo Univ

署名（自分のS鍵で暗号）



08-SEP-2006 ©1997-2006 Y.Hirose 38

署名

- 要求要件
  - 第三者によって 偽造（forge）できない
  - 受取人によって 偽造（forge）できない
  - 発行者は事後に 否認（repudiate）できない
  - 有効性はダレもが 確認＆検証（validate）できる
- 適合性
  - 秘密鍵は本人しか知りえない
    - 持ち出し不要（そして持ち出すことはない）
    - 秘密鍵は 耐タンパ性の高い格納器に格納
  - 公開鍵は公証されている

08-SEP-2006 ©1997-2006 Y.Hirose 39

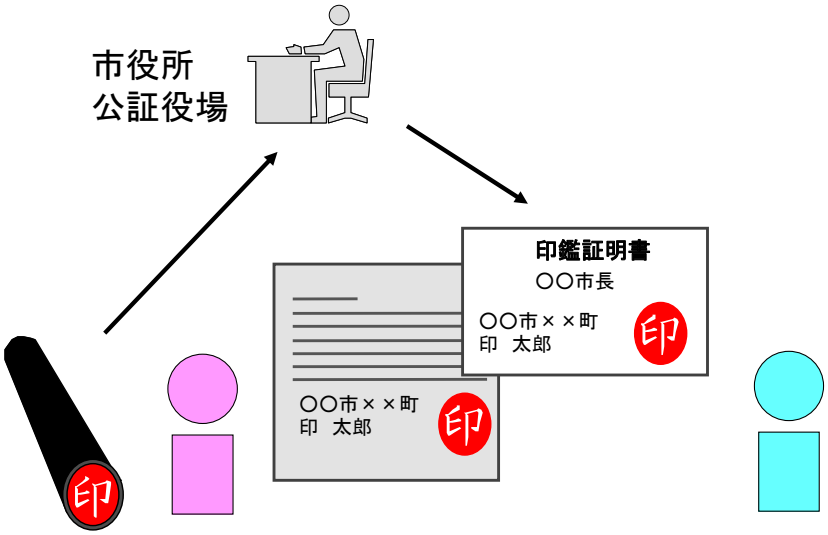
公開鍵基盤 Public key infrastructure

- 高信頼情報交換を実現する技術
  - 電子署名　（実印）
  - 電子証明書　（印鑑証明）
- 目的
  - 認証　（本人証明）
  - 電子署名　（真正証明，非否認性担保）
  - 付随して
    - 暗号化
    - 改竄防止
- それ以外は 規格 としては optional
  - 時刻認証　送付先の限定
  - 属性の認証　個の権限の適切な付与

08-SEP-2006 ©1997-2006 Y.Hirose 44

Yamamoto R, Tokyo Univ

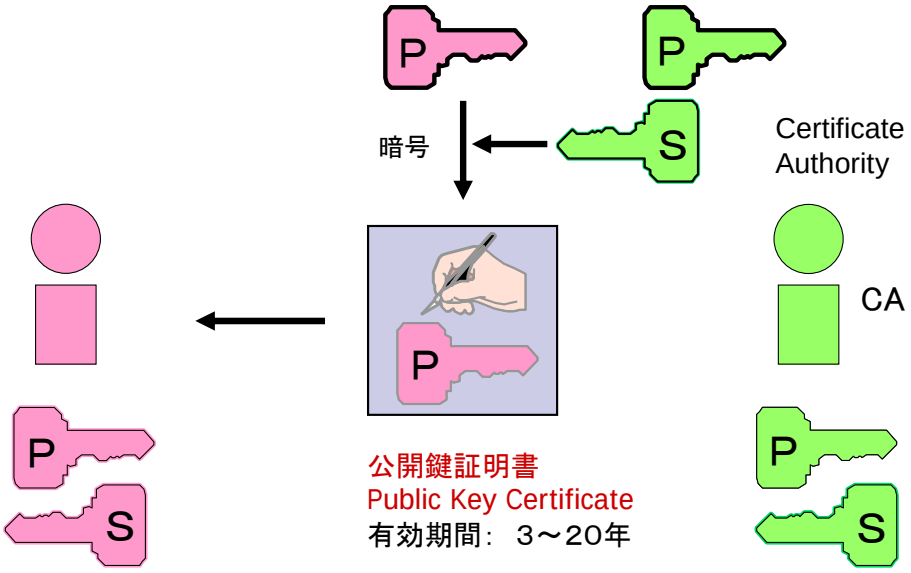
公証　～紙で運用するとき（今まで）



08-SEP-2006　©1997-2006 Y.Hirose　45

Yamamoto R, Tokyo Univ

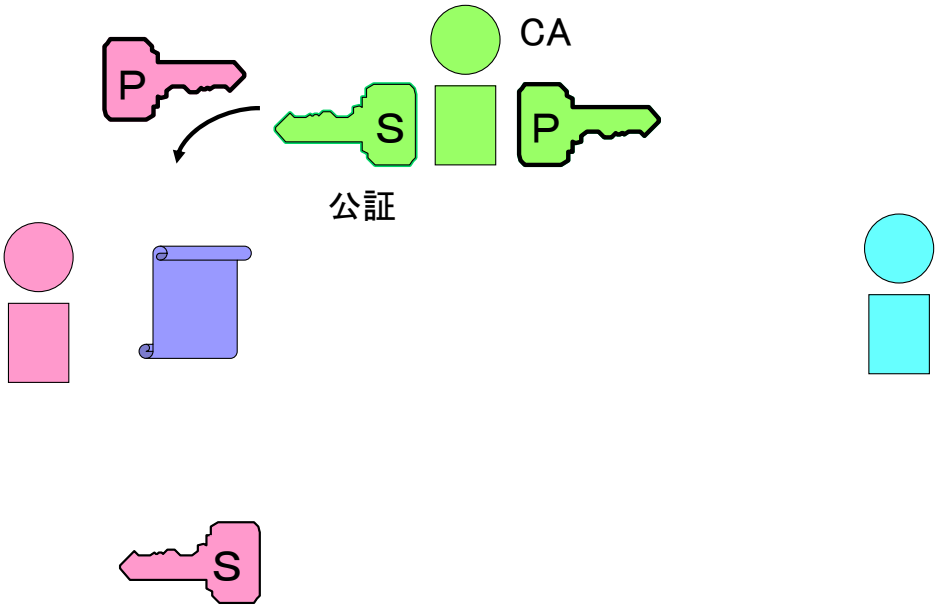
公証　～公開鍵証明発行局（CA）



08-SEP-2006　©1997-2006 Y.Hirose　46

Yamamoto R, Tokyo Univ

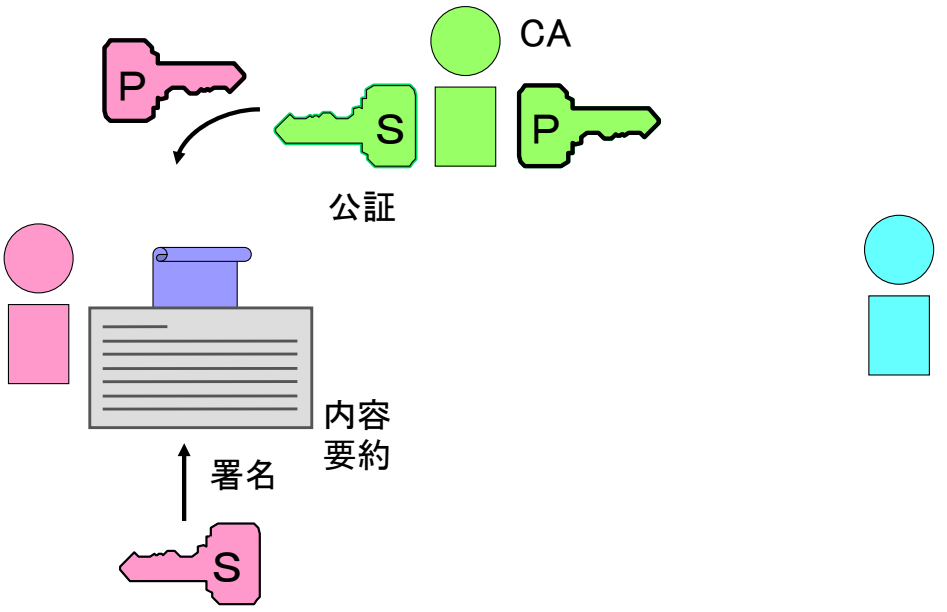
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 47

Yamamoto R, Tokyo Univ

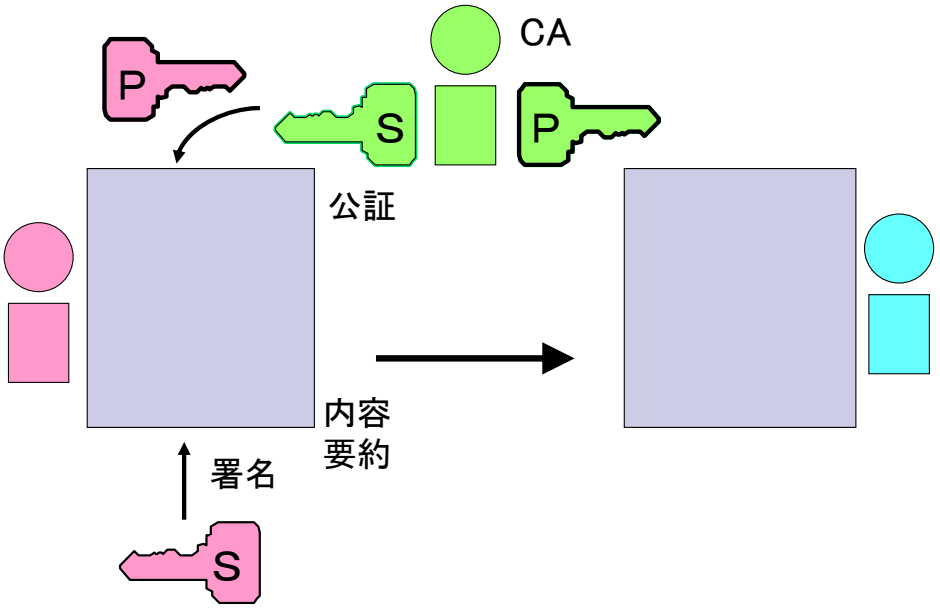
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 48

Yamamoto R, Tokyo Univ

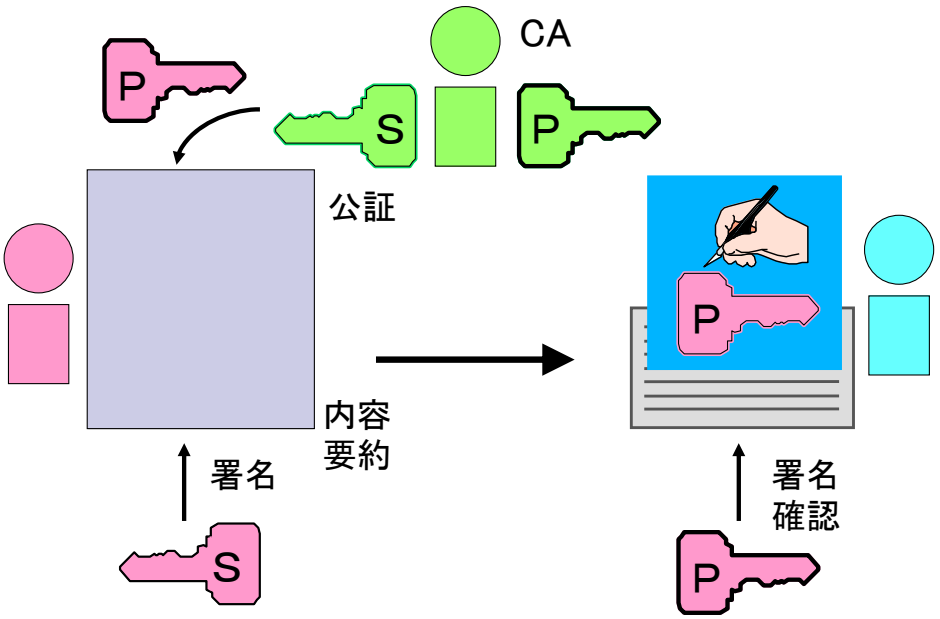
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 49

Yamamoto R, Tokyo Univ

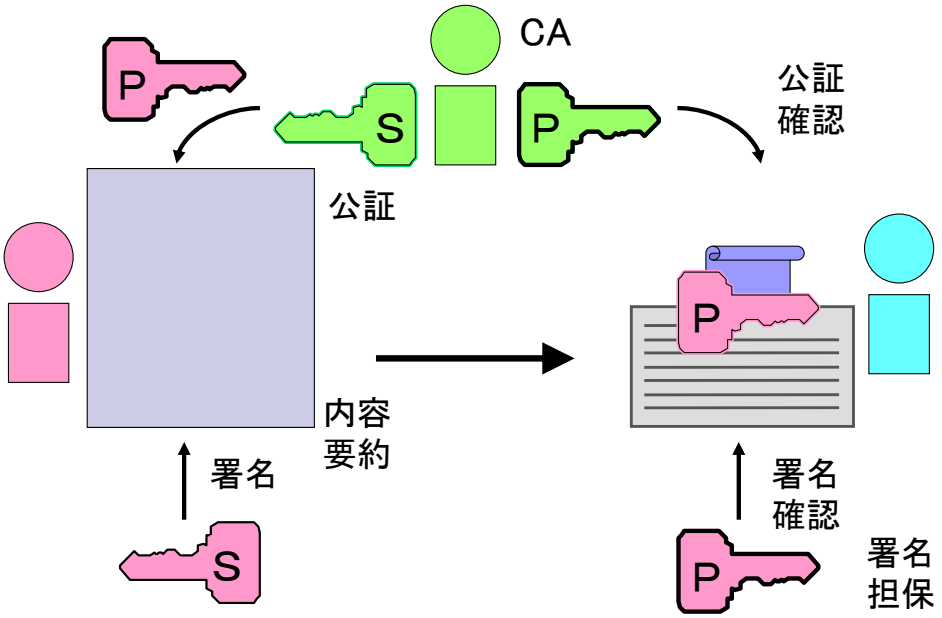
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 50

Yamamoto R, Tokyo Univ

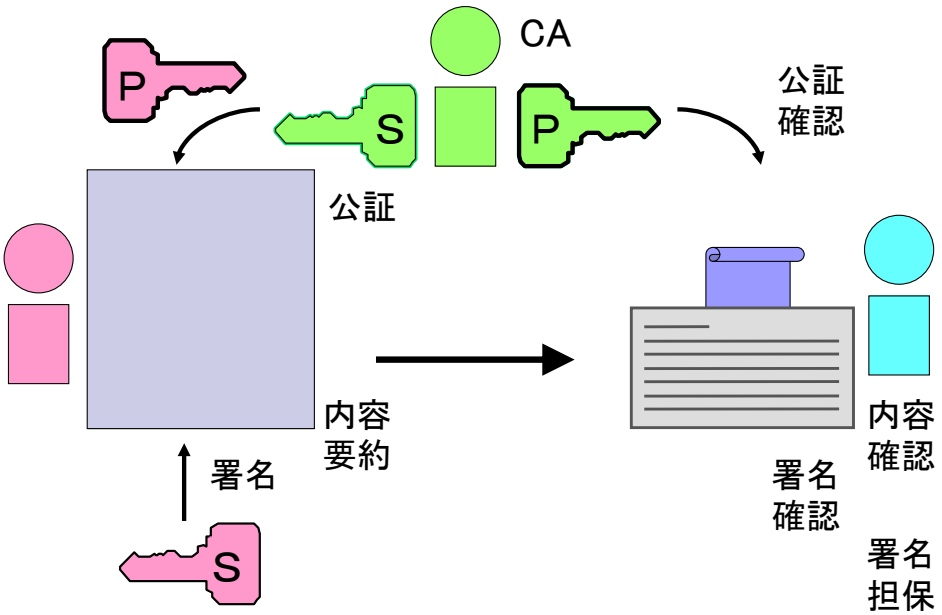
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 51

Yamamoto R, Tokyo Univ

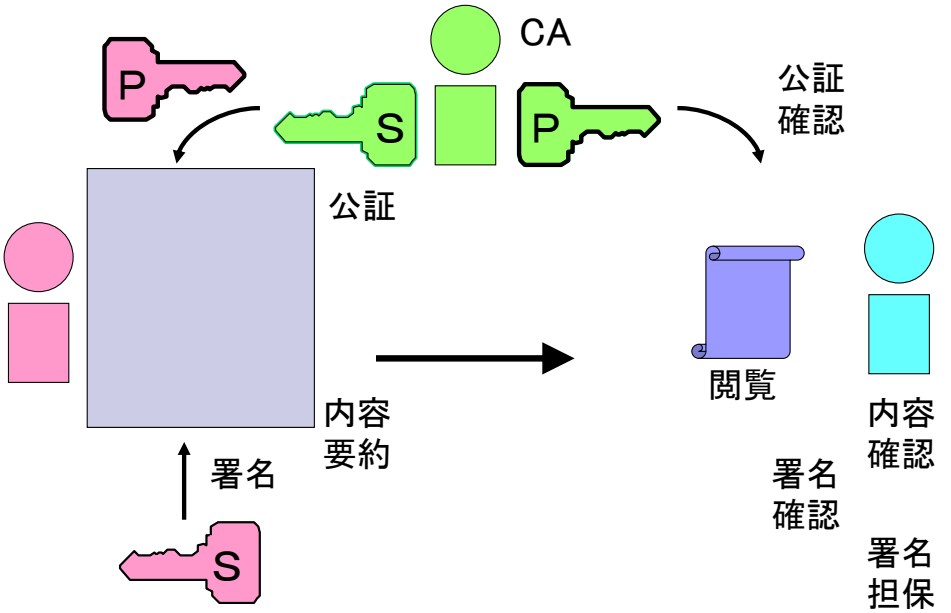
公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 52

Yamamoto R, Tokyo Univ

公開鍵基盤 PKI の全体イメージ



08-SEP-2006 ©1997-2006 Y.Hirose 53

ところで，秘密鍵はドコに保管するの？

- 端末やサーバの秘密鍵
  - マシンのなかに置くしかない
- ユーザの秘密鍵
  - 覚えるメモる　無理＆だめ；そもそも使えない
  - 磁気カード　磁気ストライプ（記憶媒体）は露出
スキミング は簡単
  - RFID　…
  - IC カード　…

08-SEP-2006 ©1997-2006 Y.Hirose 58

サイドチャネル攻撃（side-channel attack）

- 暗号装置の動作状況を物理的手段で観察して，
  装置内部の情報の取得を試みる攻撃方法.
- 従来の暗号の攻撃法の前提
  - 平文や暗号文にはアクセスできる
  - 暗号処理はブラックボックス
    - 処理中のデータには一切アクセスできない
- しかし攻撃者が処理時間や消費電力を精密に測定できるなら，
  その情報チャネルからも『情報』は漏洩する
  - タイミング攻撃
  - 故障利用攻撃
  - 電力解析攻撃
  - 電磁波解析攻撃
  - キャッシュ攻撃
  - 音響解析攻撃

米国・カナダ政府調達基準 FIPS 規格

耐タンパ性 （Tamper Proof）

- 半導体チップなどの内部の解析や改竄を
  物理的及および論理的に防衛する性能
  - 不正解読防止
  - 不正書換防止
- タンパ（temper）
  - いじくる，みだりに変更する，勝手に変更できる，
    無分別に（危険な）試みをする

altro mezzo

One-time password という アイデア

それでも
Dictionary attack（辞書攻撃）
Birthday attack（誕生日攻撃）$2^{N/2}$
Brute Force attack（力ずく攻撃：総当り攻撃）2^{N}

ならば .. これっきり それっきり もぉ これっきりぃ ですかぁぁ
あるいは カタチ としては テロメア みたいな ： S/Key

機構としては
1. 一方向性函数によって鍵の「列」を作る ＝ 鍵は複数個
   その「列」には「向き」があって，順方向と逆方向とでは，
   計算量が異なる．つまり 逆方向の鍵解読は困難である．
2. 始めに，逆方向に全部の鍵を生成しておき，順方向に
   向かって，一つづつ使い捨てる（サーバ毎に）．
3. サーバを同定するために，サーバ毎の seed を用意する．
   何番目の鍵を使うべきなのか，サーバ側から通知する．
   チャレンジ・レスポンス
4. 鍵と seed とを 組み合せて 認証する．

08-SEP-2006 ©1997-2006 Y.Hirose 40

Ticket という アイデア

Fluffy って，知ってる？ .. ハリーポッター の．
あれ Kerberos．冥界の支配者 Hades が飼う 冥府門の番犬．

機構
1. Realm を想定して，その鍵配信センター（KDC）が，
   全ての realm 内の資源（ヒト，モノ，サービス 等）を，
   鍵 とともに 管理する ... というか 支配する．
2. 各々の資源は，他の資源を利用する際には，KDC に
   リクエストして，資源利用の許可証 ticket を もらう．
3. 信頼できる第三者機関による認証を前提している．

- Trusted Third Party Authentication は良いし，ticket と
  いう発想は興味深いけれど
- その 王国 において 遍く全て を 管理する！ 対称鍵で！
- KDC (Key Distribution Center) 自体が vulnerable となる
  権限の強さと集中は，脆さ と 危うさ を 胎む
- 全ての システム資産を 一斉に Kerberos 化せねばならぬ

08-SEP-2006 ©1997-2006 Y.Hirose 41

Zero-Knowledge Proof というアイデア

ゼロ知識証明（ZKIP）
アタシ： 教えたげな〜い，ヒ・ミ・ツ！ だけど アタシ知ってるもん！
偉い人： キミが知っているということを検証しよう，話はそれからだ．

目標
自分の持っている秘密情報を相手に明かすことなく，
その秘密を保持してることを相手に納得させる方法．

知識（＝ ヒミツ を 知っている）とは
問題 を知っており，かつ その 解法（解くための変数）を知っていること．

機構
一方向性函数を活用する．
A と B とで 対話（情報交換）を行いながら，検証する．
問題と解法の同型（問題^{H}と 解法^{H}）を同時に生成できることを検証する．
騙し（fool）を抑制するために，騙し確率 を低減させる． $(1/2)^{n}$
騙し確率 の低減は，複数回の対話（問答）によって実現する．

08-SEP-2006 ©1997-2006 Y.Hirose 42

Primum non nocere

Codes, Declarations, Bill

- Nuremberg Code (1947)
- World Med Assoc: Declaration of Geneva (1948)
- World Med Assoc: Intern Code of Medical Ethics (1949, rev.83, rev.94, rev.05, rev.06)
- World Med Assoc: Declaration of Helsinki (1964, rev.75, rev.83)
- Am Hosp Assoc: Patient's Bill of Rights (1973, rev.92)
- World Med Assoc: Intern The Declaration of Lisbon (1981, rev.95)

- 1947 ニュールンベルク倫理綱領
- 1948 世界医師会: ジュネーブ宣言《医の倫理規定に併せて 改訂》
- 1949 世界医師会: 医の倫理規定《含 改訂》
- 1964 世界医師会: ヘルシンキ宣言《含 改訂》
- 1973 合衆国病院: 患者の権利章典《含 改訂》
- 1981 世界医師会: 患者の権利に関するリスボン宣言《含 改訂》

11-SEP-2006 ©1997-2006 Y.Hirose 5

CONFIDENTIALITY

- 信頼 に応えること
- 信頼 に応えている ことを 説明できること
  - 信頼に応えるための 環境や状況があること
  - 信頼に応えるための 環境や状況を構築済か または 構築努力していることを 説明できること
- 信頼 とは
  - 権利と期待が secure であると信ずるに足ること
  - 権利と期待が secure であるように種々の事柄が管理されている と信ずるに足ること

11-SEP-2006 ©1997-2006 Y.Hirose 10

脅威〔一般論〕

- 盗む
  - 盗聴する，盗み見する，盗難する
- 漏らす / 漏れる
- 詐称する
- 壊す / 壊れる
  - 改竄する，破壊する，消す；壊れる，汚染と揮発，消える
- 取り違える
  - ヒト，属性，組織，モノ，手順
- 不適切な権限管理による 開示 や 隠蔽
  - 見る必要が ある のに 見ることが できない
  - 見る必要が ない のに 見ることが できてしまう

GMITS ISO/TR13355 → ISO 27001

- 機密性（Confidentiality)
  - データおよび情報が，正当と認められるときに，正当と認められる方法で，正当と認められる個人，組織，およびプロセスにのみ開放されること
- 完全性 (Integrity)
  - データおよび情報が，正確で完全であること
- 可用性 (Availability)
  - データ，情報および情報システムが，要求された方法で適時にアクセス可能かつ利用可能であること
- 信憑性 / 真正性 (Authenticity)
  - 利用者，プロセス，システム，および情報，または資源の身元（identity）が主張通りであることを保証すること
- 追跡性 (Accountability)
  - 主体の行為からその主体にのみ至る形跡を辿れることを保証すること
- 非否認性 (Non-Repudiation)
  - その行為を実施したことを事後に否認できないように保証すること
- 信頼性 (Reliability)
  - 意図した動作と結果に整合性があること

真正性 （厚生労働省 :: 高度情報化社会推進諮問委員会）

- 真正性
  - 完全性
  - 信憑性
  - 追跡性
  - 非否認性
  - 信頼性
- 手法
  - 認証
  - 確定操作
  - 署名
  - ほか
- 残された問題
  - そもそものデータ（情報ソース）
    - 正確性　確実性
  - ほか

11-SEP-2006 ©1997-2006 Y.Hirose 62

見読性 （厚生労働省）

- 見読性
  - 機密性
  - 可用性
  - 信憑性
  - 追跡性
  - 非否認性
- 手法
  - 暗号
  - 認証
  - 属性認証と権限管理
  - ほか
- 残された問題
  - 臨床現場に即した妥当な権限管理
  - 自己制御権　と　コミットメント
  - ほか

11-SEP-2006 ©1997-2006 Y.Hirose 63

保存性 （厚生労働省）

- 保存性
  - 真正性
    - 完全性，信憑性，追跡性，非否認性，信頼性
  - 見読性
    - 機密性，可用性，信憑性，追跡性，非否認性
- 手法
  - 権限
  - ほか さまざま
- 残された問題
  - 長期保管 ということ
    - 偶然？の毀損
    - 媒体の物性と環境（湿度温度とその変化，磁場や光，汚染と揮発）
    - 媒体との物理的なインターフェイス仕様
    - ソフトウエア，ソフトウエアのファイル書式

11-SEP-2006 ©1997-2006 Y.Hirose 64

セキュリティ管理標準の種類

- 技術的対策
  - ISO/IEC 15408 ⇒ JIS X5070
    - CC : Common Criteria
      - Evaluation criteria for IT security
      - EAL：Evaluation Agreement Level
- 組織的対策
  - BS 7799 ⇒ ISO/IEC 17799 ⇒ JIS X5080
    - ISMS : Information Security Management System
      - 適合度評価
- 具体的手法
  - BS PD3000 ⇒ ISO/IEC TR13335 (GMITS)
    - GMITS : Guidelines for the management of IT Security
    - ISMS

11-SEP-2006 ©1997-2006 Y.Hirose 67

施策の経緯と法令と〔大きな流れ〕

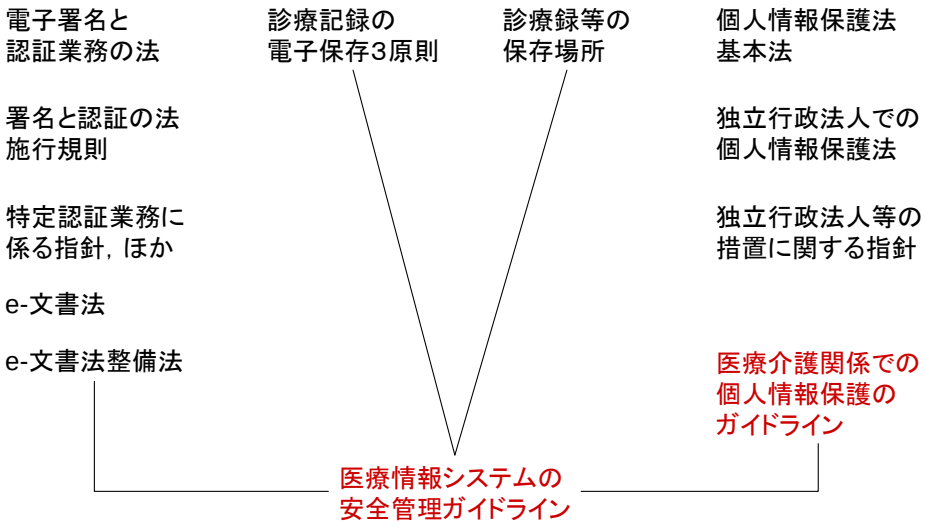
- 平成12年11月29日　高度情報通信ネットワーク社会形成基本法 成立
- 平成13年　1月　6日　高度情報通信ネットワーク社会形成基本法 施行

- 平成13年　1月　IT基本法に基づく IT戦略本部　の設置
- 平成13年　1月22日　e-Japan 戦略
- 平成13年　3月29日　e-Japan 重点計画
- 平成13年　6月26日　e-Japan 2002 プログラム
- 平成14年　6月18日　e-Japan 重点計画-2002
- 平成15年　7月　2日　e-Japan 戦略 II
- 平成15年　8月　8日　e-Japan 重点計画-2003
- 平成16年　2月　6日　e-Japan 戦略 II 加速化パッケージ
- 平成16年　6月15日　e-Japan 重点計画-2004
- 平成17年　2月24日　IT政策パッケージ-2005
- 平成18年　1月19日　IT新改革戦略
- 平成18年　7月26日　重点計画-2006

施策の経緯と法令と〔規格と指針〕

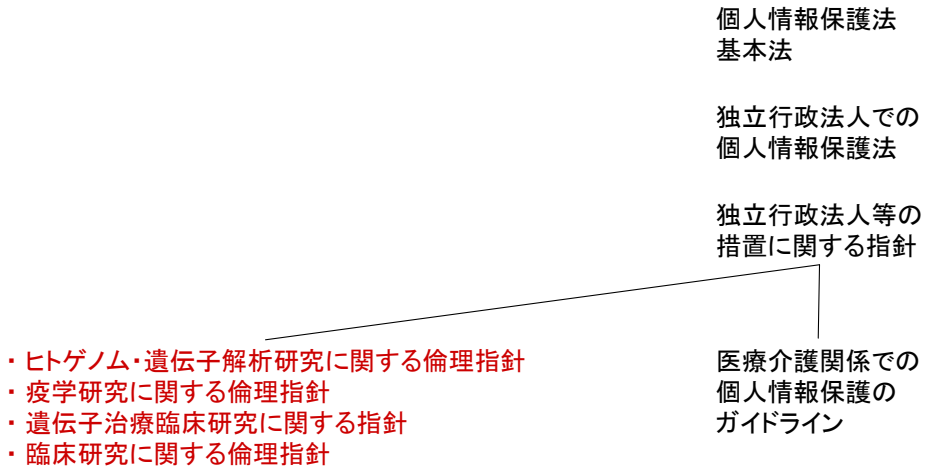
- ISO
  - ISO TS17090
  - ISO/IEC 15408 (CC)
  - ISO/IEC 17799 (ISMS)
  - ISO/IEC TR13335 (GMITS)
- OECD
  - OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
  - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Other examples
  - FIPS 140-2 197 171
  - PKCS #1 #3 #5 #6 #7 #8 #9 #10 #11 #12 #13 #15

施策の経緯と法令と〔概略：臨床業務〕



11-SEP-2006 ©1997-2006 Y.Hirose 16

施策の経緯と法令と〔研究に関して〕



11-SEP-2006 ©1997-2006 Y.Hirose 17

４．提言について

本WGが今年度第１四半期に提示した「厚生労働省医政局長宛の提言（案)」には，特段に改変すべきところはないと考えている．
法令等は国内外の時代潮流に即していないとは語りえず，法令もガイドラインもその中で最小限を求めるに留まっていることは前節を参照すれば明らかと思われるし，種々の開発言語においても必要となるライブラリは出揃っている．

なお前述の２節において述べた外部通信におけるパケット制御の仔細などについて，関係ガイドラインへの盛り込みを要請することについては，一応は可能ではある．とはいうものの，一つに，具体の技術要件は極めて短期間に変わりうること，そして今一つに，そのような指針こそ将に本部長会あるいは類する組織団体が社会貢献として発信すべき事項であると目されうるためである，その存在意義として．
したがって本WGとしては，そのような事項を要請するべきではないという立場をとる．

５．そのほか標記主題以外の若干の解説と助言

ごく掻い摘んだところを挙げておくに留める：

臨床業務
- 院外で編集したい　非対面診療となる＝違法性が高い
- 院外で見たい　完璧にセキュアなトラストチャネルを確立できるならば

臨床実習
- 利用目的　用途の事前提示と承諾
  - 症例に基づく教育
  - 監督下　合法かつ必要
  - 非監督下　違法性が高い
  - 院外搬出　匿名化しても原則禁止

臨床研究（診療情報を用いる研究）
- 利用目的　用途の事前提示と承諾
  - 症例に基づく研究
- 事業者内　連結可能ならば厳密な管理を要する：管理区域内で実施

であること・と・であることを説明（証明）すること・は異なる．

５節に関わる備考：

- 個人情報の定義と事例は関連法令に明記されているが，その要点は当該個人の識別可能性である．つまり，当該個人を識別しうる情報群が，当該情報塊に含まれているか否かである．なお大学等の研究機関が研究を行う際の根拠文書は各種研究等の指針となる．
- 個人情報は，当該個人の識別可能性が除かれることによって匿名化されうる．ただし，氏名・年齢・性別・住所等の削除範囲について，定型的一律処理のみで匿名化されたと目することは必ずしも妥当とは目されえない（例：離島僻地の患者情報等）．
- 匿名化（識別可能性の除去）と暗号化（分割を含む）とは異なり，暗号化されていても個人情報は個人情報である．暗号化のみでは第三者閲覧可能性の低減策を超ええない．
- 連結可能匿名化と連結不可能匿名化との差異は，匿名化情報の中に，当該個人を識別しうる情報群との連結可能性を確保する符号が残存しているか否か，による．
- 個人情報は事業者単位で認定される．同一事業者内において，一つの事業部門から他の事業部門へ個人情報が提供されるとき，これを第三者提供とは見なさない．
  なお同一事業者内における部門間提供においても，利用目的の限定ならびにその通知事実に基づいて妥当性が認定されうる．また通常は事前同意の範囲に照らして妥当性判断が為される．
- 事業者の一つの事業部門において個人情報と認定された情報塊は，当該事業者内の個人情報管理室で連結可能匿名化された後，当該事業者内の他の事業部門に提供された場合にも，これは個人情報として取り扱われる．
- 保有個人情報の取扱状況の記録
  関係指針の遵守ならびに関連法令等の趣旨の尊重は，もとより電磁記録に留まらない．電子計算機処理ならびに電磁媒体に係わる扱いの要点は次節に概覧を掲げておく．その他の媒体と処理については事業者内に整備すべき諸規程とその遵守状況の記録に依る．

- 事業者の，個人情報が格納された業務端末を帯出する場合には，通常の措置が施されているのみでは，保管可能性と追跡可能性が著しく減弱するか喪失するものと思われる．これらを可及的に確保するには，種々の複合した方策が必要となるものと思われる．
- 暗号化した個人情報を電子媒体に記録して帯出する場合，複合化後は，当該個人情報の善管可能性および追跡可能性を期待すること，およびその証明可能性を確保することは極めて困難であるものと思われる．

- 個人情報（非匿名化個人情報もしくは結合可能匿名化情報）を，個人が所有する端末に格納して帯出して解析編集等を実施する 法令や指針に抵触する（危険性が極めて大であり厳格な説明責任が求められる）
- 個人情報（非匿名化個人情報もしくは結合可能匿名化情報）を磁気媒体に格納して帯出して供覧に呈する等

当該事業者が特に認めた場合に限る

場合によっては事前に当該個人の同意を改めて得ておくことを要する

- 個人情報（非匿名化個人情報もしくは結合可能匿名化情報）を紙媒体に印刷して帯出し供覧に呈する等

当該事業者の許諾に依る

場合によっては事前に当該個人の同意を改めて得ておくことを要する

なお包括的な取扱状況記録等は許容されえず個別の記録が求められる

参 照：

- 電子署名及び認証業務に関する法律（平成 12 年 5 月法律第 102 号：平成 18 年 3 月改正）ほか関連する施行令，施行規則および省令
- 個人情報の保護に関する法律（平成 15 年法律第 57 号）
- 独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）
- 独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年 9 月総務省行政管理局長発通知総管情第 85 号）
- 医療情報ネットワーク基盤検討会 最終報告. http://www.mhlw.go.jp/shingi/2004/09/s0930-10.html.（平成 16 年 9 月）
- 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年 11 月法律第 149 号）ほか関連する整備法，施行令および告示等
- 厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令（平成 17 年 3 月厚生労働省令第 44 号）
- 医療介護関係事業者における個人情報の適切な取扱いのためのガイドライン（平成 16 年 12 月厚生労働省：平成 18 年 4 月改正）
- 医学研究における個人情報の取扱いの在り方に関する専門委員会：意見書の公表について（厚生労働省発表平成 16 年 12 月 24 日）別添：医学研究等における個人情報の取扱いの在り方等について
- ヒトゲノム・遺伝子解析研究に関する倫理指針（平成 16 年 12 月文部科学省・厚生労働省・経済産業省告示第 1 号）
- 疫学研究に関する倫理指針（平成 16 年 12 月文部科学省・厚生労働省告示第 1 号）遺伝子治療臨床研究に関する指針（平成 16 年 12 月文部科学省・厚生労働省告示第 2 号）
- 臨床研究に関する倫理指針（平成 16 年 12 月厚生労働省告示第 459 号）

ほか多数

以上