別紙４

研究成果の刊行に関する一覧表レイアウト（参考）

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
小尾高史 他4名	多機能ICチップを利用した任意多地点間VPNのための鍵交換手法	ワイヤレス・テクノロジーパーク2006講演予稿集		20-21	
大山永昭	IT新改革戦略における医療の情報化の概要	Japan Medical Society	5月号	53-54	
大山永昭	医療機関における個人情報保護とセキュリティシステム	日本病院会雑誌	53巻10号	118-136	
押田知己 他5名	多機能IC チップを利用したネットワークサービスにおける暗号技術の更新とサービスの継続利用の実現	電子情報通信学会2007年総合大会講演予稿集		230	
浦野雄平 他5名	多機能IC チップを利用した任意多地点間VPN における通信主体情報の秘匿	電子情報通信学会2007年総合大会講演予稿集		225	
山本隆一	遠隔画像診断のセキュリティと個人情報保護	Rad Fan	5巻1号	18-19	
山本隆一	電子カルテとプライバシー保護	日本医師会雑誌	135巻9号	1954	

多機能 IC チップを利用した任意多地点間 VPN のための鍵交換手法

New key exchange protocol for the On-Demand VPN using the smart IC chip

○小尾高史　鈴木裕之　谷内田益義　山口雅浩　大山永昭

(Takashi Obi　Hiroyuki Suzuki　Masuyoshi Yachida　Masahiro Yamaguchi　Nagaaki Ohyama)

東京工業大学大学院 (Tokyo Institute of Technology)・

総合理工学研究科 物理情報システム専攻 (Interdischiplinary Graduate School of Science and Engineering , Department of Information Processing)

〒226-8503・横浜市緑区長津田町 4259-G2-2・電話 045-924-5482／FAX 045-924-5482

Yokohama MidorikuNagatsutacho 4259-G2-2 226-8503

E-mail:obi@ip.titech.ac.jp

1. はじめに

近年、インターネットを専用線と同様に利用できる VPN サービスが大きな広がりを見せている。しかし、VPN の構築には利用者にネットワークの専門知識が必要なうえ、設定などを間違うと情報セキュリティ上多大な影響が発生する恐れがあるなど、誰もが容易に設置できる状況に至っていない。このような背景の下、VPN の状態管理を行う VPN 管理機関と 2 階層 PKI に対応した IC チップが搭載された通信機器を用いて、利用者の要求に応じて認証鍵などの VPN 構築に必要な設定情報を、ネットワークを介して安全に配送し[1]、任意多地点間で直ちに VPN を構築するオンデマンド VPN(OD-VPN)技術の研究開発[2]が進められている。

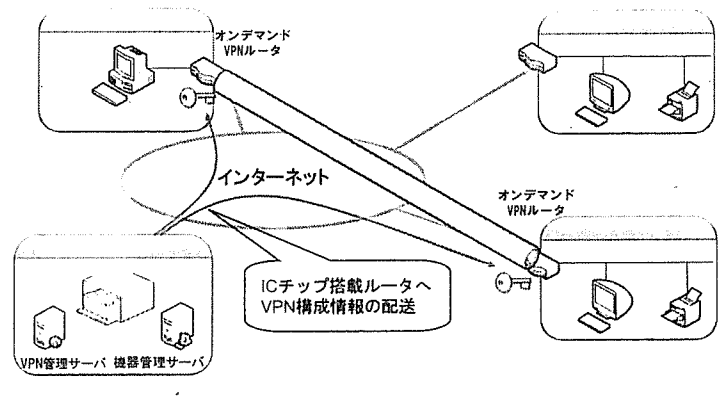


図 1. オンデマンド VPN

現在の OD-VPN（図１）は、IPsec を利用した暗号通信を行っており、そのための鍵交換手法としては、Pre-Shared Key を利用した IKE（Internet Key Exchange）を用いている。しかし、Pre-Shared Key を用いる場合、同じ通信機器においても VPN 通信路毎に異なる鍵を設定する必要があり VPN 管理機関における鍵管理が煩雑になることや、通信機器が異なる VPN 管理機関に属していた場合の鍵生成・情報共有を実現する手法が明確になっていない等の課題がある。本研究では、IKE プロトコルで用いられるデジタル署名認証方式をベースとし、機器に組み込まれた IC チップの利用と属性証明書を用いた接続権限管理とを組み合わせた鍵交換手法を提案する。さらに提案手法を用いて、異なる管理機関に属する機器間で容易に鍵交換が実現できることを示す。

2. 接続許可証を利用したデジタル署名認証ベースのオンデマンド VPN 鍵交換手法

OD-VPN では、ルータ間で IPsec による VPN を構築するために、機器相互の ID や鍵情報などを用いて IPsec-SA を確立する必要があり、現在は、IKE における Pre-Shared Key を利用した鍵交換を採用しているが、このために VPN 通信路毎に異なる鍵が必要となることや、複数の VPN 管理機関間で VPN 通信のローミングサービスを実施する場合の鍵漏洩の危険など、Pre-Shared Key をどのように管理、配送

するかが新たな課題となる。これに対して、本研究では、接続許可証を用いた接続権限管理を組み合わせた新たな鍵交換手法を提案する。

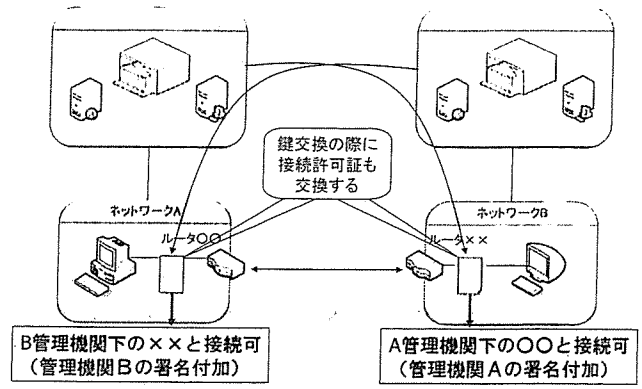


図２．提案手法

まず、デジタル署名認証方式を用いるためには、秘密鍵およびそれに対応する VPN 管理機関が発行した公開鍵証明書が必要となる。OD-VPN においては、VPN接続の可否をVPN管理機関が制御することになるため、提案手法でも IKE 時に必要となる公開鍵証明書の配送を VPN 管理機関が行うものとする。ここで、提案手法では、公開鍵証明書の検証を、各 VPN 管理機関が実施した上でセキュアチャネルを利用して IC チップに配送するため、IC チップ上で複数の CA の公開鍵証明書の検証を行う必要性はない。同時に、ルータを管理する VPN 管理機関 A は、ルータ A への接続許可証を発行し、VPN 管理機関 B へ送付し、VPN 管理機関 B から管理下にあるルータ B へ送付する(図２)。この接続許可証により接続許可の判断や異なる VPN 管理機関へのアクセス権限などを制御する。鍵交換時には、ルータ間でさきほどの接続許可証を交換し、接続許可証の内容のチェック及び署名検証を行う。仮に、ルータ A 及び B で VPN 管理機関が異なる場合でも、接続許可証の署名検証は自己が属する VPN 管理機関の公開鍵により行うため、IC チップ上で複数の CA の存在を意識する必要はない。提案手法では、接続許可証として公開鍵証明書に対応する属性証明書を用いることを想定している。これは、VPN 管理機関発行の属性証明書の送付要求及び証明書送付を Certificate Request ペイロードを利用して送付することが可能なため、従来の ISAKMP パケットの構成と機能をそのまま利用可能であり、既存の鍵交換プロトコルを変更することなく、実現が可能なためである。

3. 検証システムの構築

提案手法の有効性を確認するために、VPN 構成情報配送後からの IPsec 用の通信路暗号鍵交換部分までについて実装を行った。２台の機器(パソコン)にそれぞれ実際の IKE に則った機能を実装し、提案手法の検証システムを構築した。今回は実装の都合上、ルータ上ではなく機器上にデジタル署名認証機能・接続許可証の送付・検証・権限確認機能等を実現し、シミュレートソフトという形で鍵交換機能を実装した。この検証システムにおいて接続許可証の検証（図 3）および記載されている接続権限の確認、さらに VPN 接続で使用する通信路暗号鍵が共有されていることを確認した。

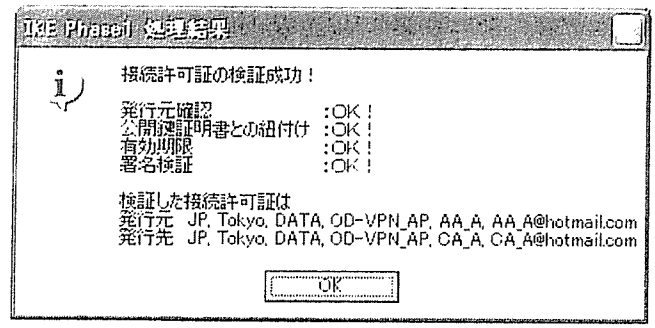


図３．接続許可証検証結果表示結果

4. まとめ

オンデマンド VPN のための鍵交換手法として、デジタル署名方式による IKE 認証方式をベースとし、接続許可証を用いて接続権限や異なる VPN 管理機関間での接続を制御する新たな鍵交換手法を提案し、検証した。今後の予定として、接続許可証の権限管理部分の詳細や異なる VPN 管理機関間の通信方法について検討が必要と考えている。なお、本研究の一部は，総務省の委託研究「高度ネットワーク認証基盤技術の研究開発」により行われた。

参考文献

[1] 小尾高史　他：「オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤」,電子情報通信学会(2004)

[2] 釜仲　他：「機器の認証に基づく安全なＶＰＮ構築技術の提案」，2004-CSEC-27, 情報処理学会(2004)

IT新改革戦略における医療の情報化の概要

大山永昭　東京工業大学フロンティア創造共同研究センター教授

全省庁でシステム改革・業務プロセスの見直し

IT戦略本部有識者本部員を務める大山教授はまず、平成十八年一月に公表されたIT新改革戦略について触れ、その基本理念として、①少子高齢化を迎えたことによる社会的な様々な問題を解消支援していくこと、業務プロセス等の簡略化と最適化のための構造改革による飛躍、②安全性と利便性の両立、国民主体の問題解決環境の整備に代表される利用者・生活者の重視、③ユビキタスネットワーク社会の実現による国際競争力の強化・国際貢献などを挙げた。

大山教授は、現代における様々な社会的問題点の解決策として『全体最適化』の必要性を説き、「たとえば現在社会保険庁のシステム改革に携わっているが、現在一千百億円かかっている管理運営費について、システムを入れ換えることで約三百億円削減できる」と指摘。「国家全体で考えても、年間一兆円かかっている管理運営費についても同様にシステムを入れ換えることで一千億円コストダウンできる。損益分岐点は五年後ぐらいになるが、五年先には、われわれは自らの情報を的確に把握し、自ら考えることのできる知的社会を実現していかなければならない。そのためには今のような年金制度、保険点数制度とは異なる分かりやすくシンプルで、さらに透明な制度を構築すること、そして全体最適化のためのグランドデザインが必要だ」とした。また、全体最適化の一環として政府が積極的に推進している電子政府について触れ、「たとえば確定申告などのように申請・申告は96%の割合でオンライン化しているが、実際にはその利用率はわずか0・6%に過ぎない。今後はこの利用率を向上させ、二〇一〇年までには50%を目指さなければならない」と述べた。さらに、電子政府推進の中で現在注目されているPMO（Program Management System）について触れ、「現在、全省庁においてシステムの棚卸しとPMOの設置が進んでいる。PMOとは、全体最適化するために必要なシステムの運営状況を検討する部署。現状では、システムの全体を理解している人間が誰もいない。これは厚生労働省だけではなく、他の省庁も同じ。これまで二年間の間に八十近いシステムを見てきたが、どこもみなシステムが完全に縦割りになっていて、お互いに何をしているのか分かっていない。どのシステムがどれくらい能力を持ち、どういう情報を扱えるのか、そのセキュリティレベルがどうなっているのか、各省庁の中でも把握されていない」と述べ、システムの刷新・統合・廃止等による業務プロセスの見直しの必要性を説いた。

大山永昭　東京工業大学フロンティア創造共同研究センター教授

次に、話を保健・医療・福祉分野の情報化に移し、その目的として、サービスの質の向上、地域格差の是正、新たなニーズへの適応、トータルコストの削減などを挙げた。ただし、諸外国とは制度的な違いがあることから、外国の手法をそのまま導入することは困難であること、そして一部の医療機関だけで行えるものではなくすべての医療機関が採用できるものでなければならないために、かえって競争環境をつくることが困難であることなどを留意点として掲げた。また、IT戦略本部で出された医療分野の情報化における達成事項について、①レセプトのオンライン化による事務経費の削減と予防医療への活用、②個人が生涯を通じて健康情報を利活用できる基盤づくり、③効果的なコミュニケーションの実現、④医療情報化インフラの整備、⑤情報化推進体制の整備とグランドデザインの策定、の五つを挙げた。

医療分野の情報化の現状について「電子政府は行政機関のネットワーク化が済み、いよいよ実稼働に向けてサイバー空間における窓口の開設やオンラインによる受付などのサイバー空間での拡張に移行しつつあるが、医療分野においてはようやく電子カルテシステムやレセプトが導入されるようになり、現在医療機関のネットワーク化を図っている段階」と指摘。今後は、強固なネットワークを組むためにも、たとえばレセプトにおいても、途中で紙を用いることのない一貫した電子化の必要性を強調した。

また、大山教授は、政府が電子政府化を、医療

分野が情報化を果たす上で、年金の納付状況、変更手続き、また検診結果、レセプト、カルテなどの保健医療情報等、本人が自らの個人情報を管理するために必要な本人確認についても言及した。「情報化が進展しているにもかかわらず、社会保障サービス等を受けるために、現状のように本人確認を何枚ものカードで行うのは無駄。一枚のカードで済ませるべき」と説き、そのためのICカードの大規模導入の必要性を強調した。

世界の状況と我が国における医療の情報化の方向

田中博　東京医科歯科大学
情報医科学センター教授

医療IT化に対する経済的インセンティブ

田中教授は、冒頭、「医療の質の向上、安全性の向上、医療費抑制のための医療のIT化に向けた政策は、日本に限らず、世界同時的に動き出している」と述べ、英国、米国等世界各国の医療IT化への状況を取り上げて説明した。

次に、医療IT化の経済評価について、「相互連携型電子カルテ（EHR）の構築経費は試算では三兆円だが、それに対して、生涯電子カルテによる医療費節減効果は五兆円以上」と述べ、電子カルテを導入することによる経済効果を強調。またそれ以外にも経済効果の裏付けとして、①EHR導入による医療費の削減効果は年約十三兆円、②EHRを広範囲に導入することにより毎年の医療費が7・5～30%減少する、③ITの普及に伴う利益は年に一千六百二十億ドルに及ぶ、といった米国の研究結果を報告した。

田中博　東京医科歯科大学情報医科学センター教授

また、医療情報化を進展させ医療資源を効率的に運用することができれば、現在の日本国民一人当たりの外来受診回数八・三回／年、平均入院日数二十五・二日も減少できることについて触れ、「外来受診回数は米国に比べるとやや少ないが、欧州諸国と比べる多い。仮にフランス並み（六・九回）に減らすことができれば一兆二千億円の医療費を削減可能なはず」と指摘。さらに、かなりの数の重複診療があるとされる老人医療について「どの程度行われているかをチェックする手段は今のところ存在しない。電子カルテネットワークが実現すれば実態把握も可能になる。仮に外来受診を四割削減できれば、総額で二兆円程度の医療費を節約できるはず」と説いた。

その他の経済効果は以下のとおり。

・画像診断

診療所や中小病院が保有しているCT、MRIは総じて性能が低く、結局は大病院で撮り直す場合が多い。当初より大病院で撮影し、ネットワークで閲覧できるようにすれば約千五百億円を節約できる。

・ペーパーレス・フィルムレス

三百床以上の病院では、紙のカルテとフィルムの保管・運用に年間一億円以上を費やしている。電子化によって総額約一千億円節約できる。

・循環器官関係（心臓病、動脈硬化、脳卒中等）の慢性疾患

これらの慢性疾患には年間約十兆円の医療費が費やされている。電子カルテネットワークの普及により、その二割を予防できれば総額二兆円の医療費を節約できる。

田中教授は、二〇〇一年、医療情報システム構築のための達成目標を設定した「保健医療のIT化のグランドデザイン」、世界最先端のIT国家を目指した「e-Japan戦略」、わが国の医療IT化政策を盛り込んだ「e-Japan重点計画」というこれまで実施されてきた医療IT政策の経緯について振り返り、わが国における医療IT化の現状について、「電子カルテは四百床以上の病院の14%で稼働している。オーダリングシステムは百床以上24・3%、五百床以上66・3%と大中規模病院で稼働率が高い」と述べた。しかし、その一方で、「保険支払者、ITベンダー、医療供給者間で電子カルテシステムを導入することに対する経済的インセンティブが持てないために二の足を踏んでいる状況にある」と医療のIT化を達成する上で現状の問題点を指摘。「今後は、医療ITの経済評価をしっかりともち、設備投資のコストもかかるが、戻ってくるお金も大きくなる、循環させることにより、医療だけではなく、それを取り巻く産業及び国民生活も豊か

〈平成17年7月・東京都〉

トピック

医療機関における個人情報保護とセキュリティシステム

東京工業大学大学院理工学研究科附属 像情報工学研究施設 教授　大山　永昭

今日は「医療機関における個人情報保護とセキュリティシステム」という内容でお話をさせていただきます。

私は，ドクター論文からずっと画像関係の仕事をしてきましたが，いわゆる電子カルテなどの医療情報の電子保存も研究してきました。現在は，IT戦略本部のなかで次期の「e-Japan戦略」を考えています。現在の「e-Japan戦略Ⅱ」は2005（平成17）年度で終了になるので，来年度からの新しい戦略の策定を開始しています。このなかで私は，主として電子政府と医療のパートを担当しています。皆さまから，いろいろなご意見をうかがい，国の戦略に反映したいと思います。

IT化の現状

（スライド1）最初に，e-Japan戦略の流れをざっと見てみます。e-Japan戦略は，2000（平成12）年に起草された「e-Japan戦略：2001」（発効は2001年）から始まっています。次が「e-Japan戦略Ⅱ」で，これは2003年からです。

IT化の現状

- 「e-Japan戦略：2001」　インフラ整備
  - 高速通信；3000万世帯
    超高速通信；1000万世帯
    平成15年度までに電子政府を構築
- 「e-Japan戦略Ⅱ」　インフラの利活用
  - 安心、元気、感動、便利なIT社会の構築
    医療、食、電子政府など7分野の例示
    情報システムのセキュリティ技術の開発支援
    知的財産の流通促進　等

スライド1

今までの動きを見ると，「e-Japan戦略：2001」ではブロードバンド，超高速ネットワークを含めた「インフラ整備」が行われました。ここ数年間でインターネットの利用環境が劇的に変わったのは皆さんご存じと思います。これもⅠつは，e-Japan戦略のなかでインフラ整備を国が積極的に進めたという背景がありました。

このインフラ整備は，予想以上に早く達成したこともあり，「e-Japan戦略Ⅱ」が2003年に出されました。ここでは「インフラの利活用」が主課題で，できあがったネットワークをどう使うか，言い換えるとICT（Information and Communication Technology）の利活用が中心テーマでした。

今の内閣官房長官の細田さんが，当時，IT担当大臣でした。スライド中に「安心，元気，感動，便利」とある4つのキャッチフレーズですが，当初は「安全，安心，そして便利」でした。それを細田IT担当大臣が「これからは少子高齢化になるけれども，社会を元気にしなければならない。そして社会に参画することで，自ら感動できるんだ」ということを言いまして，「安心，元気，感動，便利」に変わったという経緯があります。私はこのe-Japan戦略の「2001」と「Ⅱ」の両方の起草に携わりました。

今実施されているe-Japan戦略Ⅱに記されたアプリケーションのなかのトップが“医療”でした。

（スライド2）e-Japan戦略の基本理念は，このスライドにあるように，もともとは民間主導，政府による環境整備でした。すなわち，ITあるいはICTを使ったさまざまな新しいビジネスの創出や企業におけるICTを武器としたBPR（Business Process Re-engineering）の実施などのいろいろな応用を民間が行い，政府はその環境を整える，という役割分担です。

これをたとえ話にすると，民間がビジネスの種をまくので，その種が芽を出し成長して実を付けるように，国が環境を整えるというのが官・民の役割分担でした。環境整備というのは，具体的には規制緩和，法律の改正，制度の見直しなどを意味します。

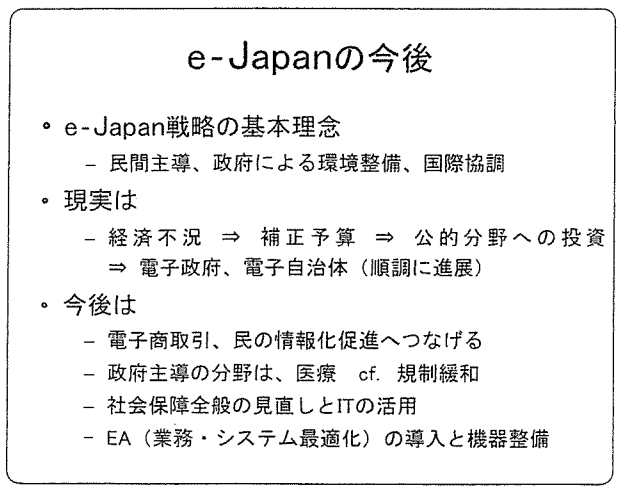
このような流れだったのですが，ご案内のように日本経済はここ何年もの間，ずっと不況が続いて補正予算が組まれました。その結果，昔ですとハコ物に予算が投入されたのですが，ICTの分野は将来性がある，社会資産あるいは社会資本としても価値があるという判断から，公的分野へのIT投入が開始されました。その結果，電子政府，電子自治体の構築が進展したという状況にあります。

あまり実感がないかもしれませんが，数字上は，2005年度内に政府に対して提出する申請・申告書類の96%はオンラインでできるようになります。受け入れ側はそこまで行っているのですが，利用率は残念ながらまだ上がっていません。税金の申告等をオンラインでやったことがある人やパスポートの申請は，すでにオンラインでできるようになっています。

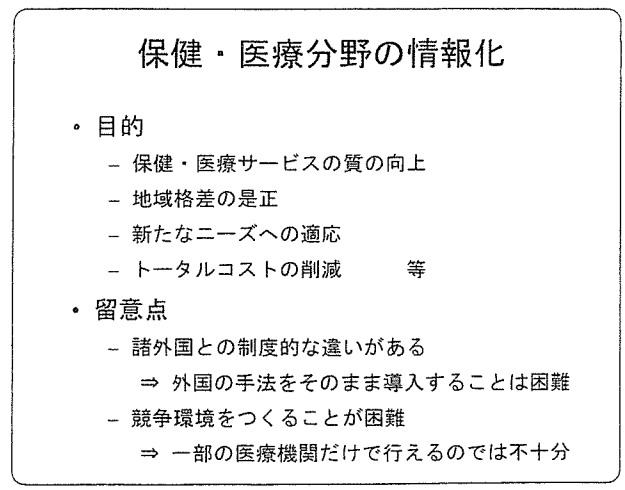
したがって，電子政府は，構築のフェーズがほぼ終わりで，2006年度以降は実稼動という話になっています。このことからも，次の政府主導分野は医療になるだろうと予測されます。ですから，2006年度からの次期戦略では，医療がトップに上がるのではないかと予想されます。

「社会保障全般の見直し」というのは，人口構成が変わってきたことに起因しますが，ICTは経営の武器ということがあるので，これを使っていかに社会保障全体をうまく回すかという問題が議論されています。医療保険制度の改革もこの（2005年）秋をめどにして方向性が出てくると思います。そういう意味では医療界，あるいは医療に関連するビジネスをおやりの皆さまにとっても，大きな変化が来るかもしれません。

（スライド3）本当は保健・医療・福祉まであるのですが，長くなりますので2つにしました。「保健・医療分野の情報化」というのは，以前から厚生労働省のグランドデザインにも書いてあるとおり，「保健・医療サービスの質の向上」，「地域格差の是正」，さらには「新たなニーズへの適応」，例えば24時間どう緊急に対応するのかとい



スライド2



スライド3

ったことが目的とされています。ただ，ここへきてやはりさまざまな観点から「トータルコストの削減」ということが出始めました。例えば年間医療費は現在30兆円超かかっています。一方，電子政府関係は中央政府で年に約１兆円です。中央政府１兆円に対して，今，古いコンピュータから新しいコンピュータに入れ替えて，システムを効率化していくことで年間1,000億から2,000億円浮くのが見えています。こういった対応は，今日のテーマと違いますので詳しくは説明しませんが，大幅な経費削減の効果があるということが予測されています。

30兆円は，医療費そのものですから，コンピュータを入れ替えれば下がるというものではありません。しかし，事務経費を含めたキャッシュフローをうまく動かせば，トータルの経費が下がるかもしれません。これが，レセプトオンライン化の話が出てきている理由の１つであると思います。

医療の情報化を進めるうえでの留意点をまとめます。医療には「諸外国との制度の違いがある」ので，外国でうまくいっている方法をそのまま持ってきてもなかなかそうはいきません。

さらには「競争環境をつくることが困難」があげられます。すなわち医療は公平・公正が基本ですので，ある地域やある病院の系列だけができるのではなく，すべての医療機関がうまく対応できる仕掛けをつくることが必要です。情報化を進めるときもこのことを念頭に置かなければならないと思います。

個人情報保護について

個人情報保護の話はご存じの方も多いかと思いますが，一部思い出していただくために整理します。

個人情報の保護は，1999（平成11）年から，内閣の高度情報通信社会推進本部個人情報保護検討部会により，その検討が開始されました。その後2005（平成17）年４月１日に個人情報保護法として全面実施されました。私もこの検討部会に参加していましたので，この法律の考え方の基本をまとめてみます。

（スライド４）OECDの８原則はもうご存じと思います。現在は，「知られたくない」だけではなく「自己情報のコントロール権」になっています。「EU指令」についてはまだEU内でばらつきがありますが，その考え方は，分野によって分け隔てなくすべての分野にかける包括法の整備です。そして，それぞれの国に個人情報保護を監督する機関を設置するというようになっています。監督機関というと日本では金融監督庁があった（現在は金融庁）ので分かりやすいかと思いますが，それぞれの企業や団体に対して，個人情報の扱いが不適切であると監督機関が判断すると，改善命令が出されて，最終的には業務停止命令を行うというものです。これは法律としては非常に厳しいやり方であると思います。

それに対して従来の日本（2005年４月１日以前の日本）と米国では，分野法と自主規制というやり方で進んできました。現在の米国の医療分野にはHIPAA（Health Insurance Portability and Accountability Act）という分野法があります。

自主規制が機能するのか，あるいは法律でなければならないのかというようなことが，個人情報保護法を起草するときの議論の焦点になりました。法律をつくるとどういう効果があるのか，どういう効力を持つのか，この辺の整理が検討会により行われ，その結果，日本では「基本法と自主規制の組み合わせ」という結論に至っています。

個人情報の保護について

- 知られたくないからコントロール権へ（OECD８原則）
- 包括法と監督機関（EU指令）
- 分野法と自主規制（米国、従来の日本）
- 基本法と自主規制の組み合わせ（H17.4.1から）
- 対策
  - 組織的対策（自主規制）と制度的対策（法律）の組み合わせ
  - 技術的対策は、保護の具体的な手段、説明責任を果たす
  - 利害得失、特性等を十分に考慮

スライド４

組織的な対策の代表例は自主規制で，制度的な対策は法律などを意味していますが，これら2つの対策で個人情報を保護します。3つ目の対策である技術的なものは，保護を実行するための具体的な手段であって，管理責任を持つ事業主や個人が，個人情報をしっかり保護していることに関する説明責任を果たすのに役立てるという位置づけになります。これらの対策には利害得失や特性があるので，そこを十分考慮して最適な組み合わせを用いることが必要です。

スライド5に，今の一般論との関係がまとめられています。まず，議論のなかで重要なことは，自主規制と法規制が利くのか利かないのかを整理することです。別の言い方をすれば，自主規制だけでは価値がないのかという逆の質問になります。

自主規制は一般的に，「社会的な信用を重要視する個人・組織には有効」といえます。別の言い方をすると，法律をつくって罰金を課したとしても，それ以上の被害を受けることがあるということです。具体的には，例えば「あの会社はどうも顧客の個人情報を漏らしているぞ」，あるいは「いい加減に扱っているぞ」という話が，もし世間に流布されたらどうなるかということです。きっと，その会社や組織は「とんでもない，そんなことを言われたら自分たちの商売に影響する」と思うでしょうから，法律の有無に係わらず個人情報の取り扱いには十分に気をつけると考えられます。すなわちその方たちには，例えば50万円の罰金よりもはるかに大きな社会的な制裁が加わるので，罰金があってもなくても，それ以前にきちんと個人情報保護をするということです。

ただし，社会が個人情報保護を強く要望する状況では，きちんと保護しているところと不十分なところを区別することが極めて困難になります。そのために，第三者による監査を実施し，プライバシーマークの付与を行うようになりました。このプライバシーマークを持っているということは，そこの企業・組織は，しかるべき個人情報保護を適切に行っているということが，監査によって確認されているということです。ですから，皆がプライバシーマークを取っていただければ，結果として自主規制が十分うまく機能するだろうと考えたわけです。

個人情報の保護について

- 自主規制と法規制の効果
  - 自主規制が有効に機能する対象
    - 社会的な信用を重要視する個人組織には有効
    - 罰金よりも大きな被害を被る
    - 第三者監査の実施とプライバシーマークの付与
  - 法規制が有効に機能する対象
    - 社会的な信用を重要視しない個人組織に対して有効
    - 民事訴訟における心証を変える ⇒ 努力義務違反

スライド5

第三者監査を行うためには当然，どうやるかという問題があります。これについては現在，実際にはJIPTEC（日本情報処理開発協会）が対応しています。さらに医療関係においても，プライバシーマークの付与についてはMEDISなどが対応を始めているという状況です。

これだけですと，自主規制だけで十分で，もう法律はいらないという話になるのですが，実際には法規制が有効に機能する対象を無視できませんでした。どういうことかというと，当然のことながら，世の中には社会的な信用を重要視しない個人・組織が存在し，それらには自主規制が機能しないからです。一方，個人情報保護に関する訴訟は民事で，刑事にはしないという考え方がもう1つの重要な点でした。

（**スライド6**）なぜ民事になったのかを説明します。まず「個別の個人情報の重要性は人により異なる」，この点がポイントです。すなわち，例えばここに私の時計があるとします。この時計をだれかが私の許可なしに持ち去ったら窃盗です。盗んだこと自体で「この人は悪い」と皆が客観的に判断できるので，刑事罰である窃盗罪が適用できます。しかし，個人情報の場合はそのように単純ではないということです。

小さい頃を思い返すと，例えばテストを受けて，

残念ながら30点あるいは20点しか取れなかったとします。それを友だちのなかには面白がって漏らす人がいました。そうすると言われた本人は，平気な人もいるかもしれないし，傷つく人もいます。一方，テストで100点を取ったときは自らしゃべっている人もいます。ほかの人が言ったら喜ぶ人もいます。これこそ，だれが何点を取ったかですから個人情報です。これでお分かりのとおり，同じ個人情報でも人によって重要性が違っていますので，同じ「個人情報を漏らした」としても窃盗罪のように扱うことができなかったということです。このような考え方から，民事訴訟が原則で刑事罰ではないという判断になりました。

一方，日本の裁判制度は裁判官の自由心証主義になっています。具体的には，例えば私が個人情報の漏洩を訴えたとします。このような場合に裁判でどうなるかというと，私は原告で，被告に対して「あなたがこういうことをしたから私はこれだけひどい目に遭った。それに対して損害賠償を求めます」という訴えになります。これが基本です。裁判官はどうするかというと，訴える私に，「どこまでひどい目に遭ったのかを証明しなさい」と言います。通常はこういう流れになると思われます。

この場合，個人情報保護で法規制が有効に機能するためには，こういう社会的な信用を重要視しない相手に対しては，もし被害者が社会的に弱い立場の人であったらなおのこと，「あなたが悪い」ということを立証するわけですから，これは大変です。そこで，基本的に努力義務を皆に課すのがいいのではないかと考えたのです。これが基本法にしようという考え方でした。基本法ができれば，今度は同じ民事訴訟でも，「あの人は個人情報保護の努力義務を全うしていない，だから私も被害を受けたのだ」という言い方ができます。これに対して裁判官は，被告人に「こういう訴えがあるけれども，個人情報保護という法律があって，これに照らし合わせてあなたはしっかりと法を重視しているかどうか見せなさい」という言い方ができると予想されます。もちろん挙証責任とまでは言えません。しかしそれで裁判官の心証が変わる可能性があると期待したわけです。

個人情報保護法は，個人の情報の利用を妨げるためにつくったわけではありません。個人の情報を利用することで，莫大な便益が生まれることもあります。例えば電話で宅配便へ電話すると，番号を伝えるだけで住所が出てきます。これは便利になっています。こういうことをできないようにするために，個人情報保護法をつくったわけでは決してないということです。この考え方がちょうど道路交通法と同じであるということです。車は不幸にして事故が起きることがあります。しかしながら車のもたらす便益を無視して，直ぐに社会的に車の利用を禁止することはできません。だから道路交通法をつくって，それによってより安全確実な車の運行を実現するようにしてきたわけで，個人情報保護法もその意味では同じです。

では被害が出たらどうするのか。これはこの法律ではなく別の救済手段を考えるということで，整理されています。

議論としてここまで来るのに１年ほどかかりました。

結果として，「個人情報を大量に扱う事業者には，行政罰を適用」となりました。罰金の話が出てきました。ここの「大量に」というところがけっこうもめました。結果として5,000件となっています。個人情報を5,000件以上持つとこの行政罰の適用対象になるわけです。なぜ5,000件なのかということに対しては，私が知る限り明確な答

個人情報の保護について

- 個人情報保護法の役割
  - 個人情報の利用を妨げるのではなく、安全・確実な利用を可能にするためのルールづくりが必要
    ⇒ 道交法と基本的に似ている
  - 個別の個人情報の重要性は人により異なる
    ⇒ 民事訴訟が原則 ⇒ 刑事罰ではない
- 個人情報を大量に扱う事業者には、行政罰を適用

スライド6

えは分かりません。

（スライド7）このような流れで個人情報保護法はできたのですが，その後，医療分野がどうなったかについて紹介します。個人情報保護法には例外規定がいくつかあります。例えば研究や教育，それから報道の関係はもともと憲法によって自由が保障されていることもあって，個人情報保護の対象にならないなどいろいろな例外がありました。ただ，一方では個人情報保護法を実施することに関して，参議院と衆議院の両院で付帯決議がされています。すなわちこの法律をつくる場合には，ほかの機微にわたる情報を扱う分野，具体的には医療や与信情報等ですが，こういったところについては分野法をつくるということも含めて，検討すべきと書いてありました。

結果として，それを受けて厚生労働省が対応したのが，その後の「個人情報保護のガイドライン」になっています。我々はこの基本法をしばしばクレープ法と呼んでいました。クレープというのは食べるクレープです。お分かりと思いますが，クレープは薄く広げて作ります。薄くすると，直ぐに焦げたり，ちょっとヘマすると穴が開いたりします。クレープ法というのは，広く薄くまず網をかけるという意味です。ですから弱いところについては，トッピングをするという考え方必要になります。もちろん，取り扱う情報が機微にわたる医療分野においてはトッピングが必要と考えていました。

医療分野の特性としては，個人の利益と公の利益の二面性があげられます。公益の面では医学研究，公衆衛生などいろいろとあります。医学研究は，もともと研究だから個人情報保護の対象外にあたります。しかしながら臨床となると，今度は保護の対象になります。

しかしながら現実には，研究と臨床の現場はどこで線が引けるかという問題が生じます。こちらは研究，こちらは臨床という線をはっきり引けるかといったときに，公益性，患者さんの利益を含めて，やはりグレーゾーンがあると思います。

したがってここはどうしても何らかのかたちでガイドラインを出して，現場の方々に理解いただく必要があるという考え方から，この基本法に加えてガイドラインが策定されました。これがちょうどトッピングの話になっているわけです。

このガイドラインは，2004（平成16）年12月24日，東大の樋口範雄先生が座長で，私が座長代理を務めたのですが，その当時はもう何としても平成16年12月中に，年度でなくて平成16年中に出

保健・医療・福祉分野における個人情報の保護について

- 取扱う情報が機微である ⇒ 安全性の強化
- 留意点
  - 個益と公益の２面性
  - 医学研究、公衆衛生など
- 基本法に加えてガイドラインの策定
  - 厚生労働省医政局長、厚生労働省医薬食品局長、厚生労働省老健局長から都道府県知事に向けた通知（平成16年12月24日）

スライド7

ガイドラインの概要

1. 利用目的の特定等（法第15条、第16条）
2. 利用目的の通知等（法第18条）
3. 個人情報の適正な取得、個人データ内容の正確性の確保（法第17条、第19条）
4. 安全管理措置、従業者の監督及び委託先の監督（法第20条～第22条）
5. 個人データの第三者提供（法第23条）
6. 保有個人データに関する事項の公表等（法第24条）
7. 本人からの求めによる保有個人データの開示（法第25条）
8. 訂正及び利用停止（法第26条、第27条）
9. 開示等の求めに応じる手続及び手数料（法第29条、第30条）
10. 理由の説明、苦情対応（法第28条、第31条）

スライド8

すという期限があったために，24日のクリスマスイブのプレゼントみたいになりました。月に2回くらいずつ研究会を開催していたという記憶があります。

具体的なガイドラインの概要はもうホームページにも出ていますし，ほかの先生方も紹介なさっていると思います。今お話ししたような背景から，このガイドラインが出てきていることをご理解いただければと思います。

（スライド8）ガイドラインの概要はここにありますが，この右側が個人情報保護法の何条に対応しているかということです。これが1から10まで条文に従って説明してあります。医療の特質というと，例えば個人情報保護の一般法では，亡くなった人は対象になっていませんが，こちらは遺族がいらっしゃるので対象になっている，というような違いがあります。

さらには先ほど触れた医学研究と臨床との関係などについて，詳しく書いてあるのがこのガイドラインです。

（スライド9）次に，社会保険庁の関係をお話ししたいと思います。

ご存じのように医療保険は，健康保険組合，政府管掌保険，国民健康保険の3つに分かれています。社会保険庁のさまざまな問題が指摘され，解体的な出直しをするという観点から，社会保険庁は年金業務と医療保険（政府管掌保険）を切り離すことになりました。これはすでに決定されています。いつからかというと平成20年になりますが，都道府県のレベルで運用される予定です。一方で，社会保障制度全般の改革の話が進んでいますが，国民健康保険についても今の市町村から都道府県レベルに移行される可能性が出ています。こうなると保険者は，公のものは都道府県レベルになり，あとは民間の健康保険組合となるわけで，このような大きな変化が始まっています。

なぜ動いているかは，先ほども触れた業務コストの削減などいろいろありますが，そういったことに，いよいよこの分野も入っていくということをご理解いただきたいと思い簡単に紹介しました。

電子政府の動向

（スライド10）電子政府の実現と医療分野の情報化はある意味で，すごく似ていると思います。

電子政府は大きく進展しましたが，その構築の手順をスライドに整理してみました。皆さんも容易に理解いただけると思いますが，第1段階は「行政内部の情報化」でした。これは基幹システムとなるコンピュータやパソコンを導入し，それらを役所内部のLANで結ぶというものです。昔の言葉でいうと職場のOA化，今はIT化と呼んでいるものが第1フェーズです。

第2フェーズは，「行政機関のネットワーク化」です。地方自治体では，LGWAN（総合行政ネットワーク）とLGPKI（地方公共団体における組織認証基盤）が出てきます。LGWANはLocal Gov-

社会保険庁の改革

- 年金業務と政府管掌保険業務の分離
- 政管健保は、都道府県レベルの公法人へ
  - 国民健康保険の都道府県への移行も検討されている
- 年金業務について
  - コア業務のみ国が引き継ぐ
  - その他の業務はアウトソース
  - 徴収業務は労働保険と一元化
- 社会保障全般の見直しとITの積極的な利用

スライド9

電子政府の実現手順

1. リアル空間において
   - 行政内部の情報化
     - 基幹システム、パソコンなどの導入
2. 行政機関のネットワーク化
   - LGWAN、LGPKIの導入
3. サイバー空間に拡張
   - サイバー空間における窓口の開設
   - オンラインによる電子ファイルの受け付け

第3ステップへ移行 ⇒ 戦略的な調達へ

スライド10

ernment Wide Area Networkの略で，行政機関間を結ぶネットワークです。LGPKIはLocal Government Public Key Infrastructureの略で，これは電子署名です。具体的には，知事や自治体の首長さんなどの公印を電子署名化したものです。中央政府は霞ヶ関WANとGPKIというのを持っています。これによって行政機関の間は地方・中央を問わず，今はネットワークで公文書のやり取りができるようになっています。これが第2フェーズです。

現在は，次の第3フェーズに入っています。このフェーズでは，インターネットなどを介して，我々一般住民，国民と行政機関との間のやり取りになります。住民，国民から行政機関へ提出する申請や申告は，一般的に上り線と呼んでいます。それに対して逆に行政機関から我々のところに来るもの，例えば各種証明書類や各種の通知などは，下り線と呼ばれています。

上り線，下り線ともに公印あるいは本人の記名・捺印を要するものがあります。公印側は第2フェーズでできているので，残る個人をどうするかが課題になりました。現在は民間の認証サービスに加えて公的個人認証サービスがあり，3年間500円で全国の自治体から電子署名サービスを受けられるようになっています。そしてこのサービスでは印鑑登録証と同じような電子証明書をもらい，住民基本台帳カードに入れて使うことになっています。住民基本台帳カードはまだ全国で1％も普及していませんので，この会場でお持ちの方がいたらすごく感謝します。制度・環境はそこまで進んでいて，あとは利用率をどう伸ばすか，それがこの「第3ステップへ移行」という意味です。

第3ステップまでいくということは，構築はほぼ終わりで，実稼動になります。よりうまく稼動させるために，効率を上げて，より安全性を高めて，より上手に稼動させる，それを「戦略的な調達」という言い方で表しています。これが来年度以降の電子政府関係の状況です。

医療分野の情報化の実現手順

1. リアル空間において
   - 電子カルテ、会計・事務システムの導入
2. 医療機関のネットワーク化
   - HPKIの実現
   - 専用回線やVPNの利用 ⇒ コスト削減
3. サイバー空間に拡張
   - サイバー空間における窓口の開設
   - 医療機関等の関連情報提供 ⇒ 質の向上
   - 保健・医療サービスの提供

スライド11

医療分野の情報化の実現手順

（スライド11）同じ手順を医療関係に当てはめたのが次のスライドです。これを見ていただくとお分かりのように，電子カルテ，会計・事務システム，レセコン，さらには放射線科のPACSの導入などはすべて第1フェーズです。このことから医療分野は残念ながら第1フェーズもまだ十分に進んでないことが分かります。第1フェーズが進まずに，第2，第3フェーズに入ったらどうなるかというと，電子政府でも経験しているように，紙と電子のデータが混在するため，結果として業務が増えて大変なことになります。ですから当然，第2，第3フェーズへ進むにしても，第1フェーズを確実に進めなければならないので，国も支援策を取ると思います。会計関係・事務関係のシステムはけっこう普及していますが，電子カルテの普及率はまだまだ低迷しています。これをどうするかが大きな課題になることは間違いないと思います。

財源をどこから確保するかという課題がありますが，電子カルテについては，保険点数化する話もあるのではないかと思います。ただ，電子カルテを導入することが目的になってはならないので，第3フェーズまで含めて，医療分野の全体の情報化をどう進めるかをしっかりと計画することが必要です。

第2フェーズは，電子政府の例でも分かるよう

に「ヘルスケアの電子署名」が必要になります。具体的にはお医者さんや保険対応する医療機関などの電子署名が必要とするようになるのですが，これらを総称してHPKI，ヘルスケアのPKIと呼んでいます。この件についてはご存じの方もいらっしゃるかと思いますが，ヘルスケアのPKIは2006年度から厚生労働省が制度的に対応することになっています。医師が最初で，医師の台帳を電子化するのが大体10月には終わると思われます。その後，医師の属性を含めた電子署名を発行し，紹介状から始まると思われます。医療機関から医療機関へ出される紹介状の電子版で，これは医師であることを確認する必要があります。保険点数も付いているので，実用的といえます。

第2フェーズには，HPKIのほかに「安全なネットワーク」が必要になります。このネットワークは，医療関連機関を結ぶものですが，このような組織は全国に約20万あります。そのため，もし，専用回線でネットワーク化するとなるとコスト負担をどうするのか，代わりにVPNでネット化したらどうなるのか，というようなことが大きな問題になってきます。

一方では，このフェーズをクリアしないと第3フェーズへ進めませんので，どのようにして安全なネットワークを構築するかは，避けて通れない重要な課題です。患者さんが病院から病院あるいは診療所へ移動したときに，もとの情報にアクセスできるようにするというのも第2フェーズです。

「e-Japan戦略―医療―」について

- 健康増進に役立てるための総合的な保健・医療サービスが提供される体制の整備
- レセプトのオンライン化 ⇒ 2004年から
- EBM（Evidence Based Medicine）およびEBH（Evidence Based Healthcare）の推進 ⇒ EBHは経済省が推進
- 医療情報のネットワーク伝送と外部保存の容認 ⇒ VPN
- 資格認証システムの構築 ⇒ 認証局の構築
- 山間僻地・離島への遠隔医療の実現 ⇒ VPN

等

スライド12

家からカルテやレセプトを見られるようにするのは第3フェーズにあたります。どちらにしろ，このような流れで情報化することが必要であるということが，お分かりいただけると思います。

今説明したネットワークの1つの解答が，今日の資料の後ろのほうに書いてあります。

（スライド12）今のe-Japan戦略に記されている，医療・保健分野の情報化をまとめます。「レセプトのオンライン化」は2004年から始めたわけですが，まだまともにできていませんが，保険局が対応しています。2004年からテストケースを始めましたが，まだオンライン化は行われていません。2010年までにやり上げることになっています。

EBM（Evidence Based Medicine），それからEBH（Evidence Based Healthcare）とありますが，この2つを実施することになっていて，EBMは当然のことながら厚生労働省が推進しています。それに対してEBHは，簡単に説明すると例えばサプリメントの効果はどうかとか，冗談半分によく言うのは，「紅茶キノコってあれはどうなったのでしょう，本当に効果があったのでしょうか」というようなことを明らかにすることを目的にしています。こちらは経済産業省が対応しています。いわゆる健康食品についても，この人にはどういうものが本当に合うのかというのをエビデンスとして蓄積していきたいということです。それからe-Japanのなかには「医療情報のネットワーク伝送と外部保存」というのが書かれていて，これはVPNになるだろうと思っています。

それから，「資格認証システムの構築」というのはHPKIのことですが，これも実はe-Japan戦略Ⅱに書かれていました。さらに「山間僻地，離島への遠隔医療の実現」も，実施しようとしています。最近では沖縄の離島に対して，インターネットの高速回線を用意するような施策が総務省によって取られています。3年計画ですが，ほぼ

どこの島もインターネットが使えるようになると期待されます。これによって，例えば那覇の中核病院から離島に対して支援することができるようになると期待されます。

このようなネットワークの構築には，専用回線にすると費用的な問題もあるので，できればインターネットにしたいところです。しかし，個人情報保護を考えたら，まさかそのまま情報を伝送するわけにはいきません。だからVPN（Virtual Private Network）が必要という話になります。

（スライド13）医療分野でのIT利用促進について説明します。これは医療情報ネットワーク基盤検討会（これは私が座長を務めさせていただきました）が，去年の9月に結論を出していたものです。どちらにしても十分なセキュリティが必要だというのは言うまでもないことです。

医療分野でのIT利用促進

- 目的
  - 医療の質の向上と効率的な医療提供体制の構築に資する
- アクション
  - 処方箋、診断書、出生証明書をはじめとする診療情報の電子化などを包括的に検討する
- 2004年９月までに結論を得る
  - 医療情報ネットワーク基盤検討会の最終報告等を活用する

<u>十分なセキュリティの確保が必須</u>

スライド13

検討会報告書の概要

1. 医療におけるPKIのあり方
   - 公的個人認証サービスまたは民間認証局による自然人の認証サービスを利用
   - 資格認証を行うための台帳を整備する
2. 書類の電子化
   - 医療機関から官へ提出される書類等は電子署名を用いることで電子化が可能
   - 処方箋の電子化については、引き続き検討

スライド14

（スライド14）検討会の報告書の概要です。読んでいただいて分かるところは除き，分かりづらい部分について説明します。

最初に「医療におけるPKIのあり方」，すなわち電子署名のあり方です。公的個人認証サービスは自治体から提供されている電子署名です。これは証明書に姓名，現住所，性別，生年月日が記されていてその有効性が確認できる仕掛けを用いています。そしてその人の登録されている公開鍵が証明されています。公的個人認証サービスが認証するのは，自然人，すなわち人として生きていますという，言い方を変えると属性がない人物です。例えば私が東工大にいる大山というときには，それは公的個人認証サービスではできません。なぜなら，公的個人認証サービスでは私が東工大の職員であるということは証明しないからです。私が東工大にいるというのは，私に付いた属性の１つです。こちらの属性付きの証明は，民間の認証サービスにより行われます。

しかしながら，法定免許の資格認証についてはちょっと違いがあります。医師であるというのも属性の１つですから，もし私が医師であれば，私が医師であるという資格の証明は，医師であることを保証できるところに証明してもらわなければなりません。当然のことながら，医師免許を持っているとともに，その免許が有効であることを保証できるのは厚生労働大臣ですから，厚生労働省が，例えば医師の台帳を整備しなければなりません。

「書類の電子化」については，医療機関から官へ提出される，例えば診断書，出生・死亡などの各種の証明書については，電子署名を使えば電子的にできるということを，厚生労働省から正式に言ってもらいました。こういうことを１つ１つ明確にすることが必要です。

処方せんについて触れると，これは電子署名で記名・捺印に当たるものはできるのですが，残念ながらまだコピー防止がしっかりできていません。そのため処方せんは電子的に作成するのはまだ許

可されていません。ニーズがあるのは分かっているのですが，処方せんにはいわゆる麻薬・劇薬の類まであるので，今はまだ危険という判断になっています。

（スライド15）次は「診療録等の電子保存」です。これは医療情報の保存と利用を分離するという前提で書かれています。言い方を変えると，データベースをそのまま保存するわけではないということです。

この報告が出る前はどうであったかを改めて説明すると，紙やフィルムなどのカルテ情報等については厳重に梱包をし，それを民間の倉庫業を含めて外に置いてもいいとなっていました。ただし条件があって，「必要な時に速やかに取り出せること」となっていました。一方，電子データについては，その情報を外部のどこかに預けるときには，その情報をだれかが見てしまう可能性があるので，預ける先は「医療機関であること」になっていました。

それを今回，個人情報保護法もできたことだし，いろいろな観点からもう少し緩和できないのかということを議論して，ここにあるように，「守秘義務等個人情報保護違反に関する罰則規定が制度的に設定されていることが必要」という結論になりました。例えば国家公務員や地方公務員，そのほか民間でもそういった公務員型の守秘義務等をかけた例においては，「制度的に守秘義務が設定されて」います。この前提条件に合致するものとしては，例えば自治体が持っているデータセンター，あるいは大学法人，これは医学部があろうとなかろうと関係なく，制度的に個人情報保護の違反に関する罰則規定があるというところについては，２つの条件を満たせばよいということになりました。

その１つは，「原則保存主体の医療機関等のみがデータ内容を閲覧できる」ことです。なぜ「原則」が付いているかというと，事故などの問題が起きたときには，医療機関の許可を得たうえで，実際にそこの人が保存されているデータに触ってもいいという言い方をしたわけです。

もう１つは「技術および運用体制などが，公正かつ中立な仕組みによって認定される」ことです。これは当然の要求です。

こういう２つの条件で，例えば自治体などのデータセンターに患者さんの情報をバックアップなどとして預けることは，今では制度的に可能になったということです。

（スライド16）次は，「その他の民間機関では」というところです。これちょっと分かりにくいのですが，前述の場合が成り立たないとき，すなわち公的なデータセンタ

検討会報告書の概要

3. 診療録等の電子保存
- 医療情報の保存と利用を分離する
- 守秘義務等個人情報保護違反に関する罰則規定が制度的に設定されていることが必要

・自治体、大学法人等については
①原則保存主体の医療機関等のみがデータ内容を閲覧できることを技術的に担保すること
②技術および運用体制などが、公正かつ中立な仕組みにより認定されること
の条件を満たすことで可能とする。

スライド15

3. 診療録等の電子保存（続き）
- その他の民間機関では

・公的なデータセンター等の整備がなされていない地域では、
①保存に係る機器は、保存主体の所有物であり、電気通信回線の確保や管理でき、かつ保存場所を借り受ける保存形態であること
②保存主体の医療機関等のみが保存情報にアクセスできることを技術的に担保すること
③技術および運用体制などが、公正かつ中立な仕組みにより認定されること
④委託契約書等で、管理者や電子保存作業従事者等にペナルティを含む厳格なルールを設定していること
の条件を満たすことで可能とする。

スライド16

ーのような機関がないときはどうするのかについて触れています。この場合には，先ほどの条件に２つ，①と④が加わっています。この①と④が加わって，全部を満たすことを要求しています。

①は「保存に係る機器は，保存主体の所有物であり，電気通信回線の確保や管理ができ，かつ保存場所を借り受ける保存形態」です。これは簡単にいうとハウジングです。

②には先ほどの「原則」がなくなっています。これはミスプリントではなくて，今度はハウジングなので，そこの貸し主が，何があっても，コンピュータの中身に手を出してはだめですとなっています。もともと機器等の所有権が保存主体になっているのですから，普通は当たり前の話なのです。③は**スライド15**の②と同じです。④は「委託契約書等で，管理者や電子保存作業従事者等にペナルティを含む厳格なルールを設定」するということです。

データセンターを含めて，民間のなかには立派にやっているところがあると思いますので，今後さらなる緩和が望まれます。一方，ここは一種のトリックになっているのですが，守秘義務と個人情報保護違反に関する罰則規定というのを，医療分野の情報に携わる人すべてにかけられれば（これが分野法だったわけです），これができれば条件を満たすので，民間を含めてOKということになります。ところが今は個人情報保護法については医療分野で法律をつくるのではなく，ガイドラインでいくということになっているので，結果としてこの部分が２つに分かれてしまい，民間のほうについては，まだ①が，これがなければもう少しやりやすいだろうと思うのですが，残念ながら今はできていません。

さまざまな手がこれからあると思いますが，何となくまだ「公務員はいいけれども，民間は危ない」という，そういったものが暗黙のうちにあるようです。この件については，皆さん方にもいろいろなご意見もあるのではないかと思います。

検討会報告書の概要

4. e-文書法案に対応して
   - 紙情報のスキャンについては、保存義務を満たすとみなす。保存義務者は、証拠性に十分配慮する。
   - 処方箋の作成は、HPKIが整備されるまで除外

（参考）
- 電子化の阻害となる法令等の改正（民間分野）
- 官については、H.14に成立したオンライン３法で対応済み
- 長期保存への対応が不可欠である

スライド17

（**スライド17**）次は「e－文書法」について触れます。官側についてはオンライン３法により，すでにすべて電子化できるようになっています。ところが民間に対して紙で保存しなければならないように義務づけている例が法律のなかにあります。カルテなど紙で書いたものは，その紙を保存しなさいとなっていますが，これを電子化して保存してもよくすることが強く望まれたことから，「e－文書法」が作成されました。もう実施されるわけですが，この法律により，紙情報――もともとの原本が紙――をスキャンしても，保存義務を満たすとしています。

具体的には300 dpiのカラーで８ビット×３色の24ビットでなければならないとか，速やかに電子署名を付すというような条件はありますが，別途規定された条件をクリアすれば，スキャナーなどで電子化して保存すれば，元の紙を捨ててもいいということです。

今回のこの法律の解釈について，随分議論があったのですが，厚生労働省は保存義務を満たすと見なすと結論しました。すなわち厚生労働省が所管している医師法等の法律が要求しているものについては，電子的にスキャンして残してあれば，当該の法律を満たすと見なすと結論したわけです。しかし医療過誤を含めた，不幸にして起こるかもしれない裁判における証拠性については，当該の医療機関が独自に判断しなさい，というのがここの意味です。

これもある意味当たり前で，最終的な判断は裁判官が行いますので，そういう意味では厚生労働省からそこまで大丈夫という保障は，もちろんできないということです。

レセプトのオンライン化

- 保険局が検討中
- 留意点
  - 被保険者、保険者、支払基金、医療機関の４者が関係する
  - 一貫した電子化が必要 ⇒ 業務の効率化とコスト削減
- 具体的な課題
  - 医療関連機関間のセキュアなネットワーク化
  - マスターコードの利用促進　20万対1.2万
  - 被保険者のオンライン資格確認 ⇒ ICカード

スライド18

医療情報ネットワークの基盤整備

1. 規模
   - 病院、診療所、薬局、薬店、健康保険組合などを総合すると20万弱
2. 実現手段
   - 専用回線やIP-VPNなどの既存ネットワークに加えて、セキュアチップ付のオンデマンドVPNなどの利用
3. 推進体制
   - 民を主とした協議会の設立　H17.2.4 ⇒ HeasNet
4. 実証実験（試験実施）
   - 厚労省と総務省と経産省のジョイントプロジェクト

スライド19

レセプトのオンライン化

スライド18にレセプトのオンライン化をまとめます。この件は，現在「保険局が検討中」です。

レセプトのオンライン化は，医療機関から支払基金だけではなく，保険者，さらには我々保険を受ける側の被保険者といった4者が関係しています。これらについては，一貫して電子化をしなければなりません。そうでないと効率は上がらないし，十分な効果も出ないことが，別の例で分かっています。したがってレセプトのオンライン化は，ここにあるように保険者，被保険者，審査支払機関，医療機関の全部を電子的にうまくつなぐことが極めて重要です。

もちろん，被保険者が持つ保険証の有効性確認をオンラインで行うことも含まれます。さらには，保険組合から支払基金，支払基金から医療機関へ行くお金の流れなども電子的に行うことによって，オンライン化による効果や効率の向上を目指すということがあります。

医療情報ネットワークの基盤整備

（スライド19）医療関連機関は全国に20万弱あります。すでに専用回線やIP-VPNなどを使っているところもあり，これらは継続してお使いいただければよいのですが，

セキュリティの基本

- 現実空間も電子空間も鍵の管理が不可欠
- 電子の鍵の特徴
  - パスワードは４～12桁、暗号鍵は数十から数百桁
  - 金属の鍵と違って、簡単にコピーできる
  - 磁気カードは、コピー防止に無力
  - だから、ICカードに鍵を記録し、読み出せなくする
- 鍵をかけなければ安全は守れない！
- 鍵をどう盗るか（破るか）が犯罪者の関心事

スライド20

セキュリティに関する問題と対策

- フィッシング詐欺
  - クレジットカード会社に大きなダメージ
- スキミングにより磁気カード偽造
  - キャッシュカードの偽造による預金者の損害
- バイオメトリクス（生体情報）の利用
  - スキミング対策として大手銀行が導入
- ICカード導入 ⇒ セキュリティの要

スライド21

一方では，まだネットワーク化されていないところもたくさんあります。

この課題を解決する1つの答えとして，セキュアチップつきのオンデマンドVPNの開発が進められ，すでに実証実験に入っています。そしてこの実用化を推進するために，平成17年2月4日に，協議会「保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム（HeasNet）」を設立しています。ここには厚労省，総務省，経済省の3省に対応いただき，協力して第2フェーズ

フィッシング詐欺とは

- Fishing ではなくPhishing ← Sophisticated
- 代表的な手順
  1. 魅力的なメールを送る ⇒ ルアー（疑似餌）
     - なんだろう？　おもしろそう！　すごい！　などで誘う
  2. メールに示されるアドレスに接続
     - 本物だと思わせる
  3. クレジットカードの番号などを入力させる
     - これでオンラインカード決済が可能 !!

スライド22

スキミングによる磁気カードの偽造

- 磁気カードに記録された情報を別のカードにコピーする
- 券面は、紙幣と同じような印刷技術で、偽造・変造の発見は可能（有人の場合）
- ATMのような無人の機器では、券面を確認していないものが多く存在
- この場合は、パスワードを盗られるとアウト
  ⇒ これが今の問題！

スライド23

バイオメトリクス（生体情報）の利用

- 指紋、虹彩、静脈など生体情報を用いる
- 手法は多岐にわたる
- クローズなシステムでは有効！
  - 機密室への入退室管理
  - キャッシュカードとの組み合わせ、でも、
    - すべてのATMに入力装置を付けなければならない
    - 手法が異なると相互利用ができない等の課題あり

スライド24

バイオメトリクスの課題

- 大規模実用化が始まる
  - キャッシュカードとの組み合わせで大規模な利用が始まる。しかしながら以下の課題を有している
    - すべてのATMに入力装置を付けなければならない
      ⇒ 高額費用
    - 手法が異なると相互利用ができない　⇒ 利便性の低下
- だから、標準化が必要
  - 客観的な評価指標の策定
  - 各認識手法のパフォーマンスの客観化
  - 技術進歩を止めてはならないことに留意

スライド25

バイオメトリクス普及への論点

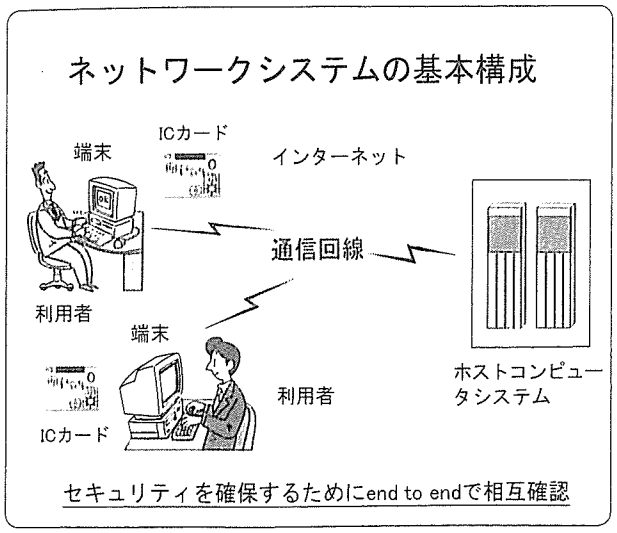
- クローズ系からオープン系へ向かうのか？
  - ATMなどの専用端末を使うのはクローズ系
    - クレジットカードも従来は専用端末を用いるクローズ系であったが、インターネット決済などによりオープン系へ
      ⇒ フィッシングなどの問題が起きる
  - 一般のPCなどを用いるのがオープン系
    - クレジットカードと同じようにデータベース化する？
    - 個人が所有する耐タンパーなメディアに記録する？

スライド26

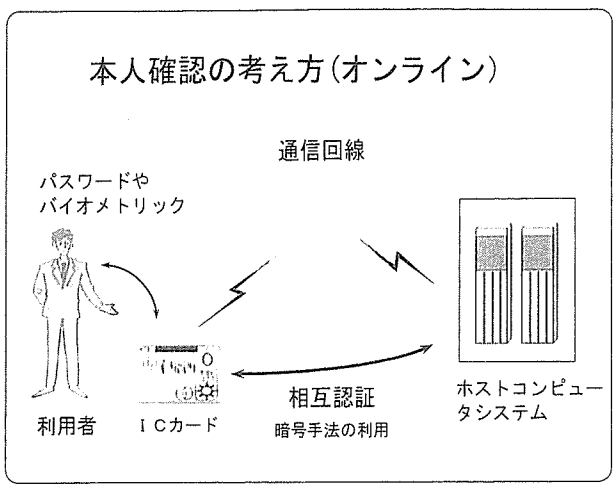
セキュリティ技術について

- 従来技術 ⇒ 例：金融系の情報システム
  - 情報システムを専用化する
  - 専用回線、専用端末、暗号技術などの利用
  - システムの仕様は非公開
- 近年の傾向 ⇒ オープンシステムに対応
  - end to end の相互認証と暗号通信
  - 暗号手法は公開 ⇒ 客観的な強度評価
  - 暗号鍵の安全な管理・運用 ⇒ スマートカード

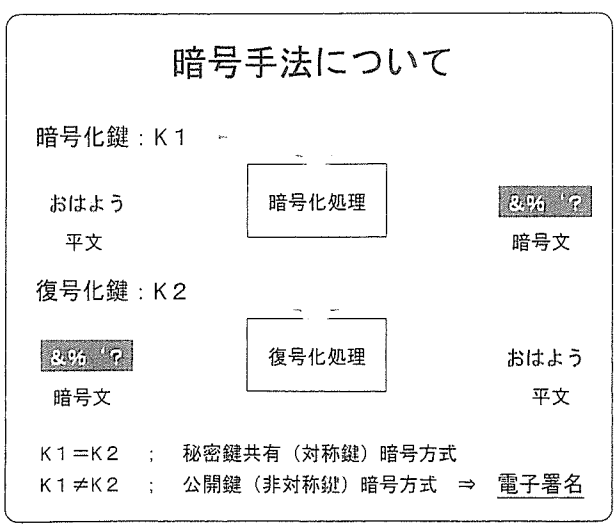
スライド27



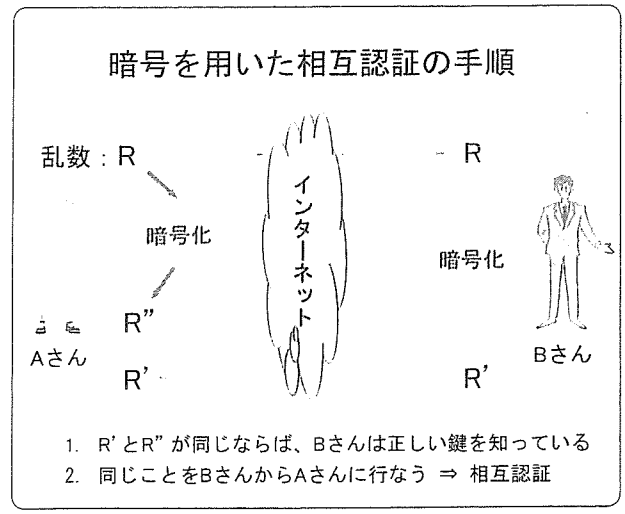
スライド28



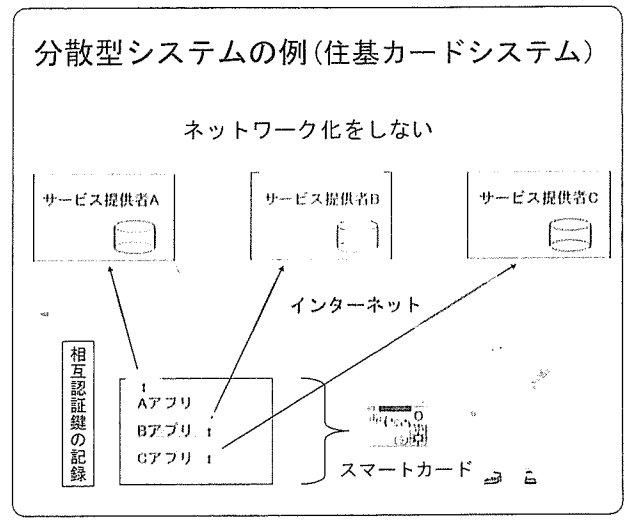
スライド29



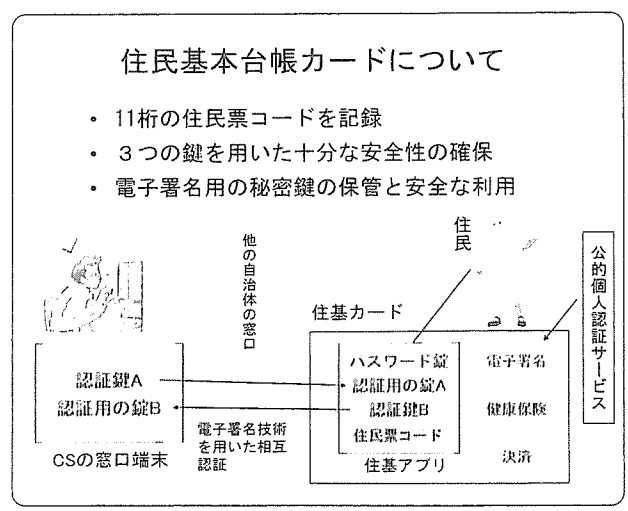
スライド30



スライド31



スライド32



スライド33

を進める動きを開始しています。

（スライド20～35）このあとセキュリティの基本の話をお見せしようと思ったのですが，時間がありません。恐縮ですが飛ばさせていただきます。バイオメトリクスの話など書いてありますので，掲載してあるスライドをご覧ください。