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。

保健・医療・福祉分野における個人情報の保護

（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。

医療分野でのIT利用の促進――検討会報告から

（**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

十分なセキュリティの確保が必須

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

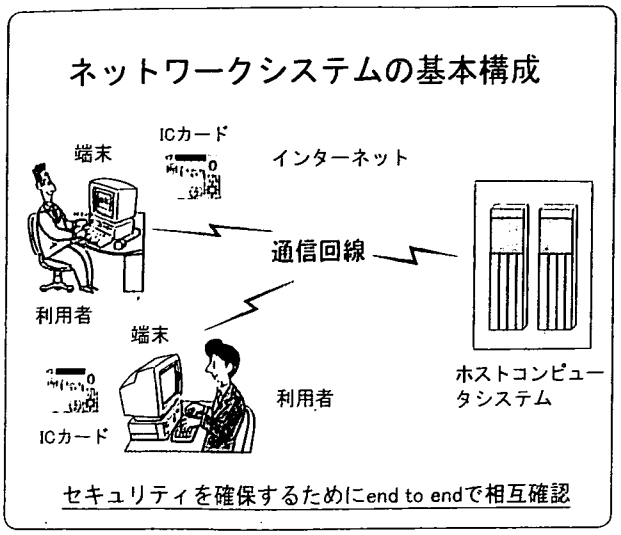
- クローズ系からオープン系へ向かうのか？
  - ATMなどの専用端末を使うのはクローズ系
    - クレジットカードも従来は専用端末を用いるクローズ系であったが、インターネット決済などによりオープン系へ
      ⇒ フィッシングなどの問題が起きる
  - 一般のPCなどを用いるのがオープン系
    - クレジットカードと同じようにデータベース化する？
    - 個人が所有する耐タンパーなメディアに記録する？

スライド26

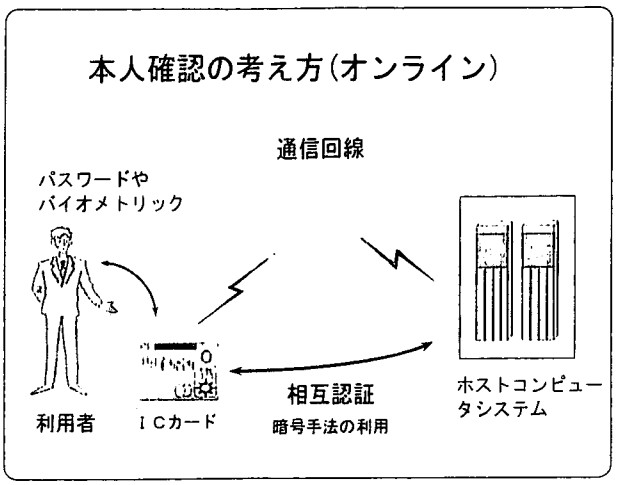
セキュリティ技術について

- 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

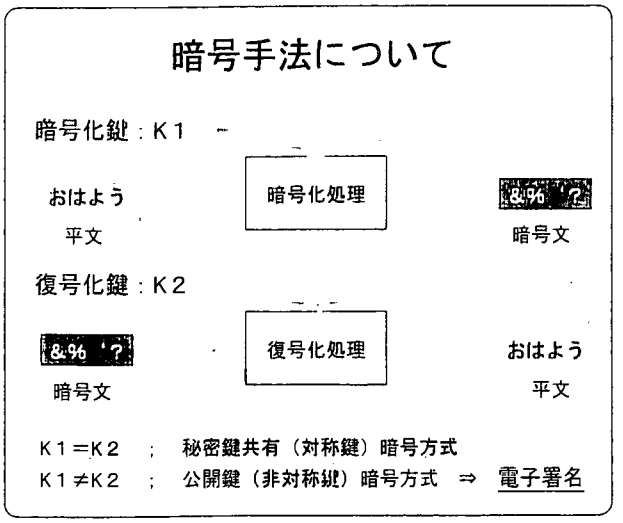
スライド27



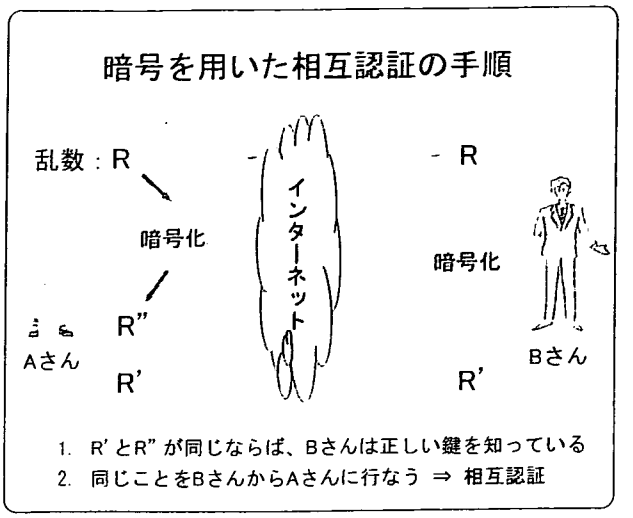
スライド28



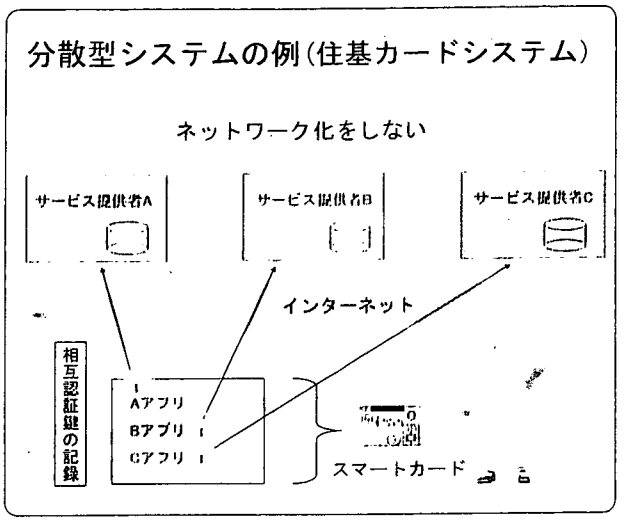
スライド29



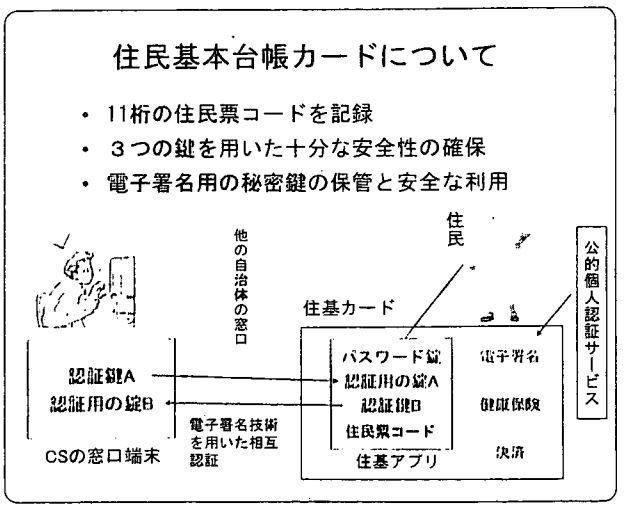
スライド30



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。

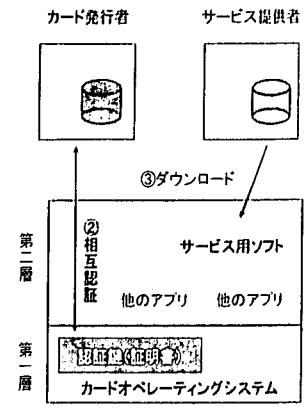
セキュアチップとは

- 特徴
  - 相互認証と暗号通信機能を有している
  - 2階層のPKIをサポートしている
    ⇒ ネットワーク経由での鍵配送が可能
  - 安全性については第三者の専門家による評価確認がなされている ⇒ セキュリティの要
  - 住基カードなどで実装済み
  - 発行管理システムは、日本の技術
  - 基本概念の開発は、NICSS ⇒ CD投票へ
- 応用
  - オンデマンドVPNやリモートメンテ・サービスなどに

スライド34

次世代スマートカードの発行管理

1. 目的
   - カード発行者が、サービス提供者へアプリのダウンロードを許可する
   - 各アプリケーションの鍵管理等を独立させる
2. ダウンロード許可の手法
   - 発行者とカードとの相互認証 ⇒ PKIベース
   - ①通常モード ⇒ ②相互認証 ⇒ ③ダウンロード可能状態 ⇒ ④通常モード



スライド35

VPN用のセキュアチップ

（スライド36）今ふれたネットワーク化をもう少し詳しく説明したいと思います。このオンデマンドVPNでは，セキュアチップと呼ばれるICカード用のコンピュータ付きのチップと暗号用のチップを用いています。世界的に見ても，最も進んでいるチップ技術は日本が持っております。これは住民基本台帳カードに使われているチップと同じです。ほかのICチップ，例えば皆さんがお持ちのクレジットカードなどに金色のチップがついているものがあると思いますが，住基カードから見ると，このチップは世代が1つ前のものになります。しかし，VISAカード，マスターカードを主メンバーとするグローバル・プラットフォームが2005年10月頃にパリで，日本との技術協力でつくられた新しい仕様を公表する予定です。この仕様は今の日本でいうと住基カードのチップとほとんど同じです。このチップの別の応用としては，2006年3月から発行される予定の電子パスポートがあげられます。電子パスポートはICチップつきのパスポートで，これによって自動化ゲート等での出入国の迅速化や，パスポートの偽造・変造の防止を実現します。電子パスポートの導入は，日本だけではなく世界的な動きになっています。さらに日本製のICチップはオーストラリアのパスポートにも採用されています。

VPN用のセキュアチップ

- VPNのメリット
  - 既存ソフトを変更せずに使える
  - すべての通信文を暗号化することにより、安全性が確保される
- VPNの課題
  - 秘密鍵は、マニュアルでセットされる ⇒ 柔軟性不足
- e-Key netとは
  - VPN用のエッヂルータにセキュアチップを設定
  - 複数鍵をサポート
  - ルータ内の暗号装置は、セキュアチップ内の秘密鍵を指定して用いる

  医療情報分野のニーズを満たすことが可能に

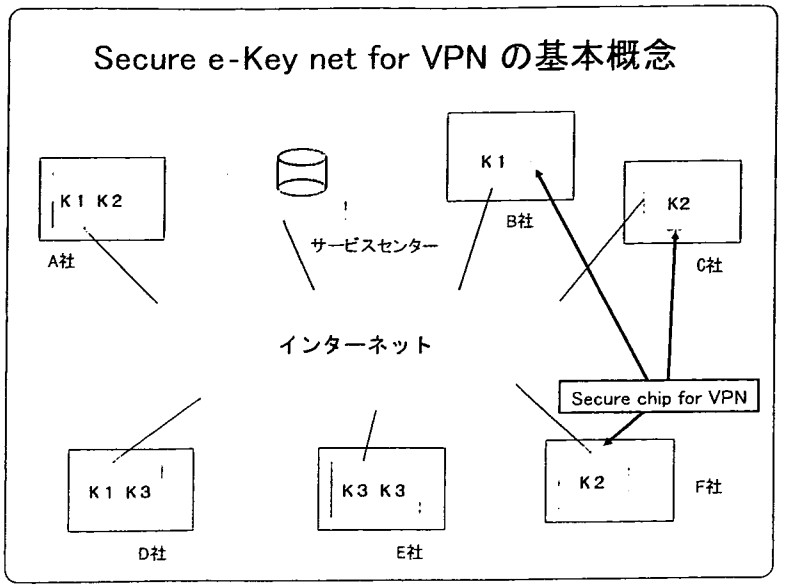
スライド36

Secure e-Key net for VPNの仕組み

ここで強調したいのは，現在このようなセキュアなチップを使ったオンデマンドのVPNがつくられているということです。VPNのメリットは，ご存じのように既存のソフトを変更せずにメッセージの暗号化ができるということです。例えば医療機器にセキュリティの機能を追加したら，薬事承認をあらためて取らなければならない場合などがあり，これでは大変です。ソフトは勝手にいじることができませんから，外づけで対応する方法

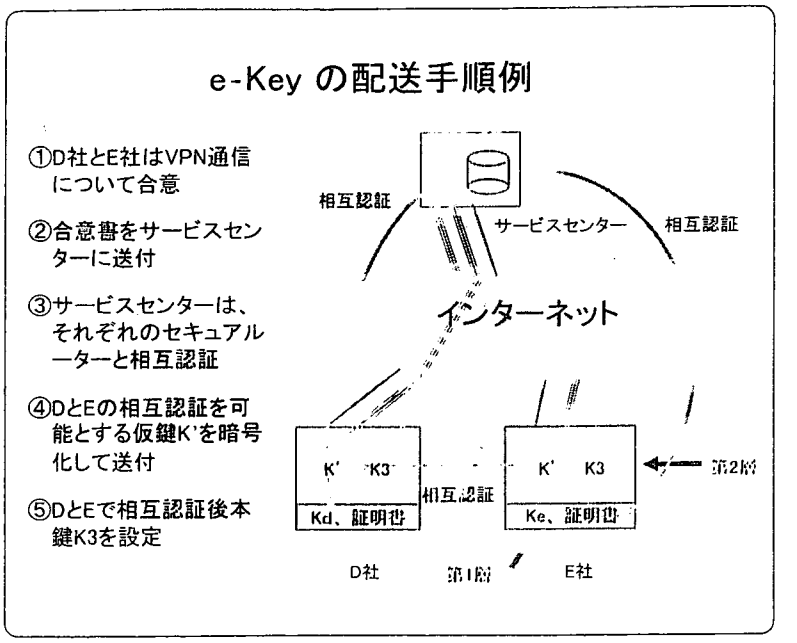
も必要になります。この観点からVPNは，医療の分野では最も使いやすいのではないかと思われます。すべての通信文を暗号化できますので，個人情報保護の観点からも十分だろうと思われます。

VPNの課題は，暗号に使う鍵をどうセットするかです。例えば20万カ所，全部の医療関連機関が同じ鍵を使っていたら，1カ所から鍵がもれた途端に安全性が崩壊します。そのため，任意の組み合わせで鍵設定をどう行うかが課題になります。この問題を解決する技術が住基カードのチップに組み込まれていたのです。



スライド37

（スライド37）すでに実証実験でサービスセンターが立ち上がっています（日本国内には当初3カ所立ち上げる予定です）。それぞれの組織に書かれている箱がエッヂルーターと考えてください。つまり外からネットワークの線がきたときに，無線でも有線でもいいですが，組織内のコンピュータとつながるもので，ちょうど出入口に設置されるルーターと思ってください。ADSLの装置を家でお持ちの方はADSLモデムに組み込まれていると思っていただいてもけっこうです。このなかに暗号装置とそれから住基カードと同じセキュアなICチップが組み込まれているということです。このチップの技術的な特徴は，2階層のPKIを積んでいることです。この技術は日本が開発した新しいICチップに実装されていて，PKIは下の層と上の層にあります。スライドに示されるようにA社，B社，C社……という具合に，これは病院と思っていただいてけっこうですが，そこに暗号装置があって，鍵がチップに入っているとお考えください。



スライド38

（スライド38）次に，インターネット経由で安全かつ確実に鍵を配送する方法について説明します。先ほどふれたサービスセンターの役割がここにあります。今，D社とE社という2社において暗号装置をどこかで買っていただいたとします。この2社間にインターネット経由でVPNを張る手順を説明します。

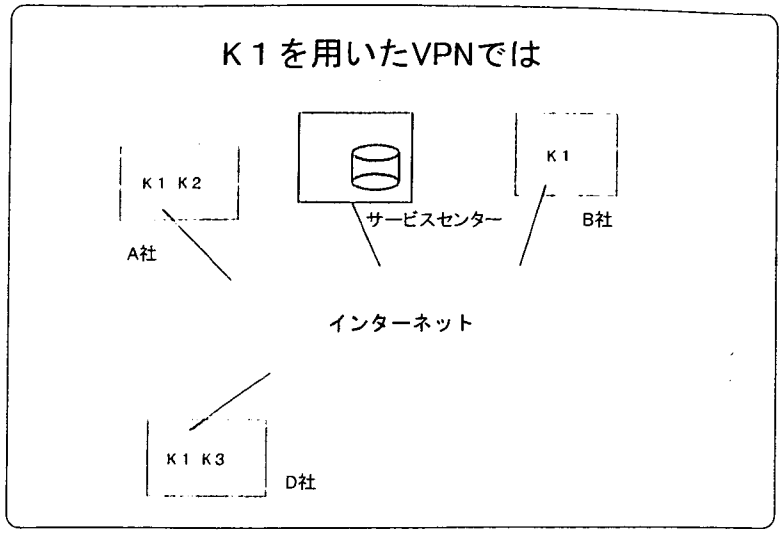
最初にこの2社が合意し，合意書をサービスセンターに送付します。電子的に送付してもいいし，紙で送ってももちろん構いません。受領したサービスセンターは，下の層のPKIを使って，相互認証を行います。これを第1層と呼んでいます。サービスセンターはそれぞれのセキュアルーターと

相互認証をかけます。相互認証をかけるので，ルーター側とは相手が正しいことが確認されるので，これで一種の暗号通信を開始することができます。これで，サービスセンターとD社のエッヂルーター間でセキュアなセッションが張られます。次に，同じように，センターはE社のルーターと相互認証して，セキュアなセッションを張ります。DとEの2社が相手確認をするための鍵は，当初から入っているわけではないので，相互認証用の鍵を暗号化して配送します。これがK´で，仮の鍵になっています。仮鍵は上の層，すなわち第2層に記録されます。以上で，サービスセンターとしての役目は終了です。

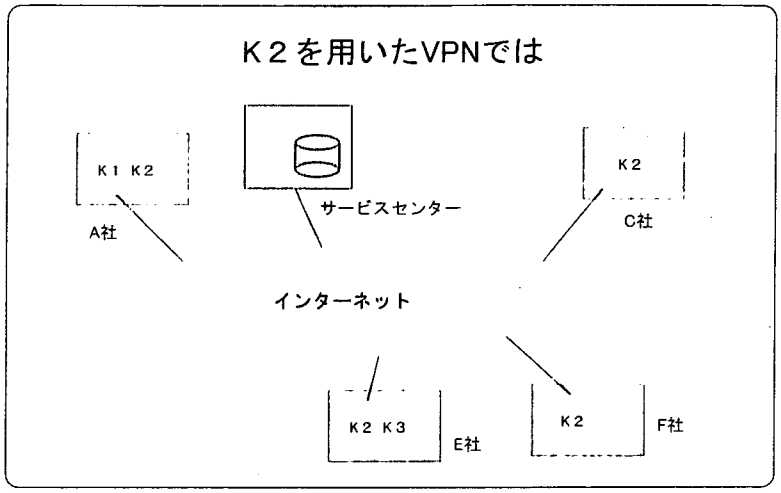
その後D社とE社は，互いに相手確認を行います。両者のルーターは相互認証して安全な通信を張ることができるので，その後，仮鍵を本番の鍵に取り替えます。こうすることで，サービスセンターは実際に用いる暗号鍵を知ることができなくなります。

以上のような手順でそれぞれのルーターに複数の認証鍵が配送されます。実際の利用場面は，例えばK1をアクティブにすると，**スライド37**の例では3社が（**スライド39**），K2を使うと4社が（**スライド40**），K3を使うと2社が（**スライド41**），論理的に異なる暗号通信ができるようになります。

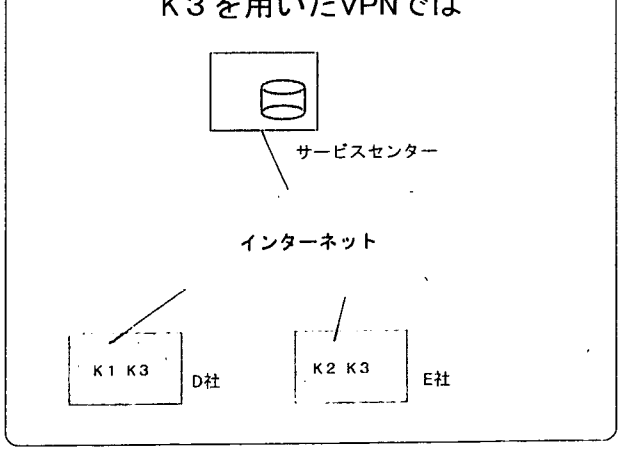
予測ではこの辺のサービスは月に2,000～3,000円で提供できるのではないかと期待しています。ルーターは大体2万円くらいの装置で，2万円が20万カ所なので総額でも40億円です。40億円ならば，場合によっては国費で整備することも可能かもしれません。もちろんこれからの議論ですが，第2フェーズを実現するのに不可欠なセキュアなネットをつくる方法としては，可能性があるかもしれないと思います。



スライド39



スライド40



スライド41

実証実験はすでに沖縄で行っています　サービスセンターは東京に立ち上がっていますが，東工大も開発に関与しましたので，アメリカの大学と

東工大との間で実験を行っています。この暗号装置をアメリカに持っていって，日本から鍵を配送してVPNが張れることを確認しています。これは技術を開発しているものから見るとけっこう感動的でした。何しろ日本のサービスセンターから「アメリカとVPNでつながった」わけですから。それも鍵を替えればどことでもつながります。秘話通信が非常に簡単にできるようになります。このセンターのルートを日本に置ければ，ひょっとすると輸出産業としても伸びてくる可能性があるかもしれません。どうやるかはこれからですが，楽しみなことです。

まとめ

（スライド42）中途半端になりましたが，私の講演をまとめます。「インターネットの安全性確保」はこれから第2フェーズに発展するためにはどうしても必要であると思います。相互認証と暗号通信，認証鍵の安全性確保と基本的な要求は，先ほど言った住基カードのチップにより実現できます。

「医療分野の情報化」では，ご案内のとおり個人情報の保護が不可欠であること，そしてそのためには医療関連機関間のネットワーク化とHPKIの導入（これは今年から導入開始される）が有効です。このなかの1つのアプリケーションがレセプトのオンライン化になります。

近未来を考えると，「人・機器・コンテンツの認証」が次の課題になると予想されます。レセプトやカルテの開示を考えると，正当な人（間違えて他の人に見せたら大変ですから）が，安全な機器（出した途端に，例えばどこかにウィルスがあって，カルテの情報をばら撒いてしまうようなのも困るわけです）で，正しい情報（本人のカルテ情報でなければならないわけですから，そこを間違えて他の人というのもダメです）にアクセスできることが必要です。その意味で「正当な人が安全な機器で正しい情報にアクセス」できる環境を，このICTの技術を使ってどう実現するかが課題になると思います。従来は安全性と利便性というのは相反するものでした。例えば家の鍵を増やせば，安全性は増しますが，利便性は低下します。このように，物理的な空間では安全性と利便性は相反しています。ところが，電子的には両者を両立させる可能性があります。ですから，電子的な空間は，安全安心そして便利になることを徹底することが重要なのです。

少々中途半端な説明になってしまいましたが，医療分野の情報化が上手く進むためのさまざまな試みと施策を紹介しました。皆さま方のご協力をお願いいたします。

まとめ

- インターネットの安全性確保について
  - 相互認証と暗号通信の導入
  - 認証鍵の安全性確保 ⇒ Sチップの利用
- 医療分野の情報化について
  - 機微な個人情報の保護が不可欠
  - 医療関連機関間のネットワーク化とHPKIの導入
- 人・機器・コンテンツの認証について
  - 正当な人が安全な機器で正しい情報にアクセス
  - レセプトやカルテの開示、コンテンツ流通などに有効

スライド42

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

Study on updating cryptographic mechanism on an apparatus with multi functional IC chip for cryptographic functions and continuity of the service for network connected apparatuses

押田知己[*1]　谷内田益義[*1]　鈴木裕之[*1]　小尾高史[*2]　山口雅浩[*1]　大山永昭[*1]
Tomoki Oshida, Masuyoshi Yachida, Hiroyuki Suzuki, Takashi Obi, Masahiro Ymaguchi, and Nagaaki Ohyama

東京工業大像情報工学研究施設[*1]
Imaging Science and Engineering Laboratory, Tokyo Institute of Technology

東京工業大学総合理工学研究科[*2]
Interdisciplinary Graduate School of Science and Engineering , Tokyo Institute of Technology

1．はじめに

現在、様々なシステムで用いられている暗号の強度が弱くなる、いわゆる危殆化が問題となることが想定されている。システムで用いられる暗号が近い将来危殆化するという予測がなされた場合、使用している暗号を安全性の高いものに更新する必要がある。しかし、現在の殆どのシステムでは使用している暗号方式の更新を想定して構築されていない。このため全体の安全性を低下させることなく新たな暗号方式に移行可能なシステム構築を考慮する必要がある。

本研究では、多機能 IC チップを利用しインターネット等のオープンな環境において安全に鍵配送を実現するネットワーク基盤である Secure e-Key Network（SeKNW）を対象として、機器に内蔵された多機能 IC チップの暗号方式の安全な更新について検討した。

具体的にはコンテンツ配信サービスを想定した応用を検討し、継続したサービス提供の可能性を検討するとともに、実験システムによりその実現可能性を検証した。

2．課題

本研究で対象とする機器には、認証等で利用する鍵などの暗号情報を格納するための多機能 IC チップが利用者端末内に取り外せない形で内蔵される。このため、認証機能で用いる暗号方式の変更が必要となった場合には、IC チップ内の暗号方式の更新も必要となる。その際には通信路上の安全性や成りすまし対策、更新する暗号ライブラリの正当性の保証といった問題以外に、機器毎に搭載する IC チップの性能が異なり新たな暗号ライブラリをモジュールとして追加可能なものと不可能なものが混在するという問題が想定される。機器毎に使用する暗号方式が異なる状況では、サービスの継続性やシステム全体の整合性を確保するための移行計画を立案する必要がある。

3．暗号方式の更新

想定するシステム全体を新たな暗号方式へ安全に移行するために考慮しなければならない利用者端末の特性を以下に挙げる。

・　オンライン状況

機器のネットワークへの接続状況によって、更新を行うタイミングは異なってくる。STB などの常時オンラインを前提とした機器であるのか、PDA のようなモバイル端末などの常時オンラインを前提としない機器であるのかによってそれぞれ対応する必要がある。

・　多機能 IC チップに対する機能拡張が可能かどうか

チップ内の暗号機能を更新するためには、拡張用ライブラリの追加やあらかじめ移行用の暗号ライブラリを予備として備えておく等の機能が IC チップに必要となる。しかし、製造コストの面からこういった機能を有しないチップを搭載した機器が流通することも考えられる。

本研究では、表 1 のような移行パターンを想定し、公開鍵証明書の有効期間を考慮した移行スケジュールと移行方法をパターン毎に検討することで上記課題の解決を図った。

表 1：移行パターンの分類

	常時オンライン可能	常時オンライン不可能
チップ機能の拡張が可能	移行パターン①	移行パターン②
チップ機能の拡張が不可能	移行パターン③	移行パターン④

4．実験システム

実験システムでは、利用権管理者によって IC チップ内の利用権管理機能の暗号方式を新たなものへ移行させ、新たな暗号方式によって認証とサービス（コンテンツ配信）を利用する部分を実装し検証を行った。

実験環境では暗号強度を切り替えることにより、利用権管理機能の認証、コンテンツの復号化等に用いる暗号方式の移行が行えることを確認した。

5．まとめ

本研究では、対象とする認証基盤で用いる暗号方式を新たなものに移行し、その上で提供されるコンテンツ配信サービスにおいてもコンテンツを新たな暗号方式に移行し保護することで利用者が継続的にサービスを利用できることを示した。さらに、提案モデルの一例を検証システムとして構築し、その有効性を示した。

参考文献

[1]　小尾，他：“オープンな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”，電気情報通信学会 2004 総合大会予稿集，2004 年 3 月

[2]　独立行政法人 情報処理推進機構：“暗号の危殆化に関する調査報告書”，2005 年 3 月

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

Privacy enhancement in the On-demand VPN that used a many functions IC chip

浦野雄平*　小尾高史**　大山永昭*　谷内田益義*　鈴木裕之*

Yuhei Urano*　Takashi Obi**　Nagaaki Ohyama*　Masuyoshi Yachida*　Hiroyuki Suzuki*

*東京工業大学 像情報工学研究施設, **東京工業大学 総合理工学研究科

* Imag. Sci, and Engineer. Lab., **Interdisciplinary Grad. School of Sci.and Engineer. , Tokyo Inst. of Tech.

1．はじめに

近年、インターネットを専用線と同様に利用する VPN サービスが大きな広がりを見せている。そして、現在、多機能 IC チップを搭載したルータを使用して、安全かつ動的な接続が可能なオンデマンド VPN[1]についての研究開発が行われている。ここで、多企業間における研究開発など、通信内容だけでなく、どのような組織間で通信が行われているかを秘匿したいという要求存在するが、現状のオンデマンド VPN は、一般的な VPN と同様に通信主体の匿名性を有しないため、このような用途に用いることができない。本研究では、中継ノードを用いたオンデマンド VPN における通信主体の匿名化手法の提案を行う

2．従来のオンデマンド VPN 通信

オンデマンド VPN では、暗号化プロトコルとして、IPsec を用いている。IPsec は第三層のプロトコルであり、通信パケットのヘッダを覗き見する事による通信主体の特定は容易であるため、通信主体の匿名性を有しない。

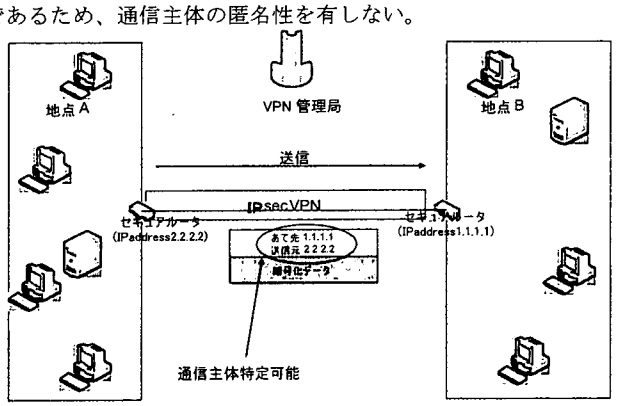


図 1 ：現状のオンデマンド VPN

3．中継ノードを用いたオンデマンドＶＰＮ匿名通信手法

一般に、第３者を中継ノードとして用いることで、間接的な通信を行い、通信パケットのヘッダを覗き見することによる通信主体の特定を防ぐ方法がとられることが多い。しかし、中継ノードを置くだけでは、トラフィック解析の脅威、中継ノードの前後におけるパケット内容の関連付けには対応できない。そこで、提案手法では、トラフィック解析の脅威に対して、中継ノードを多数用意し、その中から使用する中継ノードをランダムに選択する事で対応し、また、選ばれた中継ノード前後でのパケットの関連付けを防ぐ為に、通信を行う２者と中継ノード間で異なるオンデマンド VPN セッションを構築する。そして、通信路上での通信の機密性を保つ為に、上記オンデマンド VPN セッションで、通信主体間のオンデマンド VPN セッションをカプセル化する。これらの方法は、オンデマンド VPN の動的な VPN 構築能力により可能となる。これにより、提案手法でオンデマンド VPN において、安全な匿名通信が実現できる。また、提案手法は、従来の匿名化手法であるオニオンルーティングや、Mix-net に対して、使用プロトコルに制限がない、中継ノードの信頼性があるという点において優位である。

以下に、提案手法による具体的な通信手順を示す。

提案システム通信手順：

① 地点 A のセキュアルータ A2 が匿名通信管理局に地点 B との匿名通信開設要求

② 匿名通信管理局において、地点 A と地点 B が匿名通信サービスを受けられるかを照合。中継ノードとして C を選択

③ 匿名通信管理局から VPN 管理局に A1、A2、B 1、B2、C の匿名通信用 SPD、ルーティングテーブル構成情報配信要求

④ 匿名通信管理局からセキュアルータ A1、B1 に C のアドレスとオンデマンド VPN 開設要求を送信

⑤ A1—C 間でのオンデマンド VPN 設立（A1－C 間でのトンネル成立）

⑥ C—B1 間でのオンデマンド VPN 設立（C－B1 間でのトンネル成立）

⑦ A1、B1 から匿名管理局に VPN 開設完了通知

⑧ 匿名通信管理局からセキュアルータ A1、B1 にオンデマンド VPN 開設要求

⑨ A2—B1 間でオンデマンド VPN 設立（A1－C 間、C－B1 間のトンネルを通す）

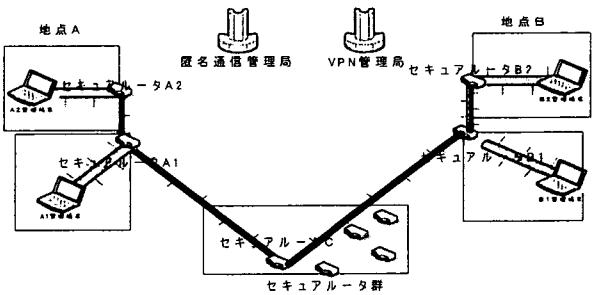


図 2 ：提案システム図

4．実装・評価

提案システムを構築し、途中点（中継ノードの前後、セキュアルータ A2 と A1 の間、B2 と B1 の間の計４点）で、パケットをキャプチャする。そしてそれらのパケット内容による通信主体の関連付けが困難である事を確認した。

5．参考文献

[1] 高橋成文，東川淳紀，山本修一郎，小尾高史，谷内田益義，大山永昭：「２階層 PKI を用いたオンデマンド VPN システム」，情報処理学会論文誌 Vol.46 No.5 1129-1136 ページ（2005 年 5 月）

特集1 遠隔画像診断の現況そして未来

Part 1 遠隔画像診断の現状と課題

遠隔画像診断のセキュリティと個人情報保護

東京大学大学院情報学環
山本隆一

遠隔画像診断のセキュリティ

遠隔画像診断はデジタル撮影された、またはデジタル化された画像情報をネットワークを介して遠隔地で診断することで、情報の安全管理という面では2つの組織と介在するネットワークにわけて考えなければならない。厚生労働省は平成17年3月に医療情報システムの安全管理に関するガイドラインを公表して、各医療機関に準拠を求めている。このガイドラインは主に施設内で運用される医療情報システムに関するものであり、外部との情報交換についても簡単な記載ではあるが、指針を示している。具体的には6章の9項で、(1)回線上では適切な暗号化を行い秘匿性を保つ、(2)回線の起点・終点の識別のための認証を行い、(3)リモートログインを制限する機能を持つこと、という3つの条件が示されている。(3)は機器を外部からオンラインでメインテナンスを行う際などに必要になる要件で、遠隔画像診断では(1)、(2)を確保しなければならない。いくつかの場合にわけてやや詳しく述べる。

ISDN

都会では今更の感があるISDNではあるが、わが国にはまだ比較的広い範囲のBroadband 0地帯、すなわち光ファイバーもADSLも利用できないところがある。ISDNは1対1で対向で接続されるので、電話番号さえ間違わなければ起点・終点の識別は問題ない。したがって暗号化さえしておけば大きな問題はない。むしろ回線速度が遠隔画像診断の質を制限することが問題であろう。

IP-VPN

インターネットではなくて、回線プロバイダが仮想専用回線として提供するもので、比較的大規模な情報共有基盤を作るのによく使われる。一般に高速で、DICOMサーバに直接書き込んで遠隔画像診断を行うことも可能である。専用回線と同じ感覚で使用できるので、2施設だけが接続されるのであれば起点・終点の識別は問題ないが、2施設だけでIP-VPNを用いるのは経費の面からも一般的ではない。通常は県域などの一定の範囲で複数の施設が接続される。もともと暗号化されたネットワークであるVPNなので、経路の秘匿性は問題ないが、起点・終点の識別はIP-VPNの機能としてはないので正しく行う必要がある。具体的にはアクセスする際に、正しく管理されたID・パスワードなどで不要なアクセスをさける必要がある。またIP-VPNはいわば広域に広がったLANを形成するような仕組みで、たとえば10施設が接続されている場合、そのうちの1施設がルーズな管理をすると、他の施設にも安全性の問題が生じる可能性がある。参加施設のすべてで共通の方針で安全管理を行わなければならない。

Internet-VPN

Broad Bandの使えるところではこの方法がもっとも安価で、正しく用いれば安全管理上も問題はない。しかし一般にはIP-VPNと同様の注意が必要である。最近は機器や利用者認証機能を備え、理論的には1対1接続を行うInternet-VPNサービスも出現しており、この方法を用いれば多少初期経費はかさむがそれぞれの施設の運用上の負担は軽くなる。

遠隔画像診断と個人情報保護

2005年に個人情報保護法が全面施行され、医療でもプライバシーがクローズアップされたが、プライバシーはプライベートとは似て非なる権利概念で、19世紀末に大衆新聞の出現ではじめて問題になり、20世紀後半にコンピュータとネットワークの急速な発達であらためて問題になった。つまり情報技術の進歩と密接に関連した権利であり、情報の価値や利活用手段が対話や手紙などの効率が悪く使い勝手の悪い情報伝達手段が主体であった時代では大きな問題にはならなかった概念である。対話と紙の記録という旧来の医療においては我々医療従事者は厳しい守秘義務とヒポクラテスの誓いからリスボン宣言にいたる医療倫理によ