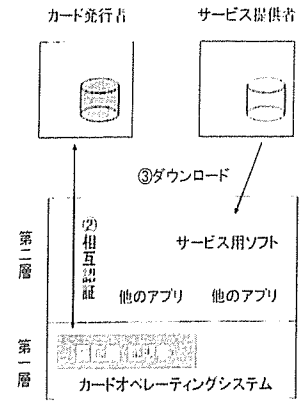
セキュアチップとは

- 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

- 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

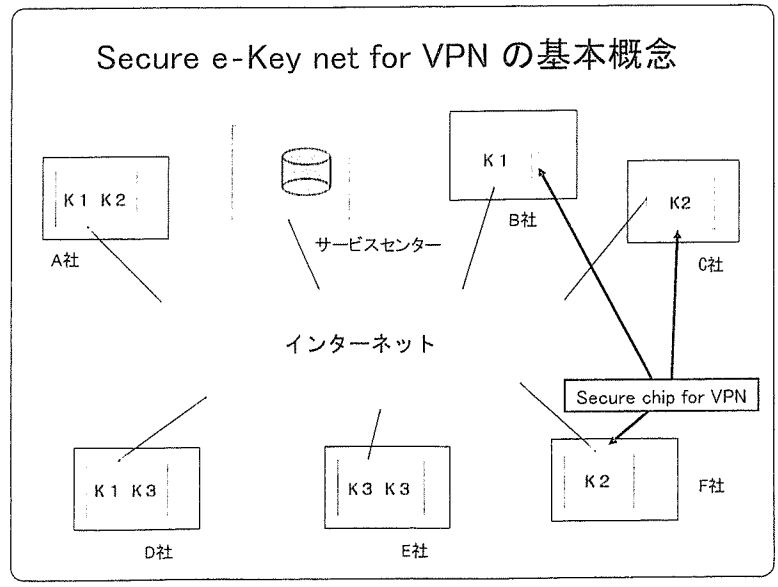
（スライド36）今ふれたネットワーク化をもう少し詳しく説明したいと思います。このオンデマンドVPNでは，セキュアチップと呼ばれるICカード用のコンピュータ付きのチップと暗号用のチップを用いています。世界的に見ても，最も進んでいるチップ技術は日本が持っております。これは住民基本台帳カードに使われているチップと同じです。ほかのICチップ，例えば皆さんがお持ちのクレジットカードなどに金色のチップがついているものがあると思いますが，住基カードから見ると，このチップは世代が１つ前のものになります。しかし，VISAカード，マスターカードを主メンバーとするグローバル・プラットフォームが2005年10月頃にパリで，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。

e-Key netのVPNの特徴

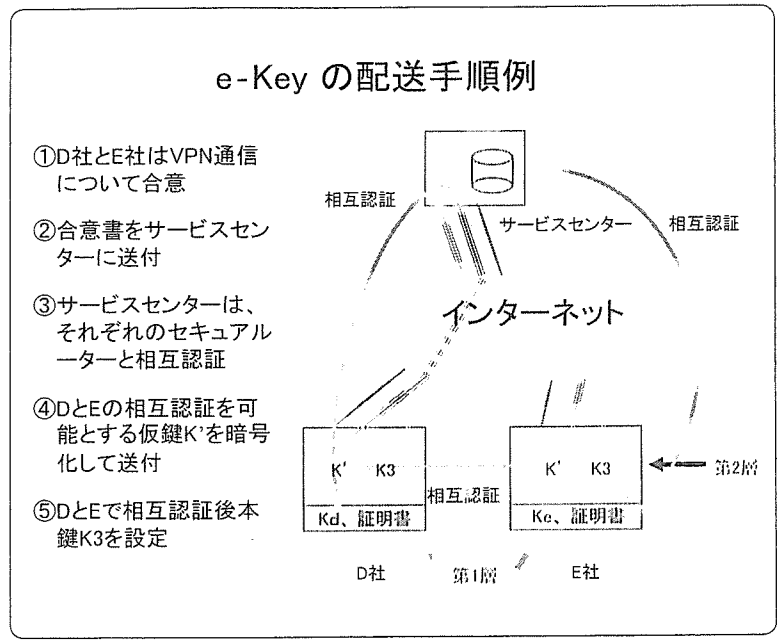
ここで強調したいのは，現在このようなセキュアなチップを使ったオンデマンドのVPNがつくられているということです．VPNのメリットは，ご存じのように既存のソフトを変更せずにメッセージの暗号化ができるということです．例えば医療機器にセキュリティの機能を追加したら，薬事承認をあらためて取らなければならない場合などがあり，これでは大変です．ソフトは勝手にいじることができませんから，外づけで対応する方法

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38

（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）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。

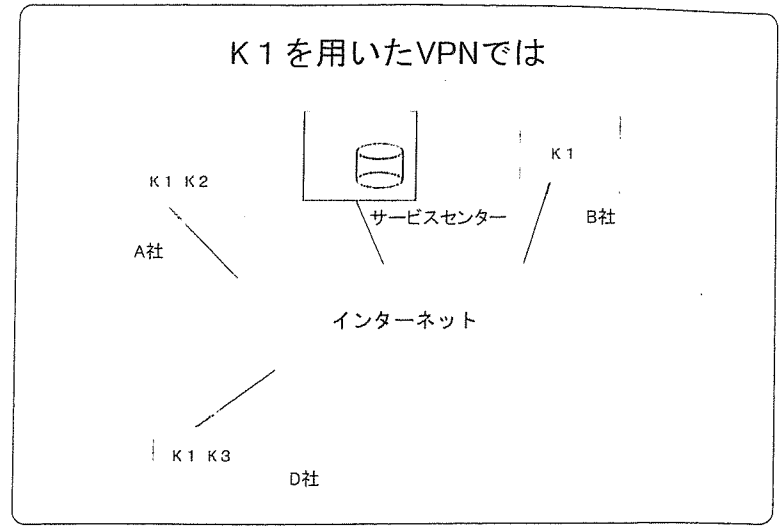
最初にこの２社が合意し，合意書をサービスセンターに送付します。電子的に送付してもいいし，紙で送ってももちろん構いません。受領したサービスセンターは，下の層のPKIを使って，相互認証を行います。これを第１層と呼んでいます。サービスセンターはそれぞれのセキュアルーターと

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。

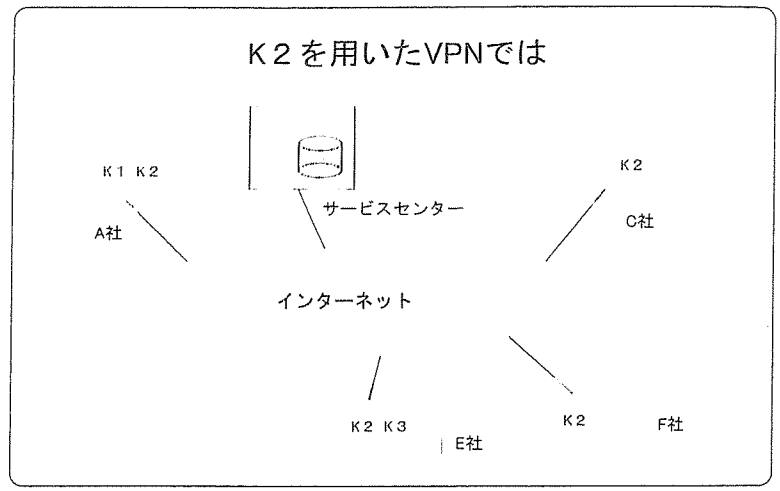
その後D社とE社は，互いに相手確認を行います。両者のルーターは相互認証して安全な通信を張ることができるので，その後，仮鍵を本番の鍵に取り替えます。こうすることで，サービスセンターは実際に用いる暗号鍵を知ることができなくなります。

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。

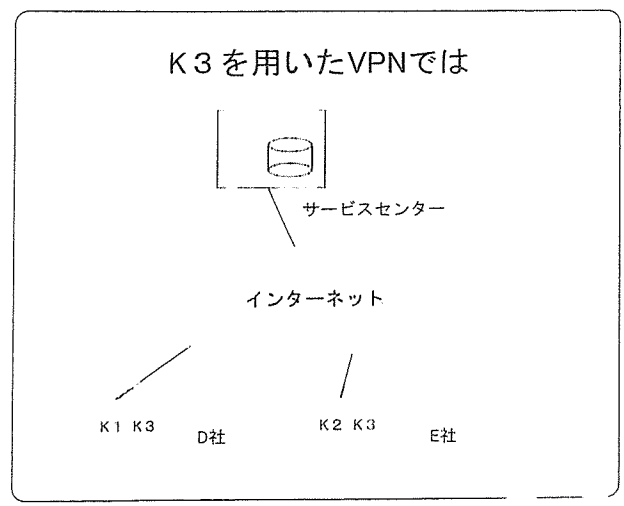
予測ではこの辺のサービスは月に2,000〜3,000円で提供できるのではないかと期待しています。ルーターは大体2万円くらいの装置で，2万円が20万カ所なので総額でも40億円です。40億円ならば，場合によっては国費で整備することも可能かもしれません。もちろんこれからの議論ですが，第2フェーズを実現するのに不可欠なセキュアなネットをつくる方法としては，可能性があるかもしれないと思います。



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，東北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

A-7-21

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。

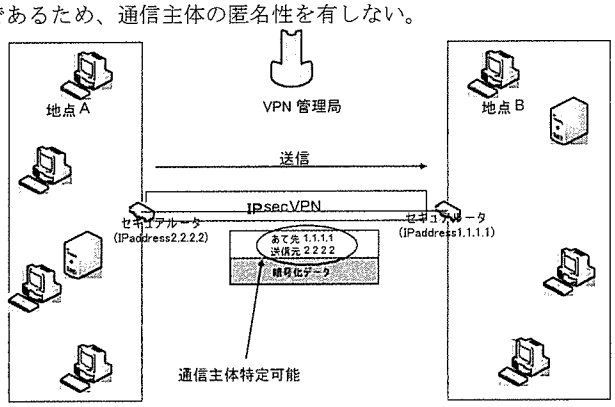


図 1：現状のオンデマンド VPN

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）

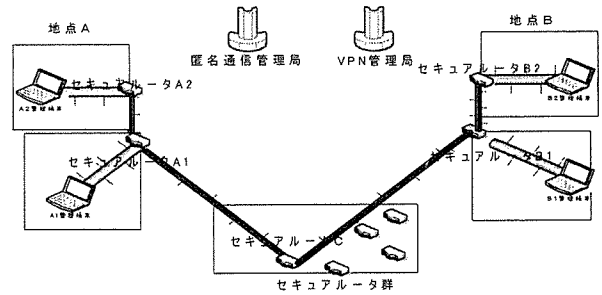


図 2：提案システム図

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

って患者様の権利を保護し、概ね成功してきた。情報が電子化されても患者様の権利の保護のあり方が変わるはずもなく、今後もその保護に成功する必要があるし、そのことに異論はないであろう。遠隔画像診断には新たな留意点も生じる。

紙の紹介状は本人が持参することがほとんどで、フィルムもそうであった。しかし遠隔画像診断では本人と情報は乖離して他施設に送られる。わが国の個人情報保護法では他の事業者に情報を提供することに関して、かなり厳しく規制している。

委託と第三者提供

遠隔画像診断で個人情報である画像情報を診断施設に提供することになるが、個人情報保護法から見れば2つの異なる提供がある。一つは委託であり、これはあらかじめ契約した機関に本来の業務を行うために個人情報を提供するが、個人情報の管理はもともとの施設が最後まで責任を負わなければならない。検体検査を外注している場合がこの典型である。患者様の受診している施設は、委託先の施設と個人情報保護に関する契約を結び、適切に監督する義務がある。その代わり、委託先に情報を提供するにあたって患者様の同意は必要ない。

一方で第三者提供は提供した情報は相手先に管理をゆだねるもので、提供元は提供が完了した時点で提供先での情報管理に関する責任はなくなる。紹介状がこの典型である。第三者提供は患者様の同意が必要である。ただ、紹介、逆紹介や、遠隔画像診断に代表されるコンサルティングは一般には医療では必須の第三者提供とされており、黙示の同意、すなわち、掲示物等でそのような第三者提供が行われることがあること、それに対していつでも非同意の意志を示すことができることを明記した上で、患者様が非同意の意志を示さなければ同意が得られていると見なして差し支えない。つまり遠隔画像診断において同意を得るという意味では大部分の患者様では委託も第三者提供も大きな違いはない。しかし、一方では提供元の施設に管理責任があり、一方では提供先の施設に管理責任がある点はしっかりと理解して選択する必要がある。

委託契約の場合の留意点

委託契約では、情報の管理責任は委託元にある。管理責任を果たすためには一般には個人情報保護に関する事項を含めた契約を交わし、委託元が個人情報保護に関して監督をすることになる。契約内容は具体的には安全管理に努め、委託元で患者様に提示した利用目的の範囲内で使用し、当該個人情報を保持する間は定期的に委託元に管理状況を報告することがなどが含まれる。委託元は報告を受け、問題があれば適切に対処しなければならない。委託の場合、一般的には診断を行う施設では診断および報告に必要な期間だけ保持し、その後、破棄するか連結不可能な匿名化をしなければならない。連結不可能な匿名化とは完全な匿名化で、たとえば画像に独自の番号を振り、別にその番号と個人情報の対応表を保持することは含まれない。

継続して遠隔画像診断を行う場合は、画像を保存し、過去の画像として将来の診断で参照することが多いが、委託契約では当該画像の診断が終了した後の保存は慎重でなければならない。委託元から診断の都度、過去の画像も含めて送付するほうが問題がない。

第三者提供（紹介）契約の場合の留意点

この場合は、診断施設は独立した施設としてあらためて個人情報を収集することになる。したがって診断施設は利用目的を示すか公表しなければならない。また苦情の申し出先なども明示する必要がある。さらに長期間保持する場合は開示や利用の停止の手続きを定めて、明示する必要がある。遠隔画像診断の場合、患者様が診断施設にこられないことがほとんどなので、一般の医療機関のように掲示物を施設内に置くことでは明示にも公表にもならない。ホームページ等で公表しておくことに加えて、可能であれば受診医療機関で患者様にパンフレットのような形態で個別に示す。委託契約と違って利用目的の範囲内であれば診断施設が画像を保持し続けることは、安全に管理していれば、本人から利用の停止の申し出がない限り個人情報保護法上の問題はない。また提供元の立場から見れば黙示の同意の上で提供している限り、提供先の画像情報に対する管理責任はない。

終わりに

安全や個人情報保護は結果的に達成できることも重要であるが、それはいわば当たり前の大前提であり、事故が起きないこと、プライバシーが侵害されないことを事前に説明できることが求められている。遠隔画像診断ではネットワークのセキュリティ確保の方法や個人情報保護法上の取扱いに複数の方法が存在する。それらを当事者すべてがただしく認識する必要がある、我々医療従事者は診断の精度を上げ、患者様にとってもっとも良いと思われる方法をとっているのであるが、患者様からみて一体感のある対応が行われてはじめて安心感のある医療につながるといえる。遠隔画像診断自体はこれからの連携医療でおおいに推進していくべきことであるが、誤解や不安を与えないために最低限の努力は必要であろう。

電子カルテとプライバシー保護

山本隆一*

1. プライバシーは電子化情報でこそ問題になる

2005年に個人情報保護法が施行され，医療でもプライバシーがクローズアップされるようになったが，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初めて問題になり，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改めて問題になった．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が主体であった時代には，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われわれ医療従事者は，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至る医療倫理によって患者の権利を保護し，おおむね成功してきた．情報が電子化されても患者の権利の保護のあり方が変わるはずもなく，今後もその保護に成功する必要があるし，そのことに異論はないであろう．しかし診療情報の電子化は患者の権利保護において2つの点で問題になる．

2. 安全管理—パラダイムシフト？

最初に明記しておきたいが，電子カルテの安全管理は決して難しいものではない．医療従事者のインテリジェンスをもって当たれば簡単とさえいえる．しかし，紙のカルテの安全管理とは全く違う対策が必要になる．つまり発想を変えなくてはならない．馬と駕籠と徒歩しかなかった江戸時代の街道の安全管理と，現在の都市の道路の安全管理は全く異なるのと同じである．

個人情報保護法への対策には過剰反応も過少反応もあったが，過少反応の代表が電子化情報の安全管理で，PCやUSBメモリの紛失事故は後を絶たない．この程度の安全管理が医療従事者にできないとは思われないが，PCやUSBメモリの紛失が診療所に厳重に保管されているカルテの紛失と同じことであるという認識が不足しているのではないだろうか．

本稿で個々の対策を述べることはできないが，厚生労働省もガイドラインを公表しており[1]，電子カルテの使用に当たっては初心に返って安全管理に当たる必要がある．

3. 利活用の高度化—自己情報のコントロール

紙にボールペンで書かれた情報は，書き写すか複写機でコピーするぐらいしか再利用の方法はない．しかし電子化情報は加工が容易で簡単にいくらでもコピーできる．コピーという動作を意識することさえない場合がある．これは重要な診療情報を最大限に活用するという意味では大変すばらしい利点といえる．しかし，容易さはしばしば安易さにつながり，情報取得時の利用目的を外れて利用することになってはプライバシーの侵害になりかねない．

電子化情報の利活用に当たっては患者に通知した利用目的の範囲内であるか，そのことを説明できるか，という点に留意する必要がある．仮にあらかじめ通知した利用目的の範囲外の利用である場合は，匿名化をしなければならない．幸い，電子化診療情報は匿名化が紙に比べれば容易であるが，単に姓名を消すだけでは，少し努力すれば本人が特定できる場合もあり，実効ある匿名化に注意する必要がある．

文　献

1) 医療情報システムの安全管理に関するガイドライン(平成17年3月)，厚生労働省(http://www.mhlw.go.jp/shingi/2005/03/s0331-8.html)．

*やまもと・りゅういち：東京大学大学院情報学環助教授．昭和54年大阪医科大学卒業．主研究領域／医療情報学(個人情報保護，電子カルテ，セキュリティー)．