

## 第65回総会学術大会シンポジウム2

会期：2009年4月18日

会場：パシフィコ横浜会議センター

## 「医療情報のセキュリティについて—技術と運用とのバランス—」

## 座長集約

細羽 実

京都医療科学大学

## 1. 医療情報分野におけるセキュリティ基盤について

喜多絃一

早稲田大学国際情報通信研究センター

## 2. 医療情報システムの安全管理に関するガイドラインと地域医療連携

野津 勤

システム計画研究所

## 3. 中核病院におけるセキュリティの運用

奥田保男

岡崎市民病院

## 4. 連携医療を支えるセキュリティ

水野正明<sup>1)</sup>・吉田 純<sup>2)</sup>

1)名古屋大学大学院医学系研究科遺伝子治療学分野

2)独立行政法人国立病院機構東名古屋病院

## 座長集約

Symposium

細羽 実

京都医療科学大学

医療機関間の連携が重要になってきつつある現在、セキュリティ確保の標準的基盤技術の導入と運用をどのように進めるべきかが緊急のテーマとなっている。2009年3月には厚生労働省から「医療情報システムの安全管理に関するガイドライン第4版」(以下「安全管理ガイドライン」)が出たところであり、その冒頭には「情報化の発展は期待できるが、医療情報の安全管理には、専門的知識も必要であり、多大な人的、あるいは設備投資などの経済的負担はかけるべきでない」との文言が書き込まれている。昨今の経済情勢の悪化のなか、セキュリティを確保し個人情報保護するためには、社会基盤の整備、導入しやすい技術と的確な運用が具体的に進められなければならない。本シンポジウムは、医療連携というシナリオを中心に、現状のセキュリティ確保の問題とそれを解く手がかりをみつけることを目的に4名のシンポジストに発表をお願いした。

喜多氏からは、医療機関が確保すべきセキュリティについての考え方、すなわち、制度的対策、技術の確立と運用により情報資産を守るという基本的な考え方が概観された。重点計画2008には「2011年度当初までに、レセプトの完全オンライン化」、「2010年度までに個人の健康情報を「生涯を通じて」把握できる基盤を作り、国民が自らの健康情報を活用し、健康増進に務めること」が挙げられている。そのためのセキュリティ基盤は、個人情報保護の観点から、国民規模で

必須といえるものである。セキュリティ技術基盤には、ネットワーク上での安全確保、保健医療福祉分野公開鍵基盤(HPKI: healthcare public key infrastructure)、社会保障カード(本人確認)、情報保存基盤(電子私書箱)などが挙げられる。情報資産を特定し、脅威を洗い出し、制度、技術、運用による対策を行うセキュリティ設計が必要である。具体的に医療機関のセキュリティが確保されているかどうか、ネットワークの接続サービスなどが安全管理のガイドラインに則っているかを第三者評価する仕組みも紹介された。

野津氏からは、「安全管理に関するガイドライン」と、IHE(integrating the healthcare enterprise)による地域医療連携システムのセキュリティについての整合性についての解説が行われた。IHEによる医療施設間情報共有(IHE-XDS: cross-enterprise document sharing)は医療連携の標準的枠組みとして注目され、水野氏からも名古屋での実証実験成果の紹介があったが、情報共有のために情報の所在をインデックスとして管理(レジストリ)し、その情報から情報提供用サーバ(リポジトリ)を持つ各医療機関の情報へのアクセスを可能とする方式である(野津氏報告 Fig. 1)。ガイドラインは外部保存にあたって、ネットワーク上でのオブジェクトセキュリティとチャネルセキュリティの対策、送り手、回線事業者、ネットワークサービス提供者、受け手の間で責任の空白をつくらないように、責任分界点の明確化を要請している。IHE-XDSはガイドラインに

おける外部保存の考え方と同等と考えるべきであり、レジストリのサービス事業者は委託となり、リポジトリによる情報共有については、患者の同意により共同利用という形を取ることも可能であるが、第三者提供とならざるをえない可能性もあることなど、が明らかにされた。

奥田氏からは、地域中核病院の現場におけるセキュリティ基盤の確保、「安全管理ガイドライン」への対応の取り組み例が紹介された。医療情報システムの構築段階として、(1)施設内に限定された運用、(2)可搬型媒体による情報連携、(3)オンラインによる情報連携、と三つのフェーズがある。現場ではセキュリティと利便性が相反することも少なくなく、運用的な工夫が必要である。病院としての善管注意義務を果たすため、利用者の本人性をID・パスワードなどで確認し、権限管理を行っている。システム間、施設間での連携では利用者管理がさらに複雑になることが予想される。現在、可搬型媒体を用いたオフライン連携による運用を行っており、適切に情報提供が行われていることを都度確認している。オンライン予約などの連携では、監査証跡と装置間の認証ができる標準化されたIHEの仕組み(IHE-ATNA: Audit Trail and Node Authentication)を導入した。アクセスログの取り扱いが課題となっている。患者IDの共通化は、セキュアな地域連携の重要な鍵であり、早期の実現が望まれる、との報告があった。

水野氏からは、「名古屋地区における、地域医療情報連携システムの標準化及び実証事業による疾患別地域医療情報連携システム実証実験」プロジェクトの紹

介が行われた。臨床目的を明確化し、それを達成するための患者中心の連携医療システムづくりを行った。脳卒中連携パス構築をテーマとし、これに応じたADL(activities of daily living)などのコードを追加し、連携のための文書をHL7 CDA: clinical document architecture R2により標準化した。情報共有技術は標準的枠組みであるIHE-XDSとした。わが国における最初の導入事例となった。IHEによるセキュリティ技術基盤(ATNAなど)もあわせて導入し、また利用者認証、HPKIの導入による電子署名も行っている。「安全管理ガイドライン」遵守のための運用管理規定を策定、ガイドラインを満たすための項目を抽出し、技術と運用による対策を行った。患者IDは地域共通の患者IDとしてシステム内に持たせている。今回の名古屋プロジェクトの成果を継承すべく、他地域への展開も進めていることなどが報告された。

本シンポジウムを通じて、医療連携におけるセキュリティ確保のため、「安全管理ガイドライン」への対応、標準化された技術的基盤の確保とそれに基づく運用を進めることについての道筋が明らかとなった。臨床現場での対応にはまだギャップがあるとみられるが、名古屋プロジェクトのように安全に稼動する例も出てきており、解決は可能と考えられる。技術の進展に見合ったセキュリティ基盤整備は継続して行い、運用もそのなかでレベルアップしていく必要がある。学会としては、今後もさまざまな現場の問題をとりまとめ、関連するガイドラインにQ/Aを発信していくべきであると考え、今回のシンポジウムがその動きのトリガになれば幸いである。

## 1. 医療情報分野におけるセキュリティ基盤について

Symposium

喜多統一

早稲田大学国際情報通信研究センター

### はじめに

セキュリティ基盤は医療情報を安全に安心して活用するために重要である。一般的な情報化の便利さ、危険さを述べ、個人情報保護の必要性、医療情報と通常の商取引とのセキュリティ要件の違いを説明する。そのうえでセキュリティ設計の考え方と医療分野におけるセキュリティ基盤を説明する。最後にそうしたセキュリティ基盤を構築、維持していくために第三者評価が重要でありその動向についても触れる。

### 1. 情報セキュリティに対する考え方

#### 1-1 情報化は非常に便利

情報化により便利な社会が出現している。情報化

により情報交換における地域や時間の制約が取り除かれ、ダイナミックな活動が可能となり、生活態度そのものも変化してきている。例えば人に会うときの地図は簡単に手に入るし、近くまで行けば携帯電話でのやり取りで相手を見つかることができる。以前のように事前の現地調査がいらなくなってきて幹事さんには隔世の感がある。

インターネットによるホテルや新幹線の予約、チケットや書籍等の購入、銀行振込も当たり前になってきている。こうした利用は取引の証跡がのこるので電話予約にくらべて安心感も与えられている。

また、ちょっとした知識はWebで検索することができて専門家を探す手間がなくなってきている。こうし

た環境は国内でも海外でも区別がなくなっている。

こうした、通常の商取引の恩恵を医療分野にもとりこむことが期待され、そのためのセキュリティが課題となっている。

## 1-2 情報の電子化は危険？

こうした便利さは逆に情報を悪用する人にもその機会を与えていることになる。特に情報化により、見えない形で情報が瞬時に交換されて、情報が目的どおり使用されない危険と怖さがある。また、情報化には初期コスト、運用経費およびリテラシーが必要となる。

また、社会的変革を急激に起こすので危険であり、部分最適ではなく、複雑系としての変革のアセスメントが必要になる。

組織のフラット化が進み、中間管理者を飛ばした中抜き管理となり意思決定方式が変わりつつある。トップの方々のじっくり考える時間を奪っているし、トップや中間管理者の付加価値も変わってきている。

対面によらない情報の共有化は仕事の流れを変えているし、また対面によらない取引は目視による安心感や人間関係による取引を奪っている。

## 1-3 個人情報保護がされない

個人情報保護って何故必要なの？ そんなに情報を隠す必要はあるの？ 知られたっていいじゃない、という声をよく聞くことがある。その人は今まで、幸いにして幸せな人生を送ってきた人である。幸せな人も交通事故や自然災害と同じでいつ被害にあうかわからない。被害に一度あうと極端に厳しくなるのもまた事実である。そうした思いをしないために事前に対策を打つべきであり、そういう状況になってしまった人への思いやりも健全な社会のためには必要である。

悪意の仕掛け人は不特定多数の情報から攻撃のターゲットを絞込む。例えば売り込み、勧誘、脅迫に情報を使用したい者にとって有利な条件の人を情報化手段で名寄せを行い絞りこんで攻めてくる。草原の獲物を待ち受けるライオンのようなものである。個人の情報は悪意をもった不特定の敵の目にさらされることを覚悟しないとイケない。

特定の個人を狙って情報を獲得する場合も守る側との戦いがある。例えば入院中のVIP情報などである。他人がそれほどでもないと思って伝えてしまうと本人や関係者に一生の打撃・影響を与える情報もある。通常の人には気のつかない差別に繋がることもある。また、情報を管理している側や入手可能な側が個人の情報を握ることにより、不正がおこり、健全な社会生活を妨げることもなる。

## 1-4 医療情報に要求される本人確認機能と可用性

商取引のための情報システムはおもにお金が入金されるか、欲した物が間違いなく受け取れるかがセキュリティ設計のポイントとなっている。事故が起こった場合は返納、返金とか賠償金で解決するとの考え方である。しかし、医療情報の場合は一生取り返しのつかない障害を与えることもありうる。医療は商取引とはことなり診療対象者や診療提供者を間違えないことが重要になる。成りすましや患者取り違いによる事故を防ぐために本人確認が重要なファクタになる。また、病気の発生は待ってくれないのでシステムがダウンしても診療は継続されなくてはならない。24時間使用できるように必要な時にすぐ使用できるような可用性が重要なファクタとなる。

# 2. セキュリティ設計の考え方

## 2-1 セキュリティの観点

セキュリティは日本語で言うと安全ということになるが、安全という言葉に対して、Security: 情報安全, Safety: 患者安全, Privacy: 個人情報保護, BCP (business continuity plan): 事業継続性が考えられる。ここではおもに情報セキュリティの観点で説明する。

## 2-2 リスク分析手法

セキュリティ設計を行うためにはリスク分析を行う必要がある。リスク分析には、ベースラインアプローチ、詳細リスク分析、組合せアプローチなどがある。

情報資産の特定を行い、情報資産の関連する部門のワークフローを作成し、各部門での情報の入力/利用/出力を把握し、脅威の洗い出しを行う。

## 2-3 対策の選択

セキュリティ対策として制度・技術・運用対策が相補ってセキュリティを確保する必要がある。対策には予防対策・事後対策がある。対策として運用による対策、技術的対策がある。その対策によりリスクが許容範囲に収まらない場合はリスク低減、リスク受容、リスク回避およびリスク移転を行い、そのリスクを許容範囲に収める。そのうえで残るリスクを残留リスクといて、当事者はそれを認識して事後対策を規定化しておく必要がある。

# 3. 医療分野のセキュリティ基盤

情報の安全性は制度的基盤、技術的基盤および運用が相補って確保される。

制度的セキュリティ基盤としては、情報の守秘および目的外所用禁止に関しては個人情報保護法とそれを実施するためのガイドラインがある。セキュリティ

は安心・安全の確保により情報を活用するための手段である。そのためのガイドラインとして「医療情報システムの安全管理に関するガイドライン」が出されている。銀行は偽造・盗難カード預金者保護法が設立して初めて熱心にセキュリティ対策を始めた。医療情報を扱う側は患者さんの情報は自分の情報ではないので運用規則をしっかりと作成し教育しないと運用が甘くなる可能性がある。

技術的セキュリティ基盤としては、電子私書箱、社会保障カード、レセプトオンライン用ネットワーク基盤、HPKI が検討されている。重点計画 2008 では、「2011 年度当初までに、レセプトの完全オンライン化」、「2010 年度までに個人の健康情報を「生涯を通じて」把握できる基盤を作り、国民が自らの健康情報を活用し、健康増進に努めること」および、「社会保障カード(仮称)」を 2011 年度中を目途に導入することを目指す」となっている。以下技術的セキュリティ基盤に関して概略を述べる。

### 3-1 ネットワーク基盤

ネットワークは「安全ガイドラインによれば」何をつかってもよいが、それぞれの特徴にあった対策を施さなければいけない。その対策のためにネットワークを以下のような三つのパターンに分けている。

- 1) クローズドなネットワークで接続する場合
- 2) オープンなネットワークで接続されている場合
- 3) モバイル端末等を使って医療機関等の外部から接続する場合

いずれにしてもチャネルセキュリティを保持するだけなので、そのなかを伝送するデータはオブジェクトセキュリティとして暗号化等のセキュアな対策を施さなくてはならない。

レセプトのオンライン請求のためのネットワーク基盤が 2011 年には普及することになっているのでそうした基盤の医療分野での活用が期待できる。

### 3-2 認証基盤

情報が正当な発信者から正当な受信者に改ざんなく送られるためにはネットワークの入り口出口、あるいは端末の操作者を認証し、なお、且つ誰が作成責任をもったデータであるかが分からないといけない。一つの施設内で情報の授受が閉じている場合は、その施設で決められたルールや方式により実施していれば、機種を変更する場合以外は支障があまりないが、地域連携など管理責任が異なる施設や利用者で情報を共有する場合はそれに適した認証基盤が必要になる。「社会保障カード(仮称)」等の認証カードも検討されている。

また、データの責任の所在を示すためには電子署名が有効である。医療の国家資格を電子証明書上からも読み取ることができる HPKI が厚生労働省を中心に運用されている。

### 3-3 データベース基盤

内閣官房 IT 担当室で提案している「デジタル新時代に向けた新たな戦略～三か年緊急プラン～」のなかにあるような「日本健康コミュニティ(仮称)構想の実現」で期待される、「デジタル技術を活用した地域医療連携による地域医療の再生」、「遠隔産科医療、遠隔画像診断等による安全・安心な医療」、「健康情報の集積・活用の実現による医療の質の向上」および「健康サービス産業の創出による生涯を通じた健康・疾病管理」のためには、医療データを蓄積して活用する必要がある。連携データベースの観点からみると、「専門医」および「かかりつけ医」からみた「地域連携クリティカルパス」を配慮した「診療情報データベース」、個人からみた「個人健康管理情報データベース」および経営者・行政・研究者からみた「統計情報データベース」が「有機的に協調したデータベース」となることが望ましい。

そのためには、電子私書箱構想により実現されることが期待される。電子私書箱はサイバー空間上に個人の信頼点を作り、個人の情報を送付依頼により個人に送付し、個人が管理できるような基盤を目指している。これは縦割されたサービスを個人の観点で統合化する役割としても優れている。現在、構想作りが始まったばかりであるが今後の進展を期待したい。

## 4. 第三者評価制度

安全な情報基盤確立のための第三者評価制度としては以下のような制度がある。

### 4-1 プライバシーマーク制度

これは、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度である。医療分野では(財)医療情報システム開発センターがプライバシーマーク付与認定を行っている。

### 4-2 ISMS(information security management system)制度

これは、国際的に整合性のとれた情報セキュリティマネジメントである ISMS の認証基準 JIS Q 27001 に対する第三者適合性評価制度であり、情報セキュリ

ティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものである。

厚生労働省の出している「安全管理のガイドライン」の第6章はこの認証基準になっている JIS Q 27001ISMS の考え方に基づきまとめられている。

#### 4-3 ISO15408

情報システムやそれを構成する機器・ソフトについて、セキュリティ機能全般および目標とするセキュリティレベルをある評価基準に基づいて評価し、その結果を認証する制度である。つまり、ユーザにおさめるシステムのセキュリティ設計・製造を ISO15408 にそって評価する制度である。

#### 4-4 HISPRO

提供されたサービスの「医療情報システムの安全管理に関するガイドライン」への適合性の評価をユーザ

視点で行っている。ISO15408 に基づいた評価制度もシステムあるいは部品の脅威に対する対策を評価するものであるが、「安全管理のガイドライン」に基づいた観点から、ベンダーのサービスを評価する必要があると提起され、HISPRO(health information security performance rating organization: 保健医療福祉情報安全管理適合性評価協会)が日本医療情報学会、日本医師会および日本薬剤師会を社員として設立され、活動を開始している。

### 5. まとめ

2011 年頃を目処にセキュリティを含めた医療情報の基盤整備が進められている。これを勘案して IHE-XDS や生涯個人健康情報システム(PHR: personal health record)の実証試験も開始されている。こうした動きを踏まえて医療情報分野におけるセキュリティ基盤のあり方と今後の方向性について解説した。

## 2. 医療情報システムの安全管理に関するガイドラインと地域医療連携

野津 勤

システム計画研究所

### はじめに

近年の課題である地域における医療施設連携による医療サービス提供のシステム形態については、IHE により XDS モデルが作成され日本のいくつかの地域でも、このモデルを参考にした地域医療連携システムが構築されている。

一方、日本国内においては、厚生労働省より「医療情報システムの安全管理に関するガイドライン」(以下、安全管理ガイドラインと略す)が発行され 2009 年 3 月には第 4 版に至っている。このなかで、医療機関が外部施設とネットワークを用いて医療情報を交信する場合の安全上の要求事項が示されている。技術的な詳細については、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(以下、HEASNET: healthcare information secure network と略す)発行の「ガイドラインの実装事例に関する報告書」が参照先に示されている。

本文においては、IHE XDS モデルと安全管理ガイドラインとの整合性に関しての留意点を述べる。

### 1. IHE XDS モデルでの形態

Fig. 1 に XDS での医療連携シナリオを示す。この Fig. 1 についての説明は IHE に関する多くの箇所で行われているため、本書ではシナリオ自体については

省略する。安全管理ガイドラインとの間では、XAD: XDS Affinity Domain(XDS のポリシーに同意した参加者によるコミュニティをいう)、レジストリ、リポジトリの三つが関与する。

IHE においては、「Template for XDS Affinity Domain Deployment Planning(以下、Template と略す)」文書により、XAD のためのポリシー作成ガイドを示している。

本文書は、ある地域における独立した XAD、複数の XAD 間連携のポリシーを定義する場合に使われるべき「決めるべき事項」の雛形として使用できる。個人情報保護方針、文書形式と内容、役割とアクセス権限のある文書定義、運営組織等のポリシーに関わる内容等、があり、XDS モデルを採用しなくても役立つ文書である。セキュリティについても多くのページを割いて示してあり、安全管理ガイドラインとの関連も深い。

### 2. ネットワーク上の安全性

ここでは、オープンなネットワークで接続される場合を解説する。閉域 IP 通信網であっても、中間で閉域ネットワークが相互接続する場合は「オープンなネットワーク」とする。安全管理ガイドラインにおいては、ネットワーク上での盗聴、改ざん、成りすましへの対応を、チャネル(ch)セキュリティ(回線上での暗号化などのセキュリティ)とオブジェクト(obj)セキュ

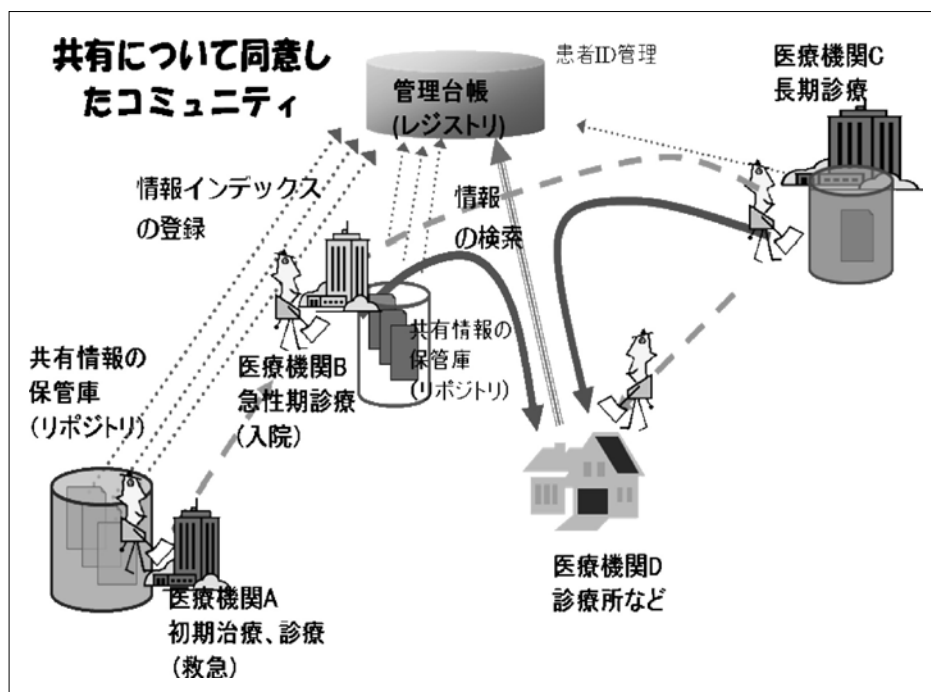


Fig. 1 XDS での医療連携シナリオ

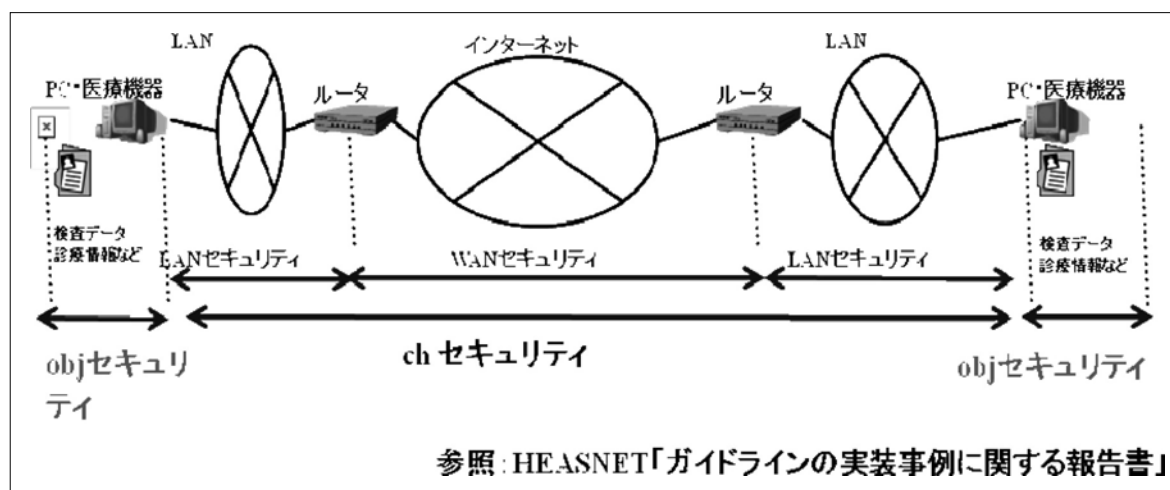


Fig. 2 オープンなネットワーク接続のセキュリティ対策

リティ(電子署名等の情報の内容へのセキュリティ)で要求している。Fig. 2 でこの概念を示す。

## 2-1 技術的対策

セキュリティ対策の目的は、意図した宛先にのみ、安全に送信されることである。そのためのセキュリティ対策であり、安全管理ガイドライン(6.11章)ではネットワーク種別の選定基準・安全管理とネットワーク事業者との責任分界の考え方(2-2に示す)とともに、以下のことを示している。

### ①チャネルセキュリティの確保

通信の起点・終点識別の認証と成りすましへの対策(相互認証)として、IPSec(internet protocol security)

+IKE(internet key exchange)で実行すること。

### ②オブジェクトセキュリティの確保

盗聴への対策として暗号化(電子政府推奨暗号を使用)、改ざんへの対策として電子署名(HPKI)+タイムスタンプを施すこと。

参考資料である HEASNET の資料では、VPN(virtual private network)利用でも設定によっては危険があり、以下の四つの対策を求めている。

### ◆VPN 接続経路の分離

通信ルートを分けることで外部からの不正なアクセスを防止し、VPN 接続のセキュアな経路を確保する。インターネット接続点において、VPN 接続とそれ以外の一般的な接続とで経路を物理的に分離し、VPN

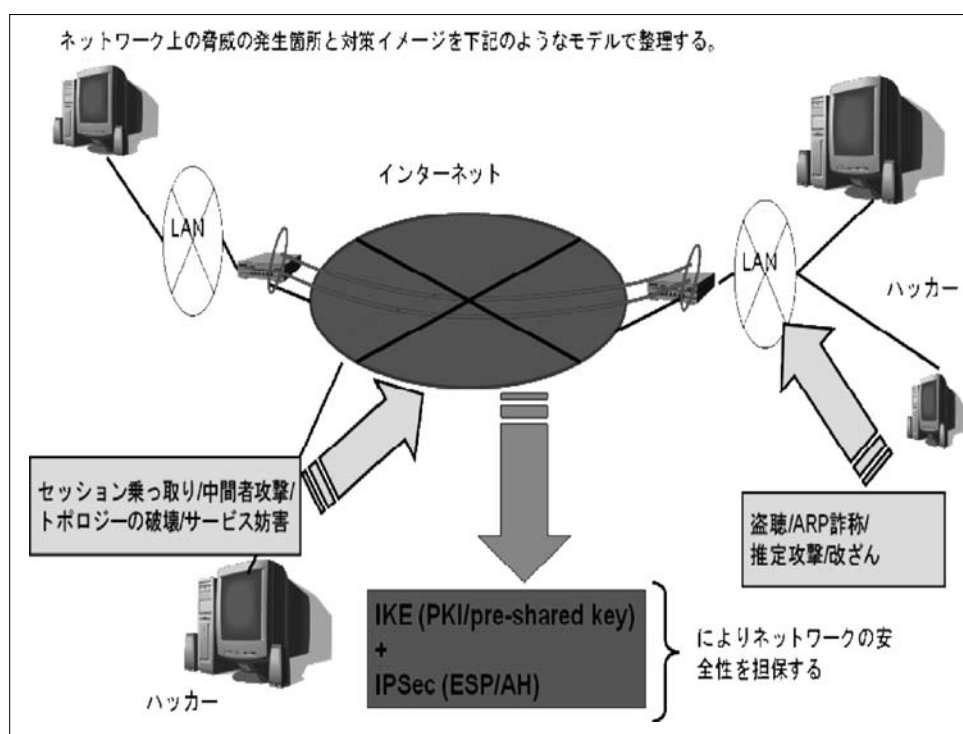


Fig. 3 オープンなネットワーク上の脅威とチャネルセキュリティ対策

接続の場合はFW(fire wall)透過後に必ず認証によって適正な接続が担保されるようにする。

#### ◆異なるVPN間の経路制御

リモート保守や情報提供サービスにおいて、契約に定められたリソース以外への不正なアクセスを防ぐため、ローカル拠点のホストまたはIPアドレスレベルで制御し、拠点間で接続されたVPNによって拠点内の許可されていないリソースに対してアクセスされないような制限を設ける。

#### ◆VPN間の不正中継禁止

ある拠点(A)の二者間契約(A-B, A-D間)で形成された二つのVPN接続によって、これらの契約の当事者でない二つの拠点(B, D)間でのVPN接続(B-D間)ができないよう、ある拠点を經由しての不正な中継アクセスを禁止する。

#### ◆ゾーンの分離

VPN接続をする端末が配置されたVPN専用ゾーンとそれ以外の通常接続用ゾーンを設け、不適切なホストからのVPN接続を防止する。VPN接続専用ゾーンと通常接続用ゾーンの間の通信を制限する。

## 2-2 運用的対策

関係者間の契約を含めての運用的対策では、責任分界点を明確化して、管理責任の空白を作らないことである。

#### ①情報の送信側・受信側の責任分界点

送信側はどの時点までが責任範囲か、受信側はど

の時点から責任が発生するかの明確化。

#### ②通信を形成する事業者の責任分界点

上記の情報の送信側・受信側だけでなく、回線事業者、ネットワークサービス提供者の間で、誰がどこまで何を担保するか、ネットワークサービス提供者の管理責任範囲はどこまでか、の管理責任範囲を明確化し、事故発生時の一義的対応者を定めておくことが求められている。

## 2-3 IHEにおけるセキュリティ対策

IHEでは「HIE(health information exchange)Security and Privacy through IHE Profiles」文書において、SecurityとPrivacyに的を絞ったポリシー策定事項を述べている。既に定められている統合プロファイルのなかで、SecurityとPrivacyに関する統合プロファイルは下記がある。

- ・ audit trail and node authentication(ATNA)
- ・ consistent time(CT)
- ・ basic patient privacy consents(BPPC)
- ・ enterprise user authentication(EUA)
- ・ cross-enterprise user assertion(XUA)
- ・ personnel white pages(PWP)
- ・ digital signatures(DSG)
- ・ notification of document availability(NAV)

XDSモデルでシステムを構築する場合は、これらの機能を用いて安全管理ガイドラインの要求事項を満たすことが有用である。



### 3. 中核病院におけるセキュリティの運用

Symposium

奥田保男

岡崎市民病院

#### はじめに

医療情報の取り扱い、医療法等で医療機関等の責任で行うことが求められている。このことから、情報の収集、保管、破棄を通じて刑法等に定められている守秘義務、個人情報保護に関する諸法および指針のほか、診療情報の扱いに関わる法令、通知、指針等により定められている要件を満たすために適切な取り扱いが求められる<sup>1)</sup>。本稿では、中核病院におけるセキュリティの基本的な要件について、可搬型媒体(以下、媒体とする)などを用いてオフラインによる情報連携を行う場合とオンラインによる情報連携を行う場合を含めて述べる。

#### 1. 基本的な要件

##### 1-1 善管注意義務

電子化された情報は、紙の媒体やフィルム等比べてその動きが一般の人にとって分かりにくい、漏えい等の事態が生じた場合には、一瞬かつ大量に情報が漏えいする可能性が高いなどといった特殊性を持つ。医療機関は、医療情報を適切に管理するための善管注意義務(行為者の職業や社会的地位に応じて通常期待されている注意義務)を果たす必要があり、それぞれの医療機関が電子化の実施範囲およびその方法を検討し、導入するシステムの機能や運用計画を選択して、それに対し求められる安全基準等への対応を決めなければならない。この場合、通常の運用時での責任と、何らかの不都合な事態(典型的には情報漏えい)が生じた場合に対処すべき責任(以下、事後責任)とについて考える必要がある。

通常運用時での責任とは、医療情報の適切な保護のための適切な情報管理ということになるが、適切な情報管理を行うことがすべてではなく、説明責任、管理責任、定期的に見直し必要に応じて改善を行う責任を含む必要がある。説明責任とは、電子的に医療情報を取り扱うシステムの機能などが、その取り扱いに関する基準を満たしていることを患者等に説明する責任。管理責任とは、医療情報を取り扱うシステムの運用管理を行う責任。定期的に見直し必要に応じて改善を行う責任とは、情報保護体制が陳腐化しないように日進月歩である技術を適宜見直して改善する責任である。

事後責任としては、説明責任と善後策を講ずる責任がある。この場合の説明責任には、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明・公表も求めら

れる。善後策を講ずる責任としては、原因を追及し明らかにする責任、損害を生じさせた場合にはその損害填補責任、再発防止策を講ずる責任などがある。

##### 1-2 本人性の確認

医療情報は機微な個人情報であるため、許可された者に限定して利用できる仕組みが必要であり、ここに「本人性」が重要となる。また、医療機関には多くの職種が従事するため、職種、所属あるいは役職などに応じて情報の区分管理とアクセス権限の管理(Table 1 参照)を行う必要がある。本人性を確認するための認証方法としては、記憶によるもの(ID、パスワード)、生体的な特徴を利用するもの(指紋、静脈、虹彩)、物理媒体を利用するもの(IC カードなど)があるが、厚生労働省から出されている「安全管理ガイドライン」では、2 要素認証を採用することが望ましいと記載されている。また、認証のために使われる情報の確かさといった問題も重要である。

複数の医療機関における情報共有は、コミュニティを形成した医療機関において技術的な手法と管理を含めた運用を統一的に取り決める必要がある。当然のことながら医療機関を越えて本人性を確保する必要があるが、個人の情報の登録などの運用を含め難しい問題がある。ここで、HPKI を用いることで本人性・実在性・国家資格の有無は認証することはできる。ただし、医療機関での役職、所属などの情報を HPKI では網羅していないため、これだけで運用できるとはいえない。

##### 1-3 不正ソフトウェア対策

セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こす代表的な不正ソフトウェアとしては、ウイルスやワームなどがある。これらへの対策としては、不正ソフトウェアのスキャン用ソフトウェアの導入が最も効果的である。

その他、医療機関において用いるアプリケーションが相互に干渉し、動作などに障害をきたす場合がある。対策として、アプリケーションの同居テストを行うことはもちろん必要であるが、どのようなアプリケーションがどの端末に入っていて、その端末の所在管理をすることも必要である。これを実際に行うためには部門による管理ではなく、総合的に管理を行う組織体制が必要となる。

Table 1 職種別登録一覧

■ : 電力LPW必要	電子カルテ	手術管理システム	汎用印刷システム	患者認証	汎用予約一覧	録入院予定オーダー医師確認登録	看護Web起動画面	ME臨床システム	手術状況一覧	生物由来物質管理システム	病診連携システム	ICU管理システム	麻薬施用者番号一括更新	薬引換え番号表示	RIS ■	GW	心電図Web	病理Web	医事システム	眼科システム	内視鏡システム	PACS ■
医師	○	○	○	○	○	○	○	○	○							○	○	○				○
医師(定期代務)	○	○	○	○	○	○	○	○	○								○	○				○
看護師・助産師	○	○	○	○	○	○	○	○	○							○						○
重症系看護師(救命センター・NICU)	○	○	○	○	○	○	○	○	○							○						○
看護師・助産師(手術室)	○	○	○	○	○	○	○	○	○							○						○
看護師・助産師(救外部門)	○	○	○	○	○	○	○	○	○						○	○						○
情報管理室	○	○	○	○	○	○	○	○	○						○	○						○
薬剤師	○	○	○	○	○	○	○	○	○				○	○		○						
放射線技師	○		○		○		○	○	○				○	○		○	○					○
検査技師	○		○		○		○	○	○	○						○	○					○
検査技師(生理)	○		○		○		○	○	○	○					○	○						○
栄養士	○		○		○		○	○	○							○	○					
病歴師	○		○		○		○	○	○							○	○		○			
医事事務員	○		○		○		○	○	○							○	○		○			
臨床工学技士	○	○	○		○		○	○	○							○	○					○
臨床工学技士(エコー)	○	○	○		○		○	○	○						○	○						○
保健師	○		○		○		○	○	○							○	○					
療法士(理学療法士・作業療法士・言語療法士・その他療法士)	○		○		○		○	○	○							○	○		○			○
外来診療(視能訓練士・歯科衛生士・心理療法士)	○		○		○		○	○	○							○	○					
ソーシャルワーカー(社会福祉士)	○		○		○		○	○	○							○	○		○			
病診連携	○		○		○		○	○	○		○								○			○
予約(クレーク)	○		○		○		○	○	○										○			
総務課(用度班)																○			○			
総務課																○						
医師(消化器科)	○	○	○	○	○	○	○	○	○							○	○	○			○	○
医師(外科)	○	○	○	○	○	○	○	○	○							○	○	○			○	○
医師(眼科)	○	○	○	○	○	○	○	○	○							○	○	○		○		○
医師(泌尿器科)	○	○	○	○	○	○	○	○	○						○	○	○	○				○
医事事務員(手術室看護助手)	○																					

#### 1-4 その他の安全管理対策

病院情報システムのサーバ、情報が保存された媒体等などは、セキュリティ区画を定義し入退室の管理、機器の盗難や紛失防止を含めた保護および措置を、物理的な方法によって行うことが求められる。

また、セキュリティ対策とは技術的あるいは物理的に行うことばかりではなく、病院情報システムを利用する者の責任と権限を明確に定め、規定や手順書を整備運用し、その実施状況を点検等によって確認することが求められる。これには、安全管理対策の評価、見直し、改善を組織的に行う必要があり体制の整備が重要である。そして、教育、訓練など人による誤りを防止することを目的とした対策もおおそかにせず定期的に行わなければならない。

## 2. 他の医療機関との情報連携

診療情報を他施設と連携する場合の手法として、情報交換(exchange)と情報共有(sharing)とがある。情報交換としては、媒体を利用してオフラインで行う、あるいは遠隔画像診断など特定の相手(施設、個人)とpoint-to-pointの通信を行う場合などが想定される。

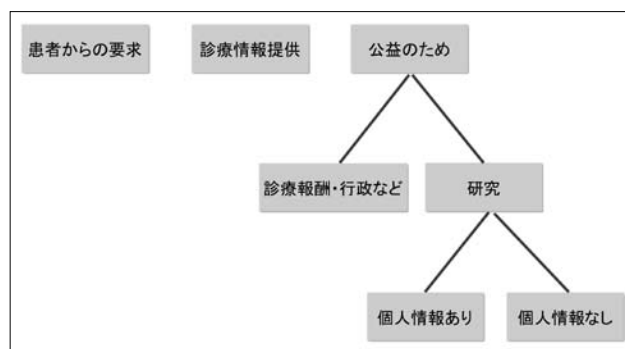


Fig. 1 電子的に情報を出力するケース

情報共有としては、複数の施設をオンラインで結び情報を連携地域内で長期にわたって共有する場合などが想定される。

#### 2-1 情報交換

画像情報などを媒体に出力するケースとしては、Fig. 1に示すものなどがあるが、前述した善管注意義務を果たすためにも、どのケースにおいても患者が不利益にならないように情報を取り扱わなければならない。

```

<?xml version="1.0" encoding="Shift_JIS" standalone="no" ?>
<AuditMessage>
  <EventIdentification EventActionCode="C" EventDateTime="2009-04-08 16:52:39"
EventOutcomeIndicator="0">
    <EventID code="RegistDecision" displayName="予約申込の登録(確定)" originalText="予約申込の登録(確定)
(C:create)" />
    <EventTypeCode code="RegistDecision" displayName="予約申込の登録(確定)" originalText="予約申込の登
録(確定)(0:sucsess)" />
  </EventIdentification>
  <ActiveParticipant AlternativeUserID="" NetworkAccessPointID="172.XX.XX.XX"
NetworkAccessPointTypeCode="2" UserID="57" UserIsRequestor="true" UserName="奥田 保男">
    <RoleIDCode code="01" displayName="医師" originalText="0000000087" />
  </ActiveParticipant>
  <AuditSourceIdentification AuditEnterpriseSiteID="奥田内科" AuditSourceID="57">
    <AuditSourceTypeCode code="1" displayName="end-user-interface" originalText="" />
  </AuditSourceIdentification>
  <ParticipantObjectIdentification ParticipantObjectDataLifeCycle="1" ParticipantObjectID="000000XXXX"
ParticipantObjectSensitivity="1" ParticipantObjectTypeCode="1" ParticipantObjectTypeCodeRole="1">
    <ParticipantObjectIDTypeCode code="000000XXXX" displayName="岡崎 太郎" originalText="変更前ステータ
ス:変更後ステータス:2" />
    <ParticipantObjectName>予約情報(患者名:岡崎 太郎)</ParticipantObjectName>
    <ParticipantObjectDetail type="text" ==> />
  </ParticipantObjectIdentification>
</AuditMessage>

```

Fig. 2 アクセスログ

患者本人が何らかの目的で医療情報を利用するために情報を提供する場合には、医療機関はその提供の正当性だけが問題であり、適切に本人に提供されていれば、その後の責任は本人に生じる。しかし、適切に扱われないことを知りながら情報提供した場合には、医療機関の責任が追及され、少なくとも医療機関の公共性を考えると不信を招くことになる。

診療情報提供あるいは公益のための情報出力の場合、至極当たり前であるが適切な情報が提供される必要がある。ここで、依頼者(出力すべき情報の選択者)と出力作業者が異なる場合、出力作業者に出力すべき情報が依頼者からの確に伝達される業務フローの確立が重要となる。また、医療機関のどこで情報を出力できるのかといった環境・設備的な問題、あるいは個人のモラルの問題、この作業歴の保存などを含めたセキュリティ対策を考える必要がある。

ケースとして、患者情報を持たない画像の出力、一つの媒体に複数の患者の情報を混在、独自の手法による保存および圧縮などにより、情報の混同あるいは読めないといった状況が起こる場合がある。これへの対策としては、情報を出力するための手段・フォーマットを標準的なものとすべきであり、IHEに示されている可搬型媒体による画像情報交換(PDI: portable data for imaging)に準拠することが求められる。また、医療機関に持ち込まれた情報を PACS に取り込む場合、患者情報などを自施設の情報に置き換える必要がある。これを行うための技術的な要件も IHE に画像データ取り込み時の患者情報の整合性

確保の方法(IRWF: import reconciliation workflow)として示されている。ここには、DICOM の MWM (modality worklist management)を用いる方法と、医事システムなどから HL7(health level seven)を利用して患者情報を取得し、情報を修正したうえで PACS に取り込む手法が示されている。どちらの手法を用いるにしても情報の置き換えには細心の注意が必要であり、誰がどの情報をいつ、どのように変換したかの履歴を残すことも忘れてはならない<sup>2)</sup>。

## 2-2 情報共有

オンラインによる施設間連携を実現するためには、技術的には情報の共有化、蓄積、解析、再構築、返信や再伝達、セキュリティを含め相互運用性の考え方が重要であり、運用的な内容としてもコミュニティを形成した施設間において組織規程(構成、経済的、責任分界点、法的事項の管理、債務、免責事項)、運用規程(保守・管理)、システムの仕様について(GUI、ユーザ認証、監査証跡)などの協議が必要である。例えば、各施設間において、患者 ID の整合性あるいは結びつけを行わない限り、誤った患者の診療情報を閲覧する可能性が生ずるなど、情報を安全に共有することは難しい。しかし、これを行うにはサーバの設置場所、導入費用、人件費、運用・管理手法などを詳細に検討する必要がある。

また、利用が正しく行われていることを監査する必要もある。Fig. 2 に筆者が勤務する岡崎市民病院においてクリニックからの診療予約を取得する時のアクセ

スログを示す。これは IHE の profile である ATNA に基づいたものであるが、クリニック自体が購入した端末に設定を行う必要があり保守および管理面に問題を残す。

その他、情報共有を行う時に利用できるおもな IHE の profile を以下に示すが、詳細については <[http://www.ihe.net/Technical\\_Framework/](http://www.ihe.net/Technical_Framework/)> にある

IHE ITI 分野技術仕様書である IT Infrastructure Technical Framework を参考にして欲しい。

- ・情報共有の基盤：Cross-Enterprise Document Sharing
- ・患者 ID の相互参照：Patient Identifier Cross-Referencing
- ・患者の問い合わせ：Patient Demographics Query

## 参考文献

1) 厚生労働省. 医療情報システムの安全管理に関するガイドライン 第4版 2009.

2) 奥田保男. 地域連携と IHE. 2009: 98-99.

## 4. 連携医療を支えるセキュリティ

Symposium

水野正明<sup>1)</sup>, 吉田 純<sup>2)</sup>

1) 名古屋大学大学院医学系研究科遺伝子治療学分野

2) 独立行政法人国立病院機構東名古屋病院

### はじめに

社会基盤の IT 化が世界規模で加速している。医療も例外ではない。そしてそれに合わせ、わが国の医療提供体制も大きく変わりつつある。連携医療はそのような社会構造の変化のなかで生まれてきた新しい医療スタイルである。ここでは連携医療構築に向けての取組みを、自験例を通して紹介し、その医療を支える電子基盤とセキュリティについて解説する。

### 1. 連携医療とは

“連携医療”の定義にはいくつもあるが、われわれは医療分野において従来築かれてきた病診連携や病病連携といった“医療連携”とは違ったものとしてとらえている。すなわち、これまでの“医療連携”が医療機関主体のつながりであったのに対し、“連携医療”は患者や市民が主体となるつながりと考えている。その目指すところは患者・市民中心の医療である。

脳卒中医療を例にして考えてみよう。現行の脳卒中医療では、疾病発症から社会復帰に至るまでには、救急救命士による病院前救護、急性期病院での急性期医療、回復期病院あるいは施設での回復期リハビリテーション医療、診療所(かかりつけ医)での維持期医療、その後障害の程度による違いはあるが介護ないし在宅医療等が展開される。脳卒中医療は決して一つの医療機関では完結しない。しかしながら現状ではこれらの医療機関がそれぞれ独立しており、必ずしも患者を中心とした連携が取れているわけではない。患者・市民中心の医療提供体制を真に構築するには、この連携を強固にした連携医療体制の確立が待たれている。

### 2. 連携医療を構築するための取り組み(自験例を含む)

連携医療を構築するための実証事業として、われわれは平成 18 年度から 3 年間経済産業省委託事業「地域医療情報連携システムの標準化及び実証事業」を実施してきた。この事業のなかでわれわれは脳卒中医療と周産期医療を取り上げ、電子基盤に支えられた連携医療のあり方を検証し、その有用性を実証した。

連携医療の構築を目指すにあたり、最も重要なものが連携施設間の共通ルールの作成である。まだ特定の疾患に限られているが保険医療制度上では、その共通ルールを“地域連携クリティカルパス”として文書化することが求められている。そこでわれわれは従来の脳卒中医療にとらわれずに脳卒中の連携医療を考えた場合、地域連携クリティカルパスに掲載されるべき連携情報とはどんなものかといった基本に戻って検討を始めた。その結果、これまでの脳卒中医療で使われてきた診療情報では十分でないことがわかった。例えば、これまで急性期病院から回復期リハビリテーション病院へ送られていた診療情報の内容は、いつ入院し、どのような手術または治療をし、どのような障害が残ったか等をまとめたサマリーであった。これらの情報も重要ではあるが、回復期リハビリテーション病院や施設がそれ以上に望む診療情報とは、一人で歩けるのか、一人でトイレが行えるのか、一人で食事ができるのか、介護人はいるのか等の極めて具体的な日常生活動作(ADL)に関わる情報であった。そこで、本事業ではこれらの情報を優先的に伝送できる仕組みを作った。さらにそれらの情報のソースをすべ

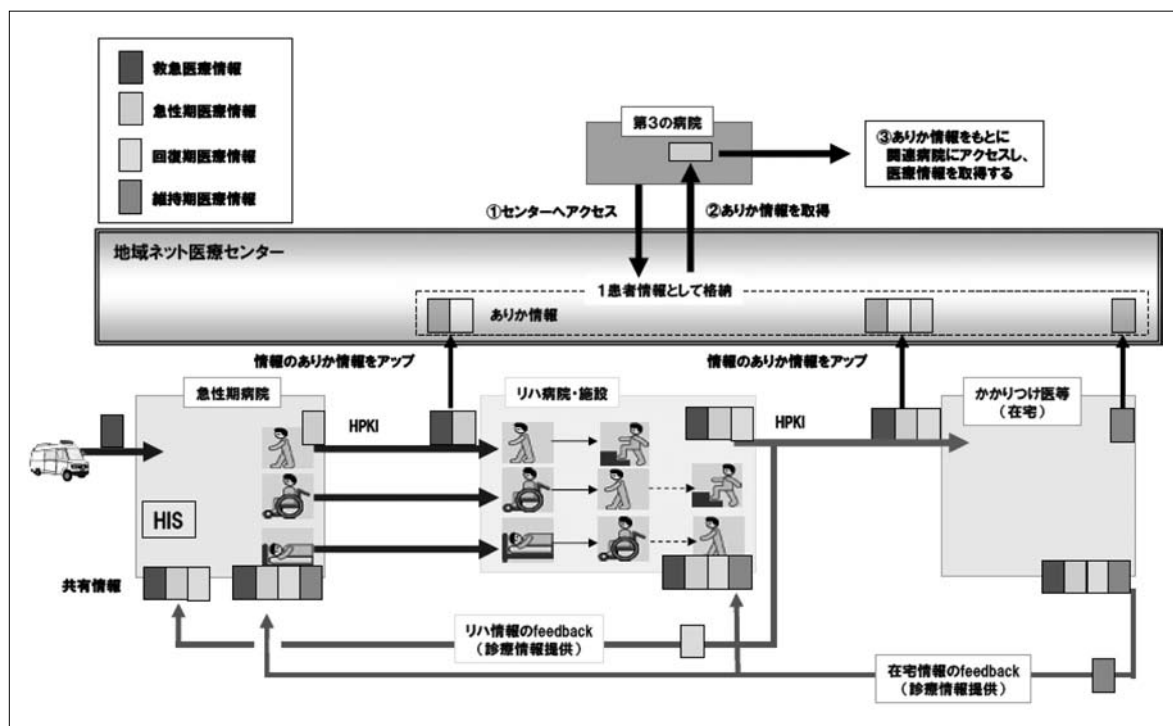


Fig. 1 脳卒中地域医療情報連携システム NAGOYA-Regional Health Information Exchange for Stroke

て主治医が一人で入力するのではなく、看護師、理学療法士、作業療法士、言語聴覚士、メディカルソーシャルワーカー、事務員等多くの異職種の方々がそれぞれの担当分を入力し、情報を合算することで信頼性を高めた。そしてこの仕組みがあれば充実した情報が得られるばかりでなく、担当者一人一人の労力の低減につながることもわかった。

次に作成した地域連携クリティカルパスを、紙ベースの運用から電子基盤上での運用へと発展させた。電子基盤上で地域連携クリティカルパスを運用するためにはクリアすべき大きな課題が二つあった。その一つが医療情報の標準化であり、もう一つが医療情報の共有化である。前者(標準化)を実現するための最初の課題は、脳卒中医療分野における医療情報の規格化および用語の統一であった。世界的な流れを鑑み、本事業では診療情報に関しては HL7 CDA R2 を、検査情報に関しては HL7 V2.5 を、画像情報に関しては DICOM をそれぞれ採用した。また、現行では定義されていない診療情報に関しては、日本 HL7 協会と日本医師会総合政策研究機構のそれぞれが策定した診療情報提供書の規格案(HL7 CDA R2)と J-MIX を基に新たに作り込んだ。現在この新規規格案については、担当組織による審議を通して汎用性のある形にすべく必要な手続きが進められている。一方、後者(共有化)を実現するためには、医療情報の所在を管理するレジストリデータベースと、医療情報

をほかの医療機関に送信するために医療情報を格納するリポジトリデータベースの構築が必要となった。このレジストリ・リポジトリシステムを動かす仕組みについては、IHE が策定し、その仕様を公開している XDS を採用した。

そしてこれらの考え方や仕組みを統合して、脳卒中連携医療を電子基盤上で実現するためのシステム、すなわち脳卒中地域医療情報連携システム[NAGOYA-Regional Health Information Exchange(RHIE)for Stroke](Fig. 1)を完成させ、その有用性を実証した。

### 3. 脳卒中地域医療情報連携システム(NAGOYA-RHIE for Stroke)におけるセキュリティ

セキュリティについては、厚生労働省の「医療情報システムの安全管理に関するガイドライン」に則って、情報の漏洩や改ざん、消失などの事故が起きないようにアクセス制御を含む利用者認証、監査証跡(アクセスログ)、電子署名システム等を実装した。同時にセキュリティポリシーを含め運用管理マニュアルも策定した。その一部を以下に示す。

#### 3-1 システム基盤(ネットワークインフラの構築)

##### 3-1-1 地域ネット医療センターと医療機関とのネットワーク接続

名古屋大学医学部附属病院内に、XDS サーバならびに PIX(patient ID cross referencing)サーバ機能を

有する地域ネット医療センターを立ち上げ、ファイアウォールルータを介して 100 M の光ファイバーネットワークと連結し、各医療機関との接続を可能にした。この光ファイバーネットワークは、名古屋大学医学部附属病院のゲートウェイサーバ用の回線とは別回線にするとともに、ファイアウォールルータでは、経路の制御とフィルタの組み合わせでサーバへのアクセスを制限するセキュリティ制御機能を付加した。

### 3-1-2 医療機関間ネットワークの構築

医療機関間ネットワークに接続する医療機関にはそれぞれファイアウォールルータとゲートウェイサーバを設置し、利用者端末としての PC を接続した。利用者端末がアクセスできるのは自らのゲートウェイサーバのみとし、センターサーバおよびほかの医療機関のゲートウェイサーバとの通信は認証を得たゲートウェイサーバ間のみとなるよう、ファイアウォールルータに経路の制御とフィルタの組み合わせを設定した。この仕組みのもとで、愛知県内 31 の医療機関を接続した。

## 3-2 システムセキュリティ

地域医療情報連携システムのレジストリ・リポジトリ機能には、上記のネットワーク制御に加え、連携情報(診療情報、検査情報、画像情報)の実体を医療機関の連携ゲートウェイ上に格納して配信・共有することから、個人情報に対する情報セキュリティ管理に対応できるような機能を実装した。

### 3-2-1 アクセス制御を含む利用者認証

利用者認証は、既設インフラである操作端末の生体認証とアカウント・パスワードの組み合わせで操作を行うこととした。一方システム上では同時に、XDS とシングルサインオン(OpenSSO: single sign-on を利用)を組み合わせた X509 形式証明書によるユーザ認証を

行う仕組みとした。共有情報へのアクセスは、情報の提供元である医療機関が公開を許可する医療機関を指定し、指定された医療機関の利用者だけがその情報を取得できるように制御した。情報のアクセス権限は、利用者の職種によって制限する機能を開発・実装した。

### 3-2-2 監査証跡(アクセスログ)

共有情報へのアクセスの痕跡を記録する監査証跡については、保健医療福祉システム工業会(JAHIS: japanese association of healthcare system industry)の監査証跡のメッセージ標準規約をベースとして、アクセスログの収集・検索・表示機能を開発・実装した。

### 3-2-3 電子署名

電子署名については、MEDIS-DC の HPKI 認証局証明書サービスを利用した。

### 3-2-4 その他

ネットワークインフラは閉域となっており、回線を契約した参加医療機関以外ではアクセスすることができず、加えてファイアウォールルータによる制限も設け、サーバ間の通信を暗号化することで盗聴による情報搾取にも対応した。

## おわりに

整形外科疾患である大腿骨頸部骨折と脳卒中で始まっている地域連携クリティカルパスをもとにした連携医療は、今後がん、心筋梗塞、糖尿病で展開されるものと思われる。各地での取り組みの多くは紙ベースでの連携であるが、これも近く電子基盤に移行していくものと予想される。本稿ではその先駆けとして、われわれが実施してきた平成 18 年度経済産業省委託事業「地域医療情報連携システムの標準化及び実証事業」の実績を中心に解説し、電子基盤上で脳卒中連携医療を支える次世代の脳卒中地域医療情報連携システム(NAGOAY-RHIE for Stroke)を紹介した。