患者情報管理体制の点検整備と双方向性情報シェア開発研究

研究分担者 山下 俊一
長崎大学大学院医歯薬学総合研究科

研究要旨

エイズ患者情報管理体制の点検整備についての問題点を明らかにする為に長崎大学に設置されている原爆被爆者データベース 30 年の歩みを総括し、その比較検証から今後の A-net の改善提言を研究目的とする。平成 21 年度は原爆被爆者データの内容を、①基本情報、②健康情報、③健康カルテ画像情報、④死亡情報、⑤腫瘍登録情報、⑥被曝線量情報、⑦その他に大別して検討した。被爆者 12 万人のデータの暗号化とリンケージによる疫学研究・医学研究等の活用以外に、患者の利便性を視野に関連病院との相互活用が課題であり双方向性情報シェアに関する新展開が必要である。

HIV 診療支援ネットワークを活用した診療連携は、長期療養を余儀なくされる患者の利便性と安全性を確保しつつ、新たな A-net の構築が早急に求められる。

A．研究目的

A-net の今後の新展開に貢献するため、原爆被爆者データベースの概要を取り纏め、エイズ患者情報管理体制の点検整備についての課題を抽出し、A-net の改善に向けた提言を研究目的とする。

B．研究方法

長崎大学大学院原爆後障害医療研究施設（原研）で対応している述べ約 12 万名の長崎市被爆者検診データ収集活用を、①基本情報、②健康情報、③健康カルテ画像情報、④死亡情報、⑤腫瘍登録情報、⑥被曝線量情報、⑦その他に大別して検討した。情報資料室の三根真理子准教授、横田賢一技官の協力による後ろ向き情報収集で定性かつ定量的解析を行い、利用頻度につても検討を行った。

（倫理面への配慮）

既報の資料を基に解析し、データは不特定非連結型で倫理規定に反しない配慮をした。

C．研究結果

被爆者データベースに収録されている 12 万人（1957 年から 2009 年 7 月）を原爆被爆者手帳保持者 29 万件、氏名 14 万件、住所 30 万件、検診結果 331 万件、原

爆手当56万件、死亡4.5万件、腫瘍登録3.8万件を母体として協定を締結した関係各機関と入力とデータ活用を継続している。これら登録データを中心に下記の7項目の解析結果を得た。

①基本情報

氏名、生年月日、住所、被爆状況情報を基本として追跡対象者76,954名(1970年生存者)のうち生存者24,034名(31.2%)死亡33,814名(43.9%)であり、転出その他で追跡不能例が19,105名(24.8%)であることが判明した。

②健康情報

健診委託医療機関からのデータは、一般、精密、がん検査の結果、その判定、診断結果がデータベースに登録され、患者への結果報告が原研から医療機関等へフィードバックされている。

③健診カルテ画像情報

健診カルテは医師の所見や治療中の疾病名等の記載があるカルテ画像が健診情報とリンクしてデータベース化されている。現在2001年度までの診療カルテのべ124万人分、170万枚の画像がデータベースとして収録されている。

④死亡情報

死亡診断者に基づき死亡原因が国際疾病分類(ICD)でコード化されている。死亡データは毎年一度長崎市死亡診断書との照合が行われ精度向上が図れている。

⑤腫瘍登録情報

長崎県がん登録情報の提供が協定化で推進され、データの活用が資料利用申請書を基に促進されている。

⑥被曝線量情報

被爆時の爆心地からの距離を100mごとに基本情報として復元地図の上から同定し、さらに旧線量推定方式であるT65 D線量および広島大学で開発されたABS93D線量推定方式に準じた方法で算出されリンケージされている。

⑦その他

各種調査とのリンケージが使用許諾を受けて活用されている。

以上の原爆被爆者追跡調査データベースを基本として健康医療情報の提供機能と役割が30年間随時更新されながら、レンタル事業として継続されている。

一方A-netは電子カルテとしての先行機能が優先され、入力内容が多岐にわたりソフト面での対応も硬直化し、臨床現場での活用が乏しく平成21年6月に運用が停止されている。しかし、患者情報の登録と臨床疫学データの供与は必要不可欠であり、A-netの新たなシステム構築が、患者の利便性と秘匿性を担保した上で強く望まれる。

D．考察

A-netの情報収集活用と対峙比較して原爆被爆者データの収集方法と検索頻度について検討した。原爆被爆者データはクローズドな放射線影響研究所コホート調査集団に対して長崎大学大学院原爆後障害医療研究施設(原研)で対応している述べ約12万名の長崎市被爆者検診データ収集活用は医療現場での利用頻度も高く、今後情報の秘匿性と公開性をどのように担保してエイズ患者情報収集活用を展開するかきめ細かな比較検証が必要である。現在長崎市原爆被爆者4万5千人の検診データが長期継続登録されている。従来からのエイズ患者情報収登録収集は極めて重要なデータバンクであり、医療サイドでのアクセスビリティのみならず医療者と患者双方向性の利用活用に

向けた対面式活用など患者参加型の新たな取組も必要となるものと予想される。

A-net の更なる利用頻度の増加に向けた有益性と効率性の改善改良が期待される。

E．結論

被爆者データベース 30 年の歩みを総括し、更なるデータの拡充と臨床研究への情報提供が新たな課題解決に向けて必要であることが再認識された。同様に HIV 診療支援ネットワークを活用した診療連携は、長期療養を余儀なくされる患者の利便性と安全性を確保しつつ、新たな A-net の構築が早急に求められる。

F．健康危機情報

無し

G．研究発表

1. Yamashita S: Molecular targeted therapy for thyroid cancer in Japan: a call to reduce the backlog. Endocr J 56(8): 919-920, 2009
2. Matsuse M, Mitsutake N, Nishihara E, Rogounovitch T, Saenko V, Rumyantsev P, Lushnikov E, Suzuki K, Miyauchi A, Yamashita S: Lack of GNAQ hotspot mutation in papillary thyroid carcinomas. Thyroid 19(8): 921-922, 2009
3. Drozd VM, Lushchik ML, Polyanskaya ON, Fridman MV, Demidchik YE, Lyshchik AP, Biko J, Reiners C, Shibata Y, Saenko VA, Yamashita S: The usual ultrasonographic features of thyroid cancer are less frequent in small tumors that develop after a long latent period after the Chernobyl radiation release accident. Thyroid 19(7): 725-734, 2009
4. Akulevich N, Saenko V, Rogounovitch T, Drozd V, Lushnikov E, Ivanov V, Mitsutake N, Kominami R, Yamashita S: Polymorphisms of DNA damage response genes in radiation-related and sporadic papillary thyroid carcinoma. Endocr Relat Cancer 16(2): 491-503, 2009
5. Taira Y, Hayashida N, Zhavaranak S, Kozlovsky A, Lyzikov A, Yamashita S, Takamura N: Urinary Iodine Concentrations in Urban and Rural Areas around Chernobyl Nuclear Power Plant. Endocr J 56(2): 257-261, 2009
6. Limsirichaikul S, Niimi A, Fawcett H, Lehmann A, Yamashita S, Ogi T: A rapid non-radioactive technique for measurement of repair synthesis in primary human fibroblasts by incorporation of ethynyl deoxyuridine (EdU). Nucleic Acids Res 37(4): e31, 2009
7. Ogi T, Limsirichaikul S, Overmeer RM, Volker M, Takenaka K, Cloney R, Nakazawa Y, Niimi A, Miki Y, Jaspers NG, Mullenders LH, Yamashita S, Fousteri MI, Lehmann AR: Three DNA Polymerases, Recruited by Different Mechanisms, Carry Out NER Repair Synthesis in Human Cells. Mol Cell 37(5): 714-727, 2010

2．学会発表

1. 1. Suzuki K, Yamauchi M, Suzuki M,

Oka Y, Yamashita S. Higher-order chromatin structure associated with radiation-induced genomic instability. The 2nd Asian Congress of Radiation Research, COEX, 2009

2. S Yamashita. Global Strategic Cancer for Radiation Health Risk Control in Nagasaki University, Radiation Risk Assessment in Medical Exposure: Shaping a global research agenda First Meeting, 2009
3. S Yamashita. Third Conference on Children's Environmental Health "Radiation safety in children's health care"2009
4. S Yamashita. Radiation Health Science from Radiation Life Science. First Open International Workshop of the Multidisciplinary European Low Dose Initiative (MELODI), 2009
5. S Yamashita. Current Condition and Future Scope of Global Radiation Health Risk Control. Japanese Society of Radiation Safety Management The 8th Annual Meeting: International Symposium, 2009
6. S Yamashita. Childhood Thyroid Cancer around Chernobyl. 2nd KID workshop in NIRS, 2009
7. S Yamashita. A multidisciplinary integrated approach for basic research on low dose risks. 2nd KID workshop in NIRS : WHO-GI meeting, 2009
8. 光武範吏、山下俊一. 甲状腺細胞における BRAF の機能. 第 82 回日本内分泌学会学術総会, 2009
9. Pavel Rumyantsev、Vladimir Saenko、Alexey Ilyin、Ulyana Rumyantseva、Tatiana Rogounovitch、光武範吏、山下俊一. Clinical course of papillary thyroid carcinoma in children and adolescent age groups. 第 82 回日本内分泌学会学術総会,2009
10. 平良文亨、林田直美、山下俊一、高村 昇. チェルノブイリ周辺におけるヨード充足状況の評価:都市部と地方の比較. 第 82 回日本内分泌学会学術総会, 2009
11. 山下俊一. 核災害と世界保健医療の対応～チェルノブイリ原発事故の経験～. 日本法科学技術学会第 15 会学術集会, 2009
12. Vladimir Saenko、Tatiana Rogounovitch、Natallia Akulevich、高村 昇、山下俊一. 放射線誘発甲状腺がんの分子疫学調査研究. 第 5 回広島大学・長崎大学連携研究事業カンファランス, 2009
13. 山下俊一. 長崎大学グローバル COE プログラムとの展開事業として. 第 5 回広島大学・長崎大学連携研究事業カンファランス, 2009
14. 山下俊一. 原爆後障害研究から世界の被ばく医療への展開. 第 50 回原子爆弾後障害研究会, 2009

H. 知的財産権の出願・登録状況

(予定も含む。)

1. 特許取得
   無し
2. 実用新案登録
   無し
3. その他
   無し

HIV診療支援ネットワークを活用した診療連携の利活用に関する研究報告書

（第 1.0 版）

平成 22 年 3 月 31 日

変更履歴表

項番	版数	変更理由	変更箇所	年月日	備考
1	1.0	新規		2010/01/08	

目次

図目次

表目次

第1章 はじめに

背景

『HIV 診療支援ネットワークシステム（以下、「A-net」と称する)』は、患者プライバシー保護を図りながら、患者の診療情報の一部をエイズ治療・研究開発センター（以下、「ACC」と称する）のホストコンピュータに入力し、エイズ治療・研究開発センターとエイズ治療ブロック拠点病院、拠点病院をネットワークで結ぶことにより、患者が受診される病院相互で診療情報を共有し、HIV 診療を円滑にし、かつ患者の地元で質の高い診療を可能にすることを目的としている。しかしながら、A-net は平成 10 年に試験運用を開始したシステムであり、システムを構成するハードウエアやソフトウエアの老朽化に加え、利便性という観点からみると満足のいくものではなく、蓄積されたデータ量とその内容からシステムそのものの利用価値も高いといえず、アクセス数も伸び悩んでいる状況である。また、当時は最新のセキュリティ対策を講じていたものが、年月の経過とともに近年のセキュリティ管理手法とは乖離したものとなりつつあり、更には現在一般的に用いられる汎用技術ではなく、あまり使われなくなった独自技術を採用していることが、今後のシステム改修や継続運用にあたっては大きな障害となってくる。

□HIV診療支援ネットワークシステム概要図(平成16年1月末現在)

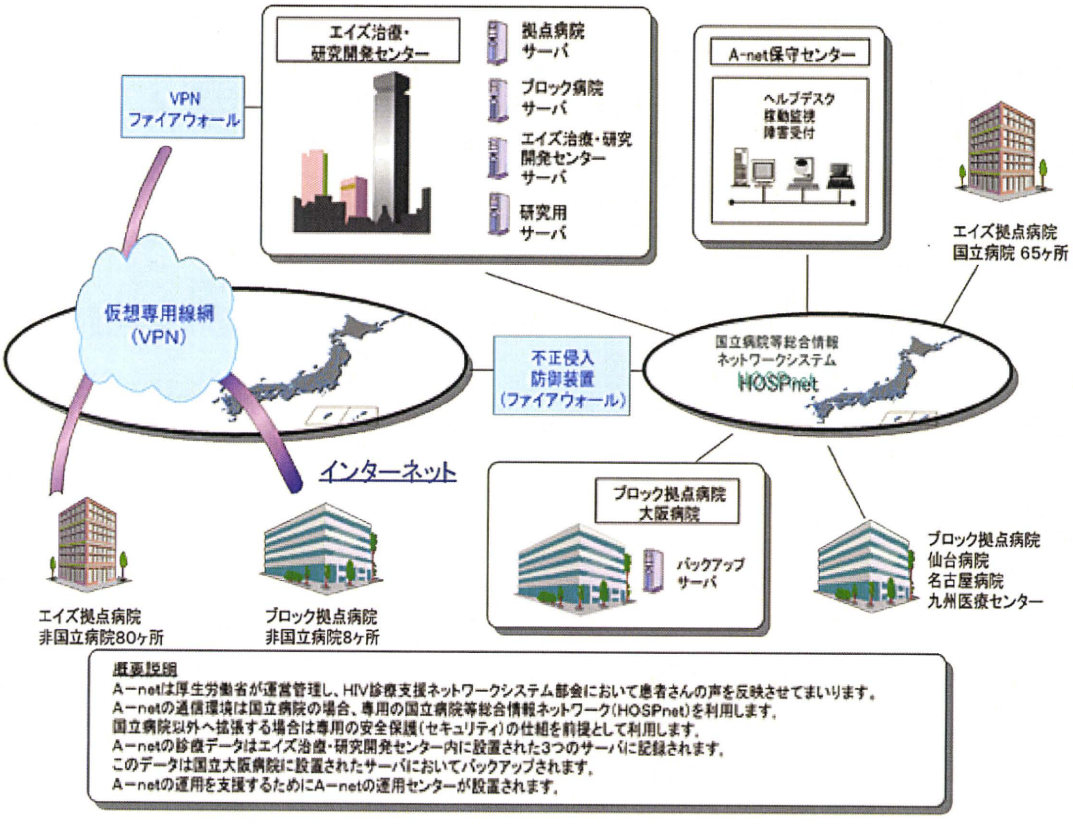


図1　HIV診療支援ネットワーク概要図

こうした状況を打開するため、現在のA-netに代わる次期A-netシステムの刷新に向け、現状の課題整理を行うとともに、医師及び患者からも積極的に利用される患者参加型システムの構築を目指し、その解決策や目指すべき方向について検討を開始した。昨年度は次期A-netのプロトタイプとなる長年蓄積可能なDBシステムを構築し、実際に医師による診療データの投入を行い、その有効性を検証した。

今年度は、ACC・エイズ治療ブロック拠点病院・拠点病院間をインターネット接続した際に、必要となる患者個人情報の取り扱い、プライバシー保護を担保する事を目的とした、暗号データ送受信プログラムを試作し、実際にデータの送受信を行うことで、有効性の検証を行う。

また、治療研究に必要な患者治療データについて、幾つかの医療機関の電子カルテシステムからの抽出を行う。抽出されたデータは、各診療機関によりデータ形態が異なるため、試作した暗号データ送受信プログラムを活用し、データ受信が完了した後、治療研究支援及び患者へのデータ公開を目的とし、データの加工及び加工の自動化を試みるツール等の試作検討を合わせて実施する。

今年度研究概要

1997年のACC開設以降、年間200名前後の新規患者が受診し、2008年には累積登録患者が2500名を突破。エイズ関連疾患は多岐にわたることから、患者ケアでは疾患ごとに各診療科との連携をとる必要がある。悪性リンパ腫では血液内科と連携をとり、サイトメガロウイルスによる疾患では眼科、カポジ肉腫では皮膚科、結核は呼吸器科との連携をとりながら診療を行っている。ニューモシスチス肺炎では口腔カンジダがほとんどのケースでみられるため、口腔外科、食道にまで浸潤している場合は消化器科との連携も欠かせない。このほか、生活習慣病の併発に対する腎臓内科、循環器科など、他科との連携がより重要になってきているのが最近の傾向である。

多剤併用療法（HAART療法）の登場で、HIV感染症は、医学的にコントロール可能な慢性疾患。抗HIV薬の進歩により治療の中心は外来となり、治療を開始した患者も、治療開始後の3～6ヶ月で状態は安定、その後は1～3ヶ月の間隔での外来通院。十分な抗ウイルス効果を得るためには、長期的な予後を考えた治療をする必要がある。感染者であっても、普通の人と同じように働きながら、主体的に治療と生活の両立に取り組み、副作用や合併症が併発しない限り、一端はじめた治療は途中で中断することなく継続しなければならない。

患者に対し、的確な服薬管理を実施するためには、患者一人一人に確かな治療経過、最新の健康状態を公開すると同時に服薬実施を促す必要がある。このため、エイズ治療各病院から患者治療データの蓄積場所となるHIV治療ブロッ

ク代表病院まで、安全に安心して運搬できるデータ通信の基盤構築が重要である。将来、患者所有の携帯型端末機器等への情報発信や情報公開、服薬自己申告等、医師や診療機関と一体となる患者参加型の医療が求められている。

昨今のネット通販、ネット銀行等、電子決済や電子取引で重要なことは、セキュリティが破られないことではなく、破られた時に誰がどう責任を負うか、損害賠償が重要となるが、エイズ治療患者にとっては、患者個人情報の取り扱い、プライバシー保護を担保する事が重要となり、通信路の暗号化だけでは不十分である。安全な暗号は、解読が困難な暗号であり、先験的に存在する概念でなく定義次第である。さらに、解読可能は現実世界で解読可能を意味するだけでなく、「理論だけでなく実装や運用も考慮」し、「現在あるいは近い将来の技術水準で脅威が現実のものになるかどうか」等で判断される。よって、暗号技術だけに頼らず、個人に関連する情報から、姓名、住所、電話番号、病院患者 ID、など個人の特定に結びつく情報をすべて除去し、又は再連結可能な情報を持たせずに分離し、個人を識別できないよう、その人と新たに付与された符号又は番号の対応表を残さない方法による匿名化を行う必要がある。「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成 16 年 12 月 24 日厚生労働省通知、平成 18 年 4 月 21 日改正）、「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 版平成 21 年 3 月厚生労働省作成）を遵守するものとする。そのため、データの暗号化と暗号化されたデータの分割、分割された暗号データの時間的・物理的な分割送受信、分割受信データの複合等、患者治療データの送受信プログラムを試作開発し、実インターネット上で安心安全を担保できることの有効性検証を行う。

別研究テーマにて、ある医療機関の電子カルテシステムから医療情報を交換するためデータ抽出を行う。抽出されたデータは、試作した暗号データ送受信プログラムを活用し、データ受信が完了した後、医師向け臨床研究支援及び患者向けデータ公開を目的とし、所定のデータ加工及び加工の自動化を試みる。データ解析、HIV 治療の予後改善を所定グラフ表示する等のツール試作を行い、患者へのデータ公開、臨床研究支援としての有効性を検証する。

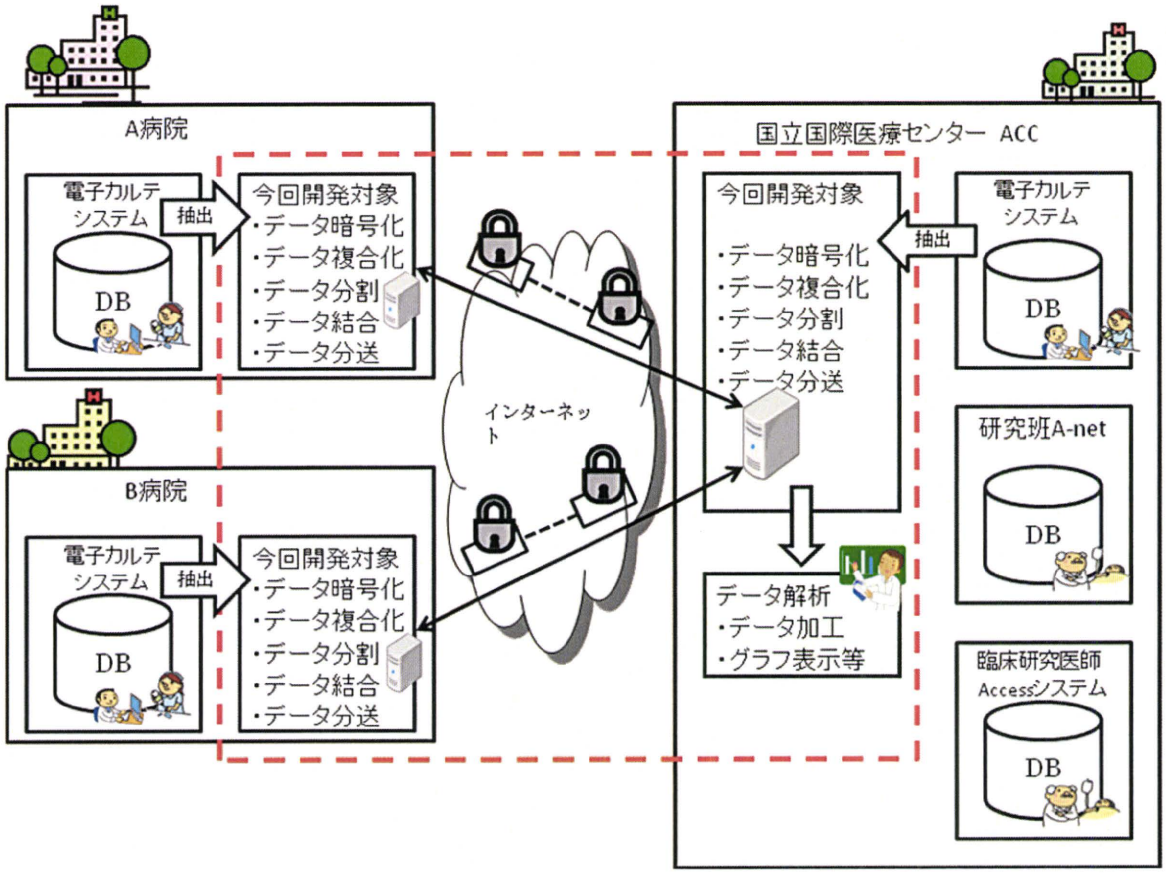


図 2　今年度実施研究概要

第2章 現 A-net 刷新に対する課題と対策

現 A-net を刷新する上での課題は以下の通り。

- HIS との連携を考慮する場合、医療機関毎に利用している HIS は様々である。その為、以下のような課題が考えられる。

  検査データの粒度が、医療機関毎にまちまちとなっている。各医療機関の HIS から抽出した検査データは、利用している HIS が違う為、抽出されるデータに差異が生じる。

  データのフォーマットも定義されている訳ではないので、抽出されたデータのフォーマットは統一されていない。(医療機関毎に独自のフォーマットである。)

- 検査結果データ・処方データをシステム上で扱う為に、患者データの匿名化が必要である。

  連結不可能データとして患者データを匿名化した場合、HIS とのデータ紐付けを行うことが不可能となる。連結不可能データである為、患者へのデータ公開を考えた場合、患者の特定が不可能になる。

上記の課題に対して、以下のアプローチで課題を解決する。

・A-net と各医療機関の HIS との連携について。

まず A-net として取り扱うデータを定義する。

どのようなデータを、患者に対して公開するのか？また、医師間では、どのようなデータを共有するのか？を考慮し、A-net で取り扱うデータを定義する。

データの定義が出来れば、各 HIS とのデータ連携については、以下のようなアプローチが考えられる。

各 HIS に対し、A-net で利用するデータを抽出する際のフォーマットを提示し、そのフォーマットに合わせたデータを抽出出来るように HIS を改変する。

各医療機関で利用している HIS から、A-net で定義したデータの抽出を行うことで、各医療機関でばらつきのあるフォーマットを統一して A-net に取り込むことが出来る。各 HIS から抽出した、A-net で利用するデータを、A-net で利用できるフォーマットに変換する、中間プログラムを作成する。中間プログラムを間に挟むことで、各医療機関でばらつきのあるフォーマットを統一し、A-net で利用するデータ定義と同様のデータとして A-net への取込が可能になる。

検査データの粒度が、医療機関毎にまちまちとなっていることについての対応は、各医療機関もしくは各医師で、入力するデータの粒度を統一する。利用している HIS 等で、入力可能なデータに制限がある場合等も考え

られる為、可能な限りA-net側で入力されたデータの粒度を吸収するような仕組みを考える必要がある。

・患者データの匿名化について。

医師間での患者データの共有を考えた場合、患者個人を特定する必要が無く、またHISとの連携も考えなければ、患者データの匿名化を行うことはさほど難しいことではない。一定のアルゴリズムをもとに患者番号を変換し、個人を特定しうるようなデータは、HISから連携させないか、連携されたとしてもA-net側で排除することで、患者データの匿名化を行うことが出来る。

患者個人を特定し、HISのデータとの連携を考えた場合、A-netで管理する患者データを匿名化（連結不可能データ化）してしまうと、HISとの連携は不可能になる。患者データの匿名化（連結不可能データ化）を行った上で、患者への検査結果データ公開、HISとの連携を行うことを実現する事は不可能である。

ただし、ある一定の条件（制約）を付けることで、患者データの匿名化を行うことは可能である。だが、匿名化の範囲が限定されてしまう為、本来の匿名化とはズレが生じる可能性がある。

患者へのデータ公開を考えた場合、A-netで管理している患者データと、公開用システムを使ってデータを閲覧しようとしている患者のデータを、紐付けることは必須である。患者データの特定が出来なければ、A-netで管理している患者のデータを、公開することは出来ないからである。

システムによる解決では無いが、公開する患者データについては、データ公開への同意をとりつけた患者のデータのみとする。

A-netで取扱う患者公開用データについては、匿名化（連結不可能データ化）を行わない。A-netで管理する患者データは、A-netで独自に採番した患者識別用番号を利用する。A-net ⇔ HIS間に中間サーバを準備し、HISから連携されてくる患者データの患者識別用IDから、A-netで管理する患者データに採番する、患者識別用番号へのデータ変換を行う。

このように中間サーバ上でデータ変換を行うことで、A-net ⇔ HIS間では患者データの匿名化を行う。(A-net上のデータを見ただけでは、容易にHISのデータを想定出来ない様にする。）この対応を行うことで、限定的な範囲ではあるが、患者データの匿名化（連結不可能データ化）を実現することが出来る。

第3章 暗号通信プログラムの試作開発と実証実験

暗号化通信ツールを試作する上で、この暗号化通信ツール試作の目的について記載する。
本研究の目的は次の通り。

患者に対し的確な服薬管理を実施する為に、患者一人一人に確かな治療経過、最新の健康状態を公開すると同時に、日々の服薬実施を促す必要がある。このため、エイズ治療を行っている各病院から、患者治療データの蓄積場所となるHIV治療ブロック代表病院まで、安全に安心してデータを運搬できる通信基盤の構築を行うことである。
このことを考えた場合、患者データの取扱い・プライバシー保護を担保した上で、患者データの各病院間での共有を実現する為には、インターネットVPNを利用したデータの送受信（通信経路を暗号化しただけのデータの送受信）では不十分である。またIP-VPNを利用したデータ通信では、インターネットVPNに比べセキュリティ等は向上するが、コストが高く将来の500拠点への展開を考えた場合、IP-VPNを利用することは難しい。

今回有効性を検証する研究内容は、IP-VPN等の高価な通信方式を利用せず、通常のインターネット回線を利用し、どのようにしてセキュリティ・プライバシー保護を担保した状態で、各病院間でのデータ共有（データの送受信）を実現するかということである。
今回は以下のような実装を行うことで、安心・安全なデータ共有（データの送受信）が行える環境が構築出来るかどうかの検証を行う。

・共有（送受信）するデータの暗号化。
・暗号化されたデータの分割。
・分割されたデータの時間的・物理的な分割送信（非同期送信）。
・分割されたデータの時間的・物理的な分割受信（非同期受信）。
・受信したデータの結合と復号による復元。

送受信するデータその物を暗号化することで、セキュリティを向上させる。こうすることで、通信経路の盗聴等でデータが漏洩した場合でも、容易にデータを復元することは出来ず、また、盗聴したデータを見ただけでは、データの内容を推測することは出来ない。

暗号化したデータを分割し、時間的・物理的に分割して送信することで、セキュリティをさらに向上させる。分割されたデータは全てを揃えて、分割された順序通りに結合しなければ、復号することは不可能となっている。データを分割する数もランダムに設定することで、第三者はデータが幾つに分割されているのか知ることが出来ず、全ての分割されたデータを盗み取ることが難しくなる。

分割されたデータは、通信経路を物理的に分割して送信することで、一

方の通信経路を盗聴されデータを盗み取られたとしても、盗んだ1つのデータだけでは復号出来ない。複数の通信経路を使いデータを送信することで、全てのデータが盗聴され盗まれるリスクを低減する。同時に幾つもの経路を盗聴されていたとしても、時間的に分割して送信することで、全ての分割されたデータを揃えることが非常に難しい状況を作る。分割したデータを送信する順番もランダムにすることで、どのような順番で盗聴したファイルを結合するかを容易には推測することが出来ない様にする。

時間的・物理的な分割送信を行うことで、元データの内容を推測することが限りなく難しい仕組みとし、第三者がデータの一部だけを盗聴し盗み出せたとしても、そのデータのみでは何も出来ない（復号することが出来ない）という状況を作りだし、安心・安全なデータ共有（データの送受信）が出来る環境・基盤を構築する。

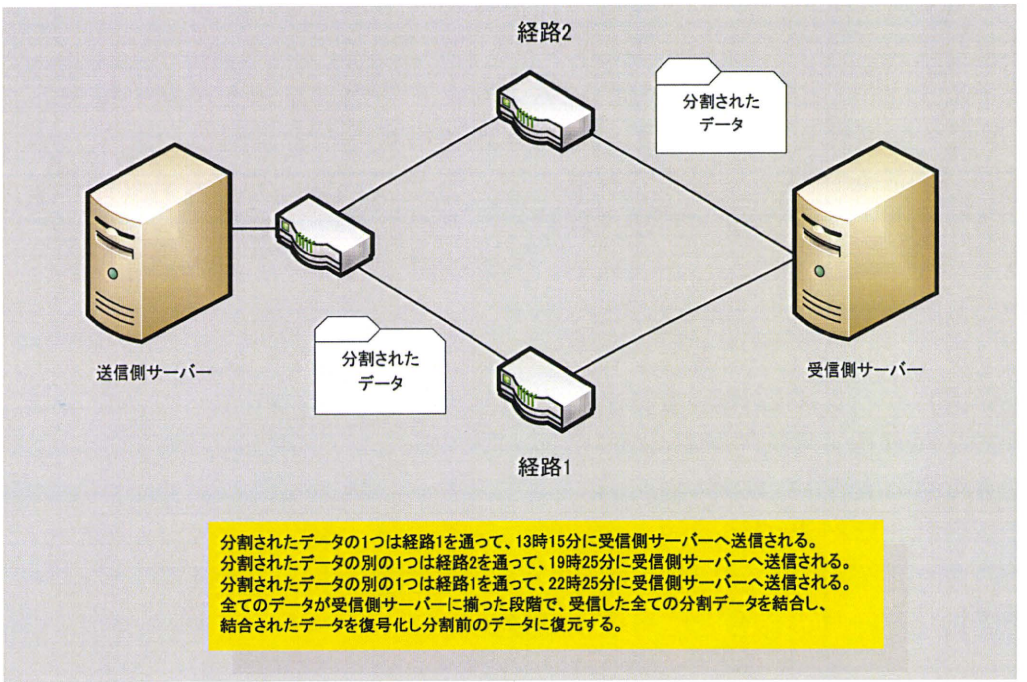


図3　時間的・物理的分割送受信イメージ

プログラム実装詳細

今回試作した暗号化通信ツールは、以下のような処理実装となっている。
処理の流れは以下の通り。

・データ送信初期処理

1. 送信対象のデータを特定し、そのデータのヘッダ情報(データ内容のサマリー)を取得する。
2. ヘッダ情報はその後のデータ送信でも利用する為、システムに保存する。(データベースに情報を登録する。)
3. 送信対象のデータを暗号化する。

4. 暗号化したデータから、メッセージダイジェストを取得し、システムに保存する。
5. 暗号化したデータを分割する。(分割時の情報をシステムに保存する。)
6. 送信対象データのヘッダ情報及びその他の情報を XML 化し、暗号化する。
7. 暗号化した XML データからメッセージダイジェストを取得する。
8. 暗号化した XML データ及びメッセージダイジェストを、データ送信先サーバに送信する。
9. データ送信先サーバから受信結果のメッセージを受取り、処理を終了する。

・データ送信処理(分割データ送信処理)

1. 送信対象となる分割データを特定する。
2. 特定した分割データを、暗号化する。
3. 暗号化した分割データを、データ送信先サーバに送信する。
4. データ送信先サーバから受信結果のメッセージを受取り、処理を終了する。

備考：分割データの送信処理は、データ分割後２４時間以内に全てのデータを送信するように制御する。送信時間帯はランダムに決定されるように制御する。データ送信先を決定する処理でも、送信経路を分けるためランダムに選択される送信先に対して、データ送信を行うような仕組みとなっている。

・データ受信処理(ヘッダ情報受信時の処理)

1. 受信した XML データを復元する。
2. 復元した XML データと、受信したメッセージダイジェストを比較し、相違が無ければ XML データを復号化する。
3. 復号した XML データを解析し、XML に格納されているデータを取り出す。
4. 取出したデータをシステムに保存する。(データベースに情報を登録する。)
5. 受信完了のメッセージをデータ送信元サーバに送信し、処理を終了する。

・データ受信処理(分割データ受信時の処理)

1. 受信した分割データを復元する。
2. 復元した分割データを復号化する。
3. 復号した分割データをシステムに保存する。受信した分割データで分割したデータが全て揃った場合は、以下の処理を実行する。受信していないデータが残っている場合は、受信完了のメッセージをデータ送信先サーバに送付し処理を終了する。
4. 受信した全ての分割データをシステムで読み込む。
5. 読み込んだ分割データと、既に受信しているヘッダ情報を元に分割データを結合する。

6. 結合したデータと、既に受信しているデータ分割前のメッセージダイジェストを比較し、相違がなければ結合したデータを復号化する。
7. 受信完了のメッセージをデータ送信先サーバに送付し処理を終了する。

備考：受信側(データ送信先サーバ)では、受信した分割データがどのようなデータであるかを、システムに保存しているヘッダ情報から判断する。受信した分割データが、元データを構成する最後のデータであるかどうかを判断し、処理を分岐する。

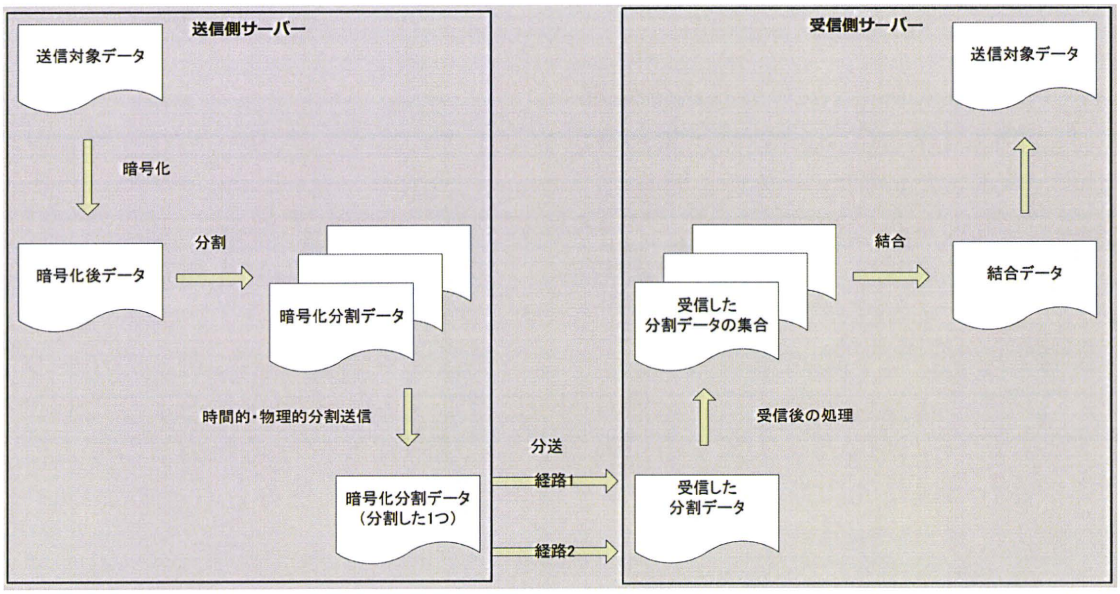


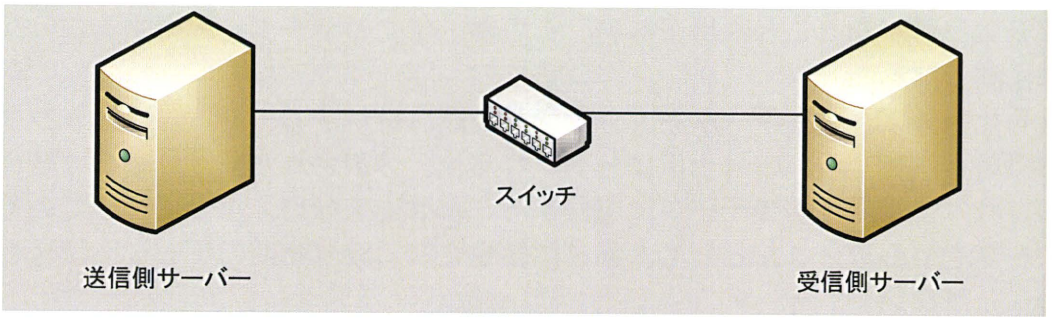
図4　処理のイメージ

実証実験結果

クローズなネットワーク環境で行った実証実験について。
社内でクローズなネットワーク環境を作成し実験を行った。

・クローズなネットワーク環境について
社内で利用したネットワーク環境は以下の通り。
送信側サーバ、受信側サーバをスイッチで接続する。
受信側サーバのNICには、IPアドレスを2つ付与する。(複数のIPアドレスに対して、分割したデータを送信する実験を行う為の設定。)
クローズなネットワーク環境を作成し、実験を実施した。
各サーバに設定したIPアドレスは以下の通り。
送信側サーバ　IP　：　192.168.1.190
受信側サーバ　IP　：　192.168.1.191
　　192.168.1.192

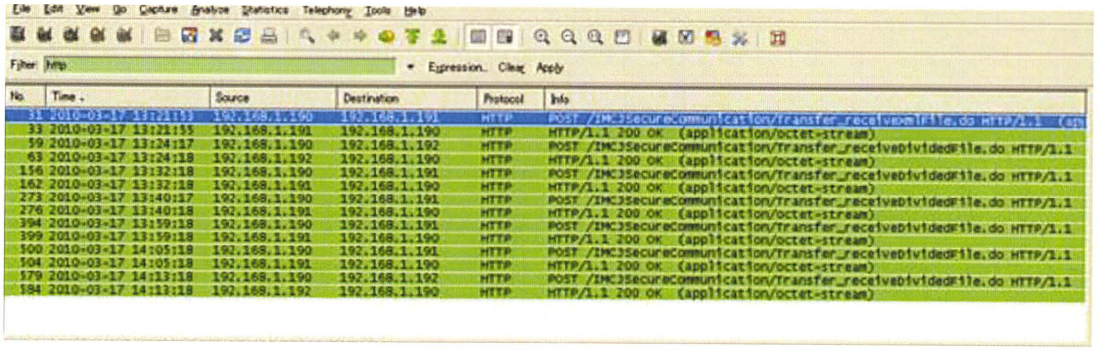
作成したネットワーク環境



本来、物理的な分割送信を行う場合、物理的な経路を２つ以上準備して行う必要がある。今回準備した機器では NIC が 1 枚となっていた為、物理的な経路を複数準備することが出来なかった。その為、NIC に IP を複数付与することで、仮想的に分割送信の実験を行った。

時間的な分送には Cron(Windows のタスクと同じ用な機能)を利用し、1 時間以内に全ての分割ファイルを送信する実験を行った。

受信側サーバで取得したパケット解析情報



分割されたデータが、ランダムな時間に送信され、送信先もランダムに決定されている。

受信側サーバに設定した IP アドレス、192.168.1.191 と 192.168.1.192 にデータが送信されている。この実証実験では、受信側サーバの NIC で受信したパケット情報を全て取得した為、192.168.1.191 に送られたパケット情報も、192.168.1.192 に送られたパケット情報も、閲覧することが出来ている。しかし、第三者がネットワークを盗聴した場合、データを送信する物理的な経路が分かれていれば、192.168.1.191 に送信したデータか、192.168.1.192 に送信したデータのどちらか一方のみしかデータを盗むことは出来ない。上記のパケット情報は、7 分割されたデータのうち、192.168.1.191 に 5 個、192.168.1.192 に 2 個送信されている。データは暗号化された後で分割されている為、どちらか片方だけのデータを盗んだとしても、結合・復号を行い、分割前のデータに復元することは不可能である。

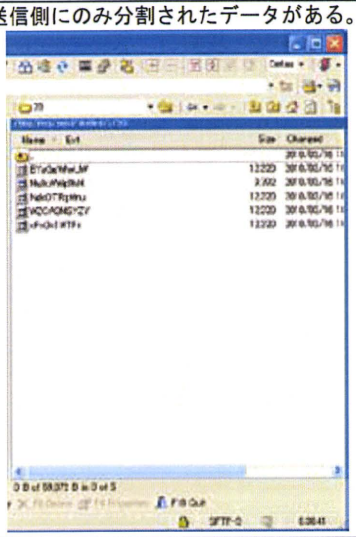
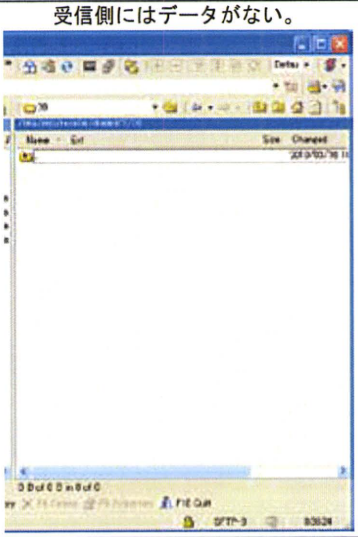
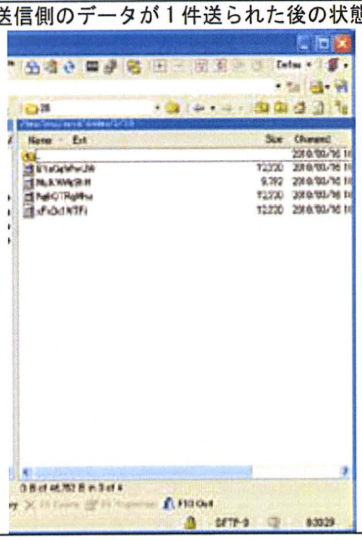
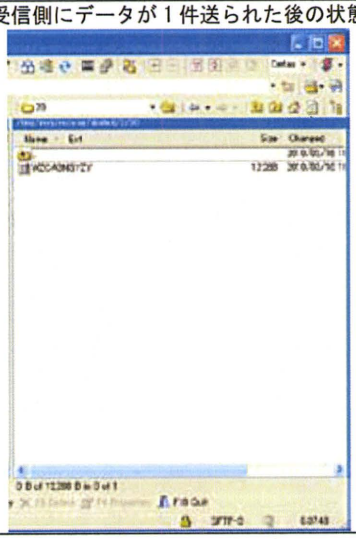
送信するタイミングも、分割したデータ毎にランダムに分けている為、複数のデータが同一の経路を通って送信されたとしても、いつデータが送信される

のかを第三者が知ることは出来ない。その為、全てのデータを取得することはより困難となる。

暗号化後分割されたデータを、分割された順に送付するのではなく、ランダムな順番で送付する。暗号化後に分割される為、分割された通りの順番で結合しなければ、暗号化前のデータに復号することは出来ない。よって、全ての分割データを盗み取られたとしても容易に結合され、暗号化前のデータに復号されることはない。

データを送信する際に付与される名前も、ランダムに半角英数字を使って生成される為、データの名前等から結合は類推することが出来ないようになっている。

分割されたデータが受信側にランダムに送信されている。

送信側サーバのデータ	受信側サーバのデータ
送信側にのみ分割されたデータがある。 	受信側にはデータがない。 
送信側のデータが1件送られた後の状態 	受信側にデータが1件送られた後の状態 

このように、暗号化された後分割されたデータは、ランダムで送られ、受信側で保存される。分割されたデータの名前も半角英数字を使い、ランダムに決