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)

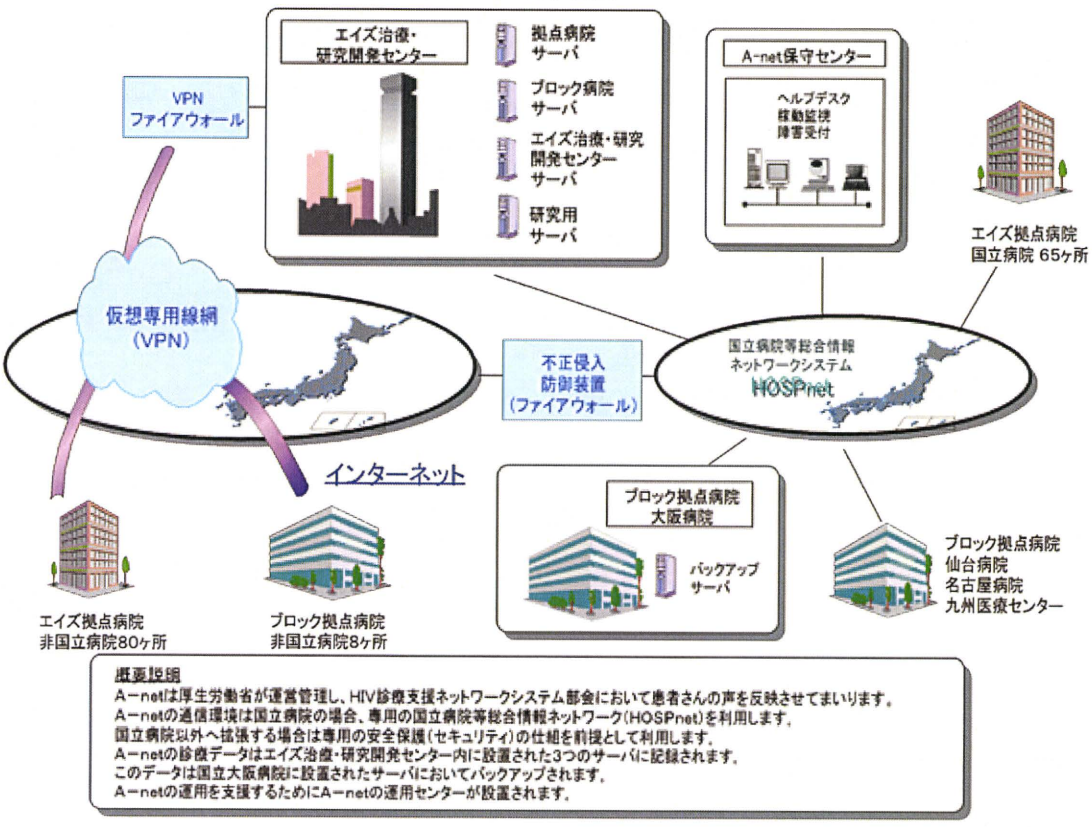


図 1　HIV 診療支援ネットワーク概要図

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。

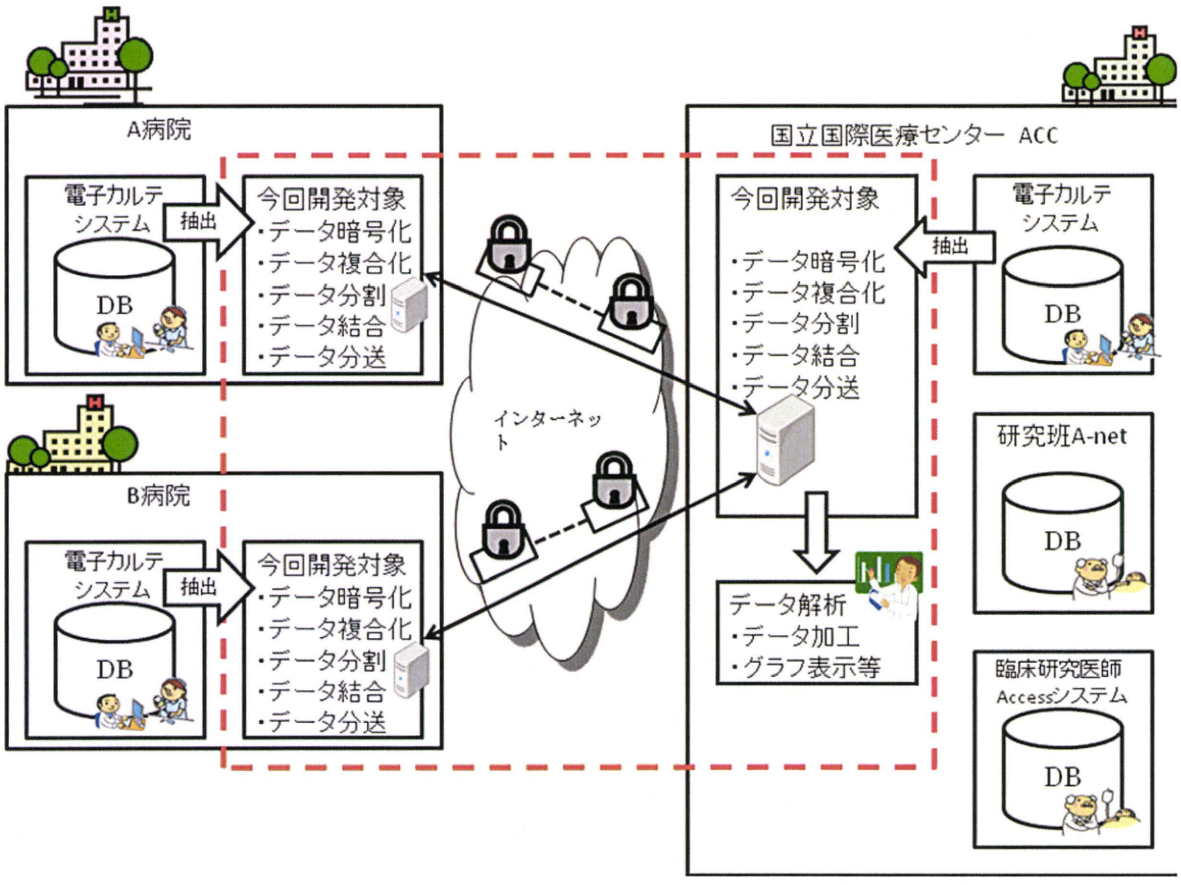


図 2　今年度実施研究概要

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。

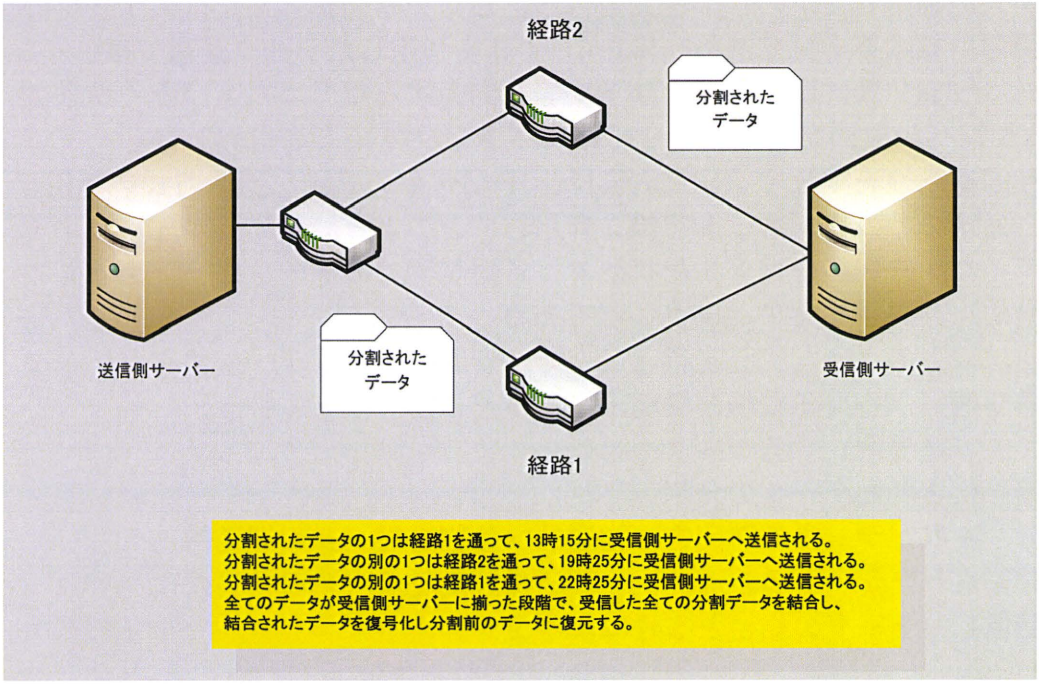


図３　時間的・物理的分割送受信イメージ

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。

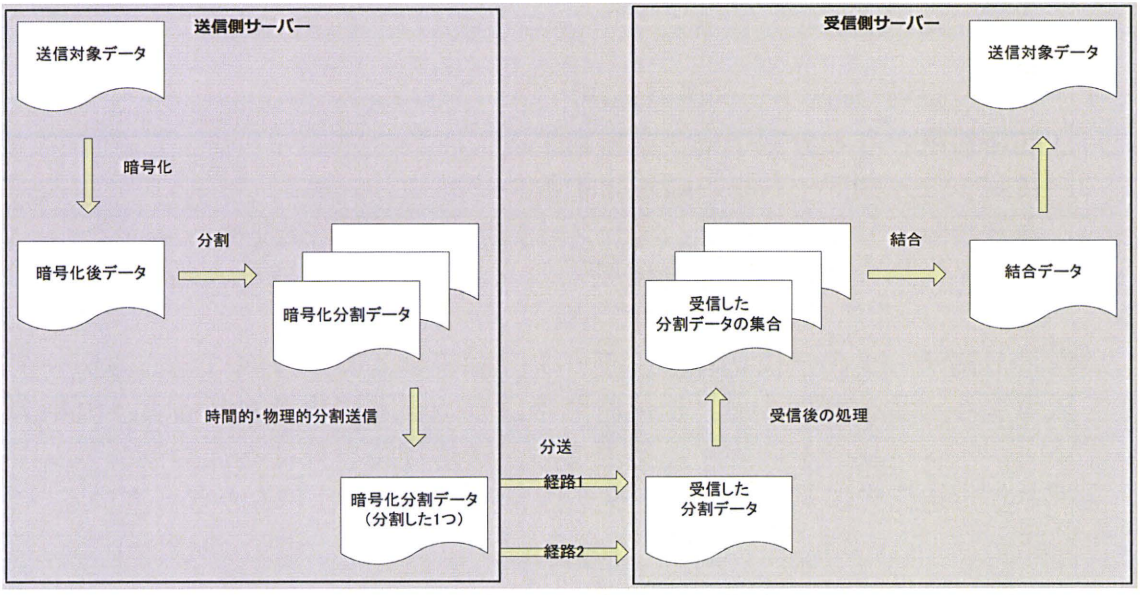


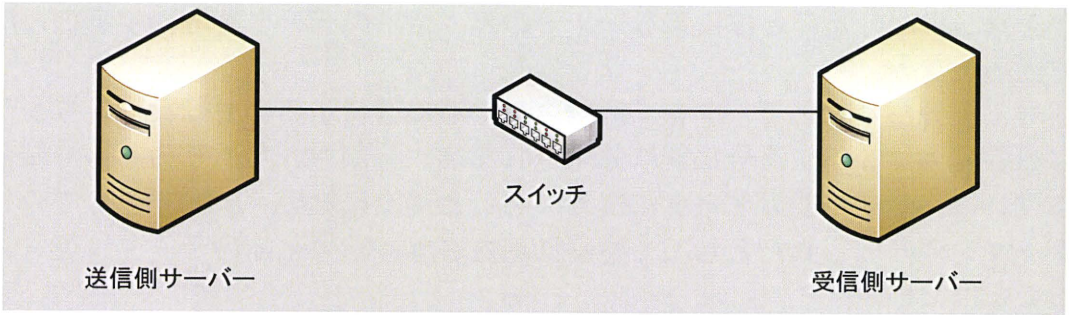
図 4　処理のイメージ

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

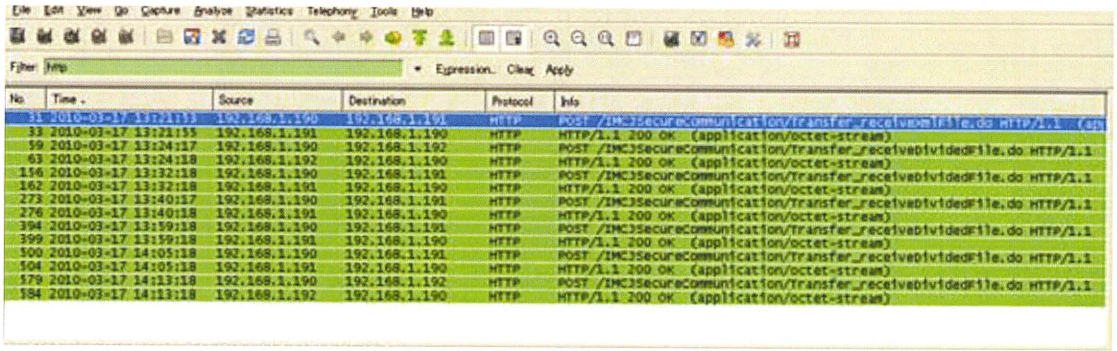
作成したネットワーク環境



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。

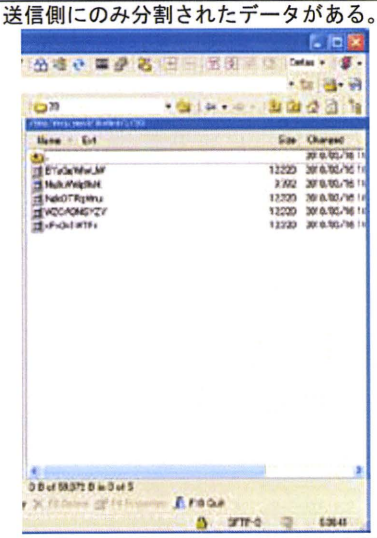
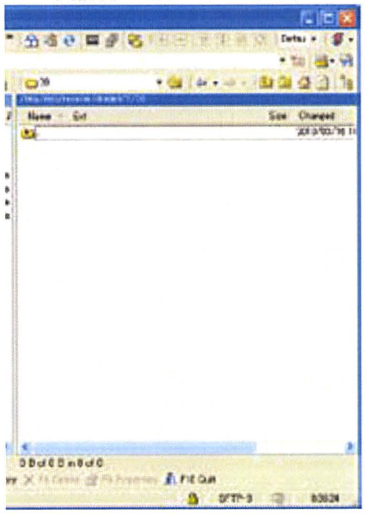
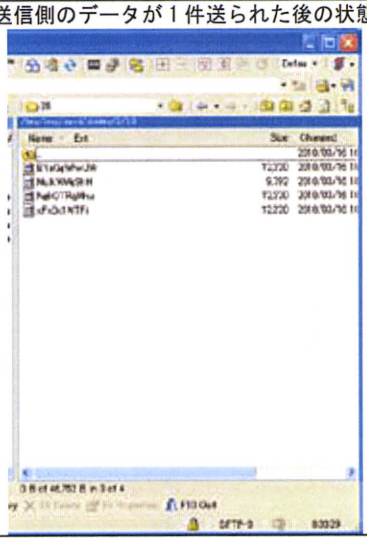
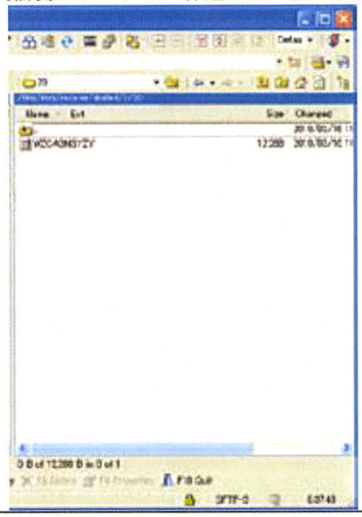
送信するタイミングも、分割したデータ毎にランダムに分けている為、複数のデータが同一の経路を通って送信されたとしても、いつデータが送信される

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。

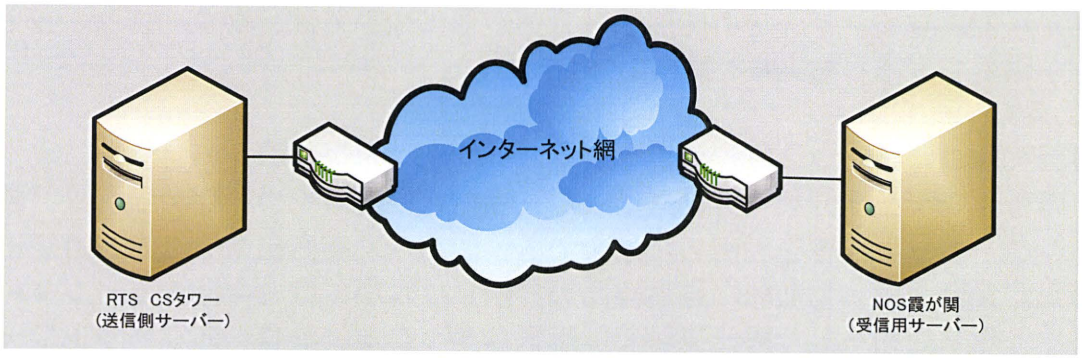
送信側サーバのデータ	受信側サーバのデータ
送信側にのみ分割されたデータがある。 	受信側にはデータがない。 
送信側のデータが 1 件送られた後の状態 	受信側にデータが 1 件送られた後の状態 

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

められている。データを送信する順番も、ランダムに決定される為、全てのデータを盗み取ることが出来、データの結合が出来たとしても、元のデータに復号することは難しい。

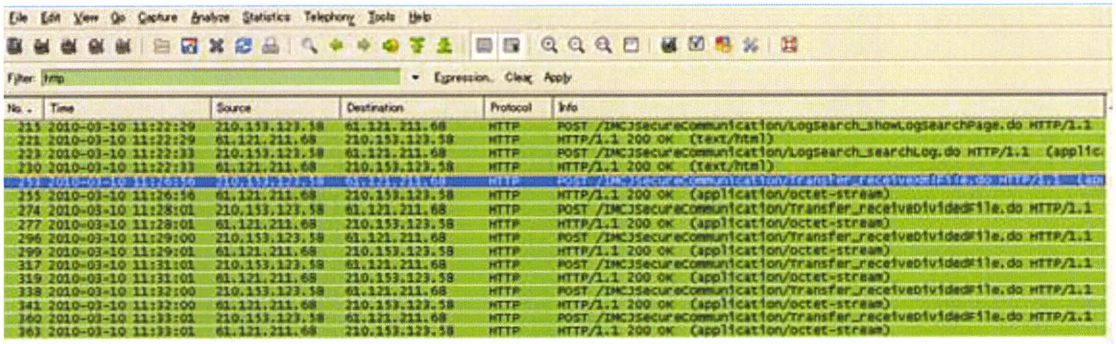
実インターネット環境を利用した実証実験について。
2010 年 3 月 10 日、ネットワンシステムズ霞が関事務所と RTS CS タワー 12F を利用し、今回試作した暗号化通信ツールの実証実験を行った。
・実験環境について
今回の実証実験は、以下の環境で行った。
RTS CS タワー 12F に設置したパソコンを送信側と設定する。
ネットワンシステムズ霞が関事務所に設置したパソコンを受信側と設定する。
実インターネット環境を利用し、データの送受信を行う。
各サーバに設定した IP アドレスは以下の通り。
送信側サーバ IP : 210.153.123.58
受信側サーバ IP : 61.121.211.68

実インターネット環境を利用したネットワーク環境



テスト用に作成した、「検査結果データ」を送信側から送信を行い、受信側で受信を行う。今回は時間の都合上、分割したデータの送信・受信は 10 分以内に終了するように設定した。(本来であれば、24 時間以内に全てのデータの送信・受信が完了するように設定する。)
本番運用を想定し、Cron を利用して Shell を起動しプログラムを動かすようにして、今回の実験を行った。

受信側サーバで取得したパケット情報



分割されたデータが、ランダムな時間に送信されている。

今回の実インターネットを利用した環境では、物理的にデータの送信経路の分割は行っていないが、受信側サーバに複数の IP を取得し、割当てることで送信先をランダムに選択し、ランダムにデータを送信することが出来る。

サーバを 2 台以上用意するか、1 台のサーバに 2 枚以上の NIC を装着し、それぞれに IP を割当てる。割当てる IP も、複数の ISP から取得した IP を割当てる等をすることで、通信経路の物理的な分割が可能になり、データの物理的な分割送信が可能になる。データの時間的な分割送信については、クローズなネットワーク環境で実施した実験と同様である。

・実証実験の考察について。

暗号化→データ分割→分割送信→データ結合→復号化の一連の流れは、実インターネット環境を利用した場合でも、問題なく実行出来ることが確認出来た。分割送信（物理的な送信経路の分割）については、今回の実インターネット環境を利用した実証実験では出来なかったが、クローズなネットワーク環境と同様に、受信側サーバで IP が複数設定されている場合でも、ランダムに 1 つの IP を選択し、選択された IP に対してデータを送信するように設計されている。

ルーティングの異なる複数の ISP から IP を取得し、その IP を受信側サーバに割当てることで、データ送信経路の物理的な分割が可能になる。

クローズなネットワーク環境では、複数の IP アドレスが付与された受信側サーバに対し、ランダムに分割したデータを送信し、全てのデータが揃った段階でデータの結合・復号がされ、分割前のデータに復元されることが確認出来た。分割されたデータを時間的に分割送信することで、第三者がデータの送信されるタイミングを知ることが出来ない為、通信経路の途中をすべて盗聴されていたとしても、流れている全てのパケット情報の中から分割されたデータを全て抜き出すことは、非常に困難になる。

分割した全てのデータを集めたとしても、分割した順番通りに結合しなければ、分割前のデータに戻すことは出来ない為、結果として暗号化前のデータに復号することも出来ない。

データの暗号化だけを行い、分割せずに一度に送信した場合、そのパケット情報が第三者に盗聴され解析されてしまうと、そのデータが万が一復号された場合には、情報の漏洩に繋がってしまう。例え堅牢な暗号化アルゴリズムを使用したとしても、復号される可能性が 0 では無い為、よりセキュリティを高める努力をし、セキュリティを確保する必要がある。

今回試作した暗号化通信ツールでは、データの暗号化を行った後、その暗号化データを分割し、分割したデータは送信前に再度暗号化される。分割されたデータを送信する時にも、物理的にデータ送信経路を分け、その経路をランダムで選択するようにしている。送信時間も分けることで、データ暗号化の時点とは非同期に、受信サーバとのデータの送受信を行い、セキュリティの確保に務めている。

実証実験でも、ネットワーク上に流れているパケットを解析するなどして、今回試作した暗号化通信ツールの有効性は確認出来た。

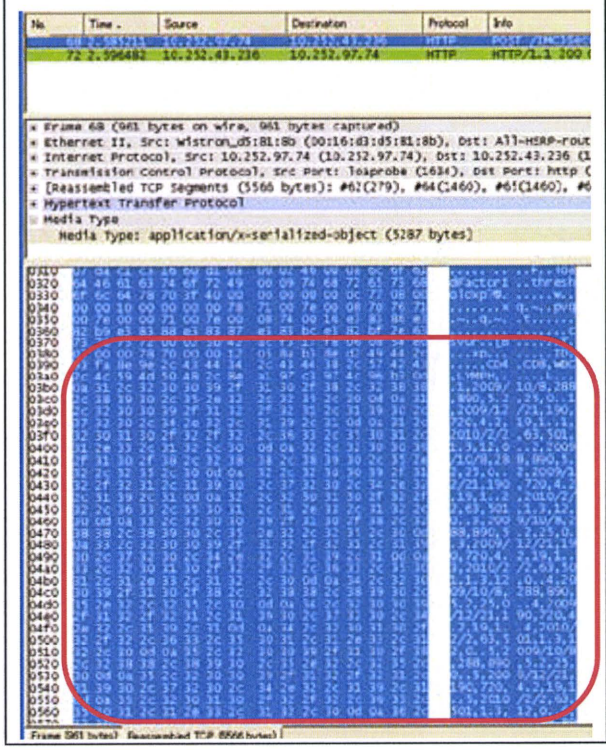
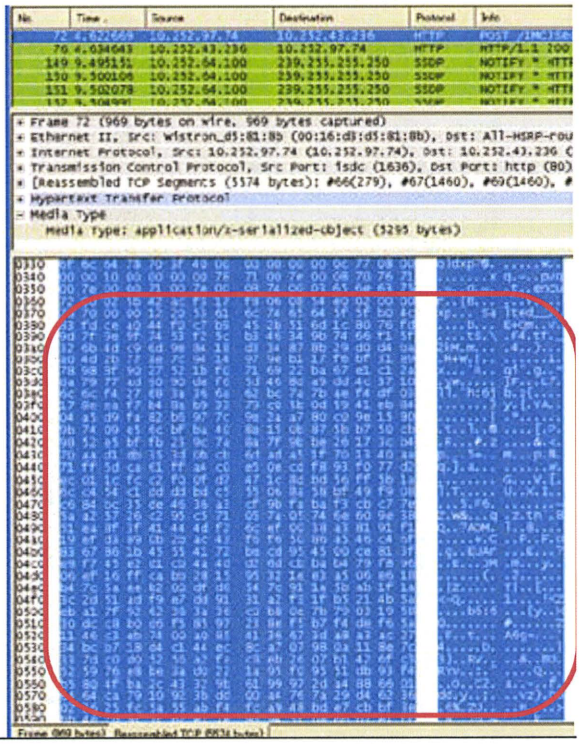
・今後の課題。

今回は２台の PC を使い、送信先・送信元を１台ずつ準備し、実証実験を行った。通信の安全性を示す為の実証実験としては、上記の環境でテストをすることで十分である。

今回試作した暗号化通信ツールは、将来的には各医療機関に配置され、利用される予定である。通信の安全性だけでなく、ツールの耐久性も検査する必要がある。今回の試作では、通信の安全性のみを検査したが、次年度以降の研究として通信量（通信相手先の量）が増えた場合の耐久性の検査を行っていく必要ある。その上で、将来の拡張性を考慮したツールとして改善を重ねていく必要がある。

参考情報

1. 暗号化をせずにデータを送信した場合のパケット情報

暗号化せずに送信した場合のパケット情報	暗号化後に送信した場合のパケット情報
	

このように、暗号化されない状態でデータ送信を行った場合、パケットを解析すると、データの中身がそのまま表示される状態となっている為、容易に送信しているデータの内容を読み取ることが出来る。
暗号化したデータを送信した場合は、パケットを解析しても、データが暗号化された状態で送信される為、容易に送信しているデータの内容を読み取ることは出来ない。

課題と対策

今回の実証実験における課題を以下に記載する。

1. データを暗号化する際の鍵(パスワード)情報の管理方法
2. 各サーバ間（送信側・受信側）での認証方法

各課題に対する対策について。
（今回の対策は時間的な制約から、試作段階では実装を見送っている。
次年度以降の研究課題として取り組んで行き、より安全な暗号化通信を実現する為の方針を記述する。）

1. データを暗号化する際の鍵(パスワード)情報の管理方法

鍵の管理については、IPA で「システムのセキュリティを維持する為には、暗号鍵の生成から廃棄までのライフサイクルを考慮した管理手法を策定・確立することが必要」ということが言われており、鍵管理のガイドライン（案）が発表されている。

鍵のライフサイクル管理としては、以下の段階がある。

1. 鍵の生成
2. 鍵の配送
3. 鍵の利用
4. 鍵の保管/バックアップ
5. 鍵の期限切れ/失効/廃棄
6. 鍵の回復

（各段階での鍵情報のリスクと対策については、鍵管理のガイドライン（案）に一般論が記載されている。）

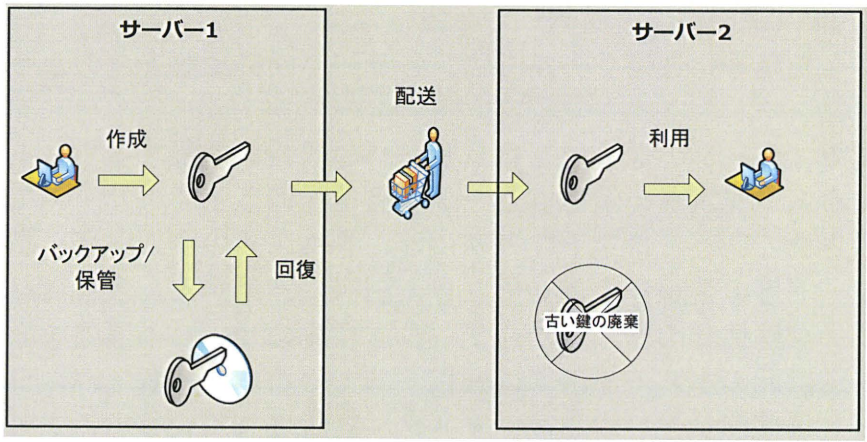


図 5　鍵管理イメージ

今回試作した暗号化通信ツールでは、「1. 鍵の生成」については乱数を用いた鍵の生成を行えるような仕組みを準備した。また、「4. 鍵の保管/バックアップ」についても鍵情報が格納されたファイルを暗号化し保管することで、セキュリティの向上に努めている。「5. 鍵の期限切れ/失効/廃棄」については、鍵の有効期限を設定可能にし、設定された有効期限を過ぎた鍵は使用出来ないようになるように設計している。ただし、今回実装した部分についても「鍵管理ガイドライン(案)」で述べられている指針の全ては満たしていない。その為、今後更なるセキュリティの向上に努める場合には、現在実装している部分についても見直しを行う必要がある。

鍵の管理で今回試作した暗号化通信ツールで実装されていない部分は、「2. 鍵の配送」「6. 鍵の回復」である。「2. 鍵の配送」については、今回試作した暗号化通信ツールを拡張し、鍵情報も暗号化通信ツールで送受信を行い、各サー

バ間で鍵情報を共有するという仕組みが考えられる。
ただし、暗号化通信を行う全てのサーバで同じ鍵情報が共有されなければ、正常に暗号化・復号が出来ないという問題が発生してしまう。このような状況を回避する方法を考える必要が有り、暗号化通信を行う全てのサーバ間で、鍵情報が同じであるということの確認が取れる（同じであることが担保出来る）仕組みを考える必要がある。
「6. 鍵の回復」については、「4. 鍵の保管/バックアップ」及び「5. 鍵の期限切れ/失効/廃棄」と併せて考える必要がある。現在の実装では、鍵の保管についてはある程度の考慮をしているが、バックアップの考慮はされていない。過去の鍵情報の廃棄についても、現在の実装では考慮されていない。
実際の運用では、過去の鍵の廃棄等も、運用次第では考慮する必要があると考える。鍵の回復についても、過去に暗号化したファイルから、再度元ファイルに復号する必要がある場合には必須となる為、鍵のバックアップ・破棄・回復については、運用上の制約やセキュリティ確保等を考慮し、指針を決定していく必要がある。

2. 各サーバ間（送信側・受信側）での認証方法

今回試作した暗号化通信ツールでは、各サーバ間の認証を次のような方法で実装した。
各サーバ間で、データの送受信を行うサーバの情報を登録するホストマスタを保持する。ホストマスタの情報はデータ送受信を行う全てのサーバで同一のデータが登録されている。ホストマスタには、各ホストのホスト名、認証に利用するパスワード等の情報を登録しておき、認証に利用する。現在実装している認証は、データ送信元のサーバからデータ送信先のサーバへ通信を確立する際に、データ送信元のホストマスタに登録されているホスト名・パスワードを送信し、データ送信先サーバのホストマスタに登録されているホスト名・パスワードと一致するかどうか、という認証を行っている。

現在実装している認証方法では、知識による認証となっている為、認証強度は弱いと考えられる。よりセキュリティを向上させる為には、各サーバが持つ属性等をホストマスタに登録出来るようにし、その属性情報を認証に利用し、認証強度を上げていくといったことが必要になる。
各サーバの属性情報を利用する方法以外でも、認証強度を上げる方法がないかどうかを調査し、現在の認証方法を拡張することで、より信頼性の高いシステムとして利用することが出来るようになる。

第4章 各病院治療データ解析

治療データ集計・解析ツールを試作する目的を記載する。

各病院のHISから抽出したデータは、フォーマットが統一されておらず、VL値に関しては様々入力がなされており、良好・その他を判断する際の障害になっている。また、データ件数も多く、人間が手作業でデータの整形から集計・解析を行うのには、多大な時間が必要となる。

そこで可能な限り汎用的に、各病院のHISから抽出した検査データを取り込めるツールを作成する。同様に処方データも取り込めるようにする。

今回作成するツールは、取り込んだ検査データ・処方データを使い、ある一定のルールのもと集計・解析までを自動的に行うツールとする。

実装ツール処理内容

データ解析・集計について、処理内容を記述する。

データ解析・集計は大きく分けて、「データ取込」、「解析・集計結果の表示」、「データ取込書式設定」から構成される。

1. データ取込について。

データ取込は、「処方データの取込」、「検査データの取込」、「データ変換」を行う機能となっている。

・処方データの取込。

処方データの取込は、取込対象ファイルに格納されている処方データを全件取り込む。取り込んだデータは、DBに格納し、保存する。

・検査データの取込。

検査データの取込は、取込対象ファイルに格納されている検査データを全件取り込む。取り込んだデータは、DBに格納し、保存する。

・データ変換。

データ変換は、次の処理を行う。

処方データから、抗HIV薬一覧として登録されている薬剤のデータのみを抜き出す。検査データを、患者別採取日別のデータとして整形する。(抽出する検査項目はCD4(実数値)、CD8、LYMPH、WBC、VLの5項目を抽出)

絞込み・整形を行った処方データ・検査データを結合し、処方データが存在する来院日は、治療有りとして扱う。(処方のみの場合も治療有りとして扱う。検査のみの場合は、治療なしとする。)

2. 解析・集計結果の表示について。

解析・集計については、次の処理を行う。データ変換が終了したデータについて、以下のデータを除外する。

・「治療有り」が一件も無い患者のデータ。

・2008年以降のデータが無い患者のデータ。

・2008 年以降のデータが存在するが、登録されているデータが 6 ヵ月未満の患者のデータ。
・直近 6 ヵ月のデータで「治療有り」が一件も無い患者のデータ。
・直近 6 ヵ月のデータで VL 値にデータが一度も入力されていない患者のデータ。
データ除外完了後、治療経過期間（年単位）別に良好・その他を集計する。
良好・その他の振分けを次の基準で行う。
最終来院日から 6 ヵ月間の VL 値で判定を行う。VL 値に含まれている文字列が、「ミケンシュツ」、「<40+」、「LT50」、「LT400」、「50 以下」の場合、良好と判断する。直近 6 ヵ月のデータ全てが良好と判断出来る場合に、該当の患者のデータは良好とする。データが全て良好と判断出来ない場合は、その他と判断する。
良好・その他を判断した結果表示については、次のような表示を行う。新規にシートを作成し、治療経過期間別に良好・その他を集計した表を表示する。
表示された表を元に、年度別の棒グラフ、年度別に良好・その他の割合を表示するグラフを作成し、表示する。

3. 各病院へのデータ取込対応について。
VL 定数、VL 指数は次のように変換し取込を行う。VL 定数と VL 指数を結合し、新たな値を作成する。“{VL 定数} ×E10 {VL 指数}“　（VL 定数は小数点以下 10 桁程度のデータが登録されている為、少数点以下の切り上げを行う。）また、次の値を良好として判断する。「0×E100」、「0×E100.3」、「0×E101」、「0×E102」無治療は値を反転させて取込を行う。（0 のデータは 1 に、1 のデータは 0 に変換する。）

解析データ

全国の病院を対象に、病院にて検査・処方を受けた患者 3300 人分のデータにて集計・解析を実施した。

解析結果

データ集計・解析結果は以下の通り。

総患者数（単位：人）	
データ集計・解析対象者	1614
データ集計・解析対象外者	1686

データ集計・解析対象者の内訳は以下の通り。

治療年数（単位：年）	良好（単位：人）	その他（単位：人）
0	35	81
1	147	113
2	139	43