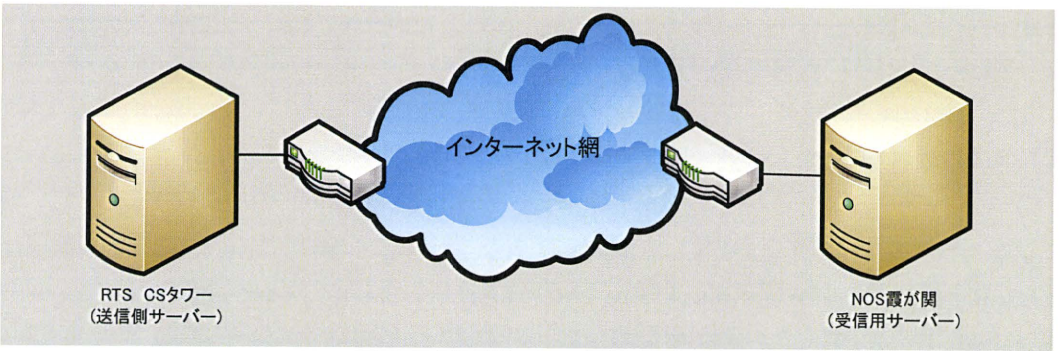
められている。データを送信する順番も、ランダムに決定される為、全てのデータを盗み取ることが出来、データの結合が出来たとしても、元のデータに復号することは難しい。

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

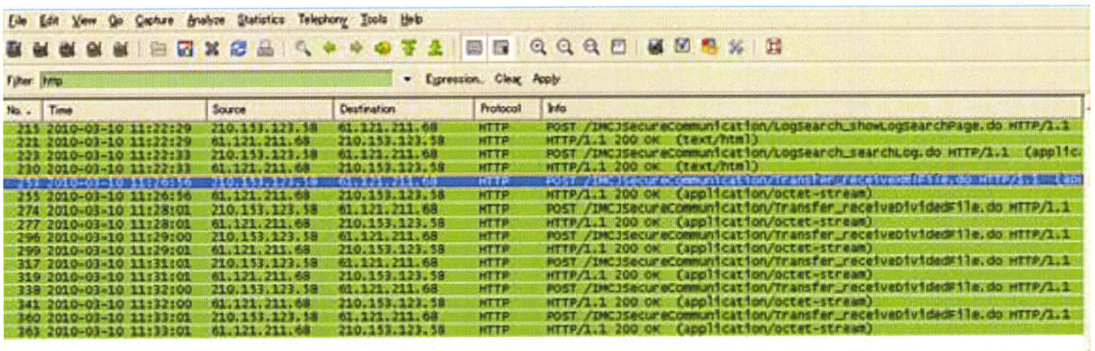
実インターネット環境を利用したネットワーク環境



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。

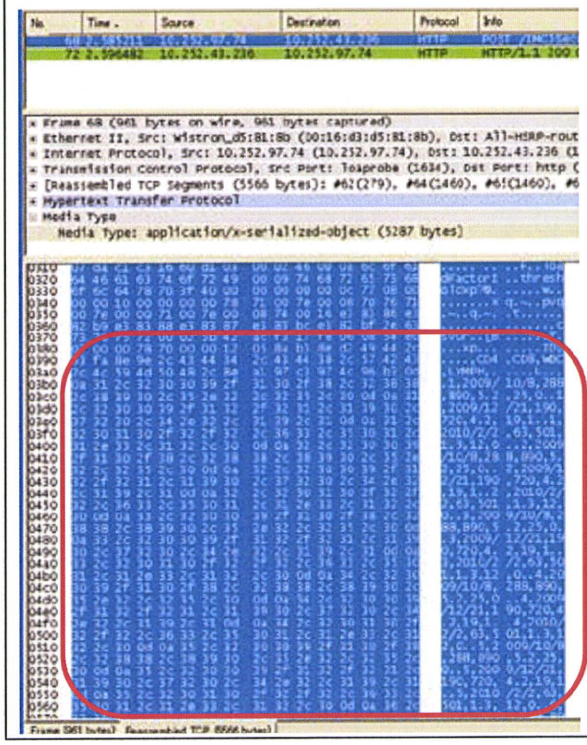
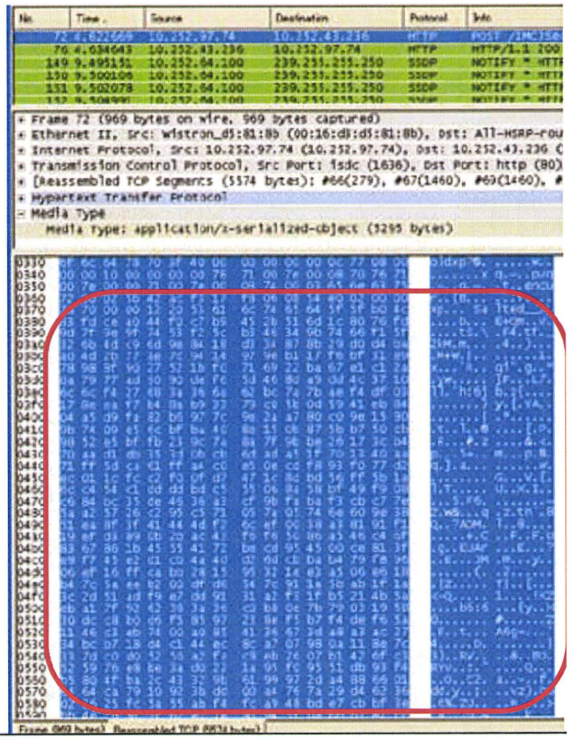
・今後の課題。

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。）

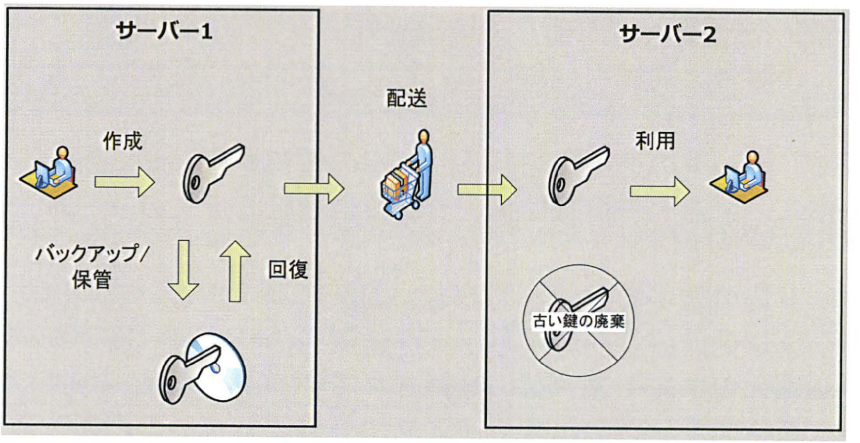


図 5　鍵管理イメージ

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。

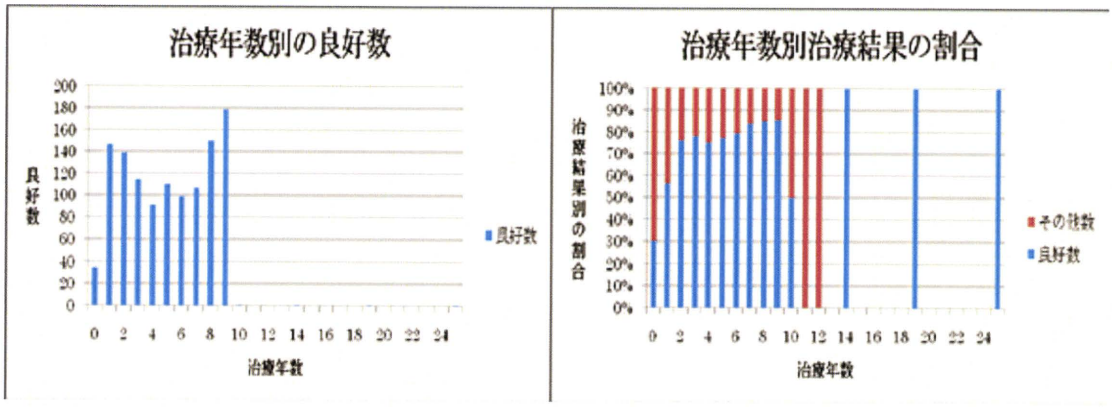
総患者数（単位：人）	
データ集計・解析対象者	1614
データ集計・解析対象外者	1686

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

3	115	32
4	91	30
5	110	32
6	99	26
7	107	20
8	150	26
9	179	30
10	1	1
11	0	3
12	0	1
14	1	0
19	1	0
25	1	0

上記の表をグラフ化。



データ集計・解析対象外の内訳は以下の通り。

対象外理由	総対象外者中の割合（単位：人）
治療実績が一度もない人	819
2008 年以降のデータが無い人	279
2008 年以降のデータはあるが、6 ヵ月以上のデータが無い人	531
直近 6 ヵ月で治療実績が一度も無い人	48
直近 6 ヵ月で VL 値にデータが一度も入っていない人	9

上記の表の通り、データ集計・解析対象外となった患者の数が、51%となっている。その内訳をみると、「治療実績が一度も無い人」のデータが、対象外患者の実に 49%を占めている。次年度以降に再度解析を行う場合、治療実績が一度も無い患者（処方を受けていない患者）も解析対象とすることで、さらに多くの患者データを集計・解析対象として扱うことが出来る。

その他にも、2008 年以前のデータしかない患者も対象に入れることで、集計・解析の母数（対象となる患者数）を増やすことが可能となる。

集計・解析したデータから判明したことは、各病院でデータフォーマット（CSV ファイルのフォーマット）やデータの入力値に、非常に大きな違いがあるということである。この違いは、作成したツールでその差を吸収することは困難である。各病院データの取込を行う際には、取込の設定だけでなく、大幅な修正を行うことで取込を行った。

集計・解析を行う病院数を増やしていく場合、このような個別対応を病院毎に行うことは、その対応に掛かるコストも時間も大幅に増大することになる。各病院で利用している HIS が異なる為、HIS から抽出したデータのフォーマットも統一されていないことで、このような問題が発生している。

【考察】

データ集計・解析を行う為には、ある程度の年数・患者数が無いデータの集合は、解析・集計を行うことが非常に困難である。また、VL 値等に入力されているデータも統一されていない為、各医師によって入力されているデータに揺らぎがあることがわかった。可能な限り揺らぎに対応はしたが、データ解析上の障害となっている。

今後より優良なデータを解析・集計から得る為には、まず各病院内でのデータの入力値の統一を図っていくことが重要である。各病院内でのデータの入力値が統一されていれば、集計・解析の判断が明確になり、より正確で優良なデータを得られることが予想される。

しかし、現状の HIS では、恐らく医師の手入力で検査データが入力されていると考えられる為、入力方法の統一は難しい。CD4 や CD8 等の数値を入力するものについては、検査毎に異なった値が入力される為、医師の手入力で入力されることは問題では無い。今回の集計・解析で入力値の揺らぎが最も多かった VL 値については、医師の手入力では無く、決まった値から選択されることが望ましい。入力方法を選択形式にしてしまえば、医師毎に入力されるデータに違いはなくなるので、入力値の揺らぎは起きようがない。

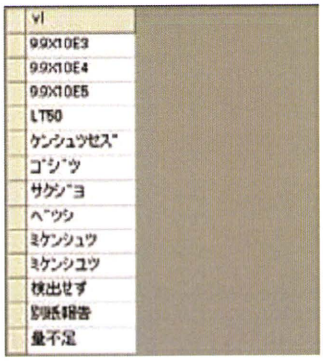
この他、同一の検査日に同一の項目（LYNPH や WBC 等）が 2 つ以上作られているデータも散見された。今回のように、VL 値のみを判断基準としている場合は問題にならないが、今後日和見感染症等を集計・解析に含めていく場合には、入力方法の統一も必要である。速報値を出す必要ある場合の入力方法や、入力されたデータが速報値であることの判別が出来るためのデータが必要である。

これらの実現には、HIS の改修が必須である。今後、患者へのデータ公開を考えた場合、各病院で入力されたデータは、一度国立国際医療センターに集約され、集約されたデータの集計・解析が行われた後、患者へと公開され医師間で共有されるというのが、公開されるデータのあるべき姿である。

医師が入力した検査データが医師間で共有され、インターネットを利用してそのデータを公開し、そのデータを元に患者が自分の現在の状態を把握し、患者自らが適正な服薬を実施していくことが、データ公開をする意義である。その為にも、各病院間の HIS の違いから、入力方法の統一を図ることは難しいかもしれないが、データの入力値を全国で統一することで、有意義なデータを患者に公開することが可能になり、集計・解析の結果として得られるデータの信憑性も高くなる。

患者へのデータ公開は、検査を受けた当日には、その患者データが閲覧可能であることが望ましい。その為には、法律的な問題や各病院の倫理等様々な問題がある。これらの問題をクリアし、患者にとって有意義で且つ医師にとっても有意義なデータを蓄積し、そのデータを活用していく必要ある。

入力値が統一されていない例（VL値で入力されている値の一例）



	vl
	9.9X10E3
	9.9X10E4
	9.9X10E5
	LT50
	ｹﾝｼｭﾂｾｽﾞ
	ｺﾞｼﾞｯ
	ｻｹｼﾞｮ
	ﾍﾞｯｼ
	ミケンシュツ
	ミケンシユツ
	検出せず
	影響報告
	量不足

VL値もミケンシュツ・ミケンシユツ・検出せず・ケンシュツセズ等、様々な入力値が登録されている。

データの活用については、集計・解析したデータでデータマイニングを行うことで、より有意義な活用が出来る。
過去に蓄積された大量のデータや、これから蓄積されていくデータを解析し、その項目の間にある相関関係を見つけ、治療に利用する。検査データだけでなく、処方データも利用することで、疫学的研究も可能になる。大量に蓄積された患者の検査データを利用して、色々な角度からデータを解析し、病気と薬の因果関係を探ることや、あるパターンでは有効な投薬も、ある一定の期間を過ぎてしまうとその効果が薄れるといった、各データ間の相関関係だけでなく、時間的な視点からの解析等、今後のHIV研究にとって有意義な統計データを取得することが出来る。
その為にも、入力されるデータは、全国で統一の値が入力される必要がある。
今回は、HISから抽出したデータをCSVに変換し、変換したCSVの中から特定の項目のみを抜き出し、データの集計・解析を行った。今回の集計・解析は、VL値のみを使った判定であり、CD4やCD8といったHIV治療では特に重要な数値については、データを出力したのみで、判定の基準に含まれていない。次年度以降も、VL値を使った良好・その他の判断を行い、それとは別にその他の項目(CD4、CD8、WBC、LYMPH)も使ったデータ解析を行い、これまでよりも有意義なデータの利活用を行っていく。

第5章 最後に

今年度の研究テーマである、
・暗号化通信ツールの試作と実証実験
・各病院の治療データ集計・解析
について総括を行い、次期 A-net のあるべき姿を検討する上での課題を述べる。

総括

・暗号化通信ツールの試作と実証実験について

可能な限り低コストで、セキュアなデータの送受信を行うという研究テーマをもとに、今回の暗号化通信ツールを試作した。

結果としては、セキュリティの強度を意識し、ツールの仕様を検討・設計したことで、ほぼ理想通りの暗号化通信ツールを試作することが出来た。ただし、現在のセキュリティ強度がどれほどのものかを、データへの攻撃を第三者にさせるなどして計測することも有効である。積み残した課題等もある為、このツールへ更なる改善を行い、よりセキュリティの高いツールとして行くことが必要となる。

・各病院の治療データの集計・解析について

今回の研究で行った、可能な限りのデータ集計・解析の自動化は、かなり多くの課題が明らかになった。

各病院で利用しているHISが異なる為、HISから抽出される治療データが、病院毎に全く異なったデータとなっていることが最大の課題である。次年度以降も、同様の治療データの集計・解析を行う場合、可能であればこちらから CSV のフォーマットを提出し、そのフォーマットに則ったデータを各病院から貰うことが出来れば、今回作成したデータ集計・解析の自動化ツールを利用することが出来る。

次年度以降の課題として、病院間で入力されるデータの不一致等を是正出来る仕組みを検討していくことが必要である。

・次年度以降への課題について

現 A-net を刷新する上で今後課題となるのは、「A-net へどのようにしてデータを登録するのか？」である。

昨年度の研究で、次期 A-net のプロトタイプとなる長年蓄積可能なデータベースの構築を行い、実際に医師よるデータ登録を行い、その有効性を検証した。

しかし、現 A-net 同様に入力するデータが多く、医師による日々の入力は不可能である。次期 A-net に期待される、「患者へのデータ公開」及び「医

師間での治療データの共有」、という二つ大きな役割を果たす為に、如何にして優良なデータをA-netに蓄積していくかということが課題である。
次期A-netへのデータ登録方法としては、以下のような案が考えられる。

1. 今年度の研究で試作した暗号化通信ツールを使った各病院で利用しているHISとの自動データ連携。
2. 昨年度の研究で次期A-netのプロトタイプとして試作したデータベースの改修を行い、患者へのデータ公開・医師間での治療データ共有に必要な最低限の項目のみを手入力する。
3. A-net へのデータ登録を医師が行うのでは無く、別途データ入力の担当者を設け、医師の替りに治療データの入力を行う。

1 ～ 3 案、全てに課題やメリット・デメリットがある為、一概にどの方法が最善であるということは出来ないが、「患者へのデータ公開」・「医師間でのデータ共有」を考えた場合、如何にして優良なデータを A-net に蓄積していくかという課題を解決していかなければならない。
医師が求めるデータと、患者が求めるデータにはギャップがあることが予想される為、どのようなデータを A-net で管理する必要があるのか？といったことも今後調査・検討していく必要ある。

附録 1. 医療情報交換の標準化

1.1 HL7 規約と IHE 活動

医療施設内や施設間で、医療機器や医療情報のシステムを相互接続した際に、システムが保有する医療情報の継続性を確保し、医療連携を推進するために、医療情報システムの相互運用性が求められている。相互運用性を確保するための最も基本的なものの一つが、相互に電子的に交換できるようにすることである。

医療情報を交換するためのメッセージの標準化規約が開発されており、広く普及している国際標準規約として HL7 (Health Level Seven) や DICOM (Digital Imaging and Communication in Medicine) があり、内容の充実化が図られている。一方、これらの標準規約に従えば、医療情報システムはすべて簡単に接続され、相互運用性が確保されるものでない。HL7 や DICOM 等では、ユースケースとメッセージの組合せが定められていないために、使用するメッセージが一意に定まらず、送信側と受信側に食い違いが生じる問題が発生する。この問題を解決する活動として、IHE (Integrating the Health-care Enterprise) がある。IHE は、標準規約をどのように使うかという視点から、規約の使い方に制約を加えて実際の現場での食い違いがないようにするガイドラインを提供している。

1.2 HL7 規約概要

HL7 の扱う情報範囲は、入退転院、診療受付、各種オーダ、結果参照、会計、マスタメンテ、免疫（予防接種）情報、薬剤副作用、臨床試験、予約、紹介、プロブレムリスト等である。日本と米国の医療制度の違いから、会計、看護オーダなど、そのまま日本で使いにくいものが多いため、日本では、保健医療福祉情報システム工業会（JAHIS）が、国際標準に準拠した情報交換規約を策定し公開している。

1.3 今回試作した解析ツールで利用したデータについて

今回のデータ解析ツールの試作で利用したデータは、各病院にデータ抽出を依頼し、CSV形式のデータとして抽出したデータを使用している。
各CSVデータは、HL7等の形式とはなっていない。HISから抽出した段階ではHL7に対応した形式となっていたが、今回の研究で利用し易くする為、手動でHL7からCSV形式に変更したデータを利用した。今後、今回の研究を元に試作したツールの更なる改良が必要な場合、HL7への対応を考慮していく必要がある。

附録2. 情報技術最新動向

2.1 アーキテクチャー最新動向

本研究で利用するアーキテクチャーの選定にあたって、以下のことを考慮する。これまでのA-netのようにVPN等を利用してセキュリティの確保を行った場合、500拠点への展開を考えた場合コストが掛かり過ぎる為、次期A-netでは可能な限りコストを抑えた構成で構築する。既存のインターネット網を利用したデータ通信を行うことで、IP-VPN等の高価な仕組みを利用せず、またIP-VPN以上にセキュアなデータ通信を実現することが出来るアーキテクチャーを選定する。

本研究で利用するアーキテクチャー（暗号化通信ツールに利用するプロトコル）は、HTTPとする。HTTPリクエスト・レスポンスを利用し、暗号化通信ツールを構築する。

HTTPを選定した理由は、データ受信の際にマルチスレッド処理に対応したオープンソースのミドルウェアが活用出来、暗号化通信ツールを作成する上で大幅な時間短縮が出来ることである。また、オープンソースのミドルウェアを利用することで、商用のミドルウェアを利用するよりもコストを抑えることが可能である。

上記以外のHTTP選定の理由は、以下の通り。

1. Javaでの扱いが容易であること。
2. ロジックを大きく変更する必要なく、HTTPSでのセキュア通信にも対応可能なこと。
3. FireWallで不要なポートを開放する必要も無いこと。
4. 複雑なネゴシエーション（通信前手順）を必要としないため、クライアント/サーバともに処理のオーバーヘッドが少ないこと。

が挙げられる。

ただし、HTTPを利用する上でのデメリットとして、長時間接続を維持しておくことが難しいということがある。接続を長時間維持しておくことが難しい為、早く応答を返す必要がある。この課題に対処する為、送信するデータのサイズを極力小さくし、送信回数を多くすることでこの課題を回避することとした。

2.1.1クラウドコンピューティング

Webサービスを提供する技術の向上により、Webブラウザだけで出来ることが増えてきた。ネットワーク・サービスを積極的に利用することで、プラットホームや環境、場所に関係なく、同じデータやサービスが使えるようになるというものである。

2.1.2Web アプリのセキュリティ対策

Web サイトの脆弱性への対策は、その対策内容や取り組みの視点によって、期待できる効果や影響が異なり、「脆弱性の原因そのものを取り除く対策（根本的対策）」や「特定の攻撃による影響のみを低減する（保険的対策）」など、選択する対策が、どのような性質を持っているのか、期待する効果を得られるものなのか、を正しく理解、把握することが重要である。

Web アプリのセキュリティ対策項目	内容	発生しうる脅威
SQL インジェクション	DB と連携したウェブアプリケーションの多くは、利用者からの入力情報を基に DB への命令文を組み立てる。命令文の組み立て方法に問題がある場合、攻撃によって DB の不正利用をまねく可能性がある	・DB に蓄積された非公開情報の閲覧 ・Web ページ改竄、パスワード変更、システム停止 ・不正ログイン ・ストアドプロシージャ等を利用した OS コマンド実行
OS コマンド・インジェクション	外部からの攻撃により、ウェブサーバの OS コマンドを不正に実行されてしまう問題	・サーバ内ファイルの閲覧、改ざん、削除 ・システム操作 ・不正なプログラムダウンロード ・他のシステムへの攻撃の踏み台
パス名パラメータの未チェック／ディレクトリ・トラバーサル	アプリケーションの中には、外部からのパラメータにサーバ内のファイル名を直接指定しているものがある。ファイル名指定の実装に問題がある場合、攻撃者に任意のファイルを指定され、アプリケーションが意図しない処理を行ってしまう可能性がある	・サーバ内ファイルの閲覧、改ざん、削除
セッション管理の不備	セッション ID（利用者を識別するための情報）を発行し、セッション管理を行っているものがある。セッション ID の発行や管理に不備がある場合、悪意のある人にログイン中の利用者のセッション ID を不正に取得され、その利用者に成りすましてアクセスされてしまう可能性がある	・ログイン後の利用者のみが利用可能なサービスの悪用 ・ログイン後の利用者のみが編集可能な情報の改ざん、新規登録など ・ログイン後の利用者のみが閲覧可能な情報の閲覧
クロスサイト・スクリプティング	検索のキーワードや個人情報登録時の確認画面、掲示板、ログ統計画面など、利用者からの入力内容や HTTP ヘッダの情報を処理し、表示するものがある。表示処理に問題がある場合、スクリプトを埋め込まれてしまう可能性がある	・本物サイト上に偽のページが表示される ・ブラウザが保存している Cookie を取得される ・任意の Cookie をブラウザに保存させられる
CSRF（クロスサイト・リクエスト・フォージェリ）	サービスの提供に際しログイン機能を設けているものがある。ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうか	・ログインした利用者のみが利用可能なサービスの悪用 ・ログインした利用者のみが編集可能な情報の改ざん

	を識別する仕組みを持たないサイトは、外部サイトを経由した悪意のあるリクエストを受け入れてしまう場合がある。ログインした利用者は、悪意のある人が用意した罠により、利用者が予期しない処理を実行させられてしまう可能性がある	
HTTP ヘッダ・インジェクション	リクエストに対して出力するHTTPレスポンスヘッダのフィールド値を、外部から渡されるパラメータの値などを利用して動的に生成するものがある。HTTPリダイレクションの実装として、パラメータから取得したジャンプ先のURL情報を、Locationヘッダのフィールド値に使用する場合や、掲示板等において入力された名前等を Set-Cookie ヘッダのフィールド値に使用する場合など。HTTPレスポンスヘッダへの出力処理に問題がある場合、攻撃者は、レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃を仕掛ける場合がある	・クロスサイトスクリプティングの脆弱性により発生しうる脅威と同じ脅威 ・任意のCookie発行 ・キャッシュサーバのキャッシュ汚染

表 1 Webアプリのセキュリティ対策

2.2 暗号技術最新動向

2.2.1暗号2010年問題

米国NIST（米国立標準技術研究所）が、2010年をもって、いくつかの暗号アルゴリズムの廃止および新たな暗号アルゴリズムへの移行を出したことに端を発し、現在使用している暗号アルゴリズムの危険性が見過ごせないものになり、2010年までに、より安全性の高いものに移行する必要が求められている。

対象となる暗号	アルゴリズム
共通鍵暗号	2-Key Triple DES ⇒ AES128bit以上
公開鍵暗号・電子署名	RSA⇒2048bit以上の鍵長のRSA DSA⇒2048bit以上の鍵長のDSA ECDSA⇒224bit以上の鍵長のECDSA
ハッシュ関数	次世代ハッシュ関数(SHA-3)が決まるまで SHA-1⇒SHA-2(SHA224/SHA256/SHA386/SHA512)

表 2 対象となる暗号アルゴリズム

共通鍵暗号	安全性評価

SAC2008 報告 Camellia：不能差分攻撃報告	・128 ビット鍵で 12 段（フルラウンド 18 段） ・256 ビット鍵で 16 段（フルラウンド 24 段）
ASIACRYPT2008 報告 MISTY1（フルラウンド 8 段）：不能差分攻撃報告	・FL 関数付きで 6 段 ・FL 関数なしで 7 段
CRYPTO2008 報告 ストリーム暗号 RC4：内部状態回復攻撃報告	計算量 2 の 579 乗

表 3　共通鍵暗号に関する安全性評価

ハッシュ関数	安全性評価
CRYPTO2008 報告 SHA-1（フルラウンド 80 段）：原像攻撃報告	44 段で計算量 2 の 157 乗
SAC2008 報告 SHA-256（フルラウンド 64 段）：衝突発見攻撃	・23 段で計算量 2 の 44.9 乗 ・24 段で計算量 2 の 53.0 乗
SHA-512（フルラウンド 80 段）：衝突発見攻撃	・23 段で計算量 2 の 18 乗 ・24 段で計算量 2 の 28.5 乗

表 4　ハッシュ関数に関する安全性評価

公開鍵暗号	安全性評価
ANTS-VIII 報告 Certicom 社の ECC Challenge でまだ解かれていない楕円曲線 ECC2K-130 に関する離散対数問題の計算量報告あり	2 万台の計算機を使用すれば 2 年で解ける見積り
ASIACRYPT2008 報告 素体上の離散対数問題に対する Pollard の ρ 法の高速化手法提案	1024 ビットのランダムな素体では従来よりも 10 倍速くなると報告

表 5　公開鍵暗号に関する安全性評価

その他暗号	安全性評価
Eurocrypt2008 報告	大手自動車メーカの多くで採用されているキーレスエントリー・システムで使われているブロック暗号 KeeLog に対し、攻撃可能な条件が 2 の 15 乗個の既知平文と暗号化 2 の 44.5 乗回分の計算量にまで削減され、はじめて現実的な脅威となった報告あり

ASIACRYPT2008 報告	欧州ストリーム暗号 F-FCSR-H に対する現実的な攻撃が報告
Eurocrypt2007 報告	MD5 衝突発見攻撃の一種（Chosen-prefix Collision）をデジタル証明書に関する署名の偽造に応用し、現実的な計算量で中間 CA 証明書の偽造に成功した報告あり（2008 の暮れ）
PKC2007 報告	多変数公開鍵暗号のℓIC を用いた署名方式に対し、署名偽装や秘密鍵の解読が可能と報告あり

表 6 その他暗号に関する安全性評価

2.2.2 電子政府推奨暗号リスト

2009年度公募カテゴリとして、「ブロック暗号：128ビットブロック暗号（鍵長128ビット/192ビット/256ビット）」、「ストリーム暗号：鍵長128ビット以上」、「メッセージ認証コード：鍵長128ビットである128ビットブロック暗号、および64ビットブロック暗号を利用したメッセージ認証コード」、「暗号利用モード：秘匿に関する128ビットブロック暗号、および64ビットブロック暗号を対象とした暗号利用モード」、「エンティティ認証：電子政府推奨暗号リスト」となり、現リストとの関係は、カテゴリは原則として残るが疑似乱数生成系は削除、リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることとなる。公募スケジュールは、

- 応募書類受付期間2009年10月1日～2010年2月4日17時
- 2010年3月頃 応募暗号説明会
- 2010年度 第一次評価（安全性評価及び実装可能性の確認）
- 2011年2月頃 第一回ワークショップ
- 2011年度 第二次評価（安全性評価の継続及び性能評価又はサイドチャネル攻撃に対する対策実現の確認）
- 2013年2月頃 次期推奨暗号リストを公開予定

となる。

2.2.3 暗号技術の最新動向

項目	内容
提案の動向	・HIGHT, CLEFIA, Present ⇒キーワード：lightweight, rfid, 省リソース, 省電力 ・FOX, MESH, mCrypton, SEA
攻撃法と安全性評価の動向	・代数的解析手法の進展：Cube Attack など、