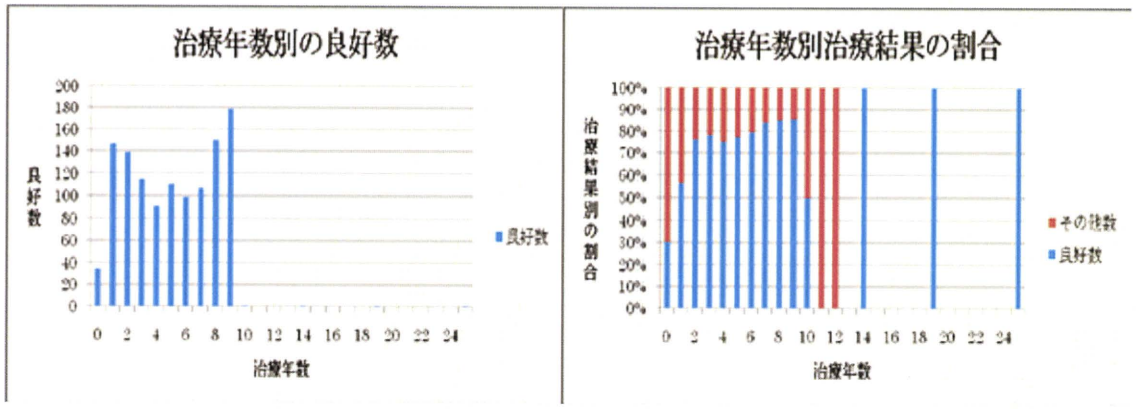
3	115	32
4	91	30
5	110	32
6	99	26
7	107	20
8	150	26
9	179	30
10	1	1
11	0	3
12	0	1
14	1	0
19	1	0
25	1	0

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。

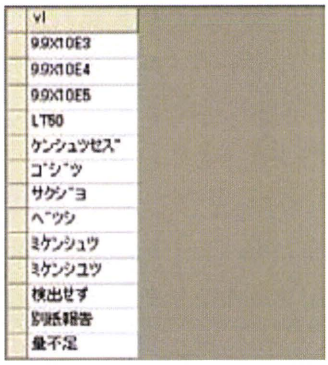
この他、同一の検査日に同一の項目（LYNPH や WBC 等）が 2 つ以上作られているデータも散見された。今回のように、VL 値のみを判断基準としている場合は問題にならないが、今後日和見感染症等を集計・解析に含めていく場合には、入力方法の統一も必要である。速報値を出す必要ある場合の入力方法や、入力されたデータが速報値であることの判別が出来るためのデータが必要である。

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
ｻｹﾝﾖ
ﾍﾞﾂｼ
ﾐｹﾝｼｭﾂ
ﾐｹﾝｼｭﾂ
検出せず
影響報告
量不足

VL 値もミケンシュツ・ミケンシュツ・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、

	SAT/SMT Solverなど解析ツールの進化 ・関連鍵攻撃：AESへの攻撃など、鍵スケジュールを積極的に利用 ・不能差分攻撃 ・線形攻撃の一般化
実装に関する傾向	・より広い範囲の製品・サービス ・より安いコスト：消費電力など ・より安全に：進化する実装攻撃への防御が必要
注目すべき暗号	・HIGHT(2006) ：ブロック長 64ビット・鍵長128ビット、RFID向け、ハードウエア性能に優れ、約3Kgateで実装可能 ・CLEFIA(2007) ：ブロック長128ビット・鍵長128/192/256ビット、ソフト・ハードともにバランス良く優位な性能 ・PRESENT(2008) ：ブロック長64ビット・鍵長80/128ビット、速度は遅いが2Kgate以下（暗号回路のみ）の実装も可能

表 7　ブロック暗号の最新動向

項目	内容
暗号利用モード	ブロック暗号の欠点を補うパッチ
最近の動向	単なるパッチから安全な暗号プリミティブの手軽な構成方法へ ・多様化、様々なバリエーション ・証明可能安全性 ・(例) Tweakable Block Cipher ：ブロック暗号からブロック暗号へ（ディスクセクタ暗号化利用モードとしての応用あり）
評価方法に関する意見	・全般（公募カテゴリ）：用途、鍵長、ブロック長等毎に分類 ・セキュリティ要件（証明可能安全性）：証明の前提が崩れたときの耐性について、例えばHMAC 鍵回復攻撃など ・パフォーマンス要件：内部で用いるプリティ部はできる限り共通化して評価すべき ・標準化・利用実績・各種標準化をどこまで扱うのか

表 8　暗号利用モードの動向

項目	内容
最近の動向	・CMAC (OMAC)の NIST SP800-38B 公開⇒日本の貢献 - 偽装困難性を一個の鍵で実現した紹介可能安全な MAC ・Hash 関数ベースの MAC への攻撃 - 脆弱なハッシュ関数を用いた場合に鍵回復攻撃が可能 ・段数を削除したブロック暗号を利用した MAC (MT-MAC, PELICAN 等) - ただし証明可能安全性は精査の必要あり

表 9 MAC の動向

項目	内容
エンティティ認証	通信相手が意図した正しい通信相手であることを確認
最新動向	・フォーマルメソッドによる安全性証明がだんだん使えるようになってきた ・しかし、プリミティブが理想化できない場合に暗号学的メソッドの融合が必要
電子政府推奨暗号リストのエンティティ認証カテゴリの評価	・形式的な手法（フォーマルメソッド）を用いた評価⇒世界初 ・暗号プリミティブが既存の場合、これらを理想的安全として評価。新規の場合、理想化せずに安全性を検証 ・ただし、フォーマルメソッドツール自体の信頼性評価が重要

表 10 エンティティ認証の動向

項目	内容
動向と現状	・1995年、SHA-1 が FIPS 180-1 ・2002年、SHA-256/384/512 が FIPS 180-2 ・2004年、SHA-224がFIPS 280-2 ・2005年、SHA-1の Collision 攻撃 実はMD5が先に Collision発見され、後にMD5WithRSA1024Encriptionのデジタル証明書が解読される ・2007年、SHA-3 competition開始、SHA-3は 2012年に選定予定
SHA-3 competition	・SHA-3 は SHA-2 の replace でなく、FIPS 180-2 への追加を想定

	・最重要の評価基準は安全性 ・ハード性能は必須ではない ・応募総数64，第一ラウンド通過51，現在42
CRYPTRECへのコメント	・現在は汎用、特殊用途やハッシュ関数関連モードの検討の余地あり ・評価項目：SHA-3 と同じでよいが、ハードウエア性能も必要では

表 11　ハッシュ関数の動向

項目	内容
IBE　（　Identity Based Encryption）	自由なビット列を公開鍵暗号として設定可能な暗号で、色々な応用が知られている
最近の動向	・標準化が進んでいる：　IEEE P1363.3，RFC5091 ・NISTも興味をもっている（NIST Workshop） ・世界で少なくとも600万人が使用
2008年度の暗号技術監視委員会の活動として、IDベース暗号WGが開設された	・報告書をまとめている最中 ・検討課題：運用（IDの信頼性、PKGの信頼性、ユーザ鍵管理、共通パラメータ管理）

表 12　IBE の動向

2.2.4本研究で採用する暗号アルゴリズムについて

本研究で採用する暗号アルゴリズムは、「AES(Advanced Encryption Standard)」を採用する。また、暗号化モードは「CBC(Cipher Block Chaining)」を利用する。

AESは、それまでの暗号規格「DES」がコンピューターの技術進歩により脆弱なものとなったため、NIST（アメリカ国立標準技術研究所）が次世代の暗号化標準（Advanced Encryption Standard）として選定したRIJNDAEL（ラインドール）という共通鍵方式の暗号化アルゴリズムで、FIPS PUB（米国連邦情報処理規格）197として規定、公開されている。ブロック長は128ビット、鍵長は128、192、256ビットから選べるようになっており、速度も「DES」に比べ非常に高速である。現在、強度、速度の両方において最も優れた暗号化アルゴリズムとして、米国政府機関における採用義務化はもとより、日本における電子政府推奨暗号やNESSIE（欧州連合の暗号規格）に公式認定されるなど、今後も世界中の多くで暗号標準への採用が進んでいくものと推測される。

よって本研究で試作する暗号化通信ツールでは、暗号化アルゴリズムとして「AES」を採用した。

2.3 漢字コード最新動向

2009 年 11 月 10 日、文部科学省の「文化審議会国語分科会」において、常用漢字表の改正案が承認された。現行の常用漢字表にある 1945 字から「銑」「錘」「勺」「匁」「脹」の 5 字を削除し、新たに 196 字を追加する改正案で、2010 年度の内閣告示を目指している。 新しい常用漢字表が告示されると、「シフト JIS」や「EUC-JP」といった従来からある文字コードを使用するシステムで大きな問題が生じる恐れがある。新しい常用漢字表 2136 字のなかに、シフト JIS や EUC-JP では書けない（扱えない）漢字が含まれている。

勺　錘　銑　脹　匁

図 6　新しい常用漢字表から削除される字種候補（5 字）

挨　曖　宛　嵐　畏　萎　椅　彙　茨　咽　淫　唄　鬱
怨　媛　艶　旺　岡　臆　俺　苛　牙　瓦　楷　潰　諧
崖　蓋　骸　柿　顎　葛　釜　鎌　韓　玩　伎　亀　毀
畿　臼　嗅　巾　僅　錦　惧　串　窟　熊　詣　憬　稽
隙　桁　拳　鍵　舷　股　虎　錮　勾　梗　喉　乞　傲
駒　頃　痕　沙　挫　采　塞　埼　柵　刹　拶　斬　恣
摯　餌　鹿　叱　嫉　腫　呪　袖　羞　蹴　憧　拭　尻
芯　腎　須　裾　凄　醒　脊　戚　羨　煎　腺　詮　箋
膳　狙　遡　曽　爽　痩　踪　捉　遜　汰　唾　堆　戴
誰　旦　綻　緻　酎　貼　嘲　捗　椎　爪　鶴　諦　溺
塡　妬　賭　藤　瞳　栃　頓　貪　丼　那　奈　梨　謎
鍋　匂　虹　捻　罵　剝　箸　氾　汎　阪　斑　眉　膝
肘　訃　阜　蔽　餅　璧　蔑　哺　蜂　貌　頬　睦　勃
昧　枕　蜜　冥　麺　冶　弥　闇　喩　湧　妖　瘍　沃
拉　辣　藍　璃　慄　侶　瞭　瑠　呂　賂　弄　籠　麓
脇

図 7　新しい常用漢字表に追加される字種候補（196 字）

表外漢字字体表には、印刷に用いるべき「印刷標準字体」として、「遡」「塡」「頬」など 1022 字が収録されている。ところが、シフト JIS や EUC-JP では、これら 1022 字をすべてはサポートできていない。そして、サポートできない文字のいくつかが、新しい常用漢字表に追加される見込みである。

常用漢字表	S-JIS	EUC-JP	UCS-2	UTF-16	UTF-8
叱	-	-	-	D842DF9F	F0A0AE9F
塡	-	8FB8B4	5861	5861	E5A1A1
剝	-	-	525D	525D	E5899D
頬	-	8FE8A4	9830	9830	E9A0B0

図 8　新しい常用漢字表にあってシフト JIS にない 4 字

したがって「叱←口へんに七」「塡」「剝」「頬」の 4 字を含む新しい常用漢字表をサポートするためには、文字コードは、Unicode（UTF-16 か UTF-8）を使う必要性がでてくる。これまでの常用漢字と同じ構成要素の字体を、やはり許容字体として併記することを要望します。その上で、「付 情報機器に搭載されている印刷文字字体の関係で…当該の字体の使用を妨げるものではない。」という文言は、削除すべき等、改定常用漢字表試案への意見が多数出されている。文字コードは、将来的に Unicode で統一される方向であると思われるが、現状、一部の OS 等では、コードが振られていない異体字の存在や、標準収録されている漢字違い、拡張漢字未対応など、様々な課題がある。

このため、患者参加型ポータルサイト構築、治療データ蓄積、印刷という概念のない患者携帯端末等への情報発信等、漢字を使用する場面での検証・考慮が求められる。

2.3.1 本研究における対応について

事前調査の結果、上記のようなことが判明した為、今回試作した暗号化通信ツールで利用する文字コードは、UTF-8 としている。

・設定したOSの文字コード　→　UTF-8
・設定したミドルウェアの文字コード　→　UTF-8

共同研究機関との診療データ共有による
多剤併用療法の成果解析報告書

（第 1.0 版）

平成 23 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		2011/01/08	

目次

はじめに 3

背景　3
今年度研究概要 4

第 1 章 各病院治療データ解析 5

実装ツール処理内容 5
解析データ 6
解析結果 6
解析ツール修正 10
総括　10