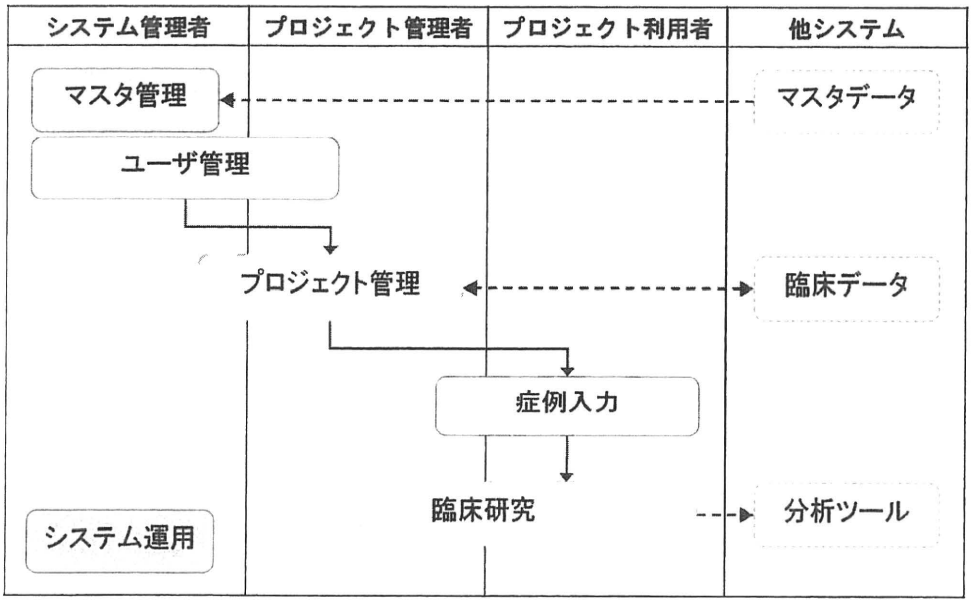

図４　運用構成図

システム構築対象として小児科、神経内科、総合診療科からそれぞれ、「ハイリスク新生児」、「自己免疫性肝疾患」、「脳卒中データベース」等のプロジェクトを設定した。

それぞれのプロジェクト毎に、プロジェクト管理者は入力ページの構築を行い、その項目に従いプロジェクト利用者がVPN経由のWeb画面にデータを入力する。

本事業は、電子カルテ（HIS）から直接データを抽出したり、HISと連携を行うものではなく、各医療機関よりデータをWeb経由で手動入力または一括取込みを行うものである。臨床研究で収集するデータは診療記録ではなく各診療科で決められたテーマに従った項目（例えば患者の基本情報や所見入力が主）ということになるが、データはSS-MIXに基づく標準ストレージに格納される。

結果、今後本事業外の他プロジェクトで収集された標準データと相互利用することにも貢献できると考える。

５．【まとめ】

今回、様々な症例収集に迅速・汎用的に対応可能な臨床研究データベースシステムを構築した。また、構築にあたりSS-MIXに基づく標準ストレージ・拡張ストレージフォルダにデータを格納することで、将来的なデータ交換にも応用できると考える。実稼働後、標準ストレージによるデータ交換によりさまざまな標準データ交換が可能となることで地域医療機関が抱える膨大な臨床研究データを大規模多施設共同臨床研究あるいは大規模コホート研究を容易とし、地域に根ざした臨床研究データを創出し、地域医療や大学病院の研究を発展させるものと考える。

６．【謝辞】

本研究は、厚生労働科研費「医療現場にとって必要な医療情報標準化の整備と利活用に関する研究（H22-医療-一般-029）」、「診療録等標準形式情報を活用した各種定型文書の作成・情報共有に関する研究（H21-医療-指定-012）」および「病院情報システム端末からの安全なインターネット直接接続に関する研究（H22-医療-一般-030）」の成果であり、感謝する。

【参考文献】

(1)山之口稔隆、中島直樹、西山謙、坂井清太郎、橋本真琴、田中雅夫、病院情報システムでのSS-MIX web参照システムを用いた他院からの紹介データ参照の運用．医療情報学29（supp１.）：631-633、2009.

演題番号：ＰＩ－６３

二次利用目的で抽出する診療データの暗号化のためのパスワード管理システム

○安徳恭彰[1)]、中島直樹[1)]、山下隆範[1)]、山之口稔隆[1)]、田中雅夫[1)]

1）九州大学病院医療情報部

e-mail：antokuy@info.med.kyushu-u.ac.jp

１．【背景】

九州大学病院（以下本院）では2008年の電子カルテ化以降、診療情報は日々データベース上に蓄積されており、データ解析の需要は日々増大している。本院では、それらのニーズに応えるべく、システムの利便性を高めるデータベース構築等を行っている[1)]が、需要に応えることと同時に二次利用に関する危惧すべき点の検討も重大な課題となっている[2)]。

九州大学病院では、電子カルテのネットワークは、研究用をはじめとするその他インターネットには接続していない。また、USBメモリ等外部メディアの利用を禁じ、データの不用意な漏洩に備えてきた。このため、これら診療情報を研究もしくはその他二次的な目的に利用する場合、専任者が抽出したデータをCD-RやUSBメモリなど外部メディアに書き込み、抽出依頼者に手渡している。しかし昨今、これら外部メディアに保存されたデータが紛失等の理由により外部に流出するといった事件の報道が後を絶たない。本院でも、過去に類似の事故が発生しており、決して他人事ではない。

そこで我々は、抽出データに対する適切なパスワード管理を開始した。十分な強度を持つパスワードによってデータファイルを暗号化し、流出や漏洩に対する対応を行ったので、紹介する。

２．【目的】

データ抽出から、依頼者がデータを受け取りファイルを開くまでの間に紛失、漏洩等が起こる危険性を考慮してパスワードによるデータ暗号化を考えた。パスワードは、基本的に第３者に推測されにくい文字列が望ましいが、それらパスワードを抽出者と依頼者の間で共有することは難しい。従来は、内線番号（数字４桁）等ある程度利用者との知識共有ができるキーワードで暗号化を行っていたが、昨今のコンピュータ技術の発達とともに、数字４桁の暗号化程度では、条件さえ整えば解読することは容易である。

そこで、適切な強度を持つパスワードを、適切な方法でデータ抽出者と依頼者間で共有することを目的としてシステムの構築をおこなった。

３．【方法】

本システムは、パスワード管理システムとして、サーバ(OpenSUSE11.2)上に、Apache2.2.13でWebサーバを構築、データベースにはMySQL5.1.51を使用した。また、本システムを利用する際の認証サーバとしては、九州大学の全学共通IDのLDAPサーバを利用した。システム運用の流れ図を図１に示す。九州大学では、SSOKIDと呼ばれる全学共通IDを運用している。このSSOKIDを使ってLDAPによる本人認証を行い、認証後、データを暗号化したパスワードの閲覧をおこなう。手順としては、データ抽出者がデータ抽出後、Webサイトにアクセスし依頼者のSSOKIDを入力し新規パスワードを発行する。抽出者は、発行されたパスワードを使ってデータファイルを暗号化、暗号化されたファイルをリムーバブルメディア

等に保存して依頼者に手渡す。暗号ファイルを受け取った依頼者は、Web サイトにアクセスし、SSOKID で認証、表示されたパスワードでファイルを複号化する。

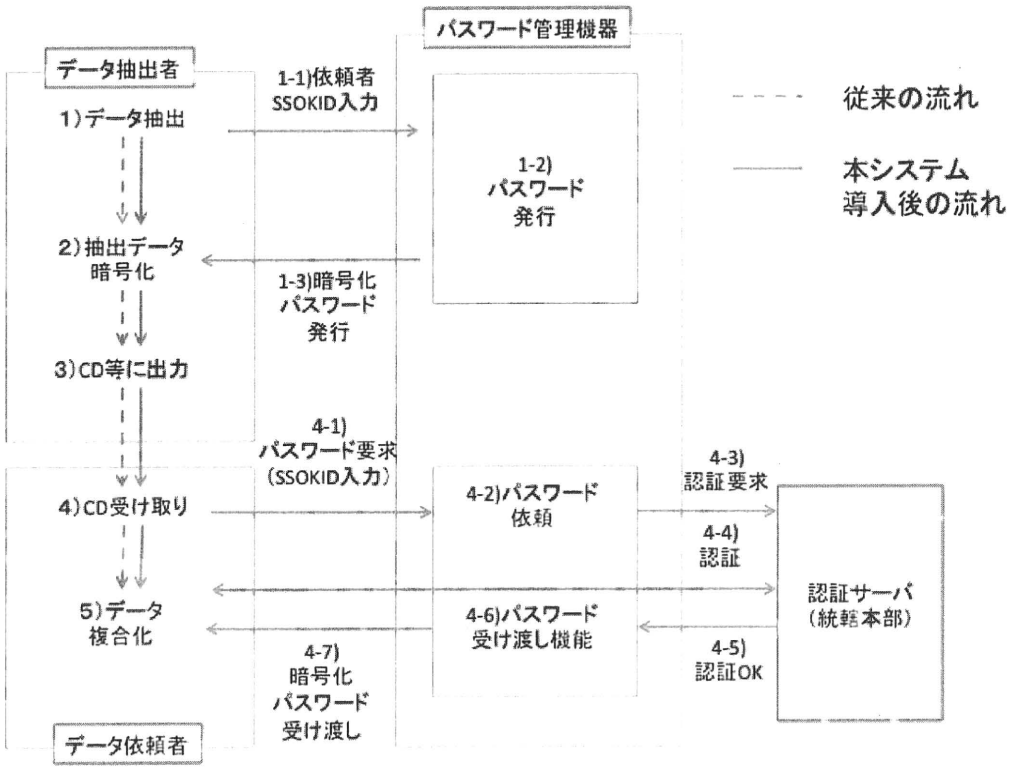

図 1　システム構成図

当初、SSOKID の ID とパスワードでの暗号化を検討したが、SSOKID のパスワードは動的に変更可能であることに対し、抽出データは抽出時に静的に暗号化される。このため、SSOKID とは独立しパスワードを管理する方式を採用し、パスワード閲覧に SSOKID による認証を用いた。

また、暗号解読の難易度を高める目的で、暗号鍵の文字列は１０文字以上とした。

４.【結果】

データ抽出者がファイルを暗号化する際のパスワード発行画面を図２に示す。データ抽出者は、SSOKID で発行画面にログイン後、依頼者の SSOKID および付加情報を入力し、発行ボタンを押してパスワードを発行する。

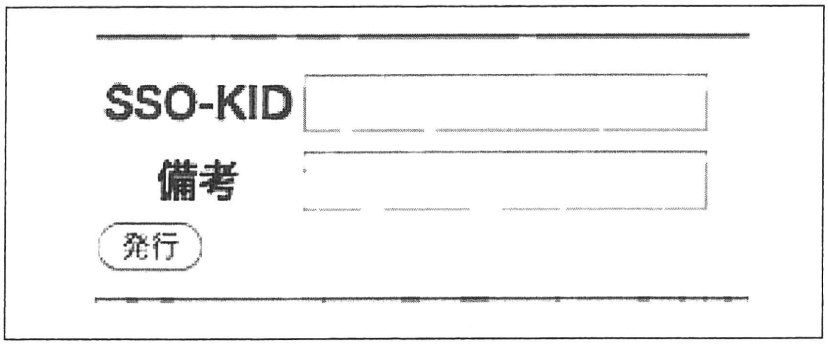

図 2　パスワード発行画面

抽出依頼者がファイルを複号化する際のパスワード確認画面を図３に示す。依頼者がログインすると、現在発行されているパスワードの一覧が表示される。付加情報を元に該当のパスワードを確認し、ファイルを複号する。

あなた（7095364168）に現在付与されているパスワードは下記の通りです。

発行日	備考	パスワード
2010-12-24 08:45:24	12月２３日情報検索用	85cxV4tL6b
2010-12-24 08:44:41	１２月２０日情報検索用	nYPrZX8Hqo

図 3　パスワード確認画面

本システム運用後の暗号を総当たりで解析する場合にかかる時間を表１に示す。解析にはフリーソフトの Zip 暗号解析ソフト Pikazip[3] を利用した。解析機器は、CPU Pentium M 1.2GHz, Memory 1GB, OS:WIndowsXP を使用した。パスワードを英小文字、数字の組み合わせと想定し、総当たりで暗号解析を行った。

表１　文字種、文字数における暗号解読にかかる時間
（検証環境：CPU Pentium M 1.2GHz, Memory 1GB, OS:Windows XP）

文字数	数字のみ	英小文字のみ	英小文字、数字
4	0 秒	0 秒	0 秒
5	0 秒	6 秒	35 秒
6	0 秒	3 分 7 秒	21 分 51 秒
7	6 秒	68 分	*13 時間程度
8	1 分 2 秒	*29 時間	*19 日程度
9	10 分 50 秒	*32 日	*1.9 年
10	*100 分	*2.26 年	*67 年

*は実測値から計算される推定値

従来の数字４桁の暗号化では、ほとんど時間をかけずに解読できたのに対し、５桁では 35 秒、６桁では２２分程度かかる結果となった。この結果を元に英数１０文字以上で行った場合を計算すると、解析にはおよそ６７年かかる。本システムは、英小文字、数字に加

え、英大文字も含んでいるため、今後、高スペックのPCによる暗号解読が行われるとしても、総当たりでの解読はほぼ不可能と考える。

また、暗号化にかかる手間としては、従来の暗号化の場合と比べ、パスワードの書き写しによる手間以外はほぼ時間の差は発生しない。

5.【考察】

電子カルテシステムと、研究用インターネットが物理的に切り離されているため、パスワード書き写し時のエラーが問題視される。これに関し、電子カルテシステム側にパスワード発行、研究用ネットワーク側に閲覧機能といった形でシステムを分散させ、何らかの形でパスワードの同期が行えれば、これらの問題は解消されるものと考える。

6.【まとめ】

診療データ抽出時の暗号化を強化するため、パスワード管理システムを構築した。大学で一斉発行している全学共通IDと連携させることで、集中的な管理を可能とした。また、従来、ある程度推測しやすいパスワードでしか暗号化できなかったものを、より強度なパスワードで暗号化することで、診療データ受け渡し時の紛失等の問題を最小限に抑えることができたと考える。

【参考文献】

(1) 安徳恭彰、若田好史、山下貴範、鴨打正浩、中島直樹、田中雅夫、前原喜彦，アウトカム志向型電子クリティカルパスにおけるデータ解析の実情，第 30 回 医療情報学連合大会（第 11 回日本医療情報学会学術大会），2010.11.19-21

(2) 安徳恭彰、中島直樹、田中雅夫、前原喜彦、久保千春,大学病院におけるデータ取り扱い規程の策定,平成21年度大学病院情報マネジメント部門連絡会議,2010.01.21.

(3) Pikazip, URL: http:// http://www.vector.co.jp/soft/win95/util/se078535.html

標準規格の動向

木村 通男[1)] 篠田 英範[2)] 吉村 仁[3)] 安藤 裕[4)] 野口 貴史[5)]
浜松医科大学医療情報部[1)] 保健医療福祉情報システム工業会[2)]
日本画像医療システム工業会[3)] 医療情報標準化推進協議会[4)]
厚生労働省 医療技術情報推進室[5)]

Trends of standards and specifications in the medical information systems

Kimura Michio[1)] Shinoda Hidenori[2)] Yoshimura Hitoshi[3)] Ando Yutaka[4)]
Noguchi Takashi[5)]
Hamamatsu Medical University[1)]
Japanese Association of HealthcareInformation Systems Industry[2)]
Japan Industries Association ofRadiological Systems[3)]
Health Information and Communication StandardsBoard[4)]
Ministry of Health, Labour and Welfare[5)]

In the medical field many standards and specifications are proposed by many standard developing organizations. Recently health information exchange becomes an urgent problem. To solve this problem standard is necessary and mandatory. On the other hand, we should use the standard and/or specification as the right standard in the right place. To develop standards and/or specifications neutrally and to maintain standards and/or specifications are important issues.

Keywords: Standardization, JAHIS, JIRA, HELICS, MHLW

1. 概要

医療情報に関する様々な規格があり、規格制定団体や標準化推進団体として保健医療福祉情報システム工業会(JAHIS)、日本画像医療システム工業会(JIRA)、医療情報システム開発センター(MEDIS-DC)、Health Level Seven(HL7)協会、Integrating the Healthcare Enterprise(IHE)協会、医療情報標準化推進協議会(HELICS)などが活動している。医療機関の地域連携が急務となっている現在、医療情報の交換や提供などを標準的な規格を使用して行うことが必須と考えられる。各団体などでは、積極的に標準化活動が進められている。例えば、JAHISは、さまざまな分野(臨床検査、生理検査、放射線、内視鏡、処方、病名など)におけるデータ交換規約が作られており、JIRAは、DICOM規格を検討している。また、MEDIS-DCでは、MEDIS標準マスターとして、医薬品HOTコードマスター/病名マスター/歯科病名マスター/臨床検査マスター/手術・処置マスター/歯科手術・処置マスター/看護実践用語標準マスター、J-MIXなどが公開されている。また、医療情報学会(JAMI)、医学放射線学会(JRS)や放射線技術学会(JSRT)などの学術団体からも各種のガイドラインなどが公開されている。

医療機関では、いろいろな規格が乱立するとどの規格を用いればよいか判断することが困難になる可能性もある。このような状況を解決するために、医療情報標準化推進協議会からは、特定の分野で使用すべき規格を推奨する「HELICS指針」が公開されている。また、厚生労働省の保健医療情報標準化会議では、『医療機関が診療情報を電子的に外部に出す場合の標準の制度化』という事項について検討を行っている。

現在の標準規格の現状と今後の厚生省標準規格を視野に入れて、各規格の概要や標準規格に求められる中立性、整合性や規格の保守・管理などについて、各演者から報告する。

(1)標準化の曲がり角　木村通男(浜松医科大学)
(2)JAHISにおける標準化活動　篠田英範(保健医療福祉情報システム工業会)
(3)JIRAにおける標準化活動　吉村仁(日本画像医療システム工業会)
(4)HELICS協議会の標準化活動　安藤裕(医療情報標準化推進協議会)
(5)厚生労働省における厚生労働省標準規格　野口貴史(厚生労働省 医療技術情報推進室)