厚生労働科学研究費補助金

医療安全・医療技術評価総合研究事業

個人情報保護を指向した地域医療連携における セキュリティシステム構築及び運用管理に関する研究

平成１９年度　総括・分担研究報告書

主任研究者　**本　多　正　幸**

平成２０（２００８）年　３月

主任研究者：

本多 正幸	長崎大学大学院・医歯薬学総合研究科医療情報学講座

分担研究者：

山野邊 裕二	国立成育医療センター
松本 武浩	長崎大学大学院・医歯薬学総合研究科医療情報学講座
中山 良幸	株式会社 日立製作所　公共システム事業部
梁瀬 和夫	ケービーソフトウェア 株式会社

研究協力者：

須藤 広明	株式会社 日立製作所　公共システム事業部
佐藤 正	株式会社 日立製作所　九州支社
藤田 龍一	ケービーソフトウェア 株式会社

「個人情報保護を指向した地域医療連携における
セキュリティシステム構築及び運用管理に関する研究」
報告書

目　次

Ⅰ．総括研究報告

主任研究者：本多正幸

第１章

総括

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
総括研究報告書

個人情報保護を指向した地域医療連携における セキュリティシステム構築及び運用管理に関する研究

（H 18-医療-一般-042）

主任研究者　本多　正幸
（長崎大学大学院・医歯薬学総合研究科医療情報学講座　教授）

研究要旨

複数の医療機関による情報共有、情報連携が必要不可欠な地域医療連携においては、個人情報保護法への対策を考慮した情報セキュリティ機能の実装が強く望まれている。当該システムは各地域にも適用可能な汎用性を持たせながら、医療機関のタイプ（病院、診療所等）の違いをも吸収する必要がある。

平成１８年度はセキュリティ技術の適用を重点的に検討した。地域医療連携システムにおけるセキュリティポリシーに関する調査では、本来、患者ごとに医療従事者のアクセス制限が設定されるべきであるが、現状不十分な環境であること等を明らかにした。個人情報保護の観点からは暗号化の対象となるＸＭＬ文書、暗号化に使用する鍵情報、暗号化の対象となるエレメント情報を選定するとともに、選定エレメントのみの暗号化が可能なプログラムのプロトタイプを製作した。また、平成１８年度はアクセス権や利用状況に基づいて暗号化対象エレメントを決定するプログラムのプロトタイプを製作する予定であったが、調査の結果、利用を予定していたＸＡＣＭＬではＸＭＬ-ＤＢに対して十分なアクセス制御が困難であったため、データベース・マネジメントシステム（ＤＢＭＳ）、　．ＮＥＴ　ｆｒａｍｅｗｏｒｋ技術を利用して機能実現できるように仕様変更し実装した。さらに、平成１６年度厚生労働科学研究、医療技術評価総合研究（研究課題名：「医療情報統合管理のための地域医療連携システム開発研究」）で検討したＸＭＬデータベース（ＸＭＬ-ＤＢ）を対象に、セキュアなデータベースシステム構築のための基盤を引き続き検討した。

これらの成果を踏まえて平成１９年度は重点的に「地域医療連携を指向したセキュアな医療情報統合管理システム」の構築を実施した。即ち、医療機関タイプ(病院、診療所等)毎に必要になる設計諸元を整理し、ＸＭＬ-ＤＢ設計、雛型ＸＭＬスキーマの実装、ＸＭＬエレメントの変換速度、効率等を指標に雛型ＸＭＬスキーマのセキュリティ機能を評価した。加えて医療情報統合管理システムにおけるセキュリティ管理の観点から単にセキュリティ技術を検討するのではなく、システム運用管理方法の検討に重点を置いた解決方法を

検討した。以上の検討を踏まえ、現実的なユースケースを意識したＸＭＬベース医療情報統合管理システムの提案と構築、管理方法を提案した。

分担研究者
松本武浩・長崎大学大学院医歯薬学総合研究科・助教授
中山良幸・(株) 日立製作所公共システム事業部・主任技師
梁瀬和夫・ケービーソフトウエア株式会社・代表取締役社長

Ａ．研究目的

我々は、これまで地域医療連携を目的に構築される医療情報統合管理システムの開発において、セキュリティ機能の向上、プライバシーの確保を基盤に、インターネット技術を活用して各患者の家庭からも医療情報の検索・参照が可能になることを目指している。本研究ではこれまでの研究成果を背景に、個人情報保護法への対策を指向したデータベースの為のセキュリティ技術の設計・構築・管理技術に関する具体的な方法論と有効性を明確にし、自動データ変換ツールを武器に地域医療連携の効率化を促進することを目的としている。(注：自動データ変換ツールとは、各種医療機関の独自形式ＸＭＬスキーマより共通ＸＭＬスキーマへの変換を自動化するツールのこと)

また、システムに格納された医療コンテンツ（医療情報）については、作成した医師から患者を含めたエンドユーザまで、利用履歴を把握するとともに不正利用監視・追跡というデータ格納後のセキュリティ対策も必要である。しかしながら、一旦、医療コンテンツをデータベースに格納した後のセキュリティ対策については十分な検討が行われてこなかった。またＸＭＬ技術をベースとしたシステムにおいては、ＸＭＬ署名、ＸＭＬ(エレメント)暗号化技術の採用とともに、ＸＭＬ鍵管理、ＸＭＬメッセージング等を利用したセキュリティ対策全般についても早急に検討する必要がある。

Ｂ．研究方法

Ｂ－１．平成１８年度研究

1．地域医療連携システムにおけるセキュリティポリシーに関する調査

2005年4月に施行された個人情報保護法への対策を指向したセキュリティシステムに関して、医療情報連携システムとしての技術的要件を整理し、技術的な意味での実現可能性と運用をも踏まえた実現可能性を検討したところ以下の諸点が判明した。

(1) 地域医療における情報連携では前方/後方連携が重要であるが、情報の診療前取得が困難である。

(2) 患者ごとに医療従事者の情報アクセス制限が設定されるべきであるが、現状不

十分な環境である。

(3) 地域医療連携データベースシステムはなるべく既存インフラ（インターネット等）を流用することが好ましいが、インターネットの保護通信のデ･ファクト･スタンダードであるＳＳＬ／ＴＬＳは２者以上の保護セッション、データの一部暗号化が困難である。

以上より、セキュリティシステムは複数セッションを保護する機能、及びＸＭＬ-ＤＢのデータ呼び出し時のコンテキストを考慮する必要がある点等が明らかになった。

２．医療情報統合管理システムにおけるＸＭＬセキュリティ技術の開発

平成１８年度は、個人情報保護の観点から暗号化の対象となるＸＭＬ文書として「診療情報紹介状」を選定した。また暗号化ＸＭＬスキーマを設計・作製し、エレメントのみの暗号化が可能なＸＭＬ文書暗号化及びＸＭＬ-ＤＢへの登録機能を具備したプログラムのプロトタイプを作製した。

ＸＭＬ署名方式としては標準的な署名方式に対応し、各種暗号化アルゴリズムも選択可能である。但し、平成１８年度に開発したアクセス制限は限定的であり、平成１９年度にセキュリティビュー技術等を加味し実装した。

Ｂ－２．平成１９年度研究

１．医療情報統合管理システムにおけるセキュリティ・データベース（ＤＢ）の設計・開発

これまで検討した医療情報管理システムにセキュリティ技術を組み込んだ場合の評価を中心に実施した。具体的には大学病院タイプ雛型ＸＭＬスキーマの利用を想定した場合のＤＢを設計するとともに、医療機関への適用性を検証した。また医療機関タイプ毎(病院、診療所タイプ等)に必要になる設計諸元を整理し、ＸＭＬ-ＤＢ設計におけるデータモデリング、データベースモデルの選定を含む論理設計及び物理設計について検討した。

２．医療情報統合管理システム(ＸＭＬ-ＤＢ)におけるトランザクション管理方法の検討(当初計画からの変更点(追加))

ＸＭＬ-ＤＢを中核にした医療情報統合管理システムでは、複数の医療機関における複数のユーザによるアクセスが想定される。実運用を想定する場合、クエリと複数の更新操作が並列に起こることが容易に想定されるが、実行結果の保証、整列化可能性そして障害からの回復といった観点から、データの一貫性を保つ機構が必要になる。即ち、トランザクションという枠組みでＸＭＬ-ＤＢ更新操作を管理することが望まれる。本研究ではＸＭＬ-ＤＢにおけるトランザクション管理機能のあり方を検討した。

３．医療情報統合管理システムにおけるセキュリティ管理方法の検討（重点的に取り組む部分）

単にセキュリティ技術を検討するのではなく、地域医療ネットワーク等での利用をイメージしたシステム運用管理方法の検討に重点を置いた解決方法を検討した(図１参照)。さらに、診療情報提供書交換実証試験及び各診療科アクセス制御試験などを行った。

エンドツーエンドのセキュリティを実現するためには、通信全体の一元的な保護ではなく、XMLセキュリティによるデータの選択的な保護（暗号化）が必要になることを明らかにするとともに、任意のXMLエレメント暗号化が可能な医療連携システムの設計・開発を実施して基本設計諸元を明確にした。

ＩＰｓｅｃやＳＳＬ／ＴＳＬでは実現が困難なエンドツーエンドのセキュアな送受信システムを部分暗号化ＸＭＬセキュリティで実装し、Ｗｅｂサービスによる職位によるエレメント暗号化、診療科によるアクセス制御機能の動作確認及び医療機関をフィールドにした実証試験を実施した。その結果、本システムの有効性を確認するとともに、今後の改良方針に言及した。

（倫理面への配慮）

今回の研究対象は、実際の病院の患者データベースは用いずに、ダミー患者データを用いた。今後の展開で、実患者データを用いる場合においても、個人識別可能な情報の匿名化などを行いセキュリティや患者プライバシー情報の保護には万全を期して行う。

Ｃ．研究結果

研究結果については、「Ｂ．研究方法」にまとめて記述した。また、詳細な結果は分担研究報告に記載した。

Ｄ．考察

Ｄ－１．国内外における研究状況

従来の電子カルテを中心とした地域医療連携では盗聴、改ざん、成りすまし、事後否定対策としてＳＳＬ暗号、セキュアストレージ(公証機能、タイプスタンプ機能を利用したストレージサーバ)を利用したセキュリティ対策が一般的であったが、医療情報のような秘匿性が高い個人情報を扱う場合はそれだけでは不十分である。本研究ではアクセス権や状況に基づくＸＭＬ署名、ＸＭＬ暗号化等を利用したセキュリティシステムを提案し、十分なセキュリティ対策の確保を目指している。ＸＭＬデータベースとＰＫＩを組み合わせることにより、新たなセキュリティ機能をＸＭＬデータベースに付与することが可能である。このようなアプローチは一般的な意味で今後の重要な課題であると認識しているが、これまで類似研究はあまり例をみない。コンピュータネットワークの分野ではＳＳＬ/ＴＬＳ、ＶＰＮ、Ｓ／ＭＩＭＥなど多くのプロトコルやデバイスで、ＰＫＩの技術が広く用いられているがデータベースへの応用例は少ない。ただ、エジンバラ大学のグループがセキュリティビューに関して報告している。

Ｄ－２．本研究の特色・独創的な点

本研究における特色および独創的な点を以下に示す。

(1) ＸＭＬスキーマ自動解析システムにより、医療情報統合管理システムにおけるデータベースでのＸＭＬ暗号化、ＸＭＬエレメント暗号化を半自動化することが可能であること。
(2) ＸＭＬ署名、ＸＭＬ暗号化、またはＸＭＬ文書の相手に応じ部分的暗号化を施したＸＭＬエレメント暗号化技術を採用していること。
(3) 医師を始めとするエンドユーザの利用状況、コンテンツの素性、不正利用監視・追跡を確認することが可能になること。
(4) ＸＭＬなどのデータ交換の標準化の技術や、ＡＳＰ／ｉＤＣ（アプリケーションサービスプロバイダー/インターネットデータセンター）技術を利用していること。
(5) 医療機関への適用のみならず、保健・福祉といった分野との連携も可能であること。

Ｄ－３．期待される成果

以下の2点が期待される成果と考える。
(1) 従来の通信経路だけを暗号化するＳＳＬでは実装できなかったサーバ上にセキュリティ技術を組み込んだ情報管理が可能になり、よって各種地域医療連携システムにおける不正利用の監視・追跡が可能になる。
(2) 複数の医療機関における情報共有がよりスムーズかつ効率的に実現できる。

本研究が対象としているセキュリティ技術は、各医療機関に対して個人情報保護法の対策に向けた重要な情報提供となり、一般的な意味でＸＭＬベースの医療情報データベース構築の際の提言になると考える。また病院や診療所などの医療環境のみならず保健所や介護施設など、保険・福祉分野への拡張も可能であり、自治体の持つ健診情報・介護等福祉情報を連携させたセキュアな総合健康サポートシステムへと発展していくものと期待できる。

平成１９年度は特にシステムの構築を実施することにより、個人情報保護法に即した複数の医療機関における情報共有がよりスムーズかつ効率的に実現できることが期待できる。

Ｅ．結論

個人情報保護の精神に則り、患者情報の取り扱いには今後更なる注意が必要である。例えば本研究で対象とした診療情報提供書を診療所の方から病院へ転送する場合を考えても、病名などの秘匿性の高い情報に関しては事務職には参照させる必要はなく、患者にとっても見せたくない項目の一つであろうと推察する。ただし、医師にはすべての情報が参照できなくてはならない。このように職種により適切な参照制限が情報の送り側の診療所の方で設定できる機能が重要であり、運用上病院側で特別な処理を介さなくとも適切な参照制限がかけられた情報連携

が可能となる。本研究で取り上げたＸＭＬセキュリティの技術を適用することにより、個人情法保護を指向した情報連携インフラが構築できることになり、本技術の適用は医療のみならず、幅広い分野で適用可能となると考える。

将来的には、「診療録等の電子媒体による保存について」（平成１１年、厚生省通知）における、３条件である「情報の真正性」「情報の見読性」「情報の保存性」を担保する技術につながることが期待される。各医療機関で独自に持っている病院情報システムでは、「情報の真正性」の確保が最も困難であるが、本研究によるＸＭＬ－ＤＢがその機能を集中的に提供することができる。

本研究成果と平成１６年度厚生労働科学研究で取り扱った「自動解析ツール」が融合されれば、セキュアな通信とセキュアなデータベース構築が連携され、幅広いユースケースで個人情報保護を指向した医療連携が実現できると期待される。このような統合データ管理システムの実現により、患者がかかりつけ以外の病院で、診療を受ける場合にも、患者に関する必要な情報が統合データ管理システムを介し得られることにより、重複検査や禁忌薬剤の投与等の回避など、病院、患者双方にメリットは大きい。特に、個人情報保護法施行に当たり医療分野においても、より確固たるセキュリティポリシーの下で、安全管理の強化が大きな命題となっている今日の状況において、本研究の中心的課題であるＸＭＬセキュリティ技術を有効に適用していくことが肝要である。患者にとっても安心できるシステムを提供する意義は非常に大きい。

Ｆ．健康危険情報

システム開発研究のため特に特記する事項なし。

Ｇ．研究発表

１．論文発表

１）Masayuki Honda, Takehiro Matsumoto, Yoshiyuki Nakayama, Hiroaki Sudo, Kazuo Yanase, Ryuichi Fujita, An Effective Approach for Development of Regional Medical Information System Using XML Technology, MEDINFO 2007, Klaus A. Kuhn et al.(Eds), Amsterdam:IOS Press, P175(1546-1547), 2007

２）本多正幸，本村妃紗美，松本武浩，中村 尚子，小渕 美樹子，クリティカルパスの評価と改善-バリアンス分析を中心とした文献調査に基づく検討-，医療情報学，27 (Suppl.)，P6-4，2007

３）中村尚子，本多正幸，クリティカルパス再構成に向けたCART適応の一般化への試み，医療情報学，27(Suppl.)，3-D-1-1，2007

４）山野辺裕二，本多正幸，相澤志優，電子カルテの GUI 部品利用動向，医療情報学，27 (Suppl.)，P2-6，2007

５）中村洋一，中野正孝，野呂千鶴子，

西口裕，本多正幸，吉田彬，健康手帳の電子化と ASP 型電子カルテシステムの利用，医療情報学，27 (Suppl.)，P7-6，2007
6）松本武浩，本多正幸，地域医療連携 IT 化の実際「あじさいネットワークの取り組み」，医療情報学，27 (Suppl.)，S13-2-F-4，2007
7）本多正幸，松本武浩，二之宮実知子，他，新病棟における IT 化推進に関する検討－IP 電話，ベッドサイド端末，セキュリティを中心として，医療情報学，26(Suppl.)，327-328，2006
8）松本武浩，木村博典，山田理恵，安日一郎，宮下光世，本多正幸，情報システムを利用した地域医療連携運用の構築と評価，医療情報学，26 (Suppl.)，323-324，2006
9）本多正幸，米国ボストン地区における地域医療連携システムの現状－医療 IT 視察ツアー報告－，医療情報学会，九州沖縄支部平成 18 年度秋季研究会，2006
10）本多正幸，米国先進医療 IT 視察ツアー報告，第 33 回日本エム・テクノロジー学会大会，8 月，2006
11）本多正幸，山野辺裕二，中山良幸，須藤広明，梁瀬和夫，地域医療連携システムの構築；ＸＭＬを利用したアプローチ，医療情報学，25(1.)，1-5，2005
12）本多正幸，中山良幸，須藤広明，ＸＭＬを利用した地域医療連携共通データベース，クリニカルプラクティス，24(11)，1194-1197，2005
13）本多正幸，山野辺裕二，中山良幸，須藤広明，梁瀬和夫，ＸＭＬを利用した地域医療連携システムの構築に向けたアプローチ，医療情報学，24(Suppl.)，1160-1161，2004
14）山野辺裕二，本多正幸，原川明美，二ノ宮実知子，ヒヤリハット事例の収集はどれだけ役立っているか－院外報告システムの構築と課題－，医療情報学，24(Suppl.)，114-115，2004
15）山野辺裕二，本多正幸，リモート端末を利用した業務中断後の再開時間の短縮，医療情報学，24(Suppl.)，442-443，2004
16）中村洋一，中野正孝，本多正幸，吉田彬，ＡＳＰ型地域健康管理情報システムの検討，医療情報学，24(Suppl.)，1156-1157，2004
17）Honda,M, Yamanobe,Y. , On the current problems of user authentication for EMR in HIS, MEDINFO 2004, M.Fieschi et al.(Eds), Amsterdam:IOS Press, 1644, 2004
18）赤澤宏平，池田充，本多正幸，中野正孝，医療統計手法の開発と統計解析の実践について（「日本医療情報学会　課題研究会報告」），医療情報学，23，193-198，2003
19）長谷川高志，秋山昌範，・・・，本多正幸（１０番目），他，遠隔保健医療研究会、活動報告（「日本医療情報学会　課題研究会報告」），医療情報学，23，199-206，2003
20）本多正幸，医療における IT 革命（「透析医療における IT 化はどこまで進んでいるか」），臨床透析，19，1175-1182，2003
21）本多正幸，山野辺裕二，川崎浩二，大園恵幸，中川和久，２つのタイプの遠隔医療システムの共存と今後の展開，医療情報学，23(Suppl.)，646-647，2003
22）本多正幸，山野辺裕二，高橋眞弓，

病院情報システムにおけるユーザ認証の
現況と課題，医療情報学，23(Suppl.)，
950-953，2003

H．知的財産権の出願・登録状況

１．特許情報

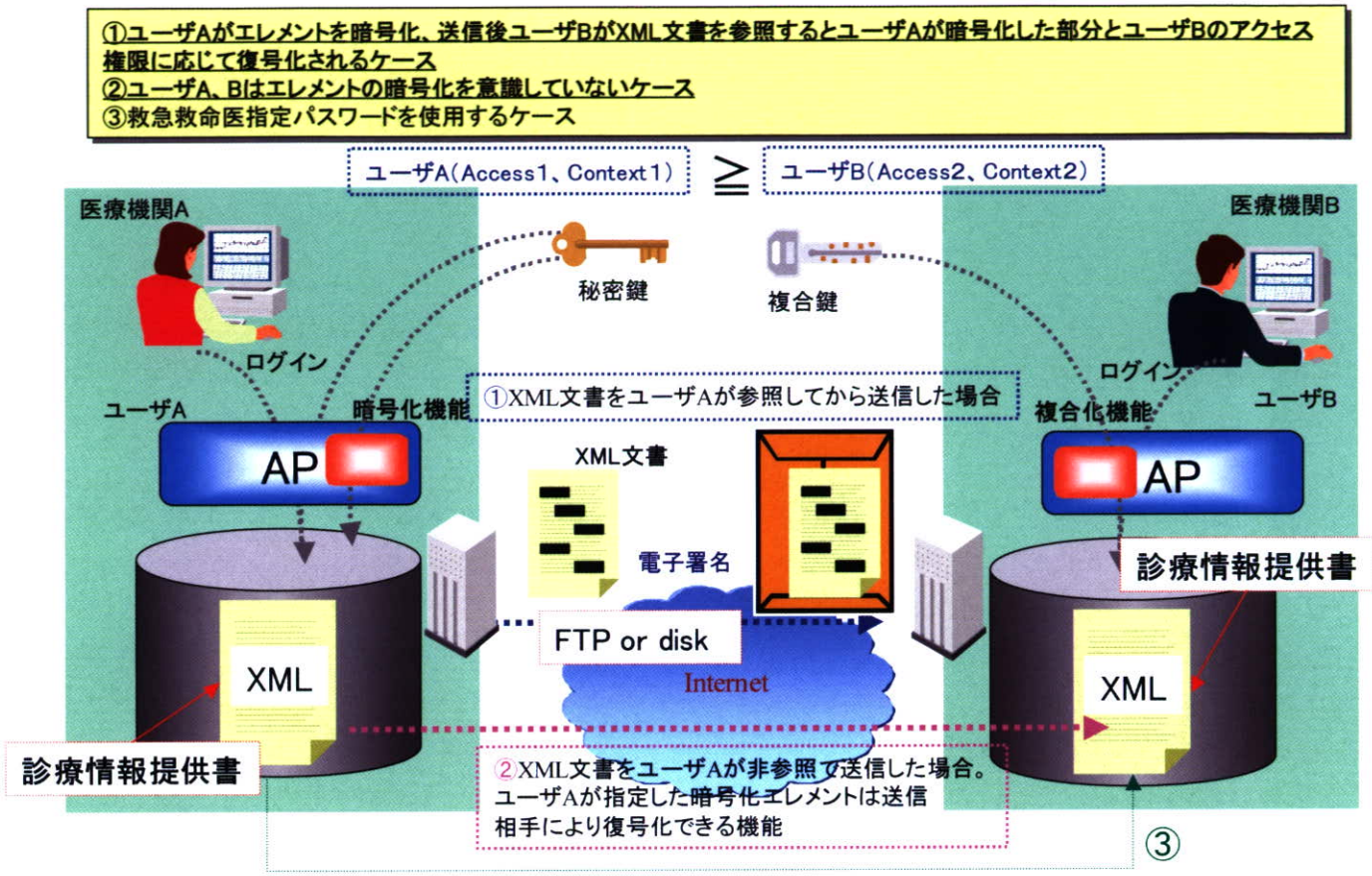
特願 2003-400516：医療情報を一元管理する医療情報管理システム（平成１５年１１月２３日）

２．実用新案登録

なし

３．その他

なし



(注)**診療情報提供書**とは、患者の病名、経過、治療内容 を記した書類(紹介状)で担当医師が作成・・・患者氏名，生年月日，性別，住所に加えて，**診療情報**として病名，紹介目的，治療経過，既往歴・家族歴，病状経過，治療経過，現在の処方，備考

図 1　地域医療連携における暗号化 XML 文書の交換様式

Ⅱ．分担研究報告

第2章

XMLセキュリティを利用した診療情報提供書システムの設計・開発

本多正幸・中山良幸・梁瀬和夫

第2章　XMLセキュリティを利用した診療情報提供書送受信システムの設計・開発

主任研究者　本多　正幸
（長崎大学大学院・医歯薬学総合研究科医療情報学講座　教授）
分担研究者　中山良幸
（株式会社日立製作所・公共システム事業部　主任技師）
分担研究者　梁瀬和夫
（ケービーソフトウエア株式会社　代表取締役社長）

研究要旨

本章ではエンドツーエンドのセキュリティを実現するためには、通信全体の一元的な保護ではなく、XMLセキュリティによるデータの選択的な保護（暗号化）が必要になることを明らかにするとともに、任意のXMLエレメント暗号化が可能な医療連携システムの設計・開発を実施して基本設計諸元を明確にしてプログラムを作製した。

A. 研究目的

昨年度、筆者らはWebサービスやebXMLなどが社会基盤の標準化を世界レベルで急速に進めていること、わが国ではいくつかの地域で病院間連携や病診連携などの地域医療連携システムが構築され、プロトタイプシステムとして稼動していること、複数の医療機関が共有するデータベース（以下単にDB）を構築する場合、セキュリティを確保したうえで予め決められた形式にそれぞれの医療機関がデータ変換を施す必要があり、システム化への課題になっていることを報告した。

一般的にコンピュータ・システムのセキュリティとしては識別、認証、許可、完全性、機密性、監査、否認防止の一部または全てを考慮する必要があることから、システム構築に当たっては医療データのXML形式変換機能に付随して、個人情報である氏名等を暗号化するＸＭＬエレメント暗号化機能、医療データの改ざんを検知するXML署名、エレメント単位のアクセス制御を可能にするＸＭＬアクセスコントロールが必要不可欠である（図2-1）。XML暗号化は、XML文書に対して秘匿性の機能を提供する技術である。暗号化方式には秘密鍵暗号方式や公開鍵暗号方式が使用可能である。XML暗号化に関しても、W3Cから”XML Encryption Syntax and Processing”の仕様が公開されている。XML暗号化には、XML文書中の指定した要素以下を暗号化するエレメント暗号と、指定した要素のコンテンツ以下を暗号化するコンテンツ暗号の2つのタイプが依存する。その他、XML文書の全体・部分暗号化や、暗号化したXML文書をさらに暗号化する仕様(Super Encryption)も存在する。

一方、コンピュータ・システム全体のセキュリティでなく、通信のセキュリティだ

けを考える「エンドツーエンド」の考え方がある。この狭義の「エンドツーエンドは」、通信において、情報の発信者から情報の受信者までの間に、情報が適切に守られていることを指す。インターネット上でセキュアな通信プロトコルとしては、ネットワーク層での保護を行う IPSec、トランスポート層での保護を行う SSL/TLS や SSH などのプロトコルが知られている。しかしながら現在のインターネットは複雑化する一方であり、必ずしも IPSec や SSL/TLS がエンドツーエンドのセキュリティを保証しない場合が存在する。例えばファイヤーウォールや NAT（Network Address Translation）などによって、多くのホストが直接 IP 通信できなくなっている。医療機関等のネットワークは、通常、ファイヤーウォールによってインターネットと隔離されていて、特定のホスト、特定のポートの通信しか許されていない。例えば診療所の医師は本研究が提供する診療情報提供書送信システムがファイヤーウォールの内側にある場合には、専用線等で繋がった紹介先の関連病院外はこのアプリケーションとの間で直接 SSL/TLS の接続を張ることができない。多くの場合、SSL/TLS 接続は DMZ（Demilitarized Zone）と呼ばれるサブネットワークにあるゲートウェイホストで一旦終端され、その後別のプロトコルでイントラネットの中にあるアプリケーションに接続されることになる。この場合、SSL/TLS で暗号化されたデータは、DMZ の中継ホストで一度復号化され、平文になる。従って、攻撃者がこの中継ホストをクラッキングした場合に通信のセキュリティが破られることになる。

本研究で取り扱う Web サービスは、もともと仲介者を通した通信を仮定している。仲介者は IP ネットワークにおけるルータとは異なり透過的でない。即ち、データの内容に対して付加価値を加えることを許可している。このような状況で、エンドツーエンドのセキュリティを実現するためには、通信全体の一元的な保護ではなく、XML セキュリティによるデータの選択的な保護（暗号化）が必要になる（図 2-3）。

本章では昨年度に引き続き「ＸＭＬセキュリティ機能付自動データ変換ツール」開発の第一歩として任意の XML エレメント暗号化が可能な医療連携システムの設計・開発を行うものである（図 2-2,表 2-1）。

B. 研究方法

B-1.研究環境

本章における研究には以下のコンピュータ環境を前提に設計に使用した。また DBMS は XML Schema に対応していること、ネットワークパケットの暗号化、監視機能を備える、統合管理ツール、統合開発環境を利用可能等の理由から総合的に選定している（表 2-2）。

●OS：Microsoft Windows XP Service Pack2

●DBMS：Microsoft SQL server 2005

●開発環境：.NET Framework 2.0

B-2.診療情報

設計・開発に供試する医療情報として診療情報提供書を選定した。診療情報提供書の例を図 2-4 に示した。

C. 研究結果及び考察

C-1.システムの概要

C-1-1.システムの基本設計

運用設計の一環としてユースケースを図2-5運用の概要に示した。基本的な手順は次の通りである。

(1) 診療所に於いて、医師が診療情報提供書（暗号化ＸＭＬファイル）を作成する。

(2) インターネット網を通じて照会先病院のネットワークまたは地域連携システムに送信する。

(3) 事務職員(医事課職員、地域連携室職員)または看護師が直接受診した診療情報提供書は暗号化／非暗号化されていて、解除しても一部情報は参照することが出来ない。診療情報提供書は必要部分（医事課職員が保険証番号、地域連携室職員、看護師が名前、年齢、等）を確認後、医師へメールにて連絡する。紹介された患者の診療情報提供書はDB等に保存し、紹介患者の来院準備等に利用される。

(4) 医師が送られた診療情報提供書を開いた場合、暗号化設定された部分を参照することが出来る。

(5) 医師が送られた診療情報提供書を開いた場合、暗号化情報をほぼ全て解除することができるが、一部、診療科が異なる場合、解除できない情報がある等の例外がある。また医師が事務職員（医事課職員、地域連携室職員）または看護師から送られた診療情報提供書を開いた場合、暗号化設定され解除された部分及び暗号化が保持された部分を解除して参照することができる。

システム構成図を図2-6に示す。システム構成は次の通りである。

(1) 診療所で作成された診療情報は指定された入力項目が暗号化されローカルPCのDBまたはファイルシステムへ保存される。

(2) また、作成された診療情報はFTPまたはSOAPプロトコルによって病院側のサーバーへ転送される。(SSL/TSL 上で通信が可能)

(3) 診療情報Webサービスでは診療所からの診療情報を受信したときあらかじめ設定されたメールアドレスへ受信通知を送付する。

(4) 病院側の本プログラムは、ClickOnceによって起動されるため、バージョンアップされた場合のプログラム配信の負担が軽減される。

C-1-2.システムの詳細設計

診療情報提供書送信用のクライアント側はVB.NET(.Net Framework 2.0)で開発を行った。プログラムの機能概要を図2-7に示す。診療情報提供書送信システムの主要な機能を次に述べる。

(1) 診療情報提供書の必要事項を入力後、次に示すプロトコルまたはストレージのうち一つを選択してクライアント側またはサーバ側ストレージに保存する事ができる。

(a) ローカルPC(NTFS)

(b) DB

(c) FTP

(d) Webサービス(XML-RPCやSOAP等を利用し、リモートサーバが管理するファイルシステムへ保存する)

(2) 保存された診療情報提供書情報を読み

込みするとともに、表示することが出来る。
(3) ログインユーザ毎の権限設定が可能とし、診療情報提供書に入力する各々のエリアについて暗号化／非暗号化の設定が可能である。
(4) 他システムからのデータ入力を簡潔にするための XML 形式でのインポート／エクスポートを可能とする。

ローカル PC(NTFS)、DB、FTP、Web サービスのうち、特に Web サービスの概要を説明する（図 2-8)。診療情報提供書送信システムの Web サービスはクライアントから要求があったサービスを処理する際に、次の機能が必要とされる。
(a) 診療情報提供書の受信
(b) 診療情報提供書の問い合わせ
(c) 診療情報提供書の送信
(d) 削除
(e) 名称変更

暗号化に関して必要となる機能は入力者である医師が入力項目の暗号化／非暗号化設定を任意に可能とする。暗号化／非暗号化設定された項目に関しては、該当ＸＭＬエレメントを暗号化する。暗号化手法は公開鍵方式とする。

C-1-3.ユーザ毎の権限
ユーザの職種（医師、看護師、医事課職員）を意識し、ユーザ ID 毎に暗号化／非暗号化解除の組み合わせが設定されている権限グループを指定する（図 2-9)。

C-1-4.診療情報保存
作成した診療情報提供書は XML 形式で保存される。文字コード体系は UTF-16 とする。

C-1-5. Web サービス
IIS6.0 及び.Net Framework 2.0 の環境で動作する。ASP.NET 上に診療情報提供書を送受信する Web サービスを構築するものとする。尚、送信した XML ファイルの保存先は DB（今回、SQL Server 2005）とする。
３階層イメージのシステムとなる

C-1-6. ＦＴＰ
診療情報提供書の送信先である診療所または病院が送信先医療機関の FTP サーバにアクセスしてファイルの送受信を行う。

C-1-7. ローカル PC（NTFS）
診療情報提供書の送信先である診療所または病院のクライアント PC のハードディスクに保存する。

C-1-8. DB
診療情報提供書の送信先である診療所または病院のネットワーク上に存在する DB にアクセスして XML ファイルの格納を行う。
２階層イメージのシステムとなる。

C-2. 画面設計及び画面遷移

C-2-1. 画面遷移
画面の全体構成及び画面遷移を次に示す（図 2-10)。

C-2-2. ログイン画面
ログイン画面の各キャプションの説明を表 2-2 に示す。入力されたユーザ ID とパスワードから DB を検索し、一致した場合ログ