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１８年度　総括・分担研究報告書

主任研究者　本　多　正　幸

平成１９（２００７）年　３月

「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

本研究では、複数の医療機関による情報共有、連携が可能な統合医療データ管理機能及び個人情報保護を目指した情報セキュリティ機能の実装を目指し、「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」を開発中である。昨年度は、地域医療連携にマッチしたＸＭＬセキュリティツールの仕様調査等を実施するとともに「ＸＭＬセキュリティ機能付自動データ変換ツール」のプロトタイプを作製・評価し、その有効性を確認した。

複数の医療機関による情報共有、情報連携を行う地域医療連携においては、個人情報保護法への対策を指向した情報セキュリティ機能を実装した「地域医療連携向けＸＭＬセキュリティシステム」の構築が強く望まれている。当該システムは、また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、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作製した。また平成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整えた。

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」の構築を実施する。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する。
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する。

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、管理方法を提案する。当初の研究計画からの主な変更点としては、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作製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ることが予想されたため、最新のセキュリティビュー技術を利用できるように平成１９年度前半までに仕様変更し、実装する予定である。

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においては、セキュリティ機能の向上、プライバシーの確保を目指しつつ、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。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を指す。

研究の必要性及び意義としては以下の点を指摘したい。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年度研究進捗

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する予定である。

Ｂ－２．平成１９年度研究計画・方法

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する。具体的には大学病院タイプ雛型ＸＭＬスキーマを利用した場合のＤＢを設計するとともに、医療機関への適用性を検証する。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、以下の項目を検討する。

(1) ＸＭＬ-ＤＢ設計…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

(2) ＸＭＬセキュリティビュー設計･･･ＸＭＬスキーマレベルでセキュリティポリシーを定義するとともにアクセス制御対象となるリソース範囲を明示的規定（当初計画からの変更点（追加））。

(3) ＸＭＬスキーマの実装…平成16年度に作成した単一医療機関タイプの雛型ＸＭＬスキーマをＤＢに実装し、ＸＭＬエレメントの変換率等を指標に雛型ＸＭＬスキーマのセキュリティレベルの評価

（注）セキュリティビューとはＸＭＬ文書の問合せに対するアクセス制御をベースとしたセキュリティ技術であり、ＸＭＬスキーマレベルでセキュリティポリシーを定義することが可能である。またアクセス制御対象となるリソース範囲を明示的に規定することができる。

参考文献：W. Fan, C. Chan and M. Garofalakis, “Secure XML Querying with Security Views”, ACM SIGMOD, 2004.

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について以下の諸点を検討する。ここでトランザクション管理機能とはデータベース内のデータを更新する一連の作業（insert、update、delete）単位を管理する機能ことである。

(1) ロック単位の選択･･･トランザクションの並列性、クエリの処理効率を評価指標に、ロックを掛けるＸＭＬデータの適正単位の明確化。

(2) ロックルールの適用評価･･･ＸＭＬデータの木構造を部分木レベルでロック可能にするルールを適応し、トランザクションのスループット、トランザクションの平均レスポンスタイム等を評価指標に適性ロックレベルの明確化。

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する（図１参照）。今後、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う予定である。

（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。

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

(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－２．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

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。

本研究成果を用いた「自動解析ツール」実現により統合データ管理システムが構築され、地域医療連携に参加する参加病院におけるインターフェース作成コストが半減し、それにより各医療機関の地域医療連携への参加可能性が飛躍的に高くなり、多くの医療機関がデータを共有できるようになる。

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, MEDINFO2007, (submitted), 2007

２）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.)，2006

３）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

４）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

５）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

６）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

７）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

８）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

９）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

10）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

11）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

12）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

13）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

14）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

15）本多正幸，山野辺裕二，川崎浩二，大園惠幸，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
16）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

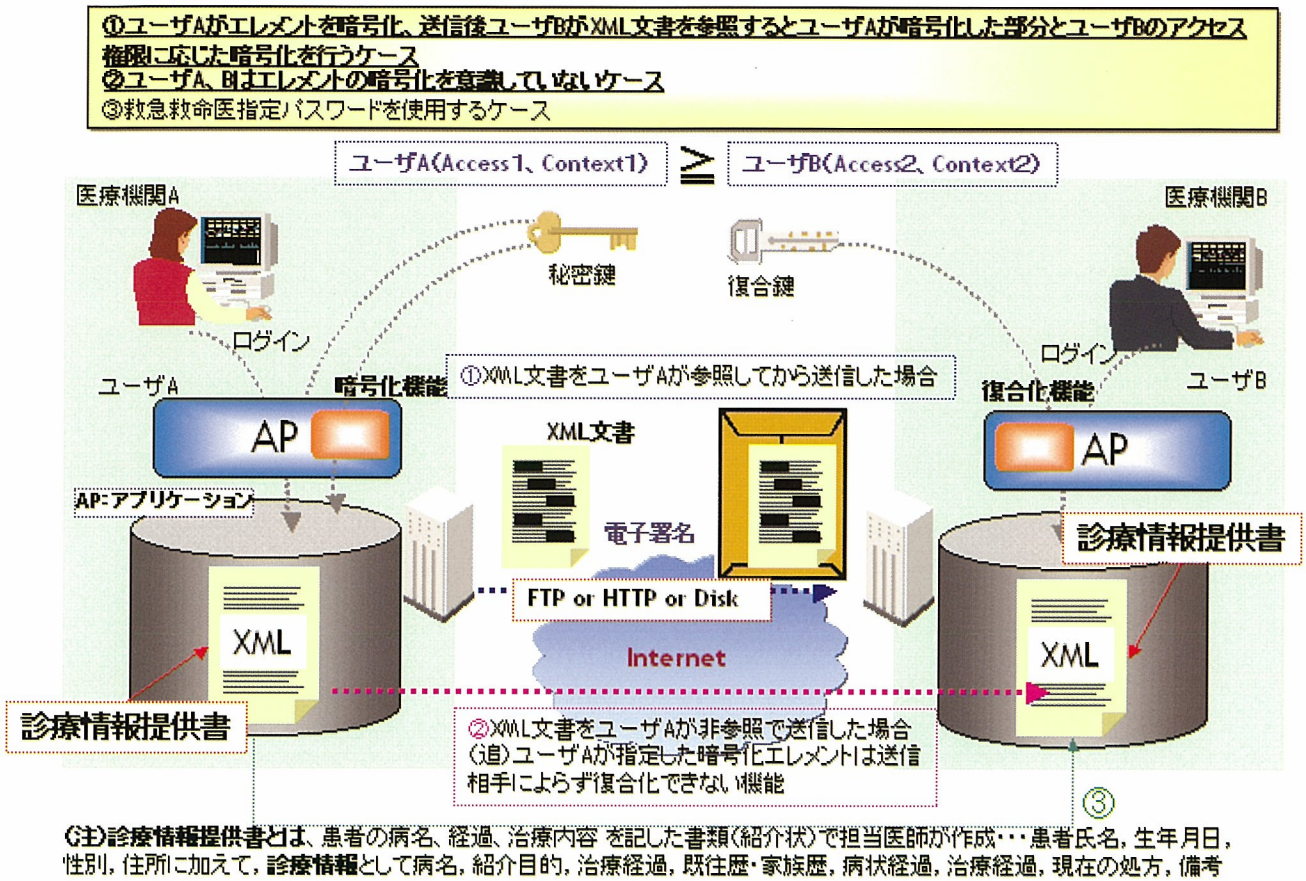

図１　地域医療連携における暗号化 XML 文書の交換様式

Ⅱ．分担研究報告

第２章　アクセス制御を中心とするセキュリティ技術状況調査

本多 正幸・中山 良幸・梁瀬 和夫

第2章　アクセス制御を中心とするセキュリティ技術状況調査

研究要旨

A. 研究目的

本研究では、医療機関における地域情報連携を「安全・安心」なものとして確立するための技術選択を目的として、主にXMLセキュリティ技術に関して調査を実施した。

本調査の特徴の1つは、単にセキュリティー技術を検討するのではなく、システムの運用管理方法の検討に重点をおきながら、これらの問題に対する解決方法を探ることを目的としている点にある。情報システム運用は、そのシステムの構成や用いる技術と密接な関係があり、運用面の検討とあわせて、セキュリティ管理のコスト（主に人的コスト）が低くなるようなシステム構成を検討する必要がある。また医療機関では、診療文書交換が重要な役割をはたすと考えられるため、本研究では公開鍵暗号方式を用いてデータベースに本人確認や改ざん検出といった機能を提供するPKIに対応可能なデータベースについて検討を加えることにする。具体的には、XMLセキュリティやネイティブXMLデータベースといった技術に着目し、これらを融合することでデータベースにおけるPKI技術の有効性について評価・検討を行う。

B. 調査内容

B-1.調査目的

医療情報連携において有効と考えられるデータベース／セキュリティ技術を広範に調査するとともにXMLデータベース、PKI技術適応上の課題・問題点の抽出を実施する。

B-2.調査方法

以下の調査方法・キーワードでヒットしたWebサイト、pdfファイル等のドキュメントを入手し、整理することで実施した。

① 検索エンジン：Google

② 検索キーワード：「セキュリティ」、「PKI」、「公開鍵・共通鍵」、「セキュリティ」、「XMLデータベース」、「アクセス制御」、「暗号化」、「エレメント」

C. 調査結果及び考察

C-1.XMLセキュリティ技術

（1）XMLにおけるセキュリティ技術

XMLベースのプロトコルを基盤とする電子商取引や電子申請の普及に伴い、情報交換におけるセキュリティのリスク管理は、企業にとって重要な問題となっている。XMLセキュリティは、Webサービスのセキュリティフレームワークとして、W3C（World Wide Web Consortium）とOASIS（Organization for the Advancement of Structured Information Standard）によって標準化が進められたものの（図2-1）、暗号化と並んで代表的かつ重要なセキュリティ技術であるアクセス制御についてはセキュリティモデルとして、必ずしも充分なものではない。

（2）XMLアクセス制御

XMLセキュリティは、Webサービスのセキュリティフレームワークとして、W3CとOASISによってSAML、XACMLの標準化が進められてきた。XACMLで規定されるアクセス制御は、リソース対象の指定に制約があり、XML問合せにおけるセキュリティモデルとして充分なものではない。これは、XACMLにおける対象リソースの指定において、XMLのノードやアクセスパスによる対象範囲の設定が難しいことに起因する。一方、XMLはデータベースと連携して、半構造データモデルとして柔軟なデータ管理を可能にした。データベースにおいて、アクセス制御はセキュリティ上の重要な機能要件であるが、複雑なデータモデルを持つXMLにおけるアクセス制御の実現は、RDBに比べ簡単ではない。ここでは、XACMLにおけるアクセス制御の概略と問題点について述べ、比較として、RDB及びXML DBにおけるセキュリティを図2-2に示す。

Fanら(2004)によりXML文書問合せに対するセキュリティモデルとして、セキュリティビューに基づくセキュアXMLクエリが研究されている。XMLセキュリティビューは、柔軟なアクセス制御ポリシーの設定と、導出されたセキュリティビューによる効率的なアクセス制御が特長である。セキュリティビューによるアクセス制御では、スキーマレベルのアクセスポリシー定義とXML文書スキーマから導出するセキュリティビューによってアクセス制御を実現しており、ユーザはXML文書またはXMLデータベースへの同時アクセスが可能であり、データアクセス時にセキュリティポリシーに記載されたアクセス権限に応じたアクセス制御が施行される（図2-3）。

（3）XACMLにおけるアクセス制御の問題点

XMLセキュリティの規格として、XMLデジタル署名やXML暗号、鍵管理のXKMS、及びOASISによるWebサービスの相互運用に関連した認証管理に関するSAML、アクセス制御に関するXACMLの規定がある。ここでは、Webサービスの相互運用におけるアクセス制御に対するセキュリティモデルを規定したXACMLについての概略と、XML文書問合せの観点から問題となるXACMLのリソース指定における規定について述べる。XACMLは、現在XACML1.0が標準であり、2004年12月にはXACML2.0がCommittee Draftと

なっている。

図 2-4 は、XACML におけるアクセス制御のデータフローを示している。XACML では、アクセス対象リソース（resource）のアクセス権限を定義するために、ポリシー記述言語が規定されており、また、リソースへの実行時の要求を表現するアクセス決定言語がある。リソースの保護ポリシーが検出された場合、リクエストの属性とポリシールール内の属性とを比較し、アクセス許可を決定する。リソース要求をクライアントからサーバに出す場合、アクセス制御を実施するエンティティを PEP（Policy Enforcement Point）と呼ぶ。PEP は、ポリシーを実行するために、要求側の属性を PIP（Policy Information Point）から取得して、PDP（Policy Decision Point）に認可決定を委託する。ポリシーストアに記述された適用可能なポリシーが PDP により評価され、認可決定が返される。PEP では、この情報を使用して適切な応答をクライアントに返すことができる。

図 2-5 は、XACML のポリシー記述言語の構造を示している。ポシリーは、対象（Target）、ルール（Rule）、責務（Obligation）の各要素から構成され、ルールには条件（Condition）を付加できる。複数のポリシーまたはポリシー集合を結合して一つのポリシー集合（PolicySet）を作る。主体（Subjects）は、要求コンテキストで示される主体の属性のルールを記述する。リソース（Resource）は、要求コンテキストが示すリソース属性に対して、ルールを適用する対象を限定し、アクセスの対象を指定する。動作（Action）は、要求コンテキストが示す動作属性に対して、ルールを適用するリソースへのアクセスに対する動作を指定する。SAML で定める Read、Write、Delete などの動作に加えて XACML では任意の動作も定義することができる。ここで XACML に特有な用語を整理しておく。

●PDP（Policy Decision Point）

定められたポリシーに従って PEP が示したアクセス要求が正しい権限を持つものかどうかを判断し、許可、不許可の決定を行うところ。SAML の PDP（ポリシー決定点）の定義と同じもの。

●PEP（Policy Enforcement Point）

アクセス要求者からの要求を受けて PDP に資源へのアクセス判断を問い、PDP の示す許可、不許可の決定に基づき資源へのアクセスの制御を実施するところ。SAML の PEP（ポリシー実行点）の定義と同じもの。

●PAP（Policy Administration Point）

PDP が参照するアクセス制御のルールを定義し、ポリシーやポリシー集合を生成するところ。

●PIP（Policy Information Point）

PEP の問合わせに対し、主体や資源や環境に関する属性値を提供するところ。SAML の属性オーソリティに相当する。

●Context

PEP と PDP 間で、認可要求と認可決定（応答）の正規化したプロトコルの構文。

●Target

ルールやポリシーで、評価すべき対象としての主体、資源、動作のルールを定めたもの。

●Condition

ルール内でTargetのルール以外にオプションとして指定する条件としての規則。

●Obligation

PDPが認可決定に当ってPEPに責務として実行を強制する指示。ポリシーで規定する。

XML宣言、文書型宣言とルート要素を含む記憶単位を文書実体と言うが、実体は整形式XML、テキスト、バイナリデータを保管することを目的にしている。実体には内部実体と外部実体の2種類があり、内部実体は文書実体内で全て定義される。外部実体は内容をＵＲＬ経由で見つかるソースから取り込んだものである。XACMLにおけるルール適用のリソースの限定は、資源識別子によるXMLデータの外部実体レベルに留まっているのが現状であり、リソースの内部実体レベルにおけるアクセス制御の対象範囲を内部構造に即して明示的に指定するには限界がある。アクセス制御の対象範囲を内部実体レベルまで拡張し、スキーマで規定されるXML文書の内部構造に即した整合性のある設定を可能にするのが、先に述べたセキュリティビューの利点の一つである。

（4）RDBのアクセス制御

標準SQLでは、セキュリティに関する規約として権限管理とロールが規定されている。権限は、データベースオブジェクトに対する特定のアクセス権限であり、ロールはいくつかの権限を纏めたものである。設定可能な権限としては、SQLのデータ定義、及びデータ操作（SELECT、INSERT、UPDATE、DELETE）に関するものであり、カラムや行単位におけるアクセス制御については規定されていない。

DBサーバのセキュリティモデルとしては、標準SQLで規定されている権限管理だけでは不十分であり、代表的な商用RDBであるOracle10gを含めた各種DBがどのようなセキュリティ機能を提供しているかを図2-6に整理した。

認証管理、通信データの暗号化はセッションや通信におけるセキュリティ管理であり、アクセス制御、データ暗号化、監査は、サーバ側のセキュリティ管理である。Oracleにおけるアクセス制御は、仮想プライベートDB（Virtual Pribate Database：VPD）と呼ばれ、オブジェクト権限による表単位でのアクセス制御に加え、行単位でのアクセス制御を可能にする。しかし、カラム単位でのアクセス制御は提供されていない。VPDは、SQL文を動的に変更するファイングレイン アクセスコントロールとユーザセッション情報を管理するアプリケーションコンテキストの二つの要素から構成され、アクセス制御ポリシーはメタデータとして管理される。

（5）XML DBのアクセス制御

XML データベースは、インターネットの普及と伴に Web 上の柔軟なデータ構造を扱う半構造データベースとして研究が進められてきた。現在 XML DB としては、XML データモデルに基づくネイティブ XML DB 以外に、階層型／オブジェクト指向の DB や RDB をベースとする XML DB があり、XML 対応 DB 製品も多数存在する。しかしながら、XML DB としてのセキュリティ機能に関しては、RDB と比較した場合、まだ充分とは言えないのが現状である。以下では、XML DB 製品の例として、Tamino、NeoCore と Oracle XML DB を取り上げる。

Tamino は、階層型 DBMS をベースにしたネイティブ XML DB の商用プロダクトであり、XPath、XQuery、XML Schema 等の規格をサポートしている。アクセス制御については、インスタンス単位でアクセス権限を設定することが可能であるが、内部データの属性あるいはインスタンス値と同期したアクセス制御の管理は階層構造に従う制約を受ける。

Oracle XML DB は、XML Schema、XPath 等をサポートする RDB 派生の XML DB である。セキュリティに関して、アクセス制御リストに関するサポートがあるが、これは WebDAV（Distributed Authoring and Versioning）の仕様に準拠した認証と操作にロールベースのアクセス制御を行うもので、XACML と同様に XML データ内部に対するアクセス権限まで制御するものではない。

次に述べる NeoCore のように、最初から XML をデータモデルとする XML DB では、RDB プロダクトで実現されているセキュリティフレームワークと同等の機能が充分に提供されていないのが現状である。これは、XML 文書が関係データベースのデータ構造に比べ、複雑で扱いにくいことに起因している。XML の自己記述的で複雑なデータ構造において、アクセス権限を管理することは、関係モデルに比べて複雑なものになる。XML DB においては、XML データ操作としての XQuery、XPath 等の規格が普及し始めた段階であり、セキュリティ機能については、まだ検討の段階にあるといえる（図 2-6）。

この分類に入る代表的な XML-DB としては NeoCore XML Management System(NeoCore XMS)がある。スキーマ定義をする際の言語として XML Schema をサポートしているものの、本来 DB に対してスキーマ定義が不要となっている。何も定義しなくても Well-formed な XML は格納できる。また、他の XML DB ではスキーマの定義が不要なものも存在し検索性能が非常に悪くなり実用上問題となるが、NeoCore XMS では自動的にすべてのタグにインデクスが張られるため常にハイパフォーマンスをキープできる。なお、このハイパフォーマンスを実現しているのが、DPP（Direct Print Protocol）という特許技術である。JavaAPI を利用してエレメントレベルでのアクセス制御が可能となっており、その他、XML エレメントへのアクセス制御と組み合わせることで、詳細な制御が可能になるものと考えられる。このようにネイティブ XMLDB では XML の構造を意識したアクセス制御の見直しのよさに利点がある。

(6) XML-DB と PKI 技術