様々な情報システムでXMLの導入が本格化してきており、XML-DBの利用も増えてきた。XML-DB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できると考えられるが、その具体的な方法や有効性についての検討はまだ十分ではなく、公開鍵暗号方式を利用してデータベースにセキュリティ機能を実装したPKI対応データベースの実装と評価・検討に関するものはほとんど報告がない。データを登録した本人を確認し、また第三者による改ざん検出を可能とするデータベースを構築し、その有効性を検討するためには、XML文書に対して署名・暗号化処理を行うXMLセキュリティと、XML文書を直接扱うことができるネイティブXMLデータベースを用いてシステムを構築すると、今後広い領域での適用が期待できる。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のに対して、データベースへの応用は多くない。また、広域の電子自治体間のデータ連携には、XMLデータベースへのPKI技術の導入は、必要不可欠であると考えられる。

これまでも述べてきたようにXMLセキュリティは、XML文書に対し署名や暗号化といった機能を提供する技術である（図2-7)。XMLに関する技術の多くは、World Wide Web Consortium（以下W3C）やOASISなどの団体から仕様が公開されているが、このXMLセキュリティもW3Cにて策定されたものである。

XML署名は、XMLドキュメントに対し、本人証明・完全性・否認防止といった機能を提供する技術である。W3Cからは"XML-Signature Syntax and Processing"と"Canonical XML"の二つを用いることを勧告している。またXML署名には、その形式によりDetached署名（署名対象となるXML文書とが別に署名要素を構築)、Enveloped署名（署名対象となるXML文書内に署名要素を含む)Enveloping署名(署名要素内部に署名対象となるXML文書を埋め込む）があり、アプリケーションの機能や用途により、それぞれ使い分けが行われている。

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ドキュメントの全体・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。これらの技術を利用したセキュリティ関連製品を図2-8に整理した。

(7) セキュリティポリシーについて

セキュリティ対策には、様々な技術が使われている。主なものとしては、ファイアウォ

ール、侵入検知予防システム（ＩＤＳ／ＩＰＳ）、検疫システム、フォレンジックツール（不正な処理や情報漏えいの証拠を掴む技術）、種々の認証技術などがある。これらの個々のシステムについては、選定や設計・構築を的確なものにするだけではなく、運用と、更新計画が的確なものとなるようにすることが肝心である。またセキュリティポリシー策定の際には、システム全体としてセキュリティを保つことができるようにしなければならない。このため、セキュリティ技術の導入とセキュリティポリシーおよびその実施手順は密接な関係にあるといえる。セキュリティ技術は、その技術的動向によって大きく変化を受けることがある。セキュリティポリシーは、セキュリティ技術の動向を見ながら適切に改訂していくことが必要である。

セキュリティを高めるためには、人的・機器面でのコストが必要になる。しかしながら、予算や人員を考慮するとセキュリティ対策の実施には、優先順位をつけざるを得ない。また、セキュリティと利便性、ユーザへのサービスは、トレードオフの関係になることが多い。不正アクセスや侵入が発生した場合には、システムの通信を遮断や、システムの停止を行う必要がある。その際、サービスの提供と、セキュリティの優先順位をはっきりさせておく必要がある。セキュリティ対策間の優先順位、サービスとセキュリティ対策間の優先順位を明確にしなければ、インシデントにも対応できないだけではなく、システム構成の整合性を保つこともできない。このような優先順位を明確にした上で、その優先順位を医師、医療機関職員、システム管理関係者に対して明確に示すことによって、システムの構築・運営方針を明確にすることが重要である。

セキュリティポリシーは、対象となる組織の資産評価、リスク評価、システム設計などをも反映する。システム設計は、セキュリティポリシーに則ってなされるべきであるが、現実のシステムでは、セキュリティポリシーよりもシステムが先に存在することが多い。また、セキュリティポリシーの実施手順は、システム構成やシステムの利用方法などによって適切に変更されるべきものである。そのため、システム構成を変更することで、セキュリティポリシーの実施手順がどのような影響を受けうるかの検討を加えることも必要がある。

セキュリティポリシーは、電子化された情報、システムなどを円滑かつ安全に運営するために不可欠である。しかしながら、セキュリティポリシーを的確に制定して運用まで含めて、監査に耐えるものにすることは容易ではない。以下に、セキュリティポリシーの制定及び実施に関する主な問題点を列記する。①~⑤は一般的、⑥は本研究で特に配慮するべき観点を示す。

①セキュリティポリシー実施手順の実現可能性の吟味が不足している。

②セキュリティポリシーの実施手順とシステム構成の関係や関連する技術についての検討が不足している。

③一度策定したセキュリティポリシーとその実施手順をどの様にして評価し、改善すべきかが明確にされていない。

④中長期的なシステム整備計画がセキュリティポリシーを十分反映していない。

⑤セキュリティ技術の発達・変化にセキュリティポリシーを対応させていく体制が十分ではない。

⑥現状のセキュリティポリシーの多くは、権限とシステムの単線的関わりを記述するが、医療分野では、公的権限と所属医療機関における権限、および患者との関係という視点を加えなければならない。

D. 結論

XMLセキュリティや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・検討を試みた。その結果、XMLデータベース、PKIを組み合わせて地域医療連携におけるセキュリティシステムを考案すると図2-9のように整理できる。即ち、XMLドキュメントのエレメント暗号化を施したうえで、医師等の医療情報へのアクセス制御が可能なものが望まれる。本章における調査結果を考慮すると参考情報としては図2-10に示したセキュリティ技術が考えられるが、以降の章ではより具体的にXMLエレメント暗号化プログラム、医療データ送受信プログラムのプロトタイプを設計・製作し、実用化に向けた課題の抽出を試みる。プロトタイプ（ツールソフト）の既存DB製品における位置付けを図2-11に整理した。

E. 研究発表

1. 論文発表

1) 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ー，医療情報学，2005（投稿中）

2. 学会発表

1) 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，2004；24(Suppl.)：1160-1161

F. 知的財産権の出願・登録状況

1. 特許取得

なし

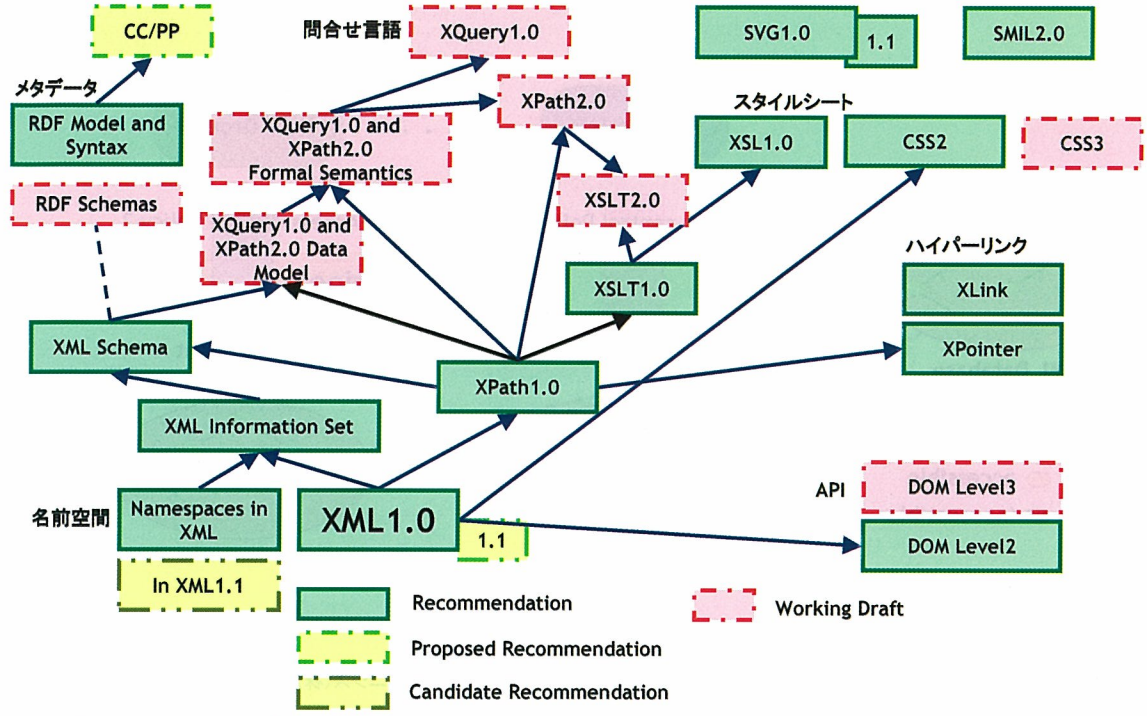
2. 実用新登

なし

3. その他

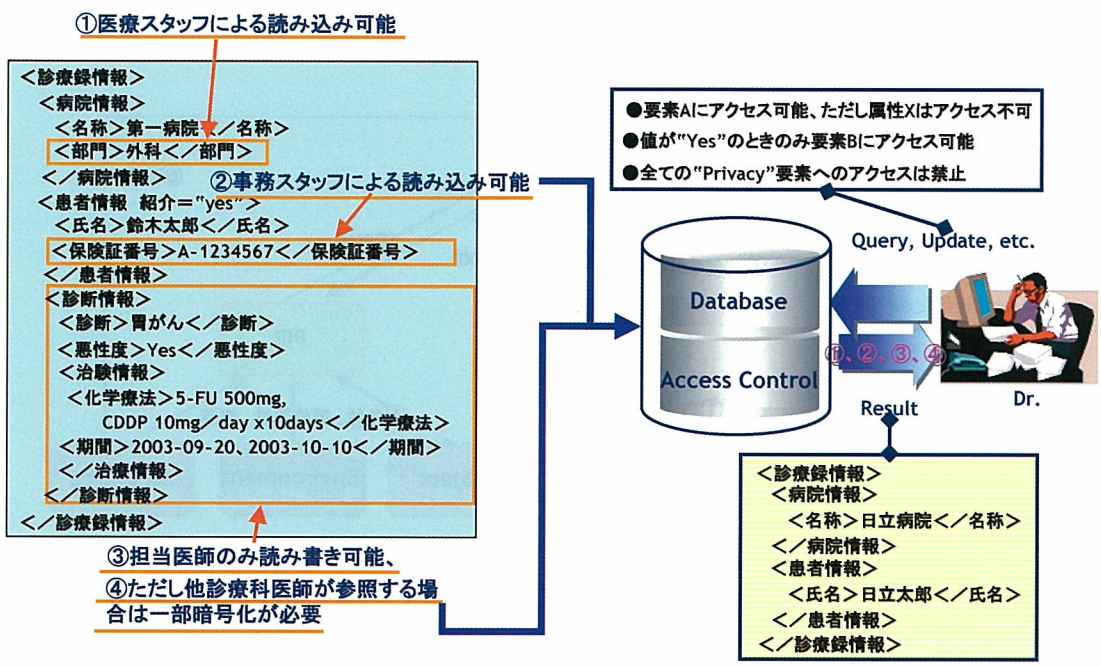
なし

図2-1 種々の標準，提案の関連



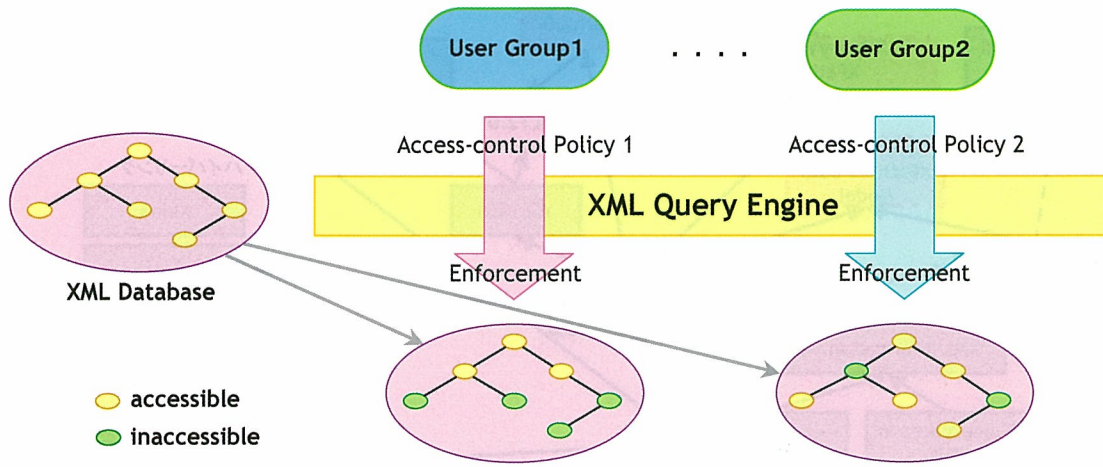
●参考：吉川 正俊．XMLとデータベース．http://www.astf.or.jp/astfinfo/mediaA/pdf/12-yoshikawa.pdf

図2-2 XMLデータベースに対するアクセス制御



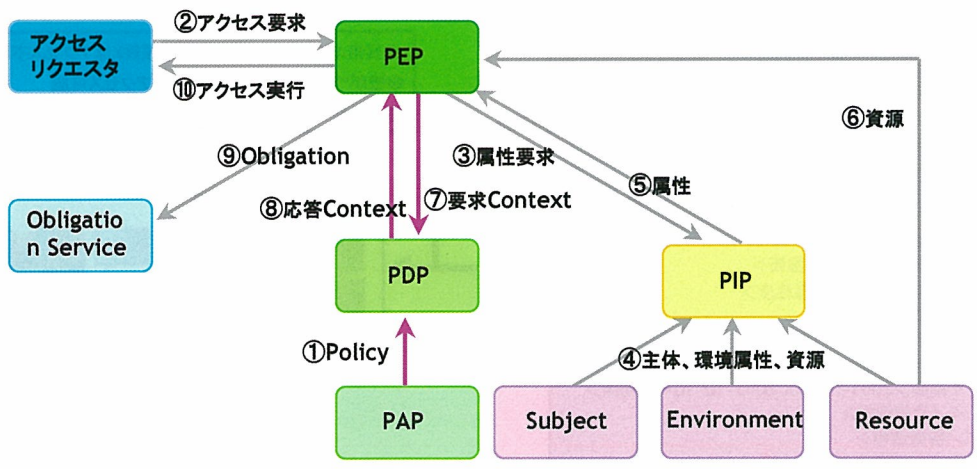
参考：工藤 道治．情報セキュリティ技術最前線"暗号とアクセス制御"
．http://www-06.ibm.com/jp/developerworks/evangelist/events/pdf/ed050120-02.pdf

図2-3 アクセス制御ポリシーの施行



参考：中山陽太郎,「セキュアXMLクエリ — セキュリティビューによるアクセス制御」, 日本ユニシス(株)技報 84号, pp.102-114, Feb. 2005

図2-4 アクセス制御のデータフロー・モデル(1)



参考：Webサービスのセキュリティ：http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html

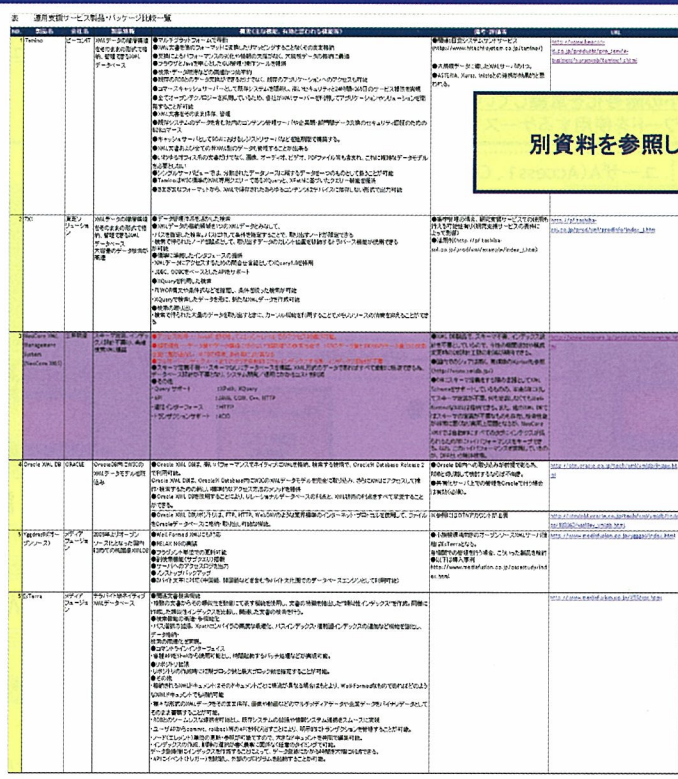
図2-5 XACMLポリシー言語構文とルールの対象<Target>の主体<Subjects>の構文例

```
<Policy  PolicyId="Policy1"
     RuleCombiningAlgId="Deny-override">          ← ルール結合アルゴリズムの指定
   <Target>                                       ← Target のSubject 、Resource、
      ／／ポリシの主体、資源、動作のルール・・・      Actionの規則
   </Target>
   <Rule  RuleID="Rule1"  Effect=Permit>
      < Target >                                  ← Rule1 : Target がマッチすれば
         <Subjects>                                 結果はPermit
            <Subject>  ・・・  </Subject>
         </Subjects>
         <Resources>                              ← Rule1 のTarget の規則
            <Resource>  ・・・  </Resource>
         </Resources>
         <Actions>
            <Action>  ・・・  </Action>
         </Actions>
      </Target>
      <Condition>  ・・・  </Condition>            ← Target 以外の規則があれば
   </Rule>                                          Conditionで記述
   <Rule  RuleID="Rule2"  Effect=Deny>
      <Target>                                    ← Rule2 : Target がマッチすれば
         ／／ルール主体、資源、動作・・・              結果はDeny
      </Target>
   </Rule>
   <Obligations>  ・・・  </Obligations>           ← 認可決定以外にPEPに強制する
</Policy>                                           責務（オプション）
```

```
<Subjects>
  <Subject>
    <SubjectMatch MatchId="function:string-match">          ← 評価関数の指定
      <SubjectAttributeDesignator
          AttributeId="identifier:subject:role"             ← 属性の指定
          />
      <AttributeValue>administrator</AttributeValue>        ← このルールで認める属
    </SubjectMatch>                                           性の値
  </Subject>
</Subjects>
```

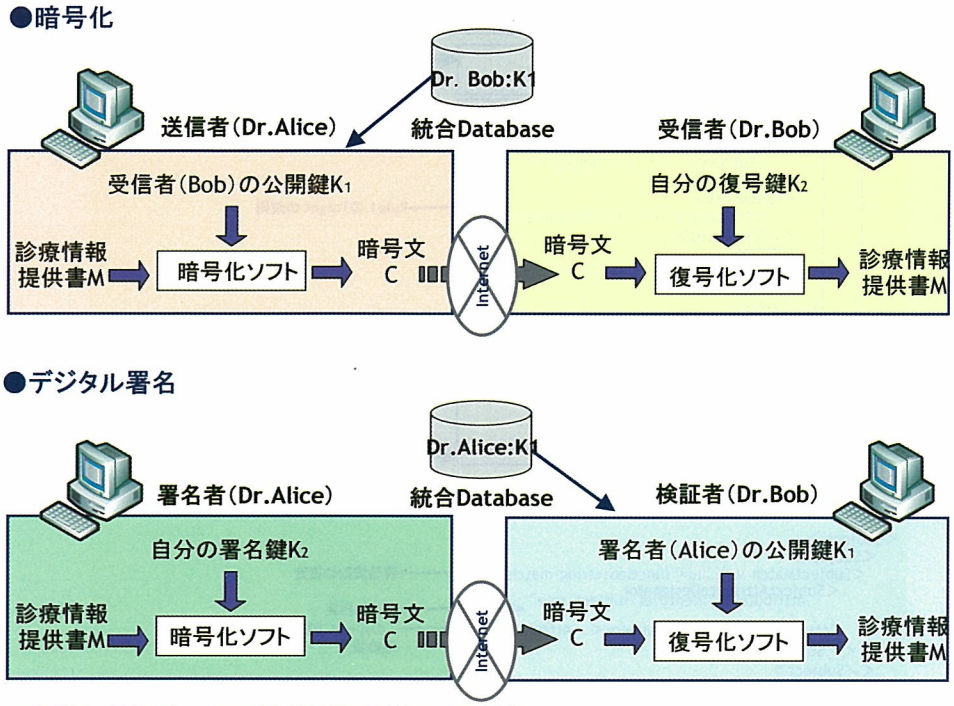
参考：Webサービスのセキュリティ：http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html

図2-6 XMLデータベース比較



別資料を参照してください

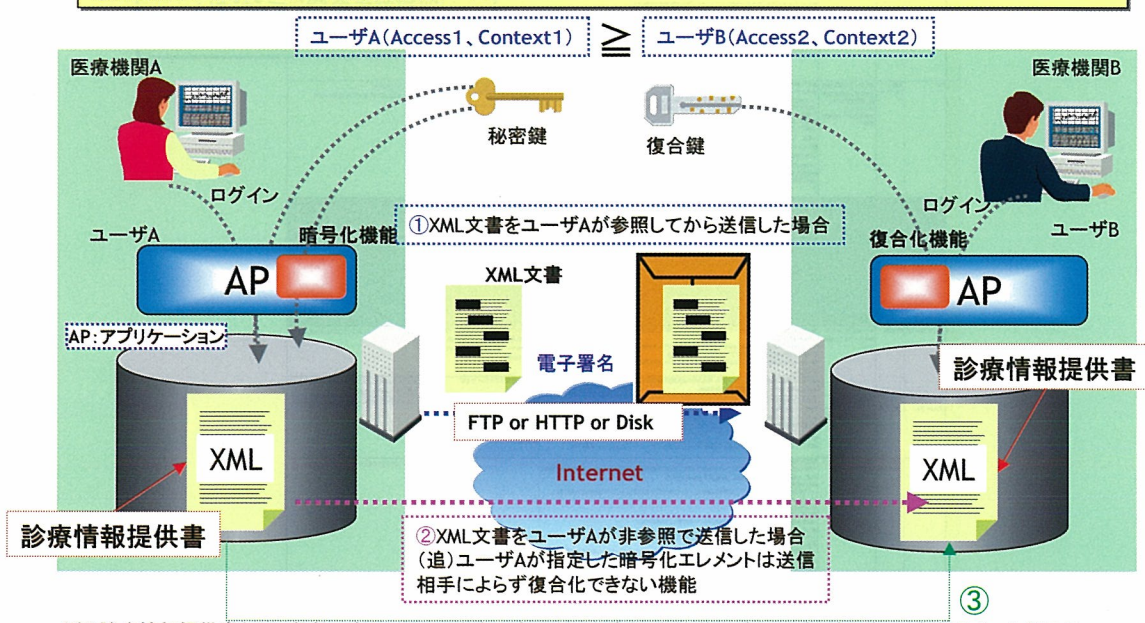
図2-7　公開鍵暗号機能



参考：工藤 道治．情報セキュリティ技術最前線"暗号とアクセス制御"
．http://www-06.ibm.com/jp/developerworks/evangelist/events/pdf/ed050120-02.pdf

図2-8　地域医療連携における暗号化XML文書の交換様式

①ユーザAがエレメントを暗号化、送信後ユーザBがXML文書を参照するとユーザAが暗号化した部分とユーザBのアクセス権限に応じた暗号化を行うケース
②ユーザA、Bはエレメントの暗号化を意識していないケース
③救急救命医指定パスワードを使用するケース



(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2-9 地域医療連携セキュリティシステム構築のステップ

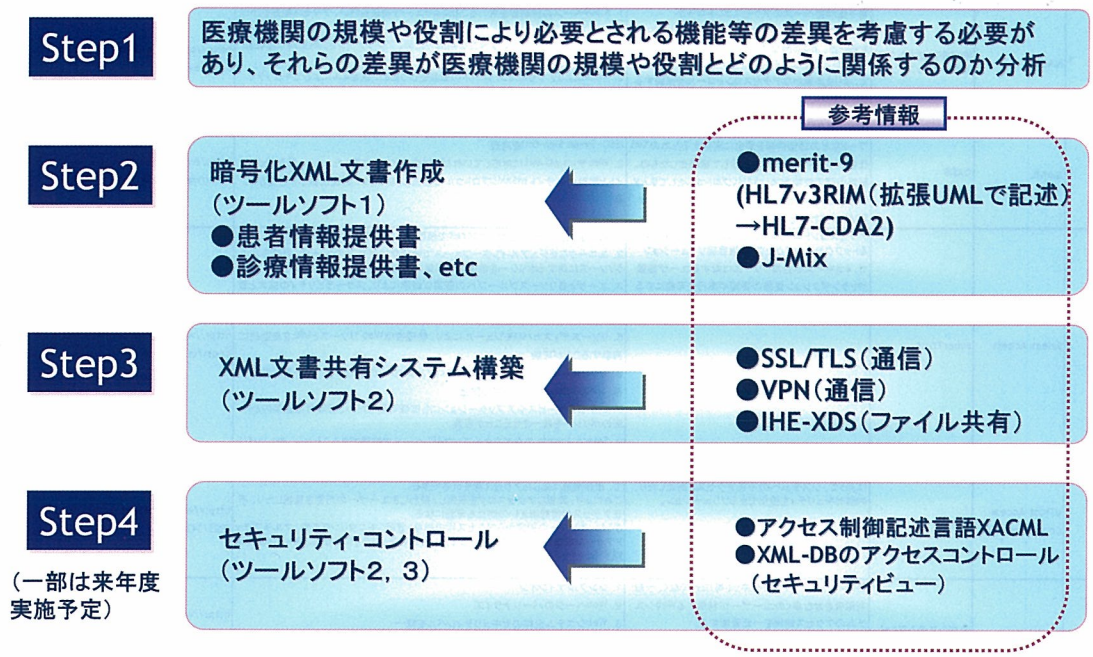


図2-10 データベース(DB)のセキュリティ機能比較

セキュリティ項目	RDB(Oracle)セキュリティ機能	XMLDBセキュリティ機能	厚労科研 セキュリティシステム (ツール開発)
認証管理	●Oracle Identity Management ●グローバル認証 ●外部認証 ●プロキシ認証 ●DB認証 ●OS認証	●XML署名(データ改ざん) ●WebDAVの仕様に準拠した認証(Oracle XML DB)	●ツールソフト2
通信データの暗号化	●Advanced Security ●パスワード暗号化		
アクセス制御 (個人情報以外に職種によりアクセス不能データが存在:臨床試験、請求、等)	●仮想プライベートDB	●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(Tamino) ●ロールベースのアクセス制御(Oracle XML DB)	●ツールソフト3 ●XACLM(XMLアクセスコントロール) ●セキュリティビュー (DTD+XPath修飾)
格納データの暗号化 (個人情報を対象)	●暗号化ツールキット		●ツールソフト1 ●XMLエレメント暗号化(ツールとして)
監査	●標準監査 ●DBA監査 ●ファイングレイン監査 ●イベントトリガー ●ログマイナー		●(ツールソフト3)

図2-11 セキュリティ技術（暗号化・アクセス制御）製品一覧

図　アクセス制御機能を実装した製品の一覧

No	名称	社名	内容	特徴	備考
1	NACS	株式会社日本システムディベロップメント	電子証明書ベースのアクセスコントロール Webアプリケーションに依存せず、その上位で動作するため、より強固なアクセスコントロールを実現することが可能な上、Webアプリケーションと連動して、よりきめ細かなアクセスコントロールを実現することも可能。	1. X.509ベースの証明書を用いることによりユーザ認証を行い、アクセス制限をかけることが可能 2. Webアプリケーションとは独立な構成のため、アプリケーション開発時に認証部分を意識する必要がない 3. NACSによりアクセスコントロールの設定を行うため、設定ミスによるセキュリティホールを防止 4. 複数のWebサーバを一元管理可能	http://solution.nsd.co.jp/products/nacs/index.html
2	SAML	OASIS	標準化団体OASISによって策定された、IDやパスワードなどの認証情報を安全に交換するためのXML仕様。AuthXMLとS2MLを統合して標準化したもの。認証情報の交換方法はSAMLプロトコルとしてまとめられており、メッセージの送受信にはHTTPもしくはSOAPが使われる。	1. 一度の認証で複数のWebサイトやサービスが利用できるシングルサインオン(SSO；Single Sign-On)を実現 2. WebサイトがSAMLに対応していれば、別のサイトへ移動したときに、移動元のサイトと移動先のサイトがSAMLプロトコルで通信し、自動的に認証情報が引き継がれる	http://www.atmarkit.co.jp/fsecurity/rensai/webserv04/webserv01.html
3	Select Access	SyberTrust	アクセスコントロールやシングルサインオンを提供するトップクラスのアクセス 権限管理ソリューションで、eコマースや企業リソースに対するユーザ権限やトランザクション資格の管理や実行を可能にするプロダクト。	1. 第三者機関のテストラボMindcraftで検証された業界トップレベルの性能 2. ユニークなビジュアルインターフェースで管理者は何百万のユーザ、何百万というリソースに対するポリシーを敏速かつ簡単に定義し、管理することが可能 3. ユーザと各リソースグループへの豊富な継承により、スケーラビリティの拡大と管理時間の削減が可能 4. Webサービスに即対応できるXMLベースのアーキテクチャ 5. リソースディスカバリモジュールにより、管理者はWeb リソースとURLを自動的に列挙することが可能 6. Secure Audit Serverが、実行時のログとポリシーの管理ログに電子署名を付与、イベントのレコードを改ざん防止 7. いかなるサービスやアプリケーションにも拡張可能なため、管理者は企業内と外部のポリシーを統一させることが可能 8. Select Access の全てをオープンなAPI ベースで拡張できることから、新しいビジネスの要求事項をサポートすることが可能	http://www.cybertrust.ne.jp/select_access/index.html
4	eTrust Access Controll r8.0 SP1	日本CA	職務や役割に基づく適切なアクセス権の付与と管理によって、システムへの不正アクセスを防止したり、内部セキュリティを強化できるソリューション。	サーバ上のリソース（ファイル、プログラム、ポートなど）に対してポリシーを設定して、職務権限に応じたアクセス権を付与できる。 これにより、詳細なアクセスログを収集し、疑わしきユーザーの行動を監視したり、不正アクセスや情報漏えいの防止も可能になる。 さらに、ポリシーの設定からアクセス権の付与・管理、モニタリングまで、マルチプラットフォーム環境で一元管理ができるため、内部セキュリティにかかるコストと作業も軽減する。	http://www.rbbtoday.com/news/20060925/34287.html
5	SiteMinder	日立システムアンドサービス	社内ネットワーク(イントラネット等)だけでなく、一般利用者を含む多くのユーザーが利用するWebシステムのアクセス制御を一元管理する。	1. シングルサインオン 2. Webページのパーソナライズ 3. Webシステム全体のセキュリティレベルを統一 4. リソースの一元管理 5. 容易なポリシー管理の権限委譲 6. 急激なサーバーにかかる負荷に対応 7. 多くのインフラストラクチャに対応	http://www.hitachi-system.co.jp/siteminder/sp/siteminder/merit/index.html
6	InfoUnity MONO	イーズ・コミュニケーションズ株式会社	アクセス管理機能を備えた分散データアクセス・ソフトウェア。社内に蓄積されている貴重な情報資産の安全で効率的な運用を実現	1. Security－データベースへのアクセスを集中管理しログとして記録 2. Accessibility－データベースの違いを意識せずひとつのDBとして利用可能 3. Usability－誰にでも簡単・自由なデータ利用を促	http://www.i-ze.com/main/product_l_outline.html

参考文献

1. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati, "A Fine-Grained Access Control System for XML Documents", ACM Transactions on Information and System Security, Volume 5, pp.169-202, May 2002

2. 林　隆志．セキュリティポリシーの策定・実施・改善に関する社会工学的研究．http://research.nii.ac.jp/kaken-johogaku/reports/H17_A06/A06-15.pdf

3. 工藤 道治．情報セキュリティ技術最前線"暗号とアクセス制御".
http://www-06.ibm.com/jp/developerworks/evangelist/events/pdf/ed050120-02.pdf

4. 中山陽太郎,「セキュアXMLクエリ — セキュリティビューによるアクセス制御」, 日本ユニシス（株）技報 84号, pp.102-114, Feb. 2005

5. 鈴木　優一．Webサービスのセキュリティ 第5回 PKIとPMIを融合させる次世代言語XACML.
http://www.atmarkit.co.jp/fsecurity/rensai/webserv05/webserv01.html

6. W.Fan, C.Chan, and M.Garofalakis, "Secure XML Querying with Security Views ", ACM SIGMOD, 2004.

7. 吉川 正俊．XMLとデータベース．http://www.astf.or.jp/astfinfo/mediaA/pdf/12-yoshikawa.pdf

図2-6　アクセス制御機能を実装した製品の一覧

No	名称	社名	内容	特徴	備考
1	NACS	株式会社日本システムディベロップメント	電子証明書ベースのアクセスコントロール Webアプリケーションに依存せず、その上位で動作するため、より強固なアクセスコントロールを実現することが可能な上、Webアプリケーションと連動して、よりきめ細かなアクセスコントロールを実現することも可能。	1. X.509ベースの証明書を用いることによりユーザ認証を行い、アクセス制限をかけることが可能 2. Webアプリケーションとは独立な構成のため、アプリケーション開発時に認証部分を意識する必要がない 3. NACSによりアクセスコントロールの設定を行うため、設定ミスによるセキュリティホールを防止 4. 複数のWebサーバを一元管理可能	http://solution.nsd.co.jp/products/nacs/index.html
2	SAML	OASIS	標準化団体OASISによって策定された、IDやパスワードなどの認証情報を安全に交換するためのXML仕様。AuthXMLとS2MLを統合して標準化したもの。認証情報の交換方法はSAMLプロトコルとしてまとめられており、メッセージの送受信にはHTTPもしくはSOAPが使われる	1. 一度の認証で複数のWebサイトやサービスが利用できるシングルサインオン(SSO:Single Sign-On)を実現 2. WebサイトがSAMLに対応していれば、別のサイトへ移動したときに、移動元のサイトと移動先のサイトがSAMLプロトコルで通信し、自動的に認証情報が引き継がれる	http://www.atmarkit.co.jp/fsecurity/rensai/webserv04/webserv01.html
3	Select Access	SyberTrust	アクセスコントロールやシングルサインオンを提供するトップクラスのアクセス 権限管理ソリューションで、eコマースや企業リソースに対するユーザ権限やトランザクション資格の管理や実行を可能にするプロダクト。	1. 第三者機関のテストラボMindcraftで検証された業界トップレベルの性能 2. ユニークなビジュアルインターフェースで管理者は何百万のユーザ、何百万というリソースに対するポリシーを敏速かつ簡単に定義し、管理することが可能 3. ユーザと各リソースグループへの豊富な継承により、スケーラビリティの拡大と管理時間の削減が可能 4. Webサービスに即対応できるXMLベースのアーキテクチャ 5. リソースディスカバリモジュールにより、管理者はWeb リソースとURLを自動的に列挙することが可能 6. Secure Audit Serverが、実行時のログとポリシーの管理ログに電子署名を付与、イベントのレコードを改ざん防止 7. いかなるサービスやアプリケーションにも拡張可能なため、管理者は企業内と外部のポリシーを統一させることが可能 8. Select Access の全てをオープンなAPI ベースで拡張できることから、新しいビジネスの要求事項をサポートすることが可能	http://www.cybertrust.ne.jp/select_access/index.html
4	eTrust Access Controll r8.0 SP1	日本CA	職務や役割に基づく適切なアクセス権の付与と管理によって、システムへの不正アクセスを防止したり、内部セキュリティを強化できるソリューション。	サーバ上のリソース(ファイル、プログラム、ポートなど)に対してポリシーを設定して、職務権限に応じたアクセス権を付与できる。 これにより、詳細なアクセスログを収集し、疑わしきユーザーの行動を監視したり、不正アクセスや情報漏えいの防止も可能になる。 さらに、ポリシーの設定からアクセス権の付与・管理、モニタリングまで、マルチプラットフォーム環境で一元管理ができるため、内部セキュリティにかかるコストと作業も軽減する。	http://www.rbbtoday.com/news/20060925/34287.html
5	SiteMinder	日立システムアンドサービス	社内ネットワーク(イントラネット等)だけでなく、一般利用者を含む多くのユーザーが利用するWebシステムのアクセス制御を一元管理する。	1. シングルサインオン 2. Webページのパーソナライズ 3. Webシステム全体のセキュリティレベルを統一 4. リソースの一元管理 5. 容易なポリシー管理の権限委譲 6. 急激なサーバーにかかる負荷に対応 7. 多くのインフラストラクチャに対応	http://www.hitachi-system.co.jp/siteminder/sp/siteminder/merit/index.html
6	InfoUnity MONO	イーズ・コミュニケーションズ株式会社	アクセス管理機能を備えた分散データアクセス・ソフトウェア。社内に蓄積されている貴重な情報資産の安全で効率的な運用を実現	1. Securityーデータベースへのアクセスを集中管理しログとして記録 2. Accessibilityーデータベースの違いを意識せずひとつのDBとして利用可能 3. Usabilityー誰にでも簡単・自由なデータ利用を促	http://www.i-ze.com/main/product_i_outline.html

第３章　暗号化対応ＸＭＬスキーマの検討

本多 正幸・中山 良幸・梁瀬 和夫

第３章　暗号化対応ＸＭＬスキーマの検討（担当：ケービーソフト、日立）

研究要旨

本研究では医療情報を記述する汎用 XML スキーマ開発の一環として暗号化 XML スキーマを設計・作成するとともにその適用性について評価した。筆者らは医療機関を大学病院タイプ、診療所タイプ、独立行政法人タイプの各タイプに分類して、医療情報の差異について検討しているが、今回は大学病院タイプの医療情報（診療情報提供書）を XML で記述した（XML ドキュメント）。サンプルデータをもとに作成した XML ドキュメントは J-MIX データ項目セットで設計された XML スキーマへマッピング後、個人情報に相当するエレメントを暗号化した。これらの結果より大学病院タイプの暗号化 XML スキーマを提案するとともにエレメントの暗号化処理時間等を指標に今後の課題について言及した。

A. 研究目的

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。一例として、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きた。しかしながら、それらのシステムは日本全国への発展を模索しながらも、その進展には問題があるように思われる。これまでの方法では、地域医療連携システムに参加する医療機関は個別に当該地域医療連携における共通データベース（DB）への変換プログラム作成が必要であり、そのためにかなりの労力や経費がかかっていたと推察され、よって新規参入機関へのハードルも高いことが問題であった。その大きな理由の一つには、複数の医療機関が共有する DB を構築する場合、あらかじ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った点にあると思われる。

XML で医療情報を記述しようとする試みとしては、平成７年に報告された医療情報 DTD である MML 規格を挙げることができる。そこで採用されたドキュメント形式は SGML である。MML 規格とは診療情報交換ためのデータ形式であり、診療録２号用紙形式に基づいて、患者 ID 情報、既往歴、病名、所見等を記述するための形式が定められている。MML は時系列でみた患者情報の流れや、診断病名などとの関係を記述する場合には適している。しかしながら広範囲な患者情報をカバーするためには、エレメントを膨大な種類用意し、メンテナンスする必要があり現実的でない、ドキュメントとして記述できる文字データ以外のもの(画像データなど)も多く含ませる可能性があるため扱いが難しい、等の課題が指摘されていた。

検体検査結果の記述方式である HL7 や DICOM 形式の画像ファイルを、前述の MML と関連づけて格納する方針を定めたものが MERIT-9 である。MERIT-9 は、利用形態での組

み合わせ・利用方式及び詳細項目の記述形式に関する項目を規定するものであり、ドキュメント定義には XML スキーマを用いている。またデータ項目については、J-MIX を基盤として追加されているものの、標準化や整理がなされていないという MML と同様の課題が残されている。

一方、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。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。本章では「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ＸＭＬスキーマの自動変換を実施するとともに任意の XML エレメント暗号化が可能な XML スキーマ（プロトタイプ）の設計・構築を行うものである。

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使用した。

●OS：Microsoft Windows 2000 Service Pack4

●ハードウェア：HITACHI FLORA 310 シリーズクラス

●メモリ容量：256MB

また、XML ドキュメントの取り扱いには XML 統合開発環境である Altova XML Suite 2004 Enterprise Edition(Altova 社製)を使用した。本製品に含まれるサブプログラムは概ね以下の機能を有している。

●xmlspy 2004 Enterprise Edition：スキーマのモデリング、XML の編集・デバッグ、XSLT 変換などを実施する際に使用した。また、多数のプログラミング言語の実行コードを生成する機能を利用して、主にマッピング後の XML ドキュメント作成のための XSLT コードを作成可能である。

●mapforce 2004 リリース 4 Enterprise Edition：XML、データベース、CSV、EDI を GUI 上でマッピングする際に使用した。

XML エレメントの暗号化には「IBM XML Security Suite for Java（XSS4J）」を利用した。XSS4J は完全な Java ライブラリであり、IBM の Web サイト alphaWorks からダウンロードできる。前提パッケージ、ダウンロードサイトについては以下の Web サイトに詳しい情報がある。

●http://www.atmarkit.co.jp/fxml/tanpatsu/16xmlsecurity/xmlsecurity04.html

B-2.データ処理方法

(1) 医療情報の入手

前述した「大学病院タイプ」の医療情報に必要なデータ項目の一例として、N 大学医学部付属病院の診療情報提供書を利用した（図 3-1)。

(2) 医療情報処理方法

医療情報の処理方法の概要を図 3-2 (1) (2) に示した。本研究では、通常、診療データ（診療情報提供書）は Excel ファイルで提供されるため、Excel 上で CSV ファイルに変換後、xmlspy にて XML ドキュメント化を実施した。

(3) 暗号化 XML スキーマの作成方法

電子保存された診療情報の交換のためのデータ項目セット(以下、単に J-MIX とする)の作成報告書に記載のある診療情報提供書を参考に患者基本情報、傷病名、経過記録に関係すると思われるデータ項目をエレメントとして採用し、XML スキーマを作成した。これを原型スタート XML スキーマと称する事とする。

XML 文書の部分的な暗号化である XML エレメント暗号を実現する手続きは次の通りである。本報告で使用した XML エレメント暗号化には SSL の利用、エレメント暗号、電子署名と正規化、XACML、XKMS といった技術のいくつかを実際に利用できるように作られたツール「IBM XML Security Suite for Java（XSS4J)」を利用した。この機能を利用するためには以下の前提パッケージが必要になる。実装には Java 言語を用いている。

- ●JDK 1.3 以上
- ●Java Cryptography Extension (JCE) 1.2.1
- ●Xerces2 Java Parser 2.0 とサンプル
- ●Xalan-Java 2.3
- ●International Components for Unicode for Java 2.0（ICU4J）

その他、XML にアクセスするための API （Application Programming Interface)として DOM（Document Object Model)、XML パーサとして Apache Xerces2 を利用している。

①暗号化処理手順

暗号化のプログラムの流れを図 3-3 に示す。暗号化を行う要素の選択と、要素全体か要素内容かの選択はユーザが指定することにした。暗号化には、公開鍵暗号アルゴリズムである RSA アルゴリズムを用いた。暗号化に用いる鍵は、暗号化が行われる前に生成し、指定したファイルに保存するか、鍵が保存されているファイルから読み込むことにより使用できるようにした。

②復号化処理手順

復号化は暗号化の手順のほぼ逆の手順で行う。本研究では復号化に用いる鍵は、暗号化

で使用した公開鍵を作成した際のプライベート鍵を使用した。

(3) XMLエレメントのマッピング方法

上記B-2(2)の手順で示したCSVファイルからのXMLドキュメントの作成手順は以下の通りである。

①xmlspy2004(Altova社製：以下、単にxmlspy)を利用して、CSVファイルからXMLドキュメントに変換する。

②mapforce2004(Altova社製:以下、単にmapforc)にて①で作成したXMLドキュメント(変換元)及び原型スタートXMLスキーマを読み込む。

③変換元のXMLドキュメント(①で作成)と変換先の原型スタートXMLスキーマ間での要素同士を相互に関連付ける（マッピング）操作により、XMLドキュメントのエレメント構造を任意の構造に変換するJavaプログラムまたはXSLTプログラムコードを自動生成させる。

④変換元のXMLドキュメント(①で作成)を、③で作成したJavaプログラムまたはXSLTプログラムコードで処理し、目的とするXMLドキュメントを作成する。このときはxmlspyを用いる。

尚、xmlspy、mapforce をサブプログラムとして含む詳細な Altova XML Suite 2004 Enterprise Edition(Altova社製)の操作方法は付属の操作マニュアルを参照した。

C. 研究結果及び考察

C-1.診療情報提供書中間ファイルの作成

B-2(2)項の方法に従い、N大学医学部付属病院「診療情報提供書」（図3-1）からCSVファイルを作成し、xmlspyにてXMLファイル形式に変換したものを図3-4に示した。また原型スタートXMLスキーマとXMLドキュメント(診療情報提供書)のマッピングの様子を図3-5に示した。

C-2.暗号化XMLスキーマの設計

各医療機関タイプにおいて、データ変換のためにXMLスキーマを適用し得る対象の1つに診療情報提供書がある。診療情報提供書については、統一された書式はなく、幾つか記載すべき項目が限定されているのみである。各項目毎には明確な規定が存在せず、項目の名称が暗黙に示す内容が記載されることが一般的である。また各項目には、文章構造についての規定はない。J-MIX の記載にあるように、診療情報提供書に該当する XML インスタンスは階層構造を持っている。トップレベルより1階層下の層では、診療情報提供書に

記載される項目をグループ化し、それらをセクションとして構成している。セクションの構成には、J-MIX 大分類が利用されている。セクションは下位のエレメントを包含するエレメントであり、セクションのエレメントには CDATA は含まれない。また、セクションは繰り返し（同一エレメント名のセクションが複数存在すること）がない。診療情報提供書の項目とセクションの関係は表 3-1 のようになっている。

各セクションで、対応する診療情報提供書のデータ項目をさらに分割してエレメントとしている。特に、医療機関、診療科等の組織、及び医師、患者等の個人については、データベースのフィールドとの交換が実現し易いように、細かくエレメントに分割している。以下、本研究で定義する各セクション中のエレメントの注意事項について、XML スキーマによる構文上の制約、あるいは対応する J-MIX データ項目の観点から述べる。

(1) HEADER セクション

①情報提供.目的区分、情報提供.目的

診療情報提供の目的が J-MIX 情報提供目的区分表（T0029）の中に該当する項目があるときには、情報提供.目的区分エレメントに該当する区分値を記述し、情報提供.目的エレメントには、J-MIX 情報提供目的区分表（T0029）の「内容」フィールドの文字列を記入する。J-MIX 情報提供目的区分表（T0029）に該当する項目がない場合は、情報提供.目的エレメントに語句として記述し、情報提供.目的区分エレメントは空エレメントとする。

②提供情報説明

診療情報提供の目的について文章による説明を記載する。例えば、フォローアップとしての診療情報提供(紹介)であれば、患者の希望によるものであるか等を記述する。一般的に、診療情報提供書の「紹介目的」欄などに記載されている文章を入れるエレメントとする。

(2) PATIENT-DATA セクション

実施記録は、検査等の実施によって得られた結果を記録する。今回、これらの検査データの形式が XML ドキュメントとして利用できる場合に限り、診療情報提供データの XML インスタンスに取込むものとする。

本研究では、前項までの結果より、N 大学医学部付属病院の診療録については患者基本情報、処方、経過記録に関する情報が中心であることから、基本的には J-MIX で提案されている診療情報提供書の XML インスタンス及び MERIT-9 等で検討されている XML スキーマの構造定義を利用することが最も効率的であると考えられる。これより、J-MIX を参考に原型スタート XML スキーマを作成し、J-MIX に該当するデータ項目がある場合は、エレメント名として J-MIX の日本語標準ラベルを採用した。データ項目とエレメントの間には 1 対 1 の関係が成立している。原型スタート XML スキーマを図 3-6 に記載した。

本研究では XML インスタンスを構成する単純エレメント及び属性に関しては、XML スキーマデータ型を適用している。J-MIX におけるデータ項目のデータ型が文法を持たない

文字列型を指定している場合においても、XML スキーマデータ型に適切なデータ型が存在する場合には、XML スキーマデータ型を採用することとした。J-MIX では複合データ型を採用していない。個々の各データ項目に対応する日本語標準ラベルが付けられているため、XML スキーマを複合データ型で構成することは出来ない。同様に MERIT-9 診療情報提供データも、XML スキーマデータ型の単純型より導出された新たな単純データ型を採用していない。また複合データ型も XML スキーマとしては定義されていない。しかしながら、実際には幾つかのエレメントの組をデータ型として扱うことができるようになっている。

(3) XML エレメントの暗号化

XML エレメントの暗号化には Altova XML suite、IBM XML Security Suite for Java（XSS4J）を利用している。図 3-5 に示した Altova Mapforce でマッピングの結果作成された XML エレメント変換のための Java プログラム、XML エレメントの暗号化に使用した XML Security Suite for Java API のコード変更箇所を各々図 3-7、8 に示した。

本研究ではこれらのプログラムを図 3-9 に示した CUI ベースの方法で動作確認を実施した。XML エレメントの暗号化の結果を図 3-10 に示す。これは個人情報保護法を念頭に「電話番号」を暗号化した例である。暗号化エレメントを表す最上位のエレメントが<EncryptedData>エレメントであり、その Type 属性に Element を指定する。その子エレメントが<CipherData>エレメント、さらにその子エレメントに<CipherValue>エレメントで、そのエレメントの内容が暗号化された値である。その他、Type 属性には Content を指定することも可能である。

C-3.暗号化 XML スキーマにおける暗号化・復号化処理時間評価

XML スキーマにおける暗号化エレメント数を変化させ、処理時間に与える影響を評価した。同時に CPU 負荷(%)、メモリ使用状況(MB)を計測し、ハードウェアとの関連性も検討した。エレメント数を 1~40(全エレメント)の場合における各々の値を表 3-2、3 に整理した。表 3-2、3 はアルゴリズムが各々RSA、Triple-DES で暗号化した場合である。処理時間を比較すると、エレメント数を 1~5 まではほとんど変化がない。RSA の場合、全エレメントである 40 エレメントを暗号化すると約 20%処理時間が増加することが解る。一方、Triple-DES の場合、増加の割合は 30~40%とやや大きい値を示している（図 3-11）。

Triple-DES は共通鍵であるにも関わらず、処理時間が公開鍵以上に必要になることが確認できた。DES はブルート・フォース・アタックに弱いことが報告されており、セキュリティの面を考慮しても公開鍵の利用が望ましいことが解る。

次に RSA の鍵長を 512、2048bit と変化させた場合の処理時間と CPU、メモリへの影響を測定した。計測値を整理したものを表 3-4～9 に示した。グラフ化したものを図 3-12～15 に示した。各鍵長において診療情報提供書（エレメント暗号化したもの）の暗号化、復号

化処理時間を比較評価したところ（図 3-16～21）、鍵長が 512bit の場合、暗号化処理時間に比較して復号化処理時間が短い。反対に、鍵長が 2024bit の場合、暗号化処理時間に比較して復号化処理時間が長くなる。一般に、RSA は一方向関数の考え方から復号化時間の方が長くなるものと考えられる。鍵長は不明であるが、横森（2001）による報告においても復号化処理時間が短くなることが示されている。鍵長と暗号化・復号化処理時間の関係については今後、詳細に検討して行きたいが、システム化する上で指摘鍵長が存在するものと考えられる。

C-4.XML ドキュメント暗号化・復号化プログラム(プロトタイプ)の開発

XML ドキュメントを読み込み、特定の要素全体（ルート要素も指定可）または要素内容を暗号化し、結果を別の XML ドキュメントとして生成する。また、暗号化された XML ドキュメントの復号化も行う Web ベースのプログラムのプロトタイプを開発した。本研究で使用するプロトタイプシステムの画面遷移を図 3-22 に示した。外部設計を図 3-23～27 に示した。以降、当該プログラムを「医療機関文書暗号化システム」と呼称することとする。

ユーザ ID、パスワードを入力しシステムにログインすると、top 画面が出現する。top 画面は３ペイン表示の構成になっている。ここで３ペインとは左側にフォルダ構成、右上に見出し、右下に内容という構成を指している。通常、XML ドキュメントは表示されていないが、左側ペインからドキュメントを選択し、上部ペインにある「表示」をクリックすると診療情報提供書が現れる。右上の見出しにある「タグ」をクリックすると XML ドキュメントとして表示され、「暗号化」をクリックすると表示項目左部にあるチェックボックスにチェックを入れた情報が「●」印で暗号化される。その他、ドキュメント保存、メール送信機能を有している。

D. 結論

本章では「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ＸＭＬスキーマの自動変換を実施するとともに任意の XML エレメント暗号化が可能な XML スキーマ（プロトタイプ）の設計・構築を行った。その結果、暗号化プログラムの動作確認を実施するとともに、Web（GUI）ベースでのプロトタイプ「医療機関文書暗号化システム」を作成し、次章で扱う診療情報提供書（XML 文書）をやり取りする医療機関間暗号化 XML 文書情報連携システムの基礎を提供することができた。

E. 研究発表

なし

F. 知的財産権の出願・登録状況

1. 特許取得

   なし

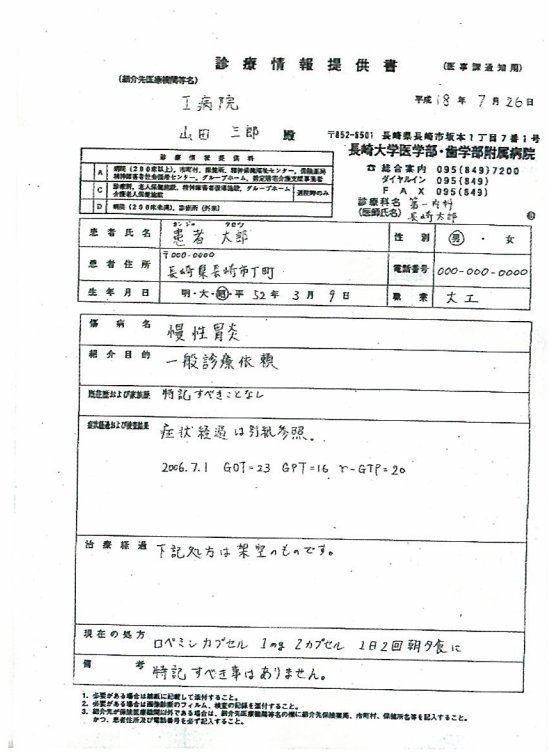
2. 実用新登

   なし

3. その他

   なし

図3-1　診療情報提供書の例



診療情報提供書　（医事課送付用）

（紹介先医療機関等名）
I病院　殿

平成18年7月26日

〒852-8501 長崎県長崎市坂本1丁目7番1号
長崎大学医学部・歯学部附属病院
総合案内 095(849)7200
ダイヤルイン 095(849)
FAX 095(849)
診療科名 第一内科
（紹介医氏名） 長崎太郎

患者氏名	患者 太郎（カンジャ タロウ）	性別	㊚・女
患者住所	〒000-0000 長崎県長崎市丁町	電話番号	000-000-0000
生年月日	明・大・㊧平 52年 3月 9日	職業	大工

傷病名	慢性胃炎
紹介目的	一般診療依頼
既往歴および家族歴	特記すべきことなし
症状経過および検査結果	症状経過は別紙参照。 2006.7.1 GOT=23 GPT=16 γ-GTP=20
治療経過	下記処方は某堂のものです。
現在の処方	ロペミンカプセル 1mg 2カプセル 1日2回朝夕食に
備考	特記すべき事はありません。

1. 必要がある場合は紹介状を添付すること。
2. 必要がある場合は画像診断のフィルム、検査の記録を添付すること。
3. 紹介先が保険医療機関以外である場合は、紹介先医療機関等名の横に紹介先保険薬局、市町村、保健所名等を記入すること。
4. 患者住所及び電話番号を必ず記入すること。

図3-2（1）　各医療機関診療データをXMLスキーマで処理する手順（1／2）