第３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

本多正幸・中山良幸・梁瀬和夫

第３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。

【研究概要】

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3-1）。

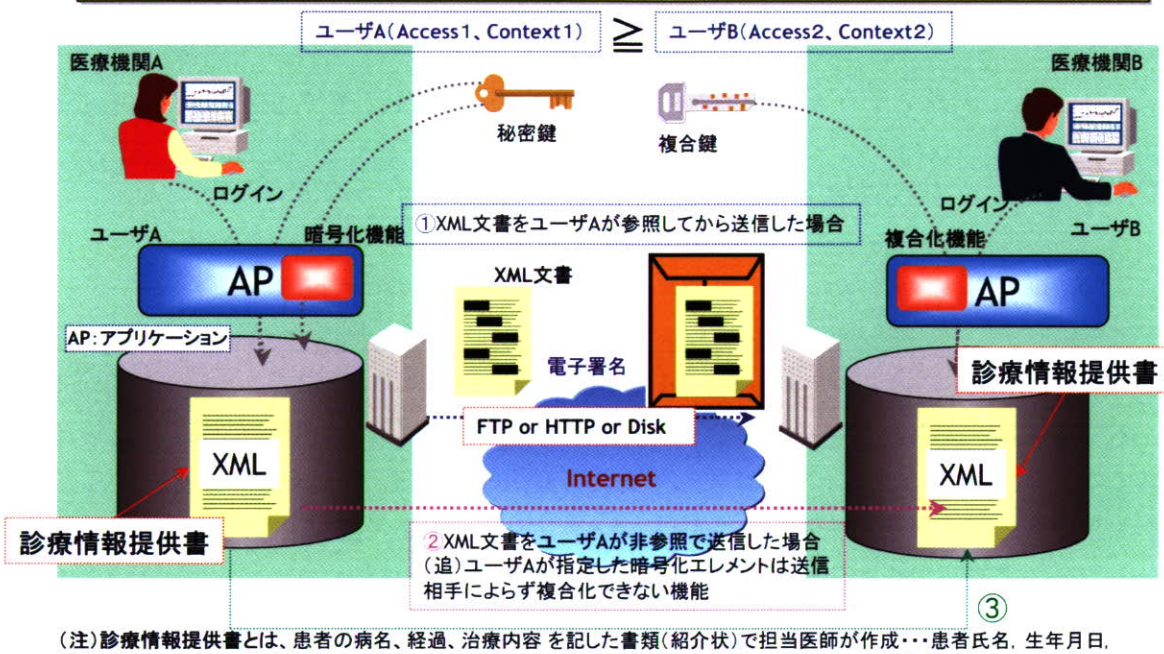
本研究で取り扱うWebサービスは、もともと仲介者を通した通信を仮定している。仲介者は IP ネットワークにおけるルータとは異なり透過的でない。即ち、データの内容に対して付加価値を加えることを許可している。このような状況で、エンドツーエンドのセキュリティを実現するためには、通信全体の一元的な保護ではなく、XMLセキュリティによるデータの選択的な保護（暗号化）が必要になる（図3-2）。

本章では「ＸＭＬセキュリティ機能付自動データ変換ツール」開発の次段階として任意の 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3-3,表3-1）。

主に任意の 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、次章システムテストに供するプログラムを作製し得た。診療情報提供書送受信システム運用設計の概要を図 3-4 に、そのシステム構成図を図 3-5 に示した。尚、詳細については平成 19 年度総括報告書を参照していただきたい。

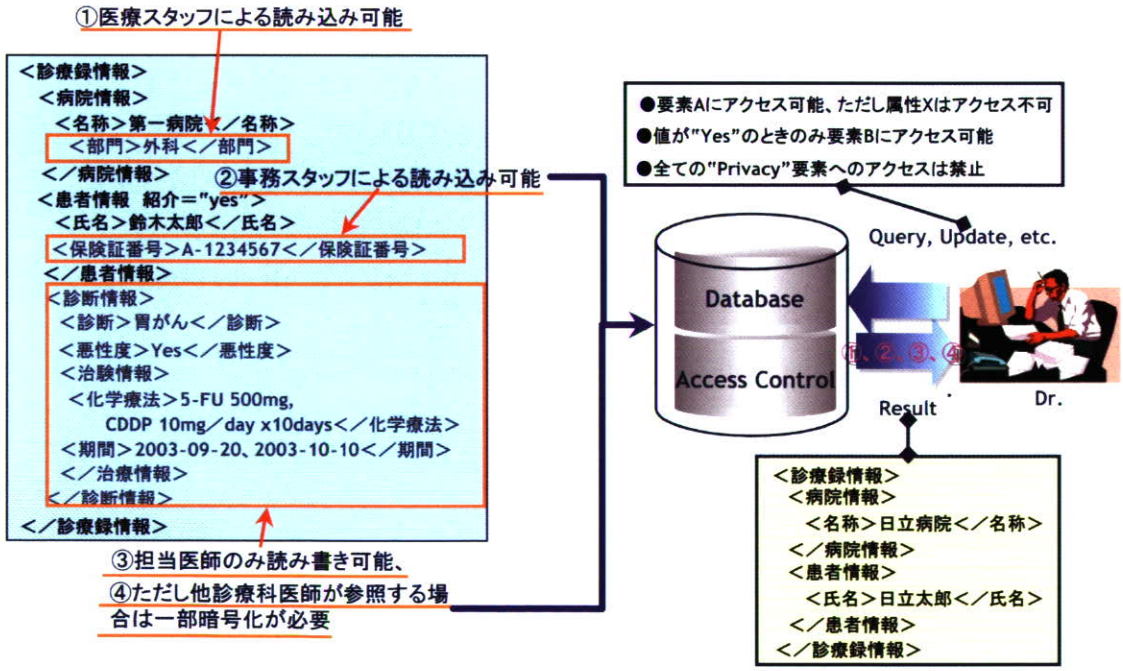
図3-1 地域医療連携における暗号化XML文書の交換様式

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3-2 データベース(DB)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3-3 地域医療連携セキュリティシステム構築のステップ

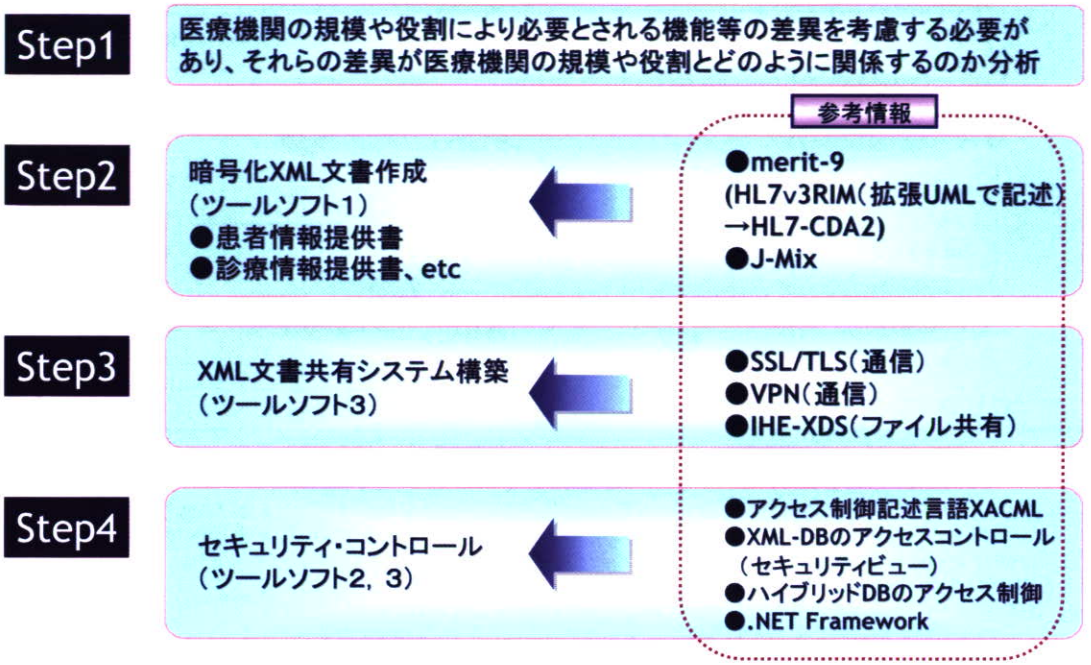
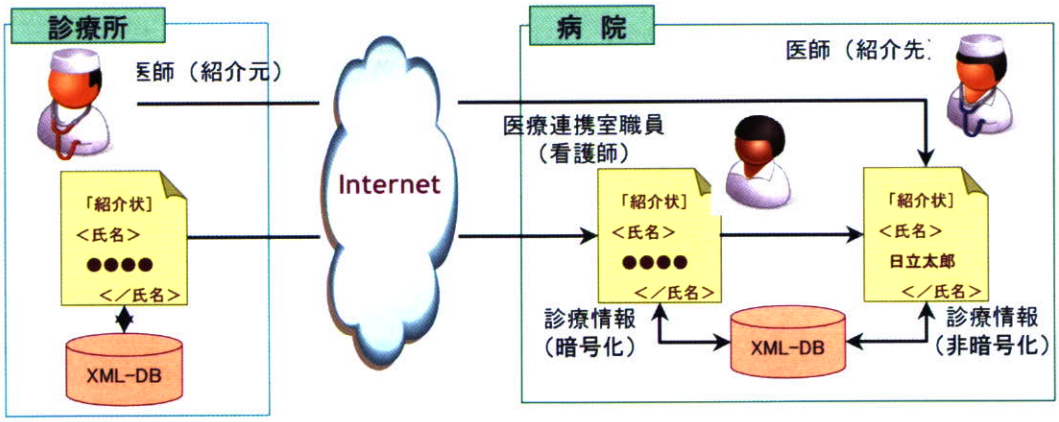


表3-1 データベース(DB)のセキュリティ機能比較

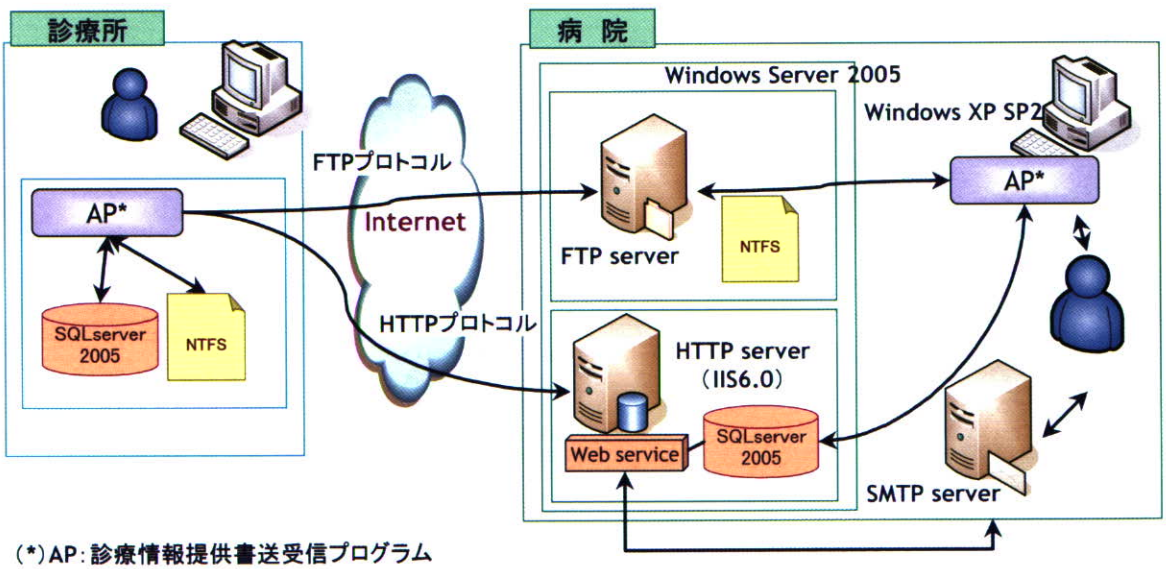
セキュリティ項目	RDB(Oracle)セキュリティ機能	XMLDBセキュリティ機能	厚労科研 セキュリティシステ (ツール開発)
認証管理	●Oracle Identity Management ●グローバル認証 ●外部認証 ●プロキシ認証 ●DB認証 ●OS認証	●XML署名(データ改ざん) ●WebDAVの仕様に準拠した認証(Oracle XML DB)	●ツールソフト2→PGPを利用して機能検証
通信データの暗号化	●Advanced Security ●パスワード暗号化		
アクセス制御 (個人情報以外に職種によりアクセス不能データが存在:臨床試験、請求、等)	●仮想プライベートDB	●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 →SQLserver2005を利用して実装 ●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→実装 ●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→検討中)

図3-4 診療情報提供書送受信システム運用設計の概要



(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。

図3-5 診療情報提供書送受信システムの構成図



(*)AP:診療情報提供書送受信プログラム

(1) 診療所で作成された診療情報提供書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提供書はFTPまたはHTTP(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上での通信も可能)。
(3) Webサービスでは診療所からの診療情報提供書を受信したとき、予め設定されたメールアドレスへ受信通知を送付する。
(4) 病院側の当該プログラムは、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保守(プログラム配信、他)の負担が軽減される。

第4章

Webサービスを利用したXMLセキュリティシステムの実用化研究

本多正幸・中山良幸・梁瀬和夫

第4章　Webサービスを利用したXMLセキュリティシステムの実用化研究

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

前年度に引き続き XML 文書の部分暗号化技術を利用し診療情報提供書をやり取りする医療機関間暗号化 XML 文書送受信システムを構築した。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、今後は、診療情報提供書入力インターフェースのブラウザ化、パッシブ・モードでの FTP 通信機能の追加等の改良が必要になることに言及した。

【研究概要】

本章では引き続き診療情報提供書（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を試作し（図 4-1）、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（表 4-1）、本システムの有効性を確認した。

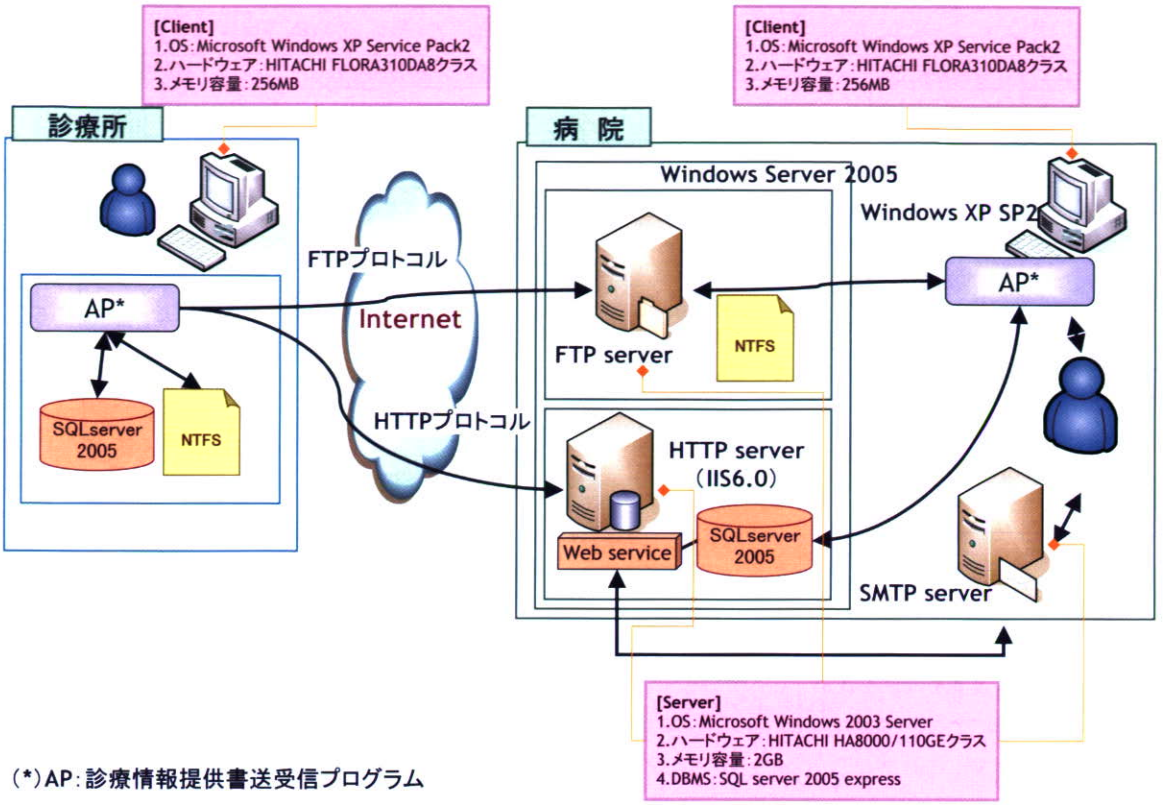
XML 文書をやり取りする診療情報提供書（XML 文書）送受信システムを試作し、職位によるエレメント暗号化、診療科によるアクセス制御機能の動作確認を行うとともに実環境を利用した送受信テストを実施した（図 4-2）。その結果、実装した各機能は問題なく動作することを確認した。今後は診療情報提供書入力インターフェースのブラウザ化、パッシブ・モードでの FTP 通信機能の追加等の改良が必要である。

質の高い地域医療を提供するために、医療の機能分化に伴って地域における情報の共有が必要となっている。われわれはそれを支援する手段としての地域医療用ネットワークシステムを長崎県下の病院で開発してきた。このようなシステムにおいてセキュリティの確保は最重要課題の 1 つである。

VPN で問題になるのは NAT トラバーサル（NAT : network address translation とは、インターネットで利用するグローバル IP アドレスと、LAN 内で使うプライベート IP アドレスを相互転換する機能のことであり、ここでは NAT 環境で LAN 内から VPN 通信を行うために必要な機能の意味）の実装に制約が多く、現実問題として VPN を利用できないユーザ（医師）が存在する

ことである。セキュリティを重視する場合には VPN ゲートウェイの背後にも別途ファイアウォールを配置し、再度アクセスをコントロールする必要性も出てくるが、運用面では実用的でないと考えられる。従って、実運用を考えると本研究で採用した部分暗号化による診療情報提供書の送受信が最もセキュリティが確保できるものと考えられる。

図4-1 システムテストの環境



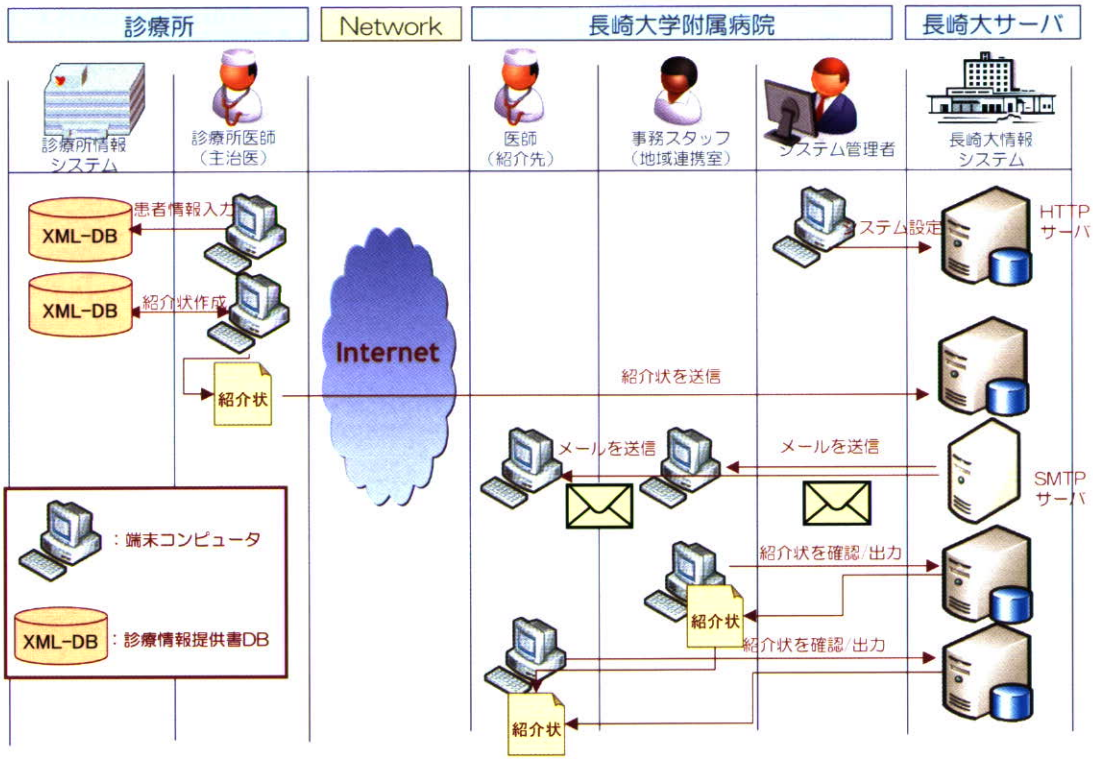
(*)AP:診療情報提供書送受信プログラム

表4-1 システムテスト考え方と実施項目

No.	項目	テスト方針	テスト項目及び内容
1	通常運用	(1)SMTPサーバからメールが送信されるか (2)送信された紹介状の内容に偏差がないか。 (3)各職位で正確に暗号化・復号化できるか。	(1)動作確認のみ (2)UNIXのdiffコマンド相当の内容でチェックする。 (3)職位の組み合わせを変化させ紹介状の内容に偏差がないことを確認する。
2		・紹介状を時間帯(朝、昼、夜)を変えて送信する	→動作確認のみ。各種テストは時間帯を可能な限り統一する。
3		・紹介状送信時にWeb閲覧が影響を受けるか	→紹介状送信時と非送信時で特定Webサイトの表示速度を計測する。CPU負荷(注3)を目安に負荷を変化させ、表示速度を計測する。
4	特異運用	・サーバ/クライアントの立上順序を変化させた場合、紹介状送信に影響はあるか	→動作確認のみ
5	性能	・紹介状を送信した場合のレスポンスはどのくらいか(暗号化項目を増減した場合)?	→暗号化項目数を変化させレスポンス(注1)を測定する。
6		・紹介状を送信し、SMTPサーバからメールが到着するまでのレスポンス・スループットはどのくらいか(送信数を増減した場合)?	→決められた時間(例えば1分間)での紹介状送信数を変化させ、レスポンス/スループット(注2)を測定する。
7		・紹介状送信時にクライアント、サーバで以下のリソースを計測する。Windows server 2003の管理ツール>パフォーマンスを利用する。 (1)CPU利用率 (2)回線利用率 (3)メモリ使用量	→項目3、5、6を測定する際に計測する。
8		・以下の紹介状送信手段の場合のレスポンス・スループットを計測する。評価基準は送信紹介状の数と暗号化項目の数とする。 (1)FTP (2)Webサービス	→項目3、5、6を測定する際に計測する。
9	既稼働業務/ネットワークへの影響	・暗号化データ項目数を変化させた(注4)ときの回線使用率への影響を計測する。回線使用率はWindows server 2003の管理ツール>パフォーマンスを利用する。	→項目3、5、6を測定する際に計測する。
10	高負荷テスト	・Webサービスでの紹介状送信ではFirewallの有無の影響を測定	→Firewall有り無しの場合に上記第8項を測定する。
11	性能	・セキュリティスキャンソフト(AntiVirus)起動の有無が紹介状通信に与える影響をみる	→AntiVirus起動の有り無しの場合に上記第8項を測定する。

(注1)レスポンス:ここでは入力画面で保存ボタンを押してから完了画面が返ってくるまでとする
(注2)スループット:ここでは決められた時間(例えば1分間)で送信可能な紹介状の数。J-Meterでのhttp、FTP送信の負荷(スレッド数)で調整する。
(注3)CPU負荷を目安に10%程度、50%程度、85%以上の3段階。
(注4)暗号化項目数は紹介状を①全く暗号化していないもの、②患者氏名から保険情報までを暗号化したもの、③全て暗号化したもの、の3段回に変化させることで設定する。

図4-2 XMLセキュリティシステム —診療情報提供書(紹介状)運用—



Ⅲ．研究成果の刊行に関する一覧表

研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
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
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
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
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
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
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
本多正幸 松本武浩 二之宮実知子 嶋瀬宏 半田正浩	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
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
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
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			2006