インを行う。ただし任意の文字列をユーザIDに入力し、Ctrl+Shift+Altを押下しながらログインすると、ユーザIDとパスワードを保持しているDBを使用せずにログインできる。ログイン後は設定画面より、前述のＤＢの接続文字列を設定する。

C-2-3. 診療情報提供書項目入力インターフェース

（1）診療情報入力インターフェース

図2-11に示した。

（2）暗号化／非暗号化

各入力項目の左にはチェックボックスがあり、「オン」にすると、対応する入力項目が守秘化される。守秘化項目が含まれているファイルを開いた場合、「オフ」することにより守秘解除される。ユーザの権限により暗号化／非暗号化の設定解除できない場合は、チェックボックスはグレーとなっている。

（3）保険情報関連項目

一人の患者に対し、複数の保険情報を追加することが出来るものとする。

C-2-4. 各種メニュー項目

診療情報提供書送信システムの各種メニューを表2-3に整理した。

C-2-5. XML表示

図2-4に診療情報提供書の入力例をXML表示させた例を図2-12示した。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-2-6. 暗号化／非暗号化表示設定インターフェース

キャプション付きコントロールの説明を表2-4に示した。

C-2-7. ファイル選択

クライアントPCからファイル操作をするための各機能ローカルファイル選択（NTFS）（図2-13、表2-5）、FTP（図2-14(1)・(2)、表2-6）、DB（図2-15(1)・(2)、表2-7(1)・(2)）、Webサービス（図2-16(1)・(2)、表2-8(1)・(2)）におけるインターフェースとキャプション付きコントロールの一覧を示した。

C-2-8. 設定インターフェース

httpプロキシ経由でWebサービスを利用する場合に設定するインターフェース及びキャプション付きコントロールの説明を（図2-17、表2-9）に示した。またユーザIDとパスワードが定義されているテーブルが含まれるアカウントDBへの接続文字列を指定するMyDBタブの設定画面とキャプション付きコントロールを（図2-18、表2-10）に示した。

C-3. ファイル仕様

C-3-1. クライアントPCファイル

クライアント PC に保存するファイルを次に示す。格納場所は以下の通り。
[格納場所]C:¥Documents and Settings¥<Windows ユーザ ID>¥Local Settings¥Application Data¥（株）日立製作所¥PROTMET¥<バージョン番号>

C-3-2. 設定ファイル
ファイル名：ProtSetting.xml にはファイル選択で指定された情報が保持されている。

C-3-3. アカウント DB
格納ファイルはファイル名：PROTMET.mdf、PROTMET.ldf であり、ログイン後の[オプション]-[設定]画面により、任意のフォルダに格納することが出来る。テーブル一覧を表 2-11 に ER 図を図 2-19 に示した。

C-3-4. Web サービス設定ファイル（サーバ側）
XML ファイルを受信後、メール通知するための設定する DTD ファイルとその設定例、キャプション付き説明の仕様を（図 2-20、表 2-12）に示した。
[格納場所] C:¥Documents and Settings¥Default User¥Application Data
[ファイル名] MailTemplate.XML

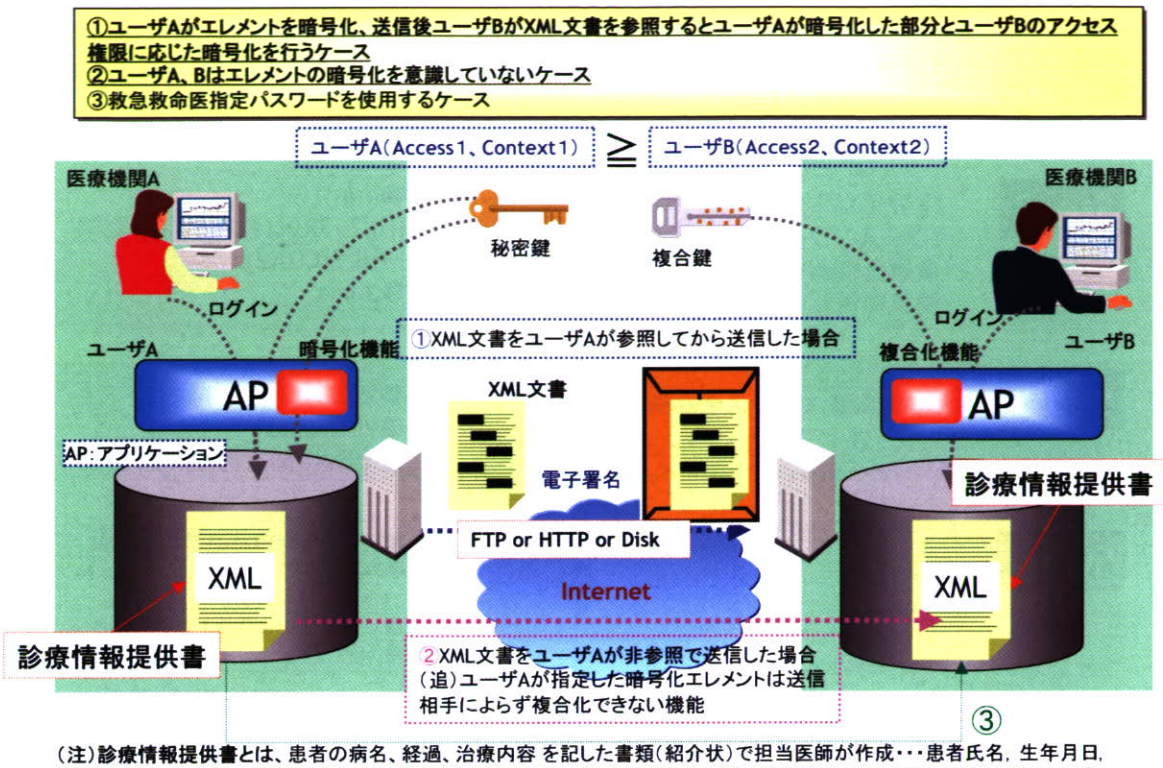
D. 結論

本章では主に任意の 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。

E. 研究発表
なし

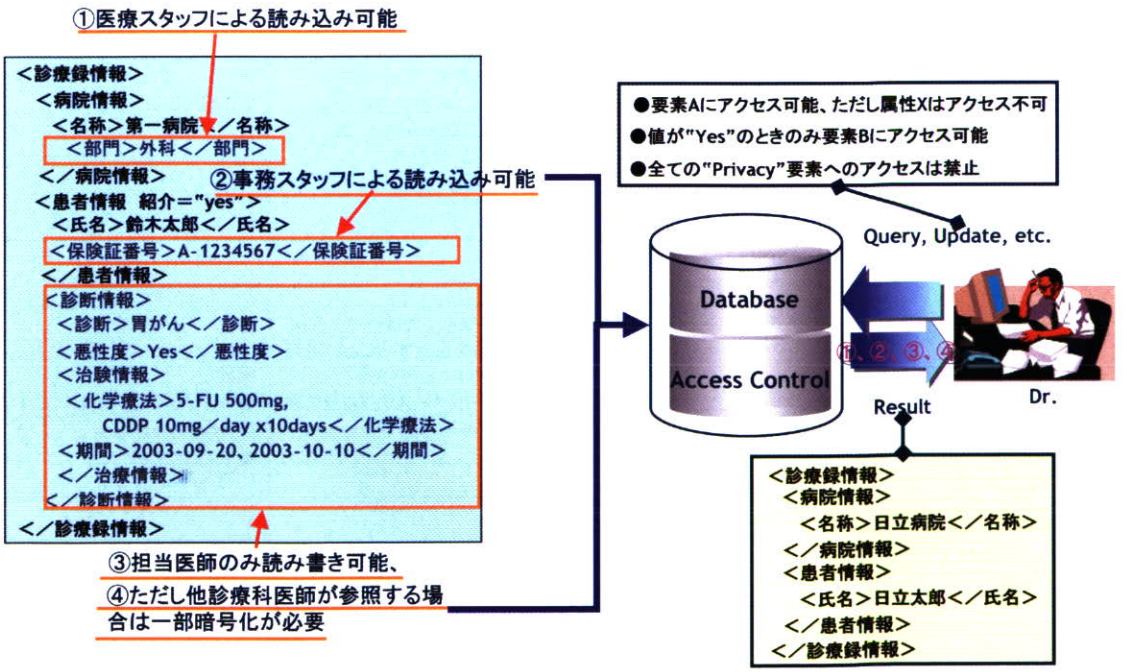
F. 知的財産権の出願・登録状況
1. 特許取得
なし
2. 実用新登
なし
3. その他
なし

図2-1　地域医療連携における暗号化XML文書の交換様式



(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2-2　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2-3 地域医療連携セキュリティシステム構築のステップ

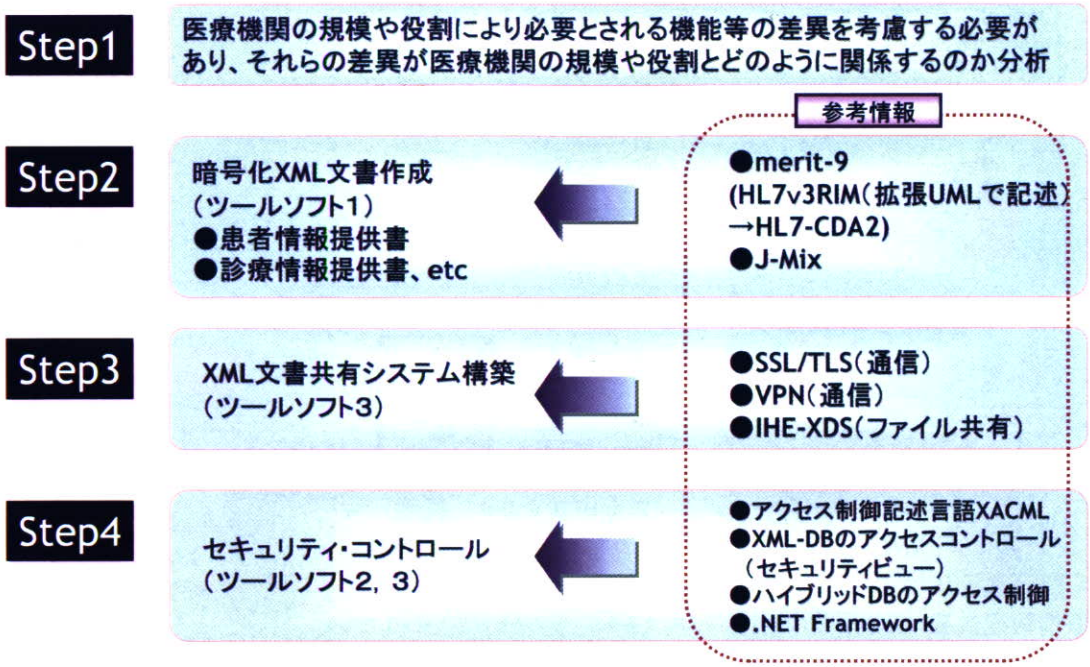


表2-1 データベース(DB)のセキュリティ機能比較

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)

表2-2 XML-DBとHybrid-DBの機能比較一覧

	製品名称	仕様/言語対応 スキーマ	運用機能 ユーザ管理/セキュリティ機能	関連ツール
ネイティブ系	Cyber Luxeon Ver2.0	DTD、XML Schemaに対応	CyberLuxeonのストレージを利用したユーザー管理、およびLDAPプロトコルを利用したディレクトリサーバーを用いてのユーザー認証が可能。	データベース管理およびクエリ発行、更新処理、データベース管理をGUIから行なえる「DXE Manager」を標準添付、ほかにコマンドラインツールやJava、XSLTを利用したWebアプリ構築用のサンプルプログラムを用意。
	EsTerra XML Storage Server	RELAX NG(妥当性検証も可能)、DTD、XML Schema(データ登録が可能)	ユーザー/グループ単位に権限を設定でき、XMLドキュメントレベルやノードレベルでアクセス制御が可能。	Excel/WordからXMLデータを抽出/挿入するツール「CabineXシリーズ」、入出力画面作成ツール「XLeaf」(Java版を今春発売予定)、Webアプリ自動構築ツール「Web Application Generator」など
	NeoCore XML Management System 3	特定のスキーマに依存しない	ユーザー単位/ユーザーグループ単位に権限設定が可能。また、ノード単位でコマンドの制約(Query/Insert/Delete/Modify/Store)をかけることができる。	全文検索エンジン「QuickSolution for NeoCore」、RDBMS連携ツール(EAIツール)「DataSpider for NeoCore」
	Tamino XML Server V4.4	XML Schema	外部Webサーバーまたは Taminoに保存された情報による認証メカニズムを利用できる。格納されたXMLデータに対してノードレベルでアクセス権限をアクセス制御リスト(ACL)として定義可能。	Webブラウザベースの管理ツール「Tamino Manager」、システム管理用バッチコマンド「argbatch」
	TX1 V2	特定のスキーマに依存しない	ユーザー単位で、Xpath表記が一致する構造パターンごとに実行権限(追加/更新/検索など)を設定可能。	DB構築/管理ツール「Xbrowser」、Webアプリケーション開発支援機能「XWeb」、RDBやNotesなどさまざまな形式のデータをXML形式に変換し、TX1に登録する「データ連携機能」
	eXist 1.1.1(安定版)	DTD、XML Schema	GUI管理クライアントおよびApache Antのタスクにより、ユーザーの管理とアクセス許可を設定できる。また、XACML 1.0/1.1によるアクセス管理も可能。	Java言語に対応した開発環境、テキストエディタ「jEdit」、Zopeコネクタ「eXistDA」
ハイブリッド系	DB2 9	XML Schema(レコードごとにスキーマの変更が可能)、DTDをサポート。スキーマレスでも可能。	基本はOSのユーザー管理機能を使用するが、Security Pluginによりユーザー独自の認証システムへの連携も可能。また、ユーザー、グループごとに行、列レベルでのきめ細かなアクセス制御が可能。	開発ツール「DB2 Developer Workbench」、統合開発環境「Visual Studio」「Rational Application Development」、RAD環境「JUSTSYSTEM xfy」、DB2 9対応の運用管理ツールなど
	Oracle Database 10g Release(10.2.0)	DTD、XML Schema	ISO/IEC 15408(Common Criteria)などの各種国際標準の認証を取得しているセキュリティ機能に加え、アクセス制御リスト(ACL)による管理が可能。	DB管理ツール「Oracle Enterprise Manager 10g」、Java開発ツール「Oracle JDeveloper 10g」、.NETアドイン「Oracle Developer Tools for Visual Studio .NET」
	Oracle Berkeley DB XML 2.3.8	DTD、XML Schema	AESを使ったデータベース暗号化を実装している。ユーザー管理機能は実装していないため、実行環境のOSのユーザー管理を利用する。	XML統合開発環境「Stylus Studio 2007 XML IDE」(日本代理店データディレクトテクノロジーズ http://www.datadirect.co.jp/products/stylus/)、「Oxygen XML Editor」(http://www.oxygenxml.com/)
	SQL Server 2005	XML Schema、XSD	Active Directoryによる統合認証、ユーザーとスキーマの分離、強固なパスワードポリシーデータの暗号化、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「Management Studio」、統合開発環境「Visual Studio 2005」

図2-4 診療情報提供書の例

診療情報提供書

平成 20 年 1 月 1 日

○○○○○○○ 医院
○○ ○○先生 御侍史

長崎大学医学部歯学部附属病院
○○○○科
TEL 095-819-7263 FAX 095-819-7267
松本 武浩 (内線 7529)

下記の患者様を紹介します。どうぞよろしくお願いいたします。

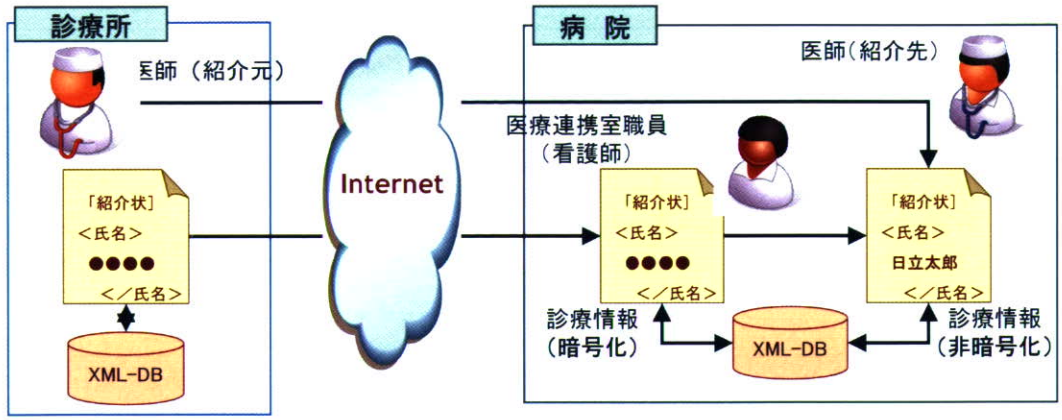
【患者氏名】 ○○○○ ○○○○様 男性
【生年月日】 昭和１８年０２月１０日 満 ６４歳

【診断名】
＃１ C型慢性肝炎
＃２ 高血圧症
＃３ 胆石症

【症状経過・検査結果・治療経過】
いつも大変お世話になります。 ご多忙中強縮ですが○○氏をご紹介いたします。
○○氏は当院にて＃１にて外来経過観察中です。 2000 年に IFN 治療を受けましたが、HCV は消失しなかったものの、その後は Ib 型高ウイルスタイプですが、肝機能正常です。
一方、以前より高血圧があり下記内服にて○○病院にて治療を受けておられましたが、今回、担当医が代わられたとのことで、お住まいの近くの医院にかかりつけ医をお願いした方が良いだろうと今回ご紹介する次第です。高血圧症に関して御高診御治療をお願いいたします。
当方は＃１に関して引き続き経過観察させていただきたいと思います。
よろしくお願いいたします。

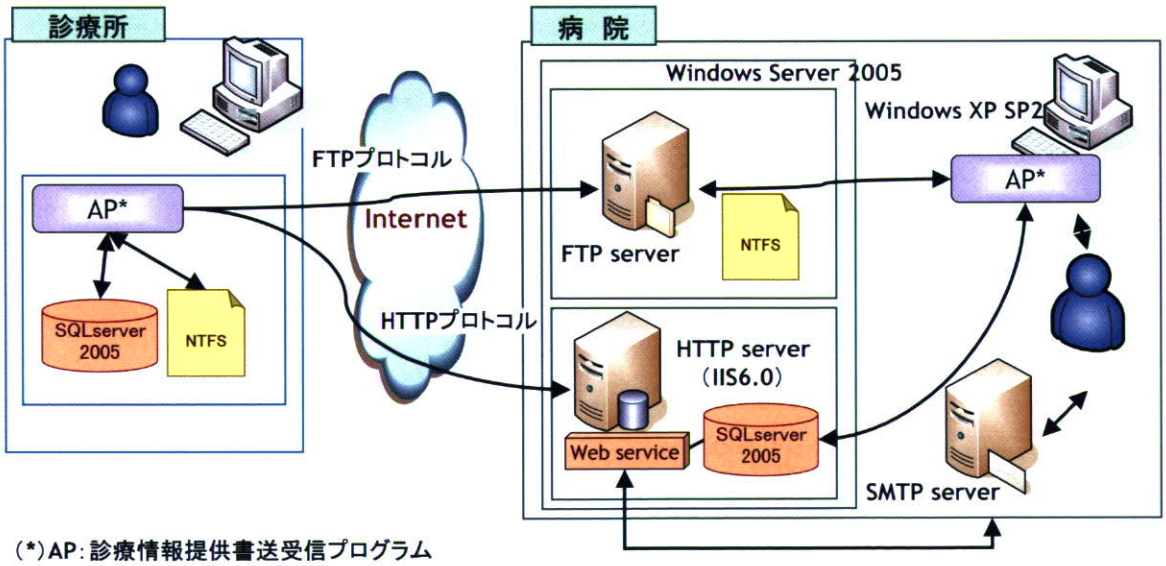
【処方】
1．ノルバスク 5ｍｇ 1ｘｍ

図2-5 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。

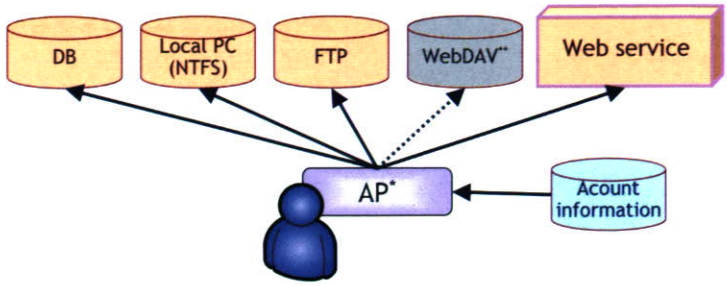
図2-6 診療情報提供書送受信システムの構成図



(*) 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。

図2-7　診療情報提供書送受信システムの機能設計



暗号化／非暗号化の権限設定

(*)AP:診療情報提供書送受信プログラム
(**)今回実装対象外

図2-8　診療情報提供書送受信システムのWebサービス

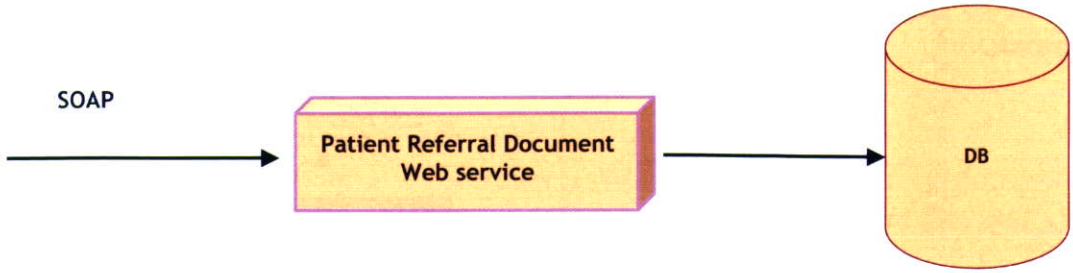
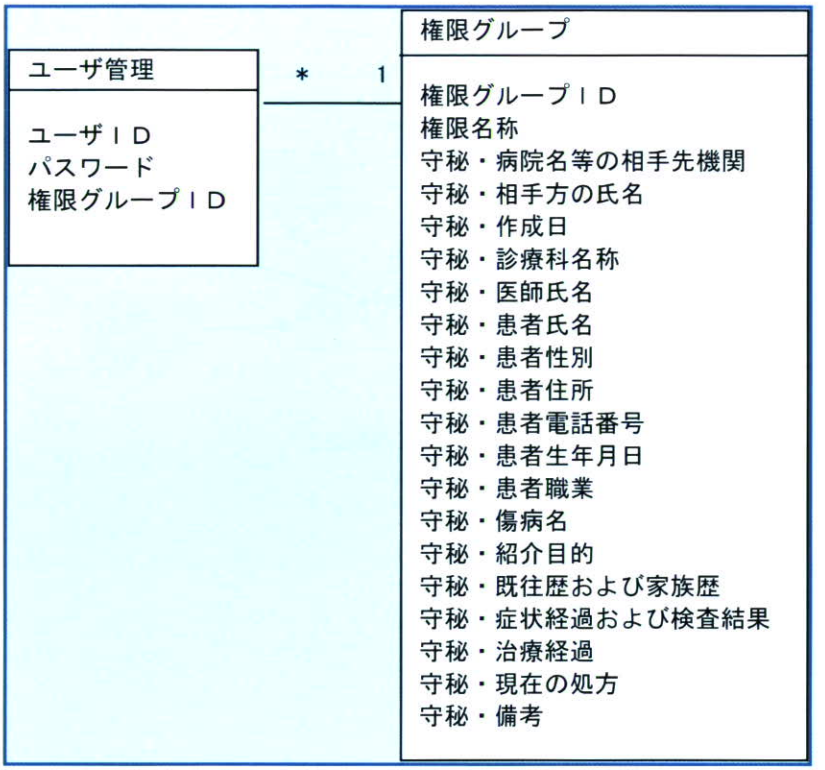


図2-9 診療情報提供書送受信システムにおけるユーザのアクセス権限



（注）守秘：暗号化／非暗号化の意

図2-10 診療情報提供書送受信システムの画面遷移

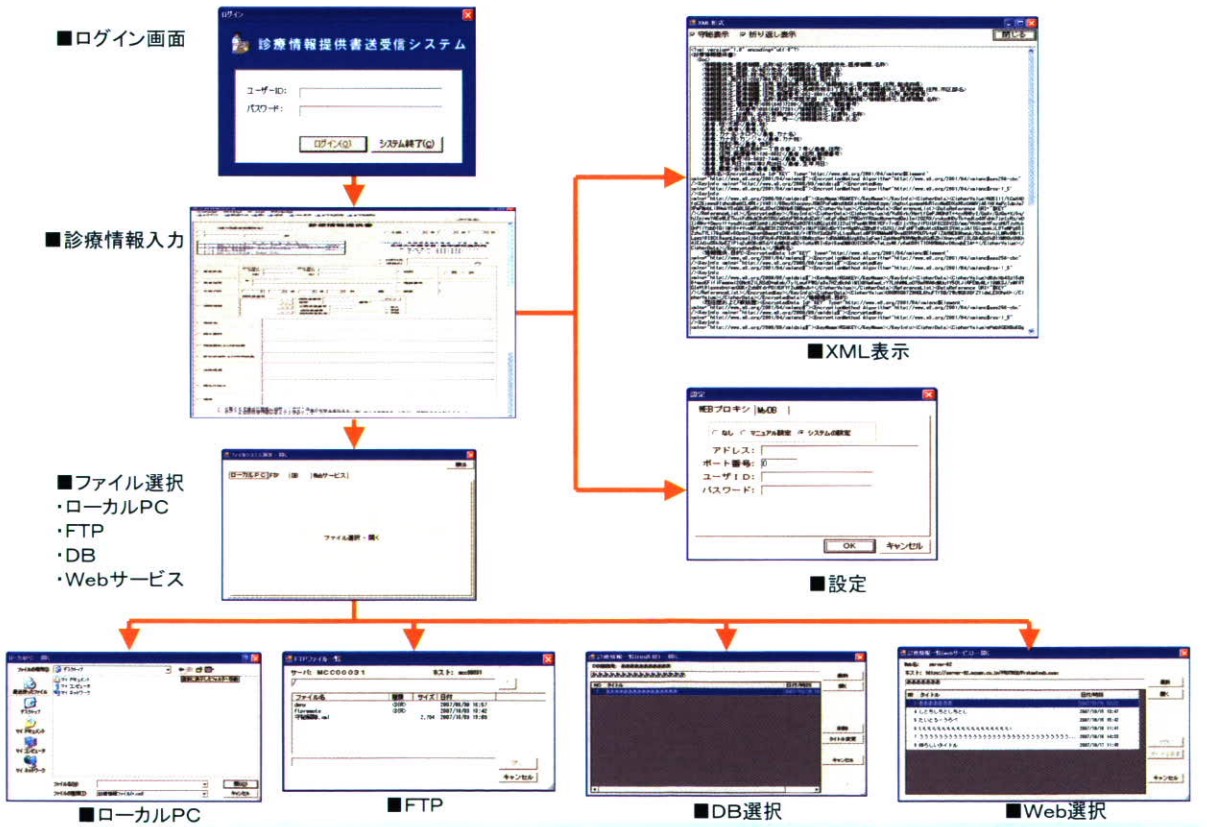
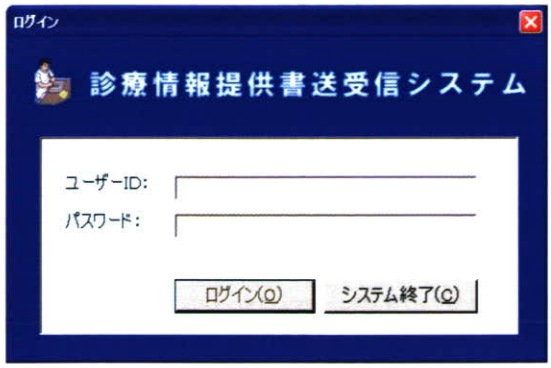


表2-2 診療情報提供書送受信システムログイン画面の各キャプション



キャプション	コントロール	説 明
ユーザＩＤ	TextBox	ユーザＩＤを入力
パスワード	TextBox	パスワードを入力
ログイン	Button	入力されたユーザＩＤとパスワードを判定し、正しければログインを行う。誤っている場合は、エラー表示を行う
システム終了	Button	本システムを終了する

図2-11 診療情報提供書入力インターフェース

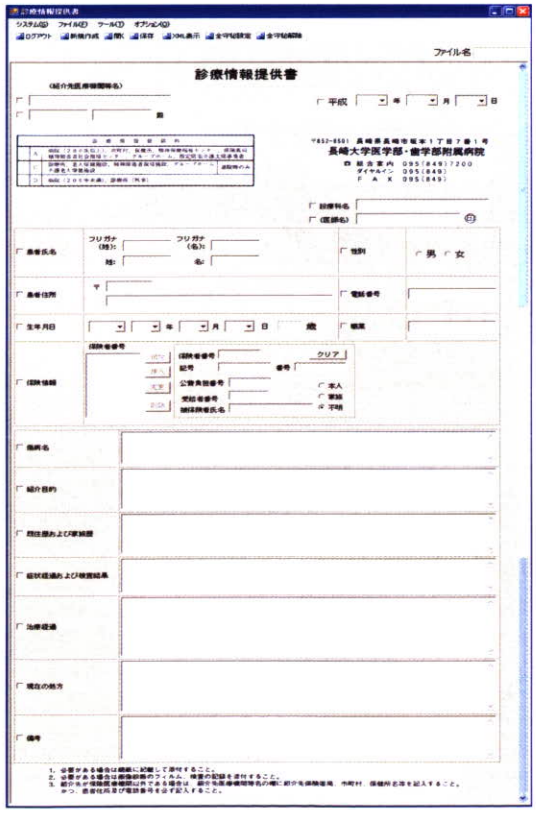


表2-3　診療情報提供書送受信システムの各種メニュー

メニュー			説　明
レベル１	レベル２	レベル３	
システム	ログアウト		ログイン画面へ戻る
ファイル	新規作成		入力項目を初期設定する （将来はテンプレート選択画面を表示する）
	開く		ファイルシステム選択画面を表示し、指定された診療情報ファイルを開く
	保存		ファイルシステム選択画面を表示し、診療情報を保存する
ツール	XML表示		表示されている診療情報画面のｘｍｌデータを表示する 守秘化されている場合は、対象エレメントが暗号化されている
	全守秘	設定	入力項目にチェックが入っているエレメントを暗号化する 暗号化された入力項目は「●●●●●●」表示される
		解除	暗号化されているエレメントを解読し平文にする 複合化されたエレメントは平文表示される
オプション	設定		次の設定をする画面を表示する (1)ＦＴＰ→設定名、ホストアドレス、リモートフォルダ、ユーザＩＤ、パスワード (2)Ｗｅｂサービス→設定名、ホストＵＲＩ、ユーザＩＤ、パスワード (3)HTTPプロキシ→プロキシアドレス、ポート番号、認証ＩＤ、認証パスワード (4)DB→SQL-Server接続文字列を指定する

図2-12　暗号化された診療情報提供書のXML形式による表示

表2-4 暗号化された診療情報提供書のXML形式による表示(キャプション付きコントロールの説明)

キャプション	コントロール	説 明
暗号化/非暗号化表示	checkbox	プロトタイプの特殊機能として追加チェックをオフすることにより、守秘化されている項目を平文として見られる。
折り返し表示	checkbox	オンの場合、一行全体を画面内に表示する。 オフの場合、折り返し無しで表示する。(横スクロールバーで左右スクロール移動を行う)
閉じる	Button	画面を閉じる

図2-13 診療情報提供書送受信システムのファイル選択(ファイルシステム)

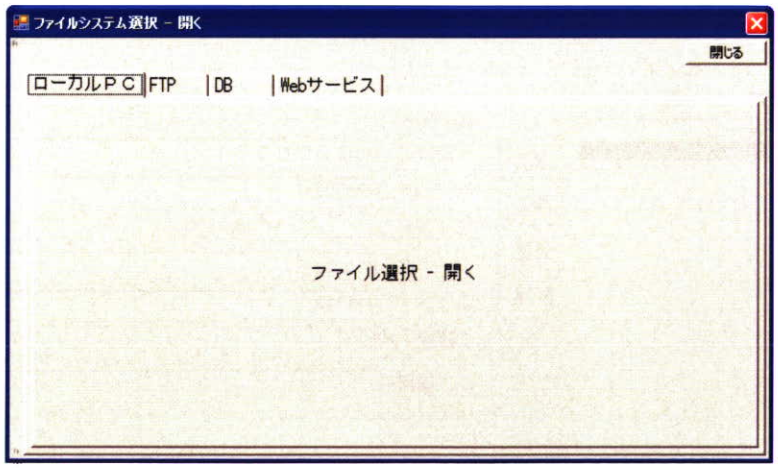


表2-5 診療情報提供書送受信システムのファイル選択(ファイルシステム キャプション付きコントロールの説明)

キャプション	コントロール	説 明
ファイル選択	button	ローカルファイルを選択するためのファイル選択画面が開く
閉じる	Button	画面を閉じる

図2-14(1) 診療情報提供書送受信システムのファイル選択(FTP)

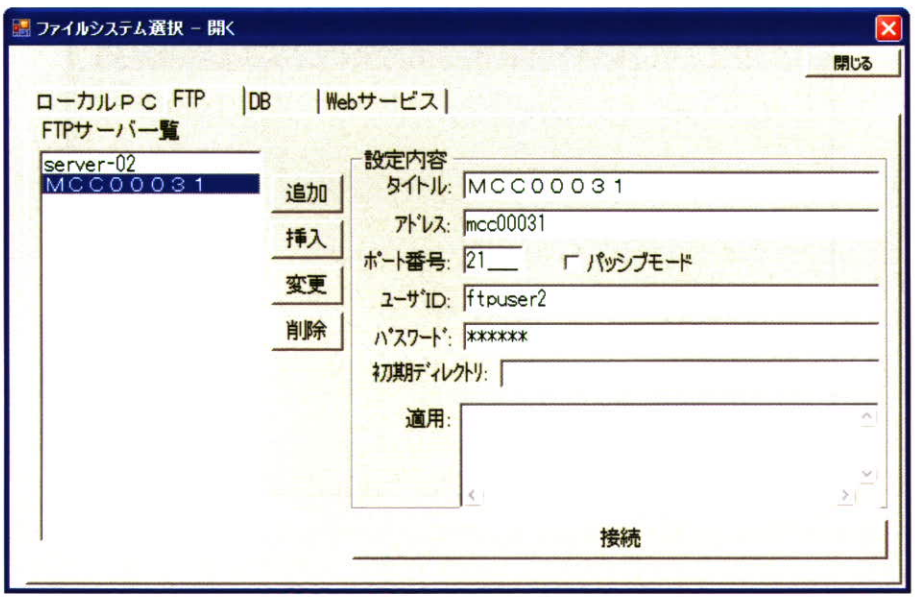
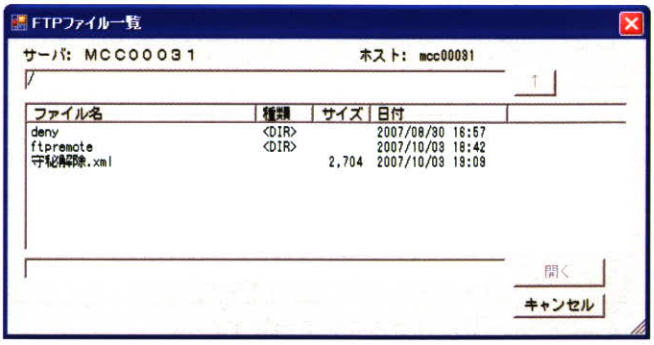


表2-6 診療情報提供書送受信システムのファイル選択(FTPキャプション付きコントロールの説明)

キャプション	コントロール	説明
ＦＴＰサーバ一覧	ListBox	登録されているＦＴＰサーバー一覧が表示される
追加	Button	設定内容で入力されたＦＴＰ設定情報を一覧の最後に追加する
挿入	Button	設定内容で入力されたＦＴＰ設定情報を一覧で指定された行に挿入する
変更	Button	一覧の指定された行のＦＴＰ設定情報を書き換える
削除	Button	指定された一覧表の情報を削除する
タイトル	TextBox	一覧に載せる名称を指定する
アドレス		ＦＴＰサーバーのアドレスまたはホスト名を指定する。
ポート番号		ＦＴＰサーバーのポート番号を指定する。通常は２１
ユーザＩＤ		ログインユーザＩＤを指定する
パスワード		ログインパスワードを指定する
初期ディレクトリ		ログイン後の初期ディレクトリを指定する
接続	Button	選択された一覧のＦＴＰサーバに接続する

FTPサーバーからファイル一覧を取得するコマンドはNLISTを使用しているが、サーバータイプはUNIXを前提にしている。
正常にフォルダが取得できない場合、FTPサーバーのファイル名種別をUNIXへ変更してください

図2-14(2) 診療情報提供書送受信システムのファイル選択(FTP)



キャプション	コントロール	説 明
ファイル名入力	TextBox	ファイル一覧で選択されたファイル名が表示されている
ファイル一覧	ListView	ＦＴＰサーバーのファイル一覧
開く	Button	指定されたファイルを開く
キャンセル	Button	画面を閉じる

図2-15(1) 診療情報提供書送受信システムのファイル選択(DB)

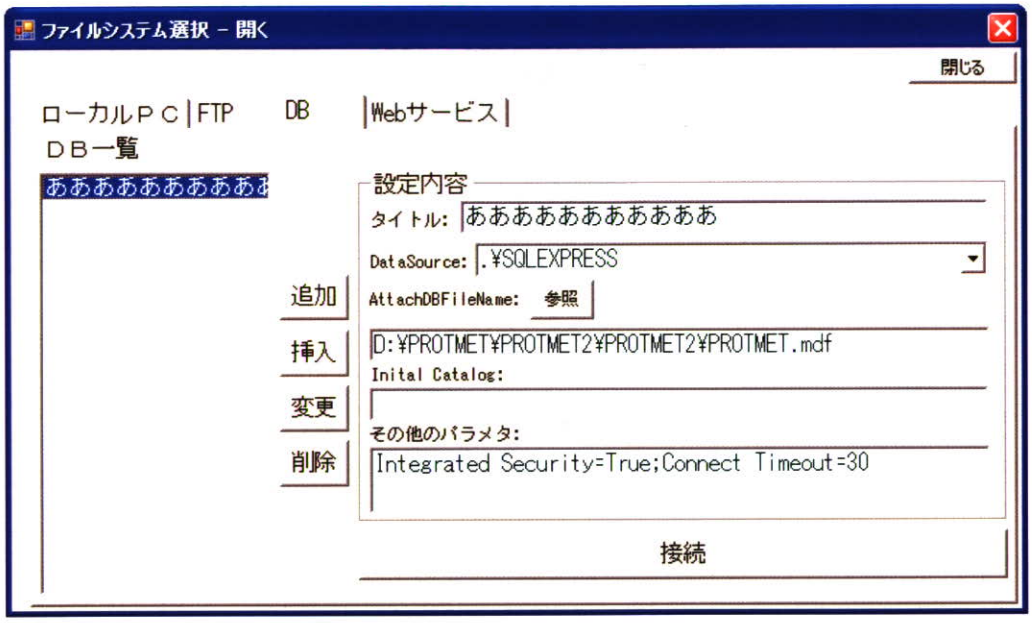


表2-7(1) 診療情報提供書送受信システムのファイル選択(DB)

キャプション	コントロール	説 明
DB一覧	ListBox	登録されているＤＢ一覧が表示される
追加	Button	設定内容で入力されたＤＢ情報を一覧の最後に追加する
挿入	Button	設定内容で入力されたＤＢ情報を一覧で指定された行に挿入する
変更	Button	一覧の指定された行のＤＢ情報を書き換える
削除	Button	指定された一覧表の情報を削除する
タイトル	TextBox	一覧に載せる名称を指定する
DataSource	ComboBox	データソースを指定する 「.¥SQLEXPRESS」:SQL-Server Express 「(local)」:自ＰＣのSQL-Server その他:「¥¥コンピュータ名¥インスタンス名」で他のＰＣに接続
AttachDBFileName	TextBox	データソースがSQL-Server Expressの場合指定する アタッチするＤＢパス名称を指定する
Initial Catalog	TextBox	データソースが SQL-Serverの場合指定する データベースの名称を指定する
その他のパラメタ	TextBox	その他の接続文字列を指定する 「User=<ユーザ名>;Password=<パスワード>」や「Integrated Security=True」などの文字列を指定する
接続	Button	選択された一覧のＤＢに接続する

図2-15(2) 診療情報提供書送受信システムのファイル選択(DB)

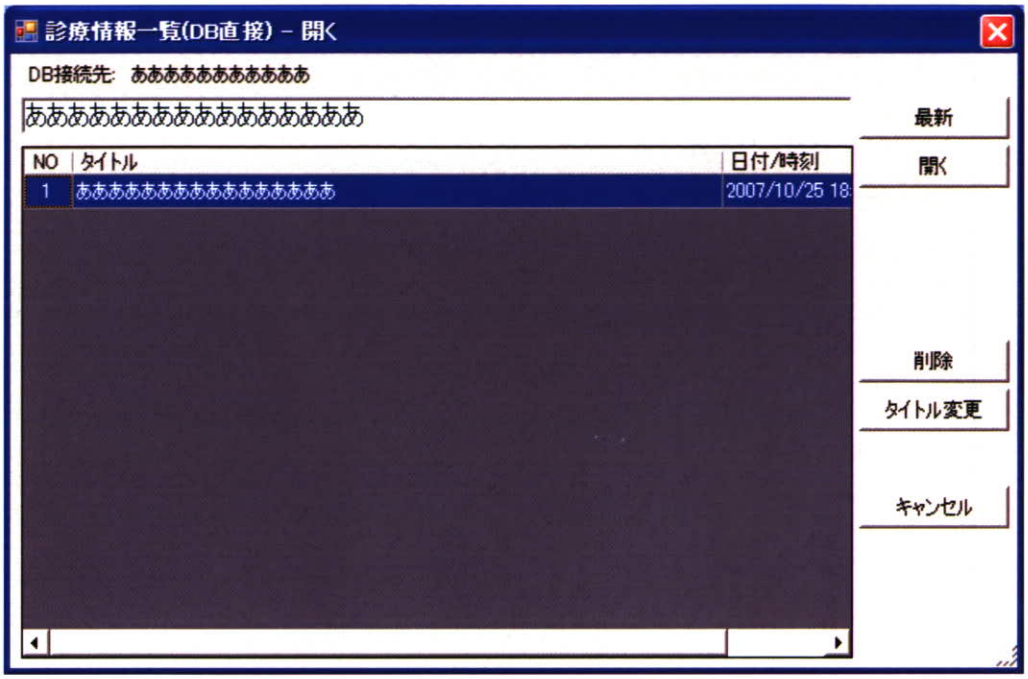


表2-7(2) 診療情報提供書送受信システムのファイル選択(DB)

キャプション	コントロール	説 明
タイトル名入力	TextBox	一覧で選択されているタイトルが表示される 直接変更することが可能 「新規保存」または「タイトル変更」実行時にここで指定されたタイトル名が設定される
一覧	GridView	ＤＢに登録されている診療情報の一覧が表示される
最新	Buttton	最新情報を表示する
開く	Button	一覧で選択されているタイトルの診療情報ファイルを開く
保存	Button	指定されたタイトルのファイルに上書き保存される
新規保存	Button	新しくタイトルを付け、保存する
削除	Button	指定されたタイトルを削除する
タイトル変更	Button	一覧で指定されているタイトルをタイトル名入力で指定されたタイトルに変更する

図2-16(1) 診療情報提供書送受信システムのファイル選択(Webサービス)

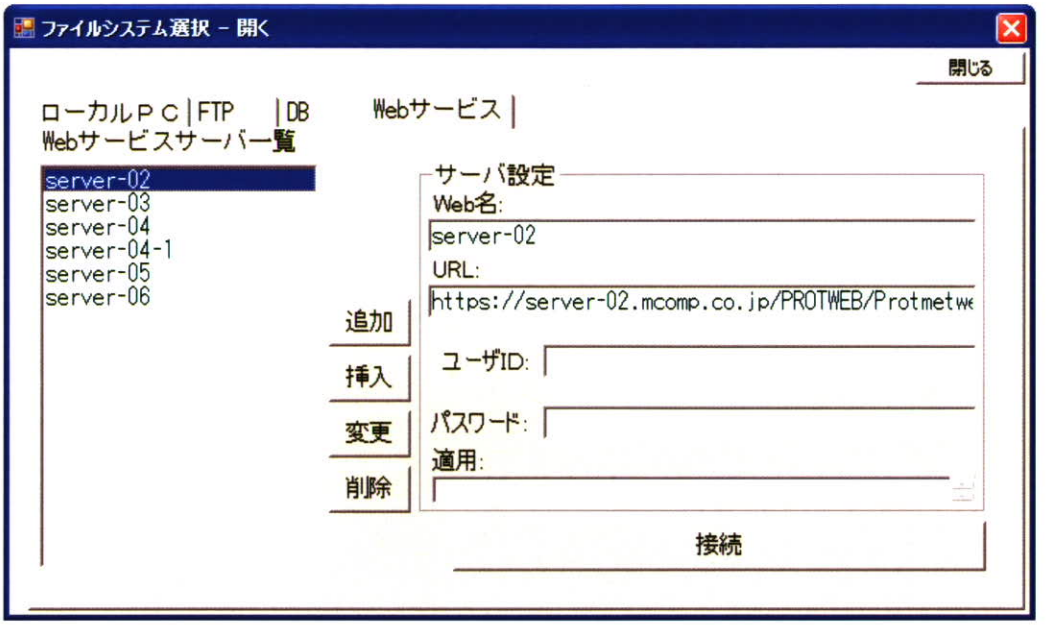


表2-8(1) 診療情報提供書送受信システムのファイル選択(Webサービス)

キャプション	コントロール	説 明
Webサービスサーバー覧	ListBox	登録されているサーバー覧が表示される
追加	Button	サーバー設定で入力されたサーバー情報を一覧の最後に追加する
挿入	Button	サーバー設定で入力されたサーバー情報を一覧で指定された行に挿入する
変更	Button	一覧の指定された行のサーバー情報を書き換える
削除	Button	指定された一覧表の情報を削除する
Web名	TextBox	Ｗｅｂサービスサーバー覧に載せる名称を指定する
URL	TextBox	サービス名のＵＲＬを指定する
ユーザID	TextBox	指定したサービスに認証が必要な場合は、ユーザＩＤを指定する。尚、認証タイプは「基本認証」をサポートしている
パスワード	TextBox	認証が必要なサーバのパスワードを指定する
適用	TextBox	動作には影響しないメモを記載する
接続	Button	選択された一覧のサーバーに接続する

図2-16(2) 診療情報提供書送受信システムのファイル選択(Webサービス)

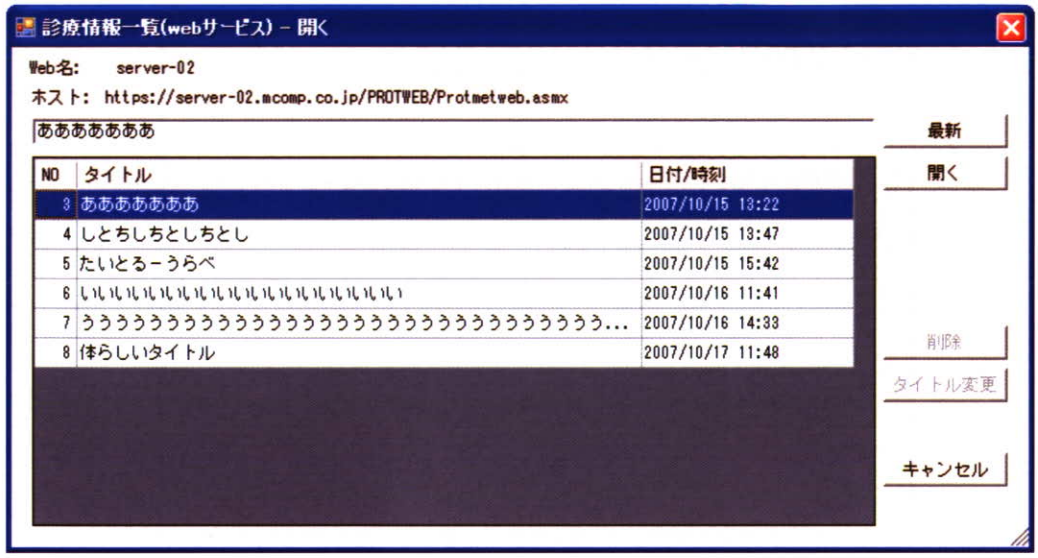


表2-8(2) 診療情報提供書送受信システムのファイル選択(Webサービス)

キャプション	コントロール	説 明
タイトル名入力	TextBox	一覧で選択されているタイトルが表示される 直接変更することが可能 「新規保存」または「タイトル変更」実行時にここで指定されたタイトル名が設定される
一覧	GridView	Webサーバーに登録されている診療情報の一覧が表示される
最新	Buttton	最新情報を表示する
開く	Button	一覧で選択されているタイトルの診療情報ファイルを開く
保存	Button	指定されたタイトルのファイルに上書き保存される
新規保存	Button	新しくタイトルを付け、保存する
削除	Button	指定されたタイトルを削除する
タイトル変更	Button	一覧で指定されているタイトルをタイトル名入力で指定されたタイトルに変更する

図2-17 HTTPプロキシ経由でWebサービスを使用する場合の設定

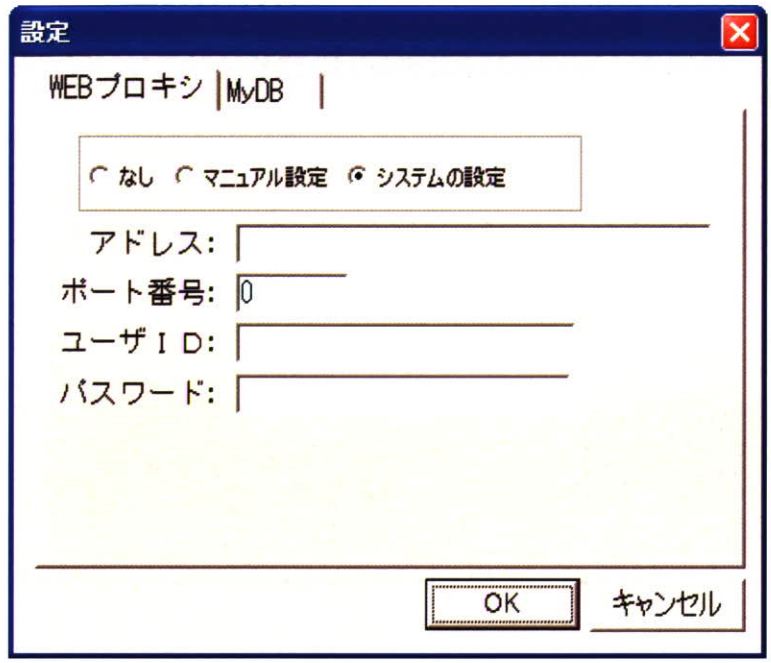


表2-9 HTTPプロキシ経由でWebサービスを使用する場合の設定

キャプション	コントロール	説 明
接続文字列	TextBox	ユーザＩＤとパスワード（ユーザ設定テーブル）が設定されているＤＢの接続文字列を指定する [%CURDIR%]文字列は、Application.LocalUserAppDataPathへ置き換わる
既定値	Button	標準値の文字列が設定される。 上記画面は、既定値ボタンが押下された直後の様子である

図2-18 ユーザ設定テーブルが含まれるアカウントDBへの接続文字列を指定する場合の設定

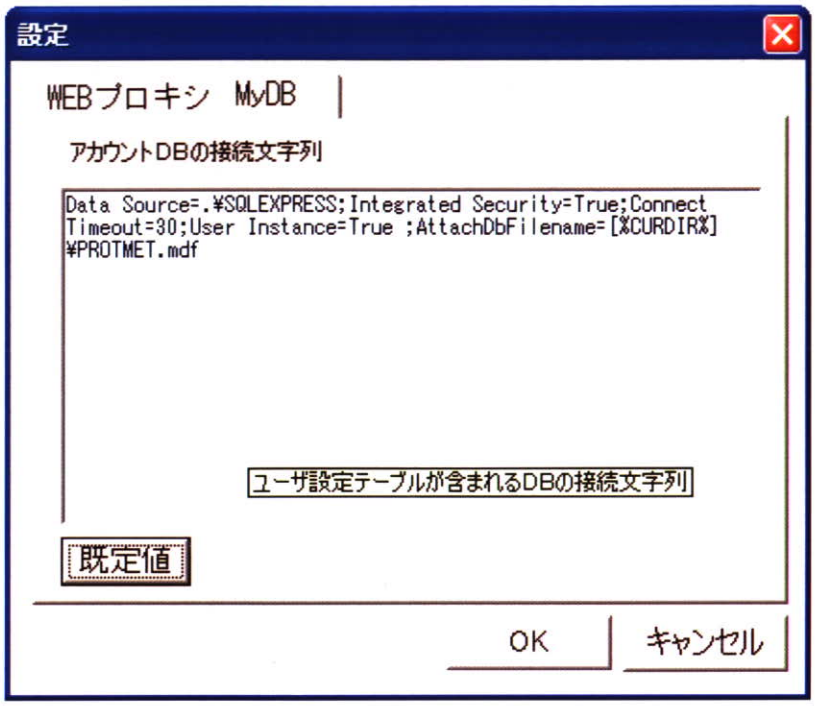


表2-10 ユーザ設定テーブルが含まれるアカウントDBへの接続文字列を指定する場合の設定

キャプション	コントロール	説 明
接続文字列	TextBox	アカウントＤＢの接続文字列を指定する [%CURDIR%]文字列は、Application.LocalUserAppDataPathへ置き換わる
既定値	Button	標準値の文字列が設定される。 上記画面は、既定値ボタンが押下された直後の様子である

図2-19 診療情報提供書送受信システムのERD(Entity Relation Diagram)

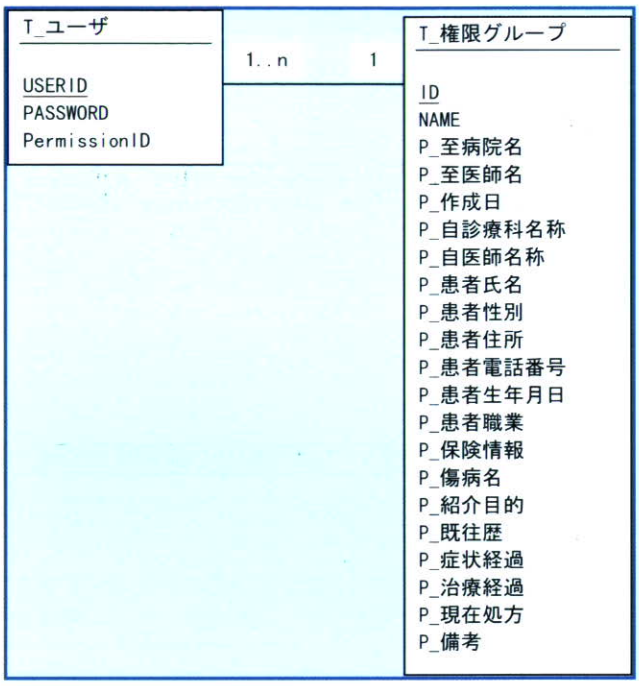


表2-11 診療情報提供書送受信システムのテーブル一覧

テーブル名	内 容
T_ユーザ	ユーザＩＤ等が格納されているテーブル
T_権限グループ	権限グループ（＝職種）が格納されているテーブル