診療情報統合システムNEXTASを用いた地域連携システム

Intra-Regional Medical Collaboration System Using NEXTAS Clinical Information Integration and Management System

鈴木　一洋[*1]　SUZUKI Kazuhiro
小林　章[*1]　KOBAYASHI Akira
坂田　大輔[*1]　SAKATA Daisuke
小山　和夫[*1]　OYAMA Kazuo

電子カルテという言葉が世の中に浸透してきた昨今，全国各地の病院でIT化が進み，従来は紙やフィルムで運用されていた病院業務も，少しずつペーパーレスあるいはフィルムレスに変わりつつある。情報の電子化には，同じデータを複数の人が同時に参照できることや，検索性の向上により過去データとの比較が容易になる等メリットが多々あるが，更なる患者サービスの向上に結びつく要素もいくつかある。本システムではこの点に注目し，一般的なInternet回線を使用しながら，情報の盗聴・改竄を防ぐセキュリティ機能と，利用者単位でのアクセスコントロール機能を持つ「地域連携システム」を構築した。本システムによって，平易な仕組みと強固なセキュリティとを両立させながら，地域中核病院で発生した診療情報を周辺の地域医療機関等と共有することが可能になる。

In today's widespread acceptance of the term "Electronic Patient Record (EPR)", highly computerized hospitals accross the nation, are moving away from a traditional paper- and film-based workflow toward a paperless or filmless workflow. Computerizing data affords us many advantages such as availability of multi-reference and easy manageability of data comparison that is facilitated by advanced computer-mediated search, encompassing some factors contributing to the improvement of patient services. Focusing on such factors, we have developed an Internet-based intra-regional medical collaboration system featuring data security against interception or falsification and per-user access control. This system allows sharing of clinical information, which the central hospitals in a region recorded, with other neighboring healthcare clinics while maintaining simple structure yet powerful security.

1. はじめに

全国各地の医療機関でIT化が進んできた。主に急性期治療を担う大病院ではオーダリングシステムやPACS(画像情報システム)が導入され，従来は紙やフィルムで運用されていた業務が大きく変わり始めた。情報が電子化され，コンピュータを用いた業務になることで，データの共有性と検索性が向上し，同じデータを同時に複数の人が参照できたり，過去データや同一症例のデータとの比較が容易にできたりするようになった。医療機関にも情報システムが定着しつつあるなかで，電子化された情報を有効活用する土壌は整ってきた。

一方，医療機関の機能分化が進められていくなか，地域全体として医療の質の向上を図るために，主に急性期治療を担う中核病院と退院後の継続的な治療を担う地域医療機関との間で，密接な連携を模索する動きが広がってきた。このような環境のなか，中核病院内で発生した検査結果やサマリ情報を地域医療機関と共有することで，地域完結型医療を技術的な側面でサポートする地域連携システムを構築した。

2. 地域連携システムとしての要件

2.1 可用性

地域連携システムの利用者は複数医療機関にわたることが一般的である。その際に大きく問題となるのは，各医療機関で使用されている情報システムが，導入の時期や担当ベンダーによってハードウェアやOSが異なることである。特にクライアントPC端末の動作環境が異なる

*1 ETS開発医療ソリューション統括部 技術部

場合，システムの可用性という点で大きな障壁となってしまう。本システムでは，システムの可用性を高めるために，クライアント・ソフトウェアはWeb Browserの使用を前提とし，クライアントPC端末のOSやそのバージョン等に依存しない構造とした。

2.2 操作性

地域連携システムの利用者は多岐にわたり，中核病院に勤務する医師や看護士から地域医療機関の開業医や介護士に至るまで，コンピュータの使用頻度や習熟度に大きな個人差がある。従って，システムの操作や画面遷移については，直感的に判り易く，かつ，操作ミスを起こしにくい構造とした。

2.3 セキュリティ

セキュリティについては，機能面と運用面とのバランスで成り立っており，全てのリスクに対して機能と運用の両面から十分な検討を行わない限り，有効なセキュリティ対策とは成り得ない。地域連携システムの対象利用者は，コンピュータの使用頻度や習熟度に個人差があるため，特に複雑な機能についてはブラックボックス化し，利用者が強く意識する必要がない仕組みとした。運用面については，導入サイトのセキュリティ・ポリシーに強く依存するため，本稿では言及しない。

2.4 通信インフラ

中核病院と多数の地域医療機関との間を結ぶ通信インフラは，採用する回線の種類によって費用が大きく変動する。本システムでは，導入にかかる費用を最小限に留めるため，通信回線については，一般的なInternet回線をインフラとして使用することを前提とした。

2.5 アクセスコントロール

Internet回線やWebを用いたシステムは利便性の高いシステムアクセスインフラであるが，同時にネットワーク上に存在するシステム機能や情報が漏洩する危険を伴う。また，個人の住所や氏名，または過去の疾病や検査などの履歴情報などの個人情報を扱うシステムでは，システム利用者に対してアクセス対象の情報種毎に情報参照権限を定めたアクセスコントロール機能を適用し，個人情報を保護する必要がある。そのため，本地域連携システムでは，2.3節に記載したセキュリティ機能に加え，患者に帰属する診療情報種別と開示対象者を患者自身が選択するというルールに基づいたアクセスコントロール機能を実装した。

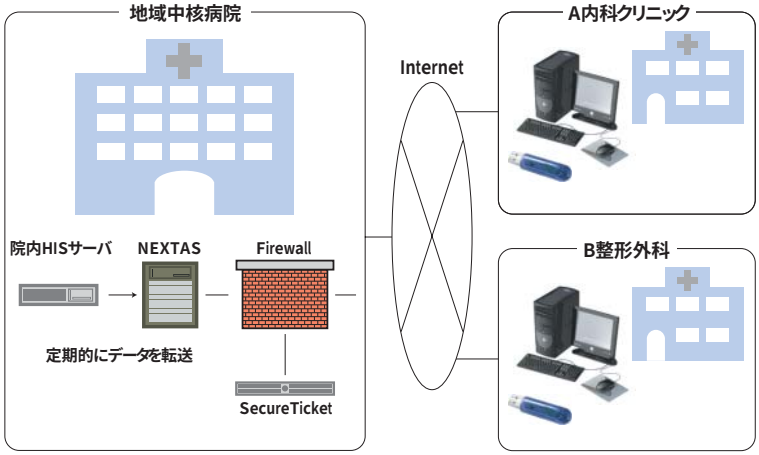

図1　地域連携システム概観

3. 地域連携システム

3.1 システム概観

地域連携システムの概観を，**図1**に示す。

地域連携システムは，地域中核病院に設置されるサーバ群と，地域医療機関に設置される複数のPC端末によって構成される。さらに地域中核病院内のサーバ群は，既設の院内HIS(病院情報システム)サーバと，地域連携用のドキュメント管理サーバNEXTAS，認証ソフトウェアパッケージSecureTicketとで構成される(詳細については次節で述べる)。NEXTASはFirewallの内側で院内HISサーバと通信可能なセグメントに設置され，SecureTicketはFirewallのDMZ(DeMilitarized Zone)に設置される。

地域医療機関と共有する情報は，院内HISサーバからNEXTASに対して定期的に送信され，NEXTASのWeb機能を通じて地域医療機関と共有される。

なお，地域医療機関からのデータ参照に際しては，SecureTicketのリバースプロキシ機能を利用した。これによって，地域中核病院外からのアクセスは，SecureTicketの認証を通過したセッションのみがNEXTASに転送されるような仕組みとなり，NEXTASのIPアドレスを一般に公開することなく，かつ，システムへのアクセスが認められていない不特定多数の人がアクセスすることを防いでいる。

3.2 NEXTAS

本節では，地域連携システムのコア・コンポーネントであるNEXTASについて記述する。

3.2.1 概要

NEXTASは，異なる部門システムでの多様な診療情報をXML形式によりデータ統合し，診療情報の一元管理を行うドキュメント管理サーバである。また，保存され

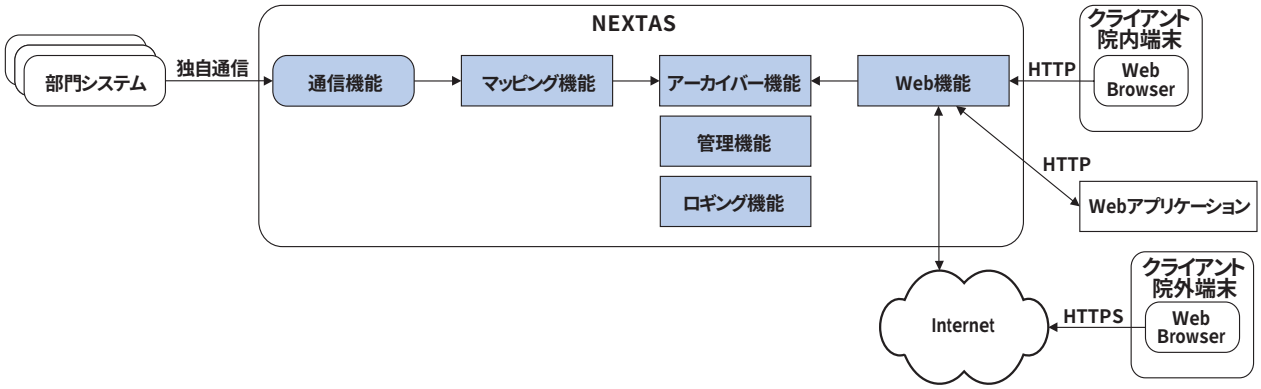

図2　NEXTAS機能概要

た診療情報をWebで公開することにより，シームレスかつ円滑な診療業務を支援する。

3.2.2　機能概要

図2に，機能概要を示す。

(1) 通信機能：汎用インタフェース(CORBA，FTP等)により，多様な通信プロトコルを持つ部門システムと接続する。

(2) マッピング機能：部門システムから格納される診療情報を独自形式から標準的なXML形式に変換する。また，各々の診療情報を独自形式にマッピングする機能は，設定情報により追加・変更ができる。

(3) ロギング機能：動作状態の正当性を保証するためのシステム保守情報，ユーザイベント等のアクセス監査情報を出力する。

(4) アーカイバー機能：診療情報の保存・更新・削除・検索の機能を提供し，標準的なXML形式により診療情報を一括管理する。

(5) 管理機能：NEXTASを管理するためのユーザアカウント設定，システム情報設定，サーバ運用操作のサービス機能を提供する。

(6) Web機能：NEXTASの検索機能により検索結果および蓄積された診療情報を，各クライアントPC端末からWeb Browserを利用することにより，クライアントのプラットフォームに依存せずにWebサービスを提供する。また，他のWebアプリケーションと連携することにより，詳細な診療情報や専門的な機能を利用する。

3.3 システムの特長

本節では，地域連携システムの特長について記述する。

3.3.1　セキュリティ機能

地域連携システムでは，ネットワーク上に存在する悪意ある第三者からの不正アクセスを防ぐことが必要である。NEXTASは，ログイン認証機能と認証時のセッションを利用した認証機能を持ち，登録利用者以外の参照要求を拒否することでセキュリティを保っている。

本システムでは，NEXTASは院外向けの診療情報サーバとして導入され，クライアントはInternet上のPC端末となる。NEXTASをInternetに接続して運用する場合，登録されていない利用者が，Internet上の任意のPC端末からNEXTASにアクセスできるため，以下のような不正利用のケースが想定される。

＜院外向けサーバで想定される不正利用のケース＞

・なりすまし

正規利用者に成りすまして，システムを利用するケース。登録利用者以外の第三者が，診療情報を参照してしまう可能性がある。

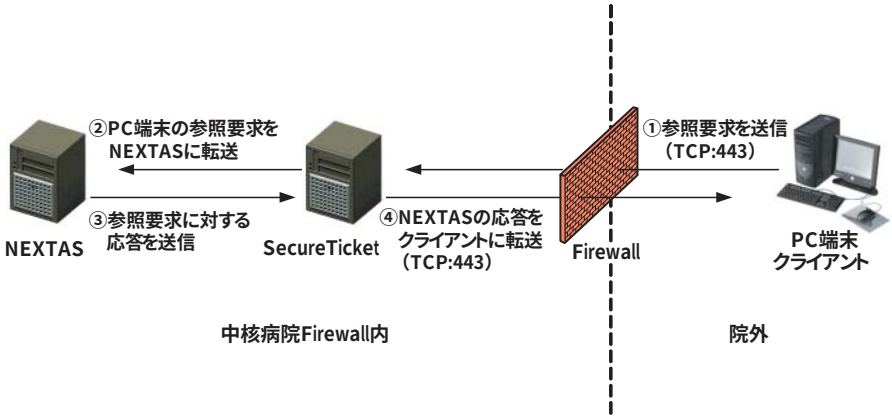

図3　NEXTASとSecureTicketの連携の仕組み

表1　フィルタリング機能

フィルタリング項目	説明
参照許可対象利用者･グループ	データ参照を許可する利用者のグループ(「○○病院外科」グループ,「××医院呼吸科」グループ　等)
文書種別	共有対象となる文書の種別(「退院サマリ」,「緊急処方」,「検体検査」　等)
文書発生診療科	共有対象となる文書が発生した診療科(「小児科」,「内科」,「脳神経外科」　等)
文書発生期間	共有対象となる文書が発生した日付の期間
文書参照可能期間	参照許可対象利用者･グループに対して,実際にデータ参照を許可する日付の期間

・DOS(Denial of Services)攻撃
　悪意のある第三者が，システムに対して短時間で数多くの参照要求を故意に送信するケース。これにより，システムの負荷が想定範囲を越え，システムが停止する可能性がある。
・サーバの乗っ取り
　悪意のある第三者が，システムのセキュリティホールを突いて，システムの操作権限を乗っ取るケース。これにより，登録利用者以外の第三者による診療情報の参照やシステムの破壊等が行われる可能性がある。

本システムでは，上記の不正利用を防止すると同時に通信の暗号化を行うために，SecureTicketを導入してセキュリティの強化を図った。SecureTicketは，当社が提供しているWeb統合セキュリティソフトであり，SecureTicketの認証情報(以下，Ticket)を持たないPC端末からのNEXTASへのアクセスを遮断する。

今回のNEXTASとSecureTicketの連携の仕組みを，**図3**に示す。

中核病院のFirewall内にNEXTASとSecure Ticketが設置されており，院外のPC端末からはSecure Ticketにのみアクセスできる。SecureTicketは，PC端末から送られてくるTCP：443ポートの参照要求を，NEXTASの特定ポートに転送する(**図3－①**，**－②**)。NEXTASは，参照要求に対する応答をSecureTicketに送信する(**図3－③**)。SecureTicketはNEXTASが送信した応答を，PC端末に転送する(**図3－④**)。

本システムでは，USBメモリにTicketを発行し，そのUSBを診療所の利用者に配布する運用を前提としている。診療所の利用者は，配布されたUSBメモリをInternetにつながっているPC端末に接続し，Web BrowserでSecureTicketにアクセスすると，NEXTASが提供する診療情報を参照することができる。

これらの仕組みにより，Ticketを持つ診療所の利用者以外は，NEXTASにさえアクセスすることができない。そのため，上で記載した「院外向けサーバで想定される不正利用のケース」は未然に防がれ，登録利用者のみの診療情報の参照，および，システムの安定稼動が実現すると考えられる。

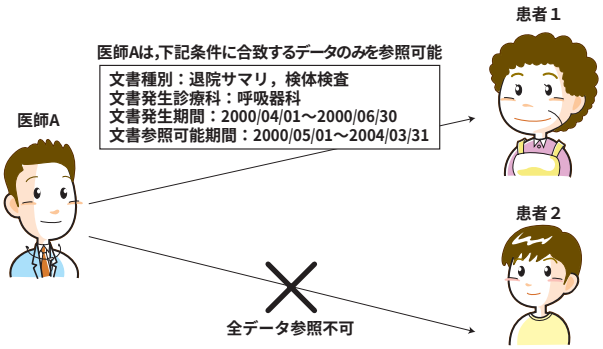

図4　アクセス・コントロールの設定例

3.3.2　アクセスコントロール機能

本システムにおいて，地域中核病院と地域医療機関との間で共有される診療情報は，患者自身が記入する同意書に基づいてフィルタリングされることを前提としている。これは，患者自身が自らの意思によって，自分自身の診療情報の中から，ある一定の条件に基づくものを，自分が指定した先生のみが参照できるようにするためである。共有するデータのフィルタリング条件は様々なパターンが想定されるが，本システムのアクセスコントロール機能では，診療情報を構成する主要データ項目の中から，**表1**の項目を用いてフィルタリングを行う。

ここで，**図4**を用いてアクセスコントロールの設定例を示す。

図4の設定の場合，医師Aは患者1のデータのうち，2000/04/01～2000/06/30の期間に呼吸器科で発生した退院サマリと検体検査のデータを，2000/05/01～2004/03/31の期間だけ参照することができる。従って，2004/04/01以降はアクセスコントロール機能によってデータ参照が拒否され，患者1のデータを閲覧することができなくなる。また患者2については，アクセスコントロール設定で全てのデータに対する参照権限が許可されていないため，データを閲覧することができない。この仕組みにより，細かい粒度でアクセスコントロールを行うことができ，患者の同意に基づくデータ共有を行うことができる。

4. おわりに

地域中核病院におけるIT化の推進は，医療分野における情報化の第一段階に過ぎない。診療所をはじめとする地域医療機関のIT基盤が整っていく中で，情報共有化の先に見えるリアルタイム双方向通信や蓄積された情報の二次活用を見据え，さらなる付加価値の創造を進めていきたい。