第1章 はじめに

1.1 背景

『HIV 診療支援ネットワークシステム（以下、「A-net」とする)』は、患者さんのプライバシー保護を図りながら、患者さんの診療情報の一部をエイズ治療・研究開発センター（以下、「ACC」とする）のホストコンピュータに入力し、エイズ治療・研究開発センターとエイズ治療ブロック拠点病院、拠点病院をネットワークで結ぶことにより、患者さんが受診される病院相互で診療情報を共有し、HIV 診療を円滑にし、かつ患者さんの地元で質の高い診療を可能にすることを目的としています。[HIV 診療支援ネットワークシステム（A-net）の説明文書より引用]

しかしながら、A-net は平成 10 年に試験運用を開始したシステムであり、システムを構成するハードウェアやソフトウェアの老朽化に加え、サポート期限の切れたハードウェアやソフトウェアも散見されるようになってきている。このような状況下で、万が一大規模なトラブルが発生した場合には、システムの復旧や継続運用が不可能な状況に陥る可能性も考えられ、大きな問題を抱えている。

また、当時は最新のセキュリティ対策を講じていたものが、年月の経過とともに近年のセキュリティ管理手法とは乖離したものとなりつつあり、更には現在一般的に用いられる汎用技術ではなく、あまり使われなくなった独自技術を採用していることが、今後のシステム改修や継続運用にあたっては大きな障害となっている。

更に、患者の個人情報の取扱いやプライバシー保護をめぐり、強固なセキュリティの確保に努めたため、利便性という観点からみると満足のいくものではなく、蓄積されたデータ量とその内容からシステムそのものの利用価値も高いとはいえず、アクセス数も伸び悩んでいる状況である。

こうした状況を打開するため、現在の A-net に代わる次期 A-net の開発に向けて、現状の課題の整理を行うとともに、医師及び患者からも積極的に利用されるシステムの構築を目指して、その解決策や目指すべき方向について検討を開始した。昨年度は次期 A-net のシステム開発において重点的に検討が必要と思われる「利便性の向上」、「セキュリティの確保」、「運用管理の向上」について研究を行った。

本研究では、昨年度の検討結果を踏まえ、次期 A-net のプロトタイプとなる DB システムを構築し、実際に診療データの投入を行い、有効性を確認する。

1.2 現状の A-net の問題点と対策

現状の A-net は、構築当時の技術的な制約から使い勝手が悪く、情報が入力されず、それ故使われないという負の連鎖に陥っている。各院では、A-net と同様の情報管理のため、独自 DB を作成する事態となっている。

(1) A-net 端末に関する問題
- A-net のデータ入力や参照などの操作は、各接続拠点となる院内に固定設置した専用端末に限定されており、台数が限られ不便
- A-net 専用端末のセキュリティ対策は物理的な立入り制限によるため、院内の特定の場所に移動しないと使用できず、使い勝手が悪い

(2) A-net システムのソフトウェアに関する問題
- データ入力項目が多すぎて、入力操作が煩雑
- 院内のシステム（電子カルテなど）と連携が無く、A-net 登録のためには 2 重入力の必要があり、負荷が高い
- A-net に登録された患者に「通し ID」が無いため、患者のトレースができない。（氏名の照合のみでは同一人物か特定できない）

(3) インフラと運用保守に関する問題
- A-net は HOSPnet をインフラに使用しており、旧 HOSPnet のベンダーである IBM にサーバ運用を委託している。昨年 HOSPnet の更新調達は他社が落札したため、同様の運用委託は困難。

1.3 今後の A-net の目指す姿

問題点を改善し、利用を促進させ、本来の目的である HIV 診療情報の共有による HIV 診療の円滑化を図る。利用率向上により、疫学的にも有効なデータ収集が可能になり、診療の質的向上につながる。

(1) 患者のトレースを実現
・患者を A-net に登録する際に、「通し ID」の様なものを発行し、引越しなどで病院を変更した場合でも同一人物か照合可能とする

(2) 患者参加型のシステムを指向
・患者が自分の診療データが閲覧できるなど、患者向けサービスを提供

(3) 利便性の向上による利用の促進
・端末のセキュリティ対策を見直し、端末設置場所や台数の制約を軽減する
・入力すべきデータ項目を選別し、入力の手間を軽減
・将来的に、院内のシステムと連動し、診察データ等から自動吸い上げとする（２重入力を止める）

(4) インフラの変更による自由度の向上
・インフラとしてインターネット回線を活用し、拠点や場所の制約を撤廃する。運用ベンダはインフラの制限なく、自由に選定可能。

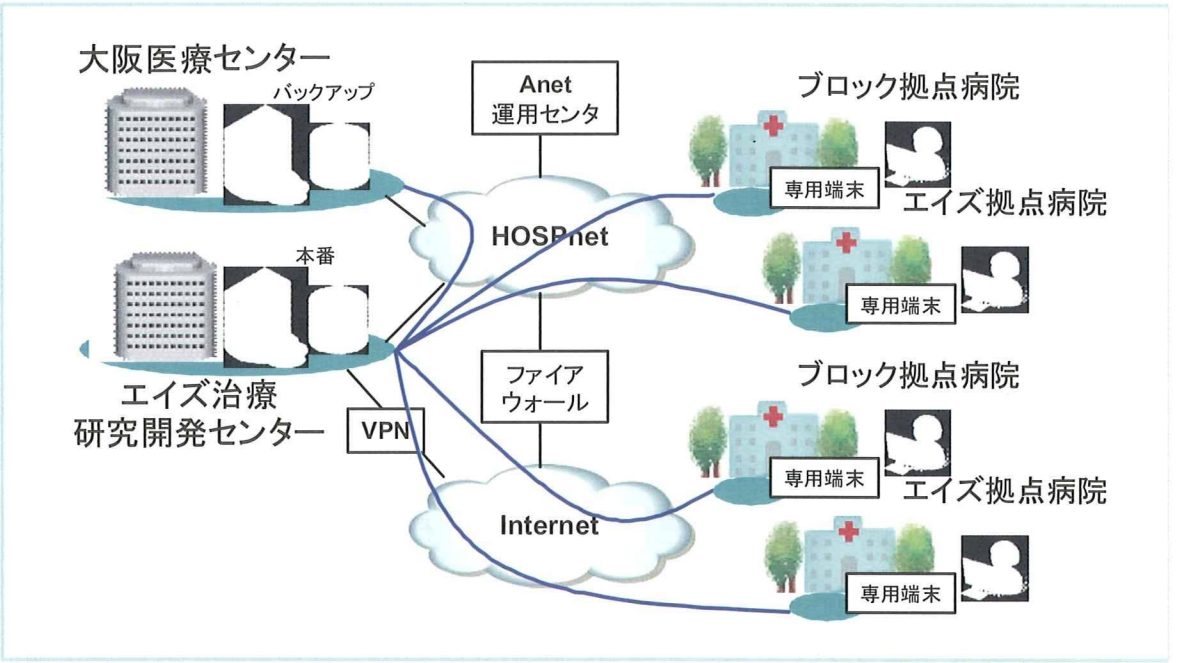

図 1.1 現状のサービスイメージ

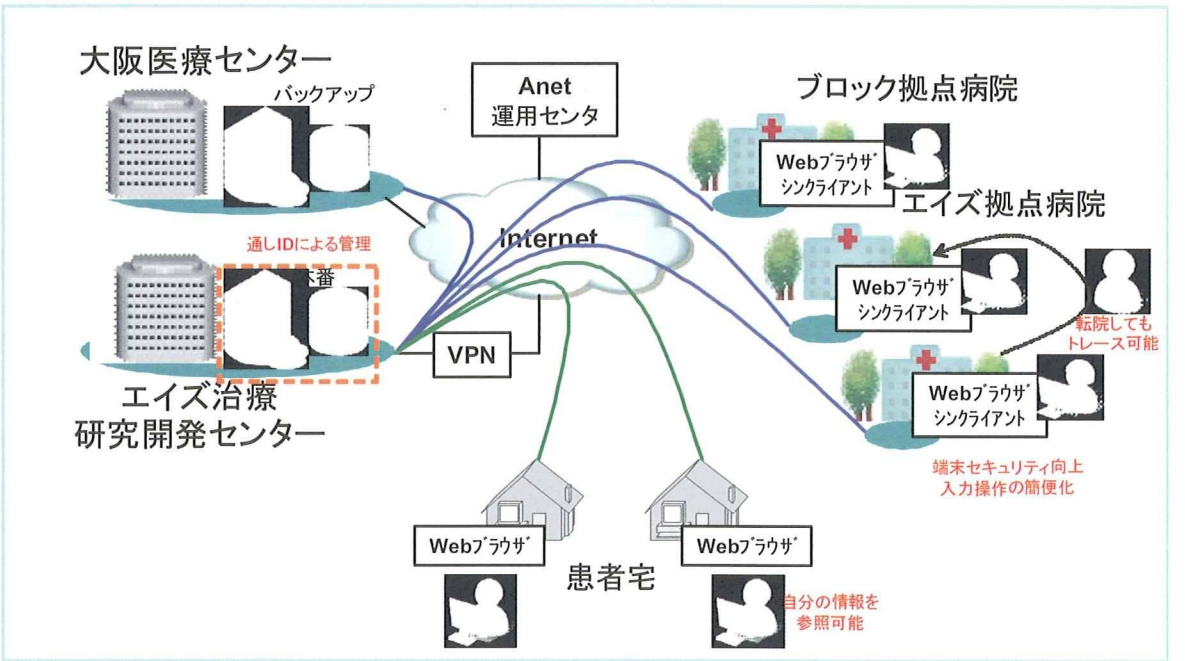

図 1.2 将来のサービスイメージ

第2章 本研究の概要

2.1 実行方針

今後の A-net の目指す姿を見定めるため、今年度は以下の取り組みを行う。

(1) 手持ちデータを収集し、一元的な管理を実施
・ 今年度の研究事業参加病院を対象に、データ収集作業を実施。研究事業参加病院からの手持ちデータは紙資料、様々な形式のファイル(MS-OFFICE 他)、独自 DB などを想定。
・ 診療情報は患者単位に、検査結果(CD4、ウイルス量)、エイズ発症の有無(日和見感染症の有る無し)、治療薬(種類と量)などの項目を時系列に並べたものとし、共通の形式に編集する。
・ AP 仕様を基にデータベースを構築し、収集／編集したデータを登録する。セキュリティ対策、研究での利活用など本番利用を見据え、DB 設計を行う

(2) 入力システムの改善
・ 入力負荷を軽減するよう、仕様を見直す。入力すべきデータ項目を選別し、入力操作を簡便化する。
・ 音声入力により、キーボード操作に不慣れでも入力可能とする。(試行)

(3) 上記内容の実施を前提に、セキュリティを担保
・ 入力システムの利便性を確保した上で、セキュリティを担保(現在の A-net のセキュリティレベルは少なくとも確保)
・ エンドポイント、ネットワーク、サーバのそれぞれで本番化を見据えたセキュリティ対策を実装する。
・ エンドポイントとなるクライアントとして、Web ブラウザに加え、シンクライアントを試行する。

2.2 実行内容

実行方針に従い、研究用のシステムを構築し、研究データの入力や各種試行を行う。

(1) 手持ちデータの収集、登録を行うためのデータベースシステムを構築
・各病院のデータを取り込むためのデータベースを開発
・各病院のデータを加工し、投入
・Web 端末からの内容参照や追加投入を行うアプリケーションを開発

(2) 入力システムの改善のため、音声入力など試行
・音声入力を試行
・入力項目を簡便化した Web 入力画面を開発

(3) セキュリティ対策の実施、各種技術の試行
・端末セキュリティ対策を促したパソコンを用意し、入力作業用に配布
・通信セキュリティ対策として、VPN 兼ファイアウォールを用意
・サーバセキュリティとして、認証や権限の制限を実装
・シンクライアント、端末用セキュリティツールを試行

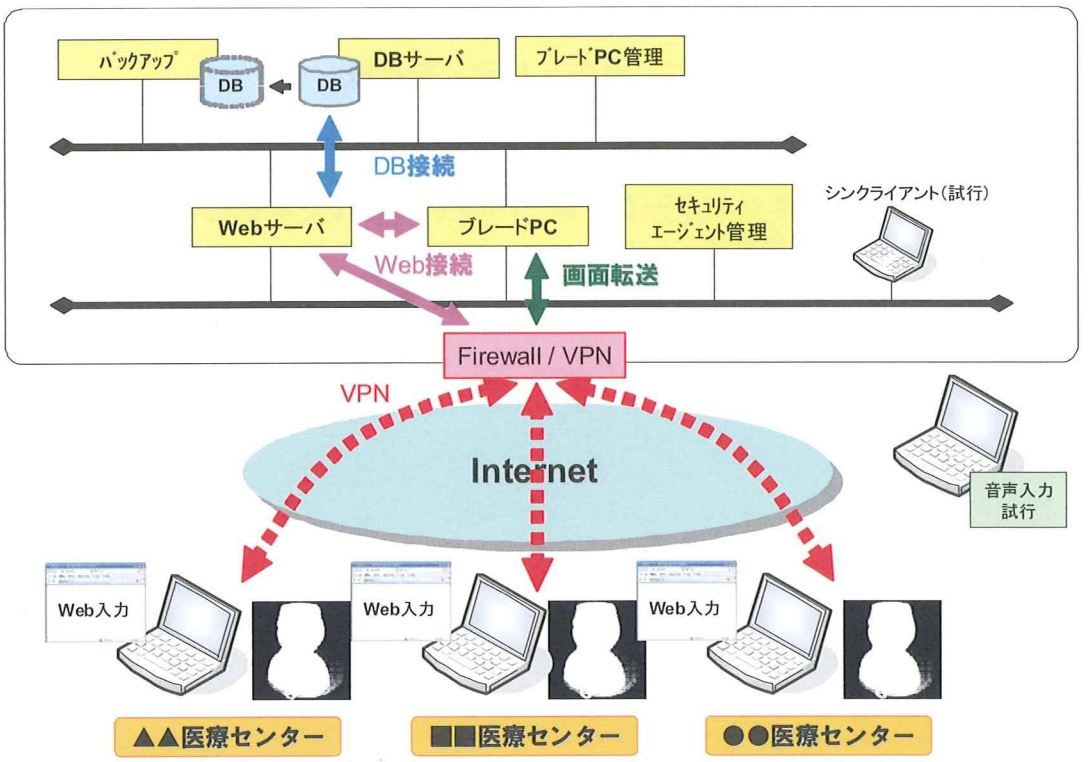

図 2.1 本研究のシステム構成イメージ

第3章 データベースシステムの構築

3.1 目的

各病院のデータを取り込むためのデータベースを開発する。患者の個人情報は持たせず、匿名による治療情報のみ登録する。研究用の情報として、CSV 形式で取り出し、活用できるようにする。

- 患者情報は匿名とし個人を特定できないようにする。
- 診療情報は患者単位に時系列に整理する。診療年月日、検査結果（CD4、VL）、医薬品の種類と量を登録可能とする。
- 初期登録は各病院のデータを加工し、センター側でまとめて DB に登録する。追加登録操作は病院単位に Web 画面から入力可能とする。
- 医薬品の種類の追加は柔軟に対応できるようにする。

3.2 システム概要

入力を簡便に行えるようにするため、入力画面数は極力少なくし、操作性を重視した。入力画面のイメージを図 3.1 に示す。

図 3.1 治療情報の入力および閲覧画面（管理者用）

各拠点病院に導入したクライアント PC より、VPN による暗号通信でファイアウォールを経由してサーバに接続する。サーバは Web サーバと DB サーバに分けており、治療情報を格納した DB サーバには直接アクセスできない構成とした。バックアップサーバより定期的に治療情報のバックアップを取得する。

後述のシンクライアント環境を介して利用することも可能である。

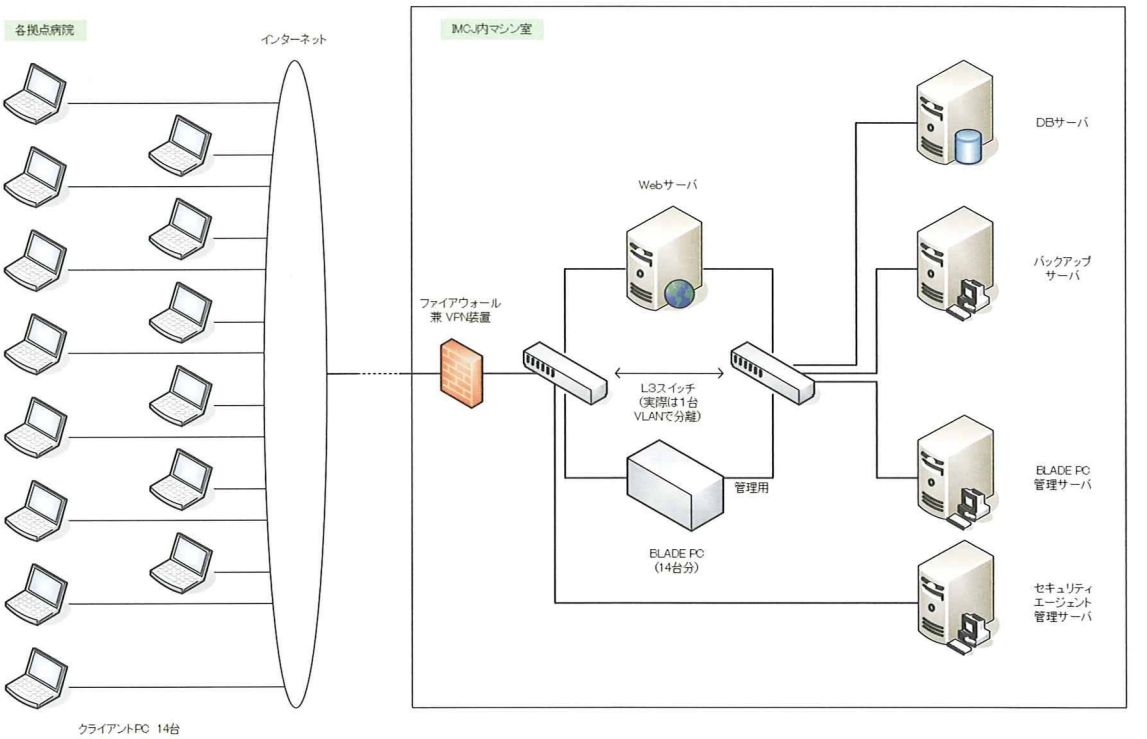

図 3.2 システム構成

図 3.3 マシン室内設置機器（各サーバ等）

3.3 システム詳細

長期的な運用に耐えうるよう、汎用性があり、かつ、先端的な技術を採用する。

(1) ソフトウェア構成

開発環境として、adobe Flex を採用した。Adobe Flex（アドビ・フレックス）は、リッチインターネットアプリケーションの統合開発環境と SDK である。デザインには MXML（Macromedia Flex Markup Language. Macromedia Flex のプレゼンテーションを記述するための XML 言語）を利用し、プログラムには ActionScript を利用している。簡単に言えば、Ajax と JavaScript を 1 つにパッケージングしたようなものである。

Web ブラウザ毎の実装の相違やバグ、挙動の差異に左右されずに動的ページを作ることが出来るため、Ajax よりも容易にクロスプラットフォームな環境での開発が出来る。

主要なミドルウェアとして、以下のものを採用した。
・HTTP ： Apache 2.2.3
・RDBMS ： PostgreSQL 8.3.5
・アプリケーションサーバ ： GlassFish 2

主要なアプリケーションとして、以下のものを採用した。
・JAVA VM ： Sun SDK 6 update11
・JDBC ドライバ ： PostgreSQL JDBC 8.3-603 (Type3)
・Apache-GlassFish 接続 ： proxy_ajp
・AP フレームワーク ： Seasar2 2.4.33
・Flex 連携 ： S2Flex2 1.1.1

ソフトウェア構成図及び連携図を次ページに示す。。

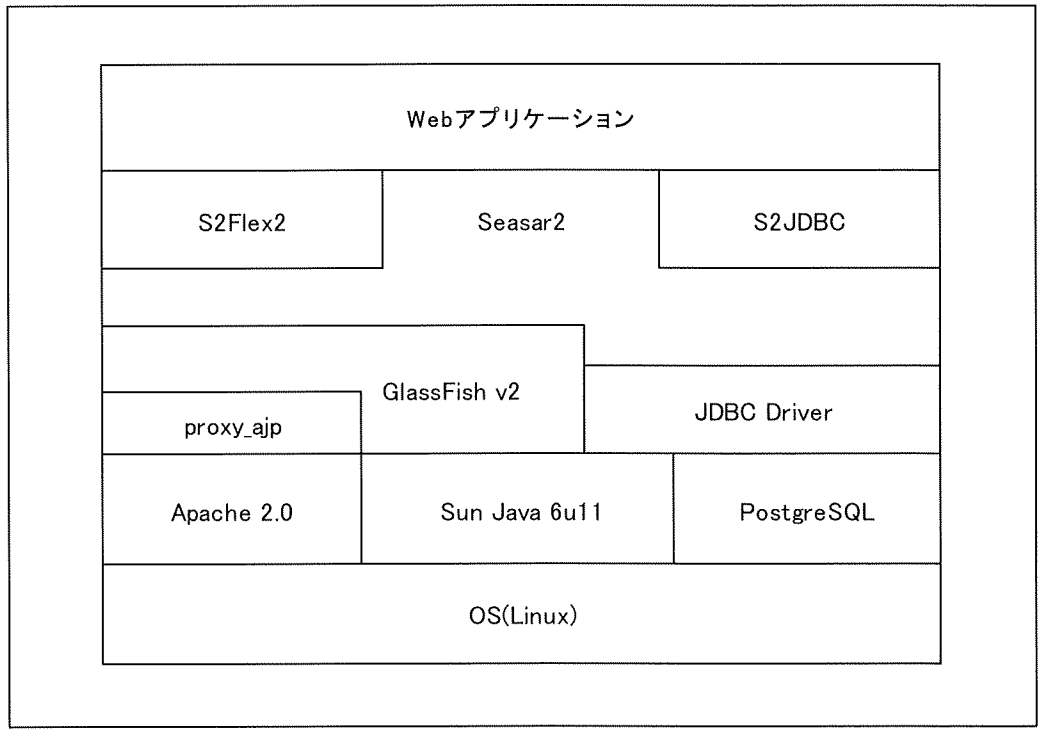

図 3.4 ソフトウェア構成図

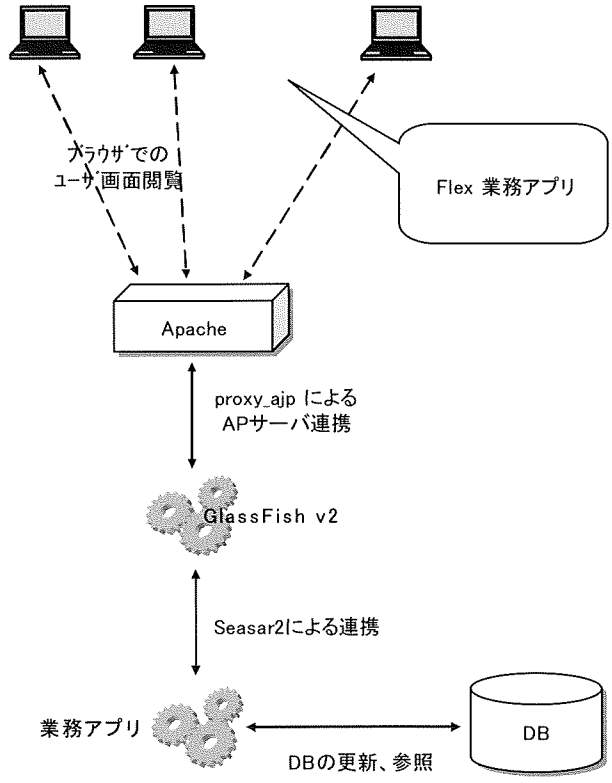

図 3.5 ソフトウェア連携図

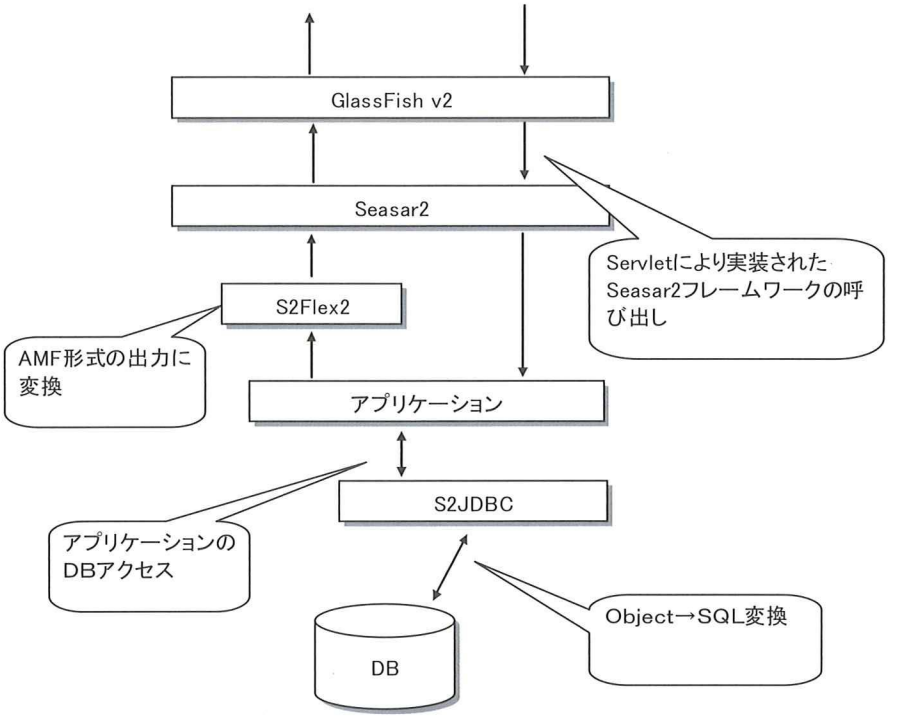

図 3.6 ライブラリの連携図

(2) データベース構成

登録拠点単位にデータベースを論理的に分割し、入力時に他拠点の情報にアクセスできないように制御可能とする。

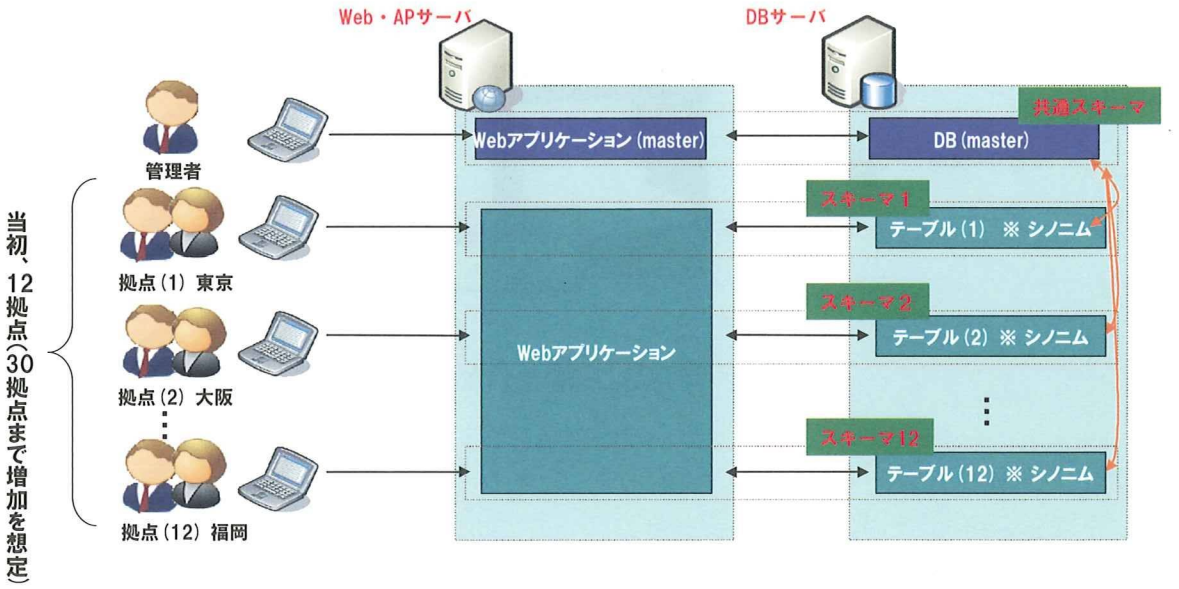

図 3.7 データベースの構成イメージ

第4章 入力システムの改善（音声入力の試行）

4.1 目的

データ入力作業の負荷を軽減するため、音声入力を試行する。

今回は医療分野でも実績の多い、アドバンストメディア社の電子カルテ向け音声認識ソフト 「AmiVoice Ex Clinic」を使用する。医療専門用語に対応した辞書を持ち、認識率を向上させている。

4.2 シンクライアントと音声入力の組み合わせ試験

通常のパソコンでの利用に加え、シンクライアントの利用もケースとして想定する。具体的なケースは以下の通り

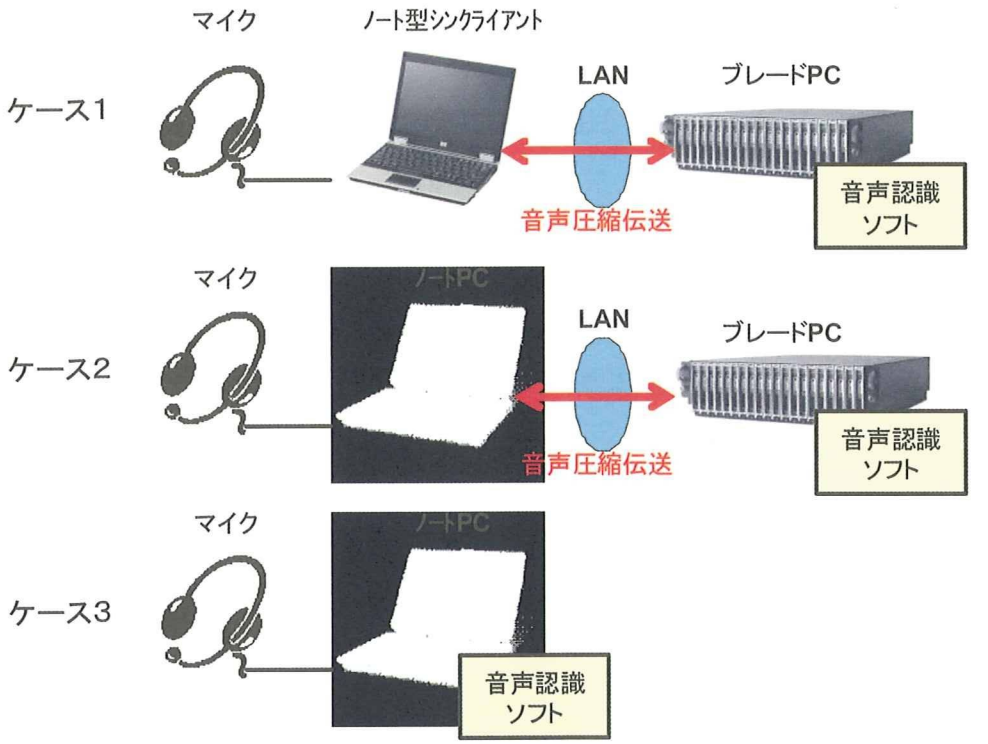

図 4.1 音声入力試験のケース別構成

No	テストケース	テスト結果
ｹｰｽ 1	ｼﾝｸﾗｲｱﾝﾄ＋ﾌﾞﾚｰﾄﾞ PC （音声入力ｿﾌﾄは ﾌﾞﾚｰﾄﾞ PC へ導入）	音声圧縮により、機械認識率が低下し、入力効率が悪い。実用には向かない。
ｹｰｽ 2	ﾉｰﾄ PC の RDP＋ﾌﾞﾚｰﾄﾞ PC （音声入力ｿﾌﾄは ﾌﾞﾚｰﾄﾞ PC へ導入）	ｼﾝｸﾗｲｱﾝﾄに比べ良いが、同様に認識率が悪く、実用に向かない。
ｹｰｽ 3	ﾉｰﾄ PC （音声入力ｿﾌﾄは そのまま PC へ導入）	入力音声をそのまま取り込むため、劣化が無く、最も認識率が良い。

結果として、ケース１のシンクライアント専用端末、ケース２の RDP ソフトによるシンクライアント接続ともに、音声認識ソフトは実用に足る認識精度を確保できなかった。LAN 経由で音声を伝送する際に、圧縮処理がされるため、音声品質が劣化することが原因と想定される。

音声認識を行う場合は、マイクを接続した PC ローカルで処理を行う必要がある。シンクライアントに比べ認識率は良かったが、チューニングなしの状態では認識率も低く不十分であった。

前述の今回開発した入力システムは音声入力に対する特別な処理を組み込んでいない。入力項目に応じて認識内容を制限（例えば年月日、薬の種類など）するなどの作りこみにより、認識率を向上させることが可能と考える。

第5章 セキュリティ対策

5.1 目的

「利便性の向上」の実現のために、どこからでもアクセス可能なインターネットの利用や市販されている端末に搭載されている Web ブラウザの使用を想定している。それらを利用する際には、不正アクセスや情報漏洩等の様々な脅威やリスクが存在するため、適切にセキュリティ対策を実施する必要がある。

5.2 実施内容

セキュリティを確保するために、エンドポイント・ネットワーク・サーバという 3 つの視点でセキュリティ対策を検討し実施した。

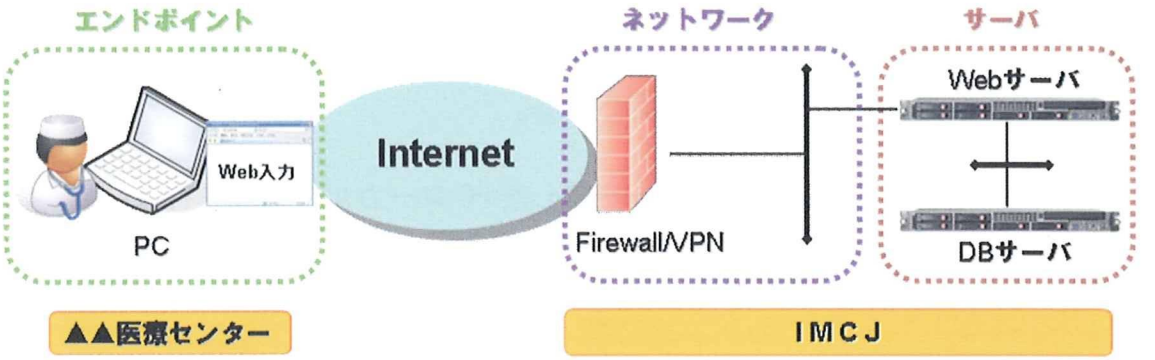

図 5.1 セキュリティ対策の実施ポイント

(1) エンドポイントセキュリティ

ア 想定脅威

インターネットや Web ブラウザの使用時に、下記の脅威が存在すると想定した。

・Web の閲覧や USB メモリ等を経由したコンピュータウイルス感染
・端末への侵入やデータの改ざん
・端末の紛失や盗難

イ 実施内容

上記の脅威に対処するため、下記の 4 つの対応策を実施した。

・アンチウイルス　　：ウィルスの感染防止
・セキュリティエージェント　：不正ソフトの動作抑止
・ハードディスクの暗号化　　：盗難等による情報漏えい防止
・シンクライアント端末　　：盗難等による情報漏えい防止

セキュリティエージェントは、セキュリティホールを利用した攻撃手法やウイルス・ワームの感染手法に着目し、ゼロデイ攻撃等を防御する機能を有している。また、ファイルの書換え等を検知する機能についても有している。そのため、セキュリティエージェントとアンチウイルスを併用することで、お互いを補完しながら、よりセキュリティを高めることが可能である。

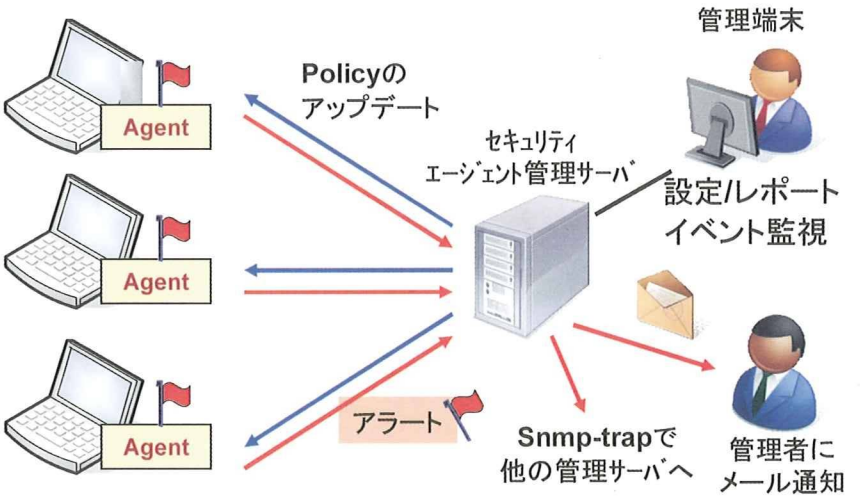

図 5.2 セキュリティエージェントによる対策イメージ

パソコンのハードディスク全体を暗号化することにより、盗難や紛失の際の情報漏洩を防止する。PC のハードディスクのデータ領域だけでなく OS などのシステム領域を含め、ハードディスク全体を自動的に暗号化する方式を採用する。データの暗号化・復号化は透過的に行われるのでユーザは暗号化を意識せず利用可能となる。

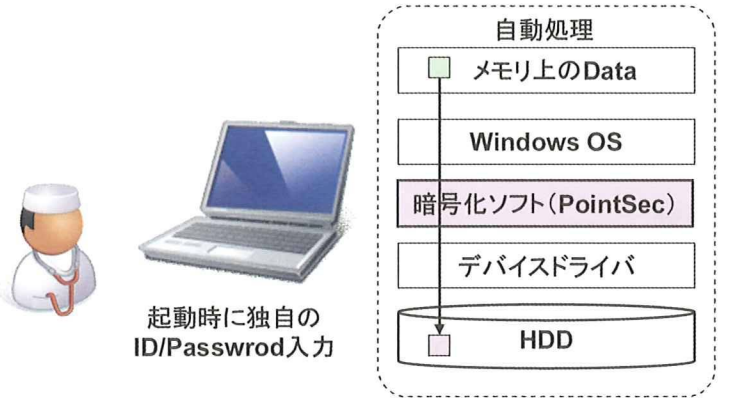

図 5.3 ハードディスク暗号化による対策イメージ

シンクライアントについては、端末上にデータを残さない仕組みのため、端末が盗難された場合でも、情報漏洩のリスクを大幅に低減できる。

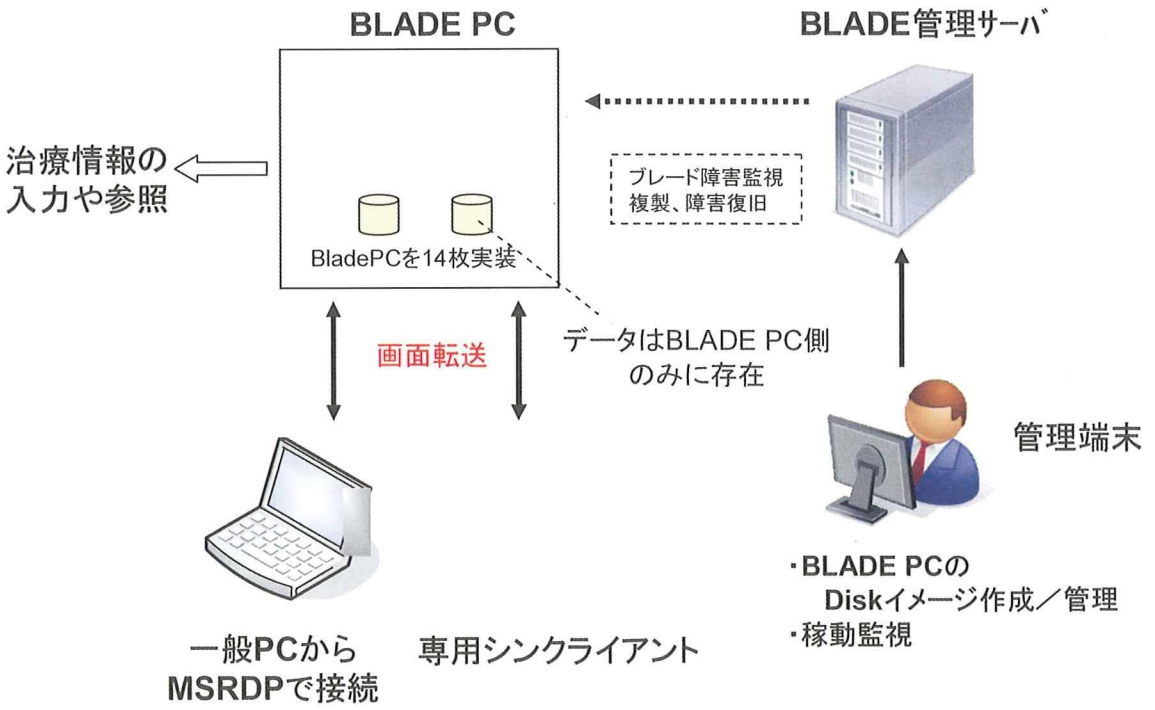

図 5.4 シンクライアントの利用イメージ

(2) ネットワークセキュリティ

ア 想定脅威

インターネットを経由した通信時に、下記の脅威が存在すると想定した。

・不正アクセス
・通信の盗聴・改ざん
・端末のなりすまし

イ 実施内容

上記の脅威に対処するため、下記の 2 つの対応策を実施した。

・ファイアウォール
・VPN(Virtual Private Network:仮想私設網)

今回はファイアウォールと VPN を 1 台の装置で実装した。

VPN については、インターネットなどの公のネットワーク上で暗号化を実施し、通信の盗聴・改ざんを防止するために利用した。

VPN のしくみとして IPsec と SSL-VPN が広く普及しており、今回は、SSL-VPN では事前にソフトウェアの配布が不要なことと、利用環境に依っては IPsec が利用できない可能性があったことの理由により SSL-VPN を採用した。端末側にソフトウェアを追加導入すれば IPsec にも対応可能である。

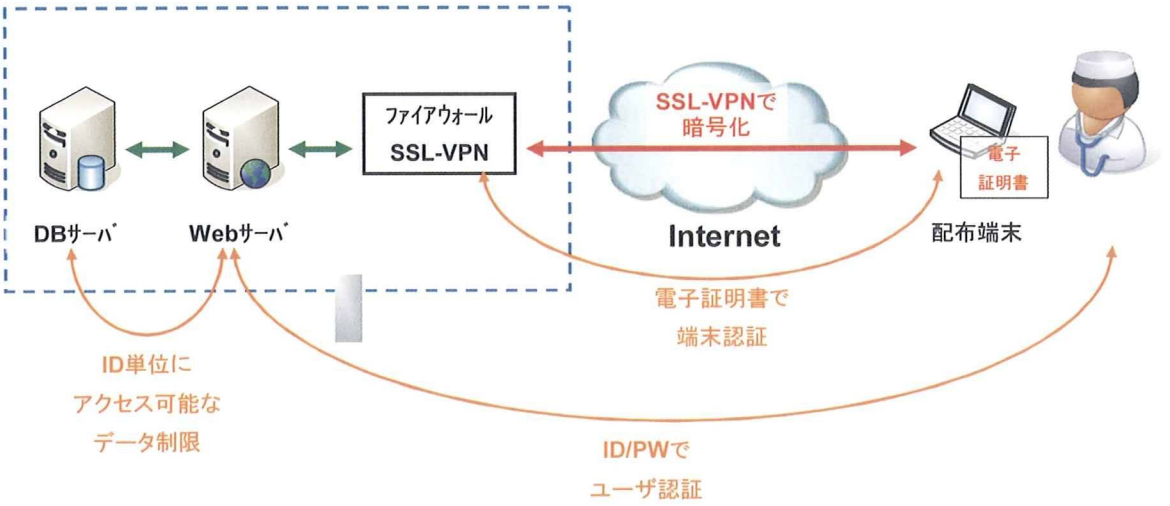

図 5.5 SSl-VPN 経由での AP 利用イメージ

VPN 接続時の認証では、端末認証とユーザ認証を行うことでなりすましを防止した。端末認証は PC 毎に発行した電子証明書（クライアント証明書）を用いて行い、更に ID／パスワードによるユーザ認証を行っている。

なお、今回は研究目的のため、電子証明書はプライベート証明書（無償）を使用した。利用対象者を広げる場合、パブリック証明書（有償）を使用することが望ましい。

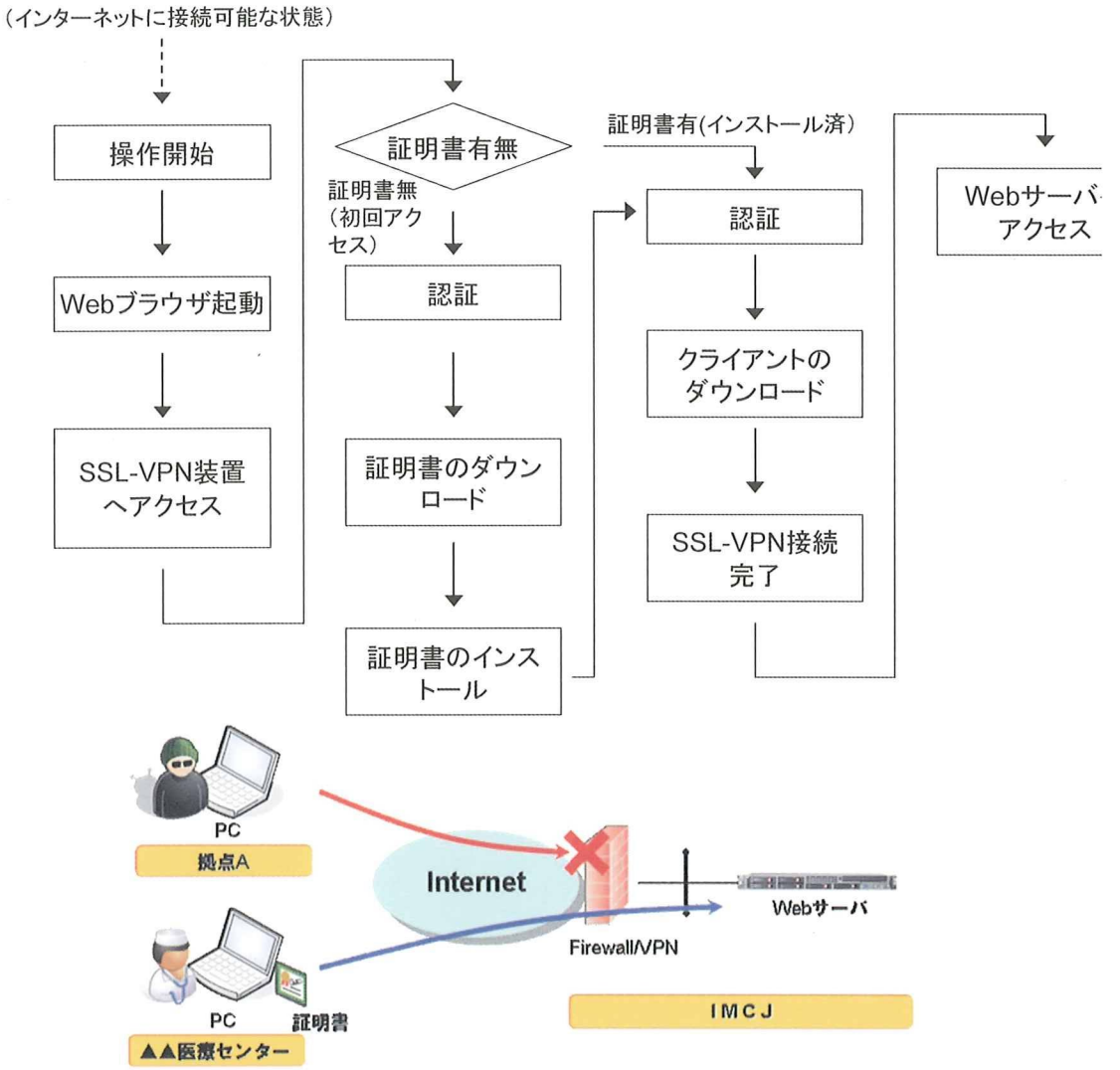

図 5.6 証明書を使用した端末認証フローとイメージ

(3) サーバセキュリティ

ア 想定脅威

クライアントへのサービス提供時に、下記の脅威が存在すると想定した。

・他のサーバや端末経由のウイルス感染
・サーバ・システムへの侵入
・データの改ざん・消失

イ 実施内容

上記の脅威に対処するため、下記の 4 つの対応策を実施した。

・アンチウイルス
・ユーザ認証／テーブル分離／アクセス管理
・フィルタリング
・ログのアーカイブ

ＤＢ上のテーブルは拠点病院単位に作成し、ユーザＩＤを対応したアクセス制限を行っている。入力の際に他の病院の患者情報や治療情報を参照できないように配慮した。

第6章 まとめ

6.1 結果総括

現行の A-net と同等以上のセキュリティ機能を備えた、HospNet を介さない、一般のインターネット環境の中での、診療支援ネットワークの構築を試みた。「セキュリティの確保」は必須条件で、さらに「利便性の向上」と「運用管理の向上」を初年度の最終目標と見据えて、ネットワークを構築した。各病院で運用されている様々なオーダリングや電子カルテから、一律にデータを拾い上げることは、当班研究の規模では無理であり、ノート PC にセキュリティを強固にした仕組みを予め組み込み、臨床現場から、セキュリティの高い通信手段を用いて、データを集約するシステムを構築した。また、シンクライアント環境およびセキュリティエージェントは、今回のシステムと組み合わせて利用できることは確認でき、セキュリティ対策については、最新技術の活用により、強化を図ることはできた。しかし、パスワードの繰り返し入力が必要になるなど、使い勝手の点で改良の余地が残った。

病院の診療システムから直接必要なデータを抜き出す技術は現段階では応用できていないため、手入力の手間を出来るだけ少なくしたいと考えたが、打ち込んだあとの処理速度が、現行の A-net と比較して飛躍的に改善したが、この提案では、多数の患者が集中する診療拠点病院での継続的な運用は成り立たないこととなり、現行の A-net と同様の運命をたどる心配は払拭できなかった。

入力システムの改善のために、音声入力の試行を行ったが、シンクライアントなどセキュリティ対策との相性は悪く、すぐに実用できる状態ではなかった。

6.2 今後の課題

今回データベースシステムの構築および入力ソフトの開発により、継続入力が可能な環境は確保できた。しかし、大量の入力が必要な病院では Web 画面から患者単位の診療情報を入力する負荷が高い。

継続性のある患者参加型のネットワークを目指し、電子カルテとの自動連携などにより、無理なく情報の蓄積を図れるようにしたい。

現在研究データは CSV 出力後、Excel などで統計処理をしているが、より本格的な統計処理を行うためのツール導入や定型的なグラフ出力など利活用のための機能を充実させたい。

音声入力を本格的に取り込むには、入力システムの大幅な改修も必要になるため、検討が必要である。

セキュリティに関しては、使い勝手とのバランスを考えた改善（例えばシン