2005年度(平成17年度) 慶應義塾大学 政策・メディア研究科 修士論文

インターネットを用いた個人を中心とした生体情報共有機構の構築に関する研究

慶應義塾大学大学院 政策・メディア研究科

橋本和樹

kazuponi@sfc.keio.ac.jp

修士論文要旨 2005 年度 (平成 17 年度)

インターネットを用いた個人を中心とした生体情報共有機構の構築に関する研究

-論文要旨-

本研究では、トレーニング・ジムや家庭で計測された生体情報を、健康管理のために、専門家やその他の個人と、インターネットを介して共有するための新しいモデルを提案した。このモデルでは、ユーザを中心とした、一貫性のある形での情報共有が可能である。また、このモデルに基づいたプロトタイプ・システムの構築も行った。

現在、成人病予防に対する関心の高まりや QOL の向上にともなって、人々の健康管理に対する意識が高まっている。医療機関やトレーニング・ジムなどの多くの場所では、健康管理や運動指導などが行われている。このような活動の内容は、血圧計や体重計などのバイタル・センサを用いて取得される、参加者の生体情報に基づいて決定されている。しかし、このような生体情報は、健康指導などを行っている各組織が個別に管理しているため、異なった組織によって企画されている複数の活動に参加しているユーザの場合、そのユーザ自身の生体情報を、一貫性のある形で利用できない。生体情報を一元的に管理し、健康管理の専門家や友人などとの情報共有を可能にすることができる情報共有モデルを提案することが、本研究の目的である。

このようなモデルの実現に当たっては、生体情報の所有権を、各組織から個人へと移行する必要がある。また、インターネット上での生体情報の共有に当たっては、以下の 2 点について考慮する必要がある。 1 点は、透過的なアクセスを実現すること、 2 点目は、ユーザが望む形で情報へのアクセスを制御できるようにすることである。本研究では、特に後者について重要だと考える。インターネット上で生体情報を共有する場合、期待しないアクセスを制限するために、誰と情報を共有するかといったことを制御できることが重要である。本研究では、このようなモデルを提案し、プロトタイプ・システム Biological Information Sharing System (BISS) の設計と実装を行った。

最後に、プロトタイプ・システムの動作検証を行い、期待通りの動作をすることを確認した。また、システムの定性的評価を行い、本研究によって一貫した健康管理が可能となることを確認した。本研究では、一貫性のある生体情報共有のためのモデルを提案し、プロトタイプ・システムを実装することで、モデルの有効性を示すことができた。

キーワード

1: 健康管理　2: 生体情報　3: 時系列データ
4: 生体情報共有機構　5: アクセスコントロール

慶應義塾大学 政策・メディア研究科
橋本和樹

Abstract of Master's Thesis Academic Year 2005

Research on Building a User-Centered Biological Information Sharing System on the Internet

- Summary -

This research proposes a new model to share biological information, which is obtained at training gyms and home for health management purposes, with health-care specialists and other individuals through the Internet. This model allows the information sharing to be user-oriented and in a consistent manner. A prototype system based on this model was developed through this research as well.

Today, there is increasing interest in health-care in the society for different purposes such as prevention of life-style related diseases and improvement in quality-of-life. Programs for health management and physical training are conducted in various locations including medical and training facilities. Such programs are based on biological information of the participants obtained by vital sensors, such as blood pressure monitor, weighing scale, and so on. Within the services provided today, however, such information belongs to each organization managing the program. Therefore, a participant cannot make use of the information consistently if he/she joins multiple programs conducted by different organizations. The purpose of this research is to propose an information sharing model to manage biological information in a unified manner, and to enable the users to share the information with other individuals, such as health-care specialists and friends.

The biological information must be owned by each individual instead of organizations in order to accomplish such a model. In addition, two issues must be taken into consideration to achieve biological information sharing on the Internet. The first issue is to insure a transparent access to the information, while the other issue is to enable users to control the access to such information according to their preference. The latter is considered to be particularly important in this research. It is essential to be able to control whom the information is shared with when making it available on the Internet as biological information needs to be protected from unexpected access. This research proposes such a model with a design and implementation of prototype system called the Biological Information Sharing System (BISS).

Finally, operation and the quality of the prototype implementation were evaluated and the system was verified to operate as expected. This proved the contribution of this research for consistent health management. In this research, a new model for consistent sharing of biological information was established, with a prototype implementation which demonstrates the validity of the model.

Keywords

1 Healthcare 2 Biological Information 3 Time Series Data
4 Biological Information Sharing System 5 Access Control

Keio University Graduate University of Media and Governance
Kazuki Hashimoto

目 次

図 目 次

表 目 次

第1章　序論

1.1　はじめに

近年、健康管理に対する関心が高まっている。今日の社会では、運動不足や食生活の偏りに起因する生活習慣病の増加や、進む高齢化などの影響で、人々の健康に対する不安は増大している。医療の分野においては、今までの早期発見・早期治療という”二次予防”だけではなく、疾病予防や健康増進という”一次予防”にも注目が集まっている。また、日本においては健康日本 21 [1] や健康増進法など、国策として健康に対する施策や方針が掲げてられている。健康増進法では、住民や地域主導によるヘルスプロモーションが求められ、様々な地域で健康を支援する地域コミュニティの形成や、自治体などによる健康増進を支援する活動が行われている。図 1.1は 2001 年にお客様生活文化研究所によって行われた調査であるが、健康に関心を持っているという回答は全体の 89%にも上っている [2]。

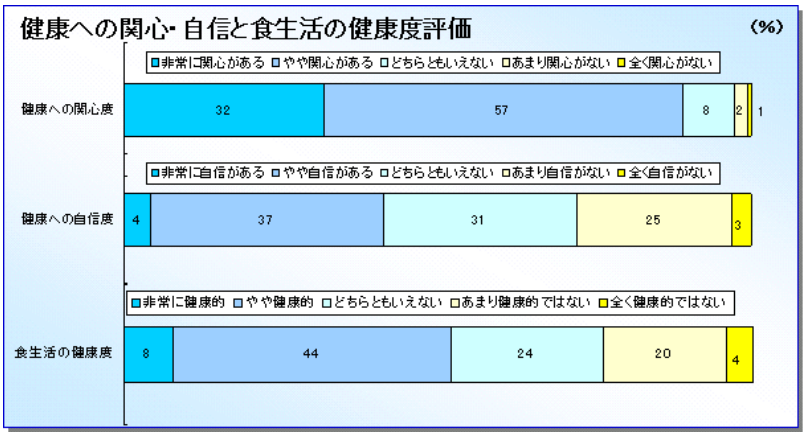

図 1.1: 健康意識の調査（2001 年度：母数 1000 人）

WHO によると、健康は「単に病気あるいは虚弱でないというだけでなく、肉体的、精神的、社会的に完全に良好な状態を指す」と定義されている。その中でも肉体的な健康状態を維持、増進するために必要な事は、自らの健康状態を把握し、健康状態をよくするための活動、行動に取り組むことであるとされている。

人間の身体の状態を把握するために、バイタルセンサ（体重計、血圧計など）がある。バイタルセンサとは、医療機関で使うような MRI や CT などの専門機器から家庭内で使用する体重計や体温計までを含む。健康状態を把握するためには継続的にバイタルセンサで計測した情報を記録していくことが重要である。これは、2003 年に日本で施行された健康増進法の中の健康診査に関わる指針の中でも述べられている。以下に、その内容を示す。

(健康診査の実施等に関する指針)

> **健康増進法**　2002 年 8 月 2 日公布、2003 年 5 月 1 日施行
>
> **第九条**　厚生労働大臣は、生涯にわたる国民の健康の増進に向けた自主的な努力を促進するため、健康診査の実施及びその結果の通知、健康手帳（自らの健康管理のために必要な事項を記載する手帳をいう。）の交付その他の措置に関し、健康増進事業実施者に対する健康診査の実施等に関する指針（以下「健康診査等指針」という。）を定めるものとする。

現在では、多種多様なバイタルセンサが様々な場所に存在する。これまでは、家庭では体重計や血圧計を使った測定しかできなかった。近年ではこれに加え、血糖値や心電図など、以前は専門機関でしか測定できなかったものまで、家庭で測定できるようになった。また、トレーニングジムなどでは、トレーニング機器からの情報を運動指導に活用している。さらには、プロのスポーツ選手のトレーニングなどのために、独自の専門的なセンサを使う研究 [3] なども盛んに行われている。

一方で、家庭用バイタルセンサのデータを計算機上で管理し、インターネットを通して健康管理やトレーニング指導を行う取り組みも増えている [4][5][6]。歩数計や家庭用自転車エルゴメータ、体組成計などから取得できるデータは、ユーザの PC 上で管理し、インターネット上で共有することができる。これにより、トレーニング指導や健康管理などを遠隔から行う事ができる。これまで、機器ベンダーやスポーツジムなどにより、生体情報を計算機上で扱い共有する機構は実現されてきた。しかし、まだサービス事業者や機関が限定されており、利用に制約があるのが現状である。

元来、生体情報とは、ユーザ自身の情報であるため、個人の管理が想定される。しかし近年では、時間の経過とともに情報量が増加するため、生体情報を個人が管理することは難しい。そこで、ユーザの所属する機関、使う機器のメーカーおよびサービス事業者が、生体情報の管理サービスを提供していた。また、インターネットを用いる際も、セキュリティやユーザ管理などといったコストの高い要求がある。そのため、既存のサービスを統合して行う事は難しかった。そこで、現状では情報を各機関が独自に管理しており、ユーザの生体情報自体が散在している。この結果、ユーザの生体情報を一元的に利用したサービス（健康管理、トレーニング指導）の実現は困難である。

1.2　研究目的

本研究では、インターネットを介した一元的な生体情報の管理機構を実現する。生体情報の所有を個人を主体に行い、場所や機関による制約を受けない健康管理及び生体情報の共有を行うことが目的である。生体情報をインターネット上で共有する際の問題点を把握し、それらの問題点を解決するモデルの提案と、そのモデルに基づく共有機構の実現を行う。本機構を用いる事により、場所や時間などの制約を取り除き、専門家と生体情報を共有した上で健康診断や、運動指導を行える。また、友人やコミュニティ上で生体情報を共有する事で、コミュニティの形成などの生体情報の二次利用が可能となる。

1.3　本論文の構成

本論文は本章に続く以下の 7 章で構成される。第 2 章では、本研究における生体情報共有機構の詳細、また本研究で実現する環境について述べる。第 3 章では、生体情報の共有に関わる関連研究について調査、分析を行い、現状の問題点に関してまとめる。第 4 章では、生体情報の取り扱いにおいて考慮すべき事項に関して述べる。第 5 章では、本研究で提案する機構の設計を述べる。第 6 章では、本機構の実装上の問題に関して述べる。第 7 章では、実現した機構の検証、評価を述べる。第 8 章では、結論を述べ本論文のまとめとする。

第2章　生体情報共有機構

2.1　概要

本研究で定義する**生体情報**とは、身体より取得される情報、またその属性情報を併せた情報を指す。つまり、体重や血圧といった時間の経過に伴って変化する身体から測定される値と、機器独自情報や測定単位などを含めた情報である。さらに、万歩計や自転車エルゴメータなどのトレーニング情報も含める。ここには、電子カルテなどやトレーニングカルテなどの専門家の処方やコメント等は含めない。また、指紋や静脈パターンなど変化しない情報は本研究の生体情報の範囲外とする。つまり、生体情報とは、健康管理などの目的のために利用する、時間の経過とともに変化する情報群と定義する。また、生体情報を計測するセンサの事を以降バイタルセンサと呼ぶ。

生体情報共有機構とは、ユーザ（生体情報を取得される人）がバイタルセンサで測定した生体情報を、情報通信基盤を用いて収集、利用する機構を指す。その上では、利便性が高く、効果的な健康管理、運動指導ができる。具体的には、身体より取得できる体重や血圧、トレーニングなどの情報を、ネットワーク上で一元的に共有できる。これは、個人が情報の所有者となることで実現される。一元的に共有された体重などの情報は、健康管理や運動指導などに利用する際に有用である。

図 2.1に生体情報共有機構の概念図を示す。図 2.1中の左下のユーザは、センサを用いて自らの生体情報を収集する。センサによって取得された生体情報は、ネットワーク上に蓄積される。ユーザはその情報を、望ましい専門家に適切に開示し、その情報を元にコミュニケーションを行う。ここで言うコミュニケーションとは、自らの体重やトレーニングの情報を使った、ダイエットサービスや医師等における診断などを指す。

また、近年、バイタルセンサを用いる機関や場所などで、インターネットを利用できる環境が整ってきた。生体情報共有機構の情報通信基盤としてインターネットを用いることで、既存の情報処理システムを生体情報の共有に使うことができる。また、インターネットを利用することにより、世界規模で利用できるシステムとなる。そのため、生体情報を様々な場所で共有でき、それを利用して容易にコミュニケーションできるようになる。

2.2　機能

生体情報共有機構に必要な処理を以下の三つに分類する。*1)* センサなどを使って、人の身体より生体情報を収集する。*2)* その生体情報をネットワーク上に蓄積していく。*3)* その上で、ユーザが生体情報を利用し、専門家とのコミュニケーションを行う。以降、生体情報共有機構実現のため、分類した三つの処理を実現する機能を明確に定義し、要件を整理する。

1. **生体情報の収集**

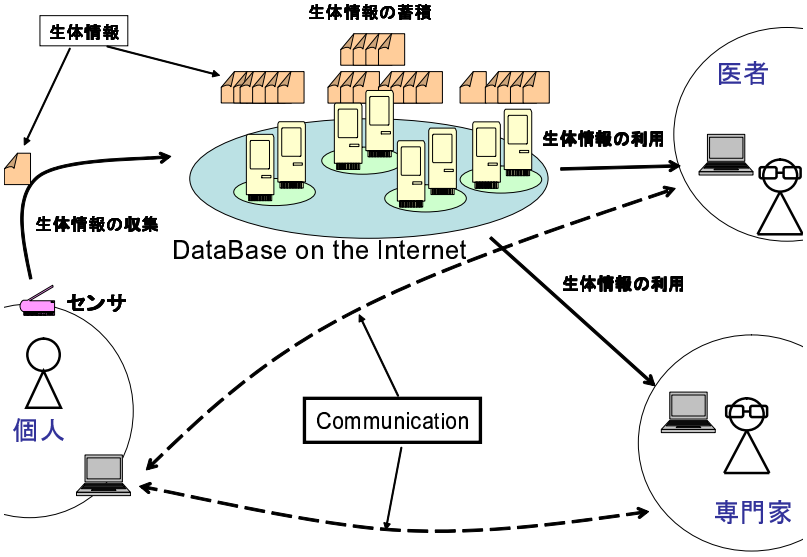

図 2.1: 生体情報共有概要

生体情報をネットワーク上で共有するために、まず生体の情報をバイタルセンサを用いて計測する必要がある。計測した情報の所有者を特定し、生体情報を収集していく。また、計測した情報がどういったデータであるか、生体情報に付随した属性情報というものも必要となる。つまり、バイタルセンサで取得した情報の所有者となる個人を特定し、その生体情報を蓄積機構に送信するために情報を加工、整形しなければならない。

2. **生体情報の蓄積**

   生体情報を蓄積するための機能として、以下の要件が満たされなければならない。まず、各々のユーザのデータが別々に保存できる。次に、時間の経過とともに増加するデータの完全性が保証できる。さらに、時間と共に増加し続けるデータを、人の一生涯サポートできる程の長期間保存できる必要がある。加えて、データの取得、編集などをサポートする蓄積機構であることが必要である。

3. **生体情報の利用**

   蓄積された情報を適切な相手に開示できなければならない。ユーザの望む情報の開示ポリシに併せ、生体情報の開示の可否判断後、適切な相手のみへ開示できる機能が必要である。後にも述べるが、自らの情報の閲覧や、専門家へ開示すること、また適切な相手以外には見せないことが実現できるべきである。

   また、実際に蓄積された情報に対して許可された権限でアクセスする際には、アクセス制御のインターフェースが定義されている必要がある。

これらの三つの機能は、各機関が他の機関が提供する機能を利用可能なように、つまりインターネットを介して組み合わせることができるように実現する。これにより、ネットワー

ク上で様々な生体情報の利用または生体情報の収集が可能となる。その結果、サービス事業者やジム等の機関も本機構を使うことができ、ユーザの利便性が向上する。

以後、これら生体情報共有機構内の三つの処理手順をそれぞれ、収集フェーズ、蓄積フェーズ、利用フェーズと呼ぶ。

2.3　本研究が実現する環境

2.3.1　既存サービス

既存サービスでは、収集、蓄積、利用の機能をそれぞれが勝手に実現している。つまり、各組織やサービス事業者が、バイタルセンサからの情報だけを使って、健康管理や運動コミュニティなどの生成を行っている。健康管理や運動コミュニティの事をサービスと呼ぶ。図 2.2に既存サービスのモデル図を示す。各運動指導や健康管理などのサービスのために、センサ収集から利用までの単一システムをサービス事業者が用意している。

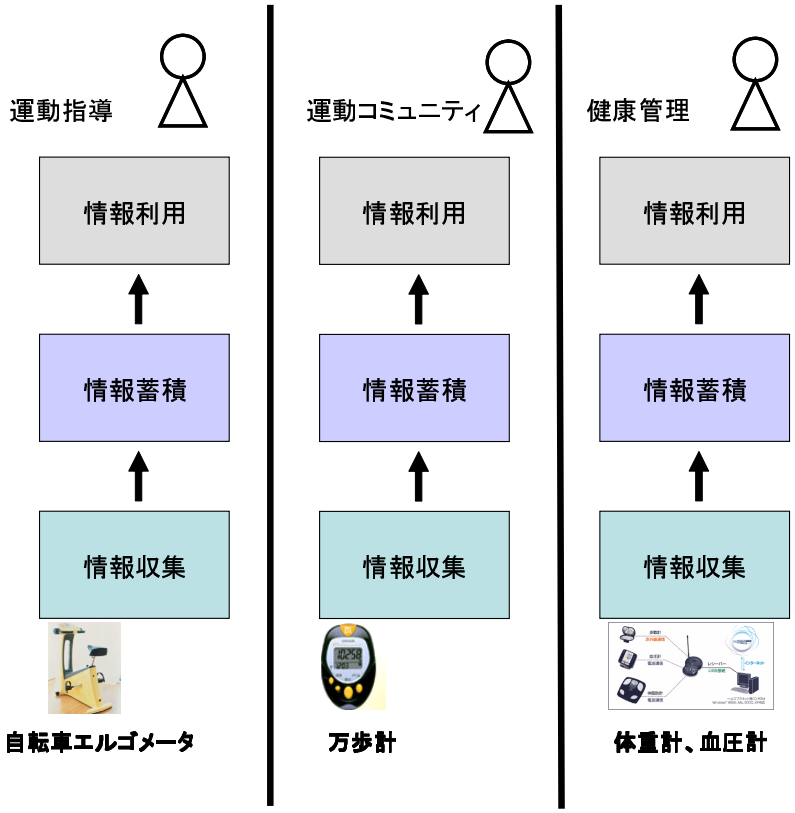

図 2.2: 既存サービス

運動指導や健康管理など、サービスごとに 1 つのシステムが存在するため、複数の問題がある。そのうちの一つとして、他サービスで使えるはずの情報でもそのサービスでしか共有できないという問題が挙げられる。また、同じ情報を扱えるシステムでも、同じ生体情報アプリケーションが利用できなければ、ユーザの利便性は向上しない。さらに、既に他のサービスを受けているユーザにとっては、他のサービスを使う事で、ユーザの生体情報が分断さ

れ、統一的な健康管理などが行えないという問題がある。つまり、健康管理や運動指導などそれぞれの生体情報アプリケーションごとに生体情報を管理しているため、収集される情報、利用できる情報、収集・利用の手法がばらばらになってしまっている。

2.3.2　提案モデル

図 2.3に、本研究の目指す個人を中心とした一貫性のあるモデルを示す。本研究では、バイタルセンサから取得された生体情報が最終的にサービスとして利用されるまでの間で、生体情報を統一的に扱う事によって、個人の全ての生体情報が利用できるモデルを提案する。既存の生体情報サービス利用の際に統一的なアクセスを行う事によって、インターネット上のどこからでも一貫した方法で個人の生体情報を収集できる。各機能が独立して存在し生体情報を透過的に扱う事で、サービスに依存せず、組織や機関等に依存しない生体情報共有が可能となる。つまり、サービス間での生体情報の分断をなくし、生体情報を使った様々なサービスをユーザが受ける事ができる機構を構築する。

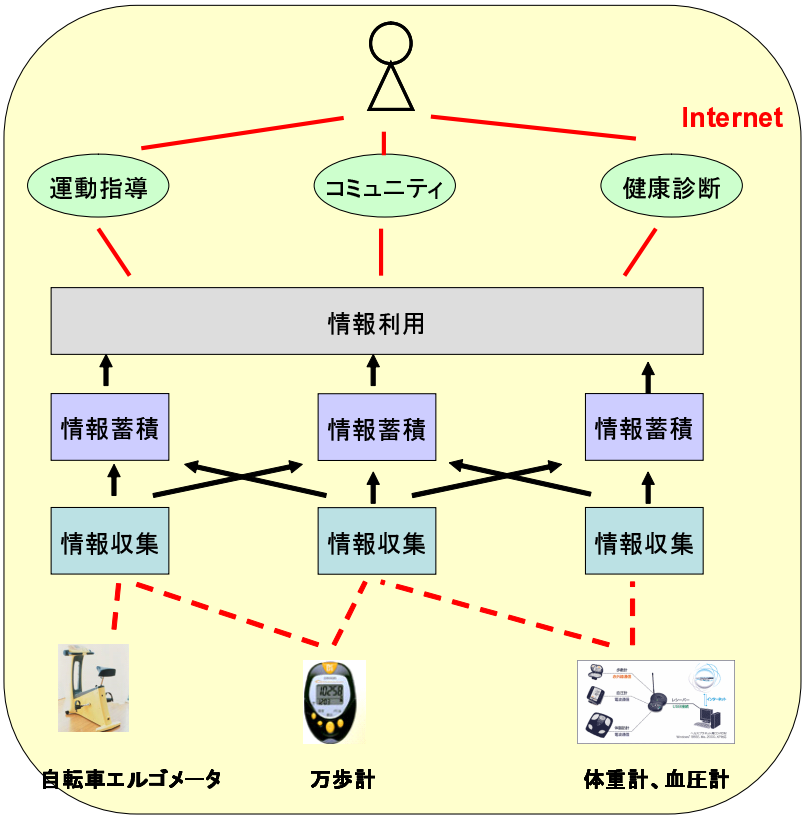

図 2.3: 本研究の目指すモデル

2.3.3　提案モデルの利用例

本研究の目指すモデルの利用例を示す。例えば、バイタルセンサとして歩数計やエルゴメータ、また体重計などを使うケースを考える。友人とは運動量を競っていて万歩計の歩数やエ

ルゴメータの回転数、時間などのデータを共有している。しかしトライアスリートでもあるため、スポーツトレーナーからは有酸素運動トレーニングの指導を受けていて、トレーナーとは心拍数の情報も共有している。さらに、糖尿病にもなりかけているので、栄養士とはカロリーコントロールのために歩数計、エルゴメータの消費カロリーを共有している。本研究ではそのような生体情報を共有した上で、様々なアプリケーションを用途別に利用する事を想定している。そのため一貫性があり、個人が所有権を持ったアクセス制御が必要となる。

2.4　実現のための課題

生体情報共有機構を実現するための要素技術として、上記の三つの機能を実現する様々な研究が行われている。収集フェーズでは、生体情報、健康情報の交換フォーマットを策定し、その通信プロトコルを決めるという研究 [7] がある。また、次章で述べる在宅健康管理システムの上で、家庭内の制御機器とセンサ間のプロトコルに関して標準化が進められている [8]。さらに、生体情報以外にも、医療情報などをアプリケーション間で共有することを考慮し、XML をベースにした MML（MedicalMarkupLanguage）[9] や HL7（HealthLevel7）[10] が標準化されている。生体情報の蓄積フェーズにおいては、既存のリレーショナルデータベースを利用する研究、XML データベース、時間の経過に伴って変化する情報を扱うデータベースの研究 [11] などがなされている。また、e ケアタウンプロジェクト [12] において、生体情報の収集、蓄積フェーズに関する研究が行われた。

本研究では、特に利用フェーズに関して焦点を当てる。情報が収集、蓄積された状態で、ユーザが生体情報を利用する場合の要件を、以下に二点挙げる。一点目は生体情報の利用フェーズにおいて、個人の生体情報を一元的に取得するためにシステムが一意に情報を特定できなければならない。つまり、様々な組織や家庭等で取得した生体情報を、ネットワーク上で一元的に管理できなければならない。二点目は、ユーザが個人の生体情報を取得できた際に、各個人の情報の共有を望む人のみに開示するといったアクセス制御が行えなければならない。つまり、生体情報の利用として、**生体情報に対する一元的なアクセス**と**生体情報に対するアクセス制御**を実現しなければならない。

2.5　まとめ

本章では、本研究で述べる生体情報共有機構の定義、概要について述べた。生体情報の機能を分類し、現在行われている既存モデルと比較し、本研究の違いを述べた。また、その機構を実現するための課題として、生体情報を透過的に扱う事とアクセス制御をモデル化する事という二点を挙げた。3 章では、課題を考慮に入れながら関連研究、技術要素に関して述べていく。

第3章　関連研究と問題点

本章では、生体情報共有機構を実現する上での既存の問題点に関して述べる。まず、既存のサービスや研究を分析し、既存の問題点を述べる。また、本研究において解決すべき事項の要素技術に関して述べ、考慮すべき事項についてまとめる。

3.1　生体情報を共有する既存のサービス及び研究

本研究で定義した生体情報共有機構に関する研究として、生体情報の共有を行っている既存サービス、研究を以下に述べ、現状の問題点について考察を行う。

3.1.1　既存サービス

既存サービスとして、e-Fitness.com、ヘルスプラネット、在宅健康管理システムの三つを説明する。

e-Fitness.com　e-Fitness.com は、バイタルセンサとして Combi 社のエアロバイク ai という自転車エルゴメータを使った商用サービス [5] である。エアロバイク ai からのデータを自宅の PC などに取り込み、その情報をインターネット経由で健康運動指導士やトレーナーに開示することによって、運動指導を受ける事ができるサービスである。自転車エルゴメータを作っているベンダーがその情報を元にサービスを行っている。モデルとしては個人の PC 等で管理する事が前提となっており、その情報をベンダーに預ける事によってサービス事業者が提供するサービスのみを受ける事ができる。

ヘルスプラネット　ヘルスプラネットは、バイタルセンサとして TANITA 社の体重計、血圧計、歩数計を用いる商用サービス [6] である。体重計、血圧計、歩数計からのデータを家庭内において Bluetooth を用いて PC に転送し、専用ソフトによって自己管理を行えるというのがこのシステムの機能である。また、その情報をインターネット上で専門家等と情報共有する事によって、健康診断サービスが受ける事ができる。モデルとしては、上記の e-Fitness.com と同様に個人が情報を管理し、それを機器ベンダーに送信する事で、サービス事業者が提供するサービスのみを受ける事ができる。

在宅健康管理システム　在宅健康管理システムとは、日本においては約 15 年前から開発が行われている遠隔で健康管理を行うシステムである。現在では JAHIS（保健医療福祉情報システム工業会）[13] が主導する、日本において 120 件以上、既に様々な形で導入されているサービスである。

現在の在宅健康管理システムとして普及しているのは、株式会社日立エンジニアリングサービスが開発している「うらら」であり、本稿内では「うらら」の事を在宅健康管理システムと呼ぶ。このシステムは「うらら」という健康測定器を用いる。測定器は、血圧、心電を測定でき、またユーザが入力することもできる。下記の図 3.1に示すように、端末機にデータが蓄積される。そして、一日一回地域の病院や情報センターなどに家庭からインターネットや電話などを使って、情報を送信する。異常等があれば病院からの連絡されたり、センターによる利用者の健康情報のモニタリング、月間のレポート等が送られる。

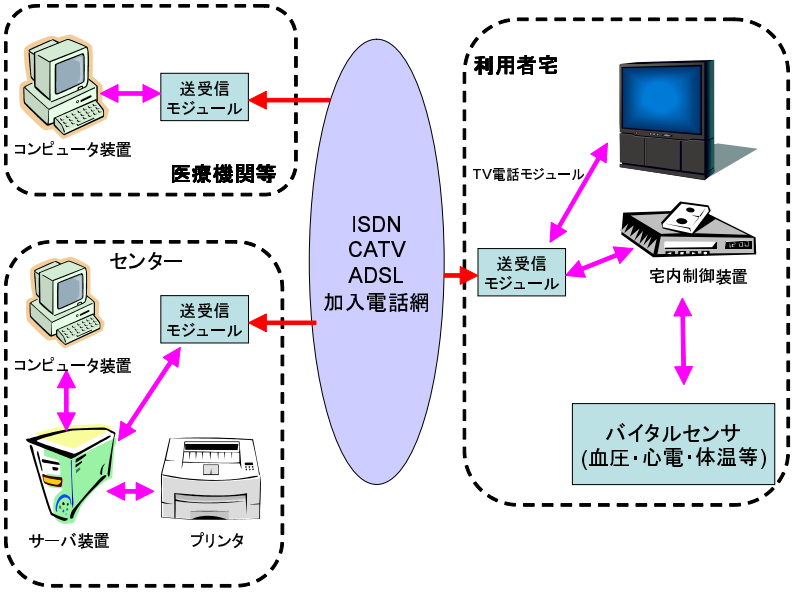

図 3.1: 在宅健康管理システム概要図

うららの特徴は、心電図と血圧計を備えた独自端末と、CATV 回線や NTT の電話回線を通して、病院等の機関が情報を管理するというところである。機器には、4 人まで家族を判別できる。また、機関向けの端末では ID カードを使った個人特定を行う事ができる。この機器では入出力端末（ボタンや液晶）を用いた問診を行う事ができ、体重等の測定器で扱えない情報に関しては自ら入力することができる。

3.1.2　既存研究

健康増進システム　技術研究組合医療福祉機器研究所によって行われている研究であり、在宅健康管理システムを元に開発されたシステム [14] である。このシステムでは、健康マットや血圧計等家庭用のバイタルセンサを各家庭に配置し、計測された情報をサービスセンター（医療機関等を対象）に情報を集め管理する。図 3.2に概要を示す。

健康増進システムの特徴は、高機能健康測定機器として、低拘束の健康機器によって利用者に負担をかけずに計測できる点である。また、データの蓄積をサービスセンターで行い、利用者が受ける事のできるサービスをサービス事業者に分けた事が特徴である。

バイタルケアネット　NPO 法人 WIN（ウェアラブル環境情報ネット推進機構）によって行われているウェアラブルセンサを用いた健康情報管理システム [15] である。図 3.3にバイタ

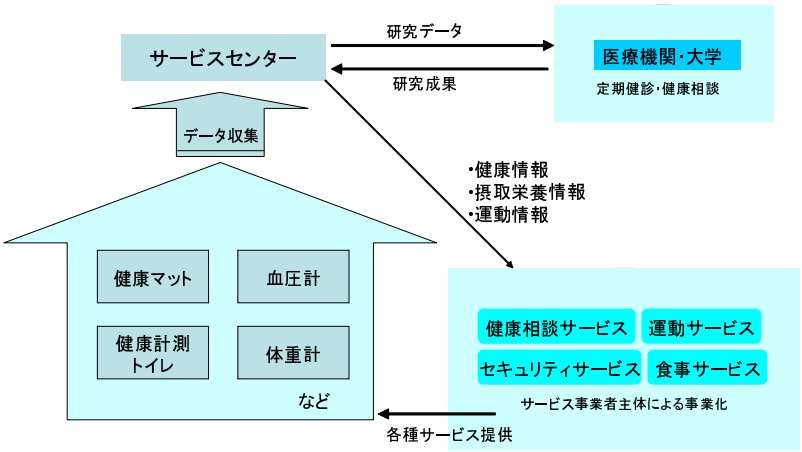

図 3.2: 健康増進システム概要図

ルケアネットの概要を示す。センサをウェアラブルセンサに限定し、その情報を元に利用者のサービスを行う基盤を開発している。救急医療のネットワーク化を目指しており、心疾患や危険度の高い疾患を持った国民のバイタル管理を行おうとしている。

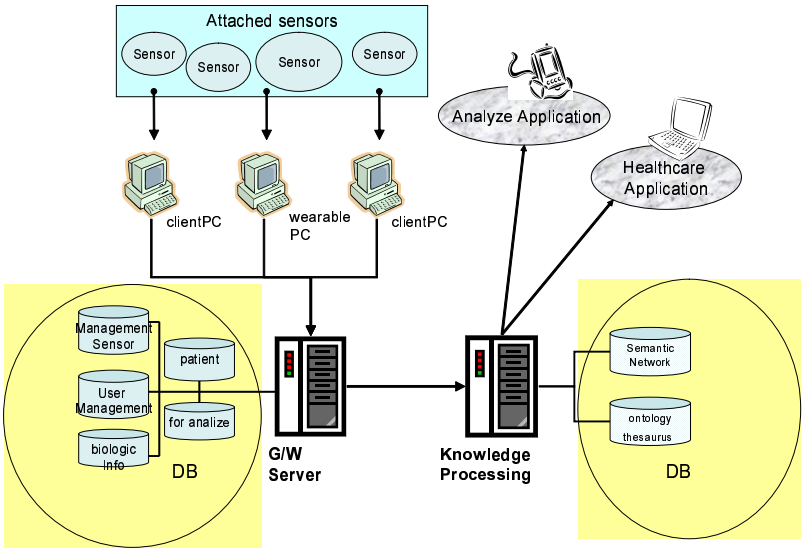

図 3.3: バイタルケアネット概要図

バイタルケアネットの特徴としては、ウェアラブルなセンサにより人間の動作や生体情報を測定し、その情報を汎用的に扱うため、ウェアラブル PC により XML データに変換し拡張性を保っている。また、ゲートウェイを置くことによってアプリケーションの汎用性を持たせている。

3.1.3　e ケアタウンプロジェクト

著者は 2003 年より e ケアタウンプロジェクト [12] に参加し、研究活動を行ってきた。e ケアタウンプロジェクトとは、総務省の「e!プロジェクト」の介護福祉分野における実証実験実施地域として藤沢が選ばれた事を受け、慶應義塾大学と NTT 東日本、藤沢市保健医療財団が合同で行ったプロジェクトである。プロジェクトの主旨として、IT を生かし地域住民の健康を支え、QOL を向上することが目的である。研究成果は [16][17] にまとめられている。その中では、本研究と同様に生体情報の共有に関する研究が行われていた。具体的には、自転車エルゴメータを用いて、健康管理を行うシステムを構築し [18]、また、運動器具などを用いた健康管理情報の収集、蓄積のフレームワークを構築した [19][20]。e ケアプロジェクトの研究では、収集、蓄積機構を実現した。しかし、利用モデルが不十分なため、様々なサービスが利用できる機構にはなっていなかった。

3.1.4　既存の研究及びサービスにおける生体情報の取り扱いに関する問題点

本研究の目的は、バイタルセンサにより計測した生体情報を、ユーザの望む形で情報を開示できるモデルを構築することである。上に挙げた既存研究のモデルにおける問題を考察する。

本研究で目指す生体情報共有において、所有者の生体情報に対する透過的なアクセスが行えなければならない。それに必要な事は、ユーザを一意に識別できる事、生体情報の所有権を本人が持つ事、また、アクセスができた際にはアクセス制御ができる事である。以上の観点から、既存研究を以下の表 3.1にまとめた。また表 3.1の一番下の列に本研究の土台となる e ケアシステムを入れた。表 3.1 内の要素に関しては以下に対応する要素内容を示す。

表 3.1: 関連研究まとめ

既存研究	個人の識別	生体情報の管理	アクセスコントロール
e-Fitness.com	なし	個人	なし
ヘルスプラネット	なし	個人	なし
在宅健康管理システム	一部制限あり [1]	センター	なし
健康増進システム	あり	センター	なし
バイタルケアネット	あり	個人	一部あり [2]
e ケアシステム	あり	個人	一部 [3]

e-Fitness.com とヘルスプラネットでは、生体情報の所有者が情報の管理を行えるが、家庭内の用途として限定しており、共有することを目的としていない。また、他の三つはインターネットを用いて蓄積し、その情報を用いたサービスを考慮している。しかし、在宅健康管理システムは家庭内で取得した情報を、各種自治体等で管理するというモデルであり、情報の二次利用ができない。つまり、ユーザからすると様々なサービスを受ける事ができない。健康増進システム、バイタルケアネットではサービス（生体情報の利用）と生体情報の蓄積が分割されており、ユーザが様々なサービスを受ける事ができる可能性がある。しかしこの

[1] 管理組織内における閉じたユーザ管理。
[2] 3 種類の簡単な開示方法が選べる。
[3] 項目ごとの開示のみ行えた。

両研究においても情報に対するアクセスコントロールは十分なものとは言えない。アクセスコントロールとして、上記の表で「なし」と書いてあるものはアクセスコントロールが必要なシチュエーションにないものがほとんどである。つまり、他組織や他サービスとの連携を考えていないため、アクセス制御が必要でない。そこで行われているアクセス制御はサービスを受けている（生体情報の収集を行っている）機関に対して全面的に信用するというモデルである。バイタルケアネットだけはアクセス制御を考慮しているが、医療機関全てに公開、自医療機関に公開、非公開という三種類の開示方法しか選べない。

既存研究において、バイタルセンサを使った生体情報の収集、蓄積は可能である。また、その情報を用いたサービス等も行われている。しかし、一元的に個人が個人の生体情報を利用するという事を考慮し、生体情報の収集、蓄積、利用を明確に分割し、個人が管理するというような共有モデルは存在しない。つまり、表 3.1にある通り、生体情報を共有する事を考慮し、アクセスコントロールまで考えられたモデルはない。ここで言うアクセスコントロールとは、生体情報の所有者が望む形で望む相手に情報を開示できる事を指す。つまり、友人等には詳細な情報ではなく、差分や平均値だけの間引いた情報で開示を行い、専門家には詳細な情報を開示する。既存の機関やサービス事業者に依存しないアクセス制御である。本研究では、この問題を解決するために生体情報の共有が行えるモデルを提案し、そのモデルに基づきシステムを構築する。

3.2　情報システムにおけるアクセスコントロール

本節では、既存のサービス、研究がアクセス制御に関して実現されていないという現状を考慮して、既存のアクセス制御技術に関する懸案事項を述べる。つまり、情報システムにおけるアクセス制御において考慮すべき事項を述べ、生体情報を共有する際に必要なアクセスコントロールを実現するための必要事項をまとめる。

3.2.1　情報システムにおけるセキュリティに関する考慮すべき点

インターネットを介した情報共有アプリケーションにおいて、システム全体のセキュリティを確保し、アクセスを適切に制御できなければならない。アクセスの制御は次節で述べる。

インターネットを扱う情報を交換するシステムにおいて、不正なアクセスや敵対的活動などからシステム内の情報やシステム全体を守る事がセキュリティ確保の目的である。情報システムのセキュリティ確保のために必要な項目に関して、ISO[21] により国際標準化が進められている。1992 年に OECD（経済協力開発機構）[22] による「情報システムのセキュリティのためのガイドライン」などにより以下の 3 項目が定義されている。また、その後 3 項目の定義が追加され、今では GMITS[23] の中で 6 項目となった。以下にその中心となる 3 項目の詳細を述べる。

- Confidentiality（秘匿性）

  秘匿性とは、特定の情報を特定の人間以外に知られないようにすることである。システム内に格納されたり通信メッセージに含まれたりした秘匿した情報を、その情報を知ることを許されていない人間による不正な読み出しや、知ることを許された人間による不正な開示から守らなければならない。

- Integrity（完全性）

  完全性とは、システムの状態が正しいことを保証することである。情報やサービスが事前の期待通りの状態であること、謝った更新、不正な更新を受けていないこと、正しさの保証がない情報を含んでいないことなどを含む。適用されるシステムやコンテキストによって、これらは、システム内の情報が互いにつじつまがあっている、システム内の情報が外界の状況を正しく表現している、システム内の情報やプログラムが不正な改竄を受けていない、システムが権限のないユーザの操作を受けていない、システムが謝った入力を受け付けていない、といった要件に対応する。

- Availability（可用性）

  可用性とは、使用の権利を持つユーザが、CPU、メモリ、ファイル、装置、情報などのシステムのリソースやサービスを使用したいときに実際に使用可能であることを示す。リソースの喪失、リソースの独占などにより、半永久的、あるいは一時的にそのリソースが使用不可能になり、必要に応じた使用が妨害されないようにしなければならない。

現在では運用の問題等を考え、Accountablity、Authenticity、Reliablity の 3 項目が追加されている。責任追跡や釈明義務等を考慮すべき Accountablity、サブジェクトの真正性を保証する Authenticity、信頼性を保証する Reliablity も考慮しなければならない。

3.2.2　情報システムにおけるアクセスコントロール技術

アクセスを適切に制御するためには、リファレンスモニタとセキュリティポリシモデルを定義、実装しなければならない。

既存の Unix システムや生体情報に関わるシステムでは全体を支配できる特権を有する点が問題とされてきた。特権ユーザの権限が不正に奪われると、システムのセキュリティを確保する方法は存在しなかった。強制的にシステムがアクセスコントロールを行い、アクセスを適切に制限するためには以下の二つの要素を定義、実装しなければならない。

1. リファレンスモニタ
2. セキュリティポリシ

リファレンスモニタ　システム上の全てのリソースに対するアクセスを正しく監視するために、リファレンスモニタ [24] という概念をシステムに導入する必要がある。図 3.4にリファレンスモニタの概要を示す。リファレンスモニタはシステム上にある全てのリソースに対するアクセスをコントロールでき、悪意のあるプロセスに修正や回避がされたりしてはならない。また、全てのリクエストが通過し、アクセスを制御できなければならない。つまり、リファレンスモニタは正確な振る舞いを行う事を保証する機構でなければならない。

図 3.4にあるように、全ての Subject（主体）は、Object（対象）にアクセスする際に必ずリファレンスモニタによって Access Validation Check が行われる。その際に何が正当で、何が不当であるかというアクセス可否の判断は、システムのセキュリティポリシによって行われる。セキュリティポリシの詳細は次段落で述べる。

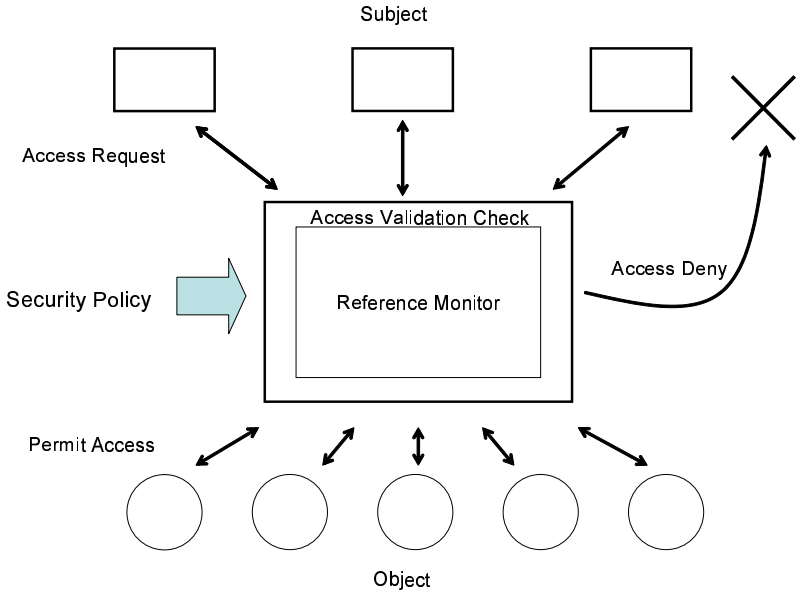

図 3.4: Reference Monitor

セキュリティポリシ　リファレンスモニタがアクセスの可否判断する場合に、「どの主体が、どの対象物を、どのように操作できるのか」という事を正確に定義しておかなければならない。アクセスコントロールにおけるセキュリティポリシとは、上記の定義の事を指す。つまり、定義されたセキュリティポリシに問題がある場合、そのシステム自体のセキュリティを保証できない。また、前節で挙げたセキュリティの確保のための 3 項目をどう表現するかによってモデルが変化する。

一般的にセキュリティポリシの中で主体を Subject(サブジェクト)、対象を Object(オブジェクト) と呼ばれる。そして、サブジェクトとオブジェクトの関係を定義したセキュリティポリシには、様々な分類が行える。以下に制御されるオブジェクトの種類による分類を示す。オブジェクトの分類は大きく分けると二つで、制御される情報の流れが多層的なモデルと多元的なモデルである。

- 多層的なモデル

  多層的なセキュリティポリシモデルとは、元々米国の軍などで適用されていたものであり、以下の図 3.5のように情報を階層化し、階層間でのアクセスを制御するモデルである。例えば上位の階層の情報は下位の階層の情報にはアクセスできないといった制御である。

  このモデルに分類される代表的なモデルとしては、Bell-LaPadula[25]、Biba Integrity Model[26]、LOMAC[27] などが挙げられる。

- 多元的なモデル

  多元的なセキュリティポリシモデルとは、情報を階層化せずに、情報を小さなコンパートメントに分けその区切りごとにアクセスをコントロールすることである。図 3.6に示すように、横方向に情報の制御が行われる。順序や重要度等の階層化された情報に対

図 3.5: 多層的なモデル

しては不向きであるが、情報が順位付けられている場合ではなく、緩やかな区分された情報を扱う際に適したモデルである。

このモデルに分類される代表的なモデルとしては、Clark-Wilson モデル [28]、Chinese Wall モデル [29]、DTE モデル [30]、RBAC モデル [31] などが挙げられる。

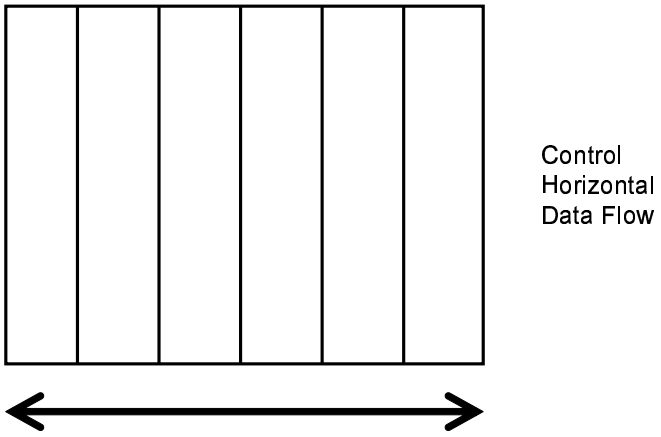

図 3.6: 多元的なモデル

上記に挙げた代表的なモデルは、セキュリティ上の目的として、秘匿性や完全性を確保するためのものである。Bell-Lapadule モデルや Chinese Wall モデルは秘匿性を重視したモデル、Biba モデルや Clark-Wilson モデルや LOMAC モデル、さらには DTE モデルなども完全性を重視したモデルである。また、RBAC モデルなどは主体の構成を変更することで、ほかのポリシと独立、または併用して利用できるモデルとなっている。

3.2.3　制御方式

上記に挙げたセキュリティポリシの分類は情報の特性に応じたものであるが、強制的にアクセスを制御するアクセスコントロールの方式が主となっている。それとは別にアクセス制御の適用手法によって、以下の二つのアクセス制御の方式が存在する。

DAC(Discretionary Access Control)：任意アクセス制御　既存の UNIX や Windows などの OS で採用されているアクセス制御方式であり、任意アクセス制御と呼ばれる。この方式では、システム内のリソースのアクセスはそのリソースの所有者にすべて委ねられている。つまり、所有者自身が書き換えを禁止している場合でも、所有者によってそのアクセス権限を変更する事ができるためセキュリティポリシの完全な適用ができない。

MAC(Mandatory Access Control)：強制的アクセス制御　強制的アクセス制御と呼ばれ、SE-Linux やセキュア OS や軍事情報のシステムなど機密管理が厳しいものに採用されている。この方式においては、システム的なポリシを超えるアクセスに関してはリソースの所有者においても許可されない。つまり、システム上の管理者が設定したセキュリティポリシをシステム全体に、またユーザのリソースに関しても適用される方式の事である。以上のような分類方式は厳密に分けられるものではなく RBAC は DAC と MAC の中間的な位置づけになる。

3.3　既存のセキュリティポリシ

セキュリティポリシの研究は現在活発に行われていて、情報システムにおいて新たに適用が考えられているセキュリティポリシを以下に述べる。

- RBAC

  Role-Based Access Control とはユーザに対して与える役割というものを元にアクセスコントロールを行うセキュリティポリシである。既存の UNIX におけるアクセスコントロールでは特権ユーザ（root）が権限を全て持つという事により、特権ユーザを不正アクセスなどにより乗っ取られた場合に、様々な弊害が起こる。そこで、役割というものを細分化し、最小特権の原理（Separation of Duties）に基づきアクセス権限を役割に対して与え、その役割をユーザが担うという事でアクセスコントロールを行うモデルである。

  RBAC は概念的なモデルであり、その適用に際して DAC と MAC の中間的な振る舞いを定義する事もできるため、近年、RBAC の研究は盛んに行われ、セキュア OS や既存の RDBMS などにも採用されはじめている。SE-Linux では TE(Type Enforcement) と RBAC を併せもったモデルで実現されている。また、RBAC は概念的なモデルであり、実際の情報システムに適用するために様々な概念を追加したモデルなどが研究されている。

- DTE

  Domain and Type Enforcement とは、サブジェクトに対してはドメインラベルを割り当て、オブジェクトに対してタイプを割り当てる事で強制的にアクセス制御を行う低レベルな MAC のモデルである。RBAC と DTE に関しては MAC の影響を抜きにして考えると、サブジェクトに対してロールを割り当てるかドメインを割り当てるかというところで違うのみで、基本的には大きな差分はない。

RBAC や DTE を複合的に組み合わせたセキュリティポリシモデル [32][33] といった RBAC を拡張したモデルなど、セキュリティポリシモデルについての研究は様々に行われている。

またヘルスケア分野を視野に入れたアクセス制御モデルなどは出てきているが、こういったアクセス制御モデルを実際にシステム化する際、概念ベースのセキュリティポリシを明確に定義しなければならない。本研究では生体情報の利用モデルを提案し、その中でアクセス制御機構内でセキュリティポリシを明確に定義し、システムを構築する。

3.4　生体情報を共有する場合のアクセスコントロール

前節までに述べてきたように、情報を共有するシステムにおいてはセキュリティポリシを明確に定義しなければならない。また、既存のモデルベースなセキュリティポリシは、セキュリティポリシをどのように適用させるかによって、システムの動作は変わってくる。つまり、ユーザが行えるアクセス制御も変わってくる。そこで生体情報の共有時にアクセスコントロールを行うモデルを構築する際の考慮すべき項目を述べる。

情報のアクセス権の所有　既存の生体情報のアクセスコントロールのモデルにおいては、ユーザが生体情報を所有するという事はあまり行われていない。つまり、生体情報を各組織やベンダー等により管理され、その上でのアクセスが管理組織によって制御されるモデルである。既存のシステムにおいて、アクセスコントロールは、実用的なレベルで行われていない[13][15][14]。しかし、自らの生体情報を専門家に開示し二次利用する場合、自らの生体情報は望む人のみに情報を開示できるべきである。しかし、現状ではアクセス権が所有者にないため、所有者が望むアクセスが実現できない。

アクセスを制御する対象　既存の生体情報のアクセスコントロールにおいてアクセスを制御していた対象というのは、個人の生体情報に対する読み込み権全て、または項目ごとというのが一般的である。つまり体重や体脂肪率など日々変化しているデータというものに関してアクセス権の対象が、ユーザ単位や体重のみ、または体脂肪率のみといった開示の手法がとられている。しかし、こういったアクセス制御の手法を取ると、ユーザがその場限りのデータや、過去のデータを開示しないなどといった事はできない。そこでアクセス権が適用される情報の最小単位というものをあらかじめ決める必要がある。

柔軟なアクセスコントロール　また、既存のアクセス制御では、情報のひとかたまりに対して読み込み、書き込み、実行などといった単純なアクセス制御が一般的であった。情報の開示といった際にも、生体情報においては差分のみの表示や過去との比較などといった様々な手法が考えられ、開示方法によって情報の意味が変化してくる。システム内においてリソースに対するアクセス手法を決める事がアクセスコントロール機構を構築する上で必要となってくる。

3.5　まとめ

本章では、本研究における生体情報共有に対して関連研究やサービスを述べ、問題点を述べた。また既存サービスなどでは行われていないアクセス制御に関して考慮すべき事項を述べた。現在は本研究の目的を目指すモデルは存在せず、新たな生体情報の利用モデルが必要

となる。次章では本研究の目的を満たすモデルについて述べ、その後システムの設計、実装について述べていく。

第4章　生体情報の取り扱いにおける考慮すべき事項

本章では、生体情報を共有する際に考慮すべき事項に関して本研究のアプローチを述べる。まず、生体情報への一元的なアクセスを可能にする生体情報の蓄積モデルに関して述べる。次に、生体情報の利用の際に考慮すべき事項をアクセス制御を中心に述べ、新たな生体情報の利用モデルを提案する。

4.1　生体情報の収集、蓄積に関する検討

生体情報の利用の際、バイタルセンサによって蓄積された情報はユーザが発見できなければならない。本節では、ユーザが生体情報をどのように収集し、蓄積するかという情報の収集蓄積モデルに関する検討を行う。生体情報の蓄積を一つのシステムで行う事は現実的ではない。そこで既存のサービス事業者ごとに情報蓄積を行い利用の際に収集するモデルと、ユーザごとに蓄積を行い利用するモデルとの比較を行う。インターネット上で生体情報の共有を行う場合、利用フェーズにおいて分散したユーザの生体情報を集める、または収集フェーズにおいて生体情報を規定の場所に蓄積するという二つの手法が考えられる。また、どちらのモデルであっても、蓄積されたサーバがサービスを提供し、クライアントがそれを利用するというクライアントサーバモデルになる。

4.1.1　分散蓄積モデル

ユーザは、ユーザの所属する機関に、分散して生体情報の蓄積を行う。例えば、家庭内で収集したデータは家庭内のパーソナルサーバに蓄積し、また、トレーニングジムで収集したデータはトレーニングジム内のサーバに蓄積する。その上でユーザが生体情報を利用する際には、各機関に分散した生体情報を集めて利用する。図 4.1に分散蓄積モデルの概要を示す。収集フェーズにおいて place a, b, c という三つの機関、または場所を想定している。UserA は place a と place c において生体情報の収集を行い、place a と place c に生体情報を蓄積する。その後利用する段階において User A の生体情報を place a と place c に問い合わせる。User B についても同様である。

ユーザが健康管理サービスを受ける場所、つまり、生体情報の収集を行う場所は様々である。分散蓄積モデルでは、ユーザの生体情報は分散しており、その情報を探索、発見することによって一元的に生体情報を取得できる。探索、発見する際には、あらかじめユーザが情報を蓄積する場所のリストを所持しておくか、ユーザがどこに何の情報を蓄積しているかといった場所と情報の項目などを全て保持しておかなければならない。

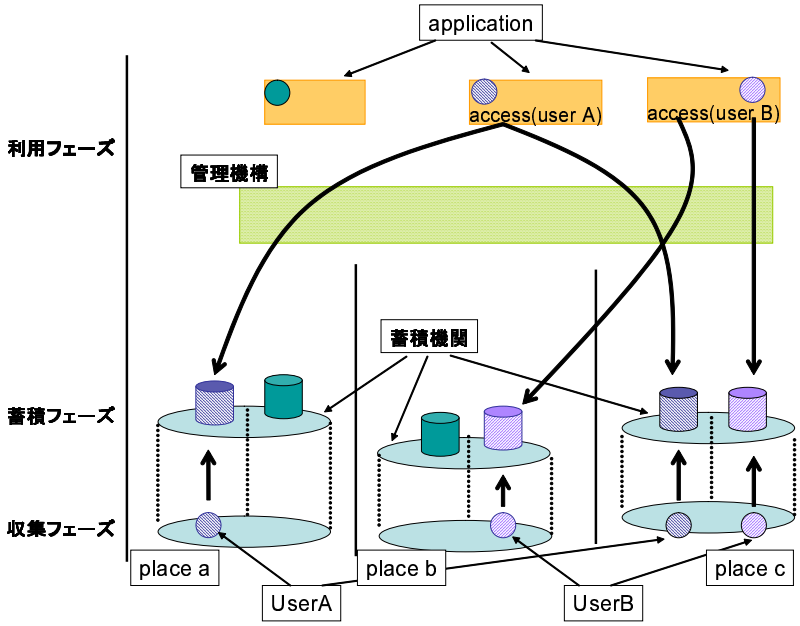

図 4.1: 蓄積場所が分散

利点　生体情報の収集の際に、その場所の情報資源を利用し、その場所に蓄積ができる点である。

欠点　蓄積された情報に対するメタ情報を管理しなければならない。ここで述べるメタ情報とは、いつどこに何の情報が蓄積されたか、もしくはどこに情報が蓄積されているかという二種類である。生体情報の収集を行う場所は様々な場所が考えられ、場所の数は膨大であり、利用フェーズにおける管理機構の実現するコストが高い。つまり、アクセス制御までを考慮するとシステムの実現が困難である。

4.1.2　集中蓄積モデル

蓄積を行う際に、ユーザが登録する任意な機関をあらかじめ決めておく。ユーザが自分で自分の情報を管理するモデルである。また、利用の際にはシステムが一意にユーザを管理し、管理機構ではユーザの認証情報と生体情報の蓄積場所を参照するポインタのみを持つ。図 4.2に集中蓄積モデルの概要を示す。図 4.1と同じく、place a, b, c という三種類の場所、機関を想定している。User A は place b に生体情報を蓄積する事をあらかじめ決めており、place a で収集したデータも place b に送られ蓄積される。その後、利用フェーズにおいて、User A の生体情報の蓄積場所が place b である事を管理機構に問い合わせ、place b にある生体情報を利用する。

利点　生体情報を利用する際、蓄積場所が決められているので、管理機構は、ユーザ情報のマッピングと情報の場所に関するポインタを持つだけでよい。

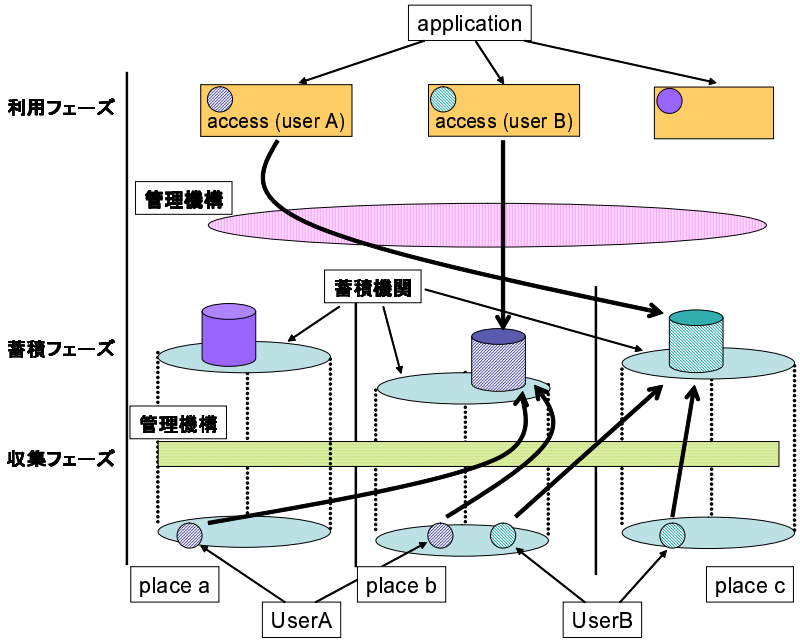

図 4.2: 蓄積場所は任意の一カ所

欠点　生体情報を収集する際、インターネット上の、任意の一カ所に情報を登録しなければならない。つまり、収集フェーズにおいてユーザ管理機構に問い合わせを行わなければいけないため、センサからの情報収集アプリケーションを新たに実装しなければならなず、既存のサービスを使う事はできない。

4.1.3　本研究のアプローチ

本研究では上記で述べた二つの手法のうち、4.1.2を選択する。つまり、生体情報の蓄積場所が任意の一カ所であるというモデルである。両者を比較した際、ユーザに対する一意な識別に関しては、収集フェーズで行うか、利用フェーズにて行うかという区別はあるものの情報の管理を行わなければならない。生体情報を一元的に管理し、アクセス制御を行うためには、ユーザの生体情報が同一の名前空間で扱えなければならない。現実的に前者のモデルを実現するには、生体情報の値以外の情報を管理することになり、生体情報が時系列な情報であること、また値の情報量は少ない事を考えると、全ての情報を一元管理するのと変わらなくなる。生体情報は多種多様な情報群であり、その情報は時間の経過に従って情報量が増加するため、4.1.1のモデルはシステムとして現実的ではない。そこで本研究では、4.1.2の生体情報の蓄積場所は任意の一カ所にあらかじめ決まっているというモデルを採用する。

また、4.1.2のモデルを採用する際に考慮すべき事項について述べる。生体情報の格納場所が任意の一カ所に決められているため、生体情報の収集、利用フェーズにおいて、システムは生体情報の格納場所を知る必要がある。つまり、ユーザとユーザの蓄積場所を何らかのシステムによって管理し、その管理機構との通信プロトコルを定める必要がある。以上の二点を実現する事により、ユーザがネットワーク上にある自らの生体情報を探し出し、利用する事が可能となる。

4.2　生体情報を利用する際のアクセス制御

本節では生体情報管理システム上で、アクセスコントロールを行う際に考慮すべき事項を述べる。第 3 章でも述べたが、生体情報の共有は個人をベースに行われていないため、アクセス制御に関する新たなモデルが必要である。そこで生体情報管理の特異点を述べ、その特徴に基づいたアクセス制御に必要な要件についてまとめ本研究における利用モデルを示す。また、既存の他情報共有モデルと比較を行い、本モデルの有用性を述べる。

4.2.1　利用シナリオ

本研究が想定している生体情報の共有には以下に挙げるような利用が考えられる。詳細を以下に述べる。

専門家との情報共有　医師や健康運動指導士など専門的な知見を持った人々が生体情報から専門的な知見により、診断や指導などを行うコミュニケーションである。例えば、ユーザの体重や血圧などの情報を元に、自身が望む栄養士に食事メニューを作成してもらい、運動管理指導士に運動のメニューを決めてもらい、健康状態を看護師や医者に見守ってもらう。

専門家との情報共有の場合は、指導を受ける場合、ユーザがどのような情報が必要かはわからない事が多い。しかし、自らが予定した専門家以外のアクセスを拒否したいという事は考えられる。

ユーザ同士の情報開示　ユーザ同士が運動記録や体重の推移などを開示しあい、禁煙マラソンなどのコミュニティを構築し、運動支援や健康管理を行うコミュニケーションである。このような取り組みは、既にインターネット上で歩数計を用いた実験プロジェクト [34] が行われており、健康行動理論の点からも有効である事が示されている。

このようなユーザ同士の生体情報を共有する場合、詳細な生体情報の開示が必要ない場合も考えられる。つまり、期間を限定したアクセスや、情報を間引いた上での表示などのアクセス制御が考えられる。

調査などの目的で情報利用　生体情報という情報本体だけでは意味を持たない情報を、統計の調査や分析等の目的で医療機関などが情報を取得する場合のことである。また、サービス事業者などが自らの管理下に置かれたユーザの生体情報ではなく、利用履歴を必要とする状況は多々存在する。そのような場合、ユーザは個人が特定されない状況において情報の開示を許す、つまり、生体情報が個人を特定しない情報での利用が考えられる。また、どこで生体情報を計測したという情報を、特定できないようなアクセス制御が考えられる。
以降では上記の利用を考慮したアクセス制御モデルを提案する。

4.2.2　主体に関して

アクセス制御を行う主体は、生体情報の所有者であるオーナとそれ以外のユーザという二種類に分類する。システム側が専門家や友人といった分類をしてしまうと、関係性の自由度が減ってしまう。そのため、本研究における主体はオーナとそれ以外という二種類に分類し、オーナ以外のユーザの中でオーナがアクセス権限を与える主体をグループ化した集団を**関係**

者と呼ぶ。生体情報の所有者である**オーナ**は、そのオーナと情報の共有を行う関係性において**関係者**を定義できる。

4.2.3　グループ化

本モデルにおいて「関係者」とは、オーナとの関係性をグループとして表現できなければならない。オーナの生体情報に対してアクセスを行う関係者の中でも、健康診断のために生体情報を開示する「主治医」や運動指導のための「トレーナー」、ダイエットなどの目的を同じくするユーザ同士の「友人」などといった自分の中でのグループというものが考えられる。また、具体的には「トレーナー」、「友人」といった中でも「ダイエットのためのトレーニングを見てもらうトレーナー」と「リハビリテーションのためのトレーナー」や、「ダイエットを一緒に行う友人」と「運動を楽しむだけの友人」というグループは、グループによってアクセスできる情報は異なるべきである。

ユーザは現実社会では対人コミュニケーションの中で、目的によって開示する情報を変えてコミュニケーションを行う。そのため、目的ごとのグループ化ができなければならない。そこで、オーナは関係者を管理するために、グループ化が必要となる。任意のグループに対する閲覧、編集はオーナが設定できなければならない。そのグループごとにアクセス権限を変更できる必要がある。つまり、オーナはユーザにグループを割り当てる事ができ、そのグループを切り替えると、ユーザのアクセス権が変化する。

4.2.4　生体情報の特異性

情報の分類　本研究における生体情報とは、人間の生体活動の結果を測定した身体のデータと、人間の生体活動に関わる活動の記録である。本研究で実際に扱う生体情報を、情報の特性によって三種類に分類する。

表 4.1: 生体情報の分類

	中身	例
個人情報	各ユーザの身体に関わる基礎情報	性別、生年月日など
身体計測情報	身体の状態を計測した情報	血圧、心拍数など
活動記録情報	身体の活動を記録した情報	トレーニング結果（万歩計の歩数等）

本研究での個人情報とは、ユーザの身体に関わる情報であり、基本的には不変の値を持つものである。つまり、バイオメトリクス認証などに使う指紋、静脈のパターン、虹彩などは個人情報の範疇に入る。また、身体計測情報とは、個人の身体から計測できる情報の中で、連続性のある情報の事を指している。つまり、体重、血圧、心泊数などという身体からの計測情報である。また、活動記録情報というのは、万歩計や自転車エルゴメータ等のトレーニングを行った結果の情報である。つまり、8000 歩歩いたという記録、または 20 分減量トレーニングを行ったという記録である。個人情報以外の情報に関しては時間の経過により変化する情報であり、過去との比較や情報の間引きなどにより意味が変化する。本研究で主に生体情報と呼んでいるのは時間によって変化する連続するデータである身体計測情報と活動記録

情報の事を指している。

情報の最小単位　本研究で扱う生体情報の最小単位は各情報ごとに違う。個人情報であれば、項目と値の組み合わせであり、身体計測情報や活動記録情報であれば、オーナ情報と項目と時間と値の組み合わせである。身体計測情報や活動記録情報の情報の最小単位の中に時間を組み込むことにより、期間を区切った情報の集合に対するアクセスが実現できる。また、それ以外の情報もバイタルセンサから取得できる項目はある。そういった情報に関しては項目ごとにアクセス制御を行う事とする。図 4.3に情報の最小単位のイメージ図を示す。

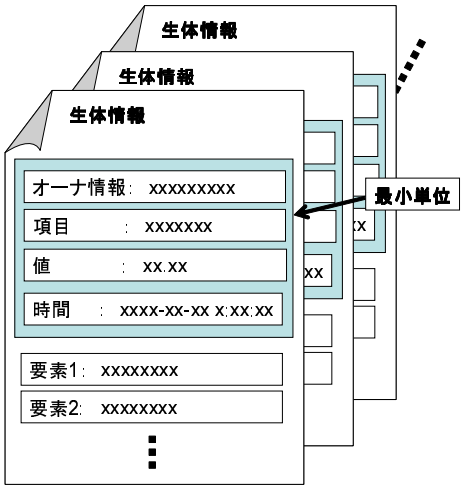

図 4.3: 情報の最小単位：イメージ

情報に対するアクセス権　時間によって変化する生体情報を扱う際に考慮すべき事項として、生体情報には間引きや概観といった情報の多様な開示手法が考えられる。また、そういった開示手法に対してアクセス制御を行う必要がある。つまり、一ヶ月間の体重の変遷を、詳細な計測時間と計測データを表示する、あるいはしないといった使い方以外に、情報の変化量や一週間ごとのデータといった間引いた情報での開示も考えられる。時間的に連続した情報の集合である生体情報の特徴として、情報を間引いた場合にも、情報を概観するという別の意味が存在する。そこで、既存の情報システムにおける read(読み) の許可、不許可といった一つの開示手法に対するアクセス制御では十分とは言えない。また、その間引きの開示手法に関しては、平均値での表示、差分のみの表示、切り上げや切り捨てなどといった概数での表示、グラフ化など様々な手法が考えられ、体重や血圧といった情報の項目によっても意味合いが違い、また概観ができるものとできないものが存在する。本研究では概観 (overview) という概念を導入し、概観のみの表示というアクセス制御を実現する。また、生体情報の利用フェーズでは、read 以外の権限として write が考えられるが、本研究ではセンサを用いた生体情報取得を前提としているため、オーナ以外の書き換えは許可しない。

4.2.5　アクセス制御の例

表 4.2、表 4.3に上記のアクセス制御モデルの実現例を示す。主治医というグループに対しては期間を限定したアクセスを許可し、彼らは詳細な情報を見る事ができる。また、ダイエットを目的とした友人というグループに対してはある期間のアクセスに対して許可しているが、許可するのは変化量のみとする。また、調査機関に対してはより制限のある形でしか見せないようなアクセス制御を実現する。

表中の overview*(n)* というのは詳細な情報表示以外の情報表示メソッドの事を示す。overview(0) はデータ本体がないアクセスメソッドとし、数字の違いによってアクセスメソッドが違う事とする。また overview(2)*(time)* と書かれてあるのは時間であり、表示してもよい期間を指している。最後に overview(2)(time)*(a b ...)* と書かれてあるのは最小単位以外のアクセスが許されている項目である。

表 4.2: アクセス制御の例

	オーナ	グループ	
		主治医	友人（ダイエット）
ユーザ情報	read, write	read	read
体重	read(all)(all)	read(time)(ab)	overview(1)(time)(a)
体脂肪率	read(all)(all)	read(time)(ab)	overview(2)(time)(b)
自転車エルゴメータ	read(all)(all)	-	overview(1)(time)(a)

表 4.3: アクセス制御の例：続き

	グループ	他人
	調査機関	
ユーザ情報	-	-
体重	overview(0)(time)(abc)	-
体脂肪率	-	-
自転車エルゴメータ	overview(0)(time)(abc)	-

4.2.6　実現できるアクセスコントロール

以上のモデルを適切にシステム化する事で以下に述べるようなアクセスコントロールが実現できる。

1. 期間を区切ったアクセス制御

   生体情報は生体から取得した時間毎に違う情報であり、時間の変化とともに意味も違ってくる。そこで、期間という区切りを用いてアクセス制御を行う。情報の最小単位を時間との組み合わせにすることにより、一年前のデータは見せないが 3ヶ月前からのデータは見せるなどといった制御が可能となる。

2. 情報の差分や平均値での表示などの多様なアクセス手法に対するアクセス制御

   例えば、現在体重が 70kg という生体情報がどのような意味を含むかは過去との比較によって変化する。つまり、一ヶ月前は 80kg で現在 70kg であるという情報と一ヶ月前 60kg で現在 70kg であるという情報は意味が違ってくる。このように差分量だけでも情報の価値があるため、一ヶ月前からの詳細なデータは開示しないが、差分量のみの開示といったアクセス制御が可能となる。

3. 組み合わせにより変化する意味へのアクセス制御

   ある項目のある時点における生体情報のスナップショットは、単体での意味と組み合わせた際の意味が違う。たとえば、70kg という体重の情報はその情報だけでは重量という意味しかない。それにオーナ情報が加わる事によって、つまりオーナの身長や体脂肪の重量など、他の生体情報が加わることによって、その体重は適正であったり肥満であったりといった意味を持つ。体重は情報を間引いて開示するが身長は詳細なデータを開示する手法や、調査機関などに対してオーナ情報だけをのぞいたアクセス制御を実現できる。

4.2.7　他利用モデルとの比較

SNS や BLOG などにおける情報共有システム　現在の SNS 等の情報共有の仕組みは生体情報共有機構と扱う情報が時間を追うごとに貯まっていくという点で同一である。図 4.4に既存の SNS や BLOG における情報利用のモデル概要を示す。既存の SNS や BLOG において、情報リソース（日記等）に対するアクセス方法は、友人には見せる、見せない、また友人の友人までの開示などといった単純なものである。

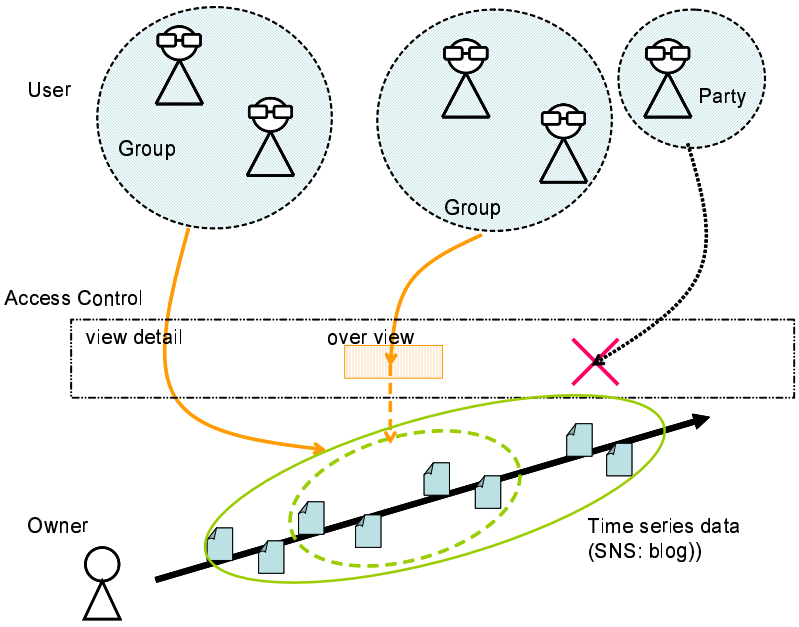

図 4.4: SNS、BLOG における情報利用モデル

SNS などの情報は日付間の差分などに意味はないため、差分に対する開示手法などは存在

しない。しかし RSS などを用いて間引いた情報に対する開示手法のみが存在する。次世代 SNS である Affelio [35] などではカテゴリやコンテンツごとの細かい開示設定が行える。しかし、RSS などによる開示手法はコンテンツ所有者が独自に設定し、統一的にアクセスを制御する事はできない。また、情報の特性上、間引き方は種類が限られており、本研究に必要となる多様なアクセス手法に対応するアクセス制御や時間を区切った情報のアクセス制御、自由なグループ化に対するアクセス制御は行えない。

提案する利用モデル　本研究で提案する利用モデルについて述べる。図 4.5に概要を示す。対象をあるグループに分類し、そのグループに対してアクセス権を設定する。その開示の仕方には詳細なデータを一定期間見せるといったものや、一定期間の中でフィルターをかけ（情報の差分のみの表示など）開示するといった複数の開示手法に対するアクセス制御が必要となってくる。

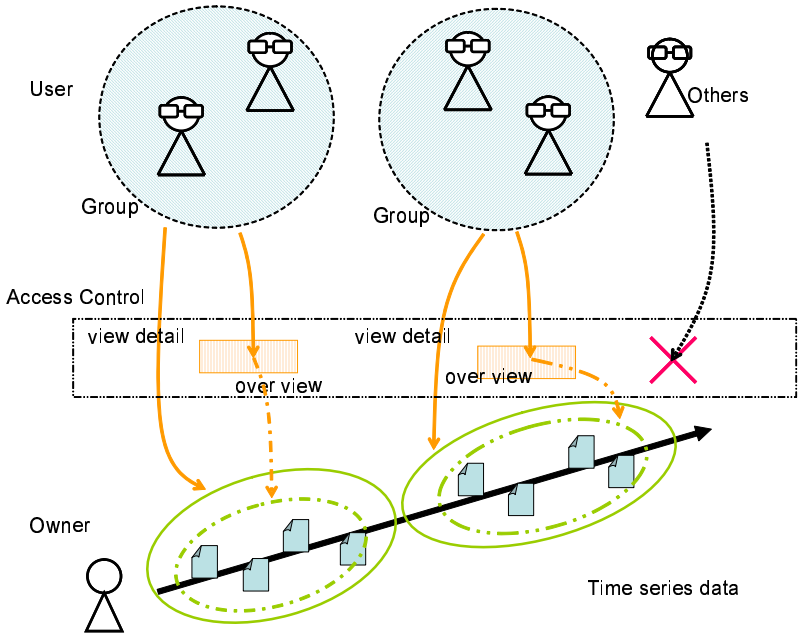

図 4.5: 提案モデル

以上のように、既存の情報利用モデルにおいては、時間の経過を意識した複数のアクセス手法に対するアクセス制御が行われるモデルはなく、生体情報を共有する際に適切なアクセス制御を実現できない。そこで本研究では、概観という新たな概念を用いて、拡張可能なアクセスメソッドに対する情報利用モデルを示した。本モデルを用いる事によって、既存のモデルでは対応しきれなかった、時間によるアクセス制御、または情報の概観に対するアクセス制御が行えるようになる。

4.3　まとめ

本章では、生体情報をインターネット上で共有する際の考慮すべき事項について検討を行った。情報の所有と情報のアクセス制御に関する生体情報特有の問題に関して述べ、解決する

モデルを提案し、既存の情報共有モデルと比較することにより、本モデルの有用性を示した。
次章では本章で述べた事を考慮した実際のシステムの設計を行う。

第5章　生体情報共有システムの設計

本章では、生体情報共有モデルを実現する BISS(Biological Information Sharing System) の設計について述べる。前章までに述べた生体情報共有モデルを実現するため、システム設計を行い、技術的な解決策を考察する。

5.1　設計方針

本システムでは、生体情報を一元的に扱う上で必要なアクセス制御機構を提供する。本システムの実現により、生体情報を一元的に扱う際に必要なアクセス制御を提供できる。本システムは生体情報を蓄積した各サーバにおいてアクセス制御を行うが、サーバ上での機能とその機能をアプリケーションが用いるためのライブラリ群を提供する。

本システムは生体情報がバイタルセンサなどを用いて決められたサーバ内に蓄えられていることを前提とする。つまり、様々なバイタルセンサからインターネットを通して機器の違いなどを受け止め生体情報を蓄積できている環境を想定している。さらに、生体情報を一元的に扱うために生体情報が蓄積されたサーバを発見し、ユーザを一意に識別、管理を行うユーザ管理機構については、ユーザ ID を識別し、サーバのネットワーク的な位置情報を管理する機能が必要である。ユーザ ID とサーバのネットワーク上の場所を管理するという機構は既存のデータベースシステムで簡単に解決可能である。そこで、本研究では既存の技術を組み合わせ解決する。

本システムは生体情報利用アプリケーション側に提供するライブラリ、生体情報を蓄積してあり、アクセス制御を行うサーバ、ユーザ管理機構によって構成される。生体情報を収集、蓄積する機構は既に存在し、本システム上で動いていると想定しているので、その蓄積された情報を取り出すインターフェースは存在すると想定する。その上で各生体情報利用アプリケーションはライブラリを通して、サーバやユーザ管理機構と通信を行い、認証、アクセス制御を行う。

アクセス制御

前章で述べたように、時間を区切ったアクセス、またある期間の差分や平均値などの間引いた情報の開示というアクセス制御を実現する。アクセス制御とは「どの主体がどの対象物を、どのように操作できるのか」という単位であるため、主体、対象、操作方法を定義し、そのアクセスポリシを表現できなければならない。

ユーザ管理機構

また、前提としてユーザの識別が一意に行われている。そのユーザごとに生体情報の格納場所があらかじめ決定されており、ネットワーク上の位置情報が取得できなければならない。そこで一つの名前空間内において一意となる識別子を用いてユーザを区別

し、ユーザの生体情報が蓄積されたサーバのネットワーク上の位置情報を返す。また、情報の収集、利用の際にユーザ認証を行い本人である事を証明しなければならない。

5.2　設計概要

図 5.1に本研究におけるシステムの設計概要を示す。生体情報共有機構には、ユーザ管理機構（User Management System）とアクセス制御機構 (Biological Server) が必要であり、生体情報利用アプリケーションからはライブラリ（BISS ライブラリ）を用いて Biological Server や User Management System を利用する。センサからの情報がユーザ管理機構に問い合わせにより正しい蓄積場所を知り、蓄積を行う。また、その情報を共有する友人や医師などもユーザ管理機構に問い合わせ、あるユーザの生体情報にアクセスする。その生体情報の利用の際にはあらかじめ生体情報のオーナによって決められたポリシに基づき、アクセス制御が適切に行われる。

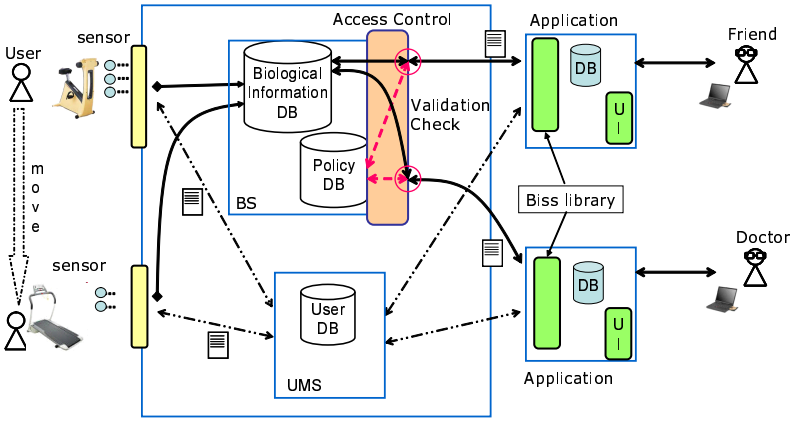

図 5.1: 設計概要図

5.3　セキュリティポリシ

本節では本研究のアクセス制御におけるセキュリティポリシ、またそのポリシの記述に関して述べる。セキュリティポリシに関しては RBAC（Role-based Access Control）を拡張して用いる。つまり、サブジェクトに関してユーザベースでアクセス制御は行わず、ユーザに与えられた役割によるアクセス制御を行う。前章で述べたアクセス権を割り当てる主体は、オーナとの関係性によってグループ化が行われる。そのオーナとの関係性を本研究ではロールと定義し、ロールに対してアクセス権限を与える事でアクセス制御を行う。

生体情報のオーナごとに異なるロール群が存在し、生体情報のオーナはユーザに与えたロール割り当てを変更することでアクセス制御を変更する。また、ロールに対するアクセス権限を変更するとそのロールを割り当てられたユーザ全てのアクセス制御が実現できる。

また、オブジェクトに対する最小単位は時間と情報本体とオーナ情報であり、アクセスする際に、時間の固まりとして期間ごとにアクセスが行われる。そこでオブジェクトに対しては時間の固まりに対してラベルを貼付し、そのラベルを元にアクセス制御を行う。

セキュリティポリシの概念図を以下の図 5.2に示す。

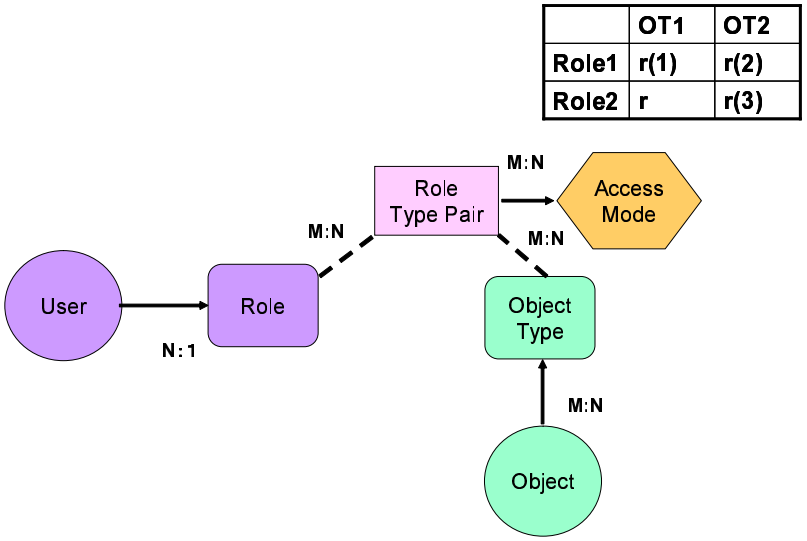

図 5.2: セキュリティポリシ概念図

5.3.1　主体に関して

本システムのユーザはユニークな ID を持ち一意に識別する事が可能である。ユーザの ID に関してはシステム内でユニークであり、ユーザを識別する事が可能である事が必要である。そのユーザ ID を元にアクセス制御を行うのであるが、本研究においては上記に述べたように、各ユーザが生体情報のオーナから割り当てられたロールによってアクセス制御を行う。つまり、各生体情報のオーナには自分のロールリストがあり、そのロールにはアクセス権限が割り当てられており、オーナだけが編集、管理できる必要がある。オーナにはロールの作成、編集、またロールに対するユーザの割り当て、また削除という機能を行えなければならない。

実際、ロールに対して割り当てるのは本システム上で一意に識別できるユーザ ID であり、各ユーザが Biological Server 内にそのロール情報は管理されている。つまり生体情報のオーナは Biological Server 内に自らの生体情報とその生体情報に対するアクセスに関わるポリシやロール情報などを管理している。

5.3.2　対象に関して

生体情報のアクセス権限を割り当てる最小単位は前章でも述べたが、一つの項目に対する値とその取得時間とオーナ情報の組み合わせである。つまり体重や血圧などといった項目のデータとそのデータが取得した時間とオーナが誰であるかという情報である。対象を指定する際には、オーナを指定し、一つのデータ項目に対してある期間を決める事でその対象データを特定する。つまり、対象に関しては期間という範囲に対してアクセス制御を行う。

5.3.3　アクセスメソッド

本システムでは、生体情報の項目ごとに複数のアクセスメソッドが存在する。つまり、体重という情報を開示する際に上記に述べたように期間を指定した後に全てのデータを開示するような手法や、期間中の平均値のみを開示するような手法など様々な手法が考えられる。また、ある生体情報の項目では可能なアクセスメソッドが違う生体情報の項目では意味が変わり得る。本システムではそのアクセスメソッドを変えたアクセス権限を設定できるアクセス制御機構を構築する。

さらにアクセスメソッド自体は Biological Server において管理、実装されている必要がある。また、そのアクセスメソッドは生体情報の項目、期間、対象となるユーザ情報を元に指定された期間中のデータを何らかの加工を行った上でアプリケーションに結果を返す。そのアクセスメソッド自体はバイタルセンサごとにどのようなアクセスメソッドが利用できるか、また情報量の過多によってアクセスメソッドは無数に存在する。そのためアクセス制御においてポリシの記述は拡張可能な形になってなければいけない。

一方で、アクセスメソッド間の関係は、階層化が可能である。つまり、詳細な情報というは差分のみの情報より情報量が多い。アクセスメソッドを行うと情報量が増減し、その増減量によってアクセスメソッドは上位、下位という定義ができる。詳細な情報を開示するというメソッドが一番上位のメソッドであり、その下の階層に差分表示や平均値表示といったメソッドが存在する。上下関係を定義する事で下位のアクセスメソッドに関してのアクセス許可ができ、ユーザの利便性があがる。

5.3.4　ポリシ記述

アクセスポリシを記述する際に、ポリシ内に表現すべき事は許可される主体と、対象と対象に対する許可されたアクセス手法である。それらを一意に識別できるように表現できなければならない。また本システムにおいてアクセス手法とは複数の拡張可能なメソッド群である。アクセスメソッドが必要な情報の間引き方は無数に存在するため、アクセスメソッドを指定する際には拡張可能な記述方式で記述できる必要がある。また、最小単位である時間とデータ本体以外のパラメータに関してはバイタルセンサによっても違い、様々な属性データが考えられる。そこで、アクセスポリシとしては処理が遅くなってしまう事が考えられるが汎用的に記述できる必要がある。

- ロール

  ポリシが対象としている主体としてはオーナとの関係性を示したロールであり、ロールを指定する識別子が必要である。

- 項目

  生体情報の項目を指定しなければならない。例としては体重、血圧などといったデータを指す。今回この項目のネーミングに関する議論は行わないが、システムとして意味的に体重を表す識別子が必要である。

- 期間

  生体情報を開示を許可した期間を指定できなければならない。

- 属性

  情報の最小単位としては、時間とデータ本体であるが、それ以外の属性情報に関して許可する付加情報を記述できなければならない。

- アクセスメソッド

  生体情報の項目に対する許可する開示手法の指定が必要である。

5.4　Biological Server

本節では、各ユーザの生体情報を保持している Biological Server について述べる。Biological Server とは、生体情報を蓄積してある情報の蓄積サーバであり、ユーザごとに存在する。しかしながら、ユーザごとに一つずつ存在するのではなく、家庭内のサーバには家族が管理されてあったり、また第三者機関などのデータセンターに複数のユーザが使う事を想定している。また、後述するがユーザには全てグローバルユニークな ID を持ち、ユーザがシステムの利用者であり、生体情報を登録している場合には、その ID と Biological Server のネットワーク上の位置情報である IP アドレスが保たれている。

以下に Biological Server の機能について述べていく。サーバ内には、アクセス制御部、認証部、通信部が存在する。

5.4.1　アクセス制御部

アクセス制御機構の設計について述べる。アクセス制御機構は Biological Server の中心的な役割を果たし、通信部よりアクセス制御要求メッセージを受け取る。その後、アクセス制御要求メッセージ内のユーザの対象となるオーナから割り当てられたロールを問い合わせる。さらに、そのロール情報を元にポリシデータベースにクエリーを投げ対象となるポリシを発見し、アクセス要求が正当であるかという可否判断を行う。図 5.3にアクセス制御の動作概要を示す。

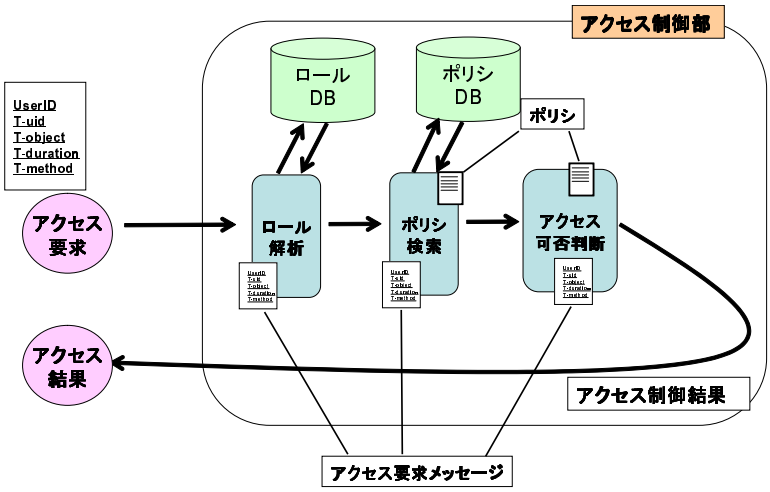

図 5.3: アクセス制御部

ロール検索　生体情報のオーナは自らの生体情報にアクセスする権限をロールに対して割り当てる。そのオーナごとに存在する複数のロールの中にユーザを割り当てる事で、オーナは生体情報に対するアクセス権限を与える。そこでユーザからアクセス要求があった場合に、アクセス要求を行ったユーザ情報とアクセス先のユーザ情報を元にロール情報をロールデータベースから取得する。その後ポリシ検索を行っていく。

ポリシ検索　アクセスポリシは生体情報のオーナが作成したロールごとに存在する。関係者リストに入っているユーザからロールを与える事でアクセス権限を変化させるため、アクセスポリシはロールごとに存在している。ユーザのロール情報を元にアクセスポリシを検索し、アクセス可否判断部にアクセス情報とポリシ情報を渡しアクセス可否判断を行う。

アクセス可否判断　渡されたアクセスポリシとアクセス要求メッセージから、対象となるパラメータのチェックを逐一行う。評価を行う項目としては、対象となる項目、さらには項目のオプション、期間、アクセスメソッドである。アクセス要求内の項目が全てアクセスポリシに適合するかどうかを判断し、評価結果としては真か偽かいずれかの値を返す。

5.4.2　認証部

Biological Server にはそのサーバにおいて生体情報を保存しているオーナ、またその生体情報を閲覧するユーザがアクセスしてくる。その際システム内における本人確認として認証が必要である。ここで認証を行う必要があるオーナとは Biological Server 内に生体情報を保存しているユーザである。また、生体情報を閲覧するユーザとは本システムの全ユーザが可能性が考えられ、全てのユーザに対する認証情報を各 Biological Server が持つのは現実的ではない。

そこで認証の仕組みを別個に用意する必要性があり、また、必要な機能は A というユーザのアクセスがシステム内において正しく A のアクセスであるという事を証明する事である。そこで、本研究では第三者機関によって証明書を発行する仕組みを用いる。

5.4.3　通信部

Biological Server の通信部においては、利用アプリケーションからの通信を受け付ける。通信開始時のメッセージングに関しては以下の図 5.4に示す。アプリケーションから認証を行い、認証が行われた後にアクセス制御の要求が起こり、結果がアプリケーションにかえってくる。また通信の際には、ユーザの識別子、トランザクションの識別子が全てのメッセージに入っている。また、認証状態を管理し認証が完了していない場合は認証部に処理を渡し、認証が完了している場合はアクセス制御部に渡す。

アクセス制御要求メッセージにはアクセスしてきたユーザの識別子、対象となる生体情報の項目、期間、またその生体情報のオーナ識別子、そして要求するメソッドが存在する。本研究において生体情報の項目名については範疇外とする。つまり、体重のデータがどのような記述子によって一意性を保っているかについては範疇外とし、一意な名前が付いているものとする。さらにアクセスメソッドに関しては複数記述可能とする。

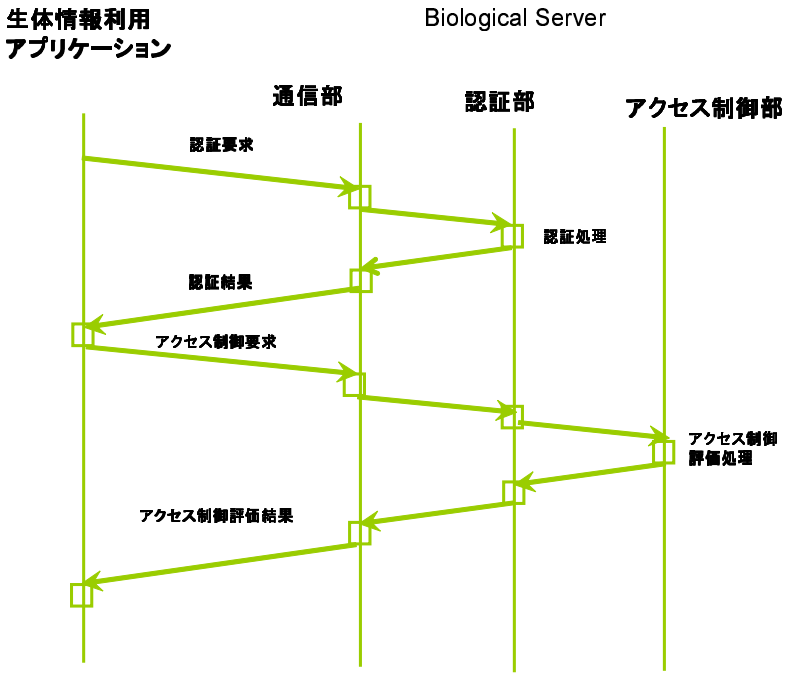

図 5.4: メッセージング概要図

5.5　User Management System

本節では、本システムにおけるユーザ管理の機構である User Management System について述べる。ユーザ識別子からそのユーザの生体情報の格納されてあるネットワーク的な位置情報を返すという事ができなければならない。また、ユーザは、対象となるオーナの分散した Biological Server の場所は知らなくても済むように User Management System に問い合わせができる必要がある。本システムにおいては、この管理機構は既存技術の組み合わせによって対処する。

User Management System は生体情報利用アプリケーションから BISS ライブラリを通して利用する。

5.5.1　ユーザ管理

User Management System 内では、本システムのユーザとして生体情報のオーナと生体情報を利用するユーザ全てを一意に識別できる識別子を割り当て、管理しなければならない。ユーザ情報の登録、変更、削除、ユーザ ID の割り当て、管理といった機能を提供する。また、ユーザ情報としては、生体情報を蓄積する Biological Server のネットワーク的な位置情報である IP アドレスを含める。管理手法として、既存のデータベースシステムを用いて、ユーザ ID、ユーザ情報、IP アドレス（蓄積場所）の管理を行う。

5.5.2　問い合わせ機構

生体情報利用アプリケーションと User Management System 間の問い合わせを定義する必要がある。すなわち、生体情報利用アプリケーションがユーザ ID をキーに生体情報蓄積場所を得る手順を決めなければならない。今回既存のデータベースを用いる事を考慮し、SQL 等の問い合わせ言語により、ユーザ ID をキーに IP アドレスを取得する必要がある。また、問い合わせは BISS ライブラリ上を通して生体情報利用アプリケーションが行う事を想定している。

5.6　まとめ

本章では、生体情報共有システム内のアクセス制御機構、ユーザ管理機構について述べた。次章より、BISS を実際に実現したプロトタイプ実装に関して述べていく。

第6章　生体情報共有システムの実装

本章では、生体情報共有システムの実装に関して述べる。

6.1　実装概要

本研究における提案モデルに基づき、生体情報共有システムのプロトタイプを実装した。実装物としては Biological Server 上で動くアクセス制御機構と生体情報利用アプリケーションが用いるアクセス制御用ライブラリである。既存の生体情報収集、蓄積機構を用いて、また認証などには他既存システムを用いることを想定している。システム構成としては以下の図 6.1に示す。アプリケーションサーバ上で生体情報利用アプリケーションを実装し、クライアントとブラウザ越しに HTTP 通信を行う。

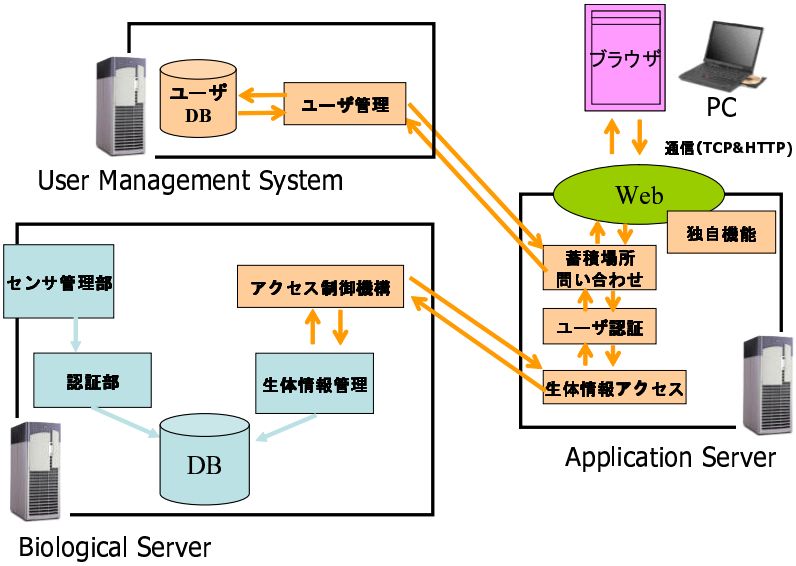

図 6.1: システム構成図

上記に述べたアクセス制御機構以外に関しては、以前開発した実装を用いる。[20] その上で、データベースに対する複数のアクセスメソッドを定義し、そのアクセスメソッドに対してアクセス制御を実現する機構を構築した。また、その共有した情報を利用し、アクセス制御を行えるサンプルアプリケーションを実装した。

6.2　実装環境

本節では、本システムで用いた実装環境について述べる。アクセス制御機構を持つ Biological Server の実装環境は以下の表 6.1に示す。Biological Server に関しては、生体情報の蓄積も行っており、リレーショナルデータベースである PostgreSQL を用いた。また、Java 言語を使用する事でマルチプラットホーム性を確保し、実装を行った。

表 6.1: Biological Server 実装環境

CPU	Intel Xeon 2.4Ghz
オペレーティングシステム	FreeBSD 5.4 STABLE
データベース	PostgreSQL 8.1
開発言語	Java(JDK 1.4.2)

また、生体情報利用アプリケーションが用いる BISS ライブラリはアプリケーションサーバに置かれる事を想定している。本システムは生体情報アプリケーションのユーザインターフェースにはサーブレットランタイムとして Jakarta Tomcat を用いた。生体情報アプリケーションのユーザはブラウザごしにアプリケーションサーバとやりとりを行う。アプリケーションサーバの実装環境は以下の表 6.2に示す。

表 6.2: アプリケーションサーバ 実装環境

CPU	Intel Pentium3 1.0Ghz
オペレーティングシステム	FreeBSD 6.0 RELEASE
開発言語	Java(JDK 1.4.2)
Web サーバ	Apache 2.0.55
サーブレットランタイム	Jakarta Tomcat 5.5.9

6.3　BISS(Biological Information Sharing System) の実装

本システムのモジュール概念図を以下の図 6.2に示す。Biological Server の Network モジュールと AccessControl モジュールがサーバ側の実装部分である。また、生体情報利用アプリケーション内で BISS ライブラリは利用され、ユーザ認証機能とアクセス要求機能と Biological Server との通信機能を実現する。それ以外の部分は Biological Server 内のデータベース管理や生体情報アプリケーション内のユーザインターフェースなどである。

6.4　BISS ライブラリの実装

Biological Server と各生体情報利用アプリケーションの間で通信を行う。生体情報利用アプリケーションと Biological Server の間でユーザ情報やアクセス制御情報を受け渡しするライブラリである。Biological Server に対して生体情報取得要求などを行う際のアクセス制御に必要な情報を受け渡しする。これらのアクセス制御に必要な情報のうちユーザ情報が UserInfo

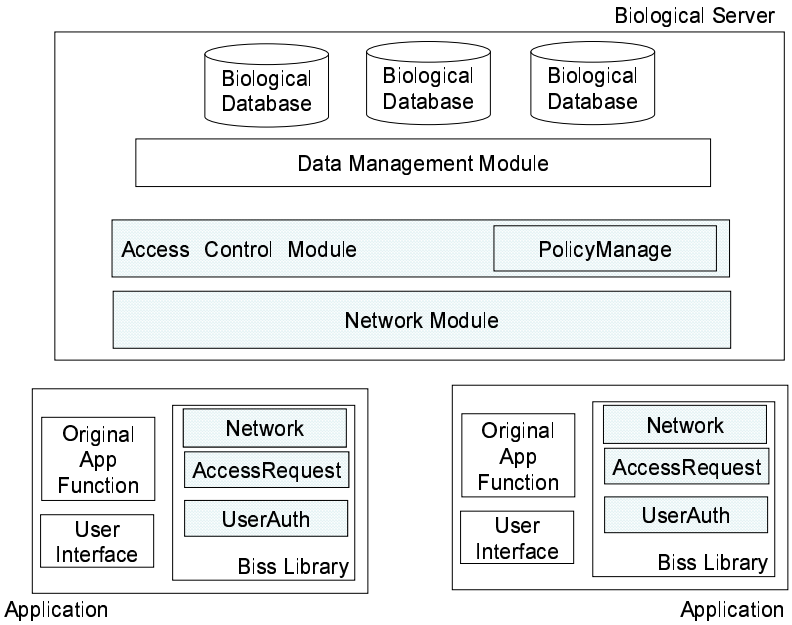

図 6.2: システム概要図

型のオブジェクトや AccessInfo 型のオブジェクトに格納されネットワークを介し、サーバに渡される。

今回生体情報利用アプリケーション用に用意したクラスライブラリは、以下の三種類である。

- UserInfo

  ユーザ ID やユーザの認証情報などを格納し、認証を行うクラス。

- BissClient

  対象となるユーザの Biological Server に対して通信を行い、情報のやりとりやセッションの管理などを行うクラス。

- AccessInfo

  ユーザの要求するアクセス情報を格納するクラス。

- UmsClient

  User Management System との通信を行い、対象となる生体情報の蓄積場所の格納場所を問い合わせを行うクラス。

以下の図 6.3にライブラリの利用例を示す。アクセス情報に関するオブジェクトで、アプリケーションサーバにクライアントからのアクセス要求を保持する。対象となるアクセス項目や期間、対象となるユーザ ID や開示手法などを保持している。

```
UserInfo uinfo = new UserInfo();
AccessInfo ainfo = new AccessInfo();


try{

  /* アクセス制御用情報設定 */
    ainfo.uid = xxxxxx;
    ainfo.object_name = "xxxxxx";
    ainfo.b_time = "xxxx-xx-xx xx:xx:xx";
    ainfo.method = "xxxx-xx-xx xx:xx:xx";
    UmsClient uclient = new UmsClient(uinfo);
    /*UMS 問い合わせオブジェクト*/

  /* ユーザ情報取得*/
    uinfo = getUserInfo();
  /* 認証 */
    ainfo.auth_flag = auth_user(uinfo);
    ainfo.bserver_addr = uclient.get_bs_server(ainfo);
    BissClient bclient = new BissClient(uinfo);

  /* 生体情報に対するアクセス要求 */
    bclient.request_access(ainfo);

  /* 以下 本体の処理 */

}catch(BissAccessControlException bac){
  /* アクセス制御が拒否された場合の処理 */
    System.out.println(bac.message);
}
```

図 6.3: Biss ライブラリ利用例

6.5　Biological Server の実装

6.5.1　アクセス制御機構

アクセス制御機構の実装について述べる。アクセス制御処理の一連の流れを図 6.4に示す。本システムのアクセス制御においては、アクセス要求があった場合に対してポリシとアクセス情報を対象の項目、期間、メソッドの順に評価していく。まず、アクセス要求をしているユーザが生体情報のオーナからどのロールが割り当てられているかの情報を取得する。次に、そのロールに対するポリシファイルを検索、取得する。その後アクセス制御の評価が始まる。図には示していないが、ロールが割り当てられていない、本研究における「他人」である場合にはロール情報取得の段階でアクセス拒否処理を行う。また、対象のポリシの有効期限が切れている、もしくは対象ポリシ内に要求された生体情報の項目が存在しない場合もアクセス拒否を行う。その後、生体情報の時間範囲評価、メソッド評価を行い、全てに合致していた場合のみアクセス許可を行いアクセス制御判定が終了する。アクセス許可、拒否どちらの場合も通信部を通し、アクセス可否判断メッセージを返す。

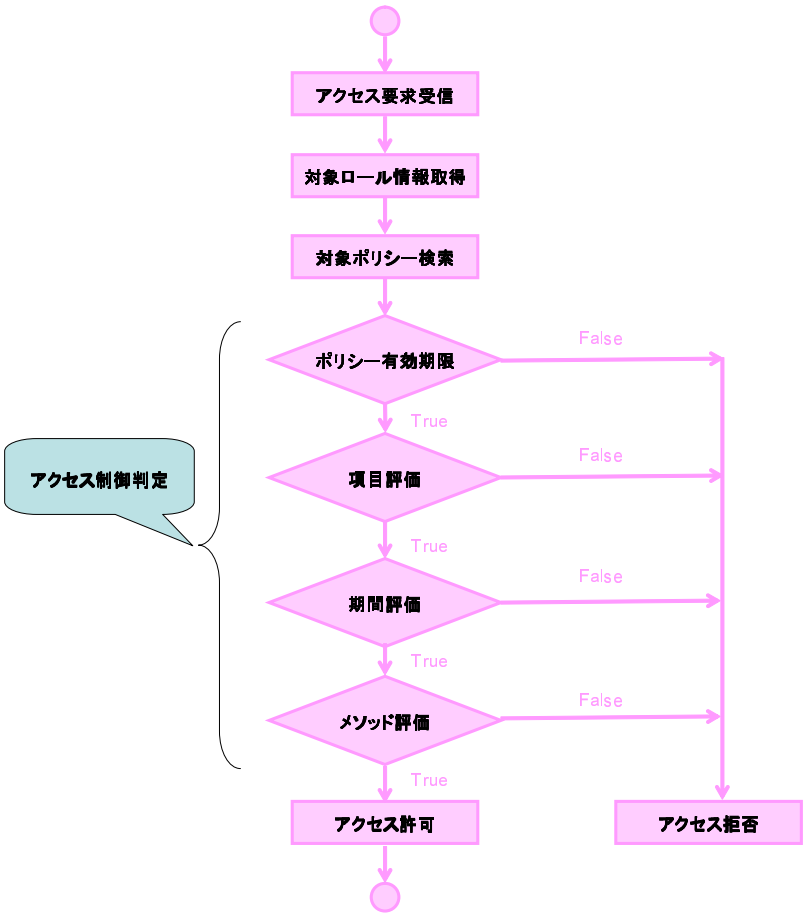

図 6.4: アクセス制御処理の流れ

6.5.2　ロール管理モジュール

生体情報のオーナごとにロールというユーザのグループが存在する。ロール管理はBiological Server 上のデータベース上で管理されていて、ロール自体を管理するテーブルとロールに対するユーザ割り当てのテーブルの二種類が存在する。それぞれのテーブルのスキーマを以下の図 6.5に示す。ロールに対する処理は Role クラスが処理を行う。Role クラスには、ロールの追加、削除、編集、ロールに割り当てるユーザの編集、ロールに割り当てるポリシファイルの変更、削除機能を実装した。

```
CREATE table user_role(
    owner_id int NOT NULL,
    user_id int NOT NULL,
    role_id int NOT NULL,
);

CREATE table role_info(
    owner_id     int NOT NULL,
    role_name    text NOT NULL,
    role_id      int NOT NULL,
    policy_file  text NOT NULL,
);
```

図 6.5: ロール管理テーブル定義

6.5.3　ポリシ検索

生体情報利用アプリケーションから送信されてきた AccessInfo オブジェクト内の情報を利用し、割り当てられてロールを user_role テーブルと role_info テーブルを元にポリシファイルを検索する。検索する SQL 文は以下の図 6.6に示す構文になる。アクセスしてきたユーザの入っているロールに対するポリシファイルをオーナ ID とユーザ ID を元に導き出している。RDBMS との接続には JDBC ドライバを用いた。ポリシに関してはサーバ上にファイルで保存されており、データベース上にパスが保存されている。

```
SELECT policy_file FROM user_role AS ur LEFT JOIN role_info AS ri \
                   ON ur.role_id = ri.role_id WHERE ur.user_id = [USERID] \
                   AND ur.owner_id= [OWNERID];
```

図 6.6: ポリシファイル検索 SQL 文

6.5.4　ポリシ実装

ポリシ検索の結果としてポリシファイルへのパスが返り値として渡される。ポリシファイル内には、ポリシの有効期限、ポリシにつけられた名前、対象となるロール、ロールに与えられたアクセスに関する情報が記述されている。ポリシファイルは Extensive Markup Language(XML) で記述されていて、Policy クラス内の load_policy メソッドによって解釈が行われる。以下の図 6.7にアクセスポリシの記述例を、以下の図 6.8にポリシファイルのスキーマを XML Schema を示す。ポリシクラスのメンバ関数としては、ポリシ読み込み、ポリシ編集、ポリシ内の項目を返すという機能を実装した。

```
<?xml version="1.0" encoding="Shift_JIS"?>
 <policy>
   <name>my doctor</name>
   <pb_time>2005/12/24</pb_time>
   <pe_time>2006/12/24</pe_time>
   <Subject>
     <role>my_doctor</role>
   </Subject>
   <Object>
     <item>
      <oname>体重</oname>
      <optional>place</optional>
      <duration>
         <b_time>2005/01/01</b_time>
         <e_time>2005/12/25</e_time>
      </duration>
   <Method>detail_view</Method>
   <Method>delta_view</Method>
     </item>
     <item>
    -以下省略-
   </Object>
 </policy>
```

図 6.7: アクセスポリシ記述例

6.5.5　アクセス可否判断モジュール

アクセス情報とポリシを比較し、アクセス可否判断を行うモジュールは、アクセス制御機構の中心を担っているリファレンスモニタの役目を果たす。XML のポリシファイルを読み込み、アクセス情報と比較を行い、アクセスが正当であるかの判断を行う。アクセス制御の流れを図 6.4に示したが、ポリシの有効期限が切れていないか、アクセス対象の項目がポリシ内に存在するか、期間が範囲内であるかどうか、メソッドが許可されているかという 4 点を判断する。ReferenceMonitor クラス内の checkaccess メソッドを用いて各判断項目を全てチェックを行う。以下に ReferenceMonitor クラスの概要を示す。

```
<?xml version="1.0" encoding="Shift_JIS"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <xsd:element name="policys">
    <xsd:complexType>
      <xsd:element name="policy">
         <xsd:element name="name" type="xsd:string" />
         <xsd:element name="Subject">
           <xsd:complexType>
             <xsd:element name="role" type="xsd:string" />
           </xsd:complexType>
         </xsd:element>
         <xsd:element name="Object">
           <xsd:complexType>
             <xsd:element name="item">
               <xsd:complexType>
                 <xsd:element name="oname" type="xsd:string" />
                 <xsd:element name="duration">
                   <xsd:complexType>
                     <xsd:element name="b_time" type="xsd:string" />
                     <xsd:element name="e_time" type="xsd:string" />
                   </xsd:complexType>
                 </xsd:element>
                 <xsd:element name="method" type="xsd:string" />
                 <!-- 省略 -->
           </xsd:complexType>
         </xsd:element>
      </xsd:element>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

図 6.8: ポリシスキーマ (XML Schema)

```
package jp.ad.wide.sfc.kazuki.biss.server;

class RefMonitor{

  boolean check_policy_date() throws RefMonitorException;
  boolean check_bio_object() throws RefMonitorException;
  boolean check_object_duration() throws RefMonitorException;
  boolean check_object_method() throws RefMonitorException;

  boolean checkaccess(Policy policy, AccessInfo ainfo){
    check_policy_date();
    check_bio_object();
    check_object_duration();
    check_object_method();
  }
}
```

図 6.9: ReferenceMonitor クラス

6.6　User Management System の実装

今回のプロトタイプ実装において、User Management System は既存のデータベースマネジメントシステム上に実装した。ユーザ ID と IP アドレスを管理するデータベースに対して、ネットワーク越しに SQL を発行する事で、生体情報利用アプリケーションは検索、編集等の管理を行える。

```
CREATE table user_bs(
    user_id int NOT NULL,
    bs_addr cidr,
);
```

図 6.10: ユーザ管理テーブル定義

6.7　まとめ

本章では、生体情報共有システムのプロトタイプ実装に関して述べた。本研究の生体情報利用モデルを実現したプロトタイプ実装として Java 言語を用いた BISS ライブラリと Biological Server 上のアクセス制御機構の実装について述べた。次章では、本システムの評価を行う。

第7章　検証および評価

本章では、本研究で構築したシステムの検証およびモデルの評価を行なう。まず、本システム（BISS）の動作検証を行い、本システムが要件にあった動作を行えた事を検証する。さらに他の既存研究との比較を行い、定性的な評価を行う。そして、本モデルの有効性、さらには実現時の問題などについて考察する。

7.1　BISS の機能検証

7.1.1　検証項目

システムの動作検証として必要な機能が実現できているかという検証を行った。本機構が行う事は、生体情報を個人を中心とする一元的な管理が行え、生体情報のオーナが望む相手に望む方式で開示できるというアクセス制御が行える事である。一元的な管理として、本モデルにおける解決策は生体情報の収集の際にあるユーザごとに決められた場所に保存するという事であった。また、本研究が目指すアクセス制御に必要な事は大きく分けると二つである。一つはデータ項目に対して期間を区切ったアクセス制御を変更できる事、もう一つはある期間に対する複数のデータ開示方法に対してユーザのロールによるアクセス制御が行える事である。

そこで本システムの機能検証として、生体情報の蓄積場所の発見機能、アクセス制御機能の検証を行った。アクセス制御機能に関しては、時間範囲の指定ができる事、またアクセスメソッドの指定が行える事の機能検証を行った。

7.1.2　生体情報の蓄積場所の発見

本研究において生体情報の蓄積場所はデータベースにより管理されていた。本研究で提供した BISS ライブラリの UMS クラスを評価用に実装し、コマンドライン上で動作を検証した。ユーザ ID を標準入力より受け付け、サーバ側から蓄積場所の IP アドレスの返答を待つ。また、その後サーバ側でデータベースのログを確かめることで検証を行う。上記の手順で検証を行った様子を図 7.1に示す。

以上の結果、生体情報の蓄積場所の発見機能は動作が検証できた。

7.1.3　アクセス制御

本システムのアクセス制御機能を動作検証する。検証手順を以下に述べる。まず、検証時のユーザ同士の関係性を示す。対象となるオーナ A の生体情報にユーザ B がアクセスする。あらかじめオーナ A がユーザ B をロール my_trainer に割り当ててあり、そのポリシは

```
###アプリケーションサーバにおいてテスト用プログラムを実行

   ecare% java UMSTest

   Input UserId : 12345
   [Send] SQL Request message...
   [Receive] IPaddr = 133.27.181.7
   Success Discovery...

   ecare%

###サーバ側ログメッセージを確認
   love% psql ums_db

   ums_db=# SELECT * FROM pg_stat_activity;
    datid | datname | procpid | usesysid | usename |    current_query
   -------+---------+---------+----------+---------+-------------------------
    16934 | ums_db  | 28304   |   100    |  ums    |        *1

    (*1: SELECT * FROM user_bs WHERE user_id = 12345)
```

図 7.1: 生体情報利用アプリケーションにおける利用例

mytrainer.xml に記述されている。その後生体情報のアクセス要求を行うテスト用プログラムにおいて各パラメータを変更しアクセスを行った。以下にその結果を示す。

まず、以下の図 7.2に示すのがオーナ A とユーザ B の関係である。オーナ A のロールである my_trainer というロールにユーザ B は所属している。

また、図 7.3に示すのが実際に my_trainer ロールに割り当てられたポリシファイルの該当部分である。体重（weight）に関しては 2005/11/01 から 2005/12/20 までの delta_view（差分表示）は許可されている。

そして、正常なアクセスをテスト用のプログラムで実行した結果が図 7.4である。テスト用プログラムは引数にアクセスの対象に関わる情報を指定する。今回はユーザ ID、対象ユーザ、項目、メソッドに関する指定を行う。

また、以下の図 7.5はアクセスメソッドを許可されないメソッドに変更した際のアクセス結果である。アクセス内容を差分表示である delta_view メソッドから詳細表示 detail_view に変更した。detail_view メソッドは、アクセスが許可され実行されると期間内の全ての情報を返す。

最後に、アクセスする期間を 2005 年 11 月 1 日から 2005 年 12 月 20 日から 2005 年 10 月 1 日から 2005 年 12 月 20 日に変更してアクセスを行いその結果を以下の図 7.6に示した。

以上のようにアクセス制御機構の動作検証として、正常なアクセス、メソッドを変えた場合、期間を変えた場合において、ポリシに記述された通りに許可、拒否が行われた。つまり、ユーザのポリシに応じて、様々なアクセス手法や期間を区切ったアクセス制御が実現でき、その動作が検証できた。

```
###オーナ A（uid= 10000）のロールには my_doctor と my_trainer がある。
ecare% psql biss
biss=# SELECT * FROM role_info WHERE owner_id = 10000;
 owner_id |   role_name   | role_id |  policy_file  |
----------+---------------+---------+---------------
  10000   |   my_doctor   |   10    | mydoctor.xml  |
  10000   |   my_trainer  |   11    | mytrainer.xml |
(2 rows)

#ユーザ B(uid=12345) に割り当てられたオーナ A のロール
biss=# SELECT * FROM user_role WHERE user_id = 12345 AND owner_id = 10000;
 owner_id |  user_id  | role_id |
----------+-----------+---------
  10000   |   12345   |    11   |
(1 rows)
```

図 7.2: ロール情報

```
###オーナ A のポリシファイル mytrainer.xml

ecare% cat mytrainer.xml

--------省略----------
      <Object>
        <item>
          <oname>weight</oname><!--対象となる項目-->
          <duration> <!--対象時間-->
            <b_time>2005/11/01 0:00:00</b_time>
            <e_time>2005/12/20 23:59:59</e_time>
          </duration>
          <method>delta_view</method><!--許可されるメソッド-->
         </item>
--------省略----------
```

図 7.3: ポリシファイル

```
### アクセス実行結果 (ユーザ ID 12345、対象ユーザ 10000、項目 体重、メソッド 詳細表示 )

ecare% java BissAccessTest -u 12345 -o 10000 -i weight -m delta_view \
                    -bt '2005-11-01 0:00:00' -et '2005-12-20 23:59:59'
connecting BServer...
[Send] Request Access
[Receive] Access check OK!
[Receive] delta_view result = 6.3 kg
connection closed...
ecare%

##アクセス許可が行われた。
```

図 7.4: アクセス実行結果

```
### メソッド変更例 (アクセスメソッドを delta_view から detail_view に変更)

ecare% java BissAccessTest -u 12345 -o 10000 -i weight -m detail_view \
                    -bt '2005-11-01 0:00:00' -et '2005-12-20 23:59:59'
connecting BServer...
[Send] Request Access
[Receive] Access check NG! (not permitted access method)
connection closed...
ecare%

###アクセスが拒否された。
```

図 7.5: アクセス実行結果 (メソッド変更時)

```
### 期間変更例 (アクセスする期間を"2005/10/01 〜 2005/12/20"に変更)

ecare% java BissAccessTest -u 12345 -o 10000 -i weight -m detail_view \
                    -bt '2005-10-01 0:00:00' -et '2005-12-20 23:59:59'
connecting BServer...
[Send] Request Access
[Receive] Access check NG! (not permitted access duration)
connection closed...
ecare%

###アクセスが拒否された。
```

図 7.6: アクセス実行結果 (期間変更時)

7.2　定性的評価

本節では、本システムと既存研究とを比較し、定性的評価を行う。本システムが既存手法と比較して、要求事項をどのように満たしているかを示す。表 7.1が他既存手法との比較を示している。

本研究では、個人が生体情報の管理を行う、つまり、自らの選んだ専門家や友人と生体情報の共有を行う事が必要である。そのために、アクセスポリシは個人が設定できなければならない。また、アクセス制御パラメータとして、時間を区切ったアクセス、多様なアクセス手法に対するアクセスが制御できなければならない。さらに、ユーザが選んだ人間以外のアクセスを認めない、つまり開示範囲を適切に設定できる事も必要である。以上の三点が本研究のアクセス制御に対する要求項目である。表 7.1の通り、要求項目を全て満たすシステムは存在しない。よって本システムは他研究と比べ、有用である事が示せた。

本システムでは、ポリシを作成、編集するのはオーナだけであり、またロールはオーナごとに存在し、オーナが自由に作成、編集が行える。さらに、アクセス制御のパラメータもポリシファイル内に`<Object>`で囲まれたタグ内に記述する事により、時間の範囲指定、メソッドの指定を行う。メソッドは拡張可能な方式で記述できなければならないが、本システムではポリシファイルは XML Schema に基づいており、スキーマを変更することで拡張可能である。ロールに対するユーザ割り当てを変更する事によって、ユーザが開示範囲を設定でき、そのユーザ以外に自らの生体情報を開示する事はできない。本システムはプロトタイプ実装であるため、実装上の洗練などの必要はあるが、最低限の要求事項は全て満たしている。

表 7.1: アクセス制御機構に関する定性的評価

	設定者	アクセス制御パラメータ		開示範囲
		時間	アクセス手法	
e-Fitness.com	個人	△	△	△
在宅健康管理システム	機関	×	×	×
バイタルケアネット	個人	×	×	△
本システム	個人	○	○	○

7.3　考察

本研究では、個人が生体情報の管理を行う事で、一貫性のある健康管理サービス等を受ける事ができるモデルを提案した。インターネット上で生体情報の管理を行う際の問題点として、情報の保存場所やアクセス制御に関して検討を行い、生体情報の利用モデルを示した。さらに、その利用モデルに基きプロトタイプとして BISS（Biological Information Sharing System）を設計、実装し、動作の検証、定性的評価を行った。その結果、本システムは検討通りの動作が確認でき、既存の他システムなどと比べて有用である事が示された。すなわち、本モデルが有用であるという事が示せた。

本研究のモデルでは、個人が所有権を持ち個人が全ての生体情報を管理する。個人が全てを管理するという事は、個人情報としては当然の事である。しかし、現実、医療情報や健康診断の情報を自らで全て管理しているという人はごく一部でしかない。その理由としては、

管理する情報が大量で管理コストが高く、また生体情報には他の情報と違い専門知識のない人々がどう開示、共有していいのかの判断を行う事が難しいという事が挙げられる。そのため、医療機関や組織に管理を委譲している。しかしながら、現在は自らが管理が行える、または、行いたいという人々も自分で管理するというモデルがないために、自らで管理できないというのは問題である。本モデルは生体情報の管理手法の一選択肢となる事が重要であると考えている。

本システムはプロトタイプとして実装を行ったため、システムとしては改良すべき点は様々な点が存在する。アクセス制御機構の本体部分以外に関してはまだまだ洗練の余地が残されている。実運用に際し、ユーザ ID の効率的な割り振りや、ユーザ管理機構の規模性、ユーザ認証の仕組みなど考えなければならない点は多々ある。しかし、提案モデルに基づいた本システムは機能要件を満たしており、動作は検証できた。その結果、本モデルは、個人を中心とした、アクセス制御を行える生体情報共有機構を実現するものである事が示せた。

7.4　まとめ

本章では、実装した本システムの動作検証、モデルからの機能による定性的評価を行い、考察を行った。次章では結論と今後の課題について述べる。

第8章　結論

8.1　まとめ

本研究では、個人を中心とした一貫性のある健康管理のために、家庭や様々な機関、場所において取得した生体情報を、専門家や他人とインターネットを通して共有する新たな情報利用モデルを提案した。さらに、そのモデルに基づいたアクセス制御機構を構築した。

現在、生体情報をバイタルセンサなどによって取得し、その情報をインターネット上で共有する事により、時間や場所などに依存しない健康管理サービスが多数存在している。しかし、その多数のサービスは各々が独自に生体情報の収集から利用までを行っていて、ユーザがサービスを透過的に受ける事は難しい。

本研究では、生体情報を組織やサービスによって分断されず、個人の生体情報を一元的に用いる事、さらに個人が全ての情報を管理し所有権を持つ事、最後に、その情報をインターネット上で共有する際に必要なアクセス制御を実現できるモデルを考案した。そのモデルに基づき、プロトタイプシステムの実装を行った。さらに、本システムの動作検証、他既存研究との定性的評価を行い、本システムの期待通りの動作が確かめられ、また他研究と比べて定性的に優れている事がわかった。その結果、本モデルの有用性を示す事ができた。

8.2　今後の課題

以下に本システムの今後の課題をまとめる。

- **ユーザインターフェース**

  本研究では、プロトタイプシステムとして動作が確認できるレベルでの実装を行った。本システムを実運用する際に、様々なユーザが利用できるユーザインターフェースは必要不可欠である。本モデルの基盤の上で専門家等との情報共有を行う際に、汎用性の高いユーザインターフェースとしてWWWを用いて情報の共有を行える仕組みを作成していく事などが考えられる。

- **ユーザビリティ向上**

  本研究では個人が全てを管理するというモデルであり、管理する情報が大量に存在する際に逐一設定していのはユーザのコストが高い。また、ユーザがシステム上のメソッドを知らなければならない事など本システムを実際に運用するためには、ユーザビリティの向上は不可欠である。ユーザビリティの向上としては、ポリシ設定時のユーザインターフェースやポリシのサンプルなどを用意するなどが考えられる。

- **ユーザ管理における規模性**

本研究のモデルをシステム化する場合に規模性というものは考慮すべき事項である。今回プロトタイプ実装としてユーザ管理の手法に関しては、既存のデータベースシステムを用いた。しかし、データ管理モデルとして、DNS(Domain Name System) のような階層型のモデルや P2P 型のモデルなど様々な規模性に富んだモデルが考えられる。また、データの分散管理を行った際には、問い合わせプロトコルなども変わってくる。今回は単一サーバ上に RDBMS を用いて管理を行ったが想定するユーザ数が 10 万、100 万となってきた場合に現実的ではなくなる。ユーザを一意に管理するためのシステム的な規模性を考慮したモデルをは今後構築していかなければならない。

- **アクセスメソッド間の関係定義**

  本研究においてアクセスメソッドに関しては今回、上下関係に関して詳細に表示する際は全てのアクセスメソッドを許可するという二階層な関係性を定義した。しかし、データの間引き方には上下関係が存在し、元の情報からの距離を元に関係性を記述が可能である。アクセスメソッドが増えた際に、上下関係を定義でき、アクセスメソッド間の関係性を定義する事でユーザの利便性は上がる。

以上を持って本稿の結論とする。

謝辞

本研究を進めるにあたり、ご指導をいただきました慶應義塾大学 環境情報学部教授 村井純博士、同学部助教授 中村修博士、同大学看護医療学部専任講師 宮川祥子博士に感謝します。また、日々厳しく助言いただいた慶應義塾大学環境情報学部専任講師 重近範行博士、同大学政策・メディア研究科 特別研究講師 南政樹氏、同大学中根雅文氏、同大学 羽田久一博士、同大学政策メディア研究科特別研究助手 内山映子博士に感謝します。また、日々の研究活動から公私にわたるまで様々な面倒を見ていただいた慶應義塾大学政策・メディア研究科 小原泰弘氏、慶應義塾大学政策・メディア研究科 三屋光史郎氏、東京大学助手 今泉英明博士、他諸先輩方に感謝します。

また、研究室に入った時からの仲間で様々な苦楽を共にした同期の慶應義塾大学政策メディア研究科修士課程二年 廣瀬峻氏、同大学山本聡氏、同大学成瀬大輔氏をはじめとする諸氏に感謝します。

日々の研究活動、また修論提出直前まで修士論文を支えてくれた後輩達、慶應義塾大学 環境情報学部 奥村祐介氏、同大学 政策・メディア研究科 小椋康平氏、同大学政策・メディア研究科 谷隆三郎氏、同大学同学部 空閑洋平氏、同大学同学部 水谷正慶氏をはじめとするその他 SING/IA メンバーである z203 の諸氏に感謝します。

また、学部時代より、私の研究の場を与えていただいた e-ケアタウンプロジェクトに感謝の意を表明します。さらに e-ケアタウンプロジェクトを支えてきた n109 の皆様、全てのスタッフに感謝の意を表明します。

徳田、村井、楠本、中村、高汐、湧川合同研究会全ての諸氏に感謝します。

最後にいつも見守り励ましてくれた小竹宏子氏に感謝を捧げます。

2006 年 1 月 12 日

橋本和樹

参考文献

[1] 財団法人 健康・体力づくり事業財団. 健康日本 21. http://www.kenkounippon21.gr.jp/.

[2] ASAHI BREWERIES. 食と健康のセンサス 2001 株式会社アサヒビール お客様生活研究所. http://www.asahibeer.co.jp/aboutus/research/culture/report_001/2001.html.

[3] Y. Ohgi and H. Ichikawa. Microcomputer-based data logging device for accelerometry in swimming. the engineering of sport 4. ujihashi. s. and haake s. j. eds.. pp637-643, Sep 2002.

[4] オムロン ヘルスケア株式会社. Walking-style.com omron inc. http://www.walking-style.com/.

[5] 株式会社 コンビウェルネス. e-fitness クラブコンビ. 株式会社 コンビウェルネス. http://www.club-combi.com/.

[6] TANITA. Health planet. (株)tanita. /urlhttp://www.tanita.co.jp/.

[7] 健医療福祉情報 システム工業会. 検診データ交換規約 v1.3. JAHIS（保健医療福祉情報システム工業会）標準 (2001/4 制定).

[8] 健医療福祉情報 システム工業会. バイタル・データ通信仕様 v1.0 part1. JAHIS（保健医療福祉情報システム工業会）標準 (2001/7 制定).

[9] MedXML コンソーシアム. Mobile markup language(mml). http://www.medxml.net/MML/default.htm.

[10] Health Level Seven. Health level seven (hl7). http://www.hl7.org/.

[11] Eamonn J. Keogh, Kaushik Chakrabarti, Michael J. Pazzani, and Sharad Mehrotra. Dimensionality reduction for fast similarity search in large time series databases, May 2001.

[12] e ケアコンソーシアム. e ケアタウンプロジェクト. http://www.e-care-project.jp/.

[13] 在宅ケア支援システム検討 WG. 在宅健康管理システム: Jahis（japanese association of healthcare information systems industry）. http://www.jahis.jp/.

[14] Tsutom Nishioka, Toshiyuki Kikuchi, and Takashi Nanba. 健康増進システム: 医療福祉機器研究所. http://www.hitachihyoron.com/2005/08/08a05.html.

[15] 特定非営利活動法人 ウェアラブル環境情報ネット推進機構. バイタルケアネット: Npo ウェアラブル環境情報ネット推進機構. http://www.npowin.org/j/.

[16] 南政樹, 橋本和樹, 廣瀬峻, 谷隆三郎, and 横山祥恵. 介護・看護をサポートするネットワークコンピューティング環境, May 2003. 情報処理学会 システムソフトウェアとオペレーティングシステム研究会.

[17] 内山映子. **療養型ヘルスケアサービスにおけるコンシューマ中心型情報共有・保護環境の構築に関する研究**. PhD thesis, 慶應義塾大学, Oct 2005.

[18] 橋本和樹, 廣瀬峻, 横山祥恵, 南政樹, and 村井純. 家庭用フィットネス機器を用いた遠隔コーチングシステムの設計と実装, May 2003. 情報処理学会システムソフトウェアとオペレーティングシステム研究会 (2003-OS-93).

[19] 橋本和樹. 遠隔コーチング環境実現のためのフレームワーク構築に関する研究, Jan 2003. 慶應義塾大学 環境情報学部 卒業論文.

[20] 橋本和樹, 廣瀬峻, 横山祥恵, 南政樹, and 村井純. インターネットトレーニングシステムの構築と評価, May 2004. 電子情報通信学会 モバイルマルチメディア研究会 (MoMuC 2004).

[21] Iso - international organization for standardization. http://www.iso.org/.

[22] Organisation for economic co-operation and development. http://www.oecd.org/.

[23] Guideline for management of it security(gmits), 2000. ISO technical report; ISO/IEC TR13335.

[24] J. Anderson. Computer security technology planning. study, Oct 1972. ESD-TR-73-51, volumes I and II, USAF Electronic Systems Div., Beford Mass.

[25] D. E. Bell and L. J. Padula. Secure computer systems: Mathematical foundations and model, 1973. National Technical Information Service. Bedford. MA. M74-244 (Available as AD-771543 Springfield, VA.).

[26] K. J. Biba. Integrity consideration for secure computer system, 1975. MTR-3153, MITRE Corporation; ESD-TR-76-372.

[27] Timothy Fraser. Lomac: Low water-mark integrity protection for cots environments. pages 230–245, 2000.

[28] David D. Clark and David R. Wilson. A comparison of commercial and military computer security policies. pages 184–194, Apr 1987.

[29] David F.C. and Michael J. Nash. The chinese wall security policy. pages 206–214, May 1989.

[30] Phil Kearns and Serge Hallyn. Deriving tools to administer domain and type enforcement. pages 151–n155, Dec 2001.

[31] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. *IEEE Press*, 29(2):38–47, Feb 1996. http://csrc.nist.gov/rbac/sandhu96.pdf.

[32] *A framework for multiple authorization types in a healthcare application system*, 2001. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=991530.

[33] Qingfeng He and Annie I. Anton. A framework for modeling privacy requirements in role engineering, Dec 1998.

[34] 大西浩文, 明石浩史, 戸倉一, 山口徳蔵, 西城一翼, 西陰研治, 中山正志, and 辰巳治之. 万歩計と行動科学を応用した次世代健康管理システムの試み. 15, Nov 2002. http://www.itrc.net/report/meet12/A11/ITRC12-oonishi.pdf.

[35] Affelio project. Affelio - the open social network-. http://www.affelio.jp/.