NAIST-DT0061003

博士論文

インターネットにおける
実空間情報の流通制御に関する研究

和泉 順子

平成 15 年 11 月 6 日

奈良先端科学技術大学院大学
情報科学研究科 情報システム学専攻

本論文は奈良先端科学技術大学院大学情報科学研究科に
博士 (工学) 授与の要件として提出した博士論文である。

論文番号:　DT0061003

報告者:　和泉 順子

審査委員:　砂原 秀樹 教授
山口 英 教授
藤川 和利 助教授

提出日:　平成 15 年 11 月 6 日

インターネットにおける
実空間情報の流通制御に関する研究*

和泉 順子

内容梗概

情報技術の発達にともない、さまざまな分野にも計算機が導入され、実空間で扱う情報の電子化が行われている。情報とは一般に、判断を下したり行動を起したりするために必要な知識であり、実世界には、交通標識、蔵書目録、気象情報、仕様書など、複雑な情報が多様に存在する。

近年、これらの各種情報の電子化により、その情報管理や業務の効率化を図られている。また、計算機の高機能化・低価格化にともない、電子化した情報を流通させる手段、つまり、情報通信基盤として、インターネットが広く利用されるようになった。

インターネットに接続した計算機を用いることで、人々は、空間的または時間的な制約を越えて多くの情報を検索・取得し、世界中の人々との情報交換や容易な情報発信が可能となる。学術情報通信基盤として登場したインターネットは、現在では、学術分野に限らず行政や金融、医療、交通、各種メディアなどの情報をも流通させる、社会基盤としての役割を担っている。

しかし、情報流通基盤の整備とは対象に、その情報の流通制御に関しては、対応が遅れ気味である。たとえば、インターネットの持つ匿名性、空間制約の撤廃、情報発信や公開の容易さ等の特性から、インターネット上でのプライバシ情報の取り扱いは、実世界のプライバシ侵害の問題と比較して複雑化している。実空間に存在する情報規制や法整備だけでは、インターネット上で発生するプライバシ侵害への対応は十分に行えない。つまり、プライバシ侵害の対象となる実世界のエンティティに帰属した情報の流通制御および管理が必要である。

そこで、本研究では、情報通信基盤としての社会性を持つインターネット上のサービスとそこで扱う情報流通の検討を通じて、インターネットにおける実空間情報の流通制御を提案する。

まず、従来のプライバシ侵害とインターネット上でのプライバシ侵害との相違を明らかにした上で、インターネット上のプライバシ侵害の特徴が、情報制御の困難さに起因するものであり、少なくとも従来のような規制強化だけでは不十分であることを説明する。たとえば、実世界での位置情報や活動履歴を含む情報は、位置情報を発信した利用者が特定可能である場合、時刻や他の情

報と組み合わせ分析することにより利用者の位置を追跡したり、個人的嗜好、消費行動などを把握することができるため、インターネット上ではプライバシ (個人情報) に関わる情報とされる。実空間の物理的な位置情報をネットワーク上で扱う際に、計算機を特定可能な ID を用いることは、インターネット上への個人情報の流出につながる。そこで、このような個人情報の不特定多数に対する無制限な流出を防ぐため、システム上で疑似識別子 (pseudo ID) を導入し、蓄積する個人情報は暗号化により保護した地理的位置情報管理システムの一提案とプロトタイプの設計を行った。

また、インターネットに接続されたセンサデバイスから実空間をプローブすることにより、情報価値の再認識と新たなサービスの発現が期待されている。たとえば、実空間に存在するエンティティとして世界中に数多く存在し、広範囲に移動する自動車を考えた場合、自動車がインターネットを介して外部社会と常時接続され、自動車のセンサデバイス情報をインターネット上に集約することで、ITS および GIS などの関連サービスの多様性と空間的・時間的広がりが得られる。

インターネット ITS プロジェクトでは、インターネットがそのオープン性を活かした情報通信基盤となることの意味について検討し、ITS 関連サービスに対する共通インタフェースの提供と、情報通信基盤仕様の策定、実現されるサービスイメージの分類等を行った。プロトタイプ車の作成や、名古屋および首都圏における大規模実証実験を通じて、インターネットを情報通信基盤として用いる様々な分野の今後のサービスの在り方と、個人情報保護を前提とした情報流通の関心の高まりを確認した。

このように、個人情報を保護した位置情報という実空間情報の管理を目的としたプロトタイプシステムの設計や ITS 分野でのサービスと市場動向調査を行った上で、利用者の移動を前提としたユビキタス環境における連続的なサービスや資源を提供するために必要な環境について検討を行った。つまり、移動してきた利用者に対して各サービスドメイン内部のポリシを反映した利用者認証および資源へのアクセス制御や権限委譲などの処理が必要であるため、公開鍵暗号基盤技術を用いたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案した。これは、利用者が自分のホーム環境で定義された個人証明書を携帯し、移動先にその証明書を適宜提示することで、移動先でのサービス提供を要求する。各サービスドメイン内では、定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけ、アクセス制御や権限委譲などの処理を行う。つまり、利用者の持つ実空間情報を検証することで、移動先でも、その場所のポリシに沿った適切な形でのサービスおよび資源などの情報を流通させ、利用することが可能となる。

キーワード: 実空間情報、移動体通信、位置情報、プライバシ、自己証明

奈良先端科学技術大学院大学 情報科学研究科 情報システム学 博士論文 NAIST-DT0061003, 平成 15

年 11 月 6 日

Studies on the distribution control dealing with real-spatial information on the Internet[†]

Michiko IZUMI

Abstract

The advance of information technology has been very rapid in recent years. Computers are introduced on the various fields, and information which is used in the real-world has been digitalized. Information usually means the knowledgement to decide something or to act. In the real-world, there are a number of information such as a road sign, a library catalogue, a weather report, a specification, and so on.

Nowadays there is a growing digitalization tendency which includes the real-world information among the research, business, or other areas for the management and efficiency. Then, the Internet have come into wide use recently as a way to distribute the digital information, that is, as a communication infrastructure.

The Internet provides the universal communication infrastructure with various equipments such as vehicles, home appliances, and computers. I can retrieve or obtain enormous informations without inconvenience from time limitation or the borders using the computers which connect to the Internet. Moreover, I are able to communicate with the people in the world easily for sending our messages to the world. The Internet is now grown up as the social infrastructure which is related to various field like research, social administration, medical technology, financing, and whatnot.

In comparison with the deployment of this infrastructure, the distribution control for the information on the Internet has been fall behind. For example, the treatment of privacy on the Internet is complicated since the peculiarity, that is, anonymously and simple way to send the messages to the world. Legal Control in real-world is not enough to keep privacy secure on the Internet. Thus, I need the distribution control for the information belonging to the entities in

the real-world.

First, I have studied for the privacy on the mobile computing, especially the tracking of geographical location information. For protecting the privacy which corresponds to real-world spatial information, I had introduced the pseudo ID, and designed the prototype system.

Then cars are adopted as a real-world entity, some sensor devices of car can probe real-world information. I can collect several information from vehicles including location information, speed, brake status, switch position of wipers, even if the exhaust gas. Using these data, several useful information can be created. For example, current weather/rain condition are created from location information and switch position of wipers. At InternetITS project, I had discussed the open, common communication infrastructure with some members from ITS field like automobile industry to make full use of real-world information from sensors of car. I had developed the specification of the common infrastructure, and also summarized primary result of in-the-field pilot programs.

The studies for the seamless communication are now tackled cause of popularization of the advanced mobile computing. Most of concerned topics are to establish of transparency of communication on the IP Layer, not to guarantee the seamlessness of services between the networks which have different management policies. That is why, the services which across some domains are divided and forced to restart even the same service are provided.

In this paper, I indicated the problem is caused that the authentication and authorization mechanism have a close relation, and these mechanism depended on specific services. The solution of this problem is consisted to separate these mechanism, and to bring up a new paradigm, which is composed the selective service provider based on the self(client) certificates. The concept is the dynamic negotiation using the profile of the entity and management policies. I have shown the availability of this new model using the application of PKI framework. Moreover, I have also derived profound considerations for the direction of the future works.

Keywords: real world information, mobile computing, spatial information, privacy, self-certificate

---

Ḋoctor Thesis,Department of Information Systems, Graduate School of Information Science,Nara Institute of Science and Technology,NAIST-DT0061003, 6 November, 2003

目次

図一覧

表一覧

Chapter 1

序　　論

本章では、研究の背景として、実空間における情報の電子化と、その流通手段としてのインターネットの発展および利用形態の変遷について概説する。また、研究の目的および位置づけと、本論文の構成について述べる。

1.1. 実空間の情報とインターネット

情報科学の発達と計算機技術の発展に伴い、人間が生活する実空間の情報が電子化される、いわゆる「情報化社会」が形成されつつある。電子化された情報は、複製や保存などの取り扱いが容易であることから、技術的または社会的に広く受け入れられており、現在では、業務情報の電子化だけでなく、行政や医療などの実空間の生活を支える情報や個人情報までも、電子化されて扱われている。本節では、実空間の情報とインターネットとの関わりについて述べる。

1.1.1. 実空間情報の電子化とその流通手段

情報とは、判断を下したり行動を起したりするために必要な知識であり、実空間においては、交通標識、蔵書目録、気象情報、業務契約書、仕様書、医療カルテ、戸籍謄本、給与明細など、複雑な情報が多様に存在する。情報を電子化することで、情報の劣化を防ぐと同時に、情報管理や業務の効率化を図ることができるため、近年の情報科学技術と計算機技術の発展にともない、学術分野だけでなく、通信、エネルギー、交通、金融、メディア、医療、流通などの重要な社会基盤に基づく実世界の情報をも電子化され、管理されるようになった。

これら電子化された情報は、いままでの情報流通手段であるマスメディアではなく、論理的なネットワークの集合体であるインターネット上で流通している。インターネットに接続した計算機を用いることで、人々は、空間的または時間的な制約を越えて多くの情報を検索・取得し、立場や国境を越えて多くの人々と情報交換することが可能となる。つまり、一方から他方への一方向の情報公開および発信にとどまらず、双方向または、個人から不特定多数への情報検索や情報発信が行われる。

たとえば、ネットオークションではインターネットを介して実空間の個人的な売買契約が行われている。電子掲示板では、実空間における一個人によって自由な発言や情報発信が可能であり、時にはマスメディアを動かすほどの物議を醸すことできる。また、銀行業務や行政手続きの一部、チケット予約などのビジネスとしての情報公開や取引など、社会的サービスとしても、インターネットは広く一般の人々に受容されている。

このような情報化社会の形成を後押しするかのように、平成 13 年 1 月、内閣府に「高度情報通信ネットワーク社会推進戦略本部 (IT 戦略本部)」が設置され、情報通信技術の活用による社会経済構造の変化に適確に対応することの緊要性の検討と、高度情報通信ネットワーク社会の形成に関する施策が迅速かつ重点的に推進しされている。また、住民基本台帳ネットワークサービスの開始など、電子政府や行政的なサービスの電子化についても深く議論されている。

このように、学術情報通信基盤として登場したインターネットは、現在ではその規模性と柔軟性を活かし、様々な実空間情報を流通させる社会基盤としての役割を担っていると云える。

1.1.2. インターネットの普及と情報発信の主体の変化

情報流通基盤の整備とは対照的に、その情報の流通制御に関しては、対応が遅れ気味である。たとえば、住民基本台帳ネットワークでは、個人情報流出や情報管理・運用の安全性などの問題に関して、平成 14 年 12 月現在も議論が続いている。このように、法整備不十分さに加えて、インターネットの持つ匿名性、空間制約の撤廃、情報発信や公開の容易さ等の特性から、インターネット上でのプライバシ情報の取り扱いは、実世界のプライバシ侵害の問題と比較して複雑化している。

従来、実空間の情報を発信する主体の多くは、新聞やテレビやラジオといった放送機構などに代表されるマスメディアであり、誤った情報の発信や、私的な情報の暴露など、プライバシ侵害に関する問題は、法の整備などの規制強化を行うことである程度の秩序が保たれていた。しかし、新聞や放送、大衆動員やビラ配布などが情報伝達、公開、発信の媒体であると同時に、今日では、インターネットが電子化された情報の発信に関する重要媒体に成長している。インターネット上に発信される情報は、情報発信の主体の多くが一般の人々、つまり実空間上での一個人であり、インターネットの持つ匿名性や空間制約の撤廃などから単一国家の法規制やその他情報規制だけでは、個人のプライバシ侵害に関する対応は十分に行えない。つまり、インターネット上で提供されるサービスにおけるプライバシ侵害の特徴は、情報制御の困難さに起因するものであり、個人レベルの情報発信活動に関しては未だに流通制御ができていない。プライバシの侵害を防ぐためにも実世界のエンティティつまり、実世界の情報発信者および利用者などに帰属する情報の流通制御および管理が必要であると考える。

1.2. インターネット接続の環境変化への対応

前節までに、電子化された種々の実空間情報がインターネットという情報通信基盤を用いて流通していることを述べた。ここでは、計算機の利用形態やインターネット接続環境の変遷による流通する実空間情報の変化について概説する。

1.2.1. 移動体通信環境の整備と普及

そもそも、人類は交通手段を発展させることにより、個人の活動範囲を広めてきた。インターネットが情報通信基盤として普及した現在でも、個人の活動範囲の広域化が、産業の多様化と発展につながっている。

インターネット技術や無線技術の発展と、計算機の高機能化と低価格化、小型軽量化に伴い、計算機の利用形態に変化が現れるようになった。かつては、固定計算機をネットワークの集合体であるインターネットへ有線ケーブルを用いて接続していた。しかし、現在では、多くの人が PDA やノート PC、携帯電話などの計算機を持ち歩き、無線通信を用いていままでの有線接続と同様のインターネット上の情報やサービスを利用している。また、遍在する公共端末や移動先の計算機を用い、計算機や情報家電、センサデバイスなどを連動させることで、計算機を持ち歩くことなく、インターネット上のサービスを利用することもできる。このように、移動体通信環境の整備と普及により、インターネット上にある電子的な情報や資源、サービスなどを「いつでもどこでも」利用することが可能となった。

行政的にも、e-Japan 重点計画 - 2002 [1] においてシームレスな移動体通信サービスの必要性が議論されている。ここでは、将来イメージとして、世界最高水準の高度情報通信ネットワークの形成のためのシームレスな移動体通信サービスが高度道路交通サービスやその他関連技術と連携した上で確立されることを検討している。

このように、移動体通信環境に対する期待は大きく、その環境整備と普及が進んでいる。しかし、遍在する計算機から実世界をプローブすることによって発現する新しいサービスの提供が可能になると同時に、位置情報や活動履歴などの動的な情報を含む個人情報の定義とその流通方法などに関する問題が発生するようになった。

1.2.2. 実空間に帰属する情報

移動体通信という、インターネットの利用法の変遷により、インターネット上で扱う情報も変化してきた。たとえば、位置検出装置の開発とそれに伴う位置情報サービスの発現や、実空間のエンティティに属するセンサから情報をプローブするサービスなど、実空間の動的に変化する情

報を収集・蓄積・加工することで、交通情報、気象情報、出欠確認、人や車の探索など、さまざまなサービスに応用が可能である。

しかし、このように実世界での位置情報や活動履歴を含む情報は、位置情報を発信した利用者が特定可能である場合、時刻や他の情報と組み合わせ分析することにより利用者の位置を追跡したり、個人的嗜好、消費行動などを把握することができるため、インターネット上ではプライバシ(個人情報) に関わる情報とされる。実空間の物理的な位置情報をネットワーク上で扱う際に、計算機または個人を特定可能である識別子 (ID) を用いることは、インターネット上への個人情報の流出につながる。このようなことを防ぐためにも、実空間情報に帰属する、情報流通のための制御機構が必要であるといえる。

1.2.3. インターネットミドルウェアの活用

移動体通信環境の普及や、それにともなう実空間に帰属する情報の流通など、社会基盤として認知されているインターネットは、データの転送という基本機能はもとより、快適で安定、安全なサービス機能が今まで以上に重要となっている。

この基本通信機能の上位機能としてネットワーク上の通信負荷をバランスさせる機能や安全なサービスを提供するための認証やユーザ管理機能などのように、複数の要素を連携させて利用者にとって使いやすく快適な環境を創出する技術の総称として、インターネットミドルウェアが存在する。

インターネットミドルウェアは、サービス、利用者、ネットワーク機器の間の仲介役となる機能層である。複数のサービスを独立に発展させつつ、利用者からはまとまりのあるサービス群として意識させることが、サービス連携に関するミドルウェアであり、ネットワークを構成する個々の要素 (伝送機器、ルータなどのネットワーク機器) に関して、連係動作の促進とネットワーク全体のサービス品質維持のための制御することが、ネットワーク連携に関するミドルウェアである。どちらのミドルウェアも、複数サービスと利用者間の関係や個々のネットワーク機器と提供サービス間の関係を、ネットワーク全体の視野から制御したり介在したりする機能である。

今後のインターネットのもつ役割としてはは、情報収集だけでなく収集した情報、特に実空間の情報を基に情報を蓄積・解析・加工し、自由に発信していく、動的な情報受発信が増加するものと予測される。

インターネットは今後、社会活動の様々な場面で一つひとつの要素のみならず、利用者が享受するサービスの視点から、ネットワーク全体をマネジメントし、また、機器利用の効率をあげていくことが重要であると考える。

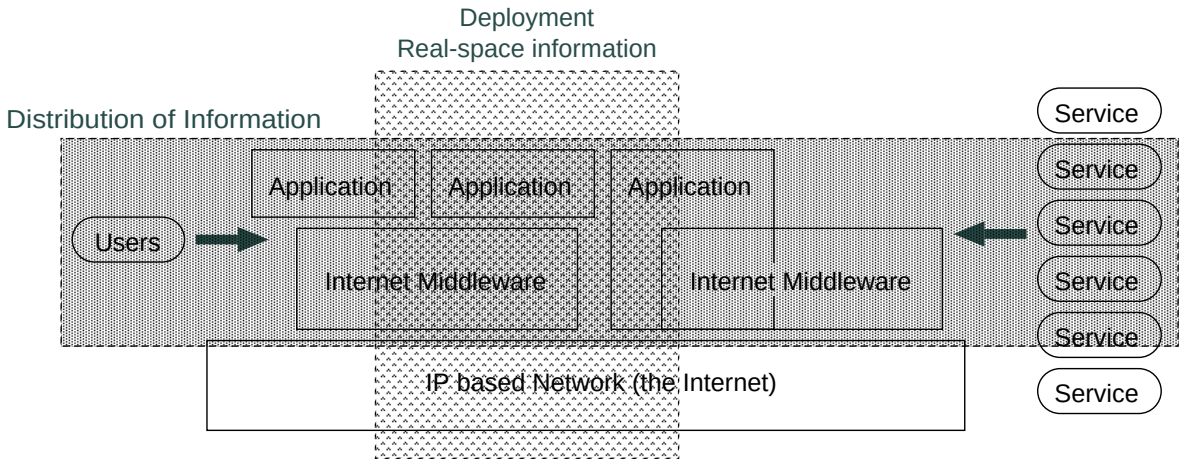

図 1.1: 研究の位置づけ (インターネットと流通制御)

1.3. 本研究の取り組みと位置づけ

インターネットが各種情報通信基盤として普及し、インターネット上の情報サービスは社会へ情報を提供する基盤としての役割が大きくなっている。この大きな局面を迎えて、インターネット上の情報サービスに関する研究は計算機や通信の分野だけでなく、広く社会の様々な分野のサービス連携を視野に入れて進める必要がある (図 1.1)。

したがって本研究では、移動体通信環境を前提とし、主に位置情報や個人情報などの実空間情報をあつかう流通制御について、ミドルウェアの構築とサービス連携の視点に基づく実空間エンティティに帰属した実空間情報の流通制御とサービスの在り方について検討する。

1.3.1. 位置情報システムとプライバシ

具体的には、まず、ミドルウェアの構築として移動体通信における位置情報を含む個人情報保護を考慮にいれた情報流通制御に関するプロトタイプシステムの設計を行う。

今日では、位置検出装置の研究開発と、無線技術や移動体通信環境の普及にともない、移動体の物理的な位置情報の有用性が増加し、位置情報システム、位置指向の情報検索サービスの需要が増加している。様々な位置検出装置の得失と、それに基づくサービスや、適応範囲について述べる。また、移動体通信での保護の対象となるプライバシとは、なにか、という点において、個人情報を定義する。これらを検討を通じ、情報発信者とも情報利用者ともなりうる移動体の物理的な位置情報は保護すべきプライバシであると考える。そこで、実空間を移動するエンティティを計算機とし、これらの情報を流通制御するために、疑似識別子 (pseudo ID) を導入した位置情報システムのプロトタイプを設計する。これは、移動体通信において保護すべきプライバシは、サー

ビス利用者のユーザプロファイルなどの個人情報だけでなく、情報発信者の動的、かつ物理的な属性情報を含むべきであることを示している。

1.3.2. インターネット自動車

次に、実空間エンティティとしての移動体を自動車とした場合の、異分野からの意見集約とサービス連携について述べる。

自動車は、利用者の意思に従って共に広範囲を移動する、バッテリを搭載している、などの理由により、移動体通信環境における移動エンティティの代表として扱うことができる。また、自動車は、数多くのセンサデバイスが搭載しているため、実世界をプローブする装置としても機能する。自動車をインターネットに接続する場合の技術的な要件やサービスの在り方についてはすでに検討されているが、ここでは、自動車を移動体通信におけるセンサデバイスとして用いることで、情報科学分野だけでなく自動車産業や交通および都市工学などの他分野との協調、サービスの連携、産業の発展を図る。つまり、インターネットを共通の情報流通およびサービス基盤とすることで、社会的要請を反映した高度道路交通サービスの分類が可能となる。また、民官学が一体となり、一つの情報通信基盤として、共通開発基盤の仕様策定と構築を行い、サービス分類の検討と学術的な調査・検証を行った点は、社会に対する貢献という意味でもたいへん有意である。

また、移動体通信において、移動体に搭載されたセンサデバイスを用いることで実空間をプローブするサービスは、近年、その有意性を評価されつつある。一つの情報としてはあまり意味をなさないものでも、移動体が広域に分布した状態で、情報がインターネット上に発信・蓄積され、それらの情報が物理的、または時間的な集合を形成することで、大きな意味をもつことを示している。これは、情報家電の発展やアドホック、またはユビキタス情報基盤におけるサービス開発にも大きく寄与するものである。

1.3.3. 自己の証明に基づく選択的サービス提供モデル

最後に、サービスの連携の視点から、実空間エンティティとしての移動体、つまりコミュニケーションの主体を個人とした場合について述べる。

ここでは、まず、インターネット上の実空間情報に対して、ユーザプロファイルを用いる情報フィルタリング技術と、サービスに対する認証およびアクセス制御技術について考察する。情報フィルタリング技術は、主に利用者のプロファイルに基づく情報の流通制御であり、その手法は多数存在するが、個人情報保護の対象はサービス利用者であって、移動体通信環境における情報発信者 (情報提供者) の個人情報保護とは性質が異なる。これは、既存の情報流通制御機構が、サービス提供者と情報提供者を同義に扱っていたり、インターネット上の情報は「すでにあるもの」と

して、そのプライバシについては考慮していないことが起因している。また、ユーザプロファイルの構成要素として利用者の動的に変化する属性を考えた場合の運用ポリシとの動的な折衝による選択的なサービス提供については深く議論されていない。

また、既存の認証システムの多くは利用者本人として認証することとそのアカウントがサービスに特化しているため、異なる運用ポリシ間を移動した場合、移動先のシステムに対する事前の利用者登録手続きが必要となる。

そこで、移動体通信においては、情報発信者とサービス提供者は必ずしも一致しないことを示し、計算機や自動車、個人などの実世界に存在するエンティティに帰属した認証とその属性、という情報を認証ミドルウェアで流通制御するモデルを検討する。

ここでは、移動してきた利用者に対して各サービスドメイン内部のポリシを反映した利用者認証および資源へのアクセス制御や権限委譲などの処理が必要であるため、公開鍵暗号基盤技術を用いたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案する。これは、利用者が自分のホーム環境で定義された個人証明書を携帯し、移動先にその証明書を適宜提示することで、移動先でのサービス提供を要求する。各サービスドメイン内では、定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけ、アクセス制御や権限委譲などの処理を行う。つまり、利用者の持つ実空間情報を検証することで、移動先でも、その場所のポリシに沿った適切な形でのサービスおよび資源などの情報を流通させ、利用することが可能となる。

1.4. 本論文の構成

まず、第一部では、従来の実空間で生じるプライバシ侵害とネットワーク上でのプライバシ侵害との相違を明らかにする。移動体通信を前提とした場合の実空間でのエンティティを計算機とし、位置情報や活動履歴を含むプライバシ (個人情報) について定義をする。その後、位置情報に関連する個人情報の不特定多数に対する無制限な流出を防ぐため、システム上で疑似識別子 (puseudo ID) を導入し、蓄積する個人情報は暗号化により保護した地理的位置情報管理システムの一提案とプロトタイプの設計について詳細を述べる。

第二部では、インターネット自動車について説明する。実空間を移動するエンティティの一つとして自動車をとりあげ、それらがインターネットに接続することで、移動体、またはインターネット上のサービス利用者にどのような情報が提供されるかを検討する。また、高度道路交通システムについて概説を行い、その共通開発基盤、通信基盤として、インターネットを用いることを提唱したインターネット ITS プロジェクトについて、その概要と 2001 年度の成果について述べる。

第三部では、移動する実世界のエンティティとして、個人を取り上げる。コミュニケーション

の主体は個人であり、特定のサービスを利用するために、現在では通常、認証を行う。ここでは、既存の認証機構についての分類を行い、異なる運用ポリシを持つサービスドメイン間の移動に伴うサービス切断の改善を目的とした、ネットワーク資源提供のためのサービスモデルを提案する。また、このモデルを公開鍵暗号基盤のフレームワークに適用することでその実現可能性を示す。

最後に、第四部では研究の総括を行う。これらの研究を通して得られた知見を述べ、今後の課題と研究方針について整理を行う。

Part I

位置情報システムとプライバシ

Chapter 2

位置情報サービス

元来、位置情報の検出装置は、測量や航海などに必要な測位技術の発展にともなって研究開発されてきた。測位技術の高精度化および多様化が進むにつれ、移動体通信環境の整備として実空間の位置情報がインターネット上で扱われるようになり、一般の人々に対する様々なサービスが提供されるようになった。本章では、既存の位置情報検出装置と、それらをインターネット上で扱うためのミドルウェアとしての置情報システム (Location-Aware Systems)**、また、これらの上で展開される位置情報に基づくサービス** (Location Based Services) **などについてまとめる。**

2.1. 位置情報検出装置

ここでは、代表的な位置情報検出装置として、汎地球測位システム (GPS)、PHS、Active Badge(赤外線)、Cricket(RF および超音波)、RFID、の 4 つを挙げる。また、位置情報の検出方法と、その応用分野について触れる。

2.1.1. 汎地球測位システム GPS

GPS(Global Positioning Systems) は、人工衛星を用いた地球規模の測位システムであり、米国国防総省が戦艦の位置を正確に把握するために開発したものである。GPS は、大まかに以下の 3 つの部分により構成されている。

- 地球をカバーする 24 個の衛星で構成される「宇宙部分」
- 衛星の軌道の監視と発信電波の制御を行う「管制制御部分」
- 航空機や船舶等の位置を決定するための「利用者部分」

現在も管理は同省が行っているおり、同様の衛星を用いた測位としては、ロシアの GLONASS、または EU における GALLILEO と呼ばれるシステムがある。

GPS 測位の原理は、各 GPS 衛星 (ナブスター) からの電波の到達時間を元に衛星と GPS 受信機間の距離を算出できることから、複数の衛星との距離を用い 3 次元的な位置を算出する、というものである。

GPS 受信機の多くは、GPS 衛星からの電波を受信するアンテナと繋がっており、受信機側で受信した信号の解析を行う。

現在、GPS はカーナビ (Car Navigation System) が自分の車の位置を把握する際に最も頼りにするシステムであり、また、携帯電話に内蔵されているものも存在する。このシステムは現在、より精度の高い D-GPS(Differential GPS) に進化し、わずか数センチメートル以下の誤差でエンティティの位置を把握することができるまでになっている。

D-GPS では、まず地上にある基地局で各 GPS 衛星の電波の誤差を計算する。そこから得た誤差補正用のデータを FM 多重放送や中波ビーコンを通じて受信し、高い精度で誤差を補正して、より正確に測位する。ナブスターは、地球上の高度約 20,200km の 6 つの軌道上に各々4 個ずつ、全部で 24 個配置されている。これは、地球上のどの地点からも 24 時間つねに 4 個以上の衛星の電波が受信できるようにとの考えに基づくものである。ナブスターと地球との位置や測定に関しては、文献 [2] に詳述してある。

WIDE InternetCAR [3] プロジェクトでは、GPS に加えて補正情報を利用することにより、インターネットに接続された移動体である自動車の測位の精度を上げることを試みている [4]。そのため、D-GPS を行うために必要となる補正情報をインターネットを通じて配布するための基盤の構築とその改良を行っている [5]。

都市工学などの高精度測位社会基盤を検討する分野では、GPS 測量の精度向上や生産性向上を図るための仮想基準点 VRS(Virtual Reference Station) および GPS を補完する技術として注目されている pseudolite などの技術 [6, 7] も検討されている。

2.1.2. PHS

今日では、PHS を通じてノートパソコンや携帯情報端末などを利用し、移動時や屋外でも 32Kbps の高速データ通信が可能となっている。PHS を用い、PIAFS(PHS Internet Access Forum Standard) という 32Kbps または 64Kbps の速度でデータ通信を行う場合の標準規格によって、モバイル・コンピューティング環境における PHS の役割は増大しており、また、PHS の電波の適応範囲である半径 100m〜500m 単位に PHS 基地局を設置することで、位置情報機能のついた PHS 端末の現在位置を検出することができる。この位置情報機能付き PHS 端末を用いて、NTT Docomo などが独自の電話網を用いた位置情報サービスを行っている。

2.1.3. Active Badge

Active Badge は、現在の AT&T Laboratories Cambridge (旧 ORL:the Olivetti Research Laboratory) で開発された位置情報検出装置である。これは、Active Badge を身に付けた人の位置を、建物内の部屋および廊下などの天井に設置したセンサを用いて検出するもので、具体的には Active Badge からは 10 秒おきに、センサに向けて赤外線を用いて自己 ID を送信する。この装置を用いた人の位置情報サービスを同研究所で行っている。

2.1.4. Cricket

無線は屋内だと論理値とかなり違う挙動を示すため、無線だけを使って正確な位置を得るのは難しい。そのため、超音波と無線を用い、音速と光速の違いを利用して位置情報を得ている [8]。

Cricket compass という機械をモバイルデバイスに付与し、デバイスの位置および指向性の特定を行うことで様々な文脈・位置依存アプリケーションを支援する。 [9] では、屋内で正確な位置情報をどうやって取得し、Cricket compass の「ソフトウェアコンパス」の機能をどのように実現しているかについて、論述している。

各デバイスの位置情報を取得するために、建物内のあちこちに Cricket beacon と呼ばれる機器を設置する。この機器はアクティブビーコンとして、無線 (RF) と超音波 (ultrasonic) を定期的にブロードキャストしている。これをデバイス側の Cricket compass に付けられたパッシブセンサが受けとって処理し、compass から各ビーコンまでの距離と角度を求める。さらにその情報と各ビーコンの位置情報とを使って、ソフトウェア的にデバイス (compass) の位置と方向を計算する。結果的に 30 度に対して 3 度くらいの誤差、40 度に対して 5 度くらいの誤差で位置測量が可能である。超音波シグナルの速度は気候条件によって大きく変わるが、4 つのビーコンからの情報 (超音波と RF の到着時間の差) を使うことで、音速がわからなくても位置情報が求まる。位置情報の導出は、基本的には GPS で使っているのと同じ方法と言える。

2.1.5. RFID

RFID(Radio Frequency ID entification) は、非接触型 IC チップ (LSD) によりエンティティ (個人、商品、など) を識別する技術である。電磁波を利用するので電池を用いなくとも情報の伝達が長期間にわたって可能である。流通分野では、従来バーコードを利用した識別が広く普及しているが、バーコードにと比較して記憶容量が多く、情報の読み込みだけでなく書き込みが可能、耐性に優れる、非接触で情報の伝達が行われる、などの利点から、それに取って代わる可能性を持っている。

IC チップには、それぞれバーコードに割り振られた識別番号のように、96 ビットで構成された

表 2.1: 位置情報検出装置精度と規模性

	精度	通信方法	位置情報の性質
GPS	1〜5m	active	絶対位置 (緯度/経度/高度)
PHS	100m〜500m	active	絶対位置 (PHS 基地局の位置と電界強度により計算)
Active Badges	高精度 (赤外線)	active	相対位置 (部屋単位)
Active Bats	9m(超音波)	active	相対位置 ($10m^2$ 毎の基地局単位)
Cricket	4x4 ft.	passive	相対位置 (16 sq. ft 毎に 1 ビーコン)
RFID		passive	相対位置

EPC(Electronic Product Code：電子製品コード) が割り振られている。96 ビットのうち、最初の 8 ビットがヘッダー部、次の 28 ビットが企業識別番号、その次の 24 ビットが商品クラス識別番号、最後の 36 ビットが商品識別番号を表している。

2.2. 位置情報システム

位置情報システムとは、現実世界の物理的な位置情報を、電子空間、またはインターネット上で扱うための仕組みを提供している。

2.2.1. GPS 携帯電話および PHS を用いた位置情報システム

GPS 受信機内蔵の携帯電話や、基地局と電波強度を用いた PHS による位置情報検索システムが存在する。位置情報の検出後は、パケット通信網を用いてそのデータをインターネット上のセンターに集積・管理する。

たとえば、GPS 携帯電話または feel H” を使用し、簡単なボタン操作で位置情報付きの業務連絡が行なえる自己申告型の外勤者管理システムなどに活用できる。

2.2.2. Geographical Location Information System(GLI system)

インターネットという仮想的な空間と現実の空間を結び付けるには、インターネット上のオブジェクトと現実世界のエンティティ(車、人、計算機、プロセス等) とを対応づけることが必要となる。GLI システムでは、現実世界のエンティティとその地理的な位置との関係を定義し、インターネット上の識別子と現実世界のエンティティの地理的位置情報との対応づけを行っている。

表 2.2: 位置情報検出装置導入コスト

	コスト	備考
GPS	基盤構築は非常に高価。受信機は一般的に入手可能	屋外でのみ有効
PHS	受信機は PHS 端末	キャリア依存
Active Badges	基地局とバッヂは安価だが、運用コストが高い	屋内の利用
Active Bats	基地局とバッヂは安価だが、運用コストが高い	ceiling sensor grid が必要
Cricket	ビーコンと受信機は安価	Oxygen プロジェクト [10] で利用
RFID		

GLI システムは、基本的には、Home Server、Area Server、Agent、Client の 4 つの要素によって構成されている。

Home Server(HS):

各エンティティの最新の位置情報 (GLI) を管理する。

Area Server(AS):

担当する地域に存在するエンティティから位置情報を取得し、管理する。

Agent:

移動するエンティティ上で動作。GPS 等から実際に地理的位置情報を取得し、各サーバに登録する。固定エンティティについては、代理登録が可能であるため、Agent は無数にある必要はない。

Client:

利用者と GLI システムとのインターフェイス。移動計算機に限定されず、固定計算機の場合もある。

これにより、利用者はインターネット上の情報を用いて現実世界の様々なエンティティを検索したり、特定のエンティティの現在位置をリアルタイムに取得できるようになった。

2.2.3. LOCATIONWARE

LOCATIONWARE は、NEC ネットワークスにより開発されている位置情報サービスシステムを構築するためのプラットフォームである[1]。LOCATIONWARE は、以下の二つのコンポーネントにより位置情報サービスシステムの構築をめざしている。

- LOCATIONWARE Gateway
  無線通信キャリアなど、位置情報基盤を持つシステムに対して提供する。この Gateway は、位置情報基盤のシステムを外部の位置情報サービス事業者のシステムと接続するためのインタフェースを提供するとともに、基盤システム内部に保持する位置情報が許可なく外部に漏れることを防止するための機能を持つ。

- LOCATIONWARE Service Development Kit
  位置情報基盤から取得した位置情報をもとに、利用者の位置に応じたサービスを提供する位置情報サービス事業者に対して提供されるミドルウェアである。上記 LOCATIONWARE Gateway との通信機能を持っており、位置情報基盤を利用したシステムの構築を容易にする。

LOCATIONWARE は、技術的な仕様については公開されていないが、位置情報サービスの基盤となる機能を共通の API(Application Program Interface) により提供している。これによりアプリケーション・サービス・プロバイダ (ASP) やユーザが、サービスを容易に提供・利用可能となる。また、ユーザの位置に応じて情報を配信する通知型サービスにおいて、携帯端末自身が将来必要と予想される情報を予めキャッシュする機能を提供することで、サービスの通信コストの低減と、不安定な無線通信環境におけるサービス提供を図る。

携帯端末の移動履歴から、移動速度・移動方向・移動パターンを抽出し、これらも位置情報としてサービス提供アプリケーションに通知する機構を提供することで、例えば高速移動中か歩行中かなど、携帯端末ユーザの行動に即したきめ細かな情報提供を行うことが可能となった。

さらに、測位方式の違いに無依存な形で携帯端末の位置を取得、管理する機構を提供ことで、サービス提供側では測位方式を意識することなく、汎用的な位置情報サービス・アプリケーションを構築することが可能となる。

2.3. 位置情報に基づくサービス

ここでは、位置検出装置を用い、位置情報システム上で提供される位置情報サービスについてまとめる。

[1] http://www1n.mesh.ne.jp/CNPWORLD/solution/service/ichijoho/

2.3.1. PHS 位置情報サービス

通話やデータ通信用に利用されていた PHS の物理的な位置を自動的に探し出し、地図上でその位置をリアルタイムに知らせるサービスとして、「いまどこサービス」 [11] が、NTT Docomo で開発されている。これは、適応範囲半径 100 m〜500 m単位の PHS 基地局を用いて、位置情報発信機能のついた PHS 端末の現在位置を FAX またはパソコンで通知するものである。また、このいまどこサービスの専用端末として、通話機能を持たない P-doco なども販売されており、子供の行き先や社員の現在位置を検索するシステムとして、現在広く認知されつつあるサービスと言える。

同様に、GPS 携帯電話、または feel H" を使用し、簡単なボタン操作で位置情報付きの業務連絡が行なえる自己申告型の外勤者管理システムが東芝ロケーションインフォ株式会社[2] から提供されている。これは、通信インフラとして、DDI ポケット網を利用している。

また、株式会社テレコムでは、ドコモパケット通信サービス (DoPa) を用いて車載機から位置情報を取得し、本部端末の地図上にその車両の現在位置を表示するシステムが提供されている。バスの場所が携帯でわかるサービスや、車両管理に関するサービスが提供されている。

このような PHS 位置情報システムは、通信キャリア各社がそれぞれ独自のサービスを展開しており、各社ごとに閉ざされたサービスである。また、PHS のアンテナ出力や設置状況によって位置情報の精度は異ることが知られている。さらに、その位置情報検索に必要なものは PHS の電話番号であるため、PHS の電話番号さえ分かっていれば誰にでもその PHS 所有者の現在位置が分かってしまう。位置情報のデータ管理も暗号化やアクセス制御機能が付加されていないため、NTT Docomo 社員の良識による情報流通と管理が必要となるが、近年、企業による顧客情報流出や、各種組織による機密情報の流出などの事件も頻発しており、インターネット上で扱う情報の蓄積方法および流通管理を慎重に行う必要があるといえる。

2.3.2. TPOCAST

LOCATIONWARE を利用し、携帯端末を対象に、そのとき・その場で・その人に最もあった WWW ページを配信するソフトウェアである。位置情報に基づく携帯端末むけ Web 情報サービスが実用化されているが、本ソフトウェアを用いることで、位置だけでなく、個々のユーザの興味にあわせた WWW ページの絞りこみ (パーソナライズ) が可能になる。旅行先でのピンポイント観光ガイド、ショッピング中の個人むけ情報・広告配信、ドライバー・歩行者むけの ITS 情報サービスなど、様々に応用可能である。

サービスの展開例としては、

[2] http://es.toshiba.co.jp/lcs/

- 観光情報配信サービス
  「観光情報 ASP サービス」により既に実現

- 車両向け情報配信サービス
  カーナビなど車載端末への情報配信サービス

- 歩行者 ITS 情報配信サービス
  健常者及び障害者を対象とした携帯端末への情報配信サービス

- 放送型情報配信サービス
  デジタル衛星放送などによる情報配信サービス

等が挙げられる。

TPOCAST では、ユーザの TPO 属性と、WWW ページの TPO 属性とを比較するための TPO 属性記述言語「TPOML」を開発し、個人の TPO 属性にあわせた WWW ページの絞りこみを実現している。また、ユーザと WWW ページの TPO 属性を比較し、適合する度合いの高いページを選ぶ選択エンジン、および、ユーザの行動履歴 (T,P) と、WWW 検索などの端末操作履歴とを用いて、ユーザ TPO 属性の重みづけを更新する嗜好学習エンジンの開発している。これにより、位置や時間とともに変わるユーザの興味を常に反映した WWW ページの選択が可能となっている。

2.3.3. Active Badge Location System

AT&T Laboratories Cambridge[3] で開発された Active Badge Location System [12] は、オフィスで Active Badge を身に付けた人の位置管理を行うための環境を提供している。Active Badge からは、10 秒おきに部屋の天井などに設置したセンサに向けて、赤外線を用いて自己の ID を送信し、ネットワークに接続されたセンサは、Active Badge から得られた情報をサーバに登録する。文献 [13] では、Active Badge を利用した位置管理システムの構造や、オフィス環境での人のいる位置を取得する場合のアプリケーション例をとりあげ、同研究所で開発している VNC(Virtual Network Computing)[4]と合わせることで、自分の計算機のウィンドウ (ホーム環境) を、一番近くにある計算機の画面に転送するアプリケーションなどの Active Office 構想を提案している。

しかし、Active Badge は、利用範囲が建物内部に限定されている。また、開発時にはこのような位置情報システムは、本質的に相互利用されるものであると考えられていたため、Active Badge を用いた人の位置検索システムが WWW 上で公開されている (WWW Active Badge Service [14])。

[3] http://www.uk.research.att.com/
[4] http://www.uk.research.att.com/vnc/

しかし、これは言い替えると、社外の者でも簡単に社内の人の位置を知ることができるため、個人のプライバシの侵害、または、このシステムを用いている組織の不利益につながるおそれがある。

2.3.4. Enhanced 911 (E911)

現在米国では E911 構想が連邦通信委員会 (FCC) を中心に進められている[5]。従来の固定電話による 911 番 (日本の 110 番や 119 番にあたる緊急番号) への通報は自動的に通報者を探知できる仕組みになっているが、「E911」はこれを携帯電話利用者にも拡張し、緊急番号に通報した携帯電話利用者の番号と場所を 50〜100m 以内の精度で特定することを目的とした技術である。

1996 年から始まった E911 構想は、2001 年時点では第一段階の「電話番号と通報場所に最も近い基地局の特定」にとどまっており、通話者が詳細な場所を通告する必要があった。最終的には、精度を 50〜100m 以内に上げる予定であるが、この計画は遅れ気味である。

FCC では 2001 年 10 月から「E911」の第二段階のサービスを各無線通信事業者が開始するように求めていたが、携帯電話機メーカーの準備不足を理由に開始延期の要請があり、10 月初め FCC もこの申請を承認した。しかし、2001 年 9 月に起きた米国同時多発テロにおいて、多くの人が携帯電話を使って助けを求めたことから、「E911」の必要性が改めて認識され、米議会では一刻も早い実施を求める気運が高まっている。

これを受け FCC では、ガイドラインの他に、大手の無線通信事業者に対して個々の達成目標を指示している。最長 2004 年 12 月 1 日までには全販売携帯電話を「E911」対応とするなど販売目標の進捗は先延ばししたものの、2005 年 12 月末には加入者の 95 %が「E911」の利用を可能とする点は変更していない。また、2001 年 9 月時点では、第一段階の E911 サービスを導入している警察署の数は全体の半分以下で、第二段階のシステムを導入しているところは一つもないと報告されているが、今後は行政側の整備も急速に進むことが予想される。

同時多発テロを契機に E911 の関心度合いは高まっており、第二段階のサービス導入は今度こそ実現に向け動き出そうとしている。

2.3.5. Cricket

位置情報の追跡は、プライバシの問題から望ましくないため、Cricket では、ユーザの位置情報を明示的に”追跡”せずに位置サービスを構築している。各ビーコンの位置情報は集中管理をせず, また、ユーザの位置情報をアクティブに発信させない。位置検出はビーコンを発信する廉価で小さな機械を屋内に撒き、その機械からの情報を得て位置データを割り出す手法である。位置情報

[5] http://www.fcc.gov/911/enhanced/

を集中的に管理していない状態で部屋の境界などを正しく認識させるために、ビーコンの置き方を工夫する必要がある。屋内での正確な位置測定は難しいが、測量値の曖昧さを複数の測量値の組合せを使うことで自己補正している。

Cricket は MIT AI ラボの Oxygen プロジェクトで実際に使われている[6]。

2.3.6. RFID を用いた位置検出システム

RFID を利用したユーザ位置検出システムは、RFID タグを貼り付けたカーペットを床に敷き詰めておき、RFID リーダを取り付けたウェアラブルな機器や人が携帯・操作する機器を検出するものである。文献 [15] では、RFID リーダを下駄 (NaviGeta) と、ユーザが操作するカートに取りつけたシステムを試作し、性能評価を行っている。これは、相対位置検出の一種であり、絶対的な位置情報を検出するものではない。

2.4. ま と め

以上のように、室内または屋外で利用可能な、様々な位置情報検出装置が開発されている。位置情報の表現方法は、絶対位置情報と相対位置情報の二つに大別される。しかし、どちらの表現も実空間の情報であって、インターネット上で扱うためには現実世界のエンティティとその地理的な位置との関係を定義し、現実世界のエンティティ(車、人、計算機、プロセス等) とインターネット上のオブジェクトとを対応づけることが必要となる。この対応のための位置情報システムをインターネット上に構築し、その上で位置情報を用いた多様なサービスが展開されている。

位置情報指向のサービスは、屋外では、主に緊急通報時の位置特定および移動する利用者の動的に変化する状況 (位置や時刻) に合わせてカスタマイズしたサービス提供が目的と言える。また、屋内では、位置情報の通信方法は、active(通知型) および passive(探索型) の二つに大別される。物品の位置把握や、室内での人の動きの追跡によるサービス案内など、物流制御および移動する利用者の動的に変化する状態に合わせたものが主流である。

いずれの場合も、移動体 (利用者) の位置特定に関するサービスが注目されているが、インターネット上に発信する情報が位置情報だけでなくその電話番号や個人を特定する識別子、場合によっては個人の行動履歴なども含まれるため、プライバシ保護への対策が重要な課題として残されている。

[6] http://oxygen.lcs.mit.edu/

Chapter 3

個人情報とプライバシ

前章で、移動体 (利用者) の位置特定に関するサービスの重要な課題として、プライバシ保護への対策を挙げた。ここでは、情報化社会の変遷にともなうプライバシの変容について述べ、実空間および電子空間、インターネット上において保護すべき個人情報の定義を確認する。また、従来のプライバシ侵害とインターネット上でのプライバシ侵害との相違を明らかにした上で、インターネット上のプライバシ侵害の特徴は、情報コントロールの困難さに起因するものであり、少なくとも従来のような規制強化だけでは不十分であることを述べる。

3.1. 個人情報とプライバシ

個人情報の広義は「個人を特定するに足る情報」ということであり、もともと、本人の身元確認などに用いられる情報である。その情報を利用する状況によって個人を特定する情報は変化するため、明確な定義があるわけではない。実空間および電子空間、インターネット上において保護すべき個人情報の定義については、各節を設け、後述する。

個人情報とプライバシという言葉は混同して用いられている場合も少なくない。これらの定義は、情報科学だけでなく、社会学や哲学など、様々な学問分野で行われており、たとえば、[16] では、プライバシ保護が「個別的」な個人のプライバシ保護の問題であるのに対して、個人情報保護とは、多数の人間に共通して生じる「集合的」なプライバシ権保護の問題であるととらえている。

本研究において、個人情報とプライバシの関係は、以下のように定義をし、明確化する。

個人データ ＜ 個人情報 ＜ プライバシ

個々のなデータが集まって体系化されることで個人情報となり、その個人情報によって何らかの行動がなされる場合にプライバシが形成されるとする。

性別、年齢、誕生日、住所、購買履歴などの個々のデータは、それ一つだけでは、個人を特定するに至らない。しかし、それらのデータを集積して体系化することで、これらのデータは個人を特定する個人情報となる。この個人情報は、その個人が秘密に保持している場合はプライバシの

侵害は発生しない。個人的な活動と共に公開・流通する場合に用いられる個人情報の集合を、プライバシとする。

したがって、本研究では、システムを構築する際には、体系化された個人データの取り扱いとして「個人情報の保護」を、また、システムによってサービスを提供・利用する際に個人情報が公開・流通する場合は、「個人のプライバシ保護」を検討する。

3.1.1. 実空間における個人情報とプライバシ

実空間における個人情報の定義は、行政が発布する条例に「何をもって個人情報と定義しているか」を理解するための手がかりがある。たとえば、2000 年 7 月に施行された「横浜市個人情報の保護に関する条例」では、次のように説明されている。

> 『この条例において「個人情報」とは、個人に関する情報であって、特定の個人が識別され、又は識別され得るものをいう。ただし、法人その他の団体に関して記録された情報に含まれる当該法人その他の団体の役員に関する情報及び事業を営む個人の当該事業に関する情報を除く。(横浜市個人情報の保護に関する条例　第 1 章　総則 (定義 2) より抜粋))』

横浜市個人情報保護制度のホームページ[1] ではこれを『氏名、住所、学歴、職歴、病歴、税金や年金の額、試験成績など、特定の個人に関する一切の情報を保護の対象とします。また、氏名などが記載されていなくても、他の情報と組み合わせることによって個人が特定される情報も含みます。』と解説している。つまり、住民票や戸籍だけではなく、学歴、職歴、病歴などの個人の活動履歴や、納税や年収などの経済活動情報、家族構成など、横浜市の機関が保有するあらゆる情報が保護の対象となる。

個人情報は、このような市町村などの行政が預かっているものだけではない。預金残高、毎月の出費などの銀行口座情報、クレジットカードで購入した商品、信用調査状況、信仰している宗教や思想、会社の勤務評価資料、趣味趣向など、さまざまな情報が銀行、クレジットカード会社、信用調査機関、所属する会社によって文書化され管理されている。

3.1.2. 電子空間における個人情報

1960 年代以降の情報技術の発達と業務の効率化を目指す時世に伴い、行政、医療、通信、教育などの様々な分野で計算機が導入され、情報の電子化が進んでいる。これにより、個人信用報告や前科前歴記録、診療記録、納税記録などさまざまな個人情報が電子化され、データベース化されるようになった。

[1] http://www.city.yokohama.jp/me/shimin/joho/index.html

個人情報は、他の情報と組み合わせ分析することにより個人的嗜好や性格、消費行動まで把握することができる。商業活動分野では消費者ニーズの確認と合理的な経営を目的としたマーケティングリサーチのため、金融分野では安全な商取引のため、個人信用情報が収集/蓄積/活用されるようになった。当事者が予想もしない形で情報が利用されたり、誤って入力された個人情報が利用されることは個人の利益や権利を侵害しかねない。そこで、自分の記録を閲覧、さらには訂正できる自己情報コントロール権を法的権利として認めることの必要性が説かれ、法制化が進んでいる。

一方、個々のデータそのものが「個人を特定するに足る」情報量を得ている場合がある。

たとえば行政分野では、日本の戸籍にあたる制度がないアメリカ合衆国では、ソーシャル・セキュリティー・ナンバー (Social Security Number) として個人情報が電子化され、情報管理されている。これは、もともとは納税者番号、つまり社会保障のための番号であり、過去のローンなど、個人的な経済状況が記録されている。アメリカ合衆国では個人の ID 番号として見なされており、たとえば、銀行口座の開設や保険会社との契約の他、政府機関への報告などに必要となる。また、場合によっては運転免許証の申請、病院の初診、電話やガスなどの公共設備を利用する際の個人の信用照会に用いられるなど、身分証明として重要な役割を担っている。

日本の行政分野においては、2002 年 8 月から住民一人一人に 11 桁の住民票コードが割り振られ、行政機関等への本人確認情報として用いられたり、市役所業務の手続きの簡略化などが図られている。また、商取引などの分野での口座番号やクレジットカード番号もこれにあたる。

このように、実空間の情報の集合体としての個人情報が電子化され、個人情報の集合体として電子空間で管理されている一方で、電子空間では、個々のデータだけで「個人を特定し得る」場合が存在する。つまり、電子空間では、実空間での振る舞い以上に、不特定多数に対する個人情報の流出などの「個人情報保護」について検討する必要がある。

3.1.3. ネットワーク空間における個人情報

ネットワーク空間における個人情報は、前節の電子空間における個人情報と同義である。しかし、ネットワークを介して、電子的な個人情報が流通する場合、個人情報そのものの他に、保護すべきプライバシが発生する。

電子化された情報は、ネットワークを介して流通し、利活用されている。オンラインショッピングや、オンラインバンキングなど、ネットワーク上での商取引の場でも、口座番号やクレジットカード番号、購買履歴や取引内容などがユーザプロファイルなどの個人情報としてシステム側に保存され、サービス向上や業務の効率化のために管理されている。

3.2. 情報化社会の変遷にともなうプライバシの変容

マスメディアの発達によって情報量が飛躍的に増大した社会 (マスメディア情報化社会) との関わりにおけるプライバシの問題は、日本では 1960 年代に入ってから本格的に論じられるようになった。従来、実空間の情報を発信する主体の多くは、新聞やテレビやラジオといった放送機構などに代表されるマスメディアであり、誤った情報の発信や、私的な情報の暴露など、プライバシ侵害に関する問題は、法の整備などの規制強化を行うことである程度の秩序が保たれていた。

しかし、1960 年代以降においては、計算機が情報を大量に処理することができるようになった社会 (コンピュータ情報化社会) との関わりにおけるプライバシの問題が注目され、さらには、1980 年代以降、計算機技術と通信技術の飛躍的発展とその結合によってネットワーク化が進展し、情報量が増大するとともにその流通が国際的にも盛んになってきた社会 (ネットワーク情報化社会) と関わるプライバシの問題も議論されるようになってきた。つまり、新聞や放送、大衆動員やビラ配布などが情報伝達、公開、発信の媒体であると同時に、今日では、インターネットが電子化された情報の発信に関する重要媒体に成長している。インターネット上に発信される情報は、情報発信の主体の多くが一般の人々、つまり実空間上での一個人であり、インターネットの持つ匿名性や空間制約の撤廃などから単一国家の法規制やその他情報規制だけでは、個人のプライバシ侵害に関する対応は十分に行えない。つまり、インターネット上で提供されるサービスにおけるプライバシ侵害の特徴は、情報制御の困難さに起因するものであり、個人レベルの情報発信活動に関しては未だに流通制御ができていない。プライバシの侵害を防ぐためにも実世界のエンティティに帰属する情報の流通制御および管理が必要であると考える。

3.3. ネットワーク上の自己情報制御の困難さ

ここでは、個人情報を流通させる上で発生するプライバシについて、ネットワーク情報社会では個人情報が自分の情報制御権から離れてしまうという観点から、例を挙げて説明する。

たとえば、行政書士が持っている行政書士電子証明書 (認証書) には、その行政書士の名前と生年月日という個人情報が含まれている。これは、公的な認証システムの常として、認証書の内容 (公開鍵を含む) が WWW 上に公開されている。一方、実世界でも、行政書士登録証 (事務所に掲示義務) に名前や生年月日という個人情報が記載されている。

記載されている情報は同じだが、自己の情報制御権という観点からは、両者の性質は大きく異なる。事務所に掲示されている行政書士登録証の生年月日情報を見るためには、事務所に訪問しなければならない。これにより、自己の個人情報を、「誰」が「いつ」見ることになるのか把握でき、また、その利用目的も多くは行政書士という資格登録者の身分を確認するために行われると

予測することができる。

ところが、WWW 上に公開されている電子的な証明書は、「誰」が「いつ」「何のために」閲覧・利用するのか予測不可能である。これは、もはや自己の情報制御から離脱している言える。このように WWW のような情報流通サービスでは、個人情報の取扱に関して、個人 (情報提供者) の意思に基づく流通制御を行う必要がある。

3.4. ま と め

ここでは、本研究での取り扱う個人情報とプライバシに関する定義を行った。また、実空間および電子空間、インターネット上において保護すべき個人情報の定義を確認し、情報化社会の変遷にともなうプライバシの変容について述べた。従来のプライバシ侵害とインターネット上でのプライバシ侵害との相違を明らかにした上で、インターネット上のプライバシ侵害の特徴は、情報コントロールの困難さに起因するものであり、少なくとも従来のような規制強化だけでは不十分であることを述べた。さらに、ネットワーク上での自己情報制御の困難さについて具体的な例を挙げて説明し、インターネット上での情報流通サービスには、個人情報の取り扱いに関して個人 (情報提供者) の意思に基づく流通制御が必要であることを述べた。

個人情報や情報公開などの情報制御は、信頼の問題と密接に関係している。これは、 8 に後述する。

Chapter 4

地理的位置情報システムとプライバシ保護

インターネット技術の急速な普及とともに、小型化・軽量化の進んだ携帯端末が市場に出回るようになった。このため、無線通信やナビゲーションシステム等を含むモバイル・コンピューティングという新しい計算機の利用方法が広まりつつある。インターネット上に固定または移動計算機が遍在している環境においては、現実空間の位置情報をネットワーク空間で検索できることが望まれる。つまり、現実空間での地理的な位置情報をネットワーク上で扱うシステムの需要が高まっている。

しかし、インターネット上の仮想空間とは異なり、現実空間での物理的な位置は個人のプライバシに関わる情報を含む場合がある。ここでは、位置情報サービスに関する研究や関連技術と、それに必要と考えられる情報セキュリティ分野での研究を報告する。

4.1. はじめに

元来、インターネットには、ネットワーク上にある資源をその現実空間の位置を意識することなく利用することができる、という特徴がある。このため、インターネットにおける情報アーキテクチャの構造上、計算機の物理的な位置と、ネットワーク空間での位置とは関連づけられていない。

しかし、インターネット技術の急速な普及と、無線技術の発達により、小型化・軽量化、または低価格化の進んだ携帯端末が市場に出回るようになった。これにより、携帯電話によるインターネット上のサービス利用や車のナビゲーションシステム等を含む、モバイル・コンピューティングという新しい計算機の利用方法が広く一般に普及し、ネットワーク・トポロジが常に変化し続けている。これにともない、プローブ情報システム [17] やココセコムサービス [18] のように、移動体から発信される位置情報を用いて、新たなサービスの発現および展開が行われるようになった。モバイルコンピューティングの普及により、移動体の位置情報は、その価値が再認識されつつあ

ると言える。

このように、インターネット上に固定または移動計算機が共生・遍在している環境においては、実空間の位置情報をネットワーク空間でも流通させ、利用可能であることが望まれる。つまり、実空間での地理的な位置情報を、ネットワーク上で扱うシステムの需要が高まっている。

しかし、これまでのインターネットでは、ネットワーク空間での位置と現実空間の位置との関連づけを行うシステムが存在しなかった。そこで、現実空間とネットワーク空間の位置の対応づけを行う GLI システム [19] が開発された。

GLI システムでは、現実世界での人や車などのエンティティと、その地理的な位置との関係を定義している。GLI システムを用いることで、現実世界の位置情報を用いてネットワーク上に存在する計算機へのアクセスが可能となった。しかし、現在の GLI システムにはセキュリティ機能が付加されていない。

インターネット上の仮想空間とは異なり、現実空間での位置は個人のプライバシに関わる情報を含んでいる。位置情報に伴う個人情報の改竄や漏洩を防ぐ必要があるため、GLI システムにおけるプライバシ保護機能は必要不可欠なものである。そこで、本稿ではプライバシを考慮した GLI システムを構築する際に必要な条件を抽出し、具体的なシステム・アーキテクチャ・モデルを提案する。

4.2. Geographical Location Information System

4.2.1. GLI システムの概要

インターネットという仮想的な空間と現実の空間を結び付けるには、インターネット上のオブジェクトと現実世界のエンティティ(車、人、計算機、プロセス等) とを対応づけることが必要となる。GLI システムでは、現実世界のエンティティとその地理的な位置との関係を定義し、インターネット上の識別子と現実世界のエンティティの地理的位置情報との対応づけを行っている。

しかし、最初のプロトタイプではサーバが複数存在する時の挙動に関しては触れていないため、拡張性に乏しかった。そこで、このシステムのスケーラビリティを考慮した結果、サーバを Area Server および Home Server に分割した図 4.1 の様なプロトタイプが実装された [20]。

現在の GLI システムは、Home Server、Area Server、Agent、Client の四つの要素によって構成されている。ここで、各要素の振る舞いについて述べる。

Home Server(HS):

各エンティティの最新の位置情報（GLI）を管理する。

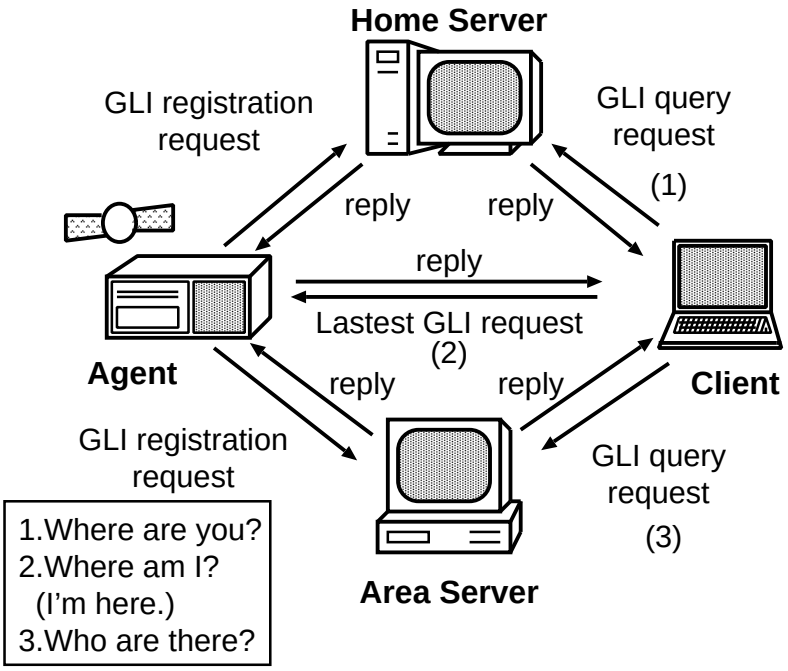

図 4.1: GLI system prototype

Area Server(AS):

担当する地域に存在するエンティティから位置情報を取得し、管理する。

Agent:

移動するエンティティ上で動作。GPS 等から実際に地理的位置情報を取得し、各サーバに登録する。固定エンティティについては、代理登録が可能であるため、Agent は無数にある必要はない。

Client:

利用者と GLI システムとのインターフェイス。移動計算機に限定されず、固定計算機の場合もある。

これにより、利用者はインターネット上の情報を用いて現実世界の様々なエンティティを検索したり、特定のエンティティの現在位置をリアルタイムに取得できるようになった。

4.2.2. 問　題　点

GLI システムから得られる地理的位置情報は、交通渋滞情報や駐車場情報、天気情報等に加工可能であるため、インターネット上で提供する情報として有益であると言える。しかし、現在の GLI システムではインターネット上の識別子として IP アドレスや FQDN(Fully Qualified Domain

Name) を使用している。このため、GLI システムから位置情報を取得した場合、その位置情報を提供した計算機が特定できる。これにより個人のプライバシを侵害することが予想される。

さらに、システムや登録・問い合わせに用いる通信路でセキュリティ機能が考慮されていない。つまり、第三者に位置情報を改竄される可能性があり、情報の完全性が保証できない。

そこで、本研究では GLI システムの構成を踏襲した上で、セキュリティ機能の備わった地理的位置情報システムの構築を目指す。

4.3. 位置情報サービスにおけるプライバシ管理のための必要条件

位置情報サービスは一般に研究開発されつつある。しかし、どのシステムにも広域分散環境での実用性を考える上では欠点を有している。ここでは、広域分散環境と個人情報（プライバシ）の保護を念頭においた位置情報サービスにおける必要条件を抽出し、それぞれについて考察する。

4.3.1. 位置情報管理に用いる識別子

位置情報を現実空間で取得し、個人情報を保護しながらインターネット上で公開、管理するためには、現実空間でのエンティティの識別子とは別の識別子も必要となる。ここでは、GLI システム上の識別子が持つべき性質について議論する。

他情報による推測の不可能性

システム管理に用いる識別子は、他情報からは生成、推測が不可能である必要がある。

識別子の有効期限の必要性

位置情報の管理に用いる識別子は、有効期限を設定し、一定期間で（または毎回）適切に変更されるべきである。

第三者による識別子生成の不可能性

管理に使用する識別子は、一意に生成されることが必要である。識別子の生成にはその所有者特有の情報（例えば、暗号やハッシュに使用される salt など）を加えることが有効である。

4.3.2. 個人情報の保護

本節では、個人情報の保護に関する手法について議論する。

データの加工方法

地理的位置情報の所有者（提供者）情報やその個人データについては、第三者に盗聴・改竄されないことが必要になる。個人情報の保護のためには、暗号技術を用いて、情報の完全性と機密性を保つ必要がある。

加工のタイミング

暗号技術を用いる場合は、その処理のタイミングによってシステムにかかる負荷やシステムを構成する要素の役割、性質等が変わる。そこで、本システムに対する情報加工のタイミングを、サーバ上のでの加工、通信路上での加工、クライアント上での加工、に分類し、各々について以下のように考察した。

サーバ上での加工

位置情報サービスを提供するサーバ上で暗号化／復号化処理を行うのは、処理の負荷としては最適であると。しかしこの場合は、サーバを信頼するという前提が必要となり、第三者がサーバに侵入した場合、情報の完全性や機密性は保たれない。また、クライアントからサーバに生の情報を渡す場合に盗聴・改竄される可能性がある。

通信路上での加工

ネットワーク上に生の情報を流さない配慮として、組織毎に内外のネットワーク管理をしている Firewall やルータ等の通信路上で暗号化／復号化する方法がある。これは、サーバやクライアントの負荷は最も軽い。しかし、ここでもサーバを信頼するという前提が必要であり、第三者がサーバに侵入したり、正規のクライアントへのなりすましには対応できない。

クライアント上での加工

Thin Client [21] の提案があるように、移動するクライアント上で処理負荷の高い暗号技術を用いるのはモバイルコンピューティング環境では有益ではない。しかし、クライアント上でデータを加工してサーバに送信することで、侵入者は通信路上やサーバを盗聴しても意味のある情報を得ることは出来ない。また、サーバを信頼するという前提は必要なく、クライアントは自分で情報を加工し、その情報取得可能者を自分で指定することも可能となる。

インターネット上に存在するサーバは必ずしも信頼出来る訳ではない、という理由から、クライアント上での加工が本システムには最適であると考える。そこで、クライアント上（本システ

ムにおける Agent、Client）で暗号技術を用い、情報の加工や情報取得可能者の指定を処理することにした。

4.3.3. 本システムの構成要素に必要な性質

識別子とデータとの分割管理

識別子に対応しているデータがそのまま同じ場所に蓄積されている場合、識別子が誰のものか判明すると対応するデータまでが知られてしまう。そのため、システム管理に用いる識別子と、その識別子に対応するデータは、分割して蓄積、管理されるべきである。識別子は検索のキーとして使うだけで、対応するデータは分割して別の場所に格納することが望ましい。

公開情報に対する、クライアントの要求に応じた検索可能性

エンティティの持つ位置情報や、エンティティの移動速度と位置、またはワイパーなどのセンサから得られる交通情報や天気情報など、一般に有益である位置情報とその付随情報に関しては、いつでも誰にでも取得可能な状態になっていることが望まれる。

非公開情報に対する、適切なクライアント以外からの検索不可能性

位置情報の提供者情報は保護され、その情報を正しく取得できるのは、その情報提供者が指定したクライアントのみに限定されるべきである。

ユーザ識別メカニズム

情報の所有者の詳細な位置情報や個人情報を要求したクライアントが、本当に情報取得の権利を持つかどうか識別するメカニズムが必要になる。したがって、アクセス制御表（ACL: Access Control List）や認証機能を用いた識別を付加することが望まれる。

通信切断時における振舞い

移動中の Agent が位置情報を取得して登録のための通信をする場合、一時的に通信媒体が変わったり通信途中で回線が切断したりする可能性がある。モバイル・コンピューティング環境では、このような突然の通信切断もシステムが関知し、適切な処理を行うことが望まれる。

以上の議論より、情報の完全性および機密性を保証するために暗号技術を用い、暗号処理はクライアント上で行う。システム管理に用いる識別子とデータの管理方法については、必要条件を検討した。これらを踏まえた上で、セキュリティに関して理論的に堅牢なシステムと実用に耐え

得る処理速度や負荷を考慮に入れたアーキテクチャモデルを提案し、プロトタイプとして構築することを目指した。

4.4. システムアーキテクチャの提案

本論文では、あらかじめクライアントで暗号化したデータをサーバ内に蓄積、管理するアーキテクチャモデルを提案する。クライアント内でデータを暗号化することで、ネットワーク上に生のデータを送信することを減らす。これにより、情報の機密性の向上が期待できる。本提案では、クライアント上での処理が増加するが、通信路上での盗聴対策に効果があり、また、第三者が GLI システムを無制限に利用することを防ぐことができる。

提案するアーキテクチャモデルの着眼点を以下にあげる。

- 個人情報の暗号化とアクセス制御機能の考察
- 情報管理のための識別子の導入

公開情報は、エンティティの地理的な位置 [緯度、経度、高度]、速度 [方向、速度]、属性 [ライトの点灯、外気温等] とする。この公開情報から、交通情報や駐車場情報、気象情報等が作成可能である。

4.4.1. 個人情報の暗号化

実際の地理的位置情報は公開可能情報とし、その情報の所有者情報には暗号化処理を施す。一つの位置的位置情報毎にアクセス制御情報を付加することで、情報取得権利を持つ利用者のみが、その情報の復号化が可能となる。

本システムに用いる場合の既存の暗号技術に関する考察を行った結果、暗号処理による処理速度の問題から、データの暗号化には共通鍵を用いる手法が適切である。したがって、地理的位置情報の暗号化には共通鍵暗号を利用する。図 4.2 のようなアーキテクチャモデルを提案する。

提案するアーキテクチャモデルを構成する要素は、Home Server、Area Server、Agent、Client の 4 つである。本論文に用いた表記法としては、以下のようなものが挙げられる。

[E{M}]:
メッセージ M を暗号化したもの（暗号文）。

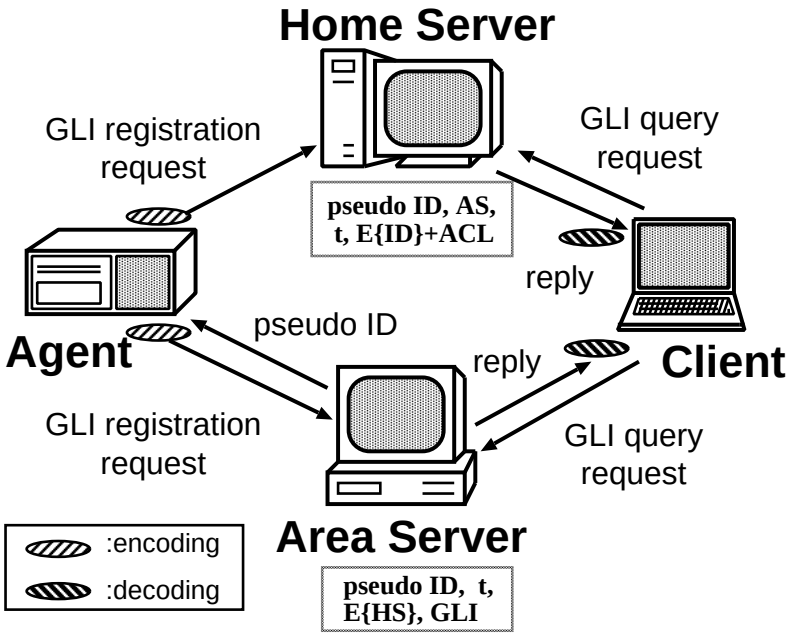

図 4.2: 提案するアーキテクチャモデル

[ACL]:

アクセス制御表（Access Control List）。

[グループ]:

同じ鍵（暗号化に用いる秘密鍵）を共有しているエンティティの一団。

[pseudo ID]:

本プロトタイプシステムで管理上用いる識別子。これだけではエンティティが誰であるか分からない。また、この識別子は AS 内で一意性を保っており、各エンティティの他の情報からは推測不可能。

[real ID]:

エンティティの元々の識別子。インターネット上の IP アドレスや FQDN やユーザ名、現実社会での名前などにあたる。

4.4.2. pseudo ID の導入

前章で述べたとおり、本システムの管理上の識別子に関して、いくつかの必要条件が存在する。これらの必要条件を考慮に入れ、地理的位置情報システムの管理に適切な識別子を導入する必要がある。

我々は、情報管理のための ID と情報自体との直接のつながりをなくし、ID からは情報の所有者を類推できない仮 ID（pseudo ID）を導入した。このような pseudo ID の生成法として、実用

的な暗号学的ハッシュ関数を用いることを検討する。実用的な暗号学的ハッシュ関数とは、(1) 独自にヒューリスティックな設計をしたもの (2) DES などのブロック暗号を連鎖モード的に用いて実現したもの、の二つに大別される [22]。

本研究の pseudo ID の生成には、ヒューリスティックな設計のハッシュ関数を採用した。用いる一方向性ハッシュ関数には、鍵付ハッシュ関数（HMAC: Keyed-Hashing for Message Authentication [23]）や SHA（Secure Hash Algorithm [24] [25]）が適当であると考える[1]。また、各 Area Server 内で一意性を保つことが重要であるため、この pseudo ID の生成には、地理的位置情報を登録する Agent の情報だけでなく、Area Server の情報も加える必要がある。

4.5. 実　　装

本章では、これまでに述べてきた要求項目をふまえたプロトタイプの実装について述べる。

4.5.1. 実 装 環 境

プロトタイプの実装を行った環境を、表 4.1 に示す。ID および HS 情報などのデータの暗号化/復号化に用いた関数は EVP_des_ede3_cbc() という tripleDES CBC mode の関数である。pseudo ID の生成には、SHA() を用いている。

表 4.1: プロトタイプの実装環境

使用した OS	FreeBSD-3.3
暗号化ライブラリ	OpenSSL-0.9.4 [26]
使用した関数	EVP_des_ede3_cbc(): 情報の暗号化 SHA(): pseudo ID 生成

また、本研究での鍵管理などの負担を考慮して、鍵配送と認証のメカニズムに、公開鍵暗号として RSA 暗号を用いること検討した。

共通鍵に関する前提

暗号化／復号化に関わる共通鍵（複数の Agent からなるグループで共有する鍵）は事前に配送されているものとする。

[1] SHA と MD5、 DES hashing との処理速度比較については、
$SHA < DES < MD5$ となっている [25]。

ここで、グループで共有している共通鍵を group key と呼び、そのグループは ID アドレスドメイン等のような階層構造を構成しているとする。Home Server は同じ共通鍵、つまり同じ group key を持つ一つ以上のグループと、それに属する Agent を管理する。

各要素が管理する情報

提案するシステムにおいて、各要素が管理する情報について述べる。

[**Home Server**]

pseudo ID と real ID との関連、つまり地理的位置情報とその情報の所有者との関連を管理する。ここでは ACL を付加した暗号化された ID と、それに対応する pseudo ID、pseudo ID を生成した Area Server 情報と登録した時刻を保持している。暗号化された ID と pseudo ID の両方が検索のキーとなり得る管理を必要とする。

なお、サーバ内では暗号化された情報を管理しており、サーバ自体は暗号・復号機能を持たない。

[**Area Server**]

Area Servre が管理する地域の情報を、携帯電話や無線通信などに見られる基地局のような働きで管理する。Area Server では、地理的位置情報の登録要請毎に pseudo ID を生成し、登録要請した Agent に返す。ここで保持する情報は、pseudo ID、Agent から送信された位置情報、時刻、暗号化された Home Server 情報である。ここでは、Agent により登録された地理的位置情報を用いて、各地の天気や交通情報などの最新の公開地域情報も作成し、管理する。

このサーバも復号化ルーチンを持たない。

[**Agent**]

登録する Home Server や自分の ID を暗号化する機能を持つ。

地理的位置情報を取得する Agent は、Area Server に公開情報と個人情報へのポインタとなる暗号化で保護された情報を登録する。また、Home Server へは暗号化と ACL によるチェックで保護された個人情報と自分の現在位置を保持している Area Server 情報を送信する。

[**Client**]

地理的位置情報を問い合わせる。

“Where are you?”、“Where am I?” などの個人情報は、Home Server に問合せ、“Who are there?” や各地の天気、交通情報などの公開地域情報は Area Server に問合せをする。問い合わせによって得られた個人情報は、group key を用いて暗号化されたものであるため、随時適当な鍵を用いて復号化する。正当な Client のみが復号化可能であり、ユーザに情報を表示できる。

ACL の必要性は、共通鍵更新に伴う鍵配送の速度にある。グループのメンバ（そのグループに

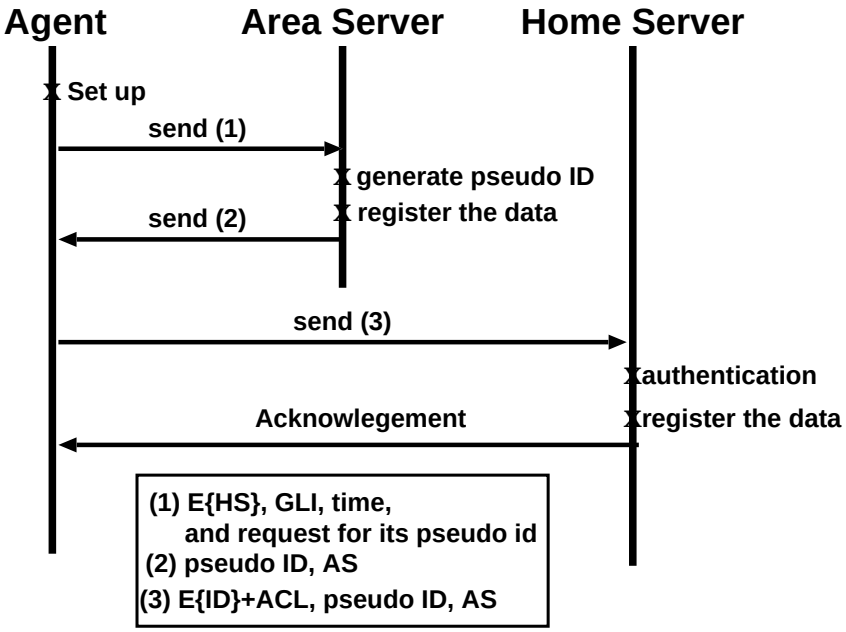

図 4.3: Registration on this prototype

属する Agent）が追加または削除により更新された場合、その group key も更新される。しかし、適切な鍵が配送される前に、更新前のメンバが更新前の鍵を用いて処理を行う場合がある。そこで、情報毎に ACL による細かなアクセス制御を施すことによって、この問題を回避した。

4.5.2. 各要素の通信手順と振舞い

登　　録

Agent は GPS などの装置によって自分の地理的位置情報を取得し、取得した時刻や自分の個人情報などとともに、情報を適切に分割、加工して各々のサーバに登録を行う。Agent が各サーバに各々の情報を登録する手順を図 4.3 に従って詳述する。

準備

1. Agent の属する Home Server 情報と Agent の現実空間での識別子を適切な group key で暗号化し、E{HS}、E{ID} を生成する。
2. GPS などの装置により、地理的位置情報（GLI）とその情報を取得した時間（time）を得る。
3. 自分の情報の検索を許可する Client のリスト（ACL）を作成する。

登録手順

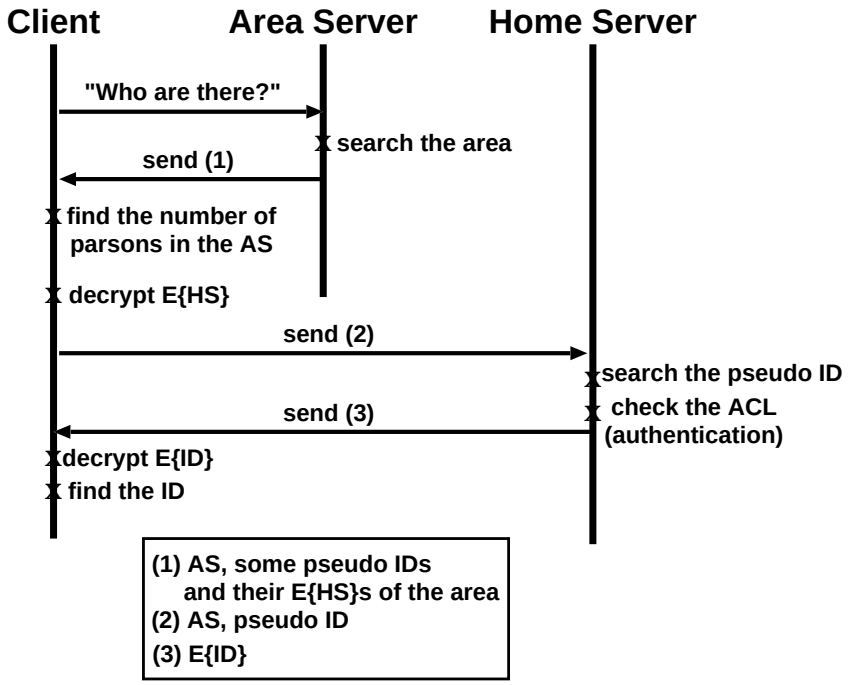

図 4.4: Query “Who are there?”

1. データセット [E{HS}, GLI, time] を自分がいる地域を管理している Area Server に送信する。
2. 送信した Area Server に、その情報に対する pseudo ID と Area Server 情報を要求する。
3. Area Server は受けとったデータセットに対する pseudo ID を生成し、それらをデータベースに蓄積する。
4. 情報蓄積が完了した後、Area Server は自分の情報 AS と、生成・蓄積した pseudo ID を Agent に返信する。
5. AS と pseudo ID を無事受けとった後、Agent は異なるデータセット [E{ID}+ACL, time, pseudo id, AS] を作成し、属する Home Server に送信する。
6. Home Server によって Agent の認証を行った後、Home Server は送信されたデータセットをデータベースに登録し、Agent に Ack を返す。

“Who are there?”

Client が、特定の地域を指定して、そこにいるエンティティの検索に対する問い合わせ（“Who are there?”）を行う手順を以下の図 4.4 に示す。

準備

- ユーザは、特定の地域情報を表示し、”Who are there?” を問い合わせる地域を選択する。

登録手順

1. Client は、ユーザが選択した地域を管理している Area Server へ、Query “Who are there?” と、その指定地域を送信する。

2. Area Server は、データベース中の GLI を用いて指定地域に存在する pseudo ID を検索し、結果を [pseudo ids, their E{HS}, AS] にまとめて Client に返答する。

3. Client はデータセットを受けとる。

4. Client は E{HS} を復号化する。復号化可能であれば、その Client は暗号化／復号化に必要な group key を共有する同じグループのメンバであることが証明される。復号化ができなかったエンティティに関しては、個人情報の保護により、ここより先の処理には進めない。

5. Home Server 情報 HS を得た Client は、データセット [AS, pseudo id] をその HS に送信する。

6. Home Server は pseudo ID を検索し、検索結果に付随するの ACL をチェックして、そのデータセットを送信してきた Client を認証する。

7. データセットを送信してきた Client が、Home Server の ACL チェックをパスすれば、Home Server は対応する情報 E{ID} を Client に返答する。

8. Client は E{ID} を復号化する。復号可能であれば、問い合わせた pseudo ID が本当は誰であったのか、という情報を得ることができる。

“Where are you?”

Client が特定のエンティティを指定して、その現在位置の検索を問い合わせる Query “Where are you?”’ についての手順を以下の図 4.5 に示す。

準備

- 問い合わせたいエンティティの ID を、適切な group key を用いて暗号化し、E{ID} をつくる。Client が問い合わせの対象とするエンティティと同じ group に所属していない場合、これを生成することはできない。

登録手順

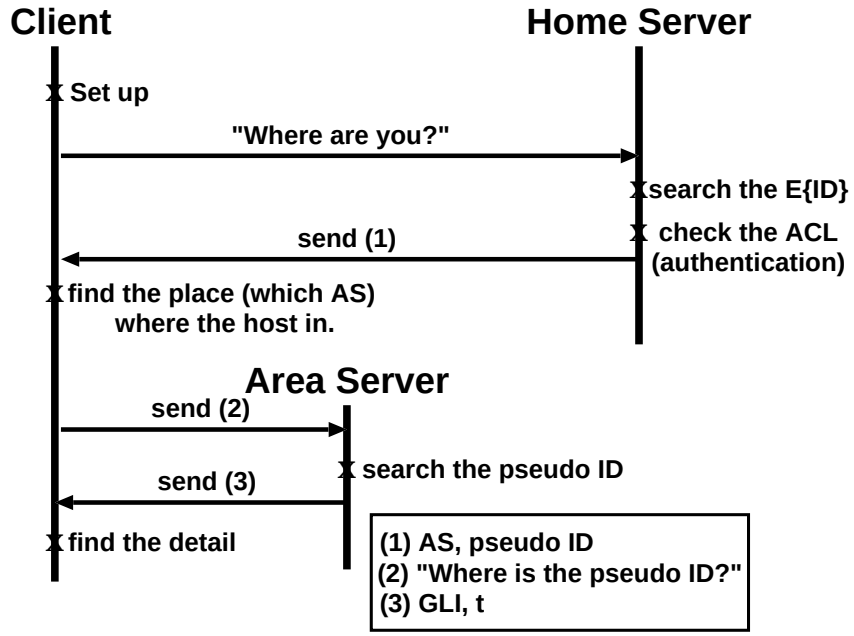

図 4.5: Query “Where are you?”

1. Client は適切な Home Server（問い合わせるエンティティが所属する Home Server）に、E{ID} と共に Query “Where are you?” を送信する。

2. Home Server は、E{ID} についてデータベース内を検索し、該当情報があれば、送信してきた Client をその情報の ACL を用いてチェックする。

3. Client がその ACL による認証をパスした場合、Home Server は問い合わせをしてきた Client にデータセット [AS, pseudo id] を返答する。

4. Client はその Area Server に、Home Server から受けとった pseudo ID を送信する。

5. Area Server はその pseudo ID について、データベース内を検索し、該当する GLI と時刻（time）を Client に返答する。

4.6. 考　　察

4.6.1. プロトタイプの実用性の検証と問題点

今回の地理的位置情報管理システムにおけるプロトタイプシステムでは、実用性を保証するには以下の問題がある。

- 分散環境における振舞い
- pseudo ID の有効期限

Agent がその地理的位置情報を登録する際に、自分の現在地を管理している Area Server を識別する方法や、両サーバの階層構造については本論文では触れていない。これは地理的位置情報システム本体の構造上の問題として、 [19] [20] を参考にしながら対応を検討する必要がある。

pseudo ID の有効期限については、登録する毎に変更する場合と、一定期間 (例えば一日、一週間等) は同じ識別子からの情報には同じものを利用する場合とを比較検討する必要がある。

4.6.2. 今後の課題

前述の問題点を解決し、実用に耐え得るプライバシ保護機能を持った地理位置情報システムとして、 [27] が検討されている。これは、本研究で用いた pseudo ID のアイディアを基に、ハッシュ処理を施した ID(HID: Hashed ID) をデータベース検索の鍵に用いたシステムである。これは、 [20] と同じ手法で分散処理における振る舞いを定義している。また、位置情報検索時の ID を復号処理の必要な暗号ではなく、時刻を鍵とした HMAC によるハッシュにより生成している。これにより、関係者にのみ判別可能な ID を生成しつつ、全体の処理の軽減と鍵配送問題を解決している。

通信の秘匿性などに関しては検討の余地があるものの、このシステムは、セキュリティを考慮した地理的位置情報管理システムとして横浜で行われた 第 58 回 IETF でのデモなどで試験運用され、評価が行われている [28]。

4.7. ま と め

インターネット技術の周知と携帯端末の普及に伴って、モバイル・コンピューティングという計算機の利用方法が広まりつつある中、位置情報はインターネット上の様々なアプリケーションにとって有意性を増している。

現在までに多くの企業や学術研究機関で位置情報サービスについての研究がなされているが、広域分散環境での実用性を備え、個人情報等のプライバシ保護を考慮したものはなかった。そこで、本研究ではセキュリティ（プライバシ保護）を考慮した地理的位置情報管理システムの提案とプロトタイプの設計を行った。

システムアーキテクチャモデルの設計にあたり、情報の完全性および機密性に関しては暗号技術を用い、システム管理上では pseudo ID を導入することによって個人情報の無制限な流出を防ぐことを確認した。

また、今回提案したアーキテクチャモデルは、インターネットにおけるプライバシを考慮した

情報流通を目的とするシステムの一例としても意味を持ち、他のネットワークアプリケーションにも応用可能であると考えられる。

Part II

インターネット自動車

Chapter 5

ITS分野におけるサービスと識別・認証技術

ITS(Intelligent Transport Systems) **とは、最先端の情報通信技術を用いて人と道路と車両とを情報でネットワークすることにより、交通事故、渋滞などといった道路交通問題の解決を目的に構築する新しい交通システムである。ここでは、高度道路交通システム** ITS **に関する事例および利用者サービスについて整理する。**

5.1. インターネット自動車とは

インターネット上のサービスを移動体から利用する場合、その移動エンティティの代表として、自動車が注目されている。これは、

- 利用者の意思に従い、共に広範囲に移動する
- バッテリを搭載している
- 世界中に存在する

などの理由が考えられる。

また、自動車には、数多くのセンサデバイスが搭載されているため、移動体情報通信におけるサービス利用端末としてだけではなく、実世界をプローブする装置としても機能する。つまり、自動車がインターネットを通じて外部社会と常時接続されることで、高度道路交通システム ITS(Intelligent Transport Systems) は、関連サービスの多様性と空間的・時間的広がりを得ることになる。

さらに、独自の通信基盤を想定し、相互運用性が低く、サービスの多様化や広域化、複数のサービスの協調などへの対応が困難な現在の ITS などの関連技術に対して、インターネットを情報通信基盤として用いることで、異なる分野の技術が共通のサービス基盤を得る。

ここでは、インターネットに自動車の構想と、高度道路交通システムとその関連技術について、まとめる。

5.2. インターネット自動車の構想

自動車の情報化は近年の重要な課題の一つである。情報化が進むことにより、自動車を高度道路交通システムに組み込んだり、一般にインターネット上に流通している情報を自動車で利用することが可能となる。

1996 年頃より、WIDE プロジェクトインターネット自動車ワーキンググループにおいて、自動車をインターネットに接続する試みが続いている。

この活動範囲は、車載機の開発から、通信インタフェースの自動切り替え、移動透過性通信プロトコルの実装と評価、高精度測位技術、実空間の地理位置情報のインターネット上での取り扱い、車両データの標準化などまで、横断的である。

たとえば、車両データ、つまり自動車の情報交換形式の定義を行うことで、自動車で取得した固有の情報を一般的な情報に正規化し、流通するための枠組を提供可能となる。これにより、動体管理システムや実空間をプローブする自動車ようなシステムを実現するとが可能となる。これらの情報の流通システムが確立した場合、扱う情報は、自動車やその運転手など、実世界のエンティティに帰属しているため、資源やサービスに対するアクセス制御、つまり情報流通の制御は不可欠なものとなる。

5.3. 高度道路交通システム (ITS)

近年、車両内における道路交通情報の提供や時刻表と連携した公共交通支援、道路管理の高度化などのような、道路交通に関するさまざまな情報サービスが注目されている。これらのサービス提供と諸問題の解決を目的とした新しい交通システムは総称して ITS(Intelligent Transport Systems) と呼ばれ、早急な展開と普及が社会的要請として認識されつつある。この要請は、ITS 関連情報の標準化に関する取り組みや、国内外における ITS 事業の活性化への大きな牽引力となっており、産学官の連携による ITS の構築が各方面で進められている。このような一連の活動の結果、現在までに、ナビゲーションシステムの高度化や自動料金収受システムなど、一部の開発分野では既に実運用に入ったものもあり、その効果が発現しつつある。

しかし、現在の ITS 関連技術は、相互運用性が低く、サービスの多様化や広域化への対応が困難となっている。これはシステム設計の際にそれぞれの開発分野で専用のプロトコルを開発し、独自の通信基盤を想定していることに起因する。このため、システムの新規構築や既存システム拡張、また、既存システム間が協調してより複雑なサービスを提供しようとした場合、システム間でのインタフェースや通信基盤などを新たに設計する必要があり、多大な開発費および開発工程が強いられることになる。このことは、民間事業者が ITS 市場経参入する際の大きな障害となり、

結果として ITS 関連技術の発展を阻害する要因ともなっている。

カーナビゲーションや道路交通情報通信システム (Vehicle Information and Communication System: VICS)、ノンストップ自動料金収受システム (Electronic Toll Collection System: ETC) 等様々なものが ITS の中に位置付けられている。

ITS の分野は、大きく政府主導で進められているものと、民間主導で進められているものに分けることがでる。ETC や走行支援道路システム (Advanced Cruise-Assist Highway System: AHS) 等の大きな設備投資が必要なものに関しては政府主導であり、カーナビゲーションのような設備投資が不要なものは主に民間主導で進められている。

Chapter 6

インターネットITSプロジェクト

e-Japan 重点計画 2002 [1] にもあるように、移動体通信に対する社会的な期待や需要は大きい。

新たな産業分野として期待されている ITS 産業の、効率的かつ多面的な研究開発推進とサービス実現を目的とした産学官共同の研究開発プロジェクトとして、インターネット ITS プロジェクトが 2001 年度より開始された。

本章では、インターネット ITS 基盤を用いたサービスの体系化、本プロジェクトのコンセプト、および策定した基盤仕様について説明する。プロジェクトでの活動を通して、インターネットというオープンな情報通信基盤を用いることで、異分野にある技術研究が協調および共生し、新たなサービスの発現することを議論した。また、実空間の情報をインターネット上で取り扱うサービスの構築にあたり、実空間のエンティティに帰属した情報流通、特に個人のプライバシ保護に関する流通制御の必要性を確認した。

インターネット ITS プロジェクトでは、インターネットがそのオープン性を活かした情報通信基盤となることの意味について検討し、ITS 関連サービスに対する共通インタフェースの提供と、情報通信基盤仕様の策定、実現されるサービスイメージの分類等を行った。

ここでは、本プロジェクトのコンセプトとそれに沿って策定した基盤仕様について概説し、インターネット ITS 基盤を用いたサービスの体系化を行う。また、各種実験の結果から、共通の基盤とインタフェースを提供することによる ITS 市場と新規事業者への貢献、技術開発の方向性を議論し、特に車両や運転者、積み荷などの識別および認証技術における情報流通制御の必要性を確認した。

6.1. インターネット普及とITS

通信をはじめとした情報科学技術では、ITS 関連システムの共通基盤として応用できる技術が飛躍的な発展を見せている。たとえば、ITS 市場で高い需要が見込まれている車両制御や無線通信などは，国際的な技術開発と市場確保の競争が発生するようになった。また、情報通信分野では，新たな社会基盤としてインターネットが普及している。

インターネットはオープンな学術ネットワークとして発展し、国内外の研究者や開発者が共通のインタフェースを利用して互換性のあるシステムを開発してきた。このような特徴は、様々なサービスが商用化された現在でも維持されており、技術開発や標準化に特定の個人や企業が強大な力を持つことがない。互換性のあるシステムを協調して設計するため、結果として柔軟性や機能拡張性を持ったサービスが提供される。

このような特長により、いくつかの既存サービスは、インターネットを共通通信基盤技術として再構築されるようになった。インターネットを利用することには、技術・社会環境・市場などの急激な変化に対して柔軟に対応できると同時に、新規事業参入者が容易に効率的かつ多面的なサービスを展開・拡張できるという利点がある。

6.2. インターネット ITS プロジェクト

6.2.1. インターネット ITS プロジェクトのコンセプト

インターネット ITS プロジェクトは、上記のような現状を受け、各種サービスに対して共通の通信基盤とインタフェースを提供することで ITS 関連システムの再構築を図ることを目的として発足した、産学官共同のプロジェクトである。すなわち、このプロジェクトが概念として掲げるインターネット ITS とは、独立した個々のサービスではなく、さまざまなサービスを実現するためのオープンな基盤技術である。

6.2.2. インターネット ITS プロジェクト参画の目的

基盤技術の確立と共通インタフェースの設定により、技術的・市場的に大きな発展が期待できる。たとえば、車両位置や速度情報等のデータを収集し、統合的に解析することによって、天候や道路交通情報を空間的・時間的により細かな粒度で得ることができる。また、車両の動態管理、車両間での情報交換、電子決済や遠隔メンテナンス等を実現することも可能になる。さらに、共通インタフェースを利用して、配車システムや地図情報発信のようなサービスを自由に構築することができる。一方、このようなサービスの多様性によって、ITS 市場に対するさまざまな業種・事業者の参加が促進されることが期待され、新たな ITS 市場の早期生成も予想される。

このように、インターネット ITS の提供する基盤技術により、自動車がインターネットを通じて外部社会と常時接続されることで、ITS は関連サービスの多様性と空間的・時間的広がりを得ることになり、さらには関連市場のオープン化と活性化が期待される。

本プロジェクトでは、上記のようなインターネット ITS の実現に向け、共通基盤仕様の策定と基盤構築、および、ITS 関連サービスに対する共通インタフェースの提供を目指している。この

ような一連の基盤技術をインターネット ITS 基盤と呼ぶ。また、基盤の構築を軸とした関連技術の研究開発促進と実行環境の共有による実証の効率化と、これに伴うより多様なサービスの提供や新規市場の開拓が期待される。

今回のインターネット ITS プロジェクトへの参画の主な目的は、自動車がインターネットを通じて外部社会と常時接続されることで、どのような情報がインターネット上を流通するのかを確認することである。すなわち、サービスを利用する実空間のエンティティを「自動車」または「乗車している人間」とし、インターネット上を流通する実空間の情報やサービスを体系的に整理することを主な目的とした。また、本プロジェクトのコンセプトを具現化した高機能実験車による各種サービスの実証実験を通して、今後の情報流通およびサービスの在り方と検討が必要な技術項目について検討をした。

6.2.3. インターネット ITS によって実現されるサービスイメージ

インターネット ITS 基盤の実現により、通信基盤としてインターネットを利用し、提供するサービスの内容やサービスの提供場所等に応じた通信事業者や通信手段を選択することが可能になる。これにより、インターネットと自動車および ITS 関連システムとの強力なコネクティビティが実現可能となる。

つまり、自動車および従来の独立した ITS 関連システムに、インターネットを通じた外部社会との接続性を提供可能となる。これにより、様々なシステムの統合による新規事業や連動・協調サービスなどが実現することが予想される。ここでは、インターネット ITS 基盤が実現した際のサービスイメージを体系化し、新規ビジネスチャンスの創出の可能性について検討する。

インターネット ITS 基盤を用いたサービスイメージ 6.1 は以下の 8 種類に分類される。

1. 受信
   情報の受信に関するサービス要素。ドライブ情報や、他公共交通機関情報、駐車場情報等を車両で受信するサービス等。大容量データのダウンロードやコンテンツ配信や、車内の各シートでの WWW 閲覧およびメール確認などのサービスを提供/享受できる。

2. 発信
   情報の発信に関するサービス要素。移動中の車内情報 (速度など) をインターネットに向けて発信することによるサービス等。これらの情報を蓄積・分析することにより、旅行時間情報や渋滞情報、降雨情報等の価値ある情報に加工できる。また、車両の状態情報を発信することにより、安全運転支援や事故や故障検知が可能となり、緊急時のドライバの情報 (生体情報等) を発信することができる。

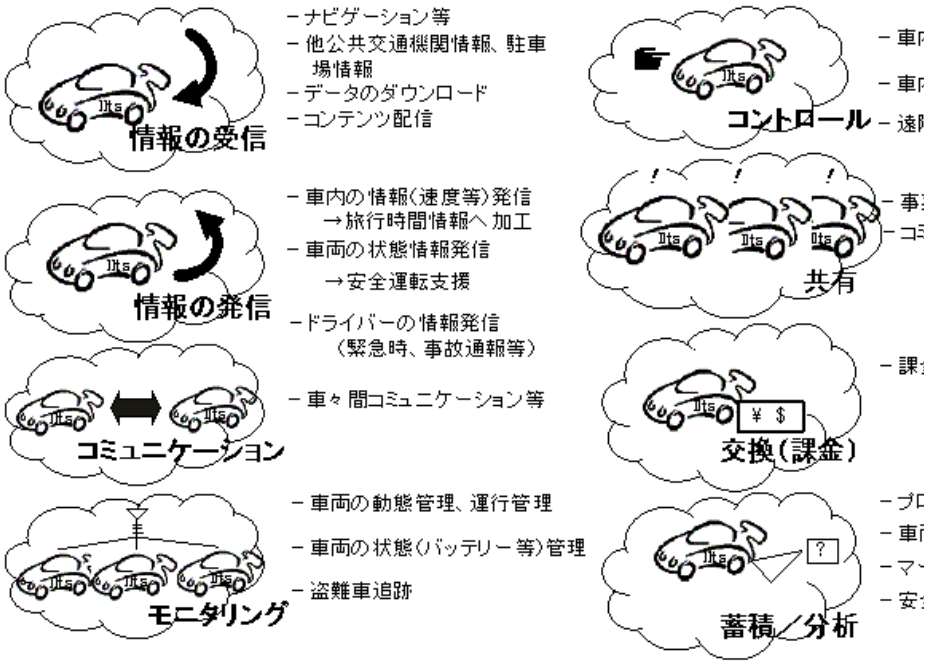

図 6.1: インターネット ITS サービスイメージの分類

3. コミュニケーション
   情報の送受信に関するサービス要素。たとえば、無線通信技術を用いた車車間通信によるコミュニケーションサービスやグループ管理機能を備え、音声および画像処理技術を用いたシステムが考えられる。

4. モニタリング
   情報の観測に関するサービス要素。移動車両の動態や、タクシーやバスなどの位置情報を管理するサービス等。エンジン停止時電源供給問題が解決された場合は、駐車時の車両監視や盗難車追跡サービスも可能となる。

5. コントロール
   操作・制御情報の送受信に関するサービス要素。ドアロックやエンジン始動など、車内機器を外部から操作するサービス、および、車内から扉や窓の施錠や家電製品の操作など、外部機器を操作するサービス等。これについては、車両と通信双方の安全性を十分に確認した後に実現されることが期待される。

6. 共有
   情報を共有することに関するサービス要素。インターネット上に集積された車両からの情報を共有し、加工することで異なる事業の共同化や連携サービスが可能となる。これにより、新しいコミュニティが創出され、新たな ITS 市場の形成が予想される。

7. 交換 (課金)
   情報とその対価の交換に関するサービス要素。料金の自動収受システムや駐車場およびガソリンスタンドなどの課金・支払いシステム等。

8. 蓄積・分析
   情報を蓄積・分析することにより高度利用を行うサービス要素。プローブ情報等の情報の集積および加工、または開発した車載機器の技術を応用したサービス等。車両開発やマーケティング、道路交通計画などに対する分析などが考えられる。また、道路管理と緊急通報に連動した保険などのサービスも期待される。車両の位置情報とあわせて、車両状態 (バッテリーや燃料、エンジン等) の情報を蓄積・管理することで、最寄りのガソリンスタンドや修理工場などを検索することも可能となる。

ここでは、サービスを利用する実空間のエンティティを主に「自動車」および「乗車している人」として捕らえている。すなわち、「自動車」から発信される各種情報の分類や、ITS 分野で今

後開発が予想されるものも含めた「利用者」一人ひとりのためのサービスに関して、横断的な意見を検討し、インターネット上を流通する実空間の情報やサービスとして体系的な整理を行った。

6.2.4. インターネット ITS プロジェクトの活動体系

インターネット ITS プロジェクトでの活動は、社会的要請に沿った技術的な研究基盤の構築からその基盤を用いたサービスの体系化まで、多岐にわたる。そのため、本プロジェクトでは、2001年度の活動体系として今年度の活動をその目的および役割ごとに分割した上でワーキンググループ (WG) を設置し、互いに連携しながら協調して検討及び研究開発を行った。WG にはプロジェクトの関係各社から技術者と決議権をもつ関係者が数名ずつ所属し、研究開発に関する議論と実働を進めた。2001 年度、本プロジェクトで設置した WG は 以下のとおりである。

- インターネット ITS 基盤の仕様策定
  基盤のシステム構成や車両データ辞書の標準化、個別車両/地理位置情報、名前空間の構築方針など、車両をインターネット側からどのように見せるかを規定する基盤仕様の検討と策定を行う。

- インターネット ITS のコンセプト検討
  インターネット ITS プロジェクトにおいて全体活動の軸となるサービスイメージの分類および技術開発コンセプトを構築する。本プロジェクトで検討したインターネットおよび車載技術を搭載した高機能実験車の制作にも取り組む。

- インターネット ITS のポータルサイト作成および運用
  インターネット ITS プロジェクトの活動を広く周知し、そのサービスを提供するための、会員管理を含む情報集約センター機能を中心としたポータルサイトを構築し運営する。

- 高機能実験車の開発
  インターネット ITS が目指す姿を想定した上で、将来実現されるであろう技術の一部を具現化した車両を製作し、技術の検証とアプリケーションの実証を行う。

これらの他に、インターネット ITS プロジェクト設立時や名古屋/首都圏の実証実験開始時などのプレス発表の開催、NETWORID+INTERROP2002(N+I2002) [29] やワイヤレスジャパン 2002 [30] などの各種イベントへの参加など、本プロジェクトの周知促進および開発した基盤技術などの普及戦略を目的とする広報活動について検討した。

6.3. 実証実験の実施

インターネット ITS で構築した基盤の有効性を検証し、2001 年度のプロジェクトの成果を正しく評価するため、2002 年 1 月から 3 月の間に大規模な実証実験を行った。ここでは、これらの大規模実証実験の目的と、プロジェクトのコンセプトを具現化した高機能実験車における実験の概要について述べる。

6.3.1. 実証実験の目的

実証実験の主な目的は、インターネット ITS が提唱するコンセプトおよび基盤仕様を実証し、技術的課題と事業化の可能性を検証することである。また、この実証実験の結果を基に、プロジェクトを広く周知させ、情報発信することも目的の一つであった。

6.3.2. 実証実験の概要

共通の ITS 基盤の構築による今後の ITS 分野の産業の成長を促進することを目的に、1 台の高機能実験車による実験と、首都圏および名古屋地区における約 1,570 台の車両を用いた大規模実証実験を 2002 年 3 月までに実施した。

ここでは、自動車がインターネットを通じて外部社会と常時接続されることで、どのような情報がインターネット上を流通するのかを確認するために、主に、プロジェクトのコンセプトを具現化した高機能実験車 (図 6.2) による各種サービスの実証実験について述べる。

コンセプト検討 WG では、インターネット ITS の技術開発およびサービスコンセプトを確立し、それに対応してインターネット ITS が目指す姿を検討した。高機能実験車の開発コンセプトは、以下の通りである。

> 車は、車外の周辺環境 (事故、天候、気温、路面状況、交通流) を”Sense”し、車内の環境 (運転者、搭乗者、音楽、目的地、予定経路) も”Sense”する。インターネット ITS の 5 年後、10 年後は、車内外の空間を”Connect”することで新しい空間を”Create”する。特に個人を認証し、一人一人に特化したサービスの実現を目指す。

これらの検討を基に、実現されるであろうシステムの一部を具現化した高機能実験車を製作し、技術の実現性検証と、アプリケーションの設計、実装、評価実験を行った。

高機能実験車は、将来にわたるインターネット ITS が目指す姿を想定した上で、実現されるであろうシステムの一部を具現化したものである。実証実験では、技術の実現性検証とアプリケーションの実証を行った。

図 6.2: 高機能実験車

技術の実現性の検証

IPv6 による車内ネットワーク化、メディアフリーの通信ルータ機能の開発により、車が外の世界とシームレスに繋がり、車がいつでも、どこでも、サービスを利用できる環境を構築し、技術的検証を行う。

- IPv6 の有効利用
- Mobile IPv6 の利用
- Mobile Network の実装
- 複数通信メディアの有効利用
- 音声インタフェース (運転者安全運転支援、乗員別健康管理、グループメディアコミュニケーション、車両動態監視)

アプリケーションの検証

実証実験を行ったアプリケーションは以下の通りである。

- 安全運転支援
  運転者の運転状態を、車内のセンサ情報と GPS 情報より解析し、安全運転診断結果として表示する。

表 6.1: インターネット ITS の開発技術と実証実験の対応 (ネットワーク基盤層)

研究開発技術	高機能実験車	首都圏実験	名古屋実験
通信インタフェース自動切り替え	メディアフリーの通信ルータ機能	DSRC と PDC-P	DSRC と PDC-P
IPv6 利用	IPb6 ベースの車内ネットワークとの構築、および WIDE ネットワークに IPv6 接続	IPv6 over IPv4	IPv6 over IPv4
MobileIP 利用	グループコミュニケーションにおいて end to end 通信	-	-
IP over DSRC	大容量コンテンツ配信	大容量コンテンツ配信およびキャッシュレス決済	大容量コンテンツ配信

- 健康管理
  各乗員毎の健康状態を、耳に装着する生体センサから脈拍情報を取得することにより表示する。
- グループコミュニケーション
  各席毎に設置したディスプレイ、マイク、カメラ、スピーカを用いたテレビ会議サービスの提供を行う。

6.4. サービス分類と実証実験の関係

インターネット ITS の共通基盤として研究開発した前述の技術は、各実験においてシステムに実装し、検証を行った。表 6.1, 6.2, 6.3 に、共通基盤として研究開発した技術と、各実験における状況を示す。

また、各実験において実証したアプリケーションと 6.2.3 節で体系化したインターネット ITS のサービス要素との関係は、表 6.4 の通りである。

表 6.2: インターネット ITS の開発技術と実証実験の対応 (サービス基盤層)

研究開発技術	高機能実験車	首都圏実験	名古屋実験
車両データ辞書	様々なサービス	様々なサービス	様々なサービス
プローブ情報管理	車両の状態、運転者の状態をリアルタイムでモニタリング	-	1,570 台のタクシー利用
会員管理および決済	DSRC を介してキャッシュレス決済	DSRC を介してキャッシュレス決済	-
位置情報管理	位置に応じたコンテンツ配信	位置に応じたコンテンツ配信	タクシーの運行管理と位置に応じたコンテンツ配信

表 6.3: インターネット ITS の開発技術と実証実験の対応 (アプリケーション基盤層)

研究開発技術	高機能実験車	首都圏実験	名古屋実験
JAVA VM	アプリケーション実行環境として利用	アプリケーション実行環境として利用	アプリケーション実行環境として利用

6.5. プロジェクト参画の成果と課題

6.5.1. 全体的な成果

インターネット ITS 共同研究グループにおいて、将来的な事業化を視野にいれた基礎的な研究開発のためのコンセプトの検討とサービスの体系化、必要技術の抽出等を行った。本プロジェクトに参加することで得られた成果は、以下の 4 点である。

- コンセプトの明確化
  インターネット ITS 基盤を利用したサービスを検討し、インターネット ITS の将来像、目指す姿を伝えるための資料を作成した。
- 共通基盤となる技術の開発およびフレームワークの具現化
  インターネット ITS の共通基盤として基盤仕様 (素案) を策定した他、共通サービス基盤の基本的な機能を検討・構築した。

表 6.4: インターネット ITS のサービス体系と実証実験

実証したアプリケーション		サービス要素							
		(1) 受信	(2) 発信	(3) コミュニケーション	(4) モニタリング	(5) コントロール	(6) 共有	(7) 交換(決済)	(8) 蓄積・分析
名古屋実験									
	タクシー業務用サービス 車両位置・動態情報				●		●		
	タクシー業務用サービス 走行実験管理				●				
	タクシー業務用サービス 道路混雑度・降雨情報	●	●						●
	乗客向け情報提供サービス	●							
	プローブ情報提供サービス	●	●						●
首都圏実験									
	ガソリンスタンド サービスガイダンス	●		●					
	ガソリンスタンド コンテンツ配信	●							●
	駐車場 入退場制御			●					
	駐車場 キャッシュレス決済							●	
	駐車場 コンテンツ配信	●							
	走行中のコンテンツ配信 プッシュ型、プル型配信	●							●
高機能実験車									
	安全運転支援		●		●				●
	健康管理		●		●				●
	グループコミュニケーション			●					

- 一部アプリケーションのフィールドでの検証
  実験システムを構築し、高機能実験車を用いた実験を実施し、システムの技術開発面、利用者からみたサービス面等に関わる知見を得た。

- プロジェクトの社会的認知
  プロジェクトについて、積極的な周知・広報活動を図ることにより、幅広く社会的認知を得た。

6.5.2. コンセプト構築に関する成果

インターネット ITS のコンセプト、サービス体系および実証実験実施のための要素技術をふまえ、コンセプトを実現するために確立すべき基盤技術を抽出し、分類した。インターネット ITS により実現される様々なサービスに関するアイディアをワーキンググループ内で収集し、これらを情報の利用者、提供者、およびその流れという視点で整理し、サービスを「情報」の視点で 8 つの要素に体系化した。これらの要素を組み合わせることにより、様々なアプリケーションが実現される。サービス体系は、インターネット ITS のサービスを分かりやすく説明する材料として、また、アイディアの発想を促すための土台として活用可能なものとした。

6.5.3. 共通サービス基盤構築に関する成果

インターネット ITS のコンセプトおよび様々なアプリケーションを想定し、検証および実証実験を行うべき機能を共通サービス基盤として抽出・検討し、実験用に構築した。今後、幅広い範囲でのアプリケーション開発を前提とし、実用化に向けた共通サービス基盤のさらなる機能改善、特に、セキュリティやプライバシ保護などを図っていく必要がある。

6.5.4. 高機能実験車に関する成果

インターネット ITS の将来像を一部具現化した実験車両を試作し、技術的可能性を調査するとともに、将来的なサービスコンセプトのデモンストレーションを行うことにより、インターネット ITS の可能性を社会にアピールすることができた。IPv6 を利用した通信ネットワークの構築と、車両情報の動的取得、車載ルータの構築、通信インタフェースの自動切り替えなどの機能を確認することができた。また、デモンストレーションを含む実施サービスとして、安全運転支援、健康管理、グループコミュニケーションの他に、全方位視覚センサを用いた車両周辺情報取得、音声ポータルサイト、車内での各席毎の WWW サイト閲覧、プッシュ型またはプル型の情報配信のための会員サービス、車両情報監視などの動作確認を行った。

6.6. 今後の研究課題について

ここでは、インターネット ITS プロジェクトの 2001 年度の活動では開発できなかった技術 (今後の展望/将来性) について述べ、インターネット上の情報流通の観点からの研究課題について整理する。

6.6.1. 全通信路の IPv6 化

今回のインターネット ITS 基盤では既存の携帯電話網などの通信基盤を用いたが、一部サービスで IPv6 対応でない部分が残っていたため、全ての通信路の IPv6 化は実現できなかった。従って、本実証実験は、IPv4 および IPv6 のネットワークが混在した、インターネットプロトコル過渡期の実験として評価している。今後、インターネットが IPv4 から IPv6 へシフトし、全ての通信基盤やサービスが IPv6 対応になることを踏まえて、サービス基盤を再構築していく必要がある。

6.6.2. すべての車載機器に対する IP アドレスの割り当て

2001 年度の実証実験では、車両に搭載している全ての機器に IP アドレスを割り当てることができなかった。設計の段階では、IPv6 や Mobile IPv6 の採用などにあるように、広大なアドレス空間での end-end 通信を前提としているため、今後、安全基準を理解した上で、車載機器の独立した通信/制御の必要性の議論と開発に向けた技術的な検討を行う必要がある。

6.6.3. セキュリティ

課金システムや情報の提供・配信システムを取り扱う情報通信基盤を構築する上で、必須となるセキュリティ機能の検討・開発および整備を行う必要がある。今後、社会基盤の一つとして普及させるため、以下の項目について検討する。

- 個人情報を扱うサービスを構築する際に必要となるプライバシ、セキュリティ対策
- 通信路の安全性を中心とする、情報の完全性と機密性の確保
- AAA(認証・承認・課金:Authentication, Authorization, Accounting) の整備

6.6.4. ビジネスチャンスの創出

インターネット ITS プロジェクトでの活動は、社会的要請に沿った技術的な研究基盤の構築からその基盤を用いたサービスの体系化まで、多岐にわたる。つまり、インターネット ITS 基盤を用いたサービスは、自動車、自動車部品、電気電子、通信関連といったインフラ提供側の企業に

とどまらず、商業・流通業、輸送事業者、ガソリンスタンド、駐車場、飲食店、小売店舗、各種コンテンツ提供者等の広汎な企業が関与できるものであるといえる。これは、今まで独立にシステム開発を行っていた産業の統合や、開発コストの低減、サービスの組合せによる新規事業の発現など、極めて大きなビジネス機会を創出するといえる。

6.6.5. 既存システムとの協調・連携

ITS に関わる取り組みとしては、官主導の VICS や ETC、安全性対策への取り組みなどが展開されている他、民間の様々なサービスも実現している。現在、ITS 分野における安全性対策として、既存のプラットフォームを用いた passive safety から、先読みや警告などのサービス提供を基にした active safety へのシフトが行われている。これには、立証責任や性能の規制、車両の識別やプライバシ保護問題、国際協調などの様々な課題が残されており、活発な議論がなされている。

車両や利用者の識別および認証技術に基づいたサービス事例としては、以下のものが挙げられる。

旅行者支援サービス

広域旅行者支援サービスとしては、511 travel information が実用化されている。これは、米国にいる旅行者が 511 に電話をすることで、現地の交通情報や乗り換え、天気などの情報を音声により得ることができる。現在は電話をかけてきた位置情報と、旅行者が能動的にサービスを選択することにより、必要なサービスを提供している。

WIM

WIM(Weigh-In-Motion) は、走行中のトラックの重さを計る技術である。基本的には路上にセンサを設置し、積み荷がない状態と積み荷がある状態のトラックの重さをチェックし、その差分と、運転手の識別情報などをセンターが管理する。これは、トラックと積み荷、および運転者の識別を電子的に行い、過積載や国境を越える際の手続きなどをスムーズに行うための技術であり、日本よりはむしろ欧州、米国などで研究開発の進んでいる技術である。これは、運転者の識別をすることにより、だれがどんな積み荷を持って、どこを通って出入国をしたか、という情報がセンター側で把握されている。

緊急通報

緊急事態が発生した場合の大まかな位置情報を用いた通知システムではなく、どの道路のどの車線のどの向きで、また、そのときの人間の様子はどのようなものか、ということを網羅した形でのサービス提供を念頭に置く必要がある。これには、availability の高い位置情報検出技術と車両および利用者識別技術が必要となる。

利用者への支援を行うものとしては、E-call システムが挙げられる。これは、車の位置情報、つまり E911 を用いた携帯電話の位置情報を基に緊急事態が発生した位置を割り出し、サービスを行うものである。これに対し、ACN(Automatic Crash Nortification) は、人の介在なしに緊急通報を行うものであり、言語や身体状態に関わらず通知を行うものである。

これらの技術でも、車両や利用者の識別と、その属性としての位置情報、時刻などの情報をより的確に収集することが必要とされる。

このように、運転者 (利用者)、車両、および積み荷の識別とその運転者 (または車両) の持つアクセス権限を保証する仕組みが必要とされており、車両の識別に関しては、AVI(Automatic Vehicle identification) および AVC(Automatic Vehicle Classification) 等、国際標準化を視野にいれた検討が行われている。

また、車両や運転者の識別により発生する問題として、個人のプライバシに関する議論が必要となる。たとえば、ロンドンやローマでは、走行している車のナンバープレートを識別する技術が開発されている。これは、物理的なチケットによる車両識別ではなく、カメラによるナンバープレートの読み取りおよび電子的に識別処理をする技術を用いている。この技術の実用化のために、プライバシ情報の取り扱いについての議論が行われている。

このように、ITS 分野では現在、様々な分野からのサービスの創出や安全性対策への取り組みなどが展開されている。インターネット ITS の基盤を利用して構築されたシステムがこれらの既存システムと協調し、研究開発および事業投資の効率化とサービスにおける様々な付加価値創出を行うために、実空間エンティティの識別・認証とサービスへのアクセス制御、および個人のプライバシ保護に関する更なる議論が必要となる。

6.7. ま と め

ここではインターネット ITS プロジェクトの概要と活動体系および実証実験により得られた知見について述べた。

インターネット ITS プロジェクトは、共通基盤の設定と構築、および、各 ITS 関連サービスに対する共通インタフェースの提供を軸とし、関連技術の研究開発促進と実行環境の共有による実証の効率化を目指した産官学共同のプロジェクトである。今後、ITS のみならず今後の移動体通信環境の各種サービスに対しても、共通の通信基盤とインタフェースを提供するように関連システムの再構築を図ることで、技術・社会環境・市場などの急激な変化に柔軟に対応した、効率的かつ多面的なサービスの実現が期待される。

プロジェクトでの活動を通して、インターネットというオープンな情報通信基盤を用いること

で、異分野にある技術研究が協調および共生し、新たなサービスの発現することを議論した。また、特に、「自動車 (車両)」や「利用者」の識別とサービス利用のための認証機能は、既存または将来的に構築されるサービスの協調や連携を考えるうえで、たいへん重要になることを確認した。つまり、実空間の情報をインターネット上で取り扱うサービスの構築にあたり、実空間のエンティティに帰属した情報流通、特に個人の識別とその利用権限を示すための認証およびアクセス制御機能や、プライバシ保護に関する流通制御の必要性を確認した。

Part III

ユビキタス環境におけるネットワーク資源提供のためのサービスモデルの提案

Chapter 7

情報フィルタリング技術とユーザプロファイル

インターネット上を流通する情報の増加にともない、利用者の個人情報や興味・嗜好を利用して情報を絞り込む情報フィルタリング技術が開発されている。ここでは、個人情報としてのユーザプロファイルを用いた情報フィルタリングの技術動向について、ユーザプロファイルの利用例や管理方法を軸に整理する。また、個人情報流出の危険性を低減するために、必要なシステム設計について検討する。

7.1. 情報フィルタリング

インターネット上には、膨大な量の情報が流通している。これらの情報は、情報検索、ブラウジング、情報フィルタリングといった方法で利用者によって収集、利用されている。これらの情報収集方法の中でも、自分にとって有用な情報を選別する、すなわち、必要な情報を切り出して収集する情報流通制御方法として、情報フィルタリングに着目する。

情報フィルタリングとは、利用者に対して送信される情報のうち、有害なものを除外したり、情報の重みづけ、優先度を与えたりする情報収集手法であり、メールの選別、消費や情報のランクづけなど、様々な場面で利用されている。

7.1.1. 情報フィルタリングの分類

現在の情報フィルタリング技術、認知的フィルタリング [31]、社会的フィルタリング、経済的フィルタリングの三つに大別される。

認知的フィルタリング (Cognitive Filtering)

情報それ自身の内容と、利用者の情報に対するニーズ (プロファイル) を比較し、与えられた情報とプロファイルの関係に基づいてフィルタリングを行う。

表 7.1: プロファイル構成要素

フィルタリングの分類	プロファイル構成要素
認知的フィルタリング	キーワード、キーワードベクトル、概念マップなど
社会的フィルタリング	利用者の地位、役職、友人関係、他の利用者とのプロファイルの類似度など
経済的フィルタリング	利用者の予算、許容できる長さなど

社会的フィルタリング (Social Filtering)

情報の内容ではなく、情報の送信者の特徴や受信者との関係に基づいてフィルタリングを行う。

経済的フィルタリング (Economic Filtering)

情報を得ることによる利益と、情報を得るために必要な対価の比に基づいてフィルタリングを行う。ここでいう対価とは、情報に対する課金のような明示的なものだけでなく、メッセージの長さやその他の心理的な要因も含んでいる。

各フィルタリング手法毎のプロファイル構成要素の一例としては、表 7.1 のものが挙げられる。本研究では、インターネット上の実空間情報の流通に関して、個人や移動計算機などの、実空間エンティティに帰属した形で選別することを目指しているため、認知的フィルタリングに着目する。

7.1.2. 関連研究分野とユーザモデル

情報フィルタリング、およびユーザモデルに関する研究は、知識マネジメント、ナレッジマネジメントなどの分野等で広く行われている。これらの分野では、複数の人による知識の共有を目的としており、文献 [32] をはじめとする協調フィルタリング (Collaborative Filtaring) に関する研究が深く行われている。

利用者の個人情報や嗜好、関心に対して動作するシステムでは、それらの利用者情報を明示的に計算機上に表現する必要がある。この表現は、ユーザモデル (ユーザプリファレンス) と呼ばれ、表現する過程をユーザモデリングとされる。

たとえば、WWW 情報空間における利用者の活動履歴を追跡する場合、WWW サーバアクセスログを利用することにより、検索エンジンへの検索キーワードの利用、または複数のブックマークを用いたモデリングが存在する。しかし、WWW サーバアクセスログや Cookies を利用した情報フィルタリングは、利用者のプライバシに関する情報を扱う。利用者の活動履歴を通じて、個人の興味・関心だけでなく、性別や年齢、住所、などの実空間における情報を掴むことが可能で

ある。しかし、このモデリングに用いる利用者プロファイルは利用者個人が自らの意志で隠蔽または提示することができないため、システム構築の際に、この管理を厳重に行う必要がある。

利用者が個人情報開示の制御権を持つことにより、プライバシーを保護できるフレームワークとして、「オープン・プロファイリング・スタンダード (OPS)」が挙げられる。

7.1.3. Open Profiling Standard (OPS)

OPS は、インターネット上に流通する利用者情報について、そののプライバシ保護を目的としている。WWW の技術スタンダードの国際管理機関である W3C[1]の P3P[2] によって検討され、現在では多くの団体企業が賛同している。

OPS は、WWW ブラウザに組み込まれる機能として策定され、利用者はあらかじめ自分の個人情報を入力し、計算機のハードディスク内に保存しておくことができる。情報の項目は、名前、住所、電話番号、メールアドレスのほか、年齢、性別、職業、非既婚の別、関心事、趣味などである。これらの「パーソナル・プロファイル」は暗号化した形で保存され、OPS を採用した WWW サイトでユーザー登録を求められた場合に提示する。

利用者が初めて訪れるサイトにアクセスすると、計算機の画面にウィンドウが現れ、サイト側が公開を求めている個人情報の項目の表示に基づき、利用者は求められた情報について「すべて公開」、「一部の項目のみ公開」、あるいは「非公開」などの選択を自分自身で決定できる。つまり、OPS は WWW における「インフォームド・コンセント (内容説明のうえでの承諾)」のフレームワークとなると言える。

また、一方で、OPS を採用した WWW サイトやソフト会社は、個人に対するサービスやアプリケーション開発の共通プラットフォームとして利用することで、利用者に関する知識に基づき、そのニーズに合わせたよりよい機能を提供できる。また、WWW サイトにとっては、利用者が許諾した情報しか利用しないことを明らかにし、利用者からの信頼を得る効果も期待できる。

OPS によって、ネットワーク上を流通する個人情報の取り扱いや表現が規定されており、現在では、Microsoft Office XP リソースキットや、データベースに対してログイン可能なアカウントを作成し、そのユーザーを許可する方法としても利用されている。

しかし、OPS によって制御できるのは、インターネット上を流通する個人情報の一部である。たとえば、WWW サイト側がブラウザ通して、利用者の計算機のハードディスクに送ってくる Cookie 情報は保護の対象とならない。利用者があるサイトを訪れると、サイト側のサーバと利用者側のハードディスクに、その利用者のサイト上での行動や登録した名前などの情報が、Cookie

[1]World Wide Web Consortium

[2]Platform for Privacy Preference Project

として蓄積される。利用者が次回そのサイトを訪れると、サイト側が Cookie で利用者を認識し、サービスをカスタマイズしたり、ターゲット広告の表示などに利用する。Cookie は、通常は、それを置いた WWW サイトにしか認識できないとされているが、これらの情報が流出した場合、個人の購買履歴や検索結果などが露出してしまう。

このように、利用者のプライバシ保護は、情報フィルタリング、特に協調フィルタリングシステム開発において重要な課題となっている。

7.2. ユーザプロファイルの利用例

利用者の情報に対するニーズや個人情報を含むユーザプロファイルを用いた情報フィルタリング技術は、現在では様々な場面で利用されている。たとえば、ユーザプロファイルを条件として情報を検索したり、無料でインターネット上のサービスを提供する代償として顧客の興味を引きそうな広告選定に利用されたりしている。また、WWW のサービスだけでなく、広告やニュースを電子メールで配信するための技術や利用者毎にウェブページの表示を変更するものもユーザプロファイルによって実現できる。近年では、利用者毎のウェブページ表示の変更に、前節で概説した OPS ではなく公開鍵暗号基盤のクライアント証明書を用いる方法も存在する。

また、携帯電話やノート PC を持ち歩くモバイルコンピューティングの普及により、現在位置にあった情報を提供するための個人の位置情報をフィルタリングに利用する技術もさかんに開発されている。

このような情報フィルタリング技術に関連する技術は、特許出願が増加している。特許出願動向の詳細については、文献 [33] に掲載されている。これらの特許出願状況と文献に関しては、特許庁が管理している特許電子図書館[3] により参照可能である。

7.3. ユーザプロファイルの取得方法

サービス提供者は、ユーザプロファイルを情報フィルタリングに用いることで、サービス利用者の個人情報を保護すると同時に、サービス範囲内の情報流通を制御している。

ユーザプロファイルの取得は、主に以下のような方法で取得している。

利用者による事前登録

利用者からサービス開始前にプロファイルを提示

[3] http://www6.ipdl.jpo.go.jp/Tokujitu/tjsogodbk.ipdl

購買履歴の取得

購買履歴をサーバ側で保存することによりプロファイルを作成

利用者の情報閲覧履歴

サーバアクセスログやブックマークなどを用いたプロファイル作成

検索条件履歴の取得

検索キーなどの入力情報を保存ことによるプロファイル作成

このように、既存の情報フィルタリング技術では、意識的、または無意識的にユーザプロファイルをサービス提供者側が収集する。つまり、サービス利用時にはユーザプロファイルはサービス提供者側に存在することになる。ユーザプロファイルの変更および有効期限やアクセスログ、Cookieなどを用いた個人情報収集はサービス利用者にとって個人情報の流出に不安を抱く大きな材料となる。

7.4. 自己情報制御機構

一個人に対して、プロファイルをサービス提供者側に登録したり、無意識の内に行動履歴を取得されたりすることを防ぐために、「自己に関わる情報について一定のコントロールをおよぼす権利 (自己情報制御権)」 [34] に関する検討が必要になる。これは、複数のプロファイルの使い分けが想定する場合にも有効である。

近年になって、インターネット上でのコンテンツ流通を安全に実現するための技術的需要が高まっている。たとえば、自己情報制御をプライバシの権利として扱う研究として、プライバシを重視したアクセス制御機構の提案 [35] では、クライアントは、自分で「ここまでは公開してかまわない」と考える範囲の個人情報をサーバに与え、サーバがそれに応じたアクセス制御を行うことが出来るシステムを提案している。さらに、認証とアクセス制御の分離、使い捨て公開鍵の利用により実現可能性を示し、匿名アクセスコントロールの枠組みを提供している。また、NTT サイバーソリューション研究所における提供者の意思に基づく情報流通のための開示制御技術 [36, 37, 38, 39] では、信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案を行っている。

しかし、これらの提案技術には、構成要素や処理が増加し、規模性に問題がある、流通させる情報やサービスを限定している、などの課題が残されている。

また、情報発信者 (情報提供者) に対する個人情報は、移動通信環境においては、位置情報や時刻などの動的な情報も含まれるため、このような情報を含めたプライバシ保護のための情報フィルタリングについては、検討されていない。

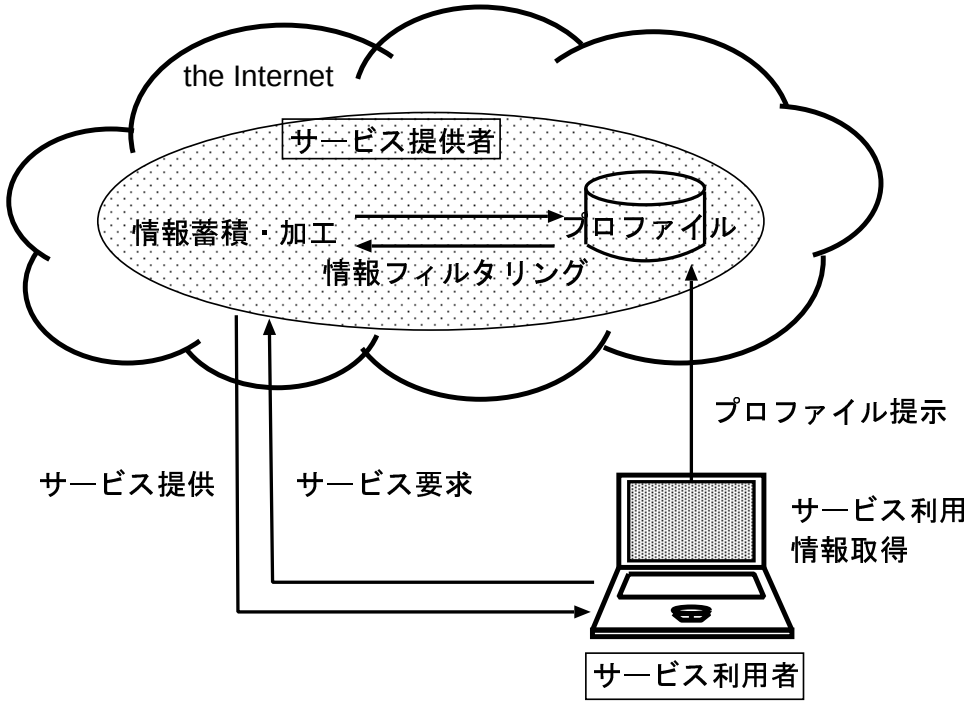

図 7.1: フィルタリング時のユーザプロファイル

7.5. ユーザプロファイルの在り方についての考察

情報フィルタリング技術の主な目的は、インターネット上に流通する膨大な量の情報を個人情報や利用者の興味・嗜好などのユーザプロファイルに基づいて制御することである。

しかし、利用するユーザプロファイルは、インターネット上のサービス提供者側に事前に登録したり、サービス側から取得可能であったりする (図 7.1)。

既存技術では、ユーザプロファイルをサーバに登録したり購買履歴、検索履歴などをサーバ側が自動的に取得したりしている。つまり、利用者は個人情報が含まれるユーザプロファイルを意識的または無意識の内にインターネット上に開示していることになる。ユーザプロファイル自体が OPS などのように暗号化などの保護処理を施されてていたとしても、利用者にとって個人情報の流出に対する不安が解消されるわけではない。

また、現在までの情報フィルタリング技術が扱う情報は、インターネット上にすでに存在する情報の選別と制御である。移動体通信によりもたらされる実空間プローブ情報は、実空間に存在するエンティティから、インターネット上に流通させるための情報を発信することで成り立っており、情報発信者、つまり、情報提供者とサービス提供者が異なる場合がある。

したがって、サービス利用者が、本人のユーザプロファイルを登録したり無意識の内に収集されたりすることなく、利用者本人が、自己情報として情報制御する仕組みが必要であると同時に、匿

名性を保った情報発信などの、情報発信者 (情報提供者) に対する個人情報保護のための情報フィルタリングが必要であると言える。

また、情報フィルタリング技術は、「情報を選別する」ためには有効な手段であるが、「サービスを付与する」ことは、サービス提供者側とサービス利用者の意思を反映した認証および権限委譲、アクセス制御などの別の枠組みが必要となる。

実空間のエンティティに帰属した形でインターネット上で実空間情報を流通制御し、サービスの連続性を保つためには、情報フィルタリングだけでなく、認証および権限委譲機構の検討が併せて必要となる。

7.6. ま と め

インターネット上を流通する情報の増加にともない、利用者の個人情報や興味・嗜好を利用して情報を絞り込む情報フィルタリング技術が開発されている。ここでは、個人情報としてのユーザプロファイルを用いた情報フィルタリングの技術動向について、ユーザプロファイルの利用例や管理方法を軸に整理した。これにより、インターネット上に存在する膨大な量の実空間情報を流通制御するための手法としては、ユーザプロファイルを情報フィルタリング技術のモデリングは有効であるといえる。

しかし、実空間情報をインターネット上で流通制御し、サービスを行うためには、インターネット上に情報を発信する「情報提供者」の自己情報制御機構とサービスの提供や移動にともなうセッションのマイグレーション等の検討が必要である。情報収集手法である本技術だけでは実現できない。

情報の選別だけでなく、シームレスなサービス提供に関しては、「信頼」に基づく認証およびサービス委譲機構が不可欠な要素と言える。

Chapter 8

認 証 機 構

インターネットとは、そもそも「ネットワークのネットワーク」であり、バラバラに存在する複数のネットワークが連結して一つのコミュニケーション空間を創っている。このコミュニケーションの主体は自律性をもったエンドシステム、つまり個人である。前章では、個人情報 (ユーザプロファイル) を用いて情報をフィルタリングする技術について検討を行った。ここでは、自律的に行動する個々の利用者が有機的に形成するコミュニケーションを考慮し、既存の認証機構 (Authentication) とおよびサービス委譲機構 (Authorization) について整理する。その上で、計算機や自動車、個人などの実世界に存在するエンティティに帰属した認証と、そのエンティティの属性という情報を認証ミドルウェアで流通制御するモデルを検討する。

8.1. 信 用 と 認 証

人間の生活は、他との通信、つまりコミュニケーションを図ることによって成り立っている。現在は、社会生活をおくる上での生活基盤として、通信、エネルギー、交通、金融、医療、流通などの領域が挙げられるが、どの基盤上のシステムも、コミュニケーションを必要としている。

人間が他とコミュニケーションを図る場合、その内容に応じて、自分が指定した通信相手が本物であるかどうか、つまり、通信相手の認識/認証といわれるものが必要になる。また、通信相手にも対しても同様に、自分が「確に本人である」ことを示す必要が生じる。お互いの認証が正しく完了すれば、信頼関係が結ばれた状態となる。信頼関係とは、お互いに信用が結ばれた関係のことをいい、他人を信用することで信用取引が成立する。つまり、信頼関係を築き、信用取引を行うためにはまず、自分が誰であるか (相手が誰であるか) を正しく示す、認証技術が必要となる。

現実の社会では、印鑑、サイン、社員証、保証書などを用いることにより、日常的に本人認証が行われ、この信用取引が成立している。しかし、電子空間、特に移動通信を考慮にいれたインターネット上のサービスを提供/享受する際に、なりすましや不正アクセス、といった悪意ある問題や、移動によるサービスの中断、繰り返し認証といった技術的な問題が残されており、必要な信頼関係の構築がなされていない。

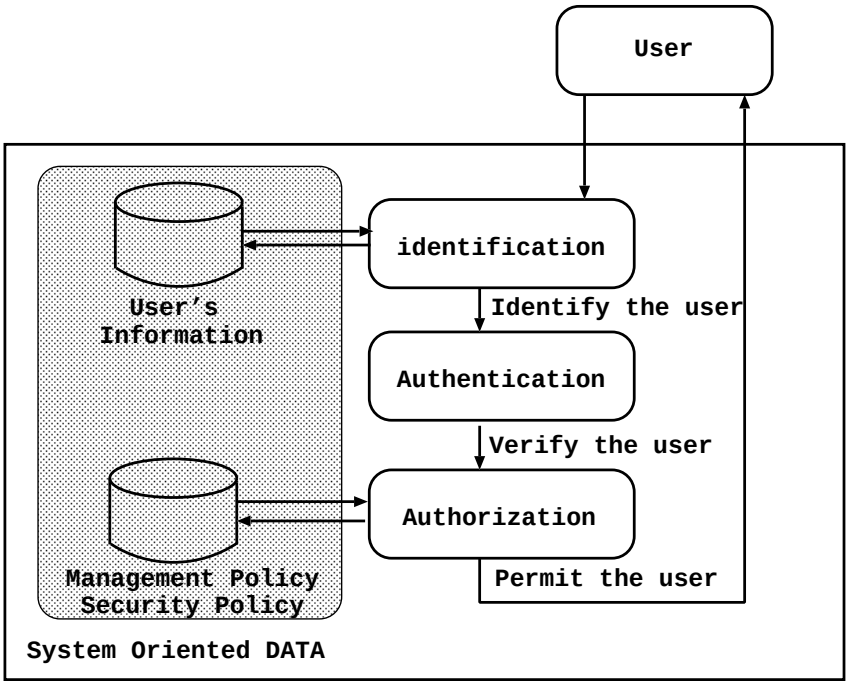

図 8.1: 識別/認証/委譲の関係

本章では、実世界での認証モデルについて概説し、電子空間、特にインターネット上に存在する代表的な認証モデルと比較をする。その上で、インターネット上での認証機構の必要性と現状の問題点を述べ、モデルの分類を行う。

8.2. 認 証 と は

認証 (Authentication) とは、計算機システムの利用者を、信頼できる形で特定する機構である。一般に、認証機構単独では意味をなさず、識別 (Identification) および委譲 (Authorization) 機構と深く関係する。

一般的な認証処理の流れ (図 8.1) は、以下のように考えられる。

1. 識別機構に利用者情報が与えられる
2. 認証機構により利用者が特定される
3. その利用者に対してシステム上での様々な処理権限が付与される

識別機構で与えられた利用者情報に基づき、その利用者が正しくその利用者であることを確認することが目的であり、システムが取り扱う利用者 (一般ユーザ、システム運用上必要な特権ユーザ、…) に依存して、適切な認証機構を検討し、設計する必要がある。

Identification(識別) 機構

システム内での利用者を表現するための方法を定める機構である。たとえば、UNIX システム上では、UID(整数値) で利用者を識別している。UNIX システムでは、利用者の利便性を確保するためにユーザ名 (英数字列) が用意され、ユーザ名から UID へのマッピングを行う機構が用意されている。

識別に利用される情報を identifier(識別子) と呼び、異なる OS では異なる識別機構を有する様に、システム毎に識別機構が存在する。識別機構は、システムの設計に深く関わっている。

Authorization(許可) 機構

利用者に対して適切な処理権限を付与するための機構であり、通常、OS などのシステムによって構成が異なる。システムがサービス利用者を識別し、認証機構で利用者が本当に正しい利用者かどうかを検証した後、その利用者に対するサービス委譲を行う。

8.3. 実世界とインターネット上における認証機構の役割

ここでは、コミュニケーションの相手との信用関係を築くという視点から、実世界での利用者 (個人) 認証の役割と、インターネット上での認証の役割について考察する。

8.3.1. 実世界における認証機構

実世界、つまり実社会においては、主に人間同士がコミュニケーションする場合に、「対峙している相手は本当に信用してよい相手かどうか」ということを検証する機構が存在する。本人証明のための認証機構として、たとえば、押印する、初対面の人と名刺を出して自己紹介をする、自動車運転免許証を出して身分提示をする、などが例として挙げられる。

この認証機構は、相互信用モデルと第三者認定モデルの二つに大別できる。

- 相互信用モデル

  相互認証モデルは、あらかじめ信頼関係を構築するための手続きをとっている個人同士が、自分自身しか持っていないものを提示することで、コミュニケーションの相手が正しい相手であることを確認している。たとえば、印鑑、サイン、合言葉、などがこれにあたり、図 8.2 のように、お互いに、その人しか知り得ない、または持ち得ないものを提示してもらった上で、事前に交換していた情報と照合し、正当性を検証する。

  また、実世界では、個人の顔や声などを覚えることによって、無意識のうちの認証が行われる相互信用モデルもある。

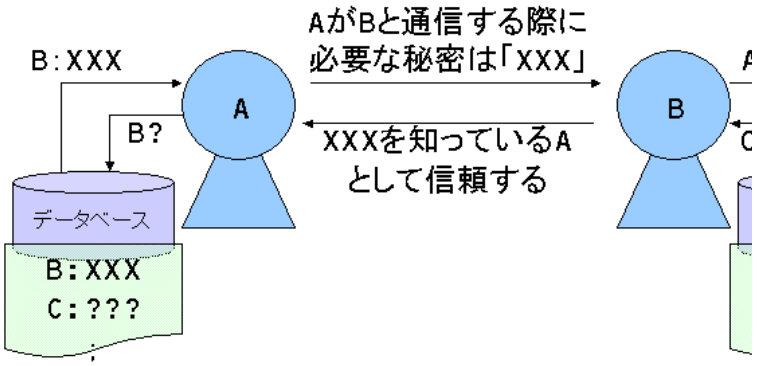

図 8.2: 相互信用モデル

相互信用モデルでは、厳密な認証が可能であるが、事前の処理が必要であるため、初対面の人間との信頼確立には適当でないといえる。

- 第三者認定モデル

  第三者認定モデルでは、信頼できる第三者から身分を証明してもらうことによって、コミュニケーションしようとする相手を検証する。実世界には、このモデルによる認証機構が数多く存在する。通貨、住民票、商品保証書、自動車運転免許証、パスポート、社員証などのように、国や企業などの組織 (信頼できる第三者) からの証明書を提示することによって価値を保証したり信頼関係を確立したりする。

  このモデルは、初対面の人との信頼を確立する必要のある一対多型のコミュニケーションに適しており、規模性にも優れている。信頼確立の際に用いられる証明書は、別途手続きを経て、検証可能である必要がある。

このように、実世界でも、コミュニケーションを行う前に相手との信用関係を築くために意識的または無意識のうちの様々な認証が行われている。認証が正しく完了されない限り、コミュニケーションの相手と信用関係を築くことができず、情報や資源の交換 (サービス) が安全に行われない。

電子化された実空間情報を扱うインターネット上にも実世界の認証と同様に、情報や資源、そ

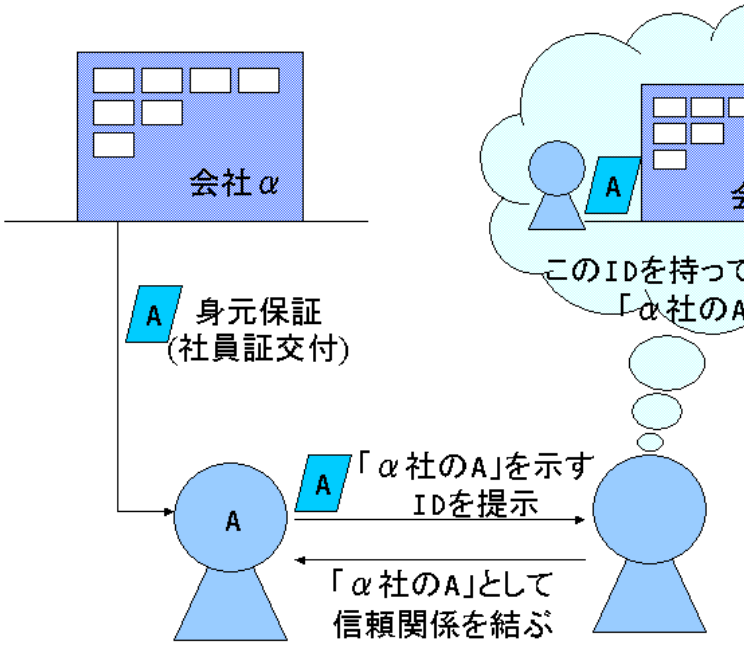

図 8.3: 第三者認定モデル

れを流通させるサービスを保護するための認証機構が必要とされている。

8.3.2. 電子空間における認証機構

電子化した実空間の情報を扱う電子空間では、単一の計算機システムと情報の流通基盤となるインターネット上とで認証の主体や手続きなどの振る舞いが異なる。ここでは、インターネットに接続されていない単一の計算機システムにおける認証機構について整理し、ネットワーク接続への対応について触れる。

8.3.3. 単一の計算機システムにおける利用者特定

単一の計算機システム、すなわちスタンドアロンで動作する計算機では、利用者の識別と認証の機能は、利用者特定として包括される。つまり、単一計算機においては、サービス利用者自身が、その計算機の前で作業していることが前提とされるため、利用者の識別ができたことは、その利用者が信用できる形で特定されたことと同意である。

単一の計算機システムでは、前節における「相互信用モデル」が多く適用されている。

ここでは、単一計算機システムにおける認証機構として、相互信用の際に用いられる「自分だけが知り得る/持ち得る情報」に注目して分類を行う。

パスワード

最も単純な認証機構であり、利用者だけが知り得る情報として、パスワードを用いる。
処理の流れは、以下のように大別される。

1. 各利用者に対して事前に特定の文字列を登録
2. 認証場に、その利用者の識別子とパスワードの組が提出される
3. 事前登録したパスワードと一致するかどうか検査
4. パスワードが一致すれば, 正当な利用者として処理

この認証の信頼性は、各利用者は自分のパスワードを記憶すること、また、他の利用者にパスワードを漏らさないこと、というルールに従うことで確保される。現在のマルチユーザシステムの大半は、パスワードによる認証を行っている。

パスワードによる認証では、パスワードの構成、パスワードの保管方法、パスワードの確認方法の三つの処理について、安全に行える設計にする必要がある。たとえば、パスワードの構成は 8 文字以下の任意文字列を使用する、パスワードの保管方法は、暗号化したパスワードと鍵をファイル (/etc/passwd) に記録する、パスワードの確認方法は、ユーザが入力したパスワードのハッシュ値と登録したもののハッシュ値が一致するかどうか検査する、などが一般的に行われている。

安全性の向上のためには、これらの他に、使い捨てパスワード (One Time Password) の利用や暗号方式の強度を上げる、などの工夫が必要である。

物 理 媒 体

IC カード近年になって研究開発と普及がすすみ、キャッシュレス決済や身分証明の場で利用されるようになっている。

IC チップが埋め込まれた IC カードは演算やデータ処理等の高度な判断機能を備えており、記憶容量に関しても磁気カードと比較して数倍から数百倍の大容量を有している。CPU の有無からメモリカードと CPU カードとに分類され、メモリカードには単にデータの記録を目的としたタイプと、メモリへのアクセスを制御するためのセキュリティ回路を備えたプロテクティッド・メモリカードとがある。欧州での使い捨てプリペイドカードはこのプロテクティッド・メモリカードに相当する。一方、CPU カードは演算機能や判断機能を有し、情報を記録するだけの受動的メディアに対する能動的メディアとなる。これは一般にスマートカードと呼ばれており、た CPU カードの内、暗号の高速処理用のコプロセッサを搭載したものをクリプトカードとも言う。

また、インタフェースの違いから、IC カードを接触型カードと非接触型カードとに分類することができる。この内、非接触型カードは内部のアンテナを通して電力供給やデータの読み書きを行う。メモリカードが主体となる非接触型タイプは通信距離によって密着型、近接型、近傍型、遠隔型の 4 つに分類される。それぞれの通信距離は、密着型が 2mm、近接型が 10cm、近傍型が 70cm、遠隔型が数 m 程度までであり、近傍型までが電磁誘導方式、遠隔型がマイクロ波方式となっている。電子乗車券やテレホンカードとして実用化が進んでいるのは近接型タイプである。接触型、非接触型の両方の機能を兼ね備えたものはコンビネーションカードまたはハイブリッドカードと呼ばれ、例えば電子マネー等の決済分野では接触型、入退出管理に関しては非接触型、という用途が期待されている。

このように、IC カードは e-Japan 重点計画の中でも取上げられ、住民基本台帳カードを始めとした電子政府・電子自治体での利用や民間分野での活用計画が始動している。身分証明に用いる場合は、利用者のみが持ち得る情報として利用者に固有な情報 (個人情報) を記録してある。

IC カードを利用者の本人確認および身分証明、つまり認証に用いる場合は、以下の必要条件を満していることが前提とされる。

- 物理媒体自体の複製が困難であること
- 各ユーザに別々の情報が付加されていること

IC カードを用いた認証の大まかな処理の流れは、利用者個別の識別子から、その利用者に割り当てられたカードに記録されているべき情報をシステム側で特定し、その結果とカードから読み出された情報とが一致するかどうかを検査するというものである。

この他に、カード内に暗号化した情報を記録パスワードシステムと組み合わせることでより安全なシステムを構築することが可能である。

IC カードフェア 2002[1]の開催などからも分かるように、今後ますます技術開発およびサービス展開が進む分野の一つであるといえる。

バイオメトリックス

人間 1 人 1 人に固有の特徴、つまり「その人物であると認識するに十分な身体的特徴を使って認証を行う仕組み」である。

利用される身体的特徴は、指紋、声紋、掌形、眼底網膜血管/虹彩パターン、手の甲の静脈パターン、顔の構造、輪郭、筆圧、署名、打鍵のスピード、打鍵の癖など、他人とは確実に異なる身体的

[1] http://www.nmda.or.jp/iccf2002/

表 8.1: 単一計算機システムにおける認証

認証に必要な情報	特徴
パスワード	最も利用されている仕組み。パスワードの構成、保管方法、確認方法を安全に行う設計が必要
物理媒体	利用者の情報を持ち歩く仕組み。紛失や盗難への対応が必要
バイオメトリックス	計測機器 (センサ) が高価だが、低価格化と商用化が進んでいる

特徴、または行動の癖を抽出して利用する。これらは一般に、静的生体特徴 (経時的変化がほとんどないと見なせるもの) があるという前提において認証に用いられている。

バイオメトリクスによる認証は、原則として、他人に盗まれることのない本人だけの証拠を使うため、他人に知られやすいパスワードや紛失の恐れがある IC カードに比べて安全性が高いといえる。認証システムそのものが高価であったり、原本データの登録に大変な手間を要することから、爆発的な普及にはつながっていなかったが、最近は、低価格化と商用化が進み、バイオメトリックスを基盤とする認証システムも認知されつつある。

しかし、多数の身体的特徴を対象にした製品が開発されているが、認証システムの閾値を十分に高く設定できるのは、指紋や手形などに限られる。証拠として使われてきた歴史が長く、正確性、利便性、コストのバランスが最も良いのは指紋認証であるが、指紋採取による偽造問題が残る。

8.3.4. ネットワーク環境への対応

インターネットとは、そもそも「ネットワークのネットワーク」であり、バラバラに存在する複数のネットワークが連結して一つのコミュニケーション空間を創っている。このコミュニケーションの主体は自律性をもったエンドシステム、つまり個人である。したがって、自律的に行動する個々の利用者が有機的に形成するコミュニケーションを考慮し、エンドユーザとしての利用者がが不便を感じることのないインタフェースと信用関係の確認のために様々な認証機構が提案されている。

最近の計算機システムは、単体で利用されることは稀であり、ネットワーク環境を前提とした認証機構が必要になる。具体的には、ある計算機で認証されたユーザについて、他の計算機でその身元をどのように安全に保証するかということを解決しなければならない。

ネットワーク環境の脅威として、盗聴、なりすまし、情報の再生 (replay) などが考えられるが、これらの脅威に対応できる強度を持った認証システムが必要となる。

8.3.5. 相互信用による認証システム

前述した実世界での認証モデルは、すでに電子空間に適応され、技術的に実現したものも存在する。相互信用モデルの代表としては、1971 年に Phil Zimmermann 氏が発表した PGP(Pretty Good Privacy) [40, 41, 42] が挙げられる。

PGP は電子メールの暗号化ソフトウェアであり、安全に電子メールのやりとりを行うためのツールとして全世界で利用されている。自分が通信相手と共有している情報やサービス利用時に必要な個人情報を、公開鍵暗号の秘密鍵を用いて暗号化する。通信相手は、通信要求をしてきた相手の公開鍵を用いて暗号化されたデータを復号化する。この PGP の利用により、相互認証 (authentication)、データの完全性 (integrity)、データの機密性 (confidentiality)、否認防止 (non-repudiation) が可能になる。

一対一の通信に必要な信用関係形成に適しているが、新しい通信対象とは改めて認証、信頼関係を形成する必要がある。つまり、厳密な認証や運用の容易さに対して、スケーラビリティに問題が残る。

8.3.6. 信頼できる第三者を使った認証システム

相互信用モデルに対し、信頼できる第三者 (Trusted Third-party authentication System) を用いた認証モデルでは、電子空間では認証局によって保証される電子証明書 (交換される認証情報を別の信頼しうる第三者によってデジタル署名したもの) が用いられる。第三者認定モデルを技術的に実現したものとしては、Kerberos, X.509 デジタル証明書を用いた PKIX(公開鍵暗号基盤) などが挙げられる。

PKIX では、実世界における実印を用いた押印のような仕組みを用いて本人確認 (認証) を行う。たとえば提出する文書に押印した場合、その押印した印鑑は印鑑証明書を役所が発行することでその所有者を証明している。同様に、デジタル署名の場合は、認証機関 (CA：Certification Authority) が証明書を発行し、保証する。「印鑑を押す」という行為の代わりに「デジタル署名」を行い、「印鑑証明書」の代わりに署名した人を保証する「電子証明書」を添付する。これら一連の行程を経ることで、手続きを電子的に行っても安全な環境が提供される。

自署名を付加して証明書を発行する CA は、最も高いセキュリティを要求されると同時に負荷の高い暗号処理を高速に行うことが要求される。そこで、図 8.4 のように、証明書作成と証明書発行、証明書の失効管理などの機能を登録局 (RA: Registration Authority) やディレクトリサービスに分散させ、運用コストの低減が図られている。

このように、信頼できる第三者認定モデルでは大規模なサービス提供が可能であり、一対多型の信用関係形成に適している。通常、アプリケーション/ミドルウェアとして構成され、現在

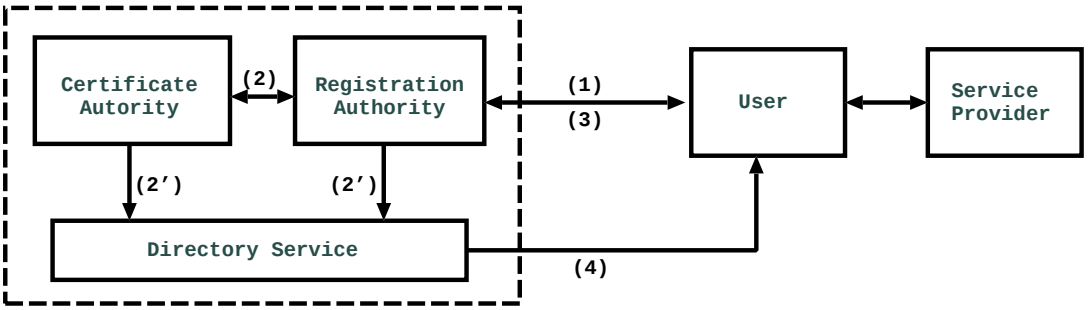

図 8.4: PKIX 認証機構の一例

では、Secure Web Access via SSL/TLS(https)、Encrypted/signed e-mail(S/MIME)、Applet Verification(Java, Active-X など) など、多くのインターネットアプリケーションで利用されている。相互信用モデルと比較して運用コストが高く、厳密な信用関係が形成されない場合があるが、スケーラビリティには優れており、初めての通信相手であっても、証明書確認のための手続きを経ることでその正当性を確認できる。

また、クライアント証明書や属性証明書を同様の手続きを経て発行することが可能であり、通信相手の認証だけでなく、自己証明や、自己のアクセス権利 (属性) を証明することも可能である。

8.4. 認証・許可・課金等に関する標準化動向

ここでは、認証や許可およびアクセス制御、課金などに関わる技術動向として、IRTF(Internet Research Task Force) における AAAARCH (Authentication Authorisation Accounting ARCHitecture) Research Group、および IETF における AAA(Authentication Authorisation Accounting) WG での標準化活動の目的と現状について述べる。

AAAARCH Research Group は、インターネットサービスに必要な認証・権限認可・アカウンティング・監査をサポートするアーキテクチャを研究・議論するグループである。短期的なテーマは IETF AAA グループが担当するが、AAAARCHResearch Group は長期的なテーマを担当し、相互接続された一般的な AAA サーバ群を組み込んだ次世代の AAA アーキテクチャと、アプリケーション特定モジュールが AAA 機能にアクセス可能とする API とを定義する。

アーキテクチャ上の焦点は、下記の AAA サービスをサポートすることである。

- 複数の組織境界間で相互稼働が可能なこと
- 広範多種のインターネットサービス間で拡張性があり, 共通であること
- AAA トランザクション概念を多数の関係者に理解させること

- アプリケーションに依存しないセッション管理機構の提供
- ローカルポリシーに合わせる強力なセキュリティ機能を持つ
- グローバルインターネットへの規模拡張可能なこと

この WG は IETF AAA WG の作業を発展させたものであり、IETF AAA WG と密接な連携を行い、同 WG にレポートしている。

WG の目標とマイルストーンとしては、以下のものが挙げられている。

- 認証とアカウンティングを含む一般的な AAA モデルを開発する
- AAA システムインターフェイスを多数の組織でチェック可能とする監査フレームワーク仕様を開発する
- 相互接続された AAA サーバのメッシュの管理をサポートするモデルを開発する
- generic model を用いてドメイン間問題を記述する
- 短期的な AAA プロトコル要件と長期的な要件とを AAA WG と協力してまとめる
- ポリシーフレームワーク WG 等と連携して分散ポリシフレームワークを定義する
- 権限認可に書くセッションに必要なアカウント処理タイプを定義させるアカウントモデルを開発する
- 提携モデルの実験ができるシミュレーションモデルの実装
- 認証情報管理モデルの開発のための RAP WG との提携
- セキュリティと AAA の構造的な思考のための GRID-Forum との提携

つまり、これらの WG では、一般的な AAA サーバ群を組み込んだ次世代の AAA アーキテクチャの策定とアプリケーション特定モジュールが AAA 機能にアクセス可能とする API とを定義することを目的としており、移動を前提とした異なるサービスドメイン間での協調認証やエンティティの属性を反映させた資源へのアクセス制御に関する議論はまだ密に行われていない。

8.5. ま と め

ここでは、実世界における認証を相互信用および第三者認定の二つのモデルに大別し、電子空間での認証の分類とインターネット上での二つのモデルの実現例を述べた。また、認証技術の動

向として IETF における AAA および IRTF における AAAARCH WG での標準化活動について概説した。

これらの識別および認証技術は、基本的に情報提供者やサービス利用者の移動を前提としていない従来のインターネットに基づく技術であり、標準化活動においても、移動体通信を念頭に置いた議論はまだ密に行われていない。

個人の計算機を持ち歩いたり、遍在する計算機を利用するユビキタス情報社会においては、提供するサービスにのための認証の対象は必ず実空間のエンティティ(利用者) となること考え、実空間情報、つまり利用者情報の流通に関して議論する必要がある。

たとえば、利用者が物理的に位置を移動し、論理的に運用ポリシの異なるサービスドメイン間を移動した場合、現在の認証方法でサービス提供の有無を考えると、移動先ドメインでの事前のアカウント登録が必要であったり、認証手続きの繰り返し、サービス切断などの不便を強いることになる。そこで、次章からは、計算機や自動車、個人などの実世界に存在するエンティティに帰属した認証と、そのエンティティの属性という情報を認証ミドルウェアで流通し、それを基にした権限委譲や資源へのアクセス制御を行うモデルを検討する。これは、サービスドメイン側の視点からは、通信相手が移動を前提としている、つまり、常に既知の利用者であるとは限らないため、既存の認証方法では検討する必要のなかった技術課題が発生する反面、広汎なサービス提供が可能になる。

Chapter 9

ユビキタス環境におけるネットワーク資源提供のためのサービスモデル

情報流通基盤として普及したインターネット上のサービスは、現在では、モバイルまたはユビキタスな環境でも利用されることが求められるようになっている。しかし、同一サービスを利用する場合にも、利用者が異なるサービスドメイン間を移動すると、インターネットへの接続性が困難、再度認証手続きを求めれる、移動先での資源が利用できない、などの問題が発生する。ここでは、利用者の移動を前提としたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案する。これにより、利用者はあらゆる場所で、その場所のポリシに沿った形でのサービスおよび資源を利用することが可能となる。

9.1. 移動体通信環境の普及とサービスの利用形態の変化

電子化された情報を流通させる情報通信基盤として、インターネットが一般に普及している。インターネットは学術機関や軍事施設での情報のやりとりだけでなく、チケット予約や電子商取引、住民票コードの利用などをはじめとする社会的、または行政的なサービスをも支えるようになった。近年では、大学や企業内だけでなく、家庭にも FTTH(Fiber to the Home) などの高速情報通信基盤が整備されはじめ、一般の生活をささえる社会基盤として認知されつつある。

また、計算機の小型化・軽量化と、IEEE802.11 規格[1]による無線 LAN 技術、Bluetooth[2]、DSRC（Dedicated Short Range Comunications:狭域無線通信）や RFID（Radio Frequency IDentification:無線周波数による非接触自動識別) タグなどの無線通信技術の発達に伴い、利用者が計算機を持ち歩き、インターネット上の情報やサービスを利用するモバイルコンピューティングの環境構築と整備が行われてきた。現在では、カフェや駅構内などからインターネットへの接続性を提供するホットスポットサービスや情報コンセントシステム [43] などの環境構築と普及が進み、利用

[1] http://www.ieee.org/wireless/
[2] http://www.bluetooth.com/

者が携帯電話や PDA、ノート PC などのモバイル端末を持ち歩くことによって、どこにいてもインターネット上のサービスが利用可能な仕組みが実現しつつある。

さらに、インターネット上で提供されるサービスの拡充と計算機資源の遍在化に伴い、ネットワークに接続された遍在する計算機を適宜利用する、ユビキタスコンピューティングの環境構築に関する研究開発および議論がされつつある。

つまり、移動体通信環境におけるインターネット上のサービス利用に対する需要が高まり、市場が拡大していると言える。

これに伴い、モバイルおよびユビキタスコンピューティング環境の構築に対する技術的要請の一部として、空間を限定することなく通信に連続性を与えるための MobileIP [44] や MANET(Mobile Ad-hoc NETworks) [45] などの技術がさかんに議論され、研究が進められてきた。しかし、これらの技術は主に IP 層における通信の連続性を確保するものであり、利用者の認証やアカウント管理、および資源へのアクセス制御に基づいたサービスの連続性に関してはほとんど議論されていない。そのため、利用者が管理形態や運用ポリシの異なるサービスドメイン間を移動すると、インターネットへの接続性が困難になったり、移動先での資源が利用できないなどの問題が発生する可能性がある。これは、従来のインターネットが移動を前提として設計されていないため、移動してきた利用者に対して、内部ポリシを反映した利用者認証および資源へのアクセス制御や権限委譲などの処理が困難であることに起因する。

したがって、ここでは、利用者の移動を前提としたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案する。このモデルは、利用者が自分のホーム環境において証明された個人証明書を携帯し、移動先にその証明書を適宜提示することで、移動先でのサービス提供を要求する。各サービスドメイン内では、定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけ、アクセス制御や権限委譲などの処理を行う機構を提案する。これにより、利用者はあらゆる場所で、その場所のポリシに沿った形でのサービスおよび資源を利用することを目指す。

9.2. 既存技術と問題点

ユビキタス環境におけるネットワーク資源の提供のために、現在までに、B-mobile や AirH” の様に、携帯電話網のローミングを利用したモバイル端末用のインターネット接続サービスや、インターネットカフェや駅構内などに設置した無線 LAN からインターネットへの接続性を提供するホットスポット、公共性の高い場所に情報端末を置く情報コンセントシステム等のサービスが提供されている。しかし、これらのサービスには、それぞれ制限が設けられているため、周辺のネッ

トワーク資源を有効に活用することが困難であるだけでなく、サービスの利便性を損なう可能性もある。

携帯電話網のローミングを利用し、特定のアクセスポイントへ接続することによるモバイル端末用インターネット接続サービスは主に「ネットワーク資源」を、ホットスポットや情報コンセントシステムは主に「場所（点）」を限定した上でサービスを提供している。つまり、携帯電話網を用いたローミング接続サービスは、場所に依存することなく利用可能であるが狭帯域高遅延であり、電波範囲などの影響でサービスが限定される場合が多い。また、ホットスポット等のサービスは、その場所では快適に提供されるが、そのドメインの運用ポリシに強く依存するため、移動した先々で同一サービスを連続して利用することができない。また、提供された計算機やネットワークの安全性に関しても問題が残ると云える。つまり、前者では「線」のサービス、後者では「点」のサービスを提供しているが、異なるサービスドメインが有機的に集合しているユビキタス環境を「面」として考える場合、利用者が異なるサービスドメイン間を移動すると、サービス提供に関して、以下のような制限や問題が独立または複合的に生じる。

- 電波強度による通信の不安定状態または切断
- 接続および認証のやりなおしが必要
- 移動先にある計算機周辺機器などの資源が利用不可能
- 事前のアカウント登録とポリシ管理が必要
- 公共端末を用いる場合の、個人情報が残る可能性

これにより、サービス利用者は地下や電波強度の弱い場所ではインターネットへの接続性が断たれる、移動先の運用ポリシに沿って管理されているプリンタが利用できない、移動するごとに認証やアクセス制御処理が繰り返される、ゲストアカウント取得などの事前処理がなければ資源を利用できない、などの不便を強いられることになる。

これは、課金やサービスの協調・連携の枠組みが異なるドメイン間で確立されていないことが原因と考えられる。つまり、従来のインターネットは利用者や計算機が移動することを前提として設計・運用されていないため、移動してきた利用者に対して、サービスドメイン内部のポリシを反映した利用者認証および資源へのアクセス制御や権限委譲などの対応が困難であることに起因する。

また、物理的な位置情報や時刻、ネットワークの状態など、利用状態や状況などの情報が動的に変化する場合にも、各サービスドメインのセキュリティポリシや運用ポリシに沿った柔軟なサー

ビスの提供を行うためには、インターネット上の分散システムの構築と運用に関して、従来の手法に囚われない新しいネットワークアーキテクチャモデルが必要となる。

つまり、場所や時間に依存することなくインターネットへの接続性やローカルな計算機周辺機器などの資源のサービスを利用する場合、利用者は複数の通信メディアを用いることが可能であり、かつ、その利用者に対して、移動先の組織での運用ポリシが的確に反映された資源へのアクセス制限および権限委譲が行われる仕組みが必要となると云える。

9.3. ネットワーク資源提供モデルの提案

ユビキタス環境におけるサービスの連続性を考える上では、「自分がたしかに自分であることを移動先で証明」した上で、「証明された人物に、移動先 (内部) の運用ポリシが反映された形で動的にネットワーク資源を提供する」というサービスモデルが必要となる。ここで、ネットワーク資源とは、インターネットへの接続性を提供するための情報や各サービスドメイン内で管理されているサービス機器などを指す。普段利用していない場所に移動した場合でもインターネットへの接続性が提供される場合は、IMAP [46, 47] や VNC(Virtual Network Computing) [21]、VPN(Virtual Private Network) [48]、PPPoE(Point-to-Point Protocol over Ethernet) [49] などの技術を用いることで、日常利用している環境へのアクセスやある程度の再現が可能となると考える。

本章では、前述の問題を解決するためのユビキタス環境におけるネットワーク資源提供モデルについて提案する。

9.3.1. ネットワーク資源提供モデル

従来のインターネット接続性の提供は、事前のアカウント登録とそれに対応するアクセス制御に依存している。しかし、ユビキタス環境では、利用者が移動するため、その移動先のサービスドメインに対する事前のアカウント登録・削除などの処理が困難である。また、動的に変化する利用者の特性や実空間の情報を反映させることができないため、運用ポリシに即した形での柔軟サービス提供や対応を行うことが困難である。

これは、利用者のホーム環境 (外部) で定義された識別子や権利などを示す属性情報を、移動先のサービスドメイン内部 (内部) ポリシに動的に対応づけることができないことに起因する.

そこで、本研究では、ユビキタス環境におけるネットワーク資源提供モデルとして、公開鍵暗号基盤で利用されている個人証明書や一時属性証明書を用いた認証とアカウント管理およびアクセス制御技術に着目した (図 9.1)。

利用者 (エンティティ) の識別および証明を行う個人証明書を用いた認証技術と、内部でのアク

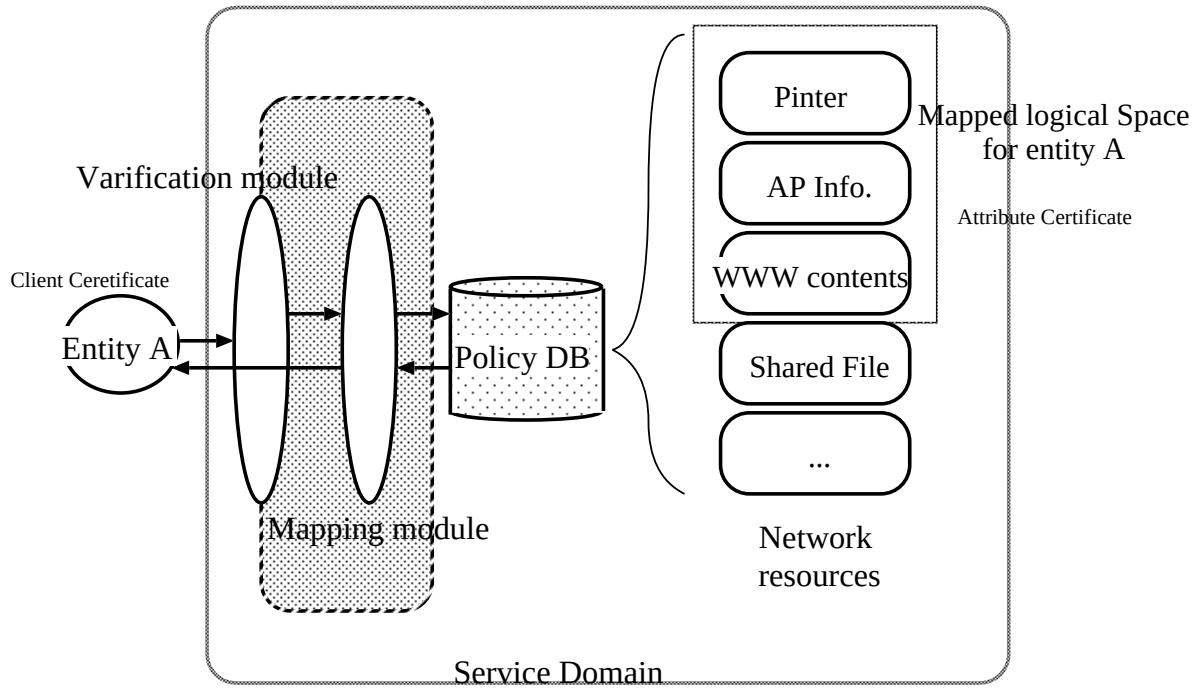

図 9.1: ネットワーク資源提供モデル

セス制御や権限委譲を表現できる属性証明書を用い、個人証明書の検証結果と内部で定義されているポリシとを対応づける機能 (Mapping module) を導入することで、エンティティと資源の利用権限との対応づけを行う。これにより、シームレスにサービスを利用するユビキタス環境において、移動先のサービス提供組織内の運用ポリシを反映させた段階的かつ動的なサービスを利用者に提供する仕組みを提案する。

9.3.2. 提案モデルの構成要素と機能

提案するネットワーク資源提供モデルに関して、抽象化した構成要素とその特性を図 9.1 に示した。ここでは、それぞれの機能について概説する。

- エンティティ
  - サービス利用者に該当
  - 移動することが前提
  - 個人を識別する情報を持ち歩く
- ネットワーク資源

  - 接続性を提供するための情報
  - プリンタや共有ファイルなどの内部 (各サービスドメイン内) で管理されているサービス機器

- 外部定義と内部ポリシとのマッピング機構
  - ネットワーク資源とエンティティのインタフェイス
  - 個人証明書検証とポリシ対応づけの二つのデーモンにより構成
  - 外部定義による利用者の識別情報を一元的に管理
  - 内部で適応するアクセス制御または権限委譲構造に対応づける
  - 内部での利用者の検証は可能

このモデルでは、ネットワーク資源として、サービスを構成するコンポーネント（情報、サーバ、メモリやディスクスペースなど）が分離されており、かつ、それぞれに利用のための権限が記されていると考える。その分離したネットワーク資源に対する権限と外部で定義 (証明) された情報を持つ利用者の権限との対応づけを、動的に定義する。

9.3.3. サービスモデルの位置づけ

ネットワークレイヤ的には、通信メディアや経路制御などのネットワーク的に下位にあるレイヤに影響することなく、運用ポリシまたはセキュリティポリシなどの上位レイヤを柔軟に反映させることのできる汎用的な認証ミドルウェアとして検討する (図 9.2)。

具体的には、IP 層の上部に、個人証明書の提示の際に自己情報制御のための選択をする機能、個人証明書の検証結果と内部サービス資源との対応づけをする機能を導入する。これにより、その上部に存在する各サービスドメイン内の運用またはセキュリティポリシが反映された形で、アプリケーション層にあるネットワーク資源を利用可能とする。

9.3.4. 個人証明書と内部ポリシとのマッピング機構

提案モデルでは、エンティティは個人識別情報を持ち歩いている。ここでは、個人識別情報として、公開鍵暗号基盤技術の個人証明書の利用を念頭に議論するが、個人を識別し、その内容を検証または証明できる情報であれば、バイオメトリックスによる生体情報の検出結果や他の情報でも対応可能とする。

公開鍵暗号基盤の個人証明書には、個人を識別する情報の他に、それを証明する機関の名前（所属）や肩書き、有効期限などの情報が記載されている。したがって、個人を識別するだけでなく、

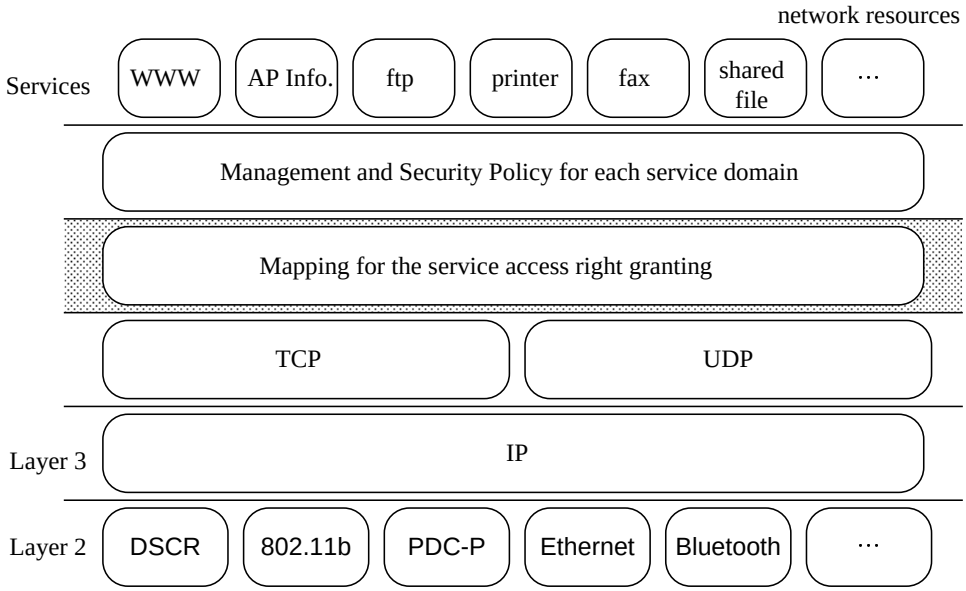

図 9.2: ネットワークレイア的な位置づけ

その発行元を検証することで、「特定の大学関係者」「大学のスタッフ」「匿名」などといった識別とその証明が可能である。

9.3.5. 一時属性証明書の配布

ネットワーク資源に対するアクセス制御や権限委譲を属性証明書として利用者に一時的に発行する。

エンティティの個人証明書の検証後、外部定義と内部ポリシとのマッピング機構によってエンティティが内部の一時的な論理空間に対応づけられ、この論理空間を記述した一時的な属性証明書などが付与される。この論理空間では、内部で定義されたポリシ適用の構造を基にした、利用可能なネットワーク資源や権限委譲の集合を扱う。これにより、外部で定義されたエンティティが、内部での特定のネットワーク資源を利用するのためのアクセス制御または権限委譲を一時的に許可された空間に対応づけられ、権利を証明された証明書を用いて活動を行う。内部で許可される空間は時限つきであるため、有効期限を短く設定することで、CRL(Certificate Revocation List: 証明書失効リスト) に関する仕組みを省略する。

9.3.6. 個人証明書の携帯

エンティティは個人識別情報を持ち歩く。移動した先で認証サービスを検索し、応答した認証サービスに向けて個人識別情報を提示する。つまり、エンティティは個人情報を格納するソフト

ウェア的またはハードウェア的なセキュリティデバイスを保持している。

個人を識別・証明する情報は、現実社会では、パスポート、免許証、クレジットカード、社員証、メンバーズカードなどの様に、利用者一人に対して複数存在する。したがって、利用者は複数の個人証明書を保持し、サービス要求を行う場合には適宜選択した上で提示する。

複数の個人識別情報の使い分けを想定する場合、「自己に関わる情報について一定のコントロールをおよぼす権利 (自己情報制御権)」 [34] に関する検討が必要になる。

これらの仕組みにより、エンティティは自分の保持する個人識別情報を選択的に提示するだけで、事前登録や申請をすることなく移動先でも適切なサービスを利用することが可能である。また、外部定義と内部ポリシとの対応づけを行うことにより、外部で定義されたエンティティに対して内部のポリシに沿った形でネットワーク資源を提供する構造が可能となる。

9.4. プロトタイプシステムの設計例

提案モデルを基に、ユビキタス環境におけるネットワーク資源提供のためのプロトタイプシステムの設計の例を示す。

ここでは、openssl-0.9.7b のライブラリを用いて個人証明書および一時属性証明書の発行および検証を行い、PostgreSQL などのリレーショナルデータベースを用いて内部ポリシを管理する。

図 9.3 は、個人証明書提示から属性証明書発行までの処理の流れ、および識別子・ネットワーク資源の割り当て処理を示している。

個人証明書と内部ポリシとのマッピング機構は、サービスドメイン内で有効な識別子 (HomeUser アカウントや Guest など) を検出するフェーズと、サービスドメイン内で利用可能な資源を決定するフェーズに分けられる。

9.4.1. リレーショナルデータベースの利用

マッピング機構では、個人証明書の検証結果と内部ポリシデータベースとの折衝を行う。内部ポリシデータベースは、あるエンティティに対して対応づけられる複数のネットワーク資源や権限を表現するために、以下の三つのテーブルにより構成される.

1. 各サービスドメイン内で有効な識別子 (account) 毎のレコードとして, 証明書記述内容を属性にもつテーブル

2. サービスドメイン内のネットワーク資源の利用権限を体系づける識別子 (group) 毎のレコードとして、ネットワーク資源を属性にもつテーブル

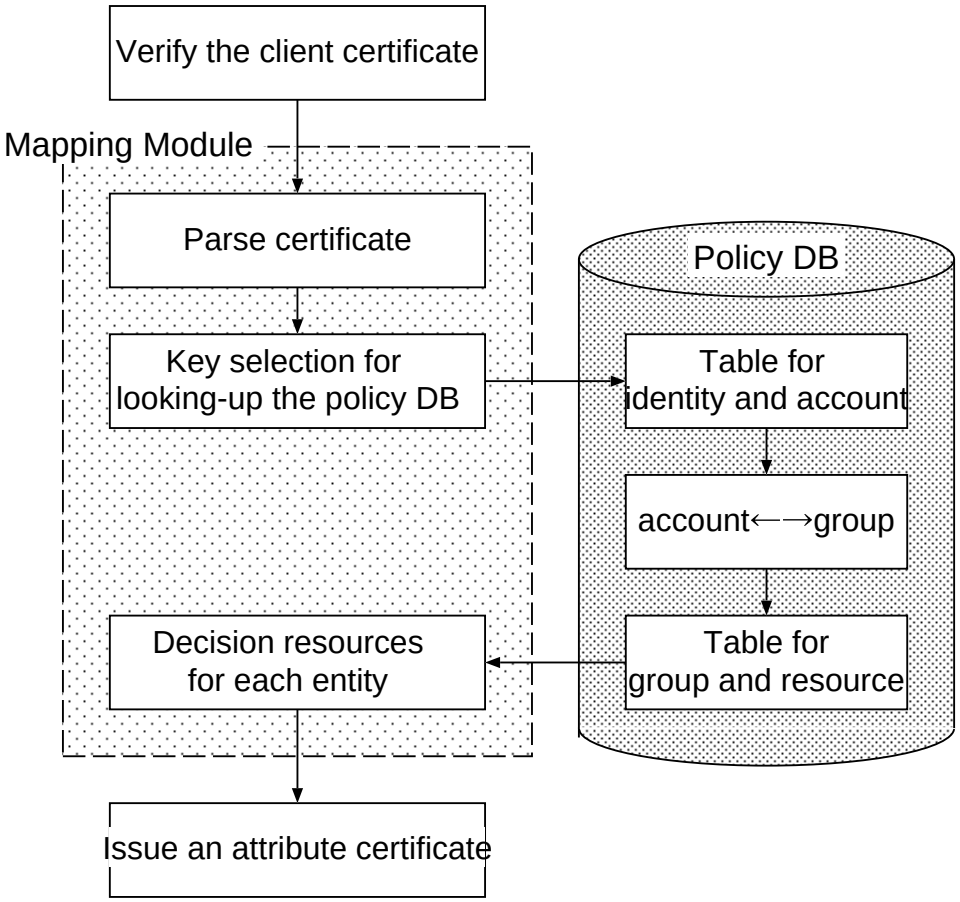

図 9.3: 識別子と資源の割り当て処理

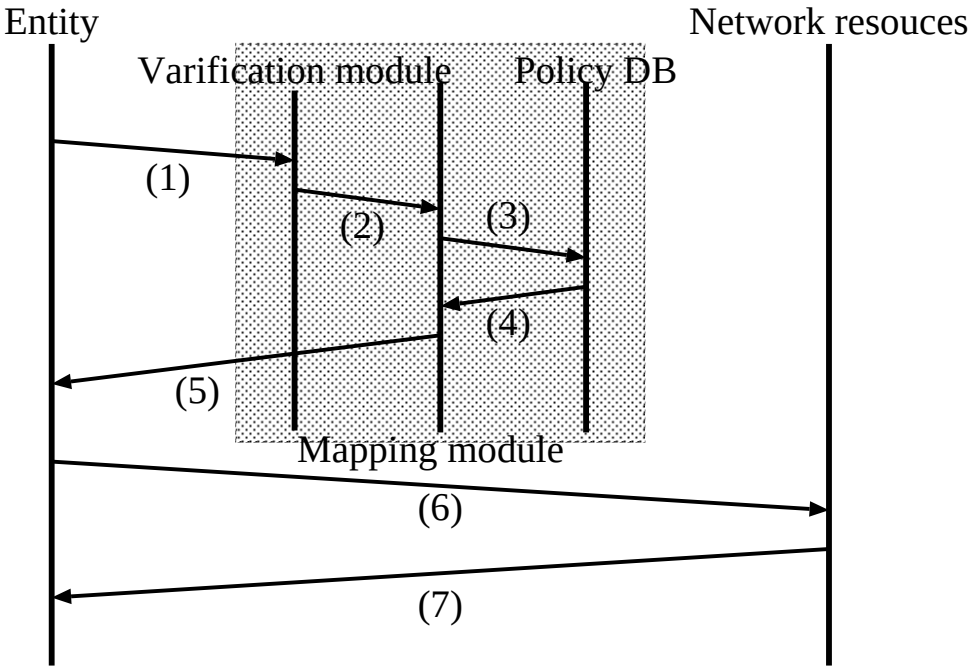

図 9.4: プロトタイプシステムの処理の流れ

3. (1)、(2) の関係を表すテーブル

図 9.4 にエンティティとネットワーク資源を含めた処理の流れを示す。

エンティティがあるサービスドメイン内に移動し、ネットワーク資源の利用を要求してから、実際にネットワーク資源を利用可能となるまでの処理は以下の 6 段階に分けられる。

1. SLP(Service Location Protocol) 等のサービス発見機構を用いて証明書を検証するサーバを発見し、自己を証明するための個人証明書を提示する。
2. 提示された証明書を検証し、その結果をマッピング機構に転送する。
3. エンティティの検証結果と内部ポリシを記述したポリシデータベースとの折衝を行う。
4. エンティティに割り当て可能な論理空間を検出する。
5. 割り当てられた論理空間を、一時属性証明書としてエンティティに発行する。
6. 一時属性証明書を用いてネットワーク資源を利用する。

証明書検証サーバとエンティティの間の通信は、SSL(Secure Socket Layer)/TSL(Transport Layer Security) などを用いて保護される必要がある。

特定のサービスドメイン内で限定されたネットワーク資源へのアクセス管理や権限委譲を行うため、プロトタイプシステムでは、そのサービスドメインで独自に作成したプライベート CA(Certificate Authority) やプライベート RA(Registration Authority) を作成し、サーバの証明書や属性証明書の発行または失効処理を行う。

9.4.2. X.509 公開鍵証明書の利用

エンティティは個人識別情報を持ち歩く。移動した先で認証サービスを検索し、応答した認証サービスに向けて個人識別情報を提示する。つまり、エンティティは個人情報を格納するソフトウェア的またはハードウェア的なセキュリティデバイスを保持しており、また、サービス発見プロトコルなどを用いて移動先での認証サービスを問い合わせる機能を持つ。その後、状況に応じて利用する個人識別情報を選択し、応答したサーバに向けて発信する。個人証明書を含む X.509 公開鍵証明書は、識別子と公開鍵がバインドされたものであり、以下の 3 つの主要コンポーネントにより構成される。

- 署名前証明書 (tbsCertificate)
- 署名アルゴリズム (signatureAlgorithm)
- 署名値 (signatureValue)

証明書の所有者や公開鍵、有効期間などの情報は、署名前証明書に記載され、署名前証明書に対する CA のデジタル署名が署名値に記述されている。署名前証明書には、発行者 (issuer)、有効期限、主体者 (subject) などの情報の他に、バージョンやシリアル番号等が記載されている。発行者や主体者は、X.500 識別名 (DN) において記述されているため、本プロトタイプシステムでは、図 9.3 の情報の切り出し処理において、この DN を属性値 (c、o、ou、cn) 毎に切り分け、マッピングモジュールでこの属性値を検索キーとして識別子テーブルと対応づける。

また、図 9.3 における属性証明書の発行には、マッピングモジュールがプライベート RA の役割を担い、発行する属性証明書に対して自分の証明書を付加することで、エンティティに対して、そのサービスドメイン内の資源利用および権限についてを証明する。

個人証明書に関する情報は、プロトタイプシステム設計時にはノート PC に X.509 個人証明書を複数保存することを想定しているが、将来的には IC カードや携帯電話に保存した X.509 個人証明書以外の個人情報を用いることや、RFC3039 [50] にある特定証明書 (Qualified Certificate) への適応も考慮する必要がある。

9.4.3. 評価項目の検討と議論

ここでは、提案モデルに基づくプロトタイプシステムを実装する場合に評価すべき項目について検討する。

スケーラビリティ

提案モデルを基にプロトタイプシステムを設計した際のスケーラビリティについてを検証する場合、比較対象は、属性証明書を用いたネットワーク資源提供モデルおよび従来のアカウント発行に基づく資源提供モデルであり、処理可能なエンティティの数と拠点数を軸とした整理と評価が必要である。しかし、本提案で用いる一時属性証明書や個人証明書に基づく認証の性能は、証明書発行頻度に依存する。つまり、証明書発行頻度はポリシに依存することになるが、性能のばらつきを吸収するための正規化が必要となるといえる。

安全性と管理・運用コスト

エンティティが提示する個人証明書は利用者の個人情報を含むため、通信路の安全性や、個人情報の蓄積および開示場所について慎重に検討する必要がある。また、安全性や柔軟性、拡張性の高いシステムを設計しても、導入・管理および運用コストの高いものは淘汰される。大規模なポリシデータベースとの連携や個人識別情報の処理時間短縮などに関して工夫するための検討が必要である。

サービスドメイン間を移動する際の処理時間

本提案モデルでは、実空間のエンティティに帰属した形でのエンティティ識別情報の提示により、単一サービスドメイン内でのサービス提供ではなく、複数の異なるサービスドメイン間でのサービスの協調を図っている。したがって、サービスドメイン間を移動する際に、エンティティ識別情報の提示と、識別情報検証から属性証明書発行までの処理が必要となる。したがって、プロトタイプシステムを設計するにあたり、これに必要な処理時間を計測し、実用に耐えうるものであるかどうかを評価する必要がある。

サービスドメイン間でのポリシの共有

本提案モデルでは、複数のサービスドメイン間を移動し、その都度各々のサービスドメイン内のポリシを反映させた形でのネットワーク資源提供を目的としている。したがって、隣接するサービスドメイン間で運用や資源割り当てに関するポリシを共有することは、移動する利用者、つまり実空間のエンティティに対する通信やサービスの連続性を保持する上で有益であるといえる。広

範囲で本モデルを適用したシステムを構築する際には、異なるサービスドメイン間でのポリシ共有方法について、更なる検討が必要となる。

新しいアプリケーションへの適応

ユビキタスコンピューティング環境では、新しい応用アプリケーションの発現やフレームワークの構築に関して研究開発が進んでいる。

たとえば、プローブ情報システム [17] や AutoID センター [51] のように、移動する計算機やセンサが情報発信を行い、インターネット上で情報が有機的に集約・加工され、有用なサービスとして提供される。つまり、情報提供者とサービス提供者 (情報加工者) が異なっている。これに特有の問題として、情報発信時は、本当にその場所から、その人によって送信された情報かどうかを保証および検証不可能であることが挙げられる。つまり、従来の情報送信技術だけでは、実空間に依存する動的な情報の正当性を検証または保証することができないため、この問題に対する対応が求められる。

本提案モデルでは、サービス利用要求を出すエンティティが、移動先で自分の個人証明書を用いて認証を行うため、これらのエンティティが送信するプローブ情報の送信元の保証は検証可能である。しかし、新しいサービスモデルの発現と共に顕在化した、サービス利用者や情報発信者の個人情報の保護、場所や時間などの動的に変化する実空間情報の正当性や完全性の保証といった問題については、さらに議論する必要がある。

以上の評価項目を考慮した上で、今後、プロトタイプシステムを実装し、提案モデルの有効性について検証していく。

9.5. ま と め

ユビキタス環境のような移動体通信環境におけるインターネット上のサービス利用に対する需要が高まり、市場が拡大している。これに伴い、モバイルおよびユビキタスコンピューティング環境の構築に対する技術的要請の一部として、主に IP 層における通信の連続性を確保する研究の開発や議論がさかんに行われてきた。しかし、利用者の認証やアカウントおよび資源へのアクセス制御に基づいたサービスの連続性に関してはほとんど議論されていない。そのため、利用者が管理携帯や運用ポリシの異なるサービスドメイン間を移動すると、インターネットへの接続性が困難になったり、移動先での資源が利用できないなどの問題が発生する可能性がある。

ここでは、利用者の移動を前提としたユビキタス環境におけるネットワーク資源提供のためのサービスモデルを提案した。このモデルでは、利用者が自分のホーム環境において証明された個

人証明書を携帯し、移動先にその証明書を適宜提示することで、移動先でのサービス提供を要求する。各サービスドメイン内では、定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけ、アクセス制御や権限委譲などの処理を行う。対応づけられた権限やネットワーク資源は、一時属性証明書に記述される。利用者はこの一時属性証明書を用いることで、あらゆる場所で、その場所のポリシに沿った形でのサービスおよび資源を利用することが可能となる。

この提案モデルに基づいたプロトタイプ設計例として、公開鍵暗号基盤の個人証明書および一時属性証明書と、リレーショナルデータベースを用いたシステムを提示し、処理の流れを示した。また、今後の課題として、このプロトタイプシステムを実装した際に評価すべき項目と、さらに議論が必要な検討課題について述べた。

Part IV

研究の総括

Chapter 10

本研究によって得られた知見と今後の課題

本研究では、インターネット上でサービス提供されている実空間における様々な情報について、実空間のエンティティに帰属する形で流通制御を行う必要性を議論し、特に移動通信環境においては、情報提供者のプライバシ保護を考慮したシステムの構築に取り組んだ。プロトタイプシステムの実装や大規模実証実験を行うプロジェクト参加を通じて、実空間情報サービスに関するいくつかの知見を得ることができた。

本章ではそれらの知見について述べ、残された要求を満すために、今後、研究が必要である技術について議論する。また、要求項目の整理と議論、また、必要となるシステムの機能要件や運用・評価実験を通して検証すべき項目などについて述べる。

10.1. 全体を通じて得られた知見

10.1.1. 情報提供者および利用者への配慮

インターネットの普及と、ユビキタスな社会の形成にともない、移動体の位置情報、道路交通や気象に関するプローブ情報、家電や端末の制御情報など、インターネット上で動的に変化する実空間の情報を扱うサービスが、今後も活発に開発されると予想される。

インターネット上で扱う情報について、通信路に対する安全性や、データの完全性・機密性に関しては、暗号技術やシステムアーキテクチャおよびネットワークプロトコルの改良などで対処が可能となる場合が多い。しかし、動的な実空間情報の流通に関しては、扱う情報とその状況によって保護の対象が変化する。たとえば、実空間のプローブシステムでは情報提供者の匿名性を保つ必要があるが、交通事故や緊急通報などでは、情報提供者を厳密に認証した上で信頼できる情報だけを扱う必要がある。また、電子選挙などでは、サービス利用者の匿名性が必要であるが、通常のインターネット上のサービス利用者に対してはなりすまし防止、否認防止などを含めた認

証機構が必要であったりする。つまり、サービス利用者だけでなく、情報提供者に対しても、実空間情報、個人情報、属性情報などに応じたプライバシ保護に関する配慮を行う必要がある。

10.1.2. 必要に応じた情報流通制御の必要性

位置情報や時刻、個人の属性や活動履歴、家電製品の制御情報など、実空間の情報は、動的に変化する。したがって、今後も変化し、増え続けるであろう実空間情報をインターネット上でサービスとして提供・利用するためには、実空間における個人のプライバシを侵害することなく、情報提供者やサービス利用者の意思と、サービス提供側の運用ポリシとが、動的に折衝する機構が必要となる。つまり、実空間の情報の流通基盤として、今後のインターネット技術の発展には QoS なども含めた状況に応じた選択的なサービス提供や、動的なポリシ折衝という機構が必要になるといえる。

実空間のエンティティ、特にコミュニケーションの主体である個人に帰属した形で、情報利用者側は自己情報制御を行い、情報提供者側は運用ポリシと提示された属性による動的かつ選択的なサービス提供をすることが望まれる。

10.1.3. 流通範囲と規模性

情報の流通範囲の設定は情報提供者および利用者の情報保護配慮を検討する上で重要な項目である。特に、地域通貨や商取引などのような情報流通では、国や地域、組織などを厳密に制限している場合が多い。

しかし、実空間の情報をインターネット上で扱うことにより物理的な空間制限および時間的制限は解消され、世界中のどこからでも、任意の時間帯に情報を検索・利用することが可能となる。したがって、インターネット上で、情報流通に基づくシームレスなサービス利用を行うために、認証機構や情報交換などに関して、流通範囲の拡大のための組織間の協調や、システムの柔軟性が求められる。一方で、サービス毎に存在する流通範囲や情報の有効性などについて、厳密に定義をする必要がある。

10.2. 地理的位置情報のプライバシ制御

10.2.1. 位置情報の分類

様々な位置情報検出装置と、その精度向上技術のの開発が進んでいる。しかし、実空間の位置情報をインターネット上で電子的な情報として扱う場合、緯度・経度・高度による表現や住所、郵便番号などのような絶対的または階層的に整理された表現と、「この部屋」「となりの人」「1A の

座席」といった相対的な表現とが存在する。アドホックネットワークなどの移動体通信、またはユビキタスな環境を作るためには、状況に応じて両方の表現が必要となるため、系の変換などを用い、正規化した形で位置情報を表現する必要がある。

10.2.2. プライバシ保護とシステム負荷への配慮

移動体通信環境においては、移動体自身が実世界をプローブする重要なセンサの役割を果たす。つまり、情報提供者とサービス提供者は必ずしも一致していない。したがって、保護すべきプライバシの対象は、サービス利用者だけでなく情報を発信する移動体、すなわち情報提供者にも及ぶ。

また、個人情報の保護、すなわち情報の機密性と完全性の保証のために有効な手段として、暗号処理が挙げられる。しかし、通常、暗号強度と処理負荷は正比例の関係があるため、余りに強固な暗号技術を利用すると、処理負荷の向上によりシステム自体の利便性が損なわれる可能性がある。したがって、システム設計時、および運用時において、保護の対象となる情報と、それに対する処理についてを慎重に検討する必要がある。

10.3. インターネット ITS プロジェクトの活動

10.3.1. 他分野からの意見集約

インターネットは、今日ではすでに重要な社会基盤の一つとして機能している。家電制御や電子商取引のようなビジネスにおける需要だけでなく、教育、医療、交通、行政など、社会生活を支える基盤なる様々な分野での情報電子化が進んでいる。現在では、これらの情報を利便性を損なわずにインターネット上で「誰でも、どこでも、いつでも」安全に利使用することが求められている。

したがって、インターネット上で構築するシステムの技術的な機能要件だけでなく、社会的なニーズ、他分野の既存技術との協調・共存を考慮し、サービスの分類や、検討が必要な項目を明確にする必要がある。

また、開発基盤、およびサービス基盤の共通化を図るうえでは、策定する仕様を公開し、関連する多くの分野からの意見集約と標準化にむけた動きが必要であると考える。

10.3.2. 実 証 実 験

共通開発基盤としてインターネットを用い、共通サービス基盤としてインターネット ITS 基盤を策定・構築した上で、その有効性の検証として、高機能実験車の制作と名古屋および首都圏 (川崎地区) における大規模実証実験を行った。

実際に構築したシステムを運用するにあたり、開発工程予測や他分野からの実験協力者からの意見反映の難しさ、実験中に発生するトラブルによって初めて認識できる問題の存在、サービス利用者からの意見など、大規模実証実験の必要性を改めて実感した。

10.4. ユビキタス環境におけるネットワーク資源提供のためのサービスモデルの提案

10.4.1. スケーラビリティ

提案モデルを基にプロトタイプシステムを設計した際のスケーラビリティについてを検証する場合、比較対象は、属性証明書を用いたネットワーク資源提供モデルおよび従来のアカウント発行に基づく資源提供モデルであり、処理可能なエンティティの数と拠点数を軸とした整理と評価が必要である。しかし、本提案で用いる一時属性証明書や個人証明書に基づく認証の性能は、証明書発行頻度に依存する。つまり、証明書発行頻度はポリシに依存することになるが、性能のばらつきを吸収するための正規化が必要となるといえる。

10.4.2. 安全性と管理・運用コスト

エンティティが提示する個人証明書は利用者の個人情報を含むため、通進路の安全性や、個人情報の蓄積および開示場所について慎重に検討する必要がある。また、安全性や柔軟性、拡張性の高いシステムを設計しても、導入・管理および運用コストの高いものは淘汰される。大規模なポリシデータベースとの連携や個人識別情報の処理時間短縮などに関して工夫するための検討が必要である。

10.4.3. サービスドメイン間を移動する際の認証処理時間

提案モデルの新規性は、あるサービスドメイン内において、外部で定義された個人証明書を検証し、内部ポリシと折衝を行い、提供可能なサービスや権限を属性証明書発行という形で記述、提供するというところにある。つまり、実空間のエンティティに帰属した形でのエンティティ識別情報の提示により、単一サービスドメイン内でのサービス提供ではなく、複数の異なるサービスドメイン間でのサービスの協調を図っている。したがって、サービスドメイン間を移動する際に、エンティティ識別情報の提示と、識別情報検証から属性証明書発行までの処理が必要となる。プロトタイプシステムを設計するにあたり、これに必要な処理時間を計測し、実用に耐えうるものであるかどうかを評価する必要がある。

10.4.4. 新しいアプリケーションへの適応

ユビキタスコンピューティング環境では、新しい応用アプリケーションの発現やフレームワークの構築に関して研究開発が進んでいる。

たとえば、プローブ情報システム [17] や AutoID センター [51] のように、移動する計算機やセンサが情報発信を行い、インターネット上で情報が有機的に集約・加工され、有用なサービスとして提供される。つまり、情報提供者とサービス提供者（情報加工者）が異なっている。これに特有の問題として、情報発信時は、本当にその場所から、その人によって送信された情報かどうかを保証および検証不可能であることが挙げられる。つまり、従来の情報送信技術だけでは、実空間に依存する動的な情報の正当性を検証または保証することができないため、この問題に対する対応が求められる。

本提案モデルでは、サービス利用要求を出すエンティティが、移動先で自分の個人証明書を用いて認証を行うため、これらのエンティティが送信するプローブ情報の送信元の保証は検証可能である。しかし、新しいサービスモデルの発現と共に顕在化した、サービス利用者や情報発信者の個人情報の保護、場所や時間などの動的に変化する実空間情報の正当性や完全性の保証といった問題については、さらに議論する必要がある。

10.4.5. 自己情報制御機構

現状で広く利用されている認証機構では、各組織の運用ポリシや利用者情報の共有が考慮されていないため、実空間のエンティティが自由に実空間上を移動しても、インターネット上では異なる運用ポリシを形成する組織間を移動することになるため、連続したサービスの利用が困難である。したがって、個人情報保護と移動体通信環境におけるサービス提供・享受の在り方という視点からは、インターネットにおけるサービス提供の判断機構における認証から自己証明へのパラダイムシフトの検討が重要である。つまり、実空間の物理的な位置、またはインターネット上の論理的な組織と運用ポリシに制限を受けない個人の自己証明と、その属性を反映し、かつ内部ポリシに沿った動的なサービス選択および情報流通制御が必要と言える。この情報流通制御に関する次の項目に関して検討を行う必要がある。

- 個人プロファイル属性の動的な変化とその正当性の検証個人プロファイルのもつ属性に関しては、住所や年齢、性別などの情報の他に、センサデバイスからの位置情報や時刻情報などの動的に変化する属性情報を含めることで、運用ポリシとのより粒度の小さい折衝を行うことができる。しかし、図 10.1 に示すように、移動体内で、センサデバイスから情報発信までのプロセス中に情報の改竄が行われる可能性が存在する。

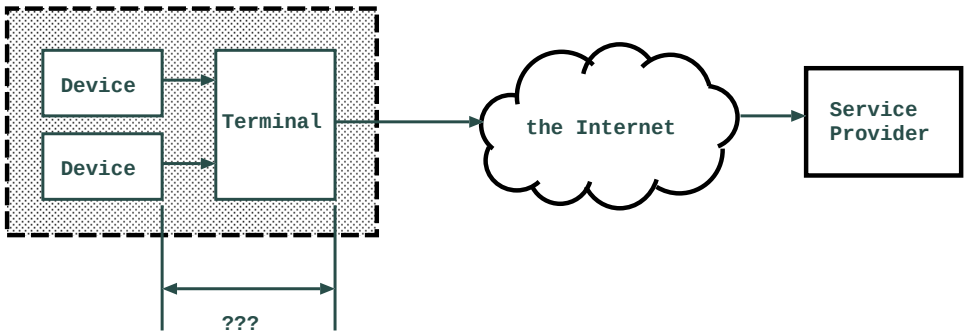

図 10.1: 動的な属性情報

この間の情報改竄不可能性が示せない限り、動的な属性を信頼関係を築いた上でのサービス選択機構に反映させることは困難であると考える。

- 個人プロファイルの移動本研究では、個人のプロファイルは、サービス提供者に事前登録をしたりサービス側から自動的に情報を収集されたりすることなく利用者側に存在し、運用ポリシ折衝時などの必要な時に提示することを提案することで、サービス利用者のプライバシを保護している。

  しかし、ユビキタスコンピューティングでの公共端末のように、遍在するホストを用いて自己証明を行う場合、そのホストの正当性の検証や、個人プロファイルの持ち運び方法について議論が必要である。

  たとえば、携帯電話に個人プロファイルを保存する、IC カードや 2 次元バーコード等を用いて個人プロファイルを移動させる、という方法が考えられるが、これは、従来の認証機能と同様に、そのデバイスの紛失や盗難によるなりすまし脅威は避けられない。また、正しく個人プロファイルを利用するホストに移植できた場合でも、そのホスト自体の安全性とサービスに対する正当性の検証可能性が確立されていなければ、自己証明後も安全なサービス享受を行うことができない。

  サービス利用後に個人プロファイルを消去、または暗号化により機密性を保ったまま移動先に一定期間保存する、といった個人プロファイルの有効期限についても深い議論が必要である。

10.4.6. 既存基盤への適用および運用と評価実験

アーキテクチャモデルの正当性は、実際の運用および実証実験を持って証明される必要がある。本研究で提案した自己証明に基づく選択的サービス提供モデルに関しても、既存の公開鍵暗号基盤によって実験運用よび評価実験をする必要がある。

本論文では、自己証明に基づく選択的サービス提供モデルを PKI フレームワークへ適用することを検討しているため、今後は、PKI に基づく認証局の運用や X.509 個人証明書配布による評価実験を行う。実験の際には、規模性とサービス選択に関する柔軟性、従来の認証機構を用いた場合との処理速度や管理・運用コストなどの評価を行う必要がある。

また、本研究で提案したネットワーク資源提供モデルをサービス連携のためのインターネットミドルウェアとして構築する場合、動的なポリシー制御 (Policy-based Management) やフィードバック制御に関しても検討を行う必要がある。

Chapter 11

結　　論

情報技術の発達にともない、さまざまな分野にも計算機が導入され、実空間で扱う情報の電子化が行われている。これらの電子化した情報を流通させる手段、つまり、情報通信基盤として、インターネットが広く利用されるようになった。

インターネットに接続した計算機を用いることで、人々は、空間的または時間的な制約を越えて多くの情報を検索・取得し、世界中の人々との情報交換や容易な情報発信が可能となる。インターネットは、現在では学術分野に限らず行政や金融、医療、交通、各種メディアなどの情報をも流通させる、社会基盤としての役割を担っている。

しかし、情報流通基盤の整備とは対象に、その情報の流通制御に関しては、対応が遅れ気味である。まず、インターネット上でのプライバシ情報の取り扱いは、実世界のプライバシ侵害の問題と比較して複雑化しており、実空間に存在する情報規制や法整備だけでは、インターネット上で発生するプライバシ侵害への対応は十分に行えないことについての議論を行った。

ここでは、実空間の情報として、主に実空間エンティティの位置と個人に関する情報の流通について取り上げた (図 11.1)。

実世界での位置情報や活動履歴を含む情報は、位置情報を発信した利用者が特定可能である場合、時刻や他の情報と組み合わせ分析することにより利用者の位置を追跡したり、個人的嗜好、消費行動などを把握することができるため、インターネット上ではプライバシ (個人情報) に関わる情報とされる。実空間の物理的な位置情報をネットワーク上で扱う際に、計算機を特定可能な ID を用いることは、インターネット上への個人情報の流出につながる。そこで、まず個人情報とプライバシに関する定義を行い、個人情報の不特定多数に対する無制限な流出を防ぐため、システム上で疑似識別子 (pseudo ID) を導入し、蓄積する個人情報は暗号化により保護した地理的位置情報管理システムの一提案とプロトタイプの設計を行った。

さらに、実空間における従来のプライバシ侵害とインターネット上でのプライバシ侵害との相違を明らかにした上で、インターネット上のプライバシ侵害の特徴が、情報制御の困難さに起因するものであり、少なくとも従来のような規制強化だけでは不十分であることを検討した。また、

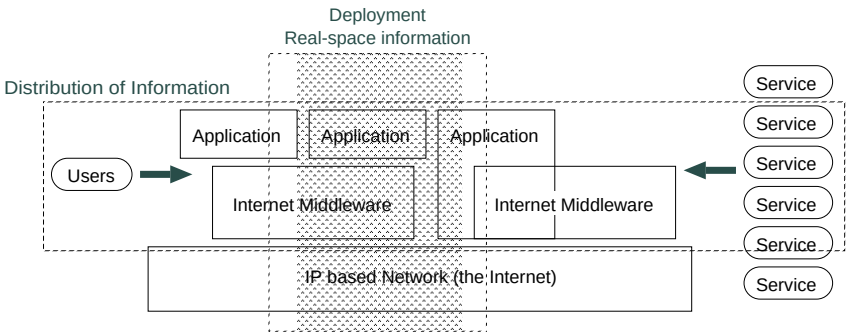

図 11.1: インターネット上での実空間情報の流通

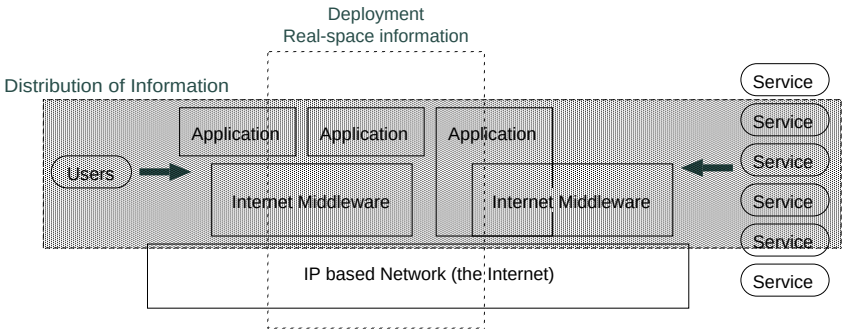

図 11.2: インターネット上のサービスの連携と検証

インターネットに接続されたセンサデバイスから実空間をプローブすることにより発現する移動体通信におけるサービスの、情報発信者に対する個人情報保護について検討を行った。

次に、世界中に数多く存在し、広範囲に移動する自動車を実空間に存在するエンティティとして実空間情報の流通制御に関わるサービスについて検討を行った (図 11.2)。

自動車がインターネットを介して外部社会と常時接続され、自動車のセンサデバイス情報をインターネット上に集約することで、ITS および GIS などの関連サービスの多様性と空間的・時間的広がりが得られる。インターネット ITS プロジェクトでは、インターネットがそのオープン性を活かした情報通信基盤となることの意味について検討し、ITS 関連サービスに対する共通インタフェースの提供と、情報通信基盤仕様の策定、実現されるサービスイメージの分類等を行った。コンセプトを具現化したプロトタイプ車としての高機能実験車の作成や、名古屋および首都圏における大規模実証実験、および、関連分野でのサービスの動向調査を通じて、インターネットを情報通信基盤として用いる様々な分野の今後のサービスの在り方と個人情報保護を前提とした情報流通の関心の高まりを確認した。

本研究では、位置情報や時刻などの実空間エンティティに付属した情報の流通やサービスの在

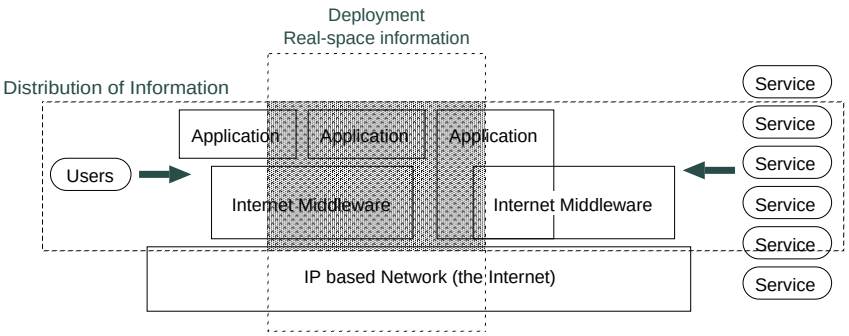

図 11.3: インターネット上での実空間情報を用いたサービスのための検討

り方について検討し、実空間情報の流通制御とそれに伴うサービス提供に関してユーザプロファイルによる情報フィルタリング技術と認証およびサービス委譲機構を検討した (図 11.3)。

その結果、プライバシ侵害の対象となる実世界のエンティティに帰属した情報の流通制御および管理が必要であることが分かった。

実空間情報をインターネットを介して流通させる場合、情報提供者の個人情報を保護する一方、情報およびサービス利用者に対する個人情報保護も考慮する必要がある。特に、移動体通信環境の普及により、インターネット上のサービスの利用形態や情報の発信方法が変化していることを考慮し、移動に伴う通信の連続性だけでなく実空間におけるエンティティ、特に利用者個人の認証および委譲情報の連続性についてを検討することで、情報通信基盤としての社会性を持つインターネット上の実空間情報の流通制御として、実空間エンティティに帰属した形でのネットワーク資源提供サービスモデルを提案した。

具体的には、サービスドメイン内のネットワーク資源提供に関して、実空間のエンティティの自己情報の提示とその正当性の検証機能、また、検証結果に対するサービス委譲、つまりネットワーク資源へのアクセス制御や権限以上の機能を分離した、ユビキタス環境におけるネットワーク資源提供モデルを提案した。利用可能なサービスは、各々のサービスドメイン内部であらかじめ決められた内部運用ポリシと個人証明書やプロファイルの属性とと動的に折衝することにより決定される。実空間エンティティ、つまり利用者は、現実社会で複数の組織 (地方自治体や会社、プロジェクトや同好会などのグループなど) に所属しているため、個人証明書を複数所有することを前提としている。自己情報を制御するために、証明書提示の状況やタイミングに基づいて、利用者本人がそれらの中から選択的に利用者情報を提示する。つまり、情報提供者やサービス利用者の意思を反映した自己情報の提示に基づいて、サービス提供側が提示された情報と運用ポリシとを動的折衝させ、提供可能なネットワーク資源を提示することが可能となった。

これにより、異なる運用ポリシ間を移動した場合でも提供者のポリシに沿った形でサービスの

連続性を保つことが可能となり、実空間の情報流通とサービス提供・享受に対する動的な情報流通の制御が実現される。本モデルの実現可能性は、個人プロファイルとして X.509 個人証明書を用い、PKI フレームワークへの適用を通じて検討した。また、サービス委譲に関して、既存認証機構と提案モデルを比較し、その得失を述べた。最後に、サービスドメイン間を移動する際の識別・認証に必要な処理時間評価の必要性、個人プロファイルの使い分けと完全性に関する保証、動的に変化する属性値等に関する議論を行い、この自己証明機能をサービス連携のためのインターネットミドルウェアとして構築する場合の動的なポリシー制御 (Policy-based Management) やフィードバック制御に関する検討の必要性など、本研究により得られた知見を基にした、今後の研究課題に関する方向性を示した。

謝　　辞

本研究は、インターネットにおいて実空間エンティティに帰属する情報を取り扱う際の流通制御に関する研究であり、多くの方から、多角的な視点でご指摘、ご指導を賜りました。特に、今後の環境変化への対応のため、移動体情報通信と情報の流通、サービスの在り方に関する技術的または社会的な意見交換の場を頂きましたことを、心より感謝いたします。

本研究の機会を与えて頂き、研究の方針や内容について、多大なるご指導を賜りました、奈良先端科学技術大学院大学 情報科学センター 砂原秀樹 教授に深甚の謝意を表します。また、様々な研究会やプロジェクト参加への機会を持たせて頂きましたことは、研究活動を行う上で、非常に有益でした。重ねてお礼申し上げます。

本研究に関する議論だけでなく、日々の研究活動に対する有益なご教示を賜りました、同大学 情報科学研究科 インターネット工学講座 山口 英 教授に心より厚くお礼申し上げます。

本論文の作成につきまして、ご厚情に満ちたご指導を賜りました、同大学 情報科学センター 藤川和利 助教授に感謝いたします。

本研究をまとめるにあたり、多大なるご指導と快適な執筆環境の提供を賜りました、同大学 電子図書館附属研究開発室 森島直人 助手と、慶応義塾大学 政策・メディア研究科 羽田久一 特別研究専任講師に心から感謝いたします。

インターネット ITS プロジェクトに参画するにあたり、様々な活動の場と貴重なご助言とを賜りました、慶應義塾大学 環境情報学部 村井 純 教授に、深くお礼申し上げます。

また、同大学 政策・メディア研究科 植原啓介 特別研究専任講師と同大学 政策・メディア研究科 佐藤雅明 特別研究専任助手をはじめ、同大学 情報環境学部 村井研究室の皆様、村井研究室秘書様方、三菱総合研究所 目黒浩一郎 研究員には、本学外で行った研究活動に関して甚大なる支援と様々なご助言を賜りました。心よりお礼申し上げます。

日々の研究活動において、活発な意見交換の場と多大なるご指導および有益な情報を賜りました、WIDE プロジェクト InternetCAR、および rover ワーキンググループの皆様、およびインターネット ITS 協議会の皆様に感謝いたします。

奈良先端科学技術大学院大学 情報科学センター 中村 豊 助手、同センター 事務補佐員 能勢佳苗 女史をはじめ、同センター 教職員の皆様には、潤沢な計算機環境と多くの交流の場を賜りました。感謝いたします。

また、垣内正年氏、中山貴夫氏、蟻川浩氏をはじめとする同センター砂原研究室の学生の皆様と、奈良先端科学技術大学院大学 附属図書館研究開発室 河合 栄治 助手、伊藤 実夏 女史をはじめとする OB・OG 諸氏、Laboratoire de telecommunications Universite catholique de Louvain Techniqual committee of Loveus Project 楳田敏之博士には、本学入学当初よりお世話になり、研究だけでなく、日々の生活に関しても有益な情報と様々なご助言、ご支援を頂きました。心よりお礼申し上げます。

最後に、主に生活面および精神面において、9 年間余りの長い長い学生生活を見守り、継続的にご支援およびご協力を頂きました、両親、祖母、姉妹に心よりお礼申し上げます。

参 考 文 献

[1] e-Japan2002 プログラム ～平成 14 年度 IT 重点施策に関する基本方針～. http://www.kantei.go.jp/jp/it/network/dai5/5siryou2.html/.

[2] 佐藤 修一. “数学セミナー”, 10 1999.

[3] WIDE Project InternetCAR WG Home page. http://www.sfc.wide.ad.jp/internetCAR/.

[4] 代表: 村井 純. “インターネットカープロジェクト 1998 年度 研究報告書”. Technical report, インターネットコンソーシアム, 3 1999.

[5] 羽田 久一. **インターネットを用いた衛星測位システムの高精度化に関する研究**. PhD thesis, 奈良先端科学技術大学院大学, 2 2001.

[6] Y.KONISHI and R.SHIBASAKI. Development of a simulation system to estimate available area of gps and pseudolite. *ACRS2001*, 8 2001.

[7] 小西勇介 and 柴崎亮介. GPS とシュードライトの利用可能範囲シミュレーションに関する研究. *GPS* **シンポジウムビギナーズセッション**, 11 2001.

[8] A.Chakraborty N.B.Priyantha and H.Balakrishnan. The cricket location-support system. *the Sixthe Annual ACM International Conference on Mobile Computing and Networking (MOBICOM2000)*, 8 2000.

[9] H. Balakrishnan N. Priyantha, A. Miu and S. Teller. The cricket compass for context-aware applications. *the Seventh Annual ACM International Conference on Mobile Computing and Networking (MOBICOM2001)*, pages 1–14, 6 2001.

[10] MIT Artificial Intelligence Laboratory, Project Oxygen Home Page. http://oxygen.lcs.mit.edu/.

[11] PHS 位置情報サービス「いまどこサービス」Home Page. http://www.docomokyusyu.co.jp/docomo/phs/imadoko_serv/index.html.

[12] V.Falcao R.Want, A.Hopper and J.Gibbonsl. “The Active Badge Location System”. In *ACM Transactions on Information Systems*, volume 10, pages 91–102. 1 1992.

[13] A.Harter and A.Hopper. “A Distributed Location System for the Active Office”. In *IEEE Network*, pages 62–70. 1994.

[14] Active Badge demo page. http://www.uk.research.att.com/abservice.html.

[15] 椎尾一郎. Rfid を利用したユーザ位置検出システム. In **情報処理学会 ヒューマンインタフェース研究会**, pages 45–50, 2000. 00-HI-88.

[16] 青柳武彦. 個人情報保護とプライバシー保護. *GLOCOM Review*, 12 2001.

[17] 和田 光示. プローブ情報システム（ipcar）プロジェクト. **情報処理学会 学会誌**, (4), 4 2002. http://www.ipcar.org/.

[18] ココセコム [位置情報提供・急行サービス]. http://www.855756.com/.

[19] F.Teraoka Y.Watanabe, A.Shinozaki and Jun Murai. “The Design and Implementation of the Geographical Location Information System”. *INET96*, 1996.

[20] 竹内 奏吾. “インターネットを利用したモバイルユーサの地理的位置検出システムの構築”. Master’s thesis, 電気通信大学 大学院情報システム学研究科, 1998.

[21] K.R.Wood T.Richadson, Q.Stafford-Fraser and A.Hopper. “Virtual Network Computing”. *IEEE INTERNET COMPUTING*, 2(1), January/February 1998.

[22] 今井 秀樹 and 杉浦 幹太. “**情報セキュリティ概論**”. 昭晃堂, 1999.

[23] H. Krawczyk, M. Bellare, and R. Canetti. *HMAC: Keyed-Hashing for Message Authentication*, February 1997. RFC 2104.

[24] FIPS PUB 180-1. “SECURE HASH STANDARD”. Technical report, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, 1993.

[25] P. Metzger and W. Simpson. *IP Authentication using Keyed SHA*, September 1995. RFC 1852.

[26] OpenSSL Project Home Page. http://www.openssl.org/.

[27] 渡辺 恭人、竹内奏吾、寺岡 文男、村井純. プライバシを考慮した地理位置情報システム. In **情報処理学会コンピュータセキュリティ研究会**, 2000. CSEC-11-4.

[28] 渡辺 恭人、竹内奏吾、寺岡 文男、村井純. 地理位置情報システムの実装と評価. In **情報処理学会マルチメディア通信と分散処理研究会**, 2002. DPS-108-3.

[29] NETWORLD + INTERROP2002. http://www.interop.jp/.

[30] Wireless Japan 2002, InternetITS & TELEMATICS. http://www.ric.co.jp/expo/wj2002/.

[31] K. R. Grant T. W. Malone and F. A. Turback. The Information Lens: An Intelligent System for Information Sharing in Organizations. *ACM CHI'86*, 1986.

[32] M.Suchak P.Bergstrom P. Resnick, N. Iacovou and J.Riedl. GroupLens: An Open Architecture for Collaborative Filtering of Netnews. *ACM 1994 Conference on Computer Supported Cooperative Work*, 1994.

[33] 紀田 馨. ユーザプロファイルを用いた情報フィルタリング技術について. **情報処理学会 学会誌**, (12), 12 2002.

[34] 浜田 良樹. "プライバシーの権利とインターネット". *Japan Cyber Security Management*, 3, 5, 6, 2000.

[35] 梅澤 健太郎、齋藤 孝道、奥乃 博. "プライバシーを重視したアクセス制御機構の提案". **情報処理学会論文誌**, 42(8):2067–2076, 8 2001.

[36] 高倉 健、山本 太郎、難波 功次、西田 玄. 提供者の意思に基づく情報流通のための開示制御技術. Technical Report NTT 技術ジャーナル 2002. vol.14, No.10, 2002.

[37] 寺西 裕一、長谷川 知洋、梅本 佳宏、佐藤 哲司. 利用制約に基づくマルチメディアコンテンツ流通システムの設計. In **情報処理学会マルチメディア通信と分散処理研究会**, pages 31–36, 1999. DPS-95-6.

[38] 山本 太郎、寺西 裕一、梅本 佳宏. 医療情報システムにおける情報開示制御方式. In **情報処理学会マルチメディア通信と分散処理研究会**, pages 19–24, 2000. DPS-100-4.

[39] 田口、須藤、坪井、山本、寺西. 医療情報の連携を実現した医療コンテンツ流通システム. In *NTT R&D*, volume 51, pages 11–20, 2002.

[40] P.Zimmermann. File formats used by PGP 2.6. available on the www via ftp://ftp.pegasus.esprit.ec.org/pub/arne/pgformat.ps.gz., May 1993.

[41] P.Zimmermann. PGP user's guide, Volume I: essential topics. Available on the WWW via ftp://ftp.pegasus.esprit.ec.org/pub/arne/pgpdoc1.ps.gz., Oct. 1994.

[42] P.Zimmermann. PGP user's guide, Volume II: special topics. Available on the WWW via ftp://ftp.pegasus.esprit.ec.org/pub/arne/pgpdoc2.ps.gz., Oct. 1994.

[43] 石橋勇人, 坂本晃, 山井成良, 安倍広多, 大西克実, and 松浦敏雄. "利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式". **情報処理学会論文誌**, Vol.42(No.1):pp.79–88, 1 2001.

[44] P. Calhoun and C. Perkins. *Mobile IP Network Access Identifier Extension for IPv4*, March 2000. RFC 2794.

[45] S. Corson and J. Macker. *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, January 1999. RFC 2501.

[46] J. Myers. *IMAP4 Authentication Mechanisms*, December 1994. RFC 1731.

[47] C. Newman. *Using TLS with IMAP, POP3 and ACAP*, June 1999. RFC 2595.

[48] P.Wolfe C.Scott and M.Erwin. *Virtual Private Networks 2nd Edition.* OŔEILLY, 2002.

[49] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler. *A Method for Transmitting PPP Over Ethernet (PPPoE)*, February 1999. RFC 2516.

[50] S. Santesson, W. Polk, P. Barzin, and M. Nystrom. *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, January 2001. RFC 3039.

[51] AutoID Center Home Page. http://www.autoidcenter.org.

Part V

付録

付　　録

研究業績一覧

学術論文

1. 和泉 順子, 森島 直人, 砂原 秀樹, “ユビキタス環境におけるネットワーク資源提供のためのサービスモデルの提案”, 電気情報通信学会和文論文誌 D-I, April 2004(掲載予定).

国際会議 (査読あり)

1. Michiko Izumi, Sohgo Takeuchi, Yasuhito Watanabe, Keisuke Uehara, Hideki Sunahara, Jun Murai: “A Proposal on a Privacy Control Method for Geographical Location Information System”. Proceedings of *INET2000 The Internet Global Summit, Yokohama, Japan*, July 18-21 2000

解説論文

1. 和泉 順子: 湧川 隆次, 川喜田 祐介, 秋山 由和, “特集 インターネット自動車, 4. インターネット ITS プロジェクトの概要”, 情報処理, vol.43, No.4, pp.369-375, April 2002.

2. 和泉 順子: “特集 インターネット ITS　2. インターネット ITS プロジェクト”, 情報通信 東海, pp 2-12, 2002 年 62 号, March 2002.

国内研究会

1. 和泉 順子, 砂原 秀樹: “地理的位置情報管理システムにおけるプライバシ制御の提案”. インターネットカンファレンス’99 論文集 pp.140, December 1999

2. 和泉 順子, 竹内 奏吾, 渡辺 恭人, 植原 啓介, 砂原 秀樹, 寺岡 文男, 村井 純: “地理的位置情報システムにおけるプライバシ管理方法”. 情報処理学会 マルチメディア, 分散, 協調とモバイル (DICOMO2000) シンポジウム論文集 pp.667 - pp.672, June 2000

3. 砂原 秀樹, 和泉 順子, 磯貝 友希, 横田 真弥, 西原 サヤ子, 江本昌子, 刈谷 亜希, 菅原 麻紀子, 畑 明恵: “地理的位置情報に基づく情報収集・検索システム”. 情報処理学会 マルチメディア, 分散, 協調とモバイル (DICOMO2000) シンポジウム論文集 pp.673 - pp.67, June 2000, (情報処理学会 MBL 研究会 2000 年度優秀論文)

4. 新井 イスマイル, 和泉 順子, 中村 豊, 藤川 和利, 砂原 秀樹: “携帯情報端末における XML 代理サーバによる属性情報管理機構の提案”. 情報処理学会 マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO2003) 論文集, pp.769 - pp.772, June 2003

5. 和泉 順子, 森島 直人, 砂原 秀樹: “ユビキタス環境におけるネットワーク資源提供モデルの提案”. 電気情報通信学会 情報セキュリティ研究会 (ISEC), pp.51 - 58, July 2003

6. 田坂 和之, 川喜田 祐介, 和泉 順子, 羽田 久一, 砂原 秀樹: “インターネット上で実空間情報を収集・管理するフレームワークの提案”. 情報処理学会 ユビキタス研究会 (UBI), November 2003(発表予定)

研究報告書

1. 渡辺 恭人, 竹内 奏吾, 和泉 順子, 小浦 大将: “第 6 部 地理的位置情報システム”. インターネット自動車コンソーシアム インターネットカープロジェクト 1998 年度 研究報告書, March 2000

2. 和泉 順子, 砂原 秀樹: “第 9 章 地理的位置情報システムのセキュリティ”. インターネット自動車コンソーシアム インターネットカープロジェクト 1999 年度 研究報告書, March 2000

3. 砂原 秀樹, 和泉 順子: “第 10 章 インターネット自動車におけるアプリケーション”. インターネット自動車コンソーシアム インターネットカープロジェクト 1999 年度 研究報告書, March 2000

4. 和泉 順子, 渡辺 恭人: “1. インターネット ITS のコンセプト”. 2001 年度 InternetITS プロジェクト研究報告書, pp. 5-9, June 2002