NAIST-IS-DD0961016

博士論文

センサネットワークを利用したサービスにおける情報セキュリティとフィジカルセキュリティに関する研究

野田　潤

2011年2月1日

奈良先端科学技術大学院大学
情報科学研究科 情報処理学専攻

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。

野田　潤

審査委員：

関 浩之 教授	（主指導教員）
伊藤 実 教授	（副指導教員）
安本 慶一 准教授	（委員）
楫 勇一 准教授	（副指導教員）

センサネットワークを利用したサービスにおける情報セキュリティとフィジカルセキュリティに関する研究*

野田　潤

内容梗概

センサネットワークによって実空間から収集する情報を活用し，従来には存在しなかった新しいサービスの検討が進められている．この際，個人情報などのプライバシ保護が大きな問題となるため，新サービスの実現にあたっては，センサネットワークに適応可能な情報セキュリティ技術の導入を併せて検討する必要がある．一方で，センサが実空間上に配備されることに起因して，センサ自体への攻撃や盗難等への配慮もこれまで以上に必要となる．これは，実空間上での物理的な物や場所へのアクセス制御に関しても十分考慮する必要があることを意味する．本論文では，センサネットワークの安全性のために，情報セキュリティに加え，センサネットワークにおける機能そのものを有効利用するフィジカルセキュリティについても議論を行う．

第 2 章ではセンサネットワークの応用の多くにおいて必要となるグループ通信の安全性強化に貢献するグループ鍵管理方式について論じる．提案方式は，ノードの属性に紐つける管理情報を用いて，個々のグループ鍵の管理の仕組みを互いに連携させる．実用的な評価も交えて，一台のノードが複数の大規模グループに所属する場合に，従来に比べ，ノードのメモリ負荷の 64%〜88%を，通信負荷の 46%〜97%を削減できることを示す．

第 3 章では，初見の端末同士でアドホックな通信路を安全に開設するために有効な，動的な鍵生成法について論じる．外部情報のセンシング時においては，セ

*奈良先端科学技術大学院大学 情報科学研究科 情報処理学専攻 博士論文, NAIST-IS-DD0961016, 2011 年 2 月 1 日.

ンサ単体で処理が完結することもあるが，センサ間やユーザの備える機器を含む機器間での通信が求められることも多い．この時，必要になる全ての通信路を予見し，暗号の鍵を用意することは困難である．提案方式は，センサが取得するユーザ状況，特にユーザの動作に関する情報の類似度に応じて，センサ情報から直接強度の異なる鍵を生成し，似た状況の端末間で自動的に鍵を共有させる手法となっている．加速度センサを用いた歩行，自動車による移動動作からの鍵生成性能評価の結果，高々2 分程度で，4 桁の PIN コード相当の強度を持つ共通鍵を共有できることを示す．

最後に，第 4 章では，センサから取得する情報を有効利用するフィジカルセキュリティ，具体的に物理的なアクセス制御について論じる．提案方式では，信用管理の新たなアーキテクチャとして，信用の確立に利用する情報に，ユーザが提示したディジタル証明書に加え，センサで取得可能なユーザのプレゼンス (存在位置) を導入する．プレゼンスの導入に際しては，プレゼンスに信頼度というパラメータを与え，確率モデル (マクロ状態を持つ隠れマルコフモデル) に基づく信頼度評価によってプレゼンスの不確実性を考慮する．被験者と RFID センサを用いた評価実験を通じて，確率モデルを用いた提案法により，得られるプレゼンスの *recall* を約 1.8 倍 (0.94 以上) に向上できることを示す．その結果，信用確立における利便性や安全性を向上できることを示す．

キーワード

センサネットワーク，情報セキュリティ，フィジカルセキュリティ，鍵管理，信用管理

Information and Physical Security for Sensor Network Services*

Jun Noda

Abstract

Sensor network services are required to solve privacy protection issues when a lot of personal information including raw data of user's motion and environments is obtained by a sensor and sent to other nodes. Therefore, new technologies for information security is needed which can be adapted to sensor networks. Physical security is another issue for protecting sensors deployed in real space against physical attacks or thefts. In this thesis, two techniques are proposed for information security from the perspective of key management. Also, a trust management which takes advantage of sensor data is discussed for physical security.

In chapter 2, a group key management scheme is proposed. In the proposed scheme, group keys of different groups help each other's key management so that keys can be updated without exposing important internal information at once. It is shown by a realistic scenario that our proposed scheme can eliminate costs for managing multiple group keys compared to other known schemes.

In chapter 3, a dynamic key generation scheme is proposed for generating a common key between terminals including sensors or users' devices based on the similarity of the users' motions measured by the acceleration sensors. Performance evaluation shows that common key equivalent to the PIN code can be generated even from a pair of human motions with moderate similarity.

*Doctoral Dissertation, Department of Information Processing, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DD0961016, February 1, 2011.

In chapter 4, a new architecture for trust management is proposed that deals with role-based access control(RBAC) policy, digital signatures, and user presence obtained by sensors in a uniform framework. The proposed architecture includes inferences about user presence from incomplete sensor signals based on the hidden Markov model. Experimental results show that the proposed architecture is effective in providing both useful and secure services.

Keywords:

sensor network, information security, physical security, key management, trust management

研究業績

論文

(1) 野田潤, 楫勇一, 中尾敏康, “複数の大規模グループに同時参加するセンサノード向けグループ鍵管理方式,” 情報処理学会論文誌「マルチメディア、分散、協調とモバイルシステム」特集, Vol.52, No.3, 2011. (採録決定)

国際会議 (査読有)

(2) Jun Noda, Mie Takahashi, Itaru Hosomi, Hisashi Mouri, Yoshiaki Takata and Hiroyuki Seki, “Integrating Presence Inference into Trust Management for Ubiquitous Systems,” Proceedings of 11th ACM Symposium on Access Control Models and Technologies (ACM SACMAT2006), pp.59-68, CA, June 2006.

特許出願

(3) “信用確立方法と信用に基づいたサービス制御システム,” 野田潤, 田口大悟, 関浩之, 高田喜朗, 仁野裕一, 特願 2004-182039 (出願日：2004.06.21).

(4) “情報処理システム、情報処理装置、情報処理方法、および情報処理プログラム,” 野田潤, 高田喜朗, 関浩之, 細見格, 高橋三恵, 特願 2005-256644 (出願日 2005.09.05).

(5) “位置情報推定方法、位置情報推定装置、及び位置情報推定プログラム,” 野田潤, 高田喜朗, 関浩之, 高橋三恵, 特願 2006-240234 (出願日 2006.09.05).

(6) “暗号鍵管理方法、そのシステム及びそのプログラム,” 野田潤，楫勇一，特願 2006-307906 (出願日 2006.11.14).

(7) “暗号鍵生成システム、暗号鍵生成方法および暗号鍵生成用プログラム,” 仁野裕一，野田潤，関浩之，中村嘉隆，南貴博, 特願 2009-31154 (出願日 2009.02.13).

(8) “鍵の生成方法、装置及びプログラム,” 野田潤，関浩之，中村嘉隆, 特願 2010-293094 (出願日 2010.12.28).

国内発表 (査読有)

(9) 野田潤，椙勇一，毛利寿志，仁野裕一，中尾敏康，“複数の属性分割を利用したセンサネットワーク向け鍵管理方式の実装と評価,” マルチメディア，分散，協調とモバイルシンポジウム (DICOMO2007), pp.524-529, July 2007. (優秀論文賞受賞)

国内発表 (査読無)

(10) Yoshiaki Takata, Jun Noda, Mie Takahashi, Itaru Hosomi and Hiroyuki Seki, “User Presence Estimation Based on a Stochastic Model in Presence-aware Trust Management,” 情報処理学会研究報告, ITE Technical Report, Vol. 29, No. 63, CE2005-80, Nov. 2005.

(11) 野田潤，椙勇一，中尾敏康，“センサネットワーク向け軽量セキュリティフレームワークの実装と評価,” 2008 年　暗号と情報セキュリティシンポジウム, 4E2-5, January 2008.

(12) 野田潤，椙勇一，中尾敏康，“大規模センサーネットワークに適したサーバデータ認証方式,” 電子情報通信学会技術研究報告, USN2008-11, July 2008.

(13) 南貴博，仁野裕一, 野田潤, 中村嘉隆, 関浩之，“ユーザの動作類似度に基づく共通鍵生成法,” 情報処理学会研究報告, 2008-CSEC-44(20), March 2009.

謝辞

本研究を進めるにあたり，主指導教員である関 浩之教授には，終始懇切なご指導とご鞭撻を賜りました．ここに心から感謝の意を表します．

副指導教員である楫 勇一准教授には，大学院入学前より様々なご指導，ご意見を賜りました．ここに謹んで感謝いたします．

ご多忙のなか，審査委員をお引き受け頂きました伊藤 実教授，安本 慶一准教授に感謝いたします．

本研究において，数多くの議論をさせて頂きました高知工科大学 高田 喜朗准教授，大阪大学 中村 嘉隆特任助教，日立ソリューションズ 南 貴博様に心より御礼申し上げます．

在学中は，研究生活全般にわたり，情報基礎学講座の皆様には良い環境をご用意頂きました．大変感謝しております．

私は現在，NEC サービスプラットフォーム研究所に務めておりますが，上司の中尾 敏康主任研究員，平池 龍一シニアエキスパート，吉田 万貴子研究部長には，職務と研究に対し暖かいご指示を頂きました．ここに深く感謝いたします．また，NEC サービスプラットフォーム研究所 ユビキタス基盤 TG の皆様には，職務と研究に関してさまざまなサポートをいただき，感謝いたします．

最後に，この 2 年間，共に苦労を分かち合った自分の家族，特に出産直後から育児で多忙ななか私を支えてくれた妻に心より感謝します．

目 次

図 目 次

表 目 次

第1章　序論

センサに通信機能を備えさせることにより実現されるセンサネットワークは，人や物に関する精密な状況や状態のリアルタイムな収集，流通を実現する [1][2][3]. 近年，センサネットワークにより生活環境に関わる様々な実空間から情報を収集し，それに基づいて新しいサービスを実現することの検討が進められている．例えば,「いまだけ・ここだけ・あなただけ」を目的とする個人の状況や利用環境に適応したサービス (個人・現場指向のサービス) などが検討されている [4]．一方，個人情報などのプライバシが保たれない場合は，センサネットワークが社会に浸透できる可能性は皆無に等しい．従って，新サービスの実現にあたっては，センサネットワークに適応可能なセキュリティ技術の導入を併せて検討する必要がある．

図 1.1 にセンサネットワークを活用するサービスのモデルの概念を示す．センサネットワークを用いたサービスモデルは，実空間に存在する人や物を表すユーザ，実空間に多数配備されるセンサ，サービス提供者であるオペレータの 3 要素から構成される．実空間の様々な場所に配備されるセンサは同じ空間に存在するユーザ，あるいは空間そのものの情報を検知 (センシング) し，センサは要求に応じて適宜これらの情報をオペレータに送信する (アグリゲート)．オペレータはセンサからの情報を分析し，サービス毎に定まる新しい価値をユーザに対して提示する (アクチュエート) ように動作する．

センサネットワークに適応可能な情報セキュリティ技術を検討するに当っては，センサネットワークの特性に十分留意する必要がある．センサネットワークは，実空間の情報を広範かつ詳細に収集するために，非常に多くのセンサを構成要素とする．従ってオペレータにとって，多数のセンサに対して個別に情報要求等のコマンドを発行して制御することは効率面から現実的ではなく，センサのグループを定義してグループ単位に管理する手段が求められる．また，センシング時に

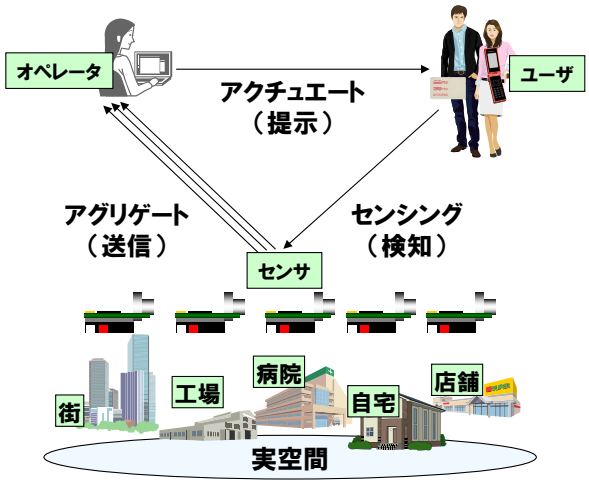

図 1.1. センサネットワークのサービスモデル

おいては，センサ単体で処理が完結することもあるが，センサ間やユーザの備える機器 (例：携帯電話や IC カードなど) を含む機器間での通信が求められることも多い．この時，必要になる全ての通信路を保護する手段を予め用意することは困難であるため，安全な通信路のアドホックな開設も想定しなければならない．さらに，センサの計算資源やメモリ資源の制約に留意する必要もある．従来のネットワークで利用される公開鍵暗号で用いられる数論的なテクニックを適用することは，これらの制約から困難であることが多い．そこで，軽量かつ小容量で実装可能な対称鍵暗号の適用が強く望まれる．しかし，対称鍵暗号を適用するに当っては，暗号化や認証の安全性の根拠となる鍵情報の配布，共有に関する管理が解決されなければならない．以上を踏まえると，センサネットワーク上での情報セキュリティのために，以下の実現が重要になると考える．

- 大規模センサグループとの通信 $(1 : n)$ に適した鍵管理
- アドホックな通信 $(1 : 1)$ に適した鍵管理

一方で，センサが実空間上に配備されることに起因して，センサ自体への攻撃や盗難等への配慮もこれまで以上に必要となる．これは，従来の情報セキュリティの議論においては見過ごしがちであるフィジカルセキュリティ，すなわち実空間上での物理的な対象 (例えば，センサが設置される部屋やセンサが格納される収

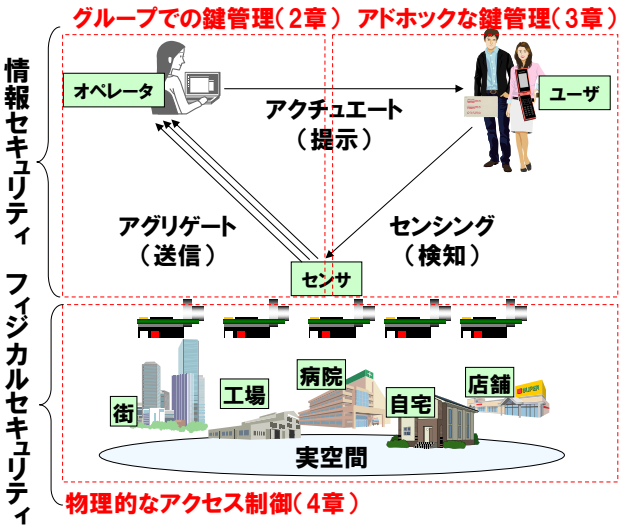

図 1.2. 論文の焦点

納ボックスなど) へのアクセス制御に関しても十分考慮する必要があることを意味する．従来のフィジカルセキュリティは，社員証の有無に応じたオフィスビルへの入退室管理に代表されるように，ユーザが持つ証明書の有無によってユーザの信用可否を判断するものが多い．一方，センサネットワークで収集可能な情報の中には，信用を判断する上での根拠となり得る情報も含まれる可能性があり，これらセンサ計測情報を積極的に応用することで，従来よりも安全性や利便性の観点で高度なフィジカルセキュリティを実現できると考えられる．そこで本論文では，センサネットワークの安全性のために，情報セキュリティに加え，センサネットワークにおける機能そのものを有効利用するフィジカルセキュリティについても議論を行う．

本論文前半では，センサネットワークの通信における情報セキュリティについて議論する．2 章では大量のセンサの管理を主目的としたグループにおける鍵管理について，3 章では，アドホックな通信を考慮した鍵管理について議論する．本論文後半の第 4 章では，フィジカルセキュリティに関する取り組みとして，センサ計測情報に基づく物理的なアクセス制御システムについて論じる．図 1.2 に本論文における焦点を整理する．

大規模数のセンサの管理を目的とした鍵管理

本論文第 2 章では，センサネットワークの多くの応用が要求するグループ通信に焦点を当て，暗号化や認証の安全性の根拠となるグループ鍵情報の管理技術について議論する．一般に同じ属性を持つセンサ端末 (ノード) は一個の同じグループに属すると考えることができる．ノードは一般に複数の属性を持つと考えられるため，一台のノードは複数のグループに同時に属することになる．グループ内で，あるいは対グループと安全な通信を行うためには，グループ内で共有させるグループ鍵の管理が重要となる．特に，ノード離脱に伴う前方安全性 (グループ鍵が外部に漏洩しても通信の秘匿性が保たれる特性) を確保することが安全にグループ鍵を管理する上で重要になる．従来法では，一台のノードが複数の大規模グループに所属する場合において，前方安全性を確保するために，メモリ負荷と通信負荷が著しく増加することがあった．本論文では，ノードの属性に紐つける管理情報を用いて，個々のグループ鍵の管理の仕組みを互いに連携させることで，従来に比べ，管理上の負荷を低減できることを示す．具体的には，適用例のもと，既存方式より，ノードのメモリ負荷の 64%〜88%を，通信負荷の 46%〜97%を削減できることを示す．

アドホックな通信を考慮した鍵管理

本論文第 3 章では，初見の端末同士でアドホックな通信路を安全に開設するために有効な，動的な鍵生成法について議論する．従来，端末間での通信用の暗号鍵は固定的もしくはキー入力による PIN コードやパスワードを利用したものが一般的で，鍵長は概して短く，鍵の設定は一般的に煩わしい．そこで人間の動作を加速度センサで計測したデータから特徴量を抽出し，できる限りユーザに負担のかかる操作を介することなく，共通鍵を生成，共有する方式を導入する．具体的には，歩行や自動車での移動といった日常的な動作から加速度情報を収集し，収集した情報の類似度に応じた強度をもつ鍵生成を行う方式を与える．被験者の動作に基づく性能評価により，類似度が高い場合は 1 分間で 217.7 bit 相当の，類似

度が中程度の動作でも約 2 分間で Bluetooth の PIN コード相当の共通鍵を生成できることを示す.

センサ計測情報に基づく物理的なアクセス制御システム

本論文第 4 章では，センサネットワークで収集する情報を活用した物理的なアクセス制御に関する取り組みとして，センサから得られる情報を解析することで得られるユーザのプレゼンス (存在位置) を，ロールベースアクセス制御 (RBAC) ポリシ，デジタル証明書とともに統一的に扱う新しい信用管理技術について論じる．信用管理技術は，サービスを利用したいユーザが公開鍵基盤 (PKI) に基づくデジタル証明書を提示し，その証明書で担保可能な一定の信用をユーザに与えること (信用の確立) によって特定のサービスの利用を許可する．本論文では，このような信用管理の新たなシステムアーキテクチャとして，信用の確立に利用する情報として，ユーザが提示したデジタル証明書に加え，そのユーザや関係者のプレゼンスを導入した信用管理システムについて議論する．プレゼンスの導入に際しては，プレゼンスに信頼度というパラメータを与え，確率モデルに基づく信頼度評価によってプレゼンスの不確実性を考慮する．具体的には，隠れマルコフモデルに人の行動特性を反映した状態遷移確率を与え，センサから直接導かれるプレゼンスの観測結果から，その信頼度を推定する方式を導入する．この信用管理システムをサービスアクセス制御システムに導入する評価実験を通じて，得られるプレゼンスの *recall* を，センサから直接得る場合と比較して約 1.8 倍 (0.94 以上) に向上できることを示す．その結果，信用確立における利便性や安全性を向上できることを示す.

第2章　複数の大規模グループに同時参加するセンサノード向けグループ鍵管理方式

1. はじめに

センサネットワークとは，センサ機能と通信機能を備える端末（ノード）と，ノードからの情報収集やセキュリティ確保を含むネットワークの管理を司る管理者（サーバ）から構成されるネットワークである．我々の生活空間や企業活動の現場に様々なセンサや端末が組み込まれ，それらがいつでもどこでもネットワークにつながる，いわゆるユビキタス情報化社会が進展する中で，センサネットワークが活用される場面がますます広がってきており，かつ，センサネットワークは大規模化してきている．例えば，BEMS（Building and Energy Management System）[30] などが大規模なセンサネットワークを活用した応用の例である．

大規模なセンサネットワークでは，サーバ側から常にすべてのノードに一律に指示を出して制御することは効率面から現実的ではなく，ノードのグループを定義してグループ単位に管理することが必須になる．例えば，ある建物の同じ階に設置されたグループに対して初期設定情報を送信したり，特定のセンシング機能を持つグループに対してコマンドを送信するような形態は，センサネットワークにおいては極めて日常的であり，多用される通信形態であるということができる．

大規模なセンサネットワーク上で安全なアプリケーションを構築・運用するためには，センサネットワークにおけるグループを安全に管理するためのグループ鍵管理が重要である．つまり，これらグループ通信の内容を暗号化する仕組みや，通信情報の改ざんや偽造を防ぐ仕組みの導入が必要となる．グループのメンバだ

けが知り得る「グループ鍵」を導入し，各種の暗号技術を使うことで上記の安全性を確保することが可能となるが，グループ鍵については，グループの実態に即した形でこれを管理する必要がある．特に大規模なセンサネットワークにおけるグループ鍵管理では，以下に述べる二つの点を十分に考慮する必要がある．

一点目は，グループ化されたノードは，時間の経過に応じて変化する可能性がある点である．現実のセンサネットワークの応用では，新しいノードを参加させて既存のグループに追加したり，故障，紛失，あるいは盗難等の理由で，既存のノードがグループから離脱する事態も起こり得る．グループから離脱するノードが発生した場合でも安全性を継続して確保するためには，離脱ノードの保有する鍵情報が悪用されないよう対策する必要があるが，ノードの紛失・盗難等の理由で離脱ノードの制御が不可能となる事態を想定すると，速やかにグループ鍵を更新し，離脱ノード以外のグループメンバに新しいグループ鍵を再配送すること（ノード無効化）が事実上唯一の解決法となる．グループに所属するメンバ数が少ない場合，離脱ノード以外に対してユニキャスト的に新しいグループ鍵を配送することも可能であるが，中・大規模グループにおいてユニキャスト的な鍵配送を行うことは，効率面から問題がある．大規模グループにおいて効率的にグループ鍵を更新する方式は，情報セキュリティの分野で多く研究されており，例えば鍵管理情報を木構造に基づいて定義する方式などがよく知られている [19].

注意すべき二点目は，一台のノードが，複数のグループに同時に所属する可能性がある点である．例えば，一台のノードが「3 階に設置されたノードのグループ」「温度センサを持つノードのグループ」に同時に属する，という形態をあらかじめ想定する必要がある．これに対する安直な解決法は，上述したようなグループ鍵管理方式を複数独立して導入することであるが，この安直な方式では，鍵記憶のためのメモリ量や鍵管理の通信負荷が，所属するグループ数に応じて増加してしまう．これは，資源が非常に限定されたノードでは，致命的な問題となることも考えられる．[23] では，グループ鍵管理のための木構造を独立して定義するのではなく一部の部分木を共通化することで，鍵個数の削減を検討している．一個の情報が複数のグループ鍵管理に貢献するという意味で興味深い点もあるが，木構造を再構築するときまで離脱ノードがグループ鍵を保持することを許すなど，

ノード離脱に関する問題を本質的に解決していないという意味で，実用的な解決法にはなっていない．

本研究では，上記二つの観点に十分留意して，大規模センサネットワークにおけるグループ鍵管理方式を提案する．具体的には，上記二つの観点に基づき，次のような四つの要件を満たすようなグループ鍵管理方式を設計する．

要件 1 任意のタイミングでグループ鍵の更新が可能である

- 第一の観点から，グループの動的な変化に追随してグループ鍵の更新を実施できるべきである

要件 2 大規模なグループを効率的に管理できる

- 大規模なセンサネットワークでは，個々のグループの規模も大きくなるので，そのような場合でも実用的な処理効率を確保できるべきである

要件 3 一台のノードが複数グループに属するときの負荷増が緩やかである

- 第二の観点から，一台のノードが複数グループに同時に所属しても，実用的な処理効率を確保できるべきである

要件 4 サービス内容から導かれる自然な属性に基いてグループを定義できる

- サービスにとって有益なグループを管理できるべきである

以降では，2 節で関連研究について，本研究の位置づけとともに説明し，3 節にて提案方式を説明する．さらに 4 節では，典型的な応用として，本章冒頭で触れた BEMS を想定し，提案方式と既存方式の比較評価を行う．最後に 5 節にてまとめる．

2. 関連研究

2.1 既存方式の分類

本研究はセンサネットワークにおける鍵管理方式の研究という範疇に入る．そのなかでも特に本研究はグループ鍵管理方式を対象とするが，本研究の位置付け・

表 2.1. センサネットワーク向け鍵管理方式の分類

管理対象	中央管理型	自律型
ペアワイズ鍵	[5],[6]	[7],[8],[9],[10],[11],[12],[13],[14],[15],[16]
グループ鍵	[17],[18],[19],[20],[21],[22],[23]	[24],[25],[26],[27]

アプローチを明確化するため，本節ではセンサネットワークにおける鍵管理方式に関する既存方式の分類・整理を試みる．センサネットワークで頻出する無線通信では，特定のノードに限定して鍵情報を送り届けることが困難であるため，暗号技術を用いて，通信路上の情報を入手したとしても，そこから有用な情報を第3者に漏洩させないことが求められる．暗号技術に基づいた鍵管理方式として，公開鍵暗号に基づく鍵管理方式，すなわち [28] に代表されるような数論的な手法を利用する方式が知られている．しかし，それらの方式はセンサネットワークに適用する上では，資源制約の厳しいノードに大規模な計算を課す必要が生じるという問題がある．従って，センサネットワークを対象とした本研究および以下に説明する既存方式では，現実的な方式として，対称鍵暗号や一方向ハッシュ関数等の軽量な処理のみで完結するシンプルな方式を採用している．

センサネットワークにおける鍵管理方式については，二つの異なる分類軸を導入し，各分類軸について，それぞれ二つの管理モデルを定義することができる．一つ目の分類軸は，管理対象となる鍵の機能に着目するものであり，ノード間の秘匿通信のために，ノードペア毎に共有されるペアワイズ鍵の管理モデル，グループでの秘匿通信のためにグループに属するノード全員で共有されるグループ鍵の管理モデルの二種類が考えられる．もう一つの分類軸は鍵管理を実現する仕組みに着目するものであり，鍵の更新時に，信頼できる鍵管理者（サーバ）の存在を仮定する中央管理型モデル，当該ノードだけで鍵更新を完了することのできる自律型モデルの二種類が考えられる．上記分類軸に従って，既存研究を分類すると，表 2.1 のようになる．

ペアワイズ鍵管理-中央管理型モデルとして，[5]，[6] がある．[5]，[6] は各ノードがサーバとの間で 1 対 1 に保持するマスタ鍵を使って，ペアワイズ鍵を送受信

ノードに個別配送する．

ペアワイズ鍵管理-自律型モデルとして，[7]-[16] がある．これらの方式では，ペアワイズ鍵を生成するための情報（鍵種）をノードに事前格納することで，アドホックに通信を開始するノード間でのペアワイズ鍵共有をローカルに実現する．鍵種の選択のため，ノードの部分集合（ある種のグループ）を想定する研究 [14] もあるが，後述するグループ鍵管理モデルと混同しないように注意する必要がある．

グループ鍵管理-中央管理型モデルにおける単純な方式 [17]，[18] では，各ノードがサーバとの間で 1 対 1 に保持するマスタ鍵を用い，サーバがグループ鍵をグループ内のノードに個別に配送する．[19]，[20]，[21] は，グループ毎に定義する木構造を利用してグループ鍵を配送する．[22] は，一方向性ハッシュ関数とグループ毎に定義する木構造を利用してグループ鍵を配送する．[23] は，グループ鍵管理のための木構造を独立して定義するのではなく一部の部分木を共通化することで，鍵個数の削減を検討している．

グループ鍵管理-自律型モデルの例として，[24]，[25]，[26]，[27] がある．[24] は，後述するような特殊なハードウェア上の仕組みを導入し，グループ鍵を含む暗号鍵管理を行う．[25]，[26] は，サーバとの通信が切断されても各ノードがローカルな計算のもとでグループ鍵を更新する仕組みを提示している．[27] は，サーバの代理者をグループ単位に設け，代理者を介して個々のグループ鍵を更新する．

2.2 本研究の位置づけ

本研究ではグループ鍵管理-中央管理型モデルを採用する．任意のノードとノードとの間の鍵共有は表 2.1 の分類でいうペアワイズ鍵の管理に相当し，本研究の枠組みで対象としない問題である．グループ鍵を管理するにあたって，機能的には，自律型モデルのほうが中央管理型モデルよりも優れている部分もある．しかし，自律型モデルでは本来サーバが行う機能を複数ノードが分担して行うことになるため，方式が複雑・非効率になったり，追加の前提条件が必要となる傾向がある．ノードが動的に動き回るアドホックな応用等では自律型モデルを採用せざるを得ない場面もあるが，4 節で述べる BEMS のように，ノードが静的に設置さ

れ，サーバとの接続性が確保されるような応用では，中央管理型モデルのほうが実用性が高いといえる．グループ鍵管理-中央管理型モデルの枠内でも様々な機能を持った方式が検討できるが，本研究では，前節で述べた四つの要件を満たす方式の実現を目的とする．以降では，これら要件を基準として，グループ鍵管理-中央管理型モデルの方式を比較する．

[17]，[18] の方式では，各ノードとサーバとの間でユニークな（ノードごとに異なる）マスタ鍵が共有されていることを前提としている．あるノードがグループから脱退する際には，グループ鍵の更新が必要になるが，この時，脱退するノード以外のすべてのグループ内ノードに対し，（新しい）グループ鍵をそのノードのマスタ鍵で暗号化して送信することを繰り返す．この方式では，グループ鍵配送にかかる通信負荷がグループ内のメンバ数に対して線形オーダで増加するため，多数のメンバを有する大規模グループでの鍵管理において，要件 2 を満たせないおそれがある．

大規模なグループにおける効率的なグループ鍵管理を実現する手法としては，[19] が広く知られている．[19] では，鍵木と呼ぶ木構造を利用してグループ鍵配送にかかる通信回数を削減する．鍵木の各頂点には暗号鍵が割り当てられており，また，葉頂点とノード（ユーザ）との間に一対一の対応関係が定義されている．各ノードには，対応する葉頂点の先祖頂点に割り当てられた暗号鍵を事前に配送しておくものとする．すべてのノードは鍵木の根頂点の鍵を共有するので，この根頂点の鍵をグループ鍵として利用する．あるノードがグループから脱退する際には，脱退ノードの持つ暗号鍵を全て無効化する必要がある．具体的には，無効化された鍵を置き換える新しい鍵を，それを保持すべき全てのノードに配送する．この時，鍵木に沿ってボトムアップ的に新しい鍵を配送することにより，全ノード数に対して対数オーダの手間で，ノード無効化処理を実現することができる．基本的に [19] は，一個のグループに対する鍵管理手法であるが，副次的に，鍵木の中間節点に対応するノード部分集合という「別のグループ」を想定することが可能である．例えば，[19] の鍵木に基づき，位置的に近接するノード集合をグループとみなす [20]，通信頻度の高いノード集合をグループとみなす [21] が存在する．しかし，これら副次的なグループは，サービス実現において有用なグルー

表 2.2. グループ鍵管理-中央管理型モデルの方式比較

方式	要件 1	要件 2	要件 3	要件 4
[17],[18]	○	×	○	○
[19],[22]	○	○	×	○
[20],[21]	○	○	×	×
[23]	×	○	○	○
提案方式	○	○	○	○

プ形態とは一致しないことがあり，要件 4 を満たせない．複数のグループを柔軟に設定したい場合，これら方式では一台のノードが独立した複数グループに加入することは考慮されていないため，鍵木を複数独立して導入する必要があり，要件 3 を満たすことができない．[22] は [19] の改良方式であり，ノード無効化処理における通信負荷を [19] より削減可能であるが，要件 3 への対応において，本質的に [19] と同じ問題がある．

[23] は，ユーザが同時に複数のグループに所属するようなケースを考え，鍵木の一部を共用化する方式について議論している．[23] では，複数の鍵木が，その部分木を一部共用するような仕組みを提案している．一個の情報が複数のグループ鍵管理に関与するため，情報の効率利用という意味では，センサネットワークでの利用に向いた方式である．致命的な問題は，ノードの新規追加やグループからのノード離脱等の操作を間欠的にしか実現できていない点にある．特に，安全運用においては，脆弱性の疑われるノードを可能な限り迅速に無効化することが求められるが，[23] では，離脱ノードが長期にわたって（次に鍵木を再構築するまで）グループ鍵を保持することを許容しているため，要件 1 を満たす方式とは言い難く，高い機密性の要求される応用での利用は難しいといえる．

以上を整理するとグループ鍵管理-中央管理型モデルについて，既存方式と提案方式における各要件への対応は表 2.2 のように整理される．4 つの要件をすべて満たす既存方式はなく，提案方式ではこれら 4 つの要件を満たすことを目的としている．定量的な評価が必要な要件 2，3 に関しては，4 節にて詳細に議論する．

グループ鍵管理-自律型モデルの既存方式を中央管理型のモデルに適用すること

ももちろん可能である．しかしながら上述の通り，自律型のモデルはサーバレスで管理可能という利点を得られる反面，実現性や効率の観点で欠点がある．例えば，特殊なハードウェア上の仕組みを導入することで，グループ鍵を含む暗号鍵管理を効率的に行おうとの試みが [24] で提案されている．[24] では，全てのノードは外部から操作できない時計を内蔵しており，特定時刻を過ぎると，ノード内部の機密情報を完全かつ確実に消去することが求められる．もし，ノード故障等の理由により機密情報の消去に失敗したり，あるいは，機密情報消去までにノードが盗難・内部解析された場合，そのノードだけでなく，応用システム全体の安全性が保証されなくなってしまう．[24] を安全に利用するためには，低コストで大量生産されるノードについて十分な動作信頼性を保証する必要があるが，それが現実的であるかどうかは，議論の分かれるところである．[25]，[26] は，ネットワークの全稼働時間を有限のセッションに分割することで，あるセッションにおけるグループ鍵をローカルに計算可能とする．鍵更新のたびにセッションを消費していくため，システム全体としての稼働時間が制限されることになる．現実のシステムでは，一部のノードを交換しつつ，永続的にシステムを維持することも一般的と考えられるが，そのような運用も行えなくなる．また，[25]，[26] では，鍵のメモリ負荷および更新に要する通信負荷において，巨大素数の対数オーダを要し，上記の中央管理型モデルの方式，例えば [19] 等に比較して効率的ではない．[27] では，各グループにクラスタヘッドと呼ぶサーバの代理者を設け，クラスタヘッドが当該グループの鍵更新を担う．各ノードは同じグループのクラスタヘッドに接続できればよいため，鍵管理の自律性は完全な中央管理型モデルに比べ高いと考えられるが，各グループにおいて鍵更新にかかる通信負荷がグループ内のメンバ数に比例し，[17]，[18] と同程度に要件 2 への対応が困難である．

また，ペアワイズ鍵管理モデルでも，マスタ鍵の代わりにノード間で共有するペアワイズ鍵を使用することで，[17]，[18] に類するグループ鍵管理を実現できる．しかし [17]，[18] と同様に，要件 2 を満たせない．

3. 提案方式

本研究では，センサネットワークの応用において，任意のグループ構造が独立して存在するのではなく，ノードの持つ「属性値」により自然に定義されるグループが複数存在することを想定し，一台のノードが自然に加入することになる複数グループを想定したグループ鍵管理方法を検討する．以下 3.1 項では，想定しているネットワーク環境と，提案方式を実現するための前提条件について述べる．3.2 項，3.3 項では，本研究で考えるグループの構造について検討し，その形式化を行う．特に 3.3 項では提案方式において重要な条件について説明する．3.4 項では，3.2 項，3.3 項で与えるグループ構造の下で安全かつ効率よくグループ鍵を更新するためのプロトコルを示す．

3.1 想定するネットワークと前提条件

本研究では，複数のノードと一台のサーバからなるセンサネットワークを考え，[19]，[22] と同様に，サーバから全ノードに対して放送型配信の可能なネットワークトポロジを想定する．放送型配信が可能であればよく，例えばサーバを中心とするスター型への適用が可能である．本節では議論の汎用性を確保するために，トポロジを特定せずに議論を行う．その後，4 節において，スター型トポロジを対象に提案方式が機能することを定量的に示す．

サーバは汎用の計算機であり，十分安全な管理体制下で運用されるものとする．すなわち，サーバから機密情報が漏えいしたり，サーバが不正行為を行うことは想定しない．これに対し，ノードについては「比較的弱い耐タンパ性を持つ記憶領域」を備え,「比較的弱い管理体制」の下で運用されることを想定する．具体的には，以下の条件が成立することを仮定する．

- ノードの内部情報が不正な解析行為によって露呈することは完全には防げないが，ノード内部情報の参照や改変には一定の時間がかかる
- ノードの盗難を完全に防ぐことは困難であるが，一定の盗難抑止措置が講じられており，複数のノードが同時に攻撃者に入手されることはない．ま

た，ノードの盗難が発生した場合は，直ちにその旨がサーバに通報される．

軍事用途などを含めたすべてのセンサネットワークの応用で上記条件を達成できる保証はないが，この条件が比較的妥当な応用は多いと考えられる．例えば，SD カード [29] 等の低コストで実用的な耐タンパ性能を提供するシステム LSI を利用可能な状況が多くなっていることや，4 節でオフィスビルの省エネルギー化のためにセンサネットワークを利用する例を想定して議論を行うように，運用上の前提として，オフィスビルへの入退室は厳重に管理されること，ビル内は多くの利用者やビデオカメラ等により衆人環視状態にあること，固定用ワイヤや振動検知アラーム等でノードに対する物理的な攻撃を抑止できること等を踏まえると，上述の条件は，かなりの程度で達成されると考えることができる．

提案方式は，上述のような環境において，脆弱性の疑われるノード内部の情報が不正利用される前に，速やかに当該ノードを無効化する手段を提供する．上記の条件が成立しない場合，提案方式では安全性が確保できなくなる場合もある．この問題については，4.4 項であらためて議論を行う．

3.2 ノードの属性から定義されるグループ構造について

多くの実用的なセンサネットワークの応用においては，何らかの「属性」に着目して各ノードを特徴づけ，同じ属性値を持つノードをグループ化して取り扱う機会が多いと考えられる．例えば，ノードの設置方角という「属性」を考え，各ノードは東，西，南，北のうち一つの属性値を持つものとすると,「東（西，南，北）の方角に設置したノードの集合」が概念的に定義されることになる．あるいは，設置フロアという別の「属性」を考えることで，例えば「3 階に設置されたノードの集合」が定義され，さらに「高次」の集合として,「3 階の東側に設置されたノードの集合」が導かれることになる．このように，ノードの持つ属性値によりノードをグループ化することは極めて自然であり，このように定義されたグループは，センサネットワークの応用においても，一定の意味を持つことが期待でき，要件 4 への対応を現実的なものとする．本研究では，上述のように定義されるグループにおけるグループ鍵について検討を行う．

グループ鍵は，グループに属するノードとサーバだけが知る秘密情報である．グループ鍵と暗号技術を用いることで，グループメンバだけに限定した同報通信等を実現することが可能となる．上述の通り，本研究で考えるグループは，センサネットワーク運用上意味のある集合となっているため，これに対してグループ鍵を与えることは，安全で信頼できるアプリケーション構築に貢献すると考えられる．

属性および属性値については，センサネットワークがどのような環境でどのような目的に使われるかで，大きく異なってくると考えられる．上述のように，設置場所に関する情報を属性値とすることは多くの局面で有効と考えられるが，例えば，一つのネットワークの中に温度センサ，人感センサ等，異なるセンシング機能を持つノードが含まれる場合には,「搭載センサ機能」という属性が必要になるであろう．あるいは，複数の事業者の設置したノードの通信下位レイヤを相互接続し，一個の密なセンサネットワークを構成するような場合においては，各ノードには「事業者」という属性が紐付けられると考えられる．何種類の属性を考えるか，何を属性とするか，各属性に対してどのような属性値を定義するかは，ネットワークの設計・運用にあたっては課題となるが，本研究では，属性および属性値は事前に決定され，外部から与えられるものとして議論を行う．ただし，すべてのノードは，定義されたすべての属性について，ちょうど一個の属性値を持つことを前提条件として仮定する．これは「特定の属性値が定義されていない」，「複数の属性値が定義されている」ことを想定しない，との仮定であるが，例えば「未定義」という属性値を新たに設定する等，運用上の対応によって，本仮定は容易に達成することができると考えられる．

N を，ノード全体からなる集合とする（サーバは N には含まれない）．集合族 $A = \{G_1, G_2, \ldots, G_m\}$ が以下の条件を満たすとき，A を N の**分割**という：

- $G_i \subset N$
- $i \neq j$ ならば $G_i \cap G_j$ は空集合である
- $G_1 \cup G_2 \cup \cdots \cup G_m = N$

いま，対象とするセンサネットワークにおいて d 個の属性を定義し，$i(i \leq d)$ 番

目の属性には m_i 種類の属性値を定義することを考える．この時,「i 番目の属性については j 番目の属性値を取る」ようなノードの集合を $G_{i,j}$ と書くことにすると，上述の属性値に関する一意性の仮定より，$A_i = \{G_{i,1}, G_{i,2}, \ldots, G_{i,m_i}\}$ は N の分割となる．本研究では，ノード集合 $G_{i,j}(1 \leq i \leq d, 1 \leq j \leq m_i)$ をノードの**一次グループ**と呼び，一般に，$G = G_{i_1,j_1} \cap G_{i_2,j_2} \cap \cdots \cap G_{i_k,j_k}$ として与えられるノード集合 G を k **次グループ**と呼ぶ．ただし，$1 \leq k \leq d$ であり，$i_1, i_2, \ldots, i_k$ は 1 以上 d 以下の相異なる整数，$1 \leq j_a \leq m_a(1 \leq a \leq k)$ とする．次数について意識する必要が無い場合，G を単にグループと呼ぶ．以上の定義より明らかな通り，本研究では，いくつかの属性値が共通するようなノードの集合をグループと呼称する．一般に，センサネットワークの応用の中には多数のグループが存在し，ノードは，その属性値に従い，複数のグループに所属することとなる．d 次グループは，集合の包含関係に関して極小のグループである．

3.3 グループ構造における条件

3.2 項で述べたグループ構造に対して，満たすべき条件を以下に示す．これは 3.4 項で述べるノード無効化に関する前方安全性を考慮する上で重要な条件となる．

条件 1 任意の d 次グループについて，その要素数は高々 1 である．

すなわち，任意の $(1, j_1), (2, j_2), \ldots, (d, j_d)$ について $G = G_{1,j_1} \cap G_{2,j_2} \cap \cdots \cap G_{d,j_d}$ が空集合となることは許すが，G が 2 個以上のノードを含むことはないと仮定する．自然に導かれる属性を使用しただけでは，本条件を満足できない場合もあると考えられるが,「d 次グループ内でのシーケンス番号」に相当する人工的な属性を一個追加すれば，上記条件を達成することができる．

図 2.1 は，提案方式におけるグループ構造を説明する図である．例えば，単一のセンサを搭載するノードが複数の設置フロアに点在する場合,「搭載センサ機能」および「設置フロア」という属性に着目でき，各々において一次グループ G_{1,j_1}, G_{2,j_2} を考えることができる．これらの集合の包含関係によって 2 次グループが定まる．ただし，同一のフロアに同じセンサを搭載するノードが高々1 つであるとは限らない場合，条件 1 を満たすために，$G_{1,j_1} \cap G_{2,j_2}$ におけるグループ内で

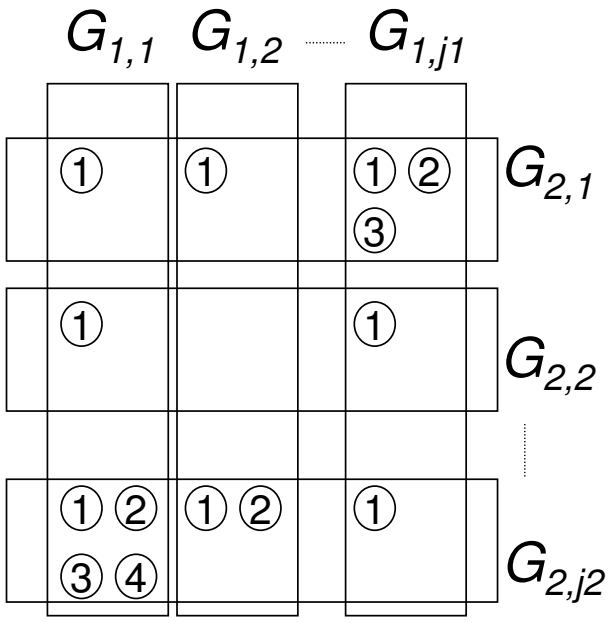

図 2.1. グループ構造の例

のシーケンス番号に相当する人工的な属性 G_{3,j_3} を追加する必要がある．この時，一次グループ G_{3,j_3} は，$G = G_{1,j_1} \cap G_{2,j_2}$ において，同じシーケンス番号を与えられるノードの集合となる．3 次グループ $G' = G_{1,j_1} \cap G_{2,j_2} \cap G_{3,j_3}$ において，要素数は高々1 であり，条件 1 を満たす．図 2.1 において，各ノードは○で示されており，○内の数字は，ノードに与える人工的な属性であるシーケンス番号を示す．

ただし，d 次グループに収容されるノードが非常に多かった場合に，d 次グループ内でのシーケンス番号に相当する属性をただ一個追加しただけでは必ずしも効率的とはならない．その場合は，以下のような拡張を与えてもよい．d 次グループにおける最大のノード数以上の葉数を持つ完全 n 分木を用意し，葉に d 次グループ内のノードを配置する．そして，頂点から葉に到るまでの各階層において「何番目の節を経るか」に相当する人工的な属性を複数追加する．本拡張によって，追加する属性値数を，d 次グループに収容される最大ノード数の対数オーダに抑えられる．図 2.1 と同様に一次グループ G_{1,j_1}，G_{2,j_2} のみが存在するとき，これらの集合の包含関係によって 2 次グループが定まる．2 次グループにおける最大のノード数が 8 のとき，図 2.2 のように高さ 3 の完全 2 分木を与え，葉に 2 次グループ内のノードを配置している．3 つの階層において，それぞれに「何番目

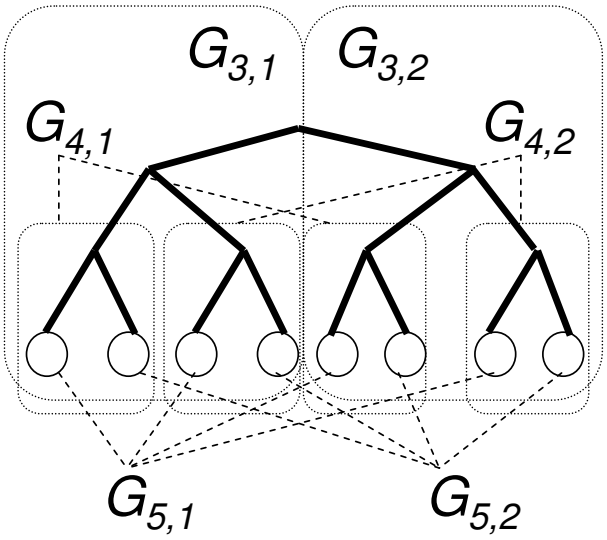

図 2.2. 人工的な属性の拡張

の節を経るか」に相当する人工的な属性 $G_{3,j_3}, G_{4,j_4}, G_{5,j_5}$ を追加している．この時，5 次グループ $G = G_{1,j_1} \cap G_{2,j_2} \cap G_{3,j_3} \cap G_{4,j_4} \cap G_{5,j_5}$ において，要素数は高々 1 であり，条件 1 を満たす．以下の議論では，この条件が満足するよう属性および属性値が定められていることを前提として議論を行う．

3.4 グループ鍵の管理方式について

グループ鍵の定義と初期化

センサネットワークの中には，前項で定義されたようなグループが多数存在する．それぞれのグループに対して個別に独立したグループ鍵を定義すると，一台のノードは，自らの所属するグループ数に比例した個数のグループ鍵を管理する必要が生じるため，大きな記憶領域が消費されてしまうことになる．この問題を避けるため，一次グループに対してのみ独立したグループ鍵を定義し，2 次以上のグループに対しては，一次グループのグループ鍵を組み合わせてグループ鍵を構成することを考える．一次グループに対してのみ独立して定義するグループ鍵を**要素鍵**と呼ぶ．サーバは，すべての一次グループ $G_{i,j}(1 \leq i \leq d, 1 \leq j \leq m_i)$ に対し，要素鍵 $k_{i,j}$ をランダムかつ独立に決定する．次に，一次グループ $G_{i,j}$ に

属する全てのノードに要素鍵 $k_{i,j}$ および要素鍵の発行時刻を運用に先立って事前に格納する．もしくは安全な通信路を仮定してその上で配送する．d 種類の属性が存在するため，一台のノードは，全部で d 個の要素鍵（およびその発行時刻）を保持することになる．グループ鍵はこれらの要素鍵から以下のように計算される．グループ G が，$G = G_{i_1,j_1} \cap G_{i_2,j_2} \cap \cdots \cap G_{i_k,j_k}$ として定義されるものとする．この時 $k(G) = h(k_{i_1,j_1}||k_{i_2,j_2}||\cdots||k_{i_k,j_k})$ と定義し，これを G の**グループ鍵**と呼ぶ．ここで h は事前に選んでおいた一方向性ハッシュ関数であり，$||$ は連接演算子を表す．グループ鍵 $k(G)$ を計算するためには，要素鍵 $k_{i_1,j_1}, k_{i_2,j_2}, \ldots, k_{i_k,j_k}$ を全て知っている必要がある．したがって，$k(G)$ を計算することができるのは，グループ G に属するノードのみとなる．

ノード無効化を考慮したグループ鍵の更新

センサネットワークに特有の脅威としてノードの盗難がある．盗難ノード内部の暗号鍵等が不正者の手に渡ると，機密情報の漏えいや通信データの偽造等が行われる可能性があるため，ノードの盗難が発覚した場合は，速やかに当該ノードの無効化を行う必要がある．盗難に遭ったノードは管理者の制御下から離れている可能性が高いため，機密情報を消去するようなコマンドを管理者が盗難ノードに向けて発信したとしても，ノードがコマンドを受信して正常に動作することは期待できない．この問題を回避するには，盗難ノードが所有するすべての鍵の使用を停止し，盗難ノード以外の全ての（権限ある）ノードに対して新しい鍵を配送する必要がある．この際，古い鍵で新しい鍵を暗号化する手法は利用できない．なぜなら，ノードを盗んだ攻撃者が通信路上の暗号文を記録・保存しておき，盗難ノード内部から暗号鍵を抽出した後に，暗号文の解読を行う可能性もあるためである．いわゆる前方安全性を確保するためには，盗難ノードが持つ鍵を一切使わずに，安全かつ効率的に新しい鍵の配送を行う必要がある．

提案方式では，一台のノードは各属性に対応して要素鍵を持つため，盗難ノードの内部には d 個の要素鍵が格納されている．盗難ノードを n とし，n に格納されている d 個の要素鍵を $k_{1,j_1}, k_{2,j_2}, \ldots, k_{d,j_d}$ とする．ノード n を無効化するには，これら d 個の要素鍵の使用を停止し，$G_{i,j_i}(1 \leq i \leq d)$ の新しい要素鍵 k'_{i,j_i}

をノード集合 $G_{i,j_i} \setminus \{n\}$ に配送する必要がある．これを安全かつ効率的に実現するため，以下のプロトコルでは,「ソルト」と呼ばれる情報を n 以外のノードに配送し，古い要素鍵とソルトから新しい要素鍵を導出することを考える．この手順は，具体的には以下のプロトコルにより与えられる．ここで $E_k(x)$ は情報 x を鍵 k で対称鍵暗号アルゴリズムにより暗号化して得られる暗号文であり，$\langle\cdot\rangle$ は，括弧内の情報から構成される更新用データを表す.

(1) サーバは，**ソルト**と呼ばれるランダムな情報 S を決定する．また，新しい要素鍵の発行時刻 t を決定する.

(2) サーバは，n 以外のノード全体からなる集合を U とする.

(3) サーバは，U が空集合になるまで以下を繰り返す.

  (a) $G_{i,j} \cap U \neq \emptyset$，$n \notin G_{i,j}$ となる一次グループ $G_{i,j}$ を一つ定め，$x_{i,j} = E_{k_{i,j}}(S, t, (1, j_1), (2, j_2), \ldots, (d, j_d))$ を計算する.

  (b) $\langle i, j, x_{i,j}\rangle$ を $G_{i,j}$ に向けて同報送信する.

  (c) $U \leftarrow U \setminus G_{i,j}$ とする.

(4) $\langle i, j, x_{i,j}\rangle$ を受信したノードは，自分が $G_{i,j}$ に属さない場合これを棄却する．自分が $G_{i,j}$ に属する場合，以下を実行する.

  (a) $x_{i,j}$ を復号し，S，t および $(l, j_l)(1 \leq l \leq d)$ を入手する.

  (b) 自分の持つ要素鍵の中に無効化される要素鍵 k_{l,j_l} があり，k_{l,j_l} の更新時刻が t よりも古いとき，$k'_{l,j_l} = h(S||k_{l,j_l})$ を計算して G_{l,j_l} の新しい要素鍵とし，この要素鍵の発行時刻を t に更新する.

無効化される要素鍵 $k_{1,j_1}, k_{2,j_2}, \ldots, k_{d,j_d}$ の更新には，古い要素鍵とソルト S が必要となる．サーバは，上記ステップ (3) において，n を含まない一次グループのみを用いて n 以外のすべてのノードを被覆する集合族を求め，各一次グループの要素鍵を用いて S を暗号化する．n はいずれの一次グループの要素鍵も持たないため，暗号化された S を復号，入手できず，また，n 以外のすべてのノードは少なくとも一個の暗号文を復号できるため，S を知ることができる．これにより，

無効化ノード n 以外の全てのノードに S を配送することが可能となり，安全に要素鍵を更新することができる．本プロトコルを実施するにあたって，[23] のようなタイミング的な制約は無く，運用中における任意の時点で実施可能である点で，要件 1 を満たすプロトコルということができる．

上記手順の負荷は，n 以外のノードを被覆する集合族の要素数に比例する．要素数が最小の被覆を求めることは，NP 困難である集合被覆問題の変形と考えられるため，厳密な最適解を効率的に求めることは難しいと考えられるが，最悪の場合であっても $G_{1,j_1}, \ldots, G_{d,j_d}$ 以外の $\sum_{i=1}^{d}(m_i - 1)$ 個の一次グループを利用すれば，求める集合被覆を構成することができる．したがって，本手順におけるサーバの暗号化操作実行回数および送信データ数は，高々 $\sum_{i=1}^{d}(m_i - 1)$ であるといえる．ノードは，自分の復号できるデータを一個だけ復号すれば良いため，一回の復号操作と，自らが所有する要素鍵のなかで更新の必要なものの個数と同じ回数のハッシュ値計算により，必要な要素鍵更新を完了することができる．また，発行時刻 t を利用することで，複数経路を通過して同一ノードに複数の同じ更新用データが到着しても混乱無く実行できる．また，攻撃者のリプレイ攻撃により混乱を生じることもない．

なお，盗難ノードが存在しない，つまり $\{n\} = \emptyset$ として同様の手順を踏むことで，単純に全てのグループ鍵を更新することも可能である．この時，サーバの暗号化操作実行回数および送信データ数は，高々 $\sum_{i=1}^{d} m_i$ である．

ノードの追加

新しいノード n を，グループ $G_{i,j}$ に追加したい場合を考える．新しくグループに参加するノード n は，自分が参加する以前に $G_{i,j}$ のグループ鍵として使われていた鍵を知る権利はない．逆に，n をグループのメンバとして追加する過程において，n が以前のグループ鍵を知ることがあってはならない．この性質をグループ鍵における後方安全性と呼ぶ．後方安全性を有するノード追加プロトコルは，$G_{i,j}$ に以前から所属するノードには要素鍵 $k_{i,j}$ を用いて新しい要素鍵 $k'_{i,j}$ を知らせ，n に対しては個別に $k'_{i,j}$ を伝達すれば良い．n に対する個別伝達については，初期化時と同様に，工場等で事前に格納するか，安全な通信路を仮定できる場合

は，その上で配送する．本プロトコルにおいて，サーバにおける暗号化操作と通信の回数は高々2 回，および既存ノードでの復号操作の回数は高々1 回である．なお，n は，d 個のグループに同時に加入しなければならない．従って本プロトコルを d 回繰り返し実行することで対応する．

4. 評価

4.1 想定する応用例

本節では，センサネットワークの有力な応用対象である BEMS[30] を例題とし，実用規模のアプリケーションに提案方式を適用した場合の効果について評価する．BEMS とはビル管理システムであり，ビルの機器・設備等の使用エネルギーや室内環境を把握し，これを省エネルギーに役立てるためのシステムである．ここでは，電気使用量を検針する機能を備えるノードと室内の温度，照度，湿度，人の在不在をセンシングする機能をそれぞれ有するノード，計 5 種類のノードをビル内の複数箇所に設置することを考える．センシング情報を収集する際には，サーバ（検針者）は対象のノードに対して，情報要求のための指令を発行する．指令を受けたノードは，センシングした結果をサーバに送り返す．サーバからノードへのダウンストリームは一対多，ノードからサーバへのアップストリームは一対一の通信となり，共にセンサネットワークで頻出する通信形態である．本研究では，一台のノードとの通信もメンバ数が 1 のグループとの通信と考えるので，一対一の通信の部分についても提案方式を適用可能である．

ネットワークの規模としては，BEMS の需要が高い高層ビルを想定する．具体例として，40 階建のビル 2 棟（A，B 棟），各階には東西南北にフロアが存在するオフィスビルを想定し，各フロアに上記の 5 種のノードを設置し，BEMS を運用することを考える．この時，サーバは以下のようなグループと通信するシナリオを考える．

- 同じ棟に存在するノード全体からなるグループ
- A 棟，B 棟を問わず，同じ階に存在するノード全体からなるグループ

- A 棟, B 棟, 階数を問わず, 同じ方角に存在するノード全体からなるグループ
- 設置場所を問わず同じ機能を有するノード全体からなるグループ
- ある棟の同じ階に存在するノード全体からなるグループ
- ある棟の同じ方角に存在するノード全体からなるグループ
- ある棟の同じ機能を有するノード全体からなるグループ
- ある階の同じ方角に存在するノード全体からなるグループ
- ある階の同じ機能を有するノード全体からなるグループ
- ある方角の同じ機能を有するノード全体からなるグループ
- 個々のノードからなるグループ

4.2 提案方式の適用について

以上のグループへの同報通信を実現するために，ノードを設置する棟，設置階数，設置方角，ノードの持つ機能のそれぞれをノードの持つ属性と考え，各属性毎に分割 A_1, A_2, A_3, A_4 を考える．この時，例えば A 棟の 2 階の東にある温度センサを搭載したノードは唯一であり，提案方式の条件 1 を満たす．ここで各集合族の取り得る要素数は，ビル構造から $m_1 = 2, m_2 = 40, m_3 = 4$ となる．センサの種類に関しては将来の拡張を事前に想定し， $m_4 = 10$ とする．これにより最大で $2 \times 40 \times 4 \times 10 = 3,200$ ノードをネットワークに収容することが可能となる．想定では，各フロアに 5 種類のセンサを設置するので，1,600 ノードが実ノード数になる．この時，適用例における一次グループは図 2.3 に示すような構成となる．すなわち設置する棟に応じ $A_1 = \{G_{1,1}, G_{1,2}\}$, 設置階数に応じ $A_2 = \{G_{2,1}, \ldots, G_{2,40}\}$，設置方角に応じ $A_3 = \{G_{3,1}, \ldots, G_{3,4}\}$，ノードの持つ機能に応じ $A_4 = \{G_{4,1}, \ldots, G_{4,10}\}$ の各集合族が定義され，グループは各集合族から選択する一次グループによって構造化される．4 次グループには高々一台のノードが存在するのみである．したがって，提案方式を適用するにあたっての条件 1

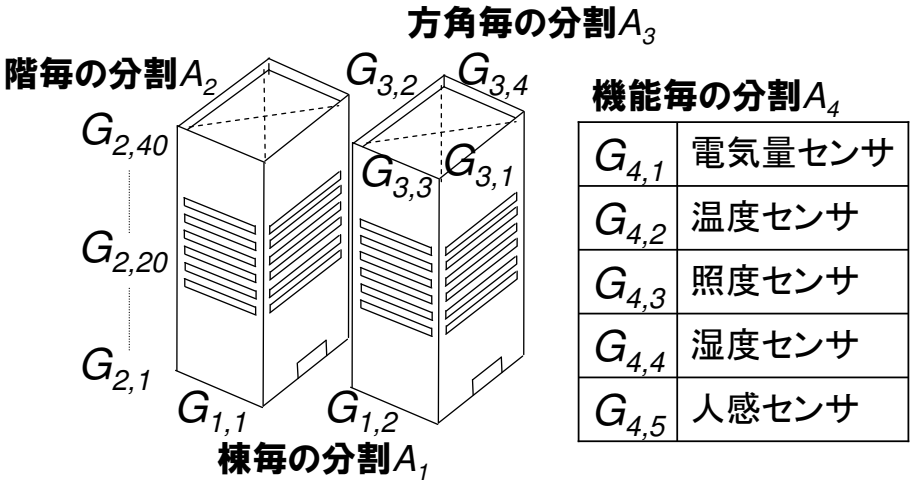

図 2.3. 適用例における一次グループ

を満たす．表 2.3 に，上記シナリオで通信するグループに対応する k 次グループを，そのグループ数および各グループのメンバ数とともに示す.

4.3 既存方式との比較

一台のノードが表 2.3 に示す 11 個の各 k 次グループに同時に加入する想定環境のもと，提案方式と既存方式との比較を行う．なお，表 2.2 において，要件 1，4 を満たさない既存方式については，所定の機能を実現できないと考え，直接的な比較対象とはしない．要件 2，3 の観点で定量的に比較をするにあたって，ネットワーク全体でサーバが管理すべき鍵数とノードが記憶する鍵数についてまず議論する．次に,「鍵更新：月初めに全てのグループ鍵を更新する」,「無効化：脆弱なノードをネットワークから切り離す」といった運用上十分に起こりうる鍵管理を想定し，それらに必要な通信負荷について議論する．提案方式は 3.1 項に示した通り，放送型配信の可能なトポロジに適応することができる．比較においては，簡単のため，既存方式を含め広く適応可能なスター型トポロジを想定して評価する．無線センサネットワークにおいて，サーバを中心とするスター型トポロジを構成する場合，サーバからの送信回数とノードの受信回数は等しくなり，これを比較することで，サーバ，ノード双方の通信負荷を評価できる．また有線センサネットワークにおけるバス型やリング型のトポロジ上に適用しても，同様の議論

表 2.3. 通信する k 次グループ

k 次グループ	グループ数	メンバ数
$G_{1,ji}$	2	800
$G_{2,j2}$	40	40
$G_{3,j3}$	4	400
$G_{4,j4}$	5	320
$G_{1,j1} \cap G_{2,j2}$	80	20
$G_{1,j1} \cap G_{3,j3}$	8	200
$G_{1,j1} \cap G_{4,j4}$	10	160
$G_{2,j2} \cap G_{3,j3}$	160	10
$G_{2,j2} \cap G_{4,j4}$	200	8
$G_{3,j3} \cap G_{4,j4}$	20	80
$G_{1,j1} \cap G_{2,j2} \cap G_{3,j3} \cap G_{4,j4}$	1,600	1

が可能である．

[17], [18] の場合，サーバで管理を要する鍵数はグループ数の総和と等しく 2,129 個となる．また，1 ノードあたりが記憶するグループ鍵数はノードが属しているグループ数と同数の 11 個である．全てのグループ鍵を更新する際，これらの方式では，グループに対して古いグループ鍵で新しい鍵を暗号化して同報すればよいので，グループ数と同数の 2,129 回の通信が発生する．また，一台のノードを無効化する際，無効化するノードを除いたグループに対し，マスタ鍵で新しいグループ鍵を個別に配送する必要があるので，$\sum_{g \in G}(|g| - 1)$ =2,028 回の通信が発生する．ここで，G はある一台のノードが属すグループの集合を，$|g|$ はグループ g のメンバ数を示す．また，マスタ鍵は 4 次グループすなわちメンバ数が 1 のグループにおけるグループ鍵と同義とみなすことができる．

提案方式では，グループ鍵は属性値に紐づける要素鍵から計算できるため，管理の必要となる鍵の個数はサーバ側において属性値の総和 $\sum_{i=1}^{4} m_i = 56$ 個，ノード側においては属性数と同数の 4 個である．56 個の要素鍵を更新すれば全グループ鍵を更新することができるため，グループ鍵更新に必要なサーバの通信回数は高々

$\sum_{i=1}^{4} m_i = 56$ 回である．また，一台のノードを無効化する際，高々$\sum_{i=1}^{4}(m_i - 1) = 52$ 回の同報通信が発生する．

[19] によって，ノード無効化の際のグループ鍵配信を効率化することが可能である．[19] では実験的な評価により，分木数を 4 程度に設定した鍵木を利用することが，効率的であるという結果を示している．以降，鍵木を完全 4 分木で構成するとして評価する．この時，ノードの無効化に必要な同報回数は鍵木の高さの 4 倍として見積もることができるので，考慮しているグループの場合，$\sum_{g \in G} 4log_4|g| \approx 128$，すなわち約 128 回の同報で実現できる．ただし，[19] を適用するためには，管理用の鍵木を定義する必要があるため，管理する鍵数が増加することを忘れてはならない．鍵木の葉頂点に割り当てる鍵は，各ノードだけで構成するメンバ数 1 のグループのグループ鍵と同義であり，鍵木の根頂点に割り当てる鍵はグループに固有のグループ鍵であるので，実際には鍵木の中間頂点に割り当てる鍵を余分に持つ必要がある．この時，サーバが管理する鍵数は，メンバ数が 1 以外のグループの集合を G' としたとき，$\sum_{g \in G'}(\sum_{k=1}^{log_4|g|-1} 4^k) = 10,772$ 個増加する．またノードの記憶する鍵数は $\sum_{g \in G}(log_4|g| - 1) \approx 22$，すなわち約 22 個増加する．さらに，[22] を使用すると，無効化時の同報回数は [19] の $3/4$ の約 96 回と見積もれ，ノードおよびサーバで記憶するべき鍵数もある程度の削減が可能である．ただし記憶しなければならない鍵数の上限値は [19] と変わらず，ノードの実装コスト削減にはそれほど大きくは貢献しない可能性もある．以上をまとめると鍵数および管理上の通信負荷の関係は表 2.4 のようになる．特に，ノードに課される負荷について，値の相対関係を積み上げグラフ (図 2.4) に明示する．なお表 2.4，図 2.4 において，提案方式で要する通信負荷と [22] で管理する鍵数は，必要とされる上限値を示す．

4.4 考察

提案方式は，一台のノードが，表 2.3 に示す 11 個の各 k 次グループに同時に属するときに，既存方式と比べノードのメモリ負荷の 64%〜88%を削減できる．また，スター型トポロジを想定した場合においてサーバおよびノードの通信負荷の 46%〜97%を削減できる．センサネットワークでは，コスト上の問題から大容量

表 2.4. 比較結果

方式	サーバの鍵数	ノードの鍵数	鍵更新負荷	無効化負荷
提案方式	56	4	56	52
[17][18]	2,129	11	2,129	2,028
[19]	12,901	33	2,129	128
[22]	12,901	33	2,129	96

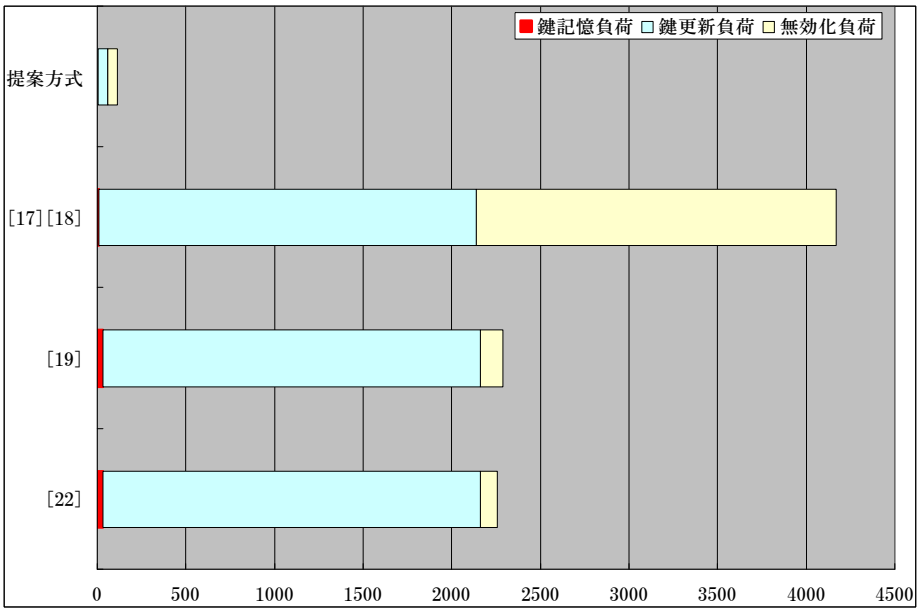

図 2.4. ノードに課される負荷

の（特に耐タンパ性を有する）記憶領域をノードに確保することが困難であることが多いため，鍵のメモリ負荷を削減できる本方式は有効であると考えられる．さらに，通信負荷を削減できることは，電力資源を多用する通信回数を抑えられるという点で，電力資源の限られるノードの長期運用化を実現する．これらは汎用のネットワークに対しても好ましい性質であるが，これを対称鍵暗号の軽量な演算のみで実現できている点が最大の特徴であり，公開鍵暗号を用いずに実現できる点で，特にセンサネットワークに有用と考える．また，鍵更新処理のタイミングに制約を設けておらず，かつサービスに必要なグループを扱える点で要件 1, 4 への対応も実現できており，[23] や [20]，[21] に対する大きな利点と考える．通信負荷についてはスター型トポロジを想定した評価であるが，スター型のトポロ

ジを構成するクラスタが親子関係を持つクラスタツリー型トポロジに適用する場合，クラスタヘッドと呼ばれるノード間で通信を中継することで通信の到達距離を長くすることが可能である．ただし，クラスタヘッドではリピータハブ的に受信したデータをそのまま転送する（再暗号化はしない）．このクラスタツリー型トポロジへの適用については，詳細には追加の条件を仮定して実験を行う必要があるものの，少なくともサーバ近辺のノードに関してはスター型と同様に受信負荷の軽減が期待される．さらに，クラスタツリーの各クラスタでも同等の効果が期待されるため，全体としての受信負荷の軽減に繋がると考えられる．予備的検討 [31] においても，実ノードで構成するクラスタツリートポロジに対し，鍵更新の効率化を図れることも確認している．また，メッシュ型のネットワークトポロジにおいても，ルーティングテーブルの構築のためにブロードキャストが用いられることが多く，これを利用することでメッシュ型のトポロジ上に提案方式を適応できる可能性も考えられる．これらのトポロジにおいてはブロードキャストの効率性が性能に影響するため，ブロードキャスト効率化を実現する手法 [32]，[33] 等を用いた上で提案方式を用いることが望ましい．

また，グループ鍵を動的に計算で導出する際のオーバヘッドについて考察する．提案方式では，表 2.4 に示したようにノードが静的に持つ鍵の数は削減されるが，その都度一方向性ハッシュ関数を用いて動的にグループ鍵を計算するため，ノードの計算負荷は増加する．これに関して [18] に，ノードの必要とする電力の 98%が計算負荷からでなく，通信負荷によるものであることが明記されている．[18] の計算は対称鍵暗号に基づいており，これは提案方式で用いる一方向性ハッシュ関数の計算コストと同等であることから提案方式に関しても同様のことが言えると考えられる．従って，計算負荷の若干の増加はあるものの，通信負荷の削減効果が大きく得られる提案方式が，電力コストの大幅な削減を可能とする点でメリットが大きいと考えられる．

次にグループ構成の変化に関する感度について考察する．適用例では，収容できるノード数を $3,200$ ノードまで考慮している．結果，グループ数は最大で $3,964$ 個に，1 グループあたりのメンバ数は平均で約 134 個増加する可能性がある．既存方式においては，管理すべき鍵数や通信負荷がグループ数または各グループの

メンバ数に応じて増加するが，提案手法においては，表 2.4 に示す値から変わることはない．すなわち，提案手法は，システムの運用前において，そのスケールを十分に検討する必要があるが，スケールさえ適切に選ばれていれば，その範囲内において非常に良好なスケーラビリティを持つということができる．

最後に，提案方式の前提条件と安全性との関係について考察する．提案方式は要素鍵の組合せで高次グループのグループ鍵を導出するため，前提条件が満たされない場合，異なるノード内部の要素鍵の同時流出によって，高次のグループ鍵の安全性が損なわれる可能性がある．一方，本前提条件が満たされない場合，[19], [22] においても，鍵木の節点に紐つける鍵が複数漏洩し，それぞれで主張されているような安全性や効率性を確保することが困難になる．その意味で，提案方式と，[19]，[22] との違いは，前提条件を明示的に扱うか（提案方式）暗黙のものとするか（[19]，[22]）という性質のものであり，必要とする前提条件は共通である．[17]，[18] との比較においては，前提条件は提案方式特有のものとなる．しかしながら，BEMS 等の応用を想定すると，これらの条件は比較的容易に満たすことができ，その場合，提案方式がより効率的に作用すると考えられる．従って，提案方式の導入時には，これら前提条件を達成するための運用上の仕組みをあわせて検討する必要がある．例えば，加速度センサ等を使って，ノードが持ち出されたことをノード自身で警報するような運用技術 [34] の導入等が有効と考えている．

5. おわりに

本章では，ノードが自身の属性の組合せに応じて同時に複数のグループに加入する可能性が高い点に着目し，属性に紐づける管理情報を用いて複数のグループ鍵の管理の仕組みを互いに連携させ，複数グループのグループ鍵管理を効率化するグループ鍵管理方式を提案した．また，適用例を与え，既存方式と比べノードのメモリ負荷の 64%〜88%，および通信負荷の 46%〜97%を削減できることを示した．適用例においては，ノードの設置場所や機能を属性としてグループを構成することを検討したが，その他の属性を採用することも可能である．応用に際し

て，効率的で有効な属性構造を構築することは重要であり，そのための指針を検討することは運用にあたっての今後の課題である．少なくとも運用における属性の選択時には，その属性値によってできるだけノードを均等に分割できる属性を選択できることが望ましい．また，複数のトポロジを想定した実験によりノードの通信負荷を詳細に評価すること，およびノード無効化プロトコルの通信回数を下界に近似するアルゴリズムの検討も興味深く，今後の検討課題とする．

第3章　行動・状況の類似度に基づく共通鍵生成法

1. はじめに

モバイル機器の性能向上により，実空間上の様々な局面でアドホック通信を行うことが可能となってきている．このようなアドホック通信において，商業的価値の高いコンテンツや，プライバシ保護の必要なライフログ等の送受信が，今後益々増大していくと予想される．有線通信や基地局を介した無線通信の場合とは異なり，アドホック通信の安全性を実現するために，固定もしくはキー入力による PIN コードやパスワードの利用が一般的となっている．しかし，この鍵長は概して短いにも関わらず，鍵の設定は一般ユーザには煩わしい．一方，セッションごとにまたはデバイス対ごとに鍵を設置する通常の共通鍵暗号を利用すれば安全性は向上する．しかし予め共通鍵を生成して何らかの安全で確実な手段で生成した鍵を事前配布する必要もあり，携帯端末間でのアドホック通信においては利便性に欠ける．そこで将来のアドホック通信の利用拡大に鑑みて安全性を損なうことなく使い易さを向上させる鍵共有法を開発することが望まれる．

機器間に安全なアドホック通信路を構築することをセキュアデバイスペアリング (SDP) と呼ぶことがある．SDP を実現する手法として，人体通信 (Body Area Network, BAN) 等の新しい通信技術を用いる手法 [35, 36] と，人間の動作のセンシング情報に基づく手法とが注目されている．BAN は人体を高電圧微小電流による送受信路として利用した通信方式であり，携帯端末によるキーレスエントリーや，握手による名刺交換など種々の応用が期待される一方，EMC(Electro-Magnetic Compatibility) の問題等，解決すべき課題もある．また，キーレスエントリーに代表される BAN のセキュリティ保全への応用においては，人体を通信路として用

いてはいるものの，秘密通信に必要な鍵情報をあらかじめ何らかの方法で事前配布しなければならないという点では従来手法と同様である．

これに対し，加速度センサ等の計測情報を一種の端末固有情報として利用することにより，安全に通信し合える端末同士であることの確認や，鍵事前配布のオーバヘッドの減少を目的とした試みがいくつかなされている．[37] [38] では周波数領域上での類似尺度であるコヒーレンス，[39] では量子化高速フーリエ変換 (FFT) を用いて，複数のセンシングデータが同一人の動作によるものかどうかを高い精度で判定する手法を示している．[40] では，2 つのセンサを手にもって振ったときの加速度データに対して，時間領域で主成分分析を行い，鍵生成を行う手法を提案している．また [41] では，コヒーレンス及び量子化 FFT を利用して鍵生成を行う手法を提案している．しかし，これらの手法を用いて鍵生成を行うためには，ユーザがセンサを 2 つ合わせて強く振る必要がある．セキュリティ強度の高い鍵を生成できる反面，端末台数が増加した場合や多数のユーザの端末を想定した場合などでは利便性の面で問題がある．高い利便性を達成するためには，通信時の鍵生成について以下のような条件を達成できることが望ましい．

(1) **日常的な動作による鍵生成：**センサを重ねて強く振るという動作を行わなくても，握手をする，並んでしばらく歩く，自動車に同乗する，といった自然で日常的な動作を行うだけで鍵共有が行えれば，ユーザにとってさらに可用性や親和性が増すと期待される [42]．また [43] では，歩行，走行，自動車や電車内にいる状態の加速度パワースペクトルにはそれぞれ際立った特徴があることが報告されている．位置情報を用いて同行判定を行う方法も提案されているが [44]，2 節で述べるように位置情報等の付加情報がなく加速度データ単独であってもかなりの精度で動作の類似度判定が可能であることがわかっている．

(2) **鍵強度の調節：**電子化名刺データやメールアドレスを交換する場合のように高いセキュリティ強度が求められるものから，ゲームのために一時的にデータを交換する場合のようにそれほど高いセキュリティ強度が必要ないものまで，種々の応用場面が考えられる．ここで，同一の暗号方式におけるセキュリティ強度は，鍵長と鍵ランダム性 (あるいはエントロピー) で定

量化できるとみなせるので，高いセキュリティ強度が求められる場合は非常に類似した動作である場合に限って (長い) 鍵を生成でき，そうでない場合は，鍵長は比較的短くてよいが，ある程度似た動作を継続すれば鍵生成が可能であることが望ましい．

そこで，本研究ではこれらの目標を実現するための，加速度センサに基づく新しい鍵生成法を提案し，その有効性を確認する．まず，類似度が必ずしも非常に高くはないデータからでも鍵生成が可能となるように，時間領域上の分散値に基づく鍵生成法を新たに提案する．この手法では加速度分散値の時系列データを動的に追跡し，先行する時区間での分散値の平均値をベースラインとして分散値の量子化を行う．これにより,「分散値の変化率」に基づき，少ない計算量で，かつ，2 つの動作間の差異を吸収して，多くの場合，同一の値に量子化できる．

また，日常動作から鍵生成を行う場合は，センサを強く振る場合に比べてセンシングデータの変化量が小さいため，類似動作対に対して共通鍵を生成しない確率 (false negative) や，非類似動作対に対して共通鍵を生成する確率 (false positive) が高くなる傾向がある．一方，完全に一致するデータ列を生成しなければならない鍵生成よりも類似度をある程度の信頼度で定量化することのほうがはるかに容易である．そこで鍵生成に先立って，2 つの加速度データの時間領域上での分散値の差分，および，コヒーレンス値を用いて類似度を 2 段階で区分し，鍵生成の可否や鍵生成法の選択を行うことで，false positive を減少させ，かつ鍵長の制御を行う．

量子化 FFT は [41] の手法に基づくが，日常的な動作の場合，仮にコヒーレンス値が高くても，手で振る場合に比べ動作のエネルギーが小さいため 0Hz 付近の重力加速度およびノイズが原因で鍵一致率は非常に低い．そこで，wavelet 変換や量子化幅の調整によって，ノイズの除去を行う．

以上の提案アルゴリズムの有効性を，被験者による実動作データに基づいて評価した．まずセンサを振る動作による予備実験を行った後，歩行や自動車への乗車など，日常動作を対象とした実験を種々行った．これらの実データを入力とし，類似度による分離能力，時間当たりの生成鍵長，鍵ランダム度を計測した．その結果，自動車への乗車の場合は 1 分間に約 217.7 bit 相当の，歩行動作では約 2 分

間で Bluetooth の PIN コード (13 bit) 相当の鍵が生成できることがわかった．このことより，分散値差分とコヒーレンスを用いた分離は鍵生成の前処理として false positive を抑えるのに有効であること，日常的な動作からもある程度の鍵長とランダム性をもつ鍵生成と鍵共有が行えること，さらに，セキュリティ強度の要求に応じた鍵生成が可能であることがわかった．

以降，本章では，人間の動作から鍵生成を行う先行研究である [40] と [41] を中心に関連研究を 2 節で紹介した後，3 節で提案手法を詳しく述べる [45]．次に種々の動作の加速度データに基づく実証実験の詳細とその結果および得られた知見について 4 節で述べ，5 節で結論と今後の課題を述べる．

2. 関連研究

加速度センサ等の計測情報を一種の端末固有情報として利用することにより，安全に通信し合える端末同士であることの確認や，鍵事前配布のオーバヘッドの減少を目的とした試みがいくつかなされている．これらの手法は，計測情報に対して時間領域解析を用いる手法と周波数領域解析を用いる手法に大別できる．また，加速度センサ等の計測情報を解釈して，ユーザの行動や状況 (コンテキスト) を推定する研究も関連する．以下にそれらのうち代表的なものを紹介する．

2.1 時間領域解析を用いる手法

[46] では，加速度，角加速度の時系列データをあらかじめ登録しておいたデータと比較し，個人認証を行う手法を提案している．[47] , [48] では共分散・相関係数を用いる手法を提案している．特に [48] では，類似したセンシング履歴をもつセンサは同一グループに属するとみなし，グループ内で安全に情報を共有する手法を提案している．具体的に，加速度データの時間領域上の相関係数を計算することによって同一の行動（移動）履歴をもつセンサとそれ以外のセンサを実用上十分な精度で分離できることを示している．

[40] では，2 つのセンサを同時に振ったときの加速度データに基づいて鍵生成を行う手法を提案している．この手法では，時間領域データを区間分割・主成分

分析・量子化・連接して鍵生成を行っており，センサ間で鍵事前格納や前処理のための通信をまったく必要とせず，完全に局所的に鍵生成を行って鍵共有が可能であることを初めて示した点で注目に値する．200Hz のサンプル周波数で計測した 5 秒間の 88 サンプルに基づく実験結果では，同時に振った 2 台のセンサが，Bluetooth PIN コード相当（13 ビット) の同一鍵を生成できる (true positive) 確率は 80% 以上 (従って，false negative の確率は 20% 以下) であり，その際に，同時に振っていない 2 台のセンサが同一鍵を誤って生成する (false positive) 確率は 1.3% であると報告されている．

2.2 周波数領域解析を用いる手法

[37] では周波数領域上での類似尺度であるコヒーレンス，[39] では量子化高速フーリエ変換 (FFT) を用いて，複数のセンシングデータが同一人の動作によるものかどうかを非常に高い精度で判定する手法を示している．2 つの周波数領域データのコヒーレンスとは，各周波数の正規化クロスパワースペクトル (複素内積値の平均を正規化したもの) を，あるカットオフ周波数まで積分 (離散の場合は加算) した値である．量子化 FFT とは，FFT の結果得られた各パワースペクトルを適切な方法で量子化したものである．

[41] では，[40] と同様に，センサを手で振ったときの加速度データに基づいて鍵生成を行うが，周波数領域上での特徴量を利用している点が異なる．具体的な特徴量として，上述したコヒーレンス [37] と量子化 FFT [39] の 2 つを採用しており，それぞれの特徴量を利用した鍵共有プロトコルを 2 つ提案している．1 つ目のプロトコルは，Diffie-Hellman の鍵共有プロトコル [28] におけるインターロック (鍵共有が man in the middle attack 等で攻撃されていないかを検証するプロトコル) を改良したものである．鍵検証においてセンシングデータを交換し，コヒーレンスを計算してその値が十分大きいならば鍵共有に成功したと判断する．51 人の被験者による約 5 秒間の合計 1530 サンプルに対して，コヒーレンスの閾値を 0.72 としたとき，false positive 0%, false negative 10.24% の性能を得ている．一方，2 つ目のプロトコルではまず，センシングされた時間領域データを小区間ごとに周波数領域へ変換してスペクトルを量子化し (量子化 FFT)，あるカットオフ

周波数まで連接する．そしてこれを鍵小片とよぶ．量子化においてはパワースペクトルの比較的小さい周波数における係数を特徴量に反映させるため量子化幅を指数的に取る．また，誤差による変動を吸収するため，量子化境界を変化させて鍵小片の候補値を数個生成する．次に小区間ごとに鍵小片の候補値を一方向ハッシュ化して交換し，相手と一致した鍵小片を連接したものを最終的な共有鍵とする．ただし鍵小片の一致率 (小区間の総区間数に対する鍵小片が一致した比率) があらかじめ定めた閾値より小さい場合は，異なる動作であると判断して鍵生成は行わない．一致率の閾値を 84%としたとき，160 対以上のサンプルに対して false positive 0%, false negative 11.96% の性能を得ている．以上の通り，[41] では，[40] に対して，鍵小片のハッシュデータを交換しなければならないという欠点はあるが，非常に性能が優れており，我々の追試においても，センサを片手にもって強く振るという動作に関しては，性能の頑健性，再現性が高いことがわかっている．

2.3 コンテキスト推定の研究

ある時間長のセンサ計測情報を解釈し，いくつかのコンテキストに分類する研究として，[49] や [50] が代表的である．ここでコンテキストはユーザの行動や状況を表し，高々数十種類に分類される．[49] は身体の 5 箇所につけた加速度センサで 20 の行動を推定する．[50] は加速度，マイク，GPS を用いて乗り物を含む 7 つの移動状況を推定する．本章の目的である鍵生成を想定する場合，これら分類数はエントロピーの観点で不足する．つまり，これら関連研究において同じコンテキストに分類されるセンサ計測情報に対しても，より粒度を細かく分類できる必要がある．この時の分類は，コンテキストを必ずしも説明できなくともよい．

3. 提案手法

3.1 アルゴリズムの概要

鍵生成において安全性の観点から重要なのは，類似しない動作対に対する共通鍵の生成 (false positive) をできる限り避けることである．しかし，歩行等の自然

な動作の加速度は変化量が小さい．このようなデータに対して，類似度が高いときかつそのときのみ共通鍵 (完全に一致したデータ列) を生成するのは困難であるが，一方，類似度だけを定量的に算出することは比較的容易である．そこで提案手法では，加速度の分散値とコヒーレンスという 2 種類の類似度によりデータ対の分類を鍵生成に先立って行うことにより，無駄な周波数領域への変換を省きつつ，false positive を低く抑える．提案する鍵生成手法全体の流れを図 3.1 に示す．以下に，その概要を説明する．

(1) 加速度の時系列データを区間分割し各区間の分散値を取ることにより，動作の種類をある程度推測できることが予備実験により確認できた．そこで，加速度の時系列データ対に対し，区間ごとにそれらの分散の差分の絶対値を取り閾値と比較する (図 3.1 の 1 つ目の条件判定)．閾値より大きければ鍵生成は行わず，以下であれば，(2) に進む．

(2) コヒーレンスは，2.2 項で述べたように周波数領域上の類似尺度であり，0 以上 1 以下の実数値を取り，各周波数の振幅と位相の双方が類似しているほど，1 に近づく．加速度の時系列データを区間分割し各区間を周波数変換する．次にそれらのコヒーレンス値を求めて平均値を取り，閾値と比較し (図 3.1 の 2 つ目の条件判定) ，閾値より大きければ量子化 FFT を用いて比較的長い鍵を生成し，そうでなければ分散値を用いて比較的短い鍵を生成する．

なお本研究では，[40] や [41] と同様，実装が容易かつ計算量が小さい手法をめざし，3 軸の加速度値から求めた加速度ベクトルの大きさ (3 軸の加速度値を x, y, z とした場合，$\sqrt{x^2 + y^2 + z^2}$) のみを用いて解析を行っている．ただし，磁気センサとジャイロ (角加速度) センサのセンシングデータと組み合わせることにより，加速度センサの 3 軸を地球固定軸に変換し，重力加速度の影響を消去することは原理的に可能であり，実用的な改良法 [51] も提案されている．

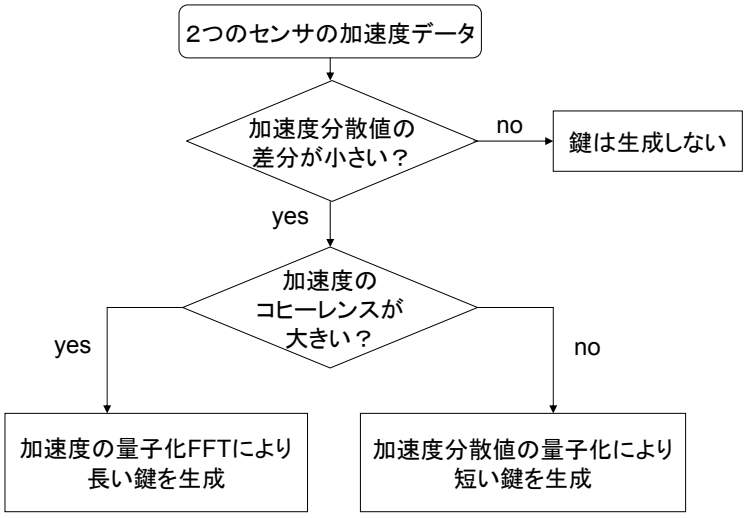

図 3.1. 鍵生成の流れ

3.2 類似度を利用した動作の分離

分散値による分離

加速度データは，動作によってその揺らぎが異なる．人間の歩行や走行などの揺らぎの大きい動作の場合は，各行動によって加速度の分散値に違いが現れる．そこで 2 つのセンサの加速度分散値を比較し，その差分が小さい場合には類似した動作を，差分が大きい場合は異なる動作をしているとみなして，異なる動作をしている場合を分離する．分散値の時間変化を求めるために，図 3.2 のように加速度を区切り，分散値を求めていく．各センサで取得した波形データを n 分割し，その k 番目の区間の t 番目のデータを $a_k(t), b_k(t)$ で表す．また $a_k(t), b_k(t)$ の平均を $\hat{a_k}, \hat{b_k}$ としたとき，区間 k の分散とその差分を以下の通りに求める．

$$v_{a_k} = \frac{1}{W_{var}} \sum_{t=1}^{W_{var}} (a_k(t) - \hat{a_k})^2 \tag{3.1}$$

$$v_{b_k} = \frac{1}{W_{var}} \sum_{t=1}^{W_{var}} (b_k(t) - \hat{b_k})^2 \tag{3.2}$$

$$Diff = |v_{a_k} - v_{b_k}| \tag{3.3}$$

この $Diff$ を各動作の類似度とし，これがある閾値を越えるかどうかで類似動作を分離する．

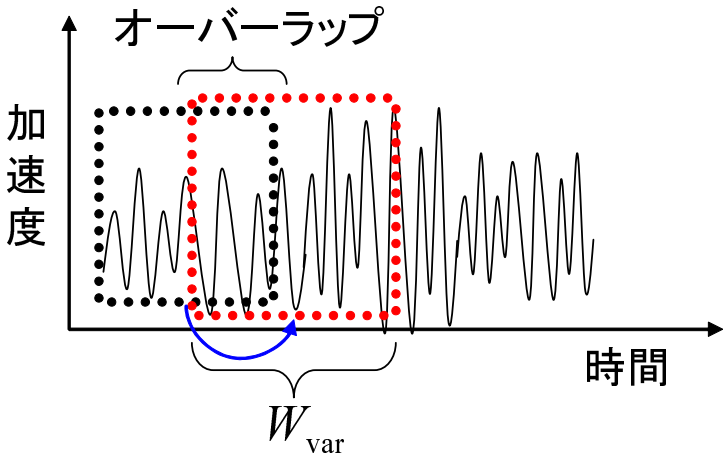

図 3.2. 区間分散の計算

コヒーレンスによる分離

分散値の差分では分離されないような似た動作対に対し，コヒーレンスを用いて類似度の判定を行う [37, 41]．まず，各センサの取得した波形データを n 分割し，その k 番目の区間の t 番目のデータをそれぞれ $a_k(t)$，$b_k(t)$ で表す．次に $a_k(t)$，$b_k(t)$ に対して，hann 窓関数 $h(t) = \frac{1-\cos(2\pi t/w)}{2}$ を用いた短時間フーリエ変換 (STFT) を行って，それぞれ各区間 k でのフーリエ係数 $x_k(f) = FFT(a_k(t) \cdot h(t))$，$y_k(f) = FFT(b_k(t) \cdot h(t))$ を得る．この x，y のクロスパワースペクトル $P_{xy}(f)$ は以下のように表すことができる ($\bar{y_k}(f)$ は $y_k(f)$ の共役複素数)．

$$P_{xy}(f) = \frac{1}{n}\sum_{k=0}^{n-1} x_k(f)\bar{y_k}(f) \tag{3.4}$$

このとき，コヒーレンスの値は以下のように算出される．

$$C_{xy}(f) = \frac{P_{xy}(f)}{P_{xx}(f)P_{yy}(f)} \tag{3.5}$$

しかし，本研究では図 3.1 のようにコヒーレンスによる分離を鍵生成に先立って行うという手順をとる．よって上記のように波形データ全体に対するコヒーレンス値を算出することは，遅延の増大や追従性の低下を意味する．そこで，データを区間分割し各区間でのコヒーレンスを算出する．本手法では，図 3.3 のように，

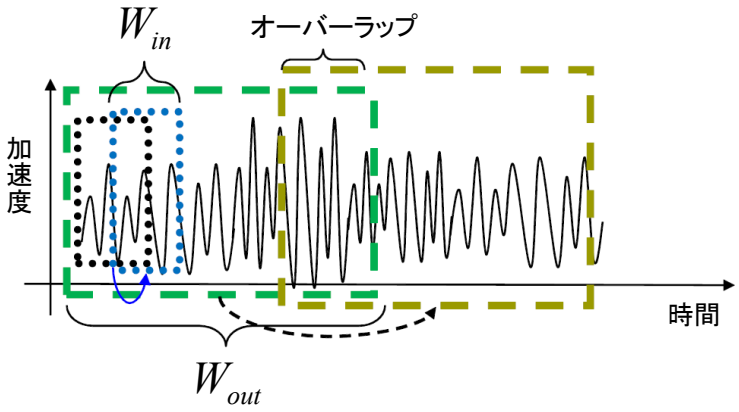

図 3.3. 区間コヒーレンスの計算

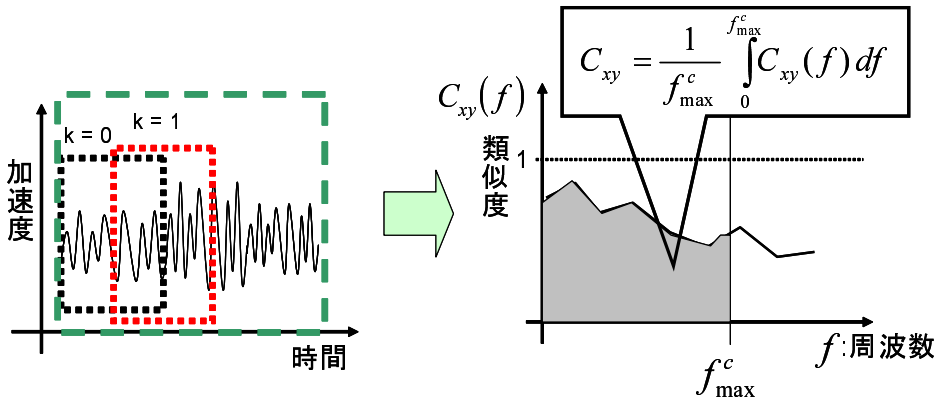

図 3.4. 類似度の計算

二重窓を用いた区間コヒーレンスを計算する．ここで，W_{out} は区間コヒーレンスを算出する区間 (外側の窓) のサイズを表し，W_{in} は上述のコヒーレンス計算における n 分割した区間 (内側の窓) のサイズを表す．また，加速度データの類似度を精査するために外側の窓，内側の窓の双方共に一定量のオーバーラップを設ける．

このようにして算出された各周波数帯のコヒーレンス値について，図 3.4 のように，観測する周波数帯の最大値 (カットオフ周波数と呼ぶ)f^c_{max} を設定し，f^c_{max} までの平均を計算する．

$$C_{xy} = \frac{1}{f^c_{max}} \int_0^{f^c_{max}} C_{xy}(f)dt \tag{3.6}$$

この C_{xy} を x，y 間の類似度とする．

3.3 鍵生成

パワースペクトルからの鍵生成

ここでは [41] で提案されている，以下の量子化 FFT に基づいた方法を改良した鍵生成法を述べる．

(1) 加速度の時系列データをサイズ W_{fft} の小区間 (矩形窓) に分割する．ただし窓は一定の度合でオーバーラップさせる．

(2) 窓内の波形に対して FFT を行い，得られたパワースペクトルのうち周波数 f^q_{max} までを量子化する．低周波が大きく，以降は小さい値に密集するパワースペクトル値の特徴を保存するため，窓内の最大値を基準にし量子バンド幅 (量子化の境界幅) を指数的に増加させる．量子バンド数 (量子化後の値の種類) b は経験的に $b = 5, 6$ 程度がよいとされており，提案法でも予備実験の結果，$b = 5$ を採用した．さらに，量子バンドの境界線付近の値が異なる量子値となるのを防ぐため，量子バンドを適当な定数 α ずつ c 回増加させ，c 通りの量子値を算出する．

(3) 周波数毎の量子値を f^q_{max} まで連結して特徴ベクトルとし，一方向ハッシュ化して互いに交換する．$c \times c$ 通りの特徴ベクトルの組み合わせのうち，一つでも一致するものがあればそれを鍵小片とする．

(4) 鍵小片が得られた窓数の総窓数に対する割合 (一致率とよぶ) が閾値以上であれば，得られた鍵小片を全て連結したものを共通鍵とする．そうでなければ鍵生成は行わない．

センサを重ねて振った場合を鍵生成すべき状況，それ以外を鍵生成すべきでない状況と仮定した場合，上記の手法は優れた性能を発揮する [40]．しかし，日常的な動作の場合，動作量が微小なため性能が劣化してしまう．そこで提案法では量子化について以下の改良を行った (図 3.5).

- 加速度データの低周波には重力加速度等の不要成分が含まれる．そこで Haar wavelet 変換により直流成分と高周波成分を除去し，窓関数 (hann 窓) を作用させてから FFT を行う．

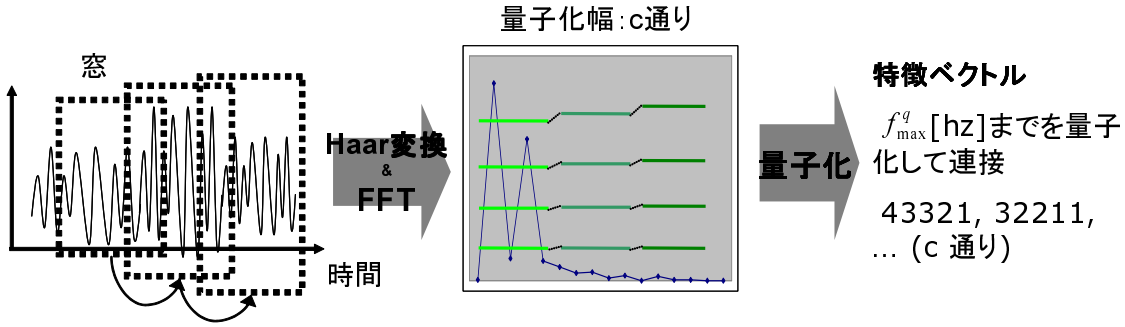

図 3.5. 量子化 FFT の改良

- もはや低周波帯のスペクトルがほとんどないので，量子化値が偏るのを防ぐために，量子化幅は指数的にではなく等間隔に増大させる．

分散値からの鍵生成

分散値は同じ動作が続けば単調な値を示し，歩行 → 停止や，歩行 → 走行など動作が変化した場合は，図 3.11 のように分散値も激しい変化を示す．提案法はこの特徴に注目し，走行中や歩行中のように同じ動作が連続して分散値の変化が単調になっている部分からは同じ量子値を生成する．また激しく変化した部分からは，その変化に見合った値を生成する．

鍵生成の手順は以下の通りである．なお分散値は，3.1 項の手法で求めたものを使用する．

(1) 分散値の分割：分散値の時系列データをサイズ W_{qnt} の小区間 (窓) に分割し一定の度合でオーバーラップさせる．また，量子化に必要な境界線のベースラインを決定するために W_{qnt} より過去の分散値を，サイズ W_{pre} だけ抜き出す．

(2) 境界線の設定：W_{pre} の平均値を基準に，図 3.6 のように等間隔の境界線を引き，b 個の量子バンドを設ける．そして W_{qnt} での平均値が含まれている量子バンドに割り振られた値で量子化する．そして 3.3 項の (2) と同様に量子バンド幅を α ずつ増加させ，c 個の候補を生成する．

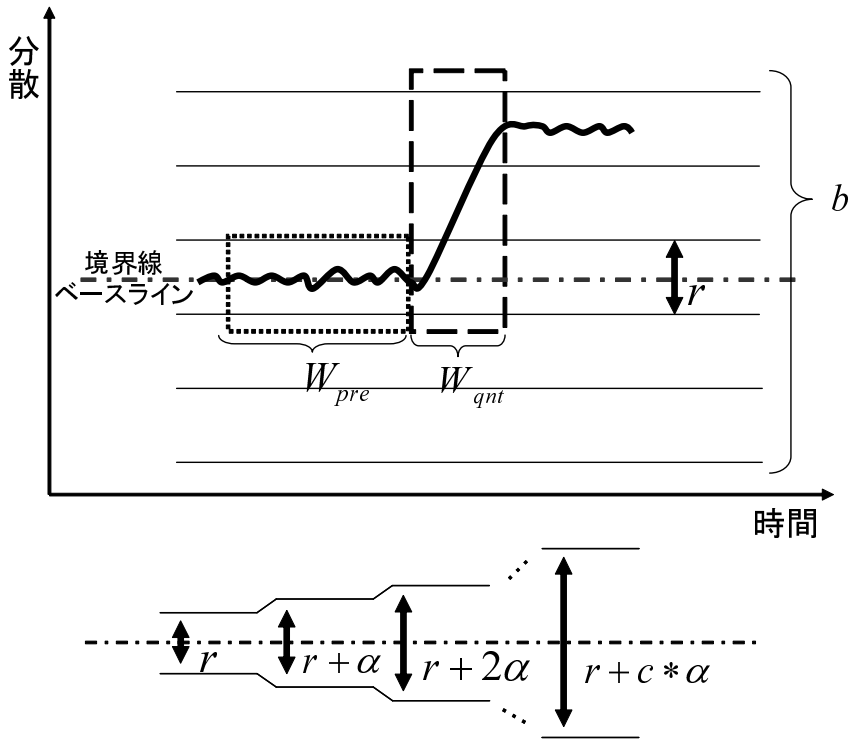

図 3.6. 分散値量子化

(3) 特徴ベクトルの生成：求めた 2 センサの量子値を 1 桁ごとに比較した場合，W_{qnt} での平均値に大きな差があるような類似していない動作でも，候補値のどれか 1 つが高確率で一致してしまう (false positive)．そこで比較する際には，量子値の時間変化を考慮することにした．求めた量子値を順に L 個連結させた後に比較することで false positive の割合を低く抑えた．ただし連結するときは，同一の量子バンド幅で求めた量子値同士を連結させる (よって連結後も候補数は c 個である)．この連結した L 個の量子値を特徴ベクトルとする (図 3.7).

(4) 特徴ベクトルの比較：3.3 項の (3)，(4) と同様に，一致した特徴ベクトルを連結して共通鍵とする．

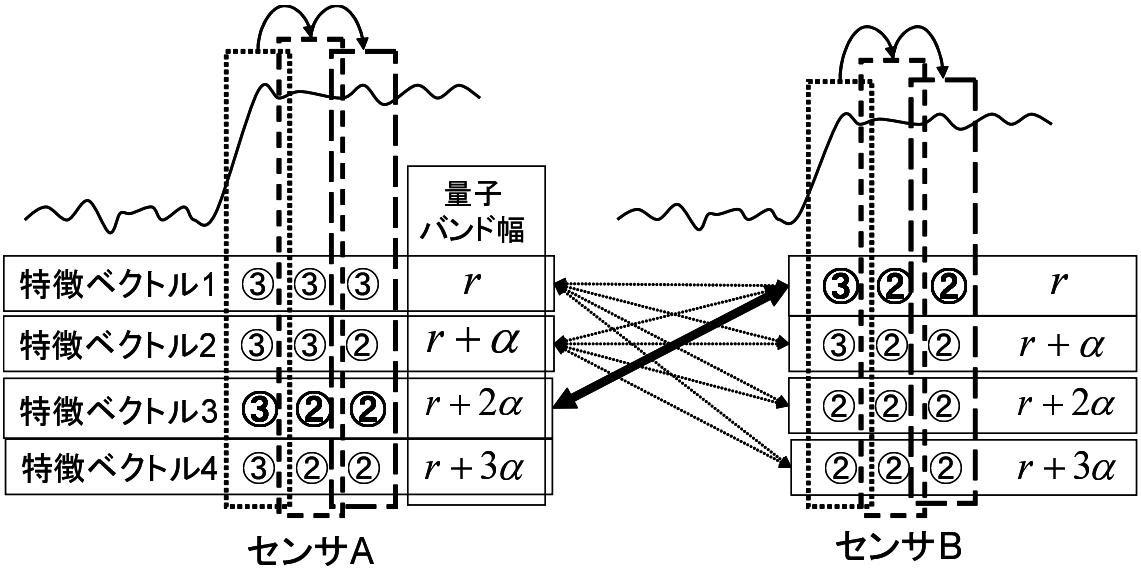

図 3.7. 特徴ベクトル生成

4. 評価実験

4.1 実験環境

本実験では，動作の加速度計測に 表 3.1 のような仕様の 3 軸加速度センサ (Wireless-T 社製 WAA-001) を使用した．加速度センサのサンプリング率は 50Hz に設定して各実験の計測を行った．センサは各被験者の胸と腰の 2 ヶ所に装着し，データ収集用のノート PC を 1 台持たせ，データを Bluetooth を用いて PC に送信する．

表 3.1. 加速度センサの仕様

サイズ	38 × 39 × 10mm
重量	17g
検出軸数	3 軸
検出範囲	±3G
最大サンプリング率	200Hz

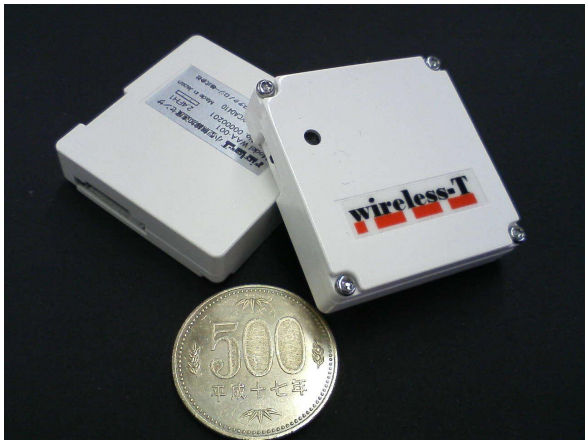

図 3.8. 加速度センサ

4.2 実験動作とシナリオ

歩行実験　3 人の被験者が 30 分程度，同じルートを移動したときの加速度を計測した．

> 具体的なルートは，本学正門 → 北大和地区センター (折り返し) → 正門 → 情報科正面玄関 → エレベータ → 情報基礎学講座 である．

街中を移動している状況を再現するため，計測中は歩行だけではなく，走行や停止といった動作も行った．また被験者には以下のような役割を与えた．

- **先導**　：ルートを好きなペースで移動する．
- **並行**　：先導役に並び歩調を合わせて移動する．
- **自由**　：誰の歩調も意識せず先導役の周辺 (20〜30 メートル）を自由に動き回る．

このときに計測した加速度データを図 3.9 に示す．

乗車実験　3 人の被験者が 2 台の自動車に分乗し，10 分程度のルートを移動したときの加速度を測定した．

> 具体的なルートは，情報科学研究科来客駐車場 → 素盞嗚神社 → 鹿ノ台中 → 鹿ノ台郵便局 → 鹿畑町交差点 → 国道 163 号線 → ローソン → スタート地点 である．

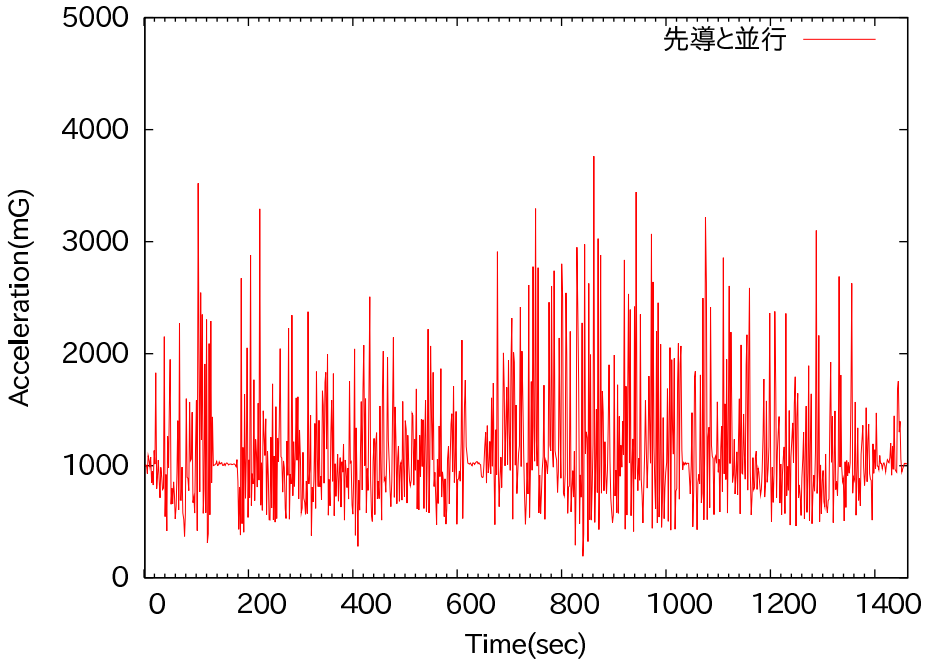

図 3.9. 加速度:歩行

被験者 3 人には以下のような役割を与えた.

- **先導** ：ルートを先導する車に乗る.
- **同乗** ：先導役と同じ車に乗る.
- **追走** ：先導役が乗る車を追走する車に乗る.

このときに計測した加速度データを図 3.10 に示す.

4.3 評価結果

分離について

実験では胸と腰の加速度データに特に大きな差は見られなかった．そこで本論文では，主に腰のセンサから得られた加速度データを用いて提案法の検証を行う．また各実験データは完全に時間同期されていると仮定する.

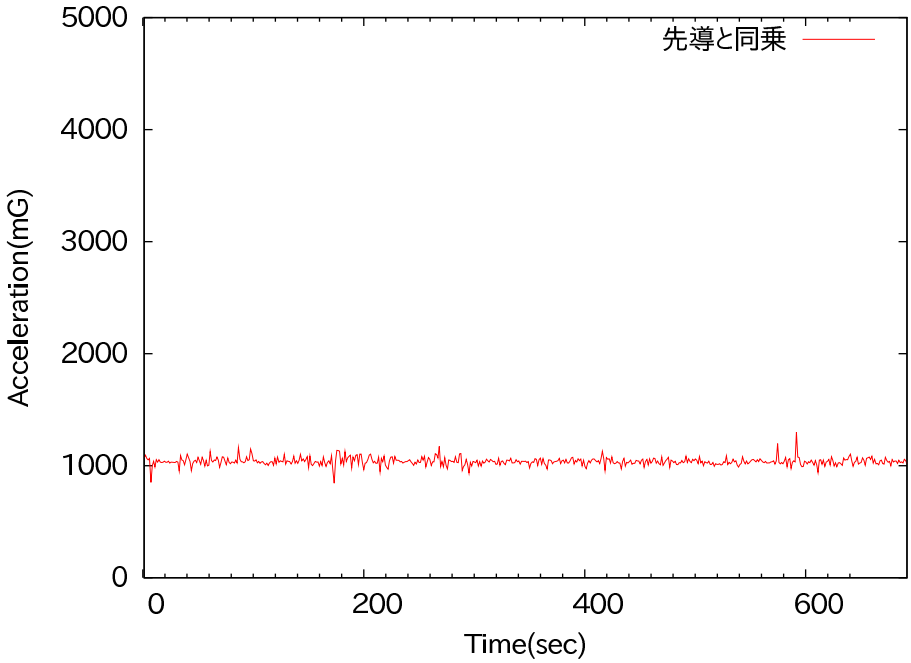

図 3.10. 加速度:乗車

分散値の差分による分離を行うために，分散値を求める窓サイズを $W_{var} = 150$, 窓のオーバーラップを 50% に固定し，分散値の差分の平均を求めた．歩行動作の先導役と並行役の分散値とその差分を図 3.11 に，先導役と自由役の分散値とその差分を図 3.12 に示す．また乗車動作の先導役と同乗役の分散値とその差分を図 3.13 に，先導役と追走役の分散値とその差分を図 3.14 に示す．参考のために，歩行と乗車の両動作で，先導役が装着している腰と胸のセンサの分散値とその差分を図 3.15, 3.16 に示す．このときの差分の平均値は表 3.2 のような結果となった．

表 3.2. 分散値の差分平均値

歩行実験			乗車実験		
並行	自由	先導の腰と胸	同乗	追走	先導の腰と胸
0.325	1.187	**0.294**	**0.231**	0.607	**0.182**

一方，コヒーレンスによる分離を行うために内窓と外窓のサイズを $W_{in} = 64$, $W_{out} = 512$，窓のオーバーラップを 50% に設定し，比較する周波数帯の上限値

f^c_{max} を変化させてコヒーレンスの値を求めた．歩行動作の先導役と並行役のコヒーレンス値の時系列変化を図 3.17，先導役と自由役の時系列変化を図 3.18 に示す．また，乗車動作の先導役と同乗役のコヒーレンス値の時系列変化を図 3.19，先導役と追走役の時系列変化を図 3.20 に示す．参考のために，歩行と乗車の両動作で，先導役が装着している腰と胸のセンサのコヒーレンス値の時系列変化を図 3.21,3.22 に示す．このときの各動作のコヒーレンス平均値は 表 3.3 のような結果となった．

表 3.3. コヒーレンスの平均値

	歩行実験			乗車実験		
	並行	自由	先導の腰と胸	同乗	追走	先導の腰と胸
f^c_{max}=5Hz	0.135	0.109	0.473	**0.647**	0.108	**0.762**
f^c_{max}=10Hz	0.107	0.091	0.437	**0.670**	0.097	**0.688**
f^c_{max}=15Hz	0.098	0.083	0.393	**0.615**	0.092	**0.558**
f^c_{max}=25Hz	0.096	0.080	0.337	**0.538**	0.088	**0.483**

鍵生成について

パワースペクトルを用いる手法の各パラメータを表3.4 のように設定し，パワースペクトルからの鍵生成を行った．分離によってこの鍵生成法が適用される主な動作は乗車であるが，手法の評価のため歩行，乗車の全データ対に対して鍵生成を行った．その結果生成された特徴ベクトルの一致率，特徴ベクトルの種類，特徴ベクトルのエントロピー，1 分あたりに生成される平均の鍵長 (生成鍵長)，1 分あたりの鍵のエントロピーは，各動作について表 3.5〜3.7 のようになった．ただし鍵のエントロピーは以下のように求める．

$$\text{鍵のエントロピー} = \text{生成鍵長} * \frac{\text{特徴ベクトルのエントロピー}}{\text{特徴ベクトルのエントロピーの最大値 (理論値)}}$$

鍵の性質として生成確率が一様である (ランダムである) ことが求められるが，この性質を備える鍵の強度は，この鍵のエントロピーの値を用いて議論することが

できる．特徴ベクトル 1 桁あたりの量子値は 5 種類だが，以降鍵長は 2 進数に換算して記述する．したがって特徴ベクトルのエントロピー最大値は W_{fft} = 32 のとき約 16.2 bit，W_{fft} = 64 のとき約 27.9 bit，W_{fft} = 128 のとき約 58.0 bit となる．

また，分散値を用いる手法の各パラメータを表 3.8 のように設定し，鍵生成を行った．分離によってこの鍵生成法が適用される主な動作は歩行であるが，手法の評価のため歩行，乗車の全データ対に対して鍵生成を行った．その結果生成された特徴ベクトルの一致率，特徴ベクトルの種類，特徴ベクトルのエントロピー，生成鍵長，1 分あたりの鍵のエントロピーは，各動作について表 3.9〜3.11 のようになった．鍵のエントロピーの求め方はパワースペクトルを用いる手法と同様である．また特徴ベクトルのエントロピー最大値は L=3 に設定したとき，約 7 bit となる．

表 3.4. パワースペクトル量子化のパラメータ

パラメータ	値
W_{fft} (FFT の窓サイズ)	32, 64, 128
W_{fft} のオーバーラップ	50%
b (量子バンド数)	5
c (量子値の候補数)	6
α (境界の増加幅)	0.333
f^q_{max} (量子化する周波数帯最大値)	10Hz

4.4 考察

分散による分離に関する考察

表 3.2 から，歩行，乗車いずれの場合も類似の動作とそれ以外をよく分離できていることが分かる．追走の場合，鍵共有を拒否するかどうかは状況や応用に依存する．拒否としたい場合は閾値を低く設定すればよい．また，静止している箇所の分散値差分が大きくなってしまっている．これは分散の対数値で差分を求め

表 3.5. パワースペクトルからの鍵生成：乗車

	同乗 分散差分:小 コヒーレンス:大			追走 分散差分:中 コヒーレンス:小		
	$W_{fft} = 32$	64	128	32	64	128
特徴ベクトルの一致率 (%)	22.5	16.0	7.2	4.52	1.14	0.49
種類 (bit)	7.1	6.4	5.0	6.0	3.6	1.6
エントロピー (bit)	6.0	5.6	4.9	5.7	3.5	1.6
生成鍵長 (bit)	587.9	417.6	196.2	118.0	29.8	13.4
鍵のエントロピー (bit)	217.7	83.8	16.6	41.5	3.7	0.4

表 3.6. パワースペクトルからの鍵生成：歩行

	並行 分散差分:小 コヒーレンス:小			自由 分散差分:大 コヒーレンス:小		
	$W_{fft} = 32$	64	128	32	64	128
特徴ベクトルの一致率 (%)	7.96	12.34	2.28	7.49	6.84	5.77
種類 (bit)	6.2	5.4	3.6	6.2	5.6	4.8
エントロピー (bit)	5.1	3.6	3.1	5.2	4.8	4.3
生成鍵長 (bit)	208.8	322.0	62.0	195.5	178.6	156.7
鍵のエントロピー (bit)	65.7	41.6	3.3	62.8	30.7	11.6

表 3.7. パワースペクトルからの鍵生成：先導役の両センサ

	乗車 分散差分:小 コヒーレンス:大			歩行 分散差分:小 コヒーレンス:小		
	$W_{fft} = 32$	64	128	32	64	128
特徴ベクトルの一致率 (%)	32.3	25.4	18.5	19.5	9.55	27.6
種類 (bit)	7.6	7.7	6.8	6.9	6.2	5.1
エントロピー (bit)	6.6	7.4	6.8	5.2	5.2	3.1
生成鍵長 (bit)	842.4	662.0	502.7	509.9	249.3	749.5
鍵のエントロピー (bit)	343.2	175.6	58.9	163.7	146.5	40.1

表 3.8. 分散値量子化のパラメータ

パラメータ	値
W_{var} (分散算出の窓サイズ)	150
W_{qnt} (量子化対象の窓サイズ)	5, 10, 20
W_{pre} (過去データ窓サイズ)	$W_{qnt} \times 3$
W_{var}, W_{qnt} のオーバーラップ	50%
r (境界幅の初期値)	0.5
b (量子バンド数)	5
c (量子値の候補数)	4
α(境界の増加幅)	0.166
L (量子値の連結数)	3

ているため，分散値の低い個所は小さな揺らぎも大きな差として判断してしまうのが原因である．

コヒーレンスによる分離に関する考察

表 3.3 の通り，歩行実験ではいずれの対もコヒーレンス値は小さく，乗車実験では同乗と追走をよく分離している．また一人の被験者が装着した胸と腰のセンサ間のコヒーレンス値も歩行では平均 0.4 程度の値となり，一見よく似ているデータ対であっても，位相の違いによって確実に分離できていることが分かった．

パワースペクトルからの鍵生成に関する考察

表 3.5〜3.7 の通り，特徴ベクトルの一致率は低いものの，比較的長い鍵を生成することに成功した．分散とコヒーレンスによる分離によって，このパワースペクトルからの鍵生成手法に導かれるのは乗車動作における先導と同乗の場合のデータ対である．このデータ対から鍵を生成した場合，1 分あたりの鍵のエントロピーが最大なのは，パラメータを表 3.8 のように $W_{fft} = 32$ に設定したときであり，約 1 分間で 217.7 bit 相当の鍵が生成できた．ちなみに乗車動作の先導役が

表 3.9. 分散値からの鍵生成 乗車

	同乗 分散差分:小 コヒーレンス:大			追走 分散差分:中 コヒーレンス:小		
	W_{qnt}=5	10	20	5	10	20
特徴ベクトルの一致率 (%)	97.9	100	100	61.81	74.19	85.71
種類 (bit)	4.4	3.8	2.8	3.7	3.8	3.2
エントロピー (bit)	3.9	3.6	2.6	3.0	3.5	3.1
生成鍵長 (bit)	28.3	16.3	7.2	18.1	12.2	6.4
鍵のエントロピー (bit)	15.8	8.4	2.7	7.8	6.1	2.8

表 3.10. 分散値からの鍵生成 歩行

	並行 **分散差分:小 コヒーレンス:小**			自由 分散差分:大 コヒーレンス:小		
	W_{qnt}=5	10	20	5	10	20
特徴ベクトルの一致率 (%)	98.1	98.4	96.6	52.3	50.8	46.7
種類 (bit)	4.0	4.0	3.5	1.6	0	0
エントロピー (bit)	1.6	2.0	2.25	0.3	0	0
生成鍵長 (bit)	29.4	17.1	7.9	15.7	9.0	3.9
鍵のエントロピー (bit)	6.7	4.9	2.6	0.7	0	0

表 3.11. 分散値からの鍵生成 先導役両センサ

	乗車 分散差分:小 コヒーレンス:大			**歩行** **分散差分:小 コヒーレンス:小**		
	W_{qnt}=5	10	20	5	10	20
特徴ベクトルの一致率 (%)	86.0	93.8	100	96.2	98.7	100
種類 (bit)	4.0	3.32	3	4.9	4.4	4.17
エントロピー (bit)	3.4	2.6	2.7	2.9	3.2	3.7
生成鍵長 (bit)	25.3	15.5	7.2	29.0	17.6	8.4
鍵のエントロピー (bit)	12.3	5.8	2.8	12.0	8.1	4.4

装着した腰と胸のセンサのデータ対からは約 343.2 bit 相当の鍵が生成できる．各動作とも特徴ベクトルの種類とエントロピーの間に大きな差がないことから，生成された特徴ベクトルには大きな偏りがないことが分かる．

パワースペクトルから鍵生成を行った場合，加速度が小刻みに激しく変化する乗車動作であれば，類似した動作 (同乗) から生成した特徴ベクトルの一致率，類似していない動作 (追走) から生成した特徴ベクトルの一致率は，表 3.5 のように動作類似度 (表 3.3) に適合した結果となる．しかし歩行データを用いて鍵生成を行った場合，類似した動作 (並行)，類似していない動作 (自由) ともに同程度の一致率となってしまった (表 3.6)．これは，歩行動作の特徴が出る周波数帯が一定の帯域に非常に集中しているため，歩行の状況に関わらず同じような特徴ベクトルが生成されしてしまうことが原因だと考えられる．実際，乗車は **10 分間**で特徴ベクトルのエントロピーは約 6 bit(理論上の最大値は約 16.2 bit) であるが歩行は **30 分間**かけても特徴ベクトルのエントロピーは約 5 bit と，乗車動作に比べ，歩行動作では時間あたりに生成される鍵の種類が少ない．このような場合を排除することが必要であるため，あらかじめ分散値およびコヒーレンスで類似度に応じて動作を分類しておくことは有効であると考えられる．

分散値からの鍵生成に関する考察

分散値からの鍵生成は表 3.9〜3.11 の通りとなり，似た動作からは特徴ベクトルの一致率が非常に高く安定した鍵生成が可能であることがわかった．2 つの分離によって，分散値からの鍵生成に導かれるのは歩行動作における先導と並行の場合のデータ対である．このデータ対から鍵を生成した場合で 1 分間あたりの鍵のエントロピーが最大なのは，パラメータを表 3.8 の $W_{qnt} = 5$ としたときであり，1 分間で約 6.7 bit 相当の鍵が生成できた．ちなみに歩行動作の先導役が装着した腰と胸のセンサのデータ対からは約 12.0 bit 相当の鍵が生成できた．減速や加速といった変化に富む動作が含まれていれば，並んで歩く場合は約 2 分間，1 人で 2 つのセンサを持った場合は約 1 分間で Bluetooth の PIN コード相当 (13bit) の鍵が生成できる．歩行動作のデータから鍵生成を行った場合，生成された特徴ベクトルの種類とエントロピーとの間に 1 bit 以上の差が出ている．一方，乗車

動作のデータの場合は鍵の種類とエントロピーにあまり差がない．これは単調な動作が多い歩行 (図 3.11) では同一の特徴ベクトルが生成されやすいが，振動が多く加速度の変化が激しい乗車 (図 3.13) では多くの種類の特徴ベクトルが偏ることなく生成されたからである．この鍵生成法は乗車，歩行を問わず類似した動作は特徴ベクトルの一致率が高く，類似していない動作は一致率が低くなり，動作の類似度に適合した結果となった．車の追走に関しては 4.4 項で述べたように，利用状況に依存して鍵生成するかどうかを判断し，パラメータを設定する必要がある．また，実験データでは，$W_{qnt} = 5$ が鍵長，一致率共に良い結果となったが，W_{qnt} が小さすぎると，動作の時間的なずれから受ける影響が大きくなることに注意が必要である．

5. まとめ

本研究では歩行や自動車への乗車など日常的な動作を利用して鍵生成を行うための鍵生成アルゴリズムを提案した．医療分野などで導入可能性が高いウェアラブルセンサとユーザの備えるモバイル機器が，数分間の歩行動作のみで自動的に安全な通信路を開設するような応用が想定される．また，車載センサとユーザ機器との安全な自動接続も同様に可能である．その他にも，センサネットワークの運用開始時に，センサを設置する段階において，持ち運ぶセンサに自動的に共通の鍵を共有させ，設置の手間を軽減するような使い方も考えられる．提案方式は，まず各動作の類似度を加速度の分散値やコヒーレンスを利用して算出し，算出した類似度に応じて具体的に類似度の高い動作対は，周波数領域のパワースペクトルを用いて鍵生成を行い，類似度が中程度の動作対からは，加速度の分散値を用いて鍵生成を行った．

性能評価の結果，振動パターンが異なる日常的な歩行や乗車といった動作から提案手法に基づいて鍵生成が可能なことを確認した．乗車動作の先導役と同乗役のデータ対は類似度に基づいてパワースペクトルから鍵が生成され，約 1 分間で 217.7 bit 相当の鍵が生成可能であることを確認した．一方，歩行動作の先導役と並行役のデータ対は類似度に基づいて分散値から鍵が生成され，動作の変化が激

しい箇所からは，約 1 分間で最大 6.7 bit 相当の鍵が生成可能であることを確認した．比較的長い鍵を生成できるパワースペクトルからの鍵生成は，類似しない動作対からも共通鍵を生成してしまう問題を抱えているが，事前にコヒーレンスによる類似動作の分離を行うことで，この問題が解決することを確認した．分散値からの鍵生成は比較的短い鍵長ではあるが，歩行，乗車の両動作に用いることができ，汎用性の高さを確認した．

分散値からの鍵生成法では，10〜20 メートル離れた場所で先導役を追跡した時の先導役と追跡役のデータ対から生成される特徴ベクトルの一致率も高くなる．これは先導役と完全に横並びにならなくても共通鍵が生成できるという点では利便性が高いといえる．しかし一方で関係のない人とも共通鍵を生成されてしまうという点では脆弱性ともいえる．そこで今後の課題として，並行役と追跡役の間の分離が可能な手法を検討することが考えられる．また，今回は 3 軸加速度センサのデータのみを用いて鍵生成を行ったが，加速度以外の光や音，温度，気圧などのセンサにより，人の周辺状況の類似度を測定し，それに応じた鍵生成法を検討することが今後の課題である．ただし加速度センサのようにある程度変化に富んだデータを計測できるセンサでないと鍵生成は難しいことがわかっているため，これを満足するセンサの調査を進めている．現時点で，マイクで計測する環境音の時系列データから鍵生成が可能であることの確認ができており，実験を通じた評価を継続的に行っていく．

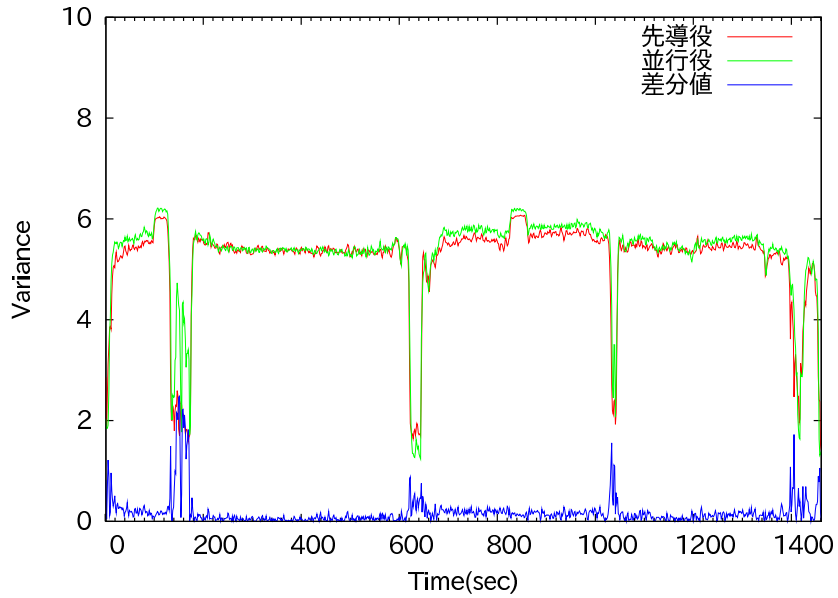

図 3.11. 分散値と差分:歩行 先導と並行

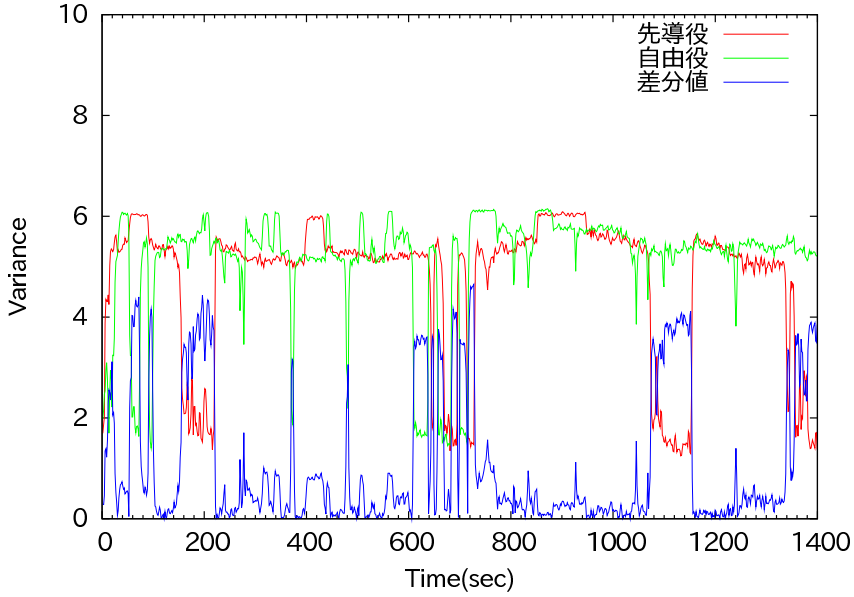

図 3.12. 分散値と差分:歩行 先導と自由

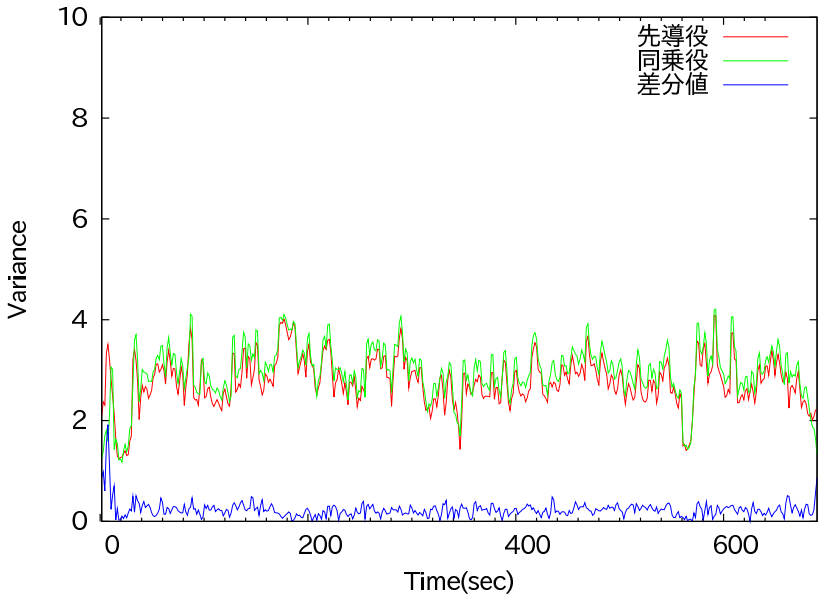

図 3.13. 分散値と差分:乗車 先導と同乗

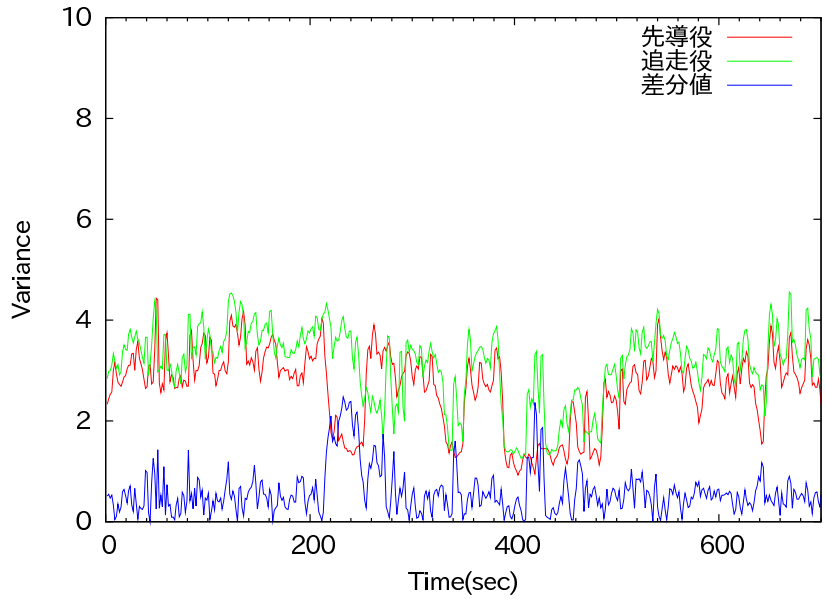

図 3.14. 分散値と差分:乗車 先導と追走

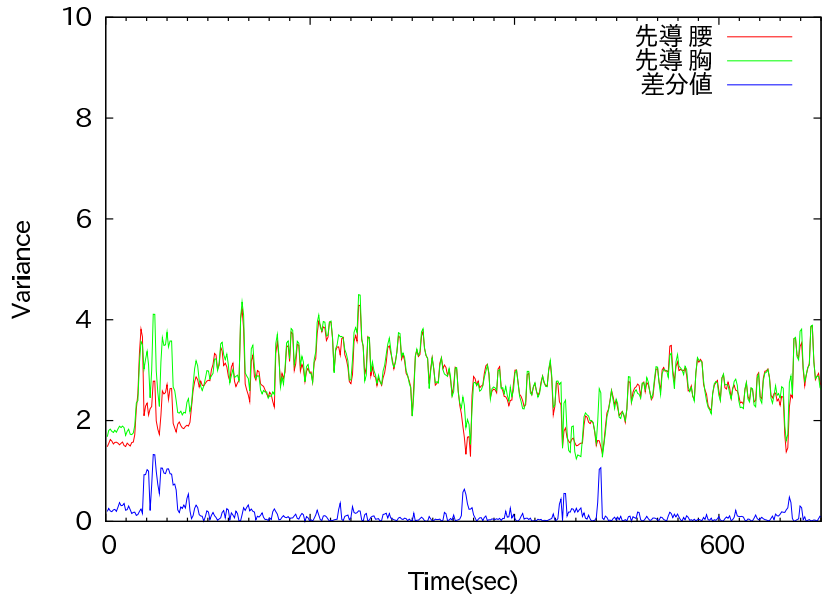

図 3.15. 分散値と差分:乗車 先導役の腰と胸

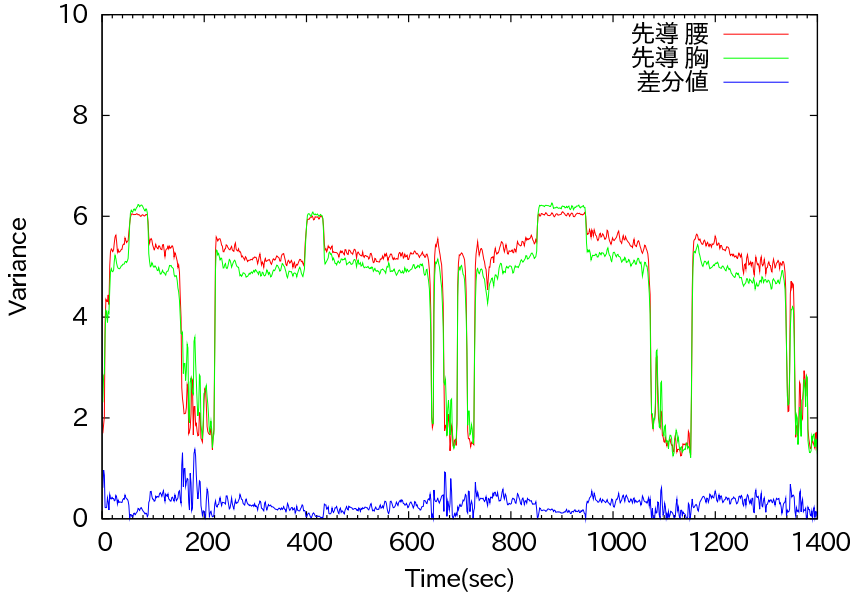

図 3.16. 分散値と差分:歩行 先導役の腰と胸

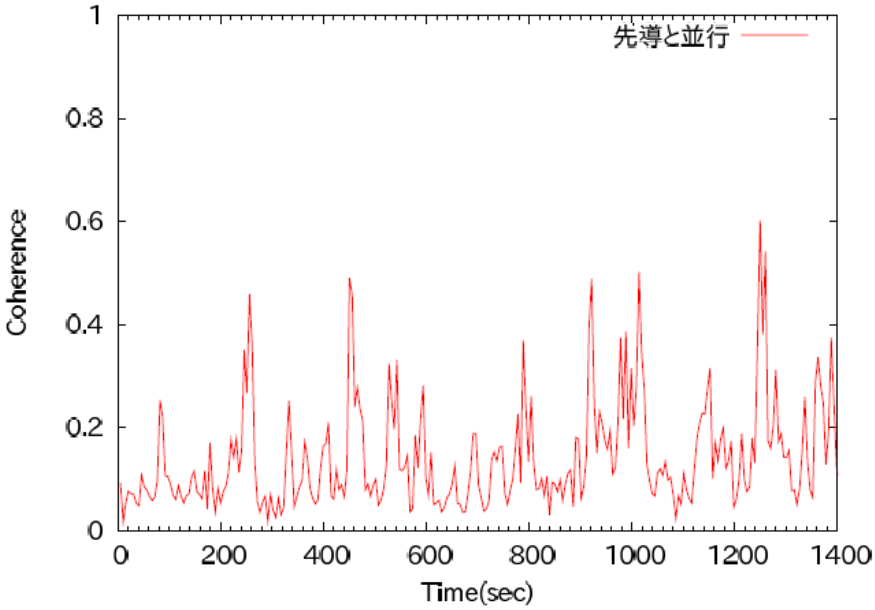

図 3.17. コヒーレンス:歩行 先導と並行

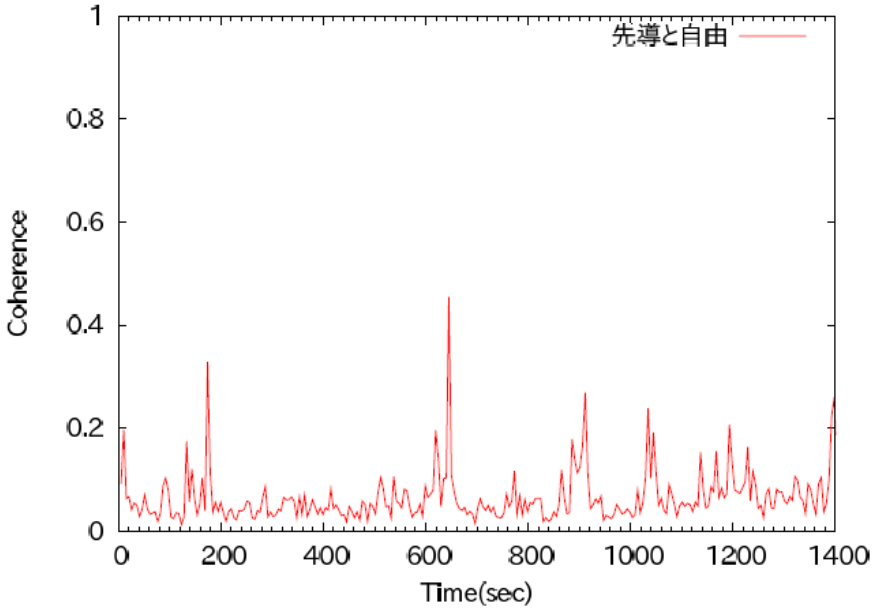

図 3.18. コヒーレンス:歩行 先導と自由

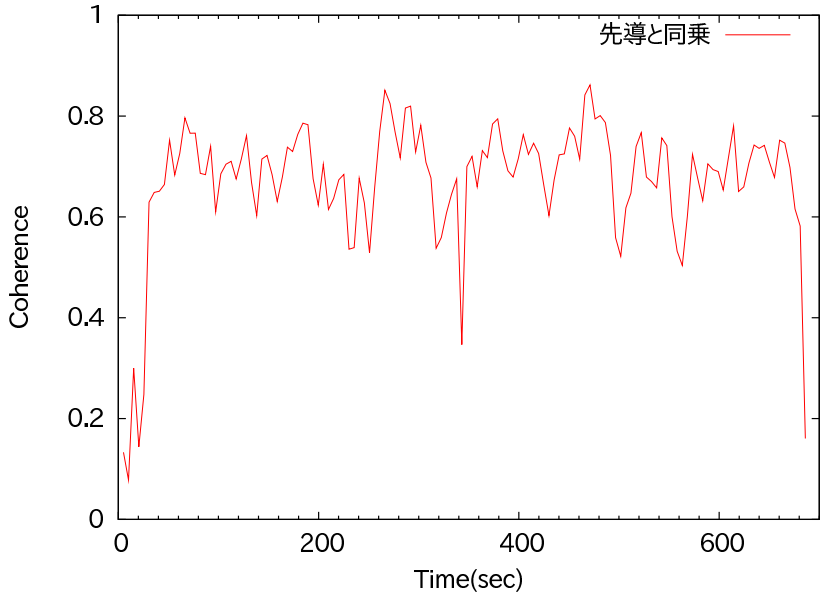

図 3.19. コヒーレンス:乗車 先導と同乗

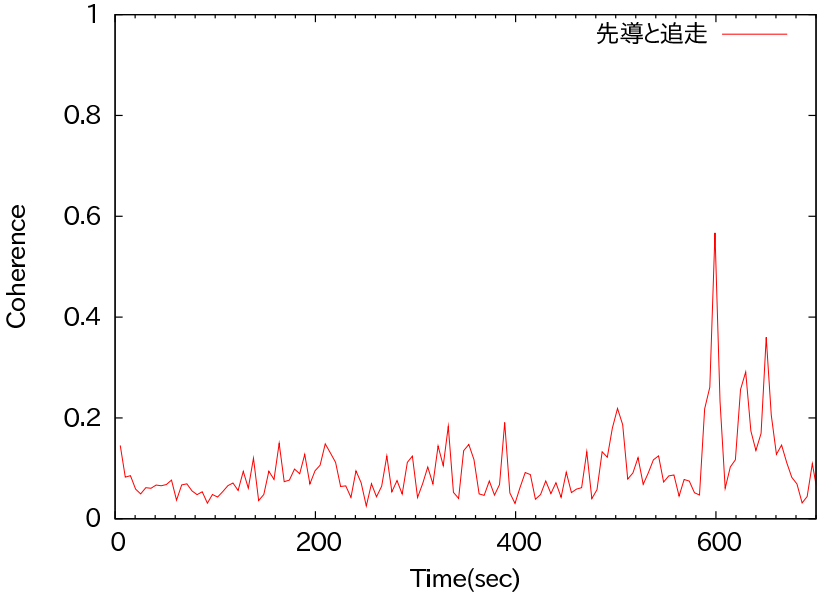

図 3.20. コヒーレンス:乗車 先導と追走

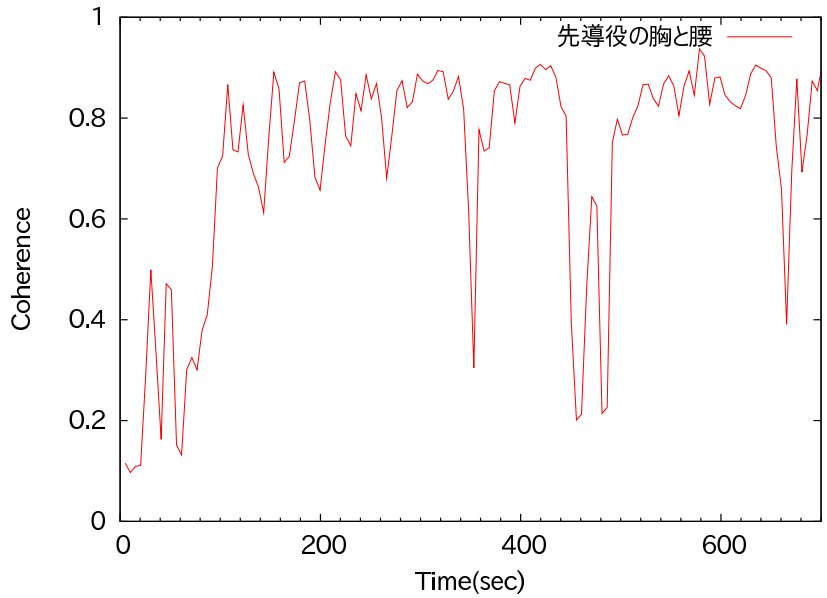

図 3.21. コヒーレンス:乗車 先導役の腰と胸

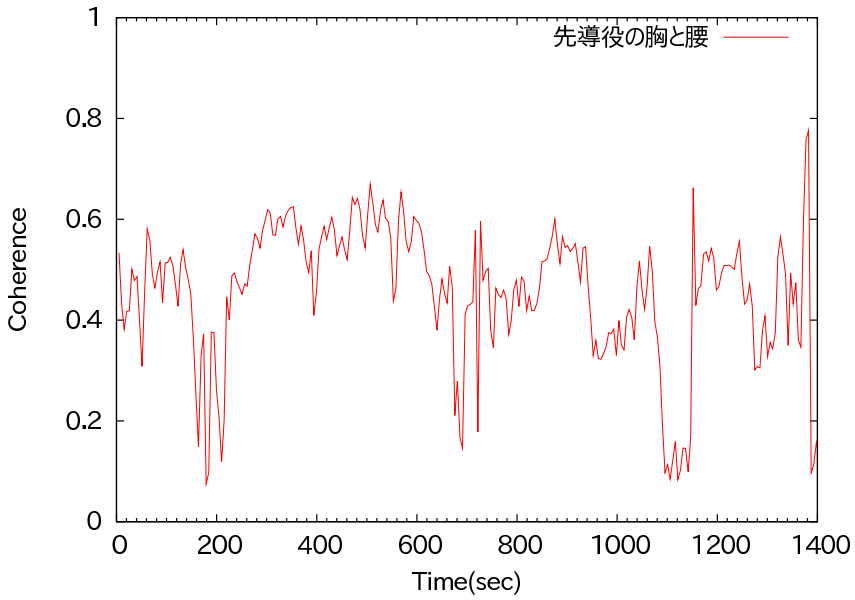

図 3.22. コヒーレンス:歩行 先導役の腰と胸

第4章　プレゼンスアウェア信用管理システム

1. はじめに

計算機ネットワーク上で提供されるサービスが拡大されるに従い，セキュリティ保護等を目的としたシステム管理運用技術が益々重要となっている．パスワード等に基づく従来のシステム管理では，登録された各ユーザに対し，どのサービスが提供可能かを定めておく．しかし，不特定多数のユーザにサービスを提供するユビキタス環境では，全ユーザを予めシステムに登録するのは不可能である．そこで近年，公開鍵基盤 (PKI) に基づくシステム管理運用技術として，信用管理技術が注目されている．信用管理とは，ユーザが提示したディジタル証明書に基づいてユーザに一定の信用 (role) を割り当て (信用確立)，その信用に応じて特定のアクセス権の付与やサービスの提供を行う技術である．ここで，ディジタル証明書とは，身元保証や公共機関の発行する証明書のように，ユーザの本人性や属性を記述するためのものである．

ユビキタス環境では，屋内外を問わずあらゆる場面で IT とネットワーク技術を利用した様々なサービス提供者と出会う可能性が飛躍的に高くなると考えられるため，信用管理技術が益々重要になる．特に，センサネットワークを応用して収集可能なユーザのコンテクスト情報に基づき，ユーザにアクセス権を与える取り組みが重要になると考えられている [52]．例えば，ある企業のオフィスにおいて，正社員とともに同じ部屋に居るときのみゲストに社内データへのアクセスを許可したり，通常時は患者のプライバシのために主治医のみに開示を限定する電子カルテに関し，緊急時には同じ治療室にいる別の医者にも開示を認めることなどが考えられる．

以上を鑑みるとコンテクスト情報に基づき，ユーザにアクセス権を与えることは重要であると考えられるが，既存の信用管理技術をセンサネットワークと繋げるにあたってはいくつかの解決すべき問題がある．例えば，ディジタル証明書やセンサネットワークから得られる情報 (センサ出力) のような異質の情報を入力としアクセス権を導出する必要がある．さらに，センサ出力には不確実性が含まれ，時には正確でないことがある．

本章では，これらを踏まえ，代表的なコンテキスト情報であるユーザのプレゼンス (存在位置) を扱うことのできる信用管理システムを提案する．提案システムは以下を特徴とする．

- TPL[59] のようなポリシ記述言語に基づいて，ロールベースアクセス制御 (role-based access control, RBAC) と PKI およびプレゼンスを統合する基盤を提供する．ディジタル証明書や，後述するプレゼンス推論エンジンによって推論されるユーザのプレゼンス，およびユーザの予定表などの異種の情報は全て，一階述語論理の原子論理式で表現する．詳細を 2 節に示す．

- システムの振る舞いは一階述語論理によって形式化される．従って，信用管理の手順は予め与えられる信用管理ポリシに基づいて自動化可能である．また形式意味論を持つことからシステムの動作が論理的に推論可能であり，与えたポリシの形式的な検証が可能となる．これらの詳細は，3 節にて信用管理ポリシを解釈する信用管理ポリシエンジンの実際の動作とともに説明する．

- 提案システムは，隠れマルコフモデル (HMM) に基づき，不確実性を含むセンサ出力からユーザのプレゼンスを推論する．HMM を用いたプレゼンスの推論について，4 節にて詳細を示す．HMM では，ユーザのプレゼンスを (予め定義される) 各位置に存在する確率として扱う．そして，この確率値はユーザがある位置に居ることの信頼度として，信用管理ポリシエンジンに利用される．プレゼンス推論の精度は重要であるため，HMM を用いたプレゼンス推論にいくつかの独自の改良を施している．4 節ではこれら工夫についても併せて説明する．

- 実験的評価のため，オフィス内におけるサービスへのアクセス制御システムに提案システムを組み込んだ．センサとして RFID タグを使った位置検知センサを用いた．そして RFID タグを所有する被験者のプレゼンスを推論することで，プレゼンス推論エンジンの定量的な評価を行った．これらについては 5 節，6 節に詳細を示す．

関連研究

証明書の位置付けやポリシ記述言語などの違いによって，種々の信用管理モデルが提案されている．文献 [67] では，主にアクセス制御のための信用管理システムを property-based system と capability-based system に分類している．property-based system では，証明書の発行とアクセス制御をできる限り分離し，ディジタル証明書とは，一般的な推薦書，身元保証や公共機関の発行する証明書のように，特定の組織に依存しない属性のみを記述するためのものであるという立場を取る．具体的には，ディジタル証明書として主に属性証明書を用いる．代表的なものに，TPL[59] がある．この方法の利点は証明書の発行局とアクセス制御を分離設計できることである．一方，capability-based system では，積極的にアクセス権そのものや RBAC の role をディジタル証明書に含めるというもので，主に権限証明書を用いる．この立場を取るものに，PolicyMaker[54] とそれを発展させた KeyNote[55], 及び SPKI[57] がある．この方法の利点は，ディジタル証明書の柔軟性が高いこと，欠点はディジタル証明書がアクセス制御に依存することである．なお [66] では，信用管理に用いられるポリシ記述言語を対象として，それに求められる要件を整理し，TPL や KeyNote を含め，代表的なポリシ記述言語を比較している．

提案する信用管理モデルは TPL のように property-based system に分類される．提案モデルの特徴的な利点は，PKI の証明書やユーザのプレゼンスのような異種の情報を形式的かつ統一的に表現できる点にある．これは，アプリケーションと信用管理とセンサネットワークとをうまく分離できることを意味する．また，システムの振る舞いは形式意味論に基づき完全に予測可能である．これは，信用管理ポリシエンジンの自動化の観点で有用である．また，与えるポリシが正しく動作するかを検証することも可能である．筆者らの知る限り，同様の特徴を持つ信用管理モデルは存在しない．

コンテクスト情報をアクセス制御に組み込む研究がいくつか知られている [56]. [53] は RBAC の拡張モデルを与えるために，空間的な位置情報を扱える階層的スキーマ言語を提案している．しかしながら，実装にあたっての課題等については議論がなされていない．CSAC[60] は，我々の提案手法に近いアプローチをとっている．[60] では，サービス提供者が，サービス要求を容認するかどうかをコンテクストプロバイダに問い合わせて決定する．[9] では旅行者向けのサービスへの適用について議論されている．我々のポリシ記述言語は一階述語論理に基づき，[60] と比較して，より一般的なコンテクスト情報をポリシに組み込むことができる．

ユーザのプレゼンスを推定する研究に関し，ベイズモデルに基づくものが知られている．RightSPOT[61] は，static な (時間軸上の状態遷移を行わない) ベイズモデルを利用している例であり，位置間の関係と，その位置における観測情報だけを用いてユーザのプレゼンスを推定する．我々はユーザの時間的な振る舞いをモデルに取り込むことが推定結果の高精度化に繋がると考えている．これを実現するものとして，HMM を含む temporal な (時間軸上の状態遷移を行う) ベイズモデルを利用するものがある．SmartMoveX[62] は HMM を利用するシステムの例である．またベイジアンフィルタ [58] は temporal なベイズモデルを使った一般的な推定方法であり，static な依存関係を時間的に連続なものに拡張する．4.2 で示すように，HMM は単純な方法で各状態における持続長を表現でき，プレゼンス推定の精度向上に有用であると考えられるため，提案システムでは，時間帯とユーザのスケジュール情報を可観測変数として利用する HMM を用いる．これは，[58] において示されてはいないがダイナミックベイジアンネットワーク (DBN) の一種である．また，[63] では DBN を用いて GPS の信号から，非可観測変数である移動モード ($\in \{\mathrm{bus}, \mathrm{foot}, \mathrm{car}\}$) を推定する方法が示されているが，[63] は我々とは全く異なる確率モデルを採用している．

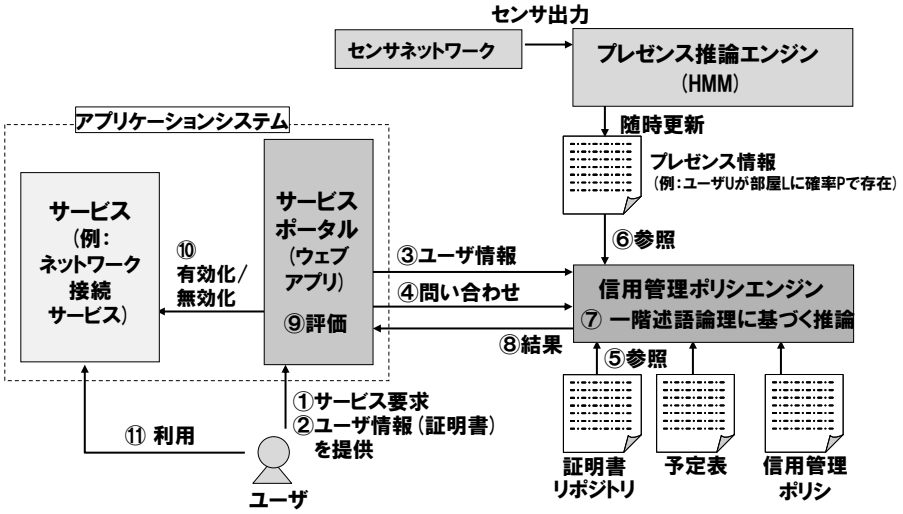

図 4.1. 信用管理システムのアーキテクチャ

.

2. プレゼンスアウェア信用管理システム

2.1 概要

図 4.1 は提案するユーザプレゼンスを利用した信用管理システム (プレゼンスアウェア信用管理システム) を示す．信用管理ポリシエンジンはユーザに role(権限) を与え，アプリケーションシステムはユーザの role をもとに提供するサービスの種類を決定する．提案モデルの主な特徴は信用管理ポリシエンジンが，ディジタル証明書だけでなく，プレゼンス推論エンジンで推論されるユーザのプレゼンスを利用する点である．この特徴は次の点で柔軟なセキュリティポリシを実現する．

ユビキタスシステムにおける設計上の課題は安全性と利便性のトレードオフにある．サービスを授受する際に，多くの証明書をシステムがユーザに要求すればするほど，ユーザの利便性は下がる．提案モデルでは，ユーザのプレゼンスを適切に用いることによって，セキュリティ寄りの設計と利便性寄りの設計の両方を実現できる．例えば，安全性を高めたい場合には，システムはパスワードやディジタル証明書に加えてユーザのプレゼンスを認証のために併せて要求できる．もし，ユーザがある位置に存在するというプレゼンスの信頼度が一定値未満である場合は，あるリソースにアクセスすることを許可しないといったポリシを実現す

ることは容易である．一方で，ユーザのプレゼンスは利便性向上のためにも有用である．一時的に権限を別のユーザに委譲したい場合などに，自分と同じ位置にいるというユーザのプレゼンスの信頼度が一定値以上であるなら，そのユーザにアクセスを許可するなどのポリシを実現できる．

2.2 プレゼンス推論エンジン

プレゼンス推論エンジンはセンサから出力される情報を入力とする．センサ出力は必ずしも正確でないことがあるため，真の値を推論する体系的な方法を備えることが望ましい．これを実現するために，推論エンジンは隠れマルコフモデル (HMM) を利用する．HMM の状態集合は，ユーザの取り得るプレゼンスの集合からなる (例えば { 居室，会議室，実験室 } など)．出力記号の集合は，観測可能なセンサ出力の集合からなる．出力記号 (センサ出力) が与えられる各時刻において，プレゼンス推論エンジンはユーザが各状態 s に居る (事後) 確率を計算する．さらに，確率モデルに改良を加えるため，我々は時間帯 { AM，lunch，PM，off } と，ユーザの予定表を可観測変数として利用する．さらに，我々はある位置に存在し続ける時間長 (例えば，会議の平均的な時間は 45 分であるなど) を表現するためにマクロ状態を導入する．詳細については，4 節にて述べる．

2.3 信用管理ポリシエンジン

信用管理ポリシエンジンに与えられるポリシを，信用管理ポリシまたは信用ポリシと呼ぶ．信用管理ポリシは 2.1 項で述べたような情報を表現する確定 Horn 節によって構成される推論規則の集合である．本エンジンは，アプリケーションによるアクセス要求から生成される問合せをもとに推論を開始する．典型的な問合せは，”ユーザ A はディジタル証明書の提示無しで無線ネットワーク *wlan*1 にログインできるか？”のようなものである．次節では信用管理ポリシエンジンについて詳細に説明する．

3. 信用管理ポリシエンジン

3.1 信用管理ポリシ

信用管理ポリシは，プレゼンスやディジタル証明書の存在を表す基本述語に基づいてポリシ定義述語を定義するような，確定 Horn 節 形式の推論規則の集合である．信用管理ポリシ内に現れる述語は，基本述語及びポリシ定義述語に分類される．

基本述語:

- プレゼンス推論エンジンによって推論結果である信頼度付きプレゼンスを表す述語 (HMM の各状態における事後確率).
  例: $position(U, L, P)$ (ユーザ U が部屋 L に確率 P で存在する)
- ディジタル証明書の存在を表す述語.
  例: $cert(N, U, \textit{full-time})$ (会社 N によって，U が N の正社員であることを証明する証明書が発行されている)
- 予定表に書かれた現在の滞在位置を表す述語.
  例: $schedule(U, NY)$ (予定表によるとユーザ U がニューヨークにいる)

ポリシ定義述語 (ユーザ定義述語): ユーザへの role の割当てを表現する述語.
例: $permit(N, U, wlan1, passwd)$ (ユーザ U がパスワードで認証されれば，会社 N が U に無線ネットワーク $wlan1$ へのアクセス権を許可する)

ポリシ定義述語は，基本述語に基づいた再帰的な推論規則によって定義される．場合によっては，より信頼の置ける機関によって発行された証明書を持つユーザなどに対して，ある信頼度を持つ role を割り当てたいこともあり得る．そのような信頼度はポリシ定義述語の引数として表現することも可能である．

3.2 信用管理ポリシエンジン

信用管理ポリシエンジンは，基本述語の定義及び信用管理ポリシ (推論規則) を入力として問合せ (ポリシ定義述語からなる項) の真偽を導出する推論エンジンで

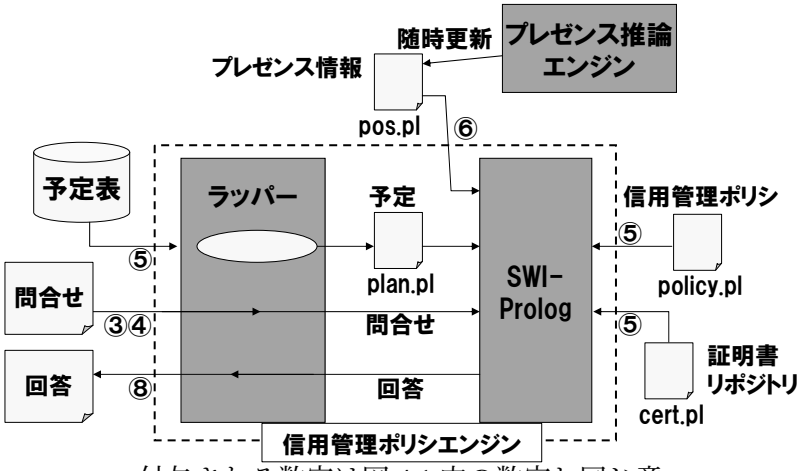

図 4.2. 信用管理ポリシエンジンの構成

ある．ここではこの推論を Prolog と同じ後向き推論 で実現するものとし，Prolog 処理系の拡張として信用管理ポリシエンジンを設計する．Prolog 処理系に対する拡張部分 (ラッパーと呼ぶ) は，ユーザ (またはユーザからのサービス要求に対して可否を判定したいサービス提供アプリケーション) から問合せを受け取り，プレゼンス推定エンジンが出力した信頼度付きプレゼンス，デジタル証明書の検証結果，予定表などを参照して基本述語を定義する単位節 (述語) を生成した上で，これらの単位節集合，信用管理ポリシ，及び問合せを Prolog プログラムとして実行する (図 4.2).

サービス提供アプリケーションは，ユーザからのサービス要求に対して可否を判断したいとき，そのユーザと要求されたサービスに対して主述語 $permit(\ldots)$ が真となるか，信用管理ポリシエンジンに問い合わせる．信用管理ポリシは，基本述語で表される各情報に基づいて，どのような条件が成り立つ場合にサービス提供を許可するかをサービスごとに記述したものとなる．

ユーザのプレゼンスは基本述語として与えられるため，信用管理ポリシエンジンは，例えば，”ユーザ A が正社員と同じ位置にいるときに，A はディジタル証明書やパスワードの提示無しで無線ネットワーク $wlan1$ にログインできる”，”ユーザ A が一人で部屋にいるときには $wlan1$ へのアクセスにディジタル証明書の提示を求める”といったプレゼンスに依存する role を割り当てることが可能である．

3.3 信用管理ポリシ例

信用管理ポリシの記述に先立って，基本述語及びポリシ定義述語を定める必要がある．これらは応用分野に即して必要なものを定義することになる．基本述語は，ラッパーがどのような情報を収集できるかに依存し，ラッパーの実装の際に固定される．一方，ポリシ定義述語は，問合せ発行者とポリシ記述者の間で合意されていればよく，ラッパーの実装に依存しない．

ここではオフィス環境でのサービス提供可否判定を例に説明する．ポリシは，以下の条件が成り立つ場合に無線 LAN 接続サービス $wlan1$ へのアクセスを許可する．

(1) 社員証を持っている社員が，居室，会議室，あるいは実験室のいずれかにいる確率が 90%以上で，その位置が予定表に記載されている位置と一致している場合，$wlan1$ へ接続可能

(2) 社員証を持っている社員が，社外にいる (居室，会議室，実験室にいる確率がいずれも 10%未満) の場合，VPN 接続ならば，パスワード認証の下 $wlan1$ へ接続可能

(3) 非常勤社員や研修生が，居室あるいは実験室のいずれかにいる確率が 90%以上で，隣に社員がいる場合，$wlan1$ へ接続可能

これらのポリシを整理したものを図 4.3 に示す．
例えば上記の規則 (1) は以下のように記述できる．

```
permit(N,U,wlan1,normal) :-
cert(N,U,full-time),
position(U,L,P), room_for_ft(L),
90 < P, schedule(U,L).
```

ここで，$permit$ の第 4 引数はサービスに関する付加情報を表し，$normal$ は通常の認証手続き不要なサービスを，$passwd$ はそのサービスに「パスワード認証の下で接続させる」ことを表す．$room\_for\_ft(L)$ は L が居室・会議室・実験室のいず

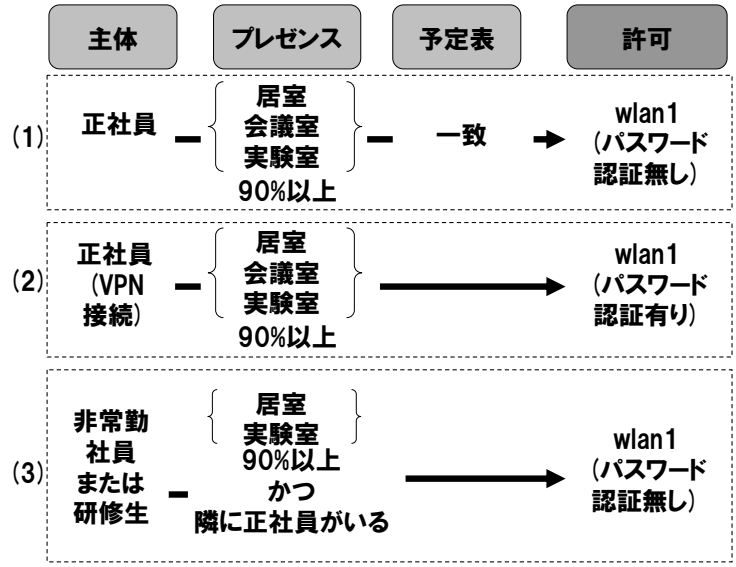

図 4.3. ポリシの例

れかであるとき真となる述語で，補助的な述語としてポリシ中で以下のように定義される．

```
room_for_ft(office).
room_for_ft(meeting_room).
room_for_ft(laboratory).
```

以下は *ichiro* が *wlan1* にアクセスできるかに関する問い合わせになる．

```
?- permit(nec, ichiro, wlan1, normal).
```

規則 (2) は，ユーザが VPN 接続を使用していることを条件に含んでいる．ユーザが VPN 接続を使用しているかどうかは，問合せを発行するサービス提供アプリケーションが信用管理ポリシエンジンに知らせるものとする．これは，以下のように，問合せ中に述語 $parameter$ の定義を記述することで行う．

```
parameter(jiro, connection, vpn).
?- permit(nec, jiro, wlan1, normal).
```

ポリシ内では，以下のように，他の基本述語と同様に $parameter$ を規則の右辺で使えばよい．

```
permit(N,U,wlan1,passwd) :- cert(N,U,full-time),
parameter(U,connection,vpn).
```

規則 (1)–(3) に対応する信用管理ポリシを以下に掲載する.

```
permit(N,U,high-wlan,normal) :-
   cert(N,U,full-time),
   position(U,L,P), room_for_ft(L),
   90 < P, schedule(U,L).

permit(N,U,high-wlan,passwd) :-
   cert(N,U,full-time),
   out_of_company(U),
   parameter(U,connection,vpn).

permit(N,U,high-wlan,normal) :-
   cert(N,U,R), part_or_trn(R),
   position(U,L,P), room_for_pot(L), 90 < P,
   position(U1,L,P1), room_for_ft(L),90 < P1,
   cert(N,U1,full-time).

out_of_company(U) :- not(inside_of_company(U)).
inside_of_company(U) :- position(U,L,P), room_for_ft(L),
                        10 =< P.
part_or_trn(part-time).
part_or_trn(trainee).

room_for_ft(office).
room_for_ft(east_office).
room_for_ft(meeting_room).
room_for_ft(laboratory).
```

```
room_for_pot(office).
room_for_pot(laboratory).
```

4. プレゼンス推論エンジン

本システムではプレゼンスを表す情報をサービス提供の可否を決める際の判断材料として用いることができる．ここでは特にユーザの居る位置をプレゼンスとして扱う．ユーザの位置はユーザのタグを読み取る RFID 技術などを使った位置検知センサによって知ることができるが，位置検知センサの出力（センサ出力）は必ずしも正確でない．すなわち，ユーザの RFID タグ等からの物理的な信号が検知不能であったり，置き忘れ等によりユーザがタグを身につけていない場合がありうるため，センサ出力は必ずしも常時正確な値を表現しているとは限らない．信用管理ポリシがアクセス権をユーザに与える場合に，ある位置に存在することを条件とする場合，ユーザがその位置に存在するにもかかわらず，センサから「そのユーザはその位置に居ない」と出力される (センサ出力が false negative である) と，信用管理システムはユーザにアクセス権を与えないことになる．そのような状況では，たとえ正規のユーザでもサービスを受けられないことになる．逆に，その位置に居ないユーザを，センサから居ると出力される (センサ出力が false positive である) と，信用管理システムは，与えてはいけないユーザにアクセス権を与えてしまうことになる．従って，ユーザのプレゼンスをできる限り正確に検知することがプレゼンスを考慮する信用管理システムにおいて，もっとも重要な課題となる．この課題を解決するため，我々はユーザの行動に関する何らかの確率モデルを定め，そのモデルと位置検知センサ等からの出力に基づいてプレゼンスの推論を行う方法をとる．

ここでは以下のような考えに基づいて確率モデルを設計する．まず，考慮の対象とするプレゼンスの集合が与えられるとする（例えば { 居室，会議室，実験室 } など）．そして，ユーザのプレゼンスはこの集合上の確率変数であると考える．この（真の）プレゼンス自体は外部から観測できないが，真のプレゼンスと相関

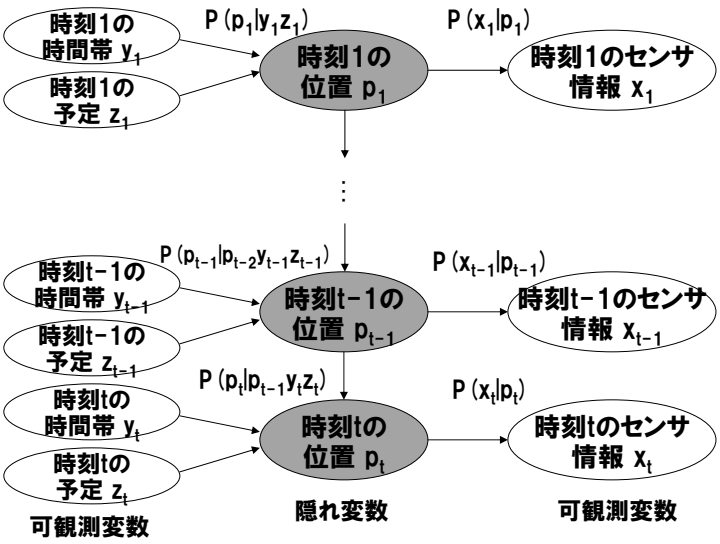

図 4.4. プレゼンス推論のための確率モデル

を持ついくつかの情報（センサ出力，予定，現在時刻など）は観測できる．また，プレゼンスは時間とともに変化し，現在のプレゼンスはそれ以前の時刻のプレゼンスとも相関を持つ（図 4.4）．図 4.4 では，各確率変数（可観測変数及び非可観測変数（隠れ変数））を楕円で表し，確率変数間に相関があることを矢印で示している．確率変数間の相関の大小は条件付き確率で表される．各条件付き確率を予め与えた上で，観測された情報から真のプレゼンスを推論することが，プレゼンス推論エンジンの目的である．

このような，時間とともに変化する隠れ変数の値を可観測変数の値に基づいて推論するための確率モデルとして，隠れマルコフモデル（HMM）[64] がある．以降では，HMM を使ったユーザのプレゼンスの推論方法について，独自に行った拡張とともに述べる．

4.1 隠れマルコフモデル (HMM)

HMM は，有限状態機械に類似した構造を持つ確率モデルである．形式的には，HMM は以下のような 5 項組 $M = (S, T, \delta, \phi, I)$ である．ただし，$\mathcal{R}$ は実数の集合を表す．

- S：状態の有限集合.
- T：出力記号の有限集合.
- $\delta : S \times S \to \mathcal{R}$　$\delta(s, s')$ は状態 s から状態 s' への状態遷移確率.
  各 $s \in S$ について, $0 \leq \delta(s, s') \leq 1 (s' \in S)$ かつ $\sum_{s' \in S} \delta(s, s') = 1$.
- $\phi : S \times T \to \mathcal{R}$　$\phi(s, a)$ は状態 s において記号 a を出力する確率.
  各 $s \in S$ について，$0 \leq \phi(s, a) \leq 1 (a \in T)$ かつ $\sum_{a \in T} \phi(s, a) = 1$.
- $I : S \to \mathcal{R}$　$I(s)$ は実行開始時に状態 s に存在する確率．$0 \leq I(s) \leq 1$ かつ $\sum_{s \in S} I(s) = 1$.

π_t は時刻 t における状態を表す確率変数とする．事後確率 $p_s(t) = \Pr(\pi_t = s \,|\, x_1 \ldots x_t)$ は，出力記号の列 $x_1 x_2 \ldots x_t \in T^*$ が観測されたときに時刻 t に状態 s にいる条件付き確率を表す．ここで，T^* は T のクリーネ閉包である．前向き確率と呼ばれる確率 $p_s(t)$ は以下の式に従って計算することができる.

$$
\begin{aligned}
f_s(t) &= \Pr(x_1 \ldots x_t,\ \pi_t = s) \\
&= \begin{cases} \phi(s, x_t) \sum_{s' \in S} f_{s'}(t-1) \delta(s', s) & t \geq 1, \\ I(s) & t = 0, \end{cases} \\
p_s(t) &= f_s(t) \big/ \Pr(x_1 \ldots x_t) = f_s(t) \big/ \big(\textstyle\sum_{s' \in S} f_{s'}(t) \big).
\end{aligned}
$$

確率 $f_i(t)$ は時刻 t において観測される x_t と，前時刻の前向き確率 $f_k(t-1)$ から計算できる．即ち，過去に観測された記号や時刻 $t-1$ より前の前向き確率を記憶しておく必要はない.

4.2 持続長分布とマクロ状態

上述のような通常の HMM では，同一状態に留まる長さは幾何分布に従う (d 時間留まる確率が d に対して指数的に減少する)．しかし，ある位置に留まる時間 (持続長) に関して「自然な長さ」が存在すると考えられる．例えば会議室に 30 秒しか居なかったり，24 時間居続けたりするのは不自然である．つまり，各位置に

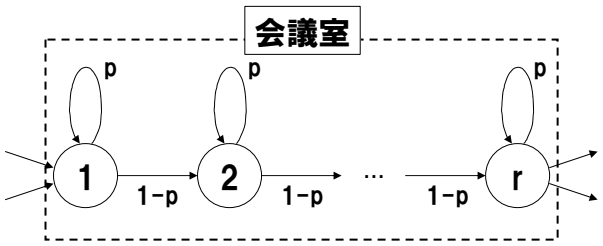

図 4.5. マクロ状態

ついて，留まる時間がある特定の長さである確率が最も高く，それより長くても短くても確率が低くなるような，山型の確率分布になるのが自然と思われる．

山型の持続長分布を持つ HMM を実現するため，本来 1 状態であるものを複数の状態で表す方法を採る．プレゼンス推論においては，各位置 l に複数の状態を割り当てる．このとき，HMM の状態が各状態のいずれにある場合でもユーザは l に居ると解釈する．一つの位置を表す状態群のことをマクロ状態と呼ぶ．マクロ状態内の構造は図 4.5 のようになる．マクロ状態は内部の状態 (ミクロ状態) の数 r と，自己ループ確率 p によって定義される．また，他のマクロ状態から遷移できるミクロ状態 (入り口) と他のマクロ状態へ遷移できるミクロ状態 (出口) がそれぞれ一つに決まっているとする．このとき，このマクロ状態に留まる持続長 d_l の分布は，以下のような負の二項分布となる．

$$\Pr(d_l = k) = \begin{cases} 0 & k < r, \\ \binom{k-1}{k-r} p^{k-r}(1-p)^r & k \geq r. \end{cases}$$

持続長 d_l の期待値は $E[d] = r/(1-p)$, 分散は $V[d] = rp/(1-p)^2$ である．また，各位置について，あらかじめ持続長の平均 μ と標準偏差 σ を与えるとき．ミクロ状態の個数 r とマクロ状態中のミクロ状態の自己ループ確率 p は，それぞれ $r = \lceil (1-p)\,\mu \rceil$ ，$p = \sigma^2/(\sigma^2 + \mu)$ となる．

位置間の遷移確率 $\Pr(\pi_t \,|\, \pi_{t-1})$ は，以下のようにミクロ状態間の遷移確率 $\Pr(\rho_t \,|\, \rho_{t-1})$ に拡張される．$[s]$ はミクロ状態 s が属するマクロ状態を表し，$[s]_{\mathrm{ent}}$ は $[s]$ の入り口であるミクロ状態，$[s]_{\mathrm{exit}}$ は出口であるミクロ状態を表す．各位置 l に対応するマクロ状態中のミクロ状態の自己ループ確率は p_l とする．

二つのミクロ状態間の遷移確率 $\Pr(\rho_t \,|\, \rho_{t-1})$ は，予め与えられる位置間の遷移

確率 $\Pr(\pi_t \,|\, \pi_{t-1})$ と，以下の式によって定義できる．

$$\Pr(\rho_t \,|\, \rho_{t-1}) = \begin{cases} \Pr([\rho_t] \,|\, [\rho_{t-1}])\,(1 - p_{[\rho_t]}) & \\ \qquad\qquad [\rho_t] \neq [\rho_{t-1}],\ \rho_t = [\rho_t]_{\mathrm{ent}},\ \rho_{t-1} = [\rho_{t-1}]_{\mathrm{exit}} & \\ 1 - p_{[\rho_t]} \quad [\rho_t] = [\rho_{t-1}] \text{ かつ } \rho_t \text{ は } \rho_{t-1} \text{の次状態} & \\ p_{[\rho_t]} \qquad \rho_t = \rho_{t-1} & \\ 0 \qquad \text{それ以外.} & \end{cases}$$

4.3 複数の可観測変数への拡張

図 4.4 に示したように，ある時刻 t における状態 π_t は，前時刻の状態 π_{t-1} に加え，現時刻が属する時間帯 y_t や現時刻における予定 z_t によって決定されると考える．従って，状態遷移確率は，4 項組 $(\pi_t, \pi_{t-1}, y_t, z_t)$ を考慮する条件付き確率 $\Pr(\pi_t \,|\, \pi_{t-1}, y_t, z_t)$ として与えられるべきである．条件付き確率 $\Pr(\pi_t \,|\, \pi_{t-1}, y_t, z_t)$ の値を $(\pi_t, \pi_{t-1}, y_t, z_t)$ の全組み合わせについて与える必要があるが，各組み合わせに対して個別に値を定義するのは，組み合わせの数が大きくなるにつれ困難となる．そこでここでは，前時刻の位置に対する条件付き確率 $\Pr(\pi_t \,|\, \pi_{t-1})$，時間帯に対する条件付き確率 $\Pr(\pi_t \,|\, y_t)$，予定に対する条件付き確率 $\Pr(\pi_t \,|\, z_t)$ を別個に与え，それらに基づいて以下のように機械的に $\Pr(\pi_t \,|\, \pi_{t-1}, y_t, z_t)$ を決める方法をとる．ここで α，β は設定者が与える重みである．

$$\begin{aligned} &\Pr(\pi_t \,|\, \pi_{t-1}, y_t, z_t) \\ &= \alpha \Pr(\pi_t \,|\, \pi_{t-1}) + \beta \Pr(\pi_t \,|\, y_t) + (1 - \alpha - \beta) \Pr(\pi_t \,|\, z_t), \\ &0 \leq \alpha,\ 0 \leq \beta,\ \alpha + \beta \leq 1. \end{aligned}$$

これは,「3 つの要因 π_{t-1}, y_t, z_t のうち 1 つが確率 α，β，$1 - \alpha - \beta$ で選択された後，その要因に対する条件付き確率に従って π_t が決まる」という確率モデルに相当する．また，α 及び β は，必ずしも定数で無くともよく，可観測変数 y_t，z_t の関数として定義してもよい．

上記の状態遷移確率 $\Pr(\pi_t \,|\, \pi_{t-1}, y_t, z_t)$ を，ミクロ状態間の遷移確率に拡張すると以下の式のようになる．ここでは，条件付き確率 $\Pr(\pi_t \,|\, y_t)$,$\Pr(\pi_t \,|\, z_t)$ はマクロ

状態に対して定義されるとし，これらは異なるマクロ状態の入り口へ遷移させる要因（下式の右辺の 1〜2 行目．この場合，出口でないミクロ状態からも遷移できる），または同じマクロ状態に留まる要因（同じく 3〜6 行目．この場合，自己ループ確率に従って，同じミクロ状態または次のミクロ状態に遷移する）として扱われる．

$$
\begin{aligned}
&\Pr(\rho_t \,|\, \rho_{t-1}, y_t, z_t) = \\
&\begin{cases}
\alpha \Pr(\rho_t \,|\, \rho_{t-1}) + \beta \Pr([\rho_t] \,|\, y_t) + (1-\alpha-\beta) \Pr([\rho_t] \,|\, z_t) \\
\qquad\qquad [\rho_t] \neq [\rho_{t-1}],\ \rho_t = [\rho_t]_{\mathrm{ent}} \\
(\alpha+\beta \Pr([\rho_t] \,|\, y_t)+(1-\alpha-\beta) \Pr([\rho_t] \,|\, z_t)) \Pr(\rho_t \,|\, \rho_{t-1}) \\
\qquad\qquad [\rho_t] = [\rho_{t-1}],\ \rho_{t-1} \neq [\rho_t]_{\mathrm{exit}} \\
\alpha\, p_{[\rho_t]} + \beta \Pr([\rho_t] \,|\, y_t) + (1-\alpha-\beta) \Pr([\rho_t] \,|\, z_t) \\
\qquad\qquad \rho_t = \rho_{t-1} = [\rho_t]_{\mathrm{exit}} \\
0 \qquad\qquad \text{それ以外.}
\end{cases}
\end{aligned}
$$

また，4.1 項で述べた前向き確率の計算は，以下のように拡張される．出力記号の列 $x_1 \ldots x_t$，$y_1 \ldots y_t$，$z_1 \ldots z_t$ が観測されたとき,、ミクロ状態 s にいる確率 (事後確率)$p_s(t) = \Pr(\rho_t = s \,|\, x_1 \ldots x_t, y_1 \ldots y_t, z_1 \ldots z_t)$ は以下のように計算される．

$$
\begin{aligned}
f_s(t) &= \Pr(\rho_t = s,\ x_1 \ldots x_t \,|\, y_1 \ldots y_t, z_1 \ldots z_t) \\
&= \begin{cases}
\Pr(x_t \,|\, \pi_t = [s]) \sum_{s' \in S} f_{s'}(t-1) \\
\qquad\qquad \times \Pr(\rho_t = s \,|\, \rho_{t-1} = s', y_t, z_t) \\
\qquad\quad t > 0, \\
I([s]) \quad t = 0 \text{ かつ } s = [s]_{\mathrm{ent}}, \\
0 \qquad \text{それ以外.}
\end{cases} \\
p_s(t) &= \Pr(\rho_t = s \,|\, x_1 \ldots x_t, y_1 \ldots y_t, z_1 \ldots z_t) \\
&= f_s(t) \big/ \big(\textstyle\sum_{s' \in S} f_{s'}(t) \big).
\end{aligned}
$$

5. 実装

オフィス環境におけるサービス (例: 無線ネットワークへの接続) を想定し，提案方式に基づきこれらサービスへのアクセス制御を実施するシステムを試作した．

本試作システムのアクセス制御は，サービスにアクセスしようとするユーザやその随伴者のプレゼンスを評価し，十分信頼できると判断すれば面倒な手続きなくアクセスを許可することが可能である．しかも刻々と変わる状況を反映し，例えば随伴者がある程度以上離れればアクセスを切断するような動的で状態変化に追随可能な制御を行う．このように，確率的な判断指標を用いる一方で従来のような「一度権限を得ればいつまでも自由に利用できる」ことのリスクを動的な管理によって低減させている．試作システムは IT サービスへのアクセス制御の例であるが，ある建物の管理室等への入退管理といった物理的なアクセス制御への応用にも有効と考えられる．

5.1 システム構成

本試作システムは，サービスが現在利用可能かどうかを信用管理ポリシエンジンにより判定し，その判定結果によりサービスの利用制御を行う．本試作システムの詳細なシステム構成は図 4.1 の通りである．信用管理ポリシエンジンのバックエンドとして動作するプレゼンス推論エンジンは，ユーザの所持する RFID タグを読み取ることでユーザの位置を検出するセンサ (RFID リーダ) から構成されるセンサネットワークと接続されている．このとき，各構成要素間の処理の流れは次のようになる．構成要素間で渡されるデータに対する安全性は保証されていると仮定する．

(1) ユーザが WEB ブラウザを介してサービスポータルにサービスの利用を要求.

(2) ユーザはユーザ情報 (ディジタル証明書) をサービスポータルに提示.

(3)(4) サービスポータルは，バックエンドに在る信用管理ポリシエンジンに対して (2) のユーザ情報を渡し，サービスの利用可否を問う.

(5)–(7) 信用管理ポリシエンジンは，(3) のディジタル証明書，過去に受信した証明書 (cert.pl)，ユーザの予定表 (plan.pl)，及びプレゼンス推論エンジンで推論する信頼度付のプレゼンスの各情報 (pos.pl) と，ポリシ (policy.pl) を照らし合わせてサービスの利用可否を決定.

(8) サービスポータルが，信用管理ポリシエンジンの判定結果 (サービス利用の可否) を受信.

(9)(10) サービスポータルは，ユーザの利用可能なサービスを知ればそのサービスを有効化，反対に利用不可能なサービスを知ればその利用を無効化する.

(11) ユーザは有効化されたサービスへアクセスできる.

信用管理ポリシエンジン

信用管理ポリシエンジンは，図 4.2 に示したように，Prolog 処理系 (SWI-Prolog) とそれへの拡張部分（ラッパー）とで構成する．Prolog 処理系へは，問合せ，信用管理ポリシ (policy.pl)，証明書リポジトリ (cert.pl) のほかに，プレゼンスの情報 (pos.pl) 及び予定表情報 (plan.pl) を入力する必要がある．以下に Prolog 処理系に入力される規則および述語を例と共に示す.

- 問い合わせ (後述)
- 信用管理ポリシ (3 節を参照)
- 証明書リポジトリの内容

```
cert(nec,ichiro,full-time).
cert(nec,hanako,full-time).
```

- 予定表に記載のあるユーザの位置

```
schedule(ichiro,meeting_room).
schedule(hanako,meeting_room).
schedule(jiro,meeting_room).
```

- プレゼンスに関する情報

```
position(ichiro,office,0).
position(ichiro,meeting_room,93).
position(ichiro,laboratory,4). ...
```

- アプリケーションシステムから与えられる情報

```
parameter(ichiro,connection,vpn).
```

信用管理ポリシと証明書リポジトリ内の証明書は予め与えられる．また，予定表に記載のある位置は，いつでも信用管理ポリシエンジンが参照可能な予定表データベースから取得可能とする．プレゼンスに関する情報はプレゼンス推論エンジンによって定期的に更新されるファイル内に蓄積される．

問合せは，ユーザが提出した証明書等を表す述語と，そのゴールからなる．例えば以下は，ユーザ jiro が非常勤職員であることを示す証明書が提出されているときに，jiro が利用可能なサービスをすべて列挙するような問合せである．ゴールは q という頭部を持つ規則として記述しなければならない．

```
cert(nec,jiro,temporary).
q :- permit(nec,jiro,S,C),write([S,C]),nl,fail.
```

プレゼンス推論エンジン

プレゼンス推論エンジンは，信用管理ポリシエンジンとは独立に動作し，予め設定された時間間隔でセンサ出力，現時刻が属する時間帯，現在の予定の 3 つを調べ，予め与えられた HMM パラメータ（状態遷移確率と出力確率）に従って前向き確率を計算する．時間帯及び予定については，時刻を入力として時間帯名及び予定名を返すような簡易なデータベースを作成し利用する．センサからの情報は，センサネットワークから定期的に取得する．ここではセッション開始プロトコル（session initiation protocol, SIP）のプレゼンスイベントパッケージ [65] に従って情報提供を行うセンサネットワークを対象としてプレゼンス推論エンジンを実装した．

5.2 動作例

図 4.6 が，ユーザ端末でサービスポータルにログインした時の画面である．ログイン時にユーザは提示するディジタル証明書を任意に選択できる．ログイン後

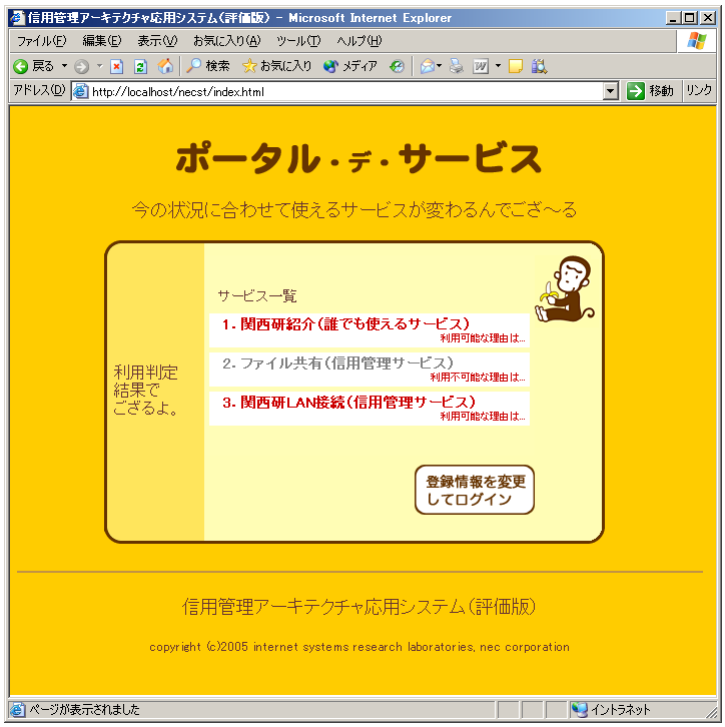

図 4.6. サービスポータルの動作例

の画面には，有効なサービスが強調して示される．これらの有効なサービスへは直にリンクが貼られているため，容易に利用を開始できる．

なお，本試作システムでは，一定周期でサービス可否判定を繰り返し行っている．ユーザのプレゼンスや周囲の状況変化により利用可能なサービスが変わると，図 4.6 の利用可能なサービス一覧を切り替えて表示する．

6. 実験

信用管理システムにプレゼンスを組み込むにあたって，プレゼンス推論エンジンの評価が重要である．信用導出においては，安全性のために，被験者 s が実際には位置 l に居ない時に,「s が高い確率 (ポリシ内で定められた閾値 θ 以上の確率) で l に居る」とプレゼンス推論エンジンが出力する回数，すなわち false positive をできる限り少なくすることが望まれる．一方，利便性のためには，s が l に居る時に,「s が高い確率 (ポリシ内で定められた閾値 θ 以上の確率) で l に居る」と

プレゼンス推論エンジンが出力する回数を最大化することが望まれる．すなわち false negative をできる限り少なくする必要がある．そこで，上記を評価するため *precision* と *recall* の尺度を導入する．被験者を s，位置を l，閾値を θ とし，A を s が実際 l に存在していた事実の集合，R はプレゼンス推論エンジンが s が確率 $p \geq \theta$ 以上で l に居ると推論した結果の集合としたとき，*precision* と *recall* は次のように定義される．ここで $|S|$ は集合 S の要素数を意味する．

$$precision := \frac{|A \cap R|}{|R|} \qquad recall := \frac{|A \cap R|}{|A|}.$$

false positive は $1 - precision$ として，false negative は $1 - recall$ として見積もることができる．

6.1 設定

あるビル内のいくつかの位置を約 30 分かけて移動するシナリオ (図 4.7) を用意し，6 名の被験者 (a〜f と呼ぶ) によるシナリオ実験を通じて，上記の尺度のもと評価を実施した．センサネットワークを介し，プレゼンス推論エンジンの入力として用いるセンサ出力を 6 秒 (0.1 分) 毎に記録した．センサネットワークと HMM の設計について以下に詳細に述べる．

センサネットワーク　本実験においてプレゼンス推論エンジンは RFID リーダを組み込んだセンサで構成されるセンサネットワークと接続される．各被験者はアクティブ RFID タグをビル内で持ち運ぶ．ビル内のあるフロアに，おおよそ各部屋につき 1 個，計 7 個のセンサを設置する．各センサは RFID タグからの信号を受信する．制御用の計算機 (コントローラ) がセンサネットワーク内に存在し，コントローラはある被験者についてのプレゼンスを求められると，当該被験者の所有するタグからの信号を受信したセンサ自身のラベルを出力する．複数のセンサが同一のタグからの信号を受信している場合，コントローラは最大の受信強度を示したセンサのラベルを返す．もし，どのセンサも当該被験者のタグからの信号を受信してない場合，コントローラは “no signal.” を返す．

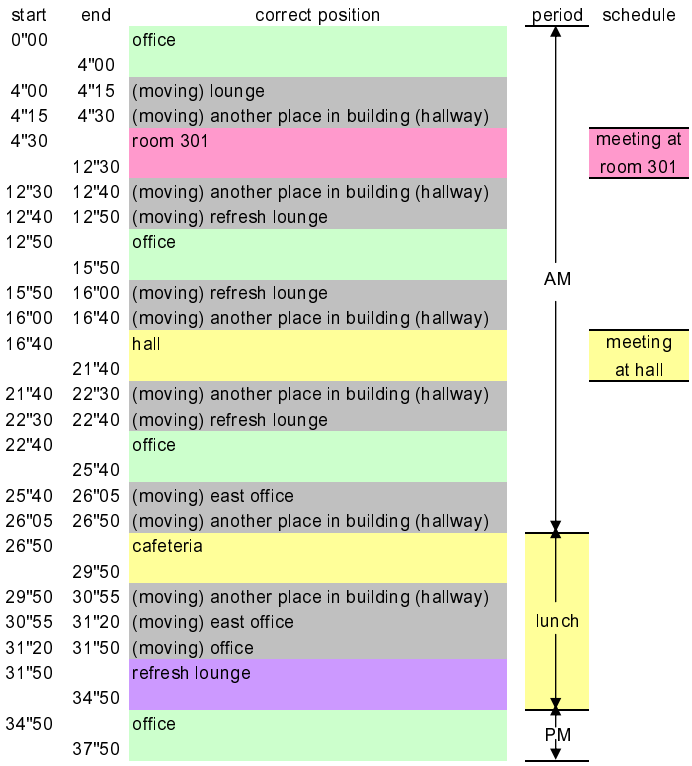

図 4.7. 実験シナリオ

HMM の設計　HMM の確率変数の取り得る値は，以下の通りとする．

- 出力記号 (x_t の値): 以下の 8 つの記号の集合．
  - 7 つの位置 (部屋) 各部屋のセンサのラベル: room_301, room_302, refresh_corner, lounge, office, east_office, laboratory.
  - 1 つの特別な記号 “no signal.”
- 位置 (π_t の値): 以下の 10 個の位置の集合．
  - センサの置かれた 7 つの位置 (部屋)
  - センサの無い 2 つの位置: hall, cafeteria.
  - 1 つの仮想的な位置 ‘another_place_in_building.’
- 時間帯 (y_t の値): AM, lunch, PM, off.

- 予定 (z_t の値):

  meeting_at_room 301, meeting_at_room 302, meeting_at_hall, no_plan.

HMM のパラメタ $\Pr(\pi_t \,|\, \pi_{t-1})$，$\Pr(\pi_t \,|\, y_t)$，$\Pr(\pi_t \,|\, z_t)$ については，ビル内の被験者の普段の行動を参照し人手によって定めた．実行開始時に存在する確率は office に対して 1 を，それ以外に対して 0 を割り当てた．持続長分布はシナリオに応じて定めた．各位置 l で，ラベル l を出力する確率に関し，0.9 以上の値を $\Pr(x_t = l \,|\, \pi_t = l)$ (またはセンサが l に無い場合 $\Pr(x_t = \text{no\_signal} \,|\, \pi_t = l)$) に割り当てた．一方，$l$ 以外を出力する確率に関しては 0.02 以下の値を割り当てた．ただし，幾つかの隣接する部屋 (l, l') では，センサネットワークから正解の部屋の隣の部屋に置かれたセンサのラベルが出力されることがあった．そこで，$\Pr(x_t = l \,|\, \pi_t = l')$ と $\Pr(x_t = l' \,|\, \pi_t = l)$ については，比較的高い確率 (0.13) を与えた．さらに，本実験環境においては部屋 room 301 のセンサがしばしば被験者のタグを見失うことがあった．そのため，出力確率の分布を以下のように修正した．

$$\Pr(x_t \,|\, \text{room\_301}) = \begin{cases} 0.5 & \text{if } x_t = \text{room 301} \\ 0.44 & \text{if } x_t = \text{no\_signal} \\ 0.01 & \text{それ以外.} \end{cases}$$

4.3 項における重み α と β は $\alpha = 1/(1 + r_{\beta,t} + r_{\gamma,t})$，$\beta = r_{\beta,t}/(1 + r_{\beta,t} + r_{\gamma,t})$ として定めた．ここで $r_{\beta,t}$ と $r_{\gamma,t}$ は，以下のように時間帯 lunch と明記された予定の有無を重視して定めるものとした．

$$r_{\beta,t} = \begin{cases} 10 & \text{if } y_t = \text{lunch} \\ 1 & \text{if } y_t = \text{off} \\ 0 & \text{それ以外.} \end{cases} \qquad r_{\gamma,t} = \begin{cases} 10 & \text{if } z_t \neq \text{no\_plan} \\ 0 & \text{if } z_t = \text{no\_plan.} \end{cases}$$

より正確な状態遷移確率や出力確率を設定するために，実データを使った学習の適用を検討できる．即ち，実際のセンサ情報や滞在位置の記録を使って，それに合致するような HMM パラメータ値を求めることが可能である．学習のためのデータとして，出力記号 (センサ情報) とそのときの状態（真の滞在位置）が得られる場合には，容易に最尤推定が行える．しかし，真の滞在位置を長時間記録

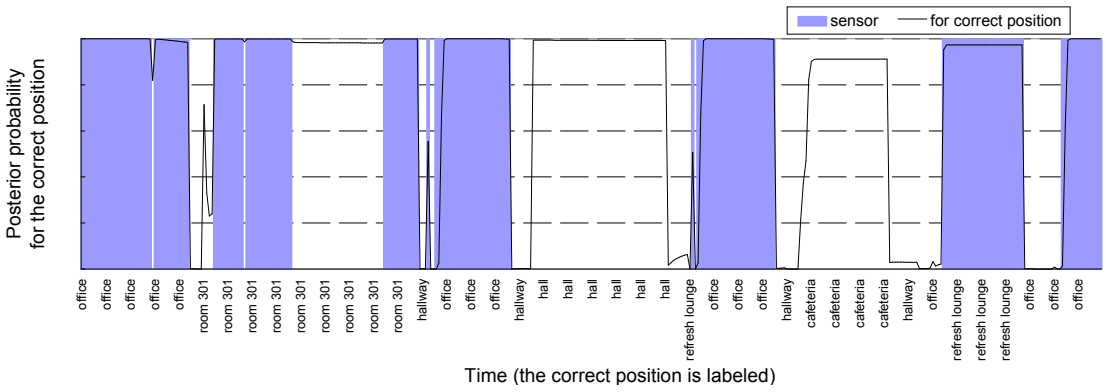

図 4.8. 被験者 a の正解位置に関する事後確率

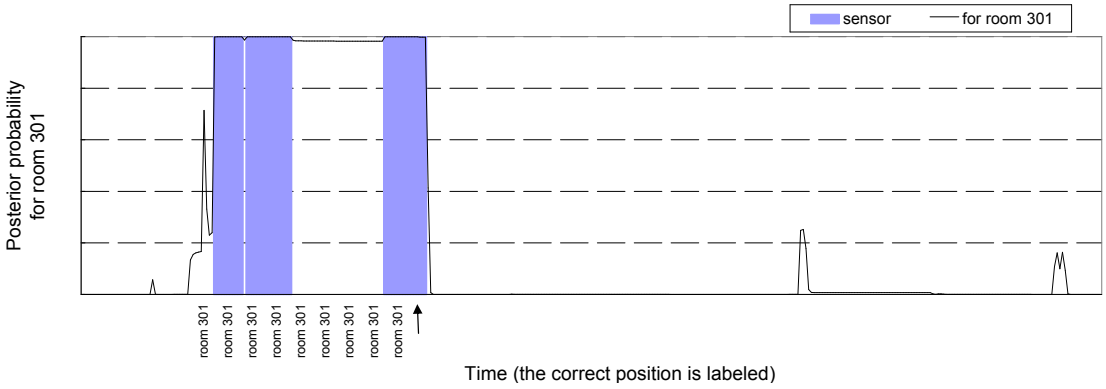

図 4.9. 被験者 a の位置 room 301 に関する事後確率

することは通常は困難である．学習のためのデータとして出力記号のみ得られる場合に用いることができる学習アルゴリズムとして，Baum-Welch アルゴリズム [68] がよく知られている．これは EM アルゴリズムと呼ばれる学習法の一種であり，反復的にパラメータの改良を行っていく．反復ごとに尤度が単調増加することが保証される（ただし局所最適解に陥ることもある）．

6.2 実験結果

図 4.8，図 4.9 は，プレゼンス推論エンジンの出力結果である，ある一人の被験者 a に対する正解位置に存在する事後確率を示す．両図において，横軸下に縦書

きされているラベルが，被験者 a の正解位置である．図 4.8 において，実線は各時刻における正解位置に居る事後確率を表し，矩形は各時刻においてセンサネットワークからの出力が正解位置を示したことを表している．この図から，プレゼンス推論の *recall* の概要が読み取れる．すなわち，矩形を確認できる時刻において，事後確率が低い場合は，プレゼンス推論の false negative を表し，矩形が示されていない時刻はセンサの出力が false negative であることを意味する．被験者がある位置から別の位置へ移動する間，正解位置に対する事後確率が低くなる (プレゼンス推論の結果が false negative である) が，それ以外のほとんどの場合，0.9 以上となっている．これは，プレゼンス推論エンジンを使用する場合において，ポリシ内で閾値を 0.9 以下に設定することで良い *recall* を得られるということを意味し，プレゼンスを考慮する信用管理アプリケーションの利便性を向上させる．図 4.9 では，実線で正解位置に関わらず各時刻における room 301 に居る事後確率を表し，矩形で各時刻においてセンサネットワークからの出力が room 301 を示したことを表している．これらから，プレゼンス推論の *precision* が説明される．すなわち，正解位置が room 301 では無い位置に時刻において，事後確率が高い箇所は，プレゼンス推論の結果が false positive であり，矩形が示されている時刻はセンサ出力の false positive と言える．センサ出力の false positive が，room 301 では無くなった直後の時刻 (図 4.9 で横軸下のラベルが上矢印の箇所) において発生していることに注意されたい．図 4.9 では, 正解位置が room 301 では無いとき，ほとんどの時刻において，room 301 に居る事後確率が 0.3 を下回っている．つまり，閾値を 0.3 以上に設定することで良い *precision* を得られるということを意味する．

いくつかの閾値を設定したときの，room 301 に関する *precision* と *recall* を表 4.1 に示す．一番下の行はセンサネットワークからの出力に関する *precision* と *recall* を示す．この表によると，ポリシ内に 0.3 から 0.9 の間の閾値を設定した場合に，センサネットワークの出力に基づく場合 (被験者 a について 0.513，全被験者の平均で 0.783) よりも，プレゼンス推論エンジンの推論結果に基づく場合 (0.94 以上) のほうが，*precision* を低下させること無く，より高い *recall* が得られたことがわかる．

表 4.1. room 301 に関する *precision* と *recall*

	被験者 a		平均	
θ	*precision*	*recall*	*precision*	*recall*
0.9	0.962	0.95	0.911	0.940
0.8	0.962	0.95	0.911	0.940
0.7	0.963	0.963	0.912	0.946
0.6	0.963	0.963	0.910	0.946
0.5	0.963	0.963	0.906	0.946
0.4	0.951	0.963	0.905	0.948
0.3	0.951	0.975	0.901	0.95
0.2	0.930	1	0.899	0.963
0.1	0.842	1	0.848	1
0	0.212	1	0.212	1
センサ	0.932	0.513	0.895	0.783

センサネットワークからの出力をそのまま利用する場合に比べ，プレゼンス推論エンジンの導入により高い *recall* を得られることは，利便性の向上に繋がる．つまり,「ある位置 l に居るユーザに対し，リソースへのアクセスを認める」というポリシを与える場合において，プレゼンス推論エンジンにより，アクセスを許可すべき状況において，許可する確率を高くできると考えられる．一方,「ある位置 l に居るユーザに対し，リソースへのアクセスを認めない」というポリシを与える場合，高い *recall* は信頼性の向上に繋がる．つまり，アクセスを許可すべきでない状況において，許可しない確率を高くできると考えられる．

7. おわりに

本章では，物理的な環境下におけるアクセス制御 (フィジカルセキュリティ) を目的に，信用判定の基準として各種デジタル証明書に加え，ユーザのプレゼンスを導入したプレゼンスアウェア信用管理システムを提案した．プレゼンスの導入に際しては，プレゼンスに信頼度というパラメータを与え，確率モデルに基づく信頼度評価によってプレゼンスの不確実性を考慮した．具体的には，隠れマルコ

フモデルに人の行動特性を反映した状態遷移確率を与え，センサから直接導かれるプレゼンスの観測結果から，その信頼度を推論する方式を導入した．この信用管理システムをネットワークアクセス制御システムのバックエンドとし，プレゼンスを信用確立に利用してアクセス制御を実施する評価を実施したところ，センサから直接得たプレゼンスを利用するよりも，利便性や安全性を向上できることを確認した．

第5章　結論

センサネットワークを利用したサービスの安全な実現のために，情報セキュリティとフィジカルセキュリティの両面での研究が必要である．情報セキュリティに関する取り組みとして，グループでの鍵管理方式とアドホックな鍵生成方式について検討を行った．また，フィジカルセキュリティに関する取り組みとして，物理的なアクセス制御方式について述べた．

最初に，センサネットワークの多くの応用が要求するグループ通信の情報セキュリティのために，一台のノードが複数の大規模グループに所属する場合に有効に作用するグループ鍵管理方式を提案した．提案方式は，ノードの属性に紐つける管理情報を用いて，個々のグループ鍵の管理の仕組みを互いに連携させることで，従来に比べ，管理上の負荷を低減できる．センサネットワークの運用においては，設置位置や機能などの概念的に直交する多くの視点でグループを定義できるため，これらの複数グループを管理できる本方式は有用であると考えられる．

次に，初見の端末同士でアドホックな通信路を安全に開設するための動的な鍵生成法を提案した．提案方式では，日常的な動作を利用して鍵生成を行う．具体的に，加速度センサから抽出する特徴量を判定し，類似度に応じて強度の異なる鍵を生成する手法を採用した．性能評価の結果，中程度以上の類似度を示す対に対し，高々2 分程度で，4 桁の PIN コード相当の強度を持つ共通鍵を共有できることが明らかになった．

最後に，センサネットワークを利用したシステムにおけるフィジカルセキュリティに関する研究として，センサネットワークにおける機能そのものを有効利用するアクセス制御システムについて提案した．提案方式では，信用管理の新たなシステムアーキテクチャとして，信用の確立に利用する情報として，ユーザが提示したディジタル証明書に加え，そのユーザや関係者のプレゼンス (存在位置) を

導入した．プレゼンスの導入に際しては，プレゼンスに信頼度というパラメータを与え，確率モデルに基づく信頼度評価によってプレゼンスの不確実性を考慮した．評価実験を通じて，センサから直接得るプレゼンスを用いるよりも，信用確立の際の利便性や安全性を向上できることを明らかにした．

ユビキタスの概念を提唱した Mark Weiser の論文“ The Computer for the 21st Century ”は,“ The most profound technologies are those that disappear. ”（最も深遠な技術は見えなくなる技術である）という文章で始まった [69]．これは，コンピュータが社会にすっかり溶け込みあたかも消えてしまうことを示したものであり，センサネットワークの浸透した社会に関してもあるべき姿を示している．見えないという特徴は人に無用な注意を喚起しないという意味では優れている．しかし，ユーザの活動に関する詳細な情報が意識せずに知られてしまうという点においては，プライバシ侵害の危惧が付きまとう．本研究は，ユーザが情報の提供を望まない条件があるならば，暗号化や認証の安全性の根拠となる鍵情報の管理やアクセス制御の観点で，それを容易に実行できる仕組みを与える．

センサネットワークおよびそれに基づくサービスの普及は，サービス提供者の便益のみならずユーザの便益を考慮しなければ不可能である．ユーザの便益は，サービス価値とプライバシ侵害への危惧のバランスで決まる．本研究は一定のサービス価値に対するユーザ便益の向上に関して，一つの回答を与えるものとなっていると確信している．

参考文献

[1] ～センサーネットワーク特集（前編）～ リアルタイムマネジメントを実現するセンサーネットワークの可能性，NEC ユビキタスネットワーク JOURNAL(オンライン)，入手先〈http://www.nec.co.jp/effort/ubiquitous/2006_0217/〉(参照 2010-12-16).

[2] 無線センサーネットワークで環境に配慮した街づくりを支援　愛・地球博で「万博アメダス」が活躍，NEC ユビキタスネットワーク JOURNAL(オンライン)，入手先〈http://www.nec.co.jp/effort/ubiquitous/2005_0819/〉(参照 2010-12-16).

[3] ユビキタスセンシングで切れ目のない食品の高度トレーサビリティを実現！～高機能電子タグによる飛騨牛の温度管理履歴閲覧実証実験（後編）～，NEC ユビキタスネットワーク JOURNAL(オンライン)，入手先〈http://www.nec.co.jp/effort/ubiquitous/hidanec/index.html〉(参照 2010-12-16).

[4] 柏市において総務省委託研究「ユビキタス・プラットフォーム技術の研究開発」の実証実験を実施，NEC プレスリリース (オンライン)，入手先〈http://www.nec.co.jp/press/ja/1011/0201.html〉(参照 2010-12-16).

[5] B. C. Neuman and T. Ts’o, Kerberos: An authentication service for computer networks, IEEE Communications Magazine, Vol.32, No.9, pp.33-38, 1994.

[6] 阪田史郎 (編著)，ZigBee センサネットワーク通信基盤とアプリケーション，pp.118-120，秀和システム,2005.

[7] L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks, Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.41-47, 2002.

[8] H. Chan, A. Perrig and D. Song, Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, pp.197-213, 2003.

[9] H. Chan and A. Perrig, PIKE: Peer intermediaries for key establishment in sensor

networks, Proceedings IEEE INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies, pp.524-535, 2005.

[10] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, Perfectly-secure key distribution for dynamic conferences, Advances in cryptology-CRYPTO'92, pp.471-486, 1993.

[11] D. Liu, P. Ning and R. Li, Establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security (TISSEC), Vol.8, No.1, pp.41-77, 2005.

[12] R. Blom, An optimal class of symmetric key generation systems, Advances in Cryptology: Proceedings of EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, April 1984, pp.335, 1985.

[13] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz and A. Khalili, A pairwise key predistribution scheme for wireless sensor networks, ACM Transactions on Information and System Security (TISSEC), Vol.8, No.2, pp.258, 2005.

[14] D. Liu, P. Ning and W. Du, Group-based key predistribution for wireless sensor networks, ACM Transactions on Sensor Networks (TOSN), Vol.4, No.2, pp.1-30, 2008.

[15] D. Liu and P. Ning, Location-based pairwise key establishments for static sensor networks, Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, pp.72-82, 2003.

[16] J. M. Jeong and Z. J. Haas, Predeployed secure key distribution mechanisms in sensor networks: current state-of-the-art and a new approach using time information, IEEE Wireless Communications, Vol.15, No.4, pp.42-51, 2008.

[17] M. V. D. Burmester and Y. Desmedt, A secure and efficient conference key distribution system, Advances in Cryptology-EUROCRYPT'94, pp.275-286, 1995.

[18] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, SPINS: Security protocols for sensor networks, Wireless networks, Vol.8, No.5, pp.521-534, 2002.

[19] C. K. Wong, M. Gouda and S. S. Lam, Secure group communications using key graphs, Proceedings of the ACM SIGCOMM'98 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp.68-79, 1998.

[20] L. Lazos and R. Poovendran, Energy-aware secure multicast communication in ad-hoc networks using geographic location information, IEEE International Conference on Acoustics Speech and Signal Processing, Vol.4, pp.201-204, 2003.

[21] T. Funayama, S. Imamura and E. Okamoto, Efficient key distribution system using communication probability, IPSJ SIG Notes, Vol.2006, No.43, pp.1-6, 2006.

[22] A. T. Sherman and D. A. McGrew, Key establishment in large dynamic groups using one-way function trees, IEEE Transaction Software Engineering, Vol.29, No.5, pp.444-458, 2003.

[23] E. Jung, A. X. Liu and M. G. Gouda, Key bundles and parcels: Secure communication in many groups, Computer Networks, Vol.50, No.11, pp.1781-1798, 2006.

[24] S. Zhu, S. Setia and S. Jajodia, LEAP: Efficient security mechanisms for large-scale distributed sensor networks, Proceedings of the 10th ACM Conference on Computer and Communication Security, ACM Press, New York, pp.62-72, 2003.

[25] D. Liu, P. Ning and K. Sun, Efficient self-healing group key distribution with revocation capability, Proceedings of the 10th ACM conference on Computer and communications security, pp.231-240, 2003.

[26] R. Dutta, E. C. Chang and S. Mukhopadhyay, Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains, Applied Cryptography and Network Security, Vol.4521, pp.385-400, 2007.

[27] S. Guo, A. N. Shen and M. Guo, A secure and scalable rekeying mechanism for hierarchical wireless sensor networks, IEICE Transaction on Information and systems, Vol.93, No.3, pp.421-429, 2010.

[28] W. Diffie and M. Hellman, New directions in cryptography, IEEE Transaction on Information Theory, Vol.22, No.6, pp.644-654, 1976.

[29] 岡田昌也，角辰己，細川拓央，SD カードおよび IC カード用システム LSI, Matsushita Technical Journal, Vol.52, No.1, pp.104-109, 2006.

[30] 下田宏，大林史明，オフィスビルの省エネルギーとプロダクティビティ照明, 電気学会論文誌 C(電子・情報・システム部門誌), Vol.128, No.1, pp.2-5, 2008.

[31] 野田潤，楫勇一，毛利寿志，仁野裕一，中尾敏康，複数の属性分割を利用したセンサネットワーク向け鍵管理方式の実装と評価，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム，pp.524-529, 2007.

[32] 古川恭史，萬代雅希，渡辺尚，指向性アンテナを利用した送信レート制御ブロードキャストについて，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2009）シンポジウム，pp.576-584, 2009.

[33] 斎藤秀雄，田浦健次朗，近山隆，適応スパニングツリーを用いた広域メッセージパッシングシステム用の集合通信 (ネットワーク)，情報処理学会論文誌コンピューティングシステム，Vol.46, No.12, pp.373-383, 2005.

[34] 西原秀明，窪田裕介，村川友章，芳賀博英，金田重郎，焦電センサと RFID による室内向け物品位置検出手法，情報処理学会第 69 回全国大会，Vol.3, pp.279-280, 2007.

[35] IEEE 802.15 Working Group for WPAN Task Group 6 (TG6) Body Area Networks. http://www.teu.ac.jp/media/ earth/FK/.

[36] R. Schmidt, T. Norgall, J. Morsdorf, J. Bernhard and T. von der Grun, Body Area Network BAN, A key infrastructure element for patient-centered medical applications, Biomedizinische Technik, pp. 365-368, 2002.

[37] J. Lester, B. Hannaford and G. Borriello, ”Are You With Me? ”- Using accelerometers to determine if two devices are carried by the same person. In Proceedings of the 2nd International Conference on Pervasive Computing (Perva-

sive2004), Lecture Notes in Computer Science 3001, pp. 33-50, Springer-Verlag, 2004.

[38] 行方エリキ, 石原進, 水野忠則, 携帯端末の動きによる個人認証　～コヒーレンスに基づく評価～. 情報処理学会研究報告, No. 2004-UBI-7, pp. 37-44, 2005.

[39] Y. Huynh and B. Schiele, Analyzing features for activity recognition. In Proceedings of the 1st Joint Conference on Smart Objects and Ambient Intelligence (sOc-EUSAI ’05), pp. 159-163. ACM Press, 2005.

[40] D. Bichler, G. Stromberg, M. Huemer and M. Low, Key generation based on acceleration data of shaking processes, In Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp2007), Lecture Notes in Computer Science 4717, pp. 304-417. Springer-Verlag, 2007.

[41] R. Mayrhofer and H. Gellersen, Shake well before use: Authentication based on accelerometer data, In Proceedings of the 5th International Conference on Pervasive Computing (Pervasive2007), Lecture Notes in Computer Science 4480, pp. 144-161. Springer-Verlag, 2007.

[42] 仁野裕一, 野田潤, 中尾敏康, 携帯電話の操作履歴情報を利用した認証方式の提案. マルチメディア，分散，協調とモバイル (DICOMO2007) シンポジウム論文集, 2007.

[43] 小川晶子, 小西勇介, 柴崎亮介，自立型ポジショニングシステム構築に向けて～着用型センサーを用いた人間の行動モード推定～，全国測量技術大会 2002 学生フォーラム発表論文集, 2002.

[44] 瀬古俊一, 西野正彬, 青木政勝, 山田智広, 武藤伸洋, 阿部匡伸，誤差情報を考慮した同行判定手法，情報処理学会研究報告, No. 2008-UBI-20, pp. 65-72, 2008.

[45] 南貴博, 仁野裕一, 野田潤, 中村嘉隆, 関浩之，ユーザの動作類似度に基づく共通鍵生成法. 情報処理学会研究報告, No. 2009-CSEC-44, 2009.

[46] KDDI 株式会社，本人認証装置，特願 2006-12408, January 2006.

[47] R. Aylward, S. D. Lovell and J. A. Paradiso, A compact, wireless, wearable sensor network for interactive dance ensembles. In Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks (BSN2006), pp. 65-68. IEEE Computer Society Press, 2006.

[48] R. Marin-Perianu, M. Marin-Perianu, P. Havinga and H. Scholten, Movement-based group awareness with wireless sensor networks. In Proceedings of the 5th International Conference on Pervasive Computing (Pervasive2007), Lecture Notes in Computer Science 4480, pp. 298-315. Springer- Verlag, 2007.

[49] L. Bao, S. S. Intille, Activity Recognition from User-Annotated Acceleration Data, In Proceedings of the 2nd International Conference on Pervasive Computing (Pervasive2004), Lecture Notes in Computer Science 3001, pp. 1-17, Springer-Verlag, 2004.

[50] 小林亜令，岩本健嗣，西山智，釈迦：携帯電話を用いたユーザ移動状態推定方式. 情報処理学会論文誌, vol.50, No.1, pp. 193-208, 2009.

[51] 佐川貢一, 煤孫光俊, 猪岡光，加速度積分による 3 次元歩行移動量の無拘束計測. 計測自動制御学会東北支部第 202 回研究集会資料 (202-10), 2002.

[52] J. Al-Muhtadi, A. Ranganathan, R. Campbell and M. D. Mickunas, Cerberus: a context-aware security scheme for smart spaces, IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom), pp. 489-496, 2003.

[53] E. Bertino, B. Catania, M. L. Damiani and P. Perlasca, GEO-RBAC: A spatially aware RBAC, 10th ACM Symp. on Access Control Models and Technologies (SACMAT), pp. 29-37, June 2005.

[54] M. Blaze, J. Feigenbaum and J. Lacy, Decentralized trust management, IEEE Security and Privacy, pp. 164-173, 1996.

[55] M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis, The KeyNote trust-management system, RFC 2704, 1999.

[56] M. J. Covington, W. Long, S. Srinivasan, A. K. Dey, M. Ahamad and G. D. Abowd, Securing context-aware applications using environment roles, 6th

ACM Symp. on Access Control Models and Technologies (SACMAT), pp. 10-20, May 2001.

[57] C. M. Ellison, B. Frantz, B. Lampson, R. L. Rivest, B. M. Thomas and T. Ylonen, SPKI certificate theory, RFC 2693, 1999.

[58] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, Bayesian filtering for location estimation, IEEE Pervasive Computing, Vol. 2, No. 3, pp. 24-33, 2003.

[59] A. Herzberg, Y. Mass, J. Mihaeli, D. Naor and Y. Ravid, Access control meets public key infrastructure, or, assigning roles to strangers, IEEE Security and Privacy, pp. 2-14, 2000.

[60] R. J. Hulsebosch, A. H. Salden, M. S. Bargh, P. W. G. Ebben and J. Reitsma, Context sensitive access control, 10th ACM Symp. on Access Control Models and Technologies (SACMAT), pp. 111-119, June 2005.

[61] J. Krumm, G. Cermak, and E. Horvitz, RightSPOT: a novel sense of location for a smart personal object, UbiComp 2003, Lecture Notes in Computer Science 2864, pp. 36-43, 2003.

[62] J. Krumm, L. Williams, and G. Smith, SmartMoveX on a graph — an inexpensive active badge tracker, UbiComp 2002, Lecture Notes in Computer Science 2498, pp. 299-307, 2002.

[63] D. J. Patterson, L. Liao, D. Fox, and H. Kautz, Inferring high-level behavior from low-level sensors, UbiComp 2003, Lecture Notes in Computer Science 2864, pp. 73-89, 2003.

[64] L. R. Rabiner and B. H. Juang, An introduction to hidden Markov models, IEEE ASSP Magazine, Vol. 3, No. 1, pp. 4-16, 1986.

[65] J. Rosenberg, A presence event package for the Session Initiation Protocol (SIP), RFC 3856, 2004.

[66] K. E. Seamons, M. Winslett, T. Yu, B. Smith, E. Child, J. Jacobson, H. Mills and L. Yu, Requirements for policy languages for trust negotiation, IEEE Int'l

Workshop on Policies for Distributed Systems and Networks (POLICY), pp. 68-79, 2002.

[67] Y. Yu, M. Winslett and K. E. Seamons, Interoperable strategies in automated trust negotiation, 8th ACM Conf. on Computer and Communications Security (CCS), pp. 146-155, 2001.

[68] 浅井潔, 確率モデルによる配列情報解析, 生物配列の統計, Part II, 岩波書店, 2003.

[69] M. Weiser, The Computer for the 21st Century. Scientific American, Vol. 265, No. 3, pp. 94-104, 1991.