JAIST Repository
https://dspace.jaist.ac.jp/

Title	ビッグデータ利活用とプライバシー保護の両立を実現するプライバシーマネジメントモデルの提案
Author(s)	荒井，正和
Citation	
Issue Date	2016-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/13730
Rights	
Description	Supervisor:小坂　満隆，知識科学研究科，修士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

修　士　論　文

ビッグデータ利活用とプライバシー保護の両立を実現する
プライバシーマネジメントモデルの提案

1350301　荒井正和

主指導教員　　小坂　満隆
審査委員主査　小坂　満隆
審査委員　　敷田　麻実
　　伊藤　泰信
　　白肌　邦生

北陸先端科学技術大学院大学
知識科学研究科

平成 28 年 8 月

目　次

第1章　序論・・1
1.1　研究の背景・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1
1.2　研究の目的・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2
1.3　研究方法とリサーチ・クエスチョン・・・・・・・・・・・・・・・・・・・・・・・・・3
1.4　本論文での構成・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・3
第2章　先行研究レビュー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・5
2.1　はじめに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・5
2.2　各国における個人情報の取扱いに関する法規制の状況・・・・・・・・・・・・・5
2.3　技術分野における取組み・・・・・・・・・・・・・・・・・・・・・・・・・・・・・8
2.3.1　PPDM (Privacy Preserving Data Mining)・・・・・・・・・・・・・・・・・・8
2.3.2　匿名化技術・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・9
2.3.3　暗号化と秘匿計算技術・・・・・・・・・・・・・・・・・・・・・・・・・・・・12
2.4　プライバシー保護プロセスにおける各種アプローチ方法・・・・・・・・・・・・14
2.4.1　個人情報保護法の体系・・・・・・・・・・・・・・・・・・・・・・・・・・・・14
2.4.2　個人情報保護法改正の背景と内容・・・・・・・・・・・・・・・・・・・・・・15
2.4.3　プライバシー・バイ・デザイン・・・・・・・・・・・・・・・・・・・・・・・・18
第3章　自治体における KDB システム利活用調査・・・・・・・・・・・・・・・・・・・・20
3.1　はじめに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・20
3.2　KDB システムの概要・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・21
3.2.1　ステークホルダーと関係性・・・・・・・・・・・・・・・・・・・・・・・・・・21
3.2.2　KDB システムの利用目的・・・・・・・・・・・・・・・・・・・・・・・・・・・22
3.3　自治体における取組み状況の予備調査・・・・・・・・・・・・・・・・・・・・・・23
3.3.1　対象・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・23
3.3.2　調査方法・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・23
3.3.3　調査結果・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・24
3.4　本調査・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・27
3.4.1　対象・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・27
3.4.2　調査方法・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・27

3.4.3　本調査結果と考察・・・・・・・・・・・・・・・・・・・・・・・・・・28
3.5　調査結果の分析・・・・・・・・・・・・・・・・・・・・・・・・・・・・・37
3.5.1　意識の重み付け・・・・・・・・・・・・・・・・・・・・・・・・・・37
3.5.2　自治体統計データとの相関関係・・・・・・・・・・・・・・・・・・・40
3.5.3　相関分析に関する考察・・・・・・・・・・・・・・・・・・・・・・・44
3.5.4　組織変革へのアプローチ・・・・・・・・・・・・・・・・・・・・・・47
第4章　アクティブ・プライバシー・マネジメントモデルの提案・・・・・・・・・・・・・・48
4.1　はじめに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・48
4.2　アクティブ・プライバシー・マネジメントモデル・・・・・・・・・・・・・・・・49
第5章　結論と含意・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・53
5.1　結論・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・53
5.2　理論的含意・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・54
5.3　実務的含意・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・54
5.4　将来研究への示唆・・・・・・・・・・・・・・・・・・・・・・・・・・・55
参考文献・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・57
付録・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・61

図　目　次

図 1-1　売上向上効果（総務省(2014)より）・・・・・・・・・・・・・・・・・・・・・・・・1
図 1-2　本研究における背景・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2
図 2-1　PPDM の分類（「@IT」匿名化技術と PPDM(2015) より）・・・・・・・・・・・・・・・・8
図 2-2　購買履歴の例・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・9
図 2-3　購買履歴を仮名化処理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・10
図 2-4　購買履歴を無名化処理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・10
図 2-5　購買履歴をｋ－匿名化処理・・・・・・・・・・・・・・・・・・・・・・・・・・・11
図 2-6　完全準同型暗号に基づく秘密計算処理（出典：情報処理 Vol54（2013））・・・・12
図 2-7　セキュアマルチパーティ計算処理（出典：情報処理 Vol54（2013））・・・・・・13
図 2-8　エストニア国　sharemind プロジェクト公式 HP・・・・・・・・・・・・・・・・・13
図 2-9　個人情報保護法体系（出典：個人情報保護委員会 HP）・・・・・・・・・・・・・14
図 3-1　ステークホルダーと関係図・・・・・・・・・・・・・・・・・・・・・・・・・・・21
図 3-2　データ分析イメージ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・22
図 3-3　利活用に対する意識調査結果・・・・・・・・・・・・・・・・・・・・・・・・・・25
図 3-4　本人通知の予定・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・26
図 3-5　統計情報の利用種別・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・28
図 3-6　データ分析への保健師の関与度合い・・・・・・・・・・・・・・・・・・・・・・・29
図 3-7　利活用の効果・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・30
図 3-8　課題や問題点・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・31
図 3-9　ビッグデータのリスク認識度・・・・・・・・・・・・・・・・・・・・・・・・・・32
図 3-10　リスクへの態度・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・33
図 3-11　プライバシーポリシー公開の有無・・・・・・・・・・・・・・・・・・・・・・・34
図 3-12　利活用の効果指標・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・37
図 3-13　リスク指標・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・37
図 3-14　利活用とリスク意識のポジショニングマップ・・・・・・・・・・・・・・・・・・38
図 3-15　特定健診受診率および指導対象者比率・・・・・・・・・・・・・・・・・・・・・40
図 3-16　高齢者（65 歳以上）比率・・・・・・・・・・・・・・・・・・・・・・・・・・・41
図 3-17　一人当たり医療費（年間）・・・・・・・・・・・・・・・・・・・・・・・・・・42

図 3-18　人口に占める要介護認定者比率・・・・・・・・・・・・・・・・・・・・・・・・・43
図 3-19　利活用とプライバシーリスク意識から見た組織タイプ・・・・・・・・・・・・・44
図 3-20　課題創出＆解決型組織へのアプローチ・・・・・・・・・・・・・・・・・・・・46
図 4-1　アクティブ・プライバシー・マネジメントモデル・・・・・・・・・・・・・・・・49
図 4-2　価値転換チェーン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・51

表　目　次

表 2-1　米国の医療関連システム・データと関連制度（出典：日立(2011)より筆者編集）・・5
表 2-2　カナダの医療関連システム・データと関連制度（出典：日立(2011)より筆者編集）・6
表 2-3　英国の医療関連システム・データと関連制度（出典：日立(2011)より筆者編集）・・7
表 2-4　医療分野における個人情報保護ガイドライン・・・・・・・・・・・・・・・・・・・15
表 2-5　個人情報保護法　改正ポイント・・・・・・・・・・・・・・・・・・・・・・・・・16
表 3-1　個人情報審議会議事録の調査結果・・・・・・・・・・・・・・・・・・・・・・・・24
表 3-2　被保険者への通知パターン・・・・・・・・・・・・・・・・・・・・・・・・・・・35
表 3-3　統計データ（自治体 H、K、O、P）・・・・・・・・・・・・・・・・・・・・・・・45
表 3-4　統計データ（自治体 A、J）・・・・・・・・・・・・・・・・・・・・・・・・・・・45
表 3-5　統計データ（自治体 B、C）・・・・・・・・・・・・・・・・・・・・・・・・・・・45

第１章序論

1.1　研究の背景

IT 技術の飛躍的な進歩に伴い、いわゆるビッグデータを活用した新たなイノベーション創出が我が国の産業発展に寄与することが期待されている（宇賀 2014）。図 1－1 に示すように、データの高度な利活用による業務・サービス革新が我が国経済および社会に与える波及効果に係る調査研究（総務省 2014）によれば、ビッグデータ活用による経済効果について、生活関連サービス・娯楽業、医療・福祉産業分野で、売上向上効果が大きいという試算もあり、国を挙げての取り組みが必要である。

産業	売上向上率
農林・水産・鉱業	2.8%
建設・土木	11.5%
製造業	9.7%
電気・ガス・熱供給・水道業	7.8%
情報通信業	18.4%
運輸・郵便業	21.4%
金融・保険業	14.5%
不動産・物品賃貸業	10.2%
学術研究・専門技術者	17.9%

産業	売上向上率
宿泊・飲食サービス業	11.3%
生活関連サービス・娯楽業	25.3%
教育・学習支援業	13.2%
医療・福祉	24.7%
複合サービス業	20.3%
その他サービス業	9.3%
上記以外の業種	27.5%
総計	11.5%

図　1-1　売上向上効果（総務省(2014)より）

いっぽうで、パーソナルデータ（個人に関する情報）の利活用については、保護すべき情報の範囲やルールが曖昧になっており、個人のプライバシー侵害に係る問題も発生しており、企業側が利用に躊躇するケースが生じている。2013 年 6 月に、JR 東日本が Suica 利用データを利用者の許諾なく外部に提供した問題が社会的に取り上げられたことは記憶に新しい。これは、JR 東日本が Suica の利用データをマーケティング目的で日立（株）に提供する際に、利用者に十分な説明がないまま他社に提供したことが、プライバシー保護の観点から、社会的に問題となったものである。法的解釈では、提供されたデータは、乗降駅、利用日時、利用額、年齢、性別など個人情報に該当しないことから、違法性はなかったものの、プライバシー保護の観点で、法的保護の対象になりうるという世論の批判の的となったのである。個人情報に関して、何がどこまで自由に利活用で

きるのかが不明確な「グレーゾーン」が発生し、保護すべき情報の範囲や事業者が遵守すべきルールが曖昧になっていることが浮き彫りになった象徴的な事例である。

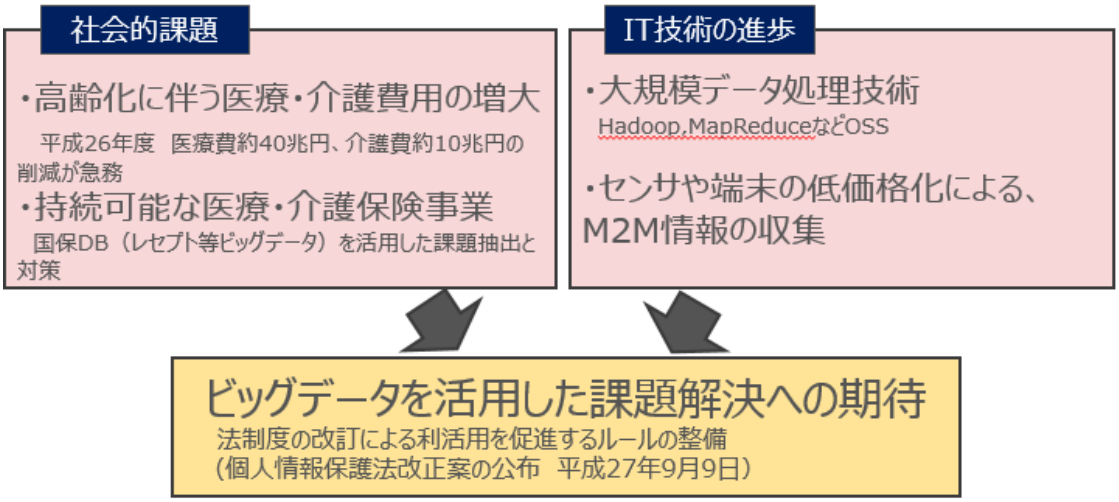

図　1-2　本研究における背景

これ以降、事業者側にとって個人情報をビジネスとして利用すること自体が「利活用の壁」となり、それを躊躇する要因になっているという認識がある。産業界全体が利活用に躊躇することなく、個人のプライバシー保護との双方のバランスを保ちながら、サービス価値創造を実現すること可能なプロセスを研究することが必要である。特に組織における利活用とリスク管理意識に焦点をあて、プライバシーリスクをマネジメントする実務的モデルを構築する。

1.2　研究の目的

本研究の目的は、ビッグデータの利活用とプライバシー保護の両立を可能とするリスクマネジメントモデルを提案することである。国民健康保健事業である、「健診・保健指導」、「医療」、「介護」における支援システムである国保データベースシステム（以下「KDB システム」という。）の活用事例分析を行い、リスクマネジメントモデルを構築する。

1.3　研究方法とリサーチ・クエスチョン

本研究では、KDB システムを用いた国民健康保健事業における自治体の取組みについて、先行研究から得られたプライバシー保護法制やプロセスのあり方、技術的な課題を踏まえ、組織に内在する利活用とリスク意識の実態をアンケート調査によって把握する。各自治体の構造的な課題とアンケート結果を重ね合わせ、組織タイプを類型化し、組織タイプ別のプライバシーマネジメントのアプローチ方法について実務的提言を加える。リサーチ・クエスチョンについては以下のように設定した。

メジャー・リサーチ・クエスチョン(MRQ)

ビッグデータの利活用とプライバシー保護の両立を実現するためのプライバシーマネジメントモデルは、どのようなものか？

サブシディアリー・リサーチ・クエスチョン(SRQ)

SRQ1：利活用の効果とリスク度合いにはどのような関係があるか？

SRQ2：リスクに対する効果的な IT 技術やルールにはどのような関係性があるか？

SRQ3：プライバシーマネジメントモデルは、組織におけるビッグデータ利活用の意思決定において、どのような影響を与えるか？

1.4　本論文の構成

本論文は５章構成となっている。第１章の序論では、研究の背景であるビッグデータの利活用ニーズと顕在化する問題、研究目的と研究方法についてまとめた。

第２章では、プライバシーマネジメントに関して法制度や匿名化等技術的な方法論について先行研究レビューを行う。また、医療分野における諸外国の取組みについても述べる。

第３章では、自治体における KDB システムの利活用調査と分析を実施する。

第４章では、前章の調査、分析結果を踏まえて、利活用とプライバシー保護の両立を実現するためのプロセスモデルである、アクティブ・プライバシー・マネジメントモデルを提案する。

第５章では、本研究の結論についてリサーチ・クエスチョンに対する回答と、理論的含意、実務的含意について述べる。

第２章先行研究レビュー

2.1　はじめに

先行研究レビューでは、国内における個人のプライバシー保護環境について、法整備と技術的側面から今後の動向も踏まえて調査をする。法整備については、主に個人情報保護法の改正内容とその効果について考察する。また技術的側面では、ビッグデータの解析過程で個人が識別または特定できてしまうという問題に対する技術的解決策としての、プライバシー保護データマイニング（以下「PPDM:Privacy-Preserving Data Mining」という。）の考え方について述べる。更にPPDMの構成要素である匿名化技術と暗号化技術についてフォーカスし、論文をもとに調査をする。また、本研究の対象となっているKDBシステムの利活用に関連し、一部諸外国のデジタルヘルスへの取り組みについても概観を加え、本研究で提案するビッグデータの利活用と保護の両立を実現する新しい概念に示唆を与えるものとなればいいと考えている。

2.2　各国における個人情報の取扱いに関する法規制の状況

米国、カナダ、英国における医療関連システム・データと関連する法制度について以下に示す。

表2-1　米国の医療関連システム・データと関連制度

（出典：日立（2011）より筆者編集）

	制度の内容
医療関連データの取扱い	・医療情報を専門に取扱う個別法として、2003年にHIPAAを整備 ・本人同意に基づいた収集を基本とする
二次利用に関する状況	・匿名化（非識別化）された医療情報の使用又は開示には制限なし ・保険者と医療機関が連携した医療の質の向上のためにデータを活用し、厳格な条件の下、個人情報を含むデータ

	の活用も可能とする

HIPAA は、医療情報の電子化推進とそれに関係するプライバシー保護やセキュリティ確保について規定した法律であり、すべての医療関連機関に適用される。医療機関に対しては、プライバシー保護方針を定めることや従業員への教育を求めている。

また二次利用に関しては、「Expert Determination」「Safe Harbor」方法のいずれかで匿名化すれば、使用又は開示には制限がないことも規定されている。Expert Determination は、提供された情報から個人が特定されるリスクが低いことを専門家が確認する方法であり、Safe Harbor とは個人の特定につながりうる１８項目の情報（氏名、住所、日付、電話番号、FAX 番号、電子メールアドレス、社会保障番号、カルテ番号、健康保険受給者番号、口座番号、証明書番号、車体番号、機器 ID、URL、IP アドレス、生態認証 ID、顔写真、その他の ID・特徴・コード）を取り除く方法である（森田ら、2014）。二次利用に関してはかなり厳格な基準とルールが明確になっていることが確認できる。

表 2-2　カナダの医療関連システム・データと関連制度

（出典：日立（2011）より筆者編集）

	制度の内容
医療関連データの取扱い	・医療情報の取扱いの詳細を、PHIPA のように州法で規定 ・本人同意に基づいた収集を基本とする
二次利用に関する状況	・匿名化（非識別化）された医療情報を活用することが可能 ・リスク判断のツールを活用した匿名化データを提供

カナダでは、行政部門と民間部門の双方を網羅する包括的な個人情報保護法は存在しない。連邦政府機関を対象とする Privacy Act、民間部門の PIPEDA がある。カナダの医療保険は連邦政府や各州で制度が異なるため、医療分野における制度も異なるものとなっている。オンタリオ州において制定された PHIPA では患者の同意にもとづき医療情報が利用できることとしている。また、同法４７条に匿名化することが二次利用の必須条件として規定している。匿名化することを求めている。

表 2-3　英国の医療関連システム・データと関連制度

（出典：日立（2011）より筆者編集）

	制度の内容
医療関連データの取扱い	・Data Protection Act という包括的なプライバシー保護の法制度を整備し、医療情報の取扱いも規定 ・本人同意に基づいた収集を基本とする
二次利用に関する状況	・本人同意なくパーソナルデータを活用するためには、本人識別性のあるデータが完全に無くなるように匿名化することが必要（医療に関するガイドライン「USE AND DISCLOSURE OF HEALTH DATA」で規定） ・国のサービスとして二次利用のためのデータを提供

Data Protection Act の特徴的な内容として、自分自身のプライバシー情報について、保有状況を知る権利、自分にとって不利益が生じる場合に、各人がデータ管理者に対してデータ処理を実施しないように要求できる権利も認めているなど、個人の権利利益を重視した内容となっている。

以上のように、米国、カナダ、英国を対象に法制度を概観した限りにおいては、各国共通に言えるのは、医療情報の利活用を推進していることである。その背景としては、医療関連データを分析することで、医療の質や費用対効果の向上を図る狙いが読み取れる。このことは、各国の医療システムと無関係ではない。例えば米国では皆保険制度が存在しないため、国民に対するあまねく公平な医療サービス提供に資するためには、医療の質向上を実現することが望まれている。

2.3　技術分野における取組み

2.3.1　PPDM (Privacy Preserving Data Mining)

プライバシー保護技術であるPPDMは、プライバシーを保護しながら分析活用する為の技術の総称であり、大別して３つの考え方がある。PPDMの分類を図2−1に示す。

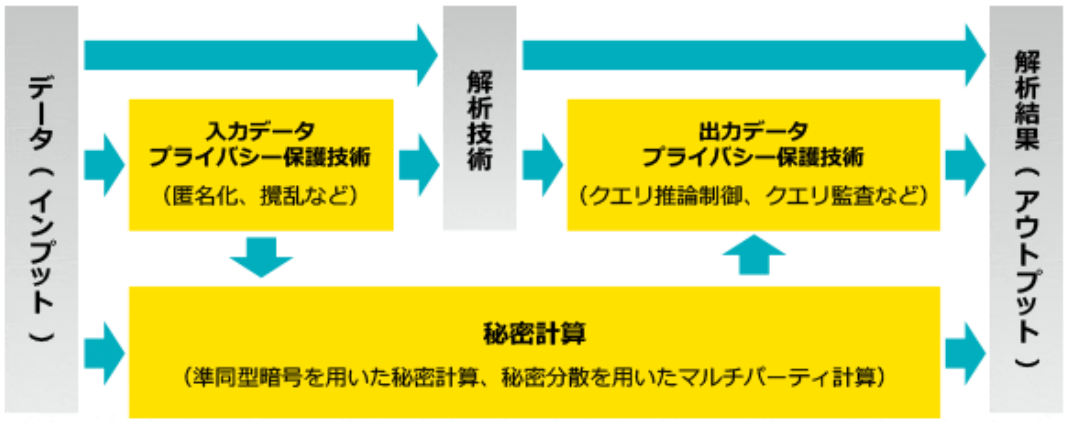

図　2-1　PPDMの分類（「@IT」匿名化技術とPPDM(2015) より）

・入力データに対するプライバシー保護技術であり、主に匿名化や一般化などの手法
・個々のデータを秘匿しつつ解析結果の抽出を可能とする、「秘密計算」技術
・出力されたデータを保護する技術であり、ノイズを加える等の方法

そもそもなぜ、PPDMの考え方が必要なのかは、後述する個人情報保護法改正内容に関係しているからである。改正点の中に、匿名加工情報の加工方法や取扱い規定の見直しがあるが、ここでいう匿名加工情報とは、特定の個人を識別できずかつ復元できないように加工された情報である。プライバシー保護の観点から、入出力データに対して、匿名化やノイズを加えることの必然性は理解できるにしても、データの利活用の段階で、匿名化することによりデータ分析の精度が低下することは、本来のデータ利活用の趣旨に反する。従って、データを秘匿した状態でも、データ解析を可能とする「秘密計算」技術を加えた３つの要素技術が必要になるのである。

現状は、PPDMが企業の実務現場において浸透している状態とは言えないが、パーソナルデータの活用と個人のプライバシー保護技術としては、個人の特定性を低減する必要性から、匿名化の為の技術と加工方法の明確化が社会的に要請される（泉、2014）。今

後改正個人情報保護法の施行に伴って、意識の変化が起きてくるのは間違いないと思われる。

2.3.2　匿名化技術

日本の医療・医学分野における個人情報の取り扱いは、法律と各種ガイドラインによって規定されている。例えば、医療・介護分野においては、厚生労働省が「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（平成22年9月17日改正）」を規定している。また、研究分野では同様に厚生労働省の「ヒトゲノム・遺伝子解析研究に関する倫理指針（平成20年12月1日一部改正）」がある。医療分野といっても、医療や医学研究では取扱う情報の種類は異なるり、一様にセンシティブな情報であることからも、取り扱いには慎重にならざるをえないことは共通している。法律やガイドラインの記載内容には曖昧性があり、情報の利活用をする側とされる側の態度を慎重にさせ、萎縮の原因になっている。法の曖昧性を踏まえて、プライバシー保護技術は大きな役割を果たすと期待される（森田、荒井、2014）。ここでは、個人情報から匿名加工情報への状態が遷移するという視点（石田、2015）を参考にして、匿名化技術について調査した。

会員ID	氏名	性別	生年月日	購入商品	購入日時
00001	鈴木　一郎	男性	1967/8/17	相続税対策	2016/1/10　13:00
00002	鈴木　二郎	男性	1972/9/24	新刊文庫本	2016/1/10　15:30
00003	荒井　琴葉	女性	1990/6/8	クッキングレシピ本	2016/1/10　19:05
00004	鈴木　三郎	男性	1985/11/28	英語教材	2016/1/10　11:25
00005	荒井　玲美	女性	1970/2/12	ヨガ	2016/1/10　16:30

図　2-2　購買履歴の例

図2-2は書店での購買履歴であり、会員ID、氏名、性別、生年月日、購入商品、購入日時が把握可能となっている。これらの項目からは、個人が特定可能であり、匿名化するためには、会員IDを仮IDに変換、氏名を削除、生年月日を年代に変換した上で、購

入日時から時間を削除した購入日に一般化する必要がある。これらの変換処理を加えたものが図 2-3 である。

会員ID		性別	年代	購入商品	購入日
abcde		男性	40	相続税対策	2016/1/10
1acbd		男性	40	週間文春	2016/1/10
35zfs		女性	20	クッキングレシピ本	2016/1/10
2g6h3		男性	40	英語教材	2016/1/10
4qrt6		女性	40	ヨガ	2016/1/10

図　2-3　購買履歴を仮名化処理

図 2-3 の情報のみからでは、個人を特定できないことがわかる。ただし、ある条件を考慮することで、個人が容易に特定できてしまう可能性がでてくることに注意が必要である。１点目が、もし仮 ID と会員 ID の対応表が存在したとすると、二つの情報の紐付けによって容易に個人を特定できてしまうだろう。また、改正個人情報保護法における個人情報の定義に新たに、「個人識別符号」としての文字、番号、記号その他符号も個人情報に該当することからも、仮 ID を削除する必要も生じる。

二点目は、購入商品の内容から個人が特定される可能性があることが問題となってくる。例えば、「相続税対策」の雑誌を購入した方は、年齢を加えた推測から、両親からの相続税対策を検討していることが推測され、かつ近くの金融機関で実施した相続税対策セミナーの名簿と付き合わせれば、本人が特定される可能性は排除できない。対策としては購入商品を一般化することになる。図 2-4 に加工後の状態を示す。

		性別	年代	購入商品	購入日
		男性	40	雑誌	2016/1/10
		男性	40	雑誌	2016/1/10
		女性	20	雑誌	2016/1/10
		男性	40	雑誌	2016/1/10
		女性	40	雑誌	2016/1/10

図　2-4　購買履歴を無名化処理

図 2-4 の状態では、「相続税対策」雑誌を購入した男性が誰なのか特定される可能性は低減された。同時に、雑誌を購入した４０代の男性が３名存在する状態に変化している。{男性、４０代、雑誌購入}の属性組み合わせによる識別性も同時に解消されたことになる。いっぽうで、{女性、２０代、雑誌購入}の属性が１名、{女性、４０代、雑誌購入}の属性が１名存在しており、識別性を有する状態である。そこで識別性を排除するために、購入履歴からこれら２件のデータを削除することにより、同一属性データがｋ個以上存在する状態に変化させる。この状態を「ｋ－匿名性」という。図 2-5 では、ｋ＝3 の状態に変化したものである。匿名化された最終的なデータが本来の目的に供するものか否かは別として、実際にどの状態まで匿名化すればいいかは、個人情報保護委員会規則に定める基準に従うことになる。

		性別	年代	購入商品	購入日
		男性	40	雑誌	2016/1/10
		男性	40	雑誌	2016/1/10
		男性	40	雑誌	2016/1/10

図　2-5　購買履歴をｋ－匿名化処理

この例では、ｋ－匿名化処理をすれば、個人の特定はもちろんのこと、個人を識別することすら容易ではなくなった印象を受けるが、仮にｋ＝2 の場合を含めｋの値をどの程度まで調整すれば安全かは、明確な基準を設けるのは困難だと思われる。

匿名加工情報は、特定の個人を識別できる情報を加工して作成されるものではあるが、個人情報とは別の情報と捉えるより、「識別できるか特定できない状態」あるいは「識別も特定もできない状態」に変化すると捉えたほうが本質を見失わない。再識別化・特定化によって、個人が特定される可能性は否定できない（石田、2015）。

また、匿名化の強度に反比例して、利便性は低下することは明白であるため、業種や分野によっても基準は変動するものにならざるをえないのではないかと考える。この点に関しては、個人情報保護委員会がどのような基準を定めるかは、注視していく必要がある。

2.3.3　暗号化と秘匿計算技術

秘匿計算技術は、データを秘匿化したまま統計処理等のデータ処理を行う技術である。通常、暗号化されたデータはそのままでは処理ができないが、復号化することによって可能となる。ただし、復号化した時点でデータ漏洩のリスクが発生する。秘密計算技術はこのようなリスクを低減する技術である。秘密計算の方式は、汎用的および個別対応方式２つの方式が存在する。以下に、それぞれの方式について概観する。

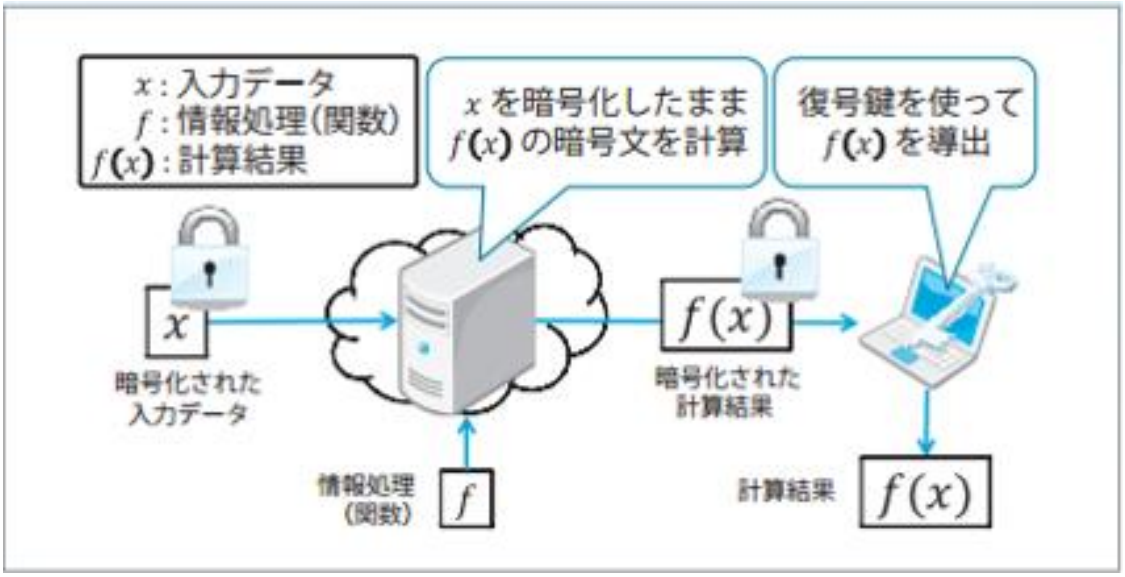

図　2-6　完全準同型暗号に基づく秘密計算処理（出典：情報処理 Vol54（2013））

完全準同型暗号は、2009 年に Craig　Gentry が提案した暗号方式であり、加法と乗法を同時に実現可能な方式である。暗号化されたデータを入力として、暗号化された計算結果を求めることができ、真の計算結果に戻すたには復号鍵が必要である。鍵長や暗号文のデータサイズが大きくなるため、膨大な計算時間を要する点がデメリットである。

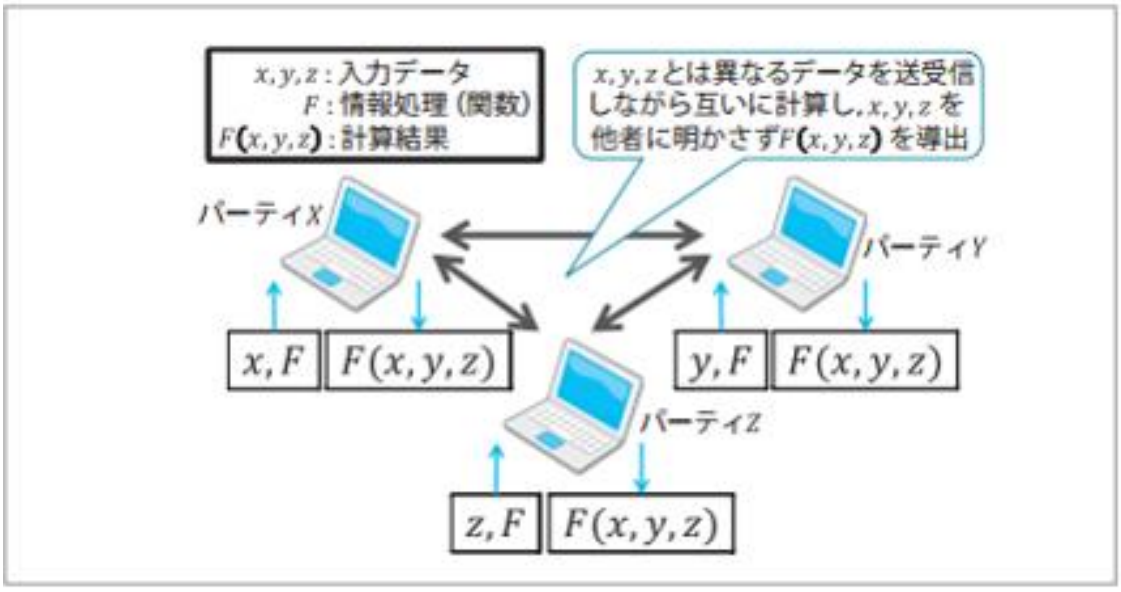

図　2-7　セキュアマルチパーティ計算処理（出典：情報処理 Vol54（2013））

セキュアマルチパーティ計算は、1986 年に Andrrew　Yao が提案した情報共有のための暗号化方式である。特徴としては、複数人がそれぞれ秘密のデータを持ち、互いに秘密データを公開することなく、所定の計算結果を導出することが可能である。

尚、秘密計算技術の応用事例は、国内では NTT が医療統計分野において秘密計算技術を世界初の実証を成功させている（NTT 持株会社ニュースリリース http://www.ntt.co.jp/news2012/1202/120214a.html、2012）。また、海外ではエストニアの sharemind プロジェクトで 2013 年に遺伝子解析において応用例が発表されている。

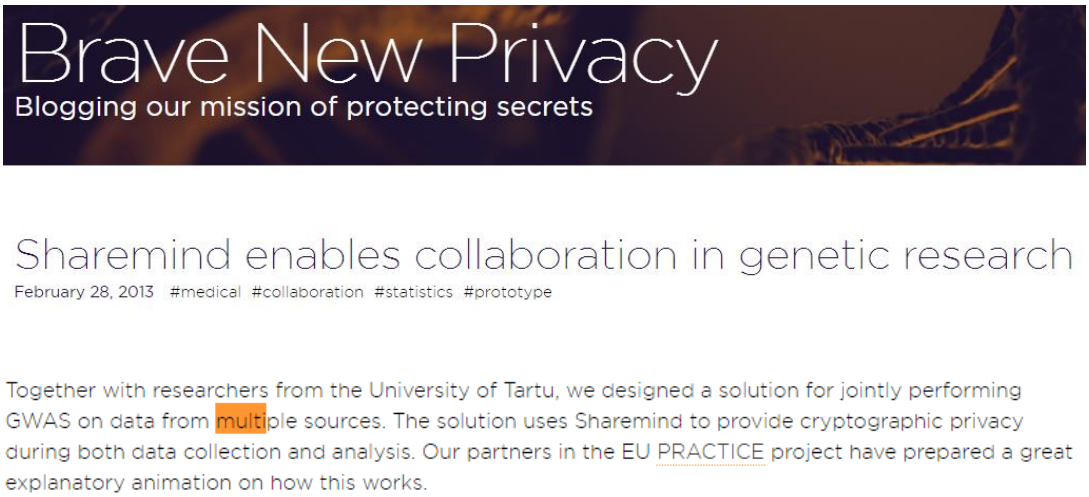

図　2-8　エストニア国　sharemind プロジェクト公式 HP

（出典：sharemind 公式 HP：https://sharemind.cyber.ee/collaborative-medical-research/）

2.4　プライバシー保護プロセスにおける各種アプローチ方法

2.4.1　個人情報保護法の体系

日本における個人情報保護に関する法律・ガイドラインの体系を以下に示す。個人情報保護法を底辺に、民間分野と公的分野で上位の法律・ガイドラインを定めている体系を持つ。尚、個人情報保護法の４章～7 章については民間事業者を対象とする義務、罰則規定を定めた内容となっている。

図　2-9　個人情報保護法体系（出典：個人情報保護委員会 HP）

医療分野における個人情報保護ガイドラインは、民間分野の事業分野ごとのガイドラインを定めており、現在は医療と研究に関する８つのガイドラインが定められている。

表　2-4　医療分野における個人情報保護ガイドライン

<table>
<tr><th colspan="2">分野</th><th>所管府省</th><th>ガイドラン名称</th></tr>
<tr><td rowspan="10">医療</td><td rowspan="5">一般</td><td rowspan="5">厚生労働省</td><td>医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン</td></tr>
<tr><td>健康保険組合等における個人情報の適切な取扱いのためのガイドライン</td></tr>
<tr><td>医療情報システムの安全管理に関するガイドライン</td></tr>
<tr><td>国民健康保険組合における個人情報の適切な取扱いのためのガイドライン</td></tr>
<tr><td>国民健康保険団体連合会等における個人情報の適切な取扱いのためのガイドライン</td></tr>
<tr><td rowspan="3">研究</td><td>文部科学省
厚生労働省
経済産業省</td><td>ヒトゲノム・遺伝子解析研究に関する倫理指針（告示）</td></tr>
<tr><td>厚生労働省</td><td>遺伝子治療等臨床研究に関する指針（告示）</td></tr>
<tr><td>文部科学省
厚生労働省</td><td>人を対象とする医学系研究に関する倫理指針</td></tr>
</table>

2.4.2　個人情報保護法改正の背景と内容

近年の情報通信技術の進歩に伴い、多種多様なデータ、いわゆるビッグデータを活用した新産業やサービスの創出が期待されている。いっぽうで、ビッグデータを取り扱うにあたっては、特に個人に関する情報の取り扱いに関する法整備が追いついていない状況にあり、個人のプライバシーに関わる問題が顕在化されているのも事実である。現在、個人情報保護法の制定から１０余年が経過したが、ビッグデータの利活用においていかに利活用を促進しつつ、個人のプライバシーに配慮するかという観点から、制度見直しが検討されてきた。そして、2013 年 12 月 20 日、高度情報通信ネットワーク社会推進戦略本部（以下「IT 戦略本部」という。）において、「パーソナルデータの利活用に関する制度見直し方針」（以下「見直し方針」という。）が決定された。その後「パーソナルデータに関する検討会（以下「親会」という。）」において、見直し方針に基づき検討が重ねられ、2014 年 6 月 24 日に、「パーソナルデータの利活用に関する制度改正大綱」の発表、2015 年 9 月 3 日に「個人情報の保護に関する法律及び行政手続きにおける特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」（以下、「改正個人情報保護法」という。）が成立、同月 9 日公布された。

改正個人情報保護法の具体的な改正内容について下記に示すとともに、主な改正点について概説する。

表　2-5　個人情報保護法　改正ポイント

主な改正点	該当条項	改正内容
個人情報の定義	2条1項、2項	従来の定義に加え、「個人識別符号が含まれるもの」が追加された。
要配慮個人情報（人種、信条、病歴等が含まれる個人情報）	2条3項、17条2項、23条2項	取得は、原則本人同意が必要。要配慮個人情報については、オプトアウト規定に基づく第三者提供はできない。
小規模取扱事業者	2条5項（5号を削除）	5000人以下の個人情報を取り扱う小規模取扱事業者も、適用除外がなくなった（適用されるようになった）
匿名加工情報	2条9項、10項、36～39条	・個人情報を加工→匿名個人情報を作成 ・作成方法は、個人情報保護委員会規則に従う ・安全管理措置は、個人情報保護委員会規則に従う ・匿名加工情報に含まれる情報の項目を、個人情報保護委員会規則に従って、公表する必要がある
利用目的の制限の緩和	15条2項	関連すると合理的に認められる利用目的へなら、本人同意なく、利用目的を変えられる。
オプトアウト規定による第三者提供	23条2～4項	個人情報保護委員会規則の定めに応じて、本人への事前通知等を行い、さらに個人情報保護委員会に届け出る
外国事業者への第三者提供	24条	個人情報保護委員会規則の条件に合わない限り、本人同意が必要
トレーサビリティの確保	25条、26条	・第三者提供する場合は、個人情報保護委員会規則で定めに従い、必要な事項を記録し、保管することが必要 ・第三者から提供を受ける場合は、個人データの取得の経緯等を確認することが必要
データベース提供罪	83条	不正の利益目的で提供・盗用したときは、刑事罰

・要配慮個人情報（17条2項、23条2項）

改正法では、個人情報の定義の中に新たに、「要配慮個人情報」が追加されることになる。その定義は「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに配慮を要するもの」とする。要配慮個人情報については、取得する際は、一部の例外を除き原則として本人同意を得ることが義務付けられる。本研究でとりあげる

KDB システムで取り扱うデータが、一部例外に含むかが論点になるが、改正法では国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合にあり、本人同意を得ることで事務遂行に支障を及ぼす恐れがある場合は認めている。

第三者提供については、オプトアウト手続きによる第三者提供を認めないようにした。これらはいずれも本人の認識しえないところで、本人の情報が不当に取り扱われないようにするための措置である。尚、「オプトアウト」と相対する「オプトイン」の意味については、本人から事前の同意を得る行為を「オプトイン」と言い、本人が反対しない限り、同意したものとみなして情報を取り扱い、事後的に本人が反対の意思表示をできる状態にすることを「オプトアウト」と言う。

・匿名加工情報（2 条 9、10 項、36～39 条）

匿名加工情報の定義については、「特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたもの」としている。また 36 条～39 条では、個人情報取扱事業者に対する義務を規定した。作成にあたっては、特定の個人を識別すること及び個人情報を復元することができないようにするために、個人情報保護委員会規則で定めた基準に従い、加工することを求めている。加えて当該匿名加工情報に含まれる個人に関する情報の項目を公表することも必要としている。

・利用目的の制限の緩和（15 条 2 項）

「利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない」が条文であるが、変更される点は関連性の程度を表現する文言として、「相当の関連性」から「相当の」が削除されたのみである。相当の意味する程度の解釈に幅を残した内容となっている。

・オプトアウト規定による第三者提供（23 条 2～4 項）

個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、個人データを第三者に提供することができるものに変更された。改正前から比べると個人情

報保護委員会規則に従うことと報告義務が加わったことになり、オプトアウトによる第三者提供については、より厳格になったと言える。

個人情報保護法の改正については、IT 戦略本部での親会の議論を注視してきたところではあるが、当初の目的の一つであったパーソナルデータの利活用をいかに促進していくかという観点から踏まえると、個人的な見解ではあるが、個人情報の保護強化に偏った内容になった感が否めない。

2.4.3 プライバシー・バイ・デザイン

1990 年代にカナダのアン・カブキアン（Ann Cavoukian）氏によって提唱された概念で、プライバシー保護を目的として利用される技術及び対策を、システム設計及びその構築段階から検討・実施し、ライフサイクル全般において体系的かつ継続的に取り組む仕組みである。プライバシー保護策を導入することで、ビジネスの利便性を損なうような二律背反の状態に陥らないためのアプローチである。プライバシー・バイ・デザイン（以下 PbD という。）の実現には下記に示す 7 つの基本原則が必要とされている。

PbD の七つの基本原則

1. リアクティブ（事後）ではなくプロアクティブ（事前）：事後の措置でなく事前に予防する。
2. デフォルト設定でプライバシー保護：個人情報が自動的に保護されることで、プライバシー対策を提供する。
3. 設計時に組み込むプライバシー対策：プライバシー対策はシステム設計時に組み込まれており、必要不可欠な構成基盤となっている。
4. 全ての機能に対してのゼロサムではなくポジティブサム：プライバシー対策がビジネスの効果を後押しするという考え方である。
5. エンドツーエンドのセキュリティ：データライフサイクル全体に対応し、ライフサイクル全体の保護を保証する。
6. 可視化と透明性：ステークホルダーは、何が情報技術、組織や社会基盤に関係するかオープンにする。

7. 個人のプライバシー尊重：個人に主体を与え、個人の利益を考慮しなければならない。

7つ目の概念は、特にPbDのシンボリックな概念であると考えるもので、プライバシー保護を事業者任せにすることなく、情報提供者の信頼を得る考えとしくみを備えることが重要である。パーソナルデータの収集と活用にあたり、事業者がPbDの概念に基づき実施すべき対応について、収集される情報が情報提供者にとって許容できるか否かは、本人の価値観に依存するものであり、本人の判断によって決まるものである。それを可能とするためには、サービスを提供する事業者が、どのような情報をどのように収集し、どう取扱うのかを説明する必要がある（八津川、2015）。その上で、プライバシー侵害リスクを回避するためには、情報収集対象者への配慮と透明性を担保しうるプライバシーポリシーを明記することが必要である。プライバシーポリシーに明記すべき重要事項（八津川、2015）は、下記のとおりである。

・事業者が取得する情報内容、取得方法、利用目的

・取得した情報の第三者提供時の対応

・利用者に対し情報取得の停止、変更、削除等自己の情報コントロールの機会提供

第３章

自治体におけるKDBシステム利活用調査

3.1　はじめに

「日本再興戦略」（平成25年６月14日閣議決定）において、「全ての健康保険組合に対し、レセプト等のデータの分析、それに基づく加入者の健康保持増進のための事業計画として「データヘルス計画」の作成・公表、事業実施、評価等の取組を求める」ことが示された。これを受けて、保険者（自治体）が「健診・保健指導」「医療」「介護」の３分野について、①「統計情報」、②「個人の健康に関するデータ」を管理するKDBシステムを活用し、集団及び個人の健康課題を明確にし、効率的かつ効果的な保健事業に取り組むこととなった。

KDBシステムの活用を推進するにあたり、想定されるさまざまな課題が想定される。まずデータ分析には、健康・医療の観点から専門的な知見が必要と思われるが、自治体ではどのように取り組んでいるのか。また、KDBシステムで扱うデータは、特に配慮を要する個人情報であるという認識であり、個人のプライバシー保護の観点から、利活用に萎縮するというバイアスが生じている状況があるのではないかという疑念も抱く。パーソナルデータの利活用を推進する目的で、個人情報保護法が改正される予定であり、法整備の環境も整いつつあるが、改正内容については、解釈の幅の余地を残す内容にもなっている。これらの要因を踏まえて、現場における利活用と保護を両立するプライバシーマネジメントモデルが必要ではないかという問題意識を持つに至った。そこで、先行研究で得られた知見をもとに、KDBシステムの利用実態についてアンケート調査を実施し、調査結果の分析を試みた。

3.2　KDB システムの概要

3.2.1　ステークホルダーと関係性

KDB システムの運用を司るステークホルダーの関係について説明する。

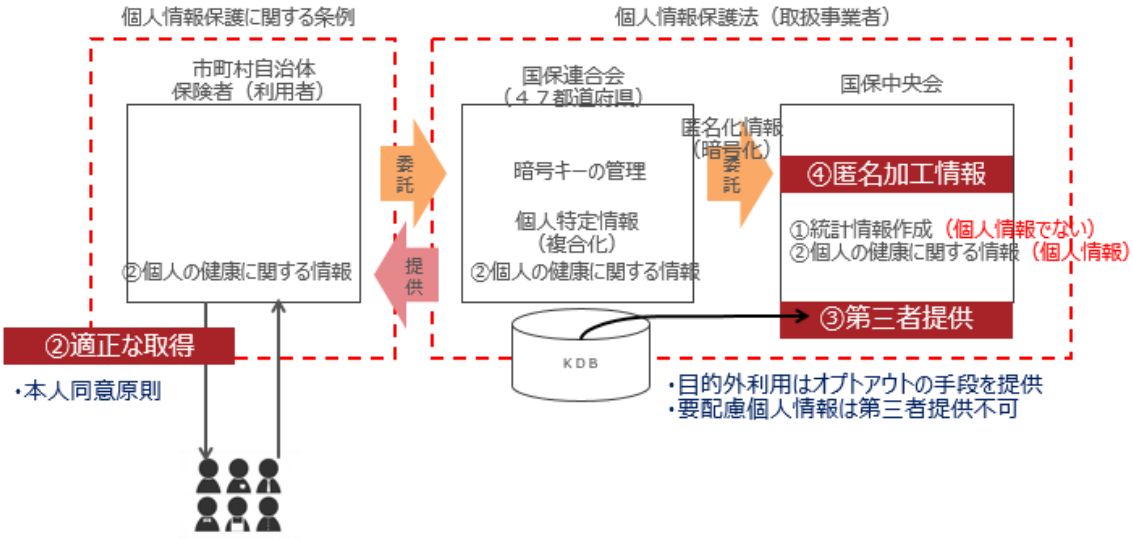

図　3-1　ステークホルダーと関係図

保険者、国民健康保険団体連合会（略称：国保連合会）、国民健康保険中央会（略称：国保中央会）は、それぞれ受委託の関係にある。特定健診、医療、介護に関する給付情報を管理し、それらの情報から「統計情報」を作成するとともに、保険者からの委託を受けて「個人の健康に関するデータ」を作成・提供する。取扱い情報が個人情報に該当するか否かは、受委託関係とデータの持ち方によって決まるものであり、厚生労働省から各都道府県の所管部へ事務連絡（事務連絡　平成 25 年 6 月 25 日）が通達されている。主な趣旨は以下のとおりである。

・国保連合会から委託を受けて国保中央会で加工された情報のうち、「統計情報」については、個人情報には当たらない。

・国保連合会は、個人が特定できる情報を暗号化した上で、国保中央会に送信する。国保連合会では暗号鍵と個人が特定できる情報との対応表を保管しており、国保中央会が国保連合会から送信されて保有する情報は個人情報保護法の個人情報にあたらない。

・国保中央会で加工された情報で「個人の健康に関する情報」については、暗号鍵を保有する国保連合会において、復号化が可能であるため個人情報に当たる。
・国保連合会が「個人の健康に関する情報」を委託の範囲で保険者に提供することは、目的内の利用であり、個人情報保護法第 16 条の利用目的による制限に該当しない。また第 23 条第 1 項第 4 号の規定により、地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合に該当するため、第三者提供の制限には該当しない。
・国保連合会及び国保連合会から委託を受けた国保中央会は、個人情報保護法に定める個人情報取扱事業者である。

3.2.2　KDB システムの利用目的

KDB システムは、国のデータヘルス事業を推進するためのしくみとして、平成 25 年 10 月より順次稼動を開始している。KDB 参加保険者数［平成 27 年 7 月処理時点］は、 国保（健診：1,868、医療：1,867）、後期高齢者医療（健診：43、医療：45）、介護保険（1,536）のデータが格納されている。（国民健康保健中央会報告による）
KDB システムで保有するデータの利用目的について、「統計情報」は地域の健康状況を確認し、他の地域の健康状況の比較することで自分の地域の特徴と優先すべき課題を把握することである。いっぽう「個人の健康に関するデータ」は、究極的には重症化予防対策の実施であり、そのアプローチとして保健指導対象者を選定することにある。KDB システムは、特定健診、医療情報、介護情報を複合的に分析できる点が大きなメリットである。

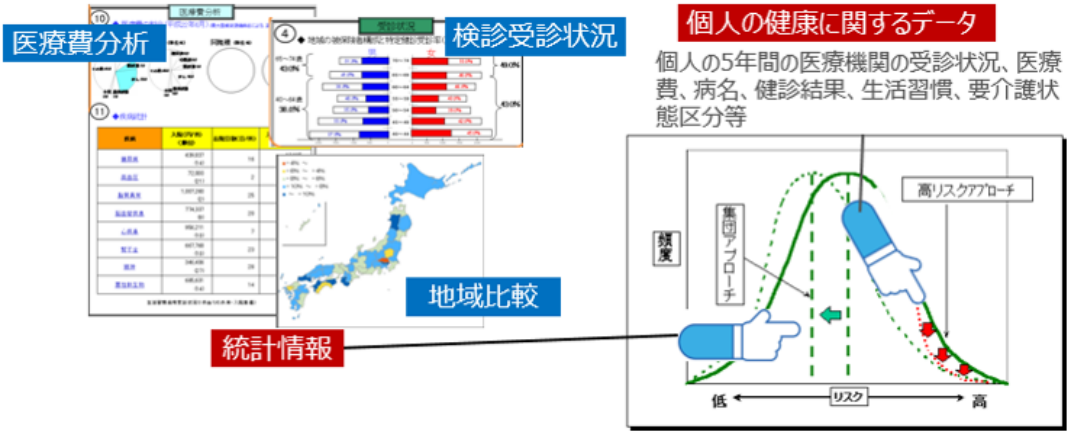

図　3-2　データ分析イメージ

3.3　自治体における取組み状況の予備調査

KDB システム導入にあたり、自治体における意思決定プロセスを調査することで、KDB システム利活用のメリットとプライバシーリスク認識に対する意識調査を実施する。

3.3.1　対象

個人情報審議会議事録をウェブサイトに公開し、かつ KDB システム導入に関する議題を扱っている任意の自治体を対象に、16 自治体を無作為に抽出した。抽出時点では、個人情報審議会議事録の内容までは把握していない。

3.3.2　調査方法

議事録内容から、利活用とプライバシー保護に関する特徴的なキーワードを抽出し、ポジティブワードとネガティブワードに分類した。双方のキーワード種別のカウント数の比較、または最終的な結論も加味して、組織における意識が利活用、プライバシー保護のどちらが強いかを客観的に判断した。

3.3.3　調査結果

16 自治体中 2 自治体については、具体的な議事内容の詳細な記載が確認できなかったため（KDB システムに関する議事案件名のみ記載されている等）、14 自治体について議事内容を確認した。表 3-1 に調査結果を示す。

表　3-1　個人情報審議会議事録の調査結果

自治体	ポジティブな発言	ネガティブな発言	凡例
A	6	0	個人情報保護、本人通知すべき、目的外利用について周知、糖尿病の重症化予防、医療費削減、データの開業医開示可否、
B			議事録確認できず
C	3	2	KDB利用に関して市民周知はしない、個人情報を利用して健康指導する場合は周知が必要、 保健指導の実施を検討、医療費分析の実施を検討、統計情報の利用
D	6	4	市民への広報周知をする、目的外利用における本人通知はしない、医療費・介護費の軽減取組み、介護予防事業、重症化予防へ活用、保健指導に活用、個人情報を活用することは賛成、外部からの侵入リスク、データの暗号化、市全体・地域の傾向把握
E	2	0	保健事業の充実、国民健康保険・介護保険の安定運営
F			議事録確認できず
G	1	0	保健事業をより効果的に行う
H	4	0	疾病予防のための健康づくりや保健指導、医療給付費・介護給付費の適正化、保健指導対象者の把握、本人通知省略は合理性あり
I	4	1	介護予防事業に資する、特定健診の受診勧奨、システム上のリスクは何か、個人情報はどんどん集めて活用すべき、市民への周知義務はない
J	3	1	要介護度の上昇抑制の原因分析、疾病リスク・医療費等の医学的知見を得る、目的内利用のため問題なし、提供情報は必要最低限に限定すべき
K	2	1	地域や全体の課題を把握、個人を対象にアプローチする、国保連合会から個人情報が漏れる可能性はあるか
L	2	1	データマッチングで新たな情報価値が生じる、健康保険・介護保険レセプトを突合し不正な給付をチェック、情報収集について漏洩のないよう扱う
M	3	0	特定健診結果をもとに保健指導、効果的な保健事業は公益上必要、本人通知は必要ない
N	5	1	要介護状態等の予防、個々の適正な介護プランの検証ができる、重複頻回受信者の抽出、医療費・介護給付費の抑制ができる、本人同意を得ない理由が不明、地域の特性情報も把握できる
O	4	5	公益性の高い利用効果を期待、個人へのアプローチに活用、統計情報活用で健康課題を把握、効果の高い保健指導ができる、プライバシーに関わる重要な個人情報、リスク管理の方法、閲覧できる情報の制限はできるか、プライバシー侵害のおそれがぬぐえない、個人の帳票利用は安全性を審議要
P			医療費や医療行為の効率化、安全管理措置でウィルス対策以上のことは何か、個人情報の保存期間の終期は、当市は住民数が多い分慎重に、条件付きで承認

表中の黒字がポジティブワード、赤字がネガティブワード、また青字はどちらの解釈にも読み取れるため中立の意味とする。最初にポジティブワードとネガティブワードの数をカウントし、ポジティブワード数が優位な場合は利活用に積極的であり、ネガティブワード数が優位な場合は利活用に消極的とみなす。14 自治体中 12 自治体が、利活用に積極的な姿勢を確認できた。また残り 2 自治体のうち、1 自治体が利活用に消極的であり、1 自治体が中立的なスタンスであった。自治体 P を中立的であると判断した理由は、議事録内容からは積極的とプライバシー保護に慎重な両方の意見が確認できたものの、最終的には「条件付きで承認」と結論付けており、一定の条件を満たさない場合は導入を見送ることもありえるという意味も含んでいるため、敢えて中立的とした。

総じて利活用に対する意識は、リスク認識はしつつも効用を優先する傾向が確認できた。内訳を見ると、特に期待する効果として多かったのは、医療費分析や削減に関して 6 自治体、効果的な保健指導が 5 自治体、疾病・介護予防が 4 自治体で確認された。

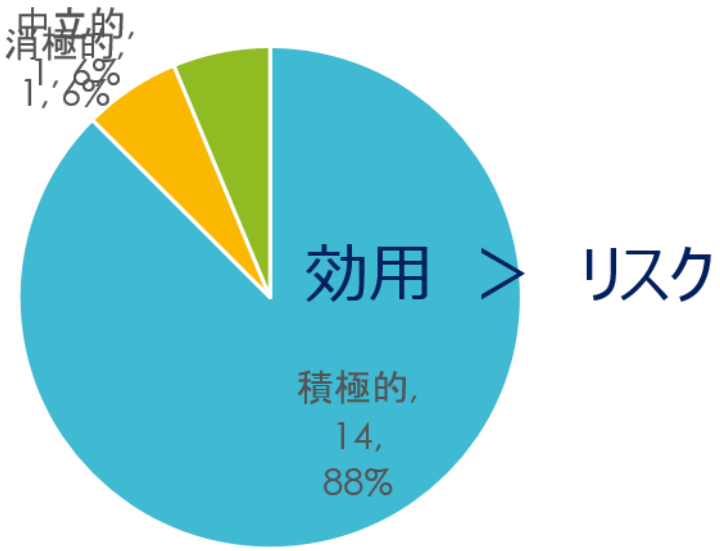

図　3-3　利活用に対する意識調査結果

次に、本人通知に対する意識調査の結果を図 3-4 に示す。

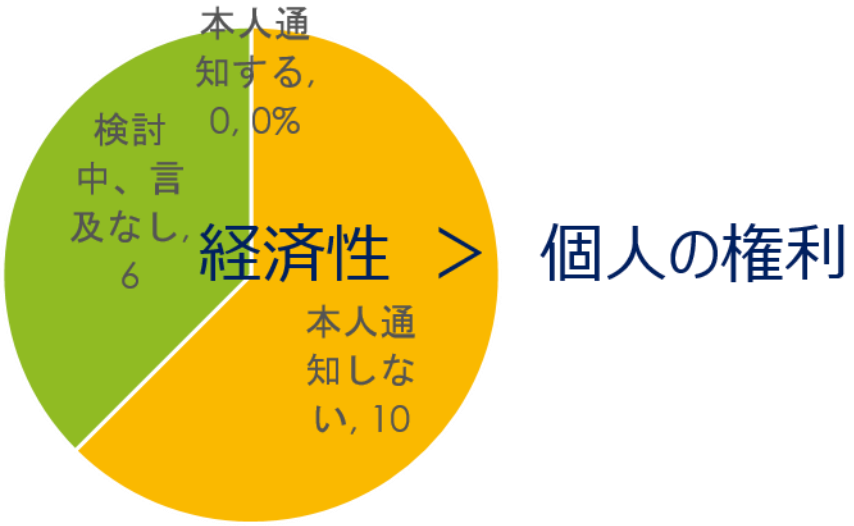

図　3-4　本人通知の予定

目的外利用にあたることへの懸念や、第三者提供するにあたって被保険者本人への通知と同意取得についての懸念が見られたものの、16 自治体中 10 自治体で、本人通知しないという見解が確認された。また、本人通知する意思がある自治体は 0（ゼロ）、6 自治体が検討中または言及がなかった。本人周知と同意を得ることについては、必ずしも全てから同意を得られる保証はないため、効果が低下する要因となるばかりでなく、一定のコストが必要になることも考えると、経済的な負担は増加する。これらの要因が影響を与えているかは、議事録からは読み取れなかったが、総じて個人の権利よりも経済性を優先するという意識が読み取れた。

予備調査の結果として、KDB システムを利活用することについては、効果に対する期待が高く、一定のリスク意識は持ちつつも経済合理性を優先するという意識であることがわかった。全国の自治体を対象に調査を実施した場合でも、この傾向になると考えてもいいのではないか。

尚、3.2.1 項で述べたとおり、厚生労働省から各都道府県の所管部へ事務連絡（事務連絡　平成 25 年 6 月 25 日）が通達された内容には、保険者に提供される情報が個人情報に該当しないとする内容を含むが、それを認識しているか否かに関係なく、利活用に対する意識調査結果であることを加えておく。

3.4　本調査

予備調査では、KDB システム導入前の意識調査にフォーカスを当てたものであったが、本調査では、実際の KDB システムのデータを活用して、データヘルス計画を推進していく現場における利活用とプライバシー保護に対する意識調査を実施した。

3.4.1　対象

予備調査を実施した 4 自治体を含め 9 自治体を選定した。抽出基準は、筆者が在住する首都圏で、人口規模の異なる自治体を選定した。内訳は政令都市規模、中核都市規模、町村規模であり、地域で抱える課題と対策のアプローチが異なると想定されることから、傾向分析をするためには有効な方法だと考えたためである。

3.4.2　調査方法

事前に電話にてアンケート協力に対する了解を得た上で、メール文書によるアンケート回答方式とした。実施時期は、2016 年 3 月上旬にアンケートのメール配布、3 月末を回答期限とした。

3.4.3　本調査結果と考察

アンケート項目は、大別してデータ利活用の観点と個人情報保護の観点で設問を作成した。アンケート項目は、利活用とプライバシー保護の意識の度合いと、具体的な取り組み状況について問う内容とした。以下にアンケート結果について示す。回答率は100%であった。尚、アンケート様式「国保ＤＢの利活用と情報保護に関するアンケート調査」については、付録を参照されたい。

データ利活用の観点

・利活用の有無については、9自治体全てが「利活用している」と回答。

・統計情報の利用種別について図3-5に示す（複数回答可）。56%が地域の全体像または地域の健康課題に関するデータを利用していることから、統計情報の主な活用目的は、地域の概観を把握することだと言える。

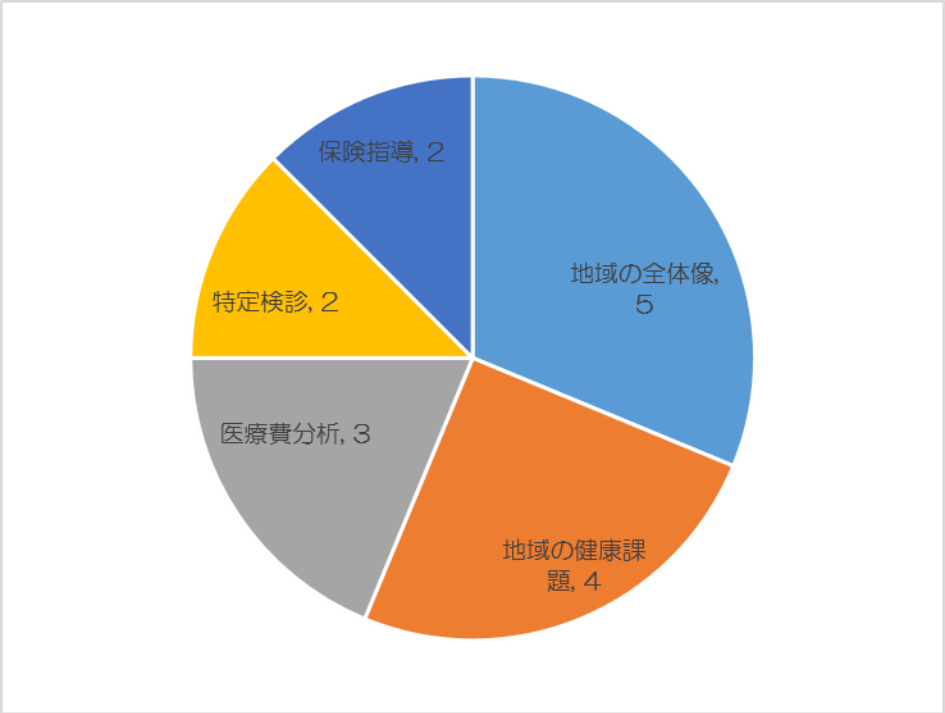

図　3-5　統計情報の利用種別

・データ分析における保健師の関与度合いについて図 3-6 に示す。「主体的に参加」、「助言する程度」を合わせて 6 自治体がデータ分析に関与している。全く関与しないとの回答は 0（ゼロ）であり、程度の差はあるものの専門家による分析が必要だという認識は共通している。

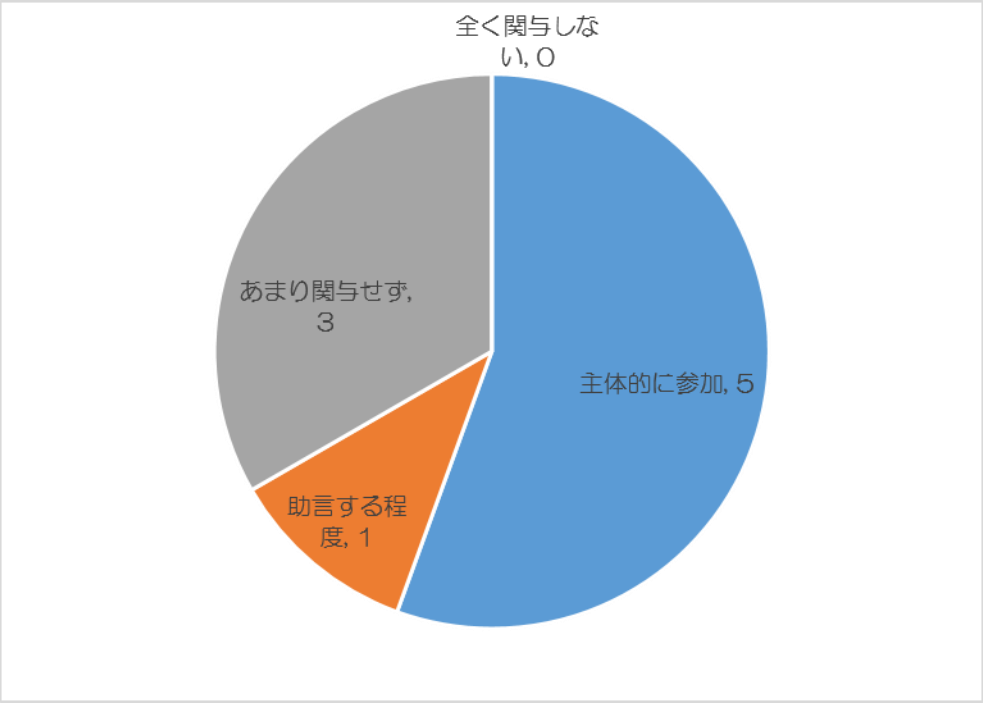

図　3-6　データ分析への保健師の関与度合い

・利活用の効果について図 3-7 に示す。

「効果あり」と回答した具体的な内容については、①地域診断（統計データ）、②生活習慣病における医療費の推移、疾病状況、通院状況の把握であった。

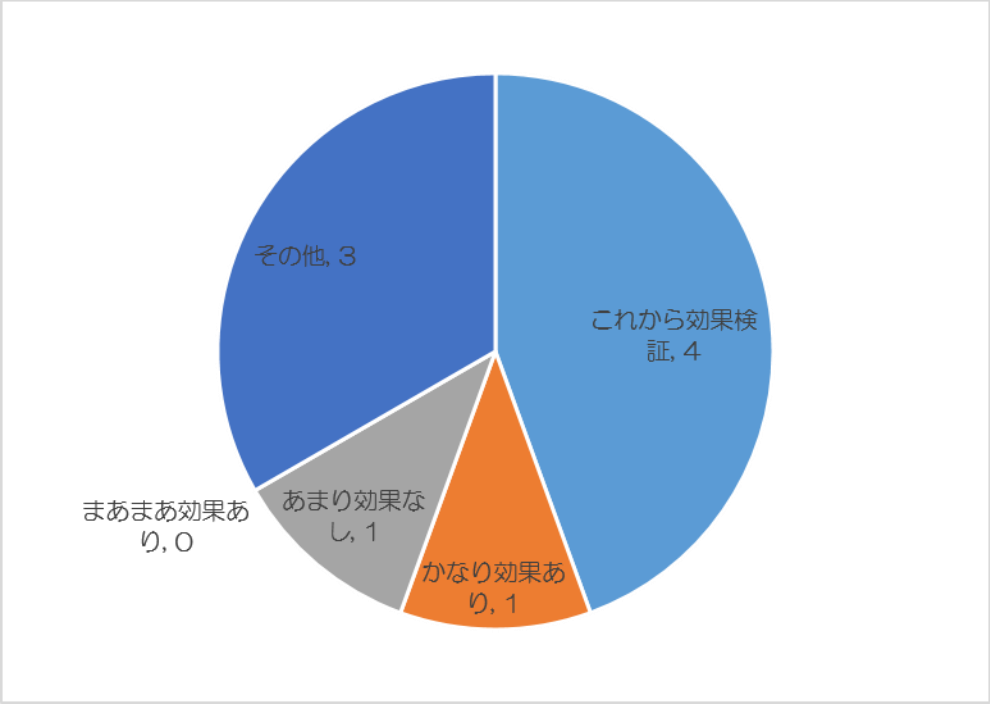

図　3-7　利活用の効果

参考）その他の回答（自由記述）

「データ分析にのみ活用しているところであり、データを活用した事業の実施に至っていない。」

「統計データを参考とすることはあり。個人データは利用しない。」

「データヘルス計画に基づいた保健事業を展開するための現状分析や評価に活用。」

・現状の課題や問題点（自由記述）について、分類結果を図 3-8 に示す。KDB システムは分析ツールとして、規定メニューを提供するものであるが、CSV データから独自に分析することも可能としている。指摘事項の大半はデータ内容に関する課題指摘であり、主にニーズとのミスマッチが確認された。具体的なコメントについては、後述しているが、KDB システム自体やデータ内容については、更なる改善の余地がありそうである。

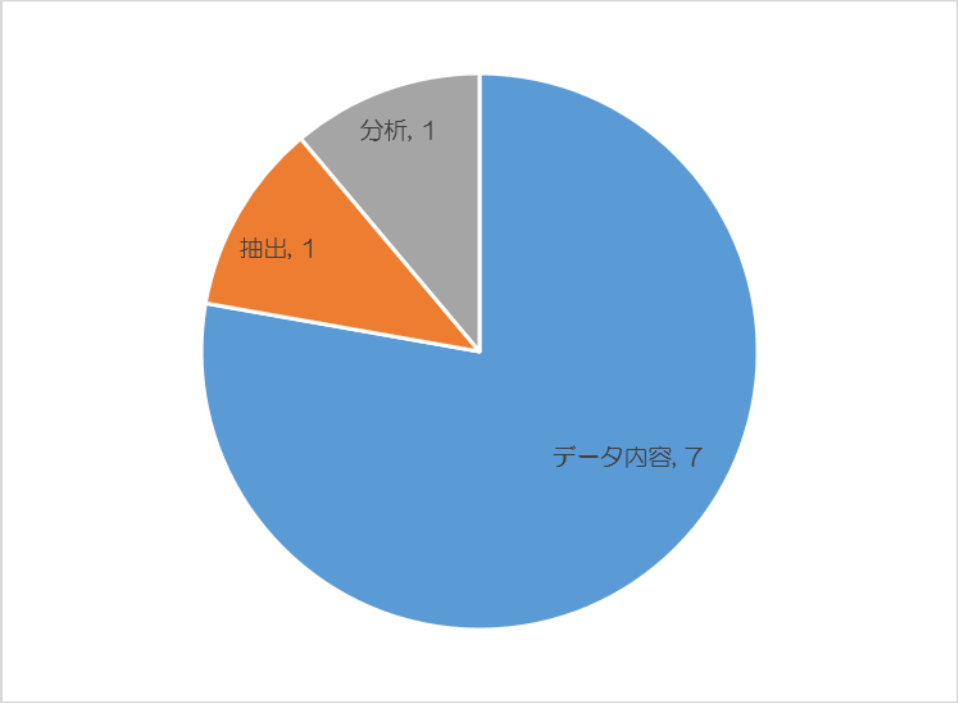

図　3-8　課題や問題点

参考）

「基礎データが正しく取り込まれていない、一部取り込めないデータがある等、エラーが多いため活用が困難。」

「国保 DB システムからでは分かり得ないことが多々あり、別途独自にレセプトデータの分析が必要な状況である。」

「レセプトと医療費の分類について、レセプトの主傷病のみ医療費が紐つけされているため、傷病ごとの正確な医療費が集計されない。」

「医療費等データの整合性に疑問がある。」

「加工しやすい CSV が出ないケースが多々ある。」

「データの精度に疑義がある。」

「本市の規模に対応しきれず、データ抽出までに時間を要する。」

「データの効果的な分析・活用に、専門的な知識が必要であり、具体的な活用例の蓄積が全国的にも少なく、活用方法を検討することが課題である。」

「メニューが限られているため、応用がきかない。」

「KDB システムの不具合により、分析データの数値が変更になることがある。」

「表示されるグラフや表等を画像として保存することができず、そのまま計画等へ転載することができない。」

個人情報保護の観点

・一般論として「ビッグデータが個人を識別または特定リスクがあることを認識しているか」との質問に対する回答結果を、図 3-9 に示す。知っているとの回答が 90%であり、感度は高い。

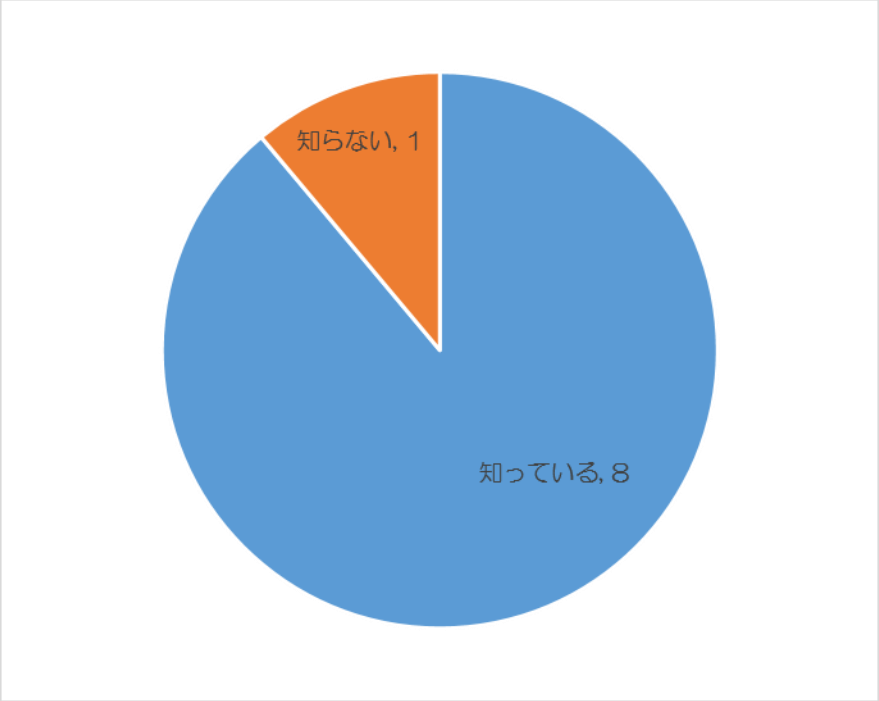

図　3-9　ビッグデータのリスク認識度

・リスクに対する態度について（自由記述）、図 3－10 に示す。75%がリスク回避の態度を示した。また、厚生労働省からの事務連絡ならびに自治体制度上において、個人情報に該当しないとの内容を認識しているのは、2 自治体であった。

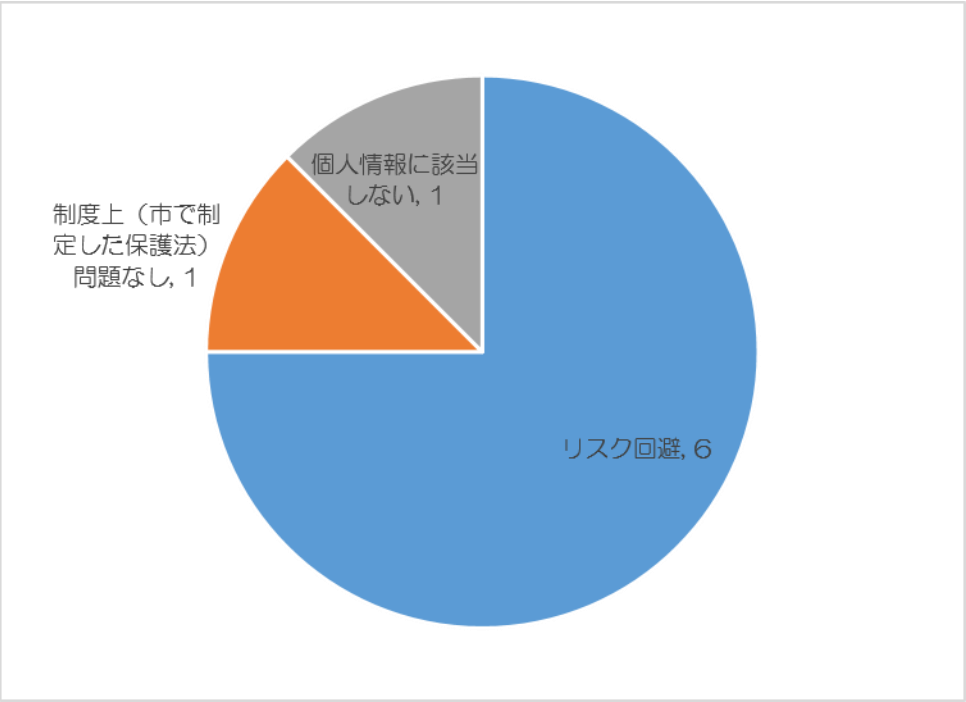

図　3-10　リスクへの態度

参考)

「プライバシー侵害が発生するような統計データは活用せず、公表はしないなどの対応をする。」

「個人を識別・特定しうるデータの利用・活用は避ける。」

「個人特定の利用を想定していない。統計のみを利用する。」

「統計データについては、分析過程で個人を識別または特定できてしまった場合でも個人アプローチには使わない。」

・プライバシーポリシーの公開または通知をしているかについて、図3−11に示す。実施しているが33%と低い結果であった。公開していない6自治体については、前質問のリスク回避態度を示した自治体と同一ではないため、個人の識別・特定リスクとの相関関係は見られなかった。本来、プライバシーポリシーの公開が持つ意味は、自治体が関係法令を遵守し、利用目的の通知・公表等の個人情報の取扱いに対する方針を宣言することで、社会的信頼を得る上で必要なものである。勿論形式的に体裁を整えることが目的ではなく、遵守するための体制と運用が重要ではあるが、組織としてのリスク認識へのコンセンサスが得られているか否かを知る上でも、重要なポイントと言える。

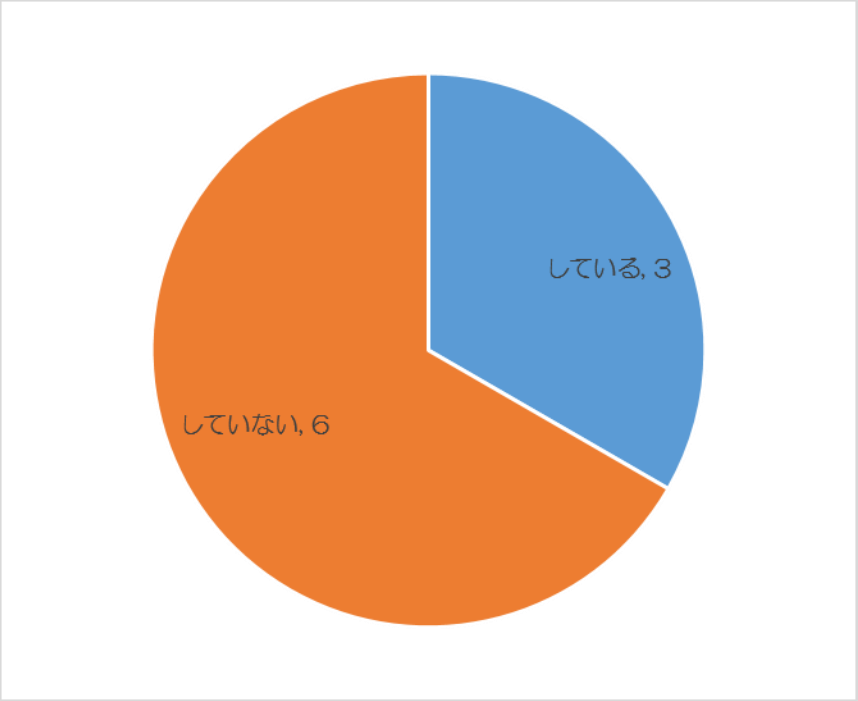

図　3-11　プライバシーポリシー公開の有無

・プライバシーポリシー以外の方法で被保険者に通知しているか否かについては、実施しているが67%であった。プライバシーポリシー公開と他の方法による公開の双方の取り組み状況について整理すると下記のとおりである。プライバシーポリシー公開を含め、何らかの方法で公開しているのが78%であった。尚、その他の方法としては、具体的例は下記のとおりであった。

・個人情報保護条例を自治体HP上に公開

・特定健康診査受診券、特定健診案内文書、問診票に記載

・国保加入全世帯への配布物（国保だより）で周知

表　3-2　被保険者への通知パターン

	プライバシーポリシー	その他方法	対象数
パターン1	○	×	1
パターン2	×	○	4
パターン3	○	○	2
パターン4	×	×	2

○：通知あり／×：通知なし

・最後の質問では、個人情報保護に関して課題や問題点について聞いた。回答結果を下記に示す。個人情報の取り扱いに関して、改正個人情報保護法施行に伴う影響や、多自治体との共有機会の提供を要望する声があり、回答結果から読み取れることとして、明確な指針や基準の必要性を望んでいることが伺える。

回答内容）

「自治体で扱うデータはKDBに限らず、多くのデータを扱うようになり、将来はその傾向が一層加速すると思われる。これらの分析は自治体だけでは困難であり、外部の協力が不可欠であるため、プライバシー保護と利活用のバランスのとれた簡素なルールが必要と考える。」

「現在、本市ではビックデータを匿名化し、目的外利用の禁止、外部漏えいの防止策等の対策を定め、その対応状況の確認等を行ったうえで共同研究相手に提供しているが、今後予定されている行政機関個人情報保護法の改正によるデータ提供の仕組み等への影響が不明である。」

「本市において、国保DBにおける個人に関する情報の活用については、レセプトや健診データ等の目的外利用にあたるため統計情報のみ活用している。」

「今後の課題として、個人に関する情報を活用して事業を実施するためには、必要最小限の個人情報のみ使用することになるため、実施する事業ごとに使用する個人情報を整理する必要がある。」

「個人情報保護やプライバシー保護に関しては各自治体の対応とされているが、他市町村がそれぞれどう対応しているのか共有する機会がほしい。」

3.5　調査結果の分析

アンケート結果を基に、各自治体の利活用とプライバシー保護の意識が、どちらに重きが置かれているか評価する。また、各自治体の抱える事情や課題が、利活用とプライバシー保護の意識にどう影響しているかを探るため、自治体が公表する統計データと重み付けされた結果の相関分析を行う。

3.5.1　意識の重み付け

利活用とリスク意識の重み付けをする簡易な方法として、リスクと利活用の効果における意識の度合いを指標化し、スコアリングする。+（プラス）は意識・認知あり、高い、強い等、－（マイナス）は意識・認知なし、低い、弱い等、できる限り客観的に判断する。

自治体	活用意識の高さ（保健師による分析）（あり：＋/なし：－）	ポピュレーションアプローチ（あり：+/なし：－）	個人へのアプローチ（あり：＋/なし：－）	効果有無（あり：＋/なし：－/空白：これから検証）	スコア
A	+	+	+	+	＋4
B	－	+	－		－1
C	－	－	－		－3
J	+	+	－		＋1
E	－	+	－	－	－2
P	+	+	－		＋1
O	+	+	－		＋1
H	+	+	－		＋2
K	+	+	－		＋1

図　3-12　利活用の効果指標

自治体	個人識別リスクの認知（あり：+/なし：－）	個人アクセス時のリスク対応意識（高い：＋/低い：－）	組織としてのＰ保護方針（Ｐポリシー公開あり：+/なし：－）	ユーザへの説明責任（高い：＋/低い：－）	スコア
A	+	－	－	+	0
B	+	+	+	－	＋1
C	+	+	－	+	＋2
J	+	－	－	－	－2
E	－	+	－	－	－2
P	+	+	－	+	＋2
O	+	+	－	+	＋2
H	+	+	－	+	＋2
K	+	+	+	+	＋4

図　3-13　リスク指標

次に、自治体別に利活用とリスク意識をスコアリングしたものを、利活用とリスク意識による４象限マップ上にプロットする。ポジショニングされる象限によって、どちらの意識が強いのかを判定する。

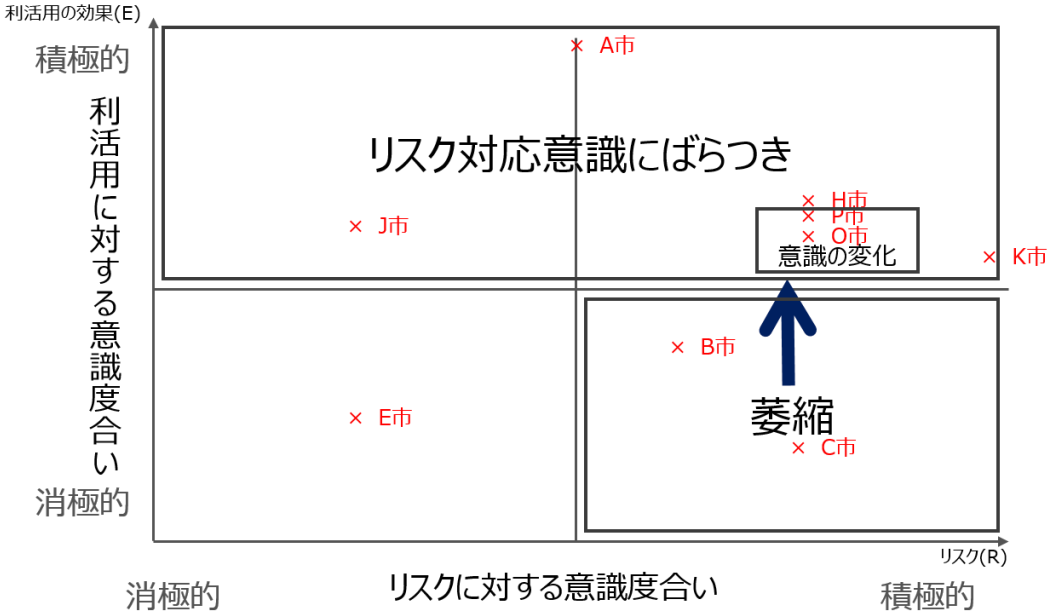

図　3-14　利活用とリスク意識のポジショニングマップ

４つの象限にプロットされたものから、主に３つの特徴的な傾向が読み取れる。

① リスク対応意識にばらつき

利活用に積極的であるが、リスク認識や対応レベルにばらつきがあることがわかった。データ利活用の目的は自治体によって異なるが、共通して「統計情報」を活用した地域住民全体に対するアプローチの試みが確認できた。その理由として、「統計情報」から個人が識別、特定されるリスクが低いことや、一人ひとりの小さな改善が大きな集団効果を見込める点にあると考えられる。リスクに対する意識はばらつきがあることも確認できた。

② 利活用意識が積極的に変化

予備調査で利活用に消極的または中立的な２自治体Ｐ、０が、利活用に積極的な姿勢に転じていることがわかった。

③ 萎縮の傾向

リスク意識が高いが、利活用に萎縮している傾向があることがわかった。

「個人に関する情報」に対する利用意識は低く、総じてリスク回避姿勢が強いことがわかった。システム的には暗号化や個人を再識別する際の復号化で用いる鍵を厳格に管理していることは公知であったとしても、「個人に関する情報」の取り扱いには非常に慎重な態度が見られ、利活用に萎縮している傾向がある。

参考までに、利活用に積極的な5自治体については、予備調査においていずれもKDBシステム導入にあたり、個人情報保護審議会の議事録からは、組織としてのコンセンサスを得られていることを確認している。また自治体Aについても、予備調査では個人への説明責任意識が低かったものの、その後やや意識の改善が見られる。

3.5.2　自治体統計データとの相関分析

自治体が公開する統計データのうち、「特定健診受診率および指導対象者比率」「高齢者（65 歳以上）比率」「一人当たり医療費（年間）」「人口に占める要介護認定者比率」について、相関関係を分析する。

・特定健診受診率および指導対象者比率との相関分析

図 3-15 に特定健診受診率および指導対象者比率との相関図を示す。特定健診受診率を外円に表示し、指導対象者比率を内円に示し、円の面積は比率に比例する。尚、データが取得できなかった自治体については非表示としている。

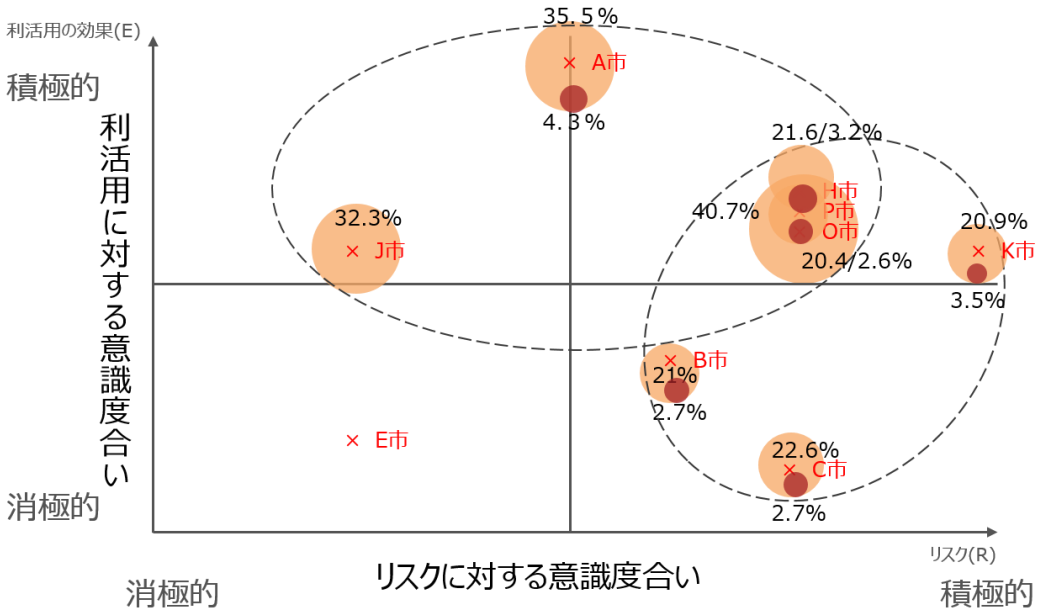

図　3-15　特定健診受診率および指導対象者比率

健診受診率、指導対象者比率が相対的に高い自治体（第一、第二象限に跨り破線で囲った部分）は、利活用に積極的な傾向がみられる。いっぽうで健診受診率、指導対象者比率が相対的に低い自治体（第三象限と第一象限の一部に跨り破線で囲った部分）は、逆の現象が見られた。指導対象者比率を高めるためには、個人へのアプローチを積極的に推進する必要があると思われるが、自治体 B、C は、保健師の関与が消極的な結果も確認されており、指導対象者比率が改善しない要因となっているかもしれない。

・高齢者（65 歳以上）比率との相関関係

図 3-16 に高齢者（65 歳以上）比率との相関図を示す。自治体人口規模を円面積で表しており、青色部分が人口に占める高齢者比率である。高齢者比率が概ね 20%を超える自治体が、比較的利活用に積極的な結果となっている。高齢化は人口構造的な課題であるため、利活用に積極的な動機付けになっている要因と言える。

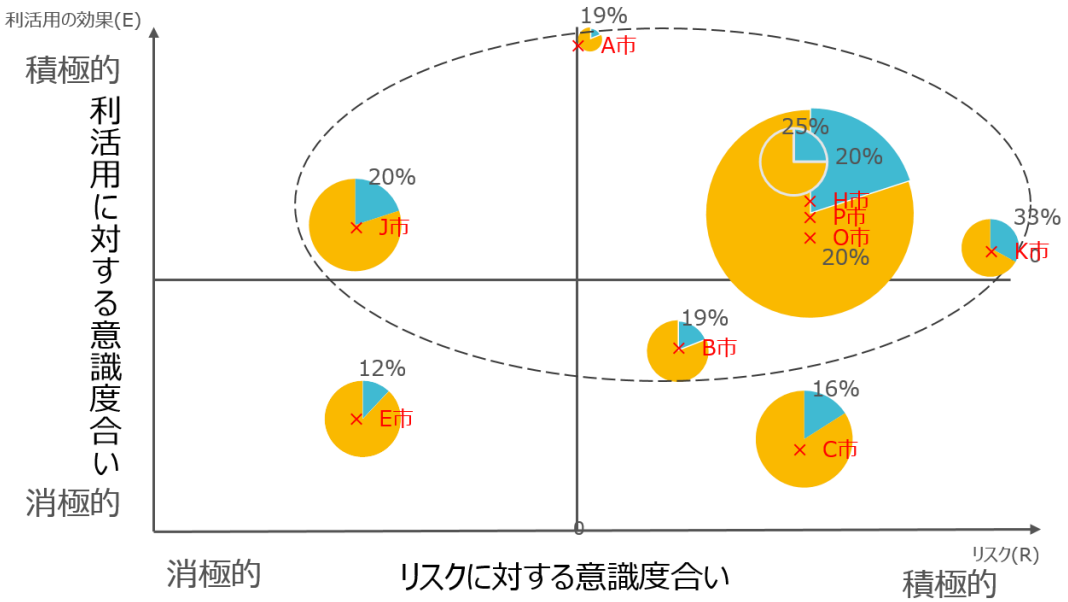

図　3-16　高齢者（65 歳以上）比率

・一人当たり医療費（年間）との相関分析

図 3-17 に一人当たり医療費（年間）との相関図を示す。円内の数値は一人当たり年間医療費（単位：万円）を示している。

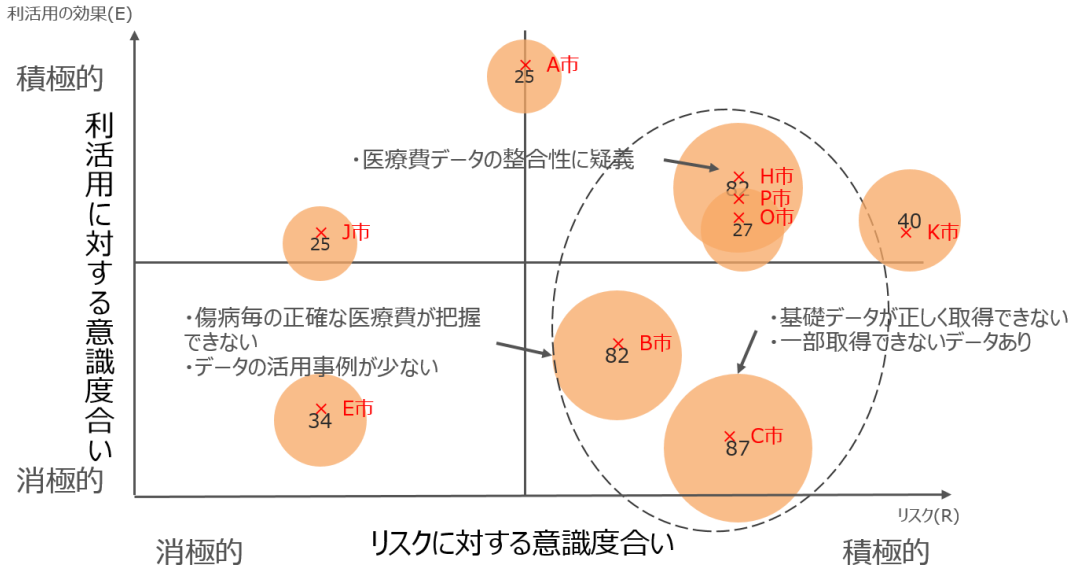

図　3-17　一人当たり医療費（年間）

前頁で示した高齢化率と医療費に強い相関関係はないと言えそうである。医療費が相対的に高い自治体は、リスクに積極的な傾向にあると言える。また自治体B、C、P、Oの共通点として、個人アクセス時のリスク対応意識が高いこと、そのうち自治体C、P、Oはユーザへの説明責任意識が高いという結果が得られている。

また、自治体B、C、Pいずれもデータ分析過程において、何らかの不備や改善要望の指摘が多く、特に医療費分析に関わるデータ分析ニーズが高いことが読み取れる。データへの信頼性低下が利活用に消極的にさせる要因になっていることが考えられる。

・人口に占める要介護認定者比率との相関分析

図 3-18 に人口に占める要介護認定者比率との相関図を示す。要介護認定者比率を円面積で示す。

図からも見られるように、利活用とリスク意識との相関関係は確認できなかった。また、他の統計データとの相関についても、特徴的な内容は見られない。

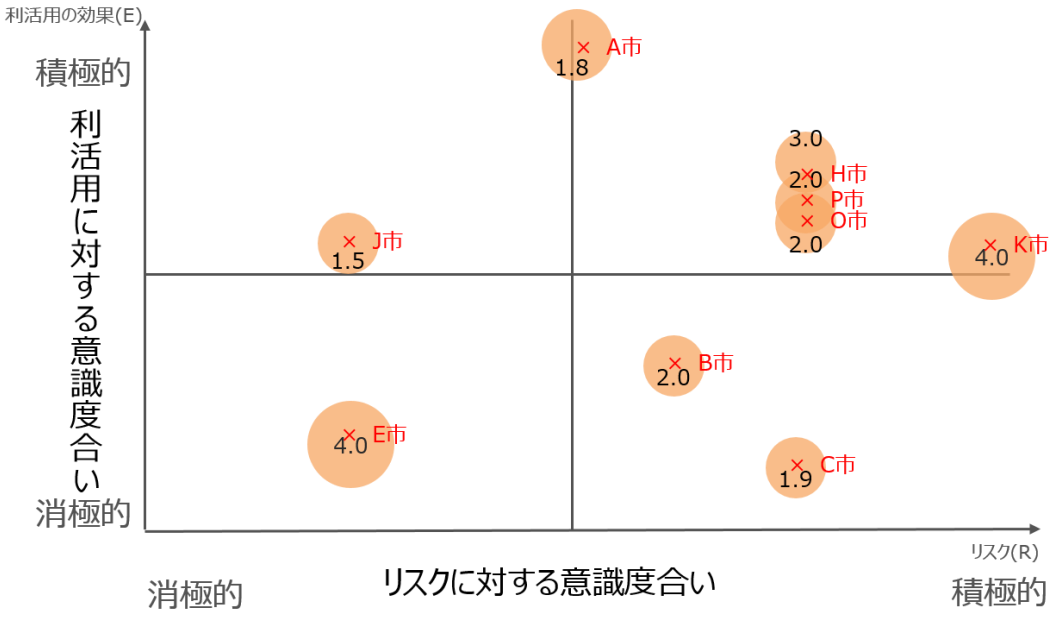

図　3-18　人口に占める要介護認定者比率

3.5.3　相関分析に対する考察

アンケート結果と統計データとの相関分析の結果より、図 3-14 で示した利活用とプライバシーリスク意識のポジショニングマップに基づいて考察を加えた。自治体の抱える課題と課題に対する意識に着目し、組織を４つのタイプに分類した。分類した組織タイプを図 3-19 に示す。

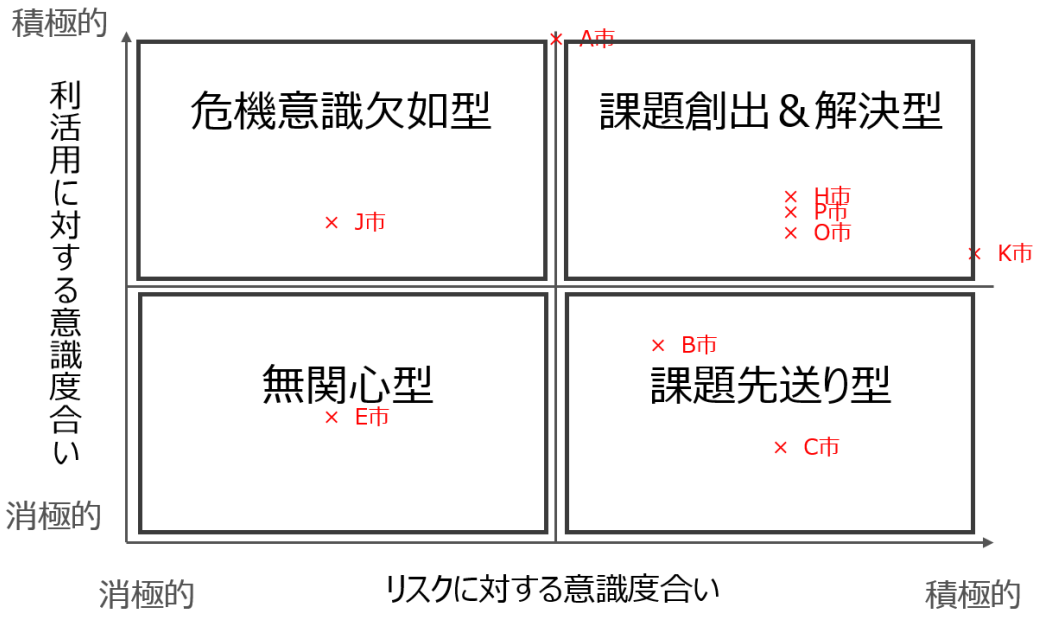

図　3-19　利活用とプライバシーリスク意識から見た組織タイプ

・課題創出＆解決型

顕在的な課題のみでなく、ビッグデータ分析を通じて潜在的課題の創出意識が高いことを意味する。統計データ相関分析から明らかになったように、顕在的な課題を抱えていることが、利活用に積極的になっている要因と言える（表 3-3 網掛け部分を参照）。自治体 O、P が利活用に積極的に転じたのも、保健師による参加やポピュレーションアプローチに積極的なことが、アンケート結果から言える。背景には両自治体が抱える課題として、高齢者比率が相対的に高い点や、自治体 P では特定健診受診率が低いことを認識した結果であると言える。

表　3-3　統計データ（自治体H、K、O、P）

自治体	特定健診受診率（保健指導者比率）	高齢者比率	一人当り医療費	要介護認定者比率
H	21.6%（3.2）	25%	82 万円	3.0%
K	20.9%（3.5）	33%	40 万円	4.0%
O	40.7%（1.5）	20%	27 万円	2.0%
P	20.4%（2.6）	20%	82 万円	2.0%

・危機意識欠如型

利活用に積極的ないっぽうで、‘個人アクセス時のリスク対応意識’と、‘ユーザへの説明責任’に対する意識が欠如しているタイプである。統計データの分析では、表 3-4 に示すとおり、自治体A、Jは相対的に課題が大きくないことが分かっており、敢えて積極的にプライバシーリスク解消に取り組む必要性がないと感じているのかもしれない。

表　3-4　統計データ（自治体A、J）

自治体	特定健診受診率（保健指導者比率）	高齢者比率	一人当り医療費	要介護認定者比率
A	35.5%（4.3）	19%	29 万円	1.8%
J	32.3%（データなし）	20%	25 万円	1.5%

・課題先送り型

プライバシーリスク対応意識は高く、課題意識は高いと思われるが、利活用に踏み出せない状態である。表 3-5 にも示すように、自治体B、Cともに一人当たり医療費が高い（表網掛け部分）。アンケート回答からは保健師の関与に消極的な回答が得られている。また自由記述回答から、医療費分析データに関する課題・問題意識を有していることからも、保健師の関与に少なからず影響しているのではないかと考える。

表　3-5　統計データ（自治体B、C）

自治体	特定健診受診率（保健指導者比率）	高齢者比率	一人当り医療費	要介護認定者比率
B	21%（2.7）	19%	82 万円	2.0%
C	22.6%（2.7）	16%	87 万円	1.9%

・無関心型

利活用に関心がない、もしくは関心はあるが組織の取り組みが停滞しているような状態であり、最も深刻な状態である。自治体Ｅがどちらの状態なのかは、相関分析からは要因を把握するこはできなかったが、課題解決や価値創造に向けた取り組みに向けた意識の変化を促すことが必要である。

3.5.4　組織変革へのアプローチ

利活用とプライバシー保護の両立を実現する組織に変革するためのアプローチ方法を考える。図 3-20 に課題創出&解決型組織へのアプローチについて示す。

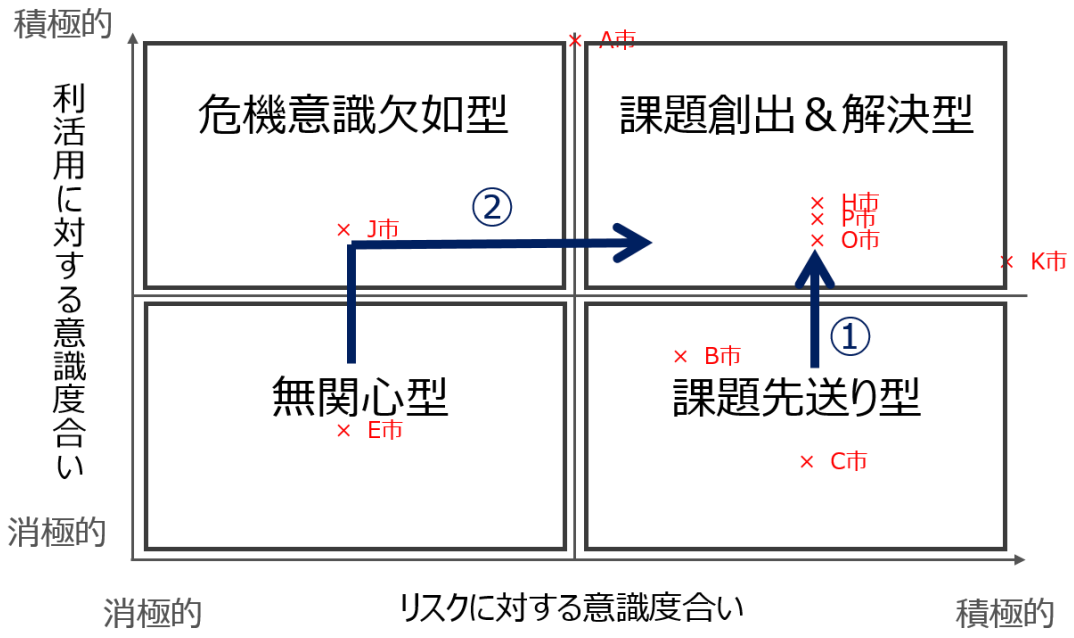

図　3-20　課題創出&解決型組織へのアプローチ

理想とする組織へ変革するためには、2 つのアプローチが有効であると考えた。①のアプローチは調査結果からも明らかになったように、組織における課題認識と共有プロセスが利活用を促進すること、また課題を先送りしている何らかの要因を排除することが必要であると考える。また、②のアプローチはプライバシーリスク対応よりも利活用を優先したアプローチが必要であることを、筆者が推奨するものである。特にビッグデータ活用が社会問題の解決に有効となるようなケースの場合は、プライバシー保護よりも利活用を優先すべきであると考える。

４章

アクティブ・プライバシー・マネジメントモデルの提案

4.1　はじめに

前章で分析した結果から、統計データに表れているような顕在的な課題が利活用の意識に影響していることが読み取れた。特に意識の変化が見られた組織において、何らかの課題認識と利活用を促進するプロセスが組織内で働いていたと仮定すれば、他の自治体にとっても示唆を与えるものになるはずである。

また、事前の電話によるアンケート承諾の際に確認できたことであるが、調査対象の殆どの自治体が同じ組織または小集団で取り組んでいると思われ、果たして利活用とプライバシー保護という難しい運営ができるのか、不安を感じざるをえなかった。本来であれば、プライバシー保護の実効性を牽制する組織は独立しているべきだと考えるためである。

本章では、分析結果から得られた知見や課題を踏まえた上で、利活用とプライバシー保護を両立させるための新しいアプローチ概念として、アクティブ・プライバシー・マネジメントモデルを提案する。

4.2　アクティブ・プライバシー・マネジメントモデル

アクティブ・プライバシー・マネジメントモデルを図 4-1 に示す。本モデルの特徴として、以下の概念を取り入れた。

・公共の利益に資する場合は、目的と効果を説明することを前提に利活用を優先

・プライバシー侵害発生時の検証と説明責任（リアクティブなリスク対応）

・利活用とプライバシー保護の両立を促進する価値転換チェーン

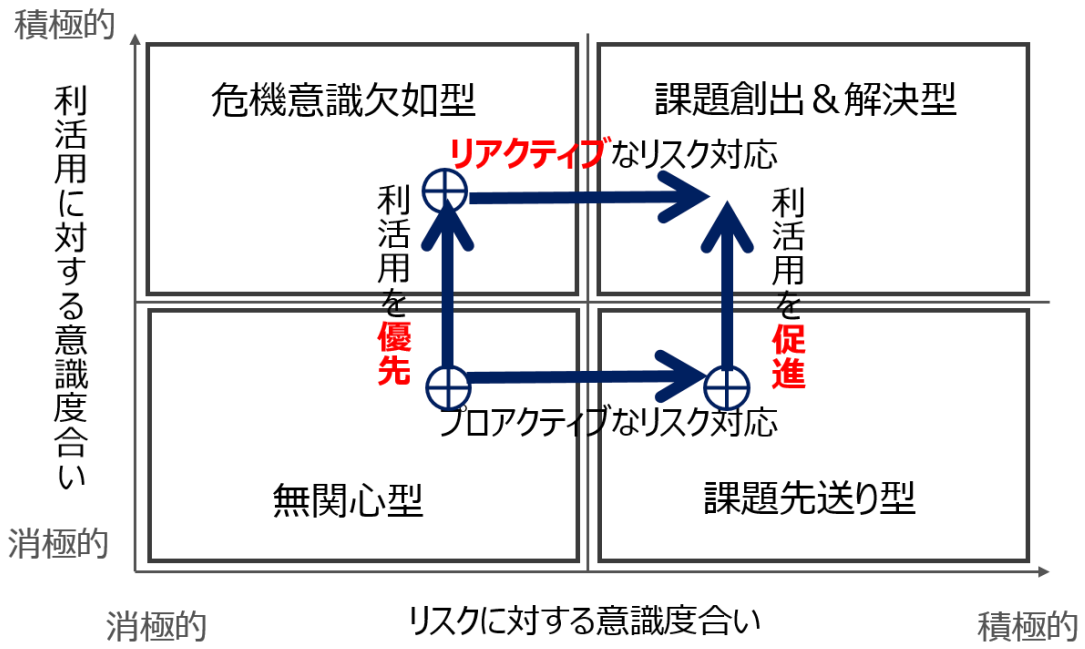

図　4-1　アクティブ・プライバシー・マネジメントモデル

公共の利益に資する目的であれば、プライバシーリスクに萎縮することなく、利活用に積極的に取り組むことを推奨したい。また、リアクティブなリスク対応アプローチは、先行研究で示したPbDの概念であるプロアクティブな考え方とは、ある意味対照的な考え方である。プロアクティブな対応が望ましいことは言うまでもないが、事後的にでもリスクに対して、組織として取り組んでいくためのアプローチが重要である。本モデルの事後的な対応は場当たり的な対応ではなく、利活用とプライバシー保護のどちらの意識に偏っているかを客観的に評価した上で、現在のポジショニングを把握した上で、適正なレベルに引き上げていくという考え方に基づいている。

プライバシー侵害の発生を完全に予想し予防することは困難である。PbDのプロアクティブな考え方を踏襲しつつも、仮にプライバシー侵害が起こった場合でも、利用者が納得できる告知や説明がなされていたかを確認し、不足する情報があれば補完するための情報提供と丁寧な説明をすることで、理解を得られるよう配慮するという取組みが現実的には必要な対応になってくるであろう。

一般論として、利活用とプライバシー保護にはトレードオフの関係にある。KDBシステムの利活用について言えば、KDBシステムのデータを多角的、多面的に分析することで、医療費削減や重症患者の削減等、活用度合いに比例して得られる期待効果は小さくない。他方で、高額医療や重症患者のデータを特定することで、プライバシー侵害リスクは高まることは容易に想像できる。とはいえ、公共の利益に資する目的でビッグデータを活用するのであれば、極度にプライバシーリスクに萎縮することなく、積極的に利活用に取り組むことを優先すべきである。避けるべきは、組織としての意思決定が、利活用に積極的であったとしても、それが実務レベルに移行するに従い、実務者の意思が強く働くことで、利活用に萎縮する傾向が強くなってしまうことである。いっぽうで、組織としてのリスク管理・統制能力が備わった自治体は利活用に前向きに取り組むことができるだろう。

また、アクティブ・プライバシー・マネジメントモデルを推進する価値転換チェーンのフレームワークを構築した。概念を図4-2に示す。価値転換チェーンは、ビッグデータ利活用とプライバシー保護の実現における価値形態の変化を表しており、組織内における活動の連鎖を再構築するためのフレームワークである。

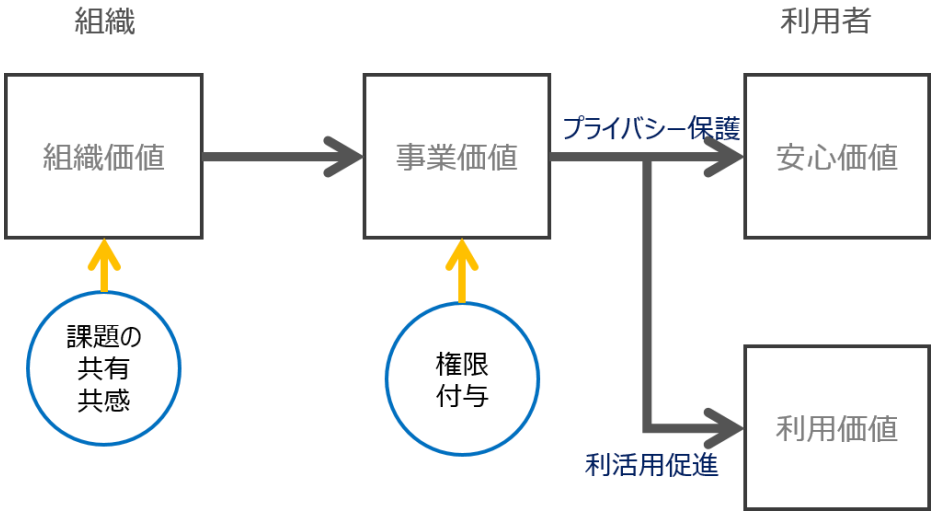

図　4-2　価値転換チェーン

アクティブ・プライバシー・マネジメントモデルを推進するための駆動装置として価値転換チェーンの概念を説明する。本フレームワークは、サッサー、ヘスケット（1994）によって提唱された組織におけるサービス・プロフィット・チェーンの概念が根底にある。利活用とパーソナルデータ保護の両立を図るためには、強固な組織内コミットメント、顧客との信頼関係、実務担当者に対して経過を含む業績結果に対する承認と評価が重要な要素となる。顧客接点の最前線に立つ実務担当者への権限付与と承認や評価が、実務担当者の責任感と自立心を高め、利用者価値向上と組織としてのリスク管理能力を高めることに繋がると考えるためである。

利活用とプライバシー保護へのアプローチにおける、価値転換チェーンの期待効果は次のとおりである。

・利活用へのアプローチ

組織内において、課題と目標の「認識」→「共有」→「共感」のプロセスを経た後、現場に対して「権限」を与えることで取り組みを推進する。ここで言う「共感」は、組織ヒエラルキーの上位職までをも含めた共感を得ることが、次の「権限」付与のための推進役として大きな意味を持つ。また、取り組み内容に対して「評価」を加えることで、利用者に対する「利用価値」を最大化する。「評価」は結果に対する評価だけでなく、

継続的な取り組み内容に対する有用性の評価でもあり、実務担当者のモチベーションに繋がるものである。

・プライバシー保護へのアプローチ

前述と同様に、組織内におけるリスクの「認識」→「共有」→「共感」のプロセスを経た後、現場に対して「権限」を与えることで取り組みを推進する。プライバシー保護の局面では、具体的に何をどのレベルまで保護策を講じればよいかの判断は難しい。法令順守は勿論であるが、しくみの活用と運用者の意識を徹底することは重要である。また、これで万全だというものがない限り、プライバシー保護策の取り組み内容に対しては「承認」という正当性を与えることで、組織としてのコンセンサスを明確にするとともに、責任の所在を明確にすることが欠かせない。これは、結果的にサービス利用者に対する説明責任を果たすことにも繋がり、「安心価値」を提供することに寄与する。

第５章　結論と含意

5.1　結論

以下に、各リサーチ・クエスチョンに対する解を示す。

SRQ1：利活用の効果とリスク度合いにはどのような関係があるか？

アンケート調査からは利活用効果を十分に把握できなかったが、利活用の期待効果が高いほど、リスク度合いは高まる傾向にあると言える。「統計情報」と「個人に関する情報」を対比した場合、「統計情報」から得られる効果よりも「個人に関する情報」に基づき、重複診療の実態や重症化予防対策の一環で、個人に直接アプローチすることは、高額医療費の抑制対策から得られる期待効果が大きい。

SRQ2：リスクに対する効果的なIT技術やルールにはどのような関係性があるか？

リスクに対する効果的な技術としては、PPDMで提唱される匿名化や暗号化技術が有効であることは公知であり、暗号化技術はKDBシステムでも採用されている。

ルールである改正個人情報保護法36条～39条に、個人情報取扱事業者の義務規定として「匿名加工情報」に関するルールが追加された。匿名加工情報を作成する際は、個人情報を復元不可能な状態で加工する必要がある。加えて、識別行為をも禁止したことで、一定の歯止めがかけられたと言える。また、匿名化技術とルールを一元的に管理・監督する独立機関である個人情報保護委員会が新設されたことで、技術の信頼性が担保される関係性が構築されることは大きな進歩である。

SRQ3：プライバシーマネジメントモデルは、組織におけるビッグデータ利活用の意思決定において、どのような影響を与えるか？

利活用とプライバシー保護のどちらの意識に偏っているか、客観的な評価を与えることができる。また利活用とプライバシー保護意識の度合いから４つの組織タイプに類型することで、目指すべき方向性の示唆を与える。

MRQ：ビッグデータの利活用とプライバシー保護の両立を実現するためのプライバシーマネジメントモデルは、どのようなものか？

組織における利活用とプライバシー保護に対する意識の度合いを客観的に判定した上で、課題創出&解決型組織へ変革するためのアプローチモデルである。特に社会的課題解決に資する目的でビッグデータを用いる場合は、プライバシー保護よりも利活用を優先すべきである。プライバシーリスク対応は必要最低限の予防措置を講じておくことに加えて、プライバシーリスクが発生した場合の説明責任を果たすことに主眼を置く。また、実務推進のために、サービス・プロフィット・チェーンの概念を根底に持つ価値転換チェーンのフレームワークを構築した。利活用とパーソナルデータ保護の両立を図るためには、組織における課題認識と共有、共感が組織価値向上に不可欠である。そして、顧客設定の最前線に立つ実務担当者への権限付与が、実務担当者の責任感を醸成し、顧客価値の最大化に繋がるものである。それは、プライバシー保護による安心価値、利活用促進による利用価値を意味する。

5.2　理論的含意

ビッグデータ利活用とプライバシー保護をいかに両立させるかは、様々な事業領域で直面する課題である。本研究では、企業利益向上に主眼を置いたサービス・プロフィット・チェーンにおけるステークホルダーの関係性に着眼し、サービスの価値創出とリスク管理をマネジメントするフレームワークを提案した。

5.3　実務的含意

自治体におけるKDBシステム利用事案に限らず、民間企業においてもビッグデータの活用事例を挙げれば枚挙に暇がない。行政と民間企業の取り組みの有り様を比較した場合、意識決定と実務段階における取り組みスタンスには違いがある。民間企業は営利追及を目的としているため、意思決定から実務まで一貫して利活用に積極的な姿勢である。他方、行政は住民に対して公共サービスの提供役務を負うことを使命としており、本研

究で実施した調査でも明らかになったように、意思決定段階では利活用に積極的であったが、実務段階でリスク回避志向におちいる傾向がある。このことは、特定の行政組織に内在する問題と言うより、これからビッグデータと向き合っていかざるをえないすべての組織が直面する課題である。

従って、本モデルは、民間企業でも利活用に萎縮する傾向にある組織においては、利活用とプライバシー保護への取り組みを積極的に推進するための有効なアプローチと考える。本モデルを自治体に広く導入し、社会資本としての医療サービスの価値向上と効率化の取り組みが必要である。

5.4　将来研究への示唆

本研究では、KDB システムの事例をモデルとして、ビッグデータの利活用とプライバシー保護の両立を実現するためのフレームワークとして、アクティブ・プライバシー・マネジメントモデルを提案した。本モデルは、民間、公共分野を問わず、普遍的に適合できる可能性があると考えているが、以下の点を考慮した更なる研究が必要と考える。

・利活用とプライバシー保護の意識評価の客観性担保

提案モデルでは、利活用とリスク意識の重み付けをする簡易な方法として、リスクと利活用の効果における意識の度合いを指標化し、スコアリングするという手法を用いた。アセスメント評価項目の選択は筆者が、評価はアンケートにより主体組織自身で回答したものであるが、より客観性を担保するためには、独立性の高い機関、例えば個人情報委員会がアセスメント項目の選定と評価を、実施した結果に基づき分析するというスキームを考える意義はある。

・アクティブ・プライバシー・モデルの適合性

本研究の事例では、大半の自治体が「統計情報」を活用すると回答しており、実際に効果があったという自治体もあった。「統計情報」のみを活用した集団へのアプローチで十分な効果が得られるのではという先入観や、人口規模が小さい自治体では集団母数が小さいが故に、個人へのアプローチ効果が大きいと期待するのは、早計である。例え

ば規模の大きい自治体でも、医療費の高騰原因が、一部の高額医療患者や重症予備軍に占める割合が高ければ、個人へのアプローチが有効なはずである。利活用のアセスメント項目に、「コスト・収益弾力性の高い要素の認識」を追加することで、利活用の効果を高めることに貢献できると考える。

参考文献

米国医療の質委員会/医学研究所　訳　医学ジャーナリスト協会（2002）『医療の質』，日本評論社

福田(2007)「公衆衛生分野における政府統計の利活用と個人情報保護」『学術の動向』，pp.30-35

八山幸司　JETRO/IPA Network（2014）『米国におけるビッグデータ活用に関する動向』
<https://www.ipa.go.jp/files/000042274.pdf>(2016/5/2 アクセス)

星野(2015)「医療ビッグデータの利活用によるサービス創出の枠組み」『UNISYS TECHNOLOGY REVIEW　第123号』，pp.3-11

五十嵐　大・高橋克己（2012）「注目のプライバシー　Differential Privacy」，pp.40-49

Inovation Nippon研究会（2013）「パーソナルデータ保護分野におけるマルチ・ステークホルダー・プロセスの役割と設計」

石田(2015)　「状態遷移の視点による「匿名加工情報」に関する一考察」『情報処理学会研究報告』，pp.1-10

伊藤・小暮（2016）「パーソナルデータのプライバシー保護を実現する匿名化・暗号化技術」，FUJITSU，pp.26-33
<http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol67-1/paper05.pdf>(2016/5/2 アクセス)

IT総合戦略本部事務局（2013）『技術検討ワーキンググループ報告書（佐藤委員提出資料）』第５回検討会【資料２－１】
<https://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf>(2016/3/5 アクセス)

IT総合戦略本部事務局（2014）『各分野の個人情報保護ガイドラインにおけるセンシティブデータの定義及び取扱い』 第７回検討会【別添４－１】
<http://www.kantei.go.jp/jp/singi/it2/pd/dai7/siryou1-2b.pdf>(2016/3/5 アクセス)

IT総合戦略本部事務局（2014）『「個人情報」等の定義と「個人情報取扱事業者」等の義務について（事務局案）詳細編』 第８回検討会【資料１－２】
<http://www.kantei.go.jp/jp/singi/it2/pd/dai8/siryou1_2.pdf>(2016/3/5 アクセス)

IT総合戦略本部事務局（2014）『「（仮称）準個人情報」及び「（仮称）個人特性性低減データ」に関する技術的観点からの考察について（中間報告）』 第９回検討会【資料２－２】

〈http://www.kantei.go.jp/jp/singi/it2/pd/dai9/siryou2-2.pdf〉(2016/3/5 アクセス)
IT 総合戦略本部事務局（2014）『第三者提供におけるオプトアウトの適正な執行について』 第１０回検討会【資料２－１】
〈http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou2-1.pdf〉(2016/3/5 アクセス)
IT 総合戦略本部事務局（2014）『パーソナルデータの利活用に関する制度改正大綱（事務局案）』第１１回検討会【資料１】
〈http://www.kantei.go.jp/jp/singi/it2/pd/dai11/siryou1.pdf〉(2016/3/6 アクセス)
伊豆、阿比留(2012)「プライバシー保護を考慮したセンサーデータの利活用について」『Computer Security Symposium 2012』, pp.201-207
泉(2014)　「パーソナルデータ活用における、プライバシー保護データマイニング(PPDM)の適用」『経営課題にAIを！ビジネス・インフォマティクス研究会資料』
實成、笠島(2007)「公衆衛生現場における行政情報の活用と個人情報保護」『学術の動向』, pp.16-25
株式会社国際社会経済研究所「高齢社会と ICT―諸外国の動向」第5回 ICT 超高齢社会構想会議 WG
〈http://www.soumu.go.jp/main_content/000219322.pdf〉(2016/4/12 アクセス)
株式会社日立コンサルティング(2011)「「医療・ヘルスケア分野におけるクラウド・コンピューティングに関する国内外の制度・技術動向等の調査研究」事業報告書」
〈http://www.meti.go.jp/meti_lib/report/2011fy/E004298.pdf〉(2016/ 3/10 アクセス)
国民健康保険中央会(2015)「国民健康保険の安定を求めて　医療保険制度の改革」, p.28
〈https://www.kokuho.or.jp/about/lib/kokuhonoantei2015.pdf〉(2016/3/13 アクセス)
森下(2015)「サービスマネジメントとしての顧客志向とおもてなし」『第6回横幹連合コンファレンス』, pp.289-292
森田、荒井(2014)　「医療データ利用におけるプライバシー保護の課題とその解決策の提案」『The 28th Annual Conference of the Japanese Society for Artificial Intelligence,2014』, pp.1-4
村上　聡（2014）「ビッグデータの利活用とプライバシー保護について」『通信ソサイエティマガジン No29』, pp.52-58
中川裕志（2014）「匿名化の実社会での利用に向けての技術課題」,『人工知能学会全国大会論文集 28』, pp.1-4

中谷、小林(2005)「ヒト組織を研究利用するための基盤整備：ヒト組織の提供から保存まで」『日薬理誌（Folia Pharmacol.Jpn.）126』，pp.391-398
根本忠明・服部伊人・佐藤健一（2010）「デジタル監視社会における個人情報保護と情報セキュリティ管理」『情報科学研究第19号』，pp.1-26
西村善博（2011）「フランスにおける個人情報保護法と個人データの統計利用に関するB.リヤンディの報告（解題と翻訳）」『統計学第100号』，pp.91-99
野中郁次郎・紺野登（1999）『知識経営のすすめ　ナレッジマネジメントとその時代』
「医療情報利活用における匿名化技術ガイド」『JIRA　医療画像システム部会　新IMIT-WG SWG3』
NTI Today(2014)「匿名化技術の最新動向とその課題」，No.64, pp.10-11
<http://www.nii.ac.jp/userdata/results/pr_data/NII_Today/64/p10-11.pdf>(2016/5/3 アクセス)
沖(2012)「医療システムでの非構造化データ活用事例」『UNISYS TECHNOLOGY REVIEW 第111号』，pp.69-77
大坂(2004)「独立行政法人国立病院機構内での個人情報共有のための環境整備」『IRYO Vol.58 No.11』，pp.621-630
大谷卓史（2014）「プライバシーは財産なのか」『情報管理vol.56 no.10』，pp.719-723
千田(2015)「高気密データも安全に二次利用可能な「秘密計算技術」」『NTT技術ジャーナル』，pp.67-70
<http://www.ntt.co.jp/journal/1403/files/jn201403067.pdf>(2016/5/20 アクセス)
千田(2013)「プライバシーを守ったITサービスの提供技術」『情報処理　Vol.54　No11』，pp.1130-1134
島津　望（2005）『医療の質と患者満足』千倉書房
新保史生（2010）『情報管理と法』 勉誠出版
宍戸常寿（2014）「パーソナルデータに関する第三者機関について」『Jurist 2014年３月号』有斐閣, pp.18-24
総務省（2014）『付注４－１　データの高度な利活用による業務・サービス確信が我が国経済および社会に与える波及効果に係る調査研究（アンケート概要）』
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nd270000.html>(2016/4/12 アクセス)
Suicaに関するデータの社外への提供についての有識者会議（2013）「Suicaに関するデータの社

外への提供について　中間とりまとめ」
<http://www.jreast.co.jp/chukantorimatome/20140320.pdf>(2016/4/12 アクセス)
鈴木正朝・高木浩光・山本一郎（2015）『ニッポンの個人情報』翔泳社
高橋（2012）「パーソナルデータ利用・流通のためのプライバシーを制御する技術」，NTT セキュアプラットフォーム研究所，pp.1-28
<http://www.soumu.go.jp/main_content/000305107.pdf>(2016/5/3 アクセス)
高橋（2015）「公的統計の高度な二次利用のための秘密計算技術の応用の研究」，総務省統計研修所，pp.1-30
<http://www.stat.go.jp/training/2kenkyu/research/pdf/resear34-1.pdf>(2016/5/3 アクセス)
高島，洋典（2012）「＜産業界の技術動向＞ビッグデータ」，京都大学電気関係教室技術情報誌，pp.8-12
<http://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/156047/1/cue27_03.pdf>(2016/5/2 アクセス)
辻、渡辺()「個人情報をめぐる制度設計の検討プロセスに関する考察」『城西大学経営紀要　第11号』，pp.45-73
宇賀克也（2014）「パーソナルデータの利活用に関する制度見直し方針について」『Jurist 2014年３月号』 有斐閣，pp.12-17
瓜生(2014)「新しい制度設計にあたっての状況認識」,pp.11-13
山本(2010)「HER が変える保健医療　-諸外国の取り組みと我が国への示唆-」『海外社会保障研究　Autumn 2010 No172』，pp.31-41
八津川(2015)　「プライバシー・バイ・デザインに基づく適正なパーソナルデータの取り扱い」『UNISYS TECHNOLOGY REVIEW 第123号』，pp.52-53
湯原伸一（2014）『「情報管理」に強くなる法務戦略』 中央経済社
@IT(2015)「匿名化技術と PPDM」
<http://www.atmarkit.co.jp/ait/articles/1503/24/news010.html>(2016/4/12 アクセス)

付録

付録１．国保ＤＢの利活用と情報保護に関するアンケート調査

下記アンケートにご協力頂き、ありがとうございます。国保ＤＢの利活用と保護の観点に関して、下記Ｑ１からＱ１２までの質問に回答願います。Ｑ１からＱ８が利活用に関する質問で、Ｑ９からＱ１２までは情報保護に関する内容になっております。

（データ利活用の観点）

Ｑ１．現在、国保データベースを活用していますか？活用程度に関係なく、活用している場合は「はい」で回答願います。

（ はい／いいえ ）

Q1 で「はい」と回答した場合、Ｑ２からＱ６まで回答ください。「いいえ」と回答した場合はＱ７について回答願います。

Ｑ２．国保データの分類としては、統計情報と個人の健康に関する情報 の２種類があると理解しています。よく用いられている統計情報メニューを教えてください。（複数可）

Ｑ３．データ分析にはある程度、専門スキル（解析スキル、医療知識）が必要と想定しています。事前の国保中央会様へのヒアリングで各自治体にて保健師の方がデータ分析に参画しているとも聞いておりますが、御自治体では保健師の方がどの程度関与していますか？該当するものを選択願います。

（主体的に参加／助言する程度／あまり関与せず／全く関与していない）

Ｑ４．これまでにデータ利活用でどの程度効果がありましたか？

（かなり効果があった／まあまあ効果があった／あまり効果がない／これから効果検証する段階／その他（ ））

Ｑ５．Ｑ４で、「かなり効果があった」「まあまあ効果があった」と回答した場合、統計データまたは個人に関する情報 どちらのデータを活用した場合に効果がありましたか？ また具体的にどのような効果があったかご教示ください。差支えない範囲で結構です。

Ｑ６．Ｑ４で「あまり効果がない」と回答した場合、今後、更に国保ＤＢの利活用を推進していくにあたり、具体的な対策や計画があれば、差支えない範囲でご教示ください。

Ｑ１で「いいえ」と回答した場合のみ

Ｑ７．活用していない理由は何ですか？差支えない範囲で結構です。

Ｑ８．国保ＤＢの利活用推進の観点から、現状の課題や問題点についてあれば、可能な範囲で結構ですのでご教示願います。

（個人情報保護の観点について）

Ｑ９．国保データベースには、統計データと個人に関する情報の２種類が存在しますが、統計データ（いわゆるビッグデータ）の場合でも 分析結果によっては、個人が識別または特定しうるというリスクがあると言われていることを知っていますか。（ 知っている／知らない ）

Ｑ１０．国保データのうち、個人に関する情報は暗号化管理されています。いっぽう統計データについては、もともと個人を識別・特定できないデータであるものの、分析過程で個人を識別または特定できてしまうケースも想定されます。個人にアプローチするメリットがあるいっぽうで、プライバシー侵害のリスクも生じますが、この場合どのような対応をされますか。

Ｑ１１．プライバシー侵害リスク回避に向けて、利用者への配慮、透明性確保のためにプライバシーポリシーを作成・公開し、被保険者（自治体住民）に公開・通知していますか。（ している／していない ）

Ｑ１２．Ｑ１１で ‘している’と回答した場合、公開・通知方法を回答願います。また差支えなければ、プライバシーポリシーの内容を添付ください。

Ｑ１３．プライバシーポリシー作成・公開の他に、被保険者（自治体住民）に対して何らかの対応をしていますか。（ している／していない ） ‘している’ と回答された場合、具体的な内容を記載願います。 例）個別に説明している、公報で通知している等

Ｑ１４．個人情報保護またはプライバシー保護の観点から、現状の課題や問題点について、何でも結構ですので可能な範囲で結構ですのでご教示願います。