

Title	データを活用したビジネスにおけるリスクマネジメント手法の考察－RCModelを用いた事例研究－[課題研究報告書]
Author(s)	諸角, 有紗
Citation	
Issue Date	2021-12
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/17606
Rights	
Description	Supervisor: 内平 直志, 先端科学技術研究科, 修士(知識科学)

課題研究報告書

データを活用したビジネスにおけるリスクマネジメント手法の考察

——RCModelを用いた事例研究——

諸角 有紗

主指導教員 内平 直志

北陸先端科学技術大学院大学

先端科学技術研究科

(1830010)

令和3年12月

目次

第1章 序論.....	1
1.1 研究の背景.....	1
1.1.1 データ流通の現状.....	1
1.1.2 データの特性.....	3
1.1.3 データの性質（法律）.....	4
1.1.4 地方公共団体のデータ活用の取組み.....	5
1.1.5 データ流通での課題.....	6
1.1.6 総括.....	7
1.2 調査の目的とリサーチ・クエスチョン.....	7
1.3 調査の方法.....	8
1.4 用語の定義.....	9
1.5 本稿の構成.....	11
第2章 先行研究.....	12
2.1 Risk Chain Model: RCMModel（2020）.....	13
2.1.1 背景.....	13
2.1.2 RCMModel の活用方法.....	13
2.1.3 RCMModel を用いた対策検討.....	15
2.2 Risk Chain Model: RCMModel（2021）.....	16
2.2.1 アップデートの背景.....	17
2.2.2 改良版 RCMModel の活用方法.....	17
2.3 RCMModel ガイド.....	18
2.3.1 ケーススタディ.....	19
2.3.2 RCMModel の構成要素.....	20
2.4 先行研究のまとめと本調査の位置付け.....	23

第3章 データの活用におけるビジネス形態.....	25
3.1 データの種類.....	26
3.1.1 データビジネスの観点.....	26
3.1.2 法律の観点.....	27
3.1.3 法律実務の観点.....	28
3.1.4 営利・非営利の観点.....	30
3.1.5 情報取得の観点.....	31
3.1.6 どのような性質のデータがあるのか (What)	31
3.2 データの活用状況.....	33
3.2.1 データの収集状況.....	34
3.2.2 データの利用状況.....	34
3.2.3 データを活用した分析の状況.....	36
3.2.4 どのようなデータの優先度が高いのか (What)	37
3.3 データの流通および共有方法.....	37
3.3.1 産業の観点.....	38
3.3.2 契約上の観点.....	38
3.3.3 既存の事例の観点.....	42
3.3.4 クリエイティブ・コモンズ・ライセンスの観点.....	43
3.3.5 どのようにデータを流通・共有すべきか (How)	45
3.4 インセンティブ.....	46
3.4.1 産業の観点.....	46
3.4.2 契約上の観点.....	47
3.4.3 法律による観点.....	48
3.4.4 データ提供活性化のために、どのようなインセンティブを与えるべきか (How)	
48	
3.5 オープンデータ.....	49

3.5.1	オープンデータの現状.....	49
3.5.2	オープンデータのルール.....	52
3.5.3	オープンデータの目的.....	53
3.5.4	オープンデータのビジネス.....	54
3.5.5	オープンデータの共創協調領域.....	54
3.6	データの活用におけるビジネスを進めるためのポイント.....	55
第4章	データ利活用に関する課題の整理.....	57
4.1	データビジネスにおけるリスクの考え方.....	57
4.1.1	リスク回避.....	57
4.1.2	リスクテイク.....	57
4.1.3	リスク源の除去.....	58
4.1.4	起こりやすさ (likelihood) の変更.....	58
4.1.5	結果 (consequence) の変更.....	58
4.1.6	リスク共有 (移転).....	58
4.1.7	リスク保有.....	58
4.2	データを流通させるプラットフォームの構成要素.....	59
4.2.1	RCModel からの構成要素の検討.....	59
4.2.2	データ.....	60
4.2.3	アプリケーション.....	61
4.2.4	システムの実行環境.....	61
4.2.5	データ取得時の管理.....	62
4.2.6	データを流通させるプラットフォームの構成要素案.....	67
4.3	データを活用したサービス提供者の構成要素.....	68
4.3.1	RCModel からの構成要素の検討.....	69
4.3.2	倫理規範.....	71
4.3.3	コミュニケーション.....	71

4.3.4 データを活用したサービス提供者の構成要素案.....	72
4.4 利用者の構成要素.....	73
4.4.1 RCModel からの構成要素の検討.....	74
4.5 データ提供者の構成要素.....	74
4.5.1 データ.....	75
4.5.2 データ提供時の管理.....	75
4.5.3 データ提供者の構成要素案.....	77
4.6 RCModel 案.....	78
第5章 データを活用するための検討項目の提示.....	80
5.1 RCModel を用いた検討（A市の構想）.....	80
5.1.1 A市のリスクシナリオ.....	81
5.1.2 A市の RCModel.....	82
5.1.3 A市のコントロールの内容.....	83
5.1.4 RCModel の課題.....	84
5.2 RCModel を用いた検討（B市の構想）.....	84
5.2.1 B市のリスクシナリオの検討方法.....	85
5.2.2 MaaS サービスの検討.....	85
5.2.3 個人認証の検討.....	89
5.2.4 健康管理の検討.....	91
5.2.5 新たな RCModel の検討方法の結果.....	94
5.3 検証結果.....	94
5.3.1 データ版の RCModel の検討方法.....	95
5.3.2 検証による課題.....	95
第6章 結論.....	96
6.1 リサーチ・クエスチョンに対する解答.....	96
6.2 実務的含意.....	97

6.3 本調査の限界と将来研究への示唆.....	98
第7章 参考文献.....	99
第8章 附録.....	102
8.1 民法.....	102
8.1.1 第85条（定義）	102
8.1.2 第180条（占有権の取得）	102
8.1.3 第206条（所有権の内容）	102
8.1.4 第239条（無主物の帰属）	102
8.2 官民データ活用推進基本法.....	102
8.2.1 第11条（国及び地方公共団体等が保有する官民データの容易な利用等）	102
8.3 個人情報保護に関する法律.....	103
8.3.1 第2条（定義）	103
8.3.2 第15条（利用目的の特定）	104
8.3.3 第16条（利用目的による制限）	104
8.3.4 第17条（適正な取得）	104
8.3.5 第18条（取得に際しての利用目的の通知等）	105
8.3.6 第19条（データ内容の正確性の確保等）	105
8.3.7 第20条（安全管理措置）	105
8.3.8 第21条（従業者の監督）	105
8.3.9 第22条（委託先の監督）	106
8.3.10 第23条（第三者提供の制限）	106
8.3.11 第24条（外国にある第三者への提供の制限）	107
8.3.12 第25条（第三者提供に係る記録の作成等）	107
8.4 著作権法.....	108
8.4.1 第2条（定義）	108
8.5 特許法.....	108

8.5.1 第 2 条（定義）	108
8.5.2 第 29 条（特許の要件）	108
8.5.3 第 66 条（特許権の設定の登録）	109
8.6 不正競争防止法.....	109
8.6.1 第 2 条（定義）	109
8.6.2 第 3 条（差止請求権）	111
8.6.3 第 4 条（損害賠償）	111
8.6.4 第 19 条（適用除外等）	111
8.6.5 第 21 条（罰則）	112
8.6.6 第 22 条.....	115

目次

図 1-1	データの流通量 (JETRO 2018)	2
図 1-2	固定通信および移動通信のトラフィック (総務省 2020a: 2)	2
図 1-3	米国および欧州のデータ速度推移 (FairInternetReport 2020)	3
図 1-4	航空運賃の CPI および試算値の比較 (総務省 2019: 8)	4
図 1-5	データを活用したビジネスの日本の強み・弱み (経済産業省 2016: 6)	7
図 1-6	調査の方法	9
図 1-7	本稿の構成	11
図 2-1	リスクインテリジェンスマップ (Deloitte 2017: 2)	12
図 2-2	RCModel の事例 (松本・江間 2020: 14)	14
図 2-3	改良版 RCModel の事例 (松本・江間 2021: 2)	18
図 2-4	RCModel (東京大学 2021: 5)	20
図 2-5	リスク要因の関係性 (東京大学 2021: 別紙)	21
図 3-1	構造化・非構造化データ (総務省 2014: 7)	30
図 3-2	データの性質 (経済産業省 2015a: 7)	30
図 3-3	データの法的保護の対象	32
図 3-4	属性別データ種別	32
図 3-5	データ収集, 蓄積, 利活用のサイクル (経済産業省 2015b: 21)	33
図 3-6	データの入手元 (総務省 2020b: 52)	34
図 3-7	データ分析手法 (総務省 2020b: 50)	35
図 3-8	データ活用の効果 (総務省 2020b: 61)	35
図 3-9	分析に活用しているデータ (総務省 2020b: 44)	36
図 3-10	何種類のデータを組合わせて分析するか (総務省 2020b: 53)	37
図 3-11	データの流通・共有方法 (経済産業省 2015c: 9)	38
図 3-12	新たな流通モデル (総務省 2017a: 18)	43
図 3-13	CC ライセンスの許諾範囲 (クリエイティブ・コモンズ・ジャパン 2021)	44
図 3-14	データの取引方法と条件	46
図 3-15	データのインセンティブ (経済産業省 2015c: 10)	47
図 3-16	データの提供によるインセンティブ	48
図 3-17	属性別データ種別とビジネス	56
図 4-1	データの活用に関する関連法令 (総務省 2017a: 30)	71
図 4-2	データを活用したビジネスの RCModel	79
図 5-1	A 市の構想 (内閣府 2021: 24)	80
図 5-2	A 市の RCModel (例)	83
図 5-3	B 市の構想 (内閣府 2021: 25)	85
図 5-4	B 市の RCModel (例: MaaS サービス)	88
図 5-5	B 市の RCModel (例: 個人認証)	90

図 5-6 B市でのリスクシナリオ（例: 健康管理） 93

表目次

表 1-1	用語の定義	10
表 2-1	リスク要因と構成要素（松本・江間 2020: 12）	14
表 2-2	リスクシナリオでの構成要素ごとのコントロールの例（松本・江間 2020: 15）	15
表 2-3	構成要素の定義（松本・江間 2020: 19-20）	16
表 2-4	リスクシナリオ事例（松本・江間 2021: 3）	18
表 2-5	採用 AI で想定されるリスクシナリオ（東京大学 2021: 4）	19
表 2-6	対応策の検討（東京大学 2021: 6）	20
表 2-7	AI を活用したシステムの構成要素（東京大学 2021: 別紙）	21
表 2-8	サービスの提供者の構成要素（東京大学 2021: 別紙）	22
表 2-9	ユーザの構成要素（東京大学 2021: 別紙）	23
表 3-1	CC ライセンスの種類（クリエイティブ・コモンズ・ジャパン 2021 から作成）	45
表 4-1	データを流通させるプラットフォームの構成要素の検討	60
表 4-2	データを流通させるプラットフォームの構成要素案	68
表 4-3	データを活用したサービス提供者の構成要素の検討	70
表 4-4	データを活用したサービス提供者の構成要素案	73
表 4-5	データを活用したサービスの利用者の構成要素の検討および案	74
表 4-6	データ提供者の構成要素案	78
表 5-1	A 市でのリスクシナリオ（例）	82
表 5-2	A 市のコントロールの内容（例）	84
表 5-3	B 市でのリスクシナリオ（例: MaaS サービス）	86
表 5-4	B 市のコントロールの内容（例: MaaS サービス）	88
表 5-5	B 市でのリスクシナリオ（例: 個人認証）	89
表 5-6	B 市のコントロールの内容（例: 個人認証）	91
表 5-7	B 市でのリスクシナリオ（例: 健康管理）	92
表 5-8	B 市のコントロールの内容（例: 健康管理）	93

第1章 序論

本章では、データを活用したサービスのリスクマネジメントについての手法に関する考察を行った背景および経緯について記載する。調査の目的とリサーチ・クエスチョンを定義し、本調査の調査方法について述べる。

1.1 研究の背景

本節では、データを活用したサービスを対象にした背景を記載するにあたり、まず、データ流通の現状を取上げ、現在、データ流通が注目されていることを述べる。次にデータの特性或データの性質（法律）を取上げ、製品、サービスとは異なった固有の性質があることを述べる。そして、データの活用を促進して行っている地方公共団体のデータ活用の取組みの現状を取上げる。最後にデータ流通のモデルの対象となるデータ流通での課題に注目する理由を述べる。

1.1.1 データ流通の現状

現在、データの流通量が爆発的に拡大している。その理由として、5Gなどの登場によるネットワークが高度化やセンサなどの設置数の増加により、様々な事象がデータ化され、実際に役に立つのか関わらず、データの流通および活用の進展が今後期待されているからである。また、現在、以前に比べ、データの処理速度が高くなったことも理由の1つである。総務省では、データを流通させるためには、以下の4つが重要とされている（総務省 2017a: 11-15）。

- ① データ流通量
- ② データの速度
- ③ データの種別
- ④ データの価値

そこで、①から④まで、現状、データの流通の推移がどのようになっているのかを述べ、世界的にデータを流通させる環境が整っているかを確認する。① データ流通量については、JETRO が公表している図 1-1 によると、データ流通量が 2015 年から急速に伸びており、データが流通できる環境が整ってきていると読取れる（JETRO 2018）。

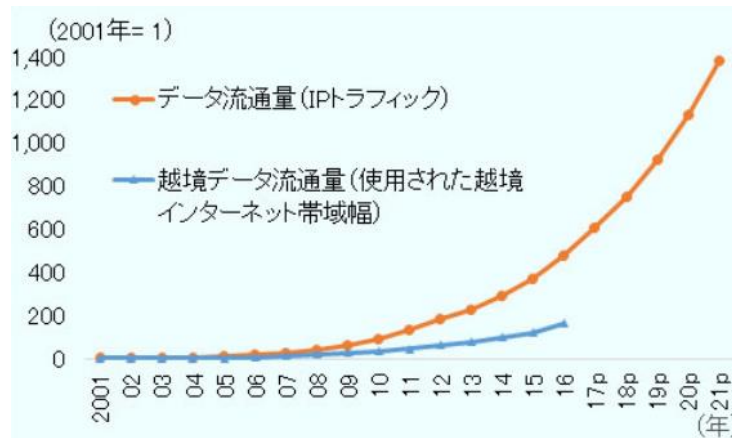


図 1-1 データの流通量 (JETRO 2018)

また、総務省が発表している固定通信および移動通信のトラフィックをまとめた図 1-2 によると、日本のデータ流通量が 2016 年を境に図 1-1 と同様、急速に伸びていることが読取れ、今後も増えていくことも予想できる (総務省 2020a: 2)。

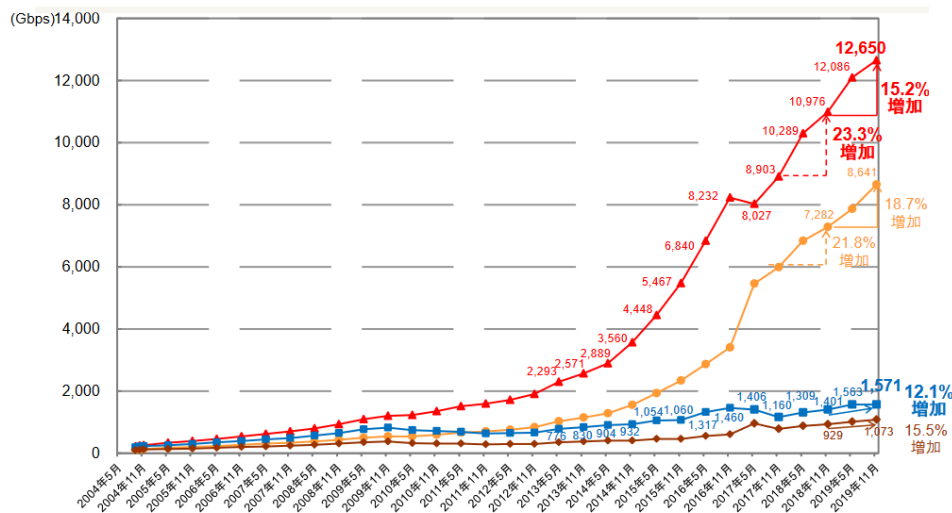


図 1-2 固定通信および移動通信のトラフィック (総務省 2020a: 2)

② データの速度については、FairInternetReport によると日本のデータはないものの、米国と欧州のデータの速度の推移は図 1-3 のとおり。伸び率は各国それぞれバラバラではあるものの減少している国はない。特にデンマークやスイスは 2019-2020 年の間に急速に伸びていることが分かる (FairInternetReport 2020)。

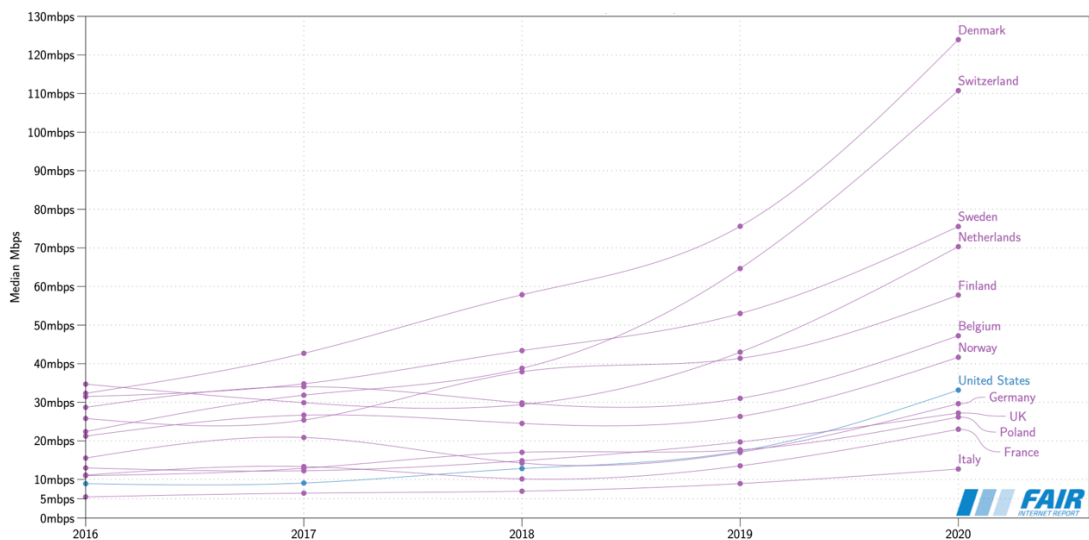


図 1-3 米国および欧州のデータ速度推移 (FairInternetReport 2020)

③ データの種別および④ データの価値については、本稿において別途提示するが、種別、価値共に増加、上昇傾向である。①から④の現状を踏まえて、データの流通するための環境は以前より格段に整っており、データの流通が今後も活発化していくことが予測できる。

1.1.2 データの特性

総務省によると、データの大きな特徴は、① デジタルのデータは非競合（第三者の消費量を減少させることなく、追加コストをかけずに利用者または全員が同じタイミングで活用できる）、② 複製のコストが不要のため、いくらデータを使用しても減少しない点である（総務省 2017a: 11-15）。

たとえば、①や②の特徴を活用した事例として、Web ページから自動でデータを集めるスクレイピングが挙げられる。総務省では、販売されているサービスおよび製品の価格変動の消費者物価指数（以下「CPI」という）を算出するにあたり、ターゲットとなるサービスまたは製品（計 585）、現地調査（約 28,000 事業所）、Web ページ、POS データを対象に価格情報を収集している。そのうち、ネット販売価格を算出するために Web スクレイピングの有用性を調査している。たとえば、2018 年 1-9 月搭乗分の国内の航空運賃調査については、Web スクレイピングを用いたことによる価格動向を適切に把握できたことにより、図 1-4 のように統計制度が向上した。人件費を減らすだけでなく、業務効率化も見込まれる旨の記載がある（総務省 2019: 8）。

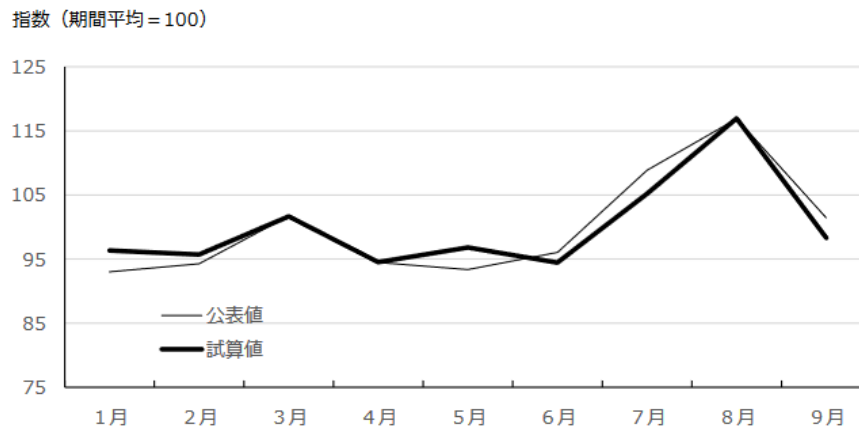


図 1-4 航空運賃の CPI および試算値の比較 (総務省 2019: 8)

一方で、2020 年、Social Data が Instagram から約 1 億件、TikTok から約 4 千万件、YouTube から約 4 百万件の個人情報を含むデータをスクレイピングし、データベース化して公開していたという問題で大きな話題になった (Asif 2020)。同様な事態を受けて、いくつかのサービス事業者は、利用規約などでスクレイピングを禁止しているものも多い。たとえば、Twitter サービス利用規約には、「本サービスへのクローリングは、robots.txt ファイルの定めによる場合は認められていますが、Twitter による事前の同意がないまま本サービスのスクレイピングをすることは明示的に禁止されています」(Twitter 2021: Twitter サービス利用規約 第 4 項 本サービスの利用) と明記されている。

なお、②の防止策として、技術としてはまだ課題が残っているものの、非代替性トークン (以下、「Non-Fungible Token」の頭文字をとって「NFT」という) 技術の登場により状況が一変する可能性がある。NFT は、元のデータにブロックチェーンを用いた所有権証明書を付ける技術である。データそのものの複製は可能ではあるが、本物である保証の代わりにになっている NFT 自体を複製することは不可能であり、元のデータの価値を上げる効果もある (Roberts 2021)。

上記より、データの特性としては、上記で取上げた①、②があり、どちらも有効活用をすれば、製品やサービスの向上につながるものの、②の特性を抑えるためのモデルや技術が生まれてきていることも事実である。

1.1.3 データの性質 (法律)

データの性質について、まず、法律上の規定から述べる。まず、民法第 85 条 (定義) にて、無体物のデータは該当せず、それに伴い、第 180 条 (占有権の

取得)にも該当しなくなる。さらに、第 180 条(占有権の取得)が該当しないことから、第 206 条(所有権の内容)および第 239 条(無主物の帰属)にも該当しないと読取れる。結果、データは、占有権、所有権の対象ではなく、当該権利の法的対象外であることが読取れるため、取扱いや条件に関してはデータの提供者と受領者間において契約など利用条件を定める必要があると考えられる(経済産業省 2019: 64-69)。そのため、データは従来の製品やサービスと同様なビジネスで提供することは、望ましくないと考えられる。

なお、上記にかかわらず、営業秘密や著作権を含む知的財産権などについては、条件によっては法的保護の対象となるため、データを取扱う際は戦略的に法的保護の対象とすべきか、または当事者間での利用条件の合意にとどめるのか、検討が必要である。営業秘密、知的財産権などは第 3 章以降にて扱う。

1.1.4 地方公共団体のデータ活用の取組み

現在、事業者間の取引だけでなく、地方公共団体においてもデータの活用促進活動が行われている。大きな動きとしては、2016 年 12 月 14 日付に官民データ活用推進基本法が公布・施行されたことである。特に当該法律の第 11 条(国及び地方公共団体等が保有する官民データの容易な利用等)の記載が、国および地方公共団体が保有するデータを活用できるよう工夫されている。なお、当該法律条項に基づき、2020 年度までに当該データの取組率を 100% 目指すことを 2017 年 5 月 30 日に閣議決定され、各地方公共団体は取組んでいるところである(内閣官房 2017a: 13)。本稿においては、内閣官房が提示している『オープンデータをはじめよう——地方公共団体のための最初の手引書』に従い、国および地方公共団体が保有するデータのうち、利用者が Web サービスなどを活用し、加工、編集おとび再配布などを許可して利用できる形に公開された以下の条件を満たすデータをオープンデータという(内閣官房 2017a: 15)。

- ① 営利目的、非営利目的を問わず二次利用可能なルールが適用されたもの
 - ② 機械判読に適したもの
 - ③ 無償で利用できるもの
- (内閣官房 2017a: 15)

上記のように地方公共団体において、オープンデータ化が行われているものの、コネクタデータが行った従業員数 300 人以下の企業の経営者や役員に対するオープンデータの利用調査より「政府や地方公共団体などが公表するオープ

ンデータを、自社の課題解決や新規企画のために活用したことがありますか？」という質問に対し、約 8 割が活用したことがないと回答している点（コネクタデータ 2021）から、環境が整備されつつあるものの、活用されるかは別の課題であることが分かる。

また、内閣府では、2030 年に向けてスーパーシティ構想を検討している。内閣府が公開している資料によると、このスーパーシティ構想のポイントは、「① 生活全般にまたがる複数分野の先端的サービスの提供」、「② 複数分野間でのデータ連携」、「③ 大胆な規制改革」（内閣府 2021: 3）としている。オープンデータを含めた分野を跨いだデータを活用して当該ポイントを達成するための様々な検討が行われている。

上記のとおり、データビジネスにおける課題があるものの、データの活用を促進している状況である。上記のデータの活用や先端サービスについて検討する際は、課題の整理をしたうえで、分野を跨いだ際の課題の検討など既存の分野を跨がないデータの活用では発生しえない課題の検討も必要である。

1.1.5 データ流通での課題

事業者間において、データの取引が活発化している一方で、データの活用促進を緩めてしまう要因がいくつかある。特に 1.1.3 項でも取上げたデータには所有権、占有権の概念がなく、法的保護が受けられないところから、各事業者の対応が異なっているところも活用促進を阻害している要因でもある。また、データを管理する際のセキュリティ、個人情報を扱った際のプライバシーが大きな要因であるとされている。これらを加え、データを公開することにより、競合他社に漏洩するリスクや開示してしまったデータをコントロールができないなど、製品、サービス提供とは異なるデータ特有の課題も存在している。たとえば、経済産業省では、データを活用したビジネスを展開する際の日本の強み・弱みを図 1-5 のとおり公開している（経済産業省 2016: 6）。

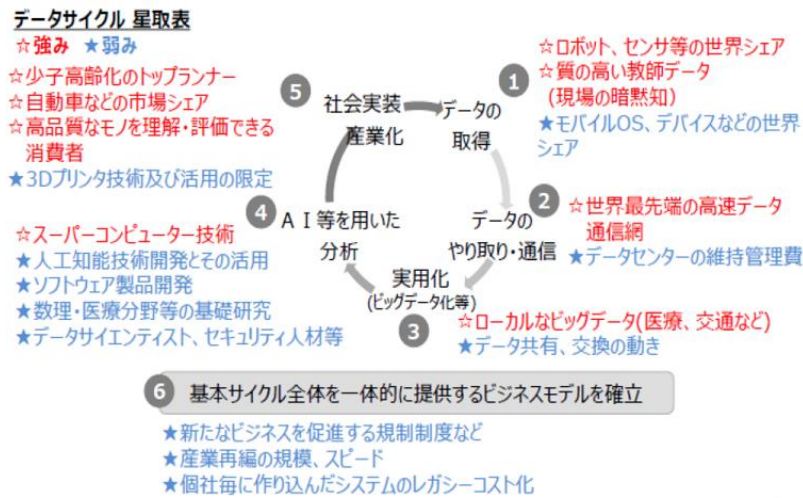


図 1-5 データを活用したビジネスの日本の強み・弱み (経済産業省 2016: 6)

図 1-5 では、強みと弱みが極端に偏っていることが読取れる点から、すでにデータの活用が行われている事例を使って、課題を洗出しが行われたものであると考える。加えて、各省庁では、データ活用に関して、課題があることを把握しているため、各省庁でデータを活用した課題の洗出しを行っている。しかし、公表されているもののまとまっていないのが現状である。

1.1.6 総括

これらの背景を踏まえ、本稿では、データのビジネスにおけるリスクマネジメントを検討するにあたり、データを活用したビジネスにおける課題を整理し、データの流れおよび課題を可視化するモデルを導き出す。また、オープンデータ等、種類が異なるデータや分野を跨いでデータを活用した際の課題の考え方や対応方法について明らかにすることで、データを利活用するための検討項目およびデータを流通させるための運用方法を提示したい。データを活用したビジネスに関する課題の検討方法を明示し、データのリスクマネジメントを検討するためのモデルを導き出す点に研究の意義を見出す。

1.2 調査の目的とリサーチ・クエスチョン

本稿では、特定の分野ではなく、様々な種類のデータを用いたサービスを対象とし、データを活用する際のリスクマネジメントの手法として、検討フレームを明示することを目的とする。

当該調査目的を達成するために、本調査では、メジャー・リサーチ・クエスチョン (以下「MRQ」という) とそれに連なるサブシディアリー・リサーチ

チ・クエスチョン（以下「SRQ」という）を次のとおりとする。

MRQ: データを活用したサービスを提供する際のリスクマネジメントはどのように行うべきか？

SRQ1: データビジネスにおけるデータの種類、データの流通方法、ビジネス形態はどのようになっているのか？

SRQ2: データを活用したビジネスにおける課題・リスクはどのようなものか？

SRQ3: データを活用したビジネスのリスクの検討モデルはどのようなものか？

これらの問いは、既に認識されているデータを活用したビジネスにおける課題・リスクを洗い出し、リスクマネジメントを行う際の指標や手順を明らかにすることが狙いである。現在、様々な省庁において、データを活用したビジネスにおける課題・リスクが提示されているため、それらを整理し、課題を検討するモデルを模索することを目的としている。現在、様々なデータを活用したサービスが存在しているものの、新規のデータを活用したサービスを検討する際に検討しなければ課題が分からず、ハレーションを起こしてうまくいかないことも多々ある。また、各省庁で提示されているデータを活用した課題・リスクについても、個々のユースケースごとに検討されているため、オープンデータやオープンデータ以外のデータ等、種類の異なるデータを扱うサービスを提供するためには何をもとに検討を行えばよいか分からず混沌としている状態である。そのため、上記の研究・クエスチョンを通じて、様々な種類のデータを活用する際に検討しなければならない課題・リスクについて形式化し、課題に対しては影響を最小限にする手法の提案を行う。

本調査は、様々なデータを活用する際の検討しなければならない課題・リスクを可視化できるモデル提示とその課題を明らかにすることに学術的意義がある。また、地方公共団体が所有しているデータを活用したサービスが政策などにより増加することは必然であり、現在、各省庁で取上げられている課題を明確にし、当該課題を現段階から検討できることに実務的意義がある。

1.3 調査の方法

本調査の手順は、図 1-6 のとおりである。本調査の対象は、データを活用したサービスサービス（地方公共団体、事業者等に限らない）である。本稿では、まず、データの種類を調査し、データを活用する際の課題を整理し、リスクモデルを作成し、実際に検討されているデータを活用したビジネスモデルに当該

リスクモデルに当てはめ、データを活用するサービスを提供する際の検討項目の提示を行う。

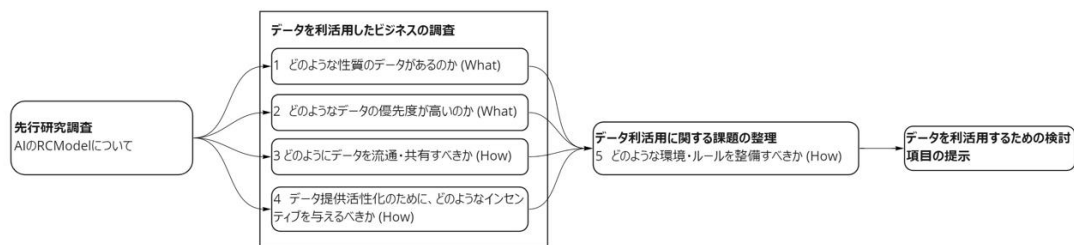


図 1-6 調査の方法

1.4 用語の定義

本稿で使用する用語の定義について、表 1-1 のとおりである。

表 1-1 用語の定義

用語	定義
地方公共団体	地方政府、地方自治体を指す。
利用規約	利用約款、定型約款を指す。事業者と大量の利用者間で一律の条件で適用する契約。
AI	Artificial Intelligence の略。
PoC	Proof of Concept の略。実際の事業で実現できるか、その効果はどれほどのものか検証する行為。
PDS	Personal Data Store の略。個人のデータ提供者が自らの意思でデータの蓄積や管理を行うための仕組み。なお、PDS には、第三者へ提供する際の制御機能がある。
データマーケットプレイス	データ取引市場。データ提供者と当該データの活用を希望するデータ利用者のマッチングの仲介を行う役割を持ち、売買などによる取引を代理で行う仕組み。
イニシャル・ロイヤリティ	ライセンス契約の締結時に一時金として支払うロイヤリティ。基本ライセンス料。
ランニング・ロイヤリティ	売上げや販売量など一定期間の結果に応じて一定率を支払うロイヤリティ。
HIPAA	Health Insurance Portability and Accountability Act; 医療保険の相互運用性と説明責任に関する法律の略。1996年に制定（数回改正）。データのプライバシーやセキュリティの条件を定めることを目的とした電子化した医療情報のプライバシーおよびセキュリティに関する米国の法律（Digital Transformation Channel 2020）。
PHI	Protected Health Information; 保護対象保健情報の略。HIPAAにおいて、定められている個人を特定できる保健情報（Digital Transformation Channel 2020）。
HITECH	Health Information Technology for Economic and Clinical Health Act; 経済的および臨床的健全性のための医療情報技術に関する法律の略。HIPAAを拡張したもので、違反者に対する罰則を厳しくする定めが含まれている（Digital Transformation Channel 2020）。
EHR	Electronic Health Record; 電子健康記録の略。デジタル版の個人医療データを指す。米国の場合、認可を得た複数の医療機関がデータを収集、管理し、医療機関の間でデータを交換することができる（Digital Transformation Channel 2020）。
偽情報	フェイクニュースとして扱われているが、流通させる目的や当該情報に含まれる誤りの程度が異なるため、本稿では、諸外国の政策文書で用いられている disinformation および misinformation を総称して偽情報という（総務省 d 2020）。
GDPR	General Data Protection Regulation; 一般データ保護規則の略。欧州連合（EUという）での「個人情報（データ）の保護という基本的人権の確保を目的とした」法律。EUを含む欧州経済領域（EEA）域内で取得したパーソナルデータを「EEA域外に移転することを原則禁止」としているもの。「行政罰規定があり、違反行為に対しては、高額な制裁金が課されるリスク」（JETRO 2021）がある。
CLOUD Act	Clarifying Lawful Overseas Use of Data Act; 海外データ合法的使用明確化法の略。米国にて、2018年3月23日に成立した「民間企業が保持する電子通信データへの国境を越えたアクセスを簡易化することを目的とした法律」（原田 2019）を指す。

1.5 本稿の構成

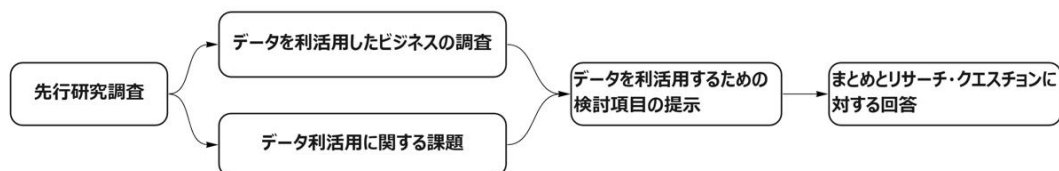


図 1-7 本稿の構成

本稿の構成は図 1-7 のとおり。はじめに、第 2 章では、先行研究を取上げる。当該先行研究では、AI を扱う際のリスクの検討モデル: RCModel を取り上げる。次に第 3 章では本研究で対象とするデータを利活用したビジネスの形態を調査するため、データビジネスに関する事例調査を行う。第 4 章では各省庁が行っているデータ利活用に関する課題について整理を行い、それらの考察についても言及する。第 5 章では、第 3 章および第 4 章で調査した結果を用いて実際に想定されているビジネスから課題を洗い出す。最後に第 6 章では、本調査のまとめ、MRQ ならびに SRQ に対する解答、実務的含意および本調査の再検討の課題について述べる。

第2章 先行研究

1.1.1 項で取上げたとおり、データの流通量が盛んになっているところから、データを活用した AI の技術も現在、注目されている。1.1.6 項で取上げたデータを活用する際に発生する課題があるように AI を活用した際にも課題が発生している。たとえば、2020 年にマサチューセッツ工科大学が約 800 億枚の画像を使用してデータセットを作成して公開していた Tiny Images が、差別的に篩い分けされ差別を助長していたとして削除した事例 (Torralba 2020) や人種差別などの懸念から IBM が顔認証を活用した技術の市場から撤退した事例 (Hirsch 2020) など、AI を活用した事業そのものを撤退する事例も発生している。

上記の背景から、AI のガバナンスを検討する必要がある、東京大学未来ビジョン研究センターおよびデロイト トーマツ リスクサービス株式会社にて AI ガバナンスに関する共同研究が行われている。当該共同研究では、東京大学が開発したリスクチェーンモデル (以下「RCModel」という) を用いて実際のケース事例と照らし合わせ、アップデートを行っている (Deloitte 2020)。なお、デロイト側もリスクに関するノウハウはかなり蓄積されており、代表例として図 2-1 のリスク インテリジェンス マップなどがあげられ (Deloitte 2017: 2)、当該マップを活用して検討もされていると推測される。

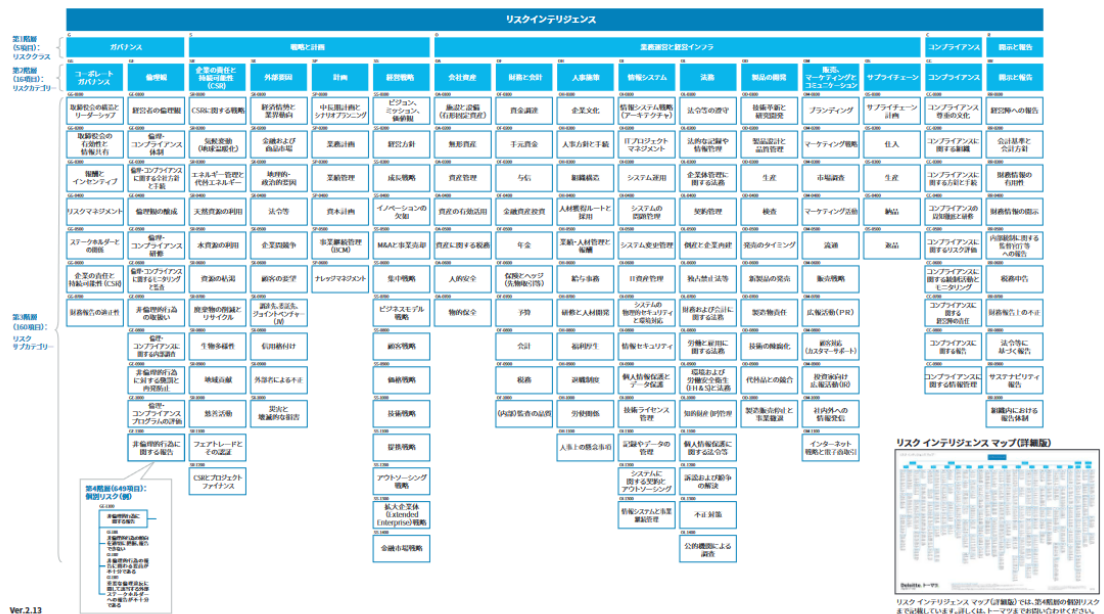


図 2-1 リスクインテリジェンスマップ (Deloitte 2017: 2)

そこで、本章では、以下についての先行研究のレビューを行う。

- ① Risk Chain Model: RCModel (2020) (2.1 節)
- ② Risk Chain Model: RCModel (2021) (2.2 節)
- ③ リスクチェーンモデル (RCModel) ガイド ver 1.0 (2021) (2.3 節)

先行研究のレビューを行った結果、データを活用したビジネスに対しても応用できるかを検討する。

2.1 Risk Chain Model: RCModel (2020)

本節では、2020年に行われたRCModelの検討方法に関する先行研究を中心に記載する。

2.1.1 背景

AIを活用したサービスの社会実装において、大きな問題となっているのが、不公平な判断による差別、制御不能による事故などであり、ここからAIの信頼性が損なわれているのが現状である。また、AIを活用したサービスの提供者は、当該サービスの利用者による故意の利用によって生じるAIの性能悪化およびAIの知識が乏しい利用者の誤用によって生じるAIの性能劣化に対するリスクにも対策を行う必要が出てきている。このような現状から、産学官民連携で、AIを活用したサービスを提供する際に、開発段階から検討を行わなければならない課題および論点に関して整理が行われているため、本論文において、当該課題および論点をどのケースにおいても検討しなければならない課題を可視化できるよう整理されている(松本・江間 2020: 3)。

2.1.2 RCModelの活用方法

本項では、RCModelの活用方法を取上げる。たとえば、「採用AIで想定されるリスクシナリオ」を検討する場合、まず、その際に発生する可能性があるリスクシナリオを洗い出し、①「AIシステム(技術)」、②「AIサービスのプロバイダ(運用)」および③「ユーザー」それぞれに要因別に把握できるよう分類して検討する(松本・江間 2020: 14)。そこから、本論文では、産学官民などで検討された「採用AIで想定されるリスクシナリオ」をいくつか抽出し検討を行い、当該抽出したシナリオを「予防：リスクを予防できない要因」、「発見：リスクの実現を発見できない要因」、「対応：リスクを発見しても適切に対応できない要因」(松本・江間 2020: 12)に表 2-1 のように分類する。

表 2-1 リスク要因と構成要素（松本・江間 2020: 12）

予防	発見	対応
<ul style="list-style-type: none"> ■ 【AI システム】データのバイアスによって公平な判断が行われない（Data Balance） ■ 【AI システム】アルゴリズムの汎化性能が損なわれ公平な判断が行われない（Generalization） 	<ul style="list-style-type: none"> ■ 【AI システム】AI の判断根拠が分からない（Interpretability） ■ 【AI システム】AI の判断結果を検証できない（Traceability） ■ 【サービス提供者】公平な判断を行う上での留意点が明確になっておらず、判断尺度が人によって大きく異なる（Fairness） ■ 【サービス提供者】特定のグループにネガティブな判断をする傾向がある場合にその情報を可視化できない（Transparency） ■ 【サービス提供者】ユーザ側での留意点について認識合わせを行わず、ユーザ側で公平な判断が行われない（Consensus） 	<ul style="list-style-type: none"> ■ 【ユーザー】AI の判断へ過度に依存することで公平な判断が行われない（Human Autonomy） ■ 【ユーザー】特定のグループに対してネガティブな判断をすることを認識していなければ公平な判断が行われない（Expectation） ■ 【ユーザー】意思決定プロセスが不明確なことで差別的な判断が補正されない（Controllability） ■ 【ユーザー】最終判断の場において公平な選考が行われない（Proper-Use）

上記を RCMModel に当てはめ、表 2-1 で取上げた「予防」→「発見」→「対応」のとおりリスクの要因が顕在化する点を検討しながら線を引くと次のとおりになる。なお、本論文上では、線は単線が必須である旨の記載はない（松本・江間 2020: 14）。

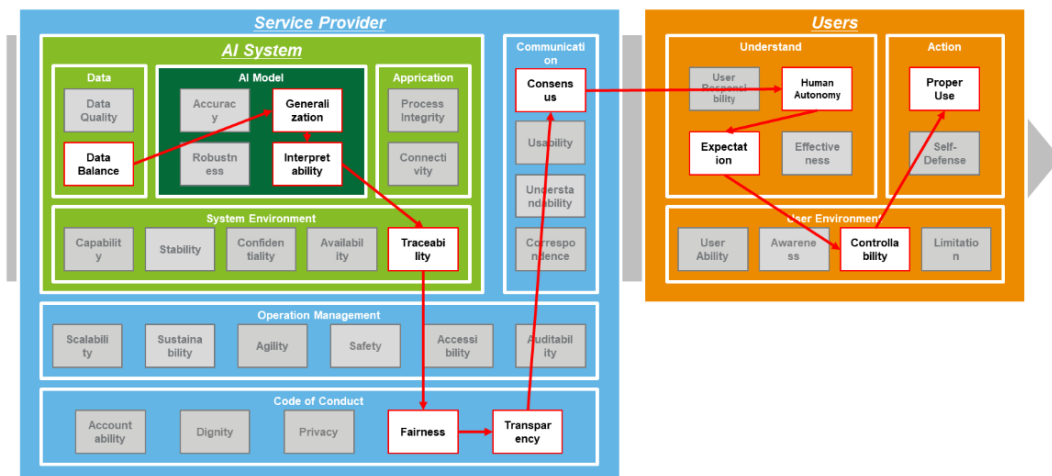


図 2-2 RCMModel の事例（松本・江間 2020: 14）

上記から RCMModel では、課題を検討する順番などを含め、可視化することができる。

2.1.3 RCMODEL を用いた対策検討

リスクを可視化しただけでは、リスクに対する課題の解決は不可能である。そこで、2.1.2 項で取上げた①～③の層ごとに構成要素を割り当てて、コントロール (=対応策) を示したのが表 2-2 のとおりである。なお、表 2-3 は、表 2-2 の構成要素を示したものである (松本・江間 2020: 15, 19-20)。

表 2-2 リスクシナリオでの構成要素ごとのコントロールの例 (松本・江間 2020: 15)

層	構成要素	コントロール
AIシステム	データの偏り(Data Balance)	学習データが特定の層 (性別等) に偏らないようにデータの割合 (男女比等) を整える
	汎化性(Generalization)	モデルの説明変数から不公平な判断につながるような特徴量 (性別, 国籍等) を除く
	解釈可能性 (Interpretability)	モデルの判断根拠(特徴量の重要度等)の情報を出力できるようにする
	検証可能性 (Traceability)	モデル学習時の公平性に係る情報 (属性別の判断結果の比較等) を保存する
AIサービスのプロバイダ	公平性(Fairness)	利活用時の判断根拠に係る情報 (判断結果に強く影響した特徴量等を保存する応募者に係る公平性の留意点 (性別, 国籍等) を整理し, 関与者に周知する
	透明性(Transparency)	特定のグループにネガティブな判断をする傾向を除けない等, ユーザ (人材採用担当者等) が留意すべき情報を開示する
	合意(Consensus)	AI サービスの予測精度・留意事項 (特定のグループにネガティブな判断をする等) ・ユーザの責任 (最終判断等) について, ユーザと合意する
ユーザ	人間の自律性 (Human Autonomy)	AI サービス側から提供される留意事項を踏まえ, 過度に AI に依存しないように判断する
	影響 (Effectiveness)	予測精度及び利用者側の留意事項を確認する
	制御可能性(Controllability)	どのユーザに合否の最終判断の権限があるかを明確にする 最終判断時の判断材料として, AI による判断の採用 / 不採用を整理する
	適正利用 (Proper Use)	特定のグループを差別するような判断となっていないか必要な確認を行い, 合否を最終判断する

表 2-3 構成要素の定義（松本・江間 2020: 19-20）

領域		構成要素	内容
AIシステム	AI Model	Accuracy	予測性能
		Generalization	汎化性能（アルゴリズムのバイアス）
		Robustness	頑健性（ノイズへの耐性）
		Interpretability	モデルの解釈可能性
	Data	Data Quality	データの品質、完全性、鮮度
		Data Balance	データの偏り（データバイアス）
	Application	Process Integrity	自動処理の正確性
		Connectivity	外部システムとのプロトコル
	System Environment	Capability	処理パフォーマンス、システムの拡張性
		Stability	安定稼働、誤り補正、反復性
		Confidentiality	機密性
		Availability	可用性
		Traceability	検証可能性、誤り検知
		Accountability	サービスに係る答責性
AIサービスのプロバイダ	Code of Conduct	Dignity	利用者の判断・権利の尊重
		Privacy	プライバシーの保護
		Fairness	公平性
		Transparency	透明性、情報の可視化
		Operation Scalability	変化に対する組織の柔軟性
		Sustainability	持続可能性、サービス品質の維持
		Agility	迅速な開発プロセス・インシデント対応
		Safety	安全性、エラーへの対応
		Accessibility	アクセスコントロール、権限管理
		Auditability	監査可能性
	Communication	Consensus	利用者との合意（目的、役割分担等）、委託先との権利関係
		Usability	使い易さ、人間系への切替、インタラクション
		Understandability	理解可能性、適切な表現（利用者の意思決定を誘導しない）
		Correspondence	利用者・関係者との連携
ユーザ	Understand	User Responsibility	利用者の責任
		Expectation	サービスの期待値、提供範囲
		Human Autonomy	意思決定の自由度
	Action	Effectiveness	サービスに係るリスク
		Proper Use	適切な利用（悪用しないこと）
	User Environment	Self-Defense	自己防衛
		User Ability	リテラシー、経験、スキル
		Awareness	AIの存在の認識
		Controllability	支配可能性、行動の選択肢
		Limitation	技術的・法的な制約

2.2 Risk Chain Model: RCMModel（2021）

本節では、2021年に行われたRCModelの検討方法に関する先行研究を中心に記載する。

2.2.1 アップデートの背景

2020年に検討されたRCModelでは、すでに検討されていた課題やリスクを抽出したうえで、実際に発生したAIを活用したサービスの事故を事例として検討を行っていた。しかし、この従来の検討方法は、当該検討を行う人の裁量によって大きく結果が異なるうえ、対応策を講じるかの優先度を付けるのが困難であった。そのため、2021年のRCModelの検討では、AIを活用したサービスに対して「実現すべき価値・目的」を設定し、以下の情報を収集し、再検討が行われた（松本・江間 2021: 1-2）。

- ・ AIを活用したサービスの利用目的/利用シーン
- ・ システム概要図
- ・ 使用するアルゴリズム/データ
- ・ AIを活用したサービスからの出力内容など
- ・ 利用者との役割分担
- ・ 開発方法や学習頻度など

2.2.2 改良版RCModelの活用方法

本項では、改良版RCModelの活用方法を取上げる。本論文にて取上げられている事例は「製造ラインの自動最適化（生産自動化）」である。「製造ラインの自動最適化（生産自動化）」の「実現すべき価値・目的」は、本論文上では、「検品品質の維持」、「検品高速化による製造量の増加」、「検品に掛かる人件費の軽減」、「企業の社会的責任」（松本・江間 2021: 2-3）で設定されている。まず、2.1.2項と同様、まず、当該事例において目的に従って優先度を付けて検討できるリスクシナリオについて表2-4のとおり、列挙する。

表 2-4 リスクシナリオ事例 (松本・江間 2021: 3)

順	実施者	コントロール	実現方法
1	サービスプロバイダ (品質管理部門責任者)	適切な検出性能の検討 (Accountability)	外観検査において実現すべき正解率の設定
2	サービスプロバイダ (AIサービス管理者)	費用対効果を踏まえたモデル性能の見直し (Sustainability)	許容する偽陰性(False-Negative)の検討
3	AIシステム (AIモデル開発者)	AIモデルの予測性能 (Accuracy)	予測性能の可視化
4	AIシステム (AIモデル開発者)	AIモデルの判断根拠の出力 (Interpretability)	判断根拠情報の可視化(XAI)
5	AIシステム (システムエンジニア)	過剰検出時のアラーム (Process Integrity)	自動アラート処理の構築
6	AIシステム (システムエンジニア)	検証可能性 (Traceability)	システムログ (画像と判断結果) の保存
7	サービスプロバイダ (AIサービス管理チーム)	モデル性能のモニタリング (Auditability)	画像の検証過検出の原因の検証
8	サービスプロバイダ (AIサービス管理者)	再学習要否の合意 (Consensus)	ユーザとの協議
9	ユーザ (工場の生産ライン責任者)	期待される検出性能の理解 (Expectation)	適切な性能の理解
10	サービスプロバイダ (AIサービス管理者)	モデルの再学習を依頼 (Agility)	際業手のプロセス・開発環境

次に RCMoel 上で線を表 2-4 で定めた順番に線を引いていくと図 2-3 のとおり。

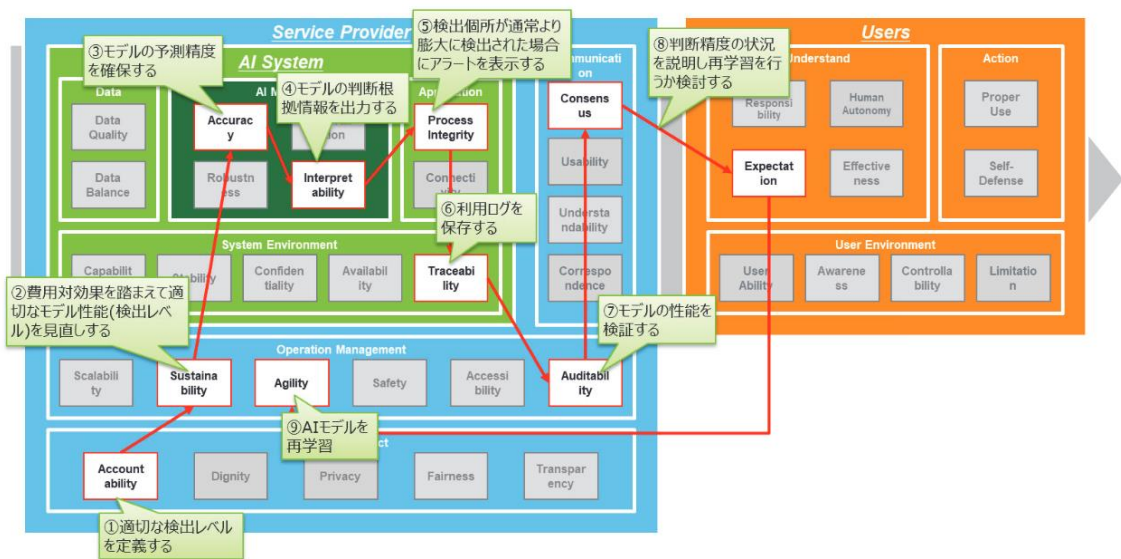


図 2-3 改良版 RCMoel の事例 (松本・江間 2021: 2)

上記より、従来版の RCMoel よりシンプルにはならないが、優先度が目的に定めているため、指標者によって変更する確率は少なくなると考えられる。

2.3 RCMoel ガイド

本節では、2021 年に東京大学から発表された『リスクチェーンモデル (RCMoel) ガイド ver 1.0 (2021)』(以下、「RCMoel ガイド」という) につい

て記載する。

2.3.1 ケーススタディ

RCModel ガイドでは、2.1.2 項で取上げた「採用 AI で想定されるリスクシナリオ」が紹介されている。まず、実現すべき価値・目的の優先順位を付けて検討を行ったうえで、当該価値・目的に対してサービス要件と関連テクノロジーを紐づける（表 2-5）。その後、各それぞれのリスクシナリオを検討し、RCModel にて線を引く（図 2-4）（東京大学 2021: 4-5）。

表 2-5 採用 AI で想定されるリスクシナリオ（東京大学 2021: 4）

実現すべき価値・目的	サービス要件と関連テクノロジー		リスクNo.	リスクシナリオ	
1 人材採用レベルの維持・向上	1-1 予測性能の維持	<ul style="list-style-type: none"> ■ AIの予測精度 ■ AIの頑健性 ■ AIの説明可能性 	R001	適切な評価	採用する職種等により、適切な期待値を設定しなければAIの貢献を正しく評価できない
			R002	予測性能の維持	AIの予測性能が劣化したことで採用レベルが低下する
			R003	ノイズによる影響	エントリーシートで使用される文字情報が若干異なるだけで(句読点の違い等)、AIの判断結果が大きく変化する
			R004	虚偽の申込	申込内容に虚偽が含まれているが、合格と判断してしまう
	1-2 AIサービスと利用者の連携	<ul style="list-style-type: none"> ■ AI依存 ■ AIへのフィードバック 	R005	過度なAI依存	人材採用担当者がAIの判断に依存しすぎることで、AIの判断誤りに気が付かない
			R006	誤ったフィードバック	人材採用担当者によるAIへのフィードバック(合否のラベル設定)が不正確なことでAIの性能が劣化する
	1-3 ビジネス環境変化への対応	<ul style="list-style-type: none"> ■ データ分布の変化 	R007	人材トレンドの変化	求める人材トレンドの変化にAIの予測傾向が対応できず、採用レベルが低下する
			R008	新たな職種	新たな職種・人材を求める際にAIモデルの予測が妥当でない可能性がある
2 採用活動に係るコストの削減	2-1 適切なサービスコスト	—	R009	コスト超過	サービス維持コストが超過する
3 海外グループを含めたサービス提供	3-1 サービスのローカライズ	<ul style="list-style-type: none"> ■ AIの学習 ■ 個別モデル開発 	R010	地域の会社への対応	地域の会社ごとに採用方針や申込者の傾向が異なることで、会社によって採用レベルが確保できなくなる
	3-2 広範囲な開発・サポート体制	<ul style="list-style-type: none"> ■ 開発体制 	R011	不十分な開発スピード	十分な開発体制が確保されていないことで、モデルの精度が劣化した際に再学習などの対応が行われない
4 企業の社会的責任(公平性のある採用活動)	4-1 倫理・コンプライアンス遵守	<ul style="list-style-type: none"> ■ AIの判断根拠 ■ AIの汎化性 	R012	判断根拠情報の不正販売	AIサービスを何度も利用することで高確率で合格判断を行うキーフレーズ等を特定し、社外へ不正販売する
			R013	公平性	特定の国/地域/人種/性別/年齢に対して不公平な予測結果を生じさせる
	4-2 情報管理	<ul style="list-style-type: none"> ■ データ管理 	R014	予測結果の目的外利用	AIの判断結果情報が別の目的に使用されることで、特定の人間に不利益を生じさせる
			R015	風評被害	AIの予測結果情報が外部に流出することで特定の人物に対して風評被害が発生する
			R016	プライバシー保護	AIシステムに蓄積された個人情報が流出する

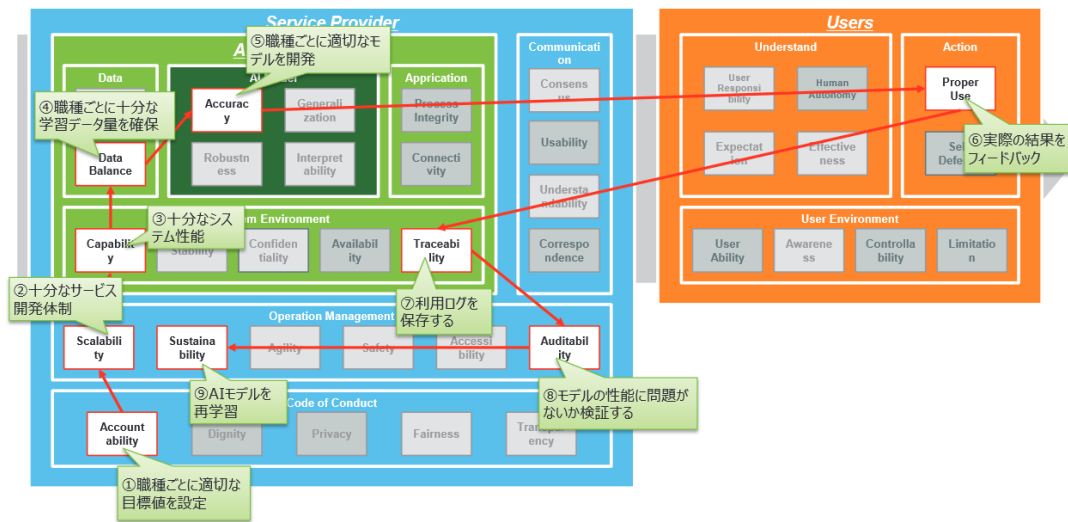


図 2-4 RCMModel (東京大学 2021: 5)

上記から、価値・目的を定めることによって図 2-2 と異なる線が描けることが分かる。上記から対応策を検討するにあたり、それぞれの役割別に構成要素別に分類することで表 2-6 のとおりリスクに対する対応の優先順位等が明確になる。なお、法制度や社会通念上により、リスクシナリオが変化する可能性があるるので適宜見直しが必要である (東京大学 2021:6)。

表 2-6 対応策の検討 (東京大学 2021: 6)

コントロールの内容		
AIシステム (A社AI開発部門)	サービスプロバイダ (A社人材採用部門)	ユーザー (A社グループ人材採用担当者)
③【Capability】複数のモデルを実行できるシステム環境を用意する (A社情報システム部門)	①【Accountability】職種ごとに適切な目標値を設定する (A社人材採用部門/A社グループ人材採用部門)	⑥【Proper Use】実際の合否結果をフィードバック (A社グループ人材採用担当者)
④【Data Balance】職種ごとに十分な学習データを確保する (A社AI開発部門)	②【Scalability】複数のモデルをサービス提供できる体制を確保する (A社人材採用部門)	
⑤【Accuracy】職種ごとに適切な予測精度を持つモデルを開発する (A社AI開発部門)	⑧【Auditability】各モデルの性能を定期的に検証する (A社人材採用部門/A社グループ人材採用部門)	
⑦【Traceability】利用時のログ情報を保存 (A社情報システム部門)	⑨【Sustainability】必要な精度を確保するためにAIモデルの再学習を依頼する (A社人材採用部門)	

2.3.2 RCMModel の構成要素

RCModel ガイドで定義されている構成要素と各役割別の構成要素は、図 2-5、表 2-7、表 2-8、表 2-9 のとおりである。

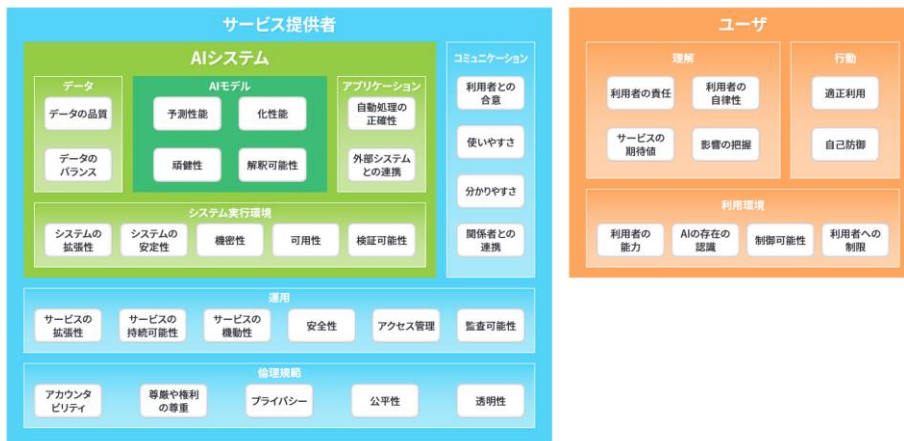


図 2-5 リスク要因の関係性（東京大学 2021: 別紙）

表 2-7 AI を活用したシステムの構成要素（東京大学 2021: 別紙）

構成要素	内容	主なコントロールの例
AIモデル		
予測性能	十分な予測性能	予測性能の検証
汎化性能	特定の事例に偏ることが少ない判断	汎化性能の検証
頑健性	ノイズ等への耐性	敵対的事例の学習
解釈可能性	モデルの判断根拠	判断根拠情報の出力
データ		
データの品質	データの品質確保	教師ラベルづけの検証 ノイズの補正 特別データの分類(戦略商品等)
データのバランス	データの分布	十分な学習データの確保 データバイアスの検証
アプリケーション		
自動処理の正確性	補助的な自動処理	異常値の補正 異常判断(過検出等)のアラート
外部システムとの連携	外部システム等との連携	データの自動連携 プロトコルの定義・実装
システム実行環境		
システムの拡張性	利用環境の増加等へ対応できるシステム環境	複数モデルを実装する環境
システムの安定性	安定稼働するシステム環境	十分なパフォーマンスの確保 IoTのメンテナンス
機密性	機能や情報が保護されたシステム環境	システムの保護 アクセスコントロールの実装
可用性	必要な時に使用できるシステム環境	システム稼働時間の確保 異常時の代替機能への切替
検証可能性	AIサービスを事後検証できるための性質	実行履歴や判断根拠の保存 開発時の学習結果の記録

表 2-8 サービスの提供者の構成要素（東京大学 2021: 別紙）

構成要素	内容	主なコントロールの例
倫理規範		
アカウントビリティ	説明責任、利用者の保護	責任関係の明確化 適切な期待値の検討
尊厳や権利の尊重	利用者側の優先権の検討	人間の介在度合の定義
公平性	サービス全体での公平性	公平性を確保する項目の定義
プライバシー	個人情報の適切な管理	プライバシーポリシーの遵守
透明性	AIサービスに係る必要な情報の開示	ステークホルダーごとに開示すべき情報の整理
運用		
サービスの拡張性	利用環境の増加等へ対応できるサービス体制	サービス提供に十分な体制 必要な言語へのサポート
サービスの持続可能性	持続的なサービスの維持	サービス要件の見直し 再学習・継続学習
サービスの機動性	適時の対応	アジャイル開発の実施
安全性	サービス全体での安全性の確保	システム外の安全対策 利用者の不正利用への対処
アクセス管理	適切なシステムの 利用権限・範囲の管理	適切なアクセス権限の設定 不正な利用者の制限
監査可能性	第三者を含む必要な監視	AIシステムのモニタリング トラブル発生時の検証 不正利用の監視
コミュニケーション		
利用者との合意	利用者との認識合わせ	利用者責任の合意 AIシステムの変更への合意
使いやすさ	AIサービスの使いやすさ	使いやすいUI
分かりやすさ	AIサービスが出力する情報の 分かりやすさ	判断根拠の分かりやすい表現
関係者との連携	利用者に対するリモートでのサポート	利用者のリモート支援 専門家との連携

表 2-9 ユーザの構成要素（東京大学 2021: 別紙）

構成要素	内容	主なコントロールの例
理解		
利用者の責任	利用者責任の理解	利用者責任の合意(最終判断等) AIシステムの変更への合意
利用者の自律性	自律的に判断すべき内容の理解	AIの判断の訂正
サービスの期待値	AIサービスに対する期待精度の理解	期待値(予測精度等)の理解 ネガティブな判断傾向の理解
影響の把握	利用者への影響の把握	AIサービスに係るリスクの理解 ワークスタイルの変化の理解
利用環境		
利用者の能力	サービス利用において 必要な知識・スキルの習得	必要なリテラシーの確保 利用者の教育
AIの存在の認識	AIの存在の認識	AIの存在の明示 利用者への通知
制御可能性	利用者側での制御	マニュアル手続の整備 AI判断の訂正機能
利用者への制限	不正利用等の防止に向けた 利用者の制限	利用者への技術的な制限 法的な制約
行動		
適正利用	正しいサービス利用	適切な目的に沿うサービス利用 教師ラベルの正しい設定
自己防御	利用者自身の保護	不利益が発生した際のクレーム 環境変化に係る事前連携

2.4 先行研究のまとめと本調査の位置付け

先行研究では、AIを活用したサービスの観点での課題やリスクを洗い出し、リスクに対する対応策の可視化するモデルを提示している。RCModel 以外にも、AIを活用したサービスの観点で課題の抽出および対応策の検討をしているものもある（内平ほか 2020）。ただし、データを活用する AI 技術ではあるものの、データの取引を対象にした観点での課題やリスクに対する対応策を可視化する手順のモデルは提示されていない。また、データそのものを活用したサービスの観点ではリスクの検討に関するモデルを論じている論文は管見の限り見当たらない。本調査では、データを活用したビジネスにおいて、データの流れから課題を検討することを目的としている。また、データには様々な種類があり、ユースケースごとに課題が大きく異なり、それぞれのユースケースで検討できるよう課題を可視化する方法を明示することが本調査では重要となる。

上記から、データそのものを活用したサービスを取扱い、リスクの検討に関するモデルを検討することに研究意義があると考えられる。なお、データの取引を対象にした観点での課題やリスクに対する対応策のモデルを検討するにあたり、データの流通に関しても可視化できる既存の RCModel を活用する。

RCModelの活用方法は、AIを活用したサービスを、データを活用したサービスの観点に置き換え、不足している検討項目については追加を行い、AI特有のリスク観点のものは削除し、整理するものとする。

第3章 データの活用におけるビジネス形態

本章では、データを扱った取引について、データの性質やビジネス形態について述べる。

データ取引においては、サービス・製品とは異なり、ビジネス形態によっては、無償の取引が多い場合もある。また、データの種類は様々であり、個人情報や秘密情報を含むデータは一般的な管理を行っているデータとは異なる運用で管理しなければならないなど制約も多い。また、事業者内で秘匿することによって価値が上がるデータがある一方で分野を跨いでデータを連携し、サービスを提供することで価値が上がるデータなど様々な形式のデータがある。

そのため、本稿においてデータを活用したビジネスにおけるリスクや課題を検討するにあたり、データの種類やデータのビジネス形態を検討する。データを活用したビジネスにおける共通のリスクや課題を検討するにあたり、当該ビジネスの競争領域、共創・協調領域の明確化を行う。なお、競争領域に関しては、それぞれの事業の事例から検討する必要があるうえ、オープンデータの活用と目的が異なるため、本稿の対象外とする。

経済産業省によると、データに関する競争領域、共創・協調領域の明確化する方法として、次の検討を行う必要があると記載されている（経済産業省2015a: 5）。

- 1 どのような性質のデータがあるのか（What）
- 2 どのようなデータの優先度が高いのか（What）
- 3 どのようにデータを流通・共有すべきか（How）
- 4 データ提供活性化のために、どのようなインセンティブを与えるべきか（How）
- 5 どのような環境・ルールを整備すべきか（How）

上記を整理することにより、データを活用したビジネスにおいて、共創・協調領域がはっきりすると記載がある。そのため、本章では、上記の1から5を踏まえて、①から④の節にて述べる。なお、オープンデータに関しては、データの性質が異なるため、別の節を設定して検討する。

- 1 どのような性質のデータがあるのか（What）
 - ① データの種類（3.1 節）
- 2 どのようなデータの優先度が高いのか（What）
 - ② データの活用状況（3.2 節）

- 3 どのようにデータを流通・共有すべきか (How)
 - ③ データの流通および共有方法 (3.3 節)
- 4 データ提供活性化のために、どのようなインセンティブを与えるべきか (How)
 - ④ インセンティブ (3.4 節)
- 5 どのような環境・ルールを整備すべきか (How)
次章以降

3.1 データの種類

データには、種類や性質が多くある。そのため、様々な分野において、分類されている事項をいくつか取上げ、整理を行う。今回取上げる観点は次の 1 から 5 のとおりである。

- 1 データビジネスの観点
- 2 法律の観点
- 3 法律実務の観点
- 4 営利・非営利の観点
- 5 情報取得の観点

上記を取上げたうえで、1.2 節で設定したリサーチ・クエスチョンに対する解答を行うために今回対象とするデータの種類を設定する。データの種類を設定するにあたり、詳細なデータに関する情報が必要なものについては追加で調査を行う。

3.1.1 データビジネスの観点

総務省では、次の 1 から 4 のとおりデータの分類が行われている（総務省 2017b: 53-54）。

- 1 「オープンデータ」
 - 1.1.4 項記載のオープンデータ。
- 2 「暗黙知（ノウハウ）をデジタル化・構造化したデータ」
事業会社や産業が所有しているパーソナルデータ以外のデータ（データとして蓄積されたノウハウを含む）。
- 3 「M2M（Machine to Machine）から吐き出されるストリーミングデータ」
センサなどの機器から収集されるデータ。

4 「個人の属性に係るパーソナルデータ」

パーソナルデータには、個人情報の保護に関する法律 第 2 条（定義）第 1 項に該当する情報に限らず、個人の属性情報、センサなどから収集された生体情報および個人情報を含む。詳細は 3.1.1.1 目のとおり。

3.1.1.1 パーソナルデータ

法律上「パーソナルデータ」という定義は存在しない。個人情報の該当要件は、個人情報の保護に関する法律 第 2 条（定義）第 1 項のとおりであるが、同条第 2 項の記載のとおり、単体のデータでは個人が特定できなくとも、複数のデータを扱うことで個人を特定できれば個人情報に該当するため、購買履歴やウェアラブル機器などでの収集された情報も含む（経済産業省 2019: 14-20）。

なお、利用者がサービスを利用する際にパーソナルデータがどのように使われているか透明性を確保して欲しいという声が上がっている。そのため、Apple および Google はこの声に対する対策を行っている。Apple では、開発者がアプリのアップロードを行う際は、どのようなデータ収集を行うかなど、データの収集の種類、利用目的を明示する必要がある（Apple 2021）。Google も同様、開発者側に対して、データの収集内容、データの利用目的はもちろんのこと、セキュリティの有無、子供向けのアプリ化の可否、利用者側のデータ設定の有無などの明記を求めており（Frey 2021）、パーソナルデータの利用に関しては、かなり注目されていることが分かる。

3.1.2 法律の観点

法律上におけるデータの取扱いについては、1.1.3 項にて記載したとおりである。ただし、次の 1 から 4 の条件を満たした場合、法的保護の対象になるため、本項では、当該条件を示し、整理を行う。

- 1 著作権（3.1.2.1 目）
- 2 特許権（3.1.2.2 目）
- 3 営業秘密（3.1.2.3 目）
- 4 限定提供データ（3.1.2.4 目）

3.1.2.1 著作権

著作権とは、著作権法 第 2 条（定義）第 1 項(1)に該当するものを指す。なお、日本では人の手を介さない機械によって生成されるデータに創作性が認められるのはほとんどなく、データそのものが著作権の保護の対象に該当する可能性はかなり低い（経済産業省 2019: 64-69）。

3.1.2.2 特許権

特許権とは、特許法第2条（定義）第1項、第29条（特許の要件）第1項、第66条（特許権の設定の登録）第1項に該当した場合、当該権利が発生する。そのため、データそのものが「自然法則を利用した技術的思想」（特許法第2条（定義）第1項）に該当する可能性はかなり低く権利の対象外（ただし、データの加工・分析方法を除く）（経済産業省 2019: 64-69）。なお、各国で特許の解釈が異なることがある。たとえば、アメリカ合衆国特許商標庁では、発明者は自然人である原則から特許申請時、AIは発明者となれないと公式に提示している（USPTO 2020）。その一方で、オーストラリアは当該USPTOの見解を支持せず、AIを発明者として認める判断を示している（IP Australia 2021）。

3.1.2.3 営業秘密

営業秘密とは、不正競争防止法第2条（定義）第6項に該当する情報を指す。そのため、不正競争防止法第2条（定義）第6項に該当する場合は、営業秘密の対象になる。不正競争防止法第2条（定義）第1項(4)乃至(10)、第3条（差止請求権）、第4条（損害賠償）、第21条（罰則）および第22条に該当する行為が行われた場合、相手方に対して差止請求や損害賠償請求などを行うことができる（経済産業省 2019: 64-69）。

3.1.2.4 限定提供データ

限定提供データとは、不正競争防止法第2条（定義）第7項に該当する情報を指す。そのため、不正競争防止法第2条（定義）第7項に該当するように運用されているデータについては、限定提供データの対象になる。不正競争防止法第2条（定義）第1項(11)乃至(16)、第3条（差止請求権）および第4条（損害賠償）に該当する行為が行われた場合、相手方に対して差止請求や損害賠償請求などを行うことができる（ただし、第19条（適用除外等）第1項(2)ロに該当する場合は除く。）（経済産業省 2019: 64-69）。

3.1.3 法律実務の観点

事業を行う際、法律の定めだけでなく、法律上の定めでは足りない箇所に関しては、当事者間における契約の定めなどで管理をしていることがある。そのため、企業法務の観点からデータについて述べる。Business Lawyersによると、法律実務の観点では、次の1から4のデータの分類が行われている（Business Lawyers 2020）。

- 1 秘密性の高いデータ/低いデータ
秘密として保護すべき必要性が高いデータを秘密性の高いデータ，秘密として取扱う必要がなく，第三者と共有が可能な秘密性の低いデータを指す（ただし，公開データではない）．秘密性の高いデータのうち，3.1.2.3 目で取上げた条件に該当する場合は営業秘密，3.1.2.4 目で取上げた条件に該当する場合は，限定提供データとなる．
- 2 パーソナルデータ/非パーソナルデータ
3.1.1.1 目と同様．
- 3 構造化データ/非構造化データ
詳細は，3.1.3.1 目のとおり．
- 4 リアルタイムデータ/非リアルタイムデータ
リアルタイムデータとは，常に更新されるような状態のデータを指す．データのリアルタイム性が重要になるため，時間が経過したデータは，価値が低下する傾向がある．

3.1.3.1 構造化データ/非構造化データ

構造化データと非構造化データ共に，センサなどにより収集された行動履歴を含む膨大なデータのことを指す（経済産業省 2019: 14-20）．

構造化データとは，事前に定められた構造となるように整形されたデータを指す．構造化データを使うことによって，機械学習のアルゴリズムを簡単に利用できるうえ，多くの利用者が簡単に利用もできる．また，構造化データの分析ツールは多く存在し，様々のツールで分析することができる（Talend 2021）．

一方，非構造化データとは，取得時のそのままの形式で保存され，使用時まで処理されないデータのことを指す．非構造化は，形式が自由なため，高速なデータ収集が可能になる特徴がある．ただし，分析などを行う際は，データの準備と分析にデータサイエンスの専門知識が必要であること，また，構造化データの分析ツールは多く存在していたが，非構造化データの操作には専用のツールが必要になることがある（Talend 2021）．

なお，総務省が公開している構造化データ，非構造化のデータのユースケース別の図でまとめたものは図 3-1 のとおりである（総務省 2014: 7）．非構造化データは，記事，法令や報告書など文字で表されているものが多いことが分かる．

	構造化データ	非構造化データ
業務システム	顧客DB 購買記録 売上データ 商品マスターDB 経理データ	業務連絡 (テキスト) 業務日報 (テキスト) 種番録 (テキスト) 資料・書類 (テキスト) 【医療】電子カルテ (テキスト)
(システム以外の) 業務活動	アンケートデータ 統計調査原票データ	システムログ (各種ログ) 自動改札機乗降機ログ (各種ログ) ETC通過記録 (各種ログ) TV会議画像 (画像、静止画、動画) 【医療】画像診断 (画像、静止画、動画)
WEBサービス (EC等)	ECサイトに於ける販売ログ :	商品レビュー (テキスト) アクセスログ、閲覧履歴 (各種ログ)
センサー GPS M2M	入退館記録 GPSデータ RFIDデータ	位置情報ログ (各種ログ) センサーログ (各種ログ) 動作履歴、故障履歴 (各種ログ)
メディア コンテンツ	データ放送データ (EPG等) :	記事 (テキスト、画像、静止画、動画) 動画・映像配信ログ (各種ログ)
パーソナルメディア ソーシャルメディア	会員属性 利用履歴 :	Blog、SNS等記事 (テキスト) アクセスログ (各種ログ) TV電話画像 (画像、静止画、動画) 電子メール添付ファイル (画像、静止画、動画)
その他	統計 統計調査データ 各種台帳類	録音音 (テキスト) 通達、公示等 (テキスト) 種番録 (テキスト) 法令 (テキスト) 各種電子納品物、設計図等 (テキスト) 種番録 (テキスト) 録音音 (音声、静止画、動画) 施工写真等 (画像、静止画、動画)

図 3-1 構造化・非構造化データ (総務省 2014: 7)

3.1.4 営利・非営利の観点

経済産業省では、データの属性、保有・管理主体に着目して、図 3-2 のとおり、データの種類を分類している (経済産業省 2015a: 7)。

属性	保有・管理主体		
	政府・非営利	営利事業者	個人・消費者
政府・非営利	① 自然環境が起源で、政府等が取得・管理 - 地形図(国土地理院) - 気象(気象庁) - インフラ関連(国交省、自治体等) 等		
営利事業者	② 事業者が作成・提出等を行い、政府等が管理 - 法人・不動産登記 - 許認可 - 規制当局への提出資料 - 決算報告書 等	③ 事業者が事業活動の中で作り出し、創出・管理 - 財務・会計・経理 - 研究開発、設計 - 知財、アルゴリズム - 生産・SCM 等	
個人・消費者	④ 人の生死等、公益性と個人性が高く政府等が管理 - 医療・レセプト・介護 - 事故・犯罪 - 税金・社会保障 - 戸籍・住民票・マイナンバー等	⑤ 消費活動を通じて創出され事業者が管理 - 移動履歴・運転履歴 - 購買・POS - 決済・電子マネー - 金融・財産 等	⑥ 個人が日常的に生活する上で創出・管理 - 基本情報 (氏名等) - 身体・健康 - 位置情報 - 交友関係 等

図 3-2 データの性質 (経済産業省 2015a: 7)

分類の仕方は、政府・非営利、営利事業者、個人・消費者の保有・管理主体と属性に分ける。そのあと、それぞれで管理しているデータで分類分けされて

いる。

3.1.5 情報取得の観点

フリーランス協会では、データ連携やデータの取得を行う際の情報の種類を特徴ごとに以下のとおり整理を行っている（フリーランス協会 2018: 12）。

- 1 公的公開情報
API 連携により取得できる情報
- 2 私的公開情報取得可能
スクレイピングにより取得できる情報。なお、1.1.2 項で取上げたとおり、スクレイピングは、Web サービスによって、利用規約上で禁止されていることがある。
- 3 非公開情報
データを保有している企業に対してデータに関する取引を依頼する必要がある情報

上記は、データを取得する方法によって分類されているものであり、当該情報がパーソナルデータに該当するかなどは問わない。

3.1.6 どのような性質のデータがあるのか（What）

本節では、どのような性質のデータがあるのか（What）という問いを解くためにデータビジネスの観点、法律の観点、法律実務の観点、営利・非営利の観点および情報取得の観点からすでに種類分けされているデータの種類について取上げた。法律の観点、法律実務の観点および情報取得の観点の結果をデータの法的保護の観点から整理すると図 3-3 のとおりになる。図 3-3 から、法的保護を受けるには特許権の該当要件などからも比較して、非公開情報にするのが妥当だということがわかる。ただし、実務上、非公開情報にした場合、データの取引が公開情報より活発ではなくなるため、データを活用したサービスの形態によって法的対象にするかどうか検討する必要がある。

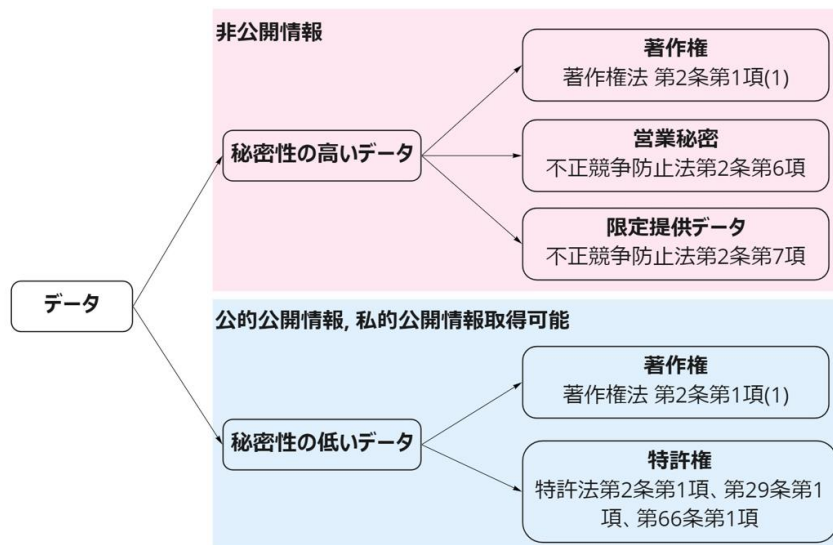


図 3-3 データの法的保護の対象

次にデータビジネスの観点、法律実務の観点および営利・非営利の観点の結果を 3.1.4 項 図 3-2 のフレームを活用して整理を行う。なお、図 3-2 に記載「政府・非営利」、「営利事業者」、「個人・消費者」の属性について、「政府・非営利」は非営利が事業者に含まれる可能性があることを検討し、地方公共団体に置き換える。「営利事業者」は、非営利が含まれたことにより、事業者に置き換え、「個人・消費者」については、個人のデータの利用者も想定できるため、利用者に置き換える。

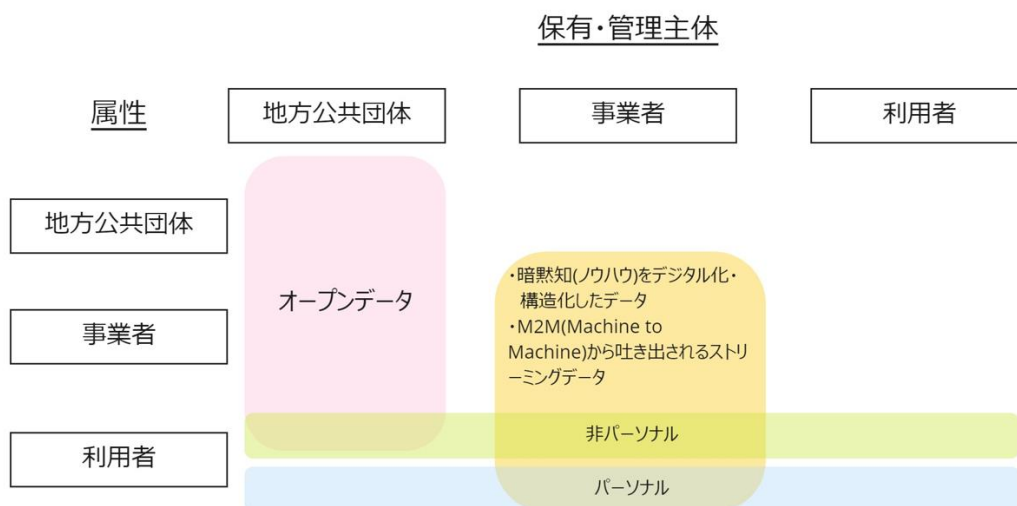


図 3-4 属性別データ種別

整理した結果が図 3-4 のとおり。1.1.5 項で取上げたスーパーシティ構想など、分野を跨いだデータの連携によるサービス提供を検討する際は、図 3-4 の被っ

ていないところのデータを融合させ、サービスに活かすことが重要であることが読取れる。

なお、データの取得する方法として、構造化データ/非構造化データ，リアルタイムデータ/非リアルタイムデータを取上げたが，どちらであっても図 3-3 や図 3-4 の結果が変わることはないが，当該データをどのようにサービスに還元するかにより，手段を選択する必要がある，選択を誤ると無駄なコストや時間が必要になることがわかった。

3.2 データの活用状況

本節では，データの活用状況を把握することを目的とする．把握するにあたり，経済産業省が公表している図3-5を参考にする．図3-5では，データを活用したビジネスにおいて，データを収集するだけでなく，それに基づいてビジネスモデルを構築し，さらにデータの収集が必要としている（経済産業省 2015b: 21）。

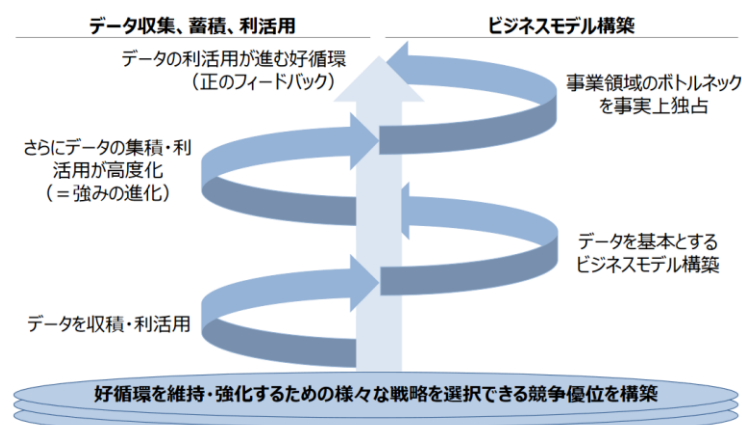


図 3-5 データ収集、蓄積、利活用のサイクル（経済産業省 2015b: 21）

上記から，現状，データの利用状況がどのようになっているのか，以下の観点から調査を行う。

- 1 データを集積・利活用
 - ① データの収集状況（3.2.1 項）
 - ② データの利用状況（3.2.2 項）
- 2 データを基本とするビジネスモデル構築
 - ③ データを活用した分析の状況（3.2.3 項）

3.2.1 データの収集状況

総務省の調査報告によると、分析に用いるデータの入手元は、図 3-6 のとおり。全体的に社内データを活用している企業が約 70~80%で一番多い。次いで外部データを購入している企業が多いものの全体的に約 30%と少ない。さらに、オープンデータや公開データとなると活用している企業が少ないことが読取れる（総務省 2020b: 52）。

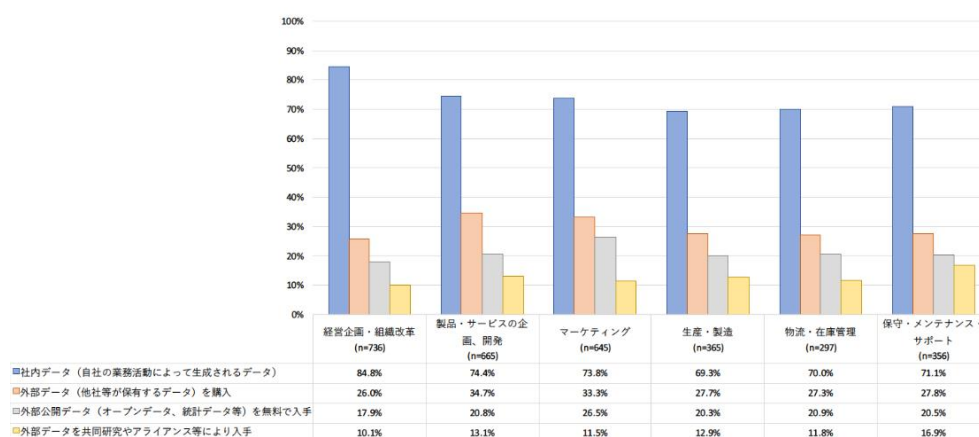


図 3-6 データの入手元（総務省 2020b: 52）

3.2.2 データの利用状況

まず、収集したデータをどのように活用しているのかを取上げる。総務省の調査報告によると、各企業のデータの活用方法については図 3-7 のとおり。データの分析方法は、データの閲覧と集計が 70%以上を占めている。一方で、「統計的な分析」や「機械学習・ディープラーニングなど人工知能（AI）を活用した予測」については、企業規模に大きな差異がみられ、データの利活用を促進するためには、「統計的な分析や機械学習・ディープラーニングなど人工知能（AI）を活用した予測」を企業規模に関係なく、容易にできるような環境を作る必要があることが分かる（総務省 2020b: 50）。

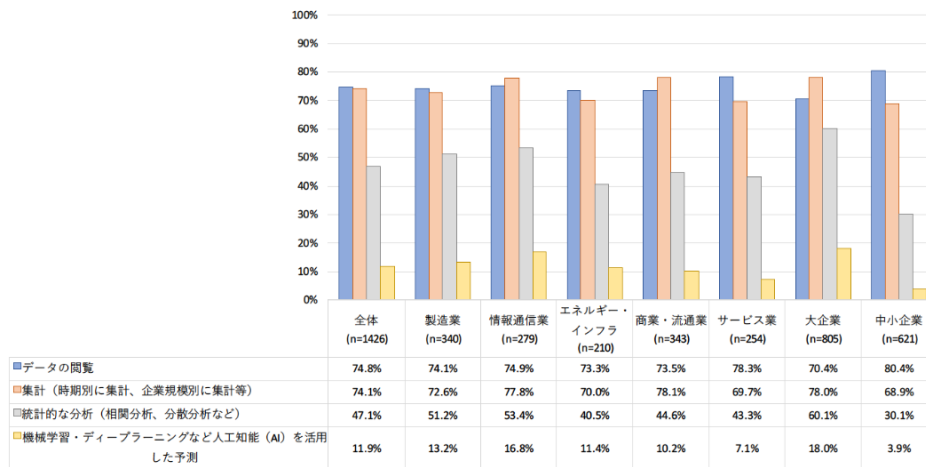


図 3-7 データ分析手法（総務省 2020b: 50）

次にデータの利用状況を検討するにあたり、データを利用した効果率について取上げる。データを収集または利用率を検討した際、データの活用に対して効果が思っていない企業が継続的にビジネスモデルを構築して検討する確率が低いと思われるためである。総務省の調査報告によると領域別でのデータを活用した際の効果について、図 3-8 のとおり。どの領域においても半数以上は効果があったと回答しているが、7 割は超えていない。一方で、あまり効果がなかった、全く効果がなかったと回答したのが 10%未満であり、データを活用することに何らかの効果を感じているということが分かる。ただ、領域による差異はあまり見られない（総務省 2020b: 61）。

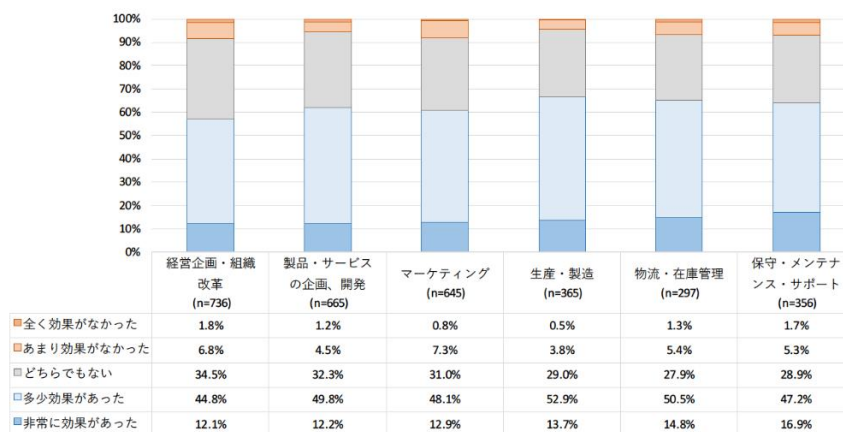


図 3-8 データ活用の効果（総務省 2020b: 61）

3.2.3 データを活用した分析の状況

データを活用したビジネスモデルを検討するにあたり、まず、どのようなデータが収集されているのかを取上げる。総務省で行われた分析に活用されているデータを5年前と現在で比較して表したグラフが公開されている(図 3-9) (総務省 2020b: 44)。ここから、POS データ、e コマースによる販売記録データ、M2Mデータを含む自動で取得されるデータの活用が活発化していることが分かる。また、電話などの音声データの活用も進んでいることがわかり、自動化に向けたサービスのための分析(業務効率)や顧客の嗜好を分析し、サービスを提供するモデルが進んでいることがこのグラフから読取れる。

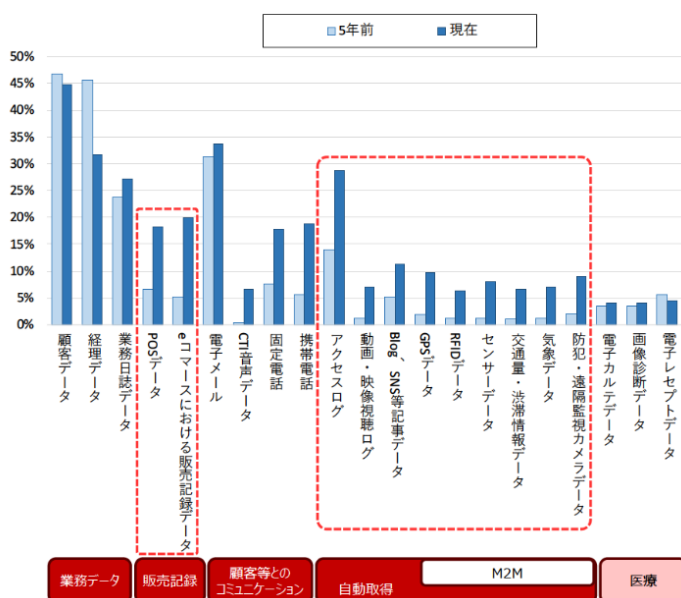


図 3-9 分析に活用しているデータ (総務省 2020b: 44)

データを活用して分析する際は、他の分野のデータと分析を行うこともある。総務省が公表しているデータの部門ごとのデータの組み合わせを行っている種類の比率は図 3-10 のとおり (総務省 2020b: 53)。すべての領域において、単独での分析を行っているのが過半数を超えおり、分野を超えた分析等はまだまだあまり主流ではないことが分かる。また、4種類以上になるとどの領域も7%を満たさないため、データの活用推進を行う際は、複数のデータを活用することに対するメリットを提示していくことが重要となると思われる。

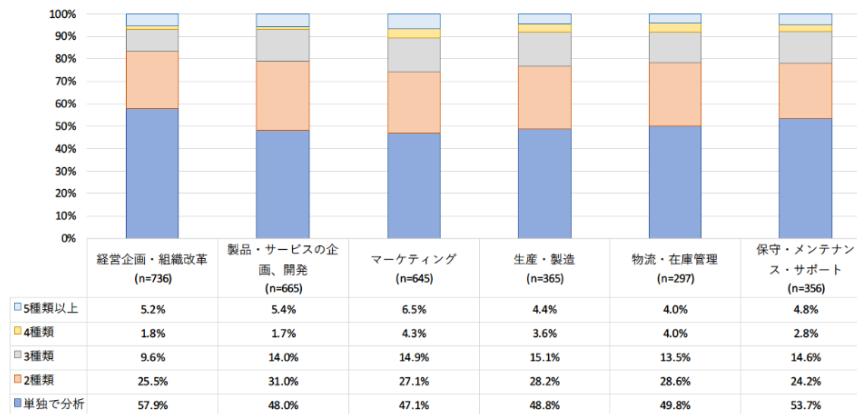


図 3-10 何種類のデータを組合わせて分析するか（総務省 2020b: 53）

3.2.4 どのようなデータの優先度が高いのか（What）

どのようなデータの優先度が高いのか（What）を検討するにあたり，データの活用状況を取上げた。グラフから，5年前までは，M2Mのデータを活用できていなかったところから，直近では，M2Mのデータ，自動化業務改善を行うためのデータ活用が注目されていることが分かった。ただ，オープンデータがうまく活用できていない点や複数の種類のデータを組合わせて活用されていることが少ない点からこの点に力を入れていくのが先行者優位になる可能性はある。また，データの活用に対して効果がないと思っている企業は少なく，効果があるという普及活動そのものは場合によっては効果が薄い可能性があると推測される。

3.3 データの流通および共有方法

データを活用する際，単にデータの取引としてデータの提供，受領だけではなく，やり取りに様々な方法がある。そのため，本節では，様々な観点のデータのやり取りについて取上げ，整理を行う。本節にて，取上げる観点は次のとおりである。

- 1 産業の観点（3.3.1項）
- 2 契約上の観点（3.3.2項）
- 3 既存の事例の観点（3.3.3項）
- 4 クリエイティブ・コモンズ・ライセンスの観点（3.3.4項）

3.3.1 産業の観点

経済産業省で行われた検討会において、データ流通・共有方法には、図 3-11 の「共有財産型」、「集約・加工型」、「取引市場型」の 3 つの類型があるのではないかと検討された（経済産業省 2015c: 9）。

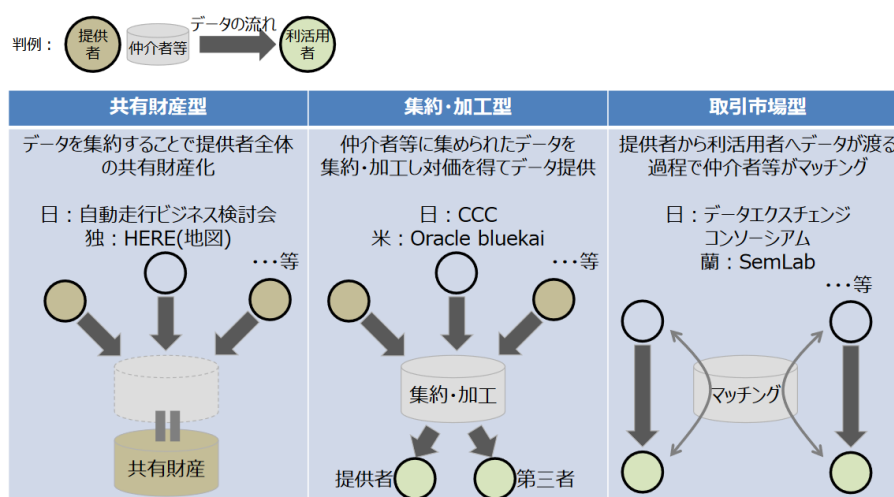


図 3-11 データの流通・共有方法（経済産業省 2015c: 9）

「共有財産型」は、データを管理するプラットフォーム上では分析、加工などは行われないと読取れ、提供者側が共有財産に管理されているデータにアクセスできると思われる一方、「集約・加工型」、「取引市場型」では何かしらのデータ加工、分析が行われるように思われ、利活用側がプラットフォーム上のすべてのデータにアクセスができるわけではなく、必要な情報を最低限提示されるようプラットフォーム側で管理されていると思われる。

3.3.2 契約上の観点

データの取引をする際、3.1.2 項でも取上げたとおり、データによっては法的保護の対象にもなるため、取引で扱うデータについて、法的保護を受ける場合は、相手方にも法的保護を受けられるよう要件に満たした管理を行う必要がある。また、取引方法も重要であり、取引方法によって対価やデータの扱いも変化する。そのため、本節では、法的保護の対象を含めたオープンデータではない場合の契約による取引方法を取上げる。

経済産業省が公開している『AI・データの利用に関する契約ガイドライン』では、データの取引形態として、次の 1 から 3 までの類型があるとしている（経済産業省 2019: 27-29）。

- 1 譲渡 (3.3.2.1 目)
- 2 ライセンス (利用許諾) (3.3.2.2 目)
- 3 共同利用 (相互利用許諾) (3.3.2.3 目)

上記の類型について、次目で取上げる。

3.3.2.1 譲渡

3.1.2 項でも取上げたとおり、データは無体物であるため、所有権の対象とはならない。そのため、所有権の譲渡という形式にするのは厳しい。データを所有権の譲渡と近い形式に行う場合は、契約上では、所有権の譲渡ではなく、データに関する一切の権限をデータの受領側に移転させ、データの提供者側は当該権利の一切の権限を失わせる手段が近いと考えられる。なお、取引を行うデータが、著作権法第2条(定義)第1項(1)に該当する場合は該当する権利の譲渡も必要となる。なお、経済産業省が提示している『AI・データの利用に関する契約ガイドライン』では、譲渡を行う際の次の方法が明示されている(経済産業省 2019: 27-29)。

- ・ データを記録した記録媒体を引き渡し、譲渡人は当該データを消去する方法
- ・ データを譲受人の記録媒体に複製し、譲渡人は当該データを消去する方法
- ・ 第三者のサーバにあるデータに対するアクセス権を譲受人に付与し、譲渡人は当該データのアクセス権を失う方法(または譲渡人が当該データの管理に係る第三者との契約上の地位を譲受人に移転させる方法)
(経済産業省 2019: 28)

なお、契約上、著作権などの譲渡を行わせる場合、炎上してしまうケースがあるため注意が必要である。たとえば、ユニクロが提供しているスマホで絵を描いてスマートフォンアプリにて登録することで、オリジナルの T シャツを作成してくれるサービス「UTme!」(UNIQLO 2021)の利用規約である。2014年5月時点の利用規約の文言に「投稿データについて、その著作物に関するすべての権利(著作権法第27条及び第28条に定める権利を含みます)を、投稿その他送信時に当社に対し、無償で譲渡します」(Top Court 2020)という記載があり、すべての権利を譲渡という形にしていたが、利用者側から反発を受け、現在は以下のように修正し、譲渡という形にはしていない。

第10条(権利帰属)

- 1 ~2 略
 - 3 投稿データの著作権は、既に他者の著作権が存在している部分を除きユーザーに帰属します。ただし、出品ユーザーは、出品データについて、当該出品データの投稿をもって、当社が他のユーザーに販売する権利を許諾したものとみなします。
 - 4 ~5 略
- (UNIQLO 2017: UTme!利用規約 第10条(権利帰属)第3項)

3.3.2.2 ライセンス (利用許諾)

ライセンス (利用許諾) とは、3.3.2.1 目で取上げた譲渡と異なる点は、データの提供者側は、データの権利を放棄せずに当該データの使用権利などを一定の範囲で許諾するものである。3.3.2.1 目で取上げた UTme!利用規約の第10条(権利帰属)の規定が該当する。また、特許やソフトウェアのライセンスと同様、非独占、独占という許諾する範囲の定めが契約上でできる。

許諾の方法として、データへのアクセス権限をデータを受領者に与え、契約終了時に当該アクセス権限を停止させるとともに、データを複製した場合は、当該複製を含め、データの消去義務を負わせておくのが望ましいとされている(経済産業省 2019: 27-29)。

一方で、データ受領者から許諾を求められるパターンも想定される。たとえば、データには限らないが、GitHub 利用規約では、利用者に対して、所有権などは利用者に残したままいくつかの権利を許諾するよう求める定めがある。(GitHub 2021)

- 3 コンテンツの所有権、投稿する権利、ライセンスの付与
お客様は、「あなたのコンテンツ」の所有権および責任を保持します。お客様が自身で作成していないものや権利を所有していないものを投稿する場合、お客様は投稿する「コンテンツ」に責任を負うこと、お客様に投稿する権利がある「コンテンツ」のみを送信すること、および投稿する「コンテンツ」に関連する第三者のライセンスを完全に遵守することに同意するものとします。
~略
- 4 当社へのライセンス許可
当社には、「あなたのコンテンツ」のホスト、公開および共有などを行うための法的権利が必要です。お客様は、当社およびその後継者に、「あなたのコンテンツ」を保存、アーカイブ、解析、および表示し、

今後の「サービス」向上を含めて「サービス」の提供のために必要に応じて付随的な複製を作成する権利を付与します。

～略

5 他のユーザへのライセンス許可

～略

お客様が自身のページおよびリポジトリを公に表示するように設定した場合、お客様は GitHub の「サービス」を通じて「あなたのコンテンツ」を使用、表示、および実演し、また GitHub の機能を通じて許可される限りにおいて（フォークなど）のみ GitHub 上で「あなたのコンテンツ」を複製する、非独占的かつ世界的ライセンスを GitHub の各「ユーザ」に付与します。～略

(GitHub 2021: GitHub 利用規約 D. ユーザ生成コンテンツ 第 3 項乃至第 5 項)

上記のとおり、サービスを提供する代わりに、許諾を求めること、また、相手によって許諾の内容を変えるということもでき、臨機応変にサービスに応じて定める必要がある。

3.3.2.3 共同利用（相互利用許諾）

共同利用（相互利用許諾）とは、契約当事者間同士保有するデータについて、契約上の定めによって権利の全部または一部を相手方に与えることをいう。

方法としては、3.3.2.2 目と同様なアクセス権限を付与するやり方が良いとされている。例えば、名刺の一括管理を行うサービスを提供している SanSan の利用規約がこの方式を採用している (Sansan 2021)。

第 2 条（サービスの概要）

本サービスの概要は以下の通りです。お客様は、当社に名刺等の情報（以下「委託データ」という）の取り扱い等を委託するものとします。

- (1) 当社は、お客様にスキャナ等の機器（以下「Sansan スキャナ」という）の貸与、その他の名刺登録手段（以下 Sansan スキャナと合わせて「Sansan スキャナ等」という）の提供を契約内容に応じて行います。
- (2) 当社は、お客様が Sansan スキャナ等に登録した名刺をインターネット経由で受信し、テキスト化处理（以下「テキスト化处理」という）を行います。
- (3) 当社は、当社独自のアプリケーション（以下「当社アプリケーション」という）において、お客様が指定した利用者（以下「利用

者」という) に対してユーザ ID (以下「ユーザ ID」という) を発行し、委託データをお客様の利用に供します。

- (4) 当社は、当社アプリケーションを通じて、その他各種付加サービス (以下「付加サービス」という) を提供します。

(Sansan 2020: Sansan サービス約款 第 2 条 (サービスの概要))

上記のとおり、データの管理はあくまで Sansan は委託を受けているという立て付けで、データ提供者が許諾した際にデータ提供者が指定した利用者に開示するといった方法を採用している。なお、契約終了後の定めは次のとおり (Sansan 2020)。

第 9 条 (契約終了の効果)

契約期間満了、解約又は解除となった場合、以下の義務が発生します。

- (1) 当社は、委託データにつき、個人情報情報を破棄します。
- (2) 当社は、解約時においてお客様へ委託データのダウンロード及びその他の委託データの保存手段を提供いたしません。但し、契約内容により、本サービスの機能として委託データのダウンロード機能を提供する場合があります。
- (3) 略

(Sansan 2020: Sansan サービス約款 第 9 条 (契約終了の効果))

上記では、利用者に対してデータの削除までは求めてはいないものの、契約終了後は、保存手段を提供しない旨が記載されている (Sansan 2020)。

3.3.3 既存の事例の観点

総務省が公開している報告書では、図 3-12 のように PDS やデータマーケットプレイスのモデルおよびケースが紹介されている。どちらも当該モデルの特徴は、データの管理は利用者に置き、利用者の意思に従ってデータの提供などの取引を行うモデルである (総務省 2017a: 16-18)。

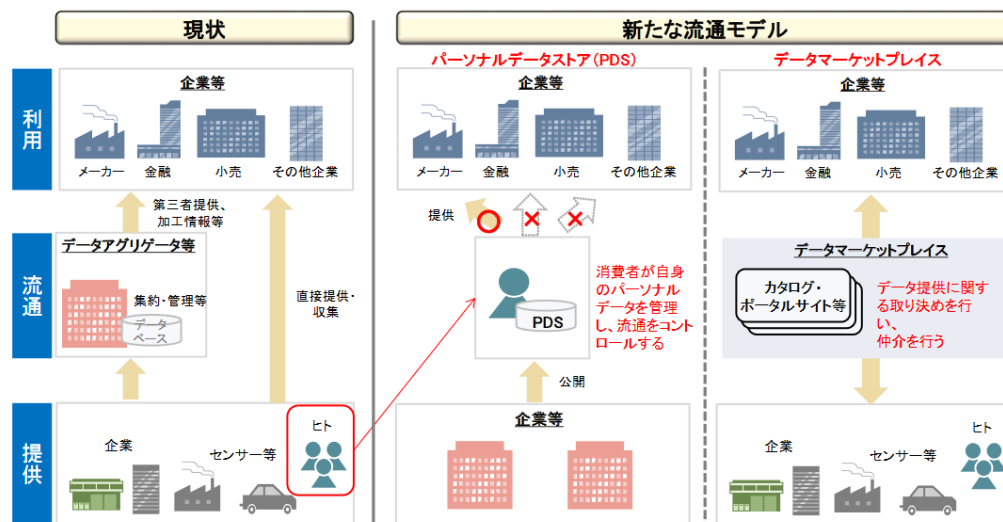


図 3-12 新たな流通モデル (総務省 2017a: 18)

次目では、総務省が公開している報告書で紹介されている PDS およびデータマーケットプレイスの事例を取上げ、事例からビジネスモデルを記載する。

3.3.3.1 PDS の事例

PDS は、欧米では実用化が進んでいる傾向がある。たとえば、米国の Datacoup では、利用者が Datacoup のサイト上で、利用者自身で提供可能なパーソナルデータを選択することで、Datacoup が代理で当該データを保有している企業とアカウントの連携を行い、データの取引を行っている。また、当該データを利用者以外の第三者が保有しているデータと一緒に匿名化を行い、マーケットに販売し、利益の一部を利用者が報酬として受領する仕組みとなっている (総務省 2017a: 21)。

3.3.3.2 データマーケットプレイスの事例

データマーケットプレイス型もサービス化が進んでおり、たとえば、米国の Factual では、世界各国の約 6,000 万の地域情報や約 65 万の製品情報などの位置情報のデータセットを提供し、アプリケーションを提供しているベンダなどに活用されている (総務省 2017a: 21)。

3.3.4 クリエイティブ・コモンズ・ライセンスの観点

データの取引において、最近用いられる利用条件としてクリエイティブ・コモンズ・ライセンス (以下、「CCライセンス」という) がある。CCライセンスとは、「インターネット時代のための新しい著作権ルールで、作品を公開する

作者が『この条件を守れば私の作品を自由に使って構いません.』という意思表示をするためのツール」(クリエイティブ・コモンズ・ジャパン 2021: 2 段落目)であり、「著作権を保持したまま作品を自由に流通させることができ、受け手はライセンス条件の範囲内で再配布やリミックスなどを行うこと」(クリエイティブ・コモンズ・ジャパン 2021: 3 段落目)を目的としている。CC ライセンスでは、図 3-13 のとおり、表示方法によって著作権の権利の主張やその逆の放棄の主張ができる。



図 3-13 CC ライセンスの許諾範囲 (クリエイティブ・コモンズ・ジャパン 2021)

そのため、表 3-1 のとおり、CC ライセンスで表示できるだけの条件でデータの取引方法があるといえる。なお、それぞれにリーガルコード (利用条件) が用意されている。

表 3-1 CC ライセンスの種類 (クリエイティブ・コモンズ・ジャパン 2021 から作成)

No.	表示名	利用条件	コモンズ証
1	表示	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 改変, 営利目的での二次利用は可能 	
2	表示-継承	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 改変した場合には「表示-継承」ライセンスでの公開義務 改変, 営利目的での二次利用は可能 	
3	表示-改変禁止	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 改変禁止 営利目的での二次利用は可能 	
4	表示-非営利	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 非営利目的に限り, 改変, 再配布は可能 	
5	表示-非営利-継承	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 非営利目的に限り, 改変, 再配布は可能 改変した場合には「表示-非営利-継承」ライセンスでの公開義務 	
6	表示-非営利-改変禁止	<ul style="list-style-type: none"> 氏名, 作品タイトルなどの著作者の情報の表示義務 改変禁止 非営利目的に限り, 再配布は可能 	

なお, 上記の表 3-1 は No.の値が低いほど, 条件が緩い CC ライセンスの種類である。

3.3.5 どのようにデータを流通・共有すべきか (How)

本節では, どのようにデータを流通・共有すべきか (How) を検討するにあたり, データの流通および共有方法について, 産業の観点, 契約上の観点, 既存の事例の観点およびクリエイティブ・コモンズ・ライセンスの観点から取上げた。取上げた内容から, 契約条件とデータの管理方法から流通・共有について検討する必要があることがわかった。なお, 取上げた観点をまとめると図 3-14 のとおり。データの権利についてどこに設定するかによって条件, 取引方法が大きく変わることが分かる。

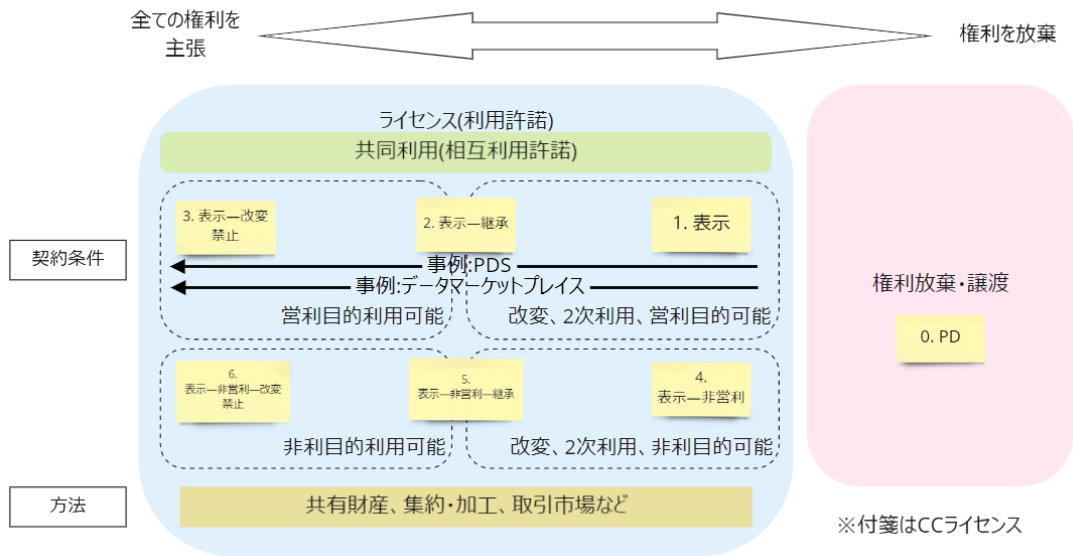


図 3-14 データの取引方法と条件

3.4 インセンティブ

データを活用したサービスにおいては、データ提供者、データの受領者、サービス提供者など様々なステークホルダーがいる。さらに、提供するデータがどのくらい価値があるかの判断は難しく、インセンティブの考え方も付随するため、難しいと思われる。

そのため、本節では、調査報告書や事例から、様々な視点からインセンティブについて、次の 1 から 3 の観点からどのような手段があるのかを取り上げ、調査を行う。なお、PDS、データマーケットプレイスで発生したインセンティブについては 3.3.3 項で取上げたため、本節では取上げない。

- 1 産業の観点 (3.4.1 項)
- 2 契約上の観点 (3.4.2 項)
- 3 法律による観点 (3.4.3 項)

3.4.1 産業の観点

経済産業省ではデータのインセンティブについて議論がされたことがあり、図 3-15 が示された。図 3-15 では、データ提供側のインセンティブを表しており、インセンティブの内容が、事業者の所有しているデータとパーソナルデータを提供した場合と似ているものの、仲介企業が大きく異なることが読取れる。どちらのパターンにおいても、サービスを得る、対価をもらう、提供したデー

タと別のものと交換の3つに分けられることが分かる（経済産業省 2015c: 10）.

データ提供側のメリット	提供されるデータの例	仲介企業・組織例	
カンパニーデータ (企業保有情報)	有益なサービスを得る	<ul style="list-style-type: none"> 企業活動データ 商取引データ 	<ul style="list-style-type: none"> コンサルティング会社 CCC (Tポイント) 等
	対価をもらう	<ul style="list-style-type: none"> 顧客情報 	<ul style="list-style-type: none"> Oracle bluekai 等
	他社データの利用 (共同研究開発、 インフラ整備等含む)	<ul style="list-style-type: none"> 自動走行関連技術 損害保険、支払ブラックリスト (制度上共有するデータ) 	<ul style="list-style-type: none"> 自動走行ビジネス協議会 保険会社、クレジットカード、 通信会社等
パーソナルデータ (個人保有情報)	有益な サービス(有料)を得る	<ul style="list-style-type: none"> レセプト情報、特定健診情 報 等 	<ul style="list-style-type: none"> データヘルス計画 等
	お金・ポイントを貰う	<ul style="list-style-type: none"> 購買データ 生活データ 	<ul style="list-style-type: none"> CCC (Tポイント) 等 SemLab 等
	他の提供者が集めた 有用データと交換	<ul style="list-style-type: none"> 写真、動画、位置情報等 料理レシピ、レストラン情報等 	<ul style="list-style-type: none"> Facebook 等 クックパッド 等

図 3-15 データのインセンティブ（経済産業省 2015c: 10）

上記は、すでにサービスが定まっている、すなわちデータを活用したサービスを提供することによって利益が出る可能性がある場合は有効の手段ではあるものの、当該データの有効性が不明な場合は、リスクが高いと思われる。

3.4.2 契約上の観点

経済産業省では、『AI・データの利用に関する契約ガイドライン』にて、データを活用したサービスにおけるインセンティブの算出方法/運用方法が次のとおり、提示されている（経済産業省 2019: 26-28）.

- 1 データを利用した価値の試験的検証
データをを用いたサービスがどのくらい価値があるか不明確なため、まず、PoC を行い検証する。当該検証結果により、効果、利益率を把握して、算出する方法.
- 2 イニシャル・ロイヤリティおよびランニング・ロイヤリティの活用
データの取引においては、継続的にデータが蓄積または更新され、アップデートすることで価値が出てくるものもある。そのため、ランニングコストとして、まず、データ収集分などのイニシャル・ロイヤリティを受領し、その後、利益が生じた場合にランニング・ロイヤリティを受領する方法.

上記は、データの有効性が不明な場合の時に検討された事項であると読取れ、データを活用したサービスを検討する際には有効ではあるものの、特定の提供したいサービスが決まっている場合などには、活用が難しいと思われる。

3.4.3 法律による観点

法律の定めにより，有益なサービスを得る，対価を得るなどのインセンティブを受領した事例がある．米国では，医療業界におけるクラウドサービスにて，HITEC が施行され，EHR の導入が進んだ．特に連邦政府が，導入支援金を提供したため，導入率が上がり，データの活用の促進にもつながっている（経済産業省 2018: 10）．なお，HITEC，HIPAA は下請事業者も対象のため，たとえば Microsoft が提供しているクラウドサービスを活用して下請の事業を行う際であっても PHI を適切に保護する旨を Microsoft と契約を締結する必要がある（Digital Transformation Channel 2020）．

3.4.4 データ提供活性化のために，どのようなインセンティブを与えるべきか（How）

本節では，データ提供活性化のために，どのようなインセンティブを与えるべきか（How）を検討するにあたり，インセンティブについて，産業の観点，契約上の観点および法律による観点からデータの提供者の視点に限らず，取上げた．それぞれの観点を取上げたところ，データを活用したサービスの検討または導入時期によって，インセンティブの方法が異なる可能性があり，図 3-16 のように整理を行った．

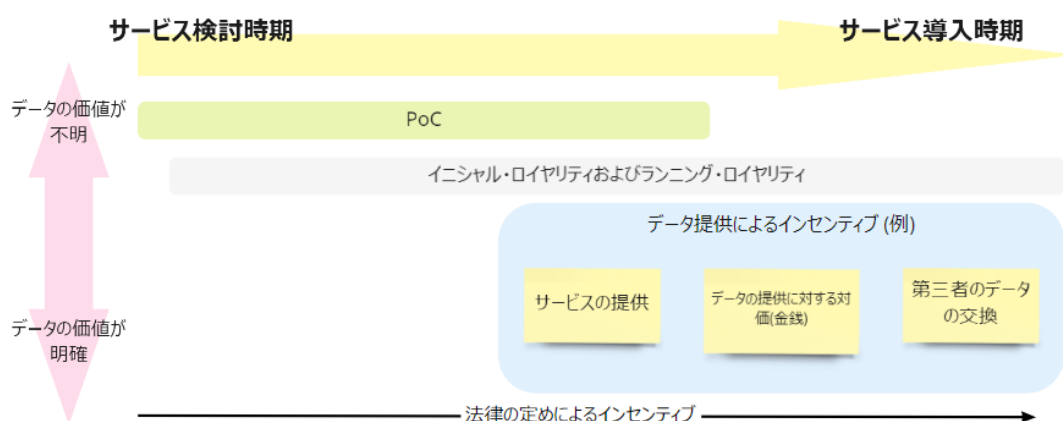


図 3-16 データの提供によるインセンティブ

上記から，データを活用したサービスを検討する際は，検討時期およびデータの価値からインセンティブの方法を検討するのが良いと思われる．

3.5 オープンデータ

オープンデータの定義は、1.1.4 項で取上げたとおりとする。また、第第 3 章の冒頭で取上げたとおり、経済産業省によるデータに関する競争領域、共創・協調領域の明確化する方法として、オープンデータも同様に以下の手順に従い調査を行う（経済産業省 2015a: 5）。以下の調査以外にも現状を把握するためにオープンデータの現状（3.5.1 項）を取上げる。

- 1 どのような性質のデータがあるのか（What）
 - ① オープンデータのルール（3.5.2 項）
- 2 どのようなデータの優先度が高いのか（What）
 - ② オープンデータの目的（3.5.3 項）
- 3 どのようにデータを流通・共有すべきか（How）
 - ③ オープンデータのビジネス（3.5.4 項）
- 4 データ提供活性化のために、どのようなインセンティブを与えるべきか（How）
 - ③ オープンデータのビジネス（3.5.4 項）
- 5 どのような環境・ルールを整備すべきか（How）

次章以降

3.5.1 オープンデータの現状

2017 年に総務省によって行われた地方公共団体に対する調査によると、3 年前より 10%増加して 20.8%の地方公共団体が、オープンデータの活用に取り組んでいる、参加している、協力している団体と回答した。また、当該地方公共団体のうち、オープンデータとして提供しているデータとして、各種調査・統計データが 71.7%と最も多く、次に各種公共施設情報が 68.3%、防災分野の各種情報が 64.3%の順となっており、3 年前と比較して増加している。一方、その他の分野のデータの取扱いは減少傾向となっている（総務省 2017c: 68-71）。しかし、3.2.1 項の図 3-6 で取上げたとおり、地方公共団体の取組としては進んでいるものの、企業による活用は進んでいない。この要因として考えられるのは、総務省によると利用可能なデータの種類が不足していると予測されている（総務省 2020c）。

なお、2018 年に筑波大学（実施協力機関：一般社団法人地方行財政調査会）による各地方公共団体に対するオープンデータに関する取組みの調査が行われたため、本項ではその結果をもとに考察を行う。調査内容、調査方法、調査期

間および回答数は次のとおり（筑波大学 2019: 3）.

1 調査内容

全国の市・特別区に対して、次の 3 つのカテゴリのアンケート調査を実施

- ① オープンデータ施策の取り組み状況
- ② 庁内における行政データの活用状況
- ③ データを巡る住民・企業等との連携・協業の実態

2 調査方法

- ① 自治体におけるオープンデータ施策、データ活用、外部との協力関係構築の進展度合いを得点化
- ② 全国の自治体を類型化し、それぞれの取組の特徴を抽出
- ③ 自治体の庁内データ活用度・外部団体関係度とオープンデータ取組との関係性

3 調査期間

2018 年 11 月～2019 年 2 月

4 回答数

上記「2 調査方法」の①と③：462 団体／全国の市・特別区の合計数 815 団体（回答率 56. 7%）

上記「2 調査方法」の②：461 団体／全国の市・特別区の合計数 815 団体（回答率 56. 6%）

（筑波大学 2019: 3）

3.5.1.1 調査結果によるクラスター

本調査結果を踏まえて、地方公共団体の類型化（クラスター分析）を行っている。方法は、アンケート調査の回答に基づき、得点化・主成分分析を行い、算出された主成分得点（主成分 1～3，累積寄与率 48. 110%）を変数としてクラスター分析されている。各クラスター名と特徴については次の 1 から 5 のとおり（筑波大学 2019: 7）.

1 先進自治体（18 団体）

総合的な取組みの進展度が高く、特に庁内におけるデータの活用が進んでいる地方公共団体

2 外部連携併行自治体（22 団体）

総合的な取組みの進展度が高く、外部連携は進展しているものの、データの活用はこれからの地方公共団体

- 3 追従自治体（180 団体）
オープンデータは一定程度進展しているものの、データの活用・外部連携はこれからの地方公共団体
- 4 データ活用先行自治体（50 団体）
庁内におけるデータの活用は一定程度進展しているものの、オープンデータ・外部連携がこれからの地方公共団体
- 5 遅延自治体（196 団体）
いずれの取り組みもこれからの地方公共団体

上記から、追従自治体と遅延自治体がかかなり多いことが読取れるが、データを活用するための推進活動を追従自治体と遅延自治体に対して行う場合は、それぞれ抱えている課題が大きく異なるため、別の施策を検討する必要であることが分かる。

3.5.1.2 オープンデータ化の作業

総務省では、地方公共団体のオープンデータ化の効果を図るために、地方公共団体に対して、Web アンケートデータを行い次の 1 から 4 のとおり、経済効果が算出されている。

- 1 費用
オープンデータ化を行うための費用について、費用がかからなかったとする回答が大半であり、100 万円未満の支出が 13 件（総務省 2020b: 11）。ここから、オープンデータ化そのものを行う費用は、地方公共団体が調達においてシステムを導入するほどの費用は掛からないことが分かる。
- 2 人件費
オープンデータ化のために、地方公共団体にて必要だった人員は、1 人から 2 人の少人数が 3 日程度の作業であった（総務省 2020b: 11）。本件についても、オープンデータ化そのものを行う人件費は、地方公共団体が調達においてシステムを導入するほどの作業が発生していないと思われる。
- 3 イメージアップ効果
オープンデータ化することにより、地方公共団体のイメージアップの効果が広告費用に換算して、100 万円未満ながら効果があったとする回答が 37 件で、効果がないという回答を上回る。次いで、500 万円未満が 2 件、1,000-2,000 万円が 1 件となり、オープンデータによる広告

宣伝費効果もあることが読取れる（総務省 2020b: 11）。

4 業務効率化効果

オープンデータ化以前に必要としていた人員と時間と比較し、従来の業務コストを少なく見積もった場合、合計1月当たり1時間程度（1年で12時間程度）（総務省 2020b: 11）で、オープンデータ化による業務の圧迫は生じていないことがここからでも読取れる。

上記から、オープンデータ化による作業デメリットは少ないと思われる。

3.5.1.3 オープンデータによる経済効果

総務省では、海外の先行事例を参考にし、経済波及効果を算出した結果、日本の経済全体へ与える効果を 2.4～4.7 兆円程度と発表している。また、オープンデータを誰でも利用しやすい環境を整えれば、追加で 1,800～3,500 億円程度の追加的経済効果が得られると推測されている（総務省 2020b: 10）。

上記から、オープンデータによる経済効果は、かなり高いと推測できる。

3.5.2 オープンデータのルール

1.1.4 項に記載したオープンデータに関する定義のほか、基本的ルールが設定されているため、本目では当該ルールを取上げる。オープンデータに関する基本的ルールは次の1から5のとおり（内閣官房 2017b: 2-4）。

- 1 オープンデータとして公開するデータの範囲
公共に関するデータについては、国民共有の財産という考えから、政策の企画・立案で使われた資料やデータを含めて、全てオープンデータとして公開することが原則。
- 2 公開データの二次利用に関するルール
各地方公共団体の Web ページ上で公開されるデータについては、公開データの二次利用を積極的に促進している。詳細は、3.5.2.1 目にて扱う。
- 3 公開環境
各地方公共団体は、Web ページで容易に検索・利用できる形でデータを公開するのが原則。
- 4 公開データの形式等
データを公開する際は、構造化データにして掲載することが原則。

5 公開済みデータの更新

リアルタイムデータは、可能な限り、迅速に公開するとともに適時適切な更新を行うことが原則。

上記のルールに該当するデータが、オープンデータとして公開されている。

3.5.2.1 利用ルールの設定

オープンデータを公開する際は、データの活用を促進するために3.3.4項で取り上げたCCライセンスを使用するよう推奨されている（内閣官房 2017a: 57-59）。

また、データの利用に関する無保証、免責については、地方公共団体がオープンデータとしてデータを公開するに当たっては、当該データの正確性、目的の達成などは保証しないこと、当該データを用いて行われた一切の行為に地方公共団体側は責任を負わないようにデータカタログサイト DATA. GO. JP の利用規約の無保証のような条項を契約上にいれる必要があるとされている（内閣官房 2017a: 57-59）。

第7条（無保証）

公表者は、本サイトで公開しているコンテンツの正確性、網羅性、特定の目的への適合性等について、一切保証しません。公表者は、本サイトで公開しているコンテンツを用いて行う一切の行為（それらを編集・加工等した情報を利用することを含む。）について、何ら責任を負うものではありません。公表者が、コンテンツにおいて、第三者に権利があることを表示・示唆している場合であっても、その表示・示唆は網羅的なものではありません。

（DATA GO JP 2021: 利用規約 第7条（無保証））

3.5.3 オープンデータの目的

オープンデータの目的について、内閣官房が公開している『オープンデータをはじめよう ―地方公共団体のための最初の手引書』によると、「国民参加・官民協働の推進を通じた諸課題の解決、経済活性化」、「行政の高度化・効率化」、「透明性・信頼の向上」（内閣官房 2017a: 16-19）としている。また、オープンデータを活用することによって、地域特有の課題が見つかり、市民が必要としているデータを活用した行政サービスが提供できることが期待されている（内閣官房 2016a: 2-3）。

3.5.4 オープンデータのビジネス

オープン&ビッグデータ活用・地方創生推進機構の『オープンデータ利活用ビジネス事例集』によると、オープンデータビジネスの特徴は、「付加価値型（市場のリーダー）」、「新価値創造型（スタートアップ）」、「プラットフォーム型（スタートアップ）」（オープン&ビッグデータ活用・地方創生推進機構 2016: 3-10）とされており、それぞれを取上げる。

3.5.4.1 付加価値型

付加価値型は、既存のビジネスに対して、オープンデータの価値を高めること型である。主に可視化などに用いられ、構造化データが原則のオープンデータでは、データの加工が発生しない方法である。ただし、オープンデータの利用制限は設けられていないため、競合も利用できることから、既存のビジネスによる市場の変動等は発生しないと考えられる（オープン&ビッグデータ活用・地方創生推進機構 2016: 3-10）。

3.5.4.2 新価値創造型

新価値創造型は、オープンデータを含む様々な分野を跨いだデータを活用し、その際に発生したアルゴリズムや分析モデルが価値を生み出す型である。データの価値が不確定の中、直接のビジネスに関係しない研究を行う事業会社は少なく、この方法は大学と協力して共同研究が行える事業会社が参画していることが多い。当該サービスではクラウドサービスが用いられるため、スタートアップが挑戦することもある（オープン&ビッグデータ活用・地方創生推進機構 2016: 3-10）。

3.5.4.3 プラットフォーム型

プラットフォーム型は、特定の領域のデータを大量に収集し、プラットフォーム化を行う型である。競合との差別化は、当該データを以下に利用者に利用しやすく提供することが重要になる。加えて、データの利用状況や利用者の状況の分析を行い、サービスを更新していくことで、さらに新しい価値を生み出すことができる手法である（オープン&ビッグデータ活用・地方創生推進機構 2016: 3-10）。

3.5.5 オープンデータの共創協調領域

オープンデータ化を行う阻害要因は少なく、現在、オープンデータ化が進ん

でいる。オープンデータは誰でも活用できるような公開データであるため、データそのものに対しては、図 3-16 のような対価などは発生しないため、オープンデータと分野を跨いだサービス（特に行政サービス）における儲け方の検討が重要になってくる。なお、オープンデータを活用したサービスはデータが無保証になる可能性があるため、当該データを活用したサービスも無保証にする必要があると思われる。

3.6 データの活用におけるビジネスを進めるためのポイント

本章では、データの活用におけるビジネス形態について検討するにあたり、データに関する競争領域、共創・協調領域の明確化する方法として、どのような性質のデータがあるのか（What）、どのようなデータの優先度が高いのか（What）、どのようにデータを流通・共有すべきか（How）、データ提供活性化のために、どのようなインセンティブを与えるべきか（How）という観点から、オープンデータとその他のデータに分けて調査を行った。データの種類については、どの観点で分類するかによってデータの種類が異なるうえ、各データの取扱いの方法が異なるため、扱うデータがどのデータの形式に当てはまるのかをきちんと把握する必要があることが分かった。また、データの管理方法によってもデータの種類が変わる可能性があるため、注意が必要である。

データの優先度や流通・共有方法に関しては、オープンデータのみを活用したサービスとオープンデータ以外のデータを活用したサービスでは、データの価値の基準が異なるため、比較は困難ではあるが、3.5.4 項で取上げたビジネスについて、図 3-4 に記載すると図 3-17 のとおりになる。今までは、付加価値創造型が主であったと思われるが、1.1.5 項で取上げたスーパーシティでは、新価値創造型やプラットフォーム型が重要になってくるのが読取れる。

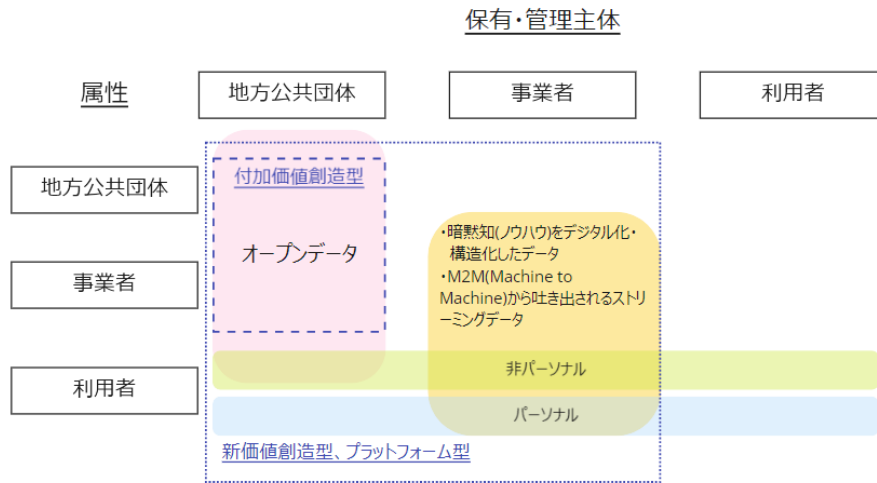


図 3-17 属性別データ種別とビジネス

また、データの流通方法およびインセンティブに関しては、オープンデータの場合とオープンデータ以外のデータでは元になるデータの価値が異なることにより、結果も異なる。しかし、図 3-17 で示したとおり、データそのものに対する対価ではなく、データを活用して提供できるサービスに対するインセンティブについては、オープンデータを活用したサービスとオープンデータ以外のデータを活用したサービスどちらも同じインセンティブとして提供することができると思われるため、オープンデータとオープンデータ以外のデータを掛け合わせたサービスを提供し、インセンティブを得ることは可能だと考えられる。

第4章 データ利活用に関する課題の整理

本章では、第3章で頭出しを行った「どのような環境・ルールを整備すべきか (How)」について検討を行う。データ活用におけるリスク検討について、情報処理推進機構でのリスクの検討方法を取上げつつ、データの活用に置き換えた場合のRCModelで取上げる構成要素について検討を行う。RCModelをデータの活用に置き換える際は、構成要素のうち、データを活用したサービスで足りないものはデータ活用に関するガイドラインから追加、不要なもの (AI特有のリスク検討の観点) は削除を行う方法で検討を行う。なお、データを活用した取引やサービスにおいては、「データ提供者 (利用者も含む)」、「データを活用したプラットフォーム」、「データを活用したサービス提供者」、「利用者」の観点から検討を行う。

4.1 データビジネスにおけるリスクの考え方

データを活用したビジネスにはリスクがあるが、すべてに対して対策を行うことやリスクを気にして事業を行わないこともリスクになる。そのため、妥当な選択ができるよう、情報処理推進機構では、データを活用したビジネスにおけるリスクマネジメントについて、次目のおり、7種類の方法を挙げている (情報処理推進機構 2020: 22-27)。

当該リスクマネジメントについて、リスク対策を行う際に検討素材にする。なお、リスクマネジメントを行う際は、以下の7種類を組合わせて行うことも効果的である場合もある。

4.1.1 リスク回避

リスク回避とは、リスクの可能性があると判断された際、当該リスクを避けるために事業活動を行わない、すなわちリスクを取らない行為である。この行為は次目以降のリスクに対する対抗策を行った場合でも、当該リスクが事業に多大な影響を与える可能性がある場合は選択すべき行為である。第2章の冒頭で扱ったIBMの顔認証の撤退の事例などが当てはまると思われる。

4.1.2 リスクテイク

リスクテイクとは、リスクが発生したとしても事業に多大な影響を与えるものではなく、リスクの中にも少しでも良い影響を与える場合は、この良い影響

を向上させる方向にしながら運用を行う行為である。良い影響、たとえば、何かしらの受託事業において、受託した場合は赤字になる可能性があるがノウハウがかなりたまる場合などが考えられる。

4.1.3 リスク源の除去

リスク源の除去とは、発生しえるリスクをなくすことを目的に行動することである。データの活用においては、特にパーソナルデータなどデータを保有することが漏洩など発生した時の事業リスクが高い一方で、当該データを保有していなければ活用することも難しいため、当該選択肢を取るべきか否かは慎重に検討する必要がある。

4.1.4 起こりやすさ（likelihood）の変更

起こりやすさの変更とは、リスクを事象が起きる可能性とリスクが起きた時の結果の二軸で評価を行い、事象が起きる可能性に対して対策を取り、リスクの発生を下げる行為である。

4.1.5 結果（consequence）の変更

結果の変更とは、上記4.1.4項で記載したとおり、リスクを事象が起きる可能性とリスクが起きた時の結果の二軸で評価を行った場合のリスクが起きた時の結果に対して対策を取る方法である。リスクが発生した際の被害を小さくするために対策を検討しておくことは重要である。

4.1.6 リスク共有（移転）

リスク共有とは、リスクが顕在化した場合に備え、保険や契約の定めなどの方法で起こりうるリスクに対する損失を補填する行為である。

4.1.7 リスク保有

リスク保有とは、リスクの検討や対応を行ったうえで、対応できていないリスクを特定し、あえて対策を取らずに様子見をするという行為である。特に軽微なリスクや通常起こりえないリスクに関して対応をとることは別のリスクを引き起こす可能性が十分あるため、リスク保有は重要な意思決定になりえる。

4.2 データを流通させるプラットフォームの構成要素

本節では、プラットフォームの事業者の立場から、RCModel で用いられているデータを流通させるプラットフォームの構成要素の検討を行う。

4.2.1 RCModel からの構成要素の検討

まず、表 2-7 の「AI を活用したシステムの構成要素（東京大学 2021: 別紙）」から「データを流通させるプラットフォームの構成要素」に置換える。AI を活用したシステムはデータを活用して AI を活用した分析などを行うため、データに置換えた場合であってもそのまま活用できる部分もあるため、AI 特有のリスクについて削除する。またコントロール例も AI 特有のものを削除すると表 4-1 のとおりである。

表 4-1 データを流通させるプラットフォームの構成要素の検討

構成要素	内容	主なコントロール例
AIモデル		
予測性能	十分な予測性能	予測性能の検証
汎化性能	特定の事例に偏ることが少ない判断	汎化性能の検証
頑健性	ノイズ等への耐性	敵対的事例の学習
解釈可能性	モデルの判断根拠	判断根拠情報の出力
データ		
データの品質	データの品質確保	教師ラベルづけの検証 ノイズの補正 特別データの分類（戦略商品等）
データのバランス	データの分布	十分な学習データの確保 データバイアスの検証
アプリケーション		
自動処理の正確性	補助的な自動処理	異常値の補正 異常判断（過検出等）のアラート
外部システムとの連携	外部システム等との連携	データの自動連携 プロトコルの定義・実装
システム実行環境		
システムの拡張性	利用環境の増加等へ対応できるシステム環境	複数モデルを実装する環境
システムの安定性	安定稼働するシステム環境	十分なパフォーマンスの確保 IoTのメンテナンス
機密性	機能や情報が保護されたシステム環境	システムの保護 アクセスコントロールの実装
可用性	必要な時に使用できるシステム環境	システム稼働時間の確保 異常時の代替機能への切替
検証可能性	AIサービスを事後検証できるための性質	実行履歴や判断根拠の保存 開発時の学習結果の記録

※（東京大学 2021: 別紙）から改変

次項にて、データを活用したビジネス特有の構成要素の検討を行う。

4.2.2 データ

データの取引を行う際に重要になるのは、取引対象となるデータの品質の確保である。本項では、データ品質に関するリスクについて取扱う。

4.2.2.1 データの品質

データの品質で懸念されている点として、過去に収集されたデータのうち、当時は価値があるデータになると想定されずに収集されているため、データ品質が統一されていないものが多くあるという点である。特にパーソナルデータに関しては、過去に同意を取得していないことも多く、活用できるか不明なデータも多くあると推測される。また、データの価値に関する認識がそれぞれ異なるため、活用の促進に影響を与えている（情報処理推進機構 2020: 29-31）。

一方で、特にリアルタイムデータなどは、陳腐化による外部的な要因からも

完璧な品質を保証することは難しいと考えられる。そのため、データ品質に関して、契約条項を定めて、リスクを軽減する手段をとるのが望ましいと思われる。契約条項の例として、データの正確性、完全性、安全性、有効性について保証を求める文言をデータ提供者に対してさだめることや欠損率の指標を設ける方法がある（情報処理推進機構 2020: 29-31）。なお、データの品質が悪く、当該データを使用したことによるシステム機器の故障、ビジネス機会の損失が発生し、特別損害を請求される可能性があるため、損害賠償の範囲を定めることも望ましいと思われる。

また、現在、偽情報の流通が活発化している。Gordon Pennycook の研究によると、利用者自身は SNS 上でニュースなどを共有する際は正確性を重視するのに対し、実際の実験では SNS 上で共有する際は正確性を重視しないという結果が出ている（Pennycook et al. 2021）。そのため、利用規約だけで対策が可能かどうかは検討を行う必要がある。

4.2.3 アプリケーション

アプリケーションについては、表 2-7 の内容を、データを流通させるプラットフォームの構成要素に置換えることによって大きな変更はないが、データ取引における懸念点があるため、本項にて取上げる。

4.2.3.1 外部システムとの連携

データを流通するプラットフォーム事業者になる場合、設計を行う際は、中立性の確保が重要となる。また、利用者が利用規約の定めを無視していないかの監視を行い、適切に取引が行われているか常に確認をすることが必要となる。この場合、利用規約がきちんと定められていることを前提とする（経済産業省 2020: 117）。

4.2.4 システムの実行環境

システムの実行環境を検討する際、検証可能性に関しては AI 特有のリスク観点のため削除を行ったが、データに関しては、信用性を上げるために証拠保全、パーソナルデータを扱う可能性のためのセキュリティを追加する。加えて、機密性に関しても本項にて取上げる。

4.2.4.1 機密性

データの管理を行うにあたり、機密性の観点から、経済産業省が公表してい

る『データ利活用のポイント集』によると「管理レベルの相違リスク」および「データ同士が混ざり合うリスク」（経済産業省 2020: 79）があるとされている。

前者は、データの所有者とデータの受領者間における管理方法の想定が不一致な状況を指す。図 3-3 に記載した秘密性の高いデータの法的保護の対象の情報を受領する場合は当該不一致を引き起こすと法的保護の対象になる可能性があるために事前確認が必要である。後者は、他社から受領したデータを含む既存に持っているデータと受領したデータが混在し、管理が届かなくなるリスクを指す。一方で、この場合の対策として、技術的に分散型のデータを管理する基盤の対策などがある（経済産業省 2020: 79）。

4.2.4.2 証拠保全

現在、不正アクセスなどによる第三者からの不正に取得されたデータが多く存在する。そのため、当該データを所持しているだけで、第三者から、不正に取得されたと疑われる可能性がある。疑われた際、当該データと自社が保有しているデータの同一性の証明を行うことは困難であると考えられる。そのため、トレーサビリティの確保やログの取得など証拠保全の運用が必要であると考えられている（経済産業省 2020: 98）。

4.2.4.3 セキュリティ

4.2.4.1 目でも扱ったとおり、データを活用したビジネスにおいて、データ消失などのセキュリティを確保するためには、分散管理などを活用するのが効果的といわれている。また、暗号化技術などを用いることも推奨されている。なお、セキュリティをうまく実現できなかった場合、利用者から信頼性を失う原因となる（総務省 2017a: 30-32）。

4.2.5 データ取得時の管理

データを取得する際には、法的観点などから注意しなければならない事項が発生するため、本項にて扱う。

4.2.5.1 法的保護

受領するデータが、3.1.2 項および 3.1.3 項で取り上げた著作権、営業秘密、限定提供データ、パーソナルデータに該当する場合は、法的保護を受ける必要があるまたは法律の定めのとおり扱う必要があるため、注意が必要である。また、これらの情報を管理する際は、当該データを管理できるよう利用規約、シ

システムの設計などが必要になる可能性もある。一方で、当該データを受領しない場合は、経済産業省では次の文言を利用規約などに入れるよう推奨している（経済産業省 2020: 83-84）。

X 条

- 1 提供者は、提供データが、適法かつ適切な方法によって取得されたものであり、第三者の知的財産権その他の権利を侵害していないこと、提供者が提供データに対する正当な権利を有することを保証する。
- 2 提供者は提供データに提供者の営業秘密及び限定提供データが含まれていないことを保証する。

（経済産業省 2020: 83-84）

また、パーソナルデータを受領しない場合は次の条項を追加することを推奨している（以下の条文の個人情報とは、本稿でのパーソナルデータを指す）。

X 条（提供データに個人情報等を含まない場合）

提供者は、提供データに個人情報の保護に関する法律に定める個人情報、匿名加工情報その他の個人に関する情報が含まれないことを保証する。

（経済産業省 2019: 110（提供データに個人情報等を含まない場合））

なお、パーソナルデータを受領する際は、

個人情報の保護に関する法律 第 15 条（利用目的の特定）、第 16 条（利用目的による制限）、第 17 条（適正な取得）、第 18 条（取得に際しての利用目的の通知等）、第 19 条（データ内容の正確性の確保等）、第 20 条（安全管理措置）、第 21 条（従業員の監督）および第 22 条（委託先の監督）に定められている運用を行わなければならない。また、個人情報の保護に関する法律 第 23 条（第三者提供の制限）、第 24 条（外国にある第三者への提供の制限）および第 25 条（第三者提供に係る記録の作成等）に定められている手続きなどが必要となる。そのため、データの提供者から意図しないパーソナルデータを受領を防ぐため、以下の条項を含めることも推奨されている（経済産業省 2020: 85-86）。

X 条（提供データに個人情報等を含む場合）

- 1 提供者は、本目的の遂行に際して、個人情報の保護に関する法律（以下「個人情報法」という）に定める個人情報又は匿名加工情報（以下「個人情報等」という）を含んだ提供データを取得者に提供する場合には、事前にその旨を明示する。
- 2 本目的の遂行に際して、提供者が個人情報等を含んだ提供データを

取得者に提供する場合には、その生成、取得及び提供等について、個人情報に定められている手続を履践していることを保証するものとする。

(経済産業省 2020: 85-86 (提供データに個人情報等を含む場合))

4.2.5.2 契約上の保護

すべてのデータ提供者とのデータのやり取りに際し、同じ契約条件で対応できれば良いが、現実、対応できない場合もある。契約条件のうち、秘密情報の定めおよび目的外利用の定めに関しては、差異があった場合にデータの管理の運用に大きな影響があると思われるため、本目にて取り上げる。

まず、秘密情報については、データ提供者との契約条件に含まれている可能性がある。大抵、契約上には秘密情報となる条件、許諾範囲、利用できる目的、秘密保持期間などの定めがあり、取引の内容によってその定めが異なる。そのため、秘密保持の規定がある場合は、受領するデータによって管理を変更する必要性が出てくる可能性がある、第三者に開示することが不可能なことがあるため、注意が必要である。また、受領したデータに対して利用目的の定めがある場合は、当該データを扱う利用者に対して、目的外利用をさせないようにしなければならなくなるため、契約上の定めについて十分に注意する必要がある (経済産業省 2020: 91-92, 106)。

4.2.5.3 権利の帰属

データを活用することによって、データの活用ににより、3.1.2.1 目や 3.1.2.2 目に該当する成果物が出来上がる可能性がある。当該データを活用して成果物が作成された際の権利の規定がない場合は、データを提供した側に権利の主張が難しくなる。仮にデータを取得するためにノウハウが必要といった場合、データ提供者にとってはデータを提供すること自体にリスクがあるため、データの提供元から将来、発生するかもしれない成果物への権利の主張をあらかじめ契約条件に入れ込んでくる可能性がある。また、データの提供者と当該データを活用してサービスを開発する事業者または個人は、プラットフォームを通じた取引場では、直接の契約関係にはならないため、クレームがプラットフォーム側に来る可能性がある。そのため、プラットフォームを提供する際は、データ提供者側と成果物の取り扱いについて整合する必要がある。また、表 3-1 の条件にも一部改変の禁止があるとおり、提供者側から提示される契約上、改変そのものが禁止されている場合もあるので注意が必要である (経済産業省 2020: 91-92, 111)。

4.2.5.4 独占禁止法

データの活用や収集に関しては、競争を促進する活動であると考えられているため、そのものの行為については不公正な取引であると認定される確率はかなり低いですが、たとえば、データを活用して発生した成果物に対して、権利をすべてデータ提供者側に譲渡することなどを条件に定めた場合は、競争を阻害する行為と認められる可能性がある（経済産業省 2020: 14-20）。

また、共同収集などを行った場合に競合のサービス内容、価格などを把握できてしまった場合は、競争を阻害する行為と認められる可能性もあるため、注意が必要である（経済産業省 2020: 82）。

4.2.5.5 データロックイン

現在、多くのパーソナルデータなどを保有し、データの活用においてサービスを提供しているプラットフォームが支配的地位の乱用として懸念されている（総務省 2017a: 30-32）。ドイツ連邦カルテル庁は Facebook に対してパーソナルデータを他のサービスに統合してサービス提供することを禁止した（公正取引委員会 2019）。これが、パーソナルデータだけでなく、現在、主流となっている M2M によるストリーミングデータを収集してサービスと統合しているサービスでも同様なことが行われる可能性がある。そのため、データロックインの状態にならないよう工夫が必要である。

4.2.5.6 責任の明確化

データの提供者と当該データを受領したい利用者とのやり取りに挟まるプラットフォームの事業者は、データの提供者と利用者それぞれの契約関係はあるものの、提供者と利用者間においては、直接の契約関係がない状態になる。そのため、提供者と利用者間でのトラブルが発生した場合、たとえばデータの品質が悪く、損害が発生した場合などのクレームを直接プラットフォーム側が受けることとなる（経済産業省 2020: 112）。そのため、責任の範囲を明確化し、契約上において、プラットフォームの事業者の免責を行うことが望ましいと思われる。

4.2.5.7 越境移転

データの取引は、輸出コストが低いこともあり、製品よりも国境を越えたやり取りが活発化している。一方で、各国では、自国で取得したデータ、自国民に関するデータなどに対して、規制を強化しているところもあり、輸出の禁止や当該データを管理する場合の定めなどデータの管理を強化しているところも

ある。また、GDPR では、関係諸国で違反していなくても適用される可能性もあるため、国境を超えるデータの取引を行う場合や規制の厳しい国のデータを扱う場合は注意が必要である（総務省 2017a: 64-65）。

また、法律を遵守して海外のサーバでパーソナルデータなどを管理していたとしても、炎上する可能性がある。たとえば、2021年3月17日付で発表されたLINEに登録されていたパーソナルデータが韓国や中国のデータサーバに保管されており、中国の企業からアクセスできていた件（谷井 2021）について、利用者に対しては利用規約にて法律で定められる範囲内で管理していたとされていたが、サービスの利用者からの反発もあり、日本のサーバでの対応に変更した（樋口 2021）。

なお、欧州では、米国が自国内の企業にて、米国に限らず管理しているデータの提供を求められることができる CLOUD Act が成立したこと（原田 2019）や Microsoft や Amazon Web Service などのクラウドサービスの依存度が高いことから、欧州独自のクラウドを構築する GAIA-X のプロジェクトを開始すると 2020年6月4日に発表した（Tung 2020）。GAIA-X には、Microsoft や AWS が参加しているものの、データ提供者のデータの主権、透明性および公正などが原則とされており、競争には当たらないとされている。また、GAIA-X に参加している企業は GDPR に準拠したサービスを提供する必要があるとされている（Schimrozik 2020）。そのため、今後、欧州にてクラウドを活用したデータを扱ったサービスを提供する場合は、GAIA-X を利用することを促される可能性があるため、法律の観点やクラウドの推奨など国を跨ぐ場合は注意が必要である。

上記から、法律だけを遵守してもハレーションが発生する可能性があるため、利用者目線でのリスク分析も必要である。

4.2.5.8 利用期間

データの提供は継続的に提供を受ける場合がある。その際、データの提供元がデータの提供できなくなるリスクを検討する必要がある。特に注意が必要なのは、データの提供元が買収されたときを想定し、契約の解除権や買収の際の通知義務など、利用規約に盛り込む必要があると考えられる（経済産業省 2020: 89-90）。

ただし、分散管理の場合は、プラットフォーム上でデータを保有しているものを除き、データ提供者側での利用期間の定めは不要ではあるが、受領者側に対し、データが提供できうる可能性も踏まえて、利用規約に免責条項などを追

加するのが望ましいと思われる。

4.2.6 データを流通させるプラットフォームの構成要素案

データを流通させるプラットフォームの構成要素について、前項で取上げた結果、表 4-2 で青字および下線にて記載したものがデータを活用したビジネスにおいて、重要なリスクの検討要素になると考えられる。全体的に利用規約の定めがかなり重要になると思われるが、越境移転など、リスクテイクやリスク保有では事業が立ち行かないものもある（表 R 欄の●）ため、4.1 節で取上げたリスクの考え方から優先順位を検討する必要があるとも思われる。

表 4-2 データを流通させるプラットフォームの構成要素案

構成要素	内容	主なコントロール例	R
データ			
データの品質	データの品質確保	データの価値評価基準の設定 利用規約の定め（損害賠償） 利用規約の定め（免責） 特別データの分類（戦略商品等）	
データのバランス	データの分布	データバイアスの検証	
アプリケーション			
自動処理の正確性	補助的な自動処理	異常値の補正 異常判断（過検出等）のアラート	
外部システムとの連携	外部システム等との連携	データの自動連携 プロトコルの定義・実装 定期的な監査	
システム実行環境			
システムの拡張性	利用環境の増加等へ対応できるシステム環境	複数モデルを実装する環境	
システムの安定性	安定稼働するシステム環境	十分なパフォーマンスの確保 IoTのメンテナンス	
機密性	機能や情報が保護されたシステム環境	システムの保護 アクセスコントロールの実装 分散管理	
可用性	必要な時に使用できるシステム環境	システム稼働時間の確保 異常時の代替機能への切替	
証拠保全	証拠保全ができる環境	定期的なログ取得 電子署名	
セキュリティ	第三者からもセキュリティがしっかりしていると見える環境	分散管理 暗号化技術	
データ取得時の管理			
法的保護	著作権，営業秘密，限定提供データ，パーソナルデータの管理	利用規約の定め（データの管理方法の定め） システム設計/分散管理	●
契約上の保護	契約条件での運用管理	利用規約の定め（秘密情報，利用目的） システム設計/分散管理	●
権利の帰属	知的財産権に関する利用条件の明確化	利用規約の定め（知的財産権）	●
独占禁止法	公正なデータの取引ができる運用	利用規約の定め（知的財産権，解除権）	
データロックイン	1つの企業が多くのデータを囲い込まない仕組み	分散管理	
責任の明確化	契約条件での責任の明確化	利用規約の定め（責任，免責）	●
越境移転	各国の法令遵守ができるデータ管理	法令調査	●
利用期間	継続的なデータ取得の管理	利用規約の定め（利用期間の定め，解除権）	

※（東京大学 2021: 別紙）から改変

4.3 データを活用したサービス提供者の構成要素

本節では、サービス提供者の立場から、RCModel で用いられているデータを活用したサービス提供者の構成要素の検討を行う。

4.3.1 RCMModel からの構成要素の検討

まず、データを活用したサービス提供者の構成要素を検討するにあたり、表 2-8 の「サービスの提供者の構成要素（東京大学 2021: 別紙）」から「データを活用したサービス提供者の構成要素の検討」に置換える。AI を活用したサービスは前節と同様、データを活用して AI を活用した分析などを行うため、データに置換えた場合であってもそのまま活用できる部分もあるため、AI 特有のリスクについて削除する。またコントロール例も同様な対応を行い、AI 特有のものを削除、修正（青字および下線）を行うと表 4-3 のとおり。

表 4-3 データを活用したサービス提供者の構成要素の検討

構成要素	内容	主なコントロール例
倫理規範		
アカウントビリティ	説明責任, 利用者の保護	責任関係の明確化 適切な期待値の検討
尊厳や権利の尊重	利用者側の優先権の検討	人間の介在度合の定義
公平性	サービス全体での公平性	公平性を確保する項目の定義
プライバシー	個人情報の適切な管理	プライバシーポリシーの遵守
透明性	データを活用した AI -サービスに係る必要な情報の開示	ステークホルダーごとに開示すべき情報の整理
運用		
サービスの拡張性	利用環境の増加等へ対応できるサービス体制	サービス提供に十分な体制 必要な言語へのサポート
サービスの持続可能性	持続的なサービスの維持	サービス要件の見直し 再学習・継続学習
サービスの機動性	適時の対応	アジャイル開発の実施
安全性	サービス全体での安全性の確保	システム外の安全対策 利用者の不正利用への対処
アクセス管理	適切なシステムの利用権限・範囲の管理	適切なアクセス権限の設定 不正な利用者の制限
監査可能性	第三者を含む必要な監視	データの連携・管理 AI-システムのモニタリング トラブル発生時の検証 不正利用の監視
コミュニケーション		
利用者との合意	利用者との認識合わせ	利用者責任の合意 データの連携・管理 AI-システムの変更への合意
使いやすさ	データを活用した AI -サービスの使いやすさ	使いやすい UI
分かりやすさ	データを活用した AI -サービスが出力する情報の分かりやすさ	データの検索が判断根拠の分かりやすい表現
関係者との連携	利用者に対するリモートでのサポート	利用者のリモート支援 専門家との連携

※（東京大学 2021: 別紙）から改変

上記から、4.2.1 項とは異なり、AI 特有のリスクでの構成要素の削除はないと思われる。なお、次項にて、データを活用したビジネス特有の構成要素の検討を行う。

4.3.2 倫理規範

構成要素の倫理規範については、表 2-8 の内容を、データを活用したサービス提供者の構成要素に置換えることによって大きな変更はないが、追加でデータを活用する際の関連法令について懸念点があるため、本項にて取上げる。

4.3.2.1 関連法令

前章で取上げたとおり、将来、分野を跨いだデータを活用し、サービスを提供されることが想定される。一方で、図 4-1 のとおり、分野ごとに異なる課題があるため、データに関する関連法令が定められていることがある（総務省 2017a: 30）。今までは提供している特定の製品・サービスに対しての関連法令について周知徹底を行っていただければよかったものの、分野を跨ぐ場合は、跨ぐ先の関連法令も把握する必要がある。また、分野を跨いだ活用を行ったことにより、想定しなかった法令に違反してしまうことが発生する可能性があり、変化も激しいため、常に最新の情報を入れておく必要がある。

産業	利活用例のイメージ	収集媒体	収集データ	主な課題の例	個人情報関係	対称特定	主な関係法令等
製造業	スマート工場による生産性向上やコスト削減等のためのデータ収集	工作機械 産業ロボット センサ等	機能状況(異常検知等) 環境情報等	・機械の所有者(リース元等)との法律関係	なし	○	民法 (事業者間の契約)
農業	農業の生産性向上のための気象データ等の観測	IoT環境センサ (温度計、湿度計等)	温度、湿度、照度等の環境データ、生育データ等	・センサ設置場所の所有者(農家等)との法律関係	なし	○	民法 (事業者・農家間の契約)
金融保険業	自動車損害保険における最適な保険商品提供のためのデータ収集	自動車、車載センサ等	走行データ(速度、ルート)等	・専用機器を取り付けて、走行することに同意した者との法律関係	△(※事業者と協力者(個人)間の契約の場合は以下と同様)	○	民法 (事業者間、事業者と協力者(個人)間の契約)
健康産業 (ヘルスケア)	ヘルスケアサービスのための体調データ収集	ウェアラブル機器	歩数、活動量、脈拍、体温等	・サービス契約の際の利用目的、第三者提供等の条件 ・診療情報、投資情報や、要配慮個人情報(病歴等)との関係	○(※目的の明示、第三者提供の際の同意等が必要)	○	個人情報保護法 民法 (事業者・消費者間の契約(サービス約款等を含む)) 消費者契約法等
サービス	スマートハウス(省エネ、見守り)における家電制御のためのデータ収集	センサ付家電	家電の使用データ、消費電力データ等	・サービス契約の際の利用目的、第三者提供等の条件		○	
広告宣伝・小売・観光	広告宣伝・小売・観光等における、嗜好・需要に合わせた最適なサービス提供のためのデータ収集	ICカード スマートフォン等	購買データ、位置情報等			△(特定多数)	
自動運転関連	自動運転のための、公道での撮影データ収集	カメラ	画像データ等	・不特定多数の個人情報(顔画像等)や、著作物の画像が含まれる可能性		不特定多数	個人情報保護法 著作権法

図 4-1 データの活用に関する関連法令（総務省 2017a: 30）

4.3.3 コミュニケーション

構成要素のコミュニケーションについても、表 2-8 の内容を、データを活用したサービス提供者の構成要素に置換えることによって大きな変更はないが、

追加の構成要素を検討する。

4.3.3.1 利用者との合意

現在、多くのサービスにおいて、複雑化かつ多種多様な利用規約など同意が求められている。しかし、すべての利用規約に目を通すどころか、利用者による同意疲れが発生している。トラブルになってから初めて読むケースも発生しており、肝心のリスクを理解した利用者への利用ができていない状態であるため（総務省 d, 2020: 12）、有効な同意の取得やその際の説明の方法について工夫する必要がある。

4.3.3.2 意識変革

4.2.5.7 目で取上げた LINE の事例のように、データの提供者となりつつある利用者側にとってデータに対する不安はかなり大きいものであると予想される。内閣官房によると、利用者側にとって「自らのデータを把握・制御できない不安」と「便益が実感できないことによる漠然とした不安」（内閣官房 2016b: 6）があるとされている。一方で、データを活用したサービスの提供者側として持っている懸念は、インシデント発生によるハレーションの高さからの「データ活用への躊躇」、 「API 開放・データ互換性確保等の技術的課題」（内閣官房 2016b: 6）といったものでそもそも利用者側の懸念とサービス事業者側の懸念が一致していないのが現状である。

そのため、サービス事業者側は、利用者の懸念を払しょくできるようデータを活用したメリットの提示や制御できるような仕組みを提供する必要がある。

4.3.4 データを活用したサービス提供者の構成要素案

データを活用したサービス提供者の構成要素について、前項で取上げた結果、表 4-4 で青字および下線にて記載したものがデータを活用したビジネスにおいて、重要なリスクの検討要素になると考えられる。4.2.6 項で取り上げた構成要素案よりも利用者に対する説明責任などの方が重要視されているが、対応策として、リスクテイクやリスク保有では事業が立ち行かないものもあった（表 R 欄の●）。

表 4-4 データを活用したサービス提供者の構成要素案

構成要素	内容	主なコントロール例	R
倫理規範			
アカウントビリティ	説明責任, 利用者の保護	責任関係の明確化 適切な期待値の検討	
尊厳や権利の尊重	利用者側の優先権の検討	人間の介在度合の定義	
公平性	サービス全体での公平性	公平性を確保する項目の定義	
プライバシー	個人情報の適切な管理	プライバシーポリシーの遵守	
透明性	データを活用した AI サービスに係る必要な情報の開示	ステークホルダーごとに開示すべき情報の整理	
関連法令	各分野に係る関連法令の厳守	定期的な関連法令の調査	●
運用			
サービスの拡張性	利用環境の増加等へ対応できるサービス体制	サービス提供に十分な体制 必要な言語へのサポート	
サービスの持続可能性	持続的なサービスの維持	サービス要件の見直し	
サービスの機動性	適時の対応	アジャイル開発の実施	
安全性	サービス全体での安全性の確保	システム外の安全対策 利用者の不正利用への対処	
アクセス管理	適切なシステムの利用権限・範囲の管理	適切なアクセス権限の設定 不正な利用者の制限	
監査可能性	第三者を含む必要な監視	データの連携・管理 AI システムのモニタリング トラブル発生時の検証 不正利用の監視	
コミュニケーション			
利用者との合意	利用者との認識合わせ	利用者責任の合意 データの連携・管理 AI システムの変更への合意 合意取得の工夫	
使いやすさ	データを活用した AI サービスの使いやすさ	使いやすい UI	
分かりやすさ	データを活用した AI サービスが出力する情報の分かりやすさ	判断根拠の分かりやすい表現	
意識変革	利用者に対する説明責任	データを活用したメリットの説明 データの管理方法の明示	
関係者との連携	利用者に対するリモートでのサポート	利用者のリモート支援 専門家との連携	

※（東京大学 2021: 別紙）から改変

4.4 利用者の構成要素

本節では、利用者の立場から、RCModel で用いられているデータを活用したサービスの利用者の検討を行う。なお、当該利用者には、データの提供者またはデータを提供する行為は含まないものとする（次節で扱うため）。

4.4.1 RCMModel からの構成要素の検討

まず、表 2-9 の「ユーザの構成要素（東京大学 2021: 別紙）」から「データを活用したサービスの利用者の構成要素」に置換える。AI を活用したシステムはデータを活用して AI を活用した分析などを行うため、データに置換えた場合であってもそのまま活用できる部分もあるため、AI 特有のリスクについて削除する。またコントロール例も AI 特有のものを削除、修正（青字および下線）すると表 4-5 のとおりである。

表 4-5 データを活用したサービスの利用者の構成要素の検討および案

構成要素	内容	主なコントロールの例
理解		
利用者の責任	利用者責任の理解	利用者責任の合意（最終判断等） <u>データの管理を行う AI</u> システムの変更への合意
利用者の自律性	自律的に判断すべき内容の理解	<u>偽情報の排除 AI</u> の判断の訂正
サービスの期待値	<u>データを活用した AI</u> サービスに対する期待精度の理解	期待値（予測精度等）の理解 ネガティブな判断傾向の理解
影響の把握	利用者への影響の把握	<u>データを活用した AI</u> サービスに係るリスクの理解 ワークスタイルの変化の理解
利用環境		
利用者の能力	サービス利用において必要な知識・スキルの習得	必要なリテラシーの確保 利用者の教育
<u>データ利活用 AI</u> の存在の認識	<u>データ利活用 AI</u> の存在の認識	<u>データ利活用 AI</u> の存在の明示 利用者への通知
制御可能性	利用者側での制御	マニュアル手続の整備 <u>AI 判断の訂正機能</u>
利用者への制限	不正利用等の防止に向けた利用者の制限	利用者への技術的な制限 法的な制約
行動		
適正利用	正しいサービス利用	適切な目的に沿うサービス利用 <u>教師レベルの正しい設定</u>
自己防御	利用者自身の保護	不利益が発生した際のクレーム 環境変化に係る事前連携

※（東京大学 2021: 別紙）から改変

なお、「データを活用したサービスの利用者の構成要素」については、表 4-5 に記載している内容を超えての記載はない。

4.5 データ提供者の構成要素

データの提供には、提供を行った金銭の対価だけでなく、3.4 節で扱ったインセンティブを受領するパターンもある。そこで、本節では、データの提供者の立場から、RCModel で用いるべき、「データ提供者の構成要素」の検討を行う。なお、RCModel には、データの提供者の立場の代わりになる構成要素がない

め、他の構成要素を参考に検討を行う。

4.5.1 データ

提供するデータに対して、4.2.2.1 目で取上げたとおり、データ提供者側にデータの品質が求められる可能性がある。そのため、次目ではデータの品質を上げる。

4.5.1.1 データの品質

データを提供する場合、4.2.2.1 目で取上げたとおり、受領者側からデータの正確性などの担保が求められる可能性がある。仮に正確性などが担保できないようなデータである場合は、正確性を保証しない旨の条件を交渉する必要がある。一方で全く正確性などを保証しない場合は、データ受領者側からデータの提供を断られる可能性があるため、保証可能な範囲まで保証することや欠損率をあらかじめ定めておくという方法もある（経済産業省 2020: 57-58）。

また偽情報に対して、データの品質を上げるために差し替えが可能な形でデータの提供を行うのが望ましいとも考えられる。

4.5.2 データ提供時の管理

4.2.5 項で取上げた事項と同じリスクが発生するため、構成要素は似ているものの、対応策が 4.2.5 項とは異なるため、本稿においても取上げる。

4.5.2.1 データ漏洩

データを提供した際の提供者側のリスクとして、価値のあるデータの場合、第三者に漏洩することによってデータの価値が下がる可能性があるうえ、法的保護の対象外にもなる可能性があるリスクが高い事象である。一方で、データ漏洩に関しては、データ提供者側で当該データの管理を行うわけではないため、提供者側としてもデータ漏洩のリスクを検討しておく必要がある。対策としては、提供の契約条件に第三者提供の禁止を盛り込む、データの管理方法をあらかじめ定める、データの管理状況を確認できるよう監査の条件を入れる、データが漏洩した場合の差し止めや損害賠償条項を盛り込む、契約終了後のデータ破棄を求めるなどである（経済産業省 2020: 38-41）。また、データを提供する場合のシステムの設計において、アクセス権や 4.2.4.2 目で取上げた証拠保全といった方法がある。

4.5.2.2 法的保護

データを提供する際、4.2.5.1 目と同様、当該データに営業秘密、著作権、限定提供データなど法的保護を受けるデータが含まれる可能性がある。データ提供者側がそれぞれに対して法的保護を受けたいか否か、また、含まれるようなデータは提供しないなど、判断によって対応は異なるが、データ受領者側から提示された条件によっては開示を行なうべきではないと判断する必要があるうえ、法的保護を受ける場合は則した管理を求める必要がある。特に限定提供データの場合は、オープンデータ化が行われた場合は法的保護が受けられなくなるため、データを提供する際は確認が必要である（経済産業省 2020: 61-63）。

なお、個人情報については、提供する際に

個人情報の保護に関する法律 第 23 条（第三者提供の制限）第 1 項に該当する場合は、本人の同意取得が必要なため（除外あり）、提供する際に該当するデータがある場合は注意が必要である（経済産業省 2020: 65-67）。

4.5.2.3 契約上の保護

提供するデータのうち、第三者から受領したデータがある場合は注意が必要である。当該第三者との契約にて、秘密情報として扱わなければならない場合、第三者提供が禁止されている場合、目的外利用が認められていない場合などがあるためである。

一方で、提供したデータが想定していない利用がされた場合において、提供側が不利益を被る場合は、目的外利用の禁止、データの利用報告、損害賠償および差し止め請求、データ修了時の廃棄などの条件を契約に盛り込む対策などを検討する必要がある（経済産業省 2020: 44-46）。

4.5.2.4 権利の帰属

4.2.5.3 目でも記載したとおり、提供したデータを活用して、3.1.2.1 目や 3.1.2.2 目に該当する成果物が出来上がる可能性がある。提供先が当該権利を主張した場合は、成果物を作成した場合を想定して、権利の帰属についてあらかじめ検討し、提供前に提供条件の合意を取る必要がある（経済産業省 2020: 60）。たとえば、当該データを活用して権利が発生している成果物に対して、無償での許諾などの条件を盛り込むなど方法は様々である（経済産業省 2020: 49-50）。ただし、改変禁止など権利を主張してしまうと、受領先が加工データなどを作成できず、データを活用できなくなる可能性もあるため注意が必要である。また、著作権などの帰属について注意が必要である。公正取引委員会では、「改

良技術の譲渡義務・独占的ライセンス義務」について以下の定めがある。

(8) 改良技術の譲渡義務・独占的ライセンス義務

- (ア)ライセンサーがライセンシーに対し、ライセンシーが開発した改良技術について、ライセンサー又はライセンサーの指定する事業者はその権利を帰属させる義務、又はライセンサーに独占的ライセンスをする義務を課す行為は、技術市場又は製品市場におけるライセンサーの地位を強化し、また、ライセンシーに改良技術を利用させないことによりライセンシーの研究開発意欲を損なうものであり、また、通常、このような制限を課す合理的理由があるとは認められないので、原則として不公正な取引方法に該当する(公正取引委員会 2007; 知的財産の利用に関する独占禁止法上の指針 (8) 改良技術の譲渡義務・独占的ライセンス義務 ア)

上記は、データの活用を想定して定められたものではないと思われるが、権利主張を厳しくし、研究意欲をなくすような条件の場合は、行為自体が認められない場合があるため、注意が必要である。

4.5.2.5 利用期間

4.2.5.8 目で記載したとおり、経済産業省では、データの提供側としても契約が終了後、データが使用されてしまうリスクを避けるために利用期間の定めをデータ提供者としてもきちんと入れることを推奨されている。加えて、提供先が買収されたとしても契約解除できるような条件を追加するのも望ましいとされている(経済産業省 2020: 71-72)。

4.5.3 データ提供者の構成要素案

データ提供者の構成要素案について、前項で取上げた結果、表 4-6 にて記載したものがデータを活用したビジネスにおいて、重要なリスクの検討要素になると考えられる。表 4-2 で扱った構成要素がほとんどでかつ、全体的に利用規約の定めがかなり重要になると思われるが、法的保護などリスクテイクやリスク保有では事業が立ち行かないものもある(表 R 欄の●)ため、4.1 節で取上げたリスクの考え方から優先順位を検討する必要があるとも思われる。なお、本検討では、データ提供者は RCMoDel には含まれていない視点のため、青文字で記載している。

表 4-6 データ提供者の構成要素案

構成要素	内容	主なコントロールの例	R
<u>データ</u>			
<u>データの品質</u>	<u>データの品質確保</u>	<u>利用規約の定め（正確性・無保証）</u> <u>データの差替え</u>	
<u>データ提供時の管理</u>			
<u>データ漏洩</u>	<u>データが漏洩しない仕組み</u>	<u>証拠保全</u> <u>利用規約の定め（損害賠償）</u> <u>利用規約の定め（第三者提供禁止）</u>	
<u>法的保護</u>	<u>著作権，営業秘密，限定提供データ，パーソナルデータの管理</u>	<u>利用規約の定め（データの管理方法の定め）</u>	●
<u>契約上の保護</u>	<u>契約条件での運用管理</u>	<u>利用規約の定め（秘密情報，利用目的）</u>	●
<u>権利の帰属</u>	<u>知的財産権に関する利用条件の明確化</u>	<u>利用規約の定め（知的財産権）</u>	●
<u>利用期間</u>	<u>継続的なデータ取得の管理</u>	<u>利用規約の定め（利用期間の定め，解除権）</u>	

4.6 RCMoDel 案

前節の結果から RCMoDel に入れ込むと図 4-2 のとおりになる。なお，データを流通させるプラットフォームの構成要素をプラットフォーム，データを活用したサービス提供者の構成要素をサービス提供者，利用者の構成要素を利用者，データ提供者の構成要素をデータ提供者とする。図 2-5 の RCMoDel 上，サービス提供者の中に AI システムが含まれているため，図 4-2 でもサービス提供者の中にプラットフォームが含まれている形にしている。加えてデータ提供者の構成要素がプラットフォームと同様のため，プラットフォーム内にデータ提供者を含む形にしている。なお，グレーの構成要素は，リスクテイクやリスク保有では対応が難しい構成要素である。また，図 4-2 での青字部分は，図 2-5 から追加した構成要素である。

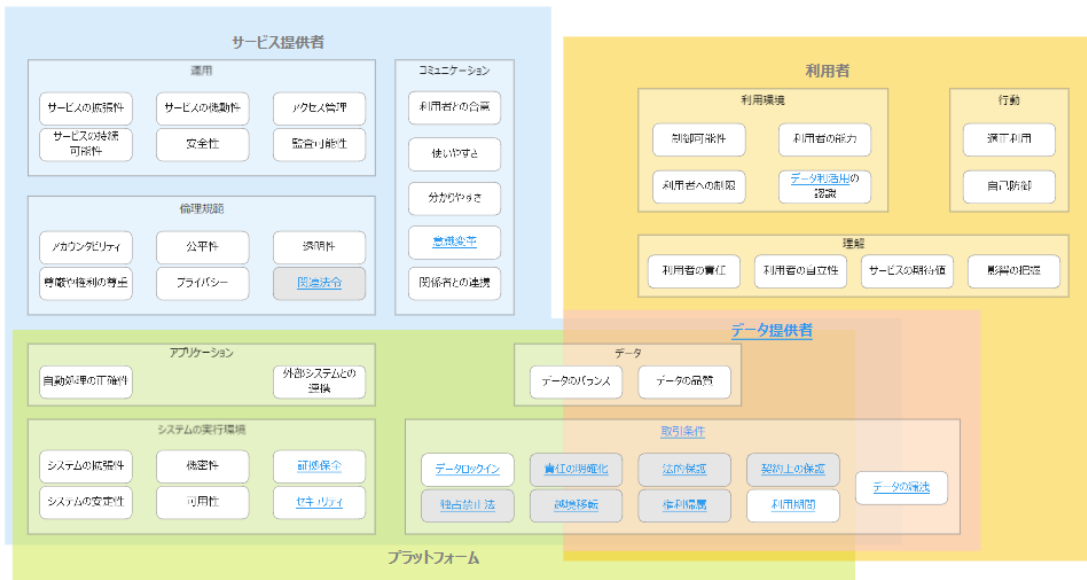


図 4-2 データを活用したビジネスの RCM Model

※（東京大学 2021: 別紙）から改変

第5章 データを活用するための検討項目の提示

本章では、前章で作成した RCModel を実際に活用して、様々な種類や性質が異なるデータを活用したサービスを提供する際のリスクについて明確化する。また、データを活用したビジネスにおける RCModel の最適な方法を検討する。様々な種類や性質のデータを活用した事例として、内閣府が公表している『「スーパーシティ」構想について』に記載されている構想を活用する。当該構想では、パーソナルデータ、オープンデータ等、異なる種類のデータを活用したサービス提供が想定されている。

5.1 RCModel を用いた検討（A市の構想）

本節では、内閣府がスーパーシティのビジネス案として公開している「後期高齢者の通院対策を図る A市の構想」（内閣府 2021: 24）を RCModel の対象にする。構想の詳細は図 5-1 のとおり。

後期高齢者の通院対策を図るA市の構想



- A市では、免許を返納した後期高齢者が急増。減少するタクシーとその料金の高さから、通院を断念する高齢者の増加も予想されている。
- このため、①高齢者の通院等の交通手段として、市民の車等も活用したボランティア・タクシー事業を、タクシー事業者自ら廉価に展開。その支払手段として、ボランティア活動によってポイントが貯まり、市からも個別に補助を行える地域電子通貨を発行。その他の行政サービスの支払いや地域貢献活動なども広く連携。
- 加えて、②通院予約や遠隔医療を積極的に活用した地域包括ケアなどとボランティア・タクシーの配車システムを連動させ、高齢者の適切な通院などを通じた社会保障費の抑制や地域交通の合理化を図る。

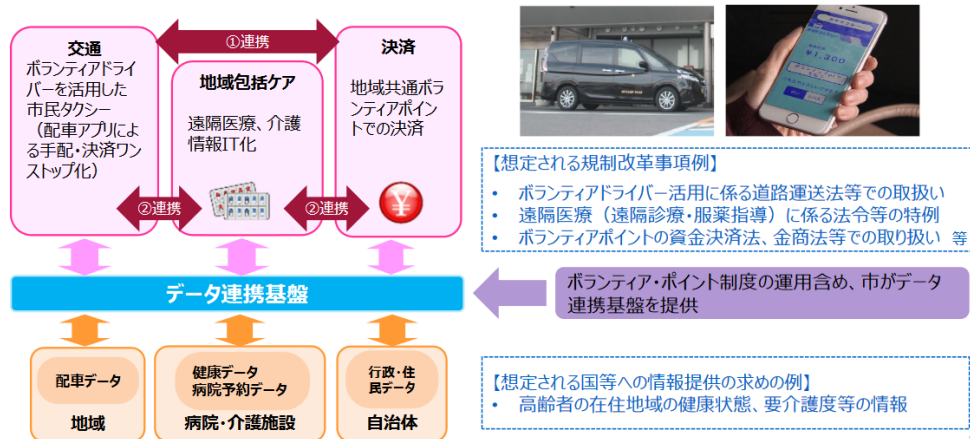


図 5-1 A市の構想（内閣府 2021: 24）

5.1.1 A 市のリスクシナリオ

A 市での実現すべき価値・目的は、図 5-1 から、①「市民の車なども活用したボランティア・タクシー事業」の実現、②地域電子通貨のポイントによる決済、③「高齢者の適切な通院」管理（内閣府 2021: 24）と仮置きする。文面からは目的の優先順位が読取れないため、今回は、記載されている順番で検討を行う。なお、表 5-1 は図 5-1 のみの情報から推測し検討したものであり、現実の課題とは異なる可能性がある。

表 5-1 A市でのリスクシナリオ（例）

実現すべき課題と目的		サービス要件	リスクシナリオ	
1	市民の車なども活用したボランティア・タクシー事業	マッチング機能（データの連携）	関連法令	関連法令の抵触によりサービスが提供できないリスク
			公平性，データ品質，監査可能性，適正利用	偽情報により，マッチングがうまくいかないリスク
			外部システムとの連携	データの連携がうまくいかないことによるサービスが提供できないリスク
		個人情報管理	データ品質	個人情報の更新がされずにサービスが提供できないリスク
			データの漏洩	個人情報の漏洩リスク
2	地域電子通貨のポイントによる決済	決済システム	関連法令	関連法令の抵触で決済の対応ができないリスク
		決済と個人情報の連携	外部システムとの連携	決済情報と個人情報が紐づかないリスク
			セキュリティ，証拠保全，適正利用，アクセス管理	なりすましのリスク
地域の商品・サービス連携	データ品質	変動が激しい商品・サービス情報と連携がいかないリスク		
3	高齢者の適切な通院管理	医療データとの連携	関連法令	関連法令の抵触によりサービスが提供できないリスク
			利用者との合意	医療データの同意管理（特に第三者提供）ができないリスク
			契約上の保護	病院側のデータの利用条件との不一致
		外部システムとの連携	医療機関同士のデータ連携ができないときのリスク	
		（利用者に対しての）分かりやすさ，UI	利用者の能力	サービスが存在しても利用されないリスク
			意識変革	医療情報が使われることへの抵抗リスク
分かりやすさ，サービスの期待値	利用者側との期待値の不一致			

今回は，図 5-1 の情報から抽出したが，経験値とどこまでをリスクとして捉えるかという点は人によって異なるため，本件も確認する人によって異なる可能性は大いにある。

5.1.2 A市のRCModel

表 5-1 から，既存のRCModelをもとに顕在化するリスクを検討しながら図 4-2 に線を引こうとしたが，ビジネスの視点，技術の視点，ユーザの視点等，それ

それぞれの視点において、リスクの顕在化が異なるため、本件では、表 5-1 で取上げた順番で線を引くこととする。図 4-2 に線を引くと図 5-2 のとおりとなった。なお、線が見にくいので 1 の目的は赤、2 の目的は青、3 の目的は紫としている。優先順位を確認する方法としては矢印がお互い重なりすぎて見にくいものの、関連法令や外部システムとの連携、データ品質など、リスクとして何を重要視して、検討しなければならないかということが可視化されたと思われる。

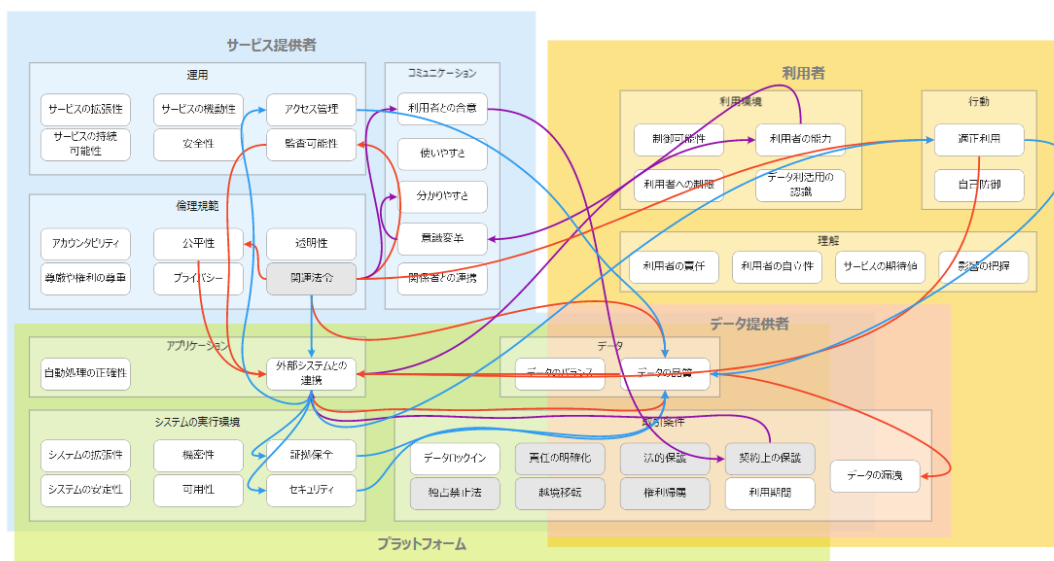


図 5-2 A 市の RCM model (例)

5.1.3 A 市のコントロールの内容

今回は目的別ではなく、図 5-2 での矢印が多い順でコントロールを記載した(表 5-2)。本件は、利用者がデータ提供者にもなりえるが、データ提供者のみも存在するため、別枠で記載している。本件では、リスクシナリオの優先順位ではなく、矢印の多いものを重視して列挙している。データ取引におけるリスクを検討する際は、RCModel にて、可視化して、矢印が多いものを重視すべき事項として取上げる方が RCM model を有効に扱えるのではないかとと思われる。

表 5-2 A 市のコントロールの内容（例）

コントロールの内容（例）			
プラットフォーム	サービス提供者	利用者	データ提供者
【外部システムとの連携】 定期的な監査 【データ品質】 定期的な更新 【証拠保全】 ログなどの保存 【セキュリティ】 関連省庁が提示しているセキュリティ要件を達成する 【契約上の保証】 提供者が不利にならないかつ第三者提供、改変等ができる条件を提示	【関連法令】 定期的な法令調査 【アクセス管理】 ログなどの保存 【公平性】 利用規約の定め 【監視可能性】 利用規約の定め 【意識変革】 データに対する透明性を明示 【分かりやすさ】 利用者に合わせて使用方法の提示 【利用者との合意】 合意事項の整理	【適正利用】 利用規約の定め 【利用者の能力】 説明要員の派遣 --データ提供者参照	【データ品質】 定期的な更新 【契約上の保証】 データの受領者側から出た利用規約の確認 【データの漏洩】 利用規約の定め

5.1.4 RCMModel の課題

本節では、A 市の事例を検討したが、リスクシナリオは検討する人によってかなり異なるリスクが出る可能性がでること、リスクを検討する立場によって顕在化の観点が異なることが課題となった。一方で立場ごとに検討するのは、工数がかかるうえ、リスク回避の対策が乖離する可能性がある。そのため、様々な種類のデータを活用したサービスにおいては、特定の立場ではなく、案件全体でどのリスクを先に検討すべきか優先順位を明確にすることが重要であると思われる。また、データのビジネスにおいてリスクを検討する際は、データの流れを把握する必要があるが、図 5-2 からは、読み取りにくいのが現状である。

上記の課題の解決策として、検討の優先順位を明確にするために、矢印の数に重点を置くこととし、リスクシナリオを表 5-1 よりも細分化して検討することとする。また、可視化するにあたり、リスクが顕在化する優先度において構成要素に対して線をひいていたが、データの流れを理解するために、データ提供者→プラットフォーム→サービス提供者→利用者の順に明記し、リスクシナリオ 1 つに対して複数の構成要素を検討することとする。

そのため、次節の B 市の事例では、上記の方法を用いて検討を行う。

5.2 RCMModel を用いた検討（B 市の構想）

本節では、内閣府がスーパーシティのビジネス案として公開している「観光

を起点とする B 市のスーパーシティ構想」(内閣府 2021: 25) を RCMoel の対象にする。構想の詳細は図 5-3 のとおり。



図 5-3 B 市の構想 (内閣府 2021: 25)

5.2.1 B 市のリスクシナリオの検討方法

B 市での実現すべき価値・目的は、図 5-3 から、①「MaaS によるものづくりツーリズム」の実現、② 個人認証 (生体認証を含む) を活用した「域内完全キャッシュレス」の提供、③ 貸与のヘルスケアウェアブル端末を活用した「健康管理やキャッシュレス」に実現 (内閣府 2021: 25) と仮置きする。文面からは目的の優先順位が読取れないため、今回は、記載されている順番が目的の高い順であると仮定して検討を行う。表 5-1 では、上位層にあるものが重要度の高いものとしていたが、今回は、検討する人によってリスクシナリオの数が変わる可能性があるため、量を重視し、洗出す。そのため、リスクの優先度は考えずに列挙を行う。また、量を重視するためにサービス要件およびリスクシナリオの構成要素を細分化および関係するものはすべて洗出しを行う。

5.2.2 MaaS サービスの検討

細分化し、リスクシナリオを洗い出したところ、数が多く、すべて RCMoel に落とし込むと可視化しても分かりにくいため、課題と目的ごとに整理を行う

こととする。

本項では、「MaaS によるものづくりツールズ」の実現について取上げる。
リスクシナリオは表 5-3 のとおりである。

表 5-3 B 市でのリスクシナリオ（例: MaaS サービス）

課題と目的		サービス要件		リスクシナリオ		No.	
1	MaaS によるものづくりツールズの実現	MaaS	地図データとの連携	データの品質, 監視可能性	古い情報や偽情報によるサービスが提供できないリスク	A1-01	
				データのバランス, システムの安定性, 公平性	偏った情報による公平性が下がるリスク	A1-02	
			オープンデータ（地図以外）との連携	データのバランス, アカウンタビリティ,	偏った量のデータによるサービスの質が異なるリスク	B1-01	
				システムの安定性, 可用性, サービスの持続可能性	膨大な量の処理によるシステムが止まるリスク	B1-02	
				外部システムとの連携, 利用者の合意	データ提供元のトラブルによるサービスが提供できないリスク	B1-03	
			産業データとの連携	データの漏洩, 証拠保全, アクセス管理	秘密性の高い産業データが漏洩するリスク	C1-01	
				機密性, 証拠保全	オープンデータとは異なるデータの管理ができないリスク	C1-02	
				契約上の保護, 機密性	秘密性が高くて開示ができない/特殊な管理を行わなければならないリスク	C1-03	
			個人の位置データと連携	セキュリティ, 外部システムとの連携, プライバシー	個人データとの紐づきによる個人情報	D1-01	
				安全性, 意識変革	個人の位置情報が他人に知られるリスク	D1-02	
			分野を跨いだデータ連携（分散管理）	契約上の保護, 機密性, 関係者との連携	管理が異なるデータの連携	D1-03	
			マッチング	個人情報管理	データの漏洩, プライバシー, アカウンタビリティ, 利用者との合意	意図しない第三者に対する個人情報の漏洩	E1-01
					データの品質, 責任の明確化, 監視可能性, 利用者の合意, 適正利用	偽情報が登録され, 混乱するリスク	E1-02
					責任の明確化, 証拠保全, 監視	なりすましのリスク	E1-03

				可能性, 利用者との合意, 利用への制限, 適正利用		
				アカウントビリティ, 意識変革, サービスの期待値	相手の個人情報が開示されず, サービスへの不安感につながるリスク	E1-04
		データの分析機能		データのバランス, アカウントビリティ, 利用者との合意, サービスの期待値	情報の偏りによる期待のサービスが提供できないリスク	F1-01
				責任の明確化, 可用性, システムの安定性, サービス持続可能性	外部的な不可抗力事態による期待のサービスが提供できないリスク	F1-02
	ものづくり	産業データ(秘密情報)との連携		契約上の保護, 機密性, 関係者との連携	管理方法が異なるデータを管理するリスク	G1-01
				法的保護, セキュリティ, 証拠保全, 機密性	法的保護を受けるデータの管理を行うリスク	G1-02
				データの漏洩, 責任の明確化, 証拠保全, セキュリティ, 監査可能性	漏洩した際のリスク	G1-03
	ツールズ	データ連携		データのバランス, 外部システムとの連携	欠けているデータがあり, レコメンドが行えないリスク	H1-01
		レコメンド機能		データの品質, 利用期間, 自動処理の正確性, 利用者との合意, サービスの持続可能性	古い情報によるレコメンドした内容が達成できないリスク	H1-02
				アカウントビリティ, 利用者との合意, 意識変革, サービスの期待値	利用者の期待感と異なるレコメンドを行うリスク	H1-03

表 5-3 から, 図 4-2 に線を引くと図 5-4 のとおりとなった. なお, 線を引く際は, データの流れから, データ提供者→プラットフォーム→サービス提供者→利用者とした. 本サービスでは, データを活用した処理などが重要になるため, プラットフォームやサービス提供者の部分の矢印が混雑しているのが分かる.

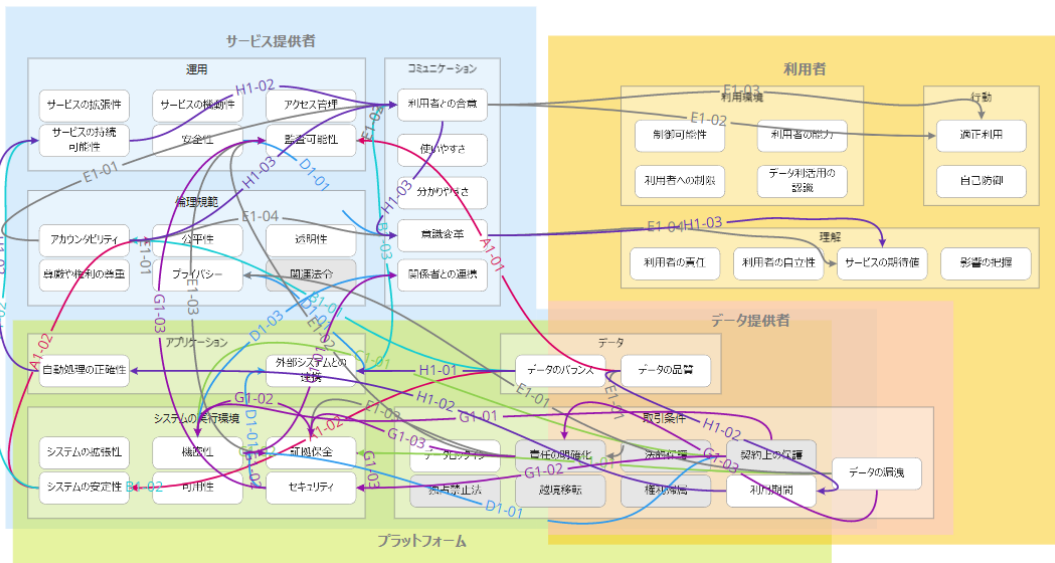


図 5-4 B 市の RCM Model (例: MaaS サービス)

図 5-4 で、矢印が多い順に各構成要素でのコントロールの整理を行うと表 5-4 となる。本件は、利用者がデータ提供者にもなりえるが、データ提供者のみも存在するため、別枠で記載している。

表 5-4 B 市のコントロールの内容 (例: MaaS サービス)

コントロールの内容 (例)			
プラットフォーム	サービス提供者	利用者	データ提供者
【責任の明確化】 契約上で明記 【機密性】 機密性のあるデータは受領しない別管理 【データの品質】 定期的なデータ更新 【データのバランス】 不足分は他社からのデータ売買も検討 【外部システムとの連携】 定期的な試験の実施 【証拠保全】 ログの保存 【システムの安定性】 保守体制の構築 【契約上の保護】 一元管理できないような条件のデータを受領しない	【意識変革】 サービスの有用性のレクチャ 【利用者との合意】 正確性が担保できない等、利用規約で合意 【アカウントビリティ】 上記の説明義務 【サービスの持続可能性】 定期的な改善、アジャイル 【監査可能性】 予想外の利用やバグが発生していないか定期的に確認 【関係者との連携】 利用者や関係者から意見を取得	【適正利用】 適正な利用がされなかったときの対処を利用規約に明記 【サービスの期待値】 利用者の目的が達成できない旨を記載 --データ提供者	【データの品質】 定期的なデータ更新 【データの漏洩】 データが漏洩した際を利用規約に明記 【責任の明確化】 利用規約上で整理

5.2.3 個人認証の検討

本項では、実現すべき価値・目的の個人認証（生体認証を含む）を活用した「域内完全キャッシュレス」の提供を取上げる。リスクシナリオは表 5-5 のとおりである。

表 5-5 B市でのリスクシナリオ（例: 個人認証）

課題と目的		サービス要件		リスクシナリオ		リスク No.
2	個人認証を活用した域内完全キャッシュレスの提供	個人認証	個人情報管理	データの品質，責任の明確化，監視可能性，利用者の合意，適正利用	偽情報により混乱するリスク	A2-01
				データの品質，監査可能性，アカウントビリティ，利用者との合意	データが更新されず，認証ができないリスク	A2-02
				法的保護，証拠保全，システムの拡張性，アクセス管理	法律に基づくデータの管理ができないリスク	A2-03
				契約上の保護，利用者との合意	目的外利用が発生するリスク	A2-04
				アカウントビリティ，意識変革，利用者との合意	利用者への合意がうまく取れないリスク	A2-05
			認証基盤	証拠保全，外部システムとの連携，サービスの機動性，アカウントビリティ	認証ができないリスク	B2-01
				アカウントビリティ，利用者との合意	異なる人を認証してしまうリスク	B2-02
			セキュリティ	セキュリティ，監査可能性，関係者との連携，適正利用	なりすましのリスク	C2-01
				意識変革，データ利活用の認識	抵抗感があり登録してくれないリスク	C2-02
			認証の読み取り機能	データの品質，自動処理の正確性，アカウントビリティ，サービスの期待値	認証が読み取れないリスク	D2-01
		キャッシュレス	キャッシュ情報との連携	外部システムとの連携，アカウントビリティ，利用者との合意	キャッシュ情報と紐づかないリスク	E2-01
				可用性，外部システムとの連携，サービスの持続可能性	連携先の事由でサービスが提供できないリスク	E2-02

			セキュリ ティ	関連法令, 利用者 との合意, 利用者 の責任	なりすましなどに対する保証 のリスク	E2-03
--	--	--	------------	-------------------------------	-----------------------	-------

表 5-5 から, 図 4-2 に線を引くと図 5-4 のとおりとなった. なお, 線を引く際は, データの流れから, データ提供者→プラットフォーム→サービス提供者→利用者とした. 本サービスでは, サービスの運用が重要になるため, サービスの提供者の部分の矢印が混雑しているのが読取れる.

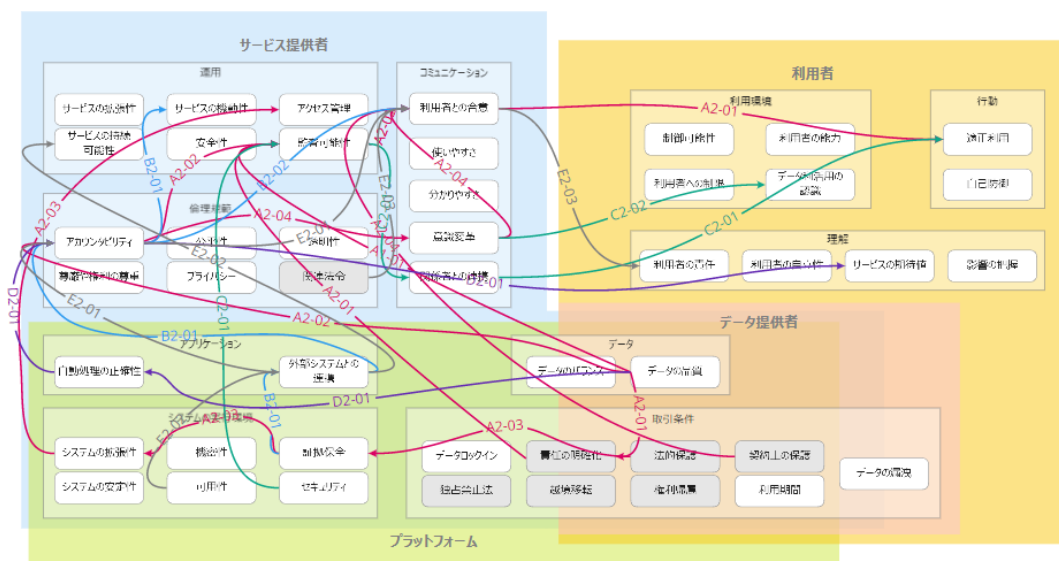


図 5-5 B 市の RCM Model (例: 個人認証)

図 5-4 で, 矢印が多い順に各構成要素でのコントロールの整理を行うと表 5-6 となる. 本件は, 利用者がデータ提供者にもなりえるが, データ提供者のみも存在するため, 別枠で記載している. 本件では, リスクシナリオの優先順位ではなく, 矢印の多いものを重視して列挙し, 少ないものについては省くものとする (グレーの構成要素は除く).

表 5-6 B市のコントロールの内容（例：個人認証）

コントロールの内容（例）			
プラットフォーム	サービス提供者	利用者	データ提供者
【外部システムとの連携】 定期的な試験の実施 【データの品質】 定期的なデータ更新/本人確認 【証拠保全】 ログの保存，電子署名の使用 【契約上の保護】 一元管理できないような条件のデータを受領しない 【法的保護】 法的保護を受けるデータをなるべく受領しない条件を定める 【責任の明確化】 利用規約での定め	【アカウントビリティ】 認証ができない場合などの精度に関する説明認識 【監査可能性】 定期的なサービス利用の監査 【利用者との合意】 サービス利用に関する事前合意 【関連法令】 関連法令の事前調査	【適正利用】 定期的な利用監視 --データ提供者参照	【データの品質】 定期的なデータ更新 --プラットフォーム参照

5.2.4 健康管理の検討

本項では，実現すべき価値・目的の貸与のヘルスケアウェアブル端末を活用した「健康管理やキャッシュレス」の実現を取上げる．リスクシナリオは表 5-7のとおりである．

表 5-7 B市でのリスクシナリオ (例: 健康管理)

課題と目的		サービス要件		リスクシナリオ		No.
3	ヘルスケアウェブ端末を活用した健康管理やキャッシュレス	ウェブ端末	アプリケーション	外部システムとの連携, サービスの持続可能性	データがうまく連携できないリスク	A3-01
			生体データの取得	関連法令, 尊厳や権利の尊重	生体情報の取得が関連法令に引っかかるリスク	B3-01
				アカウントビリティ, 利用者との合意	取得する際に利用者の同意が取れない可能性	B3-02
				データ品質, アカウントビリティ, 適正利用, 利用者との合意, 監査可能性, 影響の把握	予想外の使用によるデータ品質の低下	B3-03
		健康管理	パーソナルデータの管理	機密性, セキュリティ, プライバシー, アクセス管理	パーソナルデータを管理するリスク	C3-01
				セキュリティ, アカウントビリティ	漏洩した際の対策リスク	C3-02
			分析, 分析結果表示	データのバランス, アカウントビリティ, 利用者との合意, 意識変革, データ利活用の認識, 影響の把握	データの偏りによって正確な結果が出ないリスク (利用者の協力義務を含む)	D3-01
				アカウントビリティ, 利用者との合意, サービスの期待値	正確性を担保できないリスク	D3-02
				アカウントビリティ, 意識変革, 利用者の責任	期待と異なる結果を提示した際のリスク	D3-03

表 5-7 から, 図 4-2 に線を引くと図 5-6 のとおりとなった. なお, 線を引く際は, データの流れから, データ提供者→プラットフォーム→サービス提供者→利用者とした. 本件では, サービスの運用が重要になることが読取れる.

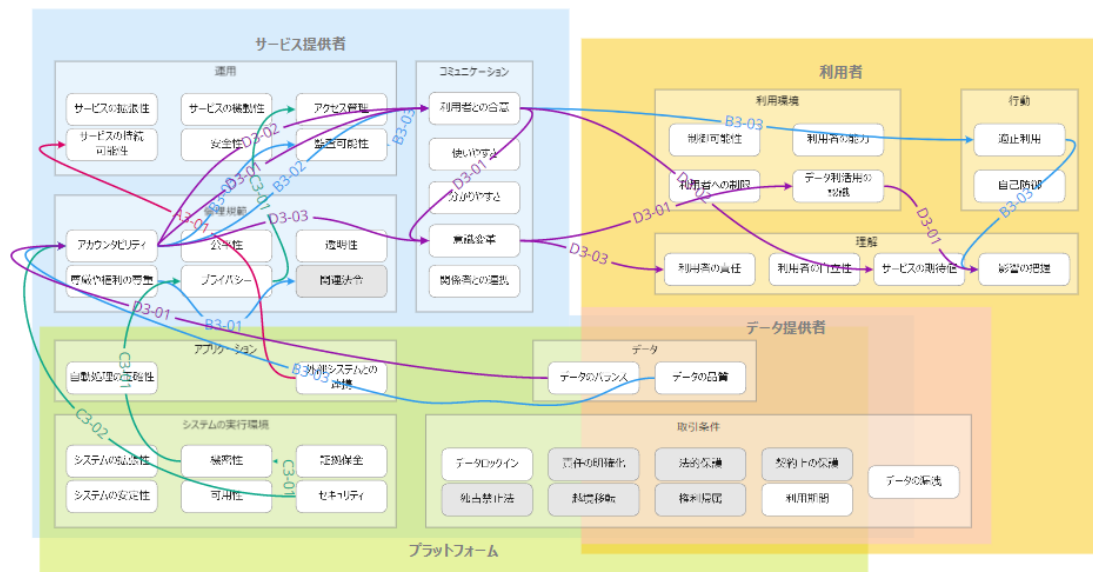


図 5-6 B市でのリスクシナリオ (例: 健康管理)

図 5-6 で、矢印が多い順に各構成要素でのコントロールの整理を行うと表 5-8 となる。本件は、利用者がデータ提供者にもなりうるが、データ提供者のみも存在するため、別枠で記載している。本件では、リスクシナリオの優先順位ではなく、矢印の多いものを重視して列挙し、少ないものについては省くものとする (グレーの構成要素は除く)。

表 5-8 B市のコントロールの内容 (例: 健康管理)

コントロールの内容 (例)			
プラットフォーム	サービス提供者	利用者	データ提供者
【セキュリティ】 各省庁で推奨されているセキュリティレベルを採用 【機密性】 受領したデータを機密性の高いという前提で管理 【データの品質】 収集時にデータの品質の最低条件の定め 【データのバランス】 不足分は第三者からの提供 【外部システムとの連携】 定期的な試験を実施	【アカウントビリティ】 分かりやすい説明を実施 【プライバシー】 セキュリティレベルの提示 【利用者との合意】 利用規約での合意 【意識変革】 データを活用した効果を提示 【関連法令】 事前の調査	【影響の把握】 サービス利用前の説明 【適正利用】 目的外使用への利用規約での定め 【サービスの期待値】 サービス利用前の効果の説明 【データ利活用の認識】 上記同様 【利用者の責任】 利用者との合意 --データ提供者参照	--プラットフォーム参照

5.2.5 新たな RCModel の検討方法の結果

本節では、5.1 節で検討した A 市の結果から 5.1.4 項にて記載した方法で検討を行った。リスクシナリオを細分化することによって時間がかかるがデータの流れから何の構成要素を検討しなければならないのかが可視化しやすくなった。デメリットとしては、細分化することによって、RCModel にて線をひく量が多くなり、分かりにくくなるため、一括ではなく、今回は課題と目的ごとに検討した。その結果、細分化することによって検討するサービスが提供者、プラットフォーム、サービス提供者、利用者のどの部分をリスクとして、注視すべきかどうかというのが B 市の事例を検討して、RCModel では把握できることが分かった。

ただし、構成要素として、該当が多い（矢印の数が多い）＝検討の優先度が高いといは言い切れないため、これを検証するためには、実際のビジネスと比較して正しいかを確認する必要がある。

5.3 検証結果

5.1 節および 5.2 節で検討した結果、データ版の RCModel においても、データを活用したビジネスでもリスクを可視化ができることが分かった。加えて、データの提供者からプラットフォーム→サービス提供者→利用者という順番で検討を行うことによって、データの流れに沿った課題を可視化することができ、矢印が多い構成要素が明確になり、リスクが顕在化するのかわからない場合において、矢印の数は検討の優先度を上げる指標にもなる。また、RCModel で課題となっていたリスクシナリオを検討する人によって異なる結果となる問題については、5.2 節で取上げた RCModel を用いた検討（B 市の構想）にて、サービス要件を細分化し、検討できるだけリスクシナリオを出し、当該リスクシナリオに対して、該当する構成要素の数を重視する検討を行ったが、この方法であれば、リスクシナリオの数が重要となるため、結果が大きく異なるといったことは発生しないと思われる。なお、データを活用したビジネスにおける RCModel の検討方法は、既存の RCModel と異なるため、次項で検討方法について扱う。さらに、検証による今後の課題についても 5.3.2 項にて取扱うものとする。

5.3.1 データ版の RCModel の検討方法

5.1 節で取上げた RCModel を用いた検討（A 市の構想）および 5.2 節で取上げた RCModel を用いた検討（B 市の構想）の結果から、最適だと思われるデータ版の RCModel の推奨の検討方法（リスクの可視化）は次のとおりである。

- 1 実現すべき価値・目的を抽出
- 2 1 で抽出した価値・目的ごとにリスクシナリオを洗出せるだけ出す
- 3 2 で洗出したリスクシナリオに対して、考えられる構成要素を出す
- 4 図 4-2 に 3 で出した構成要素に提供者→プラットフォーム→サービス提供者→利用者の順に線（矢印）をひく
- 5 4 で作成した RCModel の構成要素の矢印が多いものを優先（グレーの箇所はリスクテイクなどができないため、矢印関係なく優先）して、コントロールを記載

上記の方法で行った場合、検討サービスにおけるリスクについて、検討事項と注視しなければならない構成要素を把握することができる。

5.3.2 検証による課題

今回、検証を行い、次の 1 から 3 の事項について懸念がある。

- 1 構成要素が十分であるか
- 2 リスクシナリオが十分であるか
- 3 該当する構成要素が多い＝検討しなければならない課題となっているか

まず、構成要素の数について、図 4-2 の構成要素で十分であるかどうかを検証できていない。加えて、法律や政策などは常に変わるものであり、定期的に構成要素の更新を行う必要がある。次にリスクシナリオを洗出したが、リスクシナリオのあり洗出しの作業に関しては今までの経験が一番影響するため、様々な視点からリスクシナリオを検討しても結果が同様な状態になるか、検証が必要である。最後に、今回は概要する構成要素が多い＝検討しなければならない課題になるかは検証が必要であるため、実際の事例と照らし合わせて検討を行う必要がある。

第6章 結論

本稿では、データを活用したサービスを検討する際のリスクの検討モデルとしてどうあるべきかを明らかにした。本章では、本調査での結果を中心にまとめる。また、1.2節で設定したリサーチ・クエスチョンに対する解答を記載する。最後に将来の調査および研究への示唆を示す。

6.1 リサーチ・クエスチョンに対する解答

本項では、1.2節で設定したSRQについて解答を行い、当該解答の結果をもとに、MRQについて解答を行う。はじめに、SRQ1の問いは次のとおりである。

SRQ1: データビジネスにおけるデータの種類、データの流通方法、ビジネス形態はどのようなになっているのか?

この問いの解答としては、データの活用におけるビジネス形態について、「どのような性質のデータがあるのか」、「どのようなデータの優先度が高いのか」、「どのようにデータを流通・共有すべきか」、「データ提供活性化のために、どのようなインセンティブを与えるべきか」という観点から現状のデータの活用状況について整理ができた。また、オープンデータとそれ以外のデータの価値の考え方が異なるため、観点の解答も異なることが重要となる。

発見事項としては、オープンデータとオープンデータ以外のデータは上記の観点が一緒にはならないこと、図3-17で表したとおり、見事にオープンデータと事業者でやり取りされているデータに大きな壁があることが可視化でき、それらを統合したサービスが期待されていることが明確に分かった点である。次に、SRQ2の問いは以下のとおりである。

SRQ2: データを活用したビジネスにおける課題・リスクはどのようなものか?

この問いに対する解答として、データを活用したビジネスを検討する際のリスクを可視化したものが、図4-2のとおりである。さらに可視化した構成要素の説明は、観点ごとにデータを流通させるプラットフォームの構成要素は、表4-2、データを活用したサービス提供者の構成要素は、表4-4、利用者の構成要素は、表4-5、データ提供者の構成要素は、表4-6である。

発見事項は、リスクの対応策に対しては対応の優先順位があるが、構成要素の中には、リスクが発生しているが対応しないという判断ができないリスクも

あること、提供者の構成要素の対応策は異なるもののプラットフォームの構成要素とほぼ同じであること、データを活用したビジネスにおいてはサービスの利用者もデータの提供者になりえるため、それを前提にリスクの検討が必要であることである。次に、SRQ3の問いは以下のとおりである。

SRQ3: データを活用したビジネスのリスクの検討モデルはどのようなものか？

想定される地方公共団体で提供されるデータとパーソナルデータを活用したサービス事例において、データ版のRCModelが活用でき、リスクを可視化できることが確認できた。

発見事項は、従来（AI版）のRCModelのやり方では目的・価値を設定し、リスクシナリオを洗い出し、リスクの優先順位を設定していたが、データの活用に関しては、目的別には検討が必要ではあるものの、特にリスクとして注目しなければならないのはRCModel上で線が多く繋がれているものになるのではないかとということが確認できた。最後に、MRQの問いは、以下のとおりである。

MRQ: データを活用したサービスを提供する際のリスクマネジメントはどのように行うべきか？

本調査の結果として、データ版のRCModelでもリスクの可視化ができることが認められた。また、構成要素も整理ができ、検討すべき事項も追加で発見できた。多くのデータの種類があることが認められたが、データの特徴を捉え、それに則した対応を行う必要があり、モデルもそれに応じて変更する必要がある。

なお、観点ごとにリスクを洗い出すことによって、リスクシナリオからもビジネス検討が必要なため、この作業からもデータの流通のモデルの検討が可能となる。

6.2 実務的含意

今後、オープンデータとオープンデータではない様々な種類のデータを連携したサービスの提供は多くなる可能性があり、データを活用したビジネスにおけるリスクの管理は今後重要になると想定される。本調査の実務的含意は、データを活用したビジネスにおけるリスクを可視化する方法を作成したことにより、ビジネスの検討における参考になると思われる。なお、本調査では、実際に作成したモデルで抽出したリスクの正確性までは実際のビジネスとは比

較できていないが、今後、新規ビジネスの検討において活用されることを期待する。

6.3 本調査の限界と将来研究への示唆

本調査は先行研究の RCMoel をもとに各省庁が調査を行っているデータを活用したビジネスにおける課題を抽出してデータ版の RCMoel を作成し、課題を可視化した。オープンデータを活用し、分野を跨いだ行政サービスは、現段階においては多くはないため、当該 RCMoel での検証が難しい状態である。そのため、調査対象を増やすとともに、実際にビジネスの検討にかかわっている方々にインタビュー調査などを行い、理論の補強や正確性の検討を行い、データ版の RCMoel を常にアップデートをしていきたい。

第7章 参考文献

- Apple, 2021, “App privacy details on the App Store,” (Retrieved October 12, 2021, <https://developer.apple.com/app-store/app-privacy-details/>).
- Asif, Sudais, 2020, “Data scraping firm leaks 235m Instagram, TikTok, YouTube user records,” HackRead, (Retrieved October 12, 2021, <https://www.hackread.com/data-scraping-firm-leaks-instagram-tiktok-youtube-records/>).
- Business Lawyers, 2020, 「情報発信」, Bengo4.com, Inc., (2021年9月11日取得, <https://www.businesslawyers.jp/practices/1315>).
- コネクトデータ, 2021, 「オープンデータに関する調査」, (2021年10月13日取得, <https://delika.io/connecto-data/survey>).
- クリエイティブ・コモンズ・ジャパン, 2021, 「クリエイティブ・コモンズ・ライセンスとは」, (2021年10月13日取得, <https://creativecommons.jp/licenses/>).
- DATA GO JP, 2021, 「利用規約」, (2021年10月13日取得, <https://www.data.go.jp/terms-of-use/terms-of-use/>).
- Deloitte, 2017, 「リスク インテリジェンス マップ TM (概要版) ——賢いリスク管理へのガイダンス」, (2021年10月13日取得, <https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/strategy/cg/jp-cg-risk-map.pdf>).
- , 2020, 「東京大学未来ビジョン研究センターとデロイト トーマツ リスクサービスによる AI ガバナンスに関する共同研究プロジェクトがケース事例を公開」, (2021年10月13日取得, <https://www2.deloitte.com/jp/ja/pages/deloitte-analytics/articles/aigovernance-case-studies-utokyo.html>).
- Digital Transformation Channel, 2020, 「HIPAA/HITECH とは? 知っておきたい基本情報を解説」, リードプラス株式会社, (2021年9月20日取得, <https://www.digital-transformation-real.com/blog/what-is-hipaa-and-hitech.html#toc-0>).
- FairInternetReport, 2020, “Europe vs US Broadband Performance 2020,” FairInternetReport.com, (Retrieved October 13, 2021, <https://fairinternetreport.com/research/usa-vs-europe-internet-speed-analysis>).
- フリーランス協会, 2018, 『プロフェッショナル&パラレルキャリア フリーランス協会 ——誰もが自律的なキャリアを築ける世の中へ』 (2021年9月20日取得, https://www.kantei.go.jp/jp/singi/it2/detakatuyo_wg/dai5/dcwg_siryou2-2.pdf).
- Frey, Suzanne, 2021 “New safety section in Google Play will give transparency into how apps use data,” Android Developers Blog, (Retrieved October 12, 2021, <https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html>).
- GitHub, 2021, 「GitHub 利用規約」, (2021年10月13日取得, <https://docs.github.com/ja/github/site-policy/github-terms-of-service#d-user-generated-content>).
- 原田久義, 2019, 「【アメリカ】 海外のデータの合法的使用を明確化する法律 ——クラウド法」『外国の立法』 国立国会図書館 調査及び立法考査局, No.278-1.
- 樋口隆充, 2021, 「LINE のデータ保管, なぜ海外に? LINE 幹部が会見で説明」, IT media NEWS, (2021年10月13日取得, <https://www.itmedia.co.jp/news/articles/2110/24/news124.html>).
- Hirsch, Lauren, 2020, “IBM gets out of facial recognition business, calls on Congress to advance policies tackling racial injustice,” CNBC, (Retrieved October 12, 2021, <https://www.cnn.com/2020/06/08/ibm-gets-out-of-facial-recognition-business-calls-on-congress-to-advance-policies-tackling-racial-injustice.html>).
- IP Australia, 2021, “Commissioner to appeal court decision allowing artificial intelligence to be an inventor,”

- (Retrieved October 12, 2021, <https://www.ipaustralia.gov.au/about-us/news-and-community/news/commissioner-appeal-court-decision-allowing-artificial-intelligence>).
- JETRO, 2018, 「急増する世界の『データ』——流通量実態把握のための統計整備が課題」, 日本貿易振興機構ホームページ, (2021年10月13日取得, <https://www.jetro.go.jp/biz/areareports/2018/380fd5f0d9c4bb4d.html>).
- , 2021, 「EU一般データ保護規則 (GDPR) について」, 日本貿易振興機構ホームページ, (2021年11月3日取得, <https://www.jetro.go.jp/world/europe/eu/gdpr/>).
- 情報処理推進機構, 2020, 『企業におけるデータ利活用・保護の戦略立案のための手引書 (案) の作成 概要説明資料』.
- 経済産業省, 2015a, 『第4次産業革命への対応の方向性——官民の戦略的取組の進捗へ向けて』.
- , 2015b, 『第4次産業革命への対応の方向性——主要領域についての議論:ものづくり革新領域:流通・小売・物流領域』.
- , 2015c, 『第4次産業革命への対応の方向性 官民の戦略的取組の進捗へ向けて (討議用)』.
- , 2016, 『IoT進展に立ちはだかる中期的課題への新たなアプローチ——集めないビッグデータ, パーソナルデータストア, データ流通市場』.
- , 2018, 『データポータビリティに関する調査・検討について』.
- , 2019, 『AI・データの利用に関する契約ガイドライン——データ編 1.1版』.
- , 2020, 『データ利活用のポイント集——データ利活用の共創が生み出す新しい価値』.
- 公正取引委員会, 2017, 「知的財産の利用に関する独占禁止法上の指針」, (2021年10月13日取得, <https://www.jftc.go.jp/dk/guideline/unyoukijun/chitekizaisan.html>).
- , 2019, 「2019年3月」, (2021年10月13日取得, <https://www.jftc.go.jp/kokusai/kaigaiugoki/sonota/201903others/201903others.html>).
- 松本敬史, 江間有沙, 2020, 「AIサービスのリスク低減を検討するリスクチェーンモデルの提案」『政策提言書』 東京大学未来ビジョン研究センター, (2020年10月1日取得, https://ifi.u-tokyo.ac.jp/wp/wp-content/uploads/2020/06/policy_recommendation_tg_20200604.pdf).
- , 2021, 「AIサービスに係る『実現すべき価値・目的』と『リスクシナリオ』の類型化」 *The 35th Annual Conference of the Japanese Society for Artificial Intelligence, 2021*, (2020年10月1日取得, https://www.jstage.jst.go.jp/article/pjsai/JSIAI2021/0/JSIAI2021_1E3OS8a04/pdf-char/ja).
- 内閣官房, 2016a, 『地方公共団体オープンデータ推進ガイドライン』.
- , 2016b, 『AI, IOT時代におけるデータ活用WG中間とりまとめに向けた論点 (案)』.
- , 2017a, 『オープンデータをはじめよう——地方公共団体のための最初の手引書』.
- , 2017b, 『「オープンデータ基本指針」 (案)』.
- 内閣府, 2021, 『「スーパーシティ」構想について』.
- オープン&ビッグデータ活用・地方創生推進機構, 2016, 『オープンデータ利活用 ビジネス事例集』.
- Pennycook, Gordon, Ziv Epstein, Mohsen Mosleh, Antonio A. Arechar, Dean Eckles and David G. Rand, 2021, “Shifting attention to accuracy can reduce misinformation online,” *nature*, 592, 590–595 (2021).
- Roberts, Jeff, 2021, “The NFT Craze Offers Easy Money——And Hard Copyright Questions,” Decrypt, (Retrieved October 12, 2021, <https://decrypt.co/60394/nft-craze-easy-money-hard-copyright-questions>).

- Sansan, 2020, 「Sansan サービス約款」, (2021年10月13日取得, <https://agreement.sansan.com/ja/rule/>).
- , 2021, 「Sansan ——働き方を変えるDX」, (2021年10月13日取得, <https://jp.sansan.com/>).
- Schimroszik, Nadine and Mathieu Rosemain, 2020, “France, Germany back European cloud computing 'moonshot',” Reuters, (Retrieved October 31, 2021, <https://www.reuters.com/article/us-europe-tech/france-germany-back-european-cloud-computing-moonshot-idUSKBN23B26B>).
- 総務省, 2014, 『ビッグデータ時代における情報量の計測に係る調査研究報告書』.
- , 2017a, 『安心・安全なデータ流通・利活用に関する調査研究の請負報告書』.
- , 2017b, 『平成29年版情報通信白書』.
- , 2017c, 『地域におけるICT利活用の現状に関する調査研究報告書』.
- , 2019, 『消費者物価指数(CPI)へのウェブスクレイピングの活用について』.
- , 2020a, 『我が国のインターネットにおけるトラフィックの集計結果(2019年11月分)』.
- , 2020b, 『デジタルデータの経済的価値の計測と活用の現状に関する調査研究の請負報告書』.
- , 2020c, 『令和2年版情報通信白書第1部』.
- , 2020d, 『プラットフォームサービスに関する研究会 最終報告書』.
- Talend, 2021, 「構造化データと非構造化データの比較:完全ガイド」, talend website, (2021年9月11日取得, https://www.cdi-japan.co.jp/wp/wp-content/uploads/2017/01/CDIPPP2_.pdf).
- 谷井将人, 2021, 「LINEの個人情報, 中国の開発委託先から閲覧可能に 『説明不足だった』と謝罪」, IT media NEWS, (2021年10月13日取得, <https://www.itmedia.co.jp/news/articles/2103/17/news127.html>).
- 東京大学, 2021, 『リスクチェーンモデル(RCModel)ガイド Ver 1.0』, (2021年9月26日取得, https://ifi.u-tokyo.ac.jp/wp/wp-content/uploads/2021/07/RCM_210705.pdf).
- Top Court, 2020, 「利用規約に著作権の定めを置く場合の3つのポイントを弁護士が解説!」, (2021年10月13日取得, https://topcourt-law.com/terms_of_service/terms_of_service_copyright).
- Torralba, Antonio and Rob Fergus, Bill Freeman, 2020, “80 Million Tiny Images,” MIT, (Retrieved October 12, 2021, <https://groups.csail.mit.edu/vision/TinyImages/>).
- 筑波大学, 2019, 『地方自治体のオープンデータ施策に影響を与える要因に関する調査研究』.
- Tung, Liam, 2020, “Meet GAIA-X: This is Europe's bid to get cloud independence from US and China giants,” ZDNet, (Retrieved October 31, 2021, <https://www.zdnet.com/article/meet-gaia-x-this-is-europes-bid-to-get-cloud-independence-from-us-and-china-giants/>).
- Twitter, 2021, 「Twitter サービス利用規約」, (2021年10月13日取得, <https://twitter.com/ja/tos>).
- 内平直志, 森俊樹, 大島丈史, 2020, 「人工知能とプロジェクトマネジメント」『電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review』13(4): 277-283.
- UNIQLO, 2017, 「UTme!利用規約」, (2021年10月13日取得, <https://utme.uniqlo.com/page/terms/>).
- , 2021, 「UTme! ——スマホでデザイン, 君だけのUT!」, (2021年10月13日取得, <https://utme.uniqlo.com/>).
- USPTO, 2020, “Petition decision: Inventorship limited to natural persons,” (Retrieved October 12, 2021, <https://content.govdelivery.com/accounts/USPTO/bulletins/287fde9>).

第8章 附録

本稿では、2021年10月時点の以下の法律条文を参考にしている。

8.1 民法

8.1.1 第85条（定義）

1 この法律において「物」とは、有体物をいう。

8.1.2 第180条（占有権の取得）

1 占有権は、自己のためにする意思をもって物を所持することによって取得する。

8.1.3 第206条（所有権の内容）

1 所有者は、法令の制限内において、自由にその所有物の使用、収益及び処分をする権利を有する。

8.1.4 第239条（無主物の帰属）

- 1 所有者のない動産は、所有の意思をもって占有することによって、その所有権を取得する。
- 2 所有者のない不動産は、国庫に帰属する。

8.2 官民データ活用推進基本法

8.2.1 第11条（国及び地方公共団体等が保有する官民データの容易な利用等）

- 1 国及び地方公共団体は、自らが保有する官民データについて、個人及び法人の権利利益、国の安全等が害されることのないようにしつつ、国民がインターネットその他の高度情報通信ネットワークを通じて容易に利用できるよう、必要な措置を講ずるものとする。
- 2 事業者は、自らが保有する官民データであって公益の増進に資するものについて、個人及び法人の権利利益、国の安全等が害されることのないようにしつつ、国民がインターネットその他の高度情報通信ネットワークを通じて容易に利用できるよう、必要な措置を講ずるよう努めるものとする。
- 3 国は、官民データ活用を推進するため、官民データの円滑な流通に関連する制度（コンテンツ（コンテンツの創造、保護及び活用の促進に関する法

律（平成十六年法律第八十一号）第二条第一項に規定するコンテンツをいう。）の円滑な流通に関連する制度を含む。）の見直しその他の必要な措置を講ずるものとする。

8.3 個人情報保護に関する法律

8.3.1 第2条（定義）

- 1 この法律において「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。
 - (1) 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
 - (2) 個人識別符号が含まれるもの
- 2 この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。
 - (1) 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であつて、当該特定の個人を識別することができるもの
 - (2) 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であつて、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの
- 3 略
- 4 この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であつて、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。
 - (1) 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
 - (2) 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
- 5 略
- 6 この法律において「個人データ」とは、個人情報データベース等を構成す

る個人情報という。

8.3.2 第 15 条（利用目的の特定）

- 1 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
- 2 個人情報取扱事業者は、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。

8.3.3 第 16 条（利用目的による制限）

- 1 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
- 2 個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
- 3 前二項の規定は、次に掲げる場合については、適用しない。
 - (1) 法令に基づく場合
 - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

8.3.4 第 17 条（適正な取得）

- 1 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。
- 2 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
 - (1) 法令に基づく場合
 - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがある

るとき。

- (5) 当該要配慮個人情報、本人、国の機関、地方公共団体、第七十六条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
- (6) その他前各号に掲げる場合に準ずるものとして政令で定める場合

8.3.5 第 18 条（取得に際しての利用目的の通知等）

- 1 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
- 2 個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。
- 3 個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。
- 4 前三項の規定は、次に掲げる場合については、適用しない。
 - (1) 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - (2) 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
 - (3) 国の機関又は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であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
 - (4) 取得の状況からみて利用目的が明らかであると認められる場合

8.3.6 第 19 条（データ内容の正確性の確保等）

- 1 個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

8.3.7 第 20 条（安全管理措置）

- 1 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

8.3.8 第 21 条（従業者の監督）

- 1 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

8.3.9 第 22 条（委託先の監督）

- 1 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

8.3.10 第 23 条（第三者提供の制限）

- 1 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
 - (1) 法令に基づく場合
 - (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 2 個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、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、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
 - (1) 第三者への提供を利用目的とすること。
 - (2) 第三者に提供される個人データの項目
 - (3) 第三者への提供の方法
 - (4) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
 - (5) 本人の求めを受け付ける方法
- 3 個人情報取扱事業者は、前項第二号、第三号又は第五号に掲げる事項を変更する場合は、変更する内容について、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なければならない。
- 4 個人情報保護委員会は、第二項の規定による届出があったときは、個人情報保護委員会規則で定めるところにより、当該届出に係る事項を公表しなければならない。前項の規定による届出があったときも、同様とする。

- 5 次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。
 - (1) 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合
 - (2) 合併その他の事由による事業の承継に伴って個人データが提供される場合
 - (3) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、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いているとき。
- 6 個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、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かなければならない。

8.3.11 第 24 条（外国にある第三者への提供の制限）

- 1 個人情報取扱事業者は、外国（本邦の域外にある国又は地域をいう。以下同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある第三者（個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この条において同じ。）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

8.3.12 第 25 条（第三者提供に係る記録の作成等）

- 1 個人情報取扱事業者は、個人データを第三者（第二条第五項各号に掲げる者を除く。以下この条及び次条において同じ。）に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第二十三条第一項各号又は第五項各号のいずれか（前条の規定による個人データの提供にあつては、第二十三条第一項各号のいずれか）に該当する場合は、この限りでない。
- 2 個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情

報保護委員会規則で定める期間保存しなければならない。

8.4 著作権法

8.4.1 第2条（定義）

- 1 この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
 - (1) 著作物 思想又は感情を創作的に表現したものであつて、文芸、学術、美術又は音楽の範囲に属するものをいう。
 - (2) 著作者 著作物を創作する者をいう。
以下略

8.5 特許法

8.5.1 第2条（定義）

- 1 この法律で「発明」とは、自然法則を利用した技術的思想の創作のうち高度のものをいう。
- 2 この法律で「特許発明」とは、特許を受けている発明をいう。
- 3 この法律で発明について「実施」とは、次に掲げる行為をいう。
 - (1) 物（プログラム等を含む。以下同じ。）の発明にあつては、その物の生産、使用、譲渡等（譲渡及び貸渡しをいい、その物がプログラム等である場合には、電気通信回線を通じた提供を含む。以下同じ。）、輸出若しくは輸入又は譲渡等の申出（譲渡等のための展示を含む。以下同じ。）をする行為
 - (2) 方法の発明にあつては、その方法の使用をする行為
 - (3) 物を生産する方法の発明にあつては、前号に掲げるもののほか、その方法により生産した物の使用、譲渡等、輸出若しくは輸入又は譲渡等の申出をする行為
- 4 この法律で「プログラム等」とは、プログラム（電子計算機に対する指令であつて、一の結果を得ることができるよう組み合わされたものをいう。以下この項において同じ。）その他電子計算機による処理の用に供する情報であつてプログラムに準ずるものをいう。

8.5.2 第29条（特許の要件）

- 1 産業上利用することができる発明をした者は、次に掲げる発明を除き、その発明について特許を受けることができる。
 - (1) 特許出願前に日本国内又は外国において公然知られた発明
 - (2) 特許出願前に日本国内又は外国において公然実施をされた発明
 - (3) 特許出願前に日本国内又は外国において、頒布された刊行物に記載さ

- れた発明又は電気通信回線を通じて公衆に利用可能となつた発明
- 2 特許出願前にその発明の属する技術の分野における通常の知識を有する者が前項各号に掲げる発明に基いて容易に発明をすることができたときは、その発明については、同項の規定にかかわらず、特許を受けることができない。

8.5.3 第 66 条（特許権の設定の登録）

- 1 特許権は、設定の登録により発生する。
以下略

8.6 不正競争防止法

8.6.1 第 2 条（定義）

- 1 この法律において「不正競争」とは、次に掲げるものをいう。
 - (1) 他人の商品等表示（人の業務に係る氏名、商号、商標、標章、商品の容器若しくは包装その他の商品又は営業を表示するものをいう。以下同じ。）として需要者の間に広く認識されているものと同一若しくは類似の商品等表示を使用し、又はその商品等表示を使用した商品を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、若しくは電気通信回線を通じて提供して、他人の商品又は営業と混同を生じさせる行為
 - (2) 自己の商品等表示として他人の著名な商品等表示と同一若しくは類似のものを使用し、又はその商品等表示を使用した商品を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、若しくは電気通信回線を通じて提供する行為
 - (3) 他人の商品の形態（当該商品の機能を確保するために不可欠な形態を除く。）を模倣した商品を譲渡し、貸し渡し、譲渡若しくは貸渡しのために展示し、輸出し、又は輸入する行為
 - (4) 窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為（以下「営業秘密不正取得行為」という。）又は営業秘密不正取得行為により取得した営業秘密を使用し、若しくは開示する行為（秘密を保持しつつ特定の者に示すことを含む。次号から第九号まで、第十九条第一項第六号、第二十一条及び附則第四条第一号において同じ。）
 - (5) その営業秘密について営業秘密不正取得行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為
 - (6) その取得した後にその営業秘密について営業秘密不正取得行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、又は開示する行為
 - (7) 営業秘密を保有する事業者（以下「営業秘密保有者」という。）からそ

の営業秘密を示された場合において、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為

- (8) その営業秘密について営業秘密不正開示行為（前号に規定する場合において同号に規定する目的でその営業秘密を開示する行為又は秘密を守る法律上の義務に違反してその営業秘密を開示する行為をいう。以下同じ。）であること若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為
- (9) その取得した後にその営業秘密について営業秘密不正開示行為があったこと若しくはその営業秘密について営業秘密不正開示行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、又は開示する行為
- (10) 第四号から前号までに掲げる行為（技術上の秘密（営業秘密のうち、技術上の情報であるものをいう。以下同じ。）を使用する行為に限る。以下この号において「不正使用行為」という。）により生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供する行為（当該物を譲り受けた者（その譲り受けた時に当該物が不正使用行為により生じた物であることを知らず、かつ、知らないことにつき重大な過失がない者に限る。）が当該物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電気通信回線を通じて提供する行為を除く。）
- (11) 窃取、詐欺、強迫その他の不正の手段により限定提供データを取得する行為（以下「限定提供データ不正取得行為」という。）又は限定提供データ不正取得行為により取得した限定提供データを使用し、若しくは開示する行為
- (12) その限定提供データについて限定提供データ不正取得行為が介在したことを知って限定提供データを取得し、又はその取得した限定提供データを使用し、若しくは開示する行為
- (13) その取得した後にその限定提供データについて限定提供データ不正取得行為が介在したことを知ってその取得した限定提供データを開示する行為
- (14) 限定提供データを保有する事業者（以下「限定提供データ保有者」という。）からその限定提供データを示された場合において、不正の利益を得る目的で、又はその限定提供データ保有者に損害を加える目的で、その限定提供データを使用する行為（その限定提供データの管理に係る任務に違反して行うものに限る。）又は開示する行為
- (15) その限定提供データについて限定提供データ不正開示行為（前号に規定する場合において同号に規定する目的でその限定提供データを開示する行為をいう。以下同じ。）であること若しくはその限定提供データについて限定提供データ不正開示行為が介在したことを知って限定提

供データを取得し、又はその取得した限定提供データを使用し、若しくは開示する行為

(16) その取得した後にその限定提供データについて限定提供データ不正開示行為があったこと又はその限定提供データについて限定提供データ不正開示行為が介在したことを知ってその取得した限定提供データを開示する行為

(17)～(22) 略

2 ～5 略

6 この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であつて、公然と知られていないものをいう。

7 この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。

8 略

9 この法律において「プログラム」とは、電子計算機に対する指令であつて、一の結果を得ることができるように組み合わせられたものをいう。

10 略

11 この法律にいう「物」には、プログラムを含むものとする。

8.6.2 第3条（差止請求権）

1 不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、その営業上の利益を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

2 不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、前項の規定による請求をするに際し、侵害の行為を組成した物（侵害の行為により生じた物を含む。第五条第一項において同じ。）の廃棄、侵害の行為に供した設備の除却その他の侵害の停止又は予防に必要な行為を請求することができる。

8.6.3 第4条（損害賠償）

1 故意又は過失により不正競争を行つて他人の営業上の利益を侵害した者は、これによって生じた損害を賠償する責めに任ずる。ただし、第十五条の規定により同条に規定する権利が消滅した後にその営業秘密又は限定提供データを使用する行為によって生じた損害については、この限りでない。

8.6.4 第19条（適用除外等）

1 第三条から第十五条まで、第二十一条（第二項第七号に係る部分を除く。）

及び第二十二条の規定は、次の各号に掲げる不正競争の区分に応じて当該各号に定める行為については、適用しない。

(1) ～ (7) 略

(2) 第二条第一項第十一号から第十六号までに掲げる不正競争 次のいずれかに掲げる行為

イ) 略

ロ) その相当量蓄積されている情報が無償で公衆に利用可能となっている情報と同一の限定提供データを取得し、又はその取得した限定提供データを使用し、若しくは開示する行為

(3) 略

2 略

8.6.5 第 21 条（罰則）

1 次の各号のいずれかに該当する者は、十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する。

(1) 不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。次号において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）その他の営業秘密保有者の管理を害する行為をいう。次号において同じ。）により、営業秘密を取得した者

(2) 詐欺等行為又は管理侵害行為により取得した営業秘密を、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、使用し、又は開示した者

(3) 営業秘密を営業秘密保有者から示された者であって、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、次のいずれかに掲げる方法でその営業秘密を領得した者

イ) 営業秘密記録媒体等（営業秘密が記載され、又は記録された文書、図画又は記録媒体をいう。以下この号において同じ。）又は営業秘密が化体された物件を横領すること。

ロ) 営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成すること。

ハ) 営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること。

(4) 営業秘密を営業秘密保有者から示された者であって、その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を、不正の利益を得る目的で、又はその営業秘密保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、使用し、

又は開示した者

- (5) 営業秘密を営業秘密保有者から示されたその役員（理事，取締役，執行役，業務を執行する社員，監事若しくは監査役又はこれらに準ずる者をいう。次号において同じ。）又は従業者であって，不正の利益を得る目的で，又はその営業秘密保有者に損害を加える目的で，その営業秘密の管理に係る任務に背き，その営業秘密を使用し，又は開示した者（前号に掲げる者を除く。）
 - (6) 営業秘密を営業秘密保有者から示されたその役員又は従業者であった者であって，不正の利益を得る目的で，又はその営業秘密保有者に損害を加える目的で，その在職中に，その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし，又はその営業秘密の使用若しくは開示について請託を受けて，その営業秘密をその職を退いた後に使用し，又は開示した者（第四号に掲げる者を除く。）
 - (7) 不正の利益を得る目的で，又はその営業秘密保有者に損害を加える目的で，第二号若しくは前三号の罪又は第三項第二号の罪（第二号及び前三号の罪に当たる開示に係る部分に限る。）に当たる開示によって営業秘密を取得して，その営業秘密を使用し，又は開示した者
 - (8) 不正の利益を得る目的で，又はその営業秘密保有者に損害を加える目的で，第二号若しくは第四号から前号までの罪又は第三項第二号の罪（第二号及び第四号から前号までの罪に当たる開示に係る部分に限る。）に当たる開示が介在したことを知って営業秘密を取得して，その営業秘密を使用し，又は開示した者
 - (9) 不正の利益を得る目的で，又はその営業秘密保有者に損害を加える目的で，自己又は他人の第二号若しくは第四号から前号まで又は第三項第三号の罪に当たる行為（技術上の秘密を使用する行為に限る。以下この号及び次条第一項第二号において「違法使用行為」という。）により生じた物を譲渡し，引き渡し，譲渡若しくは引渡しのために展示し，輸出し，輸入し，又は電気通信回線を通じて提供した者（当該物が違法使用行為により生じた物であることの情を知らないで譲り受け，当該物を譲渡し，引き渡し，譲渡若しくは引渡しのために展示し，輸出し，輸入し，又は電気通信回線を通じて提供した者を除く。）
- 2 次の各号のいずれかに該当する者は，五年以下の懲役若しくは五百万円以下の罰金に処し，又はこれを併科する。
- (1) 不正の目的をもって第二条第一項第一号又は第二十号に掲げる不正競争を行った者
 - (2) 他人の著名な商品等表示に係る信用若しくは名声を利用して不正の利益を得る目的で，又は当該信用若しくは名声を害する目的で第二条第一項第二号に掲げる不正競争を行った者
 - (3) 不正の利益を得る目的で第二条第一項第三号に掲げる不正競争を行った者
 - (4) 不正の利益を得る目的で，又は営業上技術的制限手段を用いている者に損害を加える目的で，第二条第一項第十七号又は第十八号に掲げる

不正競争を行った者

- (5) 商品若しくは役務若しくはその広告若しくは取引に用いる書類若しくは通信にその商品の原産地、品質、内容、製造方法、用途若しくは数量又はその役務の質、内容、用途若しくは数量について誤認させるような虚偽の表示をした者（第一号に掲げる者を除く。）
 - (6) 秘密保持命令に違反した者
 - (7) 第十六条、第十七条又は第十八条第一項の規定に違反した者
- 3 次の各号のいずれかに該当する者は、十年以下の懲役若しくは三千万円以下の罰金に処し、又はこれを併科する。
- (1) 日本国外において使用する目的で、第一項第一号又は第三号の罪を犯した者
 - (2) 相手方に日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をする目的があることの情を知って、これらの罪に当たる開示をした者
 - (3) 日本国内において事業を行う営業秘密保有者の営業秘密について、日本国外において第一項第二号又は第四号から第八号までの罪に当たる使用をした者
- 4 第一項（第三号を除く。）並びに前項第一号（第一項第三号に係る部分を除く。）、第二号及び第三号の罪の未遂は、罰する。
- 5 第二項第六号の罪は、告訴がなければ公訴を提起することができない。
- 6 第一項各号（第九号を除く。）、第三項第一号若しくは第二号又は第四項（第一項第九号に係る部分を除く。）の罪は、日本国内において事業を行う営業秘密保有者の営業秘密について、日本国外においてこれらの罪を犯した者にも適用する。
- 7 第二項第六号の罪は、日本国外において同号の罪を犯した者にも適用する。
- 8 第二項第七号（第十八条第一項に係る部分に限る。）の罪は、刑法（明治四十年法律第四十五号）第三条の例に従う。
- 9 第一項から第四項までの規定は、刑法その他の罰則の適用を妨げない。
- 10 次に掲げる財産は、これを没収することができる。
- (1) 第一項、第三項及び第四項の罪の犯罪行為により生じ、若しくは当該犯罪行為により得た財産又は当該犯罪行為の報酬として得た財産
 - (2) 前号に掲げる財産の果実として得た財産、同号に掲げる財産の対価として得た財産、これらの財産の対価として得た財産その他同号に掲げる財産の保有又は処分に基づき得た財産
- 11 組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成十一年法律第百三十六号。以下「組織的犯罪処罰法」という。）第十四条及び第十五条の規定は、前項の規定による没収について準用する。この場合において、組織的犯罪処罰法第十四条中「前条第一項各号又は第四項各号」とあるのは、「不正競争防止法第二十一条第十項各号」と読み替えるものとする。
- 12 第十項各号に掲げる財産を没収することができないとき、又は当該財産の性質、その使用の状況、当該財産に関する犯人以外の者の権利の有無その他の事情からこれを没収することが相当でないと認められるときは、その

価額を犯人から追徴することができる。

8.6.6 第 22 条

- 13 法人の代表者又は法人若しくは人の代理人，使用人その他の従業者が，その法人又は人の業務に関し，次の各号に掲げる規定の違反行為をしたときは，行為者を罰するほか，その法人に対して当該各号に定める罰金刑を，その人に対して各本条の罰金刑を科する。
- (1) 前条第三項第一号（同条第一項第一号に係る部分に限る.），第二号（同条第一項第二号，第七号及び第八号に係る部分に限る.）若しくは第三号（同条第一項第二号，第七号及び第八号に係る部分に限る.）又は第四項（同条第三項第一号（同条第一項第一号に係る部分に限る.），第二号（同条第一項第二号，第七号及び第八号に係る部分に限る.）及び第三号（同条第一項第二号，第七号及び第八号に係る部分に限る.）に係る部分に限る.） 十億円以下の罰金刑
 - (2) 前条第一項第一号，第二号，第七号，第八号若しくは第九号（同項第四号から第六号まで又は同条第三項第三号（同条第一項第四号から第六号までに係る部分に限る.）の罪に係る違法使用行為（以下この号及び第三項において「特定違法使用行為」という.）をした者が該当する場合を除く.）又は第四項（同条第一項第一号，第二号，第七号，第八号及び第九号（特定違法使用行為をした者が該当する場合を除く.）に係る部分に限る.） 五億円以下の罰金刑
 - (3) 前条第二項 三億円以下の罰金刑
- 14 前項の場合において，当該行為者に対してした前条第二項第六号の罪に係る同条第五項の告訴は，その法人又は人に対しても効力を生じ，その法人又は人に対してした告訴は，当該行為者に対しても効力を生ずるものとする。
- 15 第一項の規定により前条第一項第一号，第二号，第七号，第八号若しくは第九号（特定違法使用行為をした者が該当する場合を除く.），第二項，第三項第一号（同条第一項第一号に係る部分に限る.），第二号（同条第一項第二号，第七号及び第八号に係る部分に限る.）若しくは第三号（同条第一項第二号，第七号及び第八号に係る部分に限る.）又は第四項（同条第一項第一号，第二号，第七号，第八号及び第九号（特定違法使用行為をした者が該当する場合を除く.）並びに同条第三項第一号（同条第一項第一号に係る部分に限る.），第二号（同条第一項第二号，第七号及び第八号に係る部分に限る.）及び第三号（同条第一項第二号，第七号及び第八号に係る部分に限る.）に係る部分に限る.）の違反行為につき法人又は人に罰金刑を科する場合における時効の期間は，これらの規定の罪についての時効の期間による。