

モビリティ分野におけるデータ取り扱いに関する
ガイドライン（案）

令和3年3月12日

目次

1.	はじめに.....	3
	(1) 背景	3
	(2) 本書で想定する主体とシステム	4
	(3) 本書の位置づけとねらい	5
	(4) 本書作成の方法	6
	(5) 本書の構成.....	10
2.	データ生成に寄与した者の心証への配慮.....	13
	(1) リスクと対応の方向性.....	13
	(2) データ取り扱い方法	13
	1) 説明と同意取得	13
	2) 利用権限の配分	13
	3) 「データの所有権」に関する業界での議論.....	14
3.	データ生成に寄与した者の営業上の利益の保護.....	15
	(1) リスクと対応の方向性.....	15
	(2) データ取り扱い方法	15
	1) 同意形成	15
	2) 監査等による実効性確保	16
4.	データの安全確保	17
	(1) リスクと対応の方向性.....	17
	(2) データ取り扱い方法	17
	1) セキュリティ管理策の実施.....	17
	2) セキュリティ認証制度の活用	18
5.	個人情報の保護.....	19
	(1) リスクと対応の方向性.....	19
	(2) データ取り扱い方法	19
	1) 個人情報の該否判断	19
	2) 同意の取得等	20
	3) 業界におけるコンセンサスの形成.....	20
6.	データに関する標準化.....	22
	(1) リスクと対応の方向性.....	22
	(2) データ取り扱い方法	22
	1) データフォーマットの標準化	22
	2) 国際的な基準や標準との調和および貢献	23

7.	著作権の保護	24
(1)	リスクと対応の方向性	24
(2)	データ取り扱い方法	24
1)	利用許諾の取得	24
2)	契約等による制限	24
8.	データの品質確保	26
(1)	リスクと対応の方向性	26
(2)	データ取り扱い方法	27
1)	データの品質	27
2)	データの鮮度	27
3)	データの継続期間	28
9.	データの信頼性確保	29
(1)	リスクと対応の方向性	29
(2)	データ取り扱い方法	29
1)	データ信頼性の向上に資する取組	29
2)	サービス利用者へのサービス品質の提示	30

1. はじめに

(1) 背景

我が国が目指すべき未来社会の姿として Society5.0 が提唱されている。Society5.0 とは、サイバー空間とフィジカル空間を高度に融合させたシステムにより経済発展と社会的課題の解決を両立する社会である。Society5.0 では、これまでの情報社会（Society4.0）から分野横断的な知識や情報の共有・連携が期待されている。

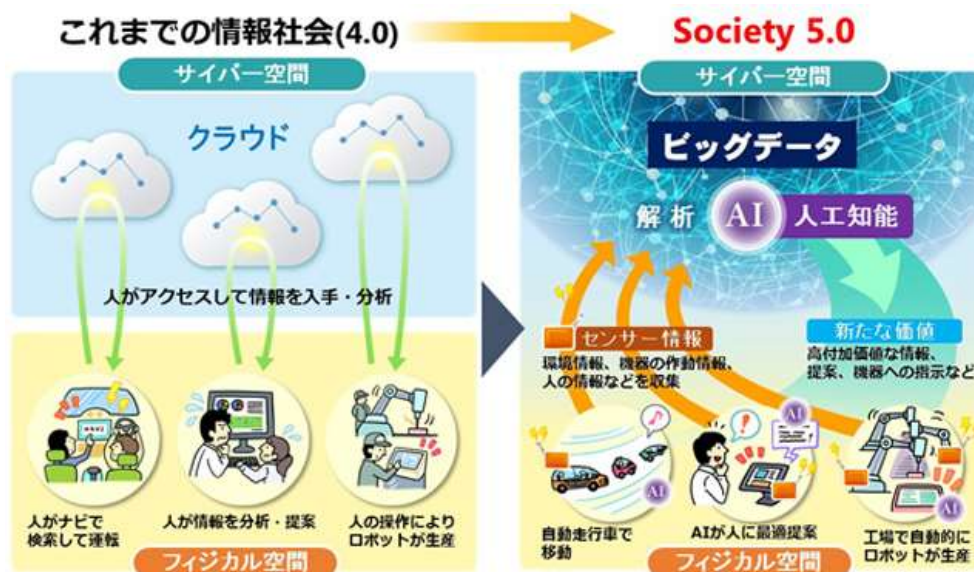


図 1 Society5.0 のイメージ

(出典) 内閣府 Web サイト (https://www8.cao.go.jp/cstp/society5_0/)

ひとたびヒトやモノの情報がサイバー空間でつながれば、社会的な課題を克服したり、今までにない新たな価値を生み出すことが可能になる。モビリティ関連データも、様々なモビリティサービスに利用することで道路交通の諸問題の解決につながるほか、モビリティも街や暮らしの一部であることから、モビリティの分野を超えて都市機能の高度化などにもつながり得る。

ここで課題は、はじめにヒトやモノの情報を、様々な用途に利活用可能なサイバー空間に乗せることが必要という点である。モビリティ関連データも現在、多くの場合は限られた主体による限られた用途にしか使われていない。というのもモビリティ関連データを広く流通させようとする、個人情報保護やセキュリティ、データの生成に寄与した者への心理上あるいは事業上の配慮、品質の確保など、様々な観点から考慮すべきことがある。これらデータを取り扱う際の負担が、モビリティ関連データを広く流通させることを躊躇させている一因と考えられる。

(2) 本書で想定する主体とシステム

モビリティ関連データ（以下、「データ」という。）を取り扱う形態は多種多様と考えられるが、本書では以下のように単純化したデータ取り扱いモデルを想定する。

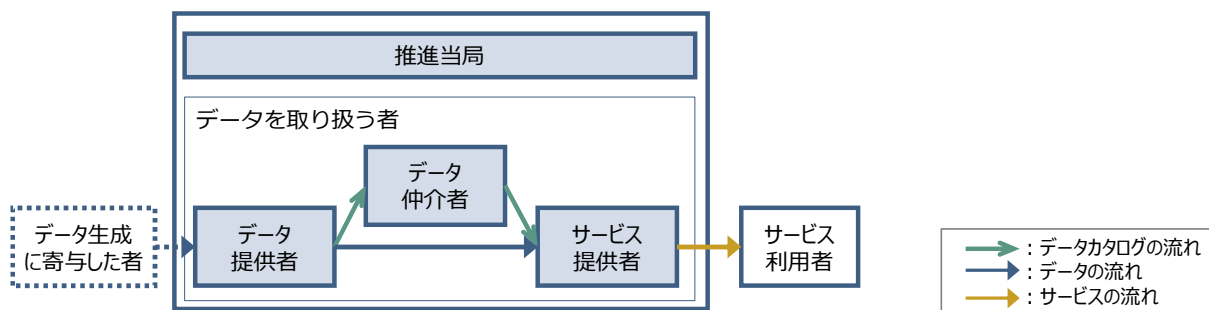


図 2 本書で想定するデータ取り扱いモデル

表 1 本書で想定するデータ取り扱いの関係主体

関係主体	役割
データ提供者	<ul style="list-style-type: none"> 自ら事業推進等によって生成されたデータ、あるいはデータ生成に寄与した者との連携により生成されたデータを、官民での利活用のために提供する者。
データ仲介者	<ul style="list-style-type: none"> データ提供者よりメタデータを収集し、潜在的なサービス提供者にデータカタログを提供する者。（マーケットプレイス型）。 メタデータをデータ仲介者が集め、オープン化することによって、サービス提供者が使いたいデータを見つけやすくなり、サービス提供者のニーズとデータ提供者をマッチングさせる仕組みを提供する。
サービス提供者	<ul style="list-style-type: none"> データ仲介者を介してマッチングしたデータ提供者からデータの提供を受け、サービスを提供する者。
推進当局	<ul style="list-style-type: none"> 直接的にデータを活用する立場ではなく、データ提供者、データ仲介者、サービス提供者がデータの流通と利活用の促進をしやすい環境整備に寄与する法律や制度設計を行う者。
データ生成に寄与した者	<ul style="list-style-type: none"> データ提供者が提供するデータの生成に、何らかの形で関係した者。 その者がいなければデータ提供に係るデータは存在しなかったという関係であり、データ提供者は様々な観点でデータ生成に寄与した者への配慮が必要な場合がある。
サービス利用者	<ul style="list-style-type: none"> サービス提供者が提供するサービスを利用する者。

(3) 本書の位置づけとねらい

「データの取り扱い」とはここでは、「データに対する一連の作業（収集、保管、加工・処理、提供、廃棄）」とした。データを取り扱う者（即ち、データ提供者、データ仲介者、サービス提供者）は、それぞれ民間であれば自らの利潤、官であれば所管事業の目的に即してデータを自律的に取り扱うと考えられる。

しかし、その枠外にいる主体（即ち、データ生成に寄与した者、サービス利用者）は直接的にデータの取り扱いに関与することは困難なため、不適切なデータの取り扱いにより自らの権利を侵害されたり、不利益を被る場合もある。

そこで本書は、データの不適切な取り扱いによる他主体の権利侵害あるいは不利益を防止するため、データを取り扱う主体が最低限遵守すべきデータ取り扱い方法を明確化することを目的とする。

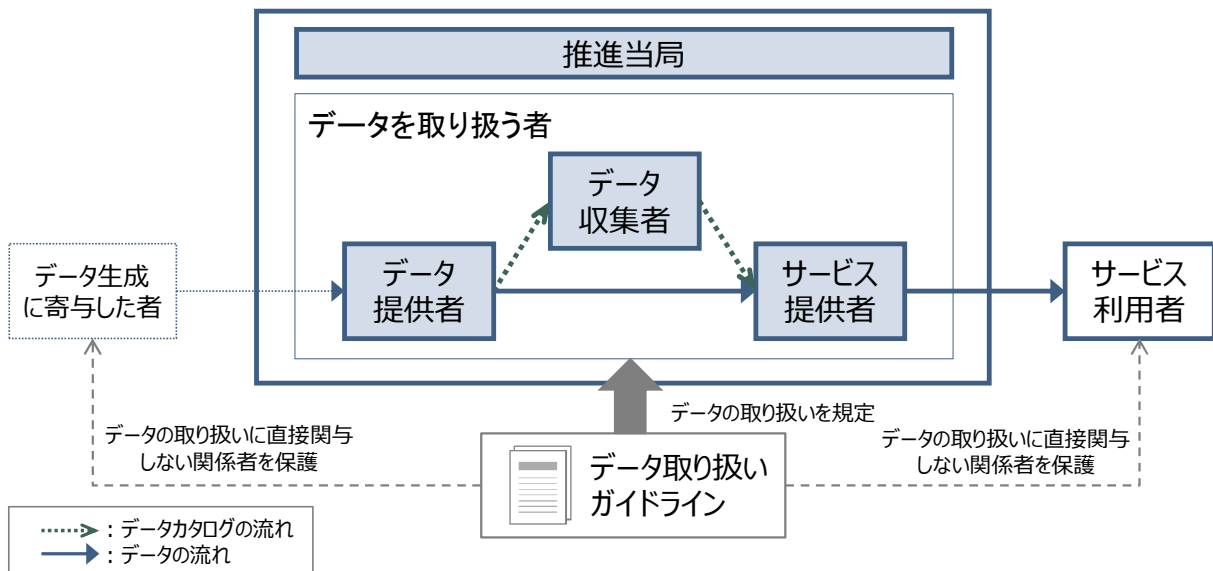


図 3 本書の位置づけ

なお、本書はデータを取り扱う者を拘束する目的ではなく、これらの者によってリファレンスとして用いられることを目的としたものである。

また、データ利活用が進むにつれてデータを取り扱う者の主体、その枠外にいる主体や、それらを取り巻く環境も変化すると考えられるため、本書も継続的に更新していくことを想定している。

(4) 本書作成の方法

参考として、本書の作成方法について述べる。過年度に戦略的イノベーション創造プログラム（SIP）においてモビリティ関連データの利活用に関する検討が行われていることから、これら過年度の検討成果から利活用のユースケースを抽出し、本検討におけるユースケースとして再定義した。

表 2 参照した過年度 SIP 検討成果

年度	関連業務報告書
平成28年度	戦略的イノベーション創造プログラム（ダイナミックマップのサービスプラットフォームに必要な調査及び検討）
平成29年度	「戦略的イノベーション創造プログラム（SIP）・自動走行システム」自動走行システムの実現に向けた諸課題とその解決の方向性に関する調査・検討におけるダイナミックマップサービスプラットフォームの試作及び検証
平成30年度	「戦略的イノベーション創造プログラム（SIP）・自動走行システム」自動走行システムの実現に向けた諸課題とその解決の方向性に関する調査・検討におけるダイナミックマップサービスプラットフォームの試作及び検証
令和元年度	「戦略的イノベーション創造プログラム（SIP）第2期／自動運転（システムとサービスの拡張）／自動運転・運転支援に係るアーキテクチャの設計及び構築のための調査研究／地理系データ流通促進ポータルサイト構築、「東京臨海部実証実験」地域及び移動・物流サービス連携等のための都市部における地理系データ整備・構築」に係る委託業務

再定義した9分野23ユースケースより商用車ユースケース（トラック運転者の安心・安全な運転環境につながる情報提供）、一般車ユースケース（車両（ドライバー）への高度な情報提供）、および歩行者ユースケース（分かりやすく円滑な移動のための情報提供）を選定した。

表 3 定義したモビリティ関連データ利活用ユースケース

分野	No	ユースケース	分野	No	ユースケース
物流	1	過疎地域での効率的な輸配送	自動車	12	車両（ドライバー）への高度な情報提供
	2	トラック運転者の安心・安全な運転環境につながる情報提供	農業	13	地図情報を活用したドローン飛行
	3	他分野のデータ基盤(SIP4D)との連携		14	地図情報を活用した農機の走行
	4	通行実績情報の蓄積	電力/通信	15	独自の地図情報や図面の共有化
パーソナルナビ	5	ストレスフリーな観光のためのアプリケーション		16	道路占用の現況確認における道路3D情報の活用
	6	ドアツードアのデマンド型乗り合い交通サービスの提供	建設	17	建設車両の走行ルート最適化
	7	平時・災害時の交通マネジメント		18	道路改築・補修が必要な箇所の抽出
	8	分かりやすく円滑な移動のための情報提供		19	届出書の作成支援
	道路管理	9	観光都市居住者に対する混雑予想に基づくアクティビティパターンと交通手段のレコメンド	20	廃棄物の管理
10		交通流異常の検知	自治体	21	緊急車両出動支援
11		道路状態異常の検知		22	路面不良や街路樹メンテナンス
			インフラ/エリア管理	23	予測情報を活用した警備業務の支援

以下に、選定した3つのユースケースのイメージを示す。

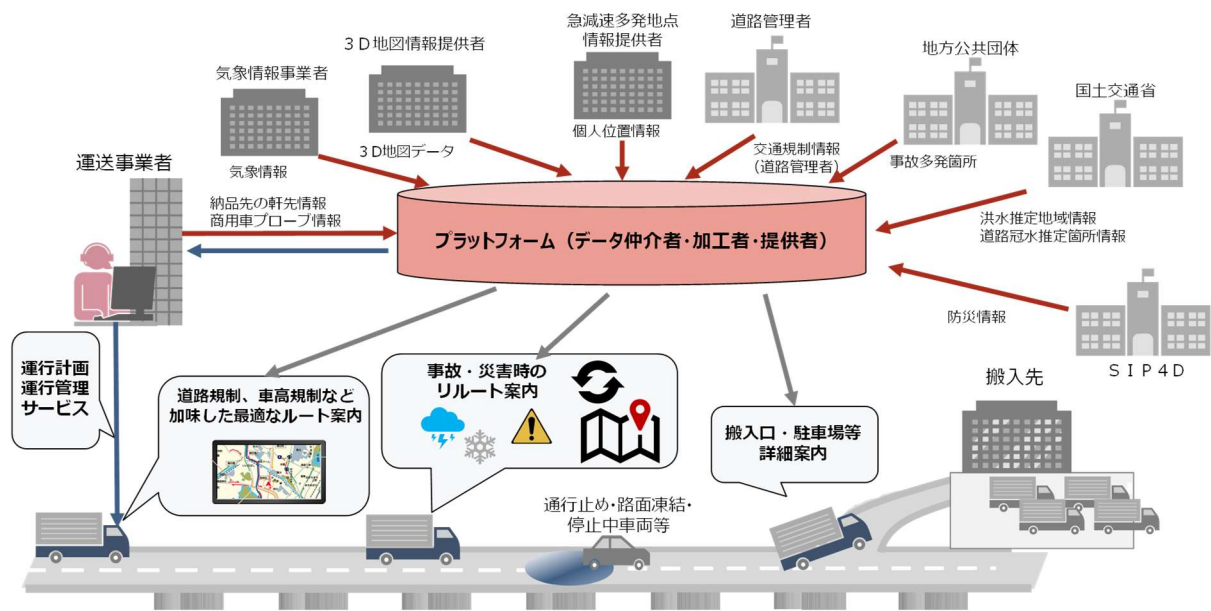


図 4 商用車ユースケース (トラック運転者の安心・安全な運転環境につながる情報提供)

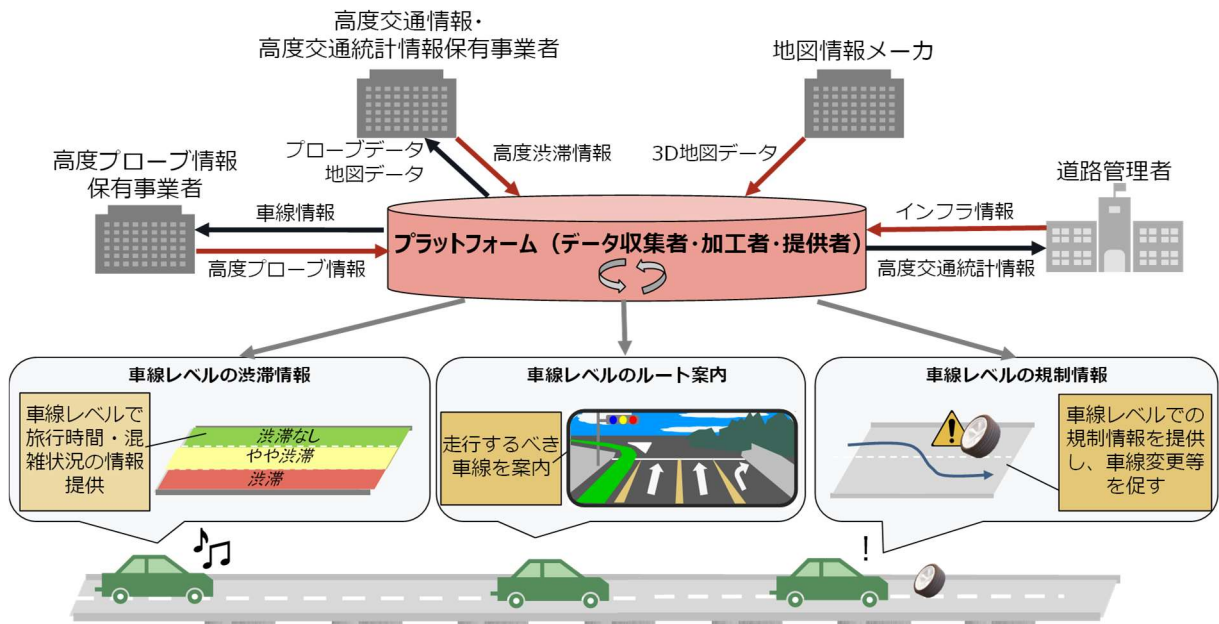


図 5 一般車ユースケース (車両 (ドライバー) への高度な情報提供)

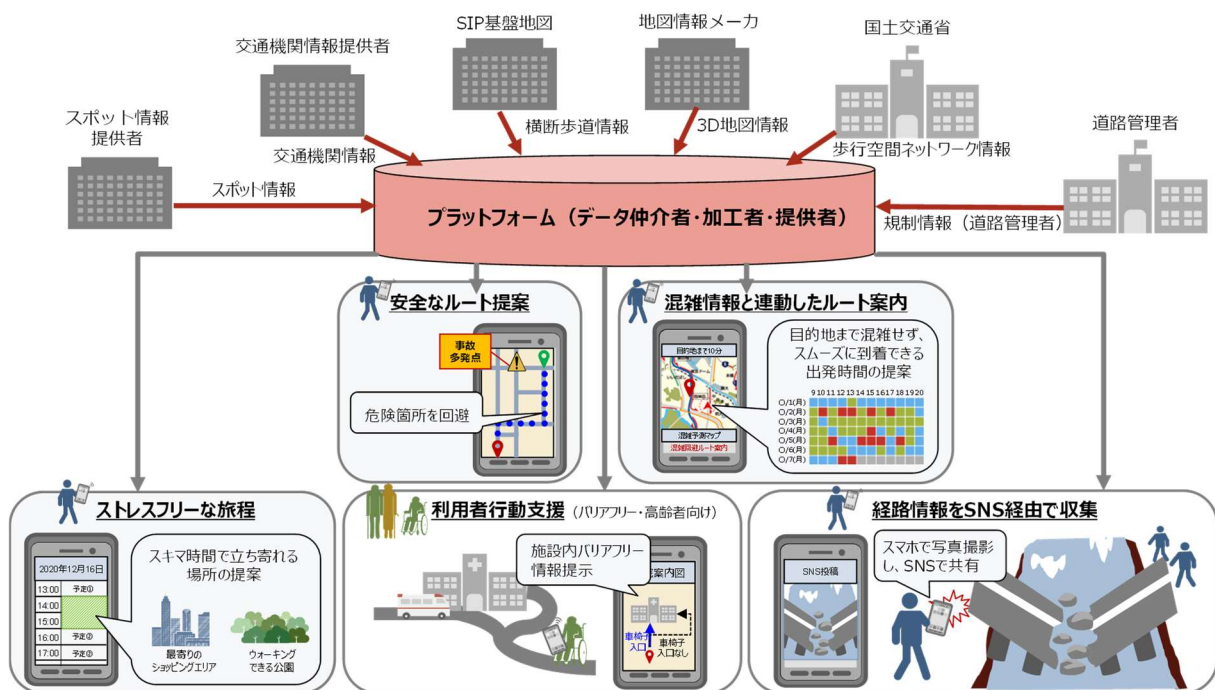
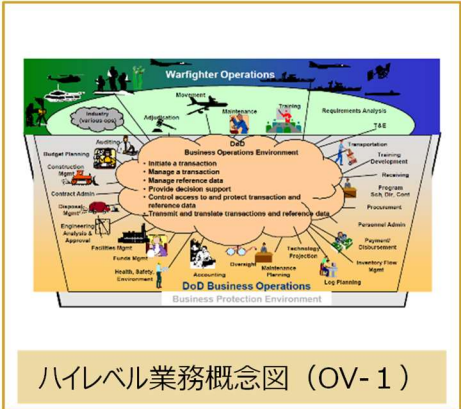


図 6 歩行者ユースケース（分かりやすく円滑な移動のための情報提供）

これら3つのユースケースについて Society5.0 リファレンスアーキテクチャによる可視化を行い、課題分析を行った。具体的には、3つのユースケースを、米国国防総省が開発したアーキテクチャ・フレームワーク（DoDAF¹）を活用し、DoDAFで定義されている各ビューにより可視化した。本検討で想定した、Society5.0 リファレンスアーキテクチャと DoDAF の各ビューとの関係を次ページに示す。

¹ DoDAF：米国国防総省アーキテクチャ・フレームワーク。統一モデリング言語（UML）をベースとして使用し、システムの構造をビジュアルに表現する記法。

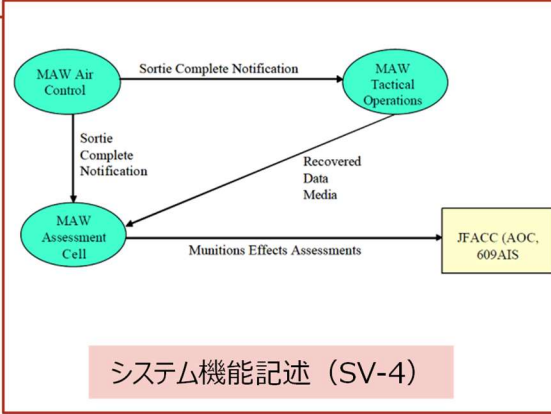
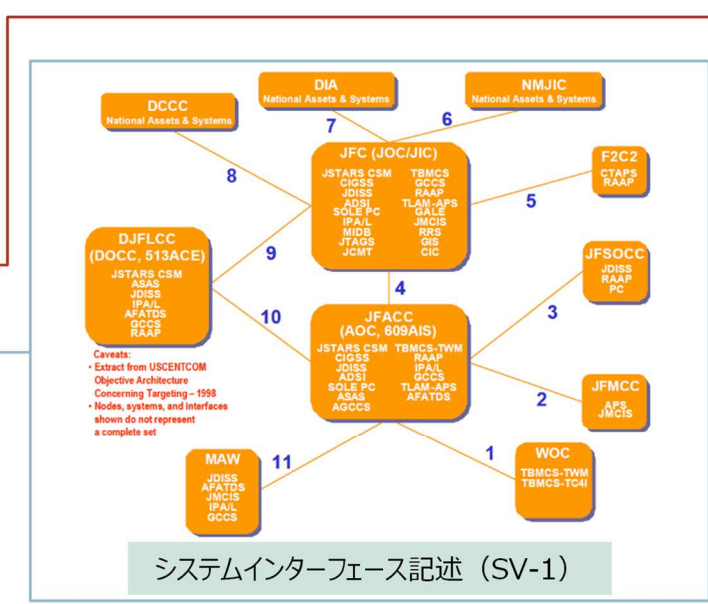
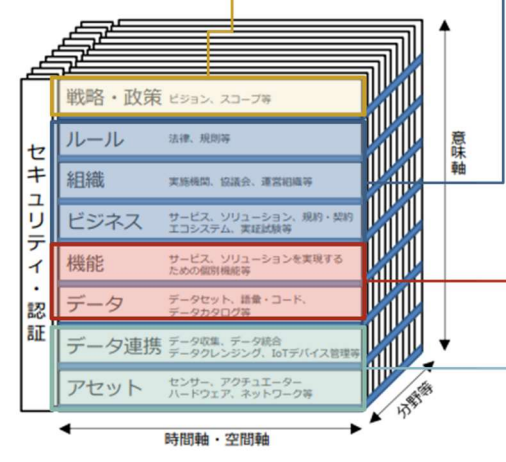
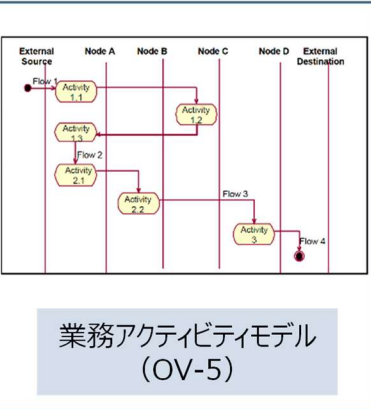
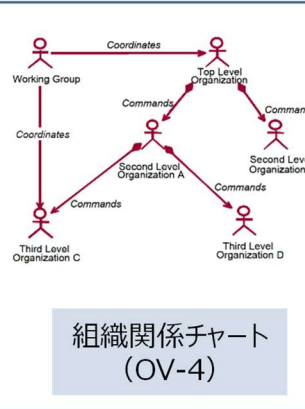


A base fact could be:
 "Battle Damage Assessment consists of three activities: Conduct Battle Damage, Conduct Munitions Effects Assessment, and Recommend Restrike"

Derived facts could be:
 "Recommend Restrike activity cannot be completed before a Battle Damage Assessment Report has been completed."
 "Recommend Restrike activity cannot be completed before a Munitions Effects Assessment Report has been completed."

A derivation used to derive this derived fact above would be:
 A Restrike Recommendation is based on facts contained in Battle Damage Assessment Reports, and Munitions Effects Assessment Reports

業務ルールモデル (OV-6a)



(出典)IPA「参照アーキテクチャ調査報告」(<https://www.ipa.go.jp/files/000010248.pdf>)より作成

図 7 Society5.0 リファレンスアーキテクチャと DoDAF の各ビューとの関係

上記で示した3つのユースケースにおいて想定されるリスクのうち、データ取り扱いに関するリスクを、以下に示す8つのリスクに集約し整理した上で、また関係各所へのヒアリング結果等も考慮しつつ、その対応方策を検討して本書としてとりまとめた。本書の出発点は3つのユースケースではあるが、本書の記載にあたっては3つのユースケース以外にも適応できるよう汎用性をもたせるよう留意した。

(5) 本書の構成

本書ではデータ取り扱いにおいて想定される以下の8つのリスクそれぞれに対して、各章においてその対応方法を記載している。

集約したリスク	対応の方向性
① データを不適切に収集することで、データ生成に寄与した者の心証を害する	<ul style="list-style-type: none"> データ提供者は、データ生成に寄与した者に説明を行い、同意を取得する 場合によってはデータ収集に寄与した者との間でデータ利用権限の取り決めを行う
② データを不適切に提供することで、データ生成に寄与した者の営業上の利益を損う	<ul style="list-style-type: none"> データ提供者は、データ生成に寄与した者との間で合意した以外の提供先に提供せず、また合意した事項以外の利用目的に用いられないようにする
③ 意図せずデータのセキュリティを損うことで、サービス品質が確保できない、あるいはデータの生成に寄与した者の心証、利益を損う	<ul style="list-style-type: none"> データを取り扱う者は、適切なセキュリティ基準に従いセキュリティ管理プロセスを構築し、運用する
④ データを不適切に収集・提供することで、個人情報保護法で保護された権利を侵害する	<ul style="list-style-type: none"> データを取り扱う者は、個人情報に該当するデータは個人情報保護法に従い取扱う または、個人情報に該当するデータに適切な匿名加工を施して取扱う
⑤ データを様々な主体から集約して使うことで、サービス品質が確保できない	<ul style="list-style-type: none"> 様々な主体からの集約が想定されるデータについては、データ提供者とサービス提供者と共同でフォーマットや位置参照の方法を標準化する
⑥ データを不適切に利用することで、データの著作権を侵害する	<ul style="list-style-type: none"> 著作権で保護されるデータは、著作権を遵守して取扱う
⑦ データの処理・加工が遅れること（鮮度の低下）により、サービス利用者が予定通りの移動ができない等の不利益が生じる	<ul style="list-style-type: none"> データ提供者とサービス提供者との間で、提供するデータの品質（正確性、完全性、有効性）、鮮度、継続性等について予め確認し、同意する
⑧ 信頼性が不明確なデータを利用することで、サービス品質が確保できない	<ul style="list-style-type: none"> サービス提供者は、サービスに求められる品質が高くない場合に限り信頼性が不明確なデータを利用する、あるいは信頼性を向上させる方策を開発する

図 8 モビリティ関連データ取り扱いにおいて想定されるリスクと対応の方向

また、本書ではデータを取り扱う者が個別に取り組むべき事項（データ取り扱い方法）の他に、業界として取り組むべき事項（ガイドラインの策定、標準化、等）の2種類について記載している。

なお、リスクへの対応は以下の2種類に分類することができる。

- A. データ生成に寄与した者の保護を目的とした対応
- B. サービス品質の向上を目的とした対応

A に該当する対応は、たとえサービスが無償であっても実施すべきと考えられる。一方、B に該当する対応は有償サービスであって高い品質などが求められる場合など選択的に実施することが可能と考えられる。

対応の方向性		A に該当	B に該当
① データ生成に寄与した者の心証への配慮	• データ提供者は、データ生成に寄与した者に説明を行い、同意を取得する。場合によってはデータ利用権限の取り決めを行う	✓	
② データ生成に寄与した者の営業上の利益の保護	• データ提供者は、データ生成に寄与した者との間で合意した以外の提供先に提供せず、合意した事項以外の利用目的に用いられないようにする	✓	
③ データの保護	• データを取り扱う者は、適切なセキュリティ基準に従いセキュリティ管理プロセスを構築し、運用する	✓	✓
④ 個人情報の保護	• データを取り扱う者は、個人情報に該当するデータは個人情報保護法に従い取扱う	✓	
⑤ データに関する標準化	• 様々な主体からの集約が想定されるデータについては、データ提供者とサービス提供者と共同でフォーマットや位置参照の方法を標準化する		✓
⑥ 著作権の保護	• 著作権で保護されるデータは、著作権を遵守して取り扱う	✓	
⑦ データの品質確保	• データ提供者とサービス提供者との間で、提供するデータの品質（正確性、完全性、有効性）、鮮度、継続性等について予め確認し、同意する		✓
⑧ データの信頼性確保	• サービス提供者は、サービスに求められる品質が高くない場合に限り信頼性が不明確なデータを利用する、あるいは信頼性を向上させる方策を開発する		✓

図 9 リスクへの対応の分類

2. データ生成に寄与した者の心証への配慮

(1) リスクと対応の方向性

データ提供者が提供するデータは、その生成に何らかの形で他者が寄与した場合もある²。例えば商用車プローブについては当該商用車を運行している運送事業者等が、データ生成に寄与した者に該当する。この場合、当該データを無断でサービス提供者に提供すると、データ生成に寄与した者の心証を害するおそれがある。

そこでデータ提供者は、データ生成に寄与した者に説明を行い、同意を取得することが望ましい。また、場合によってはデータ生成に寄与した者との間でデータ利用権限の取り決めを行うことが望ましい。

なお、データ提供者が提供するデータが、データ提供者自らの活動のみに基づいて生成された場合には本章は適用されない。

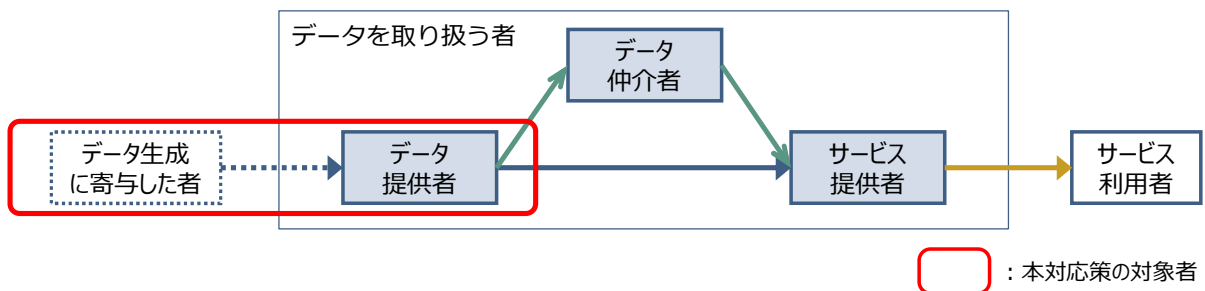


図 10 本章の対象者

(2) データ取り扱い方法

1) 説明と同意取得

実際にデータを提供する前に、データ生成に寄与した者に断りを入れておくことは心証の悪化を回避することに有効と考えられる。

そこでデータ提供者は、データをサービス提供者に提供する際には、予めデータ生成に寄与した者に対して提供するデータの内容、提供先、提供先での利用目的などについて説明し、提供について同意を得ておくことが望ましい。

2) 利用権限の配分

データの生成において、データ生成に寄与した者の寄与度が高い場合などは、デー

² データ生成の寄与には様々な要素があり、例えばデータ生成や価値に対する技術的寄与、データ内容面の寄与、データ生成のコスト負担（経済的寄与）、機器所有権、施設所有権、操作主体、等が挙げられる。これらの要素について寄与の度合いを考慮し、「データ生成に寄与した者」が存在するか個別に判断することとなる。

データ生成に寄与した者がいわゆる「データの所有権」を主張することも想定される。我が国の法制度上、無体物であるデータに所有権は認められていないが、一般的にはデータへのアクセスや利用をコントロールできる権限（つまりデータの利用権限）を主張しているものと理解される。データ生成に寄与した者の活動がなければデータは存在していないことを考慮すると、そうした主張を無視することも公平とはいえないと考えられる。

そこでデータ提供者は、データ生成に寄与した者の主張に一定の合理性がある場合には、データの創出／取得、保存／管理、利用、当事者などの観点から総合判断して、データ生成に寄与した者との間で利用権限の配分を白紙の状態から公平に取り決めることが望ましい。³

3) 「データの所有権」に関する業界での議論

データ提供者とデータを生成に寄与した者が個別にデータ利用権限を交渉して取り決める場合、上記のとおり白紙の状態から公平に取り決めることが原則ではあるが、現実的には両者の力関係やデータの利用権限に対する理解の違いなどから原則どおりに取り決めがなされるとは限らない。

そこで業界において、一般論としていわゆる「データの所有権」、つまりデータの利用権限が双方にそれぞれどの程度分配されるべきものか、ケーススタディなどを通じて議論を行い「相場観」を形成することが考えられる。あるいは、そうした議論の結果をガイドラインなどの形で明確化することが考えられる。

³ 利用権限の分配の具体的な方法や考え方は、IoT 推進コンソーシアムおよび経済産業省が策定した「データの利用権限に関する契約ガイドライン Ver.1.0」（平成 29 年 5 月）などが参考となる。

3. データ生成に寄与した者の営業上の利益の保護

(1) リスクと対応の方向性

データ提供者が提供するデータには、その提供先によってはデータの生成に寄与した者の営業上の利益を損なうおそれがあるものがある。例えばある運送事業者 A の商用車から収集したプローブ情報が競争相手の運送事業者 B に渡った場合、プローブ情報を解析することで運送事業者 A の顧客を知ることができる。そのため運送事業者 A からみれば、プローブ情報の提供が顧客を失うリスクとなる。同様に、プローブ情報に CAN⁴情報が含まれていれば、これを解析して競争相手が製造する自動車の動作特性を把握し得る。歩行者のナビゲーションを目的として収集したシェアサイクル情報から、競争相手の営業状況を把握し得る。

そこでデータ提供者は、データ生成に寄与した者との間で合意した以外の提供先に提供せず、また合意した事項以外の利用目的に用いられないようにすることが望ましい。

なお、データ提供者が提供するデータが、データ提供者自らの活動のみに基づいて生成された場合には本章は適用しない。

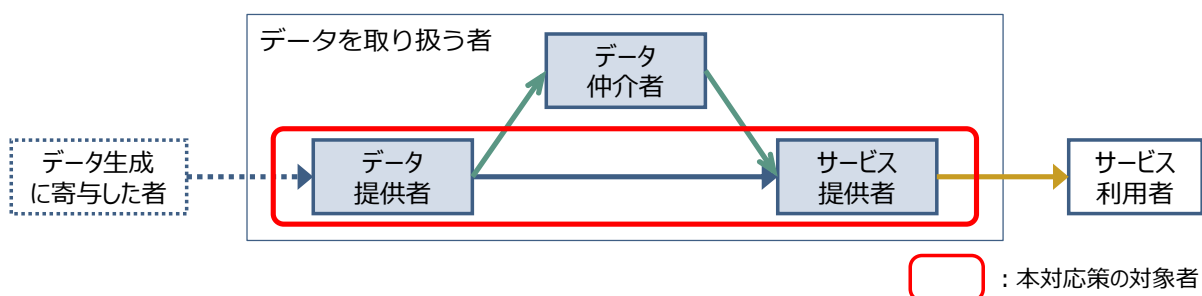


図 11 本章の対象者

(2) データ取り扱い方法

1) 同意形成

上記 2. により、データ提供者はデータの生成に寄与した者との間でデータの提供先や利用目的等について同意を得ていると考えられる。同意した提供先にのみデータを提供することは当然であるが、データは提供先からも転々流通する可能性があることから提供先に対しても同意内容を継承させることが必要と考えられる。

そこでデータ提供者は、提供に先立ち提供データの内容、第三者提供禁止、目的外

⁴ CAN (Controller Area Network) : 自動車などの機械の内部で、電子回路や各装置を横断的に接続するための通信規格の一種。自動車では、電子制御装置やエンジン、ブレーキ、センサーなどの部品をつなぎ、各部の状態を伝達したり制御情報を送るために使われる。

利用禁止、目的外加工等禁止、提供データへの権限（開示、内容の訂正、追加等の可否）、派生データの扱い、契約終了後の扱い（破棄、消去等）等⁵について予め提供先のサービス提供者と同意することが望ましい。この同意条件は、上記2. でデータ生成に寄与した者から得た同意の範囲内とする。

2) 監査等による実効性確保

データは無体物であり同一のものが容易に複製できるため、サービス提供者も自らがデータを利用しつつ、さらにデータを同意に反して外販して二重の利益を得るようなことも容易に実行することができる。データ提供者にとっては同意が誠実に履行されているか外部から把握することは難しく、これがデータ提供を躊躇させる一因にもなっていると考えられる。

そこで同意内容の実効性を高めるため、同意内容に基づいたデータ利用を行っているか確認するため、サービス提供者に対して書面（電磁的記録を含む。）による報告あるいは書面（電磁的記録を含む。）の開示を求めたり、サービス提供者に対して実地監査を行う方法も考えられる。その場合は、事前の同意条件に書面（電磁的記録を含む。）の報告や開示、実地監査権についても盛り込んでおくことが必要と考えられる。

また、提供したデータについて、不正競争防止法で規定する「限定提供データ」の要件⁶を満たすようにすることで法的保護の対象とし、サービス提供者への牽制効果を得ることも考えられる。これらの要件を満たした場合、サービス提供者が不正の利益を得る目的、またはデータ提供者に損害を加える目的（図利加害目的）で、同意内容に違反してデータを使用または開示した場合、データ提供者はサービス提供者に対して差止請求（不正競争防止法第3条）、損害賠償請求（同第4条）等の救済を受けることが可能である。

⁵ 同意すべき事項については、経済産業省が策定した「AI・データの利用に関する契約ガイドライン 1.1 版」（令和元年12月）などが参考となる。

⁶ 「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（不正競争防止法第2条第7項）。そのため限定提供データの要件は、①業として特定の者に提供する情報であること、②電磁的方法により相当量蓄積されていること、③電磁的方法により管理されていること、④技術上又は営業上の情報であること、⑤秘密として管理されていないこと、の5つとなる。

4. データの安全確保

(1) リスクと対応の方向性

データ仲介者は、データカタログを潜在的なサービス提供者に広く提供するため、インターネットにおいてデータカタログを公開すると考えられる。また、実際のデータのやり取りはデータ提供者とサービス提供者の間で、システム同士を接続し自動でデータ交換を行う API (Application Programming Interface) や、電子メール等によるインターネット経由のやりとり、あるいは記憶媒体によるやりとりが発生すると考えられる。こうした組織外とのやりとりに紛れてマルウェアあるいは不正アクセス等によるサイバー攻撃を受けると、意図せずデータの安全（機密性、完全性、可用性）を損ないかねない。データが漏洩するなど機密性が損なわれた場合、当該データの生成に寄与した者の心証あるいは利益を損なうおそれがある。データが改ざんされるなど完全性が損なわれると、そのデータを用いても意図したサービスが提供できない。データが暗号化されたり破損されるなど可用性が損なわれた場合はサービスの停止につながりかねない。

そこで、データを取り扱う者は、(場当たりにセキュリティ管理策を講じるのではなく)適切なセキュリティ基準に従いセキュリティ管理プロセスを構築し、運用することで、データの安全を継続的に確保することが望ましい。

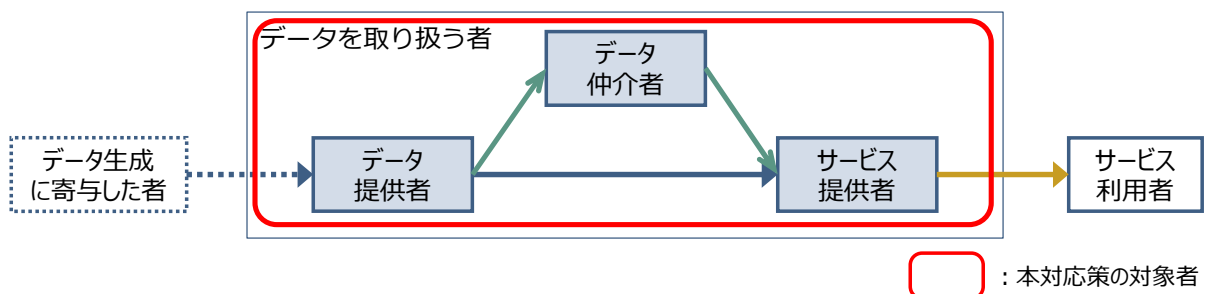


図 12 本章の対象者

(2) データ取り扱い方法

1) セキュリティ管理策の実施

データを取り扱う者は、自らが実施しているセキュリティ対策の度合いに応じて、以下のように段階的にセキュリティ対策を高度化していくことが必要と考えられる⁷。

まず、データを取り扱う者は早急に実施可能なセキュリティ対策として、ソフトウェアの最新化、ウィルス対策ソフトの導入、パスワード管理の強化、共有設定の見直

⁷ セキュリティ対策の段階的な高度化については、情報処理推進機構（IPA）が作成した「中小企業の情報セキュリティ対策ガイドライン」が参考となる。

し、脅威や攻撃の手口の把握等を実施することが望ましい。

次に、経営者が情報セキュリティ基本方針の作成と組織内への周知、上記セキュリティ対策の実施状況の把握、問題箇所への対策の決定等、組織的な取り組みを開始することが望ましい。

最後に、本格的なセキュリティ管理策の実施へ移行させることが望ましい。情報セキュリティに関する責任部門の決定、組織内の情報システムの予算化、関係主体からの期待や要求、想定されるリスク等を考慮したセキュリティ規則の決定⁸を行うことが望ましい。さらに、委託契約時には、契約書面による情報セキュリティ方針の確認と委託先の監督の実施や、組織内における情報セキュリティ対策の実施状況の定期的な点検を行い、改善を行うことも望ましい。なお、既にセキュリティ管理プロセスを設けている場合には、データの提供、利用時に同プロセスに即した形でデータのセキュリティの確認が業務の中で定常的に行われているかの点検を行うことが望ましい。

更に高度なセキュリティ対策が求められる場合は、強化策として、情報セキュリティに関わる情報収集と組織内での共有、安全なウェブサイトの構築、クラウドサービス利用時のセキュリティ対策の実施、外部のセキュリティサービスや技術的対策事例の活用を行うことが望ましい。さらに組織内では、詳細なリスク分析を実施することで、問題点を洗い出すことも望ましい⁹。

2) セキュリティ認証制度の活用

データを取り扱う者が関係主体とデータカタログやデータをやりとりする際、相手方が上記のような PDCA サイクルに基づくセキュリティ管理システムにより継続的にデータの保護に努める者であるか否か、外部から把握することは一般的には難しいと考えられる。

この場合、ISO/IEC 27001 等¹⁰のセキュリティ認証の取得状況は、セキュリティ管理システムの妥当性の判断材料となる。

⁸ セキュリティ規則の決定には、法律や規制、情報セキュリティ事故の傾向等の外部要因と、組織の経営方針、情報セキュリティ基本方針、管理体制等の内部要因を考慮する必要がある。

⁹ リスク分析を行う際のチェックリストの一例として、情報処理推進機構（IPA）が作成した「中小企業の情報セキュリティ対策ガイドライン」の「リスク分析シート」等が存在する。

¹⁰ ISO/IEC 27001:2013（情報セキュリティマネジメントシステム—要求事項）のこと。セキュリティ認証制度としてはその他、ISO/IEC 27017:2015（ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）、ISO/IEC 27018:2019（PII プロセッサとして作動するパブリッククラウドにおける個人識別情報(PII)の保護のための実施基準）等が存在する。

5. 個人情報の保護

(1) リスクと対応の方向性

「モビリティ関連データ」には個人に関する情報も含まれる場合がある。例えば一般車から収集するプローブ情報には車両（の所有者）あるいはドライバーと紐づくIDや車両の走行に伴って生成される走行履歴などが含まれ、個人に関する情報と考えられる。この個人に関するデータが個人情報に該当する場合には、これを不適切に扱うことで個人情報の保護に関する法律（以下、「個人情報保護法」という。）等に規定された本人の権利を侵害するおそれがある。

そこで、データを取り扱う者は、個人情報に該当するデータは個人情報保護法に規定された手続きに従い取り扱うことが必要である。

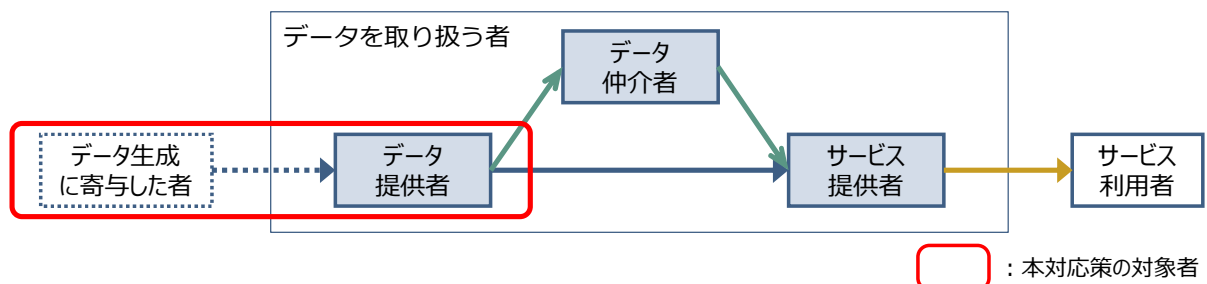


図 13 本章の対象者

(2) データ取り扱い方法

1) 個人情報の該否判断

個人情報保護法等の規定は、取り扱うデータが法律上の「個人情報」の定義（個人情報保護法第2条第1項）に該当する場合にのみ適用される。

そこでデータ提供者は、提供するデータが個人情報に該当するか判断することが必要である。すなわち、データが「当該情報に含まれる氏名、生年月日その他の記述等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¹¹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。）」（同第2条第1項第1号）あるいは「個人識別符号が含まれるもの」（同第2条第1項第2号）のいずれかに該当する場合には、当該データは個人情報となる¹²。例えば一般

¹¹ 行政機関の場合には行政機関の保有する個人情報の保護に関する法律（以下、「行政機関個人情報保護法」という。）が適用される。行政機関個人情報保護法では他の情報との照合可能性を判断する際に容易性が求められない点に注意が必要である（行政機関個人情報保護法第2条第2項第1号）。即ち、行政機関においては容易に照合できなくとも照合可能性さえあれば当該情報は文理上、個人情報に該当することとなる。

¹² どのような情報が個人情報に該当するか、個人情報保護委員会が策定した「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成28年11月）等が参考となる。

車から収集するプローブ情報には、一般的にはそれ単独では特定の個人を識別できる記述等は含まれていないと考えられるが、ID や走行履歴などを他の情報（例えば顧客リスト等）と容易に照合することで特定の個人を識別できる場合には個人情報となる。またドラレコ等で撮影した画像や映像を収集する場合には、画像や映像に映り込んでいる本人が識別できる場合には個人情報となる¹³。

2) 同意の取得等

データが個人情報に該当する場合は、当該のデータは個人情報保護法を遵守した取り扱いが必要となる。

そこでデータ提供者は、サービス提供者に提供するデータが個人情報に該当する場合は、予め本人よりデータ提供に関する同意を得ておくことが必要である（同第 23 条第 1 項）。また、サービス利用者が本人である場合には、サービス利用を申し込む際に併せてサービス提供者経由で同意を取得する方法も考えられる。同意を得るにあたっては、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すことが望ましい。同意は明示的なものであることが望ましく、例えば同意する旨の書面（電磁的記録を含む。）の受領、確認欄へのチェック、ホームページ上のボタンのクリック、等の方法が考えられる。

また、本人から同意を取得していないサービス提供者にデータを提供する場合には、個人情報から生成した匿名加工情報（同第 2 条第 9 項）を生成して提供する方法も考えられる¹⁴。匿名加工情報であれば、本人の同意なくサービス提供者に提供することが可能である。

3) 業界におけるコンセンサスの形成

個人情報の該否判断、本人からの同意取得の方法（説明方法、説明すべき事項（第三者提供先、提供先での利用目的（意義）、等）、同意方法等）、匿名加工の方法や度合い等については、データ提供者がそれぞれ重複して検討するのではなく、業界としてコンセンサスを形成し、これをそれぞれ適用することが効率的と考えられる。

そこで業界団体などにおいて、データ提供のユースケースを設定し、その際の上記の具体的方法の判断基準や手続きを業界ガイドラインとして定めることが考えられ

¹³ 画像や映像の取り扱いについては、IoT 推進コンソーシアム、総務省、経済産業省が策定した「カメラ画像利活用ガイドブック Ver.2.0 版」（平成 30 年 3 月）等が参考となる。

¹⁴ 匿名加工情報の生成方法については、個人情報保護委員会が策定した「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」（平成 28 年 11 月）、個人情報保護委員会事務局が策定した「匿名加工情報 パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」（平成 29 年 2 月）等が参考となる。

る。

匿名加工情報とは、措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。特に匿名加工情報の生成方法については個人情報保護委員会規則で定める基準に従うこととされているが（同第 36 条第 1 項）、その具体的な方法については業界ごとに設立する認定個人情報保護団体において策定する個人情報保護指針にて定めることが期待されている（同第 53 条第 1 項）。個人情報保護指針の策定には消費者の意見を代表する者、その他の関係者（データ提供者、サービス提供者それぞれの代表者、等）の意見を聴いて、また個人情報保護法の規定の趣旨に沿って定めることが望ましい。

6. データに関する標準化

(1) リスクと対応の方向性

例えばサービス提供者が日本全国を対象としたサービスを提供しようとした場合、データの地理的なカバレッジを確保するために同種のデータを複数のデータ提供者から収集する場合が想定される。このときデータフォーマットや地物などの位置を指し示す方法（位置参照方式）がバラバラだとサービス提供者は統一的にデータを扱うことができない。そのためデータ変換にコストを要したり、また提供するサービスにも制約やサービス品質への影響も想定される。

そこで、様々な主体からの集約が想定されるデータについては、データ提供者とサービス提供者の連携の下、フォーマットや位置参照の方法を標準化することが望ましい。

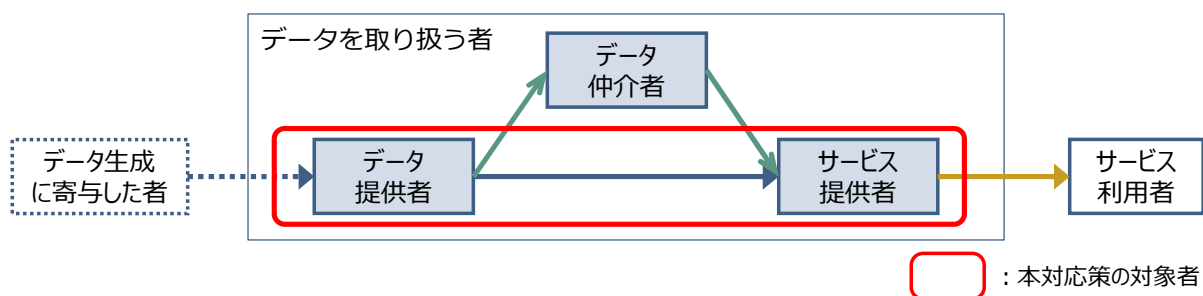


図 14 本章の対象者

(2) データ取り扱い方法

1) データフォーマットの標準化

データ提供者が提供するデータは、基本的にはサービス提供者に提供することを一義としたものではなく、データ提供者が自ら他の用途で利用するために収集したものである場合が多いと考えられる。そのためサービス提供者が一方的にデータフォーマットを定めても、データ提供者がそれに応えられる保証はない。

そこで業界において、データ提供者とサービス提供者の合議により標準化すべきデータ項目を特定し¹⁵、特定したデータ項目についてデータフォーマットを標準化することが望ましい。またデータフォーマットのみならず、データフォーマットにどのようなデータを格納すべきか定めたデータ辞書の標準化も併せて行うことが望ましい。

¹⁵ 標準化には多大な労力と時間を必要とする。そのため標準化すべきデータ項目は網羅的に設定するのではなく必要性に照らして絞り込むことが望ましい。標準化の必要性はサービス提供者が現にサービスに利用しようとしているデータであること、複数のデータ提供者から収集せざるを得ない実情があること、複数のサービス提供者が利用を見込んでいること等を総合的に考慮することが必要と考えられる。

2) 国際的な基準や標準との調和および貢献

自動車あるいは ITS 分野では国際的な調和を図るべく、国連欧州経済委員会の下部に位置する自動車基準調和世界フォーラム（WP29）において国際的な基準を、あるいは国際標準化機構（ISO）の技術委員会（ISO/TC22、ISO/TC204）等において国際標準化を、それぞれ策定している。

そこで上記の基準化・標準化活動においては既存の国際標準あるいは国際協調の取組みを尊重することが望ましい。また、既存の国際基準や標準が存在しない場合には国内の標準化活動を通じて定めた標準を積極的に国際基準、あるいは国際標準化の場に提案し、国際基準化・国際標準化を主導することが望ましい。

7. 著作権の保護

(1) リスクと対応の方向性

SNS などに掲載されるデータには写真や映像が含まれており、これらのデータを加工、分析するには著作権による許諾が必要となる。例えば、SNS などにアップロードされた画像を解析して、施設や道路、標識などの新設情報を分析し、歩行者ナビゲーションに資するデータを生成することは、著作権保護の観点から著作権者であるデータ生成に寄与した者に無断で実施することはできない。同様に、Web サイト上に閲覧可能な形で掲載されている画像や動画、各種データ等を収集し、分析して新たなデータを生成するためには、各 Web サイトが設定し開示している情報の再利用条件の規定の遵守が必要である。

そこで、データを取り扱う者は、著作権で保護されるデータは著作権を遵守して取り扱うものとする。

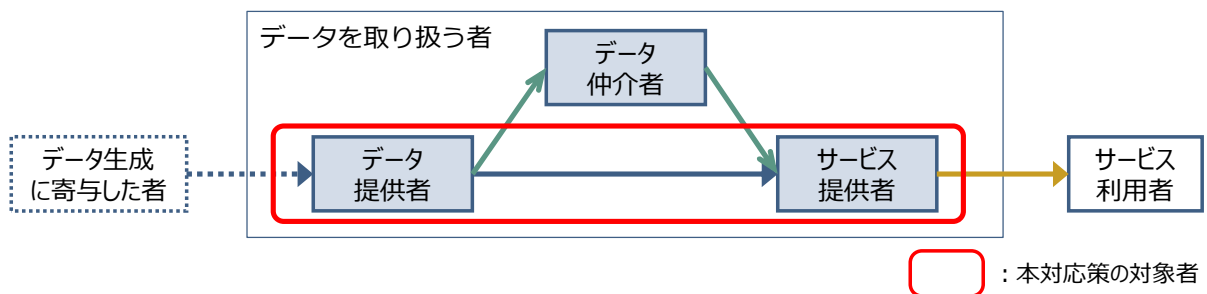


図 15 本章の対象者

(2) データ取り扱い方法

1) 利用許諾の取得

データ提供者が SNS などに投稿された画像等を解析するために、データ生成に寄与した者である当該 SNS サービスの利用者に対して、その都度個別に利用許諾を取することは困難である。

そのため、データ提供者は予めサービス利用規約にて当該サービスを利用して投稿されたデータの利用許諾を取ること、具体的には、投稿されたデータの著作権をデータ提供者が有することとすることが望ましい。

2) 契約等による制限

データの流過程において、著作権の許諾を得た主体が判別できなくなり、結果的にサービス提供者がその責を負ってしまうことのないよう、データの流通の過程においては、主体間で著作権の取り扱いに関して取り決めが求められる。

そのため、サービス提供者がデータ提供者からデータの提供を受ける場合、有償、無償によらず、契約事項として著作権の取り扱いに関する条項を設けることが望ましい。

8. データの品質確保

(1) リスクと対応の方向性

サービス利用者に提供するデータは、センサー等の機器も含み、データ生成に寄与した者の差異により品質に差がでることがある。例えば、同種のセンサーであってもメーカーや型番等に応じて検出できる単位に差があることや、データ生成に寄与した者の主観により入力された値に差が出ることなどがあり、品質を一定に保てないことがある。

また、サービス利用者に提供するデータは、サービス利用者がジャストインタイムで自身の移動やそのための判断に利用できるだけのデータの鮮度を求められるケースもある。さらに、事象の特性に応じて有効期限が設定されているデータもある。例えば、事故等による通行止めの情報であれば、その事故処理が終わり通行止め解除されるまでが有効期限となるが、データの処理・加工が遅れることでサービス利用者に通行止めのデータが提供できない、もしくは通行止めが解除されているのに、いつまでも通行止めのデータを提供してしまうことで、サービス利用者が予定通りの移動ができない等の不利益が生じるおそれがある。

また、サービス利用者による対価の支払いの有無によらず、契約により一定期間データを定期的に提供するサービスである場合は、データ提供者はサービス提供者との間で取り決めたデータの提供期間の間、同頻度でのデータ提供を維持することが求められる。

そこでデータ提供者とサービス提供者との間で、提供するデータの品質（正確性、完全性、有効性）、鮮度、継続性等について予め確認し、合意することが望ましい。なお、データ取得や生成に時間を要するようなデータを取り扱う場合は、提供するサービスが成立する最低限の鮮度を考慮したサービスを設計することも重要である。

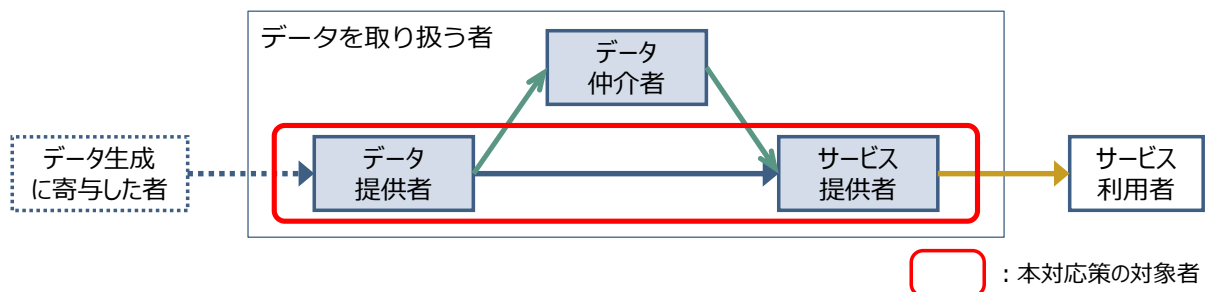


図 16 本章の対象者

(2) データ取り扱い方法

1) データの品質

サービス提供者がサービス利用者に提供するデータの品質は、サービス提供者が責任を負うこととなる。そのため、サービス提供者は自社のサービス品質を確保するための要件を明らかとし、データ提供者との間で提供を受けるデータの品質について合意しておくことが安全である。また、サービス利用者が提供されたデータを元に不利益を被ることなく利用するためには、事前に提供するデータの品質についてサービス利用者と合意しておくことが安全である。

データの品質とはデータの正確性、完全性、有効性¹⁶とされており、これらが確保できない場合に、データ品質に関して法的責任を負うことがあり得る。特にデータ提供が有償契約である場合においては、データの品質に瑕疵担保責任（契約不適合責任）の適用も可能と考えられており、賠償責任を負うこともあり得る。¹⁷

- 正確性：事実と異なるデータが含まれていないこと
- 完全性：データが全て揃っていて欠損や不整合がないこと
- 有効性：計画された通りの結果が達成できるだけの内容を伴っていること

そのためデータ提供者は、提供するデータの品質（正確性、完全性、有効性）の度合いについて、予めサービス提供者に説明し、合意を得ることが望ましい。

2) データの鮮度

何かしらの事象を表すデータの場合、その事象の開始時刻から終了時刻までの間で、時々刻々と状況が変化し、その状況に応じてサービス利用者がとるべき行動や判断が変わることがある。サービス利用者に不利益を生じさせないためには、事象の状況の変化を常に把握し、必要なタイミングで提供するデータを更新し、サービス利用者が常に最新の状況を把握できることが求められる。

そこで、提供するデータが1分～1時間程度の周期で更新が必要なデータである場合には、達成すべき鮮度についても合意を得ることが望ましい。

¹⁶ 経済産業省が策定した「AI・データの利用に関する契約ガイドライン 1.1版」（令和元年12月）においては、データの品質を正確性、完全性、有効性でとらえている。

¹⁷ そのためデータ提供者がどの範囲まで責任を負うか合意しておくことが望ましい。この場合、「データ提供者が品質について一切保証しない」と規定を置く場合も想定されるが、故意または重大な過失があれば責任を問われる可能性がある。また、「データの品質維持を努力義務」とした場合も、努力がなければ債務不履行責任を負う可能性がある点に注意が必要である。さらに、データに起因してサービス提供者がサービス利用者等との間で紛争となった場合に備え、損害金や費用の負担について予め合意しておくことが望ましい。

3) データの継続期間

サービス提供者がサービス利用者に提供するサービス内容として、一定期間継続して最新のデータを提供することを保証している場合は、データ提供者とサービス提供者においても、その期間は継続して最新のデータを提供することが求められる。

そこで、提供するデータが（ワンショットでなく）継続的に提供すべきデータである場合には、最低限維持すべき継続期間についても合意を得ることが望ましい。

9. データの信頼性確保

(1) リスクと対応の方向性

データ提供者が提供するデータには、データ生成に寄与した者の故意、または過失に関わらず、そのデータ内容を裏付ける証拠が確認できないデータが含まれることがある。また、SNS での投稿内容のデータであれば、データ生成に寄与した者の主観的な考えに基づくデータであり、データ生成に寄与した者によるバイアスがかけられているデータが含まれることがある。さらにはごく短時間で変化する事象に対して、複数のデータ生成に寄与した者が時間差でその事象を観測した場合にもほぼ同時帯でありながら異なるデータが生成されることが生じ得る。

例えば SNS への投稿内容において、当該事象が発生していないのにも関わらず、さもその事象が発生していると誤認させる投稿や、同じ事象 A に対して、投稿者 B と投稿者 C とで移動手段が異なることで生成されるデータに違いが生じることが起こる。

そこでサービス提供者は、サービスに求められる品質が高くない場合に限り信頼性が不明確なデータを利用する、あるいは信頼性を向上させる方策を検討することが望ましい。

なお、データ提供者が提供するデータが、データ提供者自らの活動のみに基づいて生成された場合には本章は適用しない。

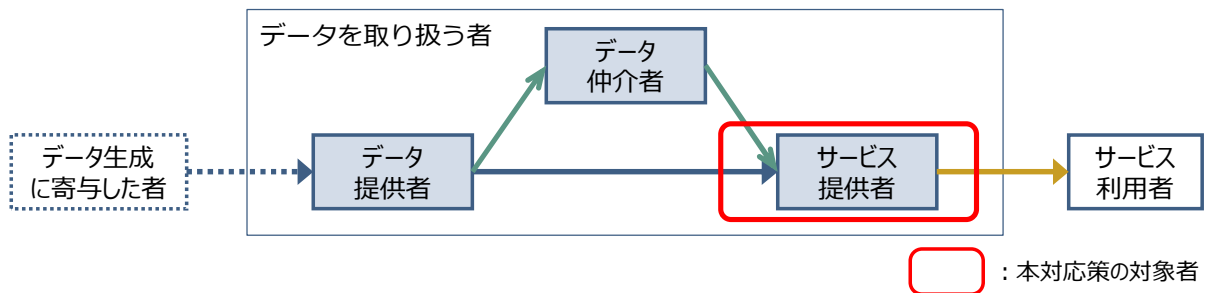


図 17 本章の対象者

(2) データ取り扱い方法

1) データ信頼性の向上に資する取組

SNS データのように、データ提供者に対して不特定多数のデータ生成に寄与した者が存在し、そのデータを活用したサービスを提供する場合には、投稿されている内容の信頼性を確保するために、データ量により担保する方法、しきい値を設けることにより担保する方法などが考えられる。

そこでサービス提供者は、SNS データ等の信頼性が不明確なデータを利用してサ

サービス提供する場合には、多数のデータを活用したり、フィルタを活用してノイズとなる投稿を除去したり、比較的信頼性が高いと考えられる画像データを解析して活用するなど、信頼性を向上する手法を開発し、適用することが望ましい。

2) サービス利用者へのサービス品質の提示

収集したデータから何かしらの事象を特定し、そのデータをサービス利用者提供するにあたっては、サービス利用者が当該データを受け取った際に、サービス利用者が自ら判断可能な情報を付け加え、判断を委ねることが考えられる。

そこでサービス提供者は、高い信頼性が求められないサービス、あるいは他に現実的な収集手段がない場合については、サービスの内容が実際の状況とは異なる場合があるなどの注意事項を、予めサービス利用者へ提示しておくことが望ましい。