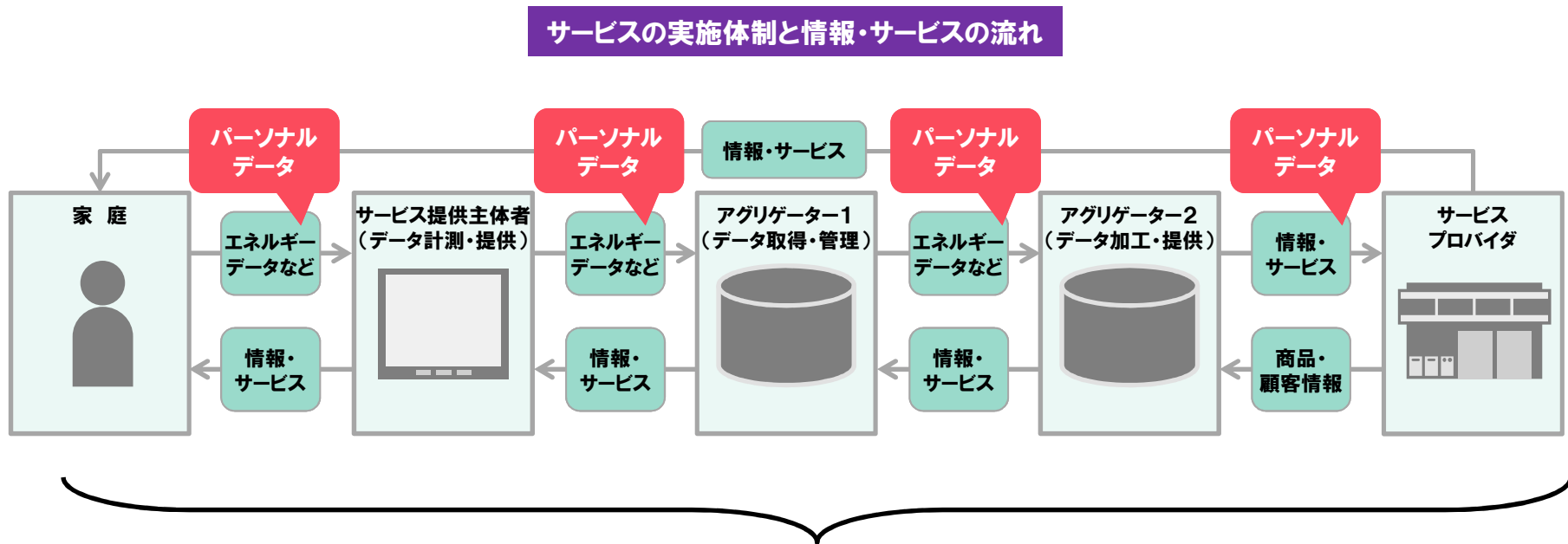


3. HEMSデータの利活用と情報保護のあり方の検討

3-1. 本ワーキンググループの背景

① 本事業における情報保護に関する課題

- HEMSを活用した事業モデルにおいては、HEMSにより取得されたエネルギーデータ(HEMSデータ)に加え、様々なパーソナルデータ等を利用することが想定されるため、個人特定のリスクが存在する。
- したがって、情報保護の観点からHEMSデータの利活用のあり方を検討する必要がある。



資料2の事例調査の結果、各事業モデルにおいても、基本的な仕組みは同じ。

3-1. 本ワーキンググループの背景

② 本事業において取り扱うHEMSデータの概要

- HEMSを活用してインセンティブを付与する際には、3種類のデータを活用する可能性があることを確認した。
- これらは、個人特定のリスクがある、パーソナルデータと位置づけることができる。
- したがって、これらのデータの情報保護のあり方を検討する。

データ	内容	具体例	情報のカテゴリー*1, 2	
			識別	特定
エネルギーデータ	家庭全体のエネルギー消費量	1時間あたりの主幹の電力消費量	×	×
	エリア(部屋)や機器別のエネルギー消費量	個人の寝室の照明の電力消費量	○	×
世帯構成員に関するデータ	個人に関する情報	氏名、性別、年齢など	○	○
	世帯全体に関する情報	世帯人数、地域、保有設備など	○	×
その他 パーソナルデータ	上記以外に家庭内で 取得可能な個人に関する情報	購買履歴、健康管理(体重、脈拍…)など	○	○
		携帯電話の位置情報など	○	×

*1:経済産業省「パーソナルデータに関する検討会 技術検討ワーキンググループ報告書」(2012.12.10)による。

「特定」:ある情報が誰の情報であるかが分かること。

「識別」:ある情報が誰か一人の情報であることが分かること。

*2:対象データ自体の利用におけるリスクについて、事務局にて評価を試みたもの。他のパーソナルデータと組合せることで生じるリスクは想定していない。

3-2. 本ワーキンググループの運営について

① ワーキンググループの運営概要

- 本ワーキンググループは“平成25年度HEMS活用によるCO2削減ポイント構築推進事業”における、HEMSデータ利活用と情報保護のあり方について各専門の有識者の議論により明確にするものである。
- 委員は、有識者4名で構成する。
- 年1回の開催予定とする。

② ワーキンググループ委員

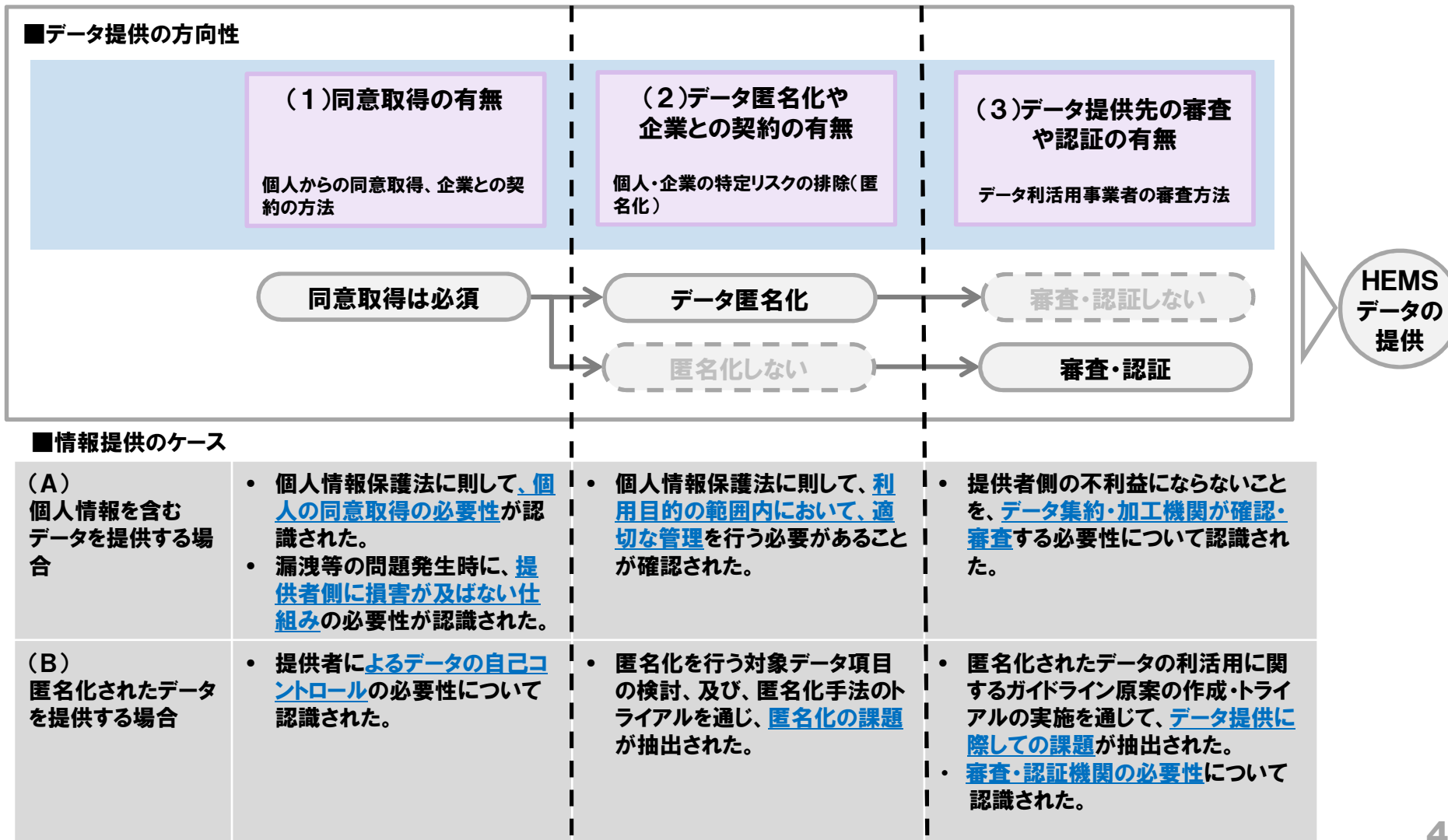
五十音順、敬称略

氏名	所属	役職	専門
喜連川 優	国立情報学研究所	所長	情報管理・利活用
新保 史生	慶応義塾大学 総合政策学部	教授	情報保護法制
田中 英彦	情報セキュリティ大学院大学	学長	情報セキュリティ
那須野 元庸	一般財団法人 日本情報経済社会推進協会	主任研究員	スマートハウス・HEMS

3-3. 情報保護のあり方に関する検討方針

① 昨年度のワーキンググループの検討結果について

- 昨年度の検討においては、下図に掲げる3つの対応項目について検討すべきこと、情報提供のケースにより、実施すべき対応が異なることが確認された。



3-3. 情報保護のあり方に関する検討方針

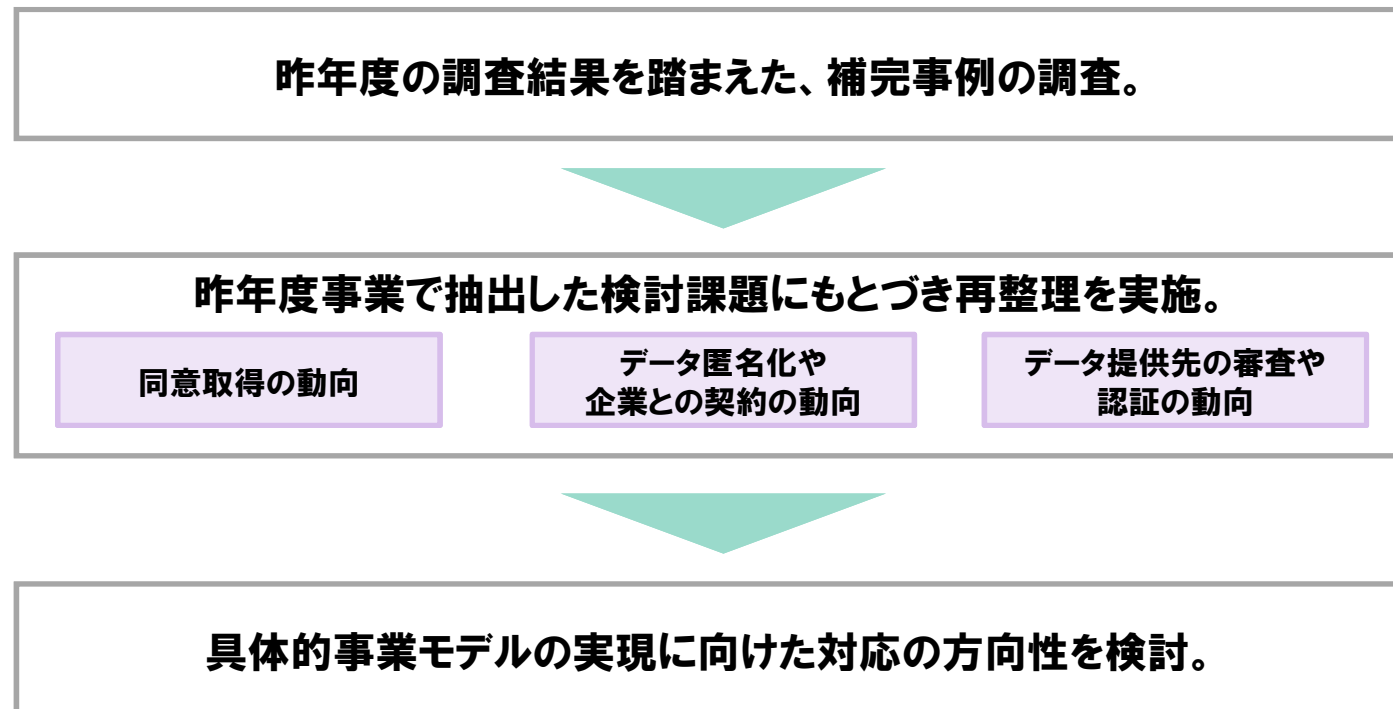
② 今年度のワーキンググループにおける検討方針

A) パーソナルデータに関する事例調査とその情報保護における検討課題の体系的な整理

- 今年度は、国外の事例も含めさらなる調査を行い、昨年度事業で抽出した検討課題の再整理を行う。
- 事例調査については、昨年度の調査結果を踏まえながら、その補完事例について、公開情報を中心に調査する。

B) HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

- 前項Aで洗い出した検討課題について、具体的な事業モデルを想定し、実現に向けた課題を整理するとともに、その対応の方向性について検討する。



3-4. パーソナルデータに関する事例調査とその情報保護における検討課題の整理

- 国内外におけるパーソナルデータに関する事例について、情報保護の観点から調査を行った。その結果、昨年度まとめた3項目：**(1)同意取得**、**(2)匿名化**、**(3)審査・認証**を引き続き検討課題とし、それぞれについて対応の方向性を示していくことで問題ないと確認した。

パーソナルデータに関する事例		主な検討課題			概要
		同意取得	匿名化	審査・認証	
既存事例	A社	○ ※1			補助金交付申請書の同意事項。
	B社	○			サービスの利用規約およびプライバシーポリシー。
	D社	○	○		サービス利用申込時の内容。
	E社	○	○		入居の際のスマートメータに関する事前承諾内容。
	F社	○	○		サービス利用申込時の内容。
	H社	○	○		データ提供サービスにおける事業者向け条項。
類似事例	Suicaデータ提供(日本)	○	○	○	JR東日本によるSuicaデータの販売に関する問題点の検討。
	Tポイント(日本)	○	○	○	Tポイントカードの契約内容、第三者へのデータ提供のあり方についての問題。
	HIPAA(米国)		○		HIPAAにおける医療情報の利用に関する制度について(匿名化の要件など)。
	Midata(英国)	○		○	Midataにおけるデータ利活用の取組みにおける情報保護の考え方について。
	オンラインゲーム(日本)	○			未成年者などの不正アクセスによるパーソナルデータ登録などの問題。
	健康・医療情報の利活用に関する意識調査(日本)	○	○	○	医療情報の利活用における消費者意識についての検討。
	ビッグデータで取り扱う生活者情報に関する意識調査(日本)	○	○		データ利活用に関する消費者意識についての検討。

(※1 ○印は、事例調査のなかで、3項目に関連した記述等があったもの。)

3-5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

1. 同意取得

1-1. 誰にどのような内容の同意を得る必要があるのか？

⇒データの種類に関わらず、利用世帯とサービス提供事業者の契約の際に、世帯主等(世帯構成員全員を代表する者)から、データの利用について包括的に明示の同意(世帯構成員の同意は明示若しくは黙示に取得されている前提)を得ることは必須。

⇒加えて、個人に関する属性情報や、個人に紐づく可能性のあるパーソナルデータ等(特に機微情報)に関しては、活用に際して事業者側で個別に判断し*1、個々の構成員からアプリケーション単位などで、明示の同意を個別に得る等、適切な対応が必要となる場合がある。

*1: 例えば、提供時には個人を特定出来ない形式の情報であっても、予期しない情報との組合せによって、個人の識別が可能となるリスク(例・米国マサチューセッツ州の医療情報(1997)など)が想定される。

⇒また、世帯に制限能力者や親族以外の構成員が存在する場合は、親権者、後見人、法定代理人など、適切な者の同意を取得する旨を、約款等で明確にする。

1-2. 同意を得られやすくする方法は何か？

⇒あらゆるリスクを想定することは困難であるため、匿名化の内容、オプトアウトの手続、データ提供先との契約による統制方法、提供予定事業者(例・ホワイトリスト)、提供範囲の階層による制限、トラブルや苦情対応などについて説明を行う。

⇒また、データ提供者が得られるメリットや、提供しない場合のデメリット、データ利用状況についての情報の提供、自己コントロール権、データ活用行為の公益性などについて説明を行うことによって心理的な抵抗感の緩和に努める。

⇒将来的には、IT総合戦略本部の検討状況を視野に入れて対応する。

3-5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

2. 匿名化

2-1. どこまでの匿名化が求められるか？

⇒HEMSデータを第三者に提供する場合、必要に応じて合理的レベルでの匿名化を行うが、提供の際に合理的に期待される匿名化レベルはケースバイケースである*1。

高レベルの匿名化が求められる場合は、情報の管理や利用を行う組織を、物理的あるいは制度的に分離し、情報を確実に保護することが必要。

*1:将来的には技術等の進展により、暗号化技術などの活用による高度なセキュリティの確保が考えられる。

⇒データの第三者への提供および共同利用等提供においては、FTC*2や総務省の3条件も参考にしつつ、提供先に対する統制(監査請求権、損害賠償請求権の設定等)を明確にして、契約によるリスクの担保を行うことが必要。

*2:FTC(=Federal Trade Commission : 米連邦取引委員会)

2-2. どのようなリスクを回避しなければならないのか？

⇒提供の時点で予期しない情報により提供先で再識別化されるリスクや、HEMSデータ等によって、個々の機器の使用状況や、在宅しているエリアなどが特定される可能性に付随するリスク(訪問販売、勧誘等に利用されるリスクや、防犯上のリスクなど)が想定される。

⇒上記のリスクについては、例えば契約文面に、他のパーソナルデータとの照合の禁止を明示する等、各事業者が対応策を整理しておくことが必要。

⇒さらに想定外のリスクも存在する可能性があるため、結果として個人の利益が侵害された場合に備えて、専門の紛争処理機関の設置等も検討すべきと考えられる。

3-5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

3. 審査・認証

3-1. どのように評価・審査して認証すべきか？

⇒当面の対応としては、データの提供先に対して、適正な(例えばプライバシーマークなど国等の基準に準拠した)第三者認証の取得を要件とすることによって一定の保護水準を確保することが望まれる。

⇒またデータ提供先との契約には、FTCや総務省の3条件も参考にしつつ、提供先との契約による監査請求権、損害賠償請求権の設定、さらに第三国への情報提供を制限する等の要件を盛り込むことが必要。

⇒将来的には、IT総合戦略本部の検討状況を視野に入れて*1対応する。

*1:参考「「パーソナルデータに関する検討会」第1回資料2-2「経済産業省におけるパーソナルデータ利活用の制度・環境整備に向けた取組みと今後の検討課題」
平成25年9月2日

⇒現時点では、個人情報の取扱いに関して専門に監視や紛争処理を行う機関はないが、将来的な第三者機関(プライバシー・コミッショナー)の設立等*2を見据えて、その活用も視野に入れることが必要。

*2:参考「「パーソナルデータに関する検討会」第5回資料3-1「パーソナルデータの利活用に関する制度見直し方針」平成25年12月

3-2. 新たな第三者認証制度の設置を検討する必要があるか？

⇒個人情報保護の運用の適正を図るとともに、データ利活用を推進する観点および、海外との通商面等でも支障が生じないよう、諸外国の個人情報保護制度との関係も考慮した、新たな第三者認証制度の設置について検討する必要がある。

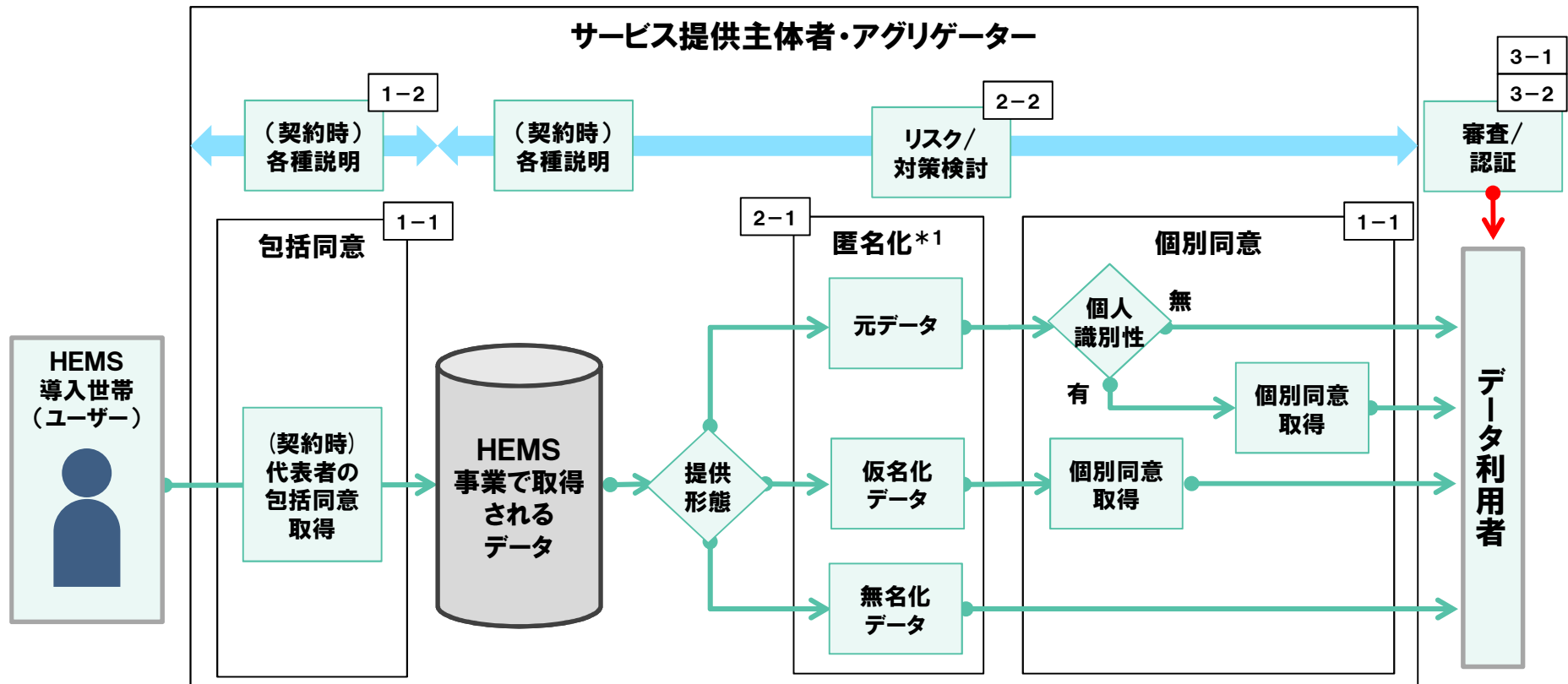
⇒認証制度においては、事業者の評価に関する大まかな基準や、推奨技術、手法等の標準化なども検討すべき。

3-5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

- 本事業で想定するデータ提供のあり方と情報保護に関する対応の方向性は下記の通り。

- 1-1. 原則としてHEMSサービスの契約において、世帯の代表者の包括同意を得る。加えて状況により個別に同意取得を行う。
- 1-2. 事前にオプトアウトの手続、苦情等への対応、メリット、デメリット、利用範囲等の説明を行いユーザーの抵抗感の緩和に努める。
- 2-1. 匿名化は状況に応じて事業者がケースバイケースで判断。情報の管理について運用面等で保護の強化に対応。
- 2-2. 情報保護のリスクについてグレーゾーンとなる場合も含め、あらかじめ想定されるリスクを整理し、他のパーソナルデータとの照合の禁止等の対応策を検討。
- 3-1. データ提供先については適正な第三者認証の取得や、契約による統制によって、一定の情報保護水準を確保。
- 3-2. 将来的な第三者機関や基準の設置を見据えて、利活用を前提に準備を行う。

データ提供の方向性



*1: 匿名化の例については、次頁参照

3-5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案

- 本事業で想定するデータおよび仮名化・無名化の例を示す。

<取得データ>				<仮名化データ>				<無名化データ>	
エネルギーデータ	電気(主幹)	仮名化	電気(主幹)	無名化	電気(主幹)				
	電気(分電盤回路) ※エアコン、冷蔵庫等の個別データを含む		電気(分電盤回路) ※エアコン、冷蔵庫等の個別データを含む		電気(分電盤回路) ※エアコン、冷蔵庫等の個別データを含む				
	ガス		ガス		ガス				
	水道		水道		水道				
世帯構成員に関するデータ	氏名		ID番号		<削除>				
	年齢		年齢		年齢				
	性別		性別		性別				
	世帯人数		世帯人数		世帯人数				
	住所: ●●県●●市●●町●番		住所: ●●県●●市 ※		住所: ●●県●●市 ※				
	築年数		築年数		築年数				
	延床面積	延床面積	延床面積						
その他パーソナルデータ	健康管理情報 (体重、血圧等)	健康管理情報 (体重、血圧等)	健康管理情報 (体重、血圧等)						
	クレジットカード番号	<削除> ※	<削除> ※						
	カードによる購買履歴	カードによる購買履歴	カードによる購買履歴						
	携帯電話の位置情報	<削除> ※	<削除> ※						

※個人を特定できる可能性が高いため削除(又は一部削除)

3-6. <補論>住戸のタイプによるHEMSデータ利用の同意取得パターンについて

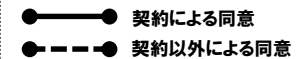
- 個人情報利用に関する同意取得について、住居の所有形態や住戸タイプなど、データ提供者の居住形態に応じて、いくつかのパターンを想定して、契約の枠組みを検討することが有益と考えられる。
- 次頁以降、個々のパターンについて、想定される契約の枠組みの例を提示する。

住宅の所有形態・住戸タイプと契約関係者

		住戸タイプ		
		戸建住宅	集合住宅	シェアハウス
所有形態	分譲住宅	パターン① ・HEMSサービス提供事業者 (・賃主) ・家庭	パターン② ・HEMSサービス提供事業者 (複数の場合も想定される) ・管理組合 ・家庭(複数)	—
	賃貸住宅		パターン③ ・HEMSサービス提供事業者 (複数の場合も想定される) ・賃主 ・家庭(複数)	パターン④ ・HEMSサービス提供事業者 ・賃主 ・入居者(複数)

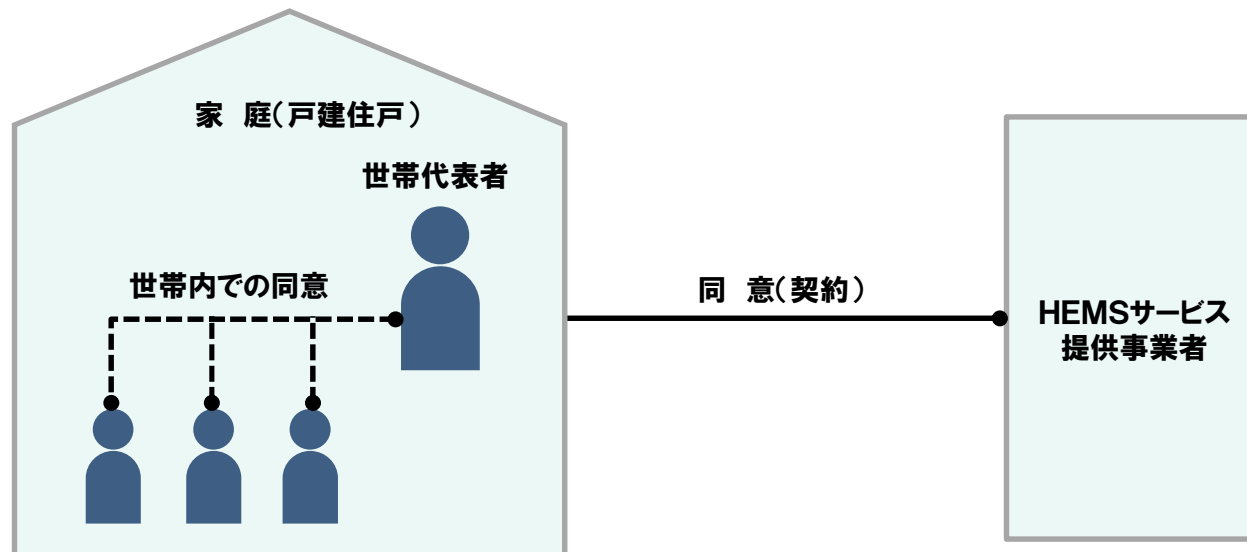
3-6. <補論> 住戸のタイプによるHEMSデータ利用の同意取得パターン(例)①

• 戸建住宅(分譲、賃貸含む)



戸建住宅(分譲、賃貸含む*1)の場合は、基本的に各世帯個別に、代表者の同意を得ることになると考えられる(代表者は、予め他の構成員から同意が得られているという前提)。

本パターンを含め、後述するいずれのパターンにおいても、買い替えや引越などに入居者や世帯が変更となる場合には、退去後のデータの取り扱いについても取り決めが必要である。特にシェアハウスの場合は、ほとんどが定期賃貸住宅契約*2のため、比較的入居者の異動が多いことが想定され、この点については留意が必要と考える。同様に、入居中の構成員の変動(成長や死去、別居等)で、データの取得範囲などが変更されることも想定されるため、そのような場合のデータの取り扱いや手続等についても、予め同意事項に盛り込んでおくべきである。

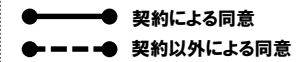


(*1 賃貸住宅の場合、貸主が契約に介在することも考えられるが、実質的に必要性が低いと思われるため、戸建住宅として包含。)

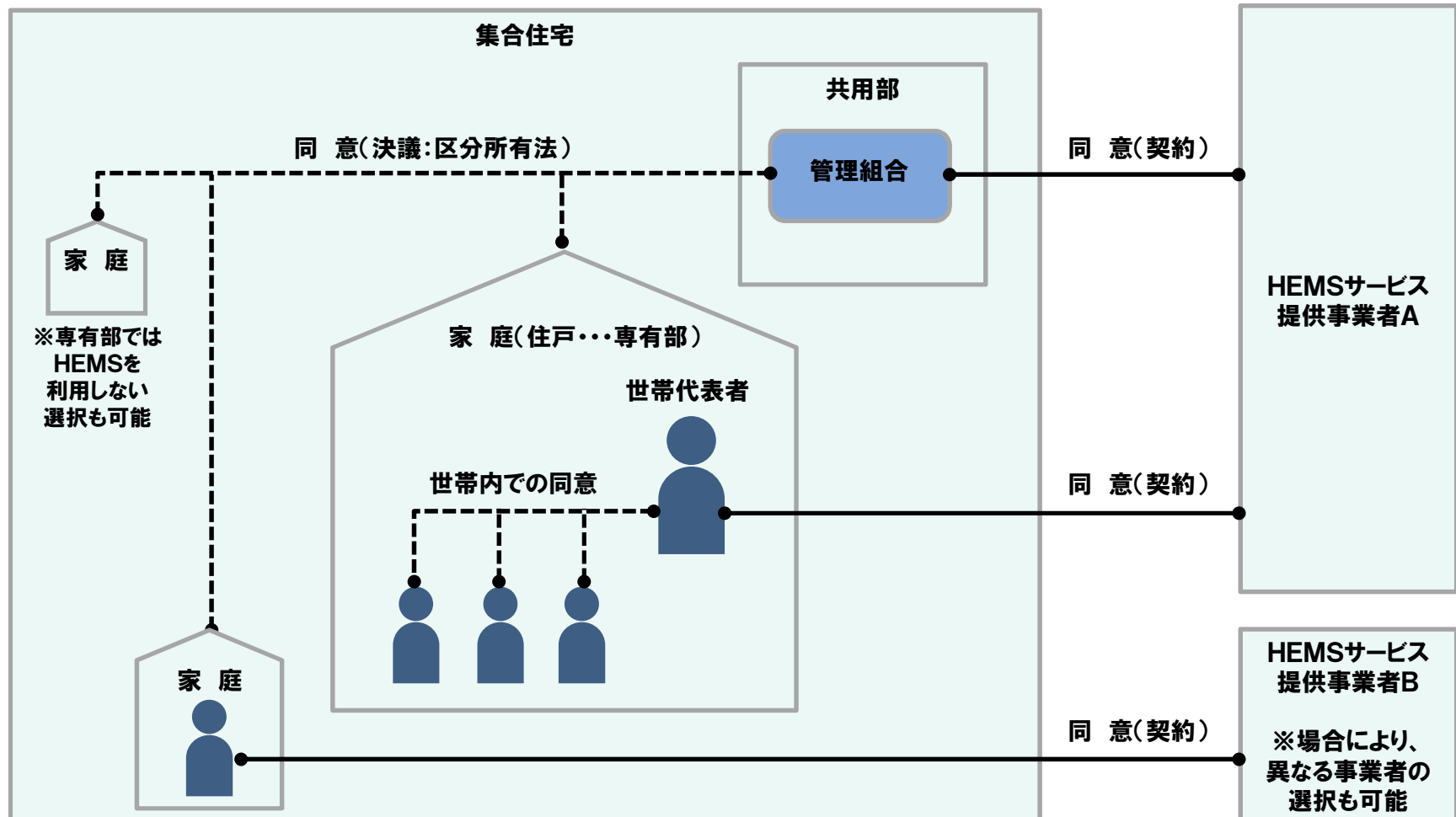
(*2 従来型の賃貸借契約が、正当事由が存在しない限り、家主からの更新拒絶ができず、自動的に契約が更新されるのに対し、定期賃貸住宅契約は、契約で定めた期間の満了により、更新されることなく確定的に賃貸借契約が終了する契約。双方が合意すれば再契約は可能。)

3-6. <補論>住戸のタイプによるHEMSデータ利用の同意取得パターン(例)②

• 分譲型集合住宅

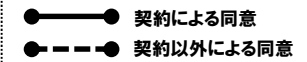


分譲型の集合住宅の場合は、共用部のデータについては、区分所有法に準じた同意取得が必要になるものと考えられる。専有部については個々の世帯との契約となるため、一般的な世帯単位での契約同様、世帯代表者の同意取得が必要と考えられる(場合によっては住戸毎に、サービスの可否や、HEMSサービス事業者が異なるということも想定される)。なお、新築住宅の場合には、分譲の際に、管理規約などと同様に、分譲事業者によって予め同意を得る方法が現実的と思われる。

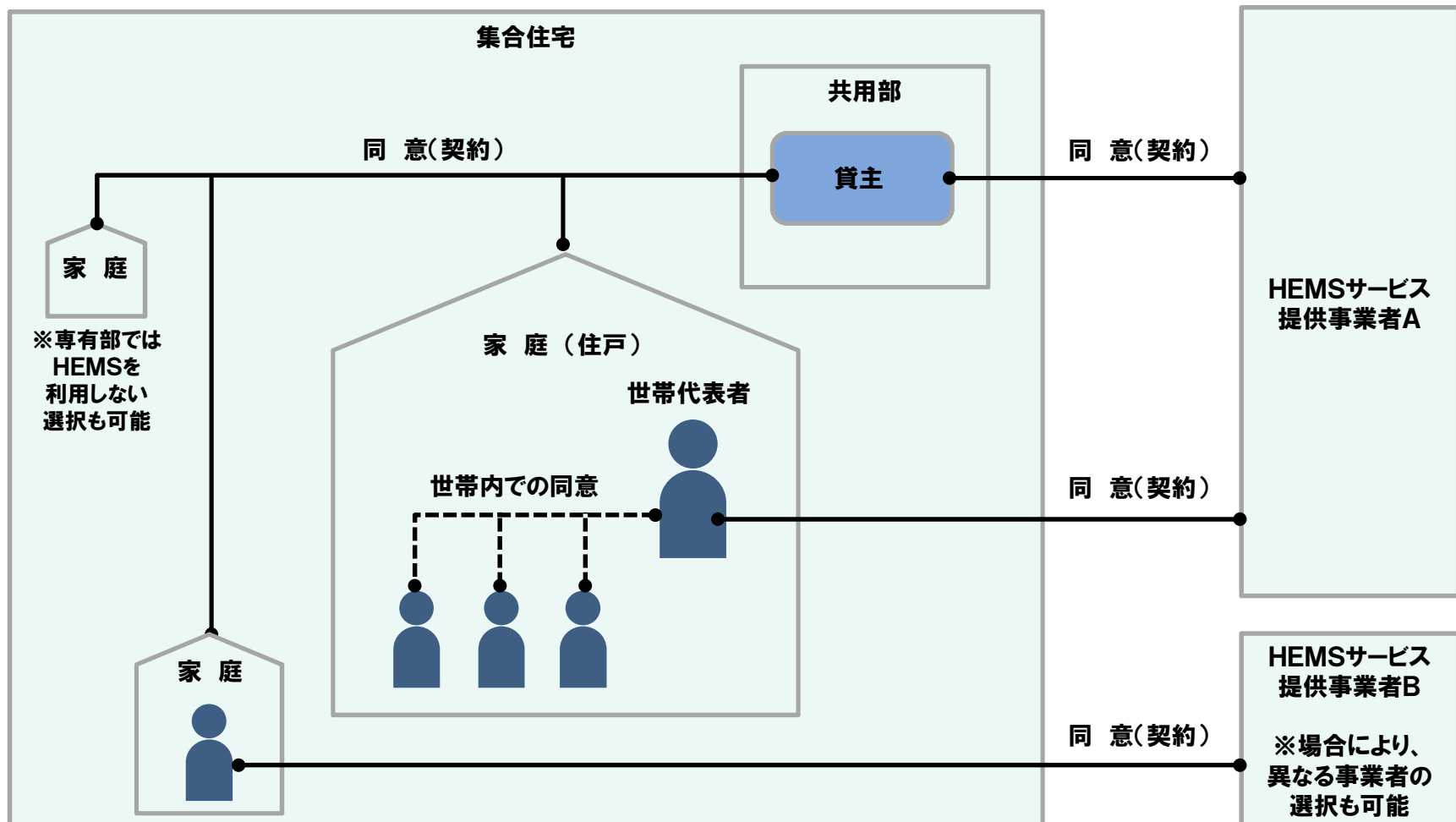


3-6. <補論>住戸のタイプによるHEMSデータ利用の同意取得パターン(例)③

• 賃貸型集合住宅

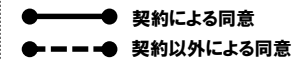


賃貸型の集合住宅の場合、共用部のデータについては、貸主がHEMSサービス提供事業者に対して1次的に同意を与え、さらに貸主と入居者との賃貸借契約時に、貸主が入居者から個別に同意を取得するというような契約構造が必要となることが考えられる。住戸毎のデータについては一般的な世帯単位での契約同様、世帯代表者からの直接の同意取得となる(場合によっては住戸毎に、サービスの可否や、HEMSサービス事業者が異なるということも想定される)。

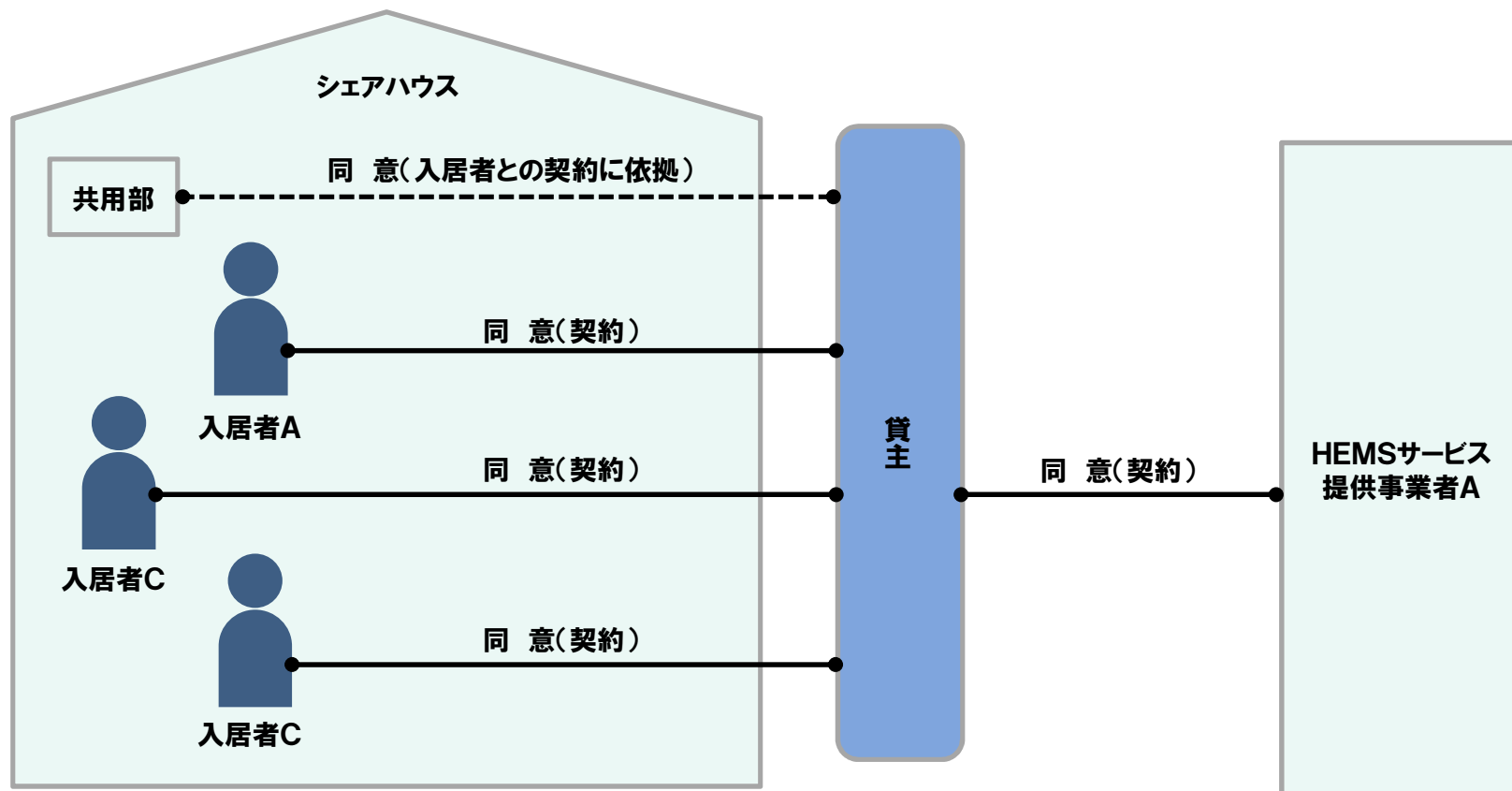


3-6. <補論>住戸のタイプによるHEMSデータ利用の同意取得パターン(例)④

• シェアハウス



最近多くなっているシェアハウスは、貸主が個々の入居者と個別に賃貸借契約を行うのが一般的である*1。しかしながら、住居の中には少なからず共用されるエリアが存在し、電力の配線系統などは必ずしも入居者の居住エリア毎に区分されているとは限らない。したがって、賃貸型の集合住宅と同様に、貸主がHEMSサービス提供事業者に対して1次的に同意を与え、さらに貸主と入居者との賃貸借契約時に、貸主が入居者から個別に同意を取得するというような契約構造が必要となることが考えられる。



(* 1 入居者の代表者1名が契約当事者となるケースもあるが、基本的に他人同士ということ想定し、個人情報の同意については個々の入居者からの同意取得が望ましいと考える)

3-7. <参考資料>ワーキンググループにおける質疑応答

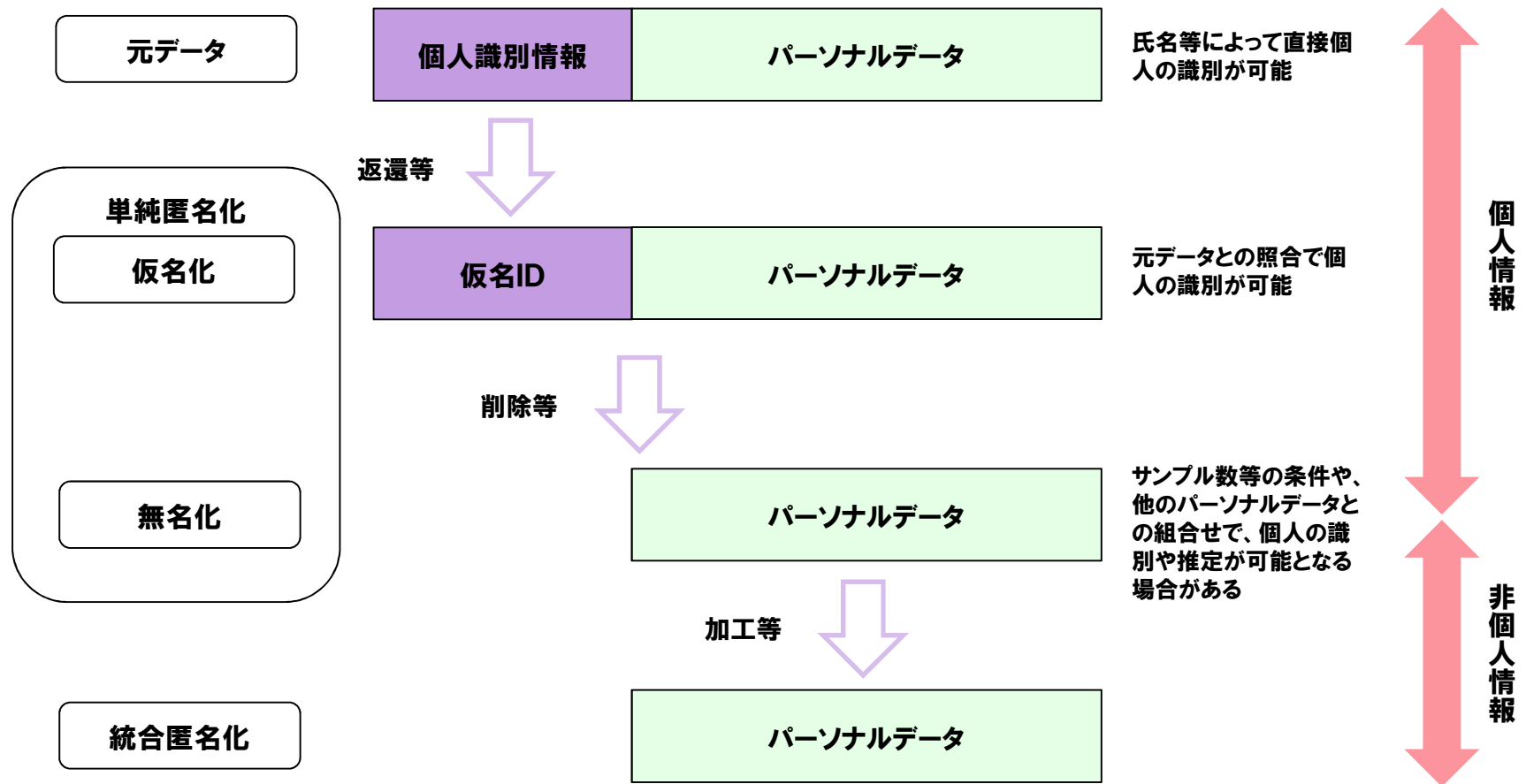
質疑応答		回答
委員名	内容	
田中	<ul style="list-style-type: none"> パーソナルデータを組み合わせて利活用するケースを想定した(個人特定のリスクに関する)解釈についても、資料のどこかに注記しておくべきである。 	<ul style="list-style-type: none"> 対応する。(2頁 *2参照)
喜連川	<ul style="list-style-type: none"> このような枠組みで議論するのは、グローバルスタンダードから見て妥当なのか。 	<ul style="list-style-type: none"> パーソナルデータに関する検討会(IT総合戦略本部)の解釈を参考に、事例調査に基づいて検討を進めている。グローバルスタンダードについては別途調査する。
田中	<ul style="list-style-type: none"> 無名化をしたとしても、特定を防ぐことは出来ないというのが今の常識であり、他のデータと紐付けることを如何に防ぐかということが基本的な問題である。 	<ul style="list-style-type: none"> その前提で検討する。
那須野	<ul style="list-style-type: none"> 匿名化してしまったデータは利用価値が低下すると考えられる。したがって、世帯情報とエネルギー情報は組み合わせて利活用するケースを想定して議論すべきと考える。 	
喜連川	<ul style="list-style-type: none"> HEMSで何が変わるかということに絞った議論をすべきである。HEMSに関連するものについての調査はどうなっているか。 	<ul style="list-style-type: none"> 基本的にはHEMSが世帯全体の情報であるということ以外は、パーソナルデータと同様であると考え。したがって、パーソナルデータの考え方を世帯の観点で応用できるのではないかと考えている。(別紙1参照)
喜連川	<ul style="list-style-type: none"> HEMSデータを利活用するために包括的な同意が必要な点が特徴的な要素になるのではないかと思う。個人情報保護法に関する議論をするのではなく、HEMSデータを利活用する際に、どのように法律を適用しなければいけないのかというのをここでは議論すべき。 	<ul style="list-style-type: none"> 包括的な同意が必要な事例としてどのようなものがあるか調査し、この事業としての特色を出していきたい。それ以外にもHEMSデータを利活用する際に(パーソナルデータの利活用とは異なる)特徴的なケースを、既存事例を応用しながら整理していく必要があると考える。(12~16頁 参照)
喜連川	<ul style="list-style-type: none"> 緊急の時に、HEMSがどう機能し、その時の個人情報保護については例外的な対応をせざるを得ないというケースも、どこかに入れておくべきである。 	<ul style="list-style-type: none"> 来年度以降の課題とする。

3-7. <参考資料>用語集

- **OECD8原則**
OECDプライバシーガイドライン(1980)におけるパーソナルデータ保護の原則。
①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則
⑦個人参加の原則、⑧責任の原則
(参考:総務省「パーソナルデータの利用・流通に関する研究会報告書 平成25年6月」)
- **無名化**
氏名等を削除し、元の情報と対応できないようにする処理。匿名データではあるが、個人情報ではないと一概にはいえない。
(参考:IT総合戦略本部 パーソナルデータに関する検討会 第1回技術検討ワーキンググループ 資料2-3 平成25年9月27日)
- **総務省3条件**
米国FTCにおける考え方等を踏まえ、以下のような条件を満たす場合は、実質的個人識別性がないといえるため、保護されるパーソナルデータには当たらないとして、本人の同意を得なくても、利活用を行うことが可能と考えられる要件。
① 適切な匿名化措置を施していること。
② 匿名化したデータを再識別化しないことを約束・公表すること。
③ 匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止すること。
この際、匿名化により非識別化されたデータと元の識別可能なデータ(連結可能匿名化における対応表を含む。)の双方を保持・使用する場合は、これらのデータは別々に保管することとすべきである。
(参考:総務省「パーソナルデータの利用・流通に関する研究会報告書 平成25年6月」)
- **パーソナルデータ取得時の手続基準等**
例えば経産省で検討されている、パーソナルデータの利活用にあたりプライバシー保護の観点から企業が取るべき手続等を想定(消費者への分かりやすい表示、消費者への選択肢の提示等)。
(参考:経済産業省「経済産業省におけるパーソナルデータ利活用の制度・環境整備に向けた取組みと今後の検討課題 2013年9月2日」)
- **事業者の評価基準等**
例えば経産省で試行されている、パーソナルデータの利活用にあたって、消費者のプライバシーを適切に保護しているかどうかについての事前相談/評価の取組み(日本版PIA(PIA: Privacy Impact Assessment))等を想定。
(参考:経済産業省「経済産業省におけるパーソナルデータ利活用の制度・環境整備に向けた取組みと今後の検討課題 2013年9月2日」)

3-7. <参考資料> 匿名化について

- 匿名化とは、特定の個人を識別できないように、又は、特定の個人を識別できる可能性を小さくするため、情報を加工する技術。



(参考: 経産省 情報大航海プロジェクトホームページ http://www.meti.go.jp/policy/it_policy/daikoukai/igvp/cp_jp/cat305/post-3.html
:IT総合戦略本部 パーソナルデータに関する検討会 技術検討ワーキンググループ 資料 ほか)

3-7. <参考資料>HEMSにおける契約の事例について

- 既存のHEMSサービスの事例について、同意取得を中心に、データ利活用の仕組み等の調査を行った。

認識されたこと

- ①いずれの事例も、世帯の包括同意として事前の同意取得が行われている。
- ②同意の有無によって、個人を特定できる状態でも外部に提供できるとするかどうかは、事例によって異なる。
- ③基本的にユーザーから見た契約者は、HEMSサービス提供事業者になっており、その先の分析代行事業者等は見えない構造となっている。ただし、業務委託等に関わる委託先として明記している場合がある。
- ③データを利用できる範囲や目的については、HEMSサービス提供事業者の業務の委託の延長というものから、目的を制限せずに自由に利用出来るというものまで様々である。
- ④HEMSサービスや関連分野で提供するサービスについてのメリットを記載するものは散見されるようであるが、データの利活用によるメリットを示しているものは見受けられない。
- ⑤匿名化したデータの利用についての記載は、事例によって異なる。
- ⑥データ提供先に対する統制の内容等は記載されていないように見受けられる。

上記の結果から考えられる主要な論点*1

HEMSデータ利用における同意所得は、世帯の包括同意取得が良いと考えられる。

事業者毎に情報の取り扱い(メリット・デメリット記載の有無、利用目的、共同利用や第三社提供の範囲、匿名化したデータの取り扱い等)についての記述レベルが異なるため、何らかのガイドラインなどで方向性を示す必要があるのではないかと考えられる。

上記のようなガイドラインの整備や、運用の標準化、事業者の適正等を図るためには、第三者機関による認証制度などが必要になるのではないかと考えられる。

結果として個人の利益が侵害された場合には、HEMSサービス提供事業者とユーザーとの1対1の関係となってしまう、訴訟等による解決では個人ユーザーの救済という点で問題があると思われ、専門の紛争処理機関などを設置することが望ましいのではないかと考えられる。

(*1 「5. HEMSデータの情報保護に関する検討課題の整理とその対応方針の提案」に詳述)