資料１－２

平成 25 年 10 月 2 日

「パーソナルデータの取扱いルール整備に向けて検討すべき論点」について（私案）

新潟大学法学部　教授　鈴木　正朝

第一　方針

１．保護すべきパーソナルデータの取扱いルールの整備は、次の二段階で対応する。

（１）ガイドライン対応

匿名化措置、その他保護すべきパーソナルデータの取扱いについては、現行法の解釈の許す範囲でガイドラインを制定しルールの明確化を図る（規制改革会議の要請に応える）。

しかし、ビッグデータビジネスの創出、振興の法的基盤整備という観点からはその効果には限界があり、十分な解決には至らないという問題がある。

（２）立法措置

上記（１）の限界に対応するため、個人情報保護法を改正する。

ビッグデータビジネスの創出、振興等日本の経済成長のためには、その手段の一つとして個人情報に関する法制度の規制改革が必要であり、具体的には、①匿名データの流通を促進し、多様な情報処理を許す法制度を実現すること、②越境データの流通を確保し、国内に世界中の多くのデータが集積し得る法的環境整備を図ること等が前提となる。

そのためには、第三者機関（情報保護委員会）の創設など EU 及び米国等国際的なプライバシー・個人データの法的保護水準に達した本人保護の強化、体制の整備が不可欠である。

また、ゲノムを含む医療情報など特定の機微（センシティブ）なデータ、その他の大量の国内個人データが人権保障のない国々に流出する場合の対応策も検討課題とするべきである。

目的：経済成長（ビッグデータビジネスの創出と振興）

↑

手段：規制改革（規制緩和を基調に一部規制強化も必要）

①匿名データの流通を促進し、多様な情報処理を許す法制度

・分野横断的情報処理によるイノベーションの促進

②越境データの流通を確保し、国内にデータが集積する法的環境整備

・国際市場を狙い外貨を獲得するデータビジネスの促進

・個人情報保護法、消費者保護法など日本法が適用、執行され、また雇用や税収が維持されるよう国内データセンター利用の誘導策の推進（事業継続性の確保）。

→EU 及び米国等国際的なプライバシー・個人データの法的保護水準に達した本人保護の強化、体制の整備（第三者機関創設）

→分野横断的情報処理によるプライバシー侵害への対応

→国内個人データが人権保障のない国々に流出する場合への対応

（日本が EU、米国の個人データのバッグドアにならないように）

第二　主要論点

論点１

どの水準まで匿名化すれば、特定の個人を識別できない情報となるか。

（第 1 回資料 3-2「パーソナルデータの取扱いルール整備に向けて検討すべき論点」（平成 25 年 9 月） 2．検討すべき論点（2）②、3 頁参照）

１．ガイドライン対応 － 現行法下での匿名化措置のルールの明確化

現行法では、個人データを第三者提供するに際して、提供元である個人情報取扱事業者の立場において、「匿名化情報」の容易照合性判断を行わなければならない。要するに、提供元において再識別不可能な匿名化措置を講ずる必要がある。

提供事業者において元情報を保有しつつ容易照合性を失わせるためには、元情報と「匿名化情報」の１対１対応関係を失わせることが求められる。こうした措置を講じたデータをここでは再識別不可能データという。

提供元が保有する個人情報に限定する場合は、再識別不可能化措置ビジネス

に有意的なデータとならない。

２．立法措置 － 「日本版 FTC３条件」の導入

上記１の匿名化措置による利用範囲の制約（限界）から、その利用範囲の拡大を図るため、FTC３条件を参考にした立法措置を講ずる。

（１）米国 FTC３条件

「① 与えられるデータセットが合理的に識別可能でなく、
② 当該事業者がそれを再識別化しないことを公式に約束し、
③ 当該事業者が当該データの全ての「下流」利用者に対してそれを非識別化したままの形で扱うことを要求した場合」[1]

（２）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）の 3 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。」[2]

（３）立法措置（案）

１）取扱いルール

---

[1] Accordingly, as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.*
* To the extent that a company maintains and uses both data that is identifiable and data that it has taken steps to de-identify as outlined here, the company should silo the data separately.
- Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (2012)

[2] 同報告書 33 頁参照

（ア）要件

提供事業者が、本人の同意なく「特定のパーソナルデータ」（以下「提供データ」という。）を第三者に提供する場合においては、次の条件を充たさなければならない。

なお、対象情報（提供データ）の定義については、別途検討が必要である。

＊個人データ+α（保護すべきパーソナルデータ）

① 技術的措置

「提供データ」について「合理的な技術的匿名化措置」を講ずること

（法律に基づき、第三者機関が行政基準（規則）を示す。）

＊容易照合性を喪失させる観点からの要請ではなく、提供先における再識別化リスクに対する安全管理的観点からの要請として規則を制定する。

② 提供先との契約

上記①で匿名化したデータ（以下「匿名データ」という。）を再識別化しないことを契約すること（強行法規）。

提供先に再提供禁止を義務付けること、または再提供先について同様の再識別化禁止を義務付けること（強行法規）。

（法律に基づき第三者機関が規則を制定し、モデル条項を告示する。）

③ 透明性の確保

匿名データを再識別化しないことを公表すること。

（公表事項と公表方法については第三者機関が告示する。）

（イ）効果

本人の同意なく、匿名データの第三者提供（販売等）及び再識別化しない範囲での多様な情報処理を行うことができる。

2）組織法 － 第三者機関（情報保護委員会）設置法の制定

米国 FTC、EU データコミッショナー相当の独立行政委員会（第三者機関）を創設すること（番号利用法附則 6 条 2 項参照）

第三者機関へ必要な権限を付与すること（例：規則、告示、行政調査、行政指導、日本版ノーアクションレター制度、PIA、行政処分、罰則、課徴金等）。

（ア）規則

（イ）行政調査

第三者機関は上記の要件が遵守されているかどうか提供事業者及び提供先を調査することができる。

＊第三者機関の職員のスキル要件の明確化と IT 人材の登用、育成の確立、必要な要員数の拡充計画

①「合理的な技術的匿名化措置」の内容

② 提供先との契約内容

③ 法定公表事項の内容

（ウ）行政指導（助言、勧告）

（エ）行政処分（命令、緊急命令）

＊主務大臣との権限関係の整理

＊越境データの停止権

（オ）行政上の義務違反に対する制裁

a. 行政刑罰（間接罰、直罰）

b. 課徴金

c. 公表

（カ）事業者支援（行政機関による法令適用事前確認手続）

事業者に対する「日本版ノーアクションレター制度」等行政機関による法令適用事前確認手続の導入を検討する。

（キ）本人保護

相談窓口の設置

＊技術 WG へのお願い

技術的観点から以下の２点について提言いただきたい。

（１）現行法の解釈論として導入可能な「再識別不可能データ」化（提供事業者において容易照合性のない技術的匿名化）措置の内容について

（２）上記「３）立法措置（案)」を前提とした「合理的な技術的匿名化措置」の内容について

論点２

対象情報の範囲：「個人情報」（「特定の個人を識別することができる」情報）及び保護すべきパーソナルデータ（いわゆる「準個人情報」）をどのように定義すべきか？

（定義）

第二条　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って、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。）をいう。

１．現行法の解釈の明確化

（１）特定個人の識別性の意義

「特定の個人を識別することができるもの」

（２）容易照合性（「他の情報と容易に照合することができ」）**の意義**

１）従来の考え方

①起草担当者説（内閣官房 個人情報保護担当室『個人情報の保護に関する法律案＜逐条解説＞』（平成 13 年 4 月）2 条 解説１（２）参照）

「他の情報と照合が容易でない場合については、個人の識別が容易ではなく、個人の権利利益を侵害するおそれも小さいと認められることから、必要最小限度の規律を定める本法においては、個人情報の範囲から除外している。具体的には、他の事業者の照合を要する場合のほか、内部でも取扱部門が異なる等の事情により照合が困難な場合がこれに当たる。」

②園部説（園部逸夫編集「個人情報保護法の解説＜改訂版＞」49 頁）

「それ自体は個人識別性がない情報について、特別の調査を行ったり、特別の

ソフトを組み込むといった特別の費用や手間をかけることなく、すなわち、事業者において通常の業務における一般的な方法で、個人を識別する他の情報との照合が可能な状態である。これに該当しない場合としては、例えば、日常的に行われていない他の事業者への特別な照会を要する場合、内部でもシステムが異なる等の事情により技術的照合が困難な場合が考えられる（事業者又は内部組織の間で組織的・経常的に相互に情報交換が行われている場合等は「容易に照合することができ」る場合に当たると考えられる。）」

③「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」等に関するＱ＆Ａ（2010 年 4 月 1 日更新）の Q14 における解釈

「**Q14**　事業者の取扱部門ごとにデータベースがあり、他の取扱部門のデータベースへのアクセスが、規程上・運用上厳格に禁止されている場合、「容易に照合することができ」（法第２条第１項）るといえますか。」

「**A14**　他の取扱部門のデータベースへのアクセスが規程上・運用上厳格に禁止されている場合であっても、双方の取扱部門を統括すべき立場の者等が双方のデータベースにアクセス可能な場合は、当該事業者にとって「容易に照合することができ」る状態にあると考えられます。ただし、経営者、データベースのシステム担当者などを含め社内の誰もが規程上・運用上、双方のデータベースへのアクセスを厳格に禁止されている状態であれば、「容易に照合することができ」るとはいえないものと考えられます。（2007.3.30）」

２）上記 Q&A14 の問題点

（ア）対象情報の定義にマネジメント的要素を採用することの問題

対象情報の該当性は外形基準から客観的に定めるべきである。

（イ）主務大臣の執行上の問題（事業者内部の状況判断の困難性）

照合の主体は個人情報取扱事業者であるところ、社内にファイアウォールを設けるという Q14 的発想においては、当該事業者内の従業者視点になっている。事業者規制法においては、事業者を対象として、その管理可能なデータの存在のみを客観的に評価することを原則とすべきである。

３）現行法のあるべき解釈

照合とは、当該事業者において当該情報（元情報）と「他の情報」とがマッチング可能な状態にデータが存在していることをいう。

ここで照合（マッチング）とは、当該情報（元情報）と「他の情報」が１対１対応になっているかどうかということが（主務大臣からみて）確認可能な客観的状態にあるか否かということである。

①個人情報（元情報）＋非個人情報（その他の情報）＝個人情報のケース

（例；顧客 DB＋顧客番号）

＊当該事業者においては顧客番号単体も個人情報に該当する。

マッチングすれば特定個人の識別が可能になる状態にある、特定個人の識別情報（元情報）と特定個人の識別性がない「その他の情報」の２つ以上の情報が当該事業者の管理下に存在すること。

②非個人情報（元情報）＋非個人情報（その他の情報）＝個人情報のケース

特定個人の識別性がない情報（元情報）と特定個人の識別性がない「その他の情報」の２つ以上の情報のマッチングによって特定個人の識別が可能になる状態で存在していること。

なお、本条からは必ずしも導かれないが次のケースも考慮しておく必要がある。

③個人情報（元情報）＋個人情報（その他の情報）＝個人情報のケース

（例；同一の顧客番号で管理している顧客 DB①＋顧客 DB②）

一見、意味のない類型のように思えるが、開示の求めの対象情報を確定する場合に問題となる。

対象情報たる個人情報の範囲、すなわち１つの個人情報とは何かという問題である。

２．立法措置（案）

（１）対象情報：「準個人情報」（保護すべきパーソナルデータ）

米国消費者プライバシー権利章典にいう「特定の消費者、コンピュータその他デバイスに合理的に連結可能なデータ」を日本の個人情報保護法に導入する。

１）「準個人情報」（仮）の定義（案）

この法律において「**準個人情報**」（仮）とは、生存する個人に関する情報であって、当該情報に含まれる識別子、識別性を有するデータその他の記述等により特定の個人が専ら利用する電子計算機及びその他の機器、カード等を識別することができるものをいう。

２）義務規定との対応

	取得	委託	第三者提供
個人情報	直接書面取得）同意 その他）通知 or 公表	同意不要 *監督義務	同意
準個人情報	同意 or 通知 or 公表	同意不要 *監督義務	同意 or オプトアウト
匿名データ	同意不要 再識別禁止	同意不要 *監督義務	同意不要 *３条件

第三　ガイドライン制定で明確化する取扱いルールと実施可能なビジネスモデルと立法措置（個人情報保護法改正）によって可能となるビジネスモデル

＜別添の図表参照＞

モデル１：　ガイドライン対応

モデル２：　立法措置で実現

第四　本人保護の強化

消去権（裁判上の請求権）の是非

第五　個人情報保護法改正は必要か？

法改正なくビッグデータビジネス等の振興は困難であり、経済成長に向けた法的基盤整備の一つとして「第三者機関（情報保護委員会）設置法」の制定及び個人情報保護法の改正は必要である。

なお、現行法上の立法的課題は、「論点表」参照のこと。

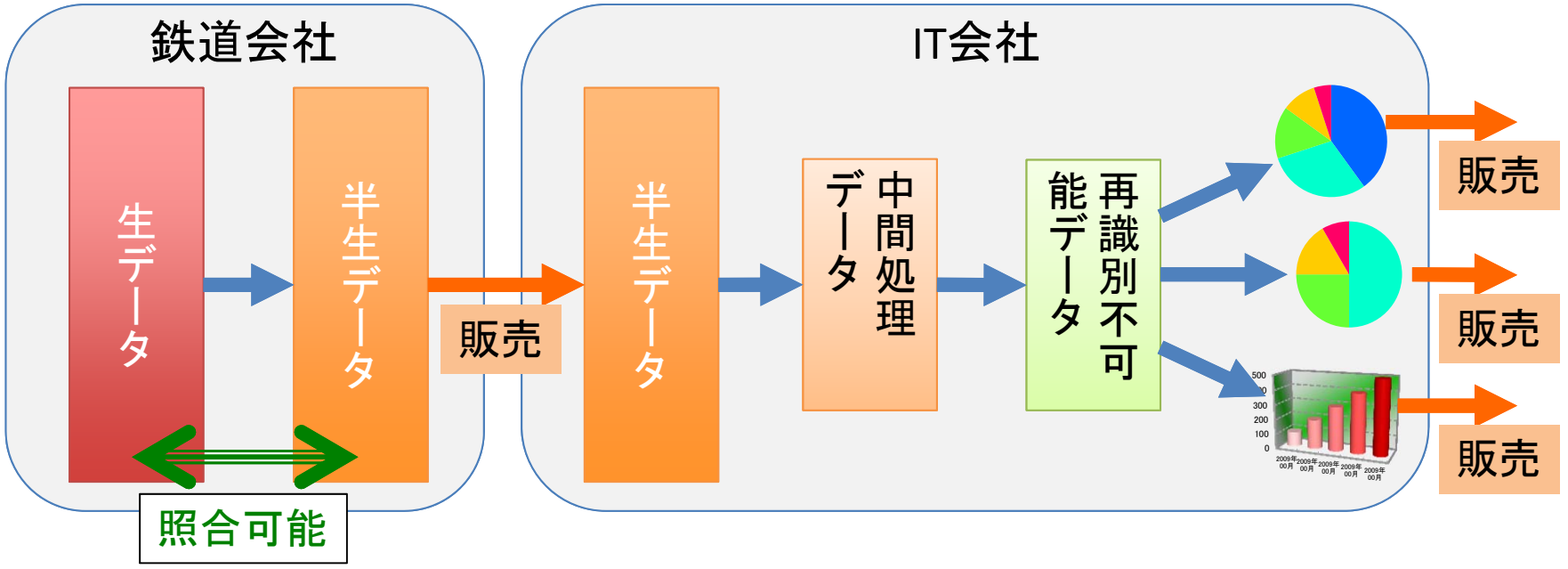
以上

資料１－２

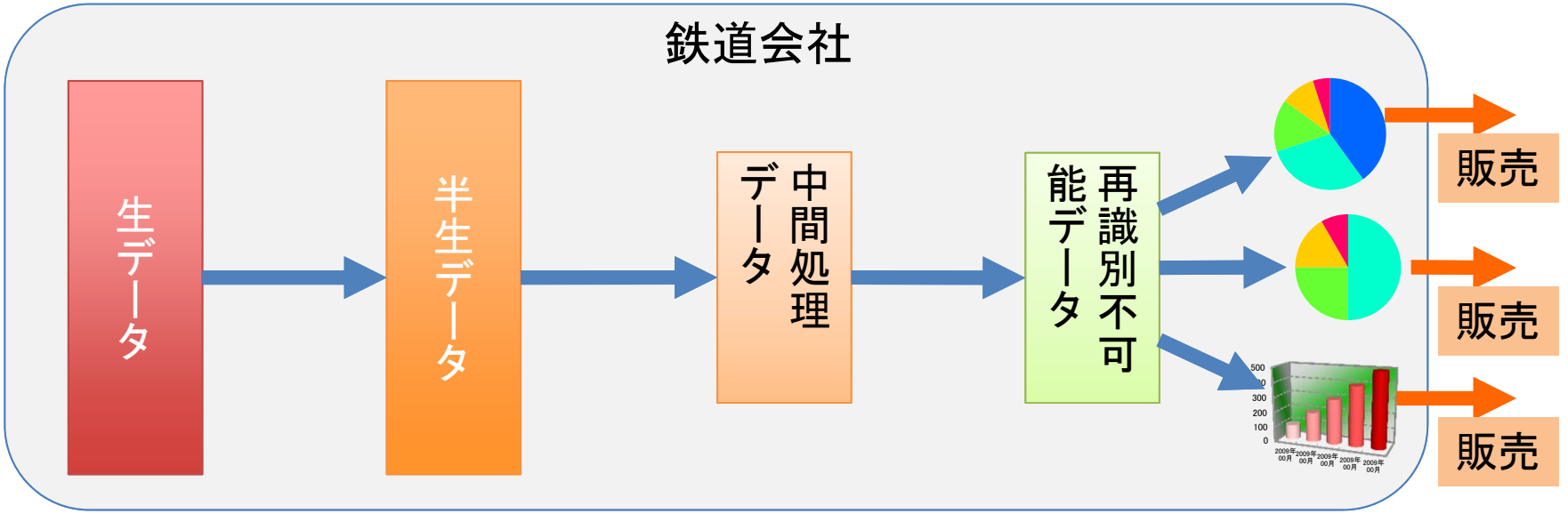
平成25年10月2日

「パーソナルデータの取扱いルール整備に向けて検討すべき論点」について（私案）

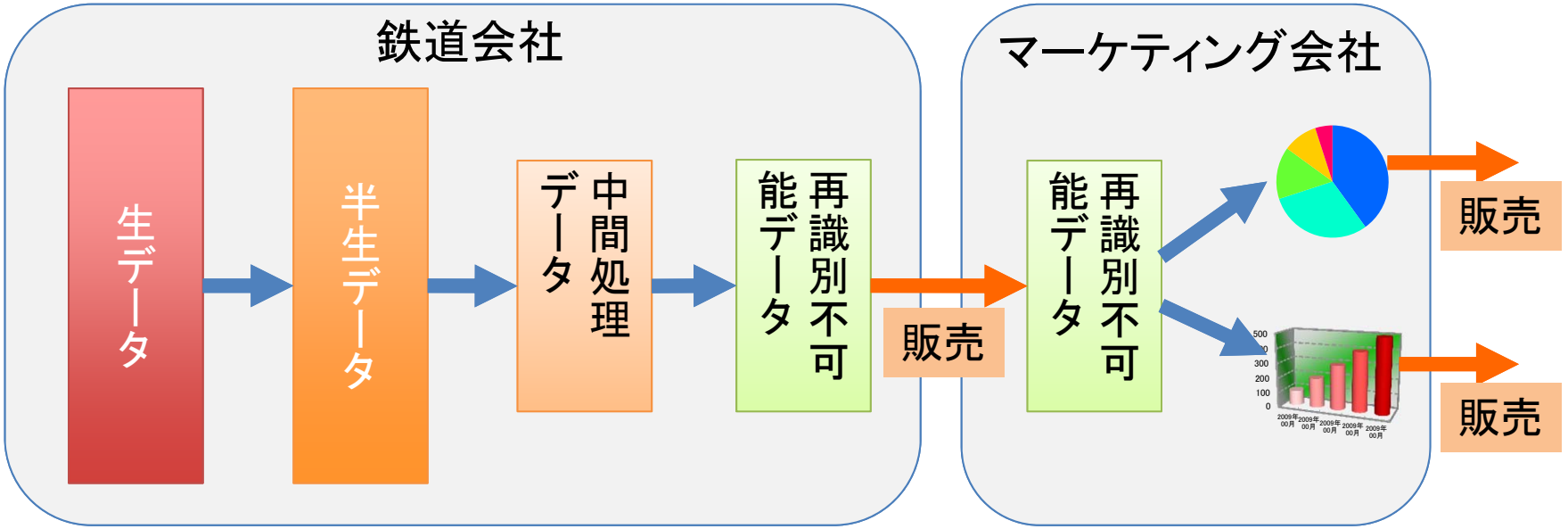
モデル１：　ガイドライン対応
モデル２：　立法措置で実現



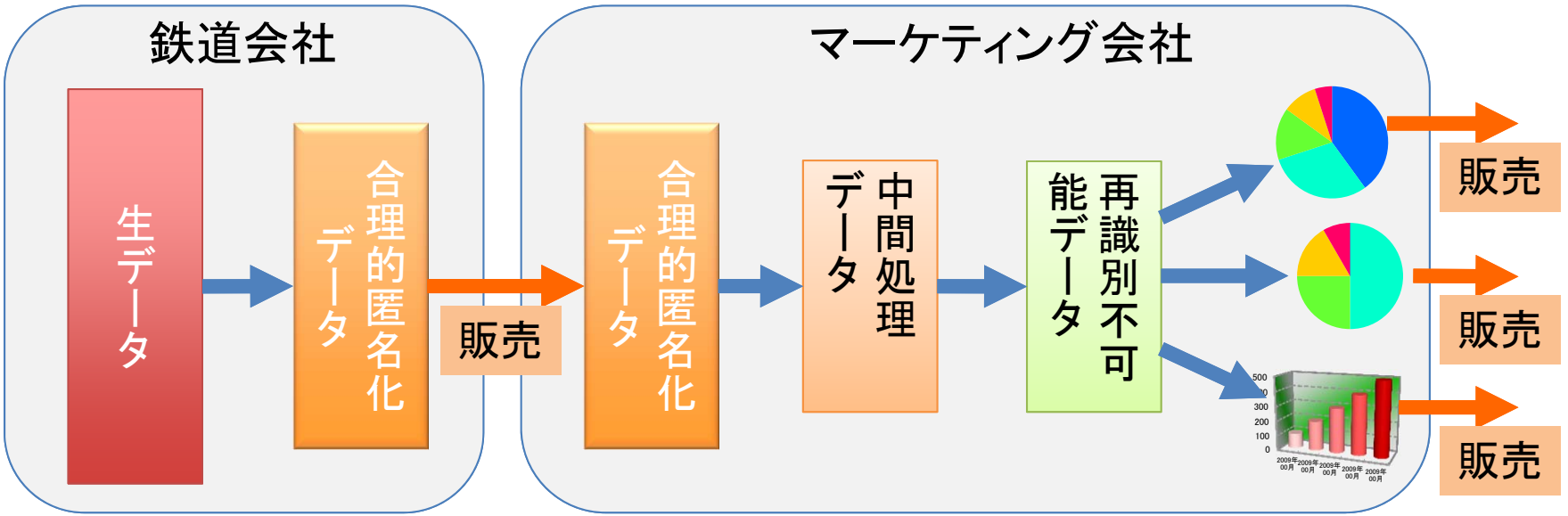
＊　某交通カードの乗車履歴データ提供事案　（現行法制下で違法）



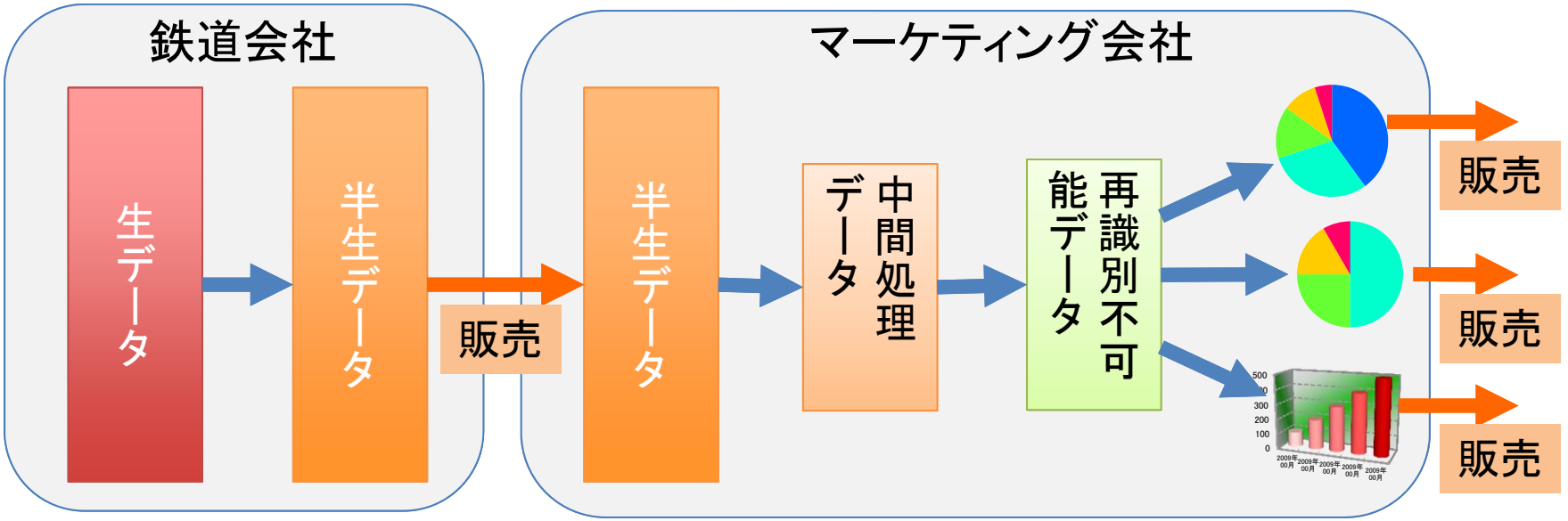
モデル1–①　現行法制下で適法な利活用ビジネス(1)



モデル1–②　現行法制下で適法な利活用ビジネス(2)



モデル2-①　立法措置によって認められる利活用ビジネス(1)



モデル2-②　立法措置によって認められる利活用ビジネス(2)