2025-12-14 情報法制学会 公募報告3

個人情報保護法と一般データ保護規則の規制単位の比較

株式会社博報堂DYホールディングス／一般財団法人情報法制研究所
猪谷誠一

猪谷誠一

2008年　広告会社に入社

　　マーケター→データサイエンティスト

2013年頃　データ保護・プライバシー研究開始

2017年頃　JILIS研究員／オンライン広告研究TFメンバー

2023年　中央大学国際情報研究科修士課程(25年修了)

2025年　JILIS上席研究員

https://researchmap.jp/sigaya/


JILIS

オーディエンスターゲティング広告における
匿名加工情報の利用に関する提言

International Data Privacy Law, 2025, Vol. 00, No. 00　ARTICLE　1

Ignored discrepancies in the fundamental concepts of data protection laws in Japan and the EU

Seiichi Igaya* and Osamu Sudoh†

Abstract

- The fundamental questions for assessing a country's data protection level are who and what fall under the umbrella of data protection legislation. Japan's Act on the Protection of Personal Information (APPI) defines regulatory subjects and information to be protected, covering less than the European Union's General Data Protection Regulation (GDPR), despite their mutual adequacy decisions.
- Many of the gaps between the APPI and the GDPR have been resolved in the dialogue towards mutual adequacy findings. However, the difference in the definitions of regulatory subjects was omitted from that resolution. Academia also failed to point out that it is, apart from a few exceptions.
- In 2019, Rikunabi, one of the largest online job board services for students in Japan, was widely reprimanded for circumventing the intent of the APPI. Rikunabi used AI-based profiling to predict job applicants' probability of declining job offers and sold this information to potential employers. This scandal symbolized the pitfalls hidden in the country's data protection legislation.
- Documents and literature since 1980 reveal that Japan inadvertently employed a definition of regulatory subjects that deviates from the Organisation for Economic Co-operation and Development Privacy Guidelines. Not only the drafters and lawmakers who approved the Bill of the APPI, but also those who criticized it as a degradation of the Guidelines, failed to acknowledge the original definition.

Introduction

In an increasingly interconnected world, personal data have become a cornerstone of modern economies and societies, influencing everything from individual privacy to global commerce. As nations strive to balance innovation with the protection of fundamental rights, data protection laws have emerged as critical tools for safeguarding personal data. Among these, the European Union's (EU) General Data Protection Regulation (GDPR) is widely regarded as a global benchmark.[1] Japan is one of the countries found to have an essentially equivalent level of data protection to the GDPR,[2] which is implemented through the Act on the Protection of Personal Information (APPI).[3] Japan also finds the EU's data protection regime to be essentially

Summary

- データ保護法の比較でも「スコープ」「実質」に加えて「構造」にも着目すべき
- 個人情報保護法とGDPRの構造の比較を行った
  - 個人情報保護法は事業者を単位にしたoperator-firstの構造
  - GDPRは処理のステージを単位にしたoperation-firstの構造
- 1事業者1サービスの前提が崩れた現代にはoperation-firstの方が合理的ではないか

はじめに

従来のデータ保護法の比較対象

従来のデータ保護法の比較は、条文に明記されるスコープと実質に着目したものがほとんどを占める

- スコープ … 保護や規制の対象となるデータ、アクター、活動
- 実質 … スコープ内のものに対する規律、義務、権利、手続き [1]

従来のデータ保護法の比較例

[欧米諸国のデータ保護法]は、大別すると、
① 一つの法律で国・地方公共団体等の公的部門（パブリック・セクター）と民間企業等の民間部門（プライベート・セクター） の双方を対象とするオムニバス方式、および
② 公的部門と民間部門とをそれぞれ別の法律で対象とするセグメント方式とに分けることができる。
前者の立法例はヨーロッパ諸国に多く、後者の立法例はアメリカにみられる。 [2]

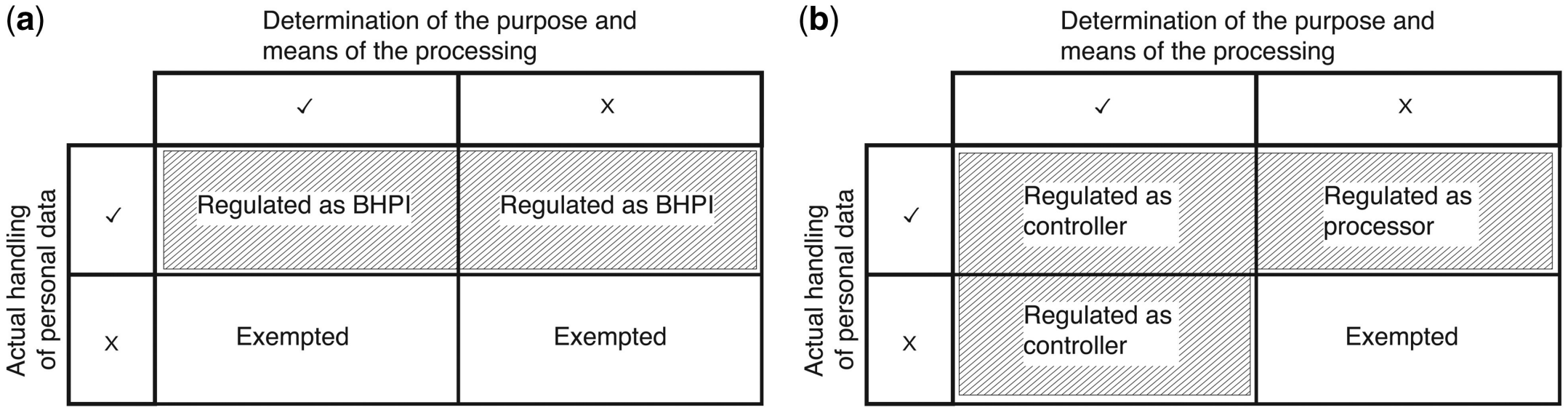
EU-GDPR

I 法2条1項「個人情報」、2項「個人識別符号」、5項「仮名加工情報」、6項「匿名加工情報」、法16条3項「個人データ」、4項「保有個人データ」について

GDPRでは、「個人データ」が法2条1項の「個人情報」に相当する。そして、GDPRの「個人データ」は、「識別され又は識別され得る自然人（『データ主体』）に関連するあらゆる情報をいう。識別され得る自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子などの識別子、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、若しくは社会的アイデンティティに特有な1つ以上の要素を参照することによって、直接又は間接に識別され得る者をいう。」と定義されている（4条(1)号）。 [3]

 [4]

従来のデータ保護法の比較例



[5]

スコープと実質以外に着目している例

[W]hat the FIPS say is less important than what the FIPS wrought: a very different approach to privacy law, one that embraces rights of privacy that do more than solely redress past harm. Influenced by the FIPS, legislatures have enacted statutes designed to avoid "privacy problems" that have nothing to do with the "injury to feelings" at the heart of the privacy torts. [6]

[I]t is clear through the scope and tone of the Japanese Constitution and the APPI that Japan places more significant emphasis on the economic salience of data than the EU. [7]

他分野での規制単位論

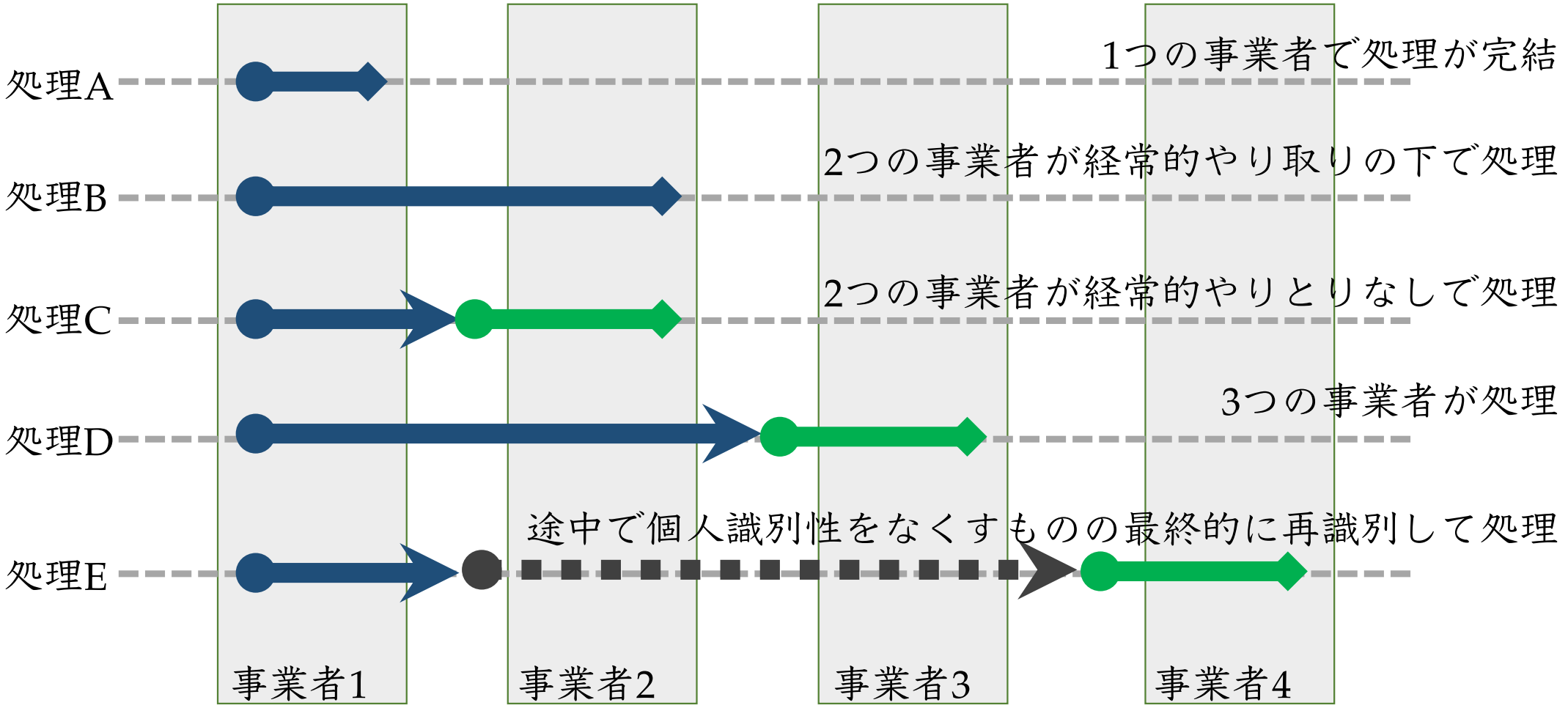
環境やfintech分野にはentity-based vs activity-basedという形で規制単位の議論がある

REACH exposure scenarios describe in generic terms the appropriate conditions for controlling exposure to an individual substance per task or work process (not per workplace!). [9]

[10]

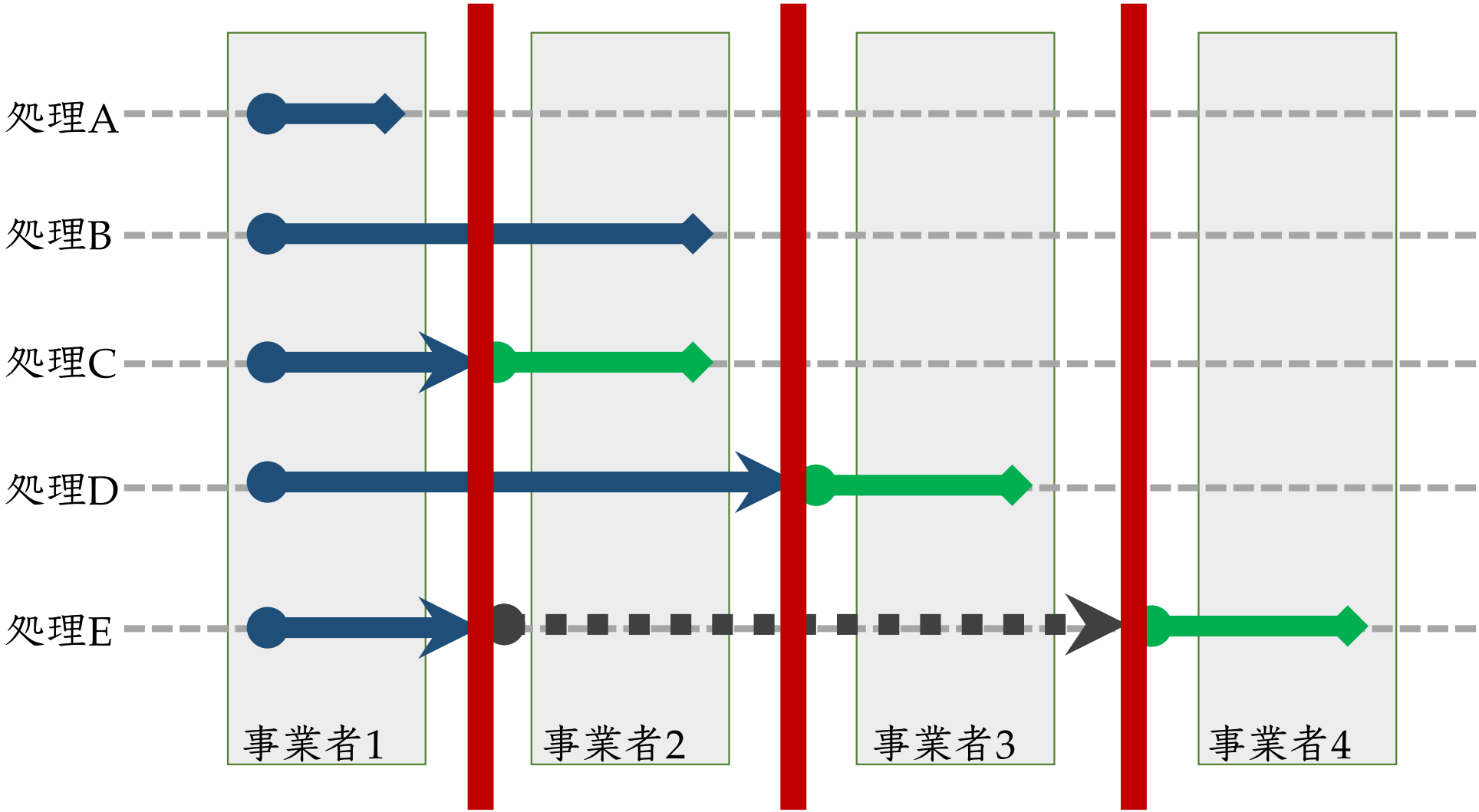
In the last several years, domestic and international policymakers have come to view these two strategies as substitutes, largely abandoning entity-based designations in favor of activities-based approaches. [11]

1事業者1処理の前提は崩れている

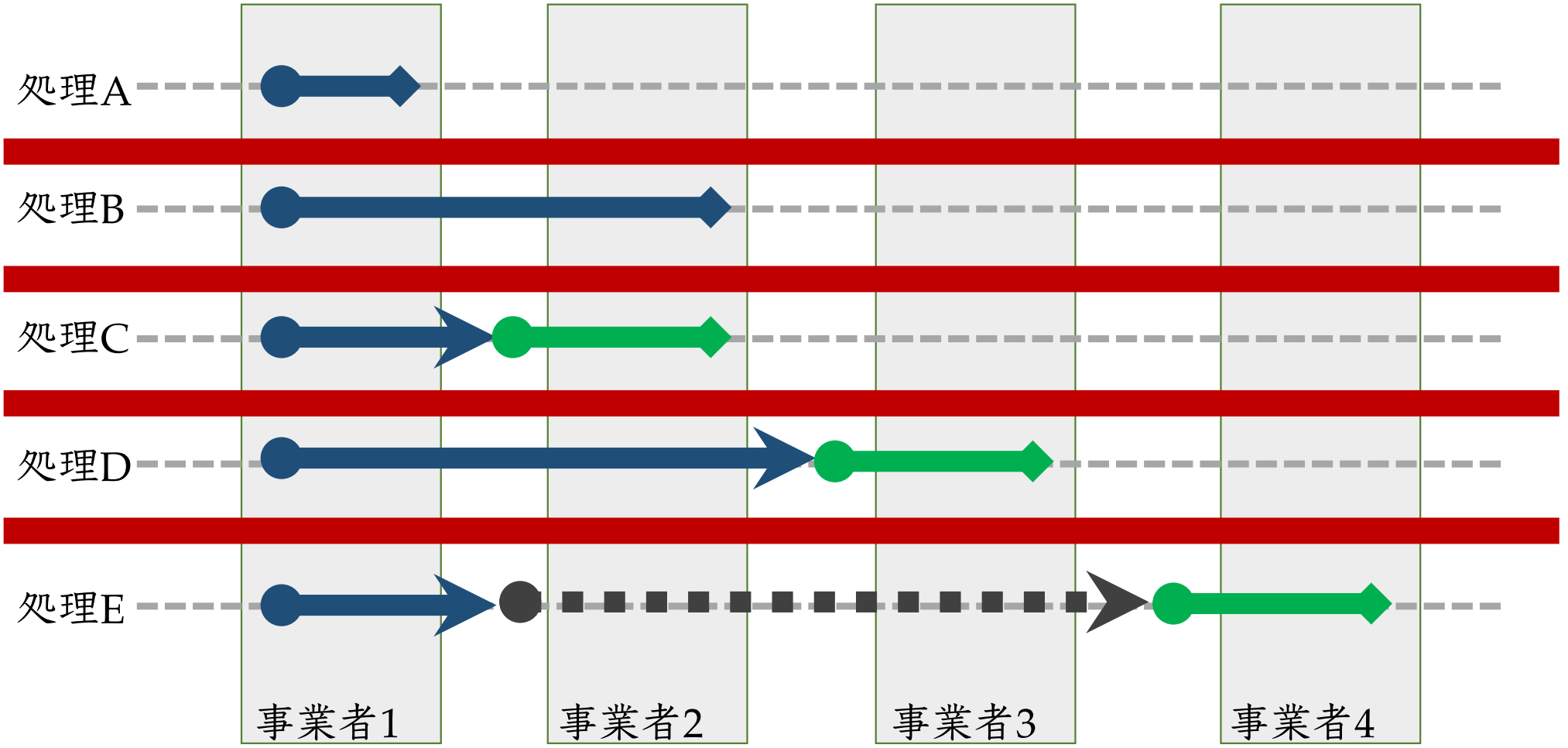


構造は具体的な規定や実務の条件になる

Operator-first構造の個人情報保護法



Operation-first構造のGDPR



個人情報保護法の構造

個人情報該当性 (2条1項関係)

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、次の各号のいずれかに該当するものをいう。
一　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。以下同じ。）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。）

「他の情報と容易に照合」できたりできなかったりする者（個々の事業者）の視点で個人情報該当性が決まる

個人情報該当性 (2条1項関係)

事業者の各取扱部門が独自に取得した個人情報を取扱部門ごとに設置されているデータベースにそれぞれ別々に保管している場合において、双方の取扱部門やこれらを統括すべき立場の者等が、規程上・運用上、双方のデータベースを取り扱うことが厳格に禁止されていて、特別の費用や手間をかけることなく、通常の業務における一般的な方法で双方のデータベース上の情報を照合することができない状態である場合は、「容易に照合することができ」ない状態であると考えられます。[...]

[13, Q.1-18]

容易照合性を否定するには事業者内に様々な措置が必要＝
事業者内には容易照合性があるのがデフォルト

第三者提供と利用目的の関係(17条1項関係)

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。

あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的　の特定に当たっては、その旨が明確に分かるよう特定しなければならない

[14, 3-1-1]

個人情報取扱事業者は、個人データの第三者への提供に当たり、あらかじめ本人の同意を得ないで提供してはならない

[14, 3-6-1]

一般的な利用目的は通知又は公表で足りるが、事業者の境界をまたぐ第三者提供は同意が必要

第三者提供の例外(27条5項関係)

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。

一　［委託］

二　［事業承継］

三　［共同利用］

特定の場合には、物理的に事業者の境界を跨いでいても
「第三者に該当しない」と擬制

第三者提供による利用目的の解除

個情法上は、第三者から個人データの提供を受ける際に、当該第三者による当該個人データの取得の経緯等を確認して記録する義務を負うが(法30条1項、3項)、当初の利用目的はこの確認記録義務の対象であるとは明記されておらず、また提供先事業者によるデータ利用が提供元事業者の特定した当初の利用目的に制限されるという明文の規定もない。
したがって、提供先事業者が特定して通知又は公表する利用目的が、当初に提供元事業者が特定した利用目的の範囲を超える場合であっても、その事自体が直ちに禁止されるわけではない。 [15, p.137]

適法に事業者の境界を超えれば、
提供前の利用目的はリセットされる

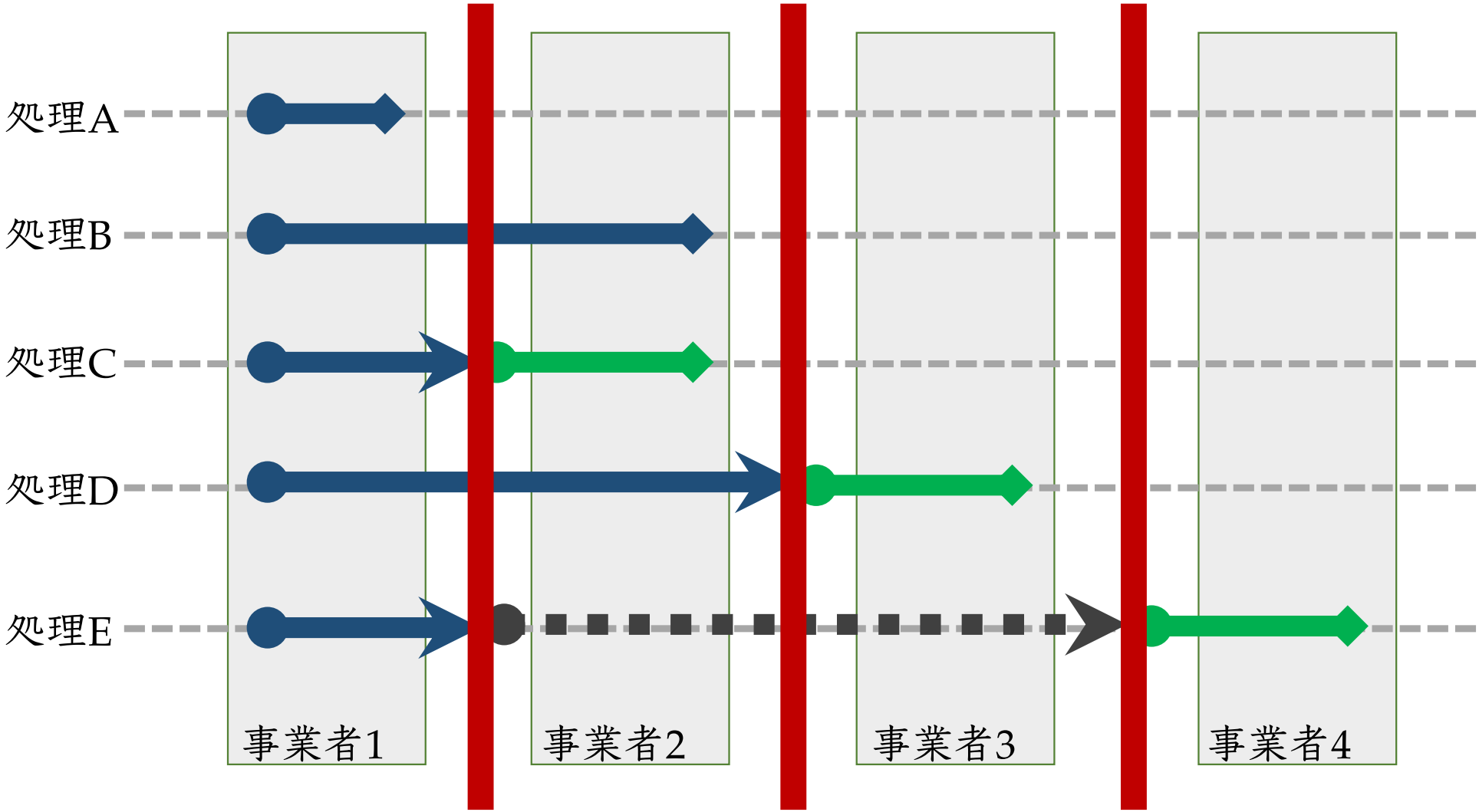
仮名加工情報関連(41,42条関係)

仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第十七条第二項、第二十六条及び第三十二条から第三十九条までの規定は、適用しない。(41条9項)

仮名加工情報取扱事業者は、法令に基づく場合を除くほか、仮名加工情報（個人情報であるものを除く。次項及び第三項において同じ。）を第三者に提供してはならない。(42条1項)

仮名加工情報の作成により利用目的変更、漏洩報告等様々な義務が適用されなくなる一方で、第三者提供は禁止

個人情報保護法は事業者境界に着目する規定が多い



事業者境界に着目した背景

この法律の仕組みは全体として取得段階で情報ファイル、あるいはそれをデータベースと呼ぶかどうかはともかくとして、ファイルを把握することは我が国でも、あるいは欧米でも先生も御存じのようにかなり難しい。ですから、できるだけ出口の提供のところで縛ろうという体系になっております。

[...]

そして、社会的にも新聞等で報道された事件というのは大量なデータベース等が不法に、あるいは不適切にだれかに提供される事例である。そういうところに国民全体が不安を感じておられるのではないか。そういう仕組みがいいのではないかということで全体ができ上がっていると思います。

[16, 藤原靜雄発言]

事業者境界に着目した背景

この法律の仕組みは全体として取得段階で情報ファイル、あるいはそれをデータベースと呼ぶかどうかはともかくとして[illegible]ルを把握することは我が国で[illegible]ようにかなり難しい。[illegible]できるだけ出口の提供のところで縛ろうという体系になっております。

[...]

そして、社会的にも新聞等で報道された事件というのは[illegible]タベース等が不法に[illegible]事例である。そ[illegible]を懸念しておられるのではないか。そういう仕組みがいいのではないかということで全体ができ上がっていると思います。

取扱いを外部から規制することの困難

漏洩や不正取得に懸念が集中していた当時の世論

[16, 藤原靜雄発言]

GDPRの構造

処理(processing)と操作(operation)

「処理」とは、自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される操作又は一群の操作を意味する。

[GDPR 4条(1)]

一切の記録や保管を伴わないデータ収集であったとしても操作である

[17, fn 13]

処理は1つ以上の操作から構成される

*Fashion ID*事件(C-40/17)

- E-コマースサイトFashion IDが自社商品ページにFacebookのLikeボタンを埋め込んだことにより、そのクリックにかかわらず訪問者の端末情報がFacebookによって取得された
- Likeボタンを埋め込んだFashion IDはjoint controllerか？
- joint controllerだとすれば、それは処理のどの範囲についてか？

*Fashion ID*事件(C-40/17)

- Fashion IDのjoint controllerとしての責任は「ウェブサイト訪問者のパーソナルデータ送信による収集と開示を含む複数の操作」に限定される [18, para 84]
- 「controlの問題は、問題となっているそれぞれの操作ごとに評価されるべきであり、処理と呼ばれている、何でもかんでも雑駁にまとめたものについて評価されるものではない。」 [19, para 99]

処理より細かく且つ複数の操作からなる「ステージ」に着目してjoint controllerの責任を分配

*IAB Europe*事件(C-604/22)

- EUのオンライン広告業界団体IAB Europeが策定した「ターゲティング広告をEU法令を遵守した形で行うための枠組み」TCFについて、IAB EuropeがGDPR違反で訴えられた事件
- TCF用データ(TC文字列)に個人やデバイスの識別子は含まれない
- TC文字列はターゲティング広告のフローの中でIPアドレスなどと紐づいてターゲティングに用いられる
- TC文字列を実際に取り扱わないIAB EuropeにとってもTC文字列はパーソナルデータか?もしそうならその責任はどこまで及ぶか?

*IAB Europe*事件(C-604/22)

- TCF枠内の処理の過程でユーザのIPアドレスと紐づくのが明らかなのであるから、TC文字列はパーソナルデータである。
- そのような解釈[TC文字列がIPアドレスと結合されることでユーザを識別し個人データとなること]は、IAB Europeそれ自身がTC文字列とユーザのデバイスのIPアドレスを結合できず、TCFの文脈で会員の所有するデータへの直接のアクセスの可能性がないという単なる事実のみによって揺らぐものではない。 [20, para 46]

分析対象となる処理が決まってはじめて
パーソナルデータ該当性が決まる

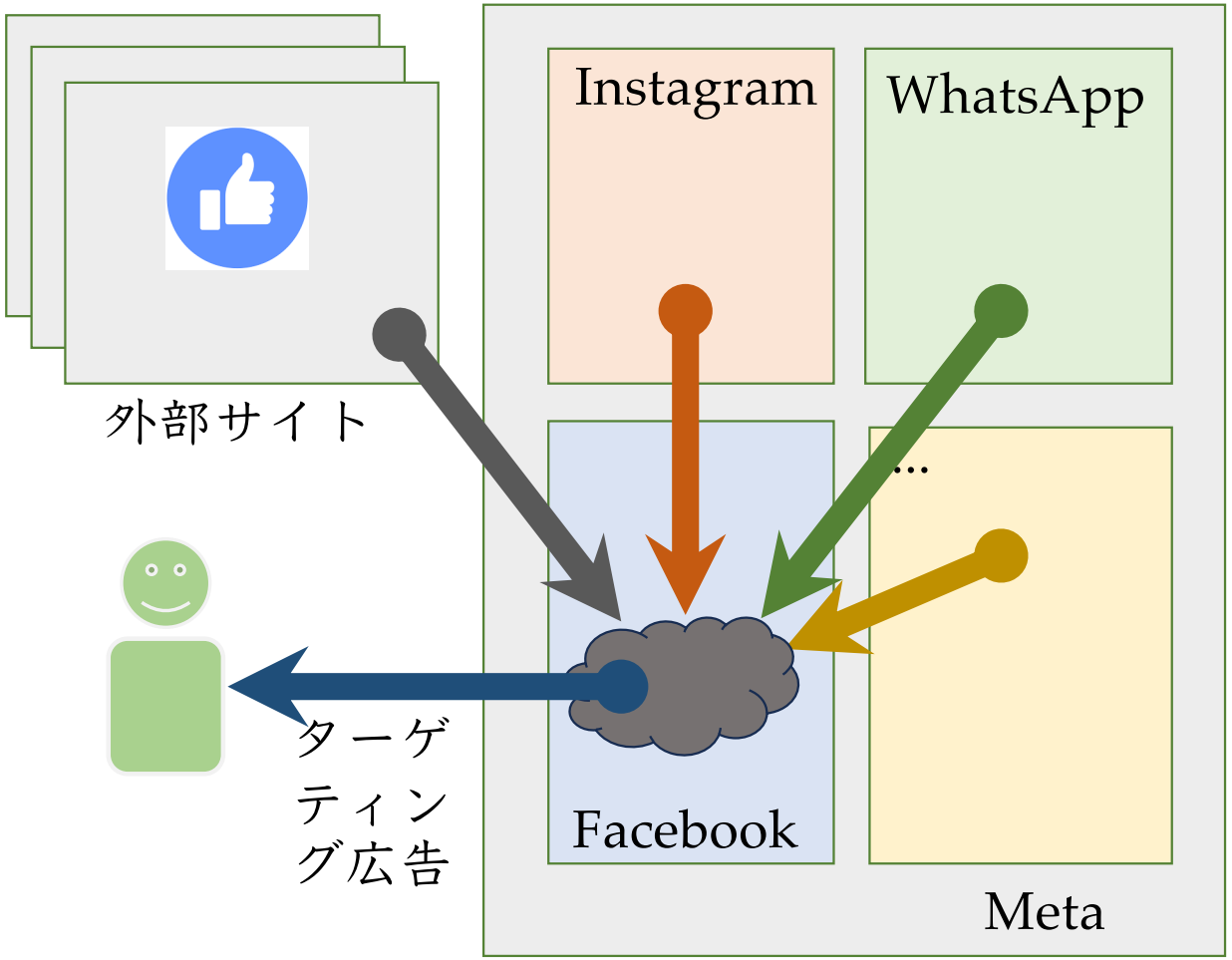
*IAB Europe*事件(C-604/22)

- ベルギーデータ保護機関の決定では、下流のOpenRTBに従った処理にまでIAB Europeの責任が及ぶとした [21, para 370]
- 一方CJEUは、ユーザからの意思表示がTC文字列の形式で記録されてからTCF参加ベンダによって行われる個人データの処理と、それに続くOpenRTBの処理とを分ける必要があり、IAB Europeは後者の処理の目的や手段の決定に影響力を有さないため、controllerとすることはできないとした。 [20, paras 73–76]

分析対象となる「ステージ」が決まってはじめて
controllerとしての責任が決まる

*Meta Platforms*事件の焦点

Facebook上でのターゲティング広告配信のため、Metaの別サービスやLikeボタンを埋め込んだ外部サイトの情報と統合したデータを作り配信を行っていた



契約履行のための処理

GDPR6条(1)(b)の適用可能性についてCJEUは

「互いに独立に実施されるサービスやサービス要素のいくつかに係る契約については、6条(1)(b)の適用はそれぞれのサービスごとの文脈で別々に検討されなければならない」とした。

[23, para 100]

事業者よりも細かい粒度で分析を行っている

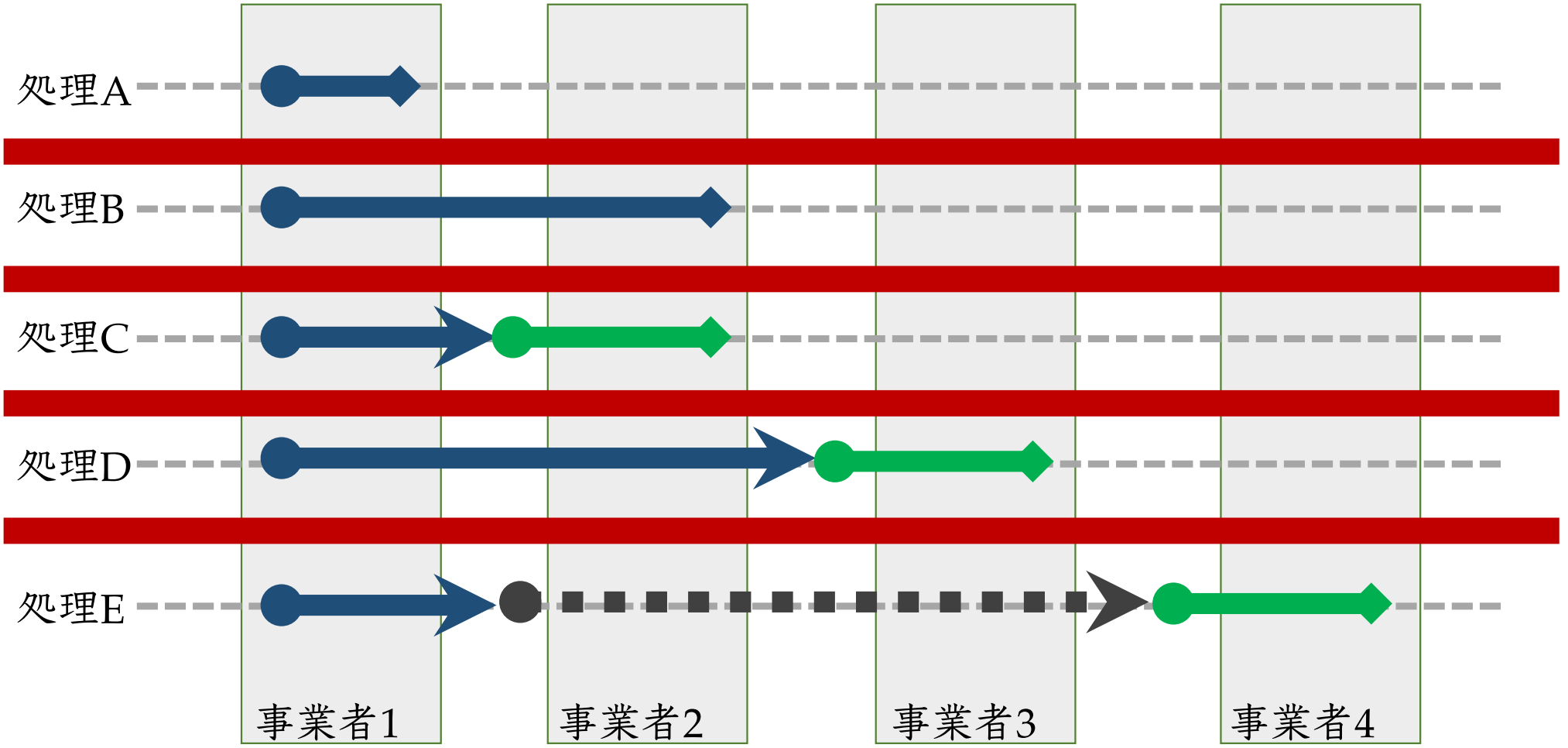
正当な利益に基づく処理

GDPR6条(1)(f)の適用可能性についてCJEUはユーザの「合理的な期待」に言及。Facebook上でのターゲティング広告にFacebook上での活動データが使われることは合理的に期待できても、Facebook外での活動データが使われることは合理的に期待できないとして、同じターゲティング広告配信という目的のための処理であってもデータソースが異なれば個別の処理の根拠が必要とした。

[23, para 148–150]

事業者よりも細かい粒度で分析を行っている

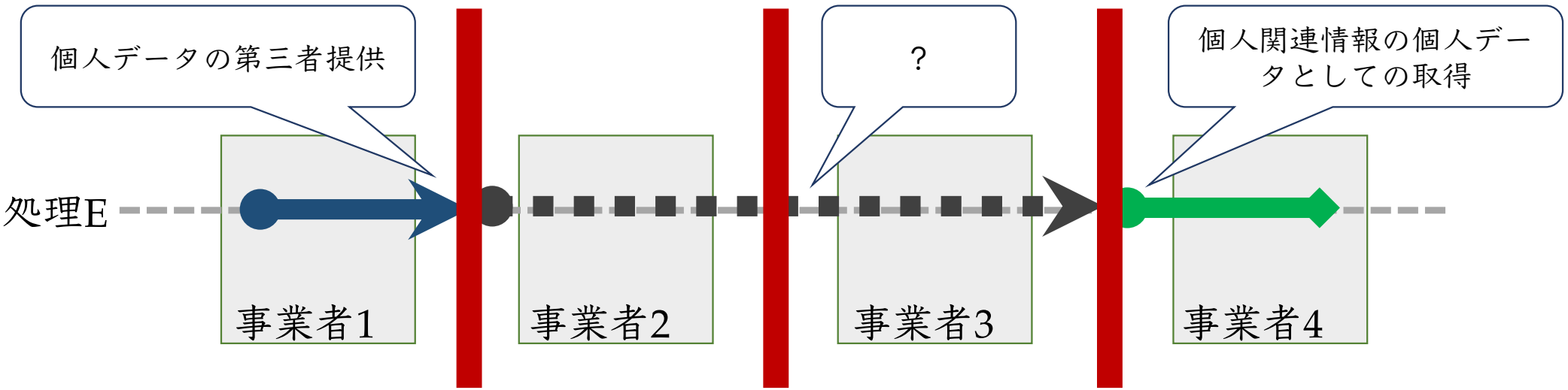
GDPRではoperationが先に決まる



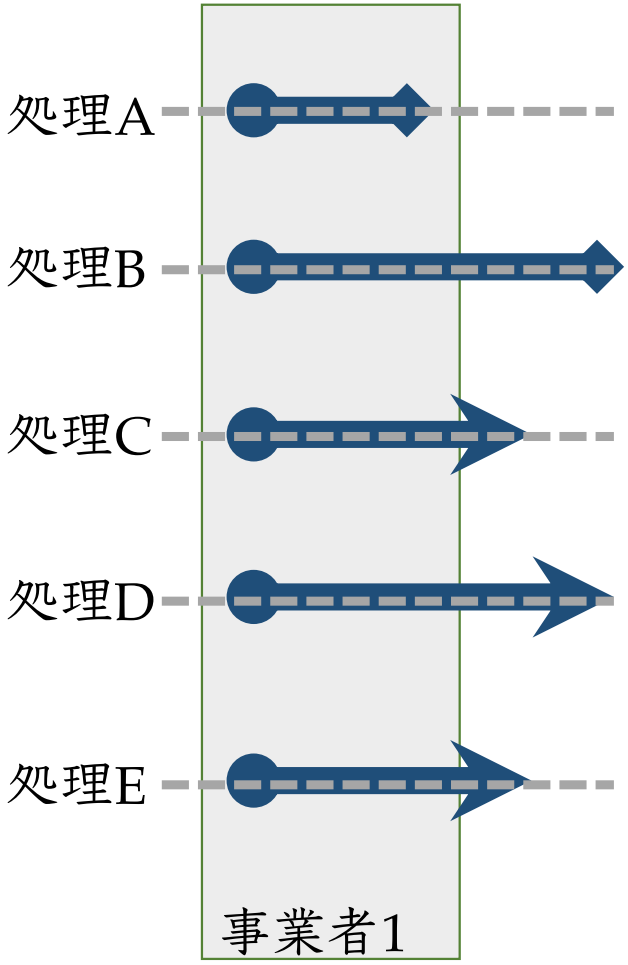
どちらの構造が望ましいか

1 purpose N operatorsへの対応力

- Operator-first構造の下では「複数事業者が1つの目的のためにデータを共有・移転して処理」に対応困難
- Operation-first構造であれば一連の処理として対応可能



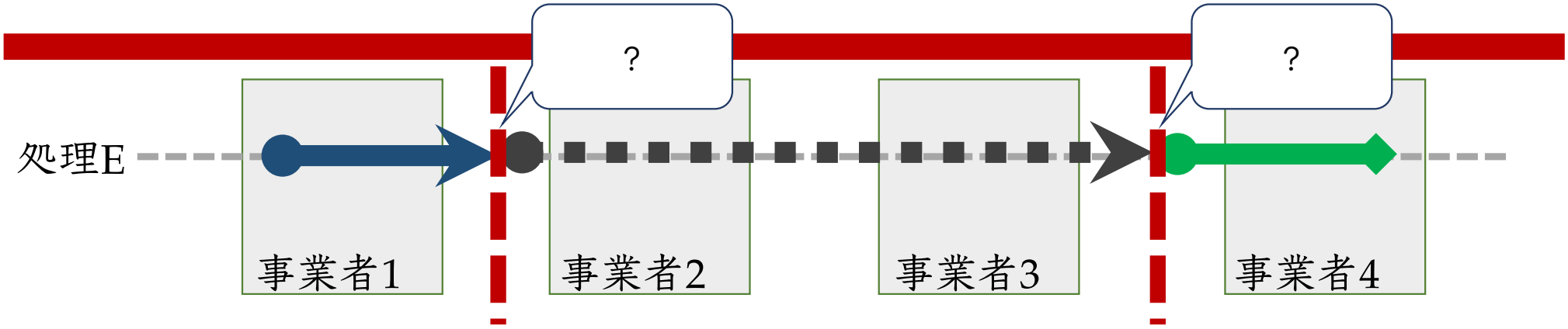
N purposes 1 operatorへの対応力



- Operator-first構造下では複数事業のデータ切分けには特別な措置が必要
  - Instagramの利用目的を変えるとFacebookの利用目的も変わる
  - 各サービスに分析部隊がいるとは限らないので容易照合性の否定が困難
- Operation-first構造であればそれぞれ独立した処理として対応可能

規制の予測可能性

- Operation-first構造下ではどこがステージの切れ目か予測困難
  - 実際、IAB Europe事件でAPD決定とCJEU決定で相違
  - ステージが分からないと責任分担の交渉もできない
- Operator-first構造なら自分の手の届く範囲のデータから規制内容が予測可能



Summary

- データ保護法の比較でも「スコープ」「実質」に加えて「構造」にも着目すべき
- 個人情報保護法とGDPRの構造の比較を行った
  - 個人情報保護法は事業者を単位にしたoperator-firstの構造
  - GDPRは処理のステージを単位にしたoperation-firstの構造
- 1事業者1サービスの前提が崩れた現代にはoperation-firstの方が合理的ではないか

References

[1] Paul Ohm, 'Focusing Privacy Law' (2025) 40 Berkeley Technology Law Journal 391.

[2] 堀部政男「情報公開・プライバシーの比較法」 in 堀部政男(編)『情報公開・プライバシーの比較法』(日本評論社 1996).

[3] 石井夏生利・曽我部真裕・森亮二(編) 『個人情報保護法コンメンタール第2版第1巻』(勁草書房 2024).

[4] 宮下紘『EU一般データ保護規則』(勁草書房 2018).

[5] Seiichi Igaya & Osamu Sudoh, 'Ignored discrepancies in the fundamental concepts of data protection laws in Japan and the EU' (2025) International Data Privacy Law ipaf015.

[6] Paul Ohm, 'Broken promises of privacy: Responding to the surprising failure of anonymization' (2010) 57(6) UCLA Law Review 1701.

[7] Flora Y Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) Harvard Journal of Law & Technology 661.

[8] Robert Baldwin, Martin Cave & Martin Lodge, Understanding Regulation: Theory, Strategy, and Practice (Oxford University Press, 2012).

References

[9] European Chemicals Agency, 'Guidance on Information Requirements and Chemical Safety Assessment' (2016).

[10] Claudio Borio, Stijn Claessens & Nikola Tarashev, 'Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs' (2022) 404 SUERF Policy Brief.

[11] Jeremy C Kress, Patricia A McCoy & Daniel Schwartcz, 'Regulating Entities and Activities: Complementary Approaches to Nonbank Systemic Risk' (2018) 92 Southern California Law Review 1455.

[12] 「キーパーソンが語る渋谷の未来 安藤忠雄」(渋谷文化Project) <https://www.shibuyabunka.com/keyperson/?id=63> accessed 21 Nov 2025.

[13] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドラインに関するQ&A」.

[14] 個人情報保護委員会「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)」.

[15] 岡田淳ほか「個人情報保護法」(商事法務 2024).

References

[16] IT戦略本部 IT戦略本部 個人情報保護法制化専門委員会 「第25回個人情報保護法制化専門委員会議事録」(2000) <https://web.archive.org/web/20061111074537/http://www.kantei.go.jp/jp/it/privacy/houseika/dai25/25gijiroku.html> accessed 9 Oct 2025.

[17] 29条作業部会, 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones - wp231' (2015).

[18] 欧州司法裁判所, Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629.

[19] 欧州司法裁判所, Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, Opinion of AG Bobek.

[20] 欧州司法裁判所, Case C-604/22 *IAB Europe* v *Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214.

[21] Gegevensbeschermingsautoriteit, 'Concerning: Complaint relating to Transparency & Consent Framework (DOS-2019-01377)' (2022).

[22] 欧州司法裁判所, Case C-268/21 *Norra Stockholm Bygg AB* v *Per Nicander AB* [2023] ECLI:EU:C:2023:145, Opinion of AG Ćapeta.

[23] 欧州司法裁判所, Case C-252/21 *Meta Platforms Inc* v *Bundeskartellamt* [2023] ECLI:EU:C:2023:537.