資料1-2

国際先端テスト
検討結果

⑩ビッグデータ・ビジネスの普及
（匿名化情報の取扱い）

規制の概要・課題

- 個人情報保護法により、個人情報取扱事業者は、「個人情報」を取り扱う際には、予め本人の同意を得ないで、特定した利用目的以外の目的での利用ができず、第三者提供が制限されている等、種々の制約が存在する。
- 個人を識別できなければ「個人情報」には該当しない。
- しかし、事業者が、収集した「個人情報」に対して どの程度の加工等を実施すれば「個人情報」に該当しなくなるのか不明確であるため、 収集した「個人情報」を利活用した新規ビジネスの創出を阻害している旨の指摘がある。

【規制所管省庁の回答（概要）】

（1）諸外国の状況(米国・EUとの比較)

（米国）

・匿名化に関する包括的な規定はない。

・ただし、FTC（連邦取引委員会）が個人情報の保護に係る調査及び法執行を行っており、3要件（①合理的な非識別化措置、②再識別化しないことを公に約束、③受領者による再識別化を契約で禁止）を満たす場合はデータの利用が可能との見解を公表している。

・第三者提供に関する包括的な規定はないが、個別分野において規定が存在する。

（EU）

・データ主体が識別できないような方法で匿名化されたデータは利用が可能とされている（EUデータ保護指令）。

・第三者提供については、原則として提供できないが、データ主体の明確な同意等があれば、提供可能となっている。

（2）規制を維持する必要性についての規制所管省庁の主張（要旨）

『日本の制度は、欧米と比較して匿名化情報の利用について厳しい規制を設けているものではない。』

『特定個人を識別できないような対応を事業者が施すことにより（欧米と同様）、属性情報や履歴情報の利用を図っていくことは現行制度でも可能。』

【規制改革会議の意見】

○現行規定ではどのような合理的な匿名化のための措置を取れば、個人情報に該当しなくなるかがわからず、事業者がビッグデータを利活用しようという発想になりにくい。

○個人情報保護法を所管する主務官庁として「こうすれば大丈夫」という、いわゆるセーフハーバー・ルールを早期に明示すべきではないか。

国際先端テストシート

（消費者庁回答）

匿名化情報の利用に関する日本と欧米の制度の比較

国名 / 視点	EU		米国	日本（個人情報の保護に関する法律）
	EU データ保護指令	EU データ保護規則提案		
「個人情報」概念の規定	規定あり ・識別された又は識別され得る自然人に関するすべての情報	同左	包括的な規定なし ただし、プライバシー権利章典において、特定の個人に連結可能なあらゆるデータ 個別分野において規定あり ・個人の識別が可能な医療情報（HIPAA） ・オンライン上で収集された個人に関する情報であって、個人識別が可能であるもの（COPPA）	規定あり ・生存する個人に関する情報であって、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。）
A．匿名化に関する規定（識別できない場合）	規定あり ・データ主体が識別できないような方法で匿名化されたデータについては利用可能	同左	包括的な規定なし ・FTC による監督（差止め、排除命令、制裁金）が及ぶ。 ・FTC レポートによると、３要件（①合理的な非識別化措置、②再識別化しないことを公に約束、③受領者による再識別化を契約で禁止）を満たす場合は利用可能 個別分野において規定あり ・識別子の除去等、一定の要件を満たす場合は利用可能（HIPAA）	規定なし ・事業者が識別できないような方法で匿名化された情報については「個人情報」に該当しないため利用可能 ・なお、事業等分野ごとのガイドラインにおいて、匿名化に関する指針を置く例がある（例：「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」や「ヒトゲノム・遺伝子解析研究に関する倫理指針」等）
B．第三者提供に関する規定（識別できる場合）	規定あり ・原則として提供できないが、次の場合は提供可能 (a)明確な同意、(b)契約の履行、(c)法的義務の遵守、(d)データ主体の重大な利益の保護、(e)公共の利益のため、(f)管理者等の正当な利益のため　等	規定あり ・原則として提供できないが、次の場合は提供可能 (a)具体的な目的のための処理に同意、(b)契約の履行、(c)法的義務の遵守、(d)データの対象者の重要な利益の保護、(e)公共の利益のため、(f)管理者の正当な利益のため　等	包括的な規定なし ・FTC による監督（差止め、排除命令、制裁金）が及ぶ。 個別分野において規定あり ・診療時等を除き、提供には本人の同意が必要（HIPAA） ・提供には両親の事前の承諾が必要（COPPA）	規定あり ・原則として提供できないが、次の場合は提供可能 (a)事前の本人の同意、(b)法令、(c)人の生命、身体又は財産の保護のために必要 (d)公衆衛生・児童の健全育成に特に必要 (e)国等に協力　等

⇒　日本の法制度は、欧米と比較して匿名化情報の利用に関して厳しい規制を設けているものではない。

特定個人を識別できないような対応を事業者が施すことにより（欧米と同様）、属性情報や履歴情報の利用を図っていくことは可能。

国際先端テストシート

（消費者庁回答）

匿名化情報の利用に関する日本と欧米の制度の比較

1　EU

(1) EU データ保護指令（「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data））〔1995 年〕

● **個人情報の概念**

「個人データ」とは、「識別された又は識別され得る自然人（以下「データ主体」という。）に関するすべての情報をいう。識別され得る個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的並びに社会的アイデンティティに特有な一つの又はそれ以上の要素を参照することによって、直接的又は間接的に識別され得る者をいう。」（第２条(a)）

● **匿名化に関する規定**

「データ保護の原則は、識別された又は識別され得る個人に関するあらゆる情報に適用すべきである。ある個人が識別できるかどうかを判断するためには、データ管理者又は当該個人を識別しようとする他の者によって用いられるあらゆる合理的な手段を考慮に入れるべきである。データ保護の原則は、データ主体がもはや識別できないような方法で匿名化されたデータについては適用すべきでない。」（前文第 26 条）

【参考】第 29 条作業部会意見（Article 29 Working Party「Opinion 4/2007 on the concept of personal data」）

特定の個人を識別できるかどうかの判断は、識別に用いられるあらゆる合理的手段の程度を考慮して、ケース・バイ・ケースで行われている。（21 頁）

なお、同意見書は、「符号化されたデータ」（key-coded data）という概念を用いているところ、例えば、名前を符号化（名前を「X1234」に置きかえる等）して管理し、当該符号を解読する鍵（符号と個人の氏名を結びつけるリスト）が別に保管されている場合、この鍵（リスト）を参照することは識別するための「合理的手段」といえるため、一連の個人に関する情報は個人データとみなすことができると指摘する。（18～19 頁）

⇒　つまり、「X1234 が週３日以上ワインを飲んでいる」というように符号化しても、「X1234」を氏名等の識別情報と結び付ける「対応表」を保有している場合は、「週３日以上ワインを飲んでいる」という情報を含め、「個人データ」に該当することになる。

※　「第 29 条作業部会」とは、EU データ保護指令第 29 条に基づいて設置される、個人データの取扱いに係る個人の保護に関する助言機関であり（第 29 条第

１項)、本指令に従って採択された各国の措置の統一的な適用に資するために、当該措置の適用を含むあらゆる問題点について検討等を行う権能を有する（第30条第１項)。

● **個人情報の第三者提供に関する規定**

構成国は、次の条件を満たす場合にのみ、個人データが取り扱われるように定めなければならない。（第７条）

(a) データ主体が明確に同意を与えた場合、又は、

(b) データ主体が当事者となっている契約の履行のために取扱いが必要な場合、又はデータ主体の請求により、契約の締結前に、その段階を踏むために取扱いが必要な場合、又は、

(c) 管理者が従うべき法的義務を遵守するために取扱いが必要な場合、又は、

(d) データ主体の重大な利益を保護するために取扱いが必要な場合、又は、

(e) 公共の利益のために、又は管理者若しくはデータの開示を受ける第三者に与えられた公的権限の行使のために行われる業務の遂行上取扱いが必要な場合、又は、

(f) 管理者又はデータの開示を受ける第三者若しくは当事者の正当な利益のために取扱いが必要な場合。ただし、これらの利益より、第１条第１項の規定に基づいて保護が必要とされるデータ主体の基本的な権利及び自由に関する利益が優先する場合には、この限りではない。

(2) EU データ保護規則提案（「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則」の提案（Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 〔General Data Protection Regulation〕））〔2012 年〕

● **個人情報の概念**

・ 「個人データ」とは、「あるデータの対象者に関するすべての情報を意味する。」（第４条(2)）

・ 「データの対象者」とは、「識別された自然人、又は管理者あるいはそれ以外の自然人や法人によって合理的な範囲で使用される手段をもって直接的又は間接的に識別された自然人のことを意味する。特に、識別番号、位置データ、オンライン識別子の参照、又はその人物のアイデンティティに関する肉体的、生理的、遺伝子的、精神的、経済的、文化的、又は社会的な一つ以上の要素の参照によって識別された自然人のことを意味する。」（第４条(1)）

● **匿名化に関する規定**

「データ保護の原則は、識別された又は識別され得る個人に関するあらゆる情報に適用すべきである。ある個人が識別できるかどうかを判断するためには、データ管理者又は当該個人を識別しようとする他の者によって用いられるあらゆる合理的な手段を考慮に入れるべきである。データ保護の原則は、データ主体がもはや識別できないような方法で匿名化されたデータについては適用すべきでない。」（前文第 23 条）

【参考】EU データ保護規則提案への欧州委員会修正案

「データ保護の原則は、識別された又は識別され得る個人に関するあらゆる情報に適用すべきである。ある個人が識別できるかどうかを判断するためには、データ管理者又は当該個人を識別しようとする他の者によって用いられるあらゆる合理的な手段を考慮に入れるべきである。この規則は、匿名化されたデータについては適用されない。匿名化されたデータとは、直接的又は間接的に、単独又は関係するデータと組み合わせた場合、自然人と結びつけることのできないあらゆるデータをいう。また、そのデータを処理する時代の技術の状況、そのデータが処理されるであろう期間の技術革新の可能性を考慮して、そのようなつながりを作り出すにあたって不均衡なほど時間、費用、労力がかかる場合も同様である。」

● **個人情報の第三者提供に関する規定**

個人データの処理は、以下の項目のうち少なくとも一つの項目が適用される場合に限り、合法とする。（第６条第１項）

(a) データの対象者が、一つ以上の具体的な目的のために、自分自身の個人データが処理されることに同意している

(b) データの対象者が当事者である契約を履行するためにその処理が必要な場合。または、契約を締結する前に、データの対象者の依頼によって対策を講じるためにその処理が必要な場合

(c) 管理者が従うべき法律上の義務を果たすために、その処理が必要な場合

(d) データの対象者の重要な利益を保護するために、その処理が必要な場合

(e) 公共の利益のために遂行される業務、または管理者に与えられた職権の行使のためにその処理が必要な場合

(f) 管理者が追求する正当な利益のためにその処理が必要な場合。ただし、特にデータの対象者が子供の場合、個人データの保護を必要とするデータの対象者の利益または基本的権利や自由が、上記の管理者の利益に優先される場合を除く。このことは、公的機関が職務の実施のために行った処理には適用しないものとする。

2　アメリカ

●　概要

アメリカでは、事業活動一般につき分野横断的に規律している法律は存在せず、高い機密性の要求される一部の分野において個別法が制定されるにとどまっている。民間企業に対しては、連邦取引委員会（FTC）が中心となって調査及び法執行を行っており、個人データ保護に関するレポートやガイドライン等も多数発表している。

これらに加えて、近年、いわゆるビッグデータビジネス等、個人情報を利用する新たなビジネスが成長している現状を踏まえ、インターネット上の個人データ保護の強化を目的とした「米国消費者プライバシー権利章典」（(The Consumer Privacy Bill of Rights)〔2012 年〕※）が発表されている。

（※）アメリカにおいて発達してきた公正な情報慣習の原則を 7 つの権利として具体化したもので、連邦議会に対して立法を呼びかけるもの。

●　個人情報の概念

・　「個人データ」とは、特定の個人に連結可能なあらゆるデータをいい、集計されたデータを含む。これは、特定のコンピュータやその他の機器に連結されたデータも含む（「米国消費者プライバシー権利章典」）。

・　個人データの概念に関する包括的な法律はなく、個別分野ごとに法律がある。

【主要な例】

・　HIPAA（「医療保険の相互運用性と説明責任に関する法律」（Health Insurance Portability and Accountability Act））〔1996 年〕
「個人情報」とは、「個人の識別が可能な医療情報」をいう。

・　COPPA 改正案（「児童オンラインプライバシー保護法」（Children's Online Privacy Protection Act）改正案）〔2012 年〕
「個人情報」とは、「オンライン上で収集された個人に関する情報であって、個人識別が可能であるもの」をいう。具体的には、(A)氏名、(B)通りの名称や都市・町の名称を含む住所等、(C)電子メールアドレス、(D)電話番号、(E)ソーシャルセキュリティナンバー、(F)FTC が定める物理的又はオンライン上特定個人に連絡可能なその他の識別子、(G)ウェブサイト等がオンライン上で収集し、(A)から(F)の識別子と組み合わされた、児童又はその児童の親に関する情報をいう。

※　米連邦取引委員会（FTC）は、2012 年 12 月 19 日に最終改正案を採択し、2013 年 7 月 1 日に発効の見通し。
改正案では、「個人情報」のリストの中に、位置情報等が新たに加えられた。

●　匿名化に関する規定

・　匿名化について、事業活動一般につき分野横断的に規律しているものは存在しない。

・　匿名化された個人データの取扱いが、「不公正又は欺瞞的行為又は慣行」（FTC 法第５条（a））に該当するとされた場合は、FTC により、差止め、排除命令、民事制裁金を課される可能性がある。

・　FTC は、米国連邦取引委員会（FTC）レポート（Federal Trade Commission「Protecting Consumer Privacy in an Era of Rapid Change」）〔2012 年〕を発表し、匿名化された個人情報の取扱いに関する指針を示している。

事業者が、

①データを合理的に非識別化（de-identify）するための措置をとる

②そのデータを再識別化（re-identify）しないことを公に約束する

③そのデータの移転を受ける者が再識別化することを契約で禁止する

との要件を満たせば、当該データは特定の顧客、コンピュータその他のデバイスに、合理的に連結可能な（reasonably linkable）データには当たらないとしている。また、事業者が、識別可能なデータとこのように非識別化されたデータの双方を保持・使用する場合は、これらのデータは別々に貯蔵すべきであるとしている。（18～22 頁）

・　さらに、特定の分野において、個別法の中で匿名化に関する規定が存在する。

【主要な例】

HIPAA（「医療保険の相互運用性と説明責任に関する法律」（Health Insurance Portability and Accountability Act））〔1996 年〕

①　「匿名化」された保険情報（de-identified health information）については、使用や開示に法律上の制限はない。

⇒　「匿名化」といえるための条件

(a) 統計学者から個人特定リスクが低いという専門的意見を書面でもらうこと（当該書面には、分析方法と分析結果の両方が含まれていなければならない）、又は

(b) 名前、電子メールのアドレス、社会保障番号、医療記録番号、健康保険受給者番号、免許証番号など親族、雇用主又は個人の家族の識別子（18 項目）の情報を除去すること

②　「限定されたデータセット」については、個人の許諾を得ずに、使用や開示することが許可される。

⇒　「限定されたデータセット」といえるための条件

・　名前、電子メールのアドレス、社会保障番号、医療記録番号、健康保険受給者番号、免許証番号など、個人、親族、雇用主又は個人の家族に関する直接的な識別子を取り除くこと

● **個人情報の第三者提供に関する規定**

・　個人データの第三者提供について、事業活動一般につき分野横断的に規律しているものは存在しないが、米国消費者プライバシー権利章典においては、「個人データを第三者に開示する事業者は、受領者が（権利章典に定められた）これらの原則を遵守する執行可能な契約上の義務を負うことを保証しなければならない。」とされている。

・　個人データの第三者提供が、「不公正又は欺瞞的行為又は慣行」（FTC 法第５条（a））に該当するとされた場合には、FTC により、差止め、排除命令、民事制裁金を課される可能性がある。

・　また、特定の分野において、個別法の中で第三者提供に関する規定が存在する。

【主要な例】

・　HIPAA（「医療保険の相互運用性と説明責任に関する法律」（Health Insurance Portability and Accountability Act））〔1996 年〕
診療時、支払時、医療業務管理時に使用する場合等を除き、個人情報の第三者提供には、本人の同意が必要とされている。

・　COPPA 改正案（「児童オンラインプライバシー保護法」（Children's Online Privacy Protection Act）改正案）〔2012 年〕
13 歳未満の児童について、両親の事前の承諾なく、個人情報を収集すること、第三者へ個人情報を開示することは禁止されている。

3　日本（「個人情報の保護に関する法律」）

●　個人情報の概念

「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。」（第２条第１項）

●　匿名化に関する規定

なし。ただし、主務大臣制の下に策定されている事業等分野ごとのガイドラインにおいて、匿名化に関する指針を置く例がみられる。

例えば、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」や「ヒトゲノム・遺伝子解析研究に関する倫理指針」等は、匿名化の定義等について記述している。

●　個人情報の第三者提供に関する規定

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。（第 23 条第１項）

一　法令に基づく場合

二　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

三　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

四　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

※　参考（履歴情報の取扱いについて）

個人情報保護法上、特定個人を識別できないように氏名等識別情報から切り離された情報は、「個人情報」には該当しないため、その取扱いにつき、個人情報保護法上の義務規定の適用はない。例えば、資料１－４の設例１において、X が対応表を廃棄することにより、購入履歴情報と氏名等を容易に照合できないようにすれば、当該購入履歴情報は「個人情報」ではないため、それを第三者に提供することにつき、個人情報保護法上、本人の同意は求められていない。

4　結論

● 日本は EU と比較して、匿名化情報の利用に係る法規制の程度が厳しいとはいえない。例えば、上記「X1234 が週３日以上ワインを飲んでいる」という事例について、EU においては、事業者が「X1234」を氏名等の識別情報と結び付ける「対応表」を保有しているのであれは、「週３日以上ワインを飲んでいる」という属性情報を含め、「個人データ」に該当することになる一方、「対応表」を廃棄するなどして識別情報と結び付かないように管理しているのであれば、当該属性情報は「個人データ」には該当しないこととなる。これは日本でも同じであり、事業者が「対応表」を保有することで特定個人を識別できるのであれば、「週３日以上ワインを飲んでいる」という属性情報は「個人情報」に該当する一方、「対応表」を廃棄するなどして特定個人を識別できないように管理しているのであれば、当該属性情報は「個人情報」には該当しないこととなる。

● 日本はアメリカと比較しても、匿名化情報の利用に係る法規制の程度が厳しいとはいえない。アメリカにおいてプライバシー侵害違反の法執行を担っている FTC の前掲レポートでは、合理的に連結可能なデータに当たらない（「個人データ」に該当しない）というためには、①合理的な非識別化措置、②再識別化しないことの公の約束、③データ移転を受ける者が再識別化することを契約で禁止、これら①ないし③の要件全てを満たさなければならない、との厳格な意見を述べているが、日本では、法律上、②や③の措置まで求められるものではない。

● このように、日本の法制度は、欧米と比較して匿名化情報の利用に関して厳しい規制を設けているものではなく、個人情報の「保護」と「活用」のバランスの観点から、例えば「対応表」を廃棄するなど、特定個人を識別できないような対応を事業者が施すことにより（欧米と同様）、属性情報や履歴情報の利用を図っていくことは可能である。