主導権を握るようになる.

1995年のEU個人情報保護指令に先立って,国際的な個人情報保護ルールを確立したのは,1980年のOECD8原則と,Convention on Privacy of the Council of Europe（ヨーロッパ評議会プライバシー条約）だった.OECDには,アメリカも入っており,日本でもこの8原則が常に援用されるようになる.ヨーロッパ条約の方は,ヨーロッパ地域における個人情報取扱についての国際的合意を定めるものとして,同地域で大きな意味を持った.

この時期には,アメリカとEU諸国の間に交渉や対話があった.OECD8原則の策定にも協力関係があり,1890年のWarren & Brandeisのプライバシーに関する古典的論文がヨーロッパで引用され,さらに2012年には,そのドイツ語訳が刊行されている[2].

また,この時期には,個人情報保護の問題を人権の問題か,または情報を利用した産業発展や公益の増進の問題かという,二者択一な発想はなかった.それは当然ながら両面に常に関係していた.OECDガイドラインでも,一方では,個人情報に関するプライバシーの権利の重要性を説きながら,他方では,国境を越えて個人情報が自由に流通することを阻害するような不統一な法の問題性を指摘していた.ヨーロッパ条約でも,前文で,個人情報の保護と国家間の情報の自由な流通の調整を明確に謳っていたのである.

1995年のEU指令も,その性格自体,harmonizing（ソフトな方法での調和達成）を図る手段であり,EU加盟国に対し3年以内において基本原則を同じくする立法を制定するよう求めていた.その内容も,基本的に,さまざまな加盟国の見解を合わせた妥協的性格を帯びざるをえなかったのである.

①指針の目的は,個人情報の域内での自由な流通を図りつつ,個人情報保護を高度なレベルで図ることとされた.

②ただし,域外適用がもくろまれ,第25条で,適切な個人情報保護法制をもたない国への情報移転を禁ずることにした.

③その適切性の判断は,それぞれの加盟国に委ねられたが,同時に,ヨーロッパ委員会にもその適切性について非加盟国と交渉する権限が認められた.ただし,その適切性の判断には,当該情報の性格や情報保存期間など,具体的な事情を考慮した判断が求められるとした.

この後者2点は,実際にきわめて大きな影響を及ぼした.第1に,個人情

[2] Samuel D. Warren & Luis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890), Dasu Recht auf Pivatheit---The Right to Privacy (Marit Hansen & Thilo Weichert translation), 36 Datenshutz und Datensicherheit 755 (2012).

報保護法の形式について，EU モデルを，EU 内外に広めた．要するに個人情報保護法という単一の法が多くの国で策定された．EU 自体，1995 年当時の 15 カ国から，2013 年には 27 カ国に増加し，しかも新規加盟国では同様の個人情報保護法が制定された．第 2 に，その内容の点でも EU モデルが世界中に拡大した．そのいずれの面でも，アメリカは蚊帳の外に置かれた．

アメリカでは，この間，特定分野だけに個人情報保護を図るという対応がなされた．情報管理義務者について特定し，情報の内容別に，個別法が策定された．医療情報に関する HIPAA，教育情報に関する FERPA，ビデオ・レンタル等に関する Video Privacy Protection Act of 1988 などがその例である．ただし，個人情報保護の内容面では，一定の共通理解があり，FIPs の遵守を定める内容となっていた．その点に着目した論者は，個人情報保護について，アメリカと EU を含む世界標準ができると予想する向きもあった．ところが，実際にはそうはならなかった．

3　個人情報保護原則の内容—EU とアメリカの相違

個人情報保護については，先に述べたような共通原則が当初存在していた．OECD8 原則はその例であり，アメリカでは「公正な情報取扱原則」(Fair Information Practices, FIPs) と呼ばれている．

その内容は以下のとおりである．

①情報利用の目的を制限する

②情報取得について制限する

③個人情報の第三者提供・開示を制限する

④正確な情報のみ取得し，利用する

⑤個人に，情報について通知し，アクセスを認め，訂正する権利を認める

⑥情報の加工・処理について，当該個人が知り，理解できるシステムを構築する

⑦個人情報のセキュリテイ（安全保護措置）を確保する

このうち，EU では，FIPs の中で，特に次の 3 原則が重視された．

イ）情報取得自体の制限（前掲②）

ロ）情報の正確性や最新性の強調（前掲④）

ハ）個人に，自らの情報について通知を受け，アクセスが認められ，訂正を請求する権利があること（前掲⑤）

そしてそれらの基盤には，これら個人情報をめぐる権利は基本的人権だとする考え方が強くなった．

他方，アメリカでは，情報処理について，個人に関与を認め，このような通知を受ける権利等が生ずるという考えは，アメリカでは限定的にしかと

られなかった．アメリカでは，事前の同意に一定の情報処理に対する同意が含まれるとされ，さらに個人の権利も，他者の表現の自由やその他の公益，社会的利益との間で調整すべき原理であるとされた．

しかも，EU では，次のような諸原則も FIPs に当然含まれるとされた（アメリカではそうではない）．

ニ）個人情報の処理をするには法的な根拠が必要である（まず規制ありき）．

ホ）第三者機関による監視があること（データ保護庁が必要）．

ヘ）個人情報保護法制が不適切な第三国への情報移転の禁止（情報処理の第三国へのアウトソーシングも禁止される）．

ト）データ処理技術の発展による自動的な情報処理は制限される．

チ）センシティブ情報にはさらに強い保護を要する．

これに対し，アメリカでは，個人情報の取得も処理も，それを禁ずる法律がない限り自由とされた（上記の規制ありきとは根本的に立場が異なる）．この背景には，合衆国第１修正による表現の自由の保護も大きく影響している（個人情報の保護より知る権利の方が，アメリカでは優越する）．

アメリカ法の特色を，以下，列挙する．

（１）表現の自由とそれを基礎づける情報取得の重要性を重視する．たとえば 2011 年の Sorrel v. IMS Health Inc. はそれを示す一例である[3]．医師向けにターゲット広告を意図する事業者がデータ販売するのを禁じたヴァーモント州法について，連邦最高裁は，それらの情報取得もそれに基づく表現の自由の基盤をなし，本件では，研究目的の取得はできるが，経済的理由での取得を禁じており，それは内容による規制にあたるとして違憲無効とした．

（２）アメリカでは，国外（たとえばインド）に個人情報処理をアウトソーシングすることも許される．

（３）個人情報に関する公的監視機関としてアメリカに存在するのは，FTC である．FTC は消費者保護や不公正な競争を規制する権限を有しており，個人情報保護についても一定の役割を果たしている．だが，対象とする企業の範囲はすべてではないし，FIPs のすべてについて責任を負うわけでもなく，さらに基本的な立場は，消費者への通知と選択の自由を保護するところにあり，それ以上の規制をするわけではない．

（４）最後に，センシティブ情報についても，アメリカ法は限定的な役割しか果たしていない．また，自動的な

[3] Sorrel v. IMS Health Inc., 131 S.Ct. 2653 (2011).

情報処理にも寛容である．前者についていえば，EUでは1978年のフランス法で一定のセンシティブ情報の規定が定められたのを受けて，1995年指令でも，「人種，政治的見解，宗教的信念，労働組合加入，健康や性に関する情報」の処理を禁じている．

（5）さらに付言するに，アメリカでは新規事業者に対し，新たな試みをする自由が認められてきた（これも，禁止法がない限りは何事も自由という国柄による）．その結果，新たな情報処理事業者がデータマイニングを行う行為は規制されないのに対し，ケーブル通信会社や電話事業者については法律があるので一定の規制があるというようなアンバランスも生じた．しかし，イノベーションを図る事業者に有利な法制度だともいえる．

このようなアメリカ法の状況はEU法とは相当に異なった様相を呈している．そして，世界はアメリカに追随しなかった．EUモデルこそが実際上，世界標準となっている．

4　EU個人情報保護指令の下でのアメリカとEUの妥協策

1995年EU個人情報保護指令第25条は，EU非加盟国との情報交換について，相手国に「適切な」個人情報保護法制を求める定めを置いた．そしてEUから見れば，アメリカ合衆国の個人情報保護法制は，「適切」とはいえないものだったはずである．しかし，公式的にEUがアメリカ合衆国を「不適格」と烙印を押したことはない．ただし，EU各国の認識はすべて，アメリカの法制度を「不十分・不適切」とする点で一致している．たとえば，1999年の指令第29条に関するワーキング・グループの次のような言明はそれを示す[4]．

「現状のような個別分野についてだけ法律で定めるパッチワーク的な法制度と自主的な規制を旨とする体制は，EUから情報移転するにふさわしい適切な情報保護体制が整っているとはいえない」．

そこで，アメリカの企業がEU基準を満たすために3つのルートが作られた．

①セーフ・ハーバー方式

②2つのモデル契約書（約款）

③企業の情報管理ルール

これらは政治的妥協だとみられてきたが，アメリカの論者の中には，これらのルート策定の際に，さまざまな利害関係者が協力して「法形成・ルー

---

[4] The Article 29 Working Party, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Governmentpdf 2 (13 kB) Choose translations of the previous link - WP 15(26.01.1999) http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

ル形成」を果たした点にこそ注目すべきだと論ずる者がいる[5].

まず,先の3つの対応について説明する.

①セーフ・ハーバー方式

その最初は,アメリカ商務省とEU委員会との間で行われた1998年の交渉に始まる.2000年7月にEU委員会は,セーフ・ハーバー合意書を公表し,EU議会はそれを拒否したものの,7月25日にEU委員会が承認して効力を発生した.

基本的なスキームは,アメリカの企業について,自主的な認証システムを構築するところにある.基準内容はEU基準に近いものとなっている.しかし,その遵守は,アメリカの連邦機関,特にFTCが所管する.実際に,この国際的合意に反したとして,グーグルやフェースブックについて,2011年と2012年に違反を認定した例もある.アメリカ企業に有利な点としては,このセーフ・ハーバー合意書に反するとしてEU市民からの訴えがなされる場合,それはアメリカでの訴えとなり,アメリカの法原則が適用になる点がある.最も重要な点としては,このセーフ・ハーバー合意書に参加している企業は,EUにおいて「適切な基準」を満たしているとみなされる.EU加盟国もこれらの企業については事前に審査する必要がなくなる.

[5] Schwartz, supra note 1, at 1990.

②モデル契約約款

2つめの方法としてEUが提供したのは,2種類のモデル契約約款である.1995年の指令26条2項に根拠を置くこの約款により,「適切な契約条項」の下での情報移転が許された.適切さをこのような契約条項で確保するという手段である.EUで「適切」と認めた契約条項を挿入することで簡易かつ安価に,アメリカの企業はEUとの取引をすることが可能になる.実際にはその内容についても,EUが一方的に定めるのではなく,多国籍企業等との間での調整が行われた.国際商業会議所なども策定に関与した.

第1のモデル約款はEU委員会によって2001年に承認された.第2のモデル約款は2004年承認である.全体としてみてその内容は,情報保護の合理的な遵守と違反があった場合の救済について,個々人に対し各企業が保証する定めとなっている.第1モデルでは,国際間の取引での個人情報の送り手と受け手に,連帯責任を負わせたが,これについては反対が多く,第2モデル案では,連帯責任ではなく個別責任が原則となっている.ただし,第2モデル約款では,デュー・ディリジェンス条項が挿入され,情報の受け手が契約条項を遵守するよう送り手に監視する義務を負わせた.

③企業の情報管理ルール

EUが認めた第3の手段として,

EU が適切と判断するような「企業としての義務的ルール」を採用するものがある．これは，アメリカ企業が個人情報を取得した場合，それを企業内または関連企業内だけで利用する場合に好都合なものとして構想された．これらの企業内での個人情報保護の体制構築によって，EU 基準により「適切」とみなすというものである．

第 29 条に関するワーキング・グループがこの策定に貢献し，2003 年に，このような内部情報管理体制を作ればそれによって「適切」とみなすというルールを作り上げた．当初は各国のデータ保護機関から承認を得る必要があったが，2007 年には単一の指導的データ保護機関から承認を受ければ EU 加盟国すべてとの取引が可能となった．

【これらの枠組みの意義】

EU とアメリカの法制度の衝突を回避するうえで，上記 3 つの方策は大きな貢献をした．EU 基準の押しつけではなく，一定の交渉がなされ，真正面からの衝突が回避されて，円滑な国際的情報流通が確保されたのである．

アメリカの企業はこれら 3 つの方策のいずれかを選択して，EU との取引を継続することができた．多国籍企業も，これらの方策を個人情報保護に関するコンプライアンスの基準とした．

このような経過について，アメリカでは，2 つの学問的モデル（見方）が提唱されている．1 つは，Anu Bradford の「ブラッセルの影響力」モデルであり[6]，そこでは EU モデルが世界的に大きな影響力を持つに至った要素が分析されている．しかし，Mary Ann Slaughter の「調和的ネットワーク形成」モデルでは[7]，むしろ EU の影響力だけでルールは形成されておらず，多様な関係者(stakeholders)が関与して交渉がなされ，一種の「調和的法形成」がなされたと見る．このモデルの方が，将来的に見ても，さまざまな政策形成関係者が関与して，真に生産的なインターネット情報流通モデルを説明するのに適しているが，新たな EU 規則案は，このような道を狭まるおそれがある．

実際，規則案の提案以前の状況は，EU の，しかもブラッセルにおける一

---

[6] Anu Bradford, The Brussels Effect, 107 Northwestern University Law Review 1 (2013)．ブラッドフォードによれば，「ブラッセルの影響力」があるとされるためにはいくつかの前提条件を満たす必要がある．

①EU 加盟国に世界市場における影響力があること．

②EU に個別的な規制能力があること．

③一定の明確な基準が定められること．

一見すると，個人情報保護法制については，これらの基準がすべて満たされ，さらに現実にも，EU モデルの個人情報保護法が EU 域外にも拡大しているのであるから，まさにこの適例であるように見える．

[7] Anne-Marie Slaughter, A New World Order 59-61 (2004, Princeton Univ Pr).

機関が策定したルールが世界を席巻したといえるほど単純ではない．さまざまな利害関係者が関与し，アメリカから見れば，EU からも一定の妥協を引き出して形成されたことがわかる．アメリカとの合意で形成された前記 3 方式がその典型であり，アメリカの存在が結果の違いをもたらした．その背景には，EU 内部でも，複数の方針の間に，相互に矛盾する要素を抱えていたこと，EU の世界市場への影響力にも一定の限界があったことがある．

1995 年指針自体が，その内部に矛盾する要素を抱えていた．個人情報を基本的人権として保護すると同時に，域内（さらに域外との）取引促進し，その中で個人情報を利用するという目的も掲げているのであるから，前者が絶対ということにはならない．指針の 56 条は，国境を越えた個人情報の交流も，国際取引の発展のために不可欠だと明言している．要するに，個人情報を保護しつつ，その利用・活用を図るのが，1995 年指針の立場だった．

EU 内部でも，それぞれの国の保護主義に対抗して，１つの自由市場を形成する努力がなされ（個人情報保護というスローガンは，実は自国産業を保護するための建前となるおそれがあること），さらに，個人情報保護についても EU 域内では「同等の」ルールを，域外には「適切な」保護ルールを要求するなかで，この 2 つの基準が同じ意味を有するのか否かについて争われてきた．そもそも域外について（EU とまったく同じではなく）「適切な」基準の遵守を求めたこと自体が，自由な個人情報の流通を手段として，国際取引の発展を図ろうとしたものと理解することができる．もちろん同じ基準を域外適用すること自体に，政治的法的な問題を生むという事情もある．

要するに，EU は（あるいは EU でも），EU の事業者（域内では自由な市場）と，人権としての個人情報保護の両方の目的を追求してきたのである．その点では，アメリカとも，他の EU 以外の国における基本的前提とも共通する理解ができる．そして，個人情報保護を絶対視するのではなく，まさに適切なバランスをとることが EU の事業者にとっても，消費者にとっても，利益である．そうだとすると，ブラッセルの影響力モデルが示唆するような，EU 基準の押しつけではなく，交渉による調整的なモデルの方が，将来的にもより適切だという判断になる．

スローター教授は，ある国が１つの基準を設定して押しつけるのではなく，世界的な秩序や基準とは，何らかの交渉ネットワークを構築しその中で調整が行われて形成されるというモデルを提唱する．

ある国の規制機関は，他国の規制機

関と連絡し，交渉し，調整的な力を発揮する．それによって全体としての効率性が高まる．ハーモナイゼーションが求められる局面では，まさにネットワークを形成した上での調整作業が行われる．そこには国家機関ばかりでなく多様な利害関係者が参加する．EU個人情報保護指針でいえば，EU 委員会，閣僚委員会，EU 議会，指令 29 条に関するワーキング・グループ，EU個人情報保護監督官，情報通信およびデータ保護に関するベルリン・グループ，それぞれの国のデータ保護監督官などが存在し，EU 外では，アメリカの商務省や FTC なども関与している．

先に述べたように，FTC がグーグルやフェースブックに対し，セーフ・ハーバー方式を実現するよう強制措置をとったことは，EU とアメリカで協調して一定のルールを現実化させようとした象徴的な例となる．

ただし，このような調整モデルにも，一定の原則が必要である．調整過程が外から見える透明性や，さまざまな関係者の参加は必然的に中央集権的なルール形成ではなく，一定範囲の権限を分属させる分権的なルール形成につながりやすいが，そのことをむしろ正当化し，意義あることだという共通認識が必要になる．

5　EU の 2012 年規則案

ところが EU 委員会の提案した 2012 年個人情報保護規則案は，これまでの状況を一変させる可能性がある．EU 内部では，これまでの指針と異なり，規則は画一的なルールを EU 全域に直接適用させる手段となる．個々の加盟国でそれと抵触するルールを定めることはできなくなる．

このような動きの背景には，第 1 に，急速な技術的発展により，個人情報の取得の規模が急増し，それが規制しにくくなったことがある．第 2 に，それに伴い，個人情報がより広範なレベルで特定しやすくなったことがある．第 3 に，少なくとも EU 委員会の認識では，1995 年指令に基づいてほぼ統一的な法制度が EU 域内にできればよかったが，各国で定めた個人情報保護法制には相当の違いがあり，やはり 1 つのルールを直接適用するのがよい，しかもそれで初めて，EU 市場における取引の発展も可能になるという見方があった．

その結果，1995 年指令の下での体制では不適切という判断がなされた．その結果生まれたのが規則案である．だが，それは EU 域内での権力関係（EU 当局と加盟国それぞれとの間の権力関係）を大きく変更すると同時に，アメリカとの間で形成されてきた均衡関係に大きな影響を与える要素を含む．

【2012 年規則案の概要―個人の権利の強化】[8]

2012 年規則案(2013 年修正も含む)は，これまでの 1995 年指令における以上の個人情報保護を定める点に大きな特色がある．

(最小範囲の個人情報しか許さないという原則の強化，情報処理を行う機関要件の厳格化，さらに忘れられる権利という新たな権利の創設，同意原則の強調など)は，現状の変更になる．個人情報の自動的処理への規制や，センシティブ情報へのいっそうの保護なども同様である．これらは EU とアメリカとの間に成立していた均衡状態を不安定化する．さらに，EU 内部でも，個人情報保護に関するルール形成についての権限配分の点で革命的な提言となっており，さまざまな利害関係者が関与してルールを形成する分権的モデルから，EU 委員会に権限を集中させる中央集権的性格を露わにしている．

①個人情報利用の範囲を限定すること

第 5 条．個人情報を用いなければ，当該目的が達成されない場合だけ，情報処理を認める．さらに，それが認められる場合でも，情報の範囲は最小限度の範囲とされる(data minimization の原則)．情報処理の目的も包括的では不可，特定された目的に限定されて，しかも取得の際の目的にその後も拘束される．

これはビッグ・データ時代に対応していると評価することもできるが，実は，ビッグ・データ時代のデータ解析は，当初の目的を越えた新たな発見を可能にするものであるだけに，このようなルールはビッグ・データ時代を否定することになりかねない[9]．情報処理の進歩が不可避であるとすれば，EU 規則が制定されこのような内容が含まれても，何らかの形で，ビッグ・データの解析を可能にするような状況が EU でも起こるのは不可避と考えられる．しかし，真正面からこれらの規定を受け取ると，新たな技術進歩への重大な規制となる．

②情報利用期間も限定されること．

その象徴が「忘れられる権利」あるいは「削除を求める権利」の創設である[10]．アメリカ側からすると，この点は，アメリカの憲法の掲げる表現の自

[8] なお 2012 年規則案は，2013 年 10 月に，EU 議会の委員会(LIBE 委員会，Committee for Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament)において一定の修正を経た後，圧倒的多数で承認されている．See, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm

[9] 樋口範雄「ビッグ・データと個人情報保護―医療情報等個別法を論ずる前提として」高橋和之先生古希記念論文集『現代立憲主義の諸相(下)』229－257 頁(有斐閣・2013 年)．

[10] Viktor Mayer-Schonberger, Delete: The Virtue of Forgetting in the Digital Age (2009)がその代表だとされる．

由と真っ向から抵触する．インターネット上に出た情報について考えると，そもそも実現可能な権利であるかにも疑問符がつく．

③同意原則を強化すること．

真の同意であることの立証責任を情報管理者に課し，とりわけデータ管理者とデータ主体との力の不均衡に意を用いて，同意の真偽・有無を判断するとしている．これらは，ネット上の取引等での「同意」について，EU側が持つ疑心を反映している．

④センシティブ情報については，第9条がその類型を具体的に列挙し，そこで認められた例外にあたらない限り情報処理を禁じている．しかも，その特別な取扱は現実的なリスクの判断によるものではなく，事前に，概括的な判断でなされている．イギリスのデータ保護庁でさえ，このような形式的で柔軟性を欠く取扱を批判している．例外的に許される場合も狭く規定されている．

⑤新たに登場してきたデータの自動処理については，いわゆるプロファイリングへのおそれと連動しており，20条で，その原則禁止を定める．

⑥最後に，規則案では罰則が強化され，罰金額が増加している．79条では，制裁金が定められる基準を定めているが，総合判断になっており予測可能性が低い上に，ある企業の世界中での歳入の2%にも及びうるとされている．数百万ドル（数十億円）にもなるということである．しかも2013年の修正で，規則を破った企業に，1億ドル（100億円）または1年間の全世界での売り上げの5％までの課徴金が課されることになり，さらに強化された．懲罰賠償制度を持ち，かつて1つの事故でも数十億円という賠償が認められる事例が大きく報道されたアメリカ人も吃驚するような金額である．

【規制権限の中央集権化】

EU規則案の特色として，規制の安定性を高めるため，EU委員会に大きな権限を委ねる点がある．EUについていわれてきた「補完性」原則への影響は明らかである．これは，原則は各加盟国のルール形成に委ねて，EUはその内容の標準化を「補完する」立場にあるとの原則を変更し，まさにEU法が直接前面に立つとする．それはEU法の原則自体の変更ではないかとの批判がある．

規則案は，個人情報保護の「安定化機構」として，European Data Protection Board (EDPD)の創設を提案している．これは29条に関するワーキング・グループの位置を高めて，機関化するものであり，その中では各国代表が議論する枠組みを維持する可能性もある．だが，各国がルールを作る前に，この機関でそれについて検

討して，承認を与える機能を認めるので，しかもそこでは単純多数決による決定が行われるので，従来の体制とは大いに異なる仕組みとなる．

より重要なのはEU委員会に大きな権限を委ねる点である．各国は，個人情報保護ルール「安定化プロセス」により，EU委員会の決定に最大限の配慮を与えなければならなくなる．しかもEU委員会で，一定の権限を別の機関に委ねて細則（あるいは具体的なルール形成）を委ねてよいとする点も，EU内部での政策決定のメカニズムの実質を大きく変えることになる．

【規則案のメリット】

しかし，規則案にも注目すべき点がある．

第1に，1995年指令以来のルール・メーキングの経緯を踏まえて，新たなルール形成の道を示唆している点である．45条では，EUの官僚，各国の規制当局，さらにNGOに対し，協力を呼びかけている．effective international co-operation mechanisms（効率的な国際的協力の仕組み）と呼ばれるこの体制が作られれば，さまざまな利害関係者が積極的に参加し，さまざまなアイデアが検討される場となる機会となる．

第2に，規則案自体には，1995年指令以来形成されてきたルールを継承している部分がある．特に，セーフ・ハーバー方式，2つのモデル約款，企業内義務的ルールの3方式が新たな体制でも有効だと明記した．最初の方式は即時有効とされ，最後の方式は43条で新たな承認手続を経る必要がある．2番目の方式も有効だとされている．

6　PII 2.0という提案と今後の方向性

アメリカにおける個人情報保護法の代表的論者であるSchwartz教授とSolove教授は，共同して，個人情報バージョン2（personally identifiable information, PII 2.0）なるものを提案した[11]．これは，個人情報保護の最大の要点である，何が個人情報であるかについて，EUでは広すぎる概念規定をし，他方でアメリカは狭すぎるとらえ方をしてきたとの認識のもとに，その中間に，今後，個人情報保護とその利活用を図る調整原理の基盤として，新たな考え方を提唱するものである．

【PII 2.0（以下，バージョン2）】

これはアメリカ法とEU法の間を架橋する概念として構想された．いずれにせよ，個人情報という概念自体を廃棄することはできない．その概念の内容が2つの法体制で大きく異なると

[11] これについては，前掲注1）の論文紹介を参照されたい．

ころが問題である．先に述べたように，このバージョン２では，個人情報とはまったくいえないものを一方の端に，他方の端には，完全に個人にリンクする情報を置いて，個人情報概念を一続きのスペクトルとして把握し，さらに大まかに３つの類型を構築して，それらに異なる法的な効果を与える．

すなわち，

①個人識別（済）情報(identified data)―個人がすでに識別されている情報（ただし，姓名が直接特定されるものだけではなく，明らかにある特定個人を示すような情報もこれに含まれるとする）

②個人識別可能情報(identifiable data)―スペクトルの中心部分にあり，個人識別が遠い可能性に過ぎないとまではいえない情報，要するに，個人識別が比較的現実的な可能性のある情報をさす．

③個人識別困難情報(non-identifiable data)―個人識別が遠い可能性としか考えられない情報．このような情報は，個人識別技術との関連では，実際上，個人識別ができない情報である．

これらの間の境界は，それぞれの場面ごとに異なり，技術の発展によって変化しうる．この３分類は柔軟な概念であり，画一的ルールではなく，柔軟な基準である．その曖昧さを非難する者もいるだろうが，むしろ現実的でプラグマテッィクな利点と見るべきである．

まず個人識別済情報が何を意味するかについては，一般的に国際的な合意がある．何しろ，個人に直接リンクする情報は，個人情報だというのであるから．アメリカでもEUでもこれについて異論はない．なお，EUでは，この中で一定の情報をセンシティブ・データであるとして，もっと強い規制を要求する．この点は，新たな規則案でも変わらない．バージョン２でも，このような取扱いはなされる．

問題は，スペクトラムの中心にあるさまざまな情報と組み合わせると個人識別ができる情報である．EUでは，これに個人識別済情報と同じ法的効果を持たせる．

しかし，バージョン２における個人識別可能情報については，識別可能であるとしても，識別の蓋然性は高度といえない場合は異なる扱いをする．個人に対するリスクは中程度から低度である．それらへの法的対応は，個人識別済情報と異なってしかるべきである．例としては，医療情報に特別なコードを付けたものや，Kuner氏のいうオペラ好きの医師の例がある．後者は，この問題の専門家であるEUのChristopher Kuner氏があげているものであり[12]，データ管理者でなくとも，

[12] Christopher Kuner, European Data

次のような例では誰かが個人を同定できる可能性があるので個人情報だという．

「X 市在住の 50 歳以上の男性のうち，医師で 2 人の娘がおり，ヴェルディのオペラが好きで，ウランス南部に別荘がある人」

データ管理者自身は合理的な手段で，これが誰かがわからないとしても，やはり誰かしらは，わかる人がいると思われるので，個人識別情報だという．つまり EU では，実際には個人識別はしていないものでも個人識別済情報として扱うわけである．

その結果，個人情報保護原則の中の，情報の正確性や最新性の確保義務を考えると，データ管理者（事業者）にこれも個人情報だとして，そのような義務を課すことになる．言い換えれば，データ管理者に，必要もないのに他の情報までわざわざ集めさせて，この人を特定させることになる．そうでなければ情報内容の正確性は維持できないからである．わざわざ事業者に不要なコストをかけさせて，個人を特定させ（個人特定済情報に変換させて），リスクを高めることになる．それは明らかに誤っており，逆に，この類型の情報については，正確性や最新性確保義務をないことにすれば，データ管理者（事業者）は，個人を特定しない範囲で利用することにするインセンティブを与えることになる．それこそが合理的な個人情報保護の仕組みである．要するに，個人識別可能情報に過ぎないとして，データ管理者に安全管理措置さえしっかりさせておけばよい．

なお，アメリカでは，2012 年の FTC レポートにおいて[13]，個人にリンクさせることが合理的に見て生ずる場合を想定した検討を行い，その中で Schwartz 教授らの提案を引用している．そこでも，リンクするリスクを最小にする措置を行えば，それは個人識別情報にならない旨の提言がなされている．そこでは，個人識別可能情報を，必要性がない限り，個人情報（個人識別済情報）にしないためのインセンティブを与える工夫が提言されており，第三者に移転する場合でも，個人識別をしないよう契約に盛り込むことなどが提言されている．

最後に，個人識別困難情報については，実際に個人にリンクする可能性はきわめて低い．たとえば，サンプル量が多い場合，合衆国民とか日本国民全体がどれだけ通信を利用しているか

Protection Law: Corporate Compliance and Regulation 92 (Oxford Univ Pr on Demand; 2 版, 2007/4/9).

[13] FTC Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

というような情報はこれにあたる．これらについては，個人情報ではないとして扱ってよい．

【バージョン２の 3 分類と法的効果の対応】

先に述べたように，上記3分類と，公正な情報取扱指針（FIPs, Fair Information Practices）の適用関係が対応する．FIPs とは，繰り返し掲げると，以下の７つだった．

①情報の利用の限定

②情報取得の限定

③個人情報開示の限定

④情報に関する正確性，適切関連性，最新性の原則（情報の質確保の原則）

⑤個人に対し認められる，通知，アクセス，訂正の権利

⑥個人情報取扱・処理に関する透明性の原則（自分の情報がいかに取り扱われているかを知ることができるという原則）

⑦個人情報の安全性の原則（漏洩防止措置）

まず，個人識別済情報については，これら 7 つの原則がすべて適用される．

次に，個人識別可能情報については，７つではなく，いくつかの原則の適用にとどまる．ただし，その場合でも，④，⑥，⑦については適用される．⑤を入れていないのは，これを入れると，個人識別可能情報について，すべて他の情報を集めて，いったん個人を識別して通知せざるを得なくなり，逆に，個人情報保護のリスクを高めること，企業に不要なコストをかける結果になることによる．EU の新たな規則案第 10 条でも，さらに情報を集める必要がないと記してあるのは，同趣旨に解することができる．

また，①から③が適用されないのは，個人に対するリスクに対し，過剰なコストを負わせるからである．さらに社会的に有用な利用法も制限する結果になる．たとえば，グーグルのインフルエンザ予想システムや，医師の質評価などの医学研究調査などは，まさにその例となる．さらに医学研究では，現在は，個人の症例からではなく，ビッグ・データから何らかの新たな発見が期待されるような研究が主流になりつつあり，その場合，取得目的が最初に予測できないという性格を有する．このような医療関係のサービス向上や研究発展を考えると，個人識別の可能性・必要性の低さに対し，①から③の原則適用は，ベネフィットに対しコストを過剰にして，それを阻害する．

ただし，個人識別可能情報についても，④（データの質の維持と向上という意味），⑤（透明性），⑥（データ管理の安全性確保）は当然適用され

る．このうち透明性は，何が行われているかを，白日の下に置くこと，それによって当該利用法の乱用防止につながり，またその意義の社会的理解も深まる点がある．⑥については，データ取扱いのシステムの質を維持し向上させるためにも必要である．また，ここでは，個人識別可能情報に付随する義務は（それが個人識別済情報に変わりうるものであるため），いわばこれらの情報に随伴してどこまでも続く性格のものであり，track and audit のシステムを構築しておく必要がある．

最後に，個人識別困難情報については，原則として上記の義務はいずれも課されないことになる．

このような発想が EU に受け入れられるかといえば，難しいと考えられる．この 3 分類は技術の進展にも適合するような柔軟な分類であるから，うまく利用すれば，個人情報保護と情報の利活用のバランスをとるための基礎的な考え方の枠組みとして機能しうる．だが，その柔軟性が，概念規定の正確さや細かさを重視する EU の法的考え方に合わないだろう．実質的に，個人情報の範囲を大きく縮減する点も，EU におけるこれまでの考え方と適合しない．

【日本の方向性】

このような中で，日本の方向性を探ることは容易ではない．

日本では，EU の 1995 年個人情報保護指令も視野に入れて，2003 年に個人情報保護法を制定した．だが，法的対応自体が一種「過剰反応」の状況を呈し，また細分化して物事をとらえる国柄が悪く出て，民間部門に対する個人情報保護法，独立行政法人に対する個人情報保護法，公的機関に対する個人情報保護法，さらにはあらゆる地方自治体のレベルで個人情報保護条例が制定されて，1000 以上の法令が割拠する状況となった．

EU 加盟 27 カ国の間で，細かな規定に差異があるどころの話ではない．しかも，これだけ熱心な法制化をしたにもかかわらず，EU からは「不適格」，すなわち「適切な」個人情報保護制度がないという烙印を押される結果となっている（そして，もしもそれが政策遂行の失敗を意味するのであれば，誰かに責任があるはずだが，それに対して誰も責任をとっていない）．

憶測を交えて記せば，どこか EU から見て不適切かというと，それは次の 3 点である．

①全国に 1 つのデータ保護庁を設置していないこと．

②データ主体（つまり国民の 1 人ひとり）に，個人情報に関する基本的な権利を認めていない（ように見える）

こと．個人情報保護法は，個人情報取扱事業者の義務として，開示請求や訂正請求に対処する義務を明記したが，個人の権利として明記していない．

③制裁または救済の点でも生ぬるい．個人情報保護法では最後の最後に罰則という規定になっており，その文面だけを見れば，実効性のないものに見える．

これらは，わが国に住んでいて，個人情報保護法の 2005 年施行以来の「過剰反応」ぶりを知っている人たちからは「誤解」としかいいようがない．これほど個人情報の漏洩を気にし，まれに漏洩があれば大事件としてメディア等で社会問題となる国が，世界にどれだけあるのかと思うが，日本の状況への理解が十分でないのは，世界への発進力のなさの証左であり，むしろ他を批判するよりわが身を省みる方がよいかもしれない[14]．

その日本国において，2013 年 6 月 14 日「世界最先端 IT 国家創造宣言について」なる閣議決定がなされた．そしてその中で，次のような項目が明記された[15]．

「オープンデータやビッグデータの利活用を推進するためのデータ利活用環境整備を行うため，IT 総合戦略本部の下に，新たな検討組織を速やかに設置し，データの活用と個人情報及びプライバシーの保護との両立に配慮したデータ利活用ルールの策定等を年内できるだけ早期に進めるとともに，監視・監督，苦情・紛争処理機能を有する第三者機関の設置を含む，新たな法的措置も視野に入れた制度見直し方針を年内に策定する」．（傍線は筆者）

その結果，IT 総合戦略本部の下にパーソナルデータに関する検討会が設置され，個人情報保護法の見直しも行われている[16]．

契機となったのは，成長戦略の柱としての IT 戦略であり IT 利用の促進という政策判断であるから，明らかに個人情報を含むさまざまな情報の利活用を図るところにある．他方で，わが国において個人情報保護の重要性が減少したということはないのであるから，どのような形で，個人情報保護法の再検討を図るか，さらにセンシティブ情報について個別法を制定する

[14] ただし，日本の個人情報保護法制度が EU から「不適格」と判断された後でも，日本と EU との取引が目に見えて減少したという話は聞かない．日本企業は，EU とアメリカとの交渉の中で出てきた 3 方式のうち，モデル契約約款を契約条項として採用するなどの方法で対処し，現実に大きな政治的経済的問題になっていないとすれば，今回の EU 規則案にも「過剰反応」すべきでないという判断もありうる．

[15] http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou1.pdf

[16] http://www.kantei.go.jp/jp/singi/it2/pd/

のかというような課題がただちに想起される.

しかも,情報化が国際化と密接に結びついている現在(つまり情報は容易に国境を越える性格を有する),本稿で記したような個人情報保護法制について,アメリカ型とEU型との対立,あるいは2つのモデルの相違は,わが国の今後の方向性を考える上でも無関係とはいえない.同時にせっかく個人情報保護法を制定しながら,EUからは理解されていないという状況も改善すべき好機である.

最後に,以上のような認識のもとに,日本法の方向性について私見を提示し,本稿の結びとする.

①現在の個人情報保護法は,第1条で「個人情報の有用性に配慮しつつ,個人の権利利益を保護することを目的とする」と謳ったが,2005年以降の実際は,個人情報の有用性を生かした利活用が阻害される場面が多かった.まさに「個人情報保護」法という名称によって,多くの人が「それは個人情報だから」という「言い訳」として活用してしまったのである.今回,経済再生戦略の柱としての情報法制度の見直しが図られるのは,本来の「個人情報活用および保護法」制定の好機である.

②EU型とアメリカ型とを比べると,日本の法制度や法意識は,どちらかといえばEU型に近い.法がない限り自由な情報利用を原則とするアメリカ法ではなく,個人情報について基本的な権利とするか否かはともかく(そもそも基本権という意味の検討が必要となる),法的根拠があって始めて情報利用ができるという,本来,この分野において公的規制があるべきだとするEU型が多数派だと考えられる.

③そうだとすると,EU規則案が実際に制定されることを踏まえて,新設された特定個人情報保護委員会をEUでいうデータ保護庁と位置づけ,個人情報に関する国民の権利を宣言し,それが侵害された場合の救済とそのための手続きも明記し,EU基準でも「適切な」ものとするのが望ましい.

④だが,他方で,正当な情報の利活用を阻害しないよう,適切な利用法を明確に定めることと,新たな情報利用についても,特定個人情報保護委員会(第三者機関)またはそこから委託された機関に申請すれば迅速に許可が出されるような仕組みを設けることが考えられる.

⑤何が個人情報であるかは,この分野の最も基本的な課題であり,技術的な進歩を踏まえれば,容易に答えが見つからない難問である.アメリカの学者によるバージョン2という発想には見るべきものがあるが,わが国では基本的に従来もEU型の定義が行われてきたわけであるから,バージョン2的な定義やそれよりさらに狭いアメ

リカ型の定義は採用が難しい. そうだとすると, EU 型の定義を採用しつつ, 事業者に合理的な匿名化の努力をするインセンティブを与えるような工夫がなされてしかるべきである. 他の情報とリンクする可能性はあるが蓋然性は少ないような個人識別可能情報については, 個人識別をしないでそれを安全に管理する事業者に, 一定の免責を認めるような仕組みは, 参考に値する.

厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）
分担研究報告書

スウェーデンの患者データの利活用に関する法制度

研究分担者　井上　悠輔　東京大学医科学研究所　助教

研究要旨

スウェーデンにおける患者データの統合，医療評価や研究活動への患者データの集合的活用を支える法制度として，患者データ法，保健データレジストリ法，研究レジストリ法その他の関連法規を検討した．スウェーデンでは，全例収載の法定レジストリ事業の長い歴史があり，医療法においてもデータを用いた医療の質の評価の重要性が明示されているなど，広範な患者データの活用の利点が認識されている．同国の基本法の理念としても，公的機関において蓄積された記録・情報の処分や用途限定は最小限に控えられており，また EU の個人データ保護指令への対応においても，指令が含む同意要件の適用除外や例外規定を医療活動に積極的に適用してきた．一方，個人のインテグリティの保護に取り組むデータ監査院の活動と医療当局との見解の相違や連携不足がたびたび問題になっている．患者データ法は，従来の守秘義務を再編し，公営医療圏など，各地の医療体制単位での患者データの管理責任を高めた．また，医療体制間の情報共有の手続きを明確化することで，国内での患者データの共有を制度的に支援するねらいもある．一方，複雑な規定の解釈が医療者や個人に十分に示されず，個人データの共有に関する当局や地域間の解釈の相違，統合作業に関する技術的な障壁なども指摘されている．またレジストリ事業については，欧州連合において検討されている個人データ保護規則の内容や解釈次第では，これまでの「柔軟な」法解釈に影響が出ることが予想されている．

A．研究目的

スウェーデンにおける個々人の患者データの処理，および医療評価や研究活動への患者データの集合的活用に関連する法制度として，患者データ法，保健データレジストリ法，そして研究レジストリ法を検討し，特にこれらの情報・データの収載をめぐる課題について検討する．

B．研究方法

法律および関連行政文書，関連する文

献を収集し，検討した．なお，検討した主たる法規の一覧は文末の「参考１」に示した．

（倫理面への配慮）

公知の資料を用いた．倫理的な観点からの配慮を要する情報は用いていない．

C．研究結果

以下，「1　現体制の概況」において個人データ法などの背景を整理したうえで，「2　保健データレジストリ法」「3　患者データ法」「4　研究レジストリ法」を検討し，考察，結論を述べる．また，本文の関連個所について関連法一覧（参考1），保健データレジストリ法にもとづく法定レジストリに収載されるデータの内容（参考2），患者データ法の概要（参考3），研究レジストリ法の仮訳（参考4）を掲載した．

1　現体制の概況

スウェーデンにおける患者データの活用は，患者データの統合と，一方でレジストリを通じた患者の集合的データの医療評価や研究への活用という二つの側面から注目できる．スウェーデンにおける日常的な医療個人情報の取扱いを規定する法律としては，個人データ法と患者データ法が基本であり，とりわけ後者は，前者を一般法とする（それゆえこれに対する例外や追加規定を示す）特別法として機能している．また，本稿では，スウェーデンの全例レジストリの根拠となっている保健データレジストリ法（SFS1998:543），研究機関におけるレジストリ運営が論点となっている研究レジストリ法（以下同 2013:794）についても触れる．この他，関連する法律には，アーカイブ法（1990:782），統計法（2001:99），司法精神医学研究レジストリ法（1999:353），情報公開・秘密法（2009:400），患者安全法（2010:659）などがあるが，これらの検討はこの調査の趣旨と紙数の関係から最低限にとどめる．

個人データ法（PUL）

現行の個人データ保護法（1998:204）は，EU データ保護指令（1995/46/EC）に対応して 1998 年に施行された．スウェーデンには個人情報を保護する世界で初めての包括的な国内法規としてデータ法（Datalag，同 1973:289）があったが，個人データ法はこれに置き換わるものであった（暫定規定について 2001 年まで効力を残した）．

個人データに関する規制はこの個人データ法が基本となるが，この法律の適用は「憲法上の表現や出版に関する自由，公的情報へのアクセスを制限する規定に反しない範囲に限られることを理解する必要がある」[1]．スウェーデン憲法

[1] Rynning, E (2005). Processing of personal data in Swedish health care and biomedical research, 381-402, Implementation of the Data Protection Directive in relation to medical research