欧州におけるプライバシー保護に係る研究開発および法制度の動向

平成 28 年 3 月

国立研究開発法人　情報通信研究機構

（欧州連携センター）

目次

はじめに

本報告書では、欧州におけるプライバシー保護に係る研究開発および法制度事情について記す。国立研究開発法人 情報通信研究機構（以下、NICT とする）は、未来志向型研究ファンド「パーソナルデータ利活用におけるプライバシー問題の解決に関する研究」に取り組んでいるが、人権意識が伝統的に高い欧州では、プライバシー保護について、世界の他地域に比べて盛んに検討されており、日本での取り組みの参考になる、

調査は、1) プライバシー保護技術の研究開発活動に対する助成への EU の基本的方針、2) EU の研究開発助成計画である第七次枠組計画およびホライゾン 2020 下におけるプライバシー保護技術に係る研究プロジェクトの事例（FP7 PRIPARE プロジェクト、FP7 PARIS プロジェクト、FP7 PRACTICE プロジェクト）、3) EU パーソナルデータ保護法の改正を巡る動向（改正の審議状況、日本に与える影響等）という 3 事項を含む。

調査方法

本調査では、インターネット及び公刊物、報道記事等を精査するとともに、インタビュー調査、そして、イベント視察調査を行った。

EU のプライバシー保護技術に係る研究プロジェクトの事例に関しては、FP7 PRIPARE プロジェクトに参加したスペインのマドリード工科大学にインタビュー調査を実施した。また、2016 年 1 月末にベルギーのブリュッセルで開催された CPDP2016[1]を視察し、FP7 PARIS プロジェクトと EU パーソナルデータ保護法の改正を巡る動向について情報を収集した。最後に、2015 年 11 月に、フランスのリヨン市で開催された「諸文化を通じたプライバシー – グローバル化した世界における一致点と相違点–」と、2016 年 1 月に同国パリ市で開催された「国際条約と協定におけるパーソナルデータ」を視察した際のレポートを本報告書末に収録する。

なお、本報告書では、情報を入手したウェブサイトの URL を参考のため注に載せているが、これらの記事はウェブサイト管理運営者の判断で随時移動、修正、削除される可能性がある。従って、本報告書の発表後、注に記された URL から情報源となった記事にアクセスできないことがありうることを、ここで前もって注記しておきたい。

[1] http://www.cpdpconferences.org
CPDP は、毎年ベルギーのブリュッセルで開催されるプライバシー保護に係る研究開発と法制度については討議する総合的イベントである。

要約

欧州連合のプライバシー保護技術の研究開発活動に対する助成への基本的方針と EU 研究プロジェクト事例

- ホライゾン 2020 では、2016 年からデジタルセキュリティの公募枠は、ICT 部門からセキュリティ部門に移行している。
- ホライゾン 2020 セキュリティ部門 2016 年～2017 年度作業プログラムでは、デジタルセキュリティの研究テーマは 8 つに分かれ、技術開発だけでなく、社会・経済学的視点からの研究や国際的対話を進める活動にも助成される。助成総額は、1 億 1800 万ユーロの予定である。
- 国際的対話を促進する活動に助成する『サイバーセキュリティとプライバシーの研究と技術革新における EU との提携と国際的対話』では、日本とアメリカが国際的対話の相手国として定められている。そのため、今後、欧州の組織が日本の組織へ、交流、提携のため、積極的に働きかける可能性がある。
- PRIPARE プロジェクトには、11 組織が参加し、全予算が 131 万ユーロである（研究期間：2013 年 10 月～2015 年 9 月）。同プロジェクトは、産業界における将来的なプライバシー・バイ・デザインの採用を準備するために、プライバシー・バイ・デザインの方法論の開発、トレーニングの実施、教材の作成、欧州委員会等への勧告を行っている。
- PARIS プロジェクトには、8 組織が参加し、全予算が 477 万ユーロである（研究期間：2013 年 1 月～2015 年 12 月）。監視システムや生物計測システムの研究開発に、プライバシー・バイ・デザインを採用する方法論を開発する。
- PRACTICE プロジェクトは、18 組織が参加し、全予算が 1046 万ユーロである（研究期間：2013 年 11 月～2016 年 10 月）。クラウドシステム全体において、データの機密性を保持するため、暗号化されたデータのコンピューテーションを実現する柔軟なアーキテクチャとツールを開発する。

EU パーソナルデータ保護法改正について

- 欧州委員会によって、2012 年に EU パーソナルデータ保護指令改正案が提案されて以来、同案は欧州議会及び欧州連合理事会で審議され、修正が重ねられてきた。だが、2015 年 12 月、欧州委員会を合わせた三機関による 6 か月間の三者協議の末、改正案について欧州議会及び閣僚理事会が最終的な合意に至っている。この結果、2016 年内に改正案は採択される見込みであり、法案採択の 2 年後には、改正法は各国で適用される予定である。
- データ保護法改正パッケージは、一般データ保護規則とデータ保護指令の二つの EU 法からなる。
  - EU 市民のデータの利用とプライバシーに係る一般データ保護規則
  - 法執行機関による EU 市民のデータの利用に係るデータ保護指令
- 一般データ保護規則は、ユーザが自分自身のデータをよりコントロールすることを可能にする権利を強化するとともに（自分自身のデータへより簡単にアクセスすることを保証する権利、忘れられる権利、データポータビリティの権利、いつ自分の

データがハッキングされたか知る権利、罰金の増額など)、EU 経済成長を促進する（EU 内で法制度を統一、ワンストップショップアプローチの採用、中小企業の優遇)とされている。また、以上に加えて、設計と初期設定によるデータプロテクションの採用義務が定められている。だが、パーソナルデータ保護法は、基本権や個人の権利の遵守を改善したが、データを利用するビジネスモデルの発展を妨げ、EU の経済成長を促進しないのではないかという批判もされている。

- EU パーソナルデータ保護指令の改正は日本の組織へも影響する。特に、改正案は、同法が EU 域外へも適用されることを定めており、EU 域外に事業者を持つ企業でも、EU 居住者のデータを取り扱う事業者に対して同法が適用される場合がある（EU 居住者に商品やサービスを提供する場合と EU 居住者の行動をモニターする場合)。したがって、日本の組織は、知らずに EU パーソナルデータ保護法に違反することがないように、同法に対応する必要がある。

General Summery

This is a general summary of the "Report on the R&D and the legal system of privacy protection in Europe". See the text of the report for more information.

EU basic policy on the funding for the R&D of privacy protection technologies and examples of EU research project

- Since 2016, Horizon 2020 ahs called for the proposals on digital security in its Security section (until 2015 in its ICT section).
- The 2016-2017 work Programme of the Security section in Horizon 2020 proposes 8 topics concerning digital security. This programme does not only assists the technological innovation, but also sociological and economic research as well as the activities promoting international dialogue. It will allocate a total of €118 million.
- In the "EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation" topic, concerning the activities promoting the international dialogue, Japan and USA are considered as the partners of this international cooperation. So, the European organizations might work on the Japanese organizations actively for exchange and cooperation.
- The PRIPARE project consists of 11 organizations and its total budget amounts to €1, 31 million (the project duration: from October 2013 to September 2015). This project prepares the future application of the Privacy and security by design in industry. To this end, it developed the Privacy by design methodology, organized training workshops, provided educational material and made recommendations to the European Commission.
- The PARIS project consists of 8 organizations and its project cost amounts to €4, 77 million (the project duration: from January 2013 to December 2015). It developed the Privacy by design methodology for the R&D on the surveillance and biometric system.
- The PRACTICE project consists of 18 organizations and its project cost amounts to €10, 46 million (the project duration: from November 2013 to October 2015). The PRACTICE project develops a flexible architecture and tools which realize the computation on encrypted data for data confidentiality in cloud computing.

EU Data protection reform

- The European Parliament and the Council of the European Union have repeatedly deliberated and amended the EU Data Protection rules reform Proposal proposed in 2012 by the European Commission. In December 2016, the European Parliament and the Council of the European Union reached the agreement on the new data protection rules, after 6 months of the "trilogue negotiations" between three institutions namely, the European Parliament, the Council of the European Union and the European Commission. The new rules will be adopted within the year 2016 and implemented in EU member states two years thereafter.
- The Data Protection Reform package consists of two legislative instruments: a General Data Protection Regulation and a Data Protection Directive. The Regulation covers the protection and free

movement of data in the European Union more broadly. The Directive deals with the processing of personal data by law enforcement authorities.

- The General Data Protection Regulation strengthens the right for citizens to better control their personal data (easier access to their own data, the right to data portability, the right to be forgotten, the right to know when their data has been hacked, raise of the penalty), and stimulates the EU's economic growth (unification of the European rules, adoption of "one-stop-shop" approach, benefits for SMEs). It also specifies the obligation to adopt Data Protection by design. The Data Protection Reform certainly achieves the fundamental right consolidation. However, it is criticized for disturbing the development of business model which uses data as well as for not stimulating the EU economic growth.
- The EU Data Protection rules Reform will have an impact on Japanese organizations. Especially, the new regulation specifies that the EU Data Protection rules are applied outside of Europe. The regulation will apply to companies based outside of Europe if they offer their services to the EU residents or if they monitor the behaviours of EU residents. So, the Japanese organizations will have to recognize the new Data Protection Regulation for not violating it.

第一部　欧州連合におけるプライバシー保護技術の研究開発の動向

欧州では、プラバイシー、そして、パーソナルデータ保護への関心が高く、欧州人権条約第8条と欧州連合基本権憲章の第7条はプライバシーの保護を、欧州連合基本権憲章の第8条はパーソナルデータ保護を基本権の一つとして定めている。そして、パーソナルデータの保護に関しては、個別の法として、1995年にパーソナルデータ保護指令が策定され、2012年に同法の改正案が提案され、4年間の審議を経て、2016年内に改正される予定である[2]。以上のようなプライバシーとパーソナルデータ保護への関心と法制度は、欧州連合（以下、EUとする）による研究開発助成制度である第7次枠組計画（期間：2007年～2013年）とホライゾン2020（期間：2014年～2020年）にも反映されている。第一部では、EUのプライバシー及びパーソナルデータ保護技術の研究開発助成の基本的方針と研究事例について記す。

第一章 欧州連合のプライバシー保護技術の研究開発活動に対する助成への基本的方針

第7次枠組計画（以下、FP7とする）及びホライゾン2020のICT部門2014年 - 2015年度作業プログラムでは、情報セキュリティ分野の研究プロジェクトは、ICT部門で公募されていた。だが、2016年 - 2017年度作業プログラムから、同分野の公募枠はICT部門からセキュリティ部門に移され、情報セキュリティ技術は他のセキュリティ技術（自然災害やテロ対策技術など）と同じ部門で助成されることになった。

ホライゾン2020 セキュリティ部門2016年～2017年度作業プログラム[3]のデジタルセキュリティに焦点を当てた公募枠では、研究テーマは8つに分かれ、技術開発だけでなく、社会・経済学的視点からの研究や国際的対話を進める活動にも助成される。助成総額は、1億1800万ユーロの予定である。

研究テーマと予算

テーマ	予算額
信用可能で安全なICTシステム・サービス・部品のための保証と認証	2350万ユーロ
中小企業、地方公共団体、個人向けのサイバーセキュリティ	2200万ユーロ
システムレベルでのデータに関連するヘルスデジタルセキュリテイの増大	1100万ユーロ
サイバーセキュリティの経済学	400万ユーロ
サイバーセキュリティとプライバシーの研究と技術革新におけるEUとの提携と国際的対話	300万ユーロ
暗号学	1850万ユーロ
先端サイバーセキュリティの脅威と脅威の要因への対策	1800万ユーロ
プライバシー、データ保護、デジタルアイデンティティー	1800万ユーロ
合計	1億1800万ユーロ

[2] 正式名称：「パーソナルデータの取り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指令」1995年成立。

[3] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

なお、助成トピックの一つである『サイバーセキュリティとプライバシーの研究と技術革新における EU との提携と国際的対話』[4]では、日本とアメリカが国際的対話のパートナーとして定められている。サイバーセキュリティ分野とプライバシー保護分野で、日本とアメリカの組織との交流、対話、共同研究開発、国際提携などを促進する活動について助成される予定であり、今後、欧州の組織が日本の組織へ、交流、提携のため、積極的に働きかける可能性がある。

以上のほか、ホライゾン 2020 ICT 部門 2016 年～2017 年度作業プログラムから情報セキュリティの公募枠がなくなったものの、クラウドコンピューティングやビッグデータ、将来インターネットなどの公募枠では、開発の際にプライバシーを考慮することが促されており、関心の高さが伺える。

第二章　欧州連合のプライバシー保護技術に係る研究プロジェクトの動向

以下に、EU のプライバシー保護技術に係る研究プロジェクトの事例として、FP7 で助成されている PRIPARE プロジェクト、PARIS プロジェクト、PRACTICE プロジェクトについて記す[5]。

第一節　FP7 PRIPARE プロジェクト

PRIPARE プロジェクトには、11 組織が参加し、全予算が 131 万ユーロである（研究期間：2013 年 10 月～2015 年 9 月）。同プロジェクトは、産業界での将来的なプライバシー・バイ・デザインの実施を準備するために、プライバシー・バイ・デザインの方法論の開発、トレーニングの実施、教材の作成、欧州委員会等への勧告を行っている。

1) FP7 PRIPARE プロジェクトの基本概要

プロジェクト名略称	PRIPARE
正式名称	研究におけるプライバシー・バイ・デザインの適用を支援することによる産業の準備
分野	ICT-2013.1.5
プロジェクト期間	2013 年 10 月～2015 年 9 月（24 ヶ月）
予算（EU 拠出分）	131 万ユーロ（109 万ユーロ）
コーディネーター	トリアログ（仏）
参加者	フラウンフォーファー協会（独）、INRIA（仏）、ウォーターフォード技術研究院（アイルランド）、KU ルーヴァン（ベルギー）、マドリッド工科大学（スペイン）、ウルム大学（独）、パリ・アメリカ大学（仏）、トリラテラル リサーチ&コンサルティング（英）、ガリシア電気通信技術センター（スペイン）、アトス（スペイン）
ウェブサイト	http://pripareproject.eu http://cordis.europa.eu/project/rcn/110590_en.html

[4] http://www.gppq.fct.pt/h2020/call.php?id=H2020-DS-2016-3&topic=DS-05-2016

[5] PRIPARE プロジェクトと PRACTICE プロジェクトについては、NICT 欧州連携センターの 2015 年 2 月発表『欧州におけるプライバシー保護技術に係る研究開発の最新動向調査』第一部第二章と第三章も参考のこと。
http://www.nict.go.jp/int_affairs/int/4otfsk000000osbq-att/a1431327954528.pdf

1) ヒアリング調査レポート: マドリッド工科大学（UPM）/ FP7 PRIPARE プロジェクト

PRIPARE プロジェクトについて、同プロジェクトに参加しているマドリッド工科大学へインタビュー調査を実施した。以下に、その概要を記す。

インタビュー調査の概要

- 日程 : 2016 年 1 月 25 日（木）午前 11 時～
- 場所 : NICT 欧州連携センター（フランス・パリ）[6]
- 先方 : マドリッド工科大学テレマティクスシステム工学部 リアルタイムシステム・テレマティックスサービスアーキテクチャ研究グループ　研究者 3 名[7]

先方の研究組織について

- 1971 年に創立されたマドリッド工科大学（以下、UPM とする）は、スペイン最大の技術系大学である（人員数 : 4 万 3000 名の学生、3600 名の教育・研究スタッフ、2000 名の事務及び技術スタッフ）
- UPM は、欧州の研究開発で積極的な役割を果たしており、EU の第四次枠組計画（1994 年以来）から、スペインの公的機関の中で最も多く EU と研究契約を締結している。
- UPM はスペインの IT 国際企業の多くの創業に関わっている。
- 研究活動の収入は 7000 万ユーロである（国内外プロジェクト及びスペイン企業・国際企業との契約）。
- FP7 PRIPARE プロジェクトへは、UPM のテレマティクスシステム工学部（以下、UPM DIT とする）が参加している。テレマティックスという言葉の意味は、英語とスペイン語では異なり、スペイン語ではコンピュータネットワーク・ソフトウェアサービスという意味であり、英語の意味よりも広い（英語では、自動車などの移動体への情報通信システムの利用を意味する）。
- 1987 年に創立された UPM DIT は、スペインにおいて、テレマティクス分野で最大の大学研究ユニットである（常勤 90 名 : 教授 13 名、准教授 28 名を含む。その他、博士課程の学生、研究アシスタントなど）。学生は約 1500 名である。
- UPM DIT は、基礎研究（科学的という意味で）と応用研究（イノベーションに関わるという意味で）の両方を実施している。
- UPM DIT は様々な研究を実施している。研究トピックは、コンピュータネットワークと通信、将来インターネット、情報システムとデータベース、組み込みシステム、テレマティクスサービスとアーキテクチャ、インテリジェントシステムである。
- これらの研究活動の他に、UPM DIT のスタッフは国際コンソーシアムやワーキンググループ、国際カンファレンスのプログラム委員会、国際イベントの開催などに携わっている。
- UPM DIT から FP7 PRIPARE プロジェクトには、ホゼ・M・デル・アラモ准教授、ホアン・カルロス・エルモ准教授、ヨド・サミュエル・マルチン研究者の 3 名が参加している。
- 同 3 名は、「リアルタイムシステム・テレマティックスサービスアーキテクチャ研究グループ」に属している。同研究グループには全部で 16 名が属している。
- 同研究グループは、現在、技術的な観点からプライバシー工学をテーマにしており、特にプライバシー・デジタルアイデンティティ管理に焦点を置いて研究をしている。暗号などの数学的観点からデジタルセキュリティの研究は実施していない。

[6] スカイプを利用し、テレビ電話によるインタビュー調査を実施した。
[7] ホゼ・M・デル・アラモ准教授、ホアン・カルロス・エルモ准教授、ヨド・サミュエル・マルチン研究者

- われわれはプライバシー工学を民間企業に技術移転する活動を行うとともに、国内外プロジェクトを実施している。
- 同3名は、複数の公的研究助成及び民間研究助成による研究開発プロジェクト（国内及び欧州プロジェクト）に参加している。
- 参加プロジェクト事例 （PRIPARE プロジェクト以外）:
  - TRANSF-ID : 特殊鉄道におけるセキュリティ向けプラットフォーム（民間研究助成）
  - ITECBAN : 銀行向けの技術的及び方法論的インフラストラクチャ（スペイン政府の研究助成）
  - OPUCE : ユーザ中心サービスの創造と実行向けのオープンプラットフォーム（FP6）
  - SEGUR@ : 情報社会におけるセキュリティとトラスト（スペイン政府の研究助成）
  - OMELETTE : 電気通信分野におけるリンクドデータ向けのオープンマッシュアップ企業サービスプラットフォーム（FP7）
  - MOET : イベント指向ミドルウェア（民間研究助成）
  - POSDATA : パーソナル・ソーシャルデータ分析（民間研究助成）
  - FREIGHTURE : 貨物運送向けの TRACK と TRACE システム（ドイツ鉄道と共同）
- これらのプロジェクトの成果は、テレコム分野（テレフォニカ、エリクソン、Everis NTT）、銀行・金融分野（サンタンデール銀行）、ソーシャルネットワーク分野（ボーダフォンのワンソーシャルウェブ、ツイッター）、運送分野（Transfesa、ドイツ鉄道）で応用されている。
- 研究グループの主な研究トピックは2つある。

1) パーソナルデータ・アイデンディティ・プライバシー管理
   - パーソナルデータ開示と忘れられる権利
   - ユーザ中心のパーソナルデータ管理向けユーザモデリングと枠組み
   - プライバシー・バイ・デザインとプライバシー・バイ・デフォルトのようなアプローチを利用するソフトウェアとシステム工学方法論へのプライバシー要件の実践的導入
   - プライバシー要件の工学（法的・ユーザ要件を含む）
   - 設計パターンとアーキテクチャのような設計にかかわる側面
   - プライバシー属性のアセスメントと保証
2) ソフトウェアとサービス工学
   - サービス指向及びイベントドリブンアーキテクチャ
   - 学際的パースペクティブから理解された非機能的アーキテクチャとサービス要件（アクセシビリティ、ユーザビリティなど）

- これらの研究は、ビッグデータやクラウドコンピューティング、IoT など、特定の分野に応用される。

FP7 PRIPARE プロジェクトについて

- われわれは、PRIPARE プロジェクトにおいて、プライバシー工学の方法論的側面に焦点を置き、研究を実施するとともに、プラクショナー向け（practitioner）の教育教材を開発した。また、われわれは研究成果の普及活動をトレーニングワークショップやカンファレンスなどで実施した。
- PRIPARE プロジェクトは、産業界の経験の少ない技術者がシステム構築の当初から、システムをプライバシー・フレンドリィに開発できるように、プライバシー・バイ・デザ

イン導入のための方法論を定義した[8]。プライバシー・バイ・デザインは抽象的なコンセプトなので、実際に適用できるように方法論を開発する必要がある。

- PRIPARE プロジェクトは、いわゆる新しい研究開発を実施するプロジェクトではなく、コーディネート支援アクションという枠組みで助成されている。だが、同プロジェクトは、方法論を開発するために、プライバシーとセキュリティ保護にかかる既存の仕組みやアプローチ（プライバシー影響評価、リスク管理など）をホーリスティックで一貫性のある仕方で融合させた。例えば、OASIS のプライバシー管理参照モデル（PMRM[9]）は PRIPARE の出発点にある。

- PRIPARE プロジェクトでは、ソフトウェアとシステム工学の開発プロセスモデルの諸段階（分析、設計、実施など）に適合する 24 のプロセスを、プライバシー・バイ・デザインを実現する方法論として定義した。
- PRIPARE の方法論は、非常に一般的なもので、どんな技術の開発にも当てはまる。だが、実際にこの方法論を利用するには、例えば、クラウドコンピューティングやビッグデータ、IoT などのトピックに合わせて、その技術開発に固有の側面を考慮しなければならない。現在、われわれは PRIPARE で開発した方法論を特定の技術へ適用する研究を実施している。
- PRIPARE の方法論は文書としてプロジェクトのウェブサイトで公表されているが[10]、近日中に、より読みやすいハンドブックが公表される予定である。
- PRIPARE プロジェクトにおけるわれわれの担当部分は、1) プライバシー要件の稼働、2) プライバシー強化のための詳細な設計である。
- 1) プライバシー要件の操作プロセス（Privacy Requirements Operationalization）とは、抽象的なプライバシー原則を満たすために順番に置かれるべき特殊技術的操作要件（specific technical operational requirements）を理解する段階である「分析（analysis）」の一部である。PRIPARE プロジェクトでは、伝統的なリスクベースアプローチ（プライバシー影響評価 が代表）を補完するために、ゴール指向の操作プロセスを開発した。このプロセスは、プライバシー・バイ・デザインの各原則ごとに、ステークホルダーに中立的で、構造化、また階層化されて、優先順位をつけられたプライバシー諸要件の標準化されたカタログを基礎とする。これらのプライバシー適合基準は、システム仕様、アーキテクチャ、プライバシー影響分析とともに、開発中のシステムへ適用可能な一組の特殊な要件を定めることを可能にする。このゴール指向アプローチは、ガイドラインとプライバシー基準の信頼可能なカタログに強く依存しており、多くの主観的考えを退け、経験を要求することが少ないので、より簡単なアプローチであると思われる。
- **2)** プライバシー強化のための詳細な設計 は、上記と同じ考えを以下の 2 つの手段を介して「設計」の段階で取り入れる。1) まず、PRIPARE プロジェクトは、特殊なプライバシー要件を満たすために必要な再利用可能な設計ソリューションを提供する。2) ついで、同プロジェクトは、証明された方策を設計に適用し、これにより、過去の経験と知識を再利用することによって、不確実さと費用を減少させることができる。このプロセスは、プライバシー諸要件（原理、ガイドライン、基準など）を（発見的に）満たすプライバシー強化設計技術のカタログに依拠し、プライバシー要件はこのカタログにマッピングされている。設計者は、このカタログから技術を選び、ついで、その技術をプライバシ

[8] PRIPARE プロジェクトの研究成果（論文など）は、以下のリンクから取得できる。
http://pripareproject.eu/outreach/publications/
[9] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
[10] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.2_draft.pdf

ー・フレンドリーなシステムの設計を洗練するために使う。このカタログは、一種の料理本のようなものとして機能し、設計者は異なる要件を異なるシナリオで満たすために最も適切な方策（レシピ）を発見する。この技術のコンセプトは、プライバシー・パターンのコンセプトに類似するが、選択プロセス（誰、いつ、何のため、どのように等）を導く側面によって、より豊かなものになっている。

- これらのプロセスの定義と関係する PRIPARE プロジェクトの研究の結果は、以下である。
  - PRIPARE のプライバシー・セキュリティ・バイ・デザイン方法論の一部として、プロセスを定義した。このプロセスにはおいては、リスクベースアプローチ、そして、ゴール指向のアプローチが要件の顕在化のために統合されている。
  - プライバシー要件のカタログ（ISO 29100 プライバシー原則に沿う仕方で、一般的原理から詳細な技術的要件まで）
  - 異なる分野のコンテンツを詳細に示すプライバシー技術のためのテンプレート
  - 電気自動車のユビキタススマート充電システムへ方法論を事例として適用した。
  - プライバシー技術のセットがプライバシー・パターンとしてフォーマットされ、「privacypatterns.eu」[11]というウェブサイトで取得できる（プライバシー・アイコン、プライバシー・ダッシュボード、レイヤードポリシー設計、ポリシーマッチングディスプレイ、など）。
- これらと他の結果とともに、プライバシー要件の工学、PIA、リスク分析、適切な実践に焦点を置いた「ICT プラクショナーのためのトレーニングモジュール」を作った。これらのモジュールは、PRIPARE トレーニング教材の一部としてすでに公表されている（近日中に開発した全ての教材が公表される予定である）[12]。
- われわれはこの教材を開発しただけでなく、大学の修士課程と企業向けトレーニングプログラム（銀行分野：スペイン・サンタンデール銀行、テレコム分野：仏オレンジ、ICT 分野：Everis NTT[13]）において試験した。

PRIPARE 方法論の普及について

- われわれは PRIPARE の方法論の普及活動も実施した。
- 研究組織向け：欧州内外で行われる多くの国際会議、国際ワークショップ（CSP、CPDP、IWPE、IEEE、IoTPTS、CITA など）で研究結果を発表し、当該領域の学会誌、定期刊行物で論文を発表した。またプライバシー・パターンに興味をよせる研究団体、研究機関と国際協力を続けた。
- プラクショナー向け：さまざまな産業フォーラムで結果発表を行った。また民間企業から委託されて、PRIPARE の研究結果を産業トレーニングプログラムに組み入れた。
- 教育向け：教育、トレーニングの資料のリポジトリの構築に貢献した。これらの資料はプライバシー工学の一般的な授業で再利用されている。

[11] https://privacypatterns.eu/#/?limit=6&offset=0
[12] https://pripare.aup.edu
[13] Everis NTT は日本企業 NTT のスペイン子会社である。
http://www.everis.com/global/en-US/home/Paginas/home.aspx

- 政策立案者向け：政策についてのワークショップも、他のワークショップと一緒に開かれており、欧州委員会と特別な会合があった。だが、この種のワークショップには、PRIPAREプロジェクトの他のパートナーがわれわれよりも積極的に参加している。
- 標準化作業：標準化団体の技術委員会と研究グループに積極的に参加し、協力している（ISO/IEC、OASIS、NIST、W3C など）。
- 以上の他、例えば、ビッグデータやクラウドコンピューティングなどの各技術の団体でPRIPARE の成果を発表している（ビッグデータ分野：ビッグデータバリュー協会[14]、クラウドコンピューティング 分野: クラウドセキュリティアライアンス[15]、IoT 分野: IoT イノベーションアライアンス（AIOTI））[16]。

PRIPARE プロジェクトが策定した方法論への反応について

- PRIPARE プロジェクトは、プライバシー・バイ・デザインを実現するために、具体的に何が問題となり、何が必要となるか知るために、ワークショップを行い、参加者からの意見を聞いた。
- PRIPARE が開発しているような方法論の必要性を認める人が大多数だったが、実際に利用するにあたっては、技術毎の特殊な問題に対応する明確なソリューションの必要性や低コストなどを要求する人々がいた。以下、PRIPARE プロジェクトが策定した方法論への反応である。
  - CPDP 2015 （法に関わる者、学者が対象）：PRIPARE の内容はまさに共同体が要求しているものである。
  - インターネット・プライバシー工学ネットワーク：IPEN[17]における第一回目のワークショップ（政策立案者、標準化推進組織が対象）：実践する側からすれば、標準が複雑で、手助けとなる道具がない。
  - IPEN 第 2 回目 （法制度とプライバシー工学プラクショナーが対象）：プライバシー工学の体系的な研究方法が必要である。法律家、エンジニア、政策立案者、ビジネスが期待するものの間にずれがある。
  - 国際プライバシー工学ワークショップ：IWPE （ICT 研究者が対象）：方法論を適用した開発物を評価する基準、技術、道具がない。方法論をさまざまな分野に適応させることが重要である。
  - CSP フォーラム[18]（欧州研究プロジェクトが対象：プライバシーへの意識を高めることが目的）：方法論を適用するためには、他のプロジェクトとの連携が必要である。
  - PRIPARE のワークショップ （欧州研究プロジェクトが対象 ：トレーニングが目的） ：方法論は必要だが、各方法が複雑で、研究と工学プロセスへスムーズに導入するためには成熟が必要である。

PRIPARE プロジェクトと EU パーソナルデータ指令改正案との関係について

- プライバシー保護には法的措置だけでは十分でなく、技術的な観点からのアプローチが必要であり、PRIPARE プロジェクトにおいて開発されたプライバシー・バイ・デザインの

[14] http://www.bdva.eu/#sidr-main
[15] https://cloudsecurityalliance.org
[16] http://www.aioti.eu/#!/page_SPLASH
[17] https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS/IPEN
IPEN は、欧州データ保護監督庁によって主導されているフォーラムであり、EU 諸機関と ICT 技術者の共同体をつなぐ役割を果たしている。
[18] http://www.cspforum.eu

方法論は価値がある。だが、PRIPARE は出発点にすぎず、他の研究によりさらに展開され、補完される必要がある。

- EU パーソナルデータ指令改正案は、プライバシー・バイ・デザインの導入を義務付けるが、その手段については強制しない。従って、同改正法が PRIPARE プロジェクトの成果を利用することを要請するわけではない。しかし、PRIPARE の方法論以外に一般的な方法論が存在しないことが実情である。

PRIPARE プロジェクト以後のプライバシーとパーソナルデータ保護の研究活動について

- PRIPARE プロジェクトは 2015 年 9 月に終了したので、その成果と課題を踏まえて、現在研究している。
  - 欧州内で、プライバシー工学の研究を学際的に提携させ、特にプライバシー工学の知識体系構築（プラクショナーとトレーニング向け）に積極的に取り組んでいる。
  - PRIPARE の方法論を特定の技術、特にクラウドコンピューティング、ビッグデータ、IoT の研究開発向けに応用する研究を実施している。例えば、われわれはスペインのビッグデータ企業と提携し、プライバシーを保護するような仕方でビッグデータのシステムを開発する方法に関して、この企業に専門的知識を供与している。
- パーソナルデータ、アイデンティティー、プライバシー管理についての研究プロジェクトは以下のものがある。
  - POSDATA（サンタンデール銀行の資金提供）：ユーザの分散したパーソナルデータの統合とユーザ中心のデータ管理向けにパーソナルデータの枠組みを定義する研究
  - SEGUR@（スペイン政府の資金提供）：プライバシー強化技術（このうち 4 つは国際特許によって保護されている）の開発
- われわれはプライバシー保護に係る学際的な研究を数多く実施しており、法律の専門家と一緒に、例えば、ビッグデータシステムの開発について民間企業に協力している。
- われわれが参加する学際的アプローチをとる研究プロジェクトは以下のものがある。
  - IPERCS : プライバシー工学分野の開発と確立のための提携とサポート活動 : 法学者と協力してプライバシー・バイ・デザインソリューションの理解を調整し、促進する。
  - PeRMIT : ヒューマンコンピュータインタラクション（HCI）と情報の流れに焦点をあて、プライバシー工学を IoT の特殊性に適応させる研究 : コンピュータセキュリティと HCI 研究者および医療現場で働く人々と協力して、プライバシーの基本的諸権利を遵守しながら携帯可能な自己定量化装置の開発をサポートする。
  - Best practices for Big Data : プラクショナー向けの適切な実践のガイダンス作成と実践例の収集 : 法律の専門家、各国のパーソナルデータ保護規制機関、政策立案者と協力して、スペインの営利企業と公的機関によるプライバシー工学実践の採用をめざす。
  - TrustedCloud : クラウドコンピューティング環境におけるプライバシー工学の諸側面の開発のために、トレーニングネットワークを構築する。
- 以上の他、欧州の組織と提携して、製品やサービスのプライバシー保護を認証するプライバシーシールの開発に参加している。このため、技術者のほか、法律、社会学、心理学の専門家が参加し、学際的な研究を行っている。プライバシーシールについて、学際的な研究を実施している理由は、プライバシーは技術と法だけの問題ではなく、実際に人々がどのようにプライバシーについて考え、どのように行動しているかを考慮する必要があるからである。また、現実に、どのようにプライバシー保護が行われているか知る必要がある。

ICT 研究者とエンジニアにとってのプライバシー・バイ・デザイン導入の困難さについて

- プライバシー・バイ・デザインを実際に取り入れるには、日々の開発においてプライバシー工学を支え、また、ソフトウェアとシステムの開発組織において適切な実践を採用し組み入れるのを可能にするような、体系的な方法、技術、道具、サポートが欠けている。
- プライバシー強化技術やソリューションを開発しても、それを体系的に利用する方法がない。
- プライバシー・バイ・デザインの採用のためには、ビッグデータ、クラウドコンピューティング、IoT といった異なる領域の特殊性を考慮する必要がある。
- 国際レベルで複数の組織が共通の研究アジェンダにおいて、共同作業を進め、力を合わせるためには、プライバシー・バイ・デザインについて組織間での合意が必要である。

プライバシー・バイ・デザインの導入に必要な点

- プライバシー・バイ・デザインが新しいソフトウェア、システム、サービスの開発プロセスに実効的に導入されるためには、以下の点で更なる進歩が必要である。
  - 要件の新しいソースを方法論へ統合すること。
  - 基本設計のレベルと設計の詳細部分について、ガイダンスを作成すること。
  - プライバシーの機密性を試験し、検証すること。
  - 方法論を IoT、ビッグデータ、クラウドコンピューティングといった異なる領域の特殊性に合わせること。
  - 欧州外の当該組織と連携すること。

プライバシー保護の国際提携の必要性について

- われわれはプライバシーのような複雑な問題を解決するためには、学際的共同作業が必要であると考えると同時に、国際的な協力が必要不可欠であると考えている。エルモ教授はコロンビアでイベリアーアメリカ・テレマティックス会議（CITA）[19]の組織での議長を務め、また、デル・アラモ教授は、エクアドルでプライバシー・バイ・デザイン関係の会議の開催に働きかけている。
- EU の「サイバーセキュリティとプライバシー研究とイノベーションにおける EU との提携協力と国際的対話」というホライゾン 2020 の公募（H2020 DS-05-2016）[20]によって、学際的協力をさらに進めようとしている（この公募では日本との対話が主要なトピックの一つである）。
- デル・アラモ氏は、プライバシー・バイ・デザインの実現を望む研究者の集まりである国際プライバシー工学ワークショップ（IWPE）[21]で議長をしている。2015 年のワークショップでは、プライバシー工学に関する国際的なイニシアチブが紹介されている。

アメリカとの提携関係について

- 政治的レベルでは、欧州の方がプライバシーの問題にアメリカよりも強く関心を持っていると言えるが、技術的レベルでは、アメリカ国立標準技術研究所（NIST）やアメリカの幾つかの大学も、プライバシー・バイ・デザインの研究を実施し、プライバシー工学の方法論を策定しており、われわれはこうしたアメリカの組織と積極的に提携して活動している。

[19] http://www.parquesoftpopayan.com/eventos/127-vii-congreso-iberoamericano-de-telematica-cita-2015
[20] http://www.gppq.fct.pt/h2020/call.php?id=H2020-DS-2016-3&topic=DS-05-2016
[21] http://ieee-security.org/TC/SPW2015/IWPE/organization.html

・ 課題の一つは、われわれのプライバシー問題へのアプローチと他国のアプローチを提携させることである。例えば、アメリカはユーザの同意を得るアプローチに強く関心を持っているが、欧州は開示データの最小限化のアプローチに焦点を置いている。

第二章　FP7 PARIS プロジェクト

PARIS プロジェクトは、8 組織が参加し、全予算が 477 万ユーロである（研究期間：2013 年 1 月～2015 年 12 月）。監視システムや生物計測システムの研究開発にあたって、プライバシー・バイ・デザインを実施する方法論を開発する。

第一節　PARIS プロジェクトの基本情報

プロジェクト名略称	PARIS
正式名称	プライバシーを保護する監視インフラストラクチャ
分野	SEC-2012.6.1-2
プロジェクト期間	2013 年 1 月～2015 年 12 月（36 ヶ月）
予算（EU 拠出分）	477 万ユーロ（349 万ユーロ）
コーディネーター	トリアログ（仏）
参加者	INRIA（仏）、KU ルーヴァン（ベルギー）、マラガ大学（スペイン）、ナミュール大学（ベルギー）、タレス コミュニケーション&セキュリティ（仏）、VISUAL TOOLS（スペイン）、オーストリア技術研究院（オーストリア）
ウェブサイト	http://www.paris-project.org/index.php/factsheet http://cordis.europa.eu/project/rcn/106634_en.html

第二節　PARIS プロジェクトの研究内容

PARIS プロジェクトは、研究内容の一部を 2016 年 1 月末にブリュッセルで開催された CPDP2016[22]で発表している。以下に、その概要を記す。

「生物計測システムのためのプライバシー影響評価テンプレートへ向けて」：ナミュール大学（ベルギー） / クレール・ガイレル氏（法学研究者）

- 生物計測システム（掌形認証、指紋認証、静脈パターン認証、顔認証など）に利用できるプライバシー影響評価（PIA）について研究を実施した。
- 民間企業が展開する生物計測システムだけを対象にした（国境コントロールシステムなどの公共機関が展開する生物計測システムは除外。）
- 個人のプライバシーへの影響だけを対象にした（組織に対する影響は除外）。
- 研究の目標は二つある。第一に、生物計測システムを展開する機会（opportunity）を評価すること、第二に、生物計測システムの設計について意思決定を支援すること。
- 生物計測システムのプライバシーへの影響を評価する際に考慮すべき適切な基準を見出すためには、EU の第 29 条パーティ（以下、WP29 とする）の意見[23]及び法学者の研究が参照されるべきであるが、同時に、各国のパーソナルデータ保護規制機関（以下、

[22] http://www.cpdpconferences.org
CPDP は、プライバシー保護技術と法制度に関する欧州最大のイベントである。
[23] 例えば、W29 が 2012 年に発表した「生物計測技術の発展についての意見」がある。
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

DPA とする）が実際に行っている規制を知る必要がある。以上の理由から、本研究では、フランスの事例研究 を実施した。

- フランスでは、2005 年から 2014 年の 10 年間に渡って、民間部門での生物計測システムの展開に関して、仏パーソナルデータ独立保護規制機関である CNIL は、458 件について検討した（認可と不認可の双方を含む）。
- フランスでは、主に仕事場の環境（84%）で、生物計測システムが展開されている（その他、学校環境 / 特に調理場へのアクセス（15%）、研究・実験環境（1%）、商業環境 / スポーツ施設なども含む（0%：ほとんどない）。
- フランスでは、「特殊認可（special authorization）」[24]を必要とする生物計測システムを展開するため理由としては、従業員のアクセスコントロールが多い（79%）（その他、研究・実験の目的、顧客のアクセスコントロール、未成年者のアクセスコントロールなど）。
- CNIL の生物計測システムに対するプライバシー影響評価基準の不十分な点：
    1. CNIL の対象となる人物のカテゴリー分け（未成年、従業員、顧客）の区別 ⇨ このカテゴリーは不明瞭なので、さらに細分化して明確にする必要がある。例えば、未成年、従業員、顧客以外の区別のカテゴリーもあるのではないか。
    2. CNIL のデータの中央保存と端末保存の区別 ⇨ この区別はだけでは不十分なので、システムの機能が人物の特定（identification）[25]なのか、証明（veryfication）なのか、あるいは、人物の特定システムの場合、他の人物特定要素と一緒に保存されているかどうかさらに区別する必要がある。
    3. CNIL が要請する明示的な同意（生物計測システムの利用には、必ず利用者の明示的な同意が必要である）⇨ 同意の条件が完全に満たされているのか検証する必要がある（未成年の場合、年齢は十分考慮されているか、拒否することが否定的な結果をもたらさないか、正当な代替え策はあるか）。
    4. EU パーソナルデータ保護指令第 7 条は、パーソナデータの処理を認可する理由として、当該組織の「正当な関心（legitimate interests）」を挙げている ⇨ パーソナルデータの処理を伴う生物計測システムを展開するために、どんなタイプの正当な関心が引き合いに出されるのか明確にする必要がある。1) 組織の経済的関心、2) 組織及び第三者や個人の関心（サーバへのアクセスコントロールに生物計測システムを利用して、パーソナルデータを保護する。また、分類された情報の保護と労働者の安全を確保する）、3) 一般的な公共の関心（生物計測システムによって、重要インフラストラクチャや制限されたエリアへのアクセスをコントロールし、保護する）。
- 以上の検討から、ガイレル氏はプライバシー影響評価のための表を作成した。

影響評価表

基準		影響	係数
人物のカテゴリー	未成年	+++	1

[24] フランスでは、生物計測システムを展開するには、CNIL に単に届け出るだけではなく、特殊認可を必要とする場合がある。
以下の資料も参考のこと。
http://www.paris-project.org/images/Paris/pdfFiles/PARIS_04-1-Gayrel-PARIS-slides-150902[1].pdf

[25] 人物の特定システムと証明システムは異なる。前者は、データベースに保存された全データから人物が誰であるか特定し（ある個人のデータを保存された全てのデータに対して照合する。指紋や DNA などの犯罪捜査でも利用される）、後者は、ある個人のデータをデータベースに保存されているその個人のデータと照合するだけである（ある個人が誰であるのかは問題にしない）。

		顧客	++	
		従業員	+	
		その他	+	
法的正当性	同意の有無	弱い同意	+++	2
		妥当な同意	+	
	正当な関心	データ管理者の正当な関心のみ	+++	
		データ管理者と第三者の正当な関心	++	
		一般的な公共の関心	+	
機能		人物の特定システム	+++	2
		人物の証明システム	+	
保存	人物の特定システム	他の人物特定要素とともにデータの中央保存	+++	1
		他の人物特定要素とは別にデータの中央保存	+	
	人物の証明システム	中央保存	++	
		端末保存	+	

・ 上記の表を用いて、生物計測システムの設計・開発以前の段階で、プライバシーへの影響を評価し、スコアを出すことが可能になる。そして、設計に勧告を出すことできる。

第三章　FP7 PRACTICE プロジェクト

PRACTICE プロジェクトの目標は、クラウドシステム全体において、データの機密性と暗号化されたデータのコンピューテーションを実現し、柔軟なアーキテクチャとツールを開発することである。

第一節　PRACTICE プロジェクトの基本概要

プロジェクト名略称	PRACTICE
正式名称	PRACTICE: クラウドにおけるプライバシーを保護するコンピューテーション
分野	ICT-2013.1.5
プロジェクト期間	2013 年 11 月～2016 年 10 月（36 ヶ月）
予算（EU 拠出分）	1046 万ユーロ（755 万ユーロ）
コーディネーター	テクニコン（オーストリア）
参加者	KU ルーヴァン（ベルギー）、ゲオルグ・アウグスト大学ゲッティンゲン（独）、ユリウス・マクシミリアン大学ヴュルツブルグ（独）、ダルムシュタット工科大学（独）、インテル（独）、アレクサンドラ研究院（デンマーク）、オーフス大学（デンマーク）、PARTICIA（デンマーク）、CYBERNETICA（エストニア）、バル＝イラン大学（イスラエル）、DISTRETTO TECNOLOGICO AEROSPAZIALE（伊）、ミラノ大学（伊）、アイントフォーヘン工科大学（蘭）、INESC PORTO（ポルトガル）、ARCELIK（トルコ）、ブリストル大学（英）、サレント大学（伊）、SAP

	（独）
ウェブサイト	http://www.practice-project.eu http://cordis.europa.eu/project/rcn/111030_en.html

第二節　PRACTICE プロジェクトの最新動向

PRACTICE プロジェクトは、現在、プロジェクトのウェブサイト上で、様々なユースケースを公表している[26]。同プロジェクトでは、暗号技術を利用して、クラウドで処理されるデータを保護し、クラウドサービス事業者にもユーザのデータを見ることができなくすることが目指されている。

- オークション向けプラットフォーム（電気と電波オークションが想定）
- プライバシーを保護するパーソナルゲノム分析・研究向け情報システム
- スマートフォン向け地理情報システム（地理情報システム事業者から、ユーザの現在の地理情報を隠しながら、地理情報システムを利用する）
- モバイル端末間のデータ共有システム（クラウド事業者に、クラウドを通して端末間で共有したデータを見えなくする）
- 安全なクラウド統計学サービス

[26] https://practice-project.eu/project-results/application-scenarios

第二部 欧州連合のパーソナルデータ保護法改正を巡る動向

第二部では、EU のパーソナルデータ保護法の改正動向について記す。まず、同法の改正動向、ついで、改正のポイントとその評価、今後の展望と課題を概観する。最後に、フランスのリヨン市で開催されたイベントである「諸文化を通じたプライバシー – グローバル化した世界における一致点と相違点–」を視察した際の報告書を収録する。

第一章　EU パーソナルデータ保護法の審議状況

欧州委員会は、2012 年 1 月に現行の EU パーソナルデータ保護指令[27]の改正案である「一般データ保護規則案」[28]を「警察・刑事司法データ保護指令案」[29]とともに提案した。前者は、主に 2 つの問題、1) 現行の EU 法が指令という法形態を持つために、各国で法文が解釈されて、国内法化されており、EU 地域圏で規制が調和してないという問題[30]、そして、2) 1995 年以来パーソナルデータの取り扱いを伴う新しいデジタル技術が生まれており、現行の法制度を近代化する必要があるという問題に対応するために提案された[31]。以下に、改正法の審議状況、改正のポイントについて概観する。

第一節　改正法の審議状況

欧州委員会によって、EU パーソナルデータ保護指令改正案が 2012 年に提案されて以来、同案は欧州議会及び欧州連合理事会（以下、閣僚理事会とする[32]）で審議され、修正が重ねられてきた。特に、2013 年には、アメリカ国家安全保障局がいくつかの米インターネット企業から彼らの欧州顧客の情報を受け取っていたことが明らかになり、このスキャンダル以降、欧州市民を、内外の安全保障機関のパーソナルデータ使用から保護する法制度の必要性が浮き彫りになって、改正案の射程は拡大した。

2015 年 12 月 15 日、欧州委員会を合わせた三機関による 6 か月間の三者協議の末、改正案について欧州議会及び閣僚理事会が最終的な合意に至っている。この結果、2016 年初頭に改正案は欧州議会及び閣僚理事会によって採択される見込みであり、法案採択の 2 年後に改正法は各国で適用される予定である[33]。

2015 年 1 月の報道発表では、欧州議会と閣僚理事会の間の溝は深く、2015 年内に両者の合意実現は危ぶまれていた[34]。特に、データ利用についての事前同意、罰金、プライバシー・バイ・デザイン、形式主義的な手続きというポイントが両機関の争点であった。例えば、パーソナル

---

[27] 正式名称：「パーソナルデータの取り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指令」1995 年成立。

[28] 正式名称：「パーソナルデータの取り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案」

[29] 正式名称：「刑事犯罪の防止、捜査、探知もしくは訴追又は刑事罰の執行のための管轄機関によるパーソナルデータ処理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指令案」

[30] 改正案の名称からわかる通り、改正法は、指令ではなく、規則という法形態で提案された。指令は、EU 加盟国で国内法化され、規制の内容を EU 加盟国で統一するのに対して、規則は EU 加盟国で法令を統一し、直接適用される。指令の場合、各国が指令を国内法化する際に、規制の手段と方法に関しては加盟国に任されるので、EU 加盟国間で規制が実際に調和的な仕方で行われないこともありうる。

[31] http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

[32] 欧州連合理事会という名称は、全く異なる組織である欧州理事会と名称が類似するため、閣僚理事会と呼ぶ。

[33] http://europa.eu/rapid/press-release_IP-15-6321_en.htm

[34] http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100

データ使用の同意を、どこまで厳密な形で、データ処理者がユーザから得なければならないかが、議論の争点の一つだった。欧州議会と欧州委員会は、「明示的な（explicit）」同意を得ることを求めたのに対して、EU 加盟国は、「あいまいではない（unambiguous）」同意、つまり、より厳密でない、緩やかな同意を求めた。また、閣僚理事会は、欧州委員会の提案である規則違反の罰金最高額を総収入の 2%とすることを支持しているのに対して、欧州議会は 5%まで増額することを望んでいた。他方で、加盟国の間でも相違があった。フランスとドイツは改正法案で提案された「ワンストップショップ」と言われるアプローチ（EU 市民や企業は自国のデータ保護規制機関との交渉のみで、EU 28 加盟国と交渉する必要はない）に懐疑的であり、英国は「規則」ではなく、「指令」という法形態で採択することを好んでいた。

2015 年 6 月 15 日、EU 諸国の法務大臣間で以下の点で改正案の合意に至り、6 月 24 日より閣僚理事会は、欧州議会及び欧州委員会との三者協議を始めることになった[35]。欧州委員会の発表によれば、閣僚理事会は主に以下の点で合意に至った[36]。

- 「一つの大陸、一つの法」：この規則は EU 全体で実効力を持つただ一つの法律となる。これによって、1 年間に 23 億ユーロのビジネス費用が削減される。その上、この法は中小企業向けに必要のない事務手続きに係る制度を見直しており、この改正だけで、1 年間に 1 億 3000 万ユーロの費用が削減される見込みである。
- 「権利の強化、追加」：「忘れられる権利（right to be forgotten）」が強化される（市民が自分のデータの処理の停止を求める場合、そのデータを処理する正当な理由がなければ、管理者はこのデータを削除しなければならない）。同様に、ユーザがサービス供給者間で個人データを移すのが容易になり（「データポータビリティの権利」）、また、いつ自分のデータがハッキングされたか知る権利が保障される。
- 「欧州では欧州の法律」：欧州外の企業も欧州へサービスを提供する場合、欧州の法律に従う。
- 「各国のデータ保護規制機関（DPA）の権限強化」：効果的に法律を施行するため、DPA の権限は強化され、違反した企業には 100 万ユーロ以内もしくは世界での年間総売り上げの 2%の罰金を科すことができる。
- 「ワンストップショップ」：上記のように争点となっていた「ワンストップショップ」アプローチを採用する。

なお、忘れられる権利に関しては、2014 年 3 月に欧州議会が承認した一般データ保護規則の草案では、「忘れられる権利（right to be forgetten）」という言葉は削除され、「削除する権利（right to erasure）」を保障するにとどまっていた。だが、2015 年 6 月の閣僚理事会の合意案では、「忘れられる権利」という文言は復活している。

さて、閣僚理事会での合意に対する批判もないわけではない。

- 改正案の第 6 条 4 は[37]、「正当な関心（legitimate interest）」のためであれば、ユーザが同意した理由以外の理由で、企業がデータを処理することを許すのではないか（ポーランド、ブルガリア、デンマーク法務大臣の批判）。
- データ処理への制約は広告収入を減少させ、ビジネスに打撃を与えてしまう（産業団体）。
- オーストリアの厳格なデータ保護法と比べて、改正案は厳密でない（オーストリア法務大臣）。
- ビジネスのビッグデータの利用から、消費者の権利を保護する必要がある（消費者団体 BEUC[38]）。

35 http://www.euractiv.com/sections/infosociety/european-council-approves-data-protection-reform-315403
36 http://europa.eu/rapid/press-release_IP-15-5176_en.htm
37 http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

さらに、改正法に反発するため、2015 年 12 月、ノキア、エリクソン、SAP などの欧州の大企業を含む企業は連合し、よりビジネスに便宜を図るよう求める書簡を EU28 加盟国の首長と欧州議会議長、欧州委員会委員長、欧州委員会法務委員、欧州委員会副委員長、欧州委員会デジタル委員に提出した[39]。 書簡では、特に以下の点が要求された。

- 欧州議会による違反した企業への罰金案（年間総売上げの 5%）を批判。
- 国際レベルでのデータの移行のため、安全かつ柔軟な基盤の保障[40]。

第二節　EU パーソナルデータ保護法改正のポイント

第一節で見たように、EU パーソナルデータ保護法改正案は紆余曲折を経て、2016 年内の採択の見通しが立っている。以下に、欧州委員会のプレス発表文書を元に、改正のポイントについて記す[41]。

0) データ保護法改正パッケージ

データ保護法改正パッケージは、一般データ保護規則と法執行機関によるデータ利用におけるデータ保護指令の二つの EU 法からなる。

- EU 市民のデータの利用とプライバシーに係る一般データ保護規則：a) 同規則は個人が自分のデータをよりコントロールできることを可能にする。b) また、同規則は、ビジネスが形式主義的な手続きを廃し、消費者の信用を強化することによって、デジタル単一市場の機会を最大限活用することを可能にする。
- 法執行機関による EU 市民のデータの利用に係るデータ保護指令：警察と刑事司法の諸機関は、被害者、承認、容疑者のデータが犯罪捜査もしくは法施行の場面でしかるべく保護されるように保障する。

1) 市民のための基本権

データ保護法改正は、EU 市民の基本権であるデータ保護の権利を強化する。最近の EUROBAROMETER の調査によれば 42、67%の EU 市民がオンライン上に上げている情報を完全にコントロールしていないことを心配しており、また 7 割の EU 市民が開示情報の企業による潜在的な利用を不安視している。新しい規則はこれらの心配に対応するために、既存の権利を強化し、個人が自分のパーソナルデータをよりコントロールすることを可能にする。

- 自分自身のデータへより簡単にアクセスすることを保証する権利（改正法第 15 条）：個人が自分のデータがどのように処理されているか、より多くの情報を取得し、また、その情報に明瞭かつ理解可能な仕方でアクセスできる。
- 消去権及び忘れられる権利（第 17 条）：自分のデータの処理の停止を求める場合、そのデータを保持する正当な理由がない限りにおいて、そのデータを消去することを求める権利。
- データポータビリティの権利（第 18 条）：自分のパーソナルデータをあるサービス供給者から別のサービス供給者へ移行しやすくなる。
- いつ自分のデータがハッキングされたか知る権利（第 32 条）

---

[38] http://www.beuc.eu/about-beuc/who-we-are
[39] http://www.euractiv.com/sections/digital/tech-industry-goes-last-minute-appeal-data-protection-320021
http://europeandatacoalition.eu/wp-content/uploads/2015/06/European-Data-Coalition-Letter-to-the-Members-of-the-Council.pdf
[40] http://www.euractiv.com/sections/digital/tech-industry-goes-last-minute-appeal-data-protection-320021
[41] http://europa.eu/rapid/press-release_IP-15-6321_en.htm
http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
[42] http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

- 法執行の強化：DPA は、EU 法を違反した企業に対して、最大で世界中での年間収入の 4%まで罰金を課すことができる（第 79 条）

2) ビジネスのための明確で近代的な法律

改正法は、単にデータ保護の規制を強化するだけではなく、加盟国間で規制を調和し、消費者の信頼を回復することで、経済成長を促進する。

- EU で統一的なデータ保護法を適用することによって、EU でビジネスを、より容易により安価で行えるようになる（法形態を「指令」から「規則」へ変更する）
- 欧州外に基盤を置く企業が、EU でサービスを提供する際、同じ法律を守らなければならない（第 3 条）。
- ワンストップショップアプローチを採用する（第 51 条）。
- 設計と初期設定によるデータプロテクションの義務（第 23 条：Data protection by design and by default）：データ保護手段が開発の初期段階から取り入れられ、また、初期設定がプライバシー・フレンドリィでなければならない。プライバシーを配慮した技術、例えば、偽名化を推奨することで、プライバシーを守りながら、ビッグデータ・イノベーションによる利益を上げる。

3) 大企業だけでなく、中小企業へも等しくもたらされる恩恵

形式的な手続きを排除することでコストを減らし、中小企業の新しい市場への参入を援助する。

- 監督機関へパーソナルデータを処理していることを通知する義務の廃止。これにより、毎年 1 億 3 千万ユーロのコスト削減の見込み（全文(70)）。
- 中小企業は、データ処理が中心的な業務内容でないかぎり、データ保護オフィサーを任命する義務はない（第 35 条）。
- 中小企業は、高いリスクがないかぎり、個人データ処理の記録を保存する必要がない（第 28 条）。

以上のほか、新しいパーソナルデータ保護法は、EU 域内での同法の適用を保障するため、「欧州データ保護会議（European Data Protection Board）」[43]という法的資格を有する EU 機関を設立する（第 64 条）。

法執行におけるパーソナルデータ保護

- 警察と刑事司法の機関に係る新しいデータ保護指令は、法施行の際の特殊性を考慮し、それぞれの加盟国の法律上の慣習を尊重しながら、捜査に必要な情報を効率的、実効的に交換することを可能にする。
  - パーソナルデータはそれが被害者のものであれ、犯罪者のものであれ、証人のものであれ、犯罪防止を含むあらゆる法執行の場面において、より保護されるようになる。EU 内で行われるすべての法執行は、個人を適切に保護しながら、必然性、均整、合法性の原理に従わなければならない。監督は独立した国内データ保護機関が保障し、法的救済がなされなければならない。
  - データ保護指令は、EU 外の法執行機関による個人データの移動の明確な規則を与え、EU 内で保障されている個人の保護レベルが決して落ちないようにする。

[43] 欧州データ保護会議は、各国でのパーソナルデータ保護法の適用を確保する目的を持つ。

第三節　EU パーソナルデータ保護法改正案の評価と展望

2015 年 12 月の三者協議での合意を受け、2016 年初頭、最終的な法案が欧州議会と閣僚理事会によって採択されたのち、パーソナルデータ保護改正法は二年以内に各加盟国内で適用されることになる。では、改正法案採択の見通しがついた現在、どのような評価が法案になされているのか。また、改正法適用までの 2 年間の移行期間はどのようなものになるのか。2016 年 1 月末にブリュッセルで開催された CPDP2016 では、以上の問題について討議するセッションが用意された。以下に、その要点について記す。

欧州議会議員によるパーソナルデータ保護法改正案の評価と課題

CPDP2016 では、欧州議会議員 5 名がパーソナルデータ保護法改正案について意見を述べるセッションが設けられ、各議員が評価と課題について述べている。

肯定的な評価

- パーソナルデータ保護法が規則という法形態で、EU 加盟国内で直接適用されるので、同法は EU の統一的な法として EU 単一市場の形成に寄与する。EU で法制度を統一することは、北米などの他の地域と国際的なデータ移動について交渉するのに必要である。
- 従来のパーソナルデータ保護法を近代化させ、従来の法を改善する。法文内に、データ保護措置のカタログが明記されている。
- パーソナルデータ保護法は、消費者の信用を回復するので、EU の経済成長に貢献する。

否定的な評価

- パーソナルデータ保護法は非常に複雑であり、不確実な点があり、異なる解釈が可能である。
- パーソナルデータ保護法は、規則という形態を持つにもかかわらず、あまりにも多くの条項において、各国での柔軟な適用に開かれており、EU 加盟国内での規制の調和は疑わしい。
- パーソナルデータ保護法は、基本権や個人の権利の遵守を改善したが、データアクセスの簡便化を実現する制度を定めていないので、データを利用するビジネスモデルの発展を妨げ、EU の経済成長を促進しない（ビッグデータの利用を過度に制限してしまう）。匿名化されたデータにより簡単にアクセスできるようにする制度にすべきであった。新しいデータ保護法は、将来的にデータの利用が経済成長を振興するという展望に反している。
- パーソナルデータ保護法は、欧州データ保護会議を設立するが、あまりにも多くの権限を与えすぎており、中国の中央政府のようである。

多くの議員が肯定的に評価したが、独アクセル・ヴォス議員は多くの点に渡って、否定的な評価を下した。以上の否定的な評価は全て、独アクセル・ヴォス議員のものであり、同議員のスピーチの後、他の議員が反論している。

課題

- 改正法は、2018 年 6 月に適用される予定であり、採択から 2 年間の移行期間がある。
- この移行期間は、パーソナルデータ保護法の実際の適用にとても重要である。同法は非常に複雑であり、移行期間中に、関係者は正しくこの法を理解しなければならない。
- 各国内での法の適用にあたっては、各国に委ねる面があり、柔軟性があるが、この柔軟性が EU 地域圏での法の調和を妨げてはならない。このため、各国の規制機関へのガイダンスが必要である。

- 法というものは一般的に各国の文化と繋がっているので、各国に共通の法を導入することは、共通の文化を導入することと等しく、各国に元来ある文化と齟齬が出る可能性がある。EU 加盟国内でも、東欧、北欧、イギリスでは文化が非常に異なり、データ保護に関する考えや保護手段の使い方に違いがある。

各国規制機関によるパーソナルデータ保護改正法の適用準備

CPDP2016 では、各国のパーソナルデータ保護規制機関（以下、DPA とする）の代表者と法学者、企業が集まり、各国内での法の適用について意見を述べるセッションも設置された。DPA は、法改正に伴う準備を開始している。仏 DPA である CNIL によれば、DPA は 3 つの異なるレベルで法改正に準備、対応しなければならない。

1. 欧州データ保護会議の設立：現在、第 29 条パーティ（WP29）は、欧州委員会への助言機関であり、データ保護に関するガイドラインなどを策定している。法改正によって、WP29 は欧州データ保護会議（EDPB）として生まれ変わる。EDPB は、WP29 とは異なる機関であり、EU 機関として法的人格を持ち、拘束力のある決定を出すことできる。
2. 各国の DPA との連携：法改正で、ワンストップショップサービスの実施が決定したため、各国の DPA が提携して、具体的な実施方法を定める必要がある。問題は、例えば、苦情が複数国にまたがる場合、協力して対応するための手段を組織することである。
3. 日常業務の変化：法改正は日常の業務も大きく変更し、他の加盟国と提携して活動することを念頭におく必要がある（具体例：法改正についてワークショップの実施、職員全員が英会話の練習など）。

第四節　EU パーソナルデータ保護法改正の日本への影響

EU のパーソナルデータ保護法の改正は日本の組織へも影響する。改正案では、EU 域外への EU 居住者のパーソナルデータの移転は基本的に禁止という原則は保持されると同時に、現行法と同様、EU 域外へのデータ移動に必要な措置について定められている（十分性認定[44]、拘束的企業準則[45]、標準契約[46]、パーソナルデータ保護法の第 39 条で新たに定められた認証システム）。

以上に加えて、改正案では、パーソナルデータ保護法が EU 域外にも適用されることが定められたことに注意する必要がある。

EU パーソナルデータ保護法の EU 加盟国域外への適用

改正案では、一定の場合について、規則の EU 外への適用 が定められた。現行のパーソナルデータ保護法では、データ管理者が EU 域内に事業所を持つ場合か、EU 域内の設備でデータ処理を行う場合のみ規制の対象であるが、改正後は、EU 域外に事業者を持つ企業でも、以下の二つの場合、EU 居住者のデータを取り扱う管理者に対してパーソナル保護法が適用される。

1) EU 居住者に商品やサービスを提供する場合

[44] EU が第三国を EU 加盟国と同程度データが保護されていると認める場合のこと。日本は十分性認定を得ていない。
[45] 多国籍企業がグループ内で従業員などのデータを移転することを可能にする制度のこと。
[46] パーソナルデータをやり取りする組織間で締結する必要がある契約のこと。欧州委員会が標準契約のモデルを策定している。
http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

2) EU 居住者の個人の行動をモニターする場合

特に、オンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者などが対象となる。したがって、日本の企業は EU パーソナルデータ保護法を熟知し、対応しなければ、知らずに同法に違反し、罰金を課される可能性がある。また、改正案では、罰金額が増額されており、EU 加盟国のパーソナルデータ保護独立規制機関は、EU 法を違反した企業に対して、最大で世界中での年間収入の 4%まで罰金を課すことができる。

第二章　欧州におけるパーソナルデータ保護法制度をめぐる最新動向

欧州において、プライバシー及びパーソナルデータ保護への関心は非常に高く、様々なイベントが開催されている。以下に、フランスのリヨン市、そして、パリ市で実施されたイベントを視察した際のレポートを収録する。リヨン市のイベントでは、セッションの一つで、EU パーソナルデータ保護法の「忘れられる権利」をめぐる問題が討議され、パリ市のイベントでは、EU と米国間のパーソナルデータ移転を規制するセーフハーバー協定の無効について EU の関係者から意見が述べられて、EU のパーソナルデータ保護法の最新動向が明らかになった。

第一節　イベント視察報告書 /「諸文化を通じたプライバシー – グローバル化した世界における一致点と相違点–」[47]

2015 年 11 月、フランスのリヨン市でパーソナルデータ保護制度をめぐるイベントが開催され、EU のパーソナルデータ保護法と他の地域の法制度との相違点、また欧州における米グーグル社の活動の取り締まりなどについて報告され、討議された。仏 DPA の CNIL 議長イザベル・ファルク＝ピエロタン氏によって、EU パーソナルデータ保護制度の最大の特徴は、パーソナルデータ保護が EU 市民の基本権の一つして考えられていることにあり、この点においてこそ、EU の法制度は他の地域の法制度とは異なり、そして、優越すると主張され、EU のパーソナルデータ保護に係る思想と制度が明確に表明されている。以下に、イベントの概要を報告する。

- 日程 : 平成 27 年 11 月 30 日（月）
- 場所 : フランス・リヨン市
- 主催者 : INRIA CAPPRIS プロジェクトチーム[48]（責任者 : ダニエル・ルメタイエ氏）
- 趣旨 : 欧州と北米（アメリカとカナダ、特にケベック州）間のパーソナルデータ保護に対するアプローチの違い（特に法制度）を検討する。

<u>全体の概要</u>

- パネルディスカッションには、特にフランスとカナダのケベック州（フランス語圏）のパーソナルデータ保護法制度の専門家（ICT 部門の研究開発者ではなく）が多く参加していた。
- フランスとカナダ間の比較に留まらず、欧州と北米のパーソナルデータ保護のアプローチの違いや欧州における米グーグルの問題などにしばしば関わった。

---

47 http://www.centrejacquescartier.com/les-entretiens/entretiens-2015lescolloques/3-la-vie-privee-a-travers-les-cultures-convergences-et-divergences-dans-un-monde-globalise/

48 https://cappris.inria.fr

- フランスからは、INRIA CAPPRIS プロジェクトの研究者の主催で、テレコム・ブルターニュ及びリヨン大学の法学部教授、フランスのパーソナルデータ保護規制機関である CNIL の代表者の他、グーグル・フランス、HP フランスという米企業の代表者がイベントに参加しした。
- 仏 INRIA は情報通信技術部門の研究開発機関であるが、パーソナルデータ保護の学際的な研究に力を入れ始めている（特に CAPPRIS プロジェクト）。

各セッションの概要[49]

パーソナルデータの移転にかかる EU 法の枠組：仏パーソナルデータ保護規制機関 CNIL の代表者

- 原理上、EU 市民のデータを EU 加盟国外へ移転することは禁止されている。だが、移転を可能にする幾つか手段がある。
- 1) 十分性認定：欧州委員会が十分なレベルのパーソナルデータ保護を保証していると認定した国は、EU 加盟国と同じように取り扱うことがある。だが、認定されるために求められる保護レベルはとても高い。また、一度十分性認定を受けても、その後、再び見直されうる。
- 2) EU からデータを十分性認定を受けていない国へ移転する場合、データを移転させる組織（例えば、企業）は、データが十分なレベルで保護されていることを保証しなければならない。
- 3) 例外措置：EU から十分性認定を受けていない国へのデータの移転を限定的な仕方で認める（一時的な措置）。
- 十分性認定について：欧州委員会が第 29 条グループ（G29）[50]に諮問した上で、認定する。G29 が第三国のデータ保護レベルを精査し、意見書を書くが、G29 に認定権はない。
- 十分性認定を受けるには非常に時間がかかる場合がある。ニュージーランドが認定されるには 10 年を要した。
- 十分性認定を受けると、パーソナルデータ保護が基本的人権の一つであることを認めたことになる。パーソナルデータ保護を基本的人権の一つと認めることは、欧州におけるパーソナルデータ保護の特徴の一つである。
- 欧州委員会による十分性認定は、各 EU 加盟国が認定したことも意味する。
- カナダ・ケベック州の例：2014 年に G29 がケベック州のパーソナルデータ保護レベルを調査した際に、G29 は、同州の法制度が、同州へ一度移転されたデータが再移転される場合にも、最初の移転と同程度のデータ保護レベルが保証されなければならないことを明記していないということを指摘した。
- EU 市民は第三国のデータ保護レベルに問題があると考えた時に、司法機関に訴訟を起こすことができる。
- EU パーソナルデータ保護指令の改正案は、データの移転に関して、1995 年成立の現行法とほぼ同じ原理を保持している。

グーグル・スペインの判決に続く検索リストから外れる権利に対する対照的なビジョン：ベルギー・ナミュール大学 法学部教授　セシル・ド・テルワニュ氏

- 2014 年 5 月に、欧州司法裁判所がグーグル・スペインに下した判決を例にして、「検索リストから外れる権利[51]」に係る問題を概観する[52]。

[49] EU のパーソナルデータ保護法制度に関係するセッションの概要についてのみ記す。
[50] G29 とは、現行の EU パーソナルデータ保護指令の第 29 条で設立が決定された組織であり、各 EU 加盟国のパーソナルデータ保護規制機関からなる集合体のこと。

- 事件の内容：2010 年に、スペイン人マリオ・コステハ・ゴンザレス氏が、スペインのパーソナルデータ保護規制機関に、自分について書かれた報道記事（未払い社会保険料徴収のために差押・不動産競売手続が行われるという内容の記事）を消去あるいは修正するように、その記事を掲載している報道サイト管理者に求め、また、その記事を消去あるいは隠すように検索エンジンサービスを提供しているグーグル・スペイン社と米グーグル本社に申し立てを行った。スペイン当局は、報道サイト管理者への訴えは退けたが、グーグル両社にはゴンザレス氏のパーソナルデータをデータインデックスから削除し、その記事を検索できないように措置を取ることを命じる決定を下した。両社はこの決定に対して、スペインの裁判所に不服申し立てを行った。他方で、スペインの裁判所は、審理の過程で欧州司法裁判所に意見照会を求めたが、2014 年 5 月、欧州司法裁判所はスペインのパーソナルデータ保護規制機関の決定を認める判決を下した。
- 画期的な判決：この欧州司法裁判所の判決は、個人が検索サービス提供業者に対して、自分の名前から検索エンジンで情報を検索してもその検索結果が表示されないように求める権利を認めたものであり、非常に画期的である。
- インターネット上のパーソナルデータの特徴：第一の特徴は、人間の記憶と違い、永遠に存在し続けることであり、消去するためには意志・決定が必要であることである。第二に、検索エンジンは、ある個人のパーソナルデータを個々の文脈から引き離しながら、並置しその個人のポートレイト（人物描写）を作ってしまうことである。これらの点が、2014 年 3 月のグーグル・スペインへの判決につながっている。
- 欧州司法裁判所の判決は専門家を驚かせるものであった：1) 同判決では、EU 法が米グーグル社のスペイン子会社であるグーグル・スペインだけでなく、アメリカで検索エンジンサービスを提供している米グーグル本社にも適用されたから。2) 原告の記事を掲載している報道サイトの管理者ではなく、報道サイト管理者と独立してデータを管理しているグーグル社に判決が下されたから。
- 重要な点：欧州司法裁判所がパーソナルデータ管理者を法のもとに処罰したのではなくて、ある個人が自分の意思で訴訟を起こしたことである。検索リストから外れる権利とは、自分のパーソナルデータ利用を自分で決定する権利を意味する。
- 検索エンジンの問題：過去の情報はインターネットから消えないので、検索エンジンは個人のポートレイトを過去の情報のみによって構成する。そして、過去の情報のみで、他者にその人物を判断させてしまう。だが、個人をその個人の過去に還元することは問題がある。なぜなら、個人は過去と比べて、変化発展していくことが可能であるからである。グーグル・スペインの事件の場合、原告の差押等の問題は決着してから長い時間が経過しており、原告の現在の情報として適切性を失っていると考えらえる。
- バランステスト：欧州司法裁判所の判決はバランステストの結果である。つまり、グーグル社の経済的利益と検索エンジンがユーザにもたらす情報にアクセスする利益よりも、原告のパーソナルデータの保護（検索エンジンによって構成される原告のポートレイトが引き起こしかねない問題を防ぐこと）が優越すると判断した結果である。
- EU パーソナルデータ保護指令の改正原案では、第 17 条が「忘れられる権利（right to be forgotten）」を定めていたが、その後の審議過程で、「消去権（right to erase）」という文言

[51] 検索リストから外れる権利とは、検索エンジンに利用されている検索リストから外れる権利（right to delisting）のこと。同権利については、CNIL の以下のサイトも参考のこと。
http://www.cnil.fr/linstitution/actualite/article/article/questions-on-the-right-to-delisting/
[52] http://curia.europa.eu/juris/document/document.jsf?docid=152065

に訂正された。個人がデータの消去を求める権利を保証する消去権は、検索リストから外れる権利と強く結びついている。

検索リストから外れる権利の行使に対する検索エンジン提供事業者の観点：グーグル・フランス 法務部門責任者 マリア・ゴンリ氏

- 2014 年 5 月にグーグル・スペインに下された欧州司法裁判所の判決以来、グーグルは非常に多くの人の要求を受け、彼らの名前から同社の検索エンジンで情報を検索しても結果が現れないようにする措置を取らなければならなくなった。
- グーグルは、2014 年 5 月の欧州司法裁判所の判決以来、多大な物的、人的負担を負っている。グーグルは 100 人以上の法律家を雇い、欧州の検索リストから個人の名前を外すことを求める要求について、ケース毎に検討している。なぜなら、欧州司法裁判所の判決によって、検索サービス事業者は、削除が公的利益に反しない限りにおいて、要求があった個人の名前を検索リストから削除しなければならなくなかったからである。グーグルはいわば判事の役割を担わなければならず、欧州全体で 32 万件の要求を受け、100 万ページ以上のウェブサイトを 1 ページづつ分析しなければならなかった。
- 要求のケースは比較的単純なものもあれば、複雑なものもある。例えば、政治家の要求を受け付けることは公的利益に反する場合があるので（選挙前に選挙人が政治家の情報をインターネットで知ることができることは公的利益と考えられる）、要求を棄却した。公的職務についていない場合でも、例えば、医療業務についている者の情報は公的利益があると考えられないわけではない。こうして、グーグルは、検索リストからある個人の名前を外すことが公的利益に反しないかどうか判断する作業に多大な労力を支払っている。
- 問題は、2015 年 5 月、グーグルが措置を欧州地域（google.uk や google.fr.などの欧州諸国向けの検索リストから個人の名前を外す）に限定して講じていたことに対して、CNIL は措置が十分であると判断せず、グーグルに全世界の地域で同様の措置をとるように命じたことである。
- 2015 年 7 月、グーグル社は CNIL に対して、異議申し立てを行った。だが、2015 年 9 月、結局 CNIL はこの申し立てを棄却している[53]。
- グーグルが CNIL に合意できない理由は、欧州司法裁判所の判決は普遍的なものではないから、そして、CNIL は情報を求める人の関心を考慮していると考えられないからである。

結論：仏パーソナルデータ保護規制機関 CNIL 議長 イザベル・ファルク＝ピエロタン氏

- 現在、デジタル技術の発展が著しく、経済、法律、社会の新しい次元が生まれているが、データはこの変化の中心にある。過去のパーソナルデータ保護の状況と異なる点は、データの移転が世界規模でなされていることである。このような状況では、パーソナルデータ保護のアプローチは、国際レベルと地域レベルを結びつけて考える必要がある。以上のため、5 つの方途がある。
- 1) すでに幾つかの規制制度がある：世界人権宣言の第 12 条はプライバシーの保護を定めているし、欧州レベルでは、欧州連合基本憲章でパーソナルデータの保護が規定されている。さらに、各国のパーソナルデータ保護規制機関は、これらの共通原理から出発し、2009 年にスペイン・マドリッドで開催された「国際データ・プライバシー保護規制機関会議」[54]

---

53 http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-met-en-demeure-google-de-proceder-aux-dereferencements-sur-toutes-les-extensions-du-mote/
http://www.cnil.fr/linstitution/actualite/article/article/droit-au-dereferencement-rejet-du-recours-gracieux-forme-par-google-a-lencontre-de-la-mis/

54 http://www.privacyconference2009.org/home/index-iden-idweb.html

において、欧州国以外の国とともに、パーソナルデータ保護制度の世界共通標準を策定した。この共通標準は、現在実際にはその大部分が機能していないが、今後再び見直される可能性がある。

- 2) 各国、各地域のパーソナルデータ保護のアプローチを混合させること：欧州と北米のパーソナルデータ保護アプローチは異なると言われているが、実際にはすでに混合が進んでいる。例えば、プライバシー・バイ・デザインの採用義務が EU パーソナルデータ保護指令改正案に盛り込まれているが、元々プライバシー・バイ・デザイン原則はカナダに由来するので、この点では欧州の法制度と北米のアプローチは混合していると言える。だが、欧州のパーソナルデータ保護アプローチの特徴を見失ってはならない。欧州の特徴とは、パーソナルデータ保護が基本的人権の一つとして規定していることであるが、プラグマティズムやイノベーションの名の下に、この基本的人権という側面をないがしろにしてはいけない。基本的人権を、消費者という次元で考えてはいけない。
- 3) 各地域のパーソナルデータ保護制度を平和的に共存させること：2013 年に、EU はすでに APEC 加盟国と両地域間のデータ移転システムについて協議を開始している。これは異なる法制度を共存させる試みである[55]。
- 4) 世界的な規模でパーソナルデータ保護規制を行うこと：世界各国の関係組織が協議し、協働でき、最終的に世界規模でパーソナルデータ保護を主導する機関を設立すべきである。これはまさに国際データ・プライバシー保護規制機関会議[56]が挑戦していることであり、同会議への参加国は増加している。最終的には、国際連合の一機関としてパーソナルデータ保護規制機関を設立すべきであり、そこで国際データ・プライバシー保護規制機関会議は中心的役割を担うことができる[57]。
- 5) 市民社会の抵抗：5、6 年前までは、パーソナルデータ保護は民間企業と規制機関が協議することによって進められてきたが、最近になって、市民社会というアクターが登場した。これは大きな変化である。例えば、2015 年 10 月、EU とアメリカ間のデータの移転について定めたセーフハーバー協定[58]に欧州司法裁判所によって無効判決が下されたばかりだが、これに対して、アメリカ内の市民団体がセーフハーバー協定と同じような協定を結んでも無駄であり、データ移転に係る協定には大きな変更が必要であると米政府に申し出ている。これはまさに G29 が米政府に望んでいることと同じであり、G29 の要求を米市民団体があと押していると言える。数年来、このような市民社会のミクロな抵抗が顕著に見られるようになってきている。
- 欧州の役割：現在、社会のセキュリティの向上を求める声が高まっており、パーソナルデータ保護と国内治安のトレードオフ（一方を重視すると他方が軽視される）が議論されているが、このようなトレードオフの議論は、セキュリティと自由の関係を考える上でとて

---

[55] http://www.apec.org/Press/News-Releases/2013/0306_data.aspx

[56] https://icdppc.org

[57] CNIL 議長イザベル・ファルク＝ピエロタン氏は、国際データ・プライバシー保護規制機関会議の理事会のメンバーの一人である。

[58] セーフハーバー協定とは、EU と米国間のパーソナルデータの移動を可能にする協定である。同協定は、セーフハーバー原則を遵守すると自己宣言する米企業には、十分なレベルでパーソナルデータの保護を行っていることを認めてきた。だが、元米諜報機関のエドワード・スノーデン氏の暴露によって、アメリカで処理されている EU 市民のフェイスブックの情報が米諜報機関によって監視されていることが明らかになり、アメリカで十分なレベルで EU 市民のパーソナルデータが保護されていないとオーストリア市民が訴えていた。2015 年 10 月に欧州司法裁判所がセーフハーバー協定に対し無効判決を下し、EU と米政府の間で新たな協定を締結するため、現在交渉が続けられている。
http://www.export.gov/safeharbor/
https://safeharbor.export.gov/list.aspx
http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

も貧しいものであり、人間の自由が場合によって変化しうると前提されている。セキュリティを高めながら、自由も確保しなければならない。このような状況において、欧州は、世界のパーソナルデータ保護政策を牽引できると考えられる。なぜなら、欧州にトレードオフという北米のプラグマティックな議論を取り入れることは可能であるが、それと同時に、欧州ではパーソナルデータ保護が基本権としてみなされており、トレードオフの議論を超えてパーソナルデータ保護政策が検討されているからである[59]。パーソナルデータ保護を基本権とみなすことがデジタル社会の市民には絶対的に必要であり、また望まれている。

第二節　イベント視察報告書 /「国際条約と協定におけるパーソナルデータ」

2016 年 1 月、フランスのパリ市で EU の代表者が、パーソナルデータ移転に係る国際協定について意見を述べるイベントが開催された。2015 年 10 月の欧州司法裁判所が EU と米国間のパーソナルデータ移転を規制するセーフハーバー協定を無効とし、今後の動向が注目されていた。第 29 条グループ議長（WP29）であるイザベル・ファルク＝ピエロタン氏は、米国との協議において、EU と米国間で妥協案を探すことを基本的に否定しており、EU は米国に対してだけでなく、日本を含めた、他国に対しても同様の方針で臨むことが容易に推測できる。

- 場所 : フランス・パリ
- 日程 : 平成 28 年 1 月 8 日（金）午後 1 時〜
- 主催 : 鉱業・テレコム研究院 パーソナル情報の価値と政策研究講座[60]
- スピーチ・パネル参加者 :
  - 欧州議会議員 市民的自由・司法・内務委員会（LIBE）: クロード・モラエス氏
  - 欧州委員会司法総局基本的権利・連合市民権担当 : ポール・ネミッツ氏
  - CNIL 議長兼第 29 条グループ議長（WP29）: イザベル・ファルク＝ピエロタン氏

<u>全体の概要</u>

- 欧州議会議員、欧州委員会担当者、仏パーソナルデータ独立保護規制機関 CNIL と WP29[61] の議長を兼任する ファルク＝ピエロタン氏が、パーソナルデータ移動の国際協定について意見を表明し、欧州の立場を示した。
- パーソナルデータの移動に関する国際協定に関しては、2015 年 10 月、欧州司法裁判所が EU と米国間のパーソナルデータの移転について定めたセーフハーバー協定に無効判決を下した。その後、欧州委員会と米政府の間で新協定について交渉が進められ、2016 年 2 月 2 日には、EU と米国間でパーソナルデータ保護の新しい国際協定（「EU-US プライバシー・シールド」）が締結されている。
- セーフハーバー協定とは、EU と米国間のパーソナルデータの移動を可能にする協定である。同協定は、セーフハーバー原則を遵守すると自己宣言する米企業には、十分なレベルでパーソナルデータの保護を行っていることを認めてきた。だが、元米諜報機関のエドワード・スノーデン氏の暴露によって、米国で処理されている EU 市民のフェイスブックの

[59] 報告者注 : CNIL のファルク＝ピエロタン氏は、パーソナルデータ保護を基本的人権の一つとして考えるならば、セキュリティとパーソナルデータ保護間のトレードオフの議論が成立しないと考えている。
[60] テレコムを含む工学系高等教育兼研究開発機関である鉱業・テレコム研究院に設置された同講座（2013 年創設）は、パーソナルデータの利活用に係る学際的な研究（コンピュータ科学、経済、法律、倫理など）を行っている。
[61] WP29 とは、現行の EU パーソナルデータ保護指令の第 29 条で設立された組織であり、各 EU 加盟国のパーソナルデータ保護規制機関（DPA）からなる集合体のこと。

情報が米諜報機関によって監視されていることが明らかになり、米国では十分なレベルでEU 市民のパーソナルデータが保護されていないとオーストリア市民が訴えを起こしていた。この訴えに対して、欧州司法裁判所はセーフハーバー制度に無効判決を下した。

スピーチの概要[62]

CNIL 議長兼第 29 条作業グループ（WP29）議長：イザベル・ファルク＝ピエロタン氏

- 2015 年は欧州司法裁判所によるセーフハーバー協定の無効判決を含め、パーソナルデータ保護に関して激動的な一年であった。
- データ移動の国際協定について議論するとき、まず 3 つの点を考慮しなくてはいけない。1) パーソナルデータ保護は、デジタル社会の発展によって国内レベルで解決可能な問題ではもはやない。2) 多くの EU 市民が非欧州国企業、特に米企業のオンラインサービスを消費しており、そのため、EU 市民のパーソナルデータが米国に移転され、分析・処理されている。3) パーソナルデータ保護に対するアプローチは文化と政治によって決定されており、各国、各地域によって異なる。欧州と米国では異なるデータ保護アプローチを採用している。欧州では、パーソナルデータ保護は基本的人権の一つして考えられているが、米国ではむしろ消費者保護として考えられる傾向がある。
- これらの 3 つの点を合わせて考えれば、各地域のデータ保護制度の間で衝突が起こるのも不思議ではないことがわかる。
- 2015 年は、このような法制度間の衝突が絶えなかった。例として、「忘れられる権利」と「検索リストから外れる権利」に関わる米グーグル社との訴訟[63]、そして、10 月の欧州司法裁判所セーフハーバー協定の無効判決を挙げることができる。
- 2015 年 10 月にセーフハーバー協定無効に係る判決[64]で、欧州司法裁判所は、EU 基本権憲章を判断の論拠の中心に置くアプローチを取った。その結果、同裁判所は、EU 域外へのデータ移転は EU 基本権憲章に違反してはならず、EU 加盟国のパーソナルデータ保護規制機関（以下、DPA とする）は違反がないように、データ処理を監視、規制しなければならないとした。これは、公共安全を目的とする国外の諜報機関によるデータ処理の場合に関しても同様である。
- 欧州司法裁判所のセーフハーバー協定無効判決の理由は、米国で EU 市民のパーソナルデータが十分な保障なく処理されており、EU 基本権憲章に違反しているからというものである。

---

[62] 欧州の欧州委員会司法総局基本的権利・連合市民権担当 ポール・ネミッツ氏と CNIL 議長兼第 29 条グループ議長（G29）イザベル・ファルク＝ピエロタン氏のスピーチとディスカッションの要点のみを記す。

[63] 2010 年に、スペイン人マリオ・コステハ・ゴンザレス氏が、スペインのパーソナルデータ保護規制機関に、自分について書かれた報道記事（未払い社会保険料徴収のために差押・不動産競売手続が行われるという内容の記事）を消去あるいは修正するように、その記事を掲載している報道サイト管理者に求めるとともに、その記事を消去あるいは隠すように検索エンジンサービスを提供しているグーグル・スペイン社と米グーグル本社に申し立てを行った。スペイン当局は、報道サイト管理者への訴えは退けたが、グーグル両社にはゴンザレス氏のパーソナルデータをデータインデックスから削除し、その記事を検索できないように措置を取ることを命じる決定を下した。両社はこの決定に対して、スペインの裁判所に不服申し立てを行った。他方で、スペインの裁判所は、審理の過程で欧州司法裁判所に意見照会を求めたが、2014 年 5 月、欧州司法裁判所はスペインのパーソナルデータ保護規制機関の決定を認める判決を下した。

[64] http://www.export.gov/safeharbor/
https://safeharbor.export.gov/list.aspx
http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

- 欧州司法裁判所の判決の背後にあるEUパーソナルデータ保護法のEU域外への適用を正当化する法的論拠は何か。主な論拠は、 EU市民のデータはEU域内で産出され、EU域内で基本権によって保護されているが、そのデータはそれが消滅するまで同じ仕方で保護されなければならず、それは域外にデータが移転されても同様であるというものである。つまり、データの移転に合わせて、データ保護も移動しなければならないという論拠である。
- EUはセーフハーバー協定、十分性認定等のパーソナルデータのEU域外への移転を規制する非常に複雑な措置を定めているが、これらの措置を利用しなくてはEU域外へのパーソナルデータの移転は許可されない。だが、このような措置を望む声は世界各国にある。現在、パーソナルデータが公共機関、民間企業によって処理されており、それを懸念する個人は米国、日本を含め、世界中に数多くおり、EUと同じようなパーソナルデータ処理の規制を望む市民が目覚めつつある。日本では、忘れられる権利の制定について検討しており、また、元米諜報機関職員のスノーデン氏による暴露後では、米企業の中にさえもパーソナルデータ保護の規制（諜報機関によるデータ処理の規制）を望む組織がある。
- パーソナルデータのEU域外への移転に関しては、ケースバイケースの対応も不可能ではないが、実施することは難しい。WP29は法的拘束力を持つ国際協定の策定を検討している。10月の欧州司法裁判所の判決後、WP29はすぐに、米国とEU間のパーソナルデータ移転を規制する政治的、法的な方策（米国におけるEU市民のパーソナルデータ保護のため）を見つけるために、EU加盟国、EU機関、米政府と協議を開始した。
- このような国際的なパーソナルデータ保護規制制度を作る試みは野心的なもののように見えるかもしれないが、新しいものではない。2009年にスペイン・マドリッドで開催された「国際データ・プライバシー保護規制機関会議」[65]では、パーソナルデータ保護制度の世界共通標準が策定されている。また、より最近では（2015年9月）、スノーデン氏による暴露後、犯罪捜査向けに米国とEU間のパーソナルデータ移転を許可し、規制する「アンブレラ協定」[66]も策定されている。
- セーフハーバー協定無効後、米国とEU間のパーソナルデータ移転を規制する制度はいかなるものになるか。様々な可能性があるが、新しい国際協定が商業協定であるだけでなく、米法執行機関によるEU市民のパーソナルデータ処理を規制する仕方についての政治的協定になることは確かである。
- 米国とEU間の溝を埋めるため、パーソナルデータ保護の国際協定を策定するには時間がかかる。だが、このような国際協定は、両地域間に信頼を回復し、市民社会の期待に応えることになる。
- 両地域間の溝を埋めることは、妥協案を考えることではない。EUはEU自身のパーソナルデータ保護制度を持ち、EU市民のパーソナルデータ保護の基礎的な保障を米国に求めているだけである。その保障の仕方は様々なものがあり得るだろう。
- 必要なことは、一種のパーソナルデータ保護に係る国際標準を策定することである。デジタル社会は、各国の国境を越えるグローバルなものなので、必然的に国際的な標準が必要となる。
- 今後のスケジュールとしては、EUは、2016年2月頭までにEUが求めているEU市民のパーソナルデータ保護の基礎的保障について、米国から回答を得るだろう。これは簡単なことはではないかもしれないが、関税などの他の分野では、EUと米国は協定を結んでお

[65] http://www.privacyconference2009.org/home/index-iden-idweb.html
[66] http://www.euractiv.com/section/digital/news/commissions-umbrella-agreement-with-us-under-fire-from-civil-liberties-meps/

り、不可能ではない。もし回答が得られない場合には、EU 域外への EU 市民のデータ移転は停止されるだろう[67]。

- 欧州委員会は米政府とのセーフハーバー協定無効に代わる制度を策定する協議において、EU 側で決定権を有する一方で、DPA は個々の米企業のパーソナルデータ移転を監視する役割を持つ。米企業が EU 市民のパーソナルデータ保護を保障しないならば、DPA はデータ移転を停止できる権限を持つ。
- EU のパーソナルデータ保護のアプローチは、ビジネスの要求と個人の要求の双方に対応するものであり、デジタル社会にとって適したものであると、私は信じている。

欧州委員会法務総局基本権と連合市民権責任者：ポール・ネミッツ氏

- パーソナルデータの経済的効果を強く主張する人が数多くいるが、それは欧州におけるパーソナルデータについての基本的な考え方とは異なる。つまり、データの経済的利便性を主張することは、EU 基本権憲章（第 7 条がプライバシーの保護、第 8 条がパーソナルデータの保護に係る）、また、第二次世界大戦直後に制定された欧州人権条約（第 8 条がプライバシーの保護に係る）の考え方とは沿わない。欧州では、パーソナルデータを保護しなければならないのは、データの利用によって、他の個人をコントロールすることが可能になる危険性があるからと考えられている。こうして、欧州人権条約では、プライバシー保護が基本権として定められている。EU 基本権憲章におけるパーソナルデータ保護は、欧州人権条約の思想を引き継いでいる。
- 米政府との交渉では、新しいデジタル社会において、パーソナルデータ保護という基本権をいかに実現するかが問題となっていると言える。デジタル社会において、自由、自己のデータを自身でコントロールする権利を確保しなければならない。
- しかし、パーソナルデータは、データのほんの一部でしかない。EU 域内では、例えば、スマートメーターなどにより、絶えず大量のデータが生み出されており、これらのデータ利用の経済的潜在性は莫大である。これらの非パーソナルデータの利用は、パーソナルデータ保護とは別の話である。欧州は、非パーソナルデータのビジネスへの利用も考慮している。
- EU のパーソナルデータ保護政策を保護貿易主義と言って非難することは、間違いである。現在、米企業がどれだけ EU のデジタル市場を占有しているかを見れば、EU がどれだけ米企業に開かれているかお分かりになろう。また、新しい EU のパーソナルデータ保護法は、パーソナルデータを利用する事業の届出を EU 域内で簡略化しており、米事業者の負担が減るだろう（ワンストップショップアプローチの採用）。

[67] 2016 年 2 月 2 日には、EU と米国間でパーソナルデータ保護の新しい国際協定（「EU-US プライバシー・シールド」）が締結されている。
http://europa.eu/rapid/press-release_IP-16-216_en.htm