パーソナルデータ利活用時の暗号・情報セキュリティ技術活用の欧州のガイドライン・法制度・標準化動向に関する調査

最終報告書

情報通信研究機構

欧州連携センター

平成 26 年 2 月 28 日

目次

はじめに

調査目的

情報通信技術の進展により、近年、個人に関する情報（パーソナルデータ）を含めた大量の情報（ビッグデータ）の分析による活用が進められているが、同時に、プライバシー面での不安も生じている。このような中、総務省では、「パーソナルデータの利用・流通に関する研究会」[1]を開催し、プライバシー保護に配慮したパーソナルデータのネットワーク上での利用・流通の促進に向けた方策について検討を行っている。

情報通信研究機構（以下、当機構とする）では、「ネットワークセキュリティ研究所セキュリティ基盤研究室」[2]において、現代暗号理論から量子セキュリティまで、実用性を重視した次世代暗号技術を確立する「セキュリティ基盤技術」に関する研究活動を行っている。セキュリティ基盤技術を実用化する際に、取り扱うデータにパーソナルデータが含まれる場合は、システム構築において、データの取扱いについて十分に検討する必要がある。

プライバシー保護に関して、欧州では世界の他の地域に先んじて活発に検討されており、欧州委員会が 2012 年 1 月にデータ保護法の改正提案を行い、今後、ガイドライン等の策定が想定されるが、ビジネス展開を重視する視点が大きい米国とは異なっていると考えられる。このような欧州の動向は、我が国のパーソナルデータの取扱いに係る制度づくりに参考となり得る。従って、欧州の法整備動向、ガイドライン等の策定動向、倫理面を調べるとともに、プライバシーを保護しながら、パーソナルデータをビッグデータ・ビジネスやクラウドサービスにおいて利活用するための欧州における研究開発・標準化動向を調査する。

また、2013 年 6 月 14 日の閣議決定「規制改革実施計画」において「ビッグデータ・ビジネスの普及（匿名化情報の取扱い）」に関し、「個人情報の保護を確保しつつ、ビッグデータ・ビジネスの普及を図る観点から、（中略）どの程度データの加工を行えば「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。）」には当たらない情報となるのか等、合理的な匿名化措置の内容」を明確化するとされている。従って、匿名化・仮名化により個人識別性をなくすことでデータ利活用を進めている実例がないか、その際、技術だけでは非識別化データの利活用や

[1] http://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/
[2] http://www.nict.go.jp/nsri/fund/index.html

他のデータとの連結等により再識別化される可能性は排除できないことから、何らかの制度・運用制限等との組合せで実現されている可能性があることに留意して、欧州の事例を調査する必要がある。

調査研究項目

（1）欧州における暗号・情報セキュリティ技術に関する動向

ビッグデータ・ビジネスやクラウドサービスにおいてパーソナルデータを利活用するにあたって、プライバシーを適切に保護することを可能とする暗号・情報セキュリティ技術の研究開発動向及び標準化の動向

（2）欧州におけるビッグデータにおけるパーソナルデータ利活用に関する取組み

ビッグデータ・ビジネスやクラウドサービスにおいてパーソナルデータを利活用するにあたってプライバシーを適切に保護するために政府が策定している法律やガイドライン、民間企業・業界団体による自主規制、その他上記（1）に該当する技術の利活用に関連する制度についての動向、倫理面の調査

（3）欧州におけるパーソナルデータの利活用に関する事例

ビジネスや公的サービスへのパーソナルデータ利活用事例（特に、匿名化・仮名化等により個人識別性をなくすことで利活用を進めている事例）、パーソナル情報の悪用、個人情報の露出等の事例。利活用事例においては、どのような技術、制度、運用制限等がデータ収集・サービス展開に関わっているかを整理するとともに、日本における制度・文化等がデータ収集・サービス展開の障害になるか分析する。

調査方法

- インターネットや刊行物等の文献調査
- 欧州における有識者へのヒアリング調査
- 関連の ICT イベントの視察及び参加

ヒアリングに関しては、EU オブザーバー紙、英オックスフォードインターネット研究院、仏ビッグデータステークホルダー団体のアライアンス・ビッグデータ、仏パーソナルデータ保護監督機関 CNIL、仏テレコム・パリテックに対してインタビュー調査を実施した（訪問、電話、メールによる）。

ICT イベントとしては、フォーラム・アテネの「PRISM（プリズム）：欧州デジタルの弱さ？」（フランス・パリ）、グーグル社の講演会「技術、革新と自由」（フランス・パリ）、テレコム・パリテック主催の講演会「監視の社会的な大規模受容：ユーザーの受動性に可能な代替え策は何か」（フランス・パリ）、欧州委員会と欧州電気通信標準化

機構主催のイベント「クラウド標準コーディネーション 結果報告」(ベルギー・ブリュッセル)、「コンピューター、プライバシー、データ&保護（CPDP)」(ベルギー・ブリュッセル）に参加した。

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、これらの記事はサイト運営者の都合で随時移動、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。

調査支援組織：ONOSO
住所：2 Boulevard Anatole France, 92100, Boulogne-Billancourt, FRANCE
電話番号：01 46 03 06 53 (フランス国外から: 0033 1 46 03 06 53)
メールアドレス：k.ono@onoso.fr
担当：小野 浩太郎

報告書全体の要約

以下に本報告書全体の要約を記す。詳細な情報に関しては、本文を参考にしていただきたい。

第一部では、欧州連合の第七次枠組計画（FP7）とホライゾン 2020 における暗号・情報セキュリティ技術の研究開発支援動向と研究事例について記した。

FP7 でも、ホライゾン 2020 でも、ICT 部門の中で情報セキュリティ分野は重要な 1 つの研究開発公募テーマとして認められており、多くの予算が割り当てられている。FP7 では、課題 1.4 か課題 1.5 の「信用可能な ICT」で情報セキュリティの研究プロジェクトが募集されている。ホライゾン 2020 では、情報セキュリティの公募枠として、ICT 部門の 2014-2015 年度作業プログラムに「ICT32：ICT サイバーセキュリティ、信用可能な ICT」が設置されている。同公募枠では、研究開発テーマとして、「エンド・ツー・エンドセキュリティのためのセキュリティ・バイ・デザイン」と「暗号」が挙げられている。さらに、研究開発の他、欧州における暗号の共同研究を発展させるプロジェクトも公募されている。

FP7 とホライゾン2020 ICT 部門情報セキュリティ分野の予算

FP7 ICT 部門の情報セキュリティ分野の予算
- 2007-2008 年度作業プログラム：ICT-2007.1.4：「安全で、信頼でき、信用されたインフラ」：予算　9000 万ユーロ
- 2009-2010 年度作業プログラム ：ICT-2009.1.4：「信用可能な ICT」：予算　9000 万ユーロ
- 2011-2012 年度作業プログラム：ICT-2011.1.4：「信用可能な ICT」：予算　8000 万ユーロ
- 2013 年度作業プログラム：ICT-2013.1.5：「信用可能な ICT」：予算　3650 万ユーロ

ホライゾン 2020 ICT 部門の情報セキュリティ分野の予算
- 2014-2015 年度作業プログラム ：ICT32：「ICT サイバー、信用可能な ICT」：予算　3800 万ユーロ予定

プライバシー・バイ・デザイン原則の採用の促しは、2013 年度ICT作業プログラムで顕著になり始め、ICT-2013.1.5：「信用可能なICT」 の他、募集する研究プロジェクトに同原則の採用を促す公募もある（例：ICT-2013.1.4：「信頼できスマートで安全なスマートシティ向けのもののインターネット」）。ホライゾン 2014-2015 年度ICT作業プログラムでは、プライバシー・バイ・デザイン原則の採用がプログラム全体に渡って促されている。なお、欧州委員会のビッグデータ戦略、「欧州データバリューチェーン戦略」では、EUデータ保護法の改正と、「プライバシー・バイ・デザイン」という理念の下、プライバシーを遵守する基礎特徴を持つ技術の開発をホライゾン 2020 では重視することがビッグデータに対するデータ保護の対応策として挙げられている。さらに、EUデータ保護法改正案の第 23 条「デザインとデフォルトによるデータ保護」において、データ管理者はデータ主体の保護を強化する「適切な技術的、組織的措置と手続き」を講じなければならないとされており、同法の改正により、プライバシー・バイ・デザイン原則の採用が強く促される見込みである。

FP7 には、情報セキュリティに係る研究プロジェクトが数多くある。例えば、暗号研究のプロジェクト「ECRYPT Ⅱ（2008 年 8 月～2013 年 1 月（54 ヶ月間）：408 万ユーロ（EU 拠出分：300 万ユーロ）：コーディネーター：ルーバン・カトリック大学（ベルギー））」、プライバシー・バイ・デザイン原則の採用を促進する研究プロジェクト「PRIPARE（2013 年 10 月～2015 年 9 月（24 ヶ月間）：131 万ユーロ（EU 拠出分：109 万ユーロ）：コーディネーター：トリアログ（仏））」、

データ管理の法的ツールセットを開発する「ENDORSE（2010年9月～2013年2月（30ヶ月）：367万ユーロ（EU拠出分：274万ユーロ）：コーディネーター：ウォーターフォード技術研究院（アイルランド)）」、クラウドコンピューティングのセキュリティを高める「PRACTICE（2013年11月-2016年10月（36ヶ月間）：1046万ユーロ（EU拠出分：755万ユーロ）：コーディネーター：テクニコン（独)）」等、研究内容も様々である。なお、PRIPAREプロジェクトは、プライバシー・バイ・デザインが現在データ保護の理論的なコンセプトではなく、どのように市場リーダーや規制機関がこの原則を実際に取り入れるか証明する段階にあることを受けた研究プロジェクトであり、EUデータ保護改正法との結びつきが強い。同プロジェクトには助言者として、プライバシー・バイ・デザイン原則を開発したカナダのオンタリオ情報・プライバシーコミッショナーオフィスのアン・カブーキアン氏が参加している。

第二部では、欧州における暗号・情報セキュリティ技術に関する標準化の動向について調査した。特に、欧州委員会と欧州の電気通信部門の標準化団体である欧州電気通信標準化機構（ETSI）が共同で実施したクラウド標準コーディネーションについて調査を行った。欧州委員会は2012年9月に「欧州におけるクラウドコンピューティングの潜在性の解放」という通達を発表し、欧州クラウドコンピューティング戦略を規定しているが、そこでは、セキュリティ、パーソナルデータ保護、信用という点が問題となっている。問題の1つとして標準の錯綜を挙げており、優先事項として、クラウドコンピューティングに対する信頼を発展させるために既存の標準を展開させるため、関係する標準を特定し、コンプライアンス認証（certification）することが必要であるとしている。このため、2012年12月、欧州委員会とETSIは「クラウド標準コーディネーションイニシアチブ（Cloud Standards Coordination：CSC)」を立ち上げ、2013年11月に発表されたCSCの最終報告書には、現在のクラウドコンピューティングの標準と技術仕様のリストが収録されている。

第三部では、欧州におけるパーソナルデータ利活用に係る制度整備の動向について記した。欧州においてパーソナルデータ保護に係る法制度はいくつもあり、欧州人権条約第8条、欧州評議会条約第108号、EUデータ保護指令、EU基本権憲章第7条と第8条、電子通信部門におけるプライバシー指令があり、人権とパーソナルデータの保護は切り離して考えられていない。なお、欧州諸国のデータ保護法はこれらの法律を遵守する仕方で、制定されている。

EU圏におけるパーソナルデータ保護に関して、現行の最も重要な法制度はEUデータ保護指令であり、この法律はEU圏にパーソナルデータ保護に係る共通の法枠組みを提供している。同法は、個人のプライバシー保護とEU圏内のパーソナルデータの自由な移動の間でのバランスを取ることを目的としており、パーソナルデータの収集と利用を制限し、各加盟国にデータ保護を所管する独立機関を設置することを要求する。同法は、パーソナルデータ保護に係るガイドラインを定めており、パーソナルデータの定義、収集と処理の目的、同意、データの特殊なカテゴリーの規定（人種や政治的見解等)、アクセス権、異議権、法的救済、監督機関への通知義務、第三国への移動、独立監督機関の設置義務、第29条作業部会の設置等について定められている。なお、同法は、匿名化されたパーソナルデータには適用されないとされている。

EUデータ保護指令は、2012年1月に改正案が欧州委員会により提案され、現在改正のため欧州連合理事会で審議が行われている。改正理由として、欧州委員会は、同法が「指令」という法的地位のため、EU各国が同法をそれぞれの仕方で国内法化し、EU圏全体で同程度のパーソナルデータ保護を実現できていないこと、急速な技術発展とグローバリゼーションがパーソナルデータ保護に関して新しい課題を惹起しており、デジタル時代に適応する新しい規則を定める必要があることを挙げている。このため、個人が自分のパーソナルデータをよりコントロールできるようにするとと

もに、EU域外も含め、パーソナルデータの保護を確保する必要がある。以上の改正の理由に加えて、同法の改正による経済的効果も想定されている。2011 年 6 月の欧州委員会の調査発表では、欧州に住む 7 割の人々は自分のパーソナルデータが誤って利用されることを懸念しており[3]、オンラインサービス等への信用を増加することで、デジタル経済一般（EU単一市場の刺激と成長促進、雇用創出、技術革新の促進）を成長させることができると考えられる。

改正のポイントとしては、法の地位を「指令（Directive）」から「規則（Regulation）」へと格上げすること、本人の明示的な同意の取得義務、アクセス権とデータポータビリティ権利の保証、忘れられる権利、各国のデータ保護監督機関の独立性と権限の強化、データ保護権利が侵害された時の行政及び司法措置を強化（罰金金額の増加）、データ漏洩の通知義務、データ保護オフィサーの指名義務、プライバシー・バイ・デザインの原理の採用、ワン・ストップ・ショップシステムの設置、パーソナルデータ保護法の第三国に設立されたデータ管理者に対する適用（EU圏内に在住する個人のデータを非EU圏で設立されたデータ管理者が処理する場合も同データ保護法の対象になる）、欧州委員会による十分性決定（adequacy decision）の明確化、十分性決定によってカバーされていない国々への国際移転規則を拘束的企業準則（Binding Corporate Rules）等による強化等がある。なお、改正法案においても、同法は匿名化されたパーソナルデータには適用されないとされている。

EUデータ保護法改正案は欧州議会での審議と修正（4000 カ所）を経て、2013 年 10 月 21 日に可決されている（賛成 51 票、反対 1 票、棄権 3 票）。欧州議会による修正は基本的に欧州委員会の原案に沿っており、データ保護をさらに強化するものであった。欧州議会の採決後、各国の閣僚からなる欧州連合理事会へと審議の場が移っているが、改正プロセスは現在進んでいない。2013 年 10 月の欧州議会による可決の時点では、2014 年 5 月に実施予定の欧州議会議員選挙の前に最終的な法案可決が望まれていたが、2015 年にずれ込む可能性が高い[4]。なお、現行のデータ保護指令の成立には 5 年が費やされている。改正法案の問題点としては、EU機関がEUデータ保護法の対象外であること、ワン・ストップ・ショップメカニズムの定義の曖昧さ、複雑さが挙げられている。また、ドイツは公共部門を同法の対象外することを望み、また、英国、スロベニア、デンマーク、ハンガリーが、規則（regulation）という法的地位で提案された法案を指令（directive）へと修正しようとしており、改正プロセスを遅滞させている国がある。

欧州諸国に目を移すと、英国では、1995 年成立の EU データ指令の国内法化に伴い、1998 年に「データ保護法（Data Protection Act）」が成立し、同法に則り、ICO（情報コミッショナー事務局）が監督機関として活動している。データ保護法の範囲外に入らないパーソナルデータの匿名化に関して、同機関は、2012 年 11 月に他国に先駆けて、「匿名化：データ保護リスク管理実践規定」という匿名化に係る実践ガイドブックを発表している。同規定は、匿名化に係る諸問題を説明し、推奨される実践を示して、パーソナルデータを匿名化する必要がある組織（官民、第三セクター）を支援することを目的としており、合計 100 ページ以上に昇る包括的な実践ガイドブックであるが、匿名化の手段について法的拘束力を持つ規則を規定しているわけではない。また、ICO はマンチェスター大学、サウサンプトン大学、オープンデータ研究院、国立統計学庁と提携し、パーソナルデータの匿名化について情報提供を行うために、UKAN（UK ANONYMISATION NETWORK）を設立している。UKAN は ICO が作成した「匿名化：データ保護リスク管理実践規定」の実践を具体的に支援している。このように、英国では ICO が匿名化に関する実践規定を作成するとともに、UKAN という組織が詳しい情報提供の役割を担っている。

ICOの匿名化ガイドブックでは、パーソナルデータに係るリスクの種類、匿名化とパーソナルデ

[3] http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en
[4] http://euobserver.com/justice/122853

ータの定義、匿名化されたデータの特徴、匿名化の利点、同意等の基本事項について説明されている。匿名化されたデータは英データ保護法の範囲外であり、匿名化されていれば、データを収集した際の目的とは異なる仕方でデータを利用できるとされる一方で、匿名化されていても、個人の再特定は複数のデータを組み合わせれば可能であるので、常に再特定の可能性は排除できず、そして予見不可能であることが指摘されており、また、空間位置情報（GPSデータ等）に関しては、ある幾つかの状況ではこの種の情報はパーソナルデータとなりうるが、そうではない場合もあるので、単純な規則は存在しないとされている。このような場合、事例の状況に基づいたふさわしい判断が必要となる。

英オックスフォード・インターネット研究院[5]では、ビッグデータの研究開発が積極的に行われているが、同研究院では、倫理委員会がプライバシー保護の方針とパーソナルデータの管理をチェックしている。また、匿名化は非常に重要なものと考えられており、取扱いに慎重を要するデータに関しては、データからいかなる個人情報も再特定化され得ないように、匿名化の後でさえも暗号がかけられ、分離されて保存されている。

フランスでは、CNIL（情報と自由国家委員会）がフランスにおけるパーソナルデータ保護監督機関として積極的に活動している。同機関は「情報と自由に係る 1978 年法」（以下、情報と自由法と略す）に基づき、データ保護に係る活動を実施している。CNILはパーソナルデータ保護担当者を企業や研究機関等の組織内に設置することを促しており、その担当者は「CIL（Correspodant informatique et libertés）」と呼ばれる。組織はCILを設置することにより、CNILとのやり取りを簡便化する等の利点がある。CNILは、2012 年 6 月に「私的生活のリスク管理」と呼ばれるパーソナルデータ保護に係るガイドブックを発表しており、匿名化に関して、推奨する実践方法について記されているが、拘束力のあるものではない。CNILが匿名化の手段や方法を強制することはなく、各企業はそれぞれ匿名化に対応しなければならない。CNILはパーソナルデータの管理に関して、対象となる組織の調査を行っているが、調査の際に匿名化の方法が情報と自由法に触れないかどうか精査している。逆に、企業から匿名化の方法に関して、助言を求められた場合にはそれに対応している。また、CNILは、2012 年 1 月に発表された米グーグル社の新プライバシー・ポリシーが情報と自由法に違反しているとして、2014 年 1 月 8 日に 15 万ユーロの罰金を課している。なお、CNILは仏ICT部門研究機関INRIA等と提携し、プライバシー・バイ・デザイン原則を実現する新しいデータ保護技術の開発にも参加している[6]。

フランスでは、CNILの他、AECDPというCILとパーソナルデータの利活用に係るステークホルダーからなる団体が自主的に匿名化措置の基準を作成しており、また、アライアンス・ビッグデータというビッグデータのステークホルダー団体が、「ビッグデータ倫理憲章」という匿名化に係る倫理面でのチェックリストを作成している。アライアンス・ビッグデータは倫理憲章をさらに発展させ、この憲章に明記された諸基準を遵守している企業のために「ラベル」を作成することを目指している。

フランスの電気通信部門の高等教育・研究機関であるテレコム・パリテック[7]では、ビッグデータの将来的な重要性を考慮し、2013 年より同技術に関して幾つもの講座を開設している[8]。大きな特徴は、民間企業と提携して研究開発を行うとともに、研究開発以外の側面、すなわち、個人情報保護等の法・政治的側面や経済的側面についても講座を開設し、ビッグデータの研究及び利活用を包括的に発展させる試みが行われていることである。

[5] http://www.oii.ox.ac.uk/research/
[6] http://www.inria.fr/equipes/privatics
[7] テレコム・パリテックは、鉱業・テレコム研究院の一機関である。
[8] http://www.telecom-paristech.fr/recherche/chaires.html

パーソナルデータの匿名化の手段に関しては、両国とも法的拘束力を持つ詳細な諸規則を定めているわけではない。

第四部では、欧州におけるパーソナルデータの利活用に係る事例について記した。まず、欧州の事例として挙げられるのは、英政府や仏政府が実施しているオープンデータ政策である。両政府は、それぞれ2010年1月と2011年12月にポータルサイト（data.gov.ukとdata.gouv.fr）を立ち上げており、公共機関が保持している情報を公表している。両サイトでは、パーソナルデータは匿名化されて、公表されている。なお、フランスのオープンデータ政策の大きな特徴は、2013年12月にポータルサイトが大きく変更され、公共機関等が情報を公表する他に、市民等もデータを公表することができるようになったことである。また、CNILはオープンデータ政策担当者とワークショップを開催し、パーソナルデータの利用に関し意見交換を行っている。ついで、ビッグデータは世界中で現在最も注目を集めている技術であり、欧州でも非常に多くの企業が設立され、様々な分野へデータ分析サービスを提供している。通常企業は、EUデータ保護法に基づく各国の法律を遵守しなければならず、また、パーソナルデータを利用する場合には、データを匿名化する必要がある。だが、ビッグデータ企業のウェブサイト上で、パーソナルデータの匿名化について詳しく説明する企業は少ない。以上の他、移動通信事業者は顧客の移動データを匿名化し、統計データへと変換して、企業や公共機関向けに移動情報を分析するサービスを提供している。仏通信事業者オレンジもスペインの事業者テレフォニカも同種の類似するサービスを提供しており、適用例としては、観光や小売サービスの改善等が考えられている。また、オレンジはアフリカ西部のコートジボワールで、同国の社会経済の発展のために電話の通信データを匿名化して開放し、研究に利用するプロジェクトを実施している。

パーソナルデータの悪用と漏洩に関しては、ICO及びCNILのウェブサイトに詳しく事件の経緯が公表されている。デートサイトによるデータ保護法の違反、ネットワーク型ビデオゲームからのパーソナル情報の漏洩、通信事業者のパーソナルデータ漏洩、医療施設における患者医療データの取扱不備、顧客の銀行情報保存の不備に係るオンラインショッピングサービス事業者への警告、従業員が有するデータへのアクセス権利の拒否等が挙げられている。これらの事例は、ICOとCNILの具体的な活動を知り、日本における制度や文化等が欧州でデータ収集・サービス展開の障害になるか理解するのに有用である。

以下に、英国とフランスにおけるパーソナルデータの悪用と漏洩事例のポイントをまとめる。

- （英）いわゆる出会い系サイトと言われるサービス業者によるデータ管理が不透明であった → パーソナルデータを管理する企業は様々であり、出会い系サイトもその中に入る
- （英）サイバー攻撃によりネットワーク型ビデオゲームのパーソナルデータが漏洩したが、その規模が大きく、漏洩したデータの内容も重要で、極めて深刻であった → サイバー攻撃には常に警戒する必要がある
- （仏）移動通信事業者がフィッシング詐欺に合い、顧客のパーソナルデータが流出した → パーソナルデータの漏洩事件が生じた場合には、法律に則り、漏洩の事実が発覚後、すぐにパーソナルデータ保護監督機関と侵害にあった顧客に通知する義務がある
- （仏）医療施設の患者データの第三者による閲覧 → 医療情報という特に秘匿されるべきデータを第三者組織が閲覧する場合には、匿名化することが必要である
- （仏）オンラインショッピングサイトの銀行情報の取扱不備 → 銀行情報の取扱いには高いセキュリティを確保することが必要となる上、オンライン決済の簡略化ために、銀行情報を保存するには顧客の同意が必要である
- （仏）雇用者の従業員が有するデータアクセス権の拒否 → 雇用者は従業員が自分のパーソナルデータへアクセスすることを要求する場合には、そのデータを開示しなければならない

以上の事例では、サイバー攻撃の他、パーソナルデータ保護の法制度に関しては、パーソナルデ

ータの管理の透明性、データ漏洩の通知義務、データの匿名化、同意の取得義務、データへのアクセス権が問題となっている。日本の企業がパーソナルデータ保護の管理と処理に係る事業を行う場合には、これらの点に注意する必要がある。

第五部では、欧州における米諜報機関の活動を巡る動向について記した。2013 年 5 月以来、元CIA（米中央情報局）職員エドワード・スノーデン氏によって告発された米諜報機関NSA（国家安全保障局）の通信傍受活動は、特にその規模の大きさから世界各国で大きな批判的な反響が起こり、欧州諸国でも盛んに報道されている。欧州委員会が作業部会を米政府機関と設立し、正式に協議するとともに、欧州各国では、法律家やICT研究開発者等が集まり、同問題について議論されている。EUと米国間の作業部会では、第一に、米国の諜報プログラムが実際に存在すること、第二に、そのプログラムに対する米国民と欧州市民の間にデータ収集の範囲や権利の保護に関して格差が存在すること、第三に、外国情報活動監視裁判所や支援する企業には秘密事項が多く、パーソナルデータの収集と処理について情報を与えられる法的あるいは行政的手段が米国民にもEU市民にもないことが明らかになった。米諜報プログラムの法的基盤としては、同作業部会によって、外国情報監視法（FISA）の第 702 条、米国愛国者第 215 条、大統領令第 12333 号が特定されている。2014 年 1 月 17 日、米オバマ大統領がNSAの諜報活動の見直しを発表しているが、それに対して、欧州委員会は同大統領の発言を歓迎するという声明を出しているものの、報道機関、さらにNSAの欧州における諜報プログラムについて調査を実施している欧州議会の市民の自由・司法・内務委員会は、オバマ大統領の発言に否定的に反応し、失望させるものであったとしている。また、米諜報機関の活動を回避するため、欧州とブラジル間に電気通信向けの海底ケーブルを敷設するプロジェクトも発表されている。

パーソナルデータ保護は世界中で現在最も注目されている ICT 政策の 1 つであるが、欧州では人権の観点からデータ保護が考えられ、その必要性に対する意識が高く、それに伴い、法制度に関する議論も豊富である。このような欧州の現状を知ることは、日本においてパーソナルデータ保護制度を策定する際に非常に有用である。

第一部　欧州連合の第七次枠組計画とホライゾン 2020 における暗号・情報セキュリティ技術の研究開発支援動向と研究事例

第一部では、パーソナルデータを利活用するにあたり、プライバシーを適切に保護することを可能とする暗号・情報セキュリティ技術の研究開発動向及び標準化の動向について記す。まず、欧州連合（EU）の大型研究開発支援プログラムである第七次枠組計画（FP7）とホライゾン 2020 における情報セキュリティの支援動向（予算等）について記し、ついで、FP7 における研究事例について記す。FP7 でも、ホライゾン 2020 でも、ICT 部門の中で情報セキュリティ分野は重要な一つの公募テーマとして認められており、多くの予算が割り当てられており、数多くの研究プロジェクトが実施されている。

第一章　欧州連合の第七次枠組計画とホライゾン2020 における暗号・情報セキュリティ技術の研究開発支援動向

本章では、EU の FP7 とホライゾン 2020 におけるパーソナルデータの保護に関わる暗号・情報セキュリティ技術の研究開発支援動向について記す。EU では、2007 年から 2013 年にかけて、大型研究開発助成プログラムである FP7 を実施していたが、ICT 部門はその重要な一部門であった。同部門に関しては、2 年毎に公募要件（テーマ、予算、審査基準等）を定めた作業プログラムが策定された（最終年の 2013 年は 1 年分）。また、2014 年より、新たな研究助成枠組プログラムとしてホライゾン 2020 が開始され、ICT 部門に関しては、2013 年 12 月に 2014～2015 年度の 2 年間の作業プログラムが策定されている。以下に、EU の FP7 とホライゾン 2020 における ICT 部門の作業プログラムを精査し、暗号・情報セキュリティ技術の研究開発支援動向に記す。

第一節　FP7 ICT 部門における支援動向

A) ICT セキュリティ分野

FP7 ICT 部門作業プログラムにおいて、暗号技術を含め、パーソナルデータの保護を目的とする研究プロジェクトは、ICT セキュリティ技術を対象とする「課題 1.4」あるいは「課題 1.5」（「ICT-2007.1.4 安全で、信頼でき、信用されたインフラ（Secure, dependable and trusted Infrastructures）」、「ICT-2009.1.4、ICT-2011.1.4、ICT-2013.1.5：信用可能な ICT （Trustworthy ICT）」で主に公募されている。同公募枠では ICT セキュリティ全般を公募対象としているが、2013 年度作業プログラムでは同公募枠内に「クラウドにおけるセキュリティとプライバシー」というテーマが定められ、欧州委員会のクラウドコンピューティングへの関心の強さが伺える。

ICT セキュリティ分野の公募予算

- 2007-2008 年度作業プログラム：ICT-2007.1.4：「安全で、信頼でき、信用されたインフラ」：予算　9000 万ユーロ
- 2009-2010 年度作業プログラム ：ICT-2009.1.4：「信用可能な ICT」：予算　9000 万ユーロ
- 2011-2012 年度作業プログラム：ICT-2011.1.4：「信用可能な ICT」：予算　8000 万ユーロ
- 2013 年度作業プログラム：ICT-2013.1.5：「信用可能な ICT」：予算　3650 万ユーロ

プライバシー・バイ・デザイン

プライバシー・バイ・デザイン原則の採用の促しについては[9]、2013 年度ICT作業プログラムで顕著になり始め、ICT-2013.1.5 :「信用可能なICT」 の他、同原則の採用を促す公募枠もある（例：ICT-2013.1.4 :「信頼できスマートで安全なスマートシティ向けのモノのインターネット」）。

B) クラウドコンピューティングとビッグデータ分野

FP7 ではクラウドコンピューティングとビッグデータの研究プロジェクトが公募されているが、その中で個人のプライバシーやセキュリティの問題に対応することがプロジェクトの採用の１つのポイントとして挙げられている。

クラウドコンピューティングに関しては、インターネットサービスを対象とする課題 1.2 で主に助成されている。同技術は 2007-2008 年度作業プログラムから、「ICT-2007.1.2： サービスとソフトウェアアーキテクチャ、インフラとエンジニアリング（予算：1 億 2000 万ユーロ： クラウドコンピューティングだけの助成ではない）」、「ICT-2009.1.2： サービスのインターネット、ソフトウェアと仮想化（予算：1 億 1000 万ユーロ： クラウドコンピューティングだけの助成ではない）」等で公募の対象となっていたものの、「クラウド」という語が普及していなかったせいで、当初作業プログラムでクラウドという語は利用されていなかった。クラウドコンピューティングが一分野として認知され、公募枠組の一つとして設定されるようになったのは2011-2012年度作業プログラムからで、「ICT-2011.1.2 : クラウドコンピューティング、サービスのインターネットと最先端ソフトウェア工学」、2013 年度作業プログラムの「ICT-2013.1.2： ソフトウェア工学、サービスとクラウドコンピューティング」において、研究プロジェクトが公募されている。

ビッグデータに関しては、デジタルコンテンツを対象とする課題 4 で主に助成されている。クラウドコンピューティングと同様に、「ビッグデータ」という言葉が一般に普及されるようになったのが非常に最近のことなので、この言葉が作業プログラムに登場するのは、2013 年度作業プログラムの「ICT-2013.4.2 : スケラブルデータ分析」を待たなくてはならないが、ビッグデータに関する研究はこの作業プログラム以前にも助成されていた（「ICT-2007.4.2 (ICT-2007.4.4) : インテリジェントコンテンツとセマンティック」、「ICT-2009.4.3： インテリジェント情報管理」「ICT-2011.4.4： インテリジェント情報管理」）。なお、「ICT-2013.4.2 : スケラブルデータ分析」では、情報の保護だけでなく、ビッグデータ利用の際の個人情報再特定に由来するプライバシーのリスクについて学際的に検討する研究ロードマップの作成も公募対象となっている。

クラウドコンピューティング分野の公募予算（課題1.2）

- 2007-2008 年度作業プログラム : ICT-2007.1.2 : サービスとソフトウェアアーキテクチャ、インフラとエンジニアリング : 予算 1 億 2000 万ユーロ （クラウドコンピューティングだけの助成ではない）
- 2009-2010 年度作業プログラム : ICT-2009.1.2 : サービスのインターネット、ソフトウェアと仮想化 : 予算 1 億 1000 万ユーロ（クラウドコンピューティングだけの助成ではない）

[9] プライバシー・バイ・デザインとは、カナダのオンタリオ情報・プライバシーコミッショナーオフィスのアン・カブーキアン氏が 1990 年代に提唱した 7 つの原則である。
原則1： リアクティブではなく、プロアクティブ。前もって予防すること目標とし、後から救済するのではない、原則2 : プライバシーをデフォルト設定、原則3 : 設計に組み込まれたプライバシー、原則4 : ゼロサムではなく、ポジティブサム（ウィン・ウィン関係を実現する）、原則5 : エンドツーエンドなセキュリティ、原則6 : 可視性と透明性 : オープン性を維持する、原則7 : ユーザープライバシーの尊重

- 2011-2012 年度作業プログラム：ICT-2011.1.2：クラウドコンピューティング、サービスのインターネットと最新ソフトウェア工学：予算　7000 万ユーロ
- 2013 年度作業プログラム：ICT-2013.1.2：ソフトウェア工学、サービスとクラウドコンピューティング：予算　4150 万ユーロ

ビッグデータ分野の公募予算（課題4）

- 2007-2008 年度作業プログラム：ICT-2007.4.2 と ICT-2007.4.4：インテリジェントコンテンツとセマンティック：予算 1 億 100 万ユーロ
- 2009-2010 年度作業プログラム：ICT-2009.4.3：インテリジェント情報管理：予算　7000 万ユーロ
- 2011-2012 年度作業プログラム：ICT-2011.4.4：インテリジェント情報管理：予算　5000 万ユーロ
- 2013 年度作業プログラム：ICT-2013.4.2：スケラブルデータ分析：予算　3100 万ユーロ

以上の他、2011-2012 年度作業プログラムの EU-ブラジル共同公募（ICT-2011.10.1：EU 拠出金：500 万ユーロ）と 2013 年度作業プログラムの EU-日本共同公募（ICT-2013.10.1: EU 拠出金：900 万ユーロ）でも、情報セキュリティやクラウドコンピューティングが研究公募の対象となっている。

第二節　ホライゾン 2020 ICT 部門における支援動向

2013 年末にFP7 が終了し、2014 年から新たな大型研究助成枠組プログラム「ホライゾン 2020」が開始されている[10]。同プログラムでは、2014 年から 2020 年の 7 年間にかけて、約 800 億ユーロの拠出が見込まれている。FP7 は 7 年間で 505 億ユーロの拠出（原子力エネルギー技術は含まない）が見込まれていたので、約 300 億ユーロの予算が増額されている。

ホライゾン 2020 では、主に「エクセレント・サイエンス」、「産業リーダーシップ」、「社会チャレンジ」という 3 つの枠組みで研究開発へ助成されるが、ICT部門は「産業リーダーシップ」に組み込まれている[11]。2014 年のICT部門の公募には、約 7 億ユーロの拠出が見込まれている[12]。ホライゾン 2020 の 2014-2015 年度ICT作業プログラムでは[13]、情報セキュリティへの配慮は多くの公募テーマに要件として含まれている（例えば、将来インターネットのための最先端 5Gネットワークインフラストラクチャ）。

プライバシー・バイ・デザイン

ホライゾン 2020 のICT部門の作業プログラムでは、プライバシー・バイ・デザイン原則の採用がプログラム全体に渡って促されている。

ビッグデータ戦略に関して、欧州委員会の通信ネットワーク・コンテンツ・技術総局[14]（通称 connect：コネクト：旧情報社会・メディア総局（infoso））のデータバリューチェーンユニットは、「欧州データバリューチェーン戦略」を発表している[15]。同戦略では、1）整合した欧州データエコシステムの促進、2）データを巡る研究と技術革新の触発とともに、3）データからバリュー（価値）を抽出するための枠組みとなる条件の改善という 3 点について記され、プライバシーの問題に関しては、個人のプライバシー侵害の懸念とパーソナルデータの再利用による利点の間で、適切なバランスを見つけることが 1 つの指針原理として挙げられている。このため、EUデータ保護法の改正

[10] http://ec.europa.eu/programmes/horizon2020/
[11] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies
[12] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/96-ict-32-2014.html#tab1
[13] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-leit-ict_en.pdf
[14] http://ec.europa.eu/dgs/connect/
[15] http://ec.europa.eu/digital-agenda/en/elements-data-value-chain-strategy

と「プライバシー・バイ・デザイン」という理念の下、プライバシーを遵守する基礎特徴を持つ技術の開発をホライゾン 2020 では重視することが対応策として挙げられている。

また、EU データ保護法改正案の第 23 条項「デザインとデフォルトによるデータ保護」において、データ管理者はデータ主体の保護を強化する「適切な技術的、組織的措置と手続き（appropriate technical and organisational measures and procedures）」を講じなければならないとされており、同法の改正により、プライバシー・バイ・デザイン原則の採用が強く促される。

ICT32：ICT サイバーセキュリティ、信用可能な ICT

ホライゾン 2020 の ICT 部門の情報セキュリティに特化された公募テーマとしては、「ICT クロスカッティング活動」の「ICT32：ICT サイバーセキュリティ、信用可能な ICT」がある。同テーマでは、研究開発として、エンド・ツー・エンドセキュリティのためのセキュリティ・バイ・デザインと暗号が挙げられている。また、研究開発の他、欧州における暗号の共同研究を発展させるプロジェクトも公募されている。予算としては、「ICT32：ICT サイバーセキュリティ、信用可能な ICT」全体に、3700 万ユーロが拠出される予定である。

暗号に関しては、以下の技術が研究テーマとして挙げられている。

- リアルタイム暗号に基づくハードウェア向けの資源効率が良く高い安全技術、
- 資源効率が良く、高く安全な準同形暗号
- 機能的暗号を含む分散された暗号
- アプリケーションとソフトウェア、ファームウェア、ハードウェア環境を結ぶ暗号ツール
- 長期間のセキュリティ向けポスト量子暗号
- 量子鍵配送システムとネットワーク

以上の他、「将来インターネット」の「ICT7：最先端クラウドインフラストラクチャとサービス」では、クラウドセキュリティに関する研究プロジェクトが募集されている。

第二章　欧州連合の第七次枠組計画における暗号・情報セキュリティ技術の研究事例

本章では、FP7 において助成されている暗号・情報セキュリティ技術に係る主な研究事例を記す。FP7 においては、暗号を含め、情報セキュリティに関して非常に多くの研究プロジェクトが実施されている。

A)　暗号：ECRYPT Ⅱ

省略プロジェクト名称	ECRYPT Ⅱ
正式名称	暗号における欧州エクセレンスネットワーク ： 第二段階
分野	ICT-2007.1.4
プロジェクト期間	2008 年 8 月～2013 年 1 月（54 ヶ月）
予算（EU 拠出分）	408 万ユーロ（300 万ユーロ）
コーディネーター	ルーバン・カトリック大学（ベルギー）
参加者	ENS（仏）、フランス・テレコム（仏）、IBM リサーチ（スイス）、アイントフォーヘン工科大学（蘭）、ローザンヌ連邦工科大学（スイス）、サレルノ大学（伊）、ブリストル大学（英）、ルール大学ボーフム（独）、王立ホロウェイ・ベッドフォード・ニューカレッジ（英）、グラーツ工科大学（オーストリア）
ウェブサイト	http://www.ecrypt.eu.org
研究内容	ECRYPT Ⅱ の目的は、官民を問わず、情報セキュリティ分野の欧州研究者

	が提携して活動することをを強化することである。このため、プロジェクト参加者は 3 つの仮想研究所へと研究能力を統合する。 ・ SymLab：共通鍵暗号アルゴリズムの研究：安全で効果的なハッシュ機能の開発、軽量暗号プリミティブの開発 ・ MAYA：公開鍵暗号アルゴリズムとプロトコルの研究：非対称的なプリミティブとプロトコルのデザインと分析、コンピューターショナル問題の硬度に対する知識の改善 ・ VAMPIRE：ハードウェアとソフトウェアの実行：効果的で安全な実行に関する新しい技術の研究、研究共同体とユーザーの架け橋となること

B)　プライバシー・バイ・デザイン原則の適用：PRIPARE

省略プロジェクト名称	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）、ルーバン・カトリック大学（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・アメリカン大学（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
研究内容	プライバシー・セキュリティ・バイ・デザイン方法論の適用を簡便化し、教材を利用して、リスク管理を強化することにより、産業界での実践を準備するために ICT 研究コミュニティによる実践を支援する。 ・ プライバシー・セキュリティ・バイ・デザインのソフトウェアとシステム工学方法論を規定すること ・ ICT システムの製品とサービスの開発と実行のための適切な実践に係る教材と、クラウドコンピューティング、モバイルサービス、サイバー事故のユーザーケースを準備すること ・ 同プロジェクトで開発した実践を適用し、トレーニングワークショップと実践支援を通して、FP7 とホライゾン 2020 の研究プロジェクトを支援すること ・ プライバシーのリスク管理のアプローチに関する教材を供給することと、ユーザーの間でリスク管理の必要性に対する意識を高めること ・ プライバシー・セキュリティ・バイ・デザインの実践、インターネットの妨げられない利活用の支援とリスク管理の創造に対するギャップを特定し、推奨を供給すること なお、同プロジェクトの助言者には、プライバシー・バイ・デザイン原則を開発したカナダのオンタリオ情報・プライバシーコミッショナーオ

	フィスのアン・カブーキアン氏がいる。

C)　データ管理の法的ツールセット：ENDORSE

省略プロジェクト名称	ENDORSE
正式名称	プライバシーを維持するデータ管理のための法・技術枠組み
分野	ICT-2009.1.4
プロジェクト期間	2010 年 9 月～2013 年 2 月（30 ヶ月）
予算（EU 拠出分）	367 万ユーロ（274 万ユーロ）
コーディネーター	ウォーターフォード技術研究院（アイルランド）
参加者	ヨーロッパ・アシステンス・イタリア、ザルツブルグ応用科学大学（オーストリア）、ザラゴザ大学（スペイン）、DL リーガル（英）、ティルブルク大学（蘭）、クリエート・ネット（伊）、ソリューダ・ネット（伊）、シーコムス（英）
ウェブサイト	http://ict-endorse.eu
研究内容	ENDORESE は、プライバシーを維持するデータ管理のための法・技術枠組みを提供することを目的とする。このため、パーソナルデータが法的に適切な仕方で扱われるように、データ管理者とデータ主体の両方に保証を与えるオープンソースで無料に手に入るツールセットを開発する。また、プライバシーとデータ保護を遵守する ICT 製品の信用価値を高めるために、認証の方法を開発する。同プロジェクトには、法律の専門家、コンピューターサイエンティスト、ソフトウェア実行者が参加する。 研究課題 ・ どのようにして公共及び民間のデータ保存に関して、特定の規格を持つ安全な仕方で個人情報が保存され、アクセスされうるか ・ どのようにして、モデル化したアプローチに基づくプライバシー維持規則を利用して、個人情報がサービスと許可された人間にさらされるのか

D)　クラウドコンピューティングのセキュリティ：PRACTICE

省略プロジェクト名称	PRACTICE
正式名称	PRACTICE： クラウドにおけるプライバシーを維持するコンピュテーション
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）
プロジェクトコーディネーター	テクニコン（独）
参加者	SAP（独）、ダルムスタット工科大学（独）、アレクサンドラ研究院（デンマーク）、Arcelik（トルコ）、バー・イラン大学（イスラエル）、サイバネティカ（エストニア）、ヴェルツブルグ大学（独）、インテル・ドイツ、ルーバン・カトリック大学（ベルギー）、INESC・ポルト（ポルトガル）、ミンホ大学（ポルトガル）、アルハス大学（デンマーク）、アインフォールド工科大学（蘭）、ブリストル大学（英）、ディストレット宇宙開発技術（伊）、サレント大学（伊）、ミラノ大学

	（伊）、パルティシア（デンマーク）、ゲッティンゲン大学（独）
ウェブサイト	http://www.practice-project.eu
研究内容	PRACTICE プロジェクトの目標は、利用されるデータの秘密を守りながら、新しいビジネスプロセスを可能にするために、クラウド上でコンピュテーションを行うことを許すクラウドコンピューティング技術の設計である。 ・ 同じクラウドサービスを利用している他のユーザーから自分のデータを隠す ・ クラウド事業者からユーザーのデータを隠す ・ 複数のサーバ間でのコンピュテーションを安全化する ・ 疑い深い人々の間でのコンピュテーションを安全化する

第二部　欧州における暗号・情報セキュリティ技術に関する標準化の動向

第二部では、欧州における暗号・情報セキュリティ技術に係る標準化の動向について記す。現在、欧州で最も注目を集めているICTの一つはクラウドコンピューティングであるが、同技術のセキュリティと標準化の問題は大きな課題として認識されており、欧州委員会と欧州の電気通信部門の標準化団体、欧州電気通信標準化機構（ETSI）は合同で同問題に取り組んでいる。以下に、EUのクラウドコンピューティング戦略におけるセキュリティと標準化の動向について記す。

第一章　EUのクラウドコンピューティング戦略におけるセキュリティと標準化の問題

まず、EUのクラウドコンピューティング戦略について概観する。クラウドコンピューティングに関して、欧州委員会は2012年9月に「欧州におけるクラウドコンピューティングの潜在性の解放」という通達を発表し、詳しく欧州クラウドコンピューティング戦略を規定している[16]。この戦略には、欧州経済の全部門でクラウドコンピューティングの受容を促進するために行うべき行動が記されている。欧州委員会は、同文書において特にクラウドコンピューティングについて、以下の3つの問題を特定している。

- デジタル単一市場の分断 ：この分断は、クラウドユーザーとプロバイダーにとって最大の懸念であるデジタルコンテンツとデータ保存場所に関する各国の法制度の違いと法律の不確かさに由来する。
- 契約に関わる問題 ：データアクセス、データのポータビリティ、コントロール、所有に関する懸念に関係する。例えば、データが損なわれた場合のようなサービスの不良に関する責任に関する懸念であり、ユーザーとプロバイダー間の契約に関わる問題である
- 標準の錯綜：クラウドコンピューティング関連の標準の錯綜した状態は、標準の多数化とともに、ポータビリティを可能にするデータフォーマットの十全な相互運用性のレベルを満たす標準の不確かさ、さらに、パーソナルデータ保護のための手段、データ漏洩とサイバー攻撃からの保護に関わる標準の不確かさに由来する

以上のように、欧州委員会のクラウドコンピューティング戦略において、パーソナルデータの保護は1つのポイントとして挙げられている。

同文書では、欧州委員会は以下の3つの主要な行動（Key Action）を行うとしている。

- 主要な行動1：標準のジャングルを切り開くこと
- 主要な行動2：安全で公平な契約条項と条件
- 主要な行動3：公共部門から技術革新と成長を促すために「欧州クラウドパートナーシップ」を確立すること

主要な行動1は、クラウド技術の標準化活動に関わる。クラウドコンピューティングの標準の多様性は相互運用性やデータポータビリティを損なうので、クラウドサービスの信頼性を確保する必要がある。米国立標準・技術機構（NIST）はすでに、広く受容されている定義を含む一連の文書を発表しており、またETSIはクラウド標準を検討するクラウドグループを設置しているが、他にも標準設定のイニシアチブが必要である。優先事項は、クラウドコンピューティングに対する信頼を発展させるために既存の標準を展開させることであり、そのために関係する標準を特定し、コンプライアンス認証（certification）が必要である。

[16] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

以上のため、欧州委員会は次の事柄を行うとしている。

- 信用され、信頼できるクラウドの提供を振興するために、ETSI に 2013 年までにステークホルダーと提携して、透明かつオープンな仕方で必要な標準（セキュリティ、相互運用性、データポータビリティ、可逆性）の詳細なマップを作成することを要請する
- 欧州標準化の新規則と一致して、パーソナルデータ保護のため、情報通信技術分野の技術仕様を EU レベルで認知することによって、クラウドコンピューティングサービスにおける信用を強化すること
- 欧州連合ネットワーク・情報セキュリティ庁（ENISA）や他の関連機関と提携し、クラウドコンピューティング分野の EU 広域随意認証スキームの展開を支援し、2014 年までにそのスキームのリストを策定すること
- 環境問題に対応するために、産業界とクラウドサービスによるエネルギーと水の消費、炭素排出のための調和された測定基準に同意すること

以上のように、クラウドの標準化作業に関しては、セキュリティ、パーソナルデータ保護、信用という点が問題となっている。

主要な行動 2 は、クラウドプロバイダーが利用する契約やSLA（Service Level Agreements）に関わり、欧州委員会は、2011 年 11 月に同委員会により提案された「欧州共通販売規則（Regulation on a Common European Sales Law）」[17]ではカバーできないクラウドコンピューティングに関わる問題に対応するモデル契約規定を作成するとしている。欧州共通販売規則案は、各国の販売法規則の多様性に由来する多くの障害を解消するために、契約に関わる単一の諸規則を確立することを目的とするが、クラウドコンピューティングに関わる「デジタルコンテンツ」の供給にも適応する規則を含む。主要な行動 2 では、同法案の対象外である「契約期限後のデータの維持」、「データの開示と完全性」、「データの場所と移動」、「データの所有権」、「クラウドプロバイダーと下請け契約によるサービスの変化の直接的かつ間接的責任」に関するモデル契約規定を定める活動を行っている。このような契約条項に対する行動は、データ保護も促進すると考えられている。国際的なデータ移動を管理する標準契約条項と、クラウドに優しい（cloud-friendly）拘束的企業準則（Binding Corporate Rules）を採用するための必要条件を確立することを通して、EUデータ保護法改正案はEU及びEEA圏外へのデータ移動時のデータ保護の連続性を強化し、個人に対するデータ保護のレベルの高さを保証するからである。つまり、欧州共通販売規則案とクラウドサービスに関わるモデル契約規定の作成はEUデータ保護法改正案を補完し、クラウドサービスに関わるパーソナルデータを保護する法規制である。

以上のように、欧州委員会のクラウド戦略では同技術のセキュリティ、個人情報の保護、信用性を高めることが重要視され、欧州委員会と ETSI はクラウドコンピューティングに係る標準をリストアップする作業を行っている。

第二章　クラウド標準化コーディネーションイニシアチブの動向

欧州委員会の「欧州におけるクラウドコンピューティングの潜在性の解放」で提案された 3 つの主要な行動のうちの 1 つは標準化活動であった。2012 年 12 月、欧州委員会とETSIはステークホルダーと提携し、クラウド標準エコシステムと重要な分野（セキュリティ、相互運用性、データポータビリティ、可逆性）について標準ロードマップを策定するために、「クラウド標準コーディネーションイニシアチブ（Cloud Standards Coordination：CSC）」を開始した[18]。そして、2013 年 12 月 11 日には、欧州委員会とETSIの主催で、ブリュッセルでCSCの 1 年間の活動結果報告イベント

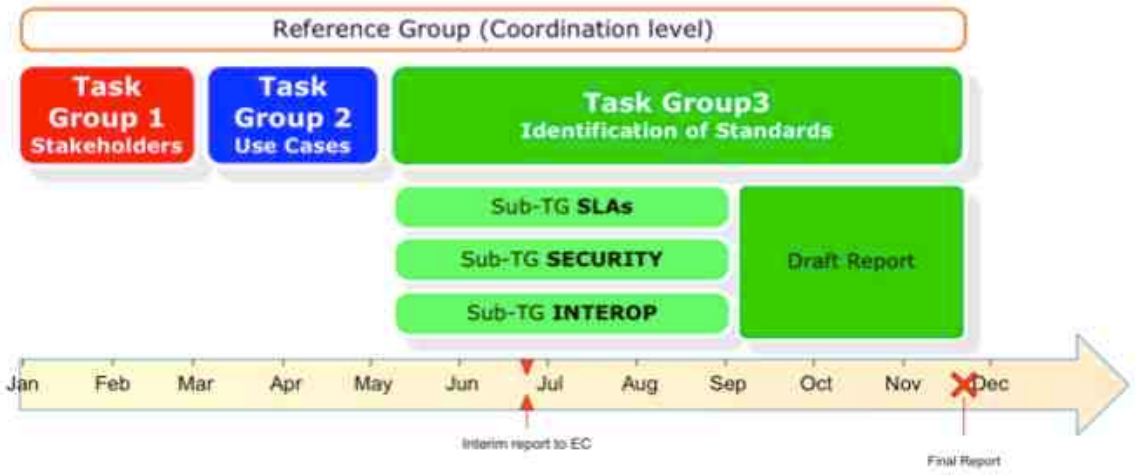
[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0635:FIN:EN:HTML
[18] http://csc.etsi.org/website/home.aspx

が実施されている。

第一節　CSC の構成と活動

CSC には 3 つのタスクグループ（TG）が設置され、それぞれステークホルダーの役割の分析（TG1）、ユーザーケースの収集（TG2）、ユーザーケースの分析と報告書作成（TG3）を担当した。TG3 には、SLA（Service Level Agreements）、セキュリティ、相互運用性に関して、それぞれ 3 つの下部グループが設置されている。セキュリティの責任者は ENISA（欧州連合ネットワーク・情報セキュリティ庁）のマルニック・デッケル氏、CSA（クラウドセキュリティアライアンス）のジェズ・ルナ氏、オアシス（OASIS）社である。

図版 CSC の組織構成



出典　CSC の活動結果報告**イベント配布資料**

TG3 はユーザーケースを分析する際に、クラウドサービスの提供・利用に共通の 3 段階（クラウドサービスの入手・クラウドサービスの作動・クラウドサービスの終了）を特定し、SLA、相互運用性、セキュリティという側面を分析している。

第二節　クラウドコンピューティング標準と技術仕様のリスト

2013 年 11 月に発表されたCSCの最終報告書には[19]、現在のクラウドコンピューティングの標準と技術仕様のリストが収録されている。以下にそのリストを収録する。

図版 現行のクラウドコンピューティングの標準と技術仕様のリスト

[19] http://ec.europa.eu/digital-agenda/en/news/cloud-standards-coordination-final-report

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[ATIS1]	ATIS	ATIS-0200003	CDN Interconnection Use Case Specification and High Level Requirements	Specification	Published
[ATIS2]	ATIS	ATIS-0200004	CDN Interconnection Use Cases and Requirements for Multicast-Based Content Distribution	Specification	Published
[ATIS3]	ATIS	ATIS-0200005	Cloud Framework for Telepresence Service	Specification	Published
[ATIS4]	ATIS	ATIS-0200006	Virtual Desktop Requirements	Specification	Published
[ATIS5]	ATIS	ATIS-0200008	Trusted Information Exchange (TIE)	Specification	Published
[ATIS6]	ATIS	ATIS-0200009	Cloud Service Lifecycle Checklist	Specification	Published
[ATIS7]	ATIS	ATIS-0200010	CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment	Specification	Published
[ATIS8]	ATIS	ATIS-I-0000001	Format of ATIS Namespace	Specification	Published
[ATIS9]	ATIS	ATIS-I-0000002	ATIS XML Schema Development Guidelines	Specification	Published
[CSA1]	CSA	CCM 3.0	Cloud Control Matrix	Specification	Published
[CSA3]	CSA	CTP	Cloud Trust Protocol	Specification	Published
[CSA4]	CSA	A6	Cloud Audit	Specification	Published
[CSA6]	CSA	PLA	Privacy Level Agreement	Specification	Published
[CSA8]	CSA	TCI	Reference Architecture - Trusted Cloud Initiative	Specification	Published
[CSA9]	CSA	OCF	Open Certification Framework	Specification	Published
[CSMIC1]	*CSMIC*	*SMI Framework 2*	*Service Measurement Index - measures for Cloud Services*	*Specification*	*Draft*

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[DMTF1]	DMTF	DSP0263	Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP Specification	Standards	Published
[DMTF2]	DMTF	DSP0264	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM)	Standards	Published
[DMTF3]	DMTF	DSP0243	Open Virtualization Format Specification V2	Standards	Published
[ETSI29]	ETSI / TC CLOUD	TS 103 142	Test Descriptions for Cloud Interoperability	Specification	Published
[EuroCloud1]	EuroCloud	Star Audit	EuroCloud Star Audit	Specification	Published
[FIW1]	*FI-WARE*	*n/a*	*SLAware: Service Level Agreements Specification*	*Specification*	*Draft*
[ISO1]	ISO/IEC	17203	OVF	Standards	Published
[ISO2]	*ISO/IEC*	*17788*	*Cloud Computing Overview and Vocabulary*	*Standards*	*Draft*
[ISO3]	*ISO/IEC*	*17789*	*Cloud Computing Reference Architecture*	*Standards*	*Draft*
[ISO4]	ISO/IEC	17826	Cloud Data Management Interface (same as SNIA CDMI)	Standards	Published
[ISO5]	ISO/IEC	27001	Information security management systems – Requirements	Standards	Published
[ISO6]	ISO/IEC	27002	Code of practice for information security controls	Standards	Published
[ISO7]	*ISO/IEC*	*27017*	*Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002*	*Standards*	*Draft*
[ISO8]	*ISO/IEC*	*27018*	*Code of practice for data protection controls for public cloud computing services*	*Standards*	*Draft*
[ISO9]	ISO/IEC	20000-1	Service management system requirements	Standards	Published
[ISO11]	*ISO/IEC*	*27036-4*	*Information security for supplier relationships — Part 4: Guidelines for security of cloud services*	*Standards*	*Draft*
[ISO12]	*ISO/IEC*	*19086*	*Cloud computing –SLA framework and terminology*	*Standards*	*Draft*
[ITU8]	ITU-T	X.1600	Security framework for cloud computing	Standards	Published
[ITU9]	*ITU-T*	*X.idmcc*	*Requirements of IdM in cloud computing*	*Standards*	*Draft*
[ITU10]	ITU-T	Y.3501	Cloud Comp Framework & High-level Requirements	Standards	Published
[ITU11]	ITU-T	Y.3510	Cloud Computing Infrastructure requirements	Standards	Published
[ITU12]	ITU-T	Y.3520	resource management framework for e2e cloud	Standards	Published
[ITU13]	*ITU-T*	*Y.ccdef*	*Cloud Computing overview and vocabulary*	*Standards*	*Draft*
[ITU14]	*ITU-T*	*Y.ccic*	*Framework of Inter-cloud*	*Standards*	*Draft*
[ITU15]	*ITU-T*	*Y.ccra*	*Cloud Computing Reference Architecture*	*Standards*	*Draft*
[ITU16]	*ITU-T*	*Y.daas*	*Requirements Reference Architecture of DaaS*	*Standards*	*Draft*
[OASIS1]	*OASIS/CAMP*	*CAMP*	*Cloud Application Management for Platforms (CAMP)*	*Specification*	*Draft*

CSC Ref	Organisation / group	Source Reference	Title	Type	Status
[OASIS5]	OASIS/TOSCA	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA)	Specification	Published
[OASIS6]	OASIS/OData		Open Data Protocol	Specification	Published
[ODCA1]	ODCA	n/a	Master Usage Model: Compute Infrastructure as a Service	Specification	Published
[ODCA2]	ODCA	n/a	Master Usage Model: Service Orchestration	Specification	Published
[ODCA3]	ODCA	n/a	Master Usage Model: Commercial Framework	Specification	Published
[ODCA4]	ODCA	n/a	Usage: Data Security Framework	Specification	Published
[ODCA5]	ODCA	n/a	Virtual Machine (VM) Interoperability in a Hybrid Cloud Environment	Specification	Published
[ODCA6]	ODCA	n/a	Master Usage Model: Software-Defined Networking	Specification	Published
[ODCA7]	ODCA	n/a	Master Usage Model: Scale out Storage	Specification	Published
[ODCA8]	ODCA	n/a	Master Usage Model: Information as a Service	Specification	Published
[ODCA9]	ODCA	n/a	Usage: Standard Units of Measure for IaaS	Specification	Published
[OG1]	*The Open Group*		*Cloud Computing Reference Architecture*	*Specification*	*Draft*
[OGF1]	OGF	GFD.183	Open Cloud Computing Interface - Core	Specification	Published
[OGF2]	OGF	GFD.184	Open Cloud Computing Interface - Infrastructure	Specification	Published
[OGF3]	OGF	GFD.185	Open Cloud Computing Interface - RESTful HTTP Rendering	Specification	Published
[OGF4]	OGF	GFD.192	Web Services Agreement (WS-Agreement)	Standards	Published
[OGF5]	OGF	GFD.193	WS-Agreement Negotiation	Specification	Published
[QuEST1]	QuEST Forum	TL9000	TL 9000 Measurements Handbook	Standards	Published
[QuEST2]	QuEST Forum	TL9000	TL 9000 Requirements Handbook	Standards	Published
[SLA1]	SLA@SOI	D.A5a	SLA: An abstract syntax for Service Level Agreements	Specification	Published
[SNIA1]	SNIA	CDMI	Cloud Data Management Interface - ISO 17826:2012	Standards	Published
[TIA1]	TIA	ANSI/TIA-942-A	Telecommunications Infrastructure Standards for Data Centers	Standards	Published

出典　CSC の活動結果報告**イベント配布資料**

以上のように、欧州では現在、欧州委員会と ETSI が提携し、クラウドコンピューティングの標準化作業が進められており、その際、セキュリティ、個人情報の保護、信用の向上が目的として挙げられている。

第三部　欧州におけるパーソナルデータ利活用に係る制度整備の動向

第三部では、パーソナルデータを利活用するにあたってプライバシーを適切に保護するために政府が策定している法律やガイドライン、民間企業・業界団体による自主規制、倫理面の活動について記す。第一章では、EU のパーソナルデータ保護に係る法制度について概観し、ついで、EU 圏のパーソナルデータ保護制度の中核をなす EU データ保護指令の概要と改正動向について記す。第二章では、欧州諸国におけるパーソナルデータ保護制度、特に英国とフランスの諸制度について記す。両国にはパーソナルデータ保護監督機関が設置され、同分野で活動している。第三章では、2014 年 1 月 22 日から 24 日にベルギー・ブリュッセルで開催された「コンピューター・プライバシー&データ保護」という国際イベントの視察レポートを収録する。同イベントでは、3 日間に渡り、多くのパネルディスカッションがなされ、欧州におけるパーソナルデータ保護の問題が数多く議論された

第一章　欧州のパーソナルデータ保護に係る法制度

まず、欧州全体のパーソナルデータ保護に関係する諸制度を概観する。欧州各国のパーソナルデータ保護に係る法制度は、基本的に欧州評議会と欧州連合という枠組みで制定された諸法に基づいている。2014 年 1 月、欧州評議会と欧州連合基本権庁は合同で、欧州圏のパーソナルデータ保護法制度を解説した「欧州データ保護法ハンドブック」を作成し、公表している[20]。以下、同ハンドブック等の資料に基づき、欧州圏統一のパーソナルデータ保護に係る法制度を概観する。

第一節 欧州のパーソナルデータ保護に係る法制度の概観

以下の法制度が、欧州ではパーソナルデータ保護に関係するとされている。

1) 欧州人権条約第 8 条：欧州評議会[21]が 1950 年に採択し、1953 年に発効された「欧州人権条約」の第 8 条はプライバシーの権利に係る条項であり、パーソナルデータの収集と利用に対する保護の権利が同条項で定められている。

2) 欧州評議会条約第 108 号：欧州評議会は、1981 年に「個人データの自動処理に係る個人の保護に関する条約」（欧州評議会条約第 108 号）の署名を開放している。

3) EUデータ保護指令：EUのデータ保護法としては、1995 年 10 月に「パーソナル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指令」（以下、EU データ保護指令とする）が成立し、各EU加盟国内で国内法化されており、同法がEU圏域でパーソナルデータ保護に係る法的ガイドラインを提供している。なお、後述のように、2012 年 1 月に同法の改正案が欧州委員会によって提案されている。

4) EU基本権憲章第 7 条と第 8 条：EUが 2000 年に宣言したEU基本権憲章の第 7 条と第 8 条は、それぞれプライバシーの尊重とパーソナルデータの保護を定めている。同憲章は元々政治文書に過ぎなかったが、2009 年 12 月のリスボン条約の発効に伴い、法的拘束力を持つようになった。

5) 電子通信部門におけるプライバシー指令：「電子通信部門におけるパーソナルデータの処理とプライバシー保護に係る指令」は、盗聴や当事者の同意を得ないパーソナルデータの保存等を禁止

[20] http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

[21] 欧州評議会（Council of Europe）は、欧州連合（European Union）とは異なる連合体であり、現在、欧州連合加盟国 28 カ国を含む 47 カ国から構成される。

するとともに、ユーザーに拒否する機会を与えることなくクッキー機能を利用することを禁止している。同指令は2002年に成立したが、2009年に改正されている。

第二節　EUデータ保護指令の概要と改正動向

A) EUデータ保護指令の概要

ついで、EUデータ保護指令を概観する[22]。同法はEU圏にパーソナルデータ保護に係る共通の法枠組みを提供しており、パーソナルデータ保護に関して最も重要なEU法である。同法は、個人のプライバシー保護とEU圏内のパーソナルデータの自由な移動の間でのバランスを取ることを目的としており、そのため、同法はパーソナルデータの収集と利用を制限し、各加盟国にデータ保護を所管する独立機関を設置することを要求する。以下に、同法の主要なポイントのみ記す。

1) 同法は、自動的手段（顧客のコンピューターデータベース等）により処理されるデータ、そして、自動的ではないファイリングシステム（伝統的な紙媒体のファイル）に収められているか、この種のファイルの収めることが意図されているデータに適用される。

2) 同法は、純粋に個人的な活動、あるいは家庭での活動において処理されるデータ、また、公共安全、国防に係る作業のようなEU法の範囲外の活動において処理されるデータには適用されない。（第3条）

3) 同法はパーソナルデータ保護に係るガイドラインを定めている。

- データの性質：パーソナルデータは公正に、合法的に処理されねばならず、特定された明示的かつ正当な目的のために収集されなければならない。また、パーソナルデータは正確でなければならず、期限付きで保存されなければならない。（第6条）
- データ処理の正当性の基準：パーソナルデータの処理に対するデータ主体の同意等に関する規定。（第7条）
- 特殊なデータのカテゴリー：人種または民族、政治的見解、宗教的または哲学的信条、労働組合への加入、健康はまたは性生活に係るデータの取扱いについて。（第8条）
- データ主体へ与えられる情報：データ管理者は特定の情報（管理者のアイデンティティ、処理の目的等）をデータ主体に与えなければならない。（第10条）
- データ主体のデータへのアクセス権：全てのデータ主体はデータ管理者から特定の情報を取得する権利を持たなければならない。（第12条）
- 同法適用の免除と制限：国内安全や国防、刑事訴追、あるいは加盟国とEUの重要な経済、金融に係る関心、データ主体の保護を守るためには、同法で定められたパーソナルデータ保護原則の適用は制限される。（第13条）
- 異議権：データ主体はデータ処理へ異議権を持たなければならない。（第14条）
- 処理の機密性と安全：データ管理者の指示なく、いかなる人もパーソナルデータを処理してはいけない。管理者は偶然、あるいは違法的なデータの破壊、漏洩等からデータを保護する適切な手段を講じなければならない。（第16条、第17条）
- データ処理の監督機関への通知義務　（第18条）
- 法的救済：あらゆる人が権利侵害に対して法的救済を得る権利を持たなければならない。（第22条、23条、24条）
- パーソナルデータの第三国への移動：パーソナルデータの第三国への移動は特定の免除条件を満たさない限り、データ保護のレベルが十分な場合にのみ許可される。（第25条、第26条）

---

[22] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm
以下の文章は改正法案及び通達の概要を示すもので、同文書の翻訳ではなく、より詳細な内容については同文書の原文を参考にしていただきたい。

- パーソナル独立監督機関の設置義務（第28条）
- 第29条作業部会の設置：全加盟国の監督機関等が第29条作業部会と呼ばれる組織を設立し、欧州委員会等に対して政策提言や助言する。（第29条、第30条）

4）同法は、匿名化されたパーソナルデータには適用されない。（前文26）

後述するように、以上のEUデータ保護指令は、2012年1月から改正手続きが開始されており、大きく変更される可能性があり、次節でその改正動向について記す。

B) EUデータ保護指令の改正の背景と理由

2012年1月25日、オンライン上のプライバシーの強化と欧州のデジタル経済を振興することを目的に、欧州委員会は1995年に成立したデータ保護指令を近代化するため、同法の改正法案であるデータ保護規則案を提案した。この提案は、2010年8月に発表された欧州デジタル戦略の「欧州のためのデジタルアジェンダ」に明記されており[23]、2010年と2011年に欧州委員会は同法改正のために、ステークホルダーに意見聴取を行っていた。以下に、旧EU指令の改正理由、新規則案（改正法案）の概要と改正動向について記す。なお、新規則案は、刑事犯罪の予防、検知、調査もしくは起訴手続き及び関連する司法活動を目的とするパーソナルデータ処理の保護に関するルールを設置する指令とともに提案されているが、後者に関しては、本報告書では取り扱わない。

EU データ保護法の改正理由

欧州委員会によれば、1995年のパーソナルデータ保護指令は、EU単一市場の機能強化、パーソナルデータ保護基本権の保護という基礎原理を実現する画期的なものであり、現在でも妥当なものである[24]。だが、1）このEU法は「指令」という法的地位を持つため、EU各国はそれぞれの仕方で国内法化しており、EU地域圏で同程度のパーソナルデータ保護を実現できていない。2）急速な技術発展とグローバリゼーションが、パーソナルデータ保護に関して新しい課題を惹起しており（特に、ソーシャルネットワーキングサイト、クラウドコンピューティング、位置情報に基づくサービス、スマートカードにより、デジタル痕跡（digital trace）を残すようになっている）、デジタル時代に適応する新しい規則を定める必要がある。以上のために、旧指令を改正し、個人が自分のパーソナルデータをよりコントロールできるようにするとともに、EU域外も含め、パーソナルデータの保護を確保する必要がある。以上の改正の理由に加えて、同法の改正による経済的効果も想定されている。2011年6月の欧州委員会の調査発表では、欧州に住む7割の人々は自分のパーソナルデータが誤って利用されることを懸念しており[25]、オンラインサービス等への信用を増加することで、デジタル経済一般（EU単一市場の刺激と成長促進、雇用創出、技術革新の促進）を成長させることができると考えられる。また、改正法により、欧州市民が厳格なEU法を遵守する安全な欧州企業のオンラインサービスを米企業のサービスに代わって利用するようになるという思惑も見える。

C) EUデータ保護規則案の概要

以下に、EUデータ保護法改正案[26]の概要について、欧州委員会が同法案と同時に発表し、改正法の主要な点について記した「接続した世界におけるプライバシーを守ること、21世紀のための欧州データ保護枠組」通達[27]に基づいて記す[28]。特に、データ保護に対する個人の権利を強化すること、デジタル単一市場にふさわしいデータ保護ルールを定めること、グローバリゼーションに対応する

[23] http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-12-review-eu-data-protection-rules
[24] http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf
[25] http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en
[26] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT
[27] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF
[28] 以下の文章は改正法案及び通達の概要を示すもので、同文書の翻訳ではない。より詳細な内容については同文書の原文を参考にしていただきたい。

ことが問題となる。

データ保護に係る個人の権利の強化

目的：パーソナルデータを管理する個人の能力を改善する

- パーソナルデータの処理に対する本人同意は、明示的に、つまり、本人による言明あるいは明確に肯定的な行為に基づいて取得されなければならない（改正法案第7条）
- 自分のデータへの容易なアクセス（第15条）とデータポータビリティの権利の保証（第18条）：データ管理者から保存されたデータの複製を獲得する権利及び妨害なくあるサービスプロバイダーから他のプロバイダーへデータを移動させる自由の保証
- インターネットユーザーにオンライン環境での「忘れられる権利」を備えさせる（ユーザーが同意を撤回し、またデータ保持の正当な根拠がない場合にはデータを消去させる権利）（第17条）
- データ管理者は、特に処理活動が子供に関係する時に、個人がどのように彼らのパーソナルデータが扱われているか十分に理解するように情報への権利を強化する（第11条）

目的：個人が自分の権利を行使する手段を改善する

- 各国のデータ保護監督機関の独立性と権限を強化する（第47条、第52条、第53条等）
- データ保護権利が侵害された時の行政及び司法措置を強化する：罰金金額の増加等（第73条から第79条）

目的：データセキュリティの強化

- プライバシーを強化する技術、プライバシー・フレンドリーな初期設定、プライバシー認証スキームの利用を促進する（第30条、第39条）
- データ管理者がデータ漏洩を不当な遅延なく、データ保護監督機関と関係する個人に通知する一般義務を導入する（第31条、第32条）

目的：データ処理の説明責任の強化

- データ管理者にデータ保護オフィサーを指名することを要求する（250名以上の組織に対して）（第35条）
- 手続きとシステムの計画段階でデータ保護手段が考慮されるように「プライバシー・バイ・デザイン」原理を導入する（第23条）
- プライバシーリスクが高いデータ処理を行う組織にデータ保護影響評価を実施する義務を導入する（第33条）

デジタル単一市場にふさわしいデータ保護ルール

目的：データ保護の単一市場を強化する

- 法の地位を「指令（Directive）」から「規則（Regulation）」へと格上げする。規則は、指令と違い、各EU加盟国内で国内法化する必要がなく、EU加盟国全域で直接効力を持つので、この改正によりEU加盟国内で法規制を統一できる。
- EU圏内でデータ保護の「ワン・ストップ・ショップ」システムを設置する。データ管理者は、その企業の主要事業所が設立された国のデータ保護監督機関と手続きを行えばよい。（第51条）
- 各国の監督機関同士の連携を迅速かつ効果的なものにするための条件をつくる。（第55条）
- EUレベルで整合性メカニズムを設置する。各国の監督機関の決定が他国の関係する監督機関の見解を考慮することを促す。（第57条）
- 第29条作業部会を独立欧州データ保護ボードへと格上げする。（第64条）

グローバル化された世界におけるデータ保護

目的：グローバリゼーションへの対応

- EUデータ保護改正法を第三国に設立されたデータ管理者にも適用可能にする（第3条）：EU圏内に在住する個人のデータのEU圏内で設立されていないデータ管理者による処理も同データ保護法の対象にする。
- 欧州委員会による十分性決定（adequacy decision）の明確化（第41条）
- 十分性決定によってカバーされていない国々への国際移転規則を拘束的企業準則（Binding Corporate Rules）等により強化し、簡素化する（第42条、第43条）

以上の他、パーソナルデータの匿名化については、法案本文ではなく、前文（23）に明記され、「保護原則は、特定されたか、特定されうる人に関するいかなる情報にも適用されるべきである」とされ、「データ保護の諸原則は、データの主体がもはや特定できないような仕方で匿名化されたデータには適用されるべきではない」とされている。

D) EU データ保護法案の改正プロセスの現状

前節では、EUデータ保護法改正案の概要を欧州委員会の通達に基づいて、主要なポイントのみ概観した。さて、同法案は欧州委員会の提出後、採択のために欧州議会と欧州連合理事会で審議される必要がある。2013年10月21日に、同法案は欧州議会での審議と修正（4000カ所以上）を経て、可決されている（賛成51票、反対1票、棄権3票）。なお、報道によれば[29]、欧州議会による可決まで、米インターネット企業、グーグル社やフェイスブック社が、欧州議会があるフランスのストラスブールやブリュッセルでEUデータ保護法案に反対する熾烈なロビー活動を行っていた。

欧州議会による原案の改正ポイント

以下に、欧州議会[30]や欧州委員会[31]の発表資料、報道記事等[32]を参考にし、欧州議会による原案改正のポイントについて記す。EUオブザーバーのニコラ・ニールセン氏によれば、全体的に、欧州議会による修正は基本的に欧州委員会の原案に沿っており、データ保護をさらに強化するものであり、米企業のロビー活動は実を結ばなかった。

第三国によるパーソナルデータ取得に抗する措置の設置

修正案では、2013年6月の米諜報機関による大規模監視活動に関する報道に答えて、第三国が企業にEU内で処理されている個人情報を暴露することを要求した場合、その企業はいかなるデータも移転する前に、当該国のパーソナルデータ保護監督機関に許可を得なければならないという条項が付け足された（第43条a）。これは、元CIA職員スノーデン氏の米諜報機関の活動に対する告発がEUデータ指令改正案に影響した結果である。

罰金額の増額

データ保護法に違反した企業は1億ユーロ、あるいは世界的な年間売上高の5%までの罰金を課されうる。原案では罰金を世界的な年間売上高の2%まで可能とするとしていたが、欧州議会の修正では罰金額がさらに強化された（第79条）。

[29] http://www.lemonde.fr/a-la-une/article/2013/06/02/tres-cheres-donnees-personnelles_3422477_3208.html

[30] http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU

[31] http://europa.eu/rapid/press-release_MEMO-13-923_en.htm

[32] https://www.twobirds.com/en/news/articles/2013/global/libe-committee-of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft

忘れられる権利と消去する権利

「忘れられる権利と消去する権利」（第 17 条）に関しては、「消去する権利」は「忘れられる権利」を含むとし、「消去する権利」という言葉だけが残された。この権利は修正により強化されて、データ管理者に消去が要求された場合、その企業を通して当該データを複製した企業にまでこの要求が通知されなければならない。

データ保護オフィサーの設置基準

250 名以上の組織に対して、データ管理者にデータ保護オフィサーを指名することを要求するとされていたが、12 ヶ月間連続して 5000 人以上のデータ主体のデータに関わる組織に要求すると修正された。つまり、ビジネスの規模ではなく、データが処理される人の数の観点から、データ保護オフィサーを指名する義務が発生することになった（第 35 条）。

EU データ法の範囲

原案では、EU機関はデータ保護法の対象外であると明記されていたが、修正案ではその文章は削除された（第 2 条）[33]。

バイオ計測データに関する規則の厳格化

仏パーソナルデータ保護監督機関CNILによれば、バイオ計測のデータに関わる規則が原案よりも厳格化された[34]。

ワン・ストップ・ショップメカニズムの修正

欧州議会により欧州委員会によって提案されたワン・ストップ・ショップメカニズムは修正され、「主導監督機関（lead supervisory authority）」という概念が導入された（第 54 条 a）。

新たな語の導入

修正案では、「仮名化されたデータ（pseudonymous data）」、「暗号化されたデータ（encrypted data）」、「プロファイリング（profiling）」、「第三者組織（third party）」という語が第 4 条定義に導入された。

なお、欧州委員会の発表では、欧州議会の修正では原案の最も重要な部分、すなわち、指令から規則への変更の維持（第 1 条）、非欧州国も欧州市場で事業を行う場合には欧州の法律に従わなければならないという条項（第 3 条）、忘れられる権利（第 17 条）、ワン・ストップ・ショップメカニズム（第 51 条）に関しては修正後も維持されたとしている。

欧州連合理事会での協議の状況

現在、欧州議会の採決後、各国の閣僚からなる欧州連合理事会へと審議の場が移っている。欧州連合理事会における協議は、2013 年 12 月 6 日の欧州委員会副委員長兼EU司法委員のヴィヴィアンヌ・レディング氏のスピーチによれば、2013 年 10 月に欧州連合理事会がワン・ストップ・ショップメカニズムについて一般的な原則に関して合意に至っていたが[35]、その後の審議で、議論が同メカニズムの詳細な部分に入り込み、結論に至っておらず、事態は後退している。

2013 年 10 月の欧州議会による可決の時点では、2014 年 5 月に実施予定の欧州議会議員選挙の前に最終的な法案可決が望まれていた。だが、2014 年 1 月 27 日の欧州委員会の発表では[36]、2013 年 12 月の審議の後退のせいで採択は遅れるが、最終的な法案の合意は 2014 年末までには可能であるとしている。しかし、実際には 2015 年にずれ込む可能性が高い[37]。なお、現行の 1995 年成立のデータ保護指令の交渉には 5 年が費やされている。

[33] http://www.euractiv.com/infosociety/data-protection-law-cover-eu-gov-analysis-528711
[34] http://www.cnil.fr/english/news-and-events/news/article/eu-data-protection-regulation-a-major-step-forward-at-the-european-parliament/
[35] 欧州連合理事会の報道発表資料：
http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138924.pdf
[36] http://europa.eu/rapid/press-release_MEMO-14-60_en.htm
[37] http://euobserver.com/justice/122853

改正法案の問題点としては、後述のEUオブザーバー等によれば、EU機関がEUデータ保護指令の対象外であること、ワン・ストップ・ショップメカニズムの定義の曖昧さ、複雑さがある。また、ドイツは公共部門を同法の対象外することを望み、また、英国、スロベニア、デンマーク、ハンガリーが、規則（regulation）という法的地位で提案された法案を指令（directive）へと修正しようとしており、改正プロセスを遅滞させている。

年一回ブリュッセルで開催される国際イベントである CPDP（Computers, Privacy & Data Protection：2014 年 1 月 22 日～24 日）では、EU データ保護法改正のパネルディスカッションが 2 回行われ、改正のポイントや今後の動向について議論された。パネルでは、できるだけ早く改正法案を成立させたい欧州委員会と、法文が厳格でないと主張するポーランドのパーソナルデータ保護監督機関の対立が浮き彫りになった。後者によれば、同案が最終的に成立する可能性もないとしており、今後の協議の難航が予想される。なお、パネルディスカッションの模様についてより詳しくは、本報告書第三部第三章に収録した同イベントの視察レポートを収録したので、そちらを参考にしていただきたい。

E) EU オブザーバー紙へのインタビュー調査

より詳しくEUデータ保護法の改正状況を知るために、EU向けニュースオンラインサイトであるEUオブザーバー紙[38]の記者ニコラ・ニールセン氏[39]にインタビュー調査を実施した。ニールセン氏は同ニュースオンラインサイトで、改正プロセスの動向について記事を執筆しており、また、2014 年 1 月 22 日から 24 日かけてブリュッセルで開催されたイベント、CPDP（Computers, Privacy & Data Protection）では、EUデータ保護法改正の現状について議論するパネルディスカッションで司会を務めていた。

日程:
2014 年 2 月 19 日（水）

場所:
ONOSO 事務所（フランス・パリ）：電話インタビュー
（○）先方：EU オブザーバー記者 ニコラ・ニールセン氏
（△）当方：ONOSO 研究員 小野浩太郎

インタビュー内容:

EU データ保護法改正を巡るロビー活動について
（△）EU データ保護法の改正を巡って、欧州議会があるストラスブールやブリュッセルでは多くのロビー活動が行われたと聞いている。どのようなロビー団体が活動していたのか。
（○）ロビー団体としては、グーグル社、フェイスブック社、HP社の他に、NGO等の様々な組織がいた。アメリカからだけではなく、欧州中から様々な組織が来ており、EUデータ保護法改正に反対する組織もあれば、賛同する組織もいた。なお、2013 年 10 月に欧州議会で可決されたEUデータ保護法修正案では原案の約 4000 箇所以上が修正されているが、LobbyPlagというウェブサイトで、原案に対して、欧州議会議員の誰がどの修正をしたか一覧できる[40]。
（△）欧州議会で改正法案が可決されたが、結局、どのロビー団体が勝ち、負けたのか。あなたのご意見を伺いたい。
（○）欧州議会は欧州委員会の改正法原案を強化する方向で修正したので、アメリカのロビー団体は負けたことになる。
（△）欧州議会は多くの点で欧州委員会提出の法案を支持したということか。

[38] http://euobserver.com
[39] http://euobserver.com/priv-immigration/121497
[40] http://lobbyplag.eu/map

（○）その通り。例えば、欧州委員会の原案では、罰金額を世界的な年間収入の 2%まで上げることが提案されていたが、それを欧州議会は 5%までに引き上げた。他の点では、データ保護オフィサーの設置基準を修正し、組織の従業員数ではなく、処理されるデータ主体の人数に変更した。

ワン・ストップ・ショップメカニズムについて

（△）ワン・ストップ・ショップメカニズムは欧州委員会の原案の重要な改正ポイントの一つであるが、欧州議会で修正されたと聞いている。同議会は同メカニズムを棄却したのか。

（○）欧州議会は欧州委員会の原案に沿う形で、ワン・ストップ・ショップメカニズムに係る条項を修正したのであり、つまり、議会は原案を支持した。だが、閣僚理事会は反対している。同理事会は、2013 年 10 月に同メカニズムに賛同していたのだが、12 月には反対に回り、この点に関しては協議に後退が見られる。現在、閣僚理事会の専門家グループで検討されているが、進展がない。

法案の改正プロセスが遅延している理由

（△）どの国が EU データ保護法の改正に反対し、遅延させているのか。

（○）特に、ドイツが遅延させている。ドイツは同法の適用範囲から公共部門が外れることを望んでいる。だが、このようなドイツの主張はおかしいという人々はいる。他には、英国、スロベニア、デンマーク、ハンガリーが、規則（regulation）という法的地位で提案された法案を指令（directive）へと修正しようとしている。

（△）フランスも反対しているのか。

（○）フランスについては詳しく覚えていないが、全般的には法案に賛同している。

（△）フランスでは CNIL が法案を支持していると聞いた。

（○）その通り。一般的に EU 加盟国のパーソナルデータ保護監督機関は、彼らの権限が改正法により強化されるので、法案を支持している。

（△）CPDP のパネルディスカッションでは、ポーランドのパーソナルデータ保護監督機関が改正に反対していたが。

（○）その通り。だが、これにはよくわからない点があり、驚きであった。ポーランド当局の代表者が言うには、改正プロセスは 2 年前に開始され、時間がかかりすぎており、欧州委員会は閣僚理事会において加盟国を説得する意志を欠いているということであった。

（△）いつ頃、同法案は採択されると思うか。

（○）2014 年に採択されると考えている人はほとんどいない。2015 年内の採択が目指されている。

元 CIA 職員スノーデン氏の告発の欧州におけるインパクトについて

（△）元 CIA 職員スノーデン氏の告発は欧州において大きなインパクトを持つか。

（○）その通り。多くの議論が巻き起こっている。欧州委員会と欧州議会は、スノーデン氏の告発によって明らかになった事実を EU データ保護法の改正のために利用しようとしている。そして、スノーデン氏の影響で、欧州議会による修正案では、非欧州国と欧州加盟国の間の法枠組みを定める第 43 条 a が導入されている。だが、国家安全の問題、つまり、スパイ行為等の取り締まりは、基本的にこの EU データ保護法案の範囲外である。

第二章　欧州諸国のパーソナルデータの利活用に係る制度

前章では、欧州のパーソナルデータ保護に係る法制度とEUデータ保護法の内容及び改正動向を概観した。EU指令は、その法の性質上、各加盟国で国内法化されねばならないが、EUデータ指保護令も各国内で国内法化されており[41]、欧州諸国のパーソナルデータ保護に係る法制度は同法に基

[41] EU データ指令の国内法化の状況については、欧州委員会司法総局のウェブサイトを参考されたい。
http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm

づき、策定されている。欧州主要国における国内法化状況に関しては、英国では 1998 年に「データ保護法（Data Protection Act）」が制定され、フランスでは 2004 年に「情報と自由に係る 1978 年法」[42]が修正され、ドイツでは 2001 年 5 月に「連邦データ保護法」[43]が制定されている。重要なことは、ビッグデータ等の利活用で問題になるパーソナルデータの匿名化については、EUデータ保護指令の範囲外であることである。なぜなら、匿名化されたパーソナルデータは同指令の範囲に入らないからである。従って、匿名化のガイドラインに関しては、各国で対応していると考えられる。以下に、匿名化を含めた欧州諸国（仏英）におけるパーソナルデータの利活用に係るガイドラインについて記す。

第一節　英国

A) ICO とデータ保護法

英国のパーソナルデータ保護監督機関は、ICO（情報コミッショナー事務局）[44]である。同機関の全人員は 388 名で、2013-2014 年度予算は 2000 万ポンドである。同国では、1995 年成立のEUデータ保護指令の国内法化に伴い、1998 年に「データ保護法（Data Protection Act）」が成立している。ICOの具体的な活動については、欧州におけるパーソナルデータの利活用事例及び悪用と漏洩事例に記した本報告書第四部第二章も参考にしていただきたい。

「匿名化：データ保護リスク管理実践規定」

同機関は、2012 年 11 月に「匿名化：データ保護リスク管理実践規定」という匿名化に係る実践ガイドブックを発表している。これはパーソナルデータ保護監督機関が作成した実践ガイドとしては欧州で初めてのものである[45]。同規定は、匿名化に係る諸問題を説明し、推奨される実践を示して、パーソナルデータを匿名化する必要がある組織（官民、第三セクター）を支援することを目的としており、匿名化の手段に関して法的拘束力を持つ諸規則を定めているわけではない。合計 100 ページ以上に昇る包括的な実践ガイドブックである。以下に要点のみ記す[46]。

- パーソナルデータに係るリスクの種類（私生活に関する情報が公になること、匿名化されたデータベースが攻撃され、個人についての情報が危うくなること、匿名化されたデータが再特定化されることによって、個人に諸問題が生じること、匿名化されたデータを漏洩した場合、公の信用が減ること、十分に編集されていなかった性質のデータが漏洩した場合の法的問題）
- 匿名化とパーソナルデータの定義（パーソナルデータの定義：ある個人をそのデータから特定可能なデータ、もしくは、そのデータと他の情報の組み合わせにより特定可能なデータを意味する）
- 匿名化されたデータの特徴（匿名化されたデータには英データ保護法は適用されない）
- 匿名化の利点（匿名化はデータ保護義務を遵守しながら、情報を公にすることを可能にすること、データが漏洩した場合に匿名化されていれば、法的制限が少ないこと、匿名化されていれば、データを収集した際の目的とは異なる仕方でデータを利用できること）
- パーソナルデータ定義の難しさ（個人は複数の異なる方法で特定されうる、つまり、一つ一つのデータは匿名化されていても、それらを組み合わせれば、特定可能になるし、ある組織がある個人のデータを匿名化して、公にしたとしても、他の組織が持つ他のデータにより再特定化されるかもしれないから。また、実際のところ、データが匿名化されているか、まだパーソナルデータのままか規定することは難しいことがありうる。事例の状況に基づいたふさわしい判断が必要となる）

---

[42] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676&dateTexte=
[43] http://www.bfdi.bund.de/EN/DataProtectionActs/DataProtectionActs_node.html
[44] http://ico.org.uk
[45] http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation
[46] より詳しい内容については英文文書そのものを参考のこと。

- 匿名化の効果（データの結合を通した再特定化のリスクは、どのようなデータが利用可能であり、将来的にどのようなデータが利用されるようになるか確かに判断することができない以上、本質的に予見不可能である。だが、再特定化のリスクは、ある特殊な目的のために必要な匿名化されたデータだけをリリースすることを促進させることによって軽減されうる）
- 匿名化と同意の関係（匿名化のプロセスには同意は必要ない。パーソナルデータの利用に同意が得られたとしても、匿名化されたデータを利用し、発表した方がより安全である）
- パーソナルデータと空間情報（GPSデータのような空間情報を扱う単純な規則は存在しない。ある幾つかの状況では、空間情報はパーソナルデータとなりうる）

以上の他、パーソナルデータと人権の関係、データの開示の仕方とリスク、パーソナルデータの管理運営、データ保護法とデータの研究向け利用免除規定について、具体例や関連する法制度とともに、パーソナルデータの匿名化の際の注意点や適切な実践が記されている。なお、ICOは現在ウェブサイト上で、匿名化実践ガイドに関する意見を同ガイドの改善のために募っている[47]。

UKAN（UK 匿名化ネットワーク）

ICOは、マンチェスター大学、サウサンプトン大学、オープンデータ研究院、国立統計学庁と提携し、パーソナルデータの匿名化について情報を提供するために、UKAN（UK ANONYMISATION NETWORK）を設立している[48]。UKANはICOが作成した「匿名化：データ保護リスク管理実践規定」の実践を支援している。UKANのウェブサイトでは、同組織にメール等で匿名化に関する質問することができるとともに、ケーススタディ等の関連資料を探すことができる。UKANのメンバーになれば、メンバー向けのサービスも受けることができる。このように、英国ではICOが匿名化に関する実践規定を作成するとともに、UKANという組織が詳しい情報提供の役割を担っている。

B) オックスフォード大学 オックスフォード・インターネット研究院における取り組み

オックスフォード大学に設置されたオックスフォード・インターネット研究院[49]では、ビッグデータの研究開発が積極的に行われており、開発の際には匿名化を行って、データを利用している。同研究院では、倫理委員会がプライバシー保護の方針とパーソナルデータの管理をチェックしている。また、匿名化は非常に重要なものと考えられており、取扱いに慎重を要するデータに関しては、データからいかなる個人情報も再特定化されえないように、匿名化の後でさえも暗号がかけられ、分離されて保存される。

オックスフォード大学 オックスフォード・インターネット研究院へのインタビュー調査（メールによる回答の抄訳）

回答日：

2014 年 2 月 26 日

回答者：

オックスフォード・インターネット研究院 ビッグデータ・リサーチオフィサー：タハ・ヤスリ氏

質問と回答

オックスフォード・インターネット研究院におけるビッグデータの研究開発活動について

« 質問»：オックスフォード・インターネット研究院には、何人の研究者がビッグデータの研究しているのか。

[47] http://www.snapsurveys.com/swh/surveylogin.asp?k=139089986579
[48] http://www.ukanon.net/
[49] http://www.oii.ox.ac.uk/research/

« 回答 »：ビッグデータに基づく研究とインターネットの社会学への量的アプローチに関わるフルタイムの研究者が 5-6 名いる。そして、社会科学におけるビッグデータの役割と倫理の問題を研究している研究者は 2-3 名いる。

« 質問 »：あなたのご意見では、なぜビッグデータは重要なのか。
« 回答 »：私は物理学のバックグラウンドを持つ計算社会科学者だが、私にとって、ビッグデータは社会システムを研究する大きなチャンスである。特にオンラインの社会システムを、量的枠組みで、また精密科学で発展した方法と概念を利用して研究することができる。これらのデータは 10 年前には利用可能ではなく、それ故、社会科学における研究は小規模の調査に基づく分析に限られていた。現在、これらのデータが利用可能になったおかげで、社会システムをその全体において、またサンプリングの問題と実験の偏りという問題を心配することなく研究できるだろう。今日では、個人に彼らが何を考え、何をしており、何をするつもりなのか質問する代わりに、我々は直接彼らの行動をリアルタイムで追跡することができる。これは生物学における顕微鏡、天体物理学における望遠鏡の発明に非常に似ている。

« 質問 »：あなたのビッグデータに係る最近の研究プロジェクトについて簡単に教えていただきたい。
« 回答 »：1996 年から 2010 年にかけて、全ての「.uk」ドメイン名のウェブページを含む英国内のウェブアーカイブに基づく研究を実施している[50]。このデータセットは 30 テトラバイトの量があり、これにより、国レベルでのウェブの歴史とその進展を、時期を限定し、高い精度で研究できる。

« 質問 »：オックスフォード・インターネット研究院には、ビッグデータの法的側面について研究している研究者はいるか。
« 解答 »：とりわけ法的側面に研究している研究者はいないと思うが、ラルフ・シュレダー博士とエリック・メイヤー博士はビッグデータの研究開発に係る倫理的側面のような問題、すなわち、ビッグデータ研究と関連する新しい規則の定義と境界、持続可能性とリスクの問題に関心がある。

« 質問 »：英国政府はビッグデータの研究開発とビジネスの振興に積極的であるか。
« 解答 »：私が知る限りでは、英国政府はオープンデータに非常に積極的であり、政府の多くのデータセットがポータルサイトで公表されている。我々の組織でも、政府の様々な部署と一緒に、長期間の協力関係を設立することを目指して、実行可能性と概念実証のプロジェクトを実施している。

ビッグデータ向けパーソナルデータの匿名化について

« 質問 »：英国には、プライバシー保護を目的とするビッグデータ向けの匿名化に係る公式ガイドラインは存在するか。
« 回答 »：これは非常に重要な問題であり、日本政府がこの問題に取り組んでいるのは興味深いことである。私が知る限りでは、特にビッグデータに係るプライバシーの問題のために準備された国家レベルでの方針は存在しない。政府の様々な部署はそれぞれ固有のプライバシー方針のガイドラインを持っている。例えば、国民保健サービスは、固有のデータ共有協定を持っており、保健に関するデータを研究者が利用する際に署名しなければならない利用規約がある。オックスフォード大学も同様に、固有のパーソナルデータに係るガイドラインとプロトコルを持っている。我々の組織では倫理委員会が非常に積極的であり、この委員会はプライバシー方針とパーソナルデータの管理に関して、組織内の全てのプロジェクトが関わる倫理問題の認可に責任がある。

[50] http://www.oii.ox.ac.uk/research/projects/?id=88

パーソナルデータの利活用事例と匿名化について

« 質問 »：英国におけるパーソナルデータの利活用を伴うサービスの事例について教えていただきたい。
« 回答 »：私はオレンジ社（フランス・テレコム）の「発展のためのデータ（Data for Development）」に関するプロジェクトを知っている[51]。このプロジェクトでは、モバイルユーザーの電話通信データを匿名化して開放することによって、多くの研究者に社会の発展に係る革新的な研究を行うチャンスが与えられる。

オックスフォード・インターネット研究院には、ビッグデータのスピンオフ企業はない。ところで、研究院内のプロジェクトにおいて、匿名化は非常に重大なものと捉えており、データからいかなる個人情報も再特定化されえないように、匿名化の後でさえも、取扱いに慎重を要するデータには暗号がかけられ、分離される。

第二節　フランス

A) CNIL と情報と自由に係る 1978 年法

フランスでは、CNIL（情報と自由に国家委員会）[52]がフランスにおけるパーソナルデータ保護監督機関として積極的に活動している。同機関は[53]、17 名の理事会を含め、全部で 174 名の人員を持ち、予算は年間 1600 万ユーロである。同機関は「情報と自由に係る 1978 年法」（以下、情報と自由法と略す）[54]に基づき、データ保護に係る活動を実施している。情報と自由法はEUデータ保護指令の制定に伴って、2004 年に改正されている。CNILはパーソナルデータ保護担当者を企業等の組織内に設置することを促しており、その担当者は「CIL（Correspodant informatique et libertés）」[55]と呼ばれる。組織はCILを設置することにより、CNILとのやり取りを簡便化する等の利点がある。なお、CNILは仏ICT部門研究機関INRIA等と提携し、プライバシー・バイ・デザイン原則を実現する新しいデータ保護技術の開発にも参加している[56]。

パーソナルデータの匿名化に関するCNILに対する電話インタビューへの回答では、CNILが匿名化の手段や方法を強制することはなく、各企業がそれぞれ匿名化に対応しなければならない。また、CNILはパーソナルデータの管理に関して、対象となる組織の調査を行っているが、調査の際に匿名化の方法が情報と自由法に触れないかどうか精査している。逆に、企業から匿名化の方法に関して、助言を求められた場合にはそれに対応している。

CNIL の具体的な活動については、欧州におけるパーソナルデータの利活用事例及び悪用と漏洩事例に記した本報告書第四部第二章も参考にしていただきたい。

a) 情報と自由法とビッグデータ ：「ビッグデータと個人情報保護：（ほとんど）不可能な挑戦？」

テレコム・パリテックの個人情報の価値・政策講座の共同責任者であるクレール・ルバロワ=バルト氏[57]は、個人情報保護の法・政治・経済・社会的側面について同校で月一回研究者等による講

[51] http://www.d4d.orange.com/home
http://www.d4d.orange.com/learn-more
[52] http://www.cnil.fr/linstitution/qui-sommes-nous/
[53] http://www.cnil.fr/linstitution/qui-sommes-nous/
[54] http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/
http://www.cil.cnrs.fr/CIL/spip.php?rubrique281
[55] http://www.cnil.fr/linstitution/missions/informer-conseiller/correspondants/
[56] http://www.inria.fr/equipes/privatics
[57] http://cvpip.wp.mines-telecom.fr
https://webperso.telecom-paristech.fr/front/frontoffice.php?SP_ID=33&

演会を開催する等、パーソナルデータ保護に関して積極的に活動している。テレコム・パリテックの卒業生向けの雑誌「テレコム」(2013 年 7 月第 169 号)[58]に寄稿された同氏の解説文「ビッグデータと個人情報保護：（ほとんど）不可能な挑戦？」は、簡単にビッグデータの問題点と仏「情報と自由法」の関係を解説しており、同法を理解するための参考となる。以下に同解説文の要点を記す。

1) 「パーソナル」データとは何か？

フランスの「情報と自由法」第 2 条はパーソナルデータの定義に関わるが、それによれば、直接的な記名情報（名字・名前、住所、メールアドレス等）と間接的な記名情報（電話番号、位置情報、行動の断片的情報等）が入る。この点から、EUの第 29 条作業部会とCNILはIPアドレスも例外なくパーソナルデータと考えている。情報がある個人に関係する時、その情報はパーソナルデータである。

2) パーソナルデータは匿名化可能か？

匿名化は、様々な手段を通して（匿名化、仮名化、不可逆な暗号化等）、情報と個人のアイデンティティの結びつきを破壊することにある。実際には、人物を特定化できないようにすることは難しい。なぜなら、情報間の可能な交差を考慮しなくてはならないからである。ところで、ビッグデータはオープンデータとともに、交差の可能性を著しく増大させるので、人物の特定化の可能性も増大させる。では、データの量が人物の特定の可能性を増大させるので、匿名は不可能であるのか。一つの結論が可能である。それは全てのデータはパーソナルデータとして見なされなければならず、従って、情報と自由法の適用範囲に入るというものである。だが、このような結論は反生産的であると我々には思われる。この結論は（匿名化する意義が薄れることから）諸々の組織に匿名化を止めることを促してしまい、パーソナルデータとプライバシーの侵害の危険を増やしてしまうだろう。人物を特定不可能にする操作は幾つものビジネルモデル（保健や行動ターゲッティング広告等）の重要な構成要素となっている。他方で、人物が特定できないように加工された情報は、常に再特定化のリスクがあるとしても、常に人の根本的な権利への侵害を減らしている。

3) どんなパーソナルデータを収集するのか？

情報と自由法の第 6 条によれば、パーソナルデータは「規定され、明示的で、正当な」目的（すなわち、用途）のために収集され、処理されなければならない。データは後からこれらの目的と相容れない仕方で処理されてはいけない。この目的の原理は、データの性質原理の前提条件である。他方で、データの保存期間は目的に必要な期間を超えてはいけない。この期限を過ぎたら、データは破壊されなければならない。こうして、忘れられる権利が現れる。しかし、これらの規則は大量のデータが保存されている場合、どのような意味を持つのか。また、情報の可能な利用を先取することが難しい場合、データの最小限の収集とその消去の原理がビッグデータの定義そのものと矛盾する場合、どのような意味を持つのか。自分自身によるデータと情報イメージの管理の問題が提起される。

4) 関係する人物にとってどのような管理が可能か？

この問いはデータが創出されたことを知らされることが前提となっている。情報と自由法の第 32 条によって認知されているこの通知される権利は、データの収集と同様に利用にも関わる。この権利は最も重要である。なぜなら、この権利はパーソナルデータへアクセスする権利と異議権の行使を条件づけているからである。収集されたデータが迅速に匿名化される場合には、この権利は軽減される。また、この権利は人物への通知が不可能であり、難しい場合には除外される。真の力を与えるのは「同意」である（情報と自由法の第 7 条で規定）。同意は、「自由で、特殊な、通知された

[58] http://cvpip.wp.mines-telecom.fr/files/2013/11/TELECOM_169extrait_C_Levallois_Barth.pdf

意志のあらゆる発露」（EUデータ指令第二条で定められた同意の定義）を指し示す。これは、許可は特殊で、規定されたコンテキスト内で与えられなければならないことを意味し、とりわけCNILによれば、米グーグルの実践はこれに対応していない[59]。また、同意が遠回しである場合もあることが確認されている。

我々は同意の原理を適切であると考えているが、この原理の輪郭を規定することはしばしば難しいことが明らかになっている。おそらく、ビッグデータは「一般関心」の目標を追求しうるし、社会全体に重要な有益をもたらすことができるという事実を考慮して、自由と情報法で定められている例外事項のリストを少し拡大させることが適切である。GPS のデータを研究して、研究者は 80%以上の正確さで、80 週間のある人物の地理的な位置を予見することができることを示した。しかし、この点に関しては警戒することが必要である。なぜなら、予見は人物の人格、特にその行動と経済的状況を規定し、分析することを可能にするからである。これは差別の可能性を垣間見させている。

5) 来るべき改革

この点からして、いかなる疑いもなく、輪郭を設定することが根本的自由の保護に対する主な課題の一つを構成する。ビッグデータがいかなるトレーサビリティと責任の外で、ブラックボックスにならないことをいかに防ぐのか。この問、そして、その他の問に、EU データ保護指令の改正は答えようとしている。

b) 匿名化の問題：「私的生活のリスク管理ガイドブック」における匿名化の実践方法

CNILは、2012 年 6 月に「私的生活のリスク管理」と呼ばれるパーソナルデータ保護に係るガイドブックを発表している。第一部はデータ保護に係るより一般的な方法論[60]に、第二部は適切な実践例[61]に捧げられている。匿名化については、「私的生活のリスク管理ガイドブック」の第二部第一章で、推奨する実践方法について記されている。以下に、その概要を記す。

一般原則

- 匿名化されなければならないものを特定すること（コンテキスト、パーソナルデータのストック形態、リスク等に応じて）
- 不可逆的な仕方で匿名化すること
- 匿名化されなければならないものが不可逆的な仕方でそうされ得ない場合には、機能的な要求を最も満たすツール（部分的消去、暗号化、ハッシュ化等）を選択すること

データベース上のパーソナルデータの匿名化に対する推奨

○ パーソナルデータを不可逆的な仕方で匿名化するためには、

- データを部分的に消去すること
- 秘密コードを伴うハッシュ化を適用すること
- 本人を特定できるパーソナルデータを中立的な文章（☆や同一の文字等）に置き換えること

○ パーソナルデータを不可逆的な仕方で匿名化できない場合には、

59 http://www.cnil.fr/linstitution/actualite/article/article/regles-de-confidentialite-de-google-une-information-incomplete-et-une-combinaison-de-donnees/

60 http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf

61 http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf

・ 元のデータに対応するかどうか匿名化されたデータをチェックする必要があるならば、秘密コードを伴う SHA-256 を利用すること、さらに、二つの異なる組織によって保持される二つの秘密コードにより二重の匿名化を行うこと
・ 元のデータを見つける必要がある場合には、暗号を利用すること

○ 開発や試験段階では、匿名化されたパーソナルデータや虚構のデータだけを利用するには、

・ 匿名化された試験のために特殊なソフトウェアを利用すること

原文の電子文書上のパーソナルデータの匿名化に対する推奨

・ フランスパーソナルデータ対応者協会（AFCDP）が策定した匿名化措置の基準に対応する措置を利用すること
・ 一定のソフトウェアにより匿名化された文書は、手作業で匿名化された箇所をチェックすること

以上のように、CNIL の「私的生活のリスク管理ガイドブック」では匿名化の実践方法について記されている。このガイドブックは、匿名化の実践方法について推奨事項、注意点を挙げているだけであり、法的拘束力がある文書ではない。

B) 米グーグル社に対する CNIL の動向

米グーグル社の新プライバシー・ポリシーに対する CNIL の動向

仏 CNIL は欧州諸国を代表して米グーグル社の欧州における事業展開を調査している。以下、CNIL とグーグル社の動向を時系列に沿って記す。

2012 年 10 月 16 日のCNILの発表によれば、同日、EU第 29 条作業部会がグーグル社の新プライバシー・ポリシーに関して、同社に勧告状を送っている。2012 年 1 月 14 日に、グーグル社は同年 3 月 1 日から秘密保持に係る新規則及び同社のほとんど全てのサービスに適用可能な新しい利用条件が有効になることを告げていたが、欧州では、同社に対して第 29 条作業部会が仏CNILに委任して、新規則に対して調査を実施した[62]。CNILは二つの質問状を送付し、4 月 20 日と 6 月 21 日に続けて返答を受けたが、不完全なものであり、グーグルはEUデータ保護指令の本質的な原則を遵守しているとは言えないことが明らかになった。新規則には、パーソナルデータの収集の範囲と潜在的な用途に関わる制限が欠如していた。まず、グーグルは、ユーザーにパーソナルデータの処理について十分な情報を与えていない。グーグルが提供する一つのサービスのユーザーは、このサービスにどのようなパーソナルデータが利用されているのか、そして、これらのデータが処理される正確な目的を決めることが不可能である。つまり、全てのデータが規則に明記された全ての目的に無差別に利用されうる。ついで、新規則では、複数のサービス間でのデータの結合が一般化されるが、それに対するユーザーによるコントロールが可能ではない。この結合は異なる目的が追求する。さらに、グーグルは処理されるパーソナルデータの保存期間を明確にしていない。以上の理由から、EU第 29 条作業部会は、グーグル社の新プライバシー・ポリシーはEUデータ保護指令に則っていないと判断し、同ポリシーの変更を求めるため、各EU加盟国のパーソナルデータ保護機関により署名された勧告状を送付した[63]。なお、これらの勧告に対して、アジア・太平洋諸国の幾つかのパーソナルデータ保護監督機関が支持を表明している（オーストラリア、香港、マカオ、メキシコ、カナダ）[64]。

62 http://www.cnil.fr/linstitution/actualite/article/article/regles-de-confidentialite-de-google-une-information-incomplete-et-une-combinaison-de-donnees/
63 http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf
64 http://www.cnil.fr/fileadmin/documents/en/APPA_SUPPORT_LETTER-Article_29_Letter.pdf

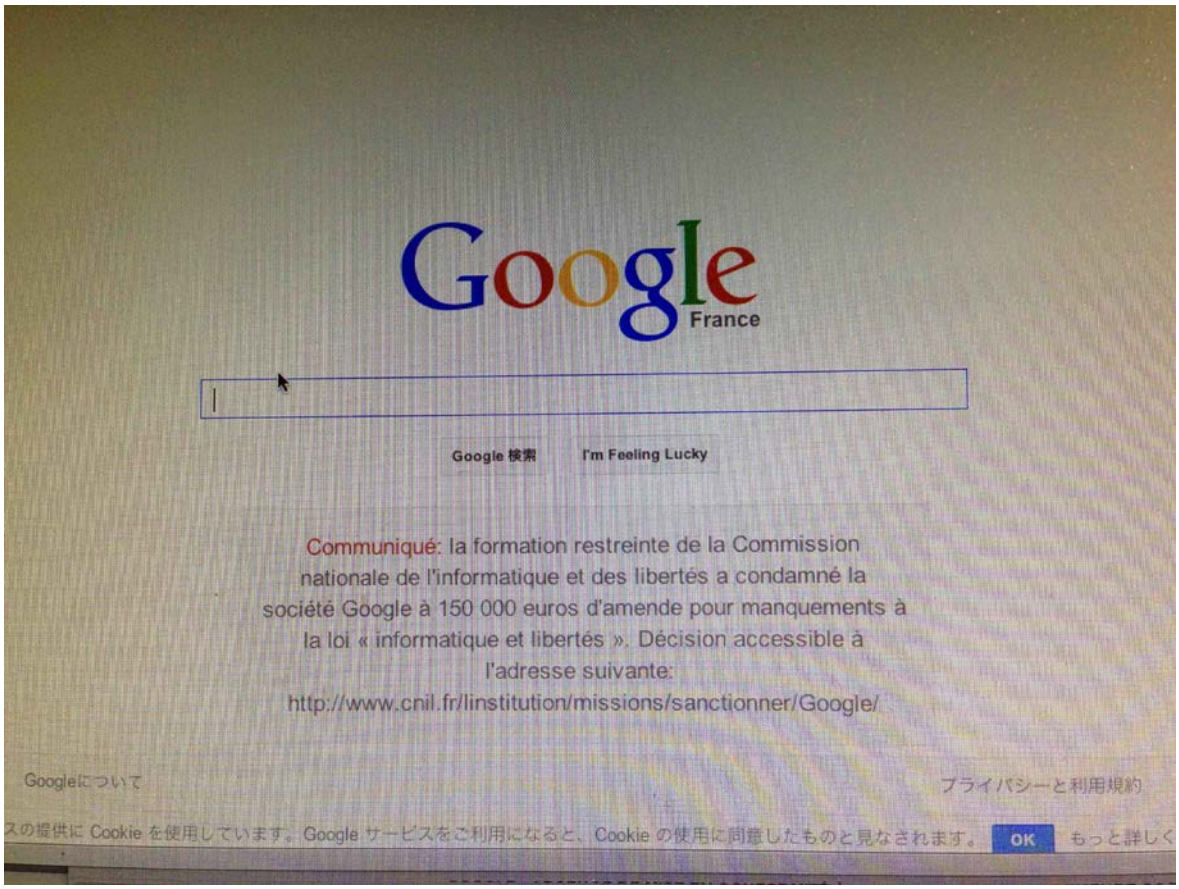
2014 年 1 月 8 日のCNILによる発表によれば[65]、同年 1 月 3 日に、CNILはグーグル社に対して、同社のプライバシー・ポリシーがフランスの情報と自由法を遵守していないとして、15 万ユーロの罰金を課した。罰金額は、CNILが下せる最高額の罰金であり、象徴的な意味は大きいと考えられている。また、罰金の他に、グーグルの仏検索サイト（https://www.google.fr）上に、この議決に関する通知を 48 時間載せることを命令している。次の点がCNILの以上の議決理由である。

1. グーグル社はユーザーに対して、十分に彼らのパーソナルデータの処理の条件と目的を知らせていない。ユーザーは収集の目的と収集されたデータの規模を理解できず、彼らの情報アクセス権、異議権、消去権を行使できない。
2. 同社はユーザーの端末上のクッキーの利用に関して、ユーザーの同意を得る義務を遵守していない。
3. 同社はパーソナルデータの保存期間を規定していない。
4. 同社はサービス全体を通して、パーソナルデータの結合を法的根拠なく行っている。

なお、CNIL の議決は、2013 年 11 月と 12 月にオランダとスペインのパーソナルデータ保護機関がそれぞれ下した結論と類似している。

このようなCNILの対応に対し、グーグルは 2 ヵ月以内にCNILの処分を不服としてコンセイユ・デタ（仏行政最高裁判所）に提訴が可能だった。2014 年 1 月 14 日に、同社はコンセイユ・デタにCNILの議決の部分的な停止を要求したが、翌月 2 月 7 日に同機関はグーグル社の要求を却下している[66]。

参考：https://www.google.fr 上に掲載されたCNILの議決に係る通知



65 http://www.cnil.fr/english/news-and-events/news/article/the-cnils-sanctions-committee-issues-a-150-000-EUR-monetary-penalty-to-google-inc/

66 http://www.cnil.fr/linstitution/actualite/article/article/le-conseil-detat-rejette-la-demande-de-suspension-de-google-inc/

グーグル南・東欧、中東、南米及びアフリカ社長講演

グーグル社の南・東欧、中東、南米及びアフリカ地域の責任者であるビオンド＝ダサロ氏は、在仏イタリア文化センターで「技術、革新と自由」という講演をし、グーグル社の活動について講演をしている。以下に、講演の要約を収録する。

1. 講演者：カルロ・ビオンド=ダサロ（グーグル南・東欧、中東、南米及びアフリカ社長）
2. 演題：「技術、革新と自由」
3. 日時：2014 年 1 月 17 日
4. 場所：在仏イタリア文化センター（在仏イタリア大使館内）
5. 参加者：情報通信研究機構 欧州連携センター長 菱沼宏之、情報通信研究機構 欧州連携センター 菅野さおり
6. 概要：

我々グーグルが関わるインターネットの 2 面性について話をする。1 つ目はコミュニケーションのツールとして、2 つ目は顧客と企業の関係性についてである。インターネットは、歴史的にはフランスでコミュニケーションの役割を担い、また英語圏にて発展してきたと言えるだろう。今日においてグーグルが画期的な存在と言えるのは、顧客と企業の関係を担う枠組みを今までにない形で提供していることだ。企業における顧客との関係性は、費用や物理的な面などで経済的や様々な制限があったが、インターネットの普及により、個人企業のような小さな企業でも安価にインターネットを通じて顧客を呼び寄せることができるようになった。旅行や保険などでも、顧客が自主的に比較できることなどは、インターネット普及以前には難しかった。

グーグル・グラスの開発については皆さんご存知かと思うが、今日ではコンタクトレンズも開発されている。今後益々繋がっている「モノ」は増えていく。

もちろん、インターネット普及によるネガティブな面というのがあることも否定はできない。例えば、新聞だと、ラ・トリビューン紙で 5 億人のネット読者がいる。イタリアやフランスの小規模新聞では 2 千万人の読者しか無いので、存続するには、さらに大量に売らなければならない。それ故に「データ(情報)」はとても大切となる。

＜（会場からの）質問（以下同じ）＞（個人データの流失・濫用の危惧を前提として、個人が)予め興味のある分野を登録しておき、それに基づいて「お知らせ機能」を付けるのは有効ではないか？
≪回答≫例えば、私がグーグル・グラスを掛けて一日を過ごし、次回の旅行についていろいろと探していたとする。そして夜に自宅で新聞をネットで読んでいると、私が探している旅行へのプロモーション（優待価格等）が出るサービスは、素晴らしいと言えるのではないか？このようなサービスは常に事前登録お知らせ事項のみでは難しい。グーグル以外にも同様のシステムは既にあるが、どうやってその情報を共有するかが問題だ。

＜質問＞（グーグルが節税のために所在地を変えていることについて、)グーグルがフランスで税金を払わないことは正当なのか？
≪回答≫グーグルはむしろ透明性があると主張させて頂きたい。どうやって既存のシステムを変化させ利益を出せるようにするのか、ということは多国籍企業の優先課題だ。例えば、エールフランスがグーグルの枠組みを通して日本又はドイツなどの商品を購入する際、一体どの時点で費用と利益が発生し、どこの国へ税金を支払うべきなのだろうか？あるフランスのサイトが米国の翻訳サービスを使った場合は？そしてそのフランスサイトへの顧客が全世界にいるという場合は？「税金」についての明確な規定と、ある国の発展との関連も見る必要がある。グーグルに限らず、多国籍企業では特に現在の経済危機を乗り越えるために経営戦略において税務は重要な位置を占めている。

＜質問＞グーグルは地域支援や開発支援などを行っているのか？

≪回答≫もちろん沢山行っている。詳しくは是非グーグルのサイトをご覧頂きたい。
例えば、100 人以上のグーグルのエンジニアがある小さな地域を支援するとしよう。これはグーグルにとって宣伝効果はある。しかしながら、その地域企業は、自己成長が 1 番で、グーグルのことは 2 番となるだろう。
グーグルは、最終消費者を常に考えて変革をしている。コミュニケーションのありかたの変化と、生活習慣の変化を受け入れていくしかない。例えばグーグルは 1 ユーロからの採算性を考えてシステムを作った初めての企業だ。これは画期的なことで、従来の企業からすると最も透明性があると言えると思う。顧客との関係が最重要であることから、顧客がメールを見たかどうかの比率を把握することは必然だ。だからこそ、その枠組みを作る必要があった。

＜質問＞NSA（米国家安全保障局）についてはどう思うか？もし貴方が米大統領だったら？
≪回答≫私が米大統領だったらすぐに NSA は停止するよ、というのは冗談だが、私にはその質問には答えかねる。我々グーグルとしての「創造」と「私生活の保護」は常に非常に重要な問題としてせめぎ合いが続き、また必然的にこれからも続いていく。しかしながら、時代と共に発展を選択せざるを得ないだろう。米国及びアジアは問題が予想されても発展と実益のためにリスクをとる傾向があるが、欧州は理念が優先されるという違いがあると言える。

＜質問＞表現の自由があるのに度々Youtube 上の投稿などをグーグルが削除をするのはなぜか？反ユダヤ主義を扱った演劇が Youtube から削除されたケース、つまり演劇では表現可能なものでも削除対象になるか？
≪回答≫ポルノ、暴力、反ユダヤ主義など削除に値するのが明白なものもあるが、報道やテレビからの流用などグーグルとしても大変難しい問題となっているものもある。あらゆる広告にも法律があるように、表現の自由とインターネットの関係は、グーグルだけでは結論は出せない。

＜質問＞法的に良いものしかダメなのか？
≪回答≫「良い」という定義が曖昧過ぎる。私が元々カトリックで、次第にプロテスタント的になり、また中東で生活をするうちにイスラム文化の素晴らしい点を発見し感銘を受けるとする。今まで「良い」と思っていた物事よりも違う「良い」ができる。また、イタリアにおいて私は個人的には左派を支持する。というのも、イタリア左派は個人主義的だからなのだが、フランスでは左派はむしろ集団的だ。
グーグルに応募をしてくるエンジニア達の一番の志望動機は何だと思われるか？私はグーグル以外の IT 企業でもエンジニア達と関わってきたが、グーグルに限らず、IT 系エンジニアの一番の動機はお金だ。企業はビジネス創造と、より早い成長を大切にする。「より良い」とは個人個人によって大きな違いがある。

＜質問＞フランス個人情報保護法の監視機関であるとともに EU 全体の保護機関である CNIL の法律にグーグルは違反していないのか？
≪回答≫当然ながら CNIL との争いは続いている。個人情報を保護することは大切で、この点に関するグーグル内の規定を変えようとしている。しかしながら、多国籍企業なので、全世界のあらゆる国の法律に合わせることは残念ながら不可能だ。

C) AFCDP の匿名化措置の基準

フランスでは、AFCDP[67]と呼ばれるCIL（組織内のパーソナル保護担当者）及びステークホルダーを組織する協会があり、イベントを実施する等、積極的な活動を行っている。同協会は「基準とラベル」という作業部会を設立し、2008 年 5 月に、パーソナルデータの匿名化手段が持たなければならない諸機能を特定した基準表を策定しており、これはステークホルダー団体の自主規制の試みと言える[68]。以下にその基準表の概要を記す。

基本基準

1. 匿名化措置は機能的な関係と依存を保持しながら、パーソナルデータの抽出を可能にしなければならない。
2. 匿名化措置は匿名化手段に広い選択を提案しなくてはならない。（貧窮化、マスキング、消去、暗号化、ずれ、虚構データの創出か、虚構データによる置き換え、データの混合、ハッシュ化、分散化、連結、難読化）
3. 匿名化措置は、各データのタイプに対して、目的と制約に応じて適切と思われる技術を選択することを可能にしなければならない
4. 匿名化措置は、これらの匿名化手段の柔軟な利用を可能にしなければならない（例えば、データの種類に応じて、手段を使い分けることができなければならない）。
5. 匿名化措置は、特定のデータに置き換えるために、固有のデータ集合を作り、持ち込み、利用

[67] http://www.afcdp.net/-Pourquoi-l-AFCDP-
[68] http://www.afcdp.net/L-AFCDP-publie-un-Referentiel-des

することを可能にしなければならない（虚構データの使用）。

6. 匿名化措置は、同じデータに対して、複数の技術を連結することを可能にしなければならない（マスキングと置き換えの組み合わせ等、二種類の技術の連結）。

7. 匿名化措置は、その実施者に匿名化作業が行われる秩序を制御することを可能にしなければならない。

8. 匿名化措置は、関係を保持しながら、（目標となるデータの）単純化の後でデータの装填を可能にしなければならない。

9. 匿名化措置は、その実施者に、可逆化の試みに対して（単純化されたデータから元のデータを獲得する）適切な抵抗を与える変形戦略を構想することを許す、匿名化技術の選択と構成の柔軟さを提案できなくてはならない。

10. 匿名化措置は、後に利用できるように、異なる方法の連結によってなされた匿名化諸戦略の記録を許さなければならない。

11. 匿名化措置は、フランス語で書かれた資料を利用可能にしなければならない

拡大基準

12. 匿名化措置は、ある期間の間で特定不可能な同一人物の書類を追跡できなければならない。

13. 匿名化措置は、データの単純化戦略構想の責任者に一つの結果を獲得させることを許す技術の選択を提案しなければならない。

D) アライアンス・ビッグデータのビッグデータ倫理憲章

仏ビッグデータのステークホルダー団体であるアライアンス・ビッグデータは、ビッグデータの利活用に係る「ビッグデータ倫理憲章」を発表しており、パーソナルデータ保護監督機関とは別に、ビッグデータの倫理的側面に対応しようとしている。同憲章はパーソナルデータの管理と処理を行う組織向けの一種のチェックリストであるが、アライアンス・ビッグデータの責任者へのインタビューによれば、同団体は倫理憲章をさらに発展させ、この憲章に明記された諸基準を遵守している企業のために「ラベル」を作成することを目指している。

アライアンス・ビッグデータへのインタビュー調査（メールによる回答の抄訳）

回答日：
2014 年 2 月 10 日

回答者：
アライアンス・ビッグデータ ポータルサイト編集委員長 ： シャルル・ユオ氏
アライアンス・ビッグデータ 事業責任者 ： アレクサンドル・ウェイズ氏

質問と回答：
アライアンス・ビッグデータの活動について
Q）いつ、どのような理由でアライアンス・ビッグデータは創設されたのか。
A）同団体は、公式には 2013 年 3 月 21 日にデジタル経済職業協会（Aproged）、キャップ・デジタル（デジタルサービスとコンテンツ産業クラスター）、GFII（フランス技術革新産業団体）、ADBS（情報・文書活用職業協会）、鋼業・テレコム研究院（フランスの工学系高等教育・研究機関）によって、ビッグデータに対する共通のビジョンを共有するために設立された。しかし、ビッグデータのステークホルダーからなる一種の連合体を創設するアイデアは、ビッグデータがいたるところで

バズワードになっていた2012年に生まれた。

Q）あなたがたの主な活動は何か。
A）我々の主な活動は、ビッグデータによる新しいビジネスチャンスを生かすために、フランスでビッグデータのエコシステムのために活動し、また欧州の他の連合体と交流することである。まず、ビッグデータについて最大限多くのニュースを一同に集めるインターネットポータルサイトを製作した。このサイト[69]は現在も存続しており、現在完全リニューアル中である。新しいウェブサイトは2014年3月に完成する予定である。ついで、我々はビッグデータを巡る情報を伝達するために、他のメディア媒体について考え、1ヶ月に2度、ニュースとインタビューを3分間放映するビッグデータTVを立ち上げた[70]。ビッグデータに関わる全ての企業名録（スタートアップ企業から大企業まで）が、数週間後にはポータルサイトに付け加えられる予定である。このアイデアは、各企業がビッグデータの製品と経験を示し、証明する公の空間をつくることにある。最近の活動はというと、6ヶ月以来ソーシャルネットワークを立ち上げており、今日では400以上のメンバーがいる。さらにビッグデータに関するイベント[71]を開催している。

Q）アライアンス・ビッグデータには、いくつの組織が参加しているのか。
A）現在、同団体のメンバーは20組織以上である（キャップ・デジタル、Aproged、GFII、ADBS、Adetem、Finance Innovation、Systematic、ラ・ロシェル大学、鋼業・テレコム研究院、the Economic Warfare School of Paris (EGE)、Groupe IES ESCP Europe Alumni、Cigref、SFIBなど）。だが、我々の日々の活動を支援してくれるスポンサーはほとんどいない。

Q）フランス政府は、ビッグデータの研究開発やビジネスの展開に積極的であるか。
A）フランス政府はビッグデータに関して非常に積極的である。我々は政府の依頼提案（Request for proposal）をフォローする等して、デジタル分野での政府の主導政策と緊密に結びついて活動している。我々の団体はフランスにおけるビッグデータに関する情報の「中継点」の役割を担っている。政府は我々の団体を、ユーザーケース、ニュース、企業名録、才能ある企業のプッシュアップなど、ビッグデータ全体の情報プラットフォームを展開するために利用しようとしている。また、フランスの新産業政策「新しいフランス産業」[72]のビッグデータ担当者ともコンタクトを持つ。

ビッグデータ倫理憲章について
Q）なぜ、あなたがたは倫理・ビッグデータ憲章を策定したのか。市民やフランスの企業、政府から要求があったのか。
A）例えば、フランスでは、公共機関はこの種の問題に包括的に対応していなかった。ビッグデータ倫理憲章の実践は、いわゆる「規範的な責務」ではないが、企業が秘密に係る権利の遵守について記された憲章を読み、チェックリストを埋めることによって、同問題に答えようとする最初の回答である。企業の道徳性の大部分はこの文書において保証される。我々のゴールは、憲章の第二ステップにあり、憲章により明記された諸基準を遵守している企業のために「ラベル」を作成することである。
　フランスにおいて、信用はビッグデータによるビジネスの展開の本質的な構成要素である。憲章は、データ処理に関してプロジェクト実行者に透明性を保持させる教育的な意義がある。

[69] www.alliancebigdata.com
[70] チャンネルには以下のアドレスからアクセスできる。
http://tinyurl.com/mjc748c
[71] http://www.congres-fan.com/
[72] http://www.redressement-productif.gouv.fr/files/la-nouvelle-france-industrielle.pdf#page=27
www.innovation2030.org/pdf/Rapport_Innovation_BDV4.pdf

Q）フランスの企業は、プライバシー侵害を避けつつビジネスを展開するために、パーソナルデータの利活用について心配や懸念を抱いているか。
A）フランス企業の創造性は、他のよく知られた企業と同じようにパーソナルデータを好き勝手に扱うことにはない。将来、我々全員が向かっているデータの世界で、各人はパーソナルデータを、それを利用し、変形し、価値を付加する企業へと制限された仕方で与えるだろうし、それは当人の恒常的な許可を伴うものだろう。これは、幾つかの非常に興味深い医療アプリケーションのケースである。我々全てが直面するのは、例えば、我々のパーソナルデータが保険に加入する際の主要な、あるいは唯一の仕方になるかどうかという問題である。また、この例では、忘れられる権利は中心的なポイントになるだろう。もしあなたが 20 代の時に病気であったとして、45 歳の時にローンを借りることができないとすれば、どうだろうか。だれがこのような世界を望むだろうか。我々の生活の仕方に対する繊細な考察においては、一般の人々の復元力を信用することが必要である。

Q）どのようにビッグデータ倫理憲章を使うのか。
A）憲章は企業にとって勧告及びチェックリストとなり、企業がそれを埋めることによって、どのように、展開しているビジネスが、収集されるパーソナルデータに対して人々が持つ権利とつながっているのか意識することになる。我々が作成しようとしているラベルは、企業家精神の育成を支援することになろう。

フランスにおけるビッグデータのためのガイドラインについて
Q）フランスでは、プライバシーを保護するため、特にパーソナルデータの匿名化について遵守すべき規則を明記したビッグデータ向け公式ガイドラインは存在するか。
A）もちろんある。フランスはプライバシー保護が世界で最も進んでいる国の一つである。CNIL は秘密の遵守をチェックする一方で、ビジネスにおけるデータ利用がデータ所有者の同意に反してなされないようにする重い任務を持つ。

Q）どのように、ビッグデータ企業がパーソナルデータの匿名化を遵守しているかどうかチェックするのか。これは、CNIL の役割か。
A）その通り。

Q）データ主体の再特定化に関する市民の懸念に関しては、どのように対応すればいいか。法律を厳格なものにすればいいか。
A）否。我々はそうは考えていない。インターネット企業がパーソナルデータを扱う仕方を前にして、人々の包括的な情報と一般の人々の復元力がそれほど無罪であるとは思えない。とはいえ、他方で、パーソナルデータを利用するアプリケーションに関してさえも、非常に良いビッグデータアプシリケーションがたくさん現れるだろう。他方で、一定の仕方で、我々は厳格にならねばらないし、過去三十年間に渡って金融部門で見られたような自由化を行ってはならない。なぜなら、その結果は市民に対する否定的なインパクトである点で同じことになりうるから。我々は欧州市場を問題にする限り、少なくとも欧州レベルでの規制を必要としている。だが、個人的な意見では、米国も同じことをすべきであると思う。また、研究プロジェクトのために「技術革新原則」を導入すべきである。

欧州とフランスにおけるパーソナルデータを利活用するサービス事例について
Q）欧州とフランスで、個人情報を匿名化するか仮名化して、ビジネスや公共サービスを提供している注目すべき事例を教えていただきたい。

A）フランスには、エタラブ（Etalab）[73]がある。これは万人向けの利用のため、パーソナルデータを匿名化して公共データを公表する政府のスピンオフである。また、政府の司法・行政情報局[74]では、ウェブ上で公表する前に、司法決定ファイルに匿名化を行っている。

Q）欧州とフランスで、個人情報の濫用あるいは漏洩の事例を知っていたら教えていただきたい。
A）裁判で訴追されている事例については知らない。だが、我々は法的限界で活動している主要な企業はほとんどないと考えてよい。

Q）パーソナルデータの再特定化を避けるために、匿名化技術を改善している研究開発プロジェクトを教えていただきたい。
A）TORPROJECT[75]を見ていただきたい。

欧州における元CIA職員スノーデン氏のインパクトについて
Q）欧州におけるスノーデン氏の告発のインパクトについて、ご意見をお伺いしたい。
A）同氏の告発のインパクトは、少なくともフランスでは、世界中で行われている米諜報活動の多様な面を示したことである。従って、ビッグデータのあらゆる面に関して、倫理的な実践と同じく信用を回復することが重要である。また、同氏の告発は、インターネットの黒い側面に対する一般の人々の意識を覚醒させた。しかし、一般の人々はどのように効果的に自分自身を守ればいいか、まだ何も知らない。なぜなら、彼らの技術レベルは、効果的な防御壁を設置するのにはあまりにも低すぎるからである。

E) テレコム・パリテックにおける取り組み

フランスの電気通信部門の高等教育・研究機関であるテレコム・パリテック[76]では、ビッグデータの将来的な重要性を考慮し、2013 年より同技術に関して幾つもの講座を開設している[77]。大きな特徴は、民間企業と提携して研究開発を行うとともに、研究開発以外の側面、すなわち、個人情報保護等の法・政治的側面や経済的側面についても講座を開設し、ビッグデータの研究及び利活用を包括的に発展させる試みが行われている。

以下に、「ビッグデータのための機械学習講座」のステファン・クレマンソン氏へのインタビュー議事録を収録する。

ヒアリング議事録　テレコム・パリテック（鉱業・テレコム研究院）

日時：

2014 年 1 月 20 日（月）午前 10 時～11 時

場所：

先方事務所（パリ）

[73] www.etalab.fr
[74] http://www.dila.premier-ministre.gouv.fr/
[75] https://www.torproject.org/index.html.en
[76] テレコム・パリテックは、鉱業・テレコム研究院の一機関である。
[77] http://www.telecom-paristech.fr/recherche/chaires.html

先方：

テレコム・パリテック 信号・イメージ処理学科教授：ステファン・クレマンソン氏[78]

当方：

情報通信研究機構 欧州連携センター長：菱沼 宏之

ONOSO 研究員：小野 浩太郎

調査目的：

ビッグデータの研究者であるテレコム・パリテック教授ステファン・クレマンソン氏に、欧州及びフランスにおける、ビッグデータの研究開発とビジネス展開に必要なパーソナルデータ保護に係る法・ガイドライン整備動向や利活用事例等について質問し、日本のパーソナルデータ保護に係るガイドライン策定の参考とする。

ヒアリングの概要：

先方の研究活動について

（△）テレコム・パリテックにおけるあなたの研究活動について教えていただきたい。

（○）私の専門は応用数学で、テレコム・パリテックの信号・イメージ処理学科でビッグデータの研究開発を実施している。私は特にボリューム、オンライン、データの多様性等の問題を取り扱っている。テレコム・パリテックは、ビッグデータに関して、仏クリテオ社[79]、仏PSAプジョー・シトロエン社、仏BNPパリバ銀行、仏サフラングループの系列企業（SNECMA社、SAGEM社、MORPHO社）[80]と提携している。

（△）テレコム・パリテックには、博士課程の学生を含め、ビッグデータを研究している人は何名ぐらいいるのか。

（○）全部で約 30 名であるが、ビッグデータの研究は学際的なので、全員がビッグデータを専門としているわけではなく、数学者やコンピューターサイエンティスト、ビッグデータの経済的側面を研究している人もいる。私はアルゴリズム、方法、方法の分析をテーマにし、実験も行っているが、概念実証が主である。仏政府と EU からビッグデータのプラットフォームを購入するための資金を受給したところであり、来年には購入する予定である。

私が主催しているビッグデータに特化されたマスターコースの講座は、昨年 2013 年 9 月に開設されたところであり、学生数は 28 名である。非常に学際的であり、経済、法、コンピューターサイエンティスト、機械学習を専門としている学生がいる。この講座では、仏電力企業 EDF や仏ガス企業 GDF 等の企業と提携し、また多くのスタートアップ企業と繋がりがある。

また、このようなビッグデータに特化されたマスターコースの他に、データサイエンティストという講座が 2014 年 5 月に開設される予定である。この講座は企業に勤める等して毎日学校で授業を受けることができない人向けの講座である。

なお、テレコム・パリテックには、クレール・バルト氏が主催するデータプライバシーを法的側面から扱う講座がある。

---

[78] http://perso.telecom-paristech.fr/~clemenco/Home.html

[79] http://www.criteo.com/fr
クリテオ社は、特に広告に関して、データ利活用サービスを提供する企業であり、2005 年に設立された。

[80] http://www.safran-group.com

（△）あなたはフランス以外の企業と提携して、ビッグデータの研究開発を実施しているか。

（○）その通り。米グーグル社と提携している。

（△）あなたはビッグデータの重要性は何であると考えているか。

（○）まず、ボリュームが重要であり、分散並列処理の問題がある。そして、速度が重要であり、オンラインアルゴリズムの逐次処理の問題がある。さらに、データの多様性が重要である。私はこれらの問題に対応する研究を行っている。また、我々は企業と提携することに積極的である。なぜなら、彼らは詳細なデータを保持しているからである。我々は数学を実際のデータに応用し、データをマーケティング等に利用可能にすることを目指している。

（△）仏政府はビッグデータの研究開発とビジネスに積極的であるか。

（○）その通り。フランスには、政府のために将来重要な技術革新の分野を特定する組織が設立されており、仏原子力企業アレバの前社長ローベルジョンがこの組織の委員長を務めている。この委員会は2013年10月に報告書を作成しているが、そこでは、ビッグデータが技術革新の将来的に重要な分野の一つとして選択された[81]。

（△）フランスでは、ビッグデータの研究開発が他の欧州諸国と比べて進んでいると聞いたことがあるが。

（○）フランスの有利な点は、応用数学の研究が進んでいることである。また、仏タレス社は、サイバーセキュリティの分野でビッグデータの研究を進めており、非常に有力である。

（△）あなたはマルコフ過程を研究しているとウェブサイトにあったが、これは匿名化にも利用しているのか。

（○）否。していない。

ビッグデータの向けパーソナルデータの匿名化について

（△）まず確認になるが、現在欧州とフランスでは、パーソナルデータは匿名化されさえすれば、データ主体（data subject）の同意なしで、当人のデータを利用可能であるか。

（○）その通り。来年、我々はビッグデータのプラットフォームを購入する予定だが、そのプラットフォーム上では全てのパーソナルデータは匿名化される。個人の健康情報や位置情報を含む社会・人口統計情報が完全に匿名化された上で、分析される。

（△）フランスには、プライバシーの保護のために、特に匿名化に関して遵守すべき規則を明確に示すビッグデータ向けのガイドラインは存在するか。

（○）その通り。フランスにはパーソナルデータ保護監督機関のCNIL[82]が、匿名化に関して遵守すべき規則を策定している。

（△）英国では、ICO（情報コミッショナー事務局）が匿名化に関する実践ガイドブックを作成しているようだが。

---

81 http://www.elysee.fr/communiques-de-presse/article/remise-du-rapport-de-la-commission-innovation-2030-presidee-par-mme-anne-lauvergeon-2/
http://www.lemonde.fr/economie/article/2013/10/11/les-sept-ambitions-d-anne-lauvergeon-pour-l-innovation-en-france_3494114_3234.html

82 CNILはクニルと一般に発音する。

（○）フランスでは、CNIL が同じようなものを作成しており、そこでは匿名化について詳しく説明されている。このようなガイドブックはインターネット上で取得できる。

テレコム・パリテックでは、我々研究者は組織内に設置された部署を通して、研究の法的側面に対応している。また、ビッグデータのマスターコースでは、ビッグデータの法的側面についても授業を行う。

先ほども申し上げたように、一般にフランスでは、匿名化すればパーソナルデータをデータ主体の同意なしで利用することができる。だが、例えば、あなたがスポーツクラブに入会しているとしよう。入会時の契約書に、パーソナルデータの利用に関する条項が小さく書かれてあって、そのスポーツクラブが広告企業等にあなたのパーソナルデータを販売するというようなことは行われている。さらに、もちろんあなたの方でもパーソナルデータの管理が法に則っているかチェックすることは可能であるとしても、実際には、パーソナルデータがどのように管理されているか知ることは誰にもできない。

（△）テレコム・パリテックでは、パーソナルデータの匿名化に関する研究を実施しているか。

（○）否。フランスでは、INRIA で実施しているかもしれない。我々はアルゴリズムの研究を実施している。だが、我々は分散アルゴリズムの研究をしており、そこではデータは決して中央集権的なシステムの中でのように自由に利用できない。ネットワーク、サーバ等からなるアーキテクチャで行われる計算の一部分を傍受しても、そこから元のデータを再構成することはできない。アーキテクチャとして、全ての情報システムが完全に接続されているわけではないからである。このような仕方で、我々はビッグデータのセキュリティの問題に対応しようとしている。セキュリティはテレコム・パリテックの重要な課題の一つである。

（△）データが分散されているから、それらを再結合することは難しいということか。

（○）その通り。いかなる時も、我々の情報システムの中では全てのデータが一緒に集められることはない。なお、分散は（地理的でなく）論理的に行われる。

（△）どのような技術がパーソナルデータの匿名化に利用できるのか。

（○）匿名化に関しては、個人を特定することを可能にする全ての情報を消去することがその手段である。だが、ユーザーの特定は難しいものではない。幾つかのパーソナルデータ（性別等の）を消去しても、様々なデータを組み合わせるだけで、個人の特定は可能である。確かなものは何もないと言える。

<u>パーソナルデータ利活用の事例について</u>

（△）テレコム・パリテックには、ビッグデータのスピンオフ企業が設立されていると聞いたが、それらはパーソナルデータを利用するのか。紹介していただきたい。

（○）その通り。テレコム・パリテックにはインキュベイター[83]（incubator：新事業支援センターの意味）があり、新しい事業の着手を支援している。インキュベイターは、テレコム・パリテックで実施されている研究を延長して行うスピンオフ企業を設立することを援助している。その他、テレコム・パリテックの研究とは関係のないスタートアップ企業の設立の支援も行っている。

私も最近スピンオフ企業を設立しており、医療診断に係るアプリケーションやモニタリングシステム、推奨システム等を開発している。だがまだ、我々の企業はウェブサイトを持たない。

[83] http://entrepreneurs.telecom-paristech.fr

（△）フランスで、パーソナルデータを匿名化、仮名化して、利活用しているビジネスや公共サービスがあれば教えてほしい。

（○）フランス政府はエタラブ（etalab）[84]という機関により、パーソナルデータを匿名化し利用してオープンデータ政策を実施していることは注目すべきである。民間企業としては、ダタ・ピュブリカ（Data Publica）[85]というスタートアップ企業も注目すべきである。

（△）欧州、またはフランスで、個人情報の濫用や漏洩の事例を知っているか。

（○）幾つか知っている。しかし、実際のところ、CNIL が全ての企業がどのようにデータを管理しているかチェックすることは不可能である。なお、先ほど述べたローベルジョンの委員会はビッグデータに関する規制を弱める方向であるようである。

（△）2014 年 1 月 8 日に、CNIL は米グーグルに対し、フランスの個人情報保護法違反で罰金を課したそうだが。

（○）そう聞いている。CNIL が提示した罰金は 15 万ユーロであり、CNIL の権限では最大の額である。しかし、世界最大手 IT 企業であるグーグルにとってはたいした額ではない。この罰金には象徴的な価値しかないだろう。CNIL は欧州委員会に対して、罰金額を引き上げることができるように働きかけるだろう。

グーグルの問題は、パーソナルデータの取扱いの問題というよりも、税金の問題が大きい。彼らは欧州で十分に税金を支払っていないと批判されている。

グーグルを規制するのは非常に難しいと思う。なぜなら、彼らの動きは非常に迅速で、新しいものを次から次へと提案する。医療情報の取扱いに関しても着手している。だが、このようなグーグルの事業は危険性を伴うものでもあろう。

米諜報機関の監視活動について

（△）2014 年 1 月 17 日、オバマ米大統領は、元 CIA 職員のスノーデン氏の暴露が世界中に巻き起こした反響を受けて、情報収集活動を見直しすると発言し、それに応えて、欧州委員会は大統領の姿勢を歓迎する意向を示している。スノーデン氏の暴露について、ご意見をお伺いしいたい。

（○）もちろん米諜報機関を非難することはできるが、彼らが本当のところどのようなことをしているのか分からないので意見することは難しい。彼らの諜報活動を防ぐ手段はない。コーディングを破ることを防ぐ手段もないし、データセンターがアメリカ国土にあれば、なおさら難しい。また、彼らがどのようなコンピューティング能力を持っているのかもよく分からない。もしかすると米諜報機関 NSA は民間企業よりも高い能力を持っているのかもしれないが、それも確かではない。確かなことは、現在、米国防総省はシリコンバレーの IT 企業と提携し活動していることである。1990 年代には、ペンタゴンはシリコンバレーをむしろ監視していたのだが、現在は異なる。しかし、これらの事情についてはよくわからないことが多い。

（△）欧州では、特にドイツのメルケル首相の携帯電話が米諜報機関に盗聴され、憤慨しているようだが。

（○）その通り。だが、それも奇妙なことで、ドイツにはアマゾンがベルリンとドレスデンに 2 つの大型リサーチセンターを持ち、ドイツの研究者は米企業のクラウドを利用している。

なお、アメリカは現在通信インフラストラクチャに投資しているようである。ビッグデータを利

[84] http://www.etalab.gouv.fr
[85] http://www.data-publica.com

用するには、大規模なインフラストラクチャが必要である。

第三章　コンピューター・プライバシー& データ保護イベントの動向

CPDP（Computers, Privacy & Data Protection）[86]とは、2007 年に開始された年一回ブリュッセルで開催される国際イベントである。欧州の研究機関、EU諸機関、欧州企業を中心に、世界各地の企業や研究機関等が一同に集まり、テーマ毎にパネルディスカッション及び研究発表を行っている。同イベントは 2014 年で 7 回目となるが、2013 年の元CIA職員スノーデン氏による米諜報機関の情報収集についての暴露がきっかけとなり、欧州でプライバシーに対する問題意識が高まりつつことを受けて、非常に注目が集まっていた。

CPDP 視察レポート

第一日目[87]

１．日時：2014 年 1 月 22 日（水）午前 8 時 45 分～午後 6 時
２　場所：ベルギー・ブリュッセル
３．参加者：ONOSO 研究員　小野 浩太郎
４．概要：

パネルタイトル：「EUデータ保護改革：バグを調節しよう」

パネル参加者：

欧州委員会司法総局：マリー＝エレーヌ・ブーランジェ氏、欧州情報の自由とデータ保護アカデミー：ピーター・シャール氏、ソフトウェア・アライアンス：トマス・ブエ氏、欧州データ保護監督官（EDPS）：ヒエルケ・ハイジマン氏、ウィルソン・ソンシニ・グッドリッチ・ロザティ：クリストファー・クネル氏、欧州連合基本権庁：マリオ・オエテイマー氏

テーマ：2012 年に開始されたEUパーソナルデータ保護指令改正プロセスが、現在直面している技術的な諸問題について検討する。

議論の概要：

a）2 年前、EU パーソナルデータ保護法の改正を開始したが、その必要性にも関わらず、現在まだ成立していない。現在、欧州委員会と各国の政府の間でコンプロマイズを進めている。2014 年 1 月から EU 議長国であるギリシアの主導の下、できるだけ早く改正法案を成立させたい（欧州委員会のブーランジェ氏）。

b）改正法の問題点の一つは、新 EU 法の範囲に関わる。第一に、公共部門を同法の対象から外すことが検討されている。公共部門には EU 統一の法は必要ないという主張があるが、やはり公共部門も EU 法の範囲に入れるべきであるという主張がパネリストからなされた（シャール氏等）。なぜなら、EU 市民は公共部門と民間部門に違いを見出していないことがあるからである。例えば、病院に関して言えば、公立の病院もあるし、民間の病院もあり、同じ病院なのに法律が異なるのはおかしい。第二に、現在の EU 法では、EU 諸機関はその範囲に含められていない。EU 機関も公共部門も含め、全ての部門が同じ EU 法の範囲に入るべきである。

c）新 EU 規則案の第 22 条項は、欧州委員会の法案では、「データ管理者の責任（Responsability）」であったが、欧州議会で修正されて、「データ管理者の責任と説明責任（Responsability and

[86] http://www.cpdpconferences.org
[87] 以下のパネルディスカッションの概要には、議論の要点のみを記す。

accountability)」とされた。

d) 欧州連合基本権庁は、CPDP の当日（2014 年 1 月 22 日）に「EU 加盟国におけるデータ保護救済措置へのアクセス」というレポートを公表し、配布している。欧州連合基本権憲章第 47 条では、権利を侵害された場合、裁判に先んじて、効果的救済を受ける権利が定められている。欧州連合基本権庁 のオエテイマー氏の指摘では、欧州委員会の新 EU 法案は、データ保護救済措置へのアクセスが明確に改善されている（各国のデータ保護監督機関の独立性の強化、異議権の行使の無料化等)。

e) 改正法案の重要なポイントの 1 つであるワン・ストップ・ショップメカニズムの導入が問題視されている。このメカニズムは欧州委員会によって明確に定義されていないことが、パネリストに問題として指摘された（ブエ氏)。欧州委員会と欧州連合理事会が同じ仕方でこのメカニズムを定義していないように思われるからである。また、このメカニズムの適用はある特殊なケースに限定されるべきであるという意見があった（ブエ氏)。さらに、欧州議会では、欧州委員会によって提案されたワン・ストップ・ショップメカニズムは修正され、「主導監督機関（lead supervisory authority)」という概念が導入された。

f) パーソナルデータの第三国への移動に関しては、第 43 条項 a が欧州議会によって新規則法案に追加された。この条項は前もって国際的な取り決めなく、第三国の裁判所や行政機関の決定に従い、データ管理者や処理者がパーソナルデータを開示することを禁止するものである。

2) 日時：1 月 22 日 午前 11 時 45 分～午後 1 時

パネルタイトル：「プライバシー・バイ・デザイン：コンセプトからデータ保護コンプライアンスの本質的構成要素へ」

パネル参加者：

プライバシー法とビジネス社：スチュアート・ドレスナー氏、モニク・アルセム法律事務所：モニク・アルセム氏、パークリーガル LLC：ジョン・アントコル氏、ナチュラルセキュリティアライアンス：アンドレ・ドラフォージュ氏、オンタリオ情報・プライバシーコミッショナーオフィス：ミシェル・シバ氏、トリアログ：アントニオ・クン氏

テーマ：プライバシー・バイ・デザインはもはやデータ保護の理論的なコンセプトではなく、どのように市場リーダーや規制機関がこの原則を実際に取り入れるか証明する段階に入っている。パネルディスカッションでは、プライバシー・バイ・デザインを標準や技術仕様に採用する取り組みを紹介し、検討する。

議論の概要：

a) EU パーソナルデータ保護改正法の第 23 条項「デザインとデフォルトによるデータ保護」において、データ管理者はデータ主体の保護を強化する「適切な技術的、組織的措置と手続き（appropriate technical and organisational measures and procedures)」を講じなければならないとされている。

b) プライバシー・バイ・デザインとは、カナダのオンタリオ情報・プライバシーコミッショナーオフィスのアン・カブーキアン氏が 1990 年代に提唱した 7 つの原則である[88]。

[88] 原則1： リアクティブではなく、プロアクティブ。前もって予防すること目標とし、後から救済するのではない、原則2：プライバシーをデフォルト設定、原則3：設計に組み込まれたプライバシー、原則4：ゼロサムではなく、ポジティブサム（ウ

c) 仏企業トリアログ[89]は、プライバシー・バイ・デザイン原則を採用するFP7 プロジェクトPRIPARE[90]のコーディネーターである。同プロジェクトは、プライバシー・セキュリティ・バイ・デザインの方法論の採用を簡便化させること、多様なステークホルダーを狙う教材を通し、リスクマネージメントを向上させることを目的とする。

d) ナチュラルセキュリティアライアンス[91]は、認証の技術仕様の管理、維持、強化、ビジネスの要求への対応、デバイスとサービスの認定、市場教育を行う欧州企業や銀行からなる団体であり、2006 年にフランスのリール市で形成された新型決済システムを考案するための産業クラスターが起源にある。同アライアンスはプライバシー・バイ・デザイン原則を採用する決済システムの仕様の開発を支援している。

3) 日時：2014 年 1 月 22 日 午後 2 時～午後 3 時 15 分

パネルタイトル：EUデータ保護改革： 現在の状況

パネル参加者：欧州データ保護監督官（EDPS）： クリストファー・ドックセー氏、EUオブザーバー： ニコライ・ニールセン氏、プライバシー・インターナショナル： アンナ・フィルダー氏、欧州委員会司法総局： フランソワーズ・ルベール氏、ギリシア常設代表団： フィリッポス・ミテルトン氏、GIODO（ポーランド・パーソナルデータ保護監督機関）： ウォジシー・ヴィウヴォウロフスキー氏

テーマ： データ保護指令の改正について、立場の異なる組織の代表者が集まり、政治的な文脈を検討する。

議論の概要：

a) 欧州データ保護監督官による現状確認：2013 年 10 月に新 EU パーソナルデータ保護規則案は欧州議会を通過したものの、各国の閣僚が集まる欧州連合理事会の審議は滞っている。例えば、ワン・ストップ・ショップメカニズムはあまりにも複雑すぎるという意見がある。

b) 欧州委員会司法総局代表者の意見： 欧州議会を通過したことにより、困難な段階は過ぎ去った。欧州連合理事会も通過できるだろう。どんな法も完全ではなく、政治家の意志、政治判断があれば、詳細な技術的な問題を乗り越えることは可能であり、新 EU 法案を成立できる。政治家はそれぞれ責任を全うすべきである。なお、米グーグル社は新 EU 規則案が成立しないことを望んでいる。

c) 欧州連合理事会の議長国であり、調整役に回っているギリシアの意見： 現在欧州連合は新しい包括的なパーソナルデータ保護法案を必要としており、困難はあるが、審議を続けていくべきである。

d) ポーランドのパーソナルデータ保護監督機関代表者の意見： 欧州委員会は新 EU 法案について

ィン・ウィン関係を実現する)、原則 5： エンドツーエンドなセキュリティ、原則 6： 可視性と透明性： オープン性を維持する、原則 7： ユーザープライバシーの尊重

[89] http://www.trialog.com

[90] http://cordis.europa.eu/projects/rcn/110590_en.html

PRIPARE の正式名称は、「PReparing the Industry to Privacy and securty-by-design by supporting its application in Research」である。

[91] http://naturalsecurityalliance.org

詳細な説明をしていない。数ヶ月前から欧州連合理事会での審議には進歩が見られない。2014年5月に行われる欧州議会議員選挙以前には、同法の成立はありえないと思うし、2014年内に、あるいは最終的に成立しないこともありえる。政治判断ではなく、明確な法文が必要である。

e) 会場からの意見：同法の成立により、各国のパーソナルデータ保護監督機関は恩恵を受けることができる。だが、同機関の独立を強めるので、各国の政府の方針と齟齬が強まる可能性がある。

<u>第二日目</u>

１．日時：2014年1月23日（木）午前8時45分～午後6時
２　場所：ベルギー・ブリュッセル
３．参加者：情報通信研究機構欧州連携センター長　菱沼宏之
４．概要：

パネルタイトル：同意と不同意

（司会：INRIA）

（クリストフ・ラザロ：仏INRIA）法、倫理、政治的状況を踏まえ、所与の文化的・社会的環境の下における「同意」について議論する。車に例えると、①貴方は、荒野でなく道路を走っている、②1人で走っている訳でなく同乗者等がいる、③全てが分かって走っている訳ではなく認識には限度がある。すなわち、「同意」には流れの中で他の人も関係しており、また、完全な情報や判断の下でなされている訳ではない。あたかも車のシートベルトのような、助けるデバイスが「同意」には必要である。

（モリツィオ・ボルギー：英国ボーネマス大学）電子メールによる等によるダイレクトメールの問題について議論する。例えば、この会議（CPDP）に登録する際、自己の情報を転送することに同意するかどうかという問題がある。欧州ではオプトアウトになっており、同意しない限り情報は転送されない。同意は、この会議への登録の条件ではなく、分離されていて、電子メールを受け取りたい場合にだけ同意すれば良い。しかし、予め（電子メール受取が）登録されている場合はどうか。英国の典型的なウェブサイトをいくつか見てみると、オプトアウト、オプトイン、プリセレクトの3種類があるが、16.2%がEUの基準を満たしているだけである。電子メール受取に同意させるための偽のウェブなどもある。電子メールのドメイン名がウェブサイトのドメイン名と一緒であると、情報が移転していないと言えるであろうが、実際のところ67%は異なるドメイン名である。結論として、有名なウェブであっても、低いレベルのコンプライアンスであるということが言える。

（ロジャー・ブラウンスワード：英国キングストン大学）幸福を最大化してストレスを最小化するのが（一般的な政策）目的である。規制当局はどう考えるか。基本的権利の観点から見ると、「同意」を真剣に考慮すべきである。規制当局が最低ラインとして考えているのは、「同意」により正当化されるということ。権利者が、十分に情報を与えられ、自由に意思決定できる環境にいるかどうか。「同意」した場合、どの範囲まで同意したのかも問題になる。権利者の同意がない場合、どのような条件で有効となるのか。データ保護・プライバシー権の観点から、緊急の場合などが（同意がなくても有効となると）考えられるが、（その範囲は）危険性が低いものでなければならない。

（ジェイン・ケイ：英国オックスフォード大学）医療分野におけるオンライン通信について議論する。プライバシーとは、英国の判例によれば、自己の特定に係る全ての事実を司るもので、（自己がそのような事実の）所有者と推測され、自律した支配権がある。医療では基本的に紙ベースでの同意が必要だが、データの質が高まってきており、それが難しくなってきている。しかしながら、本人の意思に反したり、大量サンプルデータの範囲を逸脱したりしてはならない。ガバナンスの問題として、広い意味での同意をどう捉えるか。個人のデータを研究に使用するためには明示の同意が必要であり、匿名化する際であっても同意が必要。同意を得るに当たっては、個人が意思決定の中心であるべきで、同意を分散させずにきちんと集中させるべき。同意はガバナンスの一環である。

（KDDI）プラットフォームを開発しているが、プライバシーが課題。

パネルタイトル：忘れられる権利：RTBF：Right To Be Forgotten

（司会）忘れられる権利はデータ保護規則にある。選択して忘れるのは利害のバランスが必要。タイミングはどうなるか。

（メグ・レタ・アメブローズ：米国ジョージタウン大学）カリフォルニア大学ロサンゼルス校（UCLA）の同級生の暴露事例など有名な事件では、その時はアクセスが急増するが、しばらく経つと誰も見なくなるという、情報のライフサイクルがある。すぐに必要となる情報は必ずしも正確ではないが、ウェブ上の情報は残るものであり、時間が経って必要な情報は正確でなければならない。

（アイヴァン・シェカリー：ブダペスト工科経済大学）写真や録音をすぐに消してほしいというような場合に、忘れられる権利が問題になる。有効期限を設ける、個別の期限で無効となる、など色々な方法がある。個人の生活なのか、メディアを通じたものかの違いもある。裁判における義務的公開の停止という方法もある。

（ジェフ・アウスロース：ベルギー・ICRI：法と ICT 学際センター）忘れられる権利の法的枠組を議論する。忘れられる権利とは、プライバシーが、不適切・不公正・不合理に、通常はメディアにより曝露されることに対するものであり、プライバシーと表現の自由との兼ね合いが問題となる。個人データ保護、すなわち消す権利は、切迫して合法的な場合に可能である。グーグルのスペインにおける事例の場合、国境による限界はなく、また、初めは合法でも時間の経過により問題となってきた。現在では、情報の獲得・蓄積・処理・除去は容易になっている。情報の除去は、他の利害とのバランスが必要であり、「時間」も重要な要素となる。

（ジオヴァニィ・サーター：伊ボローニャ大学）データ保護と時間の経過に関し、同意の撤回について議論する。非合法な方法で収集されたデータの除去に関して、制裁をどうするか。利得的な（Pro 過程の）法的利害としては、（公開することについての）表現の自由、民主主義、経済的利益等があり、損失的な（Con 過程の）法定利害としては、プライバシー等があり、これらがトレードオフの関係にある。利得も損失も長期的に低下していくが、目的が達成されることによって利得は一気に無くなるか減少する一方、損失が緩やかに維持されていく点が問題となる。すなわち、長期的には利得と損失が逆転していく。しかし、スキャンダルの人が議員になった時など、表現による利得が再度増えるようなこともある。損失が利得を上回る問題への対策としては、期限を設ける、通知による同意の撤回の機会を与える、ひどい不誠実な行為には制裁を加えるなどが考えられるが、新しい規則をどうすべきであろうか。

（ジェイ・スタンレー：米国 UCLA）米国は言論の自由がある。もしデータを除去したければ、時間の経過や、主題などが関わってくる。グーグルだけを取り締まるのでなく、発言者をどうするかということである。インターネットは言わば強力なコピー機であるからである。

パネルタイトル：データ保護当局（DPA）：執行の役割と経験

（司会：チャールズ・ラーブ：英国エジンバラ大学）

（モデレータ）（この会場では）オンブズマン型の DPA を好む人は少ないようである。

（エヴァ・スーラダ・キルヒメイヤー：前オーストリア・データ保護機関）オーストラリアは制裁金を課していない。

（モデレータ）会場に聞きたいが、制裁金は効果的と考えるか。

（会場）［かなり多数が賛成の挙手。否定は少数の挙手。］

（ソフィー・ルーヴォー：EDPS 欧州データ保護監督機関）当方は EU の機関。制裁金は課していないが、命令を出したり、裁判に訴えたりする。説明責任の問題である。EU 各国は国内に最低 1 つのデータ保護機関を設立するようにされている。EU データ保護指令の目的は、データ保護の文化を創ることにある。2010 年に政策を実施し、データ保護を必要とした。商業分野だけでなく公共分野にも関心を有している。自分は（各国のデータ保護機関を）年間 14 回視察した。ベンチマークは固定されていないが。説明責任が必要。

（モデレータ）会場に聞きたいが、DPA は議会の指名が良いと思うか。

（会場）［少数。］
（モデレータ）首相など政府の指名が良いと思うか。
（会場）［少し多い。］
（ロバート・ゲルマン：米国プライバシー情報政策コンサルタント）米国の関係機関としては、公民権オフィス（OCR）や連邦取引委員会（FTC）があり、FTC は私的事項の執行機関。FTC に争議件数を聞いてもブラックボックスであるが、ウェブサイトによれば533 件となっている。これは、FTC が悪いと言っているのではなく、機能的な問題である。連邦通信委員会（FCC）は通信のプライバシーを扱っているが、通信業界は FCC から FTC にしてほしいとキャンペーンしている。チャーチル元英首相は、米国は他の全てをやり尽くした後に正しいことをする、と言ったが、米国はまだ、やり尽くしている訳ではない。
（会場質問）各国の DPA に適用するベンチマークを設定することについてどう考えるか。
（アイルランド）歓迎する。
（オーストリア）単一の基準は難しいと考える。

パネルタイトル：EU とAPEC とのデータ移転の相互運用性

（司会：ノーヨン・パク：ソウル大学）
（ブレア・スチュアート：ニュージーランド・プライバシー・コミッション）APEC は世界の人口の 40%、GDP の 55%を占め、多様性もある。データ越境時のプライバシーに関しては、米・墨・日が初期から実施していたもの。
（ピーター・シャー：欧州情報自由・データ保護学術院）EU の観点から、1995 年指令が 28 か国に適用されてきた。第三国への移転については課題があった。保護レベルを欧州並みにするかどうか。スノーデンの暴露の後は、個人的なものであっても、他にも受け手がいる可能性を考える必要が出てきた。国家、インテリジェンス当局、警察などが関係する。拘束的企業準則（BCR）について説明。
（ダニエル・プラデル：仏 HP）BCR が当初の意図である固定移転のためを超えるものとなっている。すなわち、BCR がプライバシーの説明責任を果たしていることの基準にまでなっている。グローバルなエコシステムの中で、データは安全か、利用者の期待にかなうか、コンプライアンスはどうか。CHAF モデルとして、域内で確実性と調和性が必要であったが、適用性や柔軟性をどうしていくかが将来の課題。BCR と CBPR（APEC の越境プライバシールールシステム）との関係をどうするか。企業のガバナンス責任、支援技術、革新的な規制枠組が、グローバルなプライバシーの将来にとって課題。
（ノリスワデル・イスメイル：英国クオティエル・コンサルティング）ASEAN 加盟 10 か国のうち、マレーシア、シンガポール、フィリピンの 3 か国だけが、欧州データ保護指令に当たるような法律を通している。フィリピンは説明責任に加えてセキュリティも規定している。しかしながら、ある企業がこれら 3 か国で BCR を取得しても、他の国でデータ・ヘイブン（データ保護責任回避地）が生じる。BCR は企業にとって費用がかかる。2015 年までに ASEAN の経済を調和させる目標があるので、それまでに新しい CBPR を作りたい。
（モデレータ：ハーゼル・グラント）
（会場質問）韓国と日本は EU と良く議論しているが、BCR をアジアに適用できると考えるか。
（APEC）日本・韓国・台湾では稼働可能と思われる。
（司会：韓国）昨年、日本が BCR に加入し、韓国も真剣に検討中である。

パネルタイトル：ビッグデータ時代のパーソナルデータの（金銭的】価値

（司会）
（キエロン・オーハラ女史：英国サウザンプトン大学）匿名化したものの再識別化は、EU では罰則付きで法的に禁止されている。
（マイケル OECD）ビッグデータの使用・分析について。1989 年 OECD のプライバシー・ガイド

ラインがある。これは、先験的・分析的、顧客志向である。
（ジョルグ・フラジ：ベルギー・ハントン&ウイリアムス）ビッグデータのプライバシーへの挑戦の法的側面を議論する。忘れられる権利などもある。1995 年指令を踏まえ、目的を特定化し、収集した内容や影響等々、ビッグデータに関して分析し、個人への影響を考える。
（ジャッキー・テイラー女史：英国ボーナーマス大学）規制アプローチ。二次使用モデルがある。需要が先導するモデルである。スノーデンの暴露後について、新しい 2 つのモデルがある：ビッグデータ移転のため正確なモデルと、許可モデル。2014 年に新しいデータセンターを設置し、スマートシティを作ろうとしている。政策の進展により、新しい法的アプローチとしてプラットフォームアプローチを検討している。
（会場質問 KDDI）米国と比較して、EU における（知的）財産権の議論はどうなるか。
（会場質問）OECD、スノーデンについての連邦政府の対応はどうか。
（会場質問）匿名化すると市場におけるビッグデータの鍵は何になるのか。
（会場質問）経済の問題について質問する。データの売却と、個人が無償で提供することとの関係はどうか。誰がビッグデータの場所の費用を支払うのか。市民か、税金か。
（キエロン・オーハラ）財産権は視点に依る。法的に政治的に、将来に向けて考えるべき。米国の法律専門家は懐疑的である一方、オランダとドイツの弁護士は欧州のデータの保護を財産権の扱いと結び付けている。交渉によりもっと権利を持てると踏んでいるようだが、明確にすることが必要。データの売却と寄進について、また、商用化と財産化について、将来可能であれば交渉できると思う。ビッグデータの場所は人々が寄進する、又はデータをドロップすることにより、データをシェアする。小企業を含めて企業が革新する。グーグルにデータは独占されているが、人々がデータを寄進すれば良いのではないか。そうすれば公平な交換になる。ハード・ソフト。データをどこかに置くのは、デザイン等と関係してくる。
（ジャッキー）英国シティ。クラウドでのネットサーフィンを、スマートシティでどうするか。これは、スタートアップにとっての大きなエコシステムになる。

パネルタイトル：バイオメトリックにおけるプライバシー

（エルス・キンド：ベルギー・ルーベン大学）データと法的確認、同意、PbD（プライバシー・デザイン）：バイオメトリックデータの仮名化の 3 点を議論したい。バイオメトリックは特定化をもたらすが、匿名化の権利はデータの本質として必要。EU では、時によってバイオメトリックデータがセンシティブデータに分類されたりされなかったりしている。バイオメトリックデータは重大な公共の利益に関係するものであり、セーフガードをどうするかについて、同意だけでは解決しない。多様（マルチプル）な仮名化が重要である。
（ステファン・ウェーバー：デンマーク VDI/VDE/IT）モバイルにおけるバイオメトリックデータについて議論する。例えば、指紋がどうきちんと管理されているか（ローカルに端末にしか保管されていないのか）分かるであろうか、また、信頼できるであろうか。バイオメトリックデータの参照データがどう保管されているか。モバイルにおけるバイオメトリックの安全性を確認するのは大変である。Eab（欧州バイオメトリクス協会）のサイトを参照頂きたい。
（カルメラ・トロンコソ：スペイン・グラディアント）プライバシー保護が高ければ価格が高くなり、価格が低ければプライバシー保護も低くなる。プライバシー技術の適用を阻害する 4 つの原因は次のものである。①法的枠組として必ずしも強いプライバシー保護が求められていない、②現実として利用者がプライバシーをあまり要求しない、③プライバシーは費用がかかる（適用と結合により多くの作業を必要とする）、④産業界は生データを欲しがる（クッキーとウェブ公告など、データベース同士が結合可能な方が価値ある資産になる）。迅速にプライバシー保護を行うソリューション技術は進展していて利用可能なのだが、法的・社会科学的分文脈で必要とされるまでは産業界が採用しない。
（会場質問←フランク・アパラス：独 KIT）インターネット取引に関しては、法的レベルとして、

DNA などもっと良い方法があるということか。
（会場質問）市民がプライバシーを重視しない。供給側の問題か。

第三日目

１．日時：2014 年 1 月 24 日（金）午前 8 時 45 分～午後 6 時
２　場所：ベルギー・ブリュッセル
３．参加者：情報通信研究機構 欧州連携センター長　菱沼宏之
４．概要：

パネルタイトル：法執行、サイバーセキュリティ、プライバシー

（司会：マックスプランク研究所 外交・国際犯罪法）サイバー犯罪条約の存在。2010 年から公私に適用。

（アチム・クラブンデ：欧州データ保護監視機関 EDPS）サイバーセキュリティについて。ネットワーク情報セキュリティは従来からの対策分野であり、個々人が防御している。サイバー犯罪対策は、法執行に関係し、人権を制約することもある。個人というよりは社会全体に関係する。サイバーディフェンスの大きな事件は、約 5 年前にエストニアで発生している。誰が誰に行使するかが問題となる。EU では、外交・防衛当局と、内務総局、情報セキュリティ当局とが協力しており、米国とも協議している。

（セシリア・ヴァークレイジ：欧州委員会 EU 内務総局）法執行は警察当局が実施。既存法も含めて説明する。各国当局がユーロポールに情報を提供する。ユーロポールは分析ワークファイル、捜査ファイルに基づき業務を行っている。これは、人数が多くて長期間関係するような組織犯罪対策には特に有効。

（エルズ・ドゥ・ブサー：マックスプランク）法執行当局が情報収集するのは、積極的な場合だけではない。データ保護をどうするかについて、必要性と均衡が必要。私企業・私主体のデータが、航空当局、欧米協定、金融関係等のために保管されており、また、電気通信事業者等は一定のデータを保管しており、警察目的に使われることもある。しかしながら、例えば指紋情報は相互法律支援のもののために使用されてはならない。

（ウルリッヒ・シエバー：マックスプランク）データ証拠について。プライバシー保護は、データ保管だけでなく、インテリジェンス機関間でのデータ交換時にも関係する。インテリジェンス機関でのデータの流れは、まず犯罪捜査の正当化を考える。当局が目の前に存在するのに犯罪捜査に使用しないことはないであろう。犯罪捜査の正当化に関し、インテリジェンス機関は将来の犯罪抑止を考える。欧州では、権力を制限するために、犯罪捜査を行う警察と、情報収集を行うインテリジェンス機関を分離している。一方、米国で FBI は犯罪捜査と情報収集の双方の機能を有している。

（機能が分離されている欧州では、）インテリジェンス機関の情報収集は疑わしい場合だけに限定されていない。犯罪捜査のためであれば、均衡等の原則が適用されるが、インテリジェンス機関の情報収集にこのような制約はない。このような違いは、犯罪捜査には厳格であり、インテリジェンス機関の情報収集には厳格でないという点に現れる。犯罪捜査のための情報収集に対するセーフガードは、インテリジェンス機関の情報収集には適用されない。欧州やドイツでは（犯罪捜査機関とインテリジェンス機関が）分離されているが、あまり明確に分離されていない国もある（例：FBI）。インテリジェンス機関はあらゆる情報に接することができる一方、犯罪捜査のためには証拠の基準が高く、取集手段や情報源も厳格である。犯罪捜査では情報源をどう秘匿するかが問題になる。米国では（犯罪捜査の情報収集とインテリジェンス機関の情報収集とが）異なる方法と判断で行う。（欧州では）犯罪捜査のための情報収集には公平な基準が必要となる。

（議論：モデレータ：マーク・ローテンベルグ：米国 EPIC）住所やバイオメトリック情報、目の色などを情報収集することについて、また、メタデータや過去と現在と将来の犯罪捜査について議論する。現在のセーフガードは従来のものを対象としているが、新しいサイバー犯罪等に対する規制としてはいかがなものか。

（欧州 EPDS）裁判所が均衡性と必要性の原則を確立してきた。欧州立法の解釈をどうするか。一般原則が新分野にも適用されるであろう。
（EU 内務総局）2010 年 3 月、ルクセンブルグの例で、裁判所が、収集でなく使用について述べたことがある。使用が鍵であり、裁判所は、6 か月以上保持されるべきでないとした。必要性と均衡性ということである。データ収集当局、最終的には政治判断もあるが。
（ウルリッヒ：マックスプランク）犯罪捜査の場合には確実性が必要。警察は広く情報収集しようとするが、何らかの制約が必要と考えられる。IP アドレスは短期間の保存に限定されるべきであるが、それでも危険性は残る。警察からインテリジェンス機関に複写されるかもしれない。
（エルズ：マックスプランク）均衡性が保証されない。
（会場質問←EPDS）CCTV カメラなどの件。モンスター・アプローチとも呼ばれる。ハニーポットもある。
（会場質問）誰でも 100%信用に値する訳ではない。メタデータによりテロリストにつながったり、過激派につながったりする。
（モデレータ）メタデータの収集は現在、米国の最高裁で 1972 年、司法省が作成したベトナム戦争対策のデータベースは、政治的反対派のために使われていることについて、害が見られないと判示した。しかし、その後に議会が、表現・結社の自由を制約するような政府の情報取集を制限した。
（司会：マックスプランク）欧州評議会が関係するデータ保護条約について。裁判所が決定するというのはセーフガードになる。

パネルタイトル：世界レベルのプライバシー法制定の呼び掛け

（ウイレム・デボーッケローレ：ベルギープライバシー委員会）国連が国家レベルで決議を求めている。プライバシーに関して拘束力のある法的枠組を作るため、タスクフォースを作り、ベルギーとしては世界的枠組を提案したい。

パネルタイトル：クラウドへの政府のアクセス

（司会：J.H.ジェペッセン：ベルギー・民主主義と技術センター）
（モデレータ：オマー・テーン：プライバシー保護国際連盟）
（ジョリス・ヴァン・ホボーケン：ニューヨーク大学）
（コネリア・カトラー女史：マイクロソフト研究所）
（ブライアン・カニングハム：パランティエール：弁護士：ライス大統領補佐官へのアドバイザー）
NSF（全米科学財団）が NIST（米国立標準技術研究所）と議論。米国だけでなく欧州の情報収集：インテリジェント機関にも疑いの目が向けられている。
（マリ・ハンセン女史：ドイツ通信社（DPA）シュレスウィッグ・ホルスタイン）
（ブライアン）電話盗聴の件やデータベースなどに関して。米国の弁護士は、何ができるかは言うが、倫理的な問題は気にしていなかった。裁判官は、異なる政党から指名されるので、結論が異なる。
（ジョリス・ホボーケン）米国の関係で国際法が傷ついている。米国家安全保障局（NSA）は効果的なことを実施できなくなっている。
（モデレータ）まず、技術的解決手段として、暗号化の標準と、データの場所（ローカリゼーション）を議論し、その後に、政治的・法的問題を議論したい。マイクロソフトは米国でない場所に保管することにしているのか。
（コネリア）マイクロソフトは最近数か月、グローバル・ネットワーク・イニシアティブにより、政府やインテリジェント当局から要請される法執行に応じて、データセンターの場所を探している。また、暗号化戦略とロードマップを描いている。透明化の観点もあり、他国の領域に保管している。
（ブライアン）マイクロソフトの声明は顧客の観点からも重要。欧州のクラウドに移行している。

米国のインテリジェント機関のコントロールは、米国の内と外とで強さが異なる。米国が（大規模に）情報収集する唯一の国で、ロシアや中国は米国ほど規則がない。
（マリ）法的保護がない。昼夜が変わることにより、インドの当局も関係してくる。アクセスの有無が分かりづらいので、独立したオンブズマンにより監視されるべき。スノーデンの後、色々あった。欧州クラウドは現地の法執行の下にあり、説明責任が果たせる。例えば銀行の口座など、アクセスは関係者に通知されるべきであり、即時でなくても必要。現在はプロバイダーの懸念により、（当事者に）通知されていない。高価になるが、契約で考慮されるべき。
（司会）米国政府は費用・ビジネスの点から消極的だが、変革が必要。そうしないと否定的な結論になってしまう。
（コネリア）データ・ローカリゼーションの要請を逃れている者がある。犯罪捜査手続で、欧州では直接データアクセス、欧州と米国間の傘になる条約がある。少なくとも法執行ではそんなにかけ離れていない。法的枠組の見直しが必要。国際的に議論し、産業界のアプローチが重要。
（モデレータ）暗号化についてはどうか。
（ジョリス）越境監視の技術的解決手段として、複雑な課題。技術と実施を組み合わせると、暗号化。グーグルが鍵である。安全な法定アクセスによる監視が可能となる。越境監視については、監視側である NSA への技術的提供に当たり、法的・政治的セーフガードが必要。透明化を図り、安全と証明される必要がある。欧州の機関は欧州市民のデータを有している。欧州のデータセンターは米国の法的枠組の下では保証されていない。
（モデレータ）法的枠組が政府によるアクセスの正当化に必要ということか。
（ジョリス）その通り。法的議論と技術との関係では危険性がある。欧州も含めた越境監視について、英国など欧州が相互にスパイしている。国際的な監視の基準を議論してセーフガードを合意する必要がある。そうしないと大変である。
（モデレータ）例えばテロリストについての共通の基準が必要と言うことか。
（ジョリス）合意可能と思うが、インテリジェンス機関はもっと複雑。政治や経済情報もある。
（マリ）スノーデンがツイッターで昨日、技術的には死んでいないと言っていた。電子政府の法律は遮断されない。信頼モデルの問題である。クッキーの可能性で、エラーメールがあった。クッキー関係の人と話すと、匿名化を言われた。ブラウザーで防止することが必要であり、また、暗号化、ネットワーク効果が重要。自己防御が必要。自己の責務として自己防御が必要。ハイジャックやプリズムなど。外交当局者、NISTのおかげで朝メッセージを受け取る。20 年も議論している。
（ブライアン）サイバーセキュリティ法律家は解決手段を持っている。暗号化が鍵。暗号化以外の技術、ペアレント技術。過去 10 年で技術会社が保護技術を改善してきた。ロボットがアクセス、徐々なるアクセス、他の目的を制約するなど、法的制約も必要。米国の裁判所は、何回、何日、何回電話したか、などの追跡により電話記録を作成すると、実施の問題は透明化が必要。
（コネリア：マイクロソフト）暗号化のロードマップは法的要請による。我々は顧客のプライバシーを保護する。企業による直接的な手段である。公的に言及するのは法的制約による。
（モデレータ）越境情報流通への国際・国内解決手段はどうか。
（会場質問：学生）NSA の議論で混乱しているのは、テロと均衡性について、テロでなく悪い人を懲らしめるということ。なぜこんな NSA のようなことを議論しているのか。米国の宣伝でなく、欧州クラウドなど次の段階に移動すれば良いのではないか。
（ジョリス）インテリジェンスの世界を議論するのは、現実的に彼らがいなくなる訳ではないからである。テロや経済的な問題がある。枠組みは均衡性に関係してくるが、まだ透明でない。正確な目的としては、目的を明確化し、議論し、他の部局と役割を議論し、進展させるべきこと。
（モデレータ）ある政府が他国と妥協するというのもあるが、経済的にはどうか。
（ジョリス）経済的というより、外交関係、戦略的な関係である。新しい監視能力、伝統的な反テロ、反核もあるが、インターネットは、深くオープンな議論が必要。国境、国家安全保障当局が追及する話であり、国際的な性格を有している。

（コネリア）9.11 後の米欧の反テロ合意。オバマ大統領はこれをまず考えた。ビジネスの観点からすると、顧客が米国内にいるので、米国内の顧客のプライバシーは重要。
（ブライアン）米国のインテリジェンス機関は透明。40 年間も文書を公開してきた。法を犯したと言われるのは他国に関する話であり、これは米国内では違法ではない。テロに関する話とそうでない話がある。米国の機関は外国政府の情報を収集しているが、米国のインテリジェンス機関が収集するのは合法であり可能である。特段、法を犯したのではない。
（会場質問）米国のネットワーク中立性は問題。セキュリティとプライバシーとの関係はどうか。ネットワーク中立性でパスの選択をどうするか。カリフォルニアで、信頼できるパスが AT&T のサンフランシスコを経由するのか。（インターネットは）電話のような信頼性が乏しい。
（司会）（信頼性を高めると）高価になる。中国やロシアでも色々ある。
（ジョリス）エンドエンドで、利用者が決定するものであり、問題ではないと思う。サービスレベルの選択の問題である。中央制御、プロトコルの問題であり、ネットワーク中立性に関係する。
（ブライアン）ネットワーク中立性があっても、個人は難しい。パケットの速度が落ちる点など。
（マリ）フィードバックとして、何かプロジェクトがあればよろしくお願いしたい。
（会場質問）マイクロソフトに対して、透明性をどう考えるか。グーグルのデータセンターについては、マイクロソフトは何も言わないが、同じではないか。欧州の法的コミュニティは、マイクロソフトはフリー（ただ乗り）である。マイクロソフトのデータセンターが、外国情報監視法第 702 条の命令により、米国以外の市民についてはどうなるか。
（コネリア）準備するチームがあり、既にロードマップの中にいるが、企業が決定する話である。後日発表されるであろうが、今反応できることは、顧客に発生するということである。我々は異なる法的防御のリストを見ている。
（会場質問）パトリオット法（米国愛国者法）、外国情報監視法第 702 条、規制当局の問題がある。情報セキュリティの均衡性が必要ではないか。
（コネリア）その通り。
（会場質問）スマートフォンにおける暗号化のアルゴリズムは信頼できるのか。政府は利用者を信頼しているが、利用者・会社向けに自己決定できる新しい枠組みはどうか。
（ジョリス）プライバシー技術の実施は、最終利用者に向けてのものとなる。技術の適用は法的にも関係する。エンドエンドの暗号化は、犯罪捜査のアクセスの均衡性との関係で判断できない。技術の実施が重要。
（モデレータ）欧州データ保護指令について。
（マリ）法的モデルとして、データの支配をどうするか。匿名化とはリンクを断ち切ること。匿名化技術を利用者に提供するが、異なる主体である。データ処理機器は、文化が関係せず、同じような問題がある。法定結論が異なる国ではどうなるであろうか。スマートフォンはビジネスモデルがある。20 年後を見ると、セントラルモデルを見る。中国だけでなく、中央化していく。
（モデレータ）現在の法的枠組は、コントロール者が信頼できるとの前提がある。
（会場質問）例えばスマートフォンでは、誰が信頼できるコントローラか。政府か。データはどうなるのか。
（会場質問）クラウドと信頼性、管轄権、技術的挑戦について。
（ブライアン）法と管轄権の問題でなく、技術の問題では、米国の例を見ると、いかに困難かが分かる。エンジニアをいかに政府から遠ざけようが、難しいものである。
（司会）効果的な手段として、運用や、他国のデータについて、政府のアクセスは民主的であるべき。

パネルタイトル：スマートメータ・スマートグリッド：プライバシーはどうか
（司会：ブリッジ）7 年前、グーグルは検索エンジンであったが、一番良いと言っていた。今は 300 万ドル。

（ヨーハン・ラムディ：ドイツ・アリアン）スマートメータに関し、スマートグリッド・タスクフォース 2012-2014 で、6 つのセッションを行った。グリッドオペレータの悪夢はブラックアウト。（スマートグリッドでは、電力のコントロールは）市民の権利となるので、グリッドを管理できないとそうなる。我々は、エネルギー網を確立・維持し、信頼性を持って供給する。透明性も重要。
（タイマン・ウィスマン：アムステルダム大学）ユーティリティ会社が社会的に受容されるためには、データ保護とプライバシーをどうするか。データ保護第 29 条作業部会がある。2012/27 の（エネルギー効率）指令で、スマートメータは、最終消費者の実際の消費を反映すべき、実利用時間の情報を提供すべき、最低限のメーターでエネルギー効率性と利益が考慮されるべきとされた。遠隔検針を許容している。標準化においては利用者・消費者の利益が反映されるべきである。モノのインターネット（IOT）にも関係する。スマートグリッドにおける個人データ保護は、国家が規制するのでなく、汎欧州的になるべき。
（会場質問）どんな標準が必要か。
（タイマン）プライバシーを尊重。
（アレシィア・テナス：ベルギー・独立エネルギー専門家：イタリア人）物理的挑戦として、ネットワークの尊重を挙げたい。ライン（通信回線）の設置は大変。民主主義的な参加が必要。越境は、アクセス容量の関係でハードルがある。最新の投資とのギャップがある。誰が投資しているかというと、メーカーが 45%、IT・電気通信事業者が 35%である。配送事業者は容量をコントロールできる。規制当局は事業者にとって利益が上がるような効率的な枠組を作るべき。「missing money」問題を解決せずに、プライバシーの解決はない。
（マーティン・スピンドラー：ドイツ・スマートエネルギー）誰が自己の消費している電気を知っているか。普通の人は、1 年間にたった 9 分間しか電気の消費量に関与しない。
（ラファエル・ギャラット：ブリュッセル自由大学）持続可能な開発（SD）にとっては、エネルギー効率性が必要。資源・経済・技術資本と天然資源の持続可能性が課題。
（KDDI 高崎）データ保護以外の利益として、生活の質の向上など、インセンティブとして何があるか。
（ジョアン）スマートシティは、セキュリティ等の課題がある。
（タナス女史）非中央処理化が重要。

パネルタイトル：民主主義、監視、インテリジェント機関
（司会：ゲリー・ホーマン：ドイツ・パソー大学）
（モデレータ：カスパ・ボーデン：仏独立プライバシー弁護士）対 NSA。
（ピーター・スワイアー：ジョージア工科大学）欧州データ保護や、米国クリントン政権でのセーフハーバー条項がある。オバマ大統領は小さいグループを作って安全保障のレベルを上げた。その中には CIA の No.2 の人などもいる。大統領は基本的権利として考えており、同盟国との安全保障も重視している。大統領が 1 月 17 日に演説したところでは、反省しているものであり、民主主義的な動きである。先週は色々な動きがあったし、70%が報告を受け入れた。プライバシーと市民の権利は、インテリジェンス機関にとって重要となった。米国プライバシー法は、米国民と非米国民とに分けている。
（コンスタンス・カーツ女史：ドイツ・カオス・コンピューター・クラブ）メタデータや、ハッキング攻撃について話す。オバマ大統領の話については、我々は前に進むだけ。私が思うに、十分ではないが、第一歩だと思う。スノーデンの暴露で明らかになったが、監視技術に 520 億ドルがつぎ込まれた。欧州人権裁判所は迅速に判断しそうである。ドイツでの議論では、公式にコントロールされているのではないとのことである。
（ピーター）オバマ大統領の演説では、プライバシーを考慮すると言っているが、米国の政治的演説では珍しく、詳細に触れている。
（ルイーズ・アラマッツ女史：LAC：代理）国際法の観点からスノーデン曝露の問題を考える。ブ

ラジルとドイツが深く関心を持っている。2013 年 4 月に人権・表現の自由・プライバシーを議論した。反テロの論文もある。スノーデンの暴露事例に関し、スウェーデンのトップの方と 1 月 22 日にインターネットガバナンスの話題となった。国家が人権保護と反テロとの均衡をどう取るか。9 月の国連総会でインターネットガバナンスの話題となった。国連憲章との関係で、スノーデンが曝露したのは、国際法で禁止されているレベル。国連憲章の主権との関係で議論がある。12 月の国連総会でも議論された。管轄権は、米国・英国でも議論されている。国連の観点もある。

（ウォルフガング・ホフマン・リー：ハンブルグ大学・元ドイツ憲法裁判所）個人・ビジネスのデータへのアクセスに関し、利用者はどこに通信が経由しているかを気にしていない。グーグル・マイクロソフト・アップル等が国家に協力しているとも思っていないであろう。ドイツの法律では、犯罪法、データ保護法は、どこに所在しようとも、（ドイツに一定の関係があれば）適用される。ドイツ基本法での扱い。基本的権利は、従来は領土内であったが、現在はどうであろうか。衛星で通信情報が収集されていたらどうなるか。基本法によれば、国家は通信の内容を保護しなければならない。これを破れば、政治的制裁や、議会・憲法裁判所の出番であろう。憲法裁判所はITシステムの信頼性も確保する。国際合意があればなかなか難しい。米国では当局。EU法での保護は、企業だけでなく表現までも対象としている。今必要なのは、グローバルなレベルでの自由の見直しであり、これはパラダイム・シフトでもある。軍事クラウド、経済的競合がある。市民社会とインターネット社会は融合している。

（ピーター）米国も憲法がある。

（会場質問）国家としては、（電気通信事業者による）技術的保護が必要か。

（ウォルフガング）欧州は組み合わせても良い。非欧州諸国への牽制にもなる。

（ピーター）グローバルで、ITU、ロシア・中国・イラク・サウジアラビアが決議しようとしたが、インターネットの自由が問題となった。カダフィ政権下のリビアを見てほしい。中国やロシアが主導するとインターネットの自由はどうなることであろうか。

（ルイーズ）どうやって人権保護と均衡を取るか。

（会場質問）人か、それともアメリカ国家か。

（ピーター）国家は強過ぎる。1772 年に米国憲法ができた時には、米国民と非米国民との違いを設けていない。

（カスパ）1990 年の事例において、強制機関が米国外では実行できないと判示された。データ保護の観点。

（ウォルフガング）ドイツ基本権では外国人も同様。信頼性と情報システムの統合は、スノーデン後も必要である。証拠情勢が必要である。

（会場質問）外交について。

（中央大学）米国最高裁判所が NSA を憲法違反と判示する可能性があるか。プライバシーに寄っている。

（ピーター）メタデータは保護対象ではない。

（カスパ）CIA は国防総省でない。

パネルタイトル：プリズムに対する EU の反応（スノーデン関係）

（司会：ポール・ドゥ・ハート：ブリュッセル自由大学）

（モデレータ：ジオヴァニ・ブタレリー：欧州 EDPS）監視プログラムが保護に欠けていたか。詳細が不足していたか。昨年 6 月に欧州議会は決議し、FTP 合意について、米国が監視について明言しない限りとした。欧州委員会は別のアプローチを行った。昨日 1 月 23 日に草案ができた。

（アレックス・ジョエル：米国国家インテリジェンス局長）大統領が 1 月 17 日に演説し、メタデータプログラム、300 頁の報告と改善策を示した。インテリジェンス世界の変化を示した。情報が保持される対象に対するプライバシー保護に注力する。私の立場は、対テロで 2004 年に設立された独立した組織であり、弁護士や独立監視官もいる。米国政府は権利保全に万全を期する。議会も

監視している。一般的原理が通用するようにする、外交チャネルも通じて。情報アクセスの質を考えている。政策指令の第4章。商用、他の目的、国家安全保障のためにということである。
（モデレータ）EUの初期コメントをどう考えるか。
（アレックス）信頼してもらえたと思う。大統領の指示による変化が何を意味するのかを見てほしい。
（ガスパ・ボーデン：独立プライバシー弁護士）大統領政策指令28号では、外国人が名指しされている。米国市民・領土以外には何の権利もないことになっている。オバマ大統領の演説で驚いたのは声調であるが、米国市民以外という根本問題についてはどうか。外国の領土は、国籍で差が設けられている。国際的には、ICCPR（市民的及び政治的権利に関する国際規約）。新しいインテリジェント機関の外国人の定義は、米国は差別や表現を抑圧する情報を収集しないと言ったが、通常はNSAがそのような情報を収集していたのか。第2章の使用の制限について、良く聞こえるが、外国人に対する差が残っている。情報の拡散と撤去で外国人との差が取り払われただけである。欧州人権規約の観点で考えると、個人は監視を意識すべき。新しい流れでは大統領の承認が変わり、議会だけが制定できることとなる。欧州委員会は収集に関心を示していたが。
（モデレータ）レディング委員は市民保護の動きをしていたが。
（アレックス）外国人というのは、保護の対象であり、通常の人を対象としたものではない。
（マーティン・シェイニン：欧州大学連合）米国の情報収集に対するEUの反応は、EUは法の組織というだけでなく、政治的組織であるということ。国際法違反の問題。第17条、世界人権宣言第12条の問題。1995年EU指令は曖昧であり、プライバシーに恣意的である。法定に問題。FP7でのSurveillance（監視）プロジェクトは、シナリオに関係して越境犯罪を対象としている。低いスコアであり、プライバシー保護に関して効果が薄い。大統領演説は残念。中庸であって国際的に拘束力がない。ドイツ等で立法したくない。米国・英国は外国人の人権を侵している。1980年代、フランスのセネガルにおける年金の問題で、管轄権は人権の問題で捉えられた。政治的権利、EU加盟国はプライバシー侵害について米国に苦情を言うべき。20か国が苦情を言っている。独立組織は、カダフィのリビアではないので、2014年3月・6月のパネル（英国議会）で議論。電子プライバシーは議論されるべきだが、法的に空疎ではならない。既存のプライバシーは、追加のプロトコル・枠組みが与えられるべき。独自の解釈で結論となる協定が認識されるべき。
（モデレータ）満足する理由としては、基本的権利や、EU内部の話など。
（ポール・ネミッツ：EU司法総局）6月に米欧で議論を開始したが、有用であった。法的基盤について質疑を行った。大統領演説と欧州議会の圧力により、大企業に影響があった。EUは、（米国が改革を）始めるその意思を歓迎する旨、速やかに報道発表を行った。真の変革を待っている。彼らに機会を与えるものである。なぜなら、米国人は自由を尊重するし、利益にかなうからである。NSAの活動に関して、今のEUの反応と聞かれれば、議論の対象であり、圧力がかかっている。NSA拒絶キャンペーンは弱い議論である。ルクセンブルグで、拒絶には大きい理由がある。我々はセーフハーバーを議論し始めたところである。大統領演説における同等取扱に関しては、セーフハーバーを考えていく。我々は、米国が進展したと言うところに到達した。米国は欧州人権裁判所の宿題を果たした。（欧州）委員は加盟国に手紙を送り、各国のセキュリティ庁がEUのコード（裁判所）が承認するように、調整し、うまく安全保障に比例するように、EUが比例原則を確認できるよう、安全保障なので何も言わないというのではないようにした。2006年にスパイとユーロという本を書いたが、EU法の下での相互のスパイについて書いた。国家安全保障と比例原則が必要である。EUは、加盟国の無実の人に差別的でないように、安全保障と比例原則となるべき。大統領命令は、時間の経過とともに使用に制約がかかるが、情報収集の前に、公共の情報源などあらゆる手段を講じ尽くす必要がある。これで終わり、再度、異なった危険性間の均衡を取る。自由への危険、経済への危険、政治的関係への危険性ということ。
（モデレータ）スパイしたくない。欧州デジタルセーフハーバーについて。
（会場質問←EU 司法総局）法律の進展を踏まえ、基本的権利と、条約の制限を考慮すると、安全

保障のために無制限の監視を認めるという訳にはいかないであろう。米国が欧州に同等取扱を再度付与してきた。
（カスパ）9.11 から外国諜報機関の動きが変わってきた。
（会場質問）法の調和について。
（アレックス）分野が異なっており、回答できない。
（米国アレックス）欧州の皆様、透明性は大統領が約束したものなので、ご理解頂きたい。

【結論】
（ピーター・ハスティン：欧州データ保護監督者 EDPS）（本会合の結果は、）良い伝統であり、受け入れたい。本日は既に、私の EDPS としての任務終了後 8 日間経っているので、後任に道を譲りたい。
データ保護見直しは関係者の合意が見られた。強い実践と一貫性、広い対象が必要。変革とその結果は不可避。さもないと死んでしまうことになる。公私の水平的視点による実践が失敗してしまう。解決は欧州レベルで机の上に乗っており、解決が可能である。協力の一環であり、受け入れられると思う。欧州レベルの解決が適用されるが、継続が必要。
NSA や同様の機関に対して、監察（サーベイランス）が必要。監察は、長期的視点で、幅広い視点で行うべきで、大統領演説は第一歩であり、さらなる歩みを期待したい。デジタルエコシステムとして、コミュニティの発展者が必要。他の機関と進展を考えている。グローバルな視点で合意できればと思う。OECD のガイドラインが昨年 6、7 月に見直された。欧州の見直しが世界のインテリジェント機関に影響を与える。
EU の枠組は道具であり、内容と原理等を分離すべきではない。EDPS が設立から 10 年経ったが、これは良い経験であった。10 年前は規制だけで予算もなかった。それ以来、チャールズ・マークスがプライバシーのガバナンスという良い本を書き、そこから変わった。監視・諮問（コンサルテーション）が行われた。米国のオブザーバーとなった。2008 年、データ保護当局がどうみられるべきかを考えてきた。良い協力関係を、KPI（鍵となるパフォーマンスインディケータ）で協力してきた。2010 年 3 月 9 日に真に独立となった。データ保護とセーフガードに関して、効果的で均衡が取れていることが重要である。

第四部　欧州におけるパーソナルデータの利活用及び悪用、漏洩に関する事例

第四部では、欧州におけるビジネスや公的サービスへのパーソナルデータ利活用事例（特に、匿名化・仮名化等により個人識別性をなくすことで利活用を進めている事例）、パーソナル情報の悪用、個人情報の露出等の事例について記す。事例において、どのような技術、制度、運用制限等がデータ収集・サービス展開に関わっているかを整理するとともに、日本における制度・文化等がデータ収集・サービス展開の障害になるか分析する。

第一章　欧州におけるパーソナルデータの利活用の事例

まず、欧州における民間企業及び公的機関によるパーソナルデータの利活用事例について記す。

第一節　政府のオープンデータ政策

A) 英政府のオープンデータポータル：data.gov.uk

英政府は、オープンデータ政策として、2009 年 9 月から「data.gov.uk」というウェブサイト[92]を立ち上げている（一般市民向けは 2010 年 1 月より）。同サービスは、英政府が保持するパーソナルデータ以外のデータへのオンラインアクセスポイントを提供することである。公表されるデータは匿名化されている。

☆ポイント：オープンデータでは、パーソナルデータは匿名化されている。

B) 仏政府のオープンデータポータル：data.gouv.fr

フランスでは 2011 年 2 月より首相の権限の下でオープンデータ政策が進められており、ポータルサイトが 2011 年 12 月に立ち上げられた[93]。同政策の所管機関は、エタラブ（Etalab）[94]である。フランスのオープンデータ政策の大きな特徴は、2013 年 12 月にポータルサイトが大きく変更され、公共機関等が情報を公表する他に、市民等もデータを公表することができるようになったことである[95]。同ポータルサイトでは、パーソナルデータ（医療情報、税収情報）や法律により公表できないデータ（医療、国防上の機密情報）は公表されない。

さて、2013 年 7 月に、仏パーソナルデータ保護機関のCNILはエタラブとともに、オープンデータ政策におけるパーソナルデータ保護の問題を検討するためにワークショップを開催している[96]。以下に、その結論を記す。

- 今日まで、オープンデータの枠組みで公表されているデータには、パーソナルデータはほとんど含まれていないように思われる。
- けれども、オープンデータの利用者は公表され、再利用されるデータが特定化可能な人物に結びつけられるかどうか評価することを難しいと感じることがある。データの供給者も再利用者も CNIL からの情報と実践的な助言を必要としている。
- 疑義がある以上、一定の行政機関はデータの公表に非常に慎重である。
- 情報供給者が利用できるデータの匿名化を保障する道具や方法はほとんどない。この点に

[92] http://data.gov.uk/
[93] http://www.data.gouv.fr/
[94] http://www.etalab.gouv.fr/pages/Qui_sommes_nous_-5883786.html
[95] http://www.etalab.gouv.fr/article-les-decisions-sur-l-open-data-du-cimap-du-18-decembre-2013-121702565.html
[96] http://www.cnil.fr/linstitution/actualite/article/article/open-dataet-donnees-personnelles-lancement-dune-consultation-des-acteurs/

関して、技術的解決や利用推奨の要求がある。

- 目的原則と自由な再利用の間の連結の問題は明確化されねばならず、関係者は時々情報と自由法を適用する困難に出会うことがある。

以上の結論を受けて、2014 年 1 月 7 日から、CNIL はオープンデータ政策関係者が出会った問題等の経験を共有できるようにオンライン上でアンケート調査を開始している。

☆CNIL とのワークショップで明らかになったことは、オープンデータ向けに匿名化されたデータを発表する際にも慎重にならざるを得ないことがあることであり、監督機関の助言等が常に必要となる。

第二節　ビッグデータ企業

ビッグデータは世界中で現在最も注目を集めている技術であり、欧州でも非常に多くの企業が設立され、様々な分野へデータ分析サービスを提供している。例えば、仏Critoe社[97]、仏adomik社[98]、独ParStream社[99]がある。通常ビッグデータ企業は、EUデータ指令に基づく各国の法律を遵守しなければならず、パーソナルデータを利用する場合には、データを匿名化する必要がある。だが、企業のウェブサイト上で、パーソナルデータの匿名化について説明する企業は少ない。

A) 仏データ・ピュビリカ社

2011 年 7 月に設立されたデータ・ピュブリカ[100]は、仏政府のオープンデータを利用したスタートアップ企業である。同社は、フランスの公的機関や民間組織（各種の協会等）が公表しているデータ等を利用して、それらのデータを加工し、民間企業等に提供するサービスを販売している。このため、同社はデータ源の特定、データの抽出、未加工のデータの構造化されたデータへの変換、契約によってDaaS（Data as a Service）の形式でデータの供給を行い、顧客の要求に応じてデータを加工・変換するか、あるいは市場予測等のためにデータを加工している。

☆オープンデータを利用して、情報分析サービスを提供する企業がある。

第三節　移動通信事業者の顧客移動データ分析サービス

A) 仏オレンジの「フリュビジョン」と「発展のためのデータ」

仏通信事業者オレンジは、フリュ・ビジョン（Flux Vision）というリアルタイムで、顧客のデータを統計情報へと変化する技術を企業と公共機関向けに開発している[101]。例えば、この技術により、人々の移動情報を分析することが可能になる。この技術を利用したサービスにより、観光部門では旅行客の移動や観光地への訪問率を分析でき、また交通部門では乗客の経路を分析し、交通インフラストラクチャを整備することが可能になる。オレンジは、このサービスは同社が開発した不可逆な匿名化の手段に立脚しており、顧客を特定するあらゆる可能性が排除されているとしている。なお、このサービスの開発は、仏パーソナルデータ保護監督機関のCNILとの意見交換をしながら行われ、CNILのお墨付きを得ている。マルセイユ市が所在するブーシュ＝デュ＝ローヌ県で、観光客の同サービスによる移動情報分析の実験が行われている。

また、オレンジ社は「発展のためのデータ（Data for Development：略称 D4D）」というプロジェクトをアフリカ西部のコートジボワールで実施している[102]。このプロジェクトでは、同国のオレ

[97] http://www.criteo.com/fr
[98] http://www.adomik.com
[99] https://www.parstream.com
[100] http://www.data-publica.com
[101] http://www.orange-business.com/fr/produits/flux-vision

[102] http://www.d4d.orange.com/home
http://www.d4d.orange.com/learn-more

ンジのモバイルユーザーの電話通信データ（2011 年 12 月から 2012 年 4 月）を匿名化して開放し、研究者が社会・経済の発展に係る革新的な研究を行う。

☆オレンジは、監督機関である CNIL と意見交換しながら、移動情報分析システムを開発している。また、ビッグデータは発展途上国の社会経済政策にも利用されている。

B) 西テレフォニカの「ダイナミックインサイト」と「スマートステップ」

スペインの通信事業者テレフォニカも、仏オレンジと同じく、顧客のモバイルデータを匿名化し、集積して、人々の集団的な行動を理解する「ダイナミックインサイト」というシステムを開発している[103]。このシステムにより、人々の行動をほとんどリアルタイムで、毎時間、毎日観察することが可能になる。同事業者は、世界中に 3 億 900 万人の顧客（社員は 28 万 5000 人）を持ち、顧客はデータを供給している。この技術のため、テレフォニカは、MIT メディア研究所、GfK、オープンデータ研究院、世界経済フォーラムと提携している。なおテレフォニカは、このシステムは人の集団的な行動を観察するもので、個人の行動を観察するものではないとされている。

テレフォニカは、ダイナミックインサイトに基づき、独市場調査会社GfKと提携して[104]、企業や公共機関向けに「スマートステップ」という集団の行動を分析するサービスを提供している。特に、小売り、交通、レジャー、メディア等に利用できるとし、例えば、旅行者の動きに即して小売業は店舗の位置を決定することが可能になる。スマートステップの利用者としては、英スーパーマーケット、モリソンの例が挙げられる。モリソンはスマートステップを利用して売上げの増大に成功している[105]。テレフォニカ傘下の英通信事業者O2 のユーザーのデータを分析し、クーポン券を配布する地域を決定した結果である。

第二章　欧州におけるパーソナルデータの悪用及び漏洩の事例

ついで、欧州諸国（英仏）におけるパーソナルデータの悪用及び漏洩の事例について記す。

第一節　英国

英国では、パーソナルデータ保護監督機関の ICO が、データ保護法が遵守されているかどうか検査しており、その報告が同機関のウェブサイトで公表されている。以下に、同機関の報告を基に英国におけるパーソナルデータの悪用及び漏洩の事例について記す。

A) デートサイトによるデータ保護法の違反

2013 年 6 月 29 日のICOの報道発表によると[106]、ICOは英国に基盤を持つ 4 大データサイト（eHarmony, match.com, Cupid, Global Personal）に対して検査を行い、データ保護法が遵守されていない点があるとして、同 4 サイトに質問への回答を要求している。特に、ICOにより懸念されている事項は次の点である。

1. パーソナル情報の利用に同意を与える利用規約がほとんど可視的な状態にない
2. これらの利用規約が、メンバーのデータをデータサイト企業へ「永続的に」あるいは「不可逆に」利用する免許を与えてしまっている。
3. ウェブサイトがパーソナル情報の損失や損傷にいかなる責任も持たないとしている。
4. 利用規約が与えられる前に、ユーザーは個人的情報の詳細を与えるように要求されている。

☆ ポイント： このケースでは、日本ではいわゆる出会い系サイトと言われるサービス業者のパー

[103] http://dynamicinsights.telefonica.com/479/about-us
[104] http://dynamicinsights.telefonica.com/641/gfk-2
[105] http://dynamicinsights.telefonica.com/1158/a-smart-step-ahead-for-morrisons
[106] http://ico.org.uk/news/latest_news/2013/ICO-writes-to-online-dating-companies-29072013

ソナルデータ管理が問題となっている。英国の同種サイトでは、どのようにデータ管理が行われているか不透明であった結果、ICO が警告を出している。

B) ネットワーク型ビデオゲームからのパーソナルデータの漏洩

2013 年 1 月 24 日のICOの報道発表によると[107]、日ソニー・コンピューターエンターテイメント・ヨーロッパ社は、データ保護法の重大な侵害を犯したとして 25 万ポンドの罰金を課された。罰金の理由は、ソニー・プレイステーション・ネットワークプラットフォームが 2011 年 4 月にハッキングされ、英国内で数百万人の顧客のパーソナル情報（氏名、住所、メールアドレス、生年月日、アカウントパスワード、顧客の支払いカード情報）が流出した危険がある。ICOによれば、ソフトウェアがアップデートされていれば、この攻撃は防げたであろうとしている。この漏洩事件はICOに報告された中で最も申告な事例の一つであるとICO幹部は話している。

☆ポイント： このケースは、サイバー攻撃によるネットワーク型ビデオゲームのパーソナルデータ漏洩の事件であるが、漏洩規模が大きく、漏洩したデータの内容も重要で、極めて深刻である。ICOは、ソフトウェアがアップデートされていれば、この攻撃は防げたであろうとしており、パーソナルデータの徹底した管理の必要性が要求されている。

第二節　フランス

フランスでは、パーソナルデータ保護監督機関の CNIL が情報と自由法を組織が遵守しているかどうか検査しており、その報告が同機関のウェブサイトで公表されている。以下に、同機関の報告を基にフランスにおけるパーソナルデータの悪用及び漏洩の事例について記す。

A) 通信事業者のパーソナルデータ漏洩

フランスの情報と自由法の第 34 条bisでは、電子通信サービス事業者にパーソナルデータ侵害が合った場合CNILに通知し、場合によっては、侵害に関係する人にその旨を通知する義務が定められている。また、2013 年 8 月に発効した通知措置に係るEU規則はこの通知の期限や内容等を詳しく規定している[108]。CNILは通知義務に関して、詳しく同機関のウェブサイトで知らせている[109]。

2014 年 1 月 16 日、仏大手通信事業者オレンジの顧客のパーソナルデータ 80 万人分が、フィッシング詐欺により漏洩したことが明らかになった[110]。オレンジの発表では、顧客のパスワードは漏洩していないものの、氏名、郵便番号、コンタクト用のメールアドレス、電話番号（固定か携帯）が主に流出し、世帯構成、定期契約者数も流出した。80 万人は、オレンジの顧客数全体の 3%にあたる。被害者は同通信事業者の顧客向けページに成り済ましたページから、自分のパーソナルデータを入力し、データが漏洩した。なお、同事例では、オレンジはデータ漏洩が明らかになった翌日にCNILに通知し、侵害にあった顧客にも通知している。

この大規模なパーソナルデータ漏洩事件を受けて、仏パーソナルデータ保護監督機関であるCNILは、2014 年 2 月 3 日に仏主要通信事業者を集めて、パーソナルデータの侵害が生じた際の法規制枠組み、またなすべきこと、同機関が持つ検査と刑罰の権限について説明した[111]。

☆ポイント： このケースはいわゆるフィッシング詐欺によるパーソナルデータの漏洩事件である。通信事業者オレンジは法律に則り、漏洩の事実が発覚後、すぐに CNIL と侵害にあった顧客に通知

[107] http://ico.org.uk/news/latest_news/2013/ico-news-release-2013
[108] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:01:FR:HTML
[109] http://www.cnil.fr/vos-obligations/notification-de-violations/
[110] http://www.lefigaro.fr/secteur/high-tech/2014/02/03/01007-20140203ARTFIG00003-les-donnees-personnelles-de-800000-clients-orange-piratees.php
http://www.zdnet.fr/actualites/orange-pirate-les-donnees-privees-de-800-000-clients-detournees-39797547.htm
[111] http://www.cnil.fr/nc/linstitution/actualite/article/article/violation-de-donnees-personnelles-la-cnil-reunit-les-operateurs-de-communication-electronique/

している。

B) 医療施設における患者医療データの取扱不備

仏公衆衛生法では、公共及び民間の医療施設は医療活動の分析を行うことが義務づけられている。患者に対する医療行為は特殊な一覧表によってコード化されており、各行為に病気保険による返済が対応している。活動分析とコード化に誤りがないか検知するために、一定の医療施設では外部の組織に作業を依頼することがある。情報と自由法の第 10 章によれば、治療と予防活動の評価と分析を目的とするパーソナルデータの処理は CNIL の許可が必要となり、CNIL はこのような処理が病人の記名データに関わらないかどうか監視している。

2013 年 6 月 5 日と 6 日にサン・マロ病院でCNILが検査を実施した際に、公衛生法と情報と自由法を誤解し、サービス事業者が病院側の合意の下に 95 人の患者の医療ファイルに閲覧していたことが明らかになった[112]。

病院側はすぐに対応し、事業者による医療ファイルへの情報アクセスの消去、情報システムのセキュリティに係る厳格な方針の形式化し、医療情報に責任がある医者と施設により権限を与えられた者のみ患者のファイル（コンピューターで処理されたファイルと紙のファイルの両方）を閲覧できるようにし、いかなる記名情報もこの事業者にはアクセス不能になった。

☆ポイント： このケースは、医療情報という特に秘匿されるべきデータを第三者組織が閲覧していた事件である。第三者による医療情報の閲覧には匿名化が必要であった。

C) 顧客の銀行情報保存の不備に係るオンラインショッピングサービス事業者への警告

インターネット上での買い物の際に顧客により伝えられる銀行データに関しては、その性質上、保存条件が厳格であり、高いセキュリティを確保する措置を講じなければならず、情報と自由法を遵守しなければならない。また、決済後の同種データの保存に関しては、事前に顧客の同意を得て、一定の期間しか保存できない。

2012 年 2 月、CNILは仏大手レコード・書籍販売店フナックのオンラインサイト（fnac.com）を運営しているフナック・ダイレクト社の事務所で検査を行った[113]。検査の結果、銀行データ（銀行カード上の名前、カードの有効期限、セキュリティコード、カード番号）が顧客に損失を与えていなかったものの、保存条件が不十分だったことが明らかになった。また、このデータセンターは有効期限内、あるいは有効期限が切れた数百万の銀行カードに関するデータが、除去の対象となることなく保存されていた。

銀行データの収集に関しては、同社は決済後、顧客が次回の買い物の際に再びデータを入力しなくても済むように、顧客のデータを初期設定で保存していた。CNIL によれば、データ保存について顧客に伝えられた情報が不十分であると判断し、一回の決済後に銀行データを保存する際には、当人の事前の同意が必要であることを喚起している。

☆ポイント： このケースは銀行情報という高いセキュリティの確保が必要となるデータを巡る事件である。オンラインショッピングが日常的なものとなった今日、銀行のデータのセキュリティを強化することは必要不可欠である。その上、このケースでは、顧客の同意を得ることなく、銀行データを保存していたことが問題となっている。

112
http://www.cnil.fr/linstitution/actualite/article/article/mise-en-demeure-dun-centre-hospitalier-pour-non-respect-de-la-confidentialite-des-donnees-de-sa/
http://www.cnil.fr/linstitution/actualite/article/article/cloture-de-la-mise-en-demeure-adoptee-a-lencontre-du-centre-hospitalier-de-saint-malo/

113
http://www.cnil.fr/linstitution/actualite/article/article/avertissement-pour-la-societe-fnac-direct-en-raison-de-manquements-dans-la-conservation-des-donne/

D) 従業員が有するデータへのアクセス権利の拒否

自分のパーソナルデータへアクセスする権利は情報と自由法により認められた権利の１つである。2011 年 6 月、エキップメント・北ピカルディ社の従業員は同社が保持するパーソナルデータ、特にこの従業員が利用する自動車の位置情報データへアクセスし、複写することを要求したが、拒絶されたとしてCNILへ苦情を寄せた[114]。この従業員は、自分が被害に合った交通事故について裁判所で証明する必要があり、データへのアクセスの要求は正当なものであった。CNILは同社へ書状を送り、データへのアクセス権利を定めた情報と自由法第 39 条に基づき、同社は従業員がパーソナルデータにアクセスする権利を有することを伝えた。同社は、CNILの書状を無視したため、1 万ユーロの罰金をCNILは課した。

☆ ポイント： このケースは、パーソナルデータへアクセスする権利を巡る事件である。雇用者は従業員が自分のデータへアクセスすることを要求する場合には、そのデータを開示しなければならない。

以下に、上記の事例のポイントをまとめる。

- （英）いわゆる出会い系サイトと言われるサービス業者によるデータ管理が不透明であった → パーソナルデータを管理する企業は様々であり、出会い系サイトもその中に入る
- （英）サイバー攻撃によりネットワーク型ビデオゲームのパーソナルデータが漏洩したが、その規模が大きく、漏洩したデータの内容も重要で、極めて深刻であった → サイバー攻撃には常に警戒する必要がある
- （仏）移動通信事業者がフィッシング詐欺に合い、顧客のパーソナルデータが流出した → パーソナルデータの漏洩事件が生じた場合には、法律に則り、漏洩の事実が発覚後、すぐにパーソナルデータ保護監督機関と侵害にあった顧客に通知する義務がある
- （仏）医療施設の患者データの第三者による閲覧 → 医療情報という特に秘匿されるべきデータを第三者組織が閲覧する場合には、匿名化することが必要である
- （仏）オンラインショッピングサイトの銀行情報の取扱不備 → 銀行情報の取扱いには、高いセキュリティを確保することが必要となる上、オンライン決済の簡略化ために、銀行データを保存するには顧客の同意が必要である
- （仏）雇用者の従業員のデータアクセス権の拒否 → 雇用者は従業員が自分のパーソナルデータへアクセスすることを要求する場合には、そのデータを開示しなければならない

以上の事例では、サイバー攻撃の他、パーソナルデータ保護の法制度に関しては、パーソナルデータの管理の透明性、データ漏洩の通知義務、データの匿名化、同意の取得義務、データへのアクセス権等が問題となっている。日本の企業がパーソナルデータ保護の管理と処理に係る事業を行う場合には、以上の点に注意する必要がある。

114 http://www.cnil.fr/linstitution/actualite/article/article/un-employeur-sanctionne-pour-avoir-refuse-la-demande-dun-salarie-voulant-acceder-a-ses-donnee/

第五部　欧州における米諜報機関の活動を巡る動向

2013 年 5 月以来、元 CIA（米中央情報局）職員エドワード・スノーデン氏によって告発された米諜報機関 NSA（国家安全保障局）の通信傍受活動は、特にその規模の大きさから世界各国で大きな批判的な反響が起こり、欧州諸国でも盛んに報道されている。欧州各国では、法律家や ICT 研究開発者等が集まり、プリズム問題について議論されるとともに、欧州委員会が作業部会を米政府機関と設立し、正式に協議している。第五部では、欧州委員会の同問題への取り組みと欧州各国での反響について記す。

第一章　欧州委員会の米国の諜報プログラムへの取り組み

2014 年 1 月 28 日の「データ・プロテクション・デイ」の前日、欧州委員会が発表したパーソナルデータ保護政策に関する声明によれば[115]、米国の諜報活動によって米国と欧州の大西洋間の信頼関係が損なわれたとともに、同事件はアメリカに対して経済的なインパクトを与えており、アンケート調査に対する 56%の回答が米国にベースを持つクラウドサービス事業者と提携することに躊躇し、諜報活動の暴露は今後 3 年間に渡って米クラウドコンピューティング産業に 220 億ドルから 350 億ドルの減益をもたらすという評価もされており、信用の損失は収益の損失であるとし、欧州委員会は米国を非難している。

第一節　欧州委員会の 6 つの対応

2013 年 11 月、欧州委員会は米国と欧州の信頼関係を回復するために、戦略文書[116]を発表し、6 つの行動を取るとしている。

1. EU データ保護法の迅速な改正：データが海外に移転され、処理される時の明確な規則を定める強力な法枠組みが必要である。

2. 米国と欧州のデータ移転に係るセーフハーバースキームをより安全にする：欧州委員会はセーフハーバースキームの機能を改善するために、13 の推奨を与えている。2014 年夏までに対応する措置を特定する。

3. 法執行分野でのデータ保護手段を強化する：現在交渉を進めている米国と EU 間の警察・司法提携におけるデータ移転と処理に係る「アンブレラ合意」を迅速に決める。この合意は、米国と欧州の市民が同一の権利により高いレベルの保護を保証する。

4. データを取得するために、米国と EU 間の既存の相互法的支援と部門別になされた合意のような法的枠組みを利用する：米国は、一般原則として、「旅客情報合意」や「テロ資金追跡プログラム」のような米国と EU 間の相互法的支援や部門別の合意という法枠組みを利用すべきである。

5. 米国で進行中の諜報プログラムの見直しに欧州の懸念を伝える：欧州委員会は米国の諜報プログラムの見直しを歓迎する。

6. プライバシーの標準を国際的に振興する：米国は欧州評議会条約第 108 号（個人データの自

[115] http://europa.eu/rapid/press-release_MEMO-14-60_en.htm
[116] http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

動処理に係る個人の保護に関する条約）に署名すべきである。

第二節　米国と EU 間の作業部会の活動

2013 年 7 月に、米国の諜報活動に関する事実とEU市民のパーソナルデータへのインパクトを検証するため、EUと米国間で作業部会が立ち上げられており、2013 年 11 月 27 日に結果報告書が発表された[117]。それによると、第一に、米国の諜報プログラムが実際に存在すること、第二に、そのプログラムに対する米国民と欧州市民の間にデータ収集の範囲や権利の保護に関して格差が存在すること、第三に、外国情報活動監視裁判所や支援する企業には秘密事項が多く、パーソナルデータの収集と処理について情報を与えられる法的あるいは行政的手段が米国民にもEU市民にもないことが明らかになった。米諜報プログラムの法的基盤としては、外国情報監視法（FISA）の第 702 条、米国愛国者第 215 条、大統領令第 12333 号が特定されている。

第三節　米国の諜報プログラム見直しに対する反応

2014 年 1 月 17 日、米オバマ大統領がNSAの諜報活動の見直しを発表している。それに対して、まず欧州委員会は同日、同大統領の発言を歓迎するという声明を出している[118]。だが、翌日の仏主要紙であるル・モンド紙は、米大統領の見直しには本質的に諜報活動を変更するものではないとしている[119]。さらに、NSAの欧州における諜報プログラムについて調査を実施している欧州議会の市民の自由・司法・内務委員会は、オバマ大統領の発言に否定的に反応し、失望させるものであったとしている。なお、2014 年に 1 月 9 日には、欧州議会の同委員会はエドワード・スノーデン氏を証言者として招くことを決定していた。事情聴取はブリュッセルとロシア間でビデオ会議による実施が考えられている[120]。

なお、仏報道記事によれば[121]、2014 年 2 月 24 日に開催されたEU-ブラジルサミットで、欧州と南アメリカの 2 大陸間（ポルトガルのリスボン市からブラジルのフォルタレザ市）に、米諜報機関の活動を回避するために、電気通信向けの海底ケーブルを敷設することが決定した。現在まで、ブラジルは欧州へのほとんどの通信をアメリカの海底ケーブルを使用していた。この計画には 1 億 3500 万ユーロが必要となる見込みであり、ブラジルとEUから資金が拠出される予定である。

第二章　欧州諸国における米国の諜報活動への反応

欧州において、スノーデン氏の告発は様々な議論を巻き起こし、多くの講演会やパネルディスカッションが行われている。フランスのデジタル部門を活性化させるために、新しい情報通信技術についての意見交換及び議論の場を提供するフォーラム・アテナは、年に数回イベントを開催し、ある 1 つのテーマについて、会場の聴衆とともに自由に議論しているが、その一貫として、2013 年 12 月 4 日に、NSA の通信傍受プログラム「プリズム」を検討するパネルディカッションを開催した。パネルディスカッションでは、自由活発に議論がなされ、フランス、そして、欧州のプリズム問題に対する反応を見ることができる。以下に、その模様を要点のみ記す。

---

117 http://ec.europa.eu/justice/newsroom/data-protection/news/131127_en.htm
118 http://europa.eu/rapid/press-release_MEMO-14-30_en.htm?locale=en
119 http://www.lemonde.fr/international/article/2014/01/18/l-affaire-snowden-force-obama-a-reformer-la-nsa_4350403_3210.html
120 http://www.lemonde.fr/technologies/article/2014/01/18/discours-d-obama-decoit-les-eurodeputes-qui-demandent-a-entendre-snowden_4350511_651865.html
http://www.zdnet.fr/actualites/snowden-sera-entendu-par-le-parlement-europeen-39796975.htm
121 http://www.lemonde.fr/ameriques/article/2014/02/25/bresil-et-europe-prevoient-un-cable-sous-marin-pour-eviter-l-espionnage-americain_4372725_3222.html

ICT イベント視察レポート：「PRISM（プリズム）：欧州デジタルの弱さ？」

日程：

2013 年 12 月 4 日（水）：午後 6 時～8 時

場所：

フランス・パリ（ISEP：パリ電子工学高等研究院[122]）

イベント主催者：

フォーラム・アテナ（Forum ATENA）[123]

パネル参加者：

- 司会：クリストフ・デュボワ=ダミアン氏（フォーラム・アテナ事務局長兼インテリジェンスエコノミックアトリエ議長）
- フィリップ・ルクープ氏（フォーラム・アテナ議長）
- ジェラール・ペリク氏（セキュリティアトリエ議長：EADS 社）
- オリヴィエ・イテアヌ氏（控訴院弁護士兼法律アトリエ議長）

イベント参加者数

約 30 名

イベント概要（議論のポイント）

0. はじめに：クリストフ・デュボワ=ダミアン氏（フォーラム・アテナ事務局長兼インテリジェンスエコノミックアトリエ議長）

- 元 CIA 職員スノーデン氏が告発した重要なことは、通信傍受プログラムの規模の大きさであった。常にスパイ活動は行われてきたし、皆が知っていた。また、手段は時とともに変化してきたが、今回はその規模が大きかった。
- 欧州とアメリカでは、社会と個人の関係が異なり、国防と経済の分野に見られる。国防に関しては、アメリカでは個人情報の保護よりも安全性が優先され、愛国者法により電話が盗聴され、ハードディスクに保存されたデータを調べられても、政府の行動をあまり問題視しない。だが、欧州では異なる。英国はアメリカに近いところがあるものの、特にドイツでは、ナチズムと共産主義の経験があり、政府の諜報活動に最大限注意が払われる。フランスは、アメリカとドイツの中間に位置づく。そして、この違いが経済の分野にも見られる。
- スノーデン氏の告発により分かったことは、民間企業もスパイ行為の対象になり、プリズムはテロ対策だけでなく、経済戦争の手段へと拡大していることである。従って、個人の自由や民主主義の問題にだけに留まってはいけない。

1. オリヴィエ・イテアヌ氏（控訴院弁護士兼法律アトリエ議長）

- 諜報活動の手段だけでなく、この種の活動に対する法律も変化してきている。
- プリズムと愛国者法は、諜報活動の新しい 3 つの点を示す。

[122] http://www.isep.fr
[123] http://forumatena.org
フォーラムへ政府等から助成金は支給されていない。

- 第一に、2001 年 9 月のテロ事件の後、アメリカでは愛国者法が成立した。この法律は市民の監視を合法化する。この法律は暫定的なもので、5 年毎に見直す必要がある。数年前に、ある上院議員が個人情報保護を保障するため、同法の改正を望んだが、拒否されたことがある。
- 第二に、通信システムの監視活動は、通話やインターネット回線の傍受だけではなく、グーグル、アマゾン、ファイスブック、ツイッターらの IT サービス企業と提携として、アメリカ本土にあるデータセンターへ合法的に直接情報を探すことにある。
- 第三に、インターネットは、各国政府、諜報機関、大企業にとって、市民を監視するための素晴らしい場である。なぜなら、プリズムにより、インターネットを通して、市民を日常的に監視できるからである。このような監視は民主主義の敵である。

1. 質疑応答・意見・感想等

- （会場からの意見）プリズムの法律上の問題は、欧州諸国が各国の法律でもなく、欧州の法律でもなく、アメリカの法律で合法的に監視されていることだと思う。
- （会場からの質問）フランスで個人情報保護を所管する行政機関「情報処理及び自由に関する国家委員会（CNIL）」は、この問題に対して、一定の役割を果たすことができるか。
- （イテアヌ氏の回答）プリズムの問題に対して、CNIL の有効性は現在大きなものではない。CNIL はフランス国土内でしか活動できないことを忘れてはいけない。だが、同機関の活動を強化することはプリズムへの対抗策になるかもしれない。クラウド業者を諜報機関から守る法制度が必要だと思う。また、個人情報保護に関する EU 法が改正中であり、これも対抗策になるだろう。現 EU 議長国はギリシアであるが、同法の改正を加速させると公言している。同法の改正は 2 年前に開始されており、時間がかかっている。
- （会場からの質問）現在、アメリカで軍事関係の法案が審議されており、愛国者法に関連するものであると聞いたが。
- （イテアヌ氏の回答）その通り。私も詳しくは知らないが、そう聞いている。
- （会場からの意見）フランスでは常に愛国者法ばかりが話題になるが、プリズムやアップストリーム（UPSTREAM）という米監視プログラムを合法化しているのは、愛国者法ではなくて、2008 年に改正された米 FISA（外国情報監視法）の第 702 条である。FISA の対象は、2008 年以前は電気通信事業者だけであったが、改正により、その対象に ICT 事業者も含まれるようになり、クラウドサービス事業者も対象になったそうだ。

2. フィリップ・ルクープ氏（フォーラム・アテナ議長）

- グローバリゼーションが監視システムに影響を与えている。民主主義社会では、監視システムというものは民主主義の原理に従うものであり、権力者が監視システムを設置する場合には、市民の側がそのシステムを監視する制度を持つ。だが、グローバリゼーションのせいで、プリズムのような監視システムを監視する制度が現在存在しない状態であり、バランスが取れていない。

3. ジェラール・ペリク氏（セキュリティアトリエ議長：EADS 社）

- プリズムに関して、セキュリティの観点から話をしたい。現在、フランスの組織の重要情報はどこかへ流出していることは確かである。
- 2010 年に、フランスは G20、G8 の議長国であったが、その際に仏財務省の重要情報が中国へ流出していることが仏情報機関により発見された。
- だが、2012 年、大統領選の際、エリゼ宮（仏大統領官邸）の機密情報が今度はアメリカへ流れていることが発見された。この時、初めて中国だけなくて、アメリカも情報を盗んでいることがわかった。

- また、同じく 2012 年に、元 NSA 職員が企業を設立し、アメリカと欧州の公的機関、軍、企業の情報流出先をインターネット上で追跡したが、そこは中国の上海郊外にある人民解放軍の施設だったことが分かった。これにオバマ大統領は激怒したそうだが、中国側は他国によってもっと攻撃されていると考えた。そして、数ヶ月後のスノーデン氏の告発により、全ての国がアメリカにより攻撃されていることが明らかになった。
- 2012 年 12 月 15 日から 2013 年 1 月 5 日の間に、フランスで 6000 万件の電話会話が盗聴されており、その情報はアメリカに渡っている。スノーデン氏によれば、独メルケル大統領や仏オランド大統領の電話会話もアメリカにより盗聴されている。
- アメリカの通信傍受システムは、メタデータ（発信者と受信者、日時等の情報）を取得しているが、ある一定の検索ワードにより（例えば、核兵器、サイバーセキュリティ等）通話者を特定でき、ビッグデータにより、どんな活動をしているのか知ることができる。
- NSA がアメリカの都市部外に数億台のサーバを持つ非常に巨大なデータセンターを設立中である。
- アメリカはイランにウィルスを送っており、PC やスマートフォンをターゲットにスパイ活動を行っている。

3. 質疑応答・意見・感想等

（会場からの質問）欧州でアメリカと中国により大規模な通信傍受が行われていることは分かったが、それに対してどのように情報を守ればいいのか。

（ペリク氏の回答）まず、通信傍受のリスクを減少させることはできるが、ゼロにすることはできないと考えた方が良い。アメリカのクラウドサービスを提供している企業（グーグル、アマゾン等）のサービスを利用すると、愛国者法により情報を見られる恐れがあるので、リスクを減少させるためには、フランス企業によるクラウドサービスを提供することが重要である。また、中国は巨大なファイアフォールにより、独自のインターネットを構築しており、中国から米グーグルのサイトにアクセスしようとしても不可能であり、アメリカに属するインターネットと連帯していない。欧州やフランスもそうすることは可能である。また、リスクが完全になくなるわけではないが、重要な情報には暗号をかけることは有効である。なお、15 年前はマッキントッシュにはウィルスは少なかったが、現在は iPhone や iPad の流行により、ウィルスは蔓延している。

（会場からの質問）アメリカが例えばフランス人の健康情報等を監視し、盗んでも、それほど意味はないのではないか。

（ペリク氏の回答）否。米保険会社が健康情報を利用し、保険加入を拒否できるかもしれない。

（司会の意見）1780 年の第一次産業革命、1880 年の第二次産業革命の後、我々は 1980 年に開始された第三次産業革命期にいるが、フランスはこの革命に大きく失敗した。現在、クラウドやビッグデータの技術、ソーシャルネットワーキングサービスによって、1930 年代のフォーディスムに類似するような大量生産の革命期におり、個人情報の問題はあるとは言え、これに乗り遅れてはいけない。

（ペリク氏の回答）その通り。ビッグデータは全てを変える。ビッグデータにより、我々はデータそのものではなく、データ同士の関係にアプローチする。フランスは、ミニテルの発明によりインターネットへの転換に失敗したが、数学と統計の分野ではとても強く、データを処理するためのアルゴリズムが重要なビッグデータに関しては非常に有利な点を持つ。

（会場からの質問）民間企業は、ビッグデータの研究者とどのようにしてコンタクトを取ればいいのか。

（司会の意見）フォーラム・アテナでは民間企業と研究機関の橋渡しをしており、企業の力になれる。

（ペリク氏の回答）テレコム・パリテック（仏電気通信系の高等教育・研究機関）に由来するスタートアップ企業は30あるが、その半分はビッグデータに関するものである。また、アルノー・モントブール生産復興大臣はビッグデータに非常に敏感である。

人間が秘密を持つのは当然であり、秘密がなければ、人間は数字と同じである。従って、個人情報を盗むのは悪いことであると思う。

結語

以上、欧州におけるパーソナルデータ利活用時の暗号・情報セキュリティの活用に関する欧州のガイドライン・法制度・標準化動向について概観した。報告書のまとめに関しては、本報告書の冒頭に全体の要約を収録したので、そちらを参考にしていただきたい。パーソナルデータ保護は世界中で現在最も注目されているICT政策の１つであるが、欧州では人権の観点からデータ保護が考えられ、その必要性に対する意識が高く、それに伴い、法制度に関する議論も豊富である。このような欧州の現状を知ることは、日本においてパーソナルデータ保護制度を策定する際に非常に有用である。