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

（概要）

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

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[1]、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[2]。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

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

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[3]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[4]。

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[5]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[6]。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。

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。

---

[3] http://www.oii.ox.ac.uk/research/
[4] http://www.inria.fr/equipes/privatics
[5] 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。
[6] http://www.telecom-paristech.fr/recherche/chaires.html

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。