欧州におけるプライバシー保護技術に係る研究開発の

最新動向調査報告書

平成 27 年 2 月 27 日

情報通信研究機構　欧州連携センター

目次

はじめに

情報通信研究機構（以下「当機構」という。）では、セキュリティ基盤研究室において、セキュリティ基盤技術に関する研究活動を行っており、同研究室からの提案である、未来志向型研究ファンド「パーソナルデータ利活用におけるプライバシー問題の解決に関する研究」が採択され、プライバシー保護技術と、行政、法律、倫理、社会学等、非技術的な側面との連携・融合に関して検討を進める予定である。

さて、伝統的に人権意識の高い欧州では、プライバシー保護に関して、世界の他の地域に先んじて活発に議論、検討されており、プライバシーを保護しつつ、ICT を実社会へ展開していくための研究が、欧州連合（EU）の大型研究開発助成プログラムである第七次枠組計画（FP7）、そして、各国内ですでに行われており、数多くの研究プロジェクトが実施されている。FP7 の PRIPARE プロジェクトと PARIS プロジェクトは「プライバシー・バイ・デザイン」という理念の実用化に向けた研究をそれぞれ実施している。これらのプロジェクトは、データ管理者によるプライバシー・バイ・デザインの採用に係る条項を含む、EU パーソナルデータ保護法改正案の審議と並行して、研究が進められており、両者のつながりが非常に深い。プライバシー強化技術（Privacy Enhancing Technology）の研究として、FP7 の ABC4TRUST プロジェクトは、インターネット上での認証技術を属性ベースの証明（ABC : Attribute-based Credentials）により改善すること、そして、FP7 の PRACTICE プロジェクトは、暗号技術によりクラウドシステムにおけるプライバシー保護を強化することを目的としている。欧州各国に目を向ければ、フランスでは、オレンジ（フランステレコム）が中心になり、NFC 技術向けの暗号研究を対象とする LYRICS プロジェクトが実施されている。また、ベルギーの SPION プロジェクトでは、SNS ユーザーのプライバシー・ニーズを満たす、技術的により安全でより透明な SNS のフレームワークを実現することを目的としている。今後、NICT が中心となって進めるプライバシー保護技術の研究開発の参考となるように、欧州における ICT とプライバシー保護に係る最近の問題や議論とともに、これらのプロジェクトについて精査する。

調査研究項目

1) 欧州におけるプライバシー保護技術に係る研究プロジェクト

- FP7 PRIPARE プロジェクト
- FP7 PARIS プロジェクト
- FP7 ABC4TRUST プロジェクト

・ FP7 PRACTICE プロジェクト
・ フランスの LYRICS プロジェクト
・ ベルギーの SPION プロジェクト

2) 欧州における ICT とプライバシー保護に関する問題と議論
・ 特に、EU パーソナルデータ保護指令の改正動向

調査方法

・ インターネットや公刊物を利用した調査（欧州の関連組織や報道記事等の公開情報の精査）
・ 関係者へのヒアリング調査（先方訪問あるいはテレビ会議、電話インタビュー）
・ 関連 ICT イベントの視察・情報収集

ヒアリング調査としては、仏トリアログ社、独ダルムシュタット工科大学、ベルギー・KU ルーヴァンを訪問し、直接研究活動について質問した。ICT イベントについては、ベルギーで開催された SPION ワークショップ、同じくベルギーで開催された ABC4TRUST サミットの視察、調査を行った。本報告書に、ヒアリングの議事録、イベントの視察報告等も収録した。

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

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

全体の要約

以下に、本報告書全体の要約を記す。より詳しい情報については本文をご覧いただきたい。

第一部では、欧州連合の第七次枠組計画（FP7）におけるプライバシー保護技術に係る研究プロジェクトについて、EU パーソナルデータ保護指令の改正動向とともに紹介する。

プライバシーと人権

欧州におけるプライバシー保護政策の特徴の一つは、プライバシーの権利が人権として定められていることである。欧州人権条約の第 8 条、そして、欧州連合基本権憲章の第 7 条と第 8 条は、それぞれプライバシーとパーソナルデータ保護に捧げられており、法的拘束力を持つ。だが、欧州評議会加盟国の全てが欧州人権条約を批准しているわけではない（英国など）。また、欧州評議会加盟国と EU 加盟国は、欧州人権条約と欧州連合基本権憲章を国内の法体系と伝統に従って、それぞれ異なる仕方で解釈し、国内法化しているので、国によって人権保護に対するアプローチが異なる。

EU パーソナルデータ保護指令とその改正動向

欧州では、一般にプライバシーが人権の一つとして考えられている一方で、データ保護に関する個別の EU 法として、1995 年 10 月に EU パーソナルデータ保護指令が成立し、その後、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枠組みを提供している。2012 年 1 月には、同指令を近代化する改正案が欧州委員会によって提案されており、欧州議会での審議の後、現在欧州連合理事会にて審議の最中である。同改正案においては、特に、データ管理者のデータ保護・バイ・デザイン原理の採用義務（第 23 条）、データ保護影響評価の実施義務（第 33 条）、プライバシー認証スキームの促進（第 39 条）等がプライバシー保護技術の研究開発に係る重要な改正ポイントである。なお改正案では、「プライバシー（privacy）」よりも狭い意味である「データ保護（data protection）」という言葉が使用され、プライバシー・バイ・デザインではなく、「データ保護・バイ・デザイン（data protection by design）」と表現されている。

現在、データ保護・バイ・デザインについては、データ保護・バイ・デザインを実現する技術の名称、すなわち、開示データの最小限化、偽名化等のプライバシー保護措置の名称を具体的に記した文章を法文（前文第 61 パラグラフ）に付け加えるか否かという点が欧州連合理事会において議論されている。また、改正案の第 39 条は、データ保護を認証（certificate）するメカニズム、また、データ保護シールとマークの設置を促しているが、プライバシー・バイ・デザインを実施して開発された製品の認証も含み、そのような製品には、データ保護シールやマークが付けられることなる。

FP7 におけるプライバシー・バイ・デザインの方法論に係る研究プロジェクト: PRIPARE と PARIS

欧州ではプライバシー保護法制度の近代化が進められている一方で、それに合わせる仕方で、FP7 においてプライバシー保護技術の研究開発が進められている。まず、プライバシー・バイ・デザインを実施する方法論に係る FP7 プロジェクトとして、PRIPARE プロジェクトと PARIS プロジェクトがある。前者はプライバシー・バイ・デザインの一般的な方法論の策定を目指しているのに対して、後者は監視システムへのプライバシー・バイ・デザイン原理の導入を目標としている。これら 2 つのプロジェクトには、技術開発者だけでなく、プライバシー保護法の専門家、法律家もプロジェクトに参加しており、学際的な研究を実施している。特に、ベルギーの KU ルーヴァンに設置された「ICRI/CIR」という情報社会における法律と知的財産権に関

する研究を実施している機関がこれら双方のプロジェクトに加わっている。

- PRIPARE プロジェクト: 研究期間: 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）
- PARIS プロジェクト: 2013 年 1 月～2015 年 12 月（36 ヶ月）/ 予算（EU 拠出分）: 477 万ユーロ（349 万ユーロ）

KU ルーヴァンの ICRI/CIR

KU ルーヴァン法学部に設置されている ICRI/CIR は、ICT に係る法研究（特に EU 法）に関しては、欧州で五本の指に入る研究組織である。ICRI/CIR は、研究機関、中小企業及び大企業、ベルギーの政府機関とプライバシー保護所管機関、欧州委員会、イタリアに設置された EU の共同研究センター（JRC）等に、ICT に関して法的観点から助言、勧告を行っている。同機関は、数多くの EU プロジェクトに参加しており、プロジェクトパートナーの企業や研究開発組織に法律の専門知識を供給している。

FP7 におけるプライバシー強化技術に係る研究プロジェクト: ABC4TRUST と PRACTICE

プライバシー強化技術（Privacy Enhancing Techonology : PET）に関する大型 FP7 プロジェクトとして、ABC4TRUST プロジェクトと PRACTICE プロジェクトがある。前者は、ユーザーがオンライン認証の際に認証者に開示する必要がある個人情報を最小限化する技術を開発している。オンライン認証時に開示が必要な個人情報を最小限化することは、プライバシー保護の原則の一つであり、EU パーソナルデータ保護指令改正案の第 23 条において、それを実現する措置を採用することがデータ管理者の義務として定められていると同時に、PRIPARE プロジェクトでも重要視されている。後者は暗号技術により、クラウドシステム全体のセキュリティを向上させることを目標としている。特に、クラウドプロバイダーにさえユーザーの個人情報を見えなくする技術を開発しており、従来の SLA によるプロバイダーとの契約によるデータ保護を超えるものである。

- ABC4TRUST プロジェクト: 2010 年 10 月～2015 年 2 月 / 全予算（EU 拠出分）: 1359 万ユーロ（885 万ユーロ）
- PRACTICE プロジェクト: 研究期間 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）

CASED と EC SPRIDE

欧州の金融、経済の中心地である独フランクフルト市に隣接するダルムシュタット市は、欧州随一の情報セキュリティ研究開発地域であり、CASED と EC SPRIDE という二つの組織が設立されている。ダルムシュタット工科大学、ダルムシュタット応用科学大学、フラウホーファー研究所 SIT（Secure Information Technology）は、2008 年に CASED（Center for Advanced Security Research Darmstadt）という情報セキュリティの研究開発に特化した研究機関を設立している。CASED は情報セキュリティの研究に関しては欧州で最大の研究組織（約 300 名の研究者）であり、情報セキュリティに関するあらゆる研究を実施している。また、ダルムシュタット工科大学とフラウホーファー研究所 SIT は、2011 年に EC SPRIDE（European Center for Security and Privacy by Design）という組織を共同で設立している。EC SPRIDE は、プライバシー及びセキュリティ・バイ・デザインの実用化を研究しており、ドイツ連邦教育・研究省から資金を供給されている。EC SPRIDE は CASED と緊密に連携して活動する。

第二部においては、フランスとベルギーにおける国内研究プロジェクト、SPION プロジェクトと LYRICS プロジェクトを紹介する。

SPION プロジェクト

SPION プロジェクトはソーシャルネットワークにおけるプライバシー保護について、技術的な観点からだけでなく、経済、法等の観点からも研究を行う学際的な研究である。同プロジェクトは、特に、ソーシャルネットワークのプロバイダーとステークホルダーの責任に焦点を当てることにより、プライバシーとセキュリティの懸念に対応する方法を研究する。また、同プロジェクトは、ベルギーのフラマン地域圏の研究開発助成機関である科学・技術革新庁（IWT : agency for Innovation by Science and Technology）から資金を供給されている。

LYRICS プロジェクト

LYRICS プロジェクトは、e チケット等の非接触型サービスを可能にする NFC 技術向けのプライバシー強化暗号を開発する。同プロジェクトは、新しい暗号ソリューションによって、NFC ユーザーが必要最小限のパーソナルデータを開示するだけで、各種サービスを利用できるようにすることを目的とする（データ最小限化原則の適用）。同プロジェクトは、フランスの国立研究機構（ANR）から助成されている。

General Summary

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

Part I : the R&D projects on privacy protection in the EU's Seventh Framework Program (FP7) and the Reform of EU personal data directive

Privacy protection and human rights

One of the characteristics of privacy protection policy in Europe is that the right to privacy is considered as a human right. Article 8 of the European Convention on Human Rights (ECHR), and article 7 and article 8 of the Charter of Fundamental Rights of the European Union, which both have binding force, concerns the right to privacy and personal data protection. However, there are two problems. Firstly, the member states of the Council of Europe don't all ratify ECHR (ex. The UK). Secondly, the member states of the Council of Europe and the member states of the European Union interpreted and transposed these articles into their national laws by their own way, namely, according to their law system and their tradition, so their approach to human rights are not same.

EU Personal data protection directive and its Reform

In May 1995, the EU Personal data protection directive was approved as a European law on personal data protection, and transposed into national laws by the EU member states. This directive is the most important law for personal data protection in Europe. In January 2012, the European Commission proposed the Proposal for the General Data Protection Regulation (the Proposal), which reforms the EU Personal data protection directive. This proposal is now being discussed in the Council of the European Union (minister council) after discussions in the European Parliament. Some articles of the Proposal are important for the R&D of privacy protection technologies, for example, Data protection by design and by default (article 23), Data protection impact assessment (ar. 33), Certification (ar. 39) etc. The term of " data protection by design" is used in the Proposal instead of the term of "privacy by design".

As for article 23 concerning Data protection by design and by default, European ministers are discussing whether a list of names of measures which meet the principles of data protection by design and by default (ex. Minimising the processing of personal data, pseudonymising personal data) must be added to the recital 61 of the Proposal or not.

According to article 39 concerning the establishment of data protection certification mechanisms and data protection seals and marks, products made in accordance with the principles of data protection by design will have data protection seals or marks.

The R&D projects on methodology for privacy by design in FP7 : PRIPARE and PARIS

While the legal system for privacy protection is modernized in Europe by the Reform of EU Personal data protection directive, the R&D of privacy protection technologies is carried in FP7 parallel to the Reform. Two FP7 projects, PRIPARE and PARIS, concern methodology for Privacy by design. The former aims to establish a general methodology for Privacy by design, the latter to introduce the principles of privacy by design into surveillance system. These two projects are interdisciplinary, because not only engineers, but also legal specialists from ICRI/CIR in KU Leuven participate into them.

- PRIPARE : Research period : October 2013 - September 2015 / Budget (EU contribution) : about 1.3 million euro (1.09 million euro)
- PARIS : Research period : January 2013 – December 2015 / Budget (EU contribution) : about 4.77 million euro (3.49 million euro)

ICRI/CIR in KU Leuven

ICRI/CIR, a research centre for ICT laws and Intellectual property rights founded in the Law department of KU Leuven, is very famous for legal expertise (in particular concerning EU laws) in Europe. This research centre gives advice and recommendations from legal point of view to many kinds of organizations, for example, research organizations, companies (Small, medium and big enterprises), Belgian government and privacy commission, the European Commission, a EU's Joint Research Centre (JRC) in Italy. And it participates into a lot of FP7 projects for giving legal expertise to its project partners.

The R&D projects on Privacy Enhancing Technologies in FP7 : ABC4TRUST and PRACTICE

ABC4TRUST and PRACTICE are large FP7 projects on Privacy Enhancing Technology (PET). The former aims to develop technologies for minimizing personal data to disclose during online user identification. Minimization of the process of personal data is a principle of privacy protection. The goal of the latter is to improve security of the whole cloud system. It develops a technology for preventing cloud providers from seeing client's data by cryptography, which goes beyond legal approach for privacy protection such as SLA (Service Level Agreement).

- ABC4TRUST : Research period : October 2010 – February 2015 / Budget (EU contribution) : about 13.59 million euro (8.85 million euro)
- PRACTICE : Research period : November 2013 – October 2016 / Budget (EU contribution) : about 10.46 million euro (7.55 million euro)

CASED and EC SPRIDE

Darmstadt is in the biggest industrial region for information security in Europe, because it is close to Frankfurt, which is an important city for finance and economy in Europe. Two research organizations, which work closely, are in Darmstadt : CASED（Center for Advanced Security Research Darmstadt) and EC SPRIDE（European Center for Security and Privacy by Design). Founded in 2008 by the Technical University of Darmstadt, Frauhhofer Institute SIT and the University of Applied Sciences in Darmstadt, CASED is the biggest research centre for information security in Europe (about 300 researchers), which studies every subject of information security. EC SPRIDE is a research centre for Privacy and Security by Design, founded by the Technical University of Darmstadt and Frauhhofer Institute SIT in 2011, and financed by the German Federal Ministry of Education and Research.

PART II : the R&D projects on privacy protection technologies in European countries : SPION and LYRICS

SPION

SPION is a Belgian project, which studies privacy protection in social networking service (SNS) not only from the technical point of view, but also from the legal and social point of view. It is an interdisciplinary project financed by IWT, Flemish agency for Innovation by Science and Technology. This project tackles the task of mitigating privacy and security concerns by focussing on the responsibilities of service providers and stakeholder organizations. And it also proposes different stakeholders more secure and transparent ways to develop SNS.

LYRICS

Financed by ANR, Agence Nationale de Recherche, LYRICS is a French project on Privacy Enhancing Technology (PET) for NFC and contactless technologies. It develops a Privacy Enhancing Cryptography (PEC) which enables contactless services for mobile phone, for example, e-ticket. The main goal is to design new innovative cryptographic solutions that achieve the fundamental privacy principles such as data minimization.

第一部　欧州連合の第七次枠組計画におけるプライバシー保護に係る研究プロジェクトの事例

第一章　欧州におけるプライバシー保護政策の概要と動向

プライバシー保護と人権

欧州におけるプライバシー保護政策の大きな特徴は、プライバシーの権利が人権の一つとして定められていることである。欧州評議会[1]が 1950 年に採択し、1953 年に発効した「欧州人権条約」の第 8 条はプライバシー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。また、EUが 2000 年に宣言し、リスボン条約の発効ともに法的拘束力を持った「欧州連合基本権憲章」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[2]。だが、欧州評議会加盟国の全てが欧州人権条約を批准しているわけではない（英国など）。また、欧州評議会加盟国とEU加盟国は、欧州人権条約と欧州連合基本権憲章を国内の法体系と伝統に従って、それぞれ異なる仕方で解釈し、国内法化しているので、国によって人権保護に対するアプローチが異なる。

EU パーソナルデータ保護指令

欧州では、一般にプライバシーがこのように人権の一つとして考えられている一方で、データ保護に関する個別の EU 法として、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 パーソナル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枠組みを提供している。その上、電子通信部門で処理されるパーソナルデータに関して、EU パーソナルデータ保護指令を補足する法律として、「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」がある。同法は、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。なお、同指令は 2002 年に成立し、2009 年に改正され、プライバシー保護が強化されている。

EU パーソナル保護指令の改正

さて、2012 年 1 月には、情報通信技術の進歩に対応できるよう、EU パーソナルデータ保護指令を近代化する改正案が欧州委員会によって提案されており、現在審議の最中である。同改正案においては、特に、データ保護・バイ・デザイン原理の採用（第 23 条）、データ保護影響評価の実施義務（第 33 条）、プライバシー認証スキームの促進（第 39 条）等がプライバシー保護技術の研究開発に係る改正ポイントである。特に、第 23 条では、処理される個人情報を最小限化する措置を、初期設定として取り入れることがデータ管理者の義務として定められている。

欧州におけるプライバシー保護制度の近代化と研究開発

以上のように、欧州ではプライバシー保護法制度の近代化が進められている一方で、それに合わせる仕方で、FP7 においてプライバシー保護技術の研究開発が進められている。まず、プライバシー・バイ・デザインを実施する方法論に係るFP7 プロジェクトとして、PRIPAREプロジェクトとPARISプロジェクトがある。前者はプライバシー・バイ・デザインの一般的な方法論の策定を目指しているのに対して、後者は監視システムへのプライバシー・バイ・デザイン

[1] 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。http://www.mofa.go.jp/mofaj/area/ce/

[2] http://www.europarl.europa.eu/comparl/libe/elsj/charter/default_fr.htm

原理の導入を目標としている。これら 2 つのプロジェクトには、技術開発者だけでなく、プライバシー保護法の専門家、法律家もプロジェクトに参加しており、学際的な研究を実施している。特に、ベルギーのKU ルーヴァンに設置されたICRI/CIR[3]という情報社会における法律と知的財産権に関する研究を実施している機関が、これら双方のプロジェクトに加わっている。ついで、プライバシー強化技術（Privacy Enhancing Technology : PET）に関する大型FP7 プロジェクト（全予算額が 1000 万ユーロ以上）として、ABC4TRUSTプロジェクトとPRACTICEプロジェクトがある。ABC4TRUSTプロジェクトは、ユーザーがオンライン認証の際に認証者に開示する必要がある個人情報を最小限化する技術を開発している。PRACTICEプロジェクトは暗号技術により、クラウドシステム全体のセキュリティを向上させることを目標としている。特に、クラウドプロバイダーにさえユーザーの個人情報を見えなくする技術を開発しており、これは、従来のSLAによるプロバイダーとの契約によるデータ保護とは異なる技術的アプローチである。

第二章　プライバシー・バイ・デザインの方法論に係る EU 研究プロジェクト

PRIPARE プロジェクトと PARIS プロジェクトは、プライバシー・バイ・デザインの方法論に係る研究プロジェクトであり、仏トリアログ社が双方のプロジェクトコーディネーターであり、また、KU ルーヴァンが双方の法律面の研究を実施している。特に、PRIPARE プロジェクトは EU パーソナルデータ保護指令の改正と結びつきが強い。

第一節　FP7 PRIPARE プロジェクト

A) FP7 PRIPARE プロジェクトの概要

- PRIPARE プロジェクトは、プライバシー・バイ・デザインの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ことを目標とする。同プロジェクトは、1）プライバシー及びセキュリティ・バイ・デザインの方法論と実践、2）研究開発者向けのトレーニング、3）教材、4）欧州委員会等への勧告という 4 つの活動内容を持つ。その上、同プロジェクトは、プライバシー保護の参照モデルに関する標準化に寄与している。
- PRIPARE プロジェクトは、研究開発そのものというよりは、研究開発組織間のコーディネーションを支援する FP7 の「サポートアクション」という枠組みで助成されているが、単なるコーディネート以上に、プライバシー・バイ・デザインに係る方法論も策定してしようとしている。
- PRIPARE プロジェクトは、既存のプライバシー保護に係る実践（プライバシー影響評価など）を融合させ、全てのステークホルダーを考慮する包括的な方法論の策定を目指す。特に、プライバシー・バイ・デザインについて工学的観点からアプローチする OASIS の「PMRM（Privacy Management Reference Model）」が、PRIPARE プロジェクトの出発地点にある。また逆に、同プロジェクトは、PMRM を改善するために、OASIS に研究成果のフィードバックを行う。
- プライバシーとセキュリティを同じ一つの方法論に取り入れて、組み合わせて考えることが、PRIPARE プロジェクトの特徴の一つである。

[3] http://www.law.kuleuven.be/icri/en/about

- PRIPAREプロジェクトが策定する方法論は、研究開発の 7 つの段階に分け、その段階毎に異なる方法を導入していく。これらの方法は、同プロジェクトの成果物であるマニュアル（D1.2 Privacy and Security-by-Design Methodology）[4]において、詳しく説明されている。
- EU パーソナルデータ保護法の改正案に、プライバシー・バイ・デザイン（「データ保護・バイ・デザイン」）の採用に係る条項（第 23 条項）があるが、PRIPARE プロジェクトは、この改正案がなかったならば、助成されていなかっただろうと考えられている（PRIPARE プロジェクトコーディネーターのアントニオ・クン氏の見解）。
- PRIPARE プロジェクトの助言者には、プライバシー・バイ・デザイン原則を考案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・カブキアン氏がいる。

B) PRIPARE プロジェクトの基本情報

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）、KU ルーヴァン（ベルギー）、マドリッド工科大学（スペイン）、ウルム大学（独）、パリ・アメリカ大学（仏）、トリラテラル リサーチ&コンサルティング（英）、ガリシア電気通信技術センター（スペイン）、アトス（スペイン）
ウェブサイト	http://pripareproject.eu http://cordis.europa.eu/project/rcn/110590_en.html

C）KU ルーヴァンの ICRI/CIR の活動

- KU ルーヴァン法学部に設置されている ICRI/CIR は、ICT に係る法研究（特に EU 法）に関しては欧州で五本の指に入る研究組織である。
- ICRI/CIR の主な活動は、技術の急激な進歩を考慮して、様々な分野（政府、メディア、著作権、医薬、銀行、交通等）の現行の法枠組みを再考することであり、特に ICT に関しては、プライバシーを含め、メディア、電子署名、E ヘルス、コンテンツ、知的財産権、オープンデータ等に係る法的側面について研究している。
- ICRI/CIRは、研究機関、中小企業及び大企業、ベルギーの政府機関とプライバシー保護所管機関、欧州委員会、イタリアに設置されたEUの共同研究センター（JRC）[5]等に、ICT

[4] PRIPARE が作成したプライバシー・バイ・デザインの方法論のマニュアルは、同プロジェクトのウェブサイトで取得できる。http://pripareproject.eu/research/
D1.2 Privacy and Security-by-Design Methodology (Draft – Jan'15).

[5] https://ec.europa.eu/jrc/en/about/ipsc
：イタリアの JRC は欧州委員会に市民の保護とセキュリティの問題に関して助言している。

に関して法的観点から助言、勧告を行っている。同組織は、数多くのEUプロジェクトに参加しており、プロジェクトパートナーの企業や研究開発組織に助言を与えている。

PRIPARE プロジェクトについて、より詳細な情報を収集するために、同プロジェクトのコーディネーターである仏トリアログ社とベルギー・KU ルーヴァンの ICRI/CIR で研究者にヒアリング調査を実施し、次節に記す FP7 PARIS プロジェクト、そして、EU パーソナルデータ保護指令改正動向についてとともに質問した。以下に、その議事録を収録する。

ヒアリング議事録 / トリアログ社（フランス）

日程：2015 年 2 月 6 日（金）午後 2 時 30 分～午後 4 時

場所：先方事務所（フランス・パリ）

先方：

トリアログ社[6]：アントニオ・クン氏（FP7 PRIPAREプロジェクト及びFP7 PARISプロジェクトのコーディネーター）

当方：

NICT 欧州連携センター長：岡本 成男

ONOSO 研究員：小野 浩太郎

ヒアリングの概要

トリアログ社の概要

- 従業員数は 25 名である。
- 先方のクン氏は、特に組み込みシステム等に係る専門的知識の供給と研究を担当している（モノのインターネット、特にスマートグリッド、スマートホーム、スマートカー等のセキュリティとプライバシー保護を対象）。
- トリアログ社では研究開発も行っているが、企業支援の事業の割合のほうが多い（研究開発が事業の 3 分の 1 で、企業支援が残り）。研究開発と言っても、製品を開発することはほとんどない。
- 研究パートナー国は一般に欧州国である。非欧州諸国の研究パートナー国はアメリカとカナダであるが、非常に珍しい。アジア諸国には今のところパートナーはいない。日本に関心がある。
- クン氏がプライバシー・バイ・デザインについて知ったのは 2007 年ごろで、本格的に研究に取り組み始めたのは 2010 年ごろである。
- トリアログ社は、プライバシー保護技術については、EUの第六次枠組計画（FP6：2002 年～2006 年）よりEUプロジェクトに参加し始めた。車両間のデータ通信やITSに係るプライバシー保護技術のプロジェクトであるFP6 のSEVECOMプロジェクト[7]、FP7 のPRECIOSAプロジェクト[8]のコーディネーターを努めた。また、現行のプライバシー保護技術に関連

[6] http://www.trialog.com/home/
[7] http://cordis.europa.eu/project/rcn/80592_fr.html
[8] http://www.preciosa-project.org/home

するプロジェクトとしては、FP7のPRIPAREプロジェクトとPARISプロジェクト、そして、PRESERVEプロジェクト[9]に参加している。

- FP6のSEVECOMプロジェクトでは、自動車事故が発生したさいに手動あるいは自動で救急隊等へ連絡するシステムを開発したが、その際に、車両の地理情報の保護が問題となった。同プロジェクトでは、その地理情報を疑似化し、そして、それを一定の時間で常に変化させる技術により、この問題を解消した。
- クン氏によれば、プライバシー・バイ・デザインは近い将来必ず必要とされるようになり、その際トリアログ社が行っている研究は有用である。フランスでは、例えば、電力のスマートメーター開発への適用が考えられる。

プライバシー・バイ・デザインとプライバシー影響評価について

- プライバシー・バイ・デザインとプライバシー影響評価（Privacy Impact Assessment : PIA）は前者がゴール指向であるのに対し、後者はリスク指向であるという点で異なる。後者は、研究開発者に開発物にリスクがないか、適正であるか評価することを求めるのに対して、前者は、プライバシー保護を含む一定のゴールに到達するために、プライバシー保護に必要な原則（プライバシー・バイ・デザイン原則）を研究開発の設計段階で取り込むことによって実施される。だが、両者は相互に補完し合い、互いに必要不可欠である。
- PIAの問題は、マネージャー等はPIAに通じているが、実際に研究開発を行っている者はPIAについて全く知らないことが多いことである。

プライバシー保護方法論の現状

- フランスのプライバシー保護所管機関CNILは、2012年に『プライバシーリスク管理方法論』[10]という文書を発表しており、これがリスク管理の方法について説明する現在ほとんど唯一の文書である。この文書は非常に優れているが、プライバシー保護ではなく、セキュリティの問題を主眼においていることが欠点である。
- CNILには多くのエンジニアがおり、欧州でも最も強力なプライバシー保護所管機関である。
- CNILはプライバシー・バイ・デザインの採用を押し進めている。
- 標準化団体であるOASISは、「PMRM（Privacy Management Reference Model）」というプライバシー保護の参照モデルに係る文書を発表しており、非常に優れた文書である[11]。
- プライバシー・バイ・デザインを実施する方法論の開発には、関係者のプライバシー・バイ・デザイン原則への同意、プライバシー・バイ・デザイン原則の設計段階での取り入れ、標準化作業への影響を考慮する必要がある。
- 現在、政策立案者や研究開発者に対するプライバシー・バイ・デザインのトレーニングが必要である。

FP7 PRIPAREプロジェクトの概要

- PRIPAREプロジェクトは、研究開発そのものというよりは、研究開発組織間のコーディネーションを支援するFP7の「サポートアクション」という枠組みで助成されており、組織間のコーディネートを行っていて、予算はそれほど多くない。だが、このプロジェクト

[9] http://www.preserve-project.eu/about
[10] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
[11] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm

は単なるコーディネート以上に、プライバシー・バイ・デザインに係る方法論も策定してしようとしている。

- 現在、プロジェクトは研究期間のちょうど折り返し地点にいる。
- 2012年1月に欧州委員会は現行のEUパーソナルデータ保護法の改正案を提出しているが、そこにはプライバシー・バイ・デザインの採用に係る条項（第23条：データ管理者のデータ保護・バイ・デザインの採用義務）がある。PRIPAREプロジェクトは、この改正案がなかったならば、助成されていなかっただろう。
- PRIPAREプロジェクトは、1）プライバシー及びセキュリティ・バイ・デザインの方法論と実践（仏アトス社の担当）、2）研究開発者向けのトレーニング（独ユルム大学が担当）、3）教材（パリ・アメリカン大学が担当）、4）欧州委員会等への勧告（スペイン・Gradiantが担当）という4つの活動内容を持つ。トリアログ社はプロジェクト全体のコーディネートを行うとともに、プライバシー強化アーキテクチャについて研究している（クン氏の関心）。

1) 方法論

- PRIPAREプロジェクトではプライバシー保護の方法論を策定しており、現在、その第1稿（約150ページ上のハンドブック）がプロジェクトのウェブサイト上で発表されている。第2稿は今年末に発表される予定である[12]。このハンドブックがPRIPAREプロジェクトの方法論に関する主な成果となる。第2稿は論文風に書き、第1稿よりも読みやすくする予定である。
- PRIPAREが開発するプライバシー及びセキュリティ・バイ・デザインの方法は、「プライバシー及びセキュリティ・バイ・デザイン」原則を研究開発の設計段階から取り入れるため、7つの段階からなる一連のプロセス毎に導入される。研究開発者はこの方法を遵守しなければならない。ハンドブックでは、これらの段階に属する各方法内容について詳しく説明されており、研究開発者に参照モデルを提供する。

PRIPAREプロジェクトが開発した7つのプロセスからなる方法論

第一段階　分析：事前活動、機能記述と高レベルプライバシー分析、プライバシー要件の操作、詳細なプライバシー分析、リスク管理、法の遵守
第二段階　設計：トップダウン・アーキテクチャ設計、ボトムアップ・アーキテクチャ設計、プライバシー強化アーキテクチャ設計、プライバシー強化の詳細設計、ユーザー中心のユーザーインターフェイス設計
第三段階　統合：プライバシー統合
第四段階　検証：セキュリティ及びプライバシーの動的分析、セキュリティ及びプライバシーの静的分析、説明責任
第五段階　リリース：事故対応計画の作成、システム解体計画の作成、最終セキュリティ及びプライバシー検討、PIAレポートの発表
第六段階　メンテナンス：事故対応計画の実行、セキュリティ及びプライバシーの検証
第七段階　解体：解体計画の実行

- この方法論は非常に一般的であり、PRIPAREプロジェクトにおいては、具体的なテストケース（モバイル通信網、M2Mなど）を検討しているわけではない。だが、PRIPAREプロ

[12] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.2_draft.pdf

ジェクトは、「プライバシーパターンEU」[13]というプライバシー保護のユーズケースを収集し、それについてオンラインで議論し、また再利用できる場を設けている。このウェブサイトには誰でも貢献できる。

- クン氏は特にプライバシー強化アーキテクチャ方法論を研究している。プライバシーのためのアーキテクチャ特性は4つある。データ開示の最小限化（minimization）、施行（enforcement）、説明責任（accountability）、更新性（modifiability）である。
    - ✧ 最小限化は、将来的に最も期待されているアプローチ（匿名化など）であるが、採用されていくペースについてははっきりしない。ABC4TRUSTプロジェクトで開発されている、個人情報の開示を最小限化する技術は、プライバシー強化技術（PET）の一つである。
    - ✧ 施行は、組織的な措置で、組織内のデータ保護策を強化することであるが、実際には現在配慮されていない。
    - ✧ 説明責任は、データアクセスの記録などに関する説明の責任に係るが、実際には現在配慮されていない。
    - ✧ 更新性は、既存のシステムやインフラストラクチャを変更する際に、政策や暗号の強度を柔軟に更新する必要があるが、現在研究レベルで配慮されていない。

2) トレーニング

- 2015年3月9日と10日に、PRIPAREプロジェクトはトレーニングワークショップを開催する予定である[14]。PRIPAREプロジェクトが開発したプライバシー・バイ・デザインに係る方法論を参加者に紹介し、感想等を聞く予定である。このワークショップには誰でも参加できるので、日本の研究者にもぜひ参加していただきたい。

3) 教材

- PRIPAREプロジェクトでは、まだ公開できる段階ではないが、リスク管理に関する教材を制作している。子供、学生、政策立案者、研究開発者向けなど様々なレベルに対応できるように、複数の教材をつくっている。子供向けの教材にはマンガ風のデッサンが使用される。PRIPAREプロジェクトでは、パリ・アメリカン大学のクローディア・ロダ氏[15]が教材の作成のコーディネートを担当している。

4) 勧告

- 欧州連合ネットワーク・情報セキュリティ庁（ENISA）に設置されたNISプラットフォーム[16]は、サイバーセキュリティの適切な実践を特定するための官民のフォーラムである。同プラットフォームは3つの作業部会（WG）を持つが、第3作業部会（WG3）が「安全なICT研究と技術革新」をテーマとしている。PRIPAREプロジェクトはこの作業部会の議論に寄与している。

[13] https://privacypatterns.eu/#/?limit=6&offset=0
[14] http://pripareproject.eu/events/privacy-training-workshop-3/
[15] https://www.aup.edu/profile/croda
[16] https://resilience.enisa.europa.eu/nis-platform

- ENISAは2014年12月に、『プライバシー・データ保護・バイ・デザイン』という文書を発表している[17]。この文書では、法的枠組みと技術的実施措置のギャップを満たすために、現存するアプローチやプライバシー・バイ・デザインの戦略等について説明紹介している。PRIPAREプロジェクト参加者のひとりがこの文書に寄与している。
- 2015年3月の欧州議会における会議向けに、PRIPAREプロジェクト参加者であるカルメラ・トロコンコソ氏と、クン氏がそれぞれ『Adoption of PETs : Pitfalls and Solutions』、『Measure to Ingrain Prvacy : Values in Business and Society』という二つの文書を提出している。これらの文書では、教習及び教育、工学、管理という3種類の問題とそれらに対する措置について考察している。
    - ✧ 教習及び教育に関しては、プライバシー保護に関する教育をユーザーレベル、技術者レベル、マネージャーと政策立案者レベルに分けて、教育及びトレーニングを実施する必要がある。
    - ✧ 工学に関しては、PIAステークホルダーと研究開発者の間にある文化的ギャップ、PIAとプライバシー・バイ・デザインの間にあるギャップ、プライバシー・バイ・デザインと現在の実践の間にあるギャップ、研究と実践の間にあるギャップを特定している。

- 以上の4つの活動の他、プロジェクトの普及活動として、プライバシー保護に係る標準化作業へ貢献している。
    - プライバシー保護に係る標準化作業の現状
        - ✧ OASISのPMRMはすでに発表されている。
        - ✧ OASISのプライバシー・バイ・デザインに係る文書は現在策定中である。
        - ✧ プライバシー影響評価に係るISO/29134は現在策定中である。
        - ✧ 個人を特定可能な情報保護（Personal Indentifiable Information : PII）向けの実践規範に係るISO/29151は現在策定中である。
    - 問題は上記4つの標準は相互に調整されていないことである。クン氏は現在その調整に回っているが、同氏はこれら4つの調整は相互補完的だと考えている。
    - PRIPAREプロジェクト参加者は、2015年3月から開始される予定の欧州の電子工学系標準化団体であるCEN-CENLECのJWG8に参加する予定である。現在欧州は、より包括的で、欧州の状況（例：説明責任は欧州ではとても重要であるが、アメリカでは欧州ほどではない）と研究開発及び技術革新に適応した標準を必要としている。なお、クン氏によれば、国や地域毎に標準に対する要求は異なるが、原則的な部分では違いはない。すでに内部でのミーティングは始まっているものの、JWG8についての詳しい情報はまだ公表されていない。

FP7 PARISプロジェクト

- PARISプロジェクトでは、監視システムによる治安の向上と、それによるプライバシー侵害の齟齬の問題を研究する。法律の専門家と共同して、プロジェクトを進めており、同プロジェクトは学際的な研究である。
- PARISプロジェクトでは、SALT（Socio-contextual, ethicAl, Techonology Legal）フレームワークという、監視システムのプライバシー保護を強化する方法を開発している。SALTフレームワークは、研究開発の際の参照モデルとなり、監視システムの設計段階で研究開発者が採用することができる。

[17] https://resilience.enisa.europa.eu/nis-platform

- SALT フレームワークは、法律の専門家が各国の法律に基づいて作成する。同フレームワークは質問票のかたちを取り、それを研究開発者が開発のさいに利用する。
- PARIS プロジェクト内では、PRIPARE プロジェクトが用意する方法を利用する予定である。
- テストケースとしては、指紋等の生物計測システムと監視カメラシステムが考えられている。
- PRIPARE プロジェクトのほうが、PARIS プロジェクトよりも成熟している。

ヒアリング議事録 / KU ルーヴァン（ベルギー）

日程 : 2015 年 2 月 24 日（火）午後 2 時～3 時半

場所 : 先方事務所（ベルギー・ルーヴァン）

先方 :

KUルーヴァン・ICRI/CIR[18] 研究者 3 名
: ファニー・クーデル氏、パゴナ・ツォルマパツージ氏、エルス・キンド氏

当方 :

ONOSO 研究員　小野 浩太郎

ヒアリングの概要

KU ルーヴァン・ICRI/CIR について

- CRI/CIR は、KU ルーヴァンの法学部に ICRI（Interdisciplinary Centre for Law and ICT）と CIR（Centre of Intellectual Property Right）が合併することにより設立された。前身組織の ICRI は 1990 年にデュモルチエ教授により設立され、ICT に係る法研究に関しては欧州で五本の指に入る研究組織である（CIR の設立は 1988 年）。1995 年に成立した EU パーソナルデータ保護指令の法案の審議が開始されたのが 1990 年ごろであり、同時期に ICRI は設立された。
- ICRI/CR の人員は 40 名ほどである。博士課程の学生が 30 名、ポストドクター5 名、教授 4 名、研究マネージャー1 名、プロジェクトマネージャー1 名である。（その他、事務 4 名）。
- ICRI/CIRは、ルーヴァンICTセンターとiMinds[19]のメンバーであり、ベルギーのサイバー犯罪・トレーニング・研究・教育エクセレンスセンター[20]のコーディネーターもしていたことがある。
- ICRI/CIR の主な活動は、技術の急激な進歩を考慮して、様々な分野（政府、メディア、著作権、医薬、銀行、交通等）の現行の法枠組みを再考することである。ICT に関しては特に、プライバシーを含め、メディア、電子署名、E ヘルス、コンテンツ、知的財産権、オープンデータ等に係る法的側面について研究している。

[18] https://www.law.kuleuven.be/icri/en
[19] www.iminds.be
iMind はベルギーのフランドル圏の ICT 研究機関の集合体である。
[20] www.b-ccentre.be

- ICRI/CIRは、研究機関、中小企業及び大企業、ベルギーの政府機関とプライバシー保護所管機関、欧州委員会、イタリアに設置されたEUの共同研究センター（JRC）[21]等に、ICTに関して法的観点から助言、勧告を行っている。
- ICRI/CIRは、数多くの国際的また学際的なプロジェクトに参加し、研究パートナーにデータプライバシー、情報セキュリティ法、新しいメディアと通信法、情報権利管理、そして、知的財産権に関して専門知識を供給している。ICRI/CIRは欧州第5次枠組計画から参加しており、第6次枠組計画、第7次枠組計画、ホライズン2020に参加している[22]。
- フェイスブックのデータユーザーポリシーに関して、ICRI/CIRはベルギーのプライバシー保護所管機関を支援しており、2014年12月にはフェイスブックはデータユーザーポリシーを修正することを発表している[23]。

プライバシー保護と人権の関係について

- 欧州のプライバシー保護政策の最大の特徴の一つは、プライバシー保護に係る権利が人権として定められていることである。アメリカはプライバシー保護について別のアプローチを採用している。
- 欧州人権条約の第8条、そして欧州連合基本権憲章の第7条と第8条は、それぞれプライバシーとパーソナルデータ保護に捧げられており、法的拘束力を持つ。フランスのアルザスにある欧州人権裁判所とルクセンブルグの欧州連合裁判所[24]が、それぞれこれらの法に基づいて裁判を行う。
- 欧州評議会加盟国の全てが欧州人権条約を批准しているわけではない（英国など）。また、加盟国が国内の法体系と伝統に従って、欧州人権条約の条項をそれぞれ異なる仕方で解釈し、国内法化している。従って、国によって、人権保護に対するアプローチが異なる。
- 欧州連合基本権憲章は、2009年のリスボン条約の発効以来、EU加盟国に対して法的拘束力を持つが、欧州人権条約の場合と同じく、加盟国はそれぞれ国内の法体系と伝統に従って、法を解釈し、国内法化している。
- EUパーソナルデータ保護指令に定められ、国内法化された義務が遵守されているかどうかは、欧州委員会と国際法廷の他に、各国内のパーソナルデータ保護所管機関（例えば、フランスではCNIL）が監視し、検証している。

PRIPAREプロジェクトについて

- 欧州では、プライバシー・バイ・デザインについて、1990年代からすでにオランダのプライバシー保護所管機関が検討してきた。プライバシー・バイ・デザイン原則は、カナダ・オンタリオ州情報プライバシー・コミッショナーのアン・カブキアン氏[25]により議論され、議事事項として挙げられてきており、現在、自律的なコンセプトとして法枠組みに取り入れることが可能なほど成熟している。同時に、プライバシー・バイ・デザインは工学系の研究開発者のあいだでも開発されてきた。PRIPAREプロジェクトは、プライバシー・バイ・デザインに係る条項を含む、2012年1月に提案された現行のEUパーソナルデータ保護指令の改正と強く結びついている。

---

[21] https://ec.europa.eu/jrc/en/about/ipsc
：イタリアのJRCは欧州委員会に市民の保護とセキュリティの問題に関して助言している。
[22] 同議事録末に、ICRI/CIRが参加する研究プロジェクトについて記した。
[23] http://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation
[24] http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm
[25] カブキアン氏は7つのプライバシー・バイ・デザイン原則を提唱した。

- PRIPARE プロジェクトにおける ICRI/CIR の役割は、1）法的観点からプロジェクトの支援、2）プライバシー・バイ・デザインという概念の研究、3）プライバシー・バイ・デザインに係る教材の制作及び講義を行うことである。
  1）プライバシー保護に係る法律が正しく方法論に取り入られるように、PRIPAREプロジェクトの方法論に関するマニュアル[26]の作成に法的観点から寄与している。マニュアルは現在すでに第 1 稿が公表されており、2015 年末に第 2 校が発表される。
  2）プライバシー・バイ・デザインという概念の発展を研究し、この概念が EU 政策に取り入れられるように勧告を行う。
  3）a)法律家及び政策立案者向けにプライバシー・バイ・デザインに係る教材の制作及び講義を行っている。KUルーヴァン・ブリュッセルの夜間コースで講義を行っており、生徒は 80 名程いる（生徒の半数はベルギー人であるが、もう半分は外国人）。b) 研究開発者向けに教材の制作及び講義を行っている。KUルーヴァンの人工知能をテーマとする修士課程において、研究開発者向けにビッグデータのプライバシーに係る側面について授業を行っている[27]。また、2015 年 3 月に開催する予定のPRIPAREプロジェクトのワークショップに参加する予定である（パゴナ・ツォルマパツージ氏が参加予定）。ワークショップでは、プライバシー・バイ・デザインやプライバシー影響評価の説明をした後、実践的演習を行う。演習の際には、ICRI/CIRが作成した演習問題教材を利用し、参加者はその問題に答えながら、プライバシー保護について学ぶ。同ワークショップでは、ユーザーケースとして、FP7 のABC4TRUSTプロジェクトのパイロットテストを利用する[28]。

プライバシー・バイ・デザインと EU パーソナルデータ保護指令改正案について

- ［法案の審議過程］：2012 年 1 月に欧州委員会により提案された後、EUパーソナルデータ保護指令改正案は欧州議会で審議され、ついで、現在は欧州連合理事会（閣僚理事会）[29]で審議されている。後者で合意に至れば、欧州議会で再び審議される予定である。同法案は、審議が開始されてすでに 3 年が経つが、現行のEUパーソナルデータ保護法の成立には 5 年を要したことを考えれば、特別なことではない。政治家は 2015 年末の成立を目指しているが、2016 年になるもつれ込む可能性も高い。なお、この改正法案については、これまでのどの法案よりも、欧州議会等への米企業及び欧州企業のロビー活動が激しい。ロビー活動家は法案を修正し、法規定を緩和させようとしている。キンド氏の意見では、審議が長引いているのは法案に多くの修正があるからである。だが、原案の基本的な部分は維持されている。
- ［データ管理者の説明責任］：改正案の第 22 条「管理者の責任（Responsability of controller）」は、データ管理者の説明責任に係る規定を義務づけている（第 28 条 データ処理の全記録を保存する義務、第 30 条 一定のセキュリティレベルを確保する技術的、組織的措置を採用する義務、第 33 条 データ保護影響評価を実施する義務等）。
- ［プライバシー・バイ・デザインの導入］：EUパーソナルデータ保護指令改正案の前文の第 61 パラグラフと第 23 条は、データ管理者がプライバシー・バイ・デザイン原則を実現する措置を取り入れる義務に係る。なお改正案では、「プライバシー（privacy）」よりも狭い意味である「データ保護（data protection）」という言葉が使用され、「データ保護・バイ・デザイン（data protection by design）」と表現されている。現在、データ保護・バイ・デザ

[26] http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.2_draft.pdf
[27] http://www.mai.kuleuven.be/index.html
[28] ABC4TRUST プロジェクトでは、オンライン講義評価アプリケーションのパイロットテストを実施している。
[29] 欧州連合理事会は、各国の閣僚が審議するので閣僚理事会 とも呼ばれている。

インについては、データ保護・バイ・デザインを実現する技術的措置の名称、すなわち、開示データの最小限化、偽名化、匿名化等のプライバシー保護措置の名称を具体的に記した文章を法文（前文第 61 パラグラフ）に付け加えるか否かという点が欧州連合理事会において議論されている[30]。

- ［データ保護認証制度］：改正案の第 39 条は、データ保護を認証（certificate）するメカニズム、また、データ保護シールとマークの設置を促しているが、プライバシー・バイ・デザインを実施して開発された製品の認証も含み、そのような製品には、データ保護シールやマークが付けられることなる。プライバシー保護に係る認証システムに関しては、欧州ではすでに各国のプライバシー保護所管機関（ドイツやフランス）により主導して実践されており、第 39 条はこれらの実践に基づく。特に、EuroPrise[31]という欧州プライバシーシール制度は、プライバシー・バイ・デザインによってプライバシー保護を強化する情報技術の認証している。なお、審議の結果、改正案の原案の第 39 条は修正され、現段階ではより詳細に法文が書かれている。

FP7 PARIS プロジェクトについて

- FP7 PARIS プロジェクトにおける ICRI/CIR の役割は、監視システムの開発における説明責任を研究し、生物計測アプリケーションを開発する際にガイドとなるプライバシー保護に係る質問事項を制作している。

ICRI/CIR が参加する他のプロジェクトのリスト

- FP7 のBEAT（Biometrics Evaluation and Testing）[32]：生物計測技術向けの評価の枠組みを提案
- FP7 のEKSISTENZ[33]：ID盗難の問題に対応するツールや手順の研究
- FP7 のMUSES[34]：ユーザーの行動により引き起こされるリスクを減少させ、組織のセキュリティを強化
- FP7 のeVACUATE[35]：避難経路を決定するシステムの包括的な研究
- FP7 のC4E[36]：欧州のためのクラウドシステムの開発
- FP7 のFIDELITY[37]：eパスポートの研究
- ベルギー国内プロジェクトのSPION[38]：ソーシャルネットワークにおけるプライバシー保護の研究
- FP7 のFuture ID[39]：包括的なID管理システムの研究
- FP7 のFASTPASS[40]：自動国境コントロールの研究
- CIP[41]のACDC[42]：最先端サイバー防御センター

---

30 http://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf
2014 年 12 月 19 日に発表された欧州連合国理事会の文書の前文 61 パラグラフを参考。
31 https://www.european-privacy-seal.eu/EPS-en/Home
32 https://www.beat-eu.org
33 http://eksistenz.eu
34 https://www.musesproject.eu
35 http://www.evacuate.eu
36 http://www.cloudforeurope.eu
37 http://www.fidelity-project.eu
38 http://www.spion.me
39 http://www.futureid.eu
40 https://www.fastpass-project.eu
41 CIP は EU の中小企業向けの研究開発助成スキームである。
42 http://www.acdc-project.eu/?page_id=48

・ ホライゾン 2020 のWITDOM[43]：クラウド内のセンシティブデータの保存に係るセキュリティ研究

第二節　FP7 PARIS プロジェクト

A) PARIS プロジェクトの概要

・ PARIS プロジェクトは、プライバシー等の市民の権利を強化する監視インフラ開発向けの方法論的アプローチを研究する。以上のため、監視とプライバシー保護のバランスを取る理論的枠組みと、プライバシーと説明責任を考慮に入れた監視システムのデザインの研究を実施する。
・ PARIS プロジェクトでは、SALT（Socio-contextual, ethicAl, Techonology Legal）フレームワークという、監視システムのプライバシー保護を強化する方法を開発している。SALT フレームワークは、研究開発の際の参照モデルとなり、監視システムの設計段階で研究開発者が採用することができる。
・ SALT フレームワークは、法律の専門家が各国の法律に基づいて作成する。同フレームワークは質問票のかたちを取り、それを研究開発者が開発のさいに利用する。
・ テストケースとしては、指紋等の生物計測システムと監視カメラシステムが考えられている。

B) PARIS プロジェクトの基本情報

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

第三章　プライバシー強化技術（PET）に係る EU 研究プロジェクト

本章では、FP7 におけるプライバシー強化技術に係る 2 つの研究プロジェクト、ABC4TRUST プロジェクトと PRACTICE プロジェクトを紹介する。双方とも、全予算額が 1000 万ユーロを超える大型 EU プロジェクトであり、研究成果の将来的な実用化が期待される。また、これらのプロジェクトのコーディネーター（ABC4TRUST プロジェクト：フランクフルト・ゲーテ大学と PRACTICE プロジェクト：ダルムシュタット工科大学）はそれぞれ、ドイツのフランクフルト市とその隣のダルムシュタット市にあり、共にヘッセン州に属する。ドイツの経済と金融

[43] http://www.witdom.eu

の中心地であるフランクフルト近郊では、銀行、そして、大企業が集まっており、研究開発も盛んである。特にダルムシュタット市では、ダルムシュタット工科大学、フラウホーファー研究所 SIT、ダルムシュタット応用科学大学が一緒に、CASED という情報セキュリティに特化した大型研究開発組織を設立しており、同市は情報セキュリティに関しては欧州最大の研究開発拠点である。また、ダルムシュタット工科大学とフラウホーファー研究所 SIT は共同で、ドイツ連邦政府の支援の下、プライバシー・バイ・デザインの研究を行う EU SPRIDE という組織も設立している。

第一節　FP7 ABC4TRUST プロジェクト

A) ABC4TRUST プロジェクトの概要

- ABC4TRUST プロジェクトが解消しようとする問題
  - インターネット上での ID 認証の際に、ユーザーは認証に実際には必要のない個人情報も認証者に渡していることがあり、プライバシー侵害の危険がある。
- 属性ベース認証技術（Attribute-based Credentials : ABC）
  - 属性ベース認証技術（ABC）は、ユーザーの一定の属性のみ（年齢や性別など）を開示することによって、ユーザーが認証に必要のない個人情報を認証者に与えなくて済むようにすることを可能にする。
- ABC4TRUST プロジェクトの目標とパイロット試験
  - 様々な ABC 技術に共通するアーキテクチャを定義し、それらの相互運用性を実現し、連合させて、プライバシーABC システム（属性ベース認証を利用して、プライバシーを保護するシステム）を開発することを目標とする。これにより、ユーザーは同じハードウェア、ソフトウェアで複数の ABC 技術を利用できる。より具体的には、ユーザーが端末に装備されたブラウザで利用できるアプリケーションを開発する。
  - プライバシーABC システムのパイロット試験をギリシアのパトラス大学（オンライン講義評価システム）とスウェーデンのソーデルハムン市の高校（学校関係者のソーシャルネットワーク）で実施した。
- プロジェクトの成果
  - ABC4TRUSTプロジェクトは『Attribute-based Credentials for Trust』という本を出版している[44]。

B) ABC4TRUST プロジェクトの基本情報

プロジェクト略称	ABC4TRUST
正式名称	信頼のための属性ベース認証
研究期間	2010 年 10 月～2015 年 2 月
研究予算（EU 拠出分）	1359 万ユーロ（885 万ユーロ）
コーディネーター	フランクフルト・ゲーテ大学（独）
参加組織	ダルムシュタット大学（独）、IBM リサーチ（スイス）、ULD（独）、マイクロソフト（ベルギー）、ミラクル（デンマーク）、ノキア・ソリューションズ・ネットワーク（フィンランド）、CryptoExperts（仏）、Eurodocs（スウェーデン）、CTIO（ギリシア）、アレクサン

[44] http://www.springer.com/business+%26+management/business+information+systems/book/978-3-319-14438-2

	ドラ研究院（デンマーク）、Söderhamn Kommun（スウェーデン）

ABC4TRUST プロジェクトは、2015 年 2 月に研究期間を終えるが、その前月に ABC4TRUST サミットというワークショップがベルギーのブリュッセルで開催され、同プロジェクトの研究成果とパイロット試験の結果が発表された。以下に、同ワークショップの概要についての調査結果を収録する。

ABC4TRUST サミットの概要

日程 : 2015 年 1 月 20 日

場所 : ベルギー・ブリュッセル

プライバシー保護技術の研究開発に係る EU の取り組み全般について

- 「EU 助成の研究はデジタル社会において信頼（トラスト）を保持している」：欧州委員会コネクト総局 トラスト&セキュリティユニット長 : Rafael Tesoro 氏
  - 欧州委員会は、2013 年 2 月に「オープン・セーフ・確実なサイバー空間」という包括的なサイバーセキュリティ戦略を発表している。
  - 2007 年～2013 年にかけて実施された第七次枠組計画（FP7）と競争・技術革新枠組計画（CIP）[45]におけるサイバーセキュリティ部門の公募では、101 研究プロジェクトが実施され、3 億 3400 万ユーロがEUから助成された。国別に見ると、助成金を受けた額は、ドイツ、フランス、イタリア、英国の順に多い。
  - ホライゾン 2020 では、プライバシー保護に係る研究開発に関して、三つの支柱がある（プライバシーに対する新しいアプローチ、新型アプリケーションにおけるプライバシー、開発と技術革新）。
  - ホライゾン 2020 の 2014-2015 年度作業プログラムでは、暗号とセキュリティ・バイ・デザインの研究、そして、デジタルセキュリティの枠組みで、プライバシー保護の研究が助成される。

ABC4TRUST プロジェクトの概要について

- 「プライバシーを遵守する ID 管理 - ABC4TRUST の導入」：フランクフルト・ゲーテ大学 : Kai Ranneberg 氏（プロジェクトコーディネーター）
  - ID 管理の問題として、ユーザーが認証者に過度の個人情報を与えており、プライバシー侵害の恐れがある。
  - プライバシーABC 技術（ABC を利用するプライバシー保護技術）により、適切な属性を証明すること、ユーザーは最小限のコード化された要求の集合を開示することができる。
  - プライバシーABC 技術のなかでも、IBM の idemix 技術（匿名認証システム）とマイクロソフトの U-Prove 技術（開示する情報を最小限化する暗号技術）が重要である。

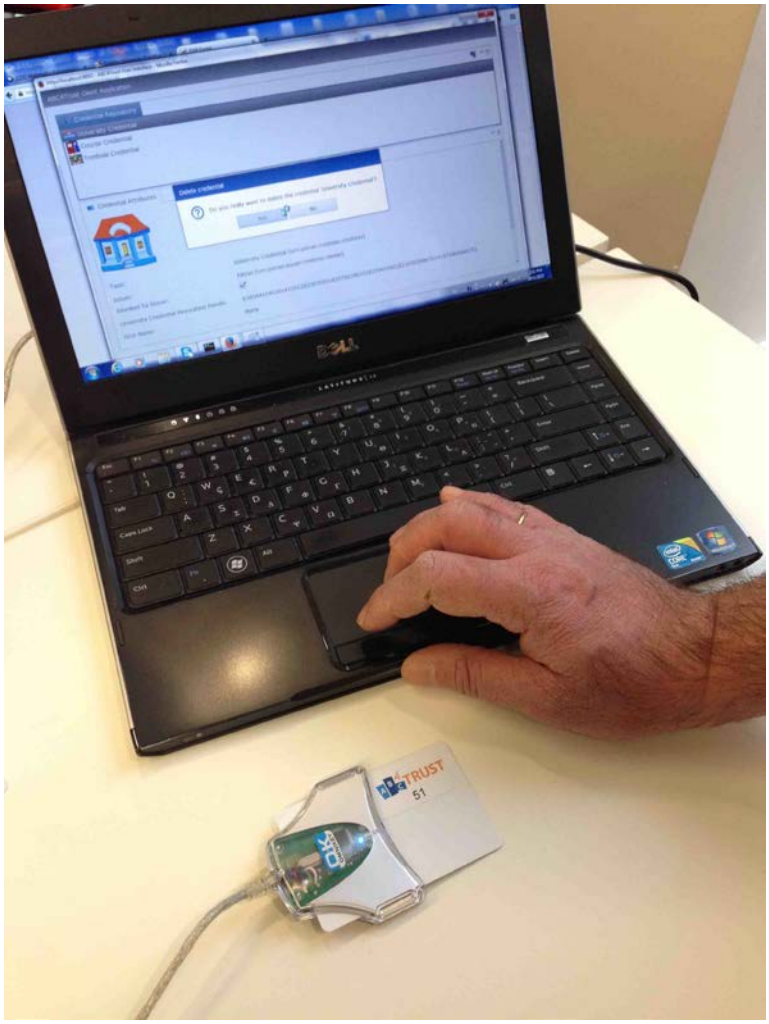
[45] CIP は EU の主に中小企業向けの研究開発助成プログラムである。
http://ec.europa.eu/cip/index_en.htm

- プライバシーABC 技術のあいだには相互運用性の問題がある。ABC4TRUST プロジェクトは、複数の ABC システムに共通の連合されたアーキテクチャを定義すること、選択された幾つかの ABC システムのオープンなリファレンス実装、パイロット試験を実施することを目標とする。
- このプロジェクトにより、セキュリティとプライバシー保護を一度に強化すること、ユーザーがひとつの技術にロックインする恐れを回避することが可能になる。またプライバシーABC 技術は、市民の ID カードと ID プラットフォームにおけるプライバシー・バイ・デザインの基礎となる。

ABC4TRUST プロジェクトで実施したパイロット試験の概要について

- 第一のパイロット試験 :「e 投票と評価」: コンピュータ技術研究院&プレス（CTI）・ディオファンタス : Yannis Stamatiou 氏
  - ギリシアのパトラス大学コンピュータ工学・情報学部において、学生による大学講義評価というケースで、プライバシーABC 技術を用いたパイロット試験を実施した。
  - 高等教育におけるオンライン講義評価アプリケーションにおいて、プライバシーABC の概念実証を行うことが目的であった。
  - 大学 ＝ ID 発行者、学生 ＝ ユーザー、講義評価システム ＝ 認証者
  - 大学がユーザーの情報を認証するための技術には idemix を利用した。どの講義に登録しているか認証する技術には U-Prove を利用した。
  - パイロット試験の内容 : 1）各学生がスマートカードと専用のカードリーダーを所持し、学生は新学期が開始するまえに、スマートカードに専用ウェブサイトから証明物（credentials : 証明された諸属性）を保存する。2）学生は講義の冒頭にスマートカードを教室に設置された非接触型リーダーに照らし、出席したことを証明する。3）学期末に、学生はスマートカードを使って、専用ウェブサイト（Firefox ブラウザのみ対応）で、登録している学部、その講義に登録していること、講義を評価するために必要なだけその講義に出席したという情報を匿名で講義評価システム（認証者）に送り、認証後、一定の質問事項に返答し、自分が登録した講義を評価する。以上の手続きの際、学生はその学生を特定できる個人情報を明かさなくてすむ。なお、学生は匿名で講義を評価できるが、二回目の評価を実施しようとしても、システムが拒絶するので（匿名であるにもかかわらず）、学生は講義評価を一回しか行うことができない。
  - パイロット試験の結果 : 多くの学生が講義評価の匿名性を評価している。
    - ✧ 80%の学生がプライバシーABC 技術を他の用途に使いたいと思っている。
    - ✧ 93.3%の学生がプライバシー保護システムを装備している電子評価を好む。
    - ✧ ほとんどの学生がプライバシーABC 技術により匿名化が行われており、プライバシーが保護されていることを感じている。
    - ✧ ほとんど全ての学生がプライバシーABC 技術に基づく講義評価を使い続けたいと思っている。

写真：ABC4TRUST で開発されたオンライン講義評価アプリケーション、スマートカード、カードリーダー



- 第二のパイロット試験：「ソーデルハムンパイロット」：Eurodocs 社：Souheil Bcheri 氏
  - スウェーデンのソーデルハムン市の高校（Norrtullskolan 校）で、学校内のソーシャルネットワークにおいて（生徒、先生、その他の職員、保護者向け）、プライバシーABC 技術の試験を実施した。
  - チャット、政治に関する議論、健康に関するカウンセリング、資料の共有とアクセスという 4 つの用途に利用できる一つのシステムを開発した。
  - 開発されたシステムにおいては、ユーザーが匿名性の程度を自分で選択できる（偽名を用いることもできる）。
  - チャットに関しては、匿名でなくても良いという生徒がいるが、政治に関する議論に関しては、匿名性を保持したい生徒が多い。
  - 生徒向けの健康カウンセリングにおいては、生徒は学校に所属していることだけを知らせることできる。
  - 問題があった場合にはインスペクターの役割を担う者がシステムの利用について調査できるように、サービスプロバイダはユーザーと最初に契約を交わし、一定の条

件に同意を求める。この契約が破られた場合、サービスプロバイダはユーザーが持つ暗号化された ID を開示できる。
  - ユーザーは学校側から受け取ったスマートカードにより認証され、ソーシャルネットワークサービスを利用できる。スマートカードには、ABC ソフトウェア、証明物（名前、クラス、生年月日、性別等）が含まれている。
  - ソーシャルネットワークサービスは、ウェブアプリケーションを通して利用できるが、ログインするさいに、匿名、偽名、名前を公開するか、また性別、年齢を選択して公開するか決定できる。

ABC4TRUST プロジェクト内で実施した研究

- 「リファレンス実装」：ミラクル社：Michael Ostergaard 氏
  - ABC4TRUST のアーキテクチャは Java で書かれており、典型的なデスクトップ及びサーバ向けに設計されている。また、スマートカードをサポートしており、ユーザーサービスとブラウザプラグインを通して、ユーザーはインタラクションできる。
- 「スマートカード上の ABC4TRUST」：クリプトエキスパート社：Pacal Paillier
  - ABC4TRUST プロジェクトで利用されるスマートカードは、U-Prove と Idemix 技術をサポートしている。
  - スマートカードはオープンソースの GitHub（C コード）で、無料で手に入る MultOS をベースにしたオープンソースのアプリケーションである。
  - スマートカードはユーザーのプライベートキーとして機能する。
  - スマートカードのバージョン 1.2 は、MultOS ML3 デュアルインターフェースカードをベースにしており、64kb の非揮発メモリ、1kb の RAM、SLE78 インフィニオンプロセッサを装備している。
  - スマートカードを利用することにより、ユーザーのプライベートキーを安全に保管し、利用することができるとともに、コンピューティング環境をより信頼のおけるものにできる。また、カードを利用することにより、論理的物理的攻撃を防ぐことができる。
  - スマートカードの必要文書は十分にそろえられており、標準化の準備が整っている。
- 「モバイル上のプライバシーABC 技術」：アレクサンドラ研究院：Gert Laessoe Mikkelsen 氏
  - 現在多くの人が利用するスマートフォン上でのプライバシーABC 技術の使用可能性（ネイティブアプリケーションか、JavaScript での開発）を研究した。
  - アンドロイド OS 向けのネイティブアプリケーションの場合には、プライバシーキーと証明物（Credentiels）をアプリケーションの内蔵メモリに保管する。
  - JavaScript による開発の場合、性能はモバイルのプラットフォームの種類による。
  - 結論としては、ネイティブアプリケーションでも、JavaScript でも、スマートフォン上でプライバシーABC 技術を利用することは可能である。
- 「映画ストリーミングアプリケーション&クラウド上のサービスとの ABC4TRUST」：IBM スイス：Anja Lehmann 氏
  - パイロット試験から、プライバシーABC 技術を普及させるのは困難であること、スマートカード統合にやや時間がかかることが分かった。また、デモ試験はプライベートのものであった。
  - 新たに、より広いユーザーを対象とするデモ試験を行い、認証者と ID 発行者をクラウドサービスとして提供した。

- 新しいデモ試験として、ウェブ上で動画をストリーミング形式で視聴するサービスを開発した（デモを専用ウェブ上で試すことができる[46]）。
- 現在の問題は動画をウェブ上で見る場合、ユーザー認証が必要となる場合があるが、その際に必要のない個人情報を動画視聴サービスプロバイダに与えすぎている。また、フェイスブック等への登録情報を利用して動画視聴サービスへ登録すると、フェイスブックと動画視聴サービスプロバイダがそれぞれ二つの情報（フェイスブックの登録情報と動画視聴サービスへの登録情報）をリンクさせることが可能になる。
- 実際には動画視聴サービスを利用するには、そのサービスを受ける資格があることと年齢（動画には年齢制限があるため）の情報があれば済む。
- IBM Identity Mixer を利用する新たに開発されたシステムでは、ユーザーはオンラインで eGovernment（ID 発行者のこと）から ID を受取り、そして、動画視聴サービスプロバイダからクーポン券を購入し、これら二つをウェブ上の認証ウオレット（Credential Wallet）に保管する。動画を視聴する際には、このウオレットを通して、動画視聴サービスプロバイダにクーポン券と年齢を認証させ、年齢制限に係る情報以外の個人情報が動画視聴サービスプロバイダに渡らない。

今回のサミットの評価

- ABC4TRUST は予算金額が 1000 万ユーロを超える大型のプロジェクトである。研究期間終了を目前にした今回のサミットでは、活発な議論がなされるとともに、プロジェクトにおける研究をまとめた本も出版されており、同プロジェクトは無事に成功したという印象を与えている。他方で、同プロジェクトでは、IBM の idemix 技術とマイクロソフトの U-Prove 技術が根幹に関わる技術として利用されており、本拠地が欧州国以外の組織の貢献が大きいことも指摘できる。

第二節　FP7 PRACTICE プロジェクト

A) PRACTICE プロジェクトの概要

- PRACTICE プロジェクトの目標は、クラウドシステム全体において、データの機密性と暗号化されたデータのコンピューテーションを実現し、柔軟なアーキテクチャとツールを開発することである。
- このプロジェクトの成果は、欧州のユーザーがクラウドシステムに支払う費用を削減させ、企業向けのクラウドの安全なプラットフォームを提供し、ユーザーのデータをクラウドプロバイダーと他のユーザーから保護することである。
- 現在、SLA 等に基づく契約により、クラウドプロバイダーとユーザーはデータの保護を確保しているが、PRACTICE プロジェクトでは、暗号技術により、クラウドプロバイダーでさえもユーザーのデータを見ることができないシステムを開発する。

B) PRACTICE プロジェクトの基本概要

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保護するコンピューテーション
分野	ICT-2013.1.5

[46] https://idemixdemo.zurich.ibm.com/#try

プロジェクト期間	2013 年 11 月～2016 年 10 月（36 ヶ月）
予算（EU 拠出分）	1046 万ユーロ（755 万ユーロ）
コーディネーター	テクニコン（オーストリア）
参加者	KU ルーヴァン（ベルギー）、ゲオルグ・アウグスト大学ゲッティンゲン（独）、ユリウス・マクシミリアン大学ヴュルツブルグ（独）、ダルムシュタット工科大学（独）、インテル（独）、アレクサンドラ研究院（デンマーク）、オーフス大学（デンマーク）、PARTICIA（デンマーク）、CYBERNETICA（エストニア）、バル＝イラン大学（イスラエル）、DISTRETTO TECNOLOGICO AEROSPAZIALE（伊）、ミラノ大学（伊）、アイントフォーヘン工科大学（蘭）、INESC PORTO（ポルトガル）、ARCELIK（トルコ）、ブリストル大学（英）、サレント大学（伊）、SAP（独）
ウェブサイト	http://www.practice-project.eu http://cordis.europa.eu/project/rcn/111030_en.html

C) CASED と EC SPRIDE

欧州の金融、そして、経済の中心地である独フランクフルト市に隣接するダルムシュタット市は、欧州随一の情報セキュリティ研究開発地域であり、1）CASED と 2）EC SPRIDE という二つの組織が設立されている。

1）CASED（ダルムシュタット先端セキュリティ研究センター）

ダルムシュタット工科大学、ダルムシュタット応用科学大学、フラウホーファー研究所SIT（Secure Information Technology）は、2008 年にCASED（Center for Advanced Security Research Darmstadt）[47]という情報セキュリティの研究開発に特化した研究機関を設立している。CASED には国外の組織も参加しており、米INTEL研究所が研究パートナーとして加わっている。CASEDは情報セキュリティの研究に関しては欧州で最大の研究組織であり、300 名の研究者がおり、暗号、ソフトウェア、ハードウェア等を問わず、情報セキュリティに関するあらゆる研究を実施している。

2) EC SPRIDE

ダルムシュタット工科大学とフラウホーファー研究所SITは、EC SPRIDE[48]（European Center for Security and Privacy by Design）という組織を共同で設立している。EC SPRIDEは、プライバシー及びセキュリティ・バイ・デザインの実用化を研究しており、ドイツ連邦教育・研究省から資金を供給されている。同センターは、安全なソフトウェア工学グループ、工学暗号プロトコルグループ、ソフトウェア研究所という 3 つの研究組織を持つ。EC SPRIDEはCASEDと緊密に連携して活動する。

[47] http://www.cased.de/en.html
[48] http://www.ec-spride.tu-darmstadt.de/en/ec-spride/

PRACTICE プロジェクトについて、より詳しい情報を収集するために、同プロジェクトの科学コーディネーターであるダルムシュタット工科大学の研究者にヒアリング調査を行った。以下に、そのヒアリング議事録を収録する。

ヒアリング議事録 / ダルムシュタット工科大学（ドイツ）

日程 : 2015 年 2 月 16 日（月）午後 2 時～2 時 45 分

場所 : 先方事務所（ドイツ・ダルムシュタット）

先方 :

ダルムシュタット工科大学　Ahmad-Reza Sadeghi教授[49]

当方 :

ONOSO 研究員　小野 浩太郎

ヒアリングの概要

先方の研究組織について

- ダルムシュタット工科大学システムセキュリティ研究所の人員は20名から30名程である。
- 同大学では基礎研究を実施している。
- 同大学は、ダルムシュタット応用科学大学、フラウホーファー研究所SIT（Secure Information Technology）とともに、CASED（Center for Advanced Security Research Darmstadt）[50] という情報セキュリティの研究開発に特化した研究機関を 2008 年に設立している。CASEDは情報セキュリティの研究に関しては欧州で最大の研究組織であり、約 300 名の研究者がいる。
- 米 INTEL 研究所が CASED に研究パートナーとして参加している。INTEL の情報セキュリティ研究開発分野の研究所が設立されているのは、米国の外では CASED だけである。
- CASED では、暗号、ソフトウェア、ハードウェア等を問わず、情報セキュリティに関するあらゆる研究が実施されている。
- CASED の非欧州国の研究パートナーには、アメリカの機関が多い（バークレー大学、プリンストン大学、スタンフォード大学、MIT、ライス大学等）。その他、シンガポール、中国、台湾、インドネシア、ヴィエトナム、韓国、日本の組織（NTT 研究所、NEC 等）とつながりがある。

ドイツの ICT 研究開発の一般的状況について

- ダルムシュタット市はドイツのシリコンバレーのような都市である。同市は、欧州中央銀行（ECB）が本拠地を持ち、世界中から多くの銀行が集まるフランクフルトからとても近い。このような地理的状況のおかげで、ダルムシュタット市には SAP、T-System 等の多くの大企業が集まっており、研究開発がとても盛んである。またフランクフルトには国際空港もあり、とても交通の便が良い。
- ドイツでは、自動車産業を筆頭に重工業が盛んであるが、近年 ICT 部門が重工業と融合しつつあり、ドイツで ICT 部門は今後さらに発展していくだろう。

[49] https://www.trust.informatik.tu-darmstadt.de/people/ahmad-reza-sadeghi/
[50] http://www.cased.de/en.html

・ 研究開発が盛んで、産業が発展傾向にあり、経済が順調なドイツに比べて、フランスは経済状況が非常に悪く、政治もうまくいっていない。英国は製造業を他国に売却してしまい、金融業しか残っていない。

FP7 PRACTICE プロジェクトについて

・ PRACTCE プロジェクトは総予算が 1000 万ユーロを超える大型の研究開発プロジェクトである。
・ PRACTICE プロジェクトの目標は、クラウドプロバイダーからユーザーまで、クラウドシステム全体のセキュリティとプライバシー保護を強化することである。
・ 現在、ユーザーは SLA（Service Level Agreement）等に基づき、一定の契約をクラウドプロバイダーと締結することによって、データの安全性を確保しているが、技術的には、クラウドプロバイダーはユーザーのクラウド上の情報を見ることが可能である。PRACTICE プロジェクトの重要な研究開発のポイントは、暗号技術により、ユーザーの情報に暗号をかけ、クラウドプロバイダーにもユーザーの情報を見ることを不可能とすることである。つまり、ユーザーにしか暗号を解けず、ユーザー以外の誰にもユーザーの情報を見れないようなクラウドシステムを開発することである。
・ PRACTICE プロジェクトでは、クラウドプロバイダーからユーザーの個人情報を保護するだけでなく、外部攻撃からクラウドシステムを保護する研究も実施している。
・ PRACTICEプロジェクトの研究開発の一部はすでに実用化されている。エストニアの CYBERNETICA社[51]は、国民の所得税申告等の税金に係るオンラインシステムを開発しており、エストニア政府は同社の技術を利用している。PRACTICEプロジェクトの全体の成果は 2 年後から実用化されていく。
・ Sadeghi 氏は、PRACTICE プロジェクトの科学コーディネーターを担当している。プロジェクトの全体のコーディネーターは、オーストリアのテクニコン社であるが、プロジェクトの開発技術内容ではなく、プロジェクト全体の進行を管理している。科学コーディネーターは開発技術内容を管理しており、他のプロジェクト参加者との技術面での提携に責任がある。
・ PRACTICE プロジェクトでは、プライバシー保護の法律の専門家と提携して、研究している。欧州ではプライバシー保護法の研究に関しては、ベルギーの KU Leuven が有名である。だが、同プロジェクトには KU Leuven 内の研究開発組織が参加しており、プライバシー保護法に関しては、ゲオルグ・アウグスト大学ゲッティンゲンの研究者が研究を行っている。
・ KU ルーヴァンはブリュッセルにとても近く、EU のプライバシー保護法の研究を盛んに行っている。
・ PRACTICE プロジェクトは、サマースクールという形態で、プロジェクトの研究発表を公開して行う予定である。それ以外にも、内部イベントを実施する予定であるが、このイベントに参加するには、同プロジェクトのコーディネーターを通して、プロジェクト参加者全てと欧州委員会の同意を得なければならない。

プライバシー・バイ・デザインについて

・ PRACTICE が開発している技術は、クラウド向けのプライバシー強化技術（Privacy Enhancing Technology : PET）となる。

[51] http://cyber.ee/en/

- ダルムシュタット工科大学とフラウホーファー研究所SITは、EC SPRIDE[52]（European Center for Security and Privacy by Design）という組織を共同で設立している。同センターは、プライバシー及びセキュリティ・バイ・デザインの実施を研究しており、ドイツ連邦教育・研究省から資金を供給されている。

その他の研究開発プロジェクトについて

- ダルムシュタット工科大学は、ドイツ研究振興協会（DFG）[53]が資金を供給するCROSSINGという国内プロジェクトに参加している（資金：2400 万ユーロ）。同プロジェクトは 2014 年に開始され、研究期間は 24 ヶ月間である。同プロジェクトでは、暗号ベースのセキュリティソリューションの研究が実施される。
- ダルムシュタット工科大学は、FP7 のFuture ID[54]というID技術の研究開発プロジェクトに参加している。この技術は、現在はそれぞれ異なるIDシステムを全て一緒に統合するシステムを開発している。全予算は 1451 万 7219 ユーロ（このうちEU拠出金は 999 万 2825 ユーロ）であり、研究期間は 2012 年 11 月から 2015 年 10 月の 36 ヶ月間である。
- ダルムシュタット工科大学は、H2020（Horizon 2020）の SuperCloud というプロジェクトに参加している（2015 年 2 月開始）。
- Sadeghi 氏は、セキュリティとプライバシー保護の双方を研究している。セキュリティの問題と違って、プライバシー保護は各地域や各国毎の法律により異なるが、両者は切り離して考えることができない。

EU 研究開発プロジェクトの問題点

- FP7 等の EU が助成するプロジェクトの幾つかは非常にいい研究成果を出しているが、全く成果が見えないプロジェクトも多い。その理由は、プロジェクトコーディネーターが研究開発の科学的・技術的内容を理解していないからである。アメリカも同じ状況であったが、国防高等研究計画局（DARPA）やアメリカ国立科学財団（NSF）等はプロジェクトコーディネーターに、プロジェクトの科学・技術的内容を把握できる者を置くようになり、状況は改善されつつある。
- 欧州では、研究プロジェクトの評価者がうまく選択されていない。EU プロジェクトに関しては、欧州委員会がプロジェクト毎に専門家を選択し、その専門家がプロジェクトを評価する仕組みを採用しているが、欧州委員会には評価者である専門家を適切に選択する能力がある者はいない。

日本との関係

- Sadeghi 氏は、数年前にドイツ連邦政府の経済相と日本を訪問し、研究開発協定について協議に参加したことがある。

[52] http://www.ec-spride.tu-darmstadt.de/en/ec-spride/
[53] http://www.dfg.de/en/research_funding/programmes/list/projectdetails/index.jsp?id=236615297
[54] http://www.futureid.eu
http://cordis.europa.eu/project/rcn/105974_en.html

第二部　欧州諸国におけるプライバシー保護技術に係る研究プロジェクト

本部においては、フランスとベルギーにおける国内研究プロジェクト、SPION プロジェクトと LYRICS プロジェクトを紹介する。SPION プロジェクトは学際的な研究であり、ソーシャルネットワークにおけるプライバシー保護について、技術的な観点からだけでなく、経済、法等の観点からも研究を行っている。LYRICS プロジェクトは、NFC 技術とサービス向けのプライバシー強化技術の開発を実施している。なお、SPION プロジェクトは、2014 年 12 月の研究期間終了に伴い、最終ワークショップを行っている。その視察報告も収録する。

第一章　SPION プロジェクト（ベルギー）

SPION プロジェクトの概要

- ソーシャルネットワークは、ユーザーの特定の個人情報を共有させることによって成功を収めているサービスである一方で、このようなサービスはユーザーのプライバシーとパーソナルデータのセキュリティという観点から多くの批判にも合っている。このため、SPIONプロジェクト[55]は、ソーシャルネットワークにおけるプライバシーとセキュリティの問題について、学際的に包括的な仕方で研究する。
- SPION プロジェクトでは、特に、ソーシャルネットワークのプロバイダーとステークホルダーの責任に焦点を当てることにより、プライバシーとセキュリティの懸念に対応する方法を研究する。制度的な研究と同時に、同プロジェクトは技術的により安全で、またステークホルダーに透明なソーシャルネットワークを開発することを目標とする。
- SPION プロジェクトは、リスク、脅威を回避するための策、そして、教材を制作する。
- SPION プロジェクトは、ベルギーのフラマン語地域圏の研究助成機関である IWT（Flemish agency for innovation by science and tehcnology）から資金を供給されている。
- プロジェクトには、ベルギーから、KU ルーヴァン法学部、KU ルーヴァンコンピューターサイエンス学部、KU ルーヴァン 電気工学部、ゲント大学教育科学部、VRIJE 大学ブリュッセル、そして、米国からカーネギーメロン大学の研究者が参加している。
- SPION プロジェクトでは学際的な研究を実施するため、いくつもの異なる作業パッケージからなる。
  - ソーシャルネットワークにおけるプライバシーの教育的側面
  - ソーシャルネットワークにおける信頼とアクセスコントロール
  - ソーシャルネットワークにおけるプライバシーの社会的側面
  - ソーシャルネットワークにおけるフィードバックとアウェアネス
  - ソーシャルネットワークにおけるプライバシーの行動の側面
  - ソーシャルネットワークにおけるプライバシーの法的側面
  - ソーシャルネットワークにおける機密性

さて、4 年間の SPION プロジェクトのクロージング・イベントとしてワークショップが開催された。教育的、技術的、法的、経済学的等の観点からの研究成果について発表が行われるとともに、教育用教材等のプロジェクトの成果物について紹介があった。以下に、視察報告を収録する。

[55] http://www.spion.me/about/

視察報告 / SPION ワークショップ「YOU ARE NOT ALONE -HOW TO TACKLE SECURITY AND PRIVACY IN ONLINE SOCIAL NETWORKS-」

1. 日時：2014 年 12 月 16 日（火）
2. 場所：ベルギー・ルーヴェン 「Faculty Club」内
3. 参加者：NICT 欧州連携センター・岡本

主な発表等は以下のとおりである。

（1）教育用教材の作成について

SNS に関するプライバシーリスクは、

a) 好ましからぬコンテンツ（ヘイトメッセージや虚偽情報等）に接してしまう「コンテンツリスク」

b) 好ましからぬ相手からのコンタクト（ヘイトメッセージを書き込まれたり、性的な関心を持たれたりする）を受けてしまう「コンタクトリスク」

c) プライバシーが意図せずサードパーティー等に流出し商業的な目的（ソーシャルアド等）に利用されてしまう「コマーシャルリスク」

の 3 つに大別できる。

SNS のプライバシーリスクに関するティーンエージャーへの教育の重要性が増している。多くの国で、プライバシー教育の必要性が強調され、カリキュラムに盛り込まれてきた。しかし、従来型の教育・教材は、SNS の利用に特化したものではなく、したがって、上記 3 つのリスク全てに対応したものでもなかった。さらに、プライバシーへの「知識・関心」を高めることは意図していたものの、実際に SNS を使う際の「態度」や「行動」を変えることができたか否かの検証も不十分であった。

このような状況を踏まえ、我々は、「Risico’s op Sociale Netwerk Sites (Risks of Social Network Sites)」という、新たなネットプライバシー教育の教材及び教師向けのインストラクションガイド（写真）の開発に取り組むとともに、この新たな教材の効果（上記 3 つのリスクに係る「知識・関心」「態度」「行動」の変化）を図るため、実際の教室における介入実験を行った。

その結果、新たな教材は、3 つ全てのリスクに対する「知識・関心」を高めることに効果があった。その一方、「態度」に関する効果ははっきりとは見られず、また「行動」に対する効果は限定的なものであった。ただし、これには介入（教材による授業）が短時間であったことや、図るべき効果が短期のものであったことなどいくつかの理由も考えられる。いずれにせよ、「態度」、「行動」を変えるために何が重要なのか等、更なる研究が必要である。

(Ellen Vanderhoven 氏 Department of Educational Studies@UGent)

(2) プライバシー情報保護のためのツールについて

ユーザが自己のプライバシー情報をより有効にコントロールできるよう、Facebook 上での友達関係等を可視化しマネジメントするための「FreeBu」というツールを開発した。
（Bo Gao 氏他 DTAI@KUL）

ソーシャルネットワーク事業者は、E2EE（End-to-End Encryption）などのより包括的な手法の提供を含め、プライバシー保護のためより積極的に暗号化に取り組むべきである。一方、暗号化では、傍受そのものを防ぐことはできず、また、コミュニケーションの頻度やデータ量などトラフィック分析による情報漏えいのリスクもある。このようなリスクに対しては難読化（obfuscation）をベースとしたツールが有効である。
(Ero Balsa 氏 iMinds/COSIC@KUL)

既存のブラウザは、JavaScript を実行する際、プライバシー情報を含む大量の情報を流通させてしまっている。我々が開発したブラウザ「FlowFox」を使用することにより、JavaScript の使用に伴う情報流通を正確にコントロールできるようになる。
(Frank Piessens 氏 iMinds/Distrinet@KUL)

(3) プライバシーの社会学的、法学的、経済学的側面について

SNS に関するプライバシーを巡っては、SNS 事業者が「ビッグブラザー」になるのではといった「surveillance」への懸念、利用者が「客」ではなく（プライバシーを売り買いされる）「商品」になってしまうのではないかといった「commodification」への懸念といった論点がある。

その背景には、皆が舞台に立つ俳優であり、誰がそれを見ている観客なのかが分からない「collapsed boundaries」という SNS 上のコミュニケーションの特質がある。

オンラインのコミュニケーションにおけるプライバシーは、オフラインのそれと本質的に異なるものではないが、SNS におけるプライバシーマネジメントは技術的なスキルとソーシャルなスキルの両方を必要とする点が特徴的である。この点において、SNS におけるプライバシーの取扱いは個人がコントロールできる範囲を超えており、プロフェッショナルな取扱いが求められるべきである。

(Ralf de Wolf 氏 iMinds/SMIT@VUB)

プライバシーの法的側面を語る時重要なのは、透明性を確保することであり、具体的には、プライバシーの取扱いに関するポリシー「notice」の通知とそれに対する同意「consent」の取得である。

しかし、プライバシーポリシーを実質的に誰も読んでいないなど、現状、「通知と同意」を軸とするルールだけでは限界がある。

プライバシーの保護に関し、ソーシャルネットワーク事業者に対し、例えば利用者からの直接の削除要求に応じたり、対立する利用者間の仲裁を行ったりといった、いわば「ゲートキーパー」としての役割を期待する声も高まっている。しかし、それは社会的責任を果たすことと裏腹に事業者による検閲の容認につながるといったリスクもある。表現の自由に与える隠れたコストが存在することにも注意しなければならない。

(Brendan Van Alsenoy 氏 iMinds/ICRI@KUL)

歴史的にはプライバシーは問題ではなかった。しかし、生物としての物理的な縄張り意識、そこから派生する外的な感覚的刺激への敏感性が、サイバースペースにおけるプライバシーへの懸念のルーツではないかと考えられる。

多くの人々が、ソーシャルメディアに書き込むべきでなかった書込みをして後悔した経験を有する。また、ソーシャルメディア上での開示（宗教等）が、時として雇用差別の温床になるとの研究成果もある。Nudge（軽い注意）、たとえば、投稿前に（ワンクッション置いて）、これが公開情報である旨の注意を表示させたり、本当に投稿してよいかボックスにチェックをさせるといった機能をシステムに組み込むことで、軽率・不要な書き込みをある程度防止することができると考えられる。

（Alessandro Acquisti 氏 CBDR@CMU）

第二章 LYRICS プロジェクト（フランス）

LYRICS プロジェクトの概要

- LYRICS プロジェクトでは、e チケット等の非接触型サービスを可能にする NFC 技術向けのプライバシー強化暗号（PEC : Privacy Enhancing Cryptography）を開発されている。
- 同プロジェクトは、とりわけ、新しい暗号ソリューションによって、NFC ユーザーが必要最小限のパーソナルデータを開示するだけで各種サービスを利用できるようにすることを目的とする（データ最小限化原則の適用）。
- 同プロジェクトのゴールは、プライバシーが強化されたサービスのための高レベルアーキテクチャの確立、非接触型モバイルサービス向けの低コスト暗号メカニズムの開発、NFC を装備した携帯電話への暗号ツールの安全な搭載、プライバシーが強化された非接触型モバイルサービスのパイロット試験の実施である。

- プロジェクトの最も重要な要素は低コストの暗号メカニズムの構想であり、幾つかのアプローチが考えられている。
  - 第一のアプローチは、SIM カードを開封防止（tamer-proof）されているものとみなす。こうして、SIM カードに組み込まれたキーを抽出することは不可能であり、組み込まれたアプリケーションは正確に動くように全て安全化されている。このアプローチは、通常対称鍵メカニズムに基づく効果的なソリューションを可能にする。だが、特定のケース、例えば、一つの SIM カードの耐タンパー性（tamper résistant：解析の困難さ）が危うくなるやいなや、潜在的な経済的損失が多大である場合には、この耐タンパー性の想定は適切ではない。同様に、SIM カードの開封防止性（tamper-proofness）を強化するにはコストがよりかかる。
  - 第二のアプローチは、SIM カードによる計算を、その計算の大部分を携帯電話に行わせることによって速度を高めることにある。このアプローチは、機密要素を SIM カード内で保護したまま、より高い効果を発揮する方法に開かれている。また、このアプローチは、SIM カード内と携帯電話内の暗号アクセラレータでの並行計算から利益を得ている。
  - 第三のアプローチは、既存のスキームの効果を改善し、新しいプライバシー強化暗号メカニズムを発明するために研究努力を行う。
  - 第四のアプローチは、NEC によって開発された暗号アクセラレータを利用する。
- 2013 年 11 月には、同プロジェクトの枠組みで、Oberthur Technologies と Atos Wordline は、欧州で初めて「パスモバイル（pass mobile）」ソリューションを発表した。パスモバイルは、非接触型サービスに関して、サービスプロバイダーのデータとユーザーのプライバシーの保護に高い保証を与える。とりわけ、公共交通機関向けに非接触型サービスを提供する。

LYRICS プロジェクトの基本情報

省略プロジェクト名称	LYRICS
正式名称	Lightweight privacY-enhancing cRyptography for mobile Contactless Services
プロジェクト期間	2011 年 12 月～2014 年 11 月（36 ヶ月）
予算	91 万 3794 ユーロ
コーディネーター	オレンジ（仏）
参加者	ATOS Wordline（仏）、ENSI de Bourges（仏）、ENSICAEN（仏）、レンヌ第一大学・IRISA（仏）、マイクロソフト（米）、パリ西ナンテール大学・MoDyCo（仏）、NEC（日）、Oberthur Techonologies（仏）
ウェブサイト	https://projet.lyrics.orange-labs.fr/?cat=4 http://www.agence-nationale-recherche.fr/?Project=ANR-11-INSE-0013