資料2

2012年11月26日パーソナルデータ研究会

プライバシー保護等に関する諸外国の最新情報と課題

筑波大学図書館情報メディア系
准教授　石井夏生利

EUの動向
～欧州委員会の立場と他の関係者の懸念を中心に～

欧州調査(2012年10月11日～18日)

- 欧州議会事務局(経済科学政策部局)
- 欧州委員会司法総局
- 欧州委員会通信総局

→担当が異なる

- 英国情報コミッショナー
- 欧州理事会事務局(刑事協力・基本権課)
- 欧州データ保護監察官事務所

→司法総局に親和的

- 加盟国常駐代表部
- リンクレーター法律事務所

欧州委員会司法総局

- 規則の厳格さ(への否定)
- 制定時期
- 忘れられる権利
  “reasonable measure”“something must be done”
- 委任立法
- CBPR(Cross Border Privacy Rules)
- 通知制度の廃止と管理費(administrative cost)の削減
- セーフハーバーの位置づけ
- 独立性
- 2%の制裁金

「個人データ」の範囲

欧州議会	✓明確化の必要性
通信総局	✓個人データの範囲拡大
ICO	✓非常に広範囲
欧州理事会	✓論点として認識
加盟国代表部	✓非常に広範囲 ✓匿名化データ ※前文第(23)項は匿名データを除外
リンクレーター	✓個人データの概念の漠然化、拡大化

「同意」の概念

欧州議会	✓ 明確化の必要性 ✓ 同意の忘却 ✓ データ流通の多方面性
通信総局	✓ 明示的かつ事後的な同意 ✓ 広告に関するビジネスモデルの問題
ICO	✓「公正かつ適法な取扱い」と事前同意 ✓「事前」同意の必要性 ✓ クッキーの取扱いと事前同意・事後同意
加盟国代表部	✓ 明示的な同意への変更理由 ✓ 読まずに明示的にクリックすることの問題 ✓ 事業者と明示的な同意の取得

負担の増加

ICO	✓ 規制過剰
欧州理事会	✓ 管理上の負担(遵守コスト)
加盟国代表部	✓ 同上
リンクレーター	✓ 古いルール(現行指令)を切望する企業

通知義務の廃止とデータ侵害通知

通信総局	✓「24時間」の起算点
ICO	✓ 通知義務の廃止への賛成と手数料問題 ✓ (侵害通知について)全侵害の報告を義務づけることの問題
欧州理事会	✓ 通知義務の廃止への賛成 ✓ (侵害通知について)小規模な侵害の通知義務、「24時間」、(本来行うべき)データ侵害の停止よりも通知義務を優先することの問題
加盟国代表部	✓ 同上 ✓ 文書化の義務と負担

忘れられる権利

ICO	✓ 政治的スローガン ✓ SNSへの投稿と就職失敗 ✓ 異議申立権（The right to object）の重要性
欧州理事会	✓ 幻想的権利 ✓ 執行の実現性、（一旦送出されたデータ）のコントロール不可能性という問題
加盟国代表部	✓ 欧州委員会の対応 ✓ 望ましい考え、理想的なシナリオ ✓ 表現の自由の問題 ✓ 権利の名前は残り、中身は修正 ✓ そこまで心配はしていない。
リンクレーター	✓ 実際の適用への疑問

域外適用と法執行

欧州議会	✓ そこまで心配する必要はない。 ✓ 27ヶ国のルールが統一化と国外投資
ICO	✓ アメリカや日本等のオンラインビジネスがヨーロッパの人々にターゲットを当てた場合、アメリカや日本の企業も法に服するべき。 ✓ 執行の困難性
欧州理事会	✓ 執行の困難性 ✓ EU域外で設立された企業、他国の法域への執行
監察官事務所	✓ 望んでいた法的措置の誕生 ✓ ヨーロッパ市民の保護の指向 ✓ one stop shop
加盟国代表部	✓ 行き過ぎ ✓ 第三国への執行の問題
リンクレーター	✓ 何も知らない企業に対する義務 ✓ 執行方法 ✓ 実際上は機能しない。

制裁金

ICO	✓ 制裁金のリスト、金額が過剰 ✓ プライバシーの保護への失敗と制裁金
リンクレーター	✓ 遵守コストと企業の判断 ✓ 本社の設立場所の選択 ✓ 複数の加盟国内での侵害行為と制裁金 ✓ 制裁金の徴収機関

委任立法

欧州議会	✓ 最小限にしたい
欧州理事会	✓ 数が多い
監察官事務所	✓ 全ての明確化は無理 ✓ ソフトなアプローチを容認 ✓ 明確化の必要性
加盟国代表部	✓ 数が多い

意見の一致：DPAの必要性

- DPAは必要である。
- “one stop shop”

監察官事務所	✓ 規則提案への明記 ✓ 非常に本質的な要素 ✓ 明確化の必要性 ✓ 評価メカニズムの具体化 ✓ 「DPAはデータ保護という基本的権利に内在」 ✓ 「外部からの影響を直接にも間接にも受けないこと」
リンクレーター	✓ DPAなしの法制度を容認する余地(の否定) ✓ 十分性を評価するための鍵となる要素 ✓ 執行は、規制者の独立性を判断する鍵となる要素

監察官事務所及びリンクレーター法律事務所は、DPAのリソースの問題と、オーストリアとドイツに関する欧州司法裁判所の事例に言及。

アメリカ

消費者プライバシー権利章典

- ✓ 2012年2月23日付政策大綱
- ✓「ネットワーク社会における消費者データプライバシー：グローバル化したデジタル経済において、プライバシーを保護しイノベーションを促進するための枠組み」

⇩

4つの要素：消費者プライバシー権利章典、執行可能な実施規範(Codes of Conduct)の策定、効果的な執行、国際的相互運用性

CBPRに言及

消費者プライバシー権利章典の7原則

原則1　個人のコントロール

- ✓ 消費者は、企業が消費者からいかなる個人データを収集し、どのように利用するかについて、コントロールを行使する権利を有する。
  - 企業は、消費者が意味のある選択を可能にするために、容易に利用でき、アクセス可能な仕組みを提供しなければならない。
  - 同様に、同意を撤回し又は制限するための手段を提供しなければならない。

原則2　透明性

- ✓ 消費者は、プライバシー及びセキュリティの実務について、容易に理解できアクセス可能な情報を得る権利を有する。
- ✓ 消費者が意味ある形でプライバシーリスクを理解し、個人のコントロールを行使するために最も役立つ時期と場所における明示的な情報提供。

消費者プライバシー権利章典の7原則

原則3　状況の尊重

- ✓ 消費者は、企業において個人データを収集し、利用し、そして提供する際には、消費者がデータを提供する状況に適合した方法によることを期待する権利を有する。
  - 個人データの利用及び開示は、企業と消費者との関係及び消費者が最初にデータを開示した状況と矛盾しない目的に限定すべき。他の目的で利用又は開示する場合には、透明性及び個人のコントロールのための高度な措置が必要。
  - 状況に関する重要な要素は、消費者の年齢及び技術への精通度である。子供及び10代の者から取得した個人データに対しては、より高い保護を与えるべき。

原則4　安全性

- ✓ 消費者は、安全かつ責任を持って個人データが取り扱われる権利を有する。
  - プライバシー及び安全性のリスク評価、責任ある安全保護措置。

消費者プライバシー権利章典の7原則

原則5　アクセス及び正確性

- ✓ 消費者は、データの機微性及びデータが不正確な場合に消費者に不利な結果をもたらすリスクに適した態様において、利用可能な書式によって、個人データにアクセスし、訂正する権利を有する。
  - 企業は適切な措置を講じること。
  - 表現の自由及び報道の自由に適合した解釈を行うこと。
  - 措置を講じる際の考慮事項：企業が収集又は維持する個人データに関する規模、範囲及び機微性、及び、その利用が消費者に経済的、物理的又は具体的被害を被らせる可能性。

原則6　制限的収集

- ✓ 消費者は、個人データを収集及び保有する企業に適切な制限を課す権利を有する。
  - 個人データの収集を目的達成に必要な範囲に限定。
  - 不要になったデータの破棄又は匿名化。

消費者プライバシー権利章典の7原則

原則7　説明責任

- ✓ 消費者は、企業が個人データを取り扱う際に、プライバシー権利章典を確実に厳守するための適切な措置とともに行わせる権利を有する。
  - 執行機関及び消費者への説明。
  - 従業員の訓練と評価、監査の実施。
  - 個人データを受領する第三者に対する契約上の義務づけ。

消費者データプライバシー立法

- ✓ 消費者プライバシー権利章典の成文化
- ✓ FTCによる直接的法執行
- ✓ 執行可能なセーフハーバーを通じた法的確実性
  - 消費者プライバシー権利章典に対応する実務規範を審査するFTCの排他的権限
  - FTCが審査・承認した実務規範を遵守する企業に対する法執行の自制
- ✓ 消費者データプライバシー保護における連邦と州の役割の均衡
- ✓ 既存の連邦データプライバシー法における効果的な保護の維持
  - 二重の負担を伴わない包括的なプライバシー保護の設定
  - 矛盾又は混乱をもたらす義務規定の改正
- ✓ セキュリティ侵害通知のための全国的基準の策定
  - 特定種類の個人データに関して、無権限アクセスが生じた場合に消費者への通知を義務づける連邦法の制定(センシティブデータを想定)。

（参考）

データ保護に関する米EU共同声明

○ 2012年3月19日、米国ブライソン商務長官とEUレディング欧州委員会副委員長が共同声明を発出。
引き続き、米EUが、データ保護に関して協力して取り組んでいくことについて、両者で発表したもの。

○ 特に以下の点について、双方で認識共有・確認。

・個人情報保護に係る個人の権利促進と商業情報プライバシー制度の相互運用性の円滑化への責任
・セーフハーバー協定の枠組みが、さらなる相互運用性の向上のための出発点となること
・プライバシーの課題への対応策についてのグローバルなコンセンサス作りへ向けて取り組むこと

（共同声明の抜粋）

「米国及びEUは、個人情報を保護するための個人の権利の促進及び商業的な情報プライバシー制度の相互運用性の円滑化への責任感を明確に共有する。」（第1段落）

「データ保護におけるより強力な環大西洋の協力は、消費者の信用を高め、グローバルなインターネットエコノミーの持続的成長、進化する環大西洋のデジタル市場を促進する。」（第2段落）

「双方は、両者で、また、国際的なパートナーとともに、プライバシーを保護するための相互認証の枠組を創設するために協力して取り組むことにコミットしている。双方は、個人情報保護の分野における基準は、国境を越えた情報・物・サービスの自由な流通を円滑化するものであるべきと考えている。」（第4段落）

「我々は、次々に生じるプライバシーの課題への対処策についてのグローバルなコンセンサス作りに向けて、他国の利害関係者とも一緒に取り組んでいきたいと考えている。」（第5段落）

「米国とEUは、セーフハーバー協定に関する各々のコミットメントを改めて確認する。この枠組みは、さらなる相互運用性の向上のための有益な出発点である。・・・(中略)・・・欧州委員会及び商務省は、この枠組みが前進的にアップデートされるよう、引き続き米EUの緊密な協力に期待する。」（第6段落）

「パーソナルデータの利用・流通に関する研究会」第1回（平成24年11月1日）資料3　11頁。

APEC、OECDの動向

Terms of Reference for the Review of the OECD Guidelines

- ✓ WPISP (Working Party on Information Security and Privacy)
- ✓ 2011年10月31日

30年の間に生じた環境変化

- 収集、利用及び蓄積される個人データの量
- 個人データによって可能となった解析範囲
- 新技術等により可能となった社会的及び経済的便益の価値と個人データの責任ある利用
- プライバシーへの脅威の程度
- プライバシーを危険にさらすことも保護することをも可能にする関係者の数及び多様性
- 個人が理解し交渉することが期待される個人データに関するやりとりの頻度及び複雑さ
- 通信ネットワーク及びプラットフォームにより裏付けられる個人データの世界的入手可能性

考慮事項

- ✓ 主要な関係者の役割及び責任
  - プライバシー保護制度の範囲拡大
  - 透明性の拡大、同意の非実効性
  - 個人データの不測の利用にかかるリスクへの対処
- ✓ データ流通の地理的な制限
  - 地理的な根拠に基づき個人データ流通を制限することへの影響
  - 世界規模のプライバシールールの策定
- ✓ 事前の実施及び執行
  - ポリシー実行のための事前アプローチ、技術的及び組織的安全保護措置、データ最小化、データ管理、データ・ポータビリティ、責任ある情報流通、データ侵害通知等

※プライバシー・バイ・デザインへの取組の促進も求められている。

CBPR（Cross Border Privacy Rules）

組織が他のAPEC参加エコノミーへの越境移転を行うための体制

エコノミーによるCBPRへの参加条件

- CPEAに参加していること
- CBPRへの参加表明書の提出
- APECの承認した責任団体(Accountability Agent)の1つを少なくとも利用すること。

※責任団体とは、CBPRの認証を求める企業によるプライバシー・ポリシー及び実務が、体制の基準となる要求事項を満たしている旨を証明する団体であって、APECの承認を受けたものをいう。

CBPRの4つの要素

- 自己評価(self-assessment)
  組織は、プライバシーポリシー及び実務がAPECのプライバシー・フレームワークの要求事項を満たしていること。
- 適合性審査(compliance review)
  責任団体になるための認定基準の充足、責任団体による適合性審査。
- 認証・受入れ(recognition/acceptance)
  責任団体がCBPRシステムに準拠した旨を認証した組織一覧の公表。
- 紛争解決及び執行(dispute resolution and enforcement)
  責任団体及びプライバシー執行機関による執行

違反組織への是正要求、CBPR参加組織からの除名、責任団体の認証シールの一時利用停止、違反組織の公表、プライバシー執行機関等への照会、その他金銭的制裁等

相互運用性

- 2012年7月25日、アメリカが最初のCBPR制度の正式参加者となり、FTCがプライバシー執行機関となった。
- 多くのAPEC加盟国の参加とCBPR制度の世界的な相互運用可能性を指向。
- CBPRとBCR(Binding Corporate Rules)の相互運用に関してアメリカ政府とCNILが議論中。
- その他、メキシコが2012年9月28日にCBPRへの参加申請