

研究成果概要

セコム財団設立40周年記念シンポジウム
AI社会におけるプライバシー保護の最新国際動向
Symposium on Privacy Protection in the AI Society by the SECOM Foundations

2019年7月4日

宮下紘

(中央大学)

Hiroshi Miyashita (Chuo University)

* セコム科学技術振興財団・挑戦的研究助成・助成課題「超スマート社会におけるプライバシー保護の法政策研究」
(平成29年度～平成31年度実施)

黒田玲子先生と宮田満先生からメンタリング等において貴重なアドバイスを頂戴しましたことに謝意を記します。

研究概要

現状

個人情報と匿名加工情報との境界が曖昧
どこまで保護し、どこから利用できるか・再識別化リスク

ビッグデータ利活用や人工知能の開発のための
社会的条件が未整備
企業側の誤解、消費者への周知・理解の不足、安全安心への不安



個人情報保護法の改正 (2017年5月30日施行)

個人情報の明確化(個人識別符号、要配慮個人情報など新たに追加)、匿名加工情報の導入、
国際協力・越境データ移転に関する規律、行政機関等における非識別加工情報の導入

国際的動向の変化

EU一般データ保護規則(2016)、アメリカカリフォルニア州消費者プライバシー法(2018)等



イノベーション促進のための法政策が必要

日本と海外との研究協力が重要

＜米欧日の比較法政策＞

Comparative legal policies

- ・新たな技術の推進のための社会倫理規範に即した法規制・法政策
- ・米欧の消費者等の権利(プロファイリングされない権利、データポータビリティ権等)の検討
- ・「ゼロサム」ではなく、「ポジティブサム」となる規制の在り方の模索

＜ベストプラクティス事例作成＞

Collections of best practices

- ・自動車の位置データ等において情報の匿名化の成功例と失敗例をそれぞれ提示(母集団や追跡範囲の限定などを検討)
- ・再識別化の技術の検討
- ・日本と海外の事例(オランダTomTomの事例など)との比較検討

＜国際協力＞

International collaboration

- ・国際シンポジウムの開催: AI政策とプライバシー保護に関する政策提言
- ・アメリカとヨーロッパの大学との共同研究(ビッグデータの利活用とプロファイリング規制等)
- ・英語による日本の法政策の発信

データ利活用とプライバシー保護の実現

ヨーロッパにおける動向

<EU一般データ保護規則（GDPR）（2018年5月25日適用開始）>

- ・規則としての直接適用（例：ドイツ連邦行政裁判決ビデオ監視のGDPR適用19.3.27）
- ・域外適用（EDPBガイドライン，GDPR適用開始から1年で446件越境事案調査）
- ・同意（例：オーストリア最高裁抱き合わせ同意無効18.8.31/ CJEU, C-673/17, Planet 49/CJEU, C-40/17, Fashion ID）
- ・情報提供の権利（例：フランスCNILによるGoogle5000万€制裁金）
- ・消去権（忘れられる権利）（例：CJEU, C-507/17, CJEU, C-136/17）
- ・データ侵害通知義務（例：オランダ20,881件/ オランダUber60万€制裁金）
- ・個人データの越境移転の規律（例：ドイツベルリン州中国レンタル自転車会社に対する調査/ 標準契約条項の無効を求める訴訟CJEU, C-311/18）
- ・制裁金（例：2019年2月時点で，11のEEA加盟国で総額55,955,871ユーロの制裁金）

<AI倫理ガイドライン（2019年4月）>

- ・4つの倫理原則：①人間の自律の尊重，②害悪防止，③公平性，④説明可能
- ・7つの主要な要件：①人間の作用と監督，②技術的堅牢性と安全性，③プライバシーとデータ統治，④透明性，⑤多様性，差別回避，公平性，⑥社会と環境の幸福，⑦説明責任

<欧州評議会条約第108号＋（2018年5月）>

- ・現代化文書の採択（前文で「人間の尊厳」を明文化）
 - ・人工知能とデータ保護に関するガイドライン（2019年1月）
- ⇒適法性，公平性，目的の特定，データ処理の比例性，プライバシーバイデザイン・デフォルト，コンプライアンスの責任と証明，透明性，データセキュリティ，リスク管理

アメリカにおける動向

<AIに関する大統領令（2019年2月）>

- ①AI研究と開発への投資、②AIリソースの解放、③AIガバナンス水準の設定、④AI労働力の構築、⑤国際的取決めとAIの利点保護

<カリフォルニア州消費者プライバシー法（2018年6月）>

- ・一定の要件を満たす企業（年間総売上2500万ドル以上、毎年5万人以上の消費者等の個人情報を買買、共有等）が対象、カリフォルニア州内で事業を営む企業が対象
- ・特定の消費者や世帯と直接的・間接的に結びつく情報が保護の対象
- ・消費者への透明性の確保（原則45日以内で無料の開示請求）
- ・州司法長官による民事制裁金最大一件につき7500ドル

* 連邦議会において2018年9月から公聴会⇒カリフォルニア州の厳格な立法を覆し連邦法を専断させる狙い

<顔認証に関する法的規律>

- ・サンフランシスコ条例（2019年5月）（カリフォルニア州オークランド、マサチューセッツ州サマービルにおいても同様の条例審議、2019年5月と6月に連邦議会下院で公聴会）
- ・Microsoftによる顔認証規律の6原則（2018年12月）：①公平性、②透明性、③説明責任、④差別禁止、⑤通知と同意、⑥適法な監視

<アルゴリズムの透明性と説明責任>

- ・連邦議会に法案提出（2019年4月）－①自動処理システムの詳細な説明、②コストベネフィット評価、③リスク評価、④リスク最小限化、違反に対しFTCの制裁金

アジアにおける動向

APECプライバシーフレームワーク（2005年）

⇒越境プライバシールール（CBPRs）（アメリカ，メキシコ，日本，カナダ，シンガポール，韓国，オーストラリア，台湾が参加）

Accountability Agentの創設（認証等による越境データ移転）

韓国個人情報保護法

- ・個人情報保護委員会の設立，賠償制度の充実等

中国インターネット安全法

- ・重要情報インフラの国内保存（データローカライゼーション）等

<アジアにおける法整備>

- ・タイ個人データ保護法（2019年）
- ・台湾個人情報保護法（2010年）
- ・シンガポール個人データ保護法（2012年）
- ・フィリピンデータ保護法（2012年）
- ・香港個人データ保護条例（1996年）
- ・マレーシア個人データ保護法（2010年）
- ・インド個人データ保護法案（2018年公表）

日本における動向と展望

日EU間の相互の円滑な個人
データ移転の枠組み構築（2019
年1月）

データ保護プライバシーコミッ
ショナー国際会議「人工知能に
関する宣言」（2018年10月）

G20
「信頼性に基
づく自由な
データ流通
（DFFT：Data
Free Flow with
Trust）」
⇒デジタル経
済に対する
人々の信頼
（トラスト）
を醸成する必
要性

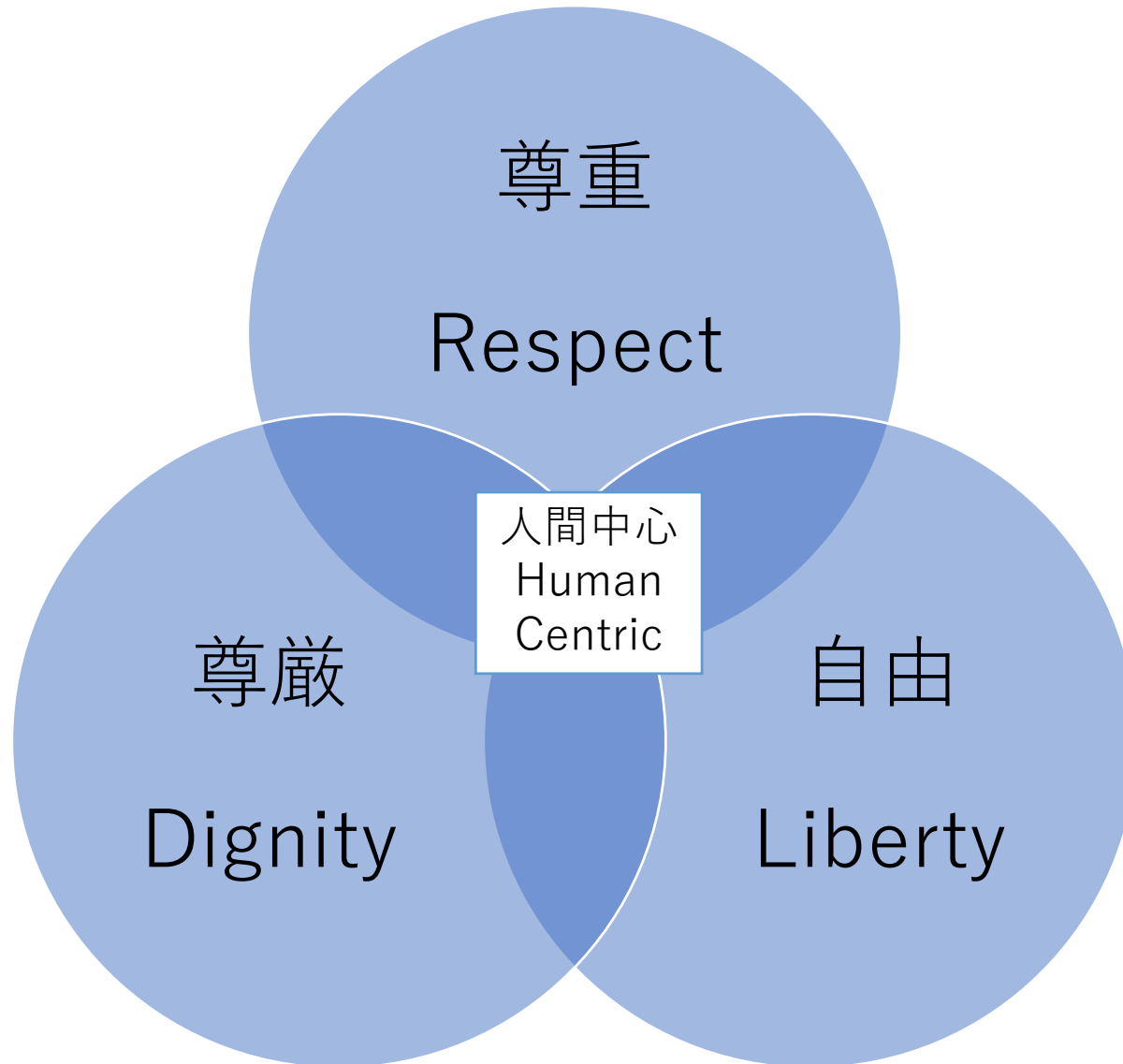
<法律>
個人情報保護に関する法律（行政機関等個人情報保護法等）
（2003年,2015年改正）
官民データ活用推進基本法（2016年）
次世代医療基盤法（2017年）
デジタル手続法（2019年）
<近時の政策文書>
IT戦略本部「デジタル時代の新たなIT政策大綱」（2019年6月）
IT戦略本部「世界最先端デジタル国家創造宣言・官民データ活用推進
基本計画」（2019年6月）
内閣府「人間中心のAI社会原則」（2019年3月）
総務省「国際的な議論のためのAI開発ガイドライン」（2017年9月）
経済産業省「AI・データの利用に関する契約ガイドライン」（2018年6
月）
国土交通省「自動運転車の安全技術ガイドライン」（2018年9月）
文部科学省「Society5.0に向けた人材育成」（2018年6月）

OECD
「人口知能に関
する理事会勧
告」（2019年5
月）
①包摂的成長，
持続可能な発展，
幸福
②人間中心の価
値と公平性
③透明性と説明
可能性
④堅牢性，セ
キュリティ，安
全
⑤説明責任

APEC越境プライバシールールシ
ステム（CBPRシステム）（2014
年4月～）

欧州評議会「人工知能とデータ
保護に関するガイドライン」
（2019年1月）

「人間中心」が意味するものは…
What is “human-centric”?



Research Overview

status quo

The blurred lines between personal data and non-personal data

Line between the protection and the utilization / risk of re-identification

A lack of improved social conditions regarding big data utilization and AI developments

Confusion by the business, lack of consumer education, concerns of safety



Amendments to Act on the Protection of Personal Information
(entered into force in May 2017)

Clarification of personal information / anonymous processing information / international cooperation and data transfer restriction / de-identified information for the administrative organs

International developments

EU General Data Protection Regulation (2016) / U.S. California Consumer Privacy Protection Act (2018)



Necessity of legal policy for promoting innovation

Importance of research collaboration with the overseas experts

<Comparative legal policies>

- legal regulation and policies consistent with the societal and ethical norms towards promoting new technologies
- consumer rights in the US and the EU (right not to subject to profiling, data portability right)
- seeking "positive-sum" instead of "zero-sum" rules

<Collections of best practices>

- best practices and bad practices of anonymization such as car's geolocation data
- re-identification techniques
- case comparisons (TomTom case in the Netherlands)

<International collaboration>

- International symposium: AI policies and privacy protection
- collaboration with the US and the European universities (big data utilization and profiling)
- publications of the Japanese legal policies in English

Realization of both data utilization and privacy protection

Developments in Europe

< **EU General Data Protection Regulation (GDPR)** entered into effect on 25 May 2018 >

- Direct application as Regulation (eg. BVerwG, GDPR requirements instead of the BDSG in video surveillance 19.3.27)
- Extraterritorial application (EDPB Guidelines, 446 cross-border investigations after one year of GDPR's entering into effect)
- Consent (eg. Austria's Supreme Court judgement on coupling ban 18.8.31/ CJEU, C-673/17, Planet 49/CJEU, C-40/17, Fashion ID)
- Right to be provided information (eg. 50 million fine against Google LLC by CNIL)
- Right to erasure (Right to be Forgotten) (eg. CJEU, C-507/17, CJEU, C-136/17)
- Data Breach Notification (eg. Netherlands, 20,881 notifications/ Netherlands, Uber €600,000 fine)
- Data Transfer Rules (eg. Berlin Commissioner's investigation against the Chinese mobike/ CJEU, C-311/18 Standard Contractual Clauses)
- Fine (eg. total 55,955,871 euro fine within 11 EEA states as of February 2019)

< **Ethics guidelines for trustworthy AI (April 2019)** >

- Ethical principles: (1) respect for human autonomy, (2) prevention of harm, (3) fairness, and (4) explicability.
- Key requirements: (1) Human agency and oversight, (2) Technical robustness and safety, (3) Privacy and data governance, (4) Transparency, (5) Diversity, non-discrimination and fairness, (6) Societal and environmental wellbeing, (7) Accountability

< **Council of Europe, Convention 108 + (May 2018)** >

- modernisation document adopted ("human dignity" in the preamble)
- Guidelines on Artificial Intelligence and Data Protection (January 2019)
lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, responsibility and demonstration of compliance (accountability), transparency, data security and risk management

Developments in the U.S.

< Executive Order (February 2019) >

(1) Investment in AI Research and Development, (2) Unleashing AI Resources, (3) Setting AI Governance Standards, (4) Building the AI Workforce, (5) International Engagement and Protecting our AI Advantage

< California Consumer Privacy Act (June 2018) >

- businesses that collect consumer data (subject to annual gross revenue over \$25 million, annually buying or sharing etc 50,000 or more personal information)
- personal information: is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household
- transparency for consumers (disclosure of information free of charge within 45 days)
- the California Attorney General's Office to pay penalties of up to \$7,500 per intentional violation

* Hearing in Senate in September 2018 ⇒ introducing the federal law with preemption over the California state law

< Disciplines on Facial Recognition >

- Ordinance of San Francisco (FILE no. 190110, May 2019) (Oakland, California & Somerville Massachusetts debating the similar ordinances, hearing in the House of Representatives in May and June 2019)
- Six Principles on Facial Recognition by Microsoft (December 2018) : (1) fairness, (2) transparency, (3) accountability, (4) non-discrimination, (5) notice and consent, (6) lawful surveillance

< Transparency and Accountability of Algorithm >

- H.R.2231 - Algorithmic Accountability Act of 2019 (April 2019) — (1) a detailed description of the automated decision system, (2) an assessment of the relative benefits and costs, (3) an assessment of the risks, (4) investigation by FTC

Developments in Asia

APEC Privacy Framework (2005)

⇒ Cross-border privacy rules (CBPRs) (USA, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, and Chinese Taipei are participating)

Accountability Agent (a government-backed data privacy certification)

Korea Personal Information Protection Act

- establishment of Personal Information Protection Commission, civil remedies

China Cyber Security Act

- critical information infrastructure operators to store personal data within China (data localization)

< Legislative developments in Asia >

- Thailand, Personal Data Protection Act (2019)
- Chinese Taipei, Personal Information Protection Act (2010)
- Singapore, Personal Data Protection Act (2012)
- Philippine, Data Protection Act (2012)
- Hong Kong Personal Data Protection Ordinance (1996)
- Malaysia, Personal Data Protection Act (2010)
- India, Personal Data Protection Bill (publicized in 2018)

Developments and Prospects in Japan

Japan-EU mutual data transfer frameworks (January 2019)

International Conference of Data Protection and Privacy Commissioners' Declaration on Artificial Intelligence (October 2018)

< Act >

Act on the Protection of Personal Information (Act for the administrative organs (2003, 2015 amendments)
Basic act on the Public-private data utilization promotion (2016)
Act on the Next Generation Medical Infrastructure (2017)
Digital Procedure Act (2019)

< Recent Policy Documents >

IT Strategic Headquarters, Outline on the New IT Policy in the Digital Era (June 2019)

IT Strategic Headquarters, Declaration to be the World's Most Advanced Digital Nation / Basic Plan of Promoting Public-Private Data Utilization (June 2019)

Cabinet Office, Social Principles of Human-centric AI (March 2019)
Ministry of Internal Affairs and Communications, AI R&D Guidelines for International Discussions (September 2017)

Ministry of Economy, Trade and Industry, Guidelines on Contracts regarding AI and Data Utilization (June 2018)

Ministry of Land, Infrastructure, Transport and Tourism, Guidelines of Technology Security of Self-Driving Cars (September 2018)

Ministry of Education, Culture, Sports, Science and Technology, Human Recurrences toward Society 5.0 (June 2018)

OECD

Recommendation on Artificial Intelligence (May 2019)

- ① inclusive growth, sustainable development and well-being
- ② human-centered values and fairness
- ③ transparency and explainability
- ④ robustness, security and safety
- ⑤ accountability

G20
DFFT : Data Free Flow with Trust
⇒ necessity of creating trust for the digital economy

APEC Cross-Border Privacy Rules System (April 2014~)

Council of Europe, Guidelines on Artificial Intelligence and Data Protection (January 2019)