

第23回AI社会論研究会 大森先生 発表資料 抜粋

研究事例：保育を支援するAI

背景

待機児童問題

保育施設の不足

保育者の不足

問題点

- 離職率の高さ
- 責任の重さ (事故への不安)
- 給与への不満

保育所

若手保育者の増加に伴い『保育の質』の低下が危惧

「自分で考え解決する力」の必要性

育ちの基礎(生きる力)

心情

意欲

態度

生活・遊びによる学び

自ら主体的に環境(ひと・もの)へとかかわる

自分から働きかける

様々な問題乗り越え自分で解決する力 ⇒ 「思考力・判断力・表現力」につながる

自分からチャレンジする
失敗してもくじけない、あきらめない
人とコミュニケーションして相談
まじめ、勤勉、動くことにまめ
自信・自己肯定感

主体的にものごとに取り組む姿(BLES-1K)

子どもの行動計測(28回×1~2h)

- 英語クラス(月4回)
- 自由遊び(不定期)
- Pepper/NAOと子ども対話(不定期)
- 園とのフォーラム7回

「関心の場」モデルに基づくアノテーション

- 周囲の活動の分類 → 「集団場」
- 個人の興味の対象 → 「関心の場」
- 物理特徴(視線・対象・表情・体の動き・動線)

集団の関心の場

職員

子ども

子ども

子ども

対観

個人の関心の場

AI型アノテーションツール プラットフォーム

全方向からの3次元姿勢データ

過去の履歴

注目個体の追跡画像

複数のRGBDセンサの統合

AI技術による状態の自動推定とユーザーによる利用と修正 → データ収集と蓄積

特徴量

このような観察でメリットがあるのは

- 子ども：突然死予防, 安心安全, 保育士の日報作成支援, 発達障害の早期検出, 個性に合わせた療育支援
- 高齢者：転倒可能性評価, 認知症レベル判断, 認知症の進度に応じた介護方法のBigData解析

保育園, 幼稚園, 小学校, 中学校, どこまで? プライバシーをどこまで集めてよいのか? 社会的コンセンサスにむけた合意はありうるのか?

AIとプライバシー・個人情報保護 に関する法的論点

筑波大学図書館情報メディア系
准教授 石井夏生利

本日の概要

- AI・ロボットとプライバシー・個人情報保護に関する法的論点を紹介する。
- 具体的には、EU、米国、カナダ、日本の議論状況に触れつつ、プロファイリング、差別的決定、透明性の欠如、通知・同意の無意味化といった論点を紹介し、予測不可能なAIの発展に対して、プライバシーや個人情報を保護するための法的対応がどこまで可能であるかを考える。

日本の議論

報告書2016

AIネットワーク化の影響とリスク

— 智連社会（^{ウインズ}WINS）の実現に向けた課題 —

平成28年6月20日

AIネットワーク化検討会議

報告書の構成

AIネットワーク化検討会議 報告書2016

『AIネットワーク化の影響とリスク – 智連社会（WINS）の実現に向けた課題 – 』

はじめに

第1章 AIネットワーク化をめぐる最近の動向

- 1 国内の動向
- 2 海外の動向

第2章 「智連社会」における人間像

- 1 問題の所在
- 2 AIネットワーク化の進展が産業構造及び雇用にもたらす影響
- 3 「智連社会」における人間像

第3章 AIネットワーク化に関する評価指標

- 1 問題の所在
- 2 AIネットワーク化の進展が社会にもたらす影響に関する評価指標
- 3 豊かさや幸せに関する評価指標

第4章 リスク・シナリオ分析（ロボットを題材にして）

- 1 問題の所在
- 2 リスク・シナリオ分析の枠組み
- 3 シナリオの具体例
- 4 リスク・シナリオ分析から得られた示唆と課題

第5章 今後の課題

結びに代えて

第4章 リスク・シナリオ分析（ロボットを題材にして）

3 リスク・シナリオの具体例（2）法制度・権利利益に関するリスク（2/3）

リスクの種類	シナリオ上想定されるリスクの内容	発生時期	生起確率	被害の規模	二次的(派生的)に生ずるリスク	リスク評価	リスク管理	リスク・コミュニケーション
消費者等の権利利益に関するリスク	愛玩用の犬型ロボットの飼い主のリテラシー不足などにより、ロボットのアップデートが確実にされなかったため、ロボットが遠隔操作ウィルスに感染して、悪用され、空き巣に入られたり、情報が漏洩するなどの被害が生ずるリスク	進展段階1	高	中	セキュリティに関するリスク、プライバシー・個人情報に関するリスク、犯罪のリスク	セキュリティ機能が更新されないことにより安全な利用が困難となる蓋然性、被害の規模等の評価	自動アップデートの整備、ウィルス感染時の停止・ネットワークからの切断等	セキュリティ機能等の更新についての状況把握・情報共有
消費者等の権利利益に関するリスク	愛玩用の犬型ロボットが歌うサービスを提供していた会社が倒産したため、サービスが継続できず、ロボットが歌わなくなり、ショックを受けた飼い主の高齢者の健康が悪化するリスク	進展段階2	中	中		AIネットワークシステムの連携により導入される他者サービス又は連携により生じたサービスの継続性等の評価	データ・ポータビリティの確保等	末端利用者の連携状況の把握、AIネットワークシステムの状況について把握するための定型化等(連携状況をブラックボックスにしない)
プライバシー・個人情報に関するリスク	サービス・ロボットのプロファイリングにより健康状態等に関する(差別に繋がる、誤った)情報が伝播するリスク	進展段階1	不確実	不確実		プロファイリングによる差別に繋がる情報の伝播のリスク等の評価	人間が介在しないプロファイリングの監視又はプロファイリング結果の修正手段の確保	プロファイリング結果等へのアクセスの確保
プライバシー・個人情報に関するリスク	サービス・ロボットとドローンがネットワークを通じて連携し、利用者とロボットとの会話に係る商品をドローンが自動的に配送するサービスにより、望まない商品が配送されるが、適切な修正が不可能であるリスク	進展段階2	中	中	消費者等の権利利益に関するリスク	AIネットワークシステムの連携により導入される他者サービス又は連携により生じたサービスの透明性等の評価	苦情窓口の開設、自宅へのロボット・ドローン等のアクセス制限等	透明性に関するルールの策定及びモニタリング、透明性確保のための連絡先フォーマットの統一化等

23

第5章 今後の課題

8. プライバシー及びパーソナルデータに関する制度的課題

- ・ A I ネットワークシステムに関するプライバシー影響評価の在り方の検討
- ・ A I ネットワークシステムに関するプライバシー・バイデザインの在り方の検討
- ・ A I ネットワークシステムの利活用の場面に即したプライバシー保護の在り方の検討
 - ロボット等を利活用する際の空間プライバシー(私生活の平穩)の保護の在り方の検討
 - AI等によるデータ処理・解析を利活用する際の情報プライバシー(パーソナルデータ)の保護の在り方の検討
 - Brain Machine Interface (BMI) 等を利活用する際の生体プライバシー(脳情報等生体情報)の保護の在り方の検討
- ・ A I ネットワークシステムを用いたプロファイリングにおけるパーソナルデータの利活用に関するルール及びパーソナルデータを利活用することにより得られたプロファイリングの結果の取扱いに関するルールの在り方の検討
- ・ パーソナルデータの保護及び競争的な利活用の促進の観点からのデータポータビリティに関する動向の注視及び検討(データポータビリティの適用範囲、方法、域外適用等の検討)
- ・ パーソナルデータの保護と利活用との両立を図るための技術的仕組み(匿名加工情報等)の在り方の検討

9. コンテンツに関する制度的課題

- ・ A I ネットワークシステムにより創造されるコンテンツに対する著作権法等知的財産法による保護の在り方の検討
- ・ A I により自動集積されるデータベースに対する著作権法等知的財産法による保護の在り方の検討
- ・ A I を利活用したコンテンツの創造等に関する寡占の動向の注視
- ・ A I ネットワーク化による著作権法等知的財産法の執行強化を見据えた著作権法等知的財産法の在り方の検討
- ・ 機械学習に適したオープンデータの提供の在り方の検討

研究開発原則

1. 透明性の原則：AIネットワークシステムの動作の検証可能性及び説明可能性を確保すること
2. 利用者支援の原則：AIネットワークシステムが利用者を支援し、利用者に選択の機会を適切に提供するように配慮すること
3. 制御可能性の原則：人間によるAIネットワークシステムの制御可能性を確保すること
4. セキュリティ確保の原則：AIネットワークシステムの頑健性及び信頼性を確保すること
5. 安全保護の原則：AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること
6. プライバシー保護の原則：AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること
7. 倫理の原則：AIネットワークシステムの研究開発において、人間の尊厳と個人の自律を尊重すること
8. アカウンタビリティの原則：AIネットワークシステムの研究開発者が利用者など関係するステークホルダーに対しアカウンタビリティを果たすこと

AIネットワーク社会推進会議(開発原則分科会)

論点の要旨 (4/8)

(4) 安全保護の原則 AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること。

○安全保護の原則が適用されるAIの範囲は、個人の生命・身体の安全に関するリスクを惹起し得るAIネットワークシステムの構成要素となり得るAIとしてはどうか。

○AIネットワークシステムにおける本質安全(運動能力等の抑制)、制御安全(監視装置等の実装)、機能安全等を確保することができるよう、その構成要素となり得るAIの設計段階において措置(セーフティ・バイ・デザイン)を講ずべきとしてはどうか。

○ロボット等アクチュエータを実装するAIネットワークシステムを利活用する際の利用者及び第三者の生命・身体の安全に関する判断を行うAIを研究開発する場合には、開発者は利用者等に対し当該判断を行うAIに関する設計の趣旨及び理由を説明すべきとしてはどうか。

○【上記三点のほか、下記(※)において、「(2) 制御可能性の原則」及び「(3) セキュリティ確保の原則」と共通の論点を所掲。】

(※) 上記「(2) 制御可能性の原則」、「(3) セキュリティ確保の原則」及び「(4) 安全保護の原則」の共通の論点

○「(2) 制御可能性の原則」、「(3) セキュリティ確保の原則」及び「(4)安全保護の原則」においては、リスクを評価し抑制するため、AIネットワークシステムの構成要素となり得るAIについて、予め制御可能性の検証(verification) [※形式的な整合性の検証] 及び妥当性確認(validation) [※実質的な妥当性の確認]を行うことが必要となる旨を定めるべきではないか。

(5) プライバシー保護の原則 AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること。

○プライバシー保護の原則において配慮されるべきプライバシーの範囲には、空間プライバシー(私生活の平穩)、情報プライバシー(個人データ)、通信の秘密及び生体プライバシーが含まれるとしてはどうか。

○AIネットワークシステムにおけるプライバシー侵害のリスクを評価するために、その構成要素となり得るAIについて予めプライバシー影響評価を行うべきとしてはどうか。

○AIネットワークシステムがその利活用に当たりプライバシーが保護されるものとなるよう、その構成要素となり得るAIの設計段階において措置(プライバシー・バイ・デザイン)を講ずべきとしてはどうか。

プライベート

プライバシー権の展開

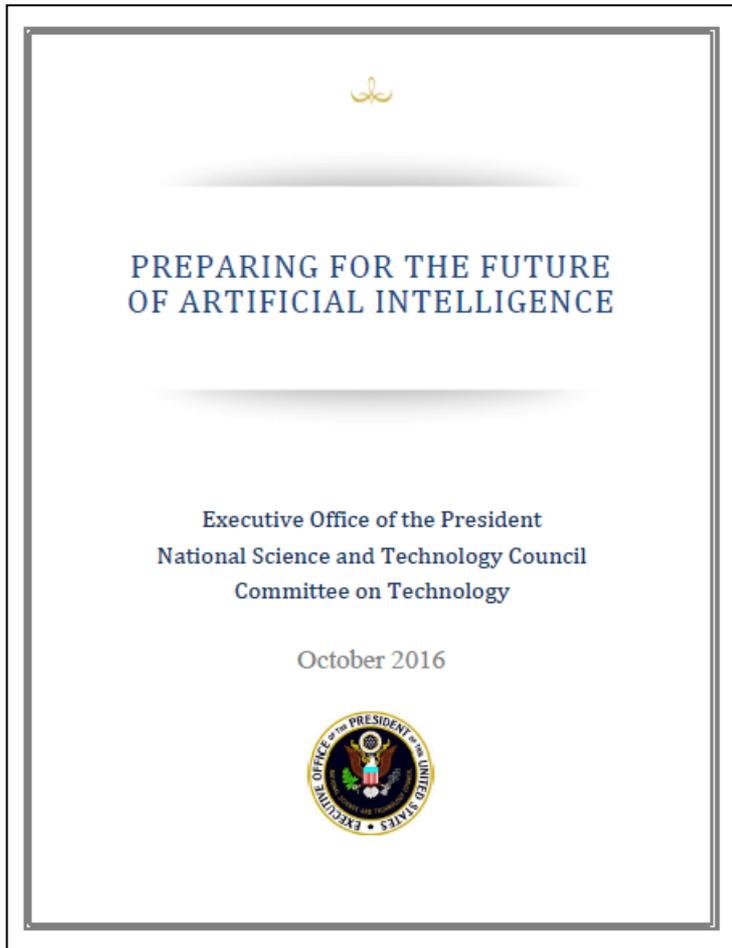
- 「ひとりではほうっておいてもらう権利」
 - Samuel. D. Warren & Louis. D. Brandeis, *The Right to Privacy*, 4 HARV.L.REV.193 (1890).
 - 秘密を守る権利、孤独を守る権利、思想・信条・感情をあらゆる形式における公開から保護される権利
 - 個人が通常、自己の思想や心情、感情をどの程度他人に伝えるべきかを決定する権利or公開の行為を完全にコントロールする権利
- 判例法の発展：不法侵入、私的事実の公開、公衆の誤認、盗用
 - William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960)
- いわゆる「自己情報コントロール権」
 - ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967).
 - プライバシーとは、個人、グループ又は組織が、自己に関する情報を、いつ、どのように、また、どの程度他人に伝えるかを自ら決定できる権利である。
- 立法化による実現

AIの与えるプライバシーへのリスク

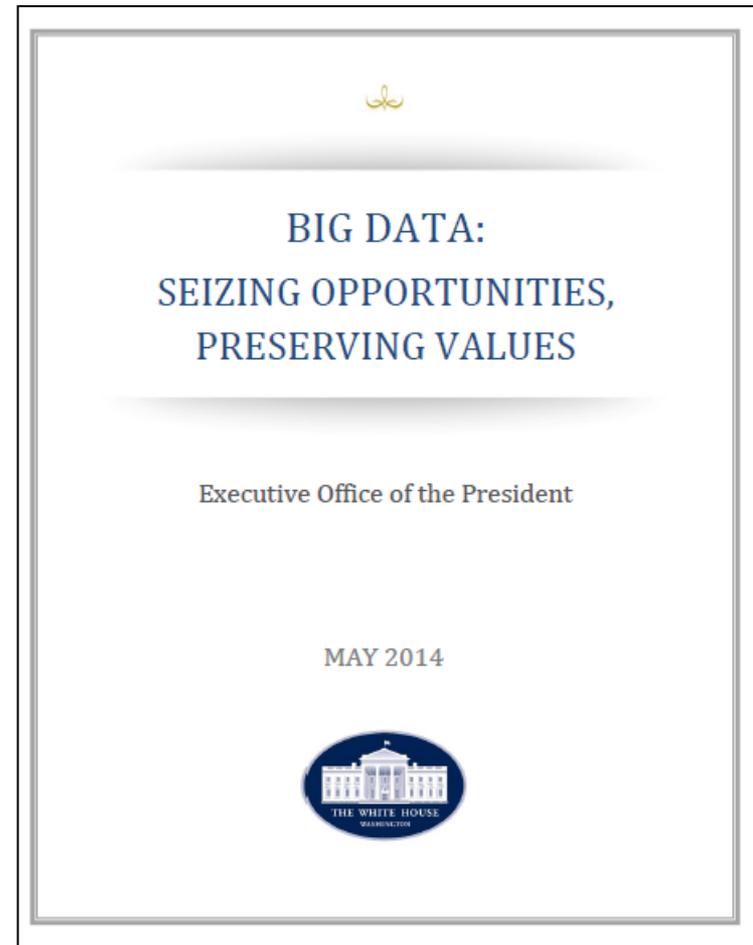
- 個人の知らないところでデジタルプロフィールが生成され、本人の意思に関係なくAIによって差別的な判断を下されるのではないか。
 - アルゴリズムの透明性の欠如
- ロボットによってセンサー機能を用いた過度な情報収集と共有が行われるのではないか
 - ヒト型ロボットに対しては、心理的障壁が低下することにより、機微な情報が安易に提供されるのではないか。

米国・EUの議論

米国の政府機関文書



https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf



http://images.politico.com/global/2014/05/01/big_data_privacy_report_may_1_2014.pdf

機械学習がもたらす プライバシーへのリスク

- 差別的決定による不当な扱いの問題
- より大量の情報にアクセスし、強力な分析を行うようになってきている。
- 透明性、訂正、救済手段の必要性
 - 雇用、信用評価、保険加入の場面のみならず、多様な状況で考慮すべき
- “Algorithmic black box”

See Pasquale F (2015) *The Black Box Society: The Secret Algorithm Behind Money and Information*. Harvard University Press, Massachusetts

Stanford

One Hundred Year Study on Artificial Intelligence (AI100)

[Home](#) [About](#) [People](#) [Framing](#) [2016 Report](#)

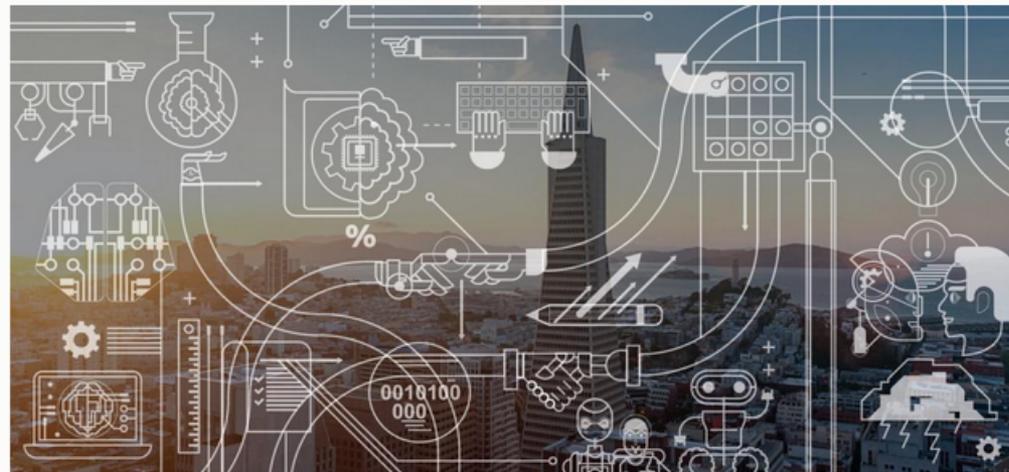
2016 Report

[Preface](#)[Executive Summary](#)[Overview](#)[Section I: What is Artificial Intelligence?](#)[Section II: AI by Domain](#)[Section III: Prospects and Recommendations for Public Policy](#)[Appendix I: A Short History of AI](#)

Related Documents

[2015 Study Panel Charge](#)[June 2016 Interim Summary](#)[Download Full Report](#)

2016 Report



Welcome to the 2016 Report

[Download Full Report in PDF](#)

Browse report online by clicking on section headings in the '2016 Report' box to the left.

プライバシーの課題

- 過去のパターンに基づく将来の行動予測
 - 信用リスクを評価するための機械学習の利用
 - 仮釈放を検討するときに、常習犯となる可能性を予測するための複雑なアルゴリズムを通じて囚人の詳細を調査
- 偏りのあるデータにより生じる差別的決定
 - 将来の行動予測を行う際に、人種や性的嗜好がAIベースの決定に用いられていないか
 - 郵便番号のような無害な情報ですら相関関係を持つ可能性
- 擬人化技術に対する人の反応
 - 人々はあたかも人であるかのように反応してしまう。

ロボット
Robot

ドローン・自動走行車
Drone&Self-driving cars

人工知能 (AI)
Artificial Intelligence

IoT
Internet of Things

カルチャー
Culture

ROBOTEER > 人工知能 (AI) > 精度85%以上…人工知能が顔相から「犯罪予備軍」見分ける

精度85%以上…人工知能が顔相から「犯罪予備軍」見分ける

関連ワード: [AI](#) [テロ](#) [中国](#) [犯罪](#) [米国](#)

 Written by バーナード・コン

Posted date:2016.12.12

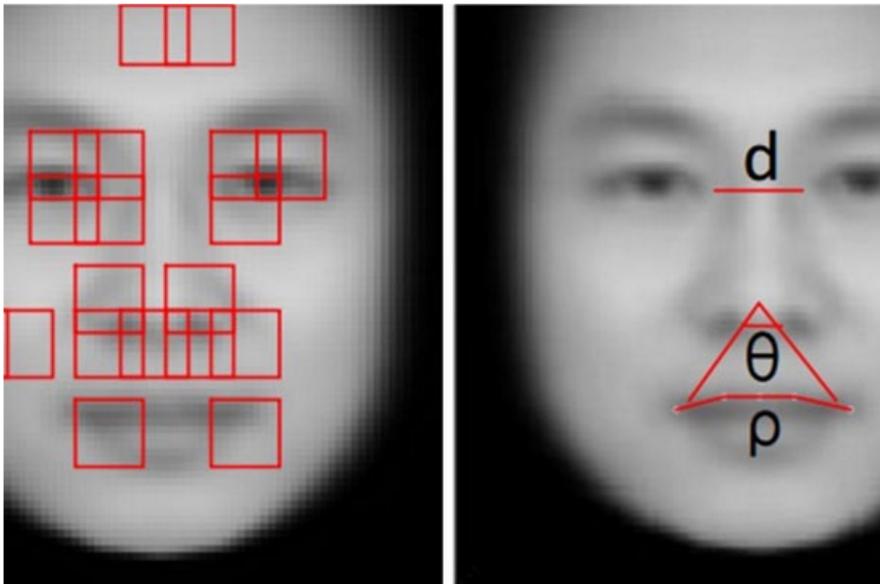


photo by arXiv.org

欧州連合(EU)

- 一般データ保護規則(General Data Protection Regulation, GDPR)
- 2016年4月27日採択、2018年5月25日適用開始
- データ保護に関する網羅的規制
- 加盟国に直接適用
- 英国の離脱

AIに特有の規定はない。

GDPRの全体構造

第1章 総則 (General Provisions) 第1条～第4条

第2章 諸原則 (Principles) 第5条～第11条

第3章 データ主体の諸権利 (Rights of the data subject)

第1節 透明性及び手続 (Transparency and Modalities) 第12条

第2節 情報及び個人データへのアクセス (Information and access to personal data) 第13条～第15条

第3節 情報及び個人データへのアクセス (Information and access to personal data) 第16条～第20条

第4節 異議申立権及び自動処理による個人に関する決定 (Right to object and automated individual decision-making) 第21条、第22条

第5節 諸制限 (Restrictions) 第23条

第4章 管理者及び取扱者 (Controller and processor)

第1節 一般的義務 (General obligations) 第24条～第31条

第2節 個人データの安全性 (Security of Personal Data) 第32条～第34条

第3節 データ保護影響評価及び事前の許可 (Data Protection Impact Assessment and Prior Consultation) 第35条～第36条

第4節 データ保護責任者 (Data protection officer) 第37条～第39条

第5節 行動規範及び認証 (Codes of conduct and certification) 第40条～第43条

第5章 第三国又は国際機関への個人データの移転 (Transfers of personal data to third countries or international organisations) 第44条～第50条

第6章 独立監督機関 (Independent supervisory authorities)

第1節 独立の地位 (Independent status) 第51条～第54条

第2節 管轄, 職務及び権限 (Competence, Tasks and Powers) 第55条～第59条

第7章 協力及び一貫性 (Cooperation and consistency)

第1節 協力 (Cooperation) 第60条～第62条

第2節 一貫性 (Consistency) 第63条～第67条

第3節 欧州データ保護会議 (European Data Protection Board) 第68条～第76条

第8章 救済, 法的責任及び罰則 (Remedies, liability and penalties) 第77条～第84条

第9章 特別な取扱状況に関する規定 (Provisions relating to specific processing situations) 第85条から第91条

第10章 委任行為及び実施行為 (Delegated acts and implementing acts) 第92条～第93条

第11章 最終条項 (Final Provisions) 第94条～第99条

プロファイリング

- 「プロファイリング」とは、「自然人に関するある一定の個人的な側面を評価するために、特に、当該自然人の業績、経済状況、健康、個人的嗜好、興味、信頼性、行動、位置又は移動に関連する側面を分析し又は予測するために、個人データの利用から構成されるあらゆる形態による個人データの自動的な取扱いをいう」(第4条(4)項)。

プロファイリングを含む、自動処理による 個人に関する決定(第22条)

- データ主体は、プロファイリングを含め、自己に関する法的効果をもたらすか、又は、それに類する重大な影響を自己にもたらす、自動的手段による取扱いのみに基づく決定に服さない権利を有する。
- オンライン上の貸付申請の自動的拒否又は人間を介在させない採用活動などの典型的な事案が想定。

自動的決定に服する場合の代替措置

- 管理者側で人を介在させる権利
 - データ主体が自己の意見を表明する権利
 - 決定に異議を唱える権利
-
- ✓ 機械学習を行うAIに適用可能？
 - ✓ どのタイミングでこの仕組みを動かすのか。

差別的判断の例

- 当初のデータの偏りが機械学習による予測を誤らせる。
- Googleのフォトアプリの例
 - デジタルフォトアルバムの写真を自動でタグ付けし、黒人を「ゴリラ」と判別した例
 - システムが白人ばかりの訓練を受けていると、白人以外の顔の認識が困難になる。
- データの偏りのみならず、人が作ったプログラムが他のバイアスを有む。

See Buttarelli G (2016) A smart approach: counteract the bias in artificial intelligence. <https://secure.edps.europa.eu/EDPSWEB/edps/pid/696>. Accessed Apr. 19, 2017; House of Commons, Science and Technology Committee (2016) Robotics and artificial intelligence: Fifth Report of Session 2016-17. <https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf>. Accessed Feb 7, 2017

義務の名宛人

- GDPRは「管理者」を名宛人としている。
- 単独で又は他者と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、当局又は他の団体をいう。」(第4条(7)項)

機械学習を行うAIを管理する者(事業者や機関)が「管理者」になれるのか？

透明性

- 第12条「データ主体が権利を行使するための情報、通知及び手続の透明性」：データ主体が権利を行使するための情報を提供する義務
- 第13条「データ主体から個人データを収集する場合に提供すべき情報」：管理者の連絡先、取扱い目的、取扱いの法的根拠など
- 第14条「データ主体から個人データを取得しなかった場合に提供すべき情報」

欧州議会

- 2017年1月27日の欧州議会法務委員会レポート：ロボットに関する民事法についての欧州委員会への勧告提案
- 私生活及び個人データ保護の権利が全てのロボット分野に適用され、EUのデータ保護のための法的枠組が全て遵守されなければならないこと、その観点で、ロボットにおけるカメラとセンサーの利用についての規則及び基準を見直すべきこと。
- 委員会には、Privacy by Design and Privacy by Default、データ最小化、目的制限などのデータ保護諸原則、透明性あるコントロールの仕組み、適切な救済が遵守され、適切な勧告及び基準が策定されEUの方針に統合されることを呼びかけ。

See European Parliament (2017) REPORT with recommendations to the Commission on Civil Law Rules on Robotics. 27 January 2017. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0005+0+DOC+PDF+V0//EN>.

Accessed Apr. 19, 2017

決議案補足説明

- プライバシーの権利は常に尊重されなければならない。ロボットエンジニアは、私的情報を保護し、適切な場合に限り利用することを保障すべきである。さらに、ロボットエンジニアは、例外的状況を除いて個人が個別に識別されないこと、また、明確かつ明白なインフォームドコンセントを得るよう保障すべきである。人と機械のインタラクションに先立ち、人によるインフォームドコンセントを求め、取得すべきである。そのようなものとして、ロボット設計者は、有効な同意、機密性、匿名性、公正な取扱い及び適正手続のための手順を策定し遵守する責任を負う。設計者は、関連するデータを破棄し、及びそれをあらゆるデータセットから取り除くことへの要請を遵守するであろう。

その他

- 明らかなオプトアウトの仕組み(キルスイッチ)を合理的な設計目的に沿う形で統合すべきである。
- 長期的には最も洗練された自律型ロボットを電子人間とし、その法的地位を定めるべきである。

Google developing kill switch for AI

🕒 8 June 2016 | Technology

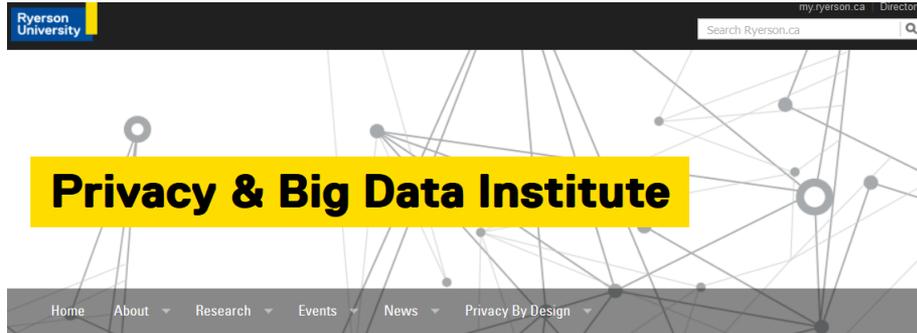
🔗 Share



Google developing Kill Switch for AI, BBC news, <http://www.bbc.com/news/technology-36472140>

プライベート・バイ・デザイン

Privacy by Design



Privacy & Big Data Institute

Home About Research Events News Privacy By Design

ANN CAVOUKIAN



Title:

Executive Director of the Privacy and Big Data Institute

Office:

VIC-712

Telephone:

416-979-5000 x3138

Email Address:

ann.cavoukian@ryerson.ca

Biography:

Appointed as the Information and Privacy Commissioner of Ontario, Canada in 1997, Dr. Ann Cavoukian served for an unprecedented three terms as Commissioner. In that time, she elevated the Office of the Information and Privacy Commissioner from a novice regulatory body to a first-class agency, known around the world for its cutting edge innovation and leadership. Dr. Cavoukian is best known for her creation of Privacy by Design – unanimously adopted as an international framework for privacy and data protection in 2010; now translated into 38 languages.

As of July 1, 2014, she began a new position at Ryerson University as the Executive Director of the Privacy and Big Data Institute – Where Big Data meets Big Privacy.

- Principle 1: Proactive not reactive:
preventative not remedial
- Principle 2: Privacy as the default setting
- Principle 3: Privacy embedded into design
- Principle 4: Full functionality: positive-sum, not zero-sum
- Principle 5: End-to-end security: full lifecycle protection
- Principle 6: Visibility and transparency: keep it open
- Principle 7: Respect for user privacy: keep it user-centric

<http://www.ryerson.ca/pbdi/privacy-by-design/7-foundational-principles/>

<http://www.ryerson.ca/pbdi/privacy-by-design/>

Privacy by Designの要点

- プライバシー(公正情報実務)が事前に組み込まれている。
- 個人の側の努力は不要である(自動的に保護される)。
- プライバシーとセキュリティ、プライバシーと事業プロセスの「両者」を実現する。
- ゼロサムではなくポジティブサム
- プライバシーは秘密を守るのではなく、個人のコントロール(選択)である。
- コンテキストが重要である。

立法化を必須とする仕組みではない。

OECD Privacy Principles

(Fair Information Practices)

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

Revised July, 2013

Privacy by Designの適用分野

Privacy by Design Application Areas

1. CCTV/Surveillance Cameras in Mass Transit Systems;
2. Biometrics Used in Casinos and Gaming Facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Devices & Communications;
5. Near Field Communications (NFC);
6. RFIDs and Sensor Technologies;
7. Redesigning IP Geolocation Data;
8. Remote Home Health Care;
9. Big Data and Data Analytics.

SmartData

- AIに適用可能とされている。
- PbD2.0
- 個人データが自らを保護する。
- 人間のクローンを作るように、サイバー空間での「代理人」を作り出し、個人の選好及び状況に応じて本人の情報を開示するか否かを管理するという構想
- 実施方法
 - ①個人データの安全保護を実施、②データのアクセスルールを「代理人」の中に設定する、③そのルールを条件に情報へのアクセス要請に応じる。
- 課題
 - 実現可能性、変動する状況にどのように対応するのか。



IPSI SMARTDATA INTERNATIONAL SYMPOSIUM
 Privacy meets Evolutionary Robotics: Protecting our Freedoms with Virtual Tools
 University of Toronto, Canada ∞ May 14-16, 2012

- Home
- About
- Program
- Speakers
- Posters
- Registration
- Resources
- Contact



The [Identity, Privacy, and Security Institute \(IPSI\)](#) at the University of Toronto in association with the [Information and Privacy Commissioner of Ontario](#) are proud to host the first **International Symposium on SmartData**.

SmartData is a vision to create Internet-based virtual agents which will act as an individual's online proxy to securely store their personal information and disclose it based upon the context of the data request and instructions authorized by the data subject.

Join us, as we feature a group of renowned international and local experts from a wide range of disciplines, discussing topics such as evolutionary robotics/computing, cognitive science, dynamical systems, neuroscience/brain imaging, philosophy of science, high performance reconfigurable computer systems and disruptive technical innovation.



A Message from Ontario's Information & Privacy Commissioner Dr. Ann Cavoukian on SmartData

<http://www.ipsi.utoronto.ca/sdis/>

SmartData

Privacy Meets Evolutionary Robotics

Editors: **Harvey, I., Cavoukian, A., Tomko, G., Borrett, D., Kwan, H., Hatzinakos, D.** (Eds.)



<http://www.springer.com/gp/book/9781461464082>

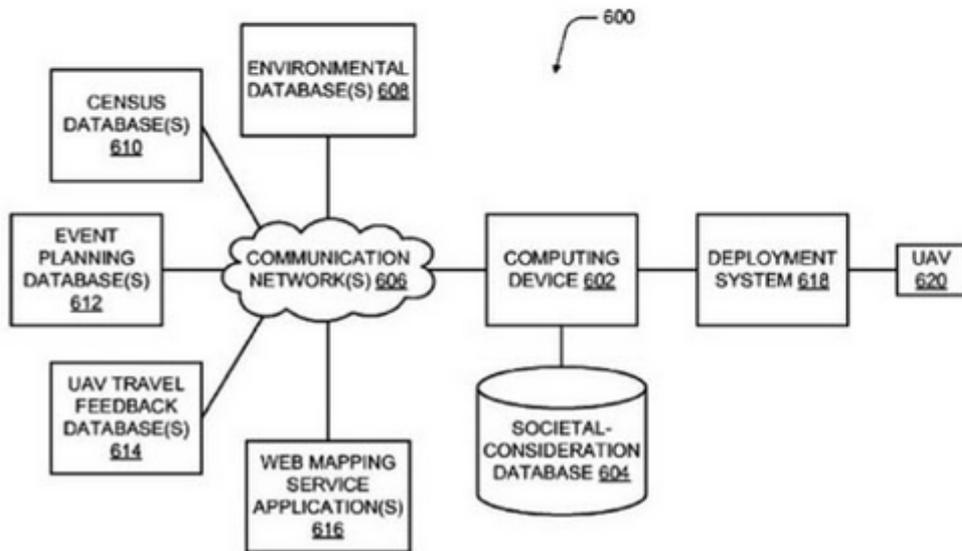
プライバシーを保護する「ドローン飛行経路」設定技術の特許登録…米Google

関連ワード：[Google](#) [セキュリティ](#) [プライバシー侵害](#) [特許](#)



Written by ロボティア編集部

Posted date:2017.02.06



<https://roboteer-tokyo.com/archives/7843>

検討：予測不可能性への対応

- 立法的対応
 - 基本諸原則、権利義務の設定、執行
- Privacy by Designの役割
 - SmartData は実現可能？
 - 技術的努力
- バイアス問題
- ブラックボックス問題
- 最後は“Kill Switch”？