

2026年9月1日(火)13時～15時
個人情報保護政策に関する懇談会

デジタルサービスと個人情報

中央大学国際情報学部
教授 石井 夏生利

資料 2
令和8年9月1日
第3回個人情報保護
政策に関する懇談会

本日の内容

- デジタルサービスが社会で普及していく中で、
 - ✓サービスの提供・利用に当たって個人情報の提供が前提となった背景
 - ✓デジタルサービスに対するサービス利用者の不安等を引き起こしている具体的な要因
 - ✓それに対応する方策

デジタルサービスと個人情報の提供

問題意識

- 消費者と事業者（プラットフォーム事業者、アプリ提供者、AIサービス事業者など）の関係
 - ✓アテンション・エコノミー
 - インターネットの普及による情報過多世界では、人々が払えるアテンション（関心）や消費時間が情報量に対し稀少となるため、これが交換財―「通貨（currency）」―としての経済的価値を持ち、流通するようになるという考え
 - ✓個人に関する情報が収集・分析・評価
 - プロファイリング
 - ✓個人又は第三者に対する働きかけ
 - 「誘導」が発生

アテンション・エコノミー、心理プロファイリングについては、山本龍彦「思想の自由市場の落日 ―アテンション・エコノミー×AI―」Nextcom Vol.44（2020年）5頁ほか。

データ処理による意思決定の誘導（可能性）①：ケンブリッジ・アナリティカ（CA）事件

- CA社は、収集したデータをもとに、「神経症的傾向とダークトライアド特性を有する集団」等の脆弱な層を特定し、広告等を通じて感情を煽るコンテンツを継続的に提示するマイクロターゲティングを行った。同社は、ニュースフィードを利用者の嗜好に合わせてカスタマイズし、類似コンテンツを優先的に表示する手法によってエンゲージメントを高め、利用者の感情や信念を反復的に強化していたとされる。
- 2018年3月17日、ガーディアン紙に掲載されたクリストファー・ワイリーの暴露記事により、CA社が2016年アメリカ大統領選挙におけるトランプ陣営の選挙運動、及び英国のブレクジット陣営の運動の双方に関与していたと報じられた。
- 本人の意思決定に影響→社会の意思決定に影響

クリストファー・ワイリー著、牧野洋訳『マインドハッキングーあなたの感情を支配し行動を操るソーシャルメディアー』（新潮社、2020年）187頁以下。Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, THE GUARDIAN (Mar. 17, 2018)、川西晶大「SNSにおける個人情報の不正利用ーケンブリッジ・アナリティカ事件」国立国会図書館『ソーシャルメディアの動向と課題：科学技術に関する調査プロジェクト報告書』（2020年3月）ほか。

データ処理による意思決定の誘導（可能性）②：リクナビ事件

- 「リクナビに自分の就活の行方が握られているようで怖い」
都内私大4年の男子学生は報道を受け、こう話す。一方で「ナビサイト経由でしか会社説明会や選考の応募ができない会社も多く、使わないわけにはいかない」（都内私大4年の女子学生）という声も一定数あった。

日経速報ニュース「就活、問われるデータ管理『辞退予測』に学生困惑」（2019年8月2日）

- 採用選考の可否判定には使っていないと各社は説明するが、「正直信じられない」と東京大大学院2年の学生は話す。「就活生に黙っていたことがますます可否に関わっているようで不信感が募る」
- データ購入企業の大和総研ホールディングス（HD）を志望し、最終面接の一つ手前で終わってしまったという関西の私立大4年生は「リクナビから買っていた情報で落とされていたとしたら残念だ」と漏らす。

日経速報ニュース「『リクナビに不信感』データ販売で学生に広がる不満」（2019年8月23日）

- 本人の行動予測が第三者の意思決定に影響を与えた可能性

AIプロファイリングとプライバシー

- AIを用いた心理プロファイリングを通じて、個人の精神へのダイレクトな「アクセス権」を「購入」できるようになってきた。

→私的領域への侵入

- ウェブの閲覧履歴や「いいね」などの行動記録から、機械学習を用いて利用者の趣味嗜好、政治的信条、精神状態などを自動予測する技術（プロファイリング）は、利用者がクリックするであろう情報を選択的にフィードし、そのアテンションを稼ぐために、既に、広く、利用されている。

→人物像の推測（イメージの決めつけ）

- 個人の認知過程に直接介入してアテンションを強制的に「奪う（grab）」ことも可能になるだろう。

→人の意思決定への介入

山本・前掲「思想の自由市場の落日 ―アテンション・エコノミー×AI―」5～6頁。

GDPRのプロファイリング関連規制

- 「プロファイリング」
 - ✓ 自然人に関する経済状況、健康、個人的嗜好、行動、位置等の側面を分析し又は予測するための個人データの自動的な処理（第4条(4)号）
- 主な規制
 - ✓ 透明性・アクセス権—決定に用いられる論理及びデータ主体に生じ得る結果（第13条～第15条）
 - ✓ 異議申立権—取扱いの停止（第21条）
 - ✓ 自動処理決定—不利益判断に服さない（第22条）
 - ✓ データ保護影響評価—自然人に関する人格的側面の体系的かつ広範囲な評価（第35条）

デジタルサービス法：オンラインPF事業者の義務

1. 広告表示の透明性

- ✓当該情報が広告であること、広告主が誰か、受信者を決めるパラメータ等の意味ある情報（DSA第26条1項）

2. GDPR第9条1項に定められる特別な種類の個人データを用いて、GDPR第4条(4)号に定義されるプロファイリングに基づき、サービス受領者に広告を表示することの禁止（DSA第26条3項）。

- ✓「特別な種類の個人データ」人種又は民族的出自、政治的思想、宗教又は信念、労働組合への加入を明らかにする個人データの取扱い、及び、遺伝データ、自然人を固有に識別することを目的とする生体データ、健康関連データ又は自然人の性生活若しくは性的嗜好に関するデータ（GDPR第9条1項）

3. 子どもがアクセスできるオンラインPF事業者に対し、そのサービスにおいて、子どものプライバシー、安全及びセキュリティを高いレベルで保障するために適切かつ均衡の取れた手段を講じること(DSA第28条1項)、子どもに対するプロファイリングに基づく広告の禁止(同条2項)。

2と3の趣旨

- 個々人向けのターゲティング広告を表示する際に、脆弱性に訴えかけるデータを用いたり、脆弱な立場に立つ者に働きかけることによる社会的弊害を考慮したものであり、特に、オンラインプラットフォームは、係る操作的な実務において特に影響を与えやすい環境にある(前文(69)項参照)。
- 子どもの保護はEUの重要な政策目的(前文(71)項参照)。

アメリカのプロファイリング規制—州法

- 包括的なプライバシー法
 - ✓ カリフォルニア州、コロラド州、コネチカット州、バージニア州、ユタ州、テキサス州、オレゴン州、モンタナ州、ケンタッキー州など
- GDPRに類する規制を持つ州（コロラド州、カリフォルニア州など）
 - ✓ GDPRに類する定義
 - ✓ 法的効果又はそれに準ずる重大な効果を生じさせる決定に資するプロファイリングに対するアクセス権、オプトアウト権
 - ✓ 高いリスクを生じさせる処理に対するリスク評価
- カリフォルニア州：自動意思決定技術（Automated Decisionmaking Technology, ADMT）
 - ✓ ADMTとは、個人情報処理し、計算処理（computation）を用いて、人間による意思決定を代替し、又は実質的に代替する技術をいう。
 - ✓ 「重大な決定」とは、金融・融資、住宅、入学・教育機会、雇用・独立請負の機会や報酬、医療サービスの提供・拒否につながる決定をいう。
 - ✓ 消費者に関する重大な決定を行うためのADMTについては、事前通知、オプトアウト権、アクセス権、独立の影響評価を義務付け。

コロラド州司法長官のウェブサイト（<https://coag.gov/resources/colorado-privacy-act/>）参照。

カリフォルニア州プライバシー保護庁のウェブサイト（<https://coppa.ca.gov/regulations/?hl=en-US>）、規則本文

（https://coppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf）、達本麻佑子ほか「個人情報保護・プライバシー 2025年の振り返りと2026年の展望 ～米国編～」長島・大野・常松法律事務所 個人情報保護・データプライバシーニュースレター第66号（2026年1月）参照。

Protect rights, autonomy and brain data

- Neurotechnology raises important questions about **mental privacy**, cognitive liberty and human dignity. Because it can generate highly sensitive data about mental states and behaviour, strong safeguards are essential to protect people from misuse and harm. Protecting brain data and ensuring informed consent reduces risks of discrimination, manipulation, and unequal power relationships. Human-centred governance is key to maintaining trust and safeguarding fundamental rights.

OECDのNeurotechnologyのウェブページ

(<https://www.oecd.org/en/topics/sub-issues/neurotechnology.html>) より。

ブレインテック時代の「メンタル・プライバシー」

- ブ레인・マシーン・インターフェース (BMI)
- AIプロファイリングとの質的な違い (22～25頁)
 - ✓個人の内心に「直接的」に迫る技術：マインド・リーディング技術
 - ✓対象とするのは脳内の神経活動そのもの
 - ✓本人の意識及び無意識への侵入
- 無意識の可視化が、個人の「人格的自律 (personal autonomy)」に深刻な影響を与え得る。 (26頁)
- 「絶対に暴かれてはならない意識・無意識」とは何か。 (同上)
- AIチャットボットとBMIが統合されたシステム
 - ✓「自己像」 (identity) を形成する主体が、自己からAIへと移転 (同上)
- いかなる種類の神経活動の可視化を具体的に禁じるべきなのか。 (同上)

小久保智淳「ブレインテック時代の「メンタル・プライバシー」ー可視化される「無意識」と人格的自律のゆくえー」Nextcom Vol.65 (2026年) 21頁以下。

監督機関のアプローチ（英国）①

- ニューロデータのプライバシーリスク
 - ✓無意識に生成されて本人がコントロールできないこと
 - ✓組織が大規模・複雑なデータを集めてメンタルヘルスなど機微な情報まで推知できてしまうこと
 - ✓単に観察・収集するのみならず、神経パターンの調整や行動変容にまで踏み込めること
 - 自動処理による個人情報利用のリスクを高め、組織側の利用目的・方法の透明性の欠如にもつながる。
- 利用の拡大
 - ✓健康・医学研究、ウェルビーイング及びスポーツ、職場（安全、生産性、採用等）、エンターテインメント及びゲーム、マーケティング、軍事及び教育分野

ICO, *ICO tech futures: neurotechnology, Why neurotechnology and neurodata?*, <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-neurotechnology/why-neurotechnology-and-neurodata/>.

ICO, *ICO tech futures: neurotechnology, Sector scenarios*, <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-neurotechnology/sector-scenarios/>.

監督機関のアプローチ（英国）②

- 規制上の課題

1. 規制上の定義：特別な種類のデータか否か
2. ニューロデータに基づく差別
3. 同意：ニューロデータと取扱いの法的根拠
4. クローズドループ処理のリスク：利用目的の変更、自動処理決定
5. ニューロデータに関する正確性、データ最小化
6. ニューロデータと研究
7. 情報に関する権利（忘れられる権利、データポータビリティ、アクセス権等）

ICO, *ICO tech futures: neurotechnology, Regulatory issues*, <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/tech-horizons-and-ico-tech-futures/ico-tech-futures-neurotechnology/regulatory-issues/>.

AI法の禁止AI

禁止事項	理由（前文）
(a)サブリミナル的・操作的技術	本人が気づかない、あるいは気づいても抵抗できない方法で、自律性・意思決定を歪めるため（前文(29)項）
(b)脆弱性の悪用	年齢・障害・社会経済状況に付け込み、行動を歪めるため（同上）
(c)社会的スコアリング	無関係な社会的文脈での不利益な取扱いにつながり、尊厳・非差別・平等の価値を侵害するため（前文(31)項）
(d)プロファイリングのみに基づく犯罪予測	無罪推定の原則に反し、実際の行動ではなく予測された行動によって人を判断することになるため（前文(42)項）
(e)顔画像の無差別スクレイピング	大量監視の感覚を助長し、プライバシー権の重大な侵害につながるため（前文(43)項）
(f)職場・教育機関での感情推知	科学的信頼性に乏しく差別的な結果を招き得るうえ、職場・教育機関における力関係の不均衡と相まって不利益な取扱いにつながるため（前文(44)項）
(g)生体データからの機微属性の推知	顔や指紋から政治的意見・宗教・性的指向等を推知することが問題であるため（前文(30)項）
(h)公共空間でのリアルタイム遠隔生体識別	常時監視の感覚を与え、集会の自由等の基本権の行使を制約し得るため（前文(32)項）

インターフェイス上の誘導：ダークパターン

- Harry Brignull (2010年～)

- “Deceptive Patterns” (欺瞞的パターン)

- 「何かを購入し又は申し込ませるなど、本人が意図しない事柄を行わせるために用いられるウェブサイト及びアプリの仕掛け」

Harry Brignull et al., *What are deceptive patterns?*, <https://www.deceptive.design/>.

- OECDデジタルエコノミー文書 (2022年)

- 営利的ダークパターンとは、消費者の自律性、意思決定又は選択を覆し又は損なうようなデジタル選択アーキテクチャの要素、特に、オンライン・ユーザー・インターフェイスを用いた事業活動をいう。それらは頻繁に消費者を欺き、強要し又は操り、様々な方法で直接的又は間接的に消費者に不利益をもたらす可能性の高いものであるが、多くの場合、係る不利益を測ることは困難又は不可能であるかもしれない。

OECD, *Dark Commercial Patterns*, OECD Digital Economy Papers, No. 336 (Oct. 26, 2022).

以下「OECD報告書」という。内容は消費者庁の仮訳

(https://www.caa.go.jp/policies/policy/consumer_research/international_affairs/assets/consumer_research/cms209_230327_01.pdf)参照。

ダークパターンの統合的な分類例①

区分	ダークパターンの名称	内容
行為の強制	強制登録	消費者は、登録を強制されるか、だまされて登録が必要だと思い込んでしまう。
	強制的情報開示/プライバシー・ザッカリング	消費者は、だまされて又は強制されて、望ましい範囲を超えて個人情報共有してしまう。
	なりすましスパム/社会的ピラミッド/アドレス帳搾取	ユーザーを操って、ほかのユーザーの情報を引き出す。
	ゲーミフィケーション	サービスの一定の機能が、サービスを繰り返し利用することでしか「獲得」できない。
インターフェイス干渉	隠された情報	重要な情報が、視覚的に不明瞭にされる。
	偽りの階層表示	企業が望む設定や製品のバージョンが、視覚的に目立つようになっている。
	事前選択	企業が望むデフォルトが事前選択されている（例：より高額な選択肢、又はプライバシー保護の度合いが低い選択肢）
	不当参照価格	誤解を招く又は虚偽の参照価格からの割引価格という形で価格が表示される。
	ひっかけ質問	意図的又は露骨な曖昧さ（例：二重否定）
	偽装広告	消費者は、広告だと明確に分からないものをクリックするよう誘導される。
	羞恥心の悪用/感情の翻弄	消費者に特定の選択肢を選ばせるための、感情を利用して人を操るフレーミング

OECD報告書別添B53頁、消費者庁仮訳63～64頁より。

データパターンの統合的な分類例②

執拗な繰り返し	執拗な繰り返し	企業が望むことを行うよう、繰り返し要請する。
妨害	キャンセルやオプトアウト困難/ごきぶり ホイホイ/クリック疲れ/容易さ	商品や企業が望む選択肢への登録・オプトインの容易さと、 キャンセル・オプトアウトの容易さが、釣り合わない。
	(価格) 比較妨害	価格や内容を比較して回ることを阻止する。
	削除不能アカウント	アカウント及び消費者情報が削除できない。
	中間通貨	費用を不明瞭にするために仮想通貨で購入を行わせる。
こっそり (スニー キング)	買物かごにこっそり追加	消費者が追加していない物品が、買物かごに入っている。
	隠れたコスト/ドリップ・プライシング	費用が不明瞭になっている、又は取引の後期段階になって明らか にされる。
	隠れ定期購入/強制的継続	サービスが、予期していない又は望まない形で自動的に更新さ れる。
	おとり商法 (おとり価格を含む)	消費者が、当初宣伝されていた商品又は価格と異なるものを提 案される。
社会的証明	アクティビティメッセージ	ほかの消費者の行動についての表示 (誤解を招く又は虚偽であ ることがある)。
	お客様の声	ほかの消費者による商品に関する発言 (誤解を招く又は虚偽で あることがある。)
緊急性	在庫わずか/大人気メッセージ	商品の数量が限られていることの表示 (誤解を招く又は虚偽で あることがある。)
	カウントダウンタイマー/期間限定メッ セージ	間もなく期限が切れるオファーや割引の表示 (誤解を招く又は 虚偽であることがある。)

OECD報告書別添B53頁、消費者庁仮訳63～64頁より。

プライバシー侵害との関係

- デフォルトでのプライバシー侵害設定（例：事前選択）、プライバシーに関連する選択や情報への関与やオプトアウトを困難にするもの（強制開示、情報の隠蔽、困難なキャンセル）、プライバシー侵害設定を受け入れるように消費者に執拗に求めたり羞恥心を抱かせるもの（ナギング、羞恥心の植え付け）など
- オーストラリアの消費者政策研究センターが実施した調査では、4人に1人が、ダークパターンが原因で望ましい範囲を超えて個人情報共有していることが判明
- 被害規模の評価の困難性、消費者が気付かない場合、サービス利用による有形的かつ即時の短期的利益と、潜在的な長期的プライバシー損失のコストとのトレードオフについての数値的な評価の困難性
- プライバシーを侵害するダークパターンの餌食となる消費者は、無料のオンラインサービスに対してより多くのデータや関心を差し出すことになり、それに相応する質の向上なしに、厚生を低下させる広告の提供を受ける可能性がある。

OECD報告書25頁、消費者庁仮訳29～30頁参照。

欧州データ保護会議(EDPB)の指針

- 「ソーシャルメディアプラットフォームのインターフェイスの欺瞞的設計パターン：認識及び回避の方法に関する3/2022指針」
- 適用されるGDPRの規定
 - データ保護諸原則（第5条）
 - 自由意志に基づく同意、同意の条件（第4条(11)号、第7条）
 - 取扱いの適法性（第6条）
 - 情報社会サービスとの関係における児童の同意（第8条）
 - 透明性ある情報提供、権利行使の容易化（第12条）
 - データ主体へ提供される情報（第13条、第14条）
 - データ主体の諸権利（第3章（第12条～第22条））
 - －異議申立権（第21条）
 - データ保護・バイ・デザイン及びバイ・デフォルト（第25条）

EDPB, *Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, version 2.0 (Adopted on Feb. 14, 2023).

EDPB指針の分類

類型	内容
オーバーロード（情報の過剰提供）	膨大な量の要求、情報、オプション、選択肢等を示すことでユーザーを圧倒して手続を妨害し、ユーザーが特定のデータ取扱方法を変更するのをやめたり、特定のデータ取扱い方法に同意したりするよう仕向ける。
見落とし	ユーザーインターフェイス又はユーザージャーニーを、ユーザーがデータ保護要素の全部又は一部を忘れるか又は見落とすようにデザインする。
スターリング（感情的な操作など）	感情に訴える、視覚的なナッジを用いるなどしてユーザーの選択に影響を及ぼす。
妨害・阻止	ユーザーの行動を困難又は不可能にすることで、自身の情報の取得やデータ管理の過程を妨害する。
フィックル（変則的）	ユーザーインターフェイスのデザインに一貫性がなく不明瞭であるため、ユーザーにとっては、取扱いの性質を理解し、自己のデータに関する適切な選択を行う事が困難であり、[データ保護]管理[ツール]が探しにくい。
レフトインザダーク（隠匿）	ユーザーインターフェイスのデザイン上、データ保護に関する情報や管理ツールが隠され、また、データの取扱い方法や利用可能な管理ツールに関する説明が分かりにくくなっている。

EDPBの前記指針65～71頁、岡田淳、呂佳勸、輪千浩平「ダークパターンに関する一考察（下）
—欧米の規制からの示唆」NBL第1237号（2023年3月）56頁以下参照。

TikTokへの執行事例（2023年）：3億4,500万ユーロの制裁金

- TikTokの新規アカウント（子どものユーザーを含む）はデフォルトで公開設定
- 「everyone」、「anyone」が登録ユーザーか、非登録ユーザーも含むかが曖昧
 - 登録時のポップアップは「Go Private」か「Skip」
 - ✓ 「Skip」を選ぶとデフォルトで公開アカウント
 - ✓ どちらも選ばない場合はデフォルト設定に基づき公開設定へ
 - 動画投稿時のポップアップは「Cancel」か「Post Now」
- 登録時ポップアップの「Skip」の選択肢が画面右側に配置
 - ユーザーに選ばれやすい。
- 公開投稿を選ぶ選択肢が画面右側、太字・濃い色のテキストで表示
 - 動画投稿ポップアップには設定変更の直接リンクがない。
- 親・保護者以外の成人ユーザーが子どもと家族共有設定を設けることができた。

Data Protection Commission, *Irish Data Protection Commission announces €345 million fine of TikTok* (Sep. 15, 2023), <https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok>.
EDPB, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)* (Adopted on Aug. 2, 2023), https://www.edpb.europa.eu/system/files/documents/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf.

デジタルサービス法：ダークパターン禁止規定

- オンラインインターフェースの設計及び構成
 - ✓オンラインPF事業者は、そのサービス利用者を欺き若しくは操る態様、又は、他にそのサービス利用者が任意かつ情報に基づいた意思決定を行う能力を実質的に歪め若しくは損なうような態様で、オンラインインターフェースを設計、構成又は運営してはならない(第25条1項)。
- ダークパターンは、サービス利用者が望まない行動や判断であって、彼らに不利な結果を伴うものに誘導するために用いることができる。（中略）取引に関する決定に誘導したり、変更が極めて困難な初期設定によって、サービス利用者の意思決定を不当に偏らせ、その自律性、意思決定、選択を歪め及び損なうような態様で欺くことなどが含まれる。但し、広告を含め、EU法を遵守した適法な実務自体がダークパターンを構成するわけではない(前文(67)項参照)。

デジタルサービスとサービス利用者の不安等

問題意識

- 想定される「消費者」と実際の「消費者」
- 「不安等」の実体
 - ✓「漏えい」のみではないはず
 - ✓被害を認識しにくく、被害が顕在化した時には手遅れ
- 実際に「不安等」を感じているか。
 - ✓無関心、理解困難
 - ✓デジタルサービスの複雑性
- 技術発展と本人関与の困難性
 - ✓同意や利用停止
- 用語の問題
 - ✓プラットフォーム、マイクロターゲティング、アテンション・エコノミー、フィルター・バブル、エコーチェンバー、プロファイリング、ダークパターン等

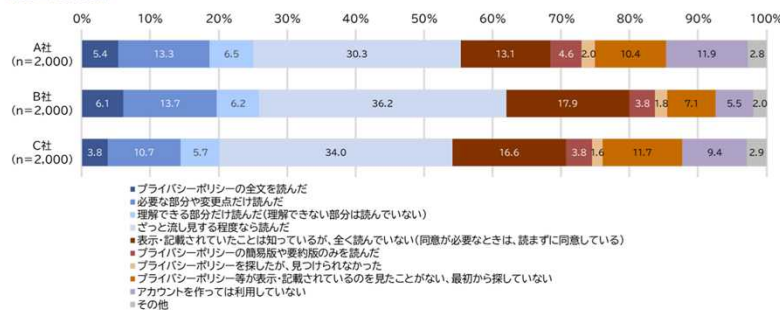
プライバシーポリシー・利用規約の問題

利用しているサービスのプライバシーポリシー確認状況(ログイン)

- プライバシーポリシーの全文を読んでいるのはA～Cのいずれも5%前後で、必要な部分や変更点のみ読んでいるとの回答を合せても2割未満、理解できる部分のみ読んだとの回答を合せても3割に達していない(2割～2.5割程度)という状況であった。
- 「ざっと流し見る程度」が3割強、これに「表示・記載されていたことは知っているが全く読んでいない」を合せるとA～Cのいずれも5割前後で、この辺りが多数派とみられる。
- 「簡易版や概要版のみ読んだ」は4%前後、「探したが見つけれなかった」は2%程度と少ない一方で、「見たことがない・最初から探していない」は1割前後と相対的にやや多めだった。

利用しているサービスのプライバシーポリシー確認状況(ログイン)

Q. ※アカウントを作りログインして利用しているサービスについてお答えください。あなたは、利用しているサービスのプライバシーポリシーを読んでいますか。最も当てはまるものをお選びください。(SA)

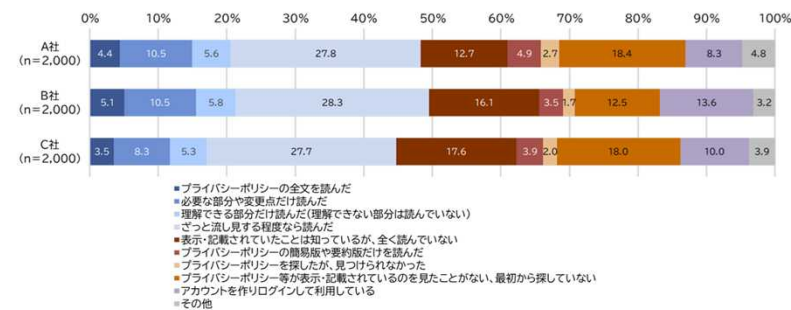


利用しているサービスのプライバシーポリシー確認状況(アカウント非保有or非ログイン)

- プライバシーポリシーの全文を読んでいるのは、A～Cのいずれも5%前後で、必要な部分や変更点のみ読んでいるとの回答を合せても1割強～1.5割、理解できる部分のみ読んだとの回答を合せても2割前後であった。それぞれ、ログインして利用しているサービスの場合よりもやや少ない。
- 「ざっと流し見る程度」が3割弱、「表示・記載されていたことは知っているが全く読んでいない」を合せると4割強で、やはりこの辺りが多数派とみられるが、これもログインして利用しているサービスよりもやや少ない結果となった。
- 「簡易版や概要版のみ読んだ」は4%～5%程度、「探したが見つけれなかった」は2%～3%程度と少ない一方、「見たことがない・最初から探していない」は1割強～2割弱とやや多めだった。なおこれらの比率はログインして利用しているサービスよりも若干高めだった。

利用しているサービスのプライバシーポリシー確認状況(アカウント非保有or非ログイン)

Q. ※アカウントを作らないで又はログインしないで利用しているサービスについてお答えください。あなたは、利用しているサービスのプライバシーポリシーを読んでいますか。最も当てはまるものをお選びください。(SA)



サービスを利用している企業に基づき3つの調査群を設定した調査結果（回答者数は各2,000名）ログイン・非ログインの双方においてプライバシーポリシーは読まれていない状況。

三菱総合研究所「プライバシーポリシーに関する利用者アンケート調査結果」総務省ICTサービスの利用環境の整備に関する研究会資料24-2利用者情報に関するワーキンググループ（第24回）（2025年5月19日）

(https://www.soumu.go.jp/main_content/001009598.pdf) 6～7頁。

1人の消費者として

- プラポリの理解・同意、トラッキングの許諾画面
- テクノロジーへの関わり方
- Cookieの利用
- 利用するブラウザ、アプリ、生成AIサービス
- その他自力で保護できる範囲

定型文。うんざりだ。オンライン上の標準規約を事実上誰も読まないことはもはや自明の理となっている。最近の研究によれば、利用規約を読むのは、電子商取引ウェブサイトのユーザーのうち、1000人に1人未満にとどまる。連邦最高裁首席判事のジョン・ロバーツ（John Roberts）でさえ、ウェブサイトの小さな活字を読まないことを認めている。しかし、利用規約は日常的に執行されている。*原著は2018年に出版

WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018).
山本龍彦、成原慧、寺田麻佑、松尾剛行訳『プライバシーの設計図 法はいかにテクノロジーのデザインに関わるべきか』（勁草書房、2026年）262頁。

スマートグラスとプライバシー①

- G7データ保護・プライバシー当局ラウンドテーブル（2026年6月）
- 医療、コンピュータサイエンス、産業、教育、個人系用途など様々に利用可能
- プライバシー上の懸念
 - ✓ 比較的低コスト、ほぼあらゆる環境（私的空間、公共の場、職場、学校など）において、気づかれることなく動画や画像が撮影可能
 - ✓ 目的外利用、有効な同意への疑問（非ユーザーを含む）、機微データの収集、権利行使の困難性
 - ✓ 同意が一般利用規約に組み込まれている場合、デバイス利用の必須前提条件として提示されている場合の同意、ユーザー以外の者が写り込んだ場合の同意
 - ✓ 生のセンサーデータによって、気分、健康状態、運転習慣等ユーザーの機微データを広範に推測する可能性
 - ✓ セキュリティリスク

CNIL, *Smart glasses, Compendium of G7 data protection and privacy authorities approaches*,
https://www.cnil.fr/sites/default/files/2026-06/g7_dpas_compendium_of_approches_on_smart_glasses.pdf.

スマートグラスとプライバシー②

- PPC（日本）、ICO（英国）、OPC（カナダ）、EDPS（EU）、CNIL（フランス）がそれぞれの立場を表明
- 共通認識
 - ✓透明性
 - ✓有効な同意の取得
 - ✓データ最小化
 - ✓プライバシー・バイ・デザイン

CNIL, *Smart glasses, Compendium of G7 data protection and privacy authorities approaches*,
https://www.cnil.fr/sites/default/files/2026-06/g7_dpas_compendium_of_approches_on_smart_glasses.pdf.

透明性と同意の有効性

スクレイピングとプライバシー

The Great Scrape: The Clash Between Scraping and Privacy

Daniel J. Solove* and Woodrow Hartzog**

Artificial intelligence (AI) systems depend on massive quantities of data, often gathered by “scraping”—the automated extraction of large amounts of data from the internet. A great deal of scraped data contains people’s personal information. This personal data provides the grist for AI tools such as facial recognition, deep fakes, and generative AI. Although scraping enables web searching, archiving of records, and meaningful scientific research, scraping for AI can also be objectionable and even harmful to individuals and society.

Organizations are scraping at an escalating pace and scale, even though many privacy laws are seemingly incongruous with the practice. In this Article, we contend that scraping must undergo a serious reckoning with privacy law. Scraping violates nearly all of the key principles of privacy laws, including fairness, individual rights and control, transparency, consent, purpose specification and secondary use restrictions, data minimization, onward transfer, and data security. Scraping ignores the data protection laws built around these requirements.

Scraping has evaded a reckoning with privacy law largely because scrapers act as if all publicly available data were free for the taking. But the public availability of scraped data shouldn’t give scrapers a free pass. Privacy law regularly protects publicly available data, and privacy principles are implicated even when personal data is accessible to others.

DOI: <https://doi.org/10.15779/Z38H96ZF9D>

Copyright © 2025 Daniel J. Solove and Woodrow Hartzog

* Eugene L. and Barbara A. Benard Professor of Intellectual Property and Technology Law, George Washington University Law School. A big thank you to our research assistants Allison Chesky, Michael Lavine, Kaitlyn Milane, Vaishali Nambiar, Bradley Neal, Rose Patton, and Philip Yu. The authors would also like to thank Steve Belorou, Guacimundo Malgren, Andy Sellars, Jessica Silbey, and Jason Schultz and the participants of the 2024 Privacy Law Scholars Conference for their helpful comments.

** Professor of Law, Boston University School of Law.

1521

- スクレイピングの広がり
 - ✓ Web検索、アーカイブ化、生成AI、学術研究目的での利用
 - ✓ AIによる問題の顕在化
- プライバシー諸原則違反
- 「公開情報」のプライバシー保護
- 「公共の利益」を軸に据えたプライバシーの再考
 - ✓ スクレイピング = 監視
 - ✓ データセキュリティの義務としてスクレイピングを位置づけ
 - ✓ 「公共の利益」のためのスクレイピングを許容し、有害又は危険なスクレイピングを制限

Daniel J. Solove and Woodrow Hartzog, *The Great Scrape: The Clash Between Scraping and Privacy*, 113 CAL. L. REV. 1521 (2025).

スクレイピングの広がり

- スクレイピング＝データの刈り取り
 - ✓web crawlers, spiders, or bots
 - ✓SNS、フィットネス、銀行業、ホスピタリティなど様々なサービスから収集
- robots.txtを用いてクロール可否をボットに対して指示
 - ✓従う義務はないが機能してきた仕組み
- AIの台頭によるスクレイピングの増加
 - ✓Clearview AIによる30億枚を超える画像のスクレイピング
 - ✓生成AIブームの火付け役であるChatGPTやDall-Eの広がり
- 前例のない規模でのスクレイピングの展開ー「スクレイピング戦争」
- 検索エンジンのためのクロールとスクレイピング
- スクレイピングを防止する技術は存在するがいたちごっこ

Solove and Hartzog, *The Great Scrape*, 1523-1533.

法的対処の難しさ

- スクレイピングに対する訴訟提起
 - ✓ 知財、価格データ、個人データなど
 - ✓ スクレイピングの適法性については結論出ず
- 特徴
 1. 殆どの訴訟は企業同士の争い
 - 個人は蚊帳の外
 2. 決定的な判断は下されていない
 - スクレイパーが勝つ場合もあればスクレイピーが勝つ場合も
 3. 殆どの請求はプライバシーではなく、財産や契約に関するもの
 - プライバシーは無視されるか考慮されず

Solove and Hartzog, *The Great Scrape*, 1533-1536.

スクレイピングとFIPPs (Fair Information Practice Principles) ①

1. 公正性 ×
← 秘密裡に行われ有害
2. 個人の権利及びコントロール ×
← 文脈による人々のプライバシーへの期待を奪い取ってしまう。
3. 透明性 ×
← スクレイパーは透明性を完全に無視、一般的な通知を行っても実際上は意味がない。
4. 同意 ×
← 一旦データがスクレイパーの手に渡ってしまえば、個人は同意するか否かを選択する能力を失ってしまう。そもそもスクレイピングが行われていることを知らない。

Solove and Hartzog, *The Great Scrape*, 1549-1558.

スクレイピングとFIPPs ②

5. 目的の特定及び二次利用の制限×

←スクレイピングは、目的を特定しないまま、無差別にデータを収集する行為

6. データ最小化×

←スクレイピングは、何らの制限や保存期間の定めもなく個人データを収集・保存する行為

7. 再移転×

←スクレイピングは、いかなる契約、制限、同意もなく第三者がデータを取得できるようにする行為である。

8. データセキュリティ×

←スクレイピングは、第三者が単にデータを「つかみ取る」行為であって、いかなるスクレイパーでも容易にデータを取得できるのであれば、データセキュリティは無意味

Solove and Hartzog, *The Great Scrape*, 1549-1558.

包括的理論の必要性①

- 主張の要点

- ① スクレイピングを「監視」の一形態とし、データセキュリティ侵害として捉える。

- 「監視」：個人の詳細情報を収集、体系的に実施、ルーティン化、人々に影響を与え、管理し、保護し、又は誘導するために実施

- 「データセキュリティ侵害」：プライバシー法の管轄下に置くと問題を複雑化させる。

- 人々の個人データを託された主体は、スクレイパーから情報を守るために、法的・組織的・技術的な多様な措置を講じる。
 - 第三者によるスクレイピングに対して合理的な保護措置を講じないことは、データを不適切に第三者へ共有することと同視。

Solove and Hartzog, *The Great Scrape*, 1567-1575.

包括的理論の必要性②

- 主張の要点（続き）

- ② 「公共の利益」に叶う場合の例外

- ✓ 全面禁止にすべきではない。

- 甚大な経済的・社会的コスト、競争の阻害（巨大PFを有利に）、研究プロジェクトや報道、AIモデルを歪める可能性（アメリカでは認められ、EUでは禁止された場合）

- 同意アプローチ

- 同意に関するプライバシー法の既存の欠陥を、さらに悪化
 - 用途が特定されず、無制限に行われる膨大なデータ収集・利用についての同意は無意味

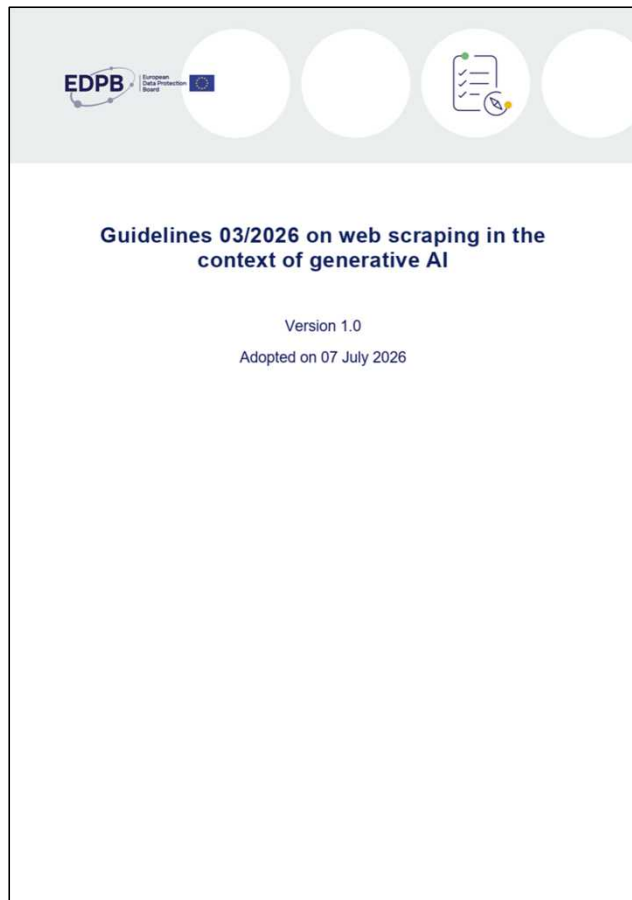
Solove and Hartzog, *The Great Scrape*, 1574-1577.

スクレイピングを許容する条件

1. スクレイピングを許容する前提として、公共の利益に焦点を当てた正当な理由を立証する義務－スクレイピングは「権利」ではなく「特権」
 - ✓公共の利益を満たさないスクレイピングは禁止すべき
 - ✓公共の利益に基づくスクレイピングの枠組みを作るべき
 - ✓利益を上げることは排除しないが、企業だけの利益を超える形での正当化が必要
2. スクレイピングが安全に行われ、搾取を防ぎ、目的が公の利益から過度に逸脱しないことを保障するための実体的保護措置
3. 公平性、十分な代表性、そして意思決定における主体性を確保するための手続的保護措置

Solove and Hartzog, *The Great Scrape*, 1577-1583.

EDPB（欧州データ保護会議）の指針



- 生成系AIの学習を目的に、インターネット上のソースからデータをスクレイピングする場合に焦点を当てている。
- 組織が自ら組織外のインターネット上の情報源からデータをスクレイピングする場合、第三者に委託してスクレイピングを行う場合が含まれる。民間企業によるウェブスクレイピングに限定。
- ウェブスクレイピングとは、自動化ツールを用いて、公開のウェブサービス（例えば、公開レジストリ、オープンデータポータル、報道機関、ソーシャルメディア、ディスカッションフォーラム、個人のウェブサイト（「ブログ」）など）から情報を抽出・保存する、一般的に用いられる技術をいう。これらのウェブサイトの多くには、個人データが含まれている可能性が高い。

EDPB, *Guidelines 03/2026 on web scraping in the context of generative AI*, version 1.0 (Adopted on Jul. 7, 2026).

データ最小化①

- 管理者は、当該処理の目的にとって必要な個人データのみを収集しなければならない。
- 大量データのスクレイピングには大きな課題があるものの、データ最小化の原則は、大量のデータを用いてAIモデル又はAIシステムを学習させることを禁止するものではない。管理者は不要なデータを収集しないよう事前評価を実施すべき。
- 収集前に講じるべき措置
 - ✓合成データの活用検討
 - ✓的確な収集基準の設定
 - ✓データマッピング・インベントリの実施
 - ✓不要な種類のデータのフィルタ除外（銀行取引データ、位置情報等）
 - ✓特定カテゴリのサイトの除外（未成年者利用サイト等）
 - ✓スクレイピング拒否サイトの除外（robots.txt、ai.txt、CAPTCHA対応）

EDPB, *Guidelines 03/2026*, paras. 35-37.

データ最小化②

- 収集過程、収集後に講じるべき措置
 - ✓構文ベースのフィルタリング（正規表現等で、電話番号・社会保障番号等の形式的パターンを検出・除外）
 - ✓実データの合成データへの置き換え（テスト・分析・学習目的、実行可能な範囲で）
 - ✓個人データの匿名化又は仮名化（実行可能な範囲で）

EDPB, *Guidelines 03/2026*, para. 38.

適法性の根拠①

- 同意は困難
- 正当な利益 (legitimate interest)
 1. 正当な利益が存在すること
 - ✓ 会話エージェント開発・不正検知・脅威検知等
 - ✓ モデルの用途が具体的に定まっていない場合は、モデル開発の目的を示すことが推奨
 - 営利的か否か、科学研究を目的とするか否か、組織にとって内部的か外部的吗
 2. 必要性
 - ✓ ①処理は追求する目的を可能にするものであるか、②同等かつ効果的で、より侵襲性の低い代替手段があるか。
 - ✓ 収集基準の絞り込み + 仮名化・合成データによる代替可能性。
 3. 利益衡量テスト（次頁）

EDPB, *Guidelines 03/2026*, paras. 44-52.

適法性の根拠②

- データ主体側の利益、基本的権利及び自由

- ✓自己決定の利益、自己の個人データに対するコントロールを維持する利益等
 - 特定の目的のためにサイト上で公開されたデータが、後にデータ主体の意思に反し、又はその認識く、生成AIの学習のためにスクレイプされ、処理される事態
- ✓表現の自由（大規模・無差別的データ収集による「萎縮効果」を通じた自己検閲のリスク）
 - AIモデルがウェブ検索ツールと連動し、匿名表現を意図していたデータ主体を特定するためにAIモデルが利用され得る
 - GDPRの定めるプロファイリングのためにAIモデルが利用され得る
- ✓尊厳への権利（ディープフェイク（画像・動画・音声）生成によるデータ主体の利益・権利・自由への影響の増大）

EDPB, *Guidelines 03/2026*, paras. 54.

適法性の根拠③

- 処理がデータ主体に与える影響
 - ✓ 処理される個人データの性質
 - 特別な種類の個人データ、位置データ、金融データ、子どものデータ
 - これらの処理はデータ主体に重大な帰結をもたらし得るため、侵害の程度の評価において考慮すべき（特に子どものデータの場合）
 - センシティブ・プライベートな性質のデータ
 - データ主体への悪影響の可能性の増大
 - 利益衡量テストにおける重みづけ
 - ✓ 処理の文脈
 - 開発段階：大量のデータ、大量のデータ主体、無差別収集
 - 対象ウェブサイトが多いほど、プライバシー・個人データ保護の基本権への干渉が増大

EDPB, *Guidelines 03/2026*, paras. 55-58.

適法性の根拠④

- データ主体にもたらす結果

- ✓問題点

- 第三者によるスクレイピングの場合、データ主体が権利行使・異議申立てをするのは実務上困難
 - 認識していたとしても、スクレイパーがデータに到達できないようにすることは困難
 - 現在の技術水準に照らして、学習後は、モデルから個人データを容易に削除できない

- ✓データ主体の予見可能性

- 考慮事項

- ソースとなるウェブサイトの性質
 - スクレイピングの対象であるウェブサイトの課す制限
 - データ主体と管理者の関係
 - データ主体の属性（未成年、公人その他の立場）

EDPB, *Guidelines 03/2026*, paras. 59-64.

適法性の根拠⑤

✓緩和措置の役割

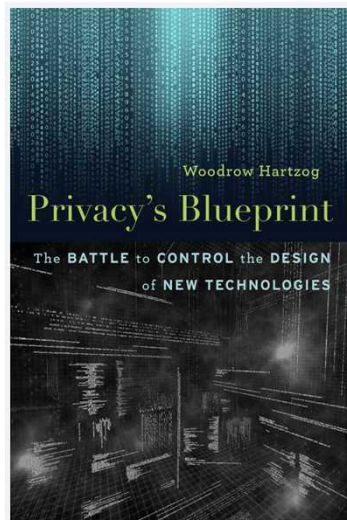
➤技術的措置・組織的措置の例（事案毎の検討を要する）

- 特定の者・集団にリスクをもたらすデータの公表物からの除外
- 特定の種類のデータ・ソースをデフォルトで除外
- 特定の個人データを除外（ログインを要するもの等）
- その他期間制限など
- 透明性（対象ウェブサイトのリスト公開等）
- 個人の権利行使（事前の異議申立権等）
- 不要な個人データの早期の削除、匿名化
- 仮名化データへの置き換え
- その他

EDPB, *Guidelines 03/2026*, paras. 65-66.

考え得る対応策

プライバシーの設計図



(<https://www.hup.harvard.edu/books/9780674976009>)



(<https://www.keisoshibo.co.jp/book/b10158529.html>)

目次

序章－プライバシーの行方をデザインする

第1編 プライバシー法においてデザインを真剣に受け止めなければならない理由

第1章 なぜデザインがすべてなのか

第2章 プライバシー法のデザインの欠落

第2編 プライバシー法のデザインアジェンダ

第3章 デザインにおけるプライバシーの価値

第4章 デザインのための境界の設定

第5章 プライバシーデザインのためのツールキット

第3編 プライバシーの設計図を適用する

第6章 ソーシャルメディア

第7章 かくれんぼテクノロジー

第8章 IoT

結論

日本語版序文の抜粋

- （石井注：2018年の原著出版からの時の経過を経ても）本書において展開した原理と議論はますます正しさを増しているのである。Cambridge Analyticaの大規模な個人情報の大量抜き出しを促したのはFacebookのデザインなのである。ユーザーがその暴露に「同意した」と論じるにあたっても、Facebookはそのシステムのデザインに依拠した。いかにプライバシーを保護しながら「コロナ」感染追跡システムを構築するかに関する論争を政府と産業界が行う際において、社会の関心を惹きつけたのは、感染監視システムのデザインであった。私たちが今日まで継続するさまざまな監視方法に慣れていくにつれ、感染監視ツールのデザイン上の選択が徐々に当たり前のものとなった。「ディープフェイク」を創出する新しいAIツールのアフォーダンスについて論争を行う際、実際に私たちが行っているのは、当該表現を可能とするデザイン上の選択に関する議論である。しかし同時にハラスメントや偽情報についても「議論している」。いつもどおり、デザインこそがすべてである。

山本、成原、寺田、松尾・前掲『プライバシーの設計図』i頁。

序章

- デザイン（人工物、ハードウェア、ソフトウェア）は遍在し、力であり、政治的である。
 - ✓情報技術において価値中立的なものは存在しない。
- プライバシーの設計図（プライバシー法のデザインアジェンダ）をデザインに適用する。
- プライバシーの価値
 - ✓信頼、目立たなさ、自律
- 立法者に対して設けるべき境界の提案
 - ✓製品安全法及び消費者保護法を通じて、欺瞞的デザイン、濫用的デザイン、危険なデザインを抑制する基準の設定
- 立法者及び裁判所がより良いデザインを促すために利用可能なツールの検討
 - *プライバシー・バイ・デザインとは異なる。

山本、成原、寺田、松尾・前掲『プライバシーの設計図』1～20頁。

第3編 プライバシーの設計図の適用①

- SNS

- ✓プライバシーポリシーは実際は反プライバシーポリシー
- ✓UIのデザインをオンライン契約の一部とすべき
 - 悪意のあるインターフェイスや欺瞞的インターフェイスを用いた契約を無効にする。
- ✓過剰な露出に対しては、データ保管を最小化するシステムデザイン、データの収集・保管・利用に関するリスク評価、UIのデザインを個人データの収集・処理と同様に取り扱う等

- かくれんぼテクノロジー

- ✓カメラ、ブラウザ、顔認識技術、ナンバープレート読み取り装置、ドローン、追跡ビーコン、スパイウェア等
 - PETsの利用可能性、データ最小化原則の採用等

山本、成原、寺田、松尾・前掲『プライバシーの設計図』265～267頁、295～327頁。

第3編 プライバシーの設計図の適用②

• IoT

- ✓IoT固有の側面：接続可能性のせいで、もはやインターネットから隔離された生活を行うという選択肢さえも奪われる。
- ✓プライバシーの設計図のIoTへの適用
 - IoTに対する同意をやめる
 - セキュリティ・バイ・デフォルト、バイ・デザイン
 - IoTセキュリティへの研究支援
 - 合理的データセキュリティの義務化
 - 強制終了スイッチ
 - IoT化を例外に

山本、成原、寺田、松尾・前掲『プライバシーの設計図』338～355頁。

おわりに：検討事項

- 自力で守ることの困難性
- プライバシーの聖域（禁止領域）の検討
- データ最小化、プライバシー・バイ・デザイン、リスク評価の重視
- 同意の有効性が残る部分の検討
 - ✓ デジタルサービスの利用に伴う同意とそれ以外
- テクノロジーのデザインに着目したプライバシー保護
- 公益性を伴う利用の検討
- ユーザー啓発について
 - ✓ 意識の高い層か否か。