総務省「デジタル空間における情報流通の健全性確保の
在り方に関する検討会」第6回（2024年1月19日）

資料6−2−1

偽・誤情報と
プライバシー・個人情報保護

中央大学国際情報学部
石井　夏生利

プライバシー侵害の類型

- いわゆるProsserの4類型
  - ➢不法侵入、私的事実の公開、公衆の誤認、盗用
  - ➢4類型は別個のものであり、異なる要素に基づく。
  - ➢一身専属的な権利、譲渡不可、死者には認められない、個人にのみ認められる権利であって、法人には認められない等

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960)

- Daniel Solove教授による分類
  - ➢①情報収集（監視、尋問）、②情報処理（集約、同定、非セキュリティ状態、二次的利用、排除）、③情報拡散（守秘義務関係破壊、開示、暴露、アクセス可能性の増大、脅迫、盗用、歪曲）、④侵襲（侵入、意思決定への介入）

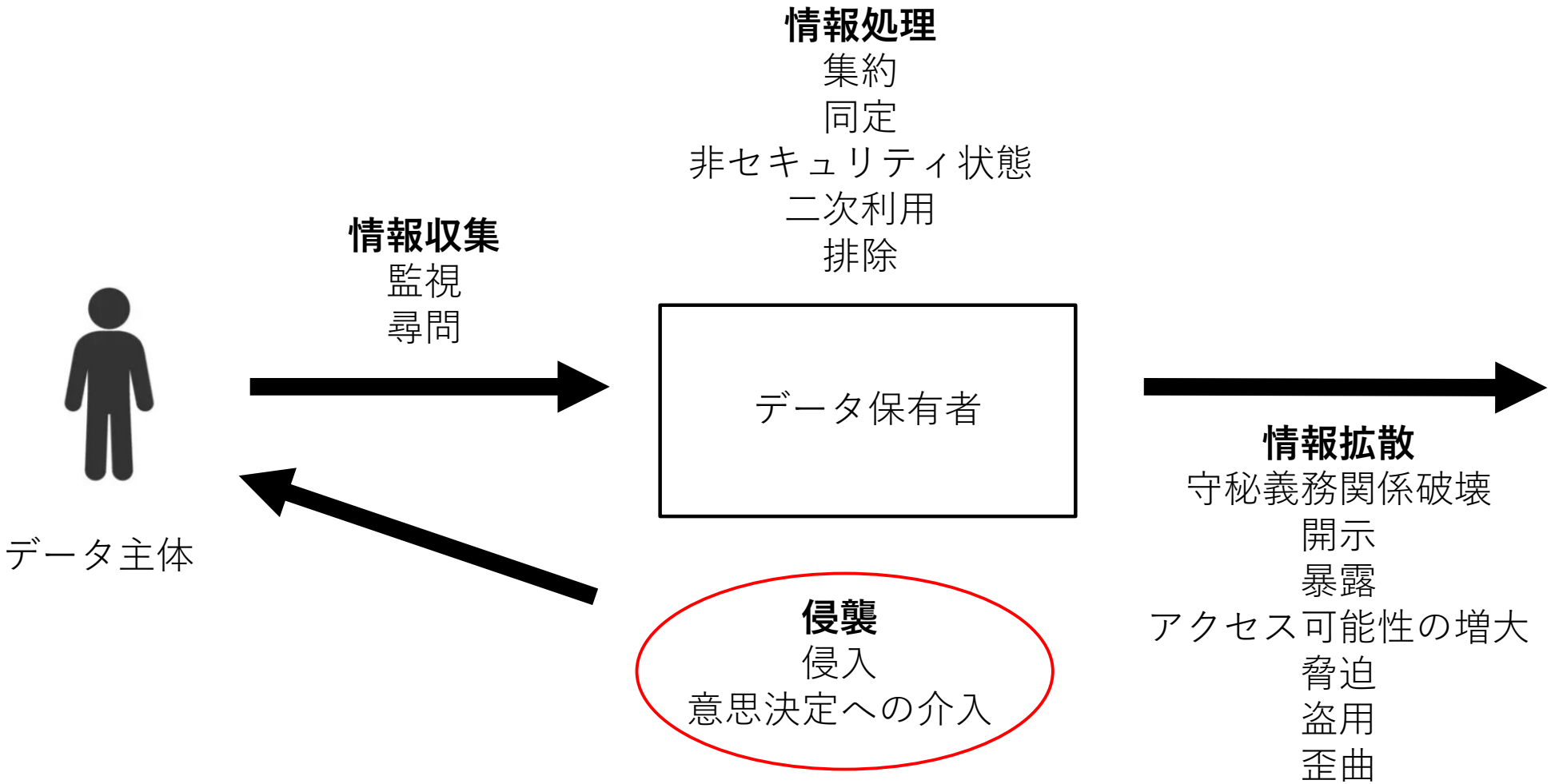
DANIEL J, SOLOVE, UNDERSTANDING PRIVACY (2010).
ダニエル・Ｊ・ソローブ著・大谷卓史訳『プライバシーの新理論－概念と法の再考』（みすず書房、2013年）

侵襲

- 「侵襲は、個人に対する直接の侵害に関わる。侵襲は、個人から離れていく活動ではなく、個人へと向かってくる活動で、必ずしも情報にかかわっているとは限らない。」
- 「侵襲は、ほかのグループとは違って、個人情報に必ずしもかかわらない（ただし、多くの事例では関係している）。（中略）意思決定への介入（Decisional Interference）は、データ主体自身にかかわるプライベートな事柄についての意思決定に立ち入ることを意味する。」

前掲・『プライバシーの新理論』145頁、146～147頁

類型モデル(Daniel Solove教授)



前掲『プライバシーの新理論』145頁、前掲『プライバシーなんていらない！？』240頁をもとに作成
（赤枠は筆者が付記）

プライバシーが浸食される過程

- 「多くの場合、単一のとてつもない行為ではなく、ゆったりとした時間の中における連続する比較的小さな行為の蓄積により、プライバシーは脅かされる。この点で、プライバシー問題は、異なる行為者による一連の小さな行為を通じて長い時間をかけて生じるある種の環境に対する害悪に類似する。社会は大規模な流出油事故には反応しがちだが、大勢の異なる行為者による緩やかな汚染は、しばしばいっそう悪い問題を引き起こす。」
- 「プライバシーが一気に失われることは、めったにない。プライバシーはしばしば時間をかけて浸食され、ほとんど感知できないうちにちょっとずつ溶けていき、どれくらいそれが失われたかは最後になってようやく分かる。」

DANIEL J, SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2013).
ダニエル・J・ソロブ著・大島義則ほか訳『プライバシーなんていらない！？』（勁草書房、2017年）34頁

社会的価値としてのプライバシー

- 「プライバシーは単に社会のルールや規範に一定の制約を加えるだけではない。そうではなく、プライバシーは、礼節を促進する社会の企てを構成している。社会は、共同体の秩序を守らせる手段として、プライバシーを保護する。プライバシーは社会的利益に対抗する個人の切り札ではなく、社会自身の規範と価値に基づく個人の保護である。プライバシーは単純に社会的コントロールから個人を解放する手段ではない。それ自体が社会の規範に由来する社会的コントロールの一形式である。それは社会に対する外的な制約ではなく、社会の内的次元に存在する。それゆえ、プライバシーは、社会的価値を有する。法が個人を保護するとき、個人的理由だけでなく社会的理由でそうする。したがって、プライバシーは、より大きな社会の善に対抗する個人の権利として評価されるべきではない。プライバシー問題は天秤の両側にある社会的利益の衡量を含んでいる。」

前掲『プライバシーなんていらない！？』55～56頁

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/.

- ダークパターンの問題点
  - 消費者の自律性の侵害
  - 民主主義及び表現の自由への脅威など、消費者の領域を超えた集団的損害の可能性
  - 消費者が気付きにくいという問題
  - 脆弱な消費者：高齢者、児童、教育水準の低い者など

OECD, *Dark Commercial Patterns*, OECD Digital Economy Papers, No. 336 (Oct. 26, 2022), https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm.

個人の認知領域の保護と個人情報・プライバシー保護

- 気付いた時には既に浸食
- 意思決定への介入（侵襲）によるプライバシー侵害
- 侵害に気付きにくい
- 1人の権利の侵害が集積することによる社会全体への影響

- 個人の認知領域の保護と個人情報・プライバシー保護の間に共通性を見いだすことができるのではないか。
- 偽誤情報自体には個人情報が含まれるとは限らないものの、個人の判断を歪める行為（侵襲）をプライバシー侵害と捉え、それによる社会への弊害をプライバシー侵害の側面から捉えることはできるのではないか。
- 本人は偽誤情報に晒されていることに気付きにくく、歪んだ判断が集積することにより、環境汚染に類する被害が情報環境においても生じるのではないか。

対策の検討

- ハードロー、共同規制、ソフトロー
- 偽・誤情報問題を検討する際の視点
  - ➢透明性、リスク評価の重要性（生貝構成員資料）
    - ✓個人情報保護法制のPIAに関する取組やマイナンバー法における特定個人情報保護評価等
- 総務省「プラットフォームサービスに関する研究会　第二次とりまとめ」
  - ➢「総務省は、違法・有害情報となる偽情報に関するプラットフォーム事業者の取組状況について、（中略）偽情報への対応に関する透明性・アカウンタビリティの確保に向けて、行動規範の策定及び遵守の求めや法的枠組みの導入等の行政からの一定の関与を具体的に検討することが必要である。」（同取りまとめ97頁）（森構成員資料）

⬇

ベースとなる基本法（目的、基本理念、基本方針等）の必要性

1980年OECDプライバシー・ガイドライン

- 第1原則：収集制限の原則(Collection Limitation Principle)
- 第2原則：データ内容の原則(Data Quality Principle)
  - 個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。
- 第3原則：目的明確化の原則(Purpose Specification Principle)
- 第4原則：利用制限の原則(Use Limitation Principle)
- 第5原則：安全保護の原則(Security Safeguards Principle)
- 第6原則：公開の原則(Openness Principle)
- 第7原則：個人参加の原則(Individual Participation Principle)
- 第8原則：責任の原則(Accountability Principle)

OECD信頼性のあるガバメントアクセスに関する高次原則

法的根拠、正当な目的、承認、データの取扱い、透明性、監督、救済

我々は、民主的価値、法の支配、プライバシー及びその他の人権と自由の保護を堅持しつつ、犯罪行為及び公の秩序と国家の安全に対する脅威を防止し、探知し及びこれらに対処することにより、国民の安全を保護するというすべての国における主権的義務と責任を認識する。

個人情報保護委員会「民間部門が保有する個人データに対するガバメントアクセスに関する宣言（仮訳）」（https://www.ppc.go.jp/files/pdf/government_access_jp.pdf）

この度、信頼性のあるガバメントアクセスに関する高次原則に係る閣僚宣言が採択されたこと は、法の支配等の民主主義の根幹に関わる共通の価値を体現し、信頼できるデータの越境移転に不可欠な要素としての個人情報の保護を図るものとして極めて重要なことであると考えている。今後とも我が国は DFFT を推進するためにこれらの取組にも献身的に貢献して参りたい。

個人情報保護委員会「OECDデジタル経済政策委員会（CDEP）閣僚会合 結果報告」資料2-1（2022年12月21日）（https://www.ppc.go.jp/files/pdf/221221_shiryou-2-1.pdf）

本検討会における主な検討事項

① デジタル空間を活用したサービスの普及・情報通信技術の進展等の状況

② デジタル空間における情報流通を巡る新たな課題と各ステークホルダーによる対応状況

③ 今後の対応にあたっての基本的な考え方

（例）基本理念：信頼性のある自由な情報流通、表現の自由、知る権利、青少年を含む利用者保護、デジタルシティズンシップ など

各ステークホルダーの役割：デジタルプラットフォーム事業者、生成AI事業者、仮想空間関係事業者、通信・放送事業者、利用者 など

④ デジタル空間における情報流通の健全性確保に向けた具体的な方策

本検討会第1回事務局資料1-3
(https://www.soumu.go.jp/main_content/000910437.pdf)（2023年11月7日）

個人情報保護法の「基本法」部分

- 個人情報保護法制の基本法部分（第1章～第3章）と一般法部分（第4章以下）
  - 目的、基本理念、基本方針等

（基本理念）
第3条　個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに鑑み、その適正な取扱いが図られなければならない。

個人情報の保護に関する基本方針

１　個人情報の保護に関する施策の推進に関する基本的な方向

（2）法の基本理念と制度の考え方

法第3条は、個人情報がプライバシーを含む個人の人格と密接な関連を有するものであり、個人が「個人として尊重される」ことを定めた憲法第13条の下、慎重に取り扱われるべきことを示すとともに、個人情報を取り扱う者は、その目的や態様を問わず、このような個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならないとの基本理念を示している。

個人情報保護委員会「個人情報の保護に関する基本方針」（2004年4月2日閣議決定・2022年4月1日最終変更）（https://www.ppc.go.jp/personalinfo/legal/fundamental_policy/）

法の基本理念と制度の考え方

① 個人情報の保護と有用性への配慮

② 法の正しい理解を促進するための取組

③ 各主体の自律的な取組と連携・協力

④ データガバナンス体制の構築

- ③の自律的な取組に当たり（中略）透明性と信頼性の確保が特に重要である。
- 各主体においては（中略）データの内容や性質、量や範囲の必要十分性、データの流れ、データの取扱いに関わる者の範囲、データの利用目的、安全管理レベル等の事前評価のため、PIA（個人情報保護評価又はプライバシー影響評価）の手法を用いることや（中略）これらによるデータガバナンスの体制を構築することが重要である。

⑤ 個人におけるデータリテラシーの向上

個人情報保護委員会ウェブサイト・前掲「個人情報の保護の基本方針」より

1　個人情報の保護に関する施策の推進に関する基本的な方向
(1) 個人情報等をめぐる状況

- これに対し、顔識別・認証技術、AI等の高度なデジタル技術を活用して行われる個人の行動、政治的立場、経済状況、趣味・嗜好等に関する高精度な推定（いわゆるプロファイリング）、さらには、大量の個人情報等を取り扱う民間事業者等の出現等が認められるところであり、ひとたび個人情報等の不適正な利用等に及んだ場合には個人の権利利益に対する大きな侵害につながるリスクが高まっている。そして、自分の個人情報等が悪用されるのではないか、これまで以上に十分な注意を払って取り扱ってほしいなどの個人の不安感が引き続き高まっている。

個人情報保護委員会ウェブサイト・前掲「個人情報の保護の基本方針」より

利用目的の特定に関する解釈

- 個人情報の利用目的を「できる限り特定」
  - ➢また、一連の個人情報の取扱いの中で、本人が合理的に予測・想定できないような個人 情報の取扱いを行う場合には、かかる取扱いを行うことを含めて、利用目的を特定する必 要があります。例えば、いわゆる「プロファイリング」といった、本人に関する行動・関心等の情報を分析する処理を行う場合には、分析結果をどのような目的で利用するかのみならず、前提として、かかる分析処理を行うことを含めて、利用目的を特定する必要が あります。具体的には、以下のような事例においては、分析処理を行うことを含めて、利用目的を特定する必要があります。

    事例1）ウェブサイトの閲覧履歴や購買履歴等の情報を分析して、本人の趣味・嗜好に応じた広告を配信する場合

    事例2）行動履歴等の情報を分析して信用スコアを算出し、当該スコアを第三者へ提供 する場合

個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」に関するQ&A（2023年12月25日更新）Q2-1（https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q2-1）

個人情報の不適正利用

（不適正な利用の禁止）

個人情報保護法第19条「個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。」

個人情報保護法ガイドライン（通則編）3-2の例（抜粋）
事例5）採用選考を通じて個人情報を取得した事業者が、性別、国籍等の特定の属性のみにより、正当な理由なく本人に対する違法な差別的取扱いを行うために、個人情報を利用する場合
(https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-2)

- ケンブリッジアナリティカ事件の例に見られるように、FacebookのDBから取得した情報から、個人に関する一定の傾向を割り出してターゲティング広告を行い、対立を煽るような議論を誘発し、最終的に社会を分断させてしまうリスクへの対応の必要性（社会を分断させるリスクがあるという点では偽誤情報と共通する問題性）

まとめ

- 個人の認知領域の保護と個人情報・プライバシー保護の共通性
- 個人の判断を歪める行為（侵襲）とプライバシー侵害
- 環境汚染に類する被害への対応
- ベースとなる基本法の必要性
  - 目的、基本理念、基本方針等
- 民主的価値、法の支配、プライバシーの関わり
- 諸原則の検討
- データガバナンス：透明性、リスク評価の重要性
  - PIA等
- プロファイリングのもたらす社会的リスク