

ダークパターン及び プロファイリングについて

— EUの動向を中心に —

MRI 三菱総合研究所

2024年4月16日

モビリティ・通信事業本部 デジタルメディア・データ戦略グループ

目次

I. ダークパターン	2
II. プロファイリング	34
III. まとめ	43
参考資料	46

I. ダークパターン

- 1. DSAの規定・言及 (1)第25条 (2)序文(67)
- 2. 各国・機関のダークパターンに関する報告書
- 3. ダークパターンの定義・説明
- 4. ダークパターンの分類 (1)全体像 (2)Harry Brignull (3)FTC (4)OECD (5)欧州委員会 (6)EDPB
- 5. ダークパターンの状況 (1)欧州委員会・CPCネットワーク (2)プリンストン大学・シカゴ大学
- 6. ダークパターンに関する規制動向

1. DSAの規定・言及 (1)第25条

- ダークパターンについては、欧州議会による修正版(2022年1月)から明示的に導入され、官報掲載版では序文(67)で言及され第25条にて規定されている。
- 具体的な規制対象や要件、判断基準等は、二次立法(欧州委員会が作成するガイドライン等)で規定・提示されるものと想定される。

第25条 オンライン・インターフェースの設計と構成

1. オンライン・プラットフォーム提供者は、そのサービスの受領者を欺いたり操作したりするような方法で、またはそのサービスの受領者が自由かつ情報に基づいた決定を行う能力をその他の方法で実質的に歪めたり損なったりする方法で、オンライン・インターフェースを設計、構成、運営しないものとする。
2. 第1項における禁止は、指令2005/29/EC又は規則(EU)2016/679の対象となる慣行には適用されないものとする。
3. 欧州委員会は、第1項が特定の慣行にどのように適用されるかについてガイドラインを発行することができ、特に以下のとおりである。
 - (a) サービスの受領者に判断を求める際に、特定の選択肢をより強調すること。
 - (b) サービスの受領者が既に選択を行っている場合に、特にユーザー体験を阻害するポップアップを表示することによって、繰り返し選択を要求すること。
 - (c) サービスの解約手続きを、サービスの加入手続きよりも難しくすること。

※ 指令2005/29/EC : 不公正商慣行指令(UCPD)
規則(EU)2016/679 : 一般データ保護規則(GDPR)

(三菱総合研究所による仮訳)

1. DSAの規定・言及 (2)序文(67)

- DSAの序文(67)では以下のとおり記載されている。

(67) オンライン・プラットフォームのオンライン・インターフェース上の**ダークパターン**とは、サービス受領者が自律的で十分な情報に基づいた選択または決定を行う能力を、意図的または結果的に、著しく歪めるまたは損なう慣行を指す。これらの慣行は、サービス受領者に負の結果をもたらすような、望まれていない行動や決定を行わせるために使用される可能性がある。したがって、オンライン・プラットフォーム提供者は、サービス受領者を欺いたり誘導したりすること、およびオンライン・インターフェースまたはその一部の構造、設計、機能性を介してサービス受領者の自律性、意思決定、または選択を歪めたり損なったりすることを禁止されるべきである。これには、オンライン・プラットフォームの提供者の利益にはなるが受領者の利益にはならないかもしれない行動に受領者を誘導するための搾取的なデザインの選択、サービス受領者に決定を求める際に視覚、聴覚、その他の要素を通じて特定の選択肢をより目立たせるなど、中立ではない方法で選択肢を提示することが含まれるべきだが、これらに限定されるべきでない。

また、既に選択がなされているにも関わらずサービス受領者に繰り返し選択を求めること、サービスの解約手続きを契約するよりも著しく面倒にすること、特定の選択を他よりも困難または時間がかかるようにすること、消費者が取引業者と遠隔契約を締結できる所定のオンライン・プラットフォームから購入を中止したりサインアウトすることを不当に困難にすること、取引に関する意思決定を促したり、変更が非常に困難なデフォルト設定によりサービス受領者を欺くこと、サービス受領者の自律性、意思決定及び選択を歪め損なう方法で意思決定を不当に偏らせること、なども含まれるはずである。しかし、**ダークパターン**を防ぐルールは、提供者がサービス受領者と直接対話して新しいサービスや追加サービスを提供することを妨げるものと理解されるべきではない。例えば広告において、EU法を遵守する合法的な慣行は、それ自体が**ダークパターン**を構成すると考えるべきではないだろう。**ダークパターン**に関するそれらの規則は、指令2005/29/EC 又は規則(EU)2016/679 によりカバーされていない範囲において、本規則の範囲に含まれる禁止慣行をカバーすると解釈されるべきである。

(三菱総合研究所による仮訳、赤字は引用における強調)

2. 各国・機関のダークパターンに関する報告書

- ダークパターンについて、欧州委員会、米国連邦取引委員会(FTC)、OECDなどが報告書を作成・公開しており、ダークパターンの定義や分類、事例を示している。

国・地域・機関	発行主体	タイトル	発行年月	URL
欧州連合(EU)	欧州委員会	Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization Final Report	2022年4月	https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418
	欧州委員会・CPC	Consumer protection: manipulative online practices found on 148 out of 399 online shops screened	2023年1月	https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418
	欧州データ保護会議(EDPB)	Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them Version 2.0 ※ SNSにおけるダークパターンが対象	2023年3月	https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en
米国	連邦取引委員会(FTC)	Bringing Dark Patterns to Light STAFF REPORT	2022年9月	https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers
国際機関	経済開発協力機構(OECD)	DARK COMMERCIAL PATTERNS OECD DIGITAL ECONOMY PAPERS	2022年10月	https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm

3. ダークパターンの定義・説明

- 「ダークパターン」の概念は、UXデザイナーのHarry Brignull氏が2010年に最初に提唱したもの。前掲の各報告書でもさまざまな定義が提案されているが、大筋では共通の内容といえる。
- 最近では「欺瞞的パターン(Deceptive Patterns)」が使われることも多い。

Harry Brignull*1

*1 <https://www.deceptive.design/>

Deceptive patterns (also known as “dark patterns”) are tricks used in websites and apps that make you do things that you didn’t mean to, like buying or signing up for something.

欺瞞的パターン(別名「ダークパターン」とは、何かを買ったり申し込んだりするなど、**利用者の意図しないことをさせる**、ウェブサイトやアプリで使われる策略である。

欧州委員会

“Dark patterns” is a concept that is generally used to refer to practices in digital interfaces that steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests.

「ダーク・パターン」とは、デジタル・インターフェースにおいて、**消費者を誘導し、欺き、強要し、あるいは操作して、しばしば消費者の利益にならない選択をさせる**ような行為を指す概念として一般に用いられている。

OECD

Dark commercial patterns are business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances.

ダーク・コマーシャル・パターンとは、**消費者の自律性、意思決定又は選択を破壊又は損なわせる、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・インターフェースを用いたビジネス手法**である。それらはしばしば**消費者を欺き、強制し、又は操作し、様々な方法で直接的又は間接的に消費者の不利益を引き起こす**可能性があるが、多くの場合、そのような不利益を測定することは困難又は不可能であろう。

4. ダークパターンの分類 (1)全体像

- 「ダークパターン」にはさまざまな手法があり、前掲の各報告書等において分類・類型が示されている。
- 総体的にはほぼ同等であるが、ラベリングやレベル分け(大分類・小分類)に異なる点もある。

Harry Brignull	FTC	OECD	欧州委員会
<ul style="list-style-type: none"> ● 比較防止 ● 羞恥心の植付け ● 偽装広告 ● 偽の希少性 ● 偽の社会的証明 ● 偽の緊急性 ● 強制された行動 ● キャンセルが難しい ● 隠された費用 ● 隠された加入 ● ナギング ● 妨害 ● 選択済み ● スニーキング ● トリック表現 ● 視覚的干渉 	<ul style="list-style-type: none"> ● 推薦(社会的証明) ● 希少性 ● 緊急性 ● 妨害 ● 忍び寄り・情報隠蔽 ● インターフェース干渉 ● 強制された行為 ● 非対称的選択 <p>※ 各類型にさらに小分類がある(後掲)</p>	<ul style="list-style-type: none"> ● 強制された行動 ● インターフェース干渉 ● ナギング(しつこい問いかけ) ● 妨害 ● スニーキング(忍び寄り) ● 社会的証明 ● 緊急性 	<ul style="list-style-type: none"> ● 誤解を招く情報 ● 誤解を招く表現 ● 情報の隠蔽 ● 提示の遅れ ● 圧力の押し付け ● 強制された受容 ● 特定のユーザーの制限 ● 特定の行為の制限 <p>※ 各類型にさらに小分類がある(後掲)</p>
<p>※ 他にもさまざまな分類がなされており、例えば以下では、「スニーキング(バスケットにこっそり入れる/隠された費用/隠された定期購入)」「緊急性(カウントダウンタイマー/期間限定通知)」「誤った指示(羞恥心の植付け/視覚的干渉/トリック質問/圧迫販売)」「社会的証明(他のユーザの活動の通知/推薦状)」「希少性(在庫僅少通知/高需要通知)」「妨害(キャンセルの難しさ)」「強制された行動(強制された登録)」を挙げている:</p> <p>“Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”, https://arxiv.org/pdf/1907.07032.pdf</p>			

4. ダークパターンの分類 (2) Harry Brignull

- Harry Brignullによる類型化*1は以下のとおり。

*1 <https://www.deceptive.design/types>

比較防止	機能や価格が複雑に組み合わせられていたり、必要な情報が見つげにくかったりするため、ユーザは商品を比較するのに苦労する。
羞恥心の植付け	ユーザが感情的に操作され、他の人がしないようなことをする。
偽装広告	ユーザは、インターフェイス要素やネイティブ・コンテンツをクリックしていると勘違いするが、実際は偽装された広告である。
偽の希少性	供給量や人気に限られていることを示す偽の表示が提示されるため、ユーザは行動を完了するよう圧力をかけられる。
偽の社会的証明	偽のレビュー、体験談、活動メッセージを見せられたユーザー、その商品が実際よりも人気がある、あるいは信用できると誤解する。
偽の緊急性	ユーザは、偽の時間制限を提示されたため、アクションを完了するよう圧力をかけられる。
強制された行動	ユーザは何かをしたいが、その見返りとして何か別の好ましくないことを要求される。
キャンセルの難しさ	ユーザは、登録や購読は簡単だが、キャンセルするのは非常に難しいと感じる。
隠された費用	ユーザは安い広告価格で誘惑される。時間と労力を費やした後、チェックアウトの時に予想外の手数料や料金を発見する。
隠された加入	明確な情報開示や明示的な同意がないまま、ユーザが知らず知らずのうちに定期購読や支払いプランに登録されている。
ナギング	ユーザが何かをしようとするとき、自分の利益にならないかもしれない別のことをするように要求され、執拗に中断される。
妨害	ユーザが障壁や障害に直面し、タスクを完了したり情報にアクセスしたりすることが困難になる。
選択済み	ユーザの意思決定に影響を与えるために、すでに選択されているデフォルトのオプションを提示する。
スニーキング	適切な情報が隠されたり、提示が遅れたりすることで、ユーザは偽りの取引に引き込まれる。
トリック表現	紛らわしい、あるいは誤解を招くような表現により、ユーザを惑わせ、行動を起こさせること。
視覚的干渉	ユーザはページ上に明確で予測可能な方法で提示された情報を見ることを期待しているが、それが隠されたり、不明瞭にされたり、偽装されたりしている。

4. ダークパターンの分類 (3)FTC 1/7

- FTCによる類型化*1は以下のとおり。

類型	種類	説明
推薦 (別名「社会的証明」)	虚偽の活動メッセージ	サイト上での他人の活動や製品への興味について、虚偽の主張をすること 例: 「24人がこの商品を見ています」
	欺瞞的な消費者の推薦	以下のような重要な情報を明らかにすることなく、虚偽の顧客推薦を用いたり、他人の経験を紹介したりすること (1) 推薦者が報酬を受け取っている (2) 推薦者が従業員や家族であるなどその企業と関係がある (3) 推薦者の体験が、同じような状況で他の人が体験する典型的なものでない
	有名人による偽りの推薦	著名人によるものと偽った体験談の掲載 または 推薦の報酬または製品の無償提供を開示することなく、著名人または著名なインフルエンサーを使用して製品を推薦すること
	パラソーシャル関係の圧力	子どもが知っていて信頼しているキャラクターを使って、ある選択をするように圧力をかけること 例: 有名なマンガのキャラクターを使い、子どもにアプリ内課金をさせる
稀少性	偽の在庫僅少メッセージ	子どもが知っていて信頼しているキャラクターを使って、ある選択をするように圧力をかけること 例: 「在庫残り1個です、ご注文はお早めに」
	偽の高需要メッセージ	需要がないのに需要があると言って、すぐには買わなければならないようなプレッシャーを与える 例: 「他の20人がこの商品をカートに入れていています」

*1 前掲報告書, Appendix A

4. ダークパターンの分類 (3)FTC 2/7

● (つづき)

類型	種類	説明
緊急性	根拠のないカウントダウン・タイマー	タイムアウトすると消えてしまう、あるいはリセットされる偽のカウントダウン・クロックを表示して、すぐには買わなければならないようなプレッシャーを与える。 例: 「キャンペーン終了まであと00:59:48」
	偽の期間限定メッセージ	「期間限定」「近日終了」など、すぐには買わなければならないようなプレッシャーを与えるが、期限がない、あるいは期限が来てもしリセットされるだけの無意味な期限
	虚偽の割引の主張	偽の「割引」または「セール」価格を提示して、すぐには買わなければならないようなプレッシャーを与えること
妨害	価格の比較防止	購入者が簡単に価格を比較できるように、商品をまとめたり、異なる尺度を使ったり(単位あたりの価格とオンスあたりの価格)、支払い回数や全体のコストを開示せずに支払いごとの価格(週あたり10ドルなど)を記載したりすること
	解約の障害	面倒で時間のかかる解約手続きを要求することで、契約は簡単だが解約は難しくすること 例: ネットで申し込ませておきながら、解約は別の手段でさせる 例: 電話による解約を要求しておきながら、電話番号を隠したり、解約窓口の人員が少なかったり、受付時間を限定したり、解約の際にセールストークやアップセルを聞かせたりする
	消滅しないアカウント	アカウントの削除を困難または不可能にすること
忍び寄り・情報隠蔽	カートへの忍び込み	購入者の許可なく、自動的にショッピングカートに商品を追加すること または 選択済みチェックボックスを使って不要な商品を買わせること

4. ダークパターンの分類 (3) FTC 3/7

● (つづき)

類型	種類	説明
忍び寄り・情報隠蔽 (つづき)	隠された情報	重要な情報や製品の重大な制限を人々に隠すこと 例: 細かい字での記載、長い利用規約、覆面ハイパーリンクの後ろ、適切な場所にマウスを置いたときだけ表示されるポップアップボックスの中、に情報を隠す
	隠されたコスト	人々が知らない隠れた手数料やその他の料金を加えること 例: 融資金額から差し引かれる非公開の手数料
	ドリップ・プライシング	商品代金の一部のみを最初に広告し、購入プロセスの後半で他の強制的な料金を課すこと 例: レジに進むと表示される「手数料」
	隠れ定期購入または強制的継続	無料トライアルを提供し、トライアル終了後に消費者が積極的に解約しない場合、自動的かつ予期しない定期的な料金を請求すること または 少額の1回限りの料金で製品を提供し、消費者の同意なしに自動的に定期購入または継続プランに登録させる
	中間通貨	消費者に仮想通貨で物を買わせることで実質的なコストを隠す 例: 子ども向けアプリの「コイン」や「ドングリ」など
インターフェース干渉	注意逸らし	スタイルとデザインを使って、ユーザーの注意をあるものに集中させ、別のものから注意を逸らすこと 例: 小計価格を明るい緑色のハイライトボックスで表示し、その下に必須の税金と手数料をハイライトせずに表示することで、最終的な合計金額が高くなることにユーザが気づかないようにする

4. ダークパターンの分類 (3)FTC 4/7

● (つづき)

類型	種類	説明
インターフェース干渉 (つづき)	偽りの階層構造または 圧力的なアップセル	<p>選択肢を与える際に、視覚的に対照的な目立たせ方を用いることで、ユーザーが特定の選択をするように誘導する</p> <p>例: 解約時に、「購読を継続する」オプションを明るいオレンジ色のボタンで提示し、「購読を解約する」オプションを小さいフォントで、オレンジ色のボタンの下に隠れた薄いグレーのハイパーリンクで提示する</p>
	偽装広告	<p>公平な製品レビューまたは独立したジャーナリズムであると偽って広告をフォーマットすること</p> <p>または</p> <p>ランキングリスト、検索エンジン、または比較ショッピングサイトが、実際には広告費に基づいているにもかかわらず、中立で公平であるかのように表示すること</p>
	おとり販売	<p>選択または相互作用により、予期しない望ましくない結果になること</p> <p>例: ユーザーがポップアップの右上にあるXをクリックしたが、ボックスを閉じる代わりにソフトウェアをダウンロードした</p> <p>例: 消費者に何かを販売したが、当初宣伝されたものとは実質的に異なることが判明した</p>
強制された行為	不正取引	<p>取引の手順を誤って表示したり、アカウントホルダーから明確なインフォームドコンセントを得なかったりするなどして、希望していないまたは購入するつもりのない商品やサービスの代金を支払わせること</p> <p>例: 「次へ」と表示されたショッピングサイトのボタンが、次の画面に進むと思わせておいて、すぐに取引を処理させる</p> <p>例: 子ども向けゲームアプリのワンクリック・ボタンが、親にリアルマネーを課金するもの</p>

4. ダークパターンの分類 (3) FTC 5/7

● (つづき)

類型	種類	説明
強制された行為 (つづき)	自動再生	ある動画が終了すると、自動的に別の動画が予期せぬまたは有害な方法で再生される 例: 最初の動画の後に、子ども向けではない動画、またはおすすり動画に見せかけたスポンサー広告が自動的に再生される
	しつこい問いかけ	ユーザーがアクションを起こしたいかどうか、邪魔になるような形で繰り返し尋ねること または ユーザーが永久に拒否できないような要求をし、その要求を何度も催促する 例: ユーザーにデータの提供やクッキーをオンにするよう求め、その選択肢を「はい」「いいえ」ではなく、「はい」「今はダメ」と繰り返し提示する
	強制的な登録または入会	タスクを完了させるために、ユーザーにアカウントを作成させたり、情報を共有させたりすること 例: 「購入を続けるにはアカウントを作成してください」
	有料プレイまたは グライディング	購入やダウンロードで入手できると言いながら、実際にそれらを手に入れるためにユーザーに課金すること または 無料版のゲームを非常に面倒で手間のかかるものにし、アプリ内課金で新機能をアンロックさせるよう誘導すること
	なりすましスパム、 ソーシャルメディア・ネズミ講、 アドレス帳搾取	ある目的のためにメールアドレスやソーシャルメディアの許可を得ておきながら、別の目的で使用する こと または ユーザーが自分のソーシャルネットワーク内の人に関する情報を共有するように仕向けること

4. ダークパターンの分類 (3) FTC 6/7

● (つづき)

類型	種類	説明
非対称的選択	ひっかけ質問	曖昧で分かりにくい言葉(多くは二重否定)を使って、ユーザーの望まない方向に誘導すること <i>例: 「最新情報のメール配信を希望しない場合はチェックを外してください」</i> <i>例: 「ローンを更新するオプションを拒否する」という文言の横にチェックボックスがあり、チェックを外しておくで自動更新の条件に同意したものと解釈される</i> <i>例: 定期購入サービスを解約しようとする時、「No, cancel」と書かれたボタンが表示され、解約は実行されない</i>
	羞恥心の植付け	恥ずかしさを利用し、選択肢を悪い決断と決めつけて、ユーザーを特定の選択から遠ざける <i>例: 定期購入でなく1回きりの購入を選択した場合、「いいえ、お金を節約したいわけではない」と表示される</i>
	事前選択	企業には有利だが、ユーザーには不利なデフォルトの選択 <i>例: 旅行保険や延長保証などのアドオン商品が、顧客が気づいてオプトアウトしない限り、購入時に自動的に付加される</i> <i>例: トラッキングクッキーを受け入れるボックスにあらかじめチェックを入れておく</i> <i>例: サイトは自動的に買い物客に最も高価なオプションを表示し、より安いまたは無料のオプションは表示しない</i>

4. ダークパターンの分類 (3) FTC 7/7

● (つづき)

類型	種類	説明
非対称的選択 (つづき)	プライバシー設定を覆す	<p>ユーザーを騙して、本当に意図した以上の情報を共有させること</p> <p>例: ユーザーに同意を求めながら、何を共有することに同意しているのかについて、明確かつ理解しやすい方法で通知しない</p> <p>例: サイトがある目的のために情報を収集しているとユーザーに伝えながら、その情報を他者と共有したり、他の目的のために使用したりする</p> <p>例: データ収集を最大化するような初期設定を含み、ユーザーがそれを見つけて変更することを難しくしている</p> <p>例: ユーザーに選択肢を与えるが、「承諾」の選択肢は太字で青い背景、「拒否」はグレーアウトして小さな文字で表示される</p>

4. ダークパターンの分類 (4)OECD 1/2

- OECDによる類型化*1は以下のとおり。

強制された行動	<ul style="list-style-type: none"> • 特定の機能にアクセスするために消費者に何かをさせようとするもの。 • 例:消費者が登録を強制されたり、それが必要であると騙されたり、必要以上の個人情報を開示させられたり、無料サービスの場合は必要以上の個人情報を開示させられて完全に利用されたりすること。サービスを利用するために、消費者の連絡先に関する情報を、場合によっては消費者の同意なく抽出・利用すること(フレンドスパミングやソーシャルピラミッド)も一例。
インターフェース干渉	<ul style="list-style-type: none"> • 情報のフレーミングを通じて、オンラインビジネスに有利な消費者の特定の行動を優遇することを目的として、フレーミング効果またはアンカー効果、デフォルト・バイアスを利用することがある。 • 例:重要な情報を視覚的に不明瞭にすること(隠し情報)、事業者により有利な選択肢をデフォルトで事前選択すること、事業者により有利な選択肢を視覚的に優先させ、誤った階層を作ること、誤解を招く元の価格または偽の高価格を参照して割引価格を表示すること(誤解を招く参照価格)、意図的または明白なあいまいさをトリック質問で用いること(二重否定など)、広告を偽ること、感情的言語またはフレームを通じて特定の選択に向かって消費者を操ること(羞恥心の植え付けまたは感情の弄びとして知られている)。
ナギング	<ul style="list-style-type: none"> • 通知や位置情報の取得など、事業者にとって都合の良いことを繰り返しつこく要求し、消費者の限られた意志や時間を搾取するものが含まれる。
妨害	<ul style="list-style-type: none"> • 行動を思いとどまらせる意図で、タスクフローやインタラクションを本来必要なものよりも難しくすることを目的として、消費者の慣性、限られた意志や時間を利用するもの。 • 例:サービスの契約やプライバシー侵害的な設定へのオプトインは簡単にできても、サービスの解約やよりプライバシーに配慮した設定へのオプトアウトは難しくすること。 • 同様の意味で、「クリック疲れ」や「クリックしやすさ」は、異なる選択肢へのクリック経路の長さを変えて、事業者が好む「シンプルな」経路を消費者に選択させることを指す。 • その他の例として、アカウントや消費者の情報の削除を困難または不可能にすること(しばしば不滅のアカウントと呼ばれる)、異なるオファーや価格を比較することを困難または不可能にすること(価格比較防止)などがある。

*1 前掲報告書, p.10-11

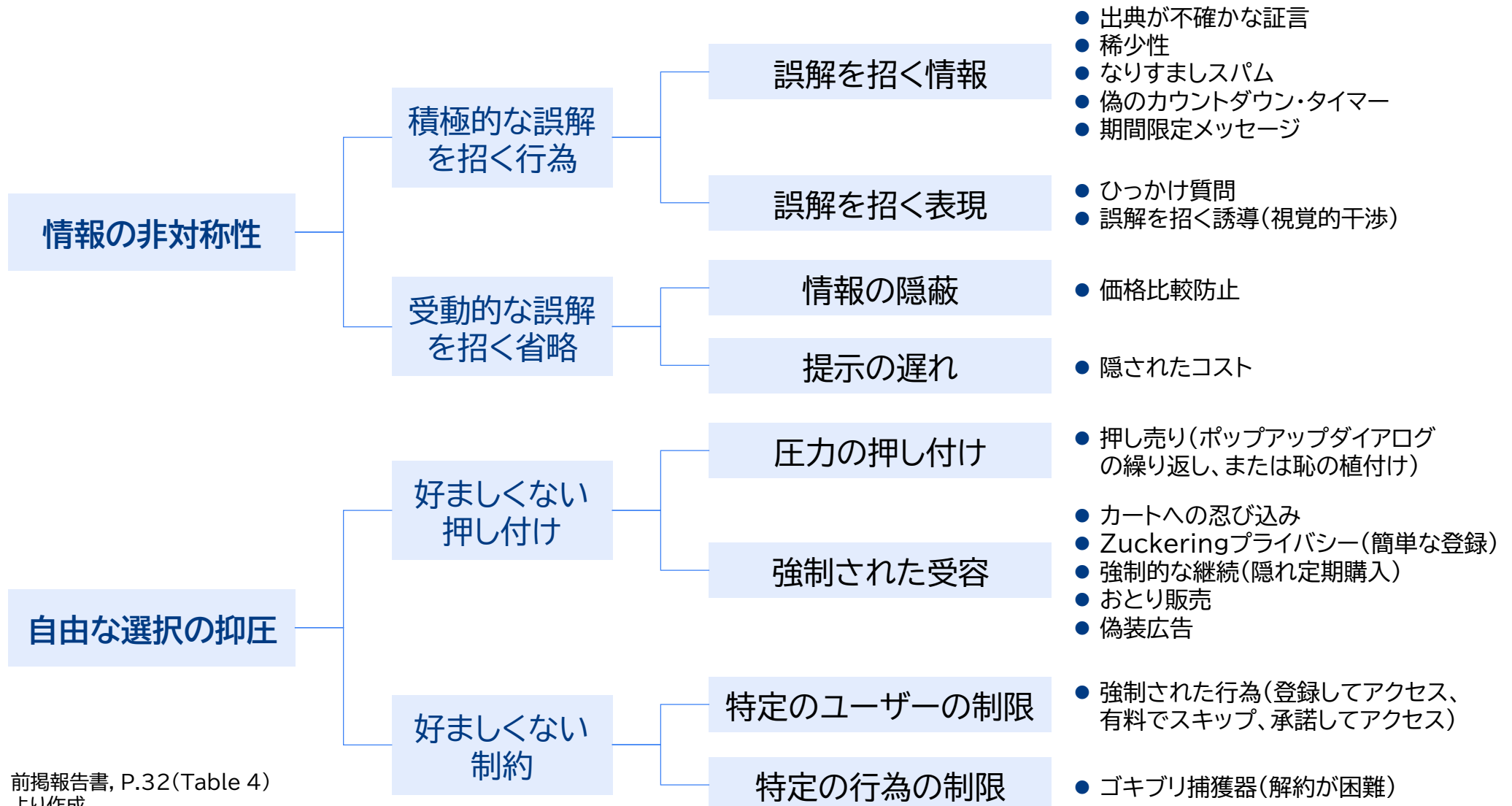
4. ダークパターンの分類 (4)OECD 2/2

- (つづき)。

スニーキング (※忍び寄り)	<ul style="list-style-type: none"> • 消費者の意思決定に関連する情報、特にコストに関する情報を隠蔽・偽装したり、開示を遅らせようとするもので、消費者の注意力の限界、デフォルト・バイアス、アンカリング効果、サンクコストの誤謬を利用する場合がある。 • 例:消費者が購入を完了しようとしているときに、新しい、潜在的に重要な非オプション料金を合計価格に追加すること(別称:ドリップ・プライシング)、先行ページのチェックボックスを介して消費者の同意なしにバスケットにアイテムをこっそり入れること、消費者の明確な同意なしに用期間も定期購入を自動的に継続すること(隠れた加入/購読の罠、強制継続としても知られている)など。 • 消費者が承諾していない商品のサービスを提供は、惰性販売またはネガティブオプション課金ともいわれる。
社会的証明	<ul style="list-style-type: none"> • 他の消費者の行動観察に基づいて意思決定のきっかけを作ろうとするもので、社会的証明のバイアスを利用する。例えば、他の消費者の行動に関する通知や、最近購入した商品に関する証言などがある。 • 行動の通知には、例えば以前購入したものを最近購入したかのように偽って知らせるなど真実味がない場合があり、証言には誤解を招く内容であったり虚偽である場合がある。
緊急性	<ul style="list-style-type: none"> • 消費者に購入を促すために、取引に現実または偽の時間的・量的制限を課し、希少性ヒューリスティックを悪用する。そのため、希少性の合図または主張と呼ばれることもある。 • 例:在庫が少ない、需要が高い、というメッセージや、取引期限や割引を示すカウントダウン・タイマーなど。

4. ダークパターンの分類 (5) 欧州委員会 1/2

- 欧州委員会が示す類型化(「伝統的」な分類)*1は以下のとおり。



*1 前掲報告書, P.32(Table 4)より作成

4. ダークパターンの分類 (5) 欧州委員会 2/2

- 欧州委員会による類型化(行動科学的分類)*1は以下のとおり。「操作的(manipulative)」≡データドリブン・パーソナライゼーションを用いたダークパターンにも注目(警戒)している。

		選択アーキテクチャ(→選択の難易度)		
		特性の複雑性 →商品特性のわかりにくさ	コストの複雑性 →コストのわかりにくさ	選択の複雑性 →選択の手間・難度
意思決定要素 (→意思決定への影響)	予算の制約に影響する →支払額を結果的に増加させる	<ul style="list-style-type: none"> ● 隠された情報 ● 視覚的干渉 ● 限定期間メッセージ ● なりすましスパム/ソーシャル・ピラミッド/アドレス帳搾取 ● Zuckeringプライバシー 	<ul style="list-style-type: none"> ● 価格比較防止 ● 中間通貨 ● 隠されたコスト ● 消滅しないアカウント 	<ul style="list-style-type: none"> ● ゴキブリ捕獲器 ● カートへの忍び込み ● 事前選択 ● 強制的な入会 ● ゲーミフィケーション ● ナギング(しつこい問いかけ)
	選好性を形成する(消費者の評価) →支払意欲増につなげる	<ul style="list-style-type: none"> ● 活動メッセージ、推薦 ● 偽りの階層構造 ● 在庫僅少メッセージ ● 高需要メッセージ ● 可愛らしさ ● 操作的な、パーソナライズされたコミュニケーションおよび広告 	<ul style="list-style-type: none"> ● おとり販売 ● 誤解を招く参考価格 ● 押付け販売 ● 操作的なパーソナライズド・プライシング 	<ul style="list-style-type: none"> ● 羞恥心の植付け ● 感情の弄び ● ひっかけ質問 ● メッセージ付きカウントダウン・タイマー ● 偽装広告 ● 操作的なパーソナライゼーションの選択(検索結果ランキング、レコメンダー・システムなどにおいて)

*1 前掲報告書, P.39(Table 7)に加筆

4. ダークパターンの分類 (6)EDPB【分類:全体像】

- EDPBのソーシャルメディアにおける欺瞞的デザインパターンのGDPRガイドラインでは、「ダークパターン」を6カテゴリ・16パターンに分類している*1。

カテゴリー	パターン
1. 過剰負荷(Overloading) ユーザーを大量の要求、情報、オプション、可能性に埋没させ、それ以上進むことを阻止し、特定のデータ慣行を維持または受け入れさせる。	1.1. 絶え間ない指示(Continuous prompting)
	1.2. プライバシー迷路(Privacy Maze)
	1.3. 多過ぎる選択肢(Too many options)
2. 省略(Skipping) ユーザーがデータ保護の全部または一部の側面を忘れていたり考えなかったりするようなインターフェースやユーザージャーニーを設計する。	2.1. 欺瞞的な居心地よさ(Deceptive snugness)
	2.2. あっちを見て(Look over there)
3. 煽り(Stirring) 感情に訴えかけたり、視覚的な刺激を与えたりすることで、ユーザーの選択に影響を与える。	3.1. 感情的舵取り(Emotional Steering)
	3.2. 簡素な見た目に隠す(Hidden in plain sight)
4. 妨害(Obstructing) ユーザーが情報を入手したりデータを管理したりする行為を困難または不可能にすることによって、そのプロセスを妨げたり阻止したりする。	4.1. 行き止まり(Dead end)
	4.2. 必要以上(Longer than necessary)
	4.3. 誤解を招く行為(Misleading action)
5. 気まぐれ(Fickle) インターフェースのデザインが不安定で一貫性がないため、処理の内容を把握し、データに関する選択を適切に行い、さまざまなコントロールがどこにあるのかを見つけることが難しい。	5.1. 階層性の欠如(Lacking hierarchy)
	5.2. 非文脈化(Decontextualising)
	5.3. 一貫性のないインターフェース(Inconsistent interface)
	5.4. 言語の不連続性(Language discontinuity)
6. 暗闇に残される(Left in the dark) データ保護に関連する情報やコントロールを隠したり、データがどのように処理され、どのようなコントロールが可能なのかユーザーにわからないままにするようにインターフェースが設計されている。	6.1. 矛盾する情報(Conflicting information)
	6.2. あいまいな表現や情報(Ambiguous wording or information)

*1 EDPB, “Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them Version 2.0”

4. ダークパターンの分類 (6)EDPB【分類:詳細 1/2】

- EDPBのガイドラインにおいて、ダークパターンの個々のパターンは以下のように説明されている。GDPRのガイドラインなので、個人データの取扱いの視点で整理されている。

カテゴリー	パターン
1. 過剰負荷 (Overloading)	1.1. 絶え間ない指示(Continuous prompting) データの提供や新たな処理目的への同意をユーザに繰り返し求めることで、処理目的に必要な以上の個人データを提供したり、データの別の利用に同意するようユーザに促すこと。このような反復的なプロンプトは、1つまたは複数のデバイスを通じて行われる可能性がある。ユーザは、利用を中断させるプラットフォームを利用するたびに要求を拒否しなければならないことに疲れ、結局屈してしまう可能性が高い。
	1.2. プライバシー迷路(Privacy Maze) ユーザが特定の情報を得たり、特定の管理権限を使用したり、データ主体の権利を行使したりしたい場合に、包括的かつ網羅的な概要が利用可能でないと、関連する情報や管理権限を得るためにあまりにも多くのページをナビゲートしなければならないため、ユーザがそれらを見つけるのは特に困難である。ユーザは、関連する情報または管理をあきらめたり見落とししたりする可能性が高い。
	1.3. 多過ぎる選択肢(Too many options) ユーザに多い(多過ぎる)選択肢を提供すること。選択肢が多過ぎるとユーザは何も選択できなくなり、特に情報が入手できない場合は、いくつかの設定を見落とししたりする。最終的には、ユーザはあきらめたりデータ保護の設定や権利を見落とししたりすることになりかねない。
2. 省略 (Skipping)	2.1. 欺瞞的な居心地よさ(Deceptive snugness) 最もデータ侵襲性の高い機能とオプションがデフォルトで有効になっている。予め選択されたオプション(デフォルト設定)を維持するように個人を促す効果により、ユーザは可能性を与えられていてもこれを変更することはまずない。
	2.2. あっちを見て(Look over there) データ保護に関連する行動や情報が、別の要素と競合している。ユーザがこの邪魔な選択肢(別の要素)を選ぶと、それが本来の目的であったとしても、もう一方のこと(データ保護に関連すること)を忘れてしまう可能性が高い。
3. 煽り(Stirring)	3.1. 感情的舵取り(Emotional Steering) 言葉遣いや視覚的要素(スタイル、色、写真など)を、非常に肯定的な眺望(良い気分、安全な気分、または報酬を感じさせる)または非常に否定的な眺望(恐怖、罪悪感、または処罰を感じさせる)で、ユーザに情報を与えるような方法で使用すること。このような方法でユーザの感情状態に影響を与えることは、ユーザにデータ保護の利益に反する行動を取らせる可能性が高い。
	3.2. 簡素な見目に隠す(Hidden in plain sight) 情報またはデータ保護のコントロールにおいて、ユーザをより制限の少ない、つまりより侵襲的なオプションに誘導するような視覚的なスタイルやテクニックを使用する。

4. ダークパターンの分類 (6)EDPB【分類:詳細 2/2】

カテゴリー	パターン
4. 妨害 (Obstructing)	4.1. 行き止まり(Dead end) ユーザが情報やコントロールを探しているときに、リダイレクトリンクが機能していなかったり、まったく利用できなかつたりして、結局見つからない。ユーザはそのタスクを達成できない状況に置かれる。
	4.2. 必要以上(Longer than necessary) ユーザがデータ保護に関連するコントロールをアクティブにする場合には、データ侵害オプションのアクティブ化に必要なステップ数よりも多くのステップを必要とする方法でユーザジャーニーを作成する。これにより、ユーザはそのようなコントロールを有効にする意欲を失う可能性が高い。
	4.3. 誤解を招く行為(Misleading action) ユーザが得られる情報と行動との間に乖離があると、ユーザは意図しないことをするようになる。ユーザが期待するものと得られるものとの差は、ユーザがそれ以上先に進むことを躊躇させる可能性が高い。
5. 気まぐれ (Fickle)	5.1. 階層性の欠如(Lacking hierarchy) データ保護に関連する情報には階層性がなく、情報が何度も表示され、いくつかの方法で提示されている。ユーザはこのような冗長性に混乱し、自分のデータがどのように処理され、どのようにコントロールできるかを十分に理解できないまま放置される可能性が高い。
	5.2. 非文脈化(Decontextualising) データ保護の情報またはコントロール機能が、文脈から外れたページにある。その特定のページにあることは直感的でないため、ユーザはその情報やコントロールを見つけにくい。
	5.3. 一貫性のないインターフェース(Inconsistent interface) 異なるコンテキスト間でインターフェースが一貫していない(例:データ保護関連のメニューがモバイルとデスクトップで同じ項目を表示していない)、またはユーザの期待に合致していない(例:オプションの位置が別のオプションと入れ替わっている)。このような違いによって、ユーザは目的のコントロールや情報を見つけられなかったり、データ保護について望まない選択をすることになる可能性がある。
	5.4. 言語の不連続性(Language discontinuity) サービスはユーザが居住する国の公用語で提供されるが、データ保護に関する情報は提供されていない。データ保護情報が提供される言語をユーザが理解できなければ、それを簡単に読むことができず、したがってデータがどのように処理されているかわからない可能性が高い。
6. 暗闇に残される (Left in the dark)	6.1. 矛盾する情報(Conflicting information) 互いに矛盾する情報をユーザに与えること。ユーザは、自分が何をすべきなのか、自分の行動がどのような結果をもたらすのかわからず、何もせず、デフォルト設定のままにしてしまう可能性が高い。
	6.2. あいまいな表現や情報(Ambiguous wording or information) ユーザに情報を提供する際に、曖昧であいまいな用語を使用すること。ユーザは、データがどのように処理されるのか、あるいは自分の個人データをどのように管理できるのかわからなくなる可能性が高い。

4. ダークパターンの分類 (6)EDPB【関連GDPR規定 1/2】

- EDPBのガイドラインでは、ダークパターンの個々のパターンに関連するGDPRの規定も示している。

カテゴリー	パターン	関連するGDPRの規定
1. 過剰負荷	1.1. 絶え間ない指示	<ul style="list-style-type: none"> • 目的の限定:5条(1)(b); • 自由な同意:7条+4条(11); • 特定の同意:7条(2)
	1.2. プライバシー迷路	<ul style="list-style-type: none"> • 透明性の原則+透明性のある情報:5条(1)(a)+12条(1); • 公正性の原則:5条(1)(a); • 容易にアクセスできる情報:12条(1); • 権利行使が容易なこと:12条(2); • 事前説明に基づく同意:7条+4条(11)
	1.3. 多過ぎる選択肢	<ul style="list-style-type: none"> • 透明性及び公正性の原則:5条(1)(a); • 透明性のある情報:12条(1)
2. 省略	2.1. 欺瞞的な居心地よさ	<ul style="list-style-type: none"> • データ保護バイデザイン及びデータ保護バイデフォルト:25条(1); • 同意:4条(11)+6条(デフォルトによる同意に基づく処理を有効にする違法行為)
	2.2. あっちを見て	<ul style="list-style-type: none"> • 透明性及び公正性の原則:5条(1)(a); • 透明性のある情報:12条(1); • 権利の行使:12条(2)
3. 煽り	3.1. 感情的舵取り	<ul style="list-style-type: none"> • 透明性及び公正性の原則:5条(1)(a); • 透明性のある情報:12条(1); • 権利の行使:12条(2); • 子どもの同意:8条; • 事前説明に基づく同意:7条+4条(11)
	3.2. 簡素な見た目に隠す	<ul style="list-style-type: none"> • 公正性の原則:5条(1)(a); • 自由な同意:7条+4条(11); • 明確な情報:12条(1); • 権利の行使:12条(2)

4. ダークパターンの分類 (6)EDPB【関連GDPR規定 2/2】

カテゴリー	パターン	関連するGDPRの規定
4. 妨害	4.1. 行き止まり	<ul style="list-style-type: none"> 容易にアクセスできる情報:12条(1); 権利の行使:12条(2); データ保護バイデザイン及びデータ保護バイデフォルト:25条(1)
	4.2. 必要以上	<ul style="list-style-type: none"> 容易にアクセスできる情報:12条(1); 権利の行使:12条(2); 異議を述べる権利:21条(1); 同意の撤回:7条(3); データ保護バイデザイン及びデータ保護バイデフォルト:25条(1)
	4.3. 誤解を招く行為	<ul style="list-style-type: none"> 透明性のある情報:12条(1); 取扱いの公正性:5条(1)(a); 事前説明に基づく同意:7条(2)+4条(11)
5. 気まぐれ	5.1. 階層性の欠如	<ul style="list-style-type: none"> 容易にアクセスできる情報:12条(1); 権利の行使:12条(2)
	5.2. 非文脈化	<ul style="list-style-type: none"> 容易にアクセスできる情報:12条(1); 透明性のある情報:12条(1); 権利の行使:12条(2)
	5.3. 一貫性のないインターフェース	<ul style="list-style-type: none"> 容易にアクセスできる情報:12条(1); 権利の行使:12条(2)
	5.4. 言語の不連続性	<ul style="list-style-type: none"> 取扱いの公正性:5条(1)(a); 理解しやすい情報:12条(1)+13条+14条 明確で平易な言語を用いた情報:12条(1)+13条+14条
6. 暗闇に残される	6.1. 矛盾する情報	<ul style="list-style-type: none"> 取扱いの公正性:5条(1)(a); 透明性のある情報:12条(1); 事前説明に基づく同意:7条(2)+4条(11)
	6.2. あいまいな表現や情報	<ul style="list-style-type: none"> 取扱いの公正性:5条(1)(a); 透明性のある情報:12条(1); 明確で平易な言語を用いた情報:12条(1) 事前説明に基づく同意:7条(2)+4条(11) 不完全な情報:13条 特定のユースケースに応じた特定の規定

4. ダークパターンの分類 (6)EDPB【ベストプラクティス 1/2】

- EDPBのガイドラインでは、ダークパターンを回避するベストプラクティスとして以下を例示している。分類と同様に、個人データ保護の観点でのベストプラクティスとなっていると考えられる。

ショートカット	ユーザが自分のデータおよびデータ保護設定を管理するために実助的な助けとなる情報、措置、または設定へのリンクは、ユーザが関連情報またはエクスペリエンスに直面するあらゆる場所で利用できるようにすべきである。(例: プライバシー・ポリシーの関連部分にリダイレクトするリンク; プライバシー・ポリシーの中で、各データ保護情報に対して、ソーシャルメディア・プラットフォーム上の関連するデータ保護ページに直接リダイレクトするリンクを提供する)
一括オプション	ユーザがより簡単に変更できるように、同じ処理目的を持つオプションを一緒に配置する一方で、ユーザがより細かく変更できる可能性を残す。ソーシャルメディア・プラットフォームが一括オプションを提示する場合、これらに予期せぬ要素や無関係な要素(例えば、異なる目的を持つ要素)が含まれてはならない。同意が必要な処理の場合、一括オプションは、同意に関するEDPBガイドライン(特にパラグラフ42-44)に従う必要がある。
連絡先情報	データ保護要求に対応するための会社の連絡先は、プライバシー・ポリシーに明記すべきである。この連絡先は、データ管理者の身元に関するセクション、権利に関するセクション、または連絡先セクションなど、ユーザが見つめることが期待できるセクションに記載すべきである。
監督当局への連絡	監督当局を具体的に明記し、そのウェブサイトまたは苦情の申立てに関連する特定のウェブサイトのページへのリンクを含めること。この情報は、権利関連のセクションなど、ユーザが見つめることが期待できるセクションに記載すること。
プライバシー・ポリシーの概観	プライバシー・ポリシーの冒頭/上部に、見出しと小見出しのある(折りたたみ可能な)目次を掲載し、プライバシー通知に含まれるさまざまな箇所を示す。各項目の名称は、正確な内容に関してユーザを明確に誘導し、探しているセクションを素早く特定してジャンプできるようにする。
変更の強調と比較	プライバシーに関する通知に変更が加えられた場合は、公開日とともに以前のバージョンにアクセスできるようにし、変更点を強調する。
一貫性のある表現	ウェブサイト全体で、データ保護について同じ文言と定義が使用されている。プライバシー・ポリシーで使用されている文言は、プラットフォームの他の部分で使用されている文言と一致する必要がある。
定義の提示	馴染みのない言葉や専門用語を使用する場合、平易な言葉で定義を示すことで、ユーザは提供された情報を理解しやすくなる。定義は、ユーザがその単語にカーソルを合わせたときに、テキストに直接表示することも、用語集で利用できるようにすることもできる。
データ保護要素の対比	データ保護に関連する要素またはアクションを、その件に直接関係しないインターフェイスで視覚的に目立つようにすること。例えば、プラットフォームにパブリック・メッセージを投稿する場合、位置情報の関連付けに関するコントロールを直接利用でき、明確に見えるようにする。
ユーザ登録時のデータ保護設定プロセス	アカウント作成直後、ソーシャルメディア・プロバイダのオンボーディング・エクスペリエンスにデータ保護に関するポイントを盛り込み、ユーザがスムーズに自分の好みを発見・設定できるようにする。例えば、最初の友人を追加したり、最初の投稿を共有した後に、データ保護に関する設定を行うようユーザを招待することで、これを行うことができる。

4. ダークパターンの分類 (6)EDPB【ベストプラクティス 2/2】

事例の利用	処理目的を明確かつ正確に記載した必須情報に加え、具体的なデータ処理を例示することで、ユーザがより具体的に理解できるようにすることができる。
離れないナビゲーション	データ保護に関連するページを閲覧している間、目次が常に画面に表示されるため、ユーザは常に関連ページ上に位置することができ、またアンカーリンクによってコンテンツ内を素早く移動することができる。
トップに戻る	ユーザのページ内ナビゲーションを容易にするため、ページ下部、またはウィンドウ下部のスティッキーエレメントにトップへ戻るボタンを設置する。
通知	個人データ処理に関連する事項、変更またはリスク(データ侵害が発生した場合など)について、ユーザの認識を高めるために通知を使用することができる。これらの通知は、受信トレイのメッセージ、ポップインウィンドウ、ウェブページ上部の固定バナーなど、いくつかの方法で実施することができる。
結果の説明	ユーザがデータ保護管理の有効化または無効化、あるいは同意の付与または撤回を希望する場合は、そのような行動の結果について中立的な方法でユーザに通知する。
デバイス間の一貫性	ソーシャルメディア・プラットフォームが異なるデバイス(コンピュータ、スマートフォンなど)で利用できる場合、データ保護に関する設定や情報は、異なるバージョン間で同じスペースに配置し、同じ動線やインターフェース要素(メニュー、アイコンなど)からアクセスできるようにする。
データ保護に関するディレクトリ	メニューの様々なセクションに簡単にアクセスできるように、データ保護に関連するすべての行動や情報にアクセスできるページをユーザに提供する。このページは、ソーシャルメディア・プロバイダーのメイン・ナビゲーション・メニュー、ユーザ・アカウント、プライバシー・ポリシーなどで見つけることができる。
文脈情報	包括的なプライバシー・ポリシーに加え、ユーザがデータの処理方法について具体的かつ継続的な情報を得られるよう、適切なタイミングで短い情報を提供する。
分かりやすいURL	データ保護の設定や情報に関連するページは、その内容を明確に反映したウェブアドレスを使用する必要がある。例えば、データ保護管理を一元化するページのURLは、[social-network.com]/data-settingsのようにすることができる。
権利行使フォーム	ユーザがGDPRの権利を行使しやすくするため、ユーザの権利の理解を助け、ユーザがこの種の要求を実行できるよう案内する専用フォームを提供する。

5. ダークパターンの状況 (1) 欧州委員会・CPCネットワーク

- 欧州では、欧州委員会とCPCネットワーク*1が、小売業者のオンラインショップのウェブサイトおよびアプリにおける欺瞞的なインターフェースやダークパターンの使用状況に関する調査を行った*2。
- 調査対象の4割近くでダークパターンが使われていることがわかった。

調査対象		ウェブサイト 399	アプリ 102
ダークパターン	偽のカウントダウンタイマー (特定の商品の購入期限を示す)	42サイト	
	消費者を特定の選択肢に誘導 (ビジュアルデザイン・言葉の選択)	54サイト	
	重要な情報を隠したり、消費者に見えにくくしたりする	70サイト	

148サイト(37.1%)が

3つのダークパターンのうち
少なくとも一つを使用

27サイト(26.5%)が

3つのダークパターンのうち
少なくとも一つを使用

※ 日本では、ユーザ調査(68.8%が目撃した、46.1%が被害に遭った、理解度16.6%、認知度44.8%)*3や、広告審査の状況(ダークパターンと考えられるサイトのアカウント非承認が増加)*4などの調査結果がある

※ 前掲のサイト・論文などでも、事例や調査結果が示されている*5

*1 Consumer Protection Cooperation NetworkはEUの消費者保護法の執行を担当する当局のネットワーク(23の加盟国及びノルウェー、アイスランドの消費者保護当局で構成)で、国境を越えた問題に取り組んでいる。

*2 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418

*3 株式会社コンセント, <https://www.concentinc.jp/news-event/news/2023/11/darkpattern-report2023/>

*4 LINEヤフー株式会社, <https://www.lycorp.co.jp/ja/news/release/001093/>

*5 <https://www.deceptive.design/hall-of-shame>, <https://arxiv.org/pdf/1907.07032.pdf>

5. ダークパターンの状況 (2)プリンストン大学・シカゴ大学 1/5

- プリンストン大学・シカゴ大学の研究者は、①ダークパターンの使用状況に関する大規模な調査、②調査結果に基づく認知バイアスの観点からの分類を実施し、2019年に発表した*1。
- 調査対象とした1万1千強のショッピングサイトのうち、1,254(11.1%)のサイトでダークパターンが発見された。また、ダークパターンについて7カテゴリ15パターンの分類を作成した。

調査目的

- ダークパターンの蔓延を示す大規模な証拠や、異なるタイプのダークパターンがどのようにユーザに害を及ぼすかについての体系的かつ記述的な調査を実施。

調査方法

- 自動的処理(ウェブクローラ、テキストクラスタリング、等)により、調査対象とするショッピングサイトとそのユーザ・インタフェースの要素と設計を抽出。
 - Alexaランキング(ウェブサイトのアクセス数のグローバルなランキング)で上位36万1千サイト(英語のサイト;ショッピングサイトに限らない)のリストをAPIから取得。
 - Webshrinker(ウェブサイトを分類するサービス)を用いて46,569のショッピングサイトを抽出し、各サイトのホームページのテキスト情報を分析して、19,455の英語のショッピングサイトのリストを作成。(2018年8月)
 - リストの対象となったサイトについて、独自に設計したクローラを用いて、ある商品を購入する場合の典型的なユーザ・インタラクション(例:商品選択→サイズ・色等の選択→カートへの商品追加→カートの表示→購入・チェックアウト)のフローを把握し、各サイト・ページのデータを収集。(収集したデータはアーカイブ化)
 - 各ページを意味のあるセグメント(約1300万セグメント)に分割し、重複要素を排除して130万セグメントに整理した。次に階層的クラスタリング分析・テキスト分析を行い、ダークパターンの可能性のあるセグメント/クラスターを抽出した。
- 抽出されたサイトやユーザ・インタフェースについて、専門家がダークパターンに該当するか否かを評価。

調査結果

- 約1万1千のショッピングサイトの約5万3千の商品ページを分析した結果、7カテゴリ・15種類に分類される1,818のダークパターンを発見した。
- これらのダークパターンを調査し、欺瞞的な行為を行っているウェブサイトを183件発見した。
- ダークパターンをターンキー・ソリューションとして提供する22の第三者組織も発見した。

*1 Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, Arvind Narayanan, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites", <https://webtransparency.cs.princeton.edu/dark-patterns/>

5. ダークパターンの状況 (2)プリンストン大学・シカゴ大学 2/5

- ダークパターンの7カテゴリ・15タイプの分類と、その検出数・比率は下記のとおり。
- 在庫僅少通知、カウントダウンタイマー、活動の通知、羞恥心の植付けなどが多く検出されている。

カテゴリ	タイプ	説明	事例数	比率
スニーキング	バスケットにこっそり入れる	ユーザの同意なしにショッピングカートに商品を追加する	7	0.4%
	隠された費用	ユーザが購入する直前に、それまで示していなかった(追加的な、かつしばしば高額な)料金がかかることを明らかにする	5	0.3%
	隠された定期購入	1回限りの料金や無料トライアルと見せかけて、ユーザに定期購入・購読の料金を請求する	14	0.8%
緊急性	カウントダウンタイマー	カウントダウンタイマーを使って、ユーザに取引や割引の有効期限が切れることを示す	393	21.6%
	期間の限定通知	期限を指定せずに、取引やセールスの期限が間もなく切れることをユーザに示す	88	4.8%
ミスディレクション	羞恥心の植付け	言葉や感情(恥)を使って、ユーザが特定の選択をしないように誘導する	169	9.3%
	視覚的干渉	スタイルとビジュアル・プレゼンテーションを用いて、ユーザを特定の選択肢に誘導したり、特定の選択肢から遠ざけたりする	25	1.4%
	トリック質問	ユーザを特定の選択に誘導するために、紛らわしい言葉を使う	9	0.5%
	圧迫販売	より高価な商品のバリエーションを事前に選択しておいたり、より高価な商品や関連商品のバリエーションを受け入れるようユーザに圧力をかけたりする	67	3.7%
社会的証明	活動の通知	ウェブサイトでの(他のユーザの)活動(購入、閲覧、訪問など)をユーザに知らせる	313	17.2%
	推薦状	誰によるものか不明な推薦状が製品ページにある	12	0.7%
希少性	在庫僅少通知	数量限定の商品であることを示し、商品へのユーザの欲求を強める	632	34.8%
	高需要通知	商品の需要が高くすぐに売り切れる可能性が高いことを示し、商品へのユーザの欲求を高める	47	2.6%
妨害	キャンセルの難しさ	ユーザがサービスを申し込むのは簡単だが、解約するのは難しい	31	1.7%
強制された行動	強制された登録	タスクを完了させるために、ユーザにアカウントの作成や情報のシェアを強要する	6	0.3%
合計			1,818	100%

5. ダークパターンの状況 (2)プリンストン大学・シカゴ大学 3/5

- 各カテゴリ・タイプについての、ダークパターンのアプローチの分類と認知バイアスの対応は下記のとおり。

カテゴリ	タイプ	分類*1					認知バイアス*1	事例数	サイト数
		非対称	隠密	欺瞞的	情報隠匿	制限的			
スニーキング	バスケットにこっそり入れる			時々	常に		デフォルト効果	7	7
	隠された費用			時々	常に		サンクコストの誤謬	5	5
	隠された定期購入			時々	常に		なし	14	13
緊急性	カウントダウンタイマー		時々	時々			希少性バイアス	393	361
	期間の限定通知		時々		常に		希少性バイアス	88	84
ミスディレクション	羞恥心の植付け	常に		常に			フレーミング効果	169	164
	視覚的干渉	時々	常に	時々			アンカリング効果&フレーミング効果	25	24
	トリック質問	常に	常に				デフォルト効果&フレーミング効果	9	9
	圧迫販売	時々	時々				アンカリング効果&デフォルト効果、希少性バイアス	67	62
社会的証明	活動の通知		時々	時々			バンドワゴン効果	313	264
	推薦状			時々			バンドワゴン効果	12	12
希少性	在庫僅少通知		時々	時々	時々		希少性バイアス	632	581
	高需要通知		時々				希少性バイアス	47	43
妨害	キャンセルの難しさ				時々	常に	なし	31	31
強制された行動	強制された登録	常に				常に	なし	6	6

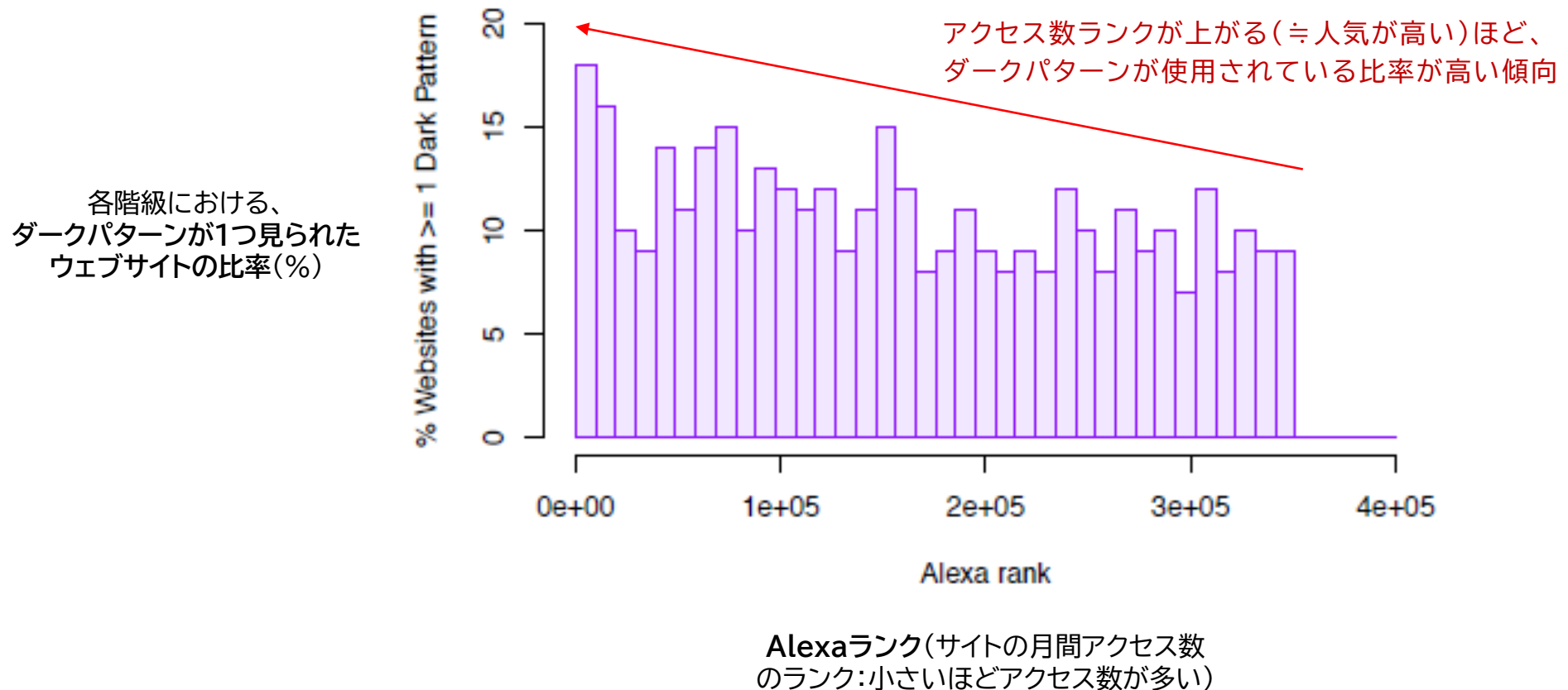
5. ダークパターンの状況 (2) プリンストン大学・シカゴ大学 4/5

- 前ページの「分類」「認知バイアス」については以下のように説明されている。

「分類」		「認知バイアス」	
非対称	<p>ユーザ・インターフェースのデザインは、インターフェースでユーザに提示される利用可能な選択肢に不均等な重みや負担を課しているか？</p> <p>例えば、ウェブサイトはウェブ上でクッキーを受け入れるための目立つボタンを提示するかもしれないが、オプトアウト・ボタンは見えにくくするか、あるいは別のページに隠すかもしれない。</p>	アンカリング効果	個人が将来の意思決定において、最初の情報(「アンカー」)に過度に依存する傾向。
隠密	<p>ユーザ・インターフェース・デザインの選択の効果は、ユーザに隠されているか？つまり、ユーザが知らないうちに、特定の購買をするようにインターフェイスが誘導しているか？</p> <p>例えば、ウェブサイトは「おとり効果」という認知バイアスを活用することがある。ユーザは、おとりの存在が単に意思決定に影響を与えるためであることを認識できず、おとりの効果を隠蔽してしまうかもしれない。</p>	バンドワゴン効果	他人が何かを評価しているように見えることにより、個人がその何かをより高く評価する傾向。
欺瞞的	<p>ユーザ・インターフェースのデザインは、肯定的な虚偽記載、誤解を招く記載、または省略によって、虚偽の信念を誘発するか？</p> <p>例えば、あるウェブサイトがユーザに期間限定の割引を提供することがある。ユーザは、ウェブサイトが割引を提供しようとしていることを認識しているかもしれないが、その取引を利用できる期間が限られていないことに気づいていない可能性がある。この誤った思い込みは、ユーザの意思決定に影響を与える。つまり、セールが繰り返し行われることを知っていれば、ユーザは違った行動をとるかもしれない。</p>	デフォルト効果	惰性により、デフォルトで割り当てられた選択肢に固執する個人の傾向。
情報隠匿	<p>ユーザ・インターフェースは、ユーザに必要な情報の提示を不明瞭にしたり、遅らせたりしていないか？</p> <p>例えば、あるウェブサイトでは、チェックアウトの最後の最後まで、商品の追加料金をユーザに開示しないことがある。</p>	フレーミング効果	同じ情報であっても、その提示のされ方によって、個人が異なる判断を下す傾向。「額縁効果」。
制限的	<p>ユーザ・インターフェースは、ユーザが利用できる一連の選択肢を制限しているか？</p> <p>例えば、あるウェブサイトでは、ユーザが既存のソーシャルメディア・アカウントのアカウントにサインアップすることだけを許可し、そのアカウントに関するより多くの情報を収集できるようにすることができる。</p>	希少性バイアス	希少価値の高いものに高い価値を見出す個人の傾向。
		サンクコストの誤謬	ある行為に資源を投入した場合、その行為によって不利益を被る可能性があっても、その行為を継続しようとする個人の傾向。

5. ダークパターンの状況 (2)プリンストン大学・シカゴ大学 5/5

- ダークパターンを含むウェブサイトのAlexaランク(サイトのアクセス数のランキング)に対する分布をみると、ダークパターンが人気のあるウェブサイトに現れやすいことが示唆された。



6. ダークパターンに関する規制動向

- 米国や欧州では、既存の法規制を用いたダークパターンに関する規制が行われている。
- 他方、EUではダークパターンに対する明示的・多面的な規制(DSA、UCPD等)も動き始めている。

全般的動向

- 米国や欧州では、合計40の法制度が、ダークパターンや欺瞞的パターンの規制に関連するという調査がある*1
 - ・ 内訳は、法律(憲法やEU法を含む):26、米国州法:7、法律に付随する規則:7
- ほとんどはダークパターンを明示的に規制対象とはしていないが、個人情報・プライバシー保護(未成年者も含む)、消費者保護・公正な商取引、競争法(公正競争)、特定業種(例:金融、与信)における顧客保護、オンラインサービス・電子商取引における顧客保護、などの規定を組み合わせる形となっている

*1 <https://www.deceptive.design/laws>

EUの動向

- EUでは、以下のように、明示的・多面的なダークパターン・欺瞞的パターンの規制の動きが始まっている

デジタルサービス法(DSA)	オンラインプラットフォーム提供者がダークパターンを使用することを禁止(第25条)
デジタル市場法(DMA)	ダークパターンや欺瞞的パターンに関する規定はないが、序文(34)および(35)で、商取引の公正性と、公正な競争とは相互に関連しており、その意味で、公序良俗を守り、プライバシーを保護し、詐欺的で欺瞞的な商行為と闘うことが重要と述べている
不公正商慣行指令(UCPD)	第5条(不公正な商慣行の禁止)、第6条(誤解を招く行為)、第7条(誤解を招く記載漏れ)、第8条(攻撃的商行為)、第9条(嫌がらせ、強制、不当な影響の使用)がダークパターンの規制に関連すると考えられている 欧州委員会の通達(「域内市場における企業対消費者の不公正な商慣行に関する欧州議会および理事会指令2005/29/ECの解釈および適用に関するガイダンス」)において、UCPDと関連付けてダークパターンの禁止に明示的に言及している(同通達4.2.7節)
データ法	序文(38)にて、データ最小化の原則から、ダークパターンに依存してデジタル・インターフェースを設計してはならないと述べ、第11条第3項(a)で禁止規定を設置
AI法(案)	「意図的に操作的もしくは欺瞞的な技法を展開するAIシステム」を禁止(第5条第1項(a))
GDPR	ソーシャルメディアにおける欺瞞的パターンに関するガイドラインを発行(前掲)

Ⅱ. プロファイリング

- 1. 定義 (GDPR)
- 2. 分類例(ソーシャルメディアにおけるターゲティング)
- 3. 規制 (1)GDPR
- 3. 規制 (2)DSA
- 3. 規制 (3)DMA
- 3. 規制 (4)現代化指令

1. 定義 (GDPR)

- GDPR(一般データ保護規則)では「プロファイリング」を以下のように定義している*1。

第4条 定義

本規則の目的のために:

(略)

- (4) 「**プロファイリング**」とは、自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱を意味する。

(略)

GDPRの「自動化された個人に対する意思決定とプロファイリングに関するガイドライン」*2では、プロファイリングは、次の三つの要素で構成されているとしている。

- ✓ 自動化された取扱いの形式でなければならない
- ✓ 個人データについて実施されなければならない
- ✓ プロファイリングの目標は、自然人についての個人的側面を評価するためのものでなければならない

*1 個人情報保護委員会仮訳「一般データ保護規則(GDPR)の条文」, <https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>

*2 個人情報保護委員会仮訳, https://www.ppc.go.jp/files/pdf/profiling_guideline.pdf

2. 分類例（ソーシャルメディアにおけるターゲティング）

- GDPRの「ソーシャルメディア・ユーザーのターゲティングに関するガイドライン」*1では、プロファイリングの一例*2として、ソーシャルメディアにおけるユーザのターゲティングを以下のように分類している。

ターゲティング方法	使用するデータ	具体例等
提供データに基づく 個人のターゲティング	「提供データ」: データ主体からソーシャルメディア・プロバイダ及び／又はターゲッターに積極的に提供される情報	<ul style="list-style-type: none"> ・ ソーシャルメディア・ユーザが自身のユーザ・プロフィールの説明に記載した年齢 ・ ユーザがアカウント作成時に登録しているメールアドレス
観察データに基づく ターゲティング	「観察データ」: データ主体がサービス又はデバイスを利用することによりデータ主体により提供されるデータ	<ul style="list-style-type: none"> ・ ソーシャルメディア・プラットフォーム上におけるデータ主体の活動(例: 共有、参照、「いいね」と評価したコンテンツ) ・ アプリが実行されるデバイスの利用(例: GPS座標、電話番号) ・ APIやSDKを使って第三者(アプリ開発者)が取得するデータ ・ ソーシャルプラグイン又はピクセルを埋め込んだ第三者のウェブサイトを通じて収集されるデータ ・ 他の第三者を通じて収集されるデータ ・ ソーシャルメディア・プロバイダが所有又は運営する企業が提供するサービスを通じて収集されるデータ
推定データに基づく ターゲティング	「推定データ」又は「派生データ」: データ主体により提供されるデータ又は管理者により観察されるデータに基づき、データ管理者が作成する	<ul style="list-style-type: none"> ・ ある個人のウェブブラウジング行動及び／又はネットワーク接続に基づき、当該個人が一定の活動又は製品に関心を持つ可能性が高いと推定できる場合がある

*1 個人情報保護委員会仮訳, https://www.ppc.go.jp/files/pdf/targeting_guideline_v2.pdf

*2 ターゲティングとプロファイリングは同義ではないが、同ガイドラインには「広告目的で推定データに基づいてソーシャルメディア・ユーザーのターゲティングを行うには、一般にプロファイリングを行う必要がある。」(パラグラフ83)、「ターゲティングに関連するプロファイリング活動には、個人が積極的に開示していない興味関心又はその他の特性を推定する活動が含まれ、これにより個人が自己の個人データを管理する能力が損なわれる可能性がある。」(パラグラフ10)、「マーケティング又は広告目的での侵襲的なプロファイリング及び追跡活動を行う場合には、管理者が正当な利益を法的根拠としてこうした活動を正当化することは困難であると考えている。」(パラグラフ56)などの記述があり、両者は密接に関連していると捉えられている。

3. 規制 (1)GDPR

- GDPRではプロファイリングに関して、第21条、第22条を含め以下の規制を設けている*1。

第9条	特別な種類の個人データの取扱い	<ul style="list-style-type: none"> 特別な種類のデータ(※)には、プロファイリング行為から派生し又は推定された特別な種類のデータが含まれる。 ※「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータ」
第13条	データ主体から個人データが取得される場合において提供される情報	<ul style="list-style-type: none"> 個人データがそのデータ主体から収集される場合、管理者が、その個人データを取得する時点において、そのデータ主体に対し提供すべき付加的情報に、「プロファイリングを含め、第22条第1項及び第4項に定める自動的な決定が存在すること、また、これが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報」が含まれる。
第14条	個人データがデータ主体から取得されたものではない場合において提供される情報	<ul style="list-style-type: none"> 個人データがデータ主体から取得されたものではない場合、管理者が、データ主体に対し提供すべき付加的情報に、「プロファイリングを含め、第22条第1項及び第4項に定める自動的な決定が存在すること、また、これが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報」が含まれる。
第15条	データ主体によるアクセスの権利	<ul style="list-style-type: none"> データ主体は、管理者から、自己に関する個人データが取扱われているか否かの確認を得る権利、並びに、それが取扱われているときは、その個人データ及び以下の情報にアクセスする権利を有する:「プロファイリングを含め、第22条第1項及び第4項に定める自動的な決定が存在すること、また、これが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデータ主体に生ずると想定される結果に関する意味のある情報」
第21条	異議を述べる権利	<ul style="list-style-type: none"> データ主体は、自己の特別な状況と関連する根拠に基づき、第6条第1項(e)又は(f)に基づいて行われる自己と関係する個人データの取扱いに対し、それらの条項に基づくプロファイリングの場合を含め、いつでも、異議を述べる権利を有する。 管理者は、データ主体の利益、権利及び自由よりも優先する取扱いについて、又は、訴えの提起及び攻撃防御について、やむをえない正当な根拠があることをその管理者が証明しない限り、以後、その個人データの取扱いをしない。 個人データがダイレクトマーケティングの目的のために取扱われる場合(プロファイリングを含む)、データ主体は、いつでも、そのようなマーケティングのための自己に関する個人データの取扱いに対して、異議を述べる権利を有する。※利益のバランスをはかる必要はない
第22条	プロファイリングを含む個人に対する自動化された意思決定	<ul style="list-style-type: none"> データ主体は、当該データ主体に関する法的効果を生じさせる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。 ※「一般に、法的な又は同様の重大な効果をもたらすプロファイリングを含む完全に自動化された個人に対する意思決定は禁止される。(例外あり。例外に該当する場合には必要な措置を講じなければならない。)」とガイドラインは説明している。
第35条	データ保護影響評価	<ul style="list-style-type: none"> 「(a) プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を生じさせ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価」を行う場合、データ管理者は、データ保護影響評価(DPIA)を実施しなければならない。

II. プロファイリング

3. 規制 (2)DSA 1/2

- DSAでは、プロファイリングに関して、以下のような言及・規定がある*1。
- 主なポイントは、プロファイリングに基づく未成年者へのターゲット広告の禁止・特別なカテゴリーの個人データを使用したプロファイリングに基づくターゲティング広告の禁止、である。

デジタルサービス法 (DSA)	序文(56)	本規則は、ホスティングサービスのプロバイダが犯罪の可能性を特定する目的でサービス受領者を プロファイリング する法的根拠を提供するものではない。
	序文(68)	<p>サービスの受領者は、特定の広告が受領者に表示されることを決定するために使用される主なパラメータに関する情報について、広告が表示されるオンライン・インターフェースから直接アクセス可能な形で得られるべきであり、プロファイリングに基づく場合を含め、その目的のために使用されるロジックについて意味のある説明が提供されなければならない。</p> <p>このような説明には、広告を提示するために使用される方法、例えば、文脈に沿った広告であるか、その他の種類の広告であるか、また、該当する場合には、使用される主なプロファイリング基準に関する情報が含まれるべきであり、また、そのような基準を変更するために利用可能な手段についても、受領者に通知されるべきである。</p> <p>広告に関する情報提供に関する本規則の要件は、規則(EU)2016/679の関連規定、特に異議申立ての権利、プロファイリングを含む自動化された個人の意思決定、特にターゲット広告のための個人データの処理に先立ちデータ主体の同意を得る必要性に関する規定の適用を妨げるものではない。</p>
	序文(69)	オンラインプラットフォームのプロバイダは、規則(EU)2016/679の第4条(4)に定義されるプロファイリングに基づく広告を、同規則の第9条(1)に言及される個人データの特別なカテゴリーを使用して、これらの特別なカテゴリーに基づく プロファイリング を使用することを含めて、提示してはならない。
	序文(70)	<p>オンラインプラットフォームは、一貫して、レコメンダーシステムが情報の表示方法にどのような影響を与え、情報がどのように提示されるかに影響を与え得るかについて、サービス受領者に適切な情報が提供されるようにすべきである。</p> <p>サービス受領者が、自分にとってどのように情報が優先されるかを理解できるように、そのようなレコメンダーシステムのパラメータを理解しやすい方法で明確に提示すべきである。</p> <p>これらのパラメータには、少なくとも、サービス受領者に提案される情報を決定する上で最も重要な基準と、プロファイリングとオンライン行動に基づいて情報が優先される場所を含む、それぞれの重要性の理由を含めるべきである。</p>
	序文(71)	オンラインプラットフォームのプロバイダは、サービス受領者が未成年者であることを合理的な確実性をもって認識している場合、サービス受領者の個人データを使用した プロファイリング に基づく広告を提示してはならない。

*1 「プロファイリング」に直接言及している部分を抜粋している(和訳は三菱総合研究所による仮訳)

3. 規制 (2)DSA 2/2

● (つづき)。

デジタルサービス法 (DSA)	序文(94)	<p>リスクの評価および軽減に関する義務は、ケースバイケースで、超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンのプロバイダが、そのレコメンダーシステムの設計を評価し、必要な場合には、例えば、そのような調整がデータ保護法に従っている場合、および情報が規則(EU)2016/679の第9条に言及された個人データの特別なカテゴリーに基づいてパーソナライズされている場合には、脆弱な状況にある人の差別につながるバイアスを防止または最小化するための措置を講じることによって、調整する必要性を引き起こすべきである。</p> <p>さらに、オンラインプラットフォームに適用される推薦システムに関する透明性義務を補完するために、超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンのプロバイダは、一貫して、サービス受領者が、規則(EU)2016/679の意味におけるプロファイリングに基づかない代替選択肢を、推薦システムの主要パラメータについて享受できるようにしなければならない。</p> <p>このような選択肢は、レコメンデーションが表示されるオンライン・インターフェースから直接アクセスできるようにすべきである。</p>
	第26条	<p>オンラインプラットフォームにおける広告</p> <p>3. オンラインプラットフォームのプロバイダは、規則(EU)2016/679の第9条(1)で言及される特別カテゴリーの個人データを使用して、規則(EU)2016/679の第4条(4)で定義されるプロファイリングに基づいて、サービス受領者に広告を提示してはならない。</p>
	第28条	<p>未成年者のオンラインでの保護</p> <p>2. オンラインプラットフォームのプロバイダは、サービス受領者が未成年者であることを合理的な確実性をもって認識している場合、サービス受領者の個人情報を使用して、規則(EU)2016/679の第4条(4)に定義されるプロファイリングに基づく広告をそのインターフェース上で提示してはならない。</p>
	第38条	<p>レコメンダーシステム</p> <p>第27条に定める要件(注:レコメンダーシステムの透明性)に加え、レコメンダーシステムを使用する超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンのプロバイダは、規則(EU)2016/679の第4条(4)に定義されるプロファイリングに基づかない少なくとも1つのオプションを各レコメンダーシステムに提供しなければならない。</p>

II. プロファイリング

3. 規制 (3)DMA 1/2

- DMAでは、プロファイリングに関して、以下のような言及・規定がある。

デジタル市場法 (DMA)	序文(72)	<p>エンドユーザから大量のデータを収集・蓄積するゲートキーパーの慣行が観察されることによる潜在的な悪影響の評価には、エンドユーザのデータ保護とプライバシーの利益が関係する。規則(EU)2016/679の第4条(4)の意味におけるプロファイリングを含むがこれに限定されない、ゲートキーパーが採用するプロファイリング慣行の適切なレベルの透明性を確保することは、コア・プラットフォーム・サービスの競争可能性を促進する。透明性は、潜在的な参入企業や新興企業が同じ範囲や深さ、同じような規模でデータにアクセスできないことを考えると、ゲートキーパーに対して、深い消費者プロファイリングを業界標準にしないよう外圧をかける。透明性の向上により、コア・プラットフォーム・サービスを提供する他の事業者は、優れたプライバシー保証を利用することで、より良い差別化を図ることができるようになるはずである。</p> <p>この透明性義務の最低限の実効性を確保するために、ゲートキーパーは、少なくとも、個人データおよび規則(EU)2016/679に沿ったユーザ活動から得られたデータに依拠しているかどうか、適用される処理など、プロファイリングが実行される根拠について、独立監査による説明を提供しなければならない、プロファイルが作成され、最終的に使用される目的、プロファイリングの期間、当該プロファイリングがゲートキーパーのサービスに与える影響、エンドユーザが当該プロファイリングの利用を効果的に認識できるようにするために取られた措置、同意を求めるための措置、同意を拒否または撤回する可能性をエンドユーザに提供するための措置。欧州委員会は、監査済みの記述を欧州データ保護委員会に移し、欧州連合のデータ保護規則の施行に役立てるべきである。欧州委員会は、欧州データ保護監督官、欧州データ保護会議、市民社会および専門家と協議の上、欧州議会および理事会の規則(EU) No 182/2011(16)および(EU) 2018/1725(17)に沿って、監査された説明の方法論および手順を開発する権限を与えられるべきである。</p>
	序文(99)	<p>本規則の実施条件を統一するため、本規則に基づく義務を効果的に遵守するためにゲートキーパーが実施すべき措置を規定する実施権限を欧州委員会に付与すべきである；ゲートキーパーに課せられた特定の義務の全部または一部を一時停止すること；ゲートキーパーに課された特定の義務の全部または一部を免除すること；ゲートキーパーが本規則に基づく義務を回避する場合に、ゲートキーパーが実施すべき措置を規定すること；ゲートキーパーを指定するための市場調査を終了すること；組織的な違反の場合に救済措置を課すこと；ゲートキーパーに対する暫定措置を命じること；ゲートキーパーを拘束する約束をすること、違反の認定を行うこと、定期的な違約金の支払額を確定すること、ゲートキーパーが提出する通知、情報提出、理由ある要請及び規制報告書の形式、内容及びその他の詳細を決定すること；相互運用性、消費者プロファイリングに使用される技術の監査対象記述の方法論および手順を実施するための運用上および技術上の取り決めを規定すること、手続き、期限の延長、手続き中の権利行使、開示条件、ならびに欧州委員会と各国当局との協力および調整に関する実務的な取り決めを規定すること。これらの権限は、規則(EU)No 182/2011に従って行使されるべきである。</p>

3. 規制 (3)DMA 2/2

● (つづき)。

デジタル市場法 (DMA)	第2条	<p>定義</p> <p>本規則においては、以下の定義が適用される：</p> <p>(略)</p> <p>(31)「プロファイリング」とは、規則(EU)2016/679の第4条(4)に定義されるプロファイリングを意味する；</p> <p>(略)</p>
	第15条	<p>監督の義務</p> <ol style="list-style-type: none"> 第3条に基づく指定後6ヶ月以内に、ゲートキーパーは、第3条(9)に基づく指定決定において列挙されたゲートキーパーがそのコアプラットフォームサービスに適用している、またはそのコアプラットフォームサービス全体にわたって適用している消費者のプロファイリング技術について、独自に監査した説明を欧州委員会に提出しなければならない。欧州委員会は、監査済みの説明を欧州データ保護委員会に提出しなければならない。 欧州委員会は、監査の方法および手順を策定するために、第46条(1)の(g)に言及する実施法を採択することができる。 ゲートキーパーは、第1項の監査された記述の概要を公開しなければならない。その際、ゲートキーパーは、その営業秘密を尊重する必要性を考慮する権利を有する。ゲートキーパーは、少なくとも年1回、その説明と概要を更新しなければならない
	第46条	<p>実施規定</p> <ol style="list-style-type: none"> 欧州委員会は、以下の適用に関する詳細な取り決めを定めた実施法を採択することができる： <p>(略)</p> <p>(g) 第15条(1)に規定されている、消費者のプロファイリングに使用される技術に関する監査説明の方法および手順。この目的のために実施法の草案を作成する場合、欧州委員会は欧州データ保護監督官に諮問するものとし、欧州データ保護会議、市民社会およびその他の関連専門家に諮問することができる；</p> <p>(略)</p>

3. 規制 (4)現代化指令

- 「EU消費者保護規則のより良い執行と現代化に関する指令」(「現代化指令」)では、プロファイリングに関して以下のような言及・規定がある*1。
- 「現代化指令」において、消費者権利指令に自動意思決定によるパーソナライズド・プライシングに関する規定を追加することが定められた。

EU消費者保護規則のより良い執行と現代化に関する指令	序文(45)	事業者は、 自動化された意思決定と消費者行動のプロファイリング に基づいて、特定の消費者または特定のカテゴリーの消費者に提供する価格をパーソナライズすることができる。したがって、消費者は、提示された価格が 自動化された意思決定 に基づいてパーソナライズされた場合、購買決定において潜在的なリスクを考慮できるよう、明確に通知されるべきである。従って、指令2011/83/EUに、 自動化された意思決定 に基づいて価格がパーソナライズされた場合に消費者に通知するための特定の情報要件を追加すべきである。この情報要件は、自動化された意思決定に基づくパーソナライズを伴わない場合、市場の需要に応じて非常に柔軟かつ迅速に価格を変更する「ダイナミック」または「リアルタイム」価格設定などの手法には適用されるべきではない。この情報要件は、特に、 プロファイリングを含む自動化された個人の意思決定 に服さない個人の権利を規定する規則(EU)2016/679を損なうものではない。
消費者権利指令(2011/83/EU)	第6条	<p>遠隔契約および構外契約における情報要件</p> <p>1. 消費者が遠隔契約または宅外契約、またはそれに対応する申し出に拘束される前に、販売者は以下の情報を明確かつ理解しやすい方法で消費者に提供するものとする：</p> <p>(略)</p> <p>(ea) 該当する場合、価格が自動意思決定に基づいてパーソナライズされたこと；</p> <p>(略)</p> <p>※「現代化指令」第4条(4)項(a)(ii)により上記(ea)が挿入される</p>

*1 <https://eur-lex.europa.eu/eli/dir/2019/2161/oj>

Ⅲ. まとめ

1.まとめ

ダークパターン

- 2010年頃から提唱され、多数の分類が示されているが、基本的にはほぼ同様であり、以下のような共通要素を持つ：

目的・結果	<ul style="list-style-type: none"> ・ 利用者の意図しない行為・選択を行わせて、 ・ 事業者の利益に資する結果(利用者の利益に反する場合あり)を得る
手段・手法	<ul style="list-style-type: none"> ・ オンライン・ユーザー・インターフェースを用いて、 ・ 消費者の自律性、意思決定又は選択を破壊又は損なわせる方法で、 ・ 消費者を誘導し、欺き、強要し、あるいは操作する ・ 複数の類型・種類のダークパターンが組み合わされるケースもある

- 欧州委員会は、データドリブン・パーソナライゼーションによる「操作(manipulation)」も警戒している
- DSAが明示的な規制を導入したが(具体的な定義、要件、判断基準等は、欧州委員会による二次立法(ガイドライン)により定められる)、データ保護・プライバシー保護、消費者保護・公正取引、競争政策の側面からも規制が行われている
- DSAの規制は、UCPDやGDPRに影響を与えない

プロファイリング

- EUではGDPRで規制されており、それを参照しつつ、特定の対象(オンラインプラットフォーム: DSA、DMA)や他の側面(消費者保護)に対する規制が強化されている
- また、米国・カリフォルニア州がプロファイリングや自動意思決定技術(ADMT)を規制する規則案を2023年11月に提出している*¹

*¹ <https://cppa.ca.gov/announcements/2023/20231127.html>

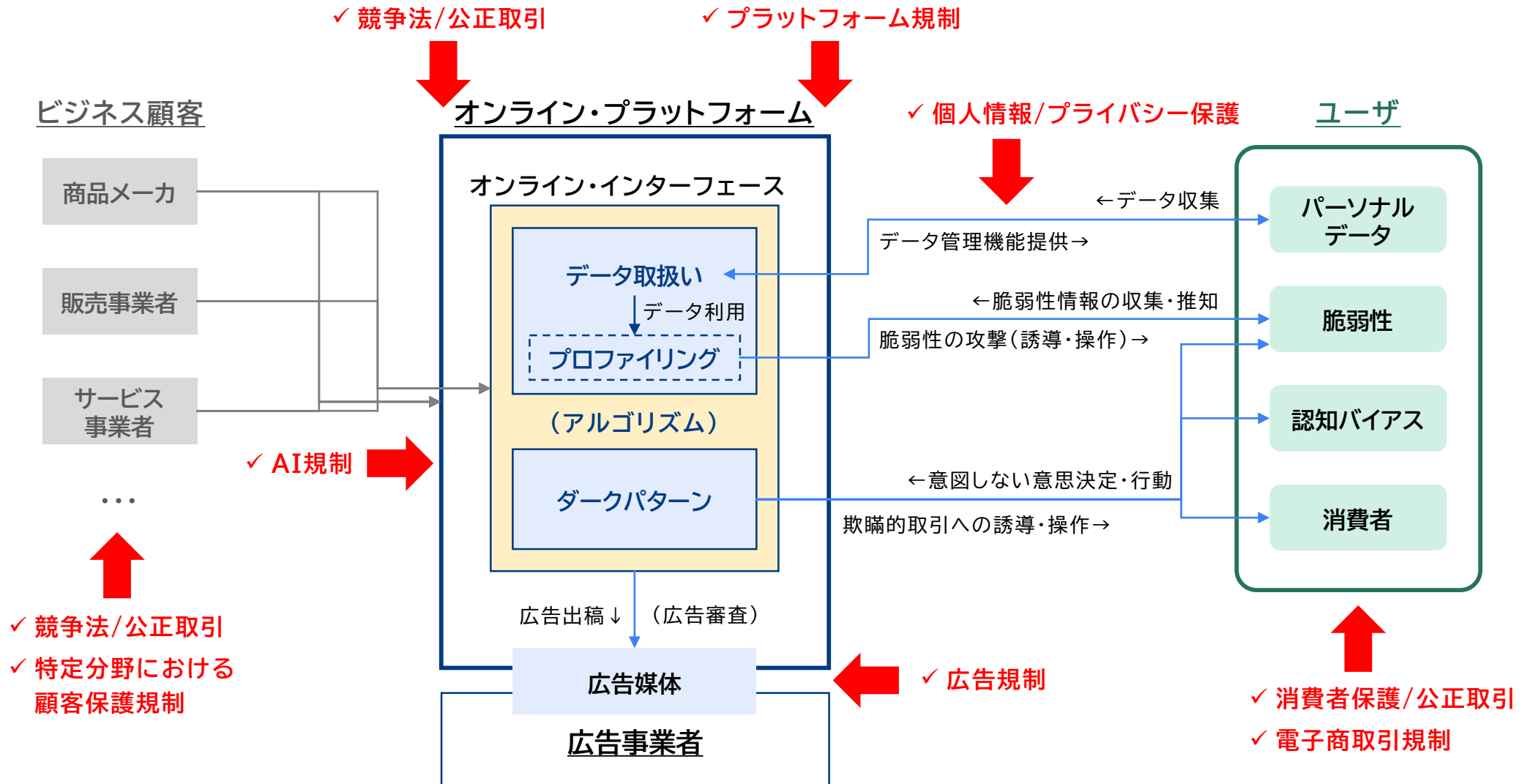
ダークパターン&プロファイリング

- プロファイリングにより個々のユーザの特徴や脆弱性を把握した上で、それに応じてダークパターンを使い分け、より効果的にユーザの「操作(manipulation)」を行うことの問題を指摘する意見・論文も複数みられる*²

*² “Tech Companies and Behaviour Manipulation?”, <https://www.sanrachna.foundation/tech-companies-and-behaviour-manipulation/>
 “THE PROBLEM OF ONLINE MANIPULATION”, <https://illinoislawrev.web.illinois.edu/wp-content/uploads/2020/06/Spencer.pdf>
 “ONLINE MANIPULATION: HIDDEN INFLUENCES IN A DIGITAL WORLD”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006 など

2. 規制の視点・アプローチ

- ダークパターン、プロファイリングは相互に関連しており、多面的な規制が実施・検討されている。



参考資料

- 参考1. DSAの規制対象事業者
- 参考2. DSAにおける対象事業者別の規律一覧
- 参考3. DSAによる事業者の主な義務【一覧】
- 参考4. DSAが規定する事業者の義務【詳細】
- 参考5. 条文構成
- 参考6. DSAにおける管轄・執行機関
- 参考7. システミック・リスク
- 参考8. 関連URL

参考1. DSAの規制対象事業者

- DSAの対象は、情報社会サービスのうちの「仲介サービス」「ホスティングサービス」「オンライン・プラットフォーム」「超大規模オンライン・プラットフォーム」だが、VLOPに該当しない零細・小規模事業者の例外規定(★)が追加された。

情報社会サービス

仲介サービス

ホスティングサービス

オンライン・プラットフォーム

超大規模 オンライン・プラットフォーム

超大規模 オンライン 検索エンジン

仲介サービス 【第2条(g)で規定】

ネットワークインフラを提供する仲介サービス。インターネットアクセスプロバイダ、ドメイン名レジストラの他、以下のホスティングサービスも含む。

第II章では、「単なる導管」、「キャッシング」、ホスティングに分類してそれぞれの免責条件を規定。★零細・小規模事業者(VLOP/VLOSEは除く)は「透明性報告義務」を免除

ホスティングサービス 【同上】

クラウドやウェブホスティングなどのホスティングサービスの他、以下のオンライン・プラットフォームを含む。

オンライン・プラットフォーム 【第2条(i)で規定:第19条・第29条で規制対象から除外する小規模オンラインプラットフォームを規定】

オンライン・マーケットプレイス、アプリストア、コラボレーション・エコノミー・プラットフォーム、ソーシャルメディア・プラットフォームなど、売り手と消費者を結びつけるオンライン・プラットフォーム。★零細・小規模事業者(VLOP/VLOSEは除く)は免除

超大規模オンライン・プラットフォーム(VLOP)、

超大規模オンライン検索エンジン(VLOSE) 【第33条で規定】

非常に大規模なオンライン・プラットフォームは、違法コンテンツの流布や社会的危害において特にリスクがある。欧州の4億5000万人の消費者のうち10%以上の消費者にリーチするプラットフォームや検索エンジンについては、特定のルールが想定されている。

出典: 図および説明文は欧州委員会による説明を用いた。(検索エンジンの部分は加筆。)

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

参考2. 対象事業者別の規律一覧

		仲介サービス	ホスティングサービス	オンライン・プラットフォーム *1	超大規模オンライン・プラットフォーム
違法コンテンツに関する措置命令、情報提供の命令	第9条・第10条	●	●	●	●
連絡先(対当局、対利用者)、法定代理人(必要な場合)	第11条・第12条・第13条	●	●	●	●
利用規約の要件	第14条	●	●	●	●
透明性報告義務	第15条	● *1	●	● *2	● *3
利用者への通知・行動の仕組み、情報提供・理由の記載義務	第16条・第17条		●	●	●
刑事犯罪の疑いに関する通知	第18条		●	●	●
苦情処理・救済の仕組みと裁判外紛争解決	第20条・第21条			●	●
信頼された旗手	第22条			●	●
不正な通知・反論に対する措置及び保護	第23条			●	●
オンライン・インターフェースの設計と構成	第25条			●	●
オンラインプラットフォームにおける広告	第26条			●	● *4
レコメンダー・システムの透明性	第27条			●	●
未成年者のオンラインでの保護	第28条			●	●
トレーダーのトレーサビリティ	第30条			● *1	●
コンプライアンス・バイ・デザイン	第31条			● *1	●
情報を通知される権利	第32条			● *1	●
超大規模オンラインプラットフォーム/検索エンジン	第33条				●
リスク評価、リスク軽減、コンプライアンス機能	第34条・第35条・第41条				●
危機対応メカニズム	第36条				●
独立監査	第37条				●
レコメンダー・システム	第38条				●
データアクセスと精査(当局・研究者)	第40条				●
監督手数料	第43条				●
行動規範、アクセシビリティの行動規範	第45条・第46条			●	●
危機の Protokol	第37条			(●)	●

参考3. DSAによる事業者の主な義務【一覧】

※ 義務の分類(横軸)は三菱総合研究所によるもの

対象事業者	利用者保護	利用規約	コンテンツ等対応	オンライン広告	説明責任・透明性	その他・全般
仲介サービス提供者	<ul style="list-style-type: none"> 利用者向け連絡窓口の設置 利用者が損害補償を求める権利 	<ul style="list-style-type: none"> 利用規約で記載・説明する事項・内容の要件 わかりやすさ、機械可読性の要件 重大な変更の利用者への通知 基本権への配慮と行動の義務 未成年者に理解できる方法での説明 	<ul style="list-style-type: none"> 違法コンテンツ仲介の免責条件 不適切な削除、アクセス制限等への異議申立・救済措置 一般的モニタリング義務なし 司法・行政当局からの措置命令・情報提供命令への報告義務 		<ul style="list-style-type: none"> コンテンツモデレーションに関する透明性報告義務(※VLOPIに該当しない零細・小規模事業者は免除) 	<ul style="list-style-type: none"> 当局向け連絡窓口・国内法定代理人の設置
ホスティングサービス (上記に追加)			<ul style="list-style-type: none"> 違法コンテンツの通知受付体制整備、対応結果の理由の投稿者への通知 刑事犯罪の疑いの当局への通知・情報提供 		<ul style="list-style-type: none"> 透明性報告への追加記載項目(違法コンテンツへの対応) 	
オンライン・プラットフォーム (上記に追加)	<ul style="list-style-type: none"> ダークパターンの禁止 未成年者のプライバシー、安全、セキュリティ保護 利用者が代表組織を通じて権利行使可能 取引事業者に関するKYBC、利用者への開示、事業者の苦情申立*1 違法な製品・サービスについて知った場合に利用者に通知*1 		<ul style="list-style-type: none"> 違法コンテンツ及び利用規約違反コンテンツへの対応に関する苦情の受付体制整備 利用者のADR利用確保 信頼された旗手 悪用対策(違法な製品・サービス提供、違法・根拠のない通知・苦情) レコメンダー・システムの透明性 	<ul style="list-style-type: none"> オンライン広告の透明性 ターゲティング広告の説明・同意取得、拒否・撤回した場合のサービス利用権保証 特別カテゴリー情報を用いたターゲティング広告禁止 未成年者に対するターゲティング広告の禁止 	<ul style="list-style-type: none"> 透明性報告への追加記載項目(苦情処理システムでの対応) 透明性報告の追加義務(ADR、違法・無根拠な通報・苦情、月間平均アクティブユーザー数) 	<ul style="list-style-type: none"> VLOPIに該当しない零細・小規模事業者の義務免除 オンライン広告の行動規範作成 アクセシビリティの行動規範作成
VLOP VLOSE (上記に追加)		<ul style="list-style-type: none"> 利用可能な救済策及び救済メカニズムを含めた利用規約提供 サービスを提供する全加盟国の言語での提供 	<ul style="list-style-type: none"> プロファイリングによらないレコメンダー・システムの提供 危機対応メカニズム(公共安全、公衆衛生等の重大な危機) 	<ul style="list-style-type: none"> オンライン広告の透明性の追加(広告に関するデータベース編纂、APIでの提供) 	<ul style="list-style-type: none"> サービスのシステミック・リスク評価の実施、リスク軽減措置の実施 透明性報告の追加義務(各言語での対応状況) 第三者による独立監査 	<ul style="list-style-type: none"> データへのアクセス(当局、研究者)、アルゴリズムの説明(当局) コンプライアンス機能 監督手数料負担 行動規範の作成 危機のプロトコル作成 欧州委員会による独占的監督権限、罰金等

参考4. DSAが規定する事業者の義務【詳細(1/3)】

※ 義務の分類(横軸)は三菱総合研究所によるもの

対象事業者	利用者保護	利用規約	コンテンツ等対応	オンライン広告	説明責任・透明性	その他・全般
仲介サービス提供者	<ul style="list-style-type: none"> ● 利用者向け連絡窓口設置(わかりやすく使いやすい窓口) ● サービス提供者が義務を侵害したことで利用者が被った損害・損失について、その補償を利用者がサービス提供者に求める権利 	<ul style="list-style-type: none"> ● 記載項目(コンテンツの制限・修正、各種アルゴリズムの説明も含む) ● 平易、ユーザーフレンドリーな記載、機械可読性 ● 重大な変更の利用者への通知 ● 基本権への配慮と行動の義務 ● 未成年者に理解できる方法での説明(未成年者を対象とする場合・未成年者の利用が多い場合) 	<ul style="list-style-type: none"> ● 違法コンテンツを仲介した場合の免責条件(自動的・中間的送信/自動的・中間的・一時的保存、通知と行動;自主的調査の許容) ● 一般的モニタリング義務なし ● 司法及び行政当局からの削除等の措置命令への報告義務(命令の適用・不適用、適用時期) ● 情報提供命令への報告義務(適用したか否か、適用時期、適用の効果) 		<ul style="list-style-type: none"> ● コンテンツモデレーションに関する明確で理解しやすい報告書を、標準化された機械可読な形式・容易にアクセスできる方法で一般に公開 ● 記載項目(当局からの命令件数・内訳;事業者によるコンテンツモデレーション内容、スタッフへの訓練内容、利用者に影響を与える措置、それらの内訳;苦情処理システムでの受理件数;自動化ツールの概要) ● 零細・小規模事業者(非VLOP)は免除 ● 欧州委員会は報告の雛形を規定可能 	<ul style="list-style-type: none"> ● 当局向け連絡窓口・国内法定代理人の設置
ホスティングサービス			<ul style="list-style-type: none"> ● 違法コンテンツの通知受付体制整備 ● 削除、アクセス制限等の対応の理由の投稿者への通知 ● 刑事犯罪の疑いの当局への通知・情報提供 		<ul style="list-style-type: none"> ● 追加記載項目(違法コンテンツの通知件数・内訳、信頼された旗手による通知件数、措置と根拠(法令、利用規約)、自動処理された件数、対応時間) 	

参考4. DSAが規定する事業者の義務【詳細(2/3)】

※ 義務の分類(横軸)は三菱総合研究所によるもの

対象事業者	利用者保護	利用規約	コンテンツ等対応	オンライン広告	説明責任・透明性	その他・全般
オンライン・プラットフォーム	<ul style="list-style-type: none"> ● ダークパターン等*1の禁止 ● 欧州委員会はダークパターンに関する指針を策定可能 ● 未成年者のプライバシー、安全、セキュリティの高い水準での保護(未成年者が利用できるサービスの場合) ● 利用者が代表組織を通じて権利行使可能 <p>【BtoBtoCプラットフォーム*2の追加義務】</p> <ul style="list-style-type: none"> ● 取引事業者に関するKYBC義務、評価の最善努力、利用者への開示、事業者の苦情申立の権利 ● 違法な製品・サービスについてした場合に利用者に通知 		<ul style="list-style-type: none"> ● 違法コンテンツ及び利用規約違反コンテンツへの対応(削除、アクセス制限等)に関する苦情(異議申立)の受付体制整備 ● 利用者の裁判外紛争解決の利用確保 ● 信頼された旗手(通報への対応、旗手の認定) ● 違法な製品・サービス事業者へのサービス停止、違法又は根拠のない通知や苦情が繰り返される場合、通知や苦情の受付停止、それらの基準策定 ● レコメンダー・システムの透明性(パラメータ等の説明、設定変更機能、等) 	<ul style="list-style-type: none"> ● 個々の広告について、広告であること、広告主、広告表示決定に用いられた主なパラメータとその変更方法を、利用者が明瞭、簡潔かつ明白な方法により、かつリアルタイムに確認できるようにする ● ターゲティング広告の説明・同意取得、拒否・撤回した場合のサービス利用権保証 ● 特別カテゴリー情報(例:性的指向、宗教、民族性など)を用いたプロファイリングに基づく広告禁止 ● 未成年者に対するプロファイリングに基づく広告の禁止 	<ul style="list-style-type: none"> ● 追加記載事項(苦情処理システムで受理した苦情の根拠、行われた決定と要した時間、決定を覆した件数) ● 透明性報告の追加義務(裁判外紛争解決機関に提出された紛争件数・解決期間;違法又は根拠のない通知や苦情の受付停止件数;月間平均アクティブユーザ数) 	<ul style="list-style-type: none"> ● 零細・小規模事業者業(非VLOP)は免除 ● オンライン広告の行動規範作成(奨励) ● アクセシビリティの行動規範作成(奨励)

*1 利用者が自由かつ十分な情報に基づいた意思決定を行う能力を、欺いたり、操作したり、あるいは実質的に歪めたり、損なったりすること

*2 「消費者が取引者と遠隔契約を締結することを可能にするオンライン・プラットフォーム」と規定

参考4. DSAが規定する事業者の義務【詳細(3/3)】

※ 義務の分類(横軸)は三菱総合研究所によるもの

対象事業者	利用者保護	利用規約	コンテンツ等対応	オンライン広告	説明責任・透明性	その他・全般
超大規模 オンライン・ プラットフォーム (VLOP) 超大規模 オンライン 検索エンジン (VLOSE)		<ul style="list-style-type: none"> ● 利用規約について、利用可能な救済策及び救済メカニズムを含めて、簡潔で容易にアクセスできる、機械可読な要約を、明確かつ不明瞭さのない言語で提供 ● サービスを提供するEU全加盟国の言語での利用規約提供 	<ul style="list-style-type: none"> ● レコメンダー・システム(プロファイリングによらないレコメンダー・システム提供) ● 危機対応メカニズム(公共安全又は公衆衛生に対する重大な脅威などの危機が発生した場合、欧州委員会は欧州デジタルサービス会議の勧告に基づきVLOP・VLOSEに対し、危機に対するサービスの寄与度の評価、必要な対策の実施、効果の報告を要求できる) 	<ul style="list-style-type: none"> ● オンライン広告の透明性の追加(広告表示から1年後まで、広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂・APIを介して一般に利用可能とする) 	<ul style="list-style-type: none"> ● 提供サービスのシステミック・リスクの評価実施(①違法コンテンツの流布、②基本的権利への悪影響、③市民の言論と選挙プロセス及び公安への悪影響、④ジェンダーに基づく暴力、公衆衛生、未成年者の保護、利用者の身体的・精神的な健康、に関する悪影響)、リスク軽減措置の実施 ● 第三者による独立監査(DSAの定める義務の実施状況、行動規範等の約束の履行状況) ● 透明性報告の追加義務(各言語でのコンテンツモデレーションの人的資源、人員の資格・専門性、教育訓練状況、モデレーションの正確性指標) 	<ul style="list-style-type: none"> ● 規制当局によるデータへのアクセス、規制当局へのアルゴリズムの説明、規制当局の審査に合格した研究者によるデータへのアクセス ● コンプライアンス機能(組織・コンプライアンス・オフィサー) ● 監督手数料の負担(サービスの規模に比例し、全世界の年間純利益の0.05%を超えない) ● 行動規範作成(奨励) ● 危機のプロトコル作成(奨励) ● 欧州委員会による調査(情報要求、聴き取り、査察、等)、暫定措置、約束、モニタリング ● 罰金(前年度の総売上高の6%を上限)

参考5. 条文構成(1/3)

第I章 総則 第1条 主題 第2条 範囲 第3条 定義	第III章 透明で安全なオンライン環境のためのデューデリ ジェンス義務 第1節 すべての仲介サービス提供者に適用される規定 第11条 加盟国当局、欧州委員会、会議への連絡先 第12条 サービス受領者の連絡窓口 第13条 法定代理人 第14条 利用規約 第15条 仲介サービス提供者に対する透明性報告義務 第2節 オンライン・プラットフォームを含むホスティングサービ スの提供者に適用される追加規定 第16条 通知と行動の仕組み 第17条 理由の記載 第18条 刑事犯罪の疑いに関する通知*1 第3節 オンライン・プラットフォームの提供者に適用される 追加規定 第19条 零細企業及び中小企業の排除 第20条 内部苦情処理体制 第21条 法廷外紛争解決 第22条 信頼された旗手 第23条 不正使用に対する措置及び保護 第24条 オンラインプラットフォームの提供者に対する透明性 報告義務 第25条 オンライン・インターフェースの設計と構成 第26条 オンライン・プラットフォームにおける広告 第27条 レコメンダー・システムの透明性 第28条 未成年者のオンラインでの保護	第4節 消費者が取引業者と遠隔契約を締結す ることを可能にするオンライン・プラッ トフォームの提供者に適用される規定 第29条 零細企業及び中小企業の排除 第30条 トレーダーのトレーサビリティ 第31条 コンプライアンス・バイ・デザイン 第32条 情報を通知される権利 第5節 システムリスクを管理するための超大規模 オンライン・プラットフォームの提供者及び 超大規模オンライン検索エンジンの提供者 の追加義務 第33条 超大規模オンライン・プラットフォーム及び 超大規模オンライン検索エンジン 第34条 リスク評価 第35条 リスクの軽減 第36条 危機対応メカニズム 第37条 独立監査 第38条 レコメンダー・システム 第39条 オンライン広告の追加的透明性 第40条 データアクセスと精査 第41条 コンプライアンス機能 第42条 透明性報告義務 第43条 監督手数料
---	--	--

参考5. 条文構成(2/3)

第Ⅲ章 (つづき)		第3節 欧州デジタルサービス会議	
第6節 デューデリジェンス義務に関するその他の規定		第61条	欧州デジタルサービス会議
第44条	標準	第62条	会議の構成
第45条	行動規範	第63条	会議の任務
第46条	オンライン広告の行動規範	第4節 超大規模オンライン・プラットフォームの提供者及び超大規模オンライン検索エンジンの提供者に関する監視、調査、遵守及びモニタリング	
第47条	アクセシビリティの行動規範	第64条	専門知識及び能力の開発
第48条	危機のプロトコル	第65条	超大規模オンラインプラットフォームの提供者及び超大規模オンライン検索エンジンの提供者の義務の執行
第Ⅳ章 実施、協力、制裁及び執行		第66条	委員会による手続開始と調査への協力
第1節 管轄当局及び各国デジタルサービス調整官		第67条	情報の要求
第49条	管轄当局及びデジタルサービス調整官	第68条	聴取り・陳述を行う権限
第50条	デジタルサービス調整官の要件	第69条	検査の権限
第51条	デジタルサービス調整官の権限	第70条	暫定措置
第52条	罰則	第71条	約束
第53条	苦情を申し立てる権利	第72条	モニタリング行為
第54条	補償金	第73条	不遵守
第55条	活動報告	第74条	罰金
第2節 権限、協調した調査及び一貫性メカニズム		第75条	第Ⅲ章第5節で定められた義務の侵害に対処するための救済措置の監督強化
第56条	権限	第76条	定期的な違約金の支払い
第57条	相互支援	第77条	刑罰の制限期間
第58条	デジタルサービス調整官の国境を越えた連携	第78条	刑罰の執行の制限期間
第59条	委員会への照会	第79条	聴取及びファイルにアクセスする権利
第60条	共同調査	第80条	決定の公表
		第81条	欧州連合司法裁判所による審査
		第82条	アクセス制限の請求と国内裁判所との連携
		第83条	欧州委員会の介入に関する実施法

参考5. 条文構成(3/3)

第IV章 (つづき)	
第5節 執行に関する共通規定	
第84条	職業上の秘密*2
第85条	情報共有システム
第86条	代理*3
第6節 委任及び実施法	
第87条	委任の行使*4
第88条	委員会手続き
第V章 最終条項	
第89条	指令2000/31/ECの修正
第90条	指令-(EU) 2020/1828の改正
第91条	見直し
第92条	超大規模オンラインプラットフォーム及び超大規模オンライン検索エンジンの提供者への適用予定
第93条	効力の発生及び適用*5

- *1 議会修正版(2022年1月)では、刑事犯罪やその疑いを知った際に、当局への通報に加えて、コンテンツの削除・無効化が義務付けられていたが、三者合意版では削除されている
- *2 欧州委員会、EU理事会、加盟国の規制当局及びそれらの職員・関係者に関する義務規定
- *3 サービス利用者側の代表組織に関する規定(代表組織の要件、利用者に代わり異議申立を行う権利等)
- *4 本規則(DSA)の規定についての委任法令を採択(二次立法)する欧州委員会の権限、DSAにおける権限の一部の欧州委員会への委任、当該権限の委任を撤回する欧州議会及びEU理事会の権限
- *5 2024年2月17日から適用(発効)

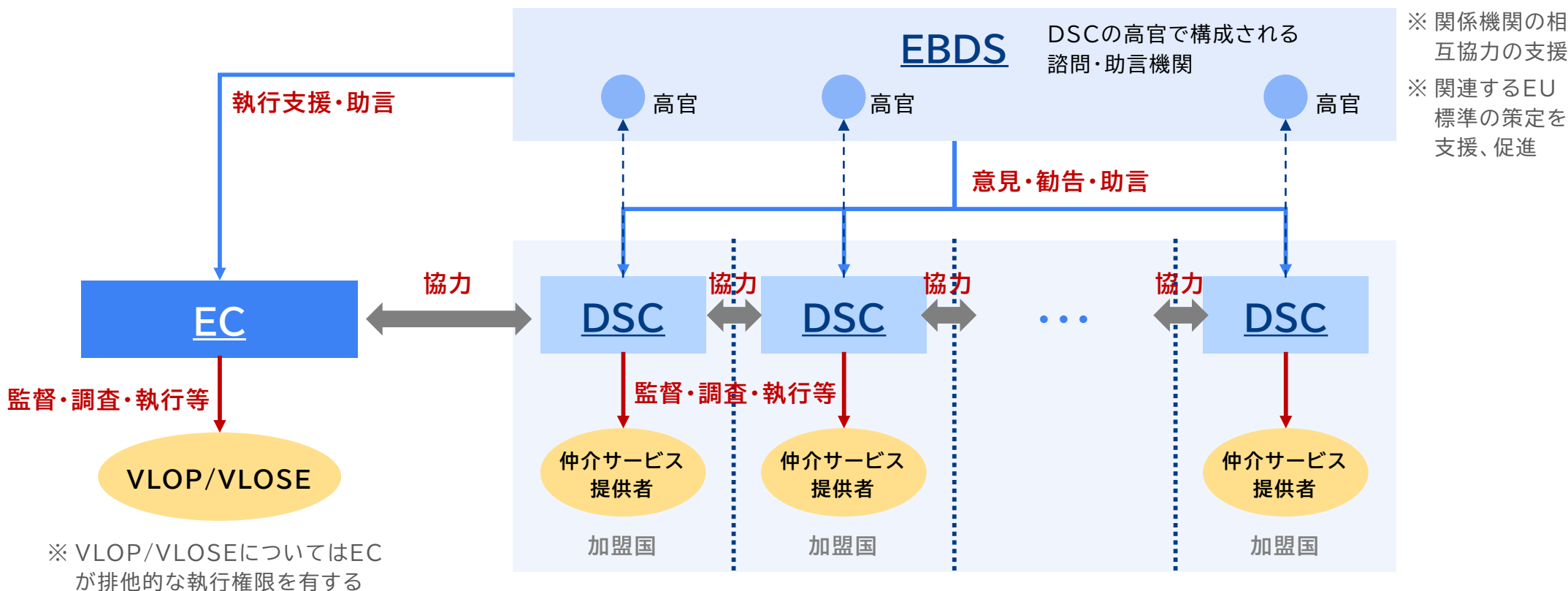
ただし、第24条第2項、第3項および第6項、第33条第3項から第6項まで、第37条第7項、第40条第13項、第43条ならびに第4章第4節、第5節および第6節は、2022年11月16日から適用される

【注】

- 第24条:第2項(EUにおけるMAU数の公表)、第3項(同・当局への伝達)、第6項(透明性報告書の様式等の策定)
- 第33条:第3項(MAU数の算定方法の策定)、第4項(VLOP/VLOSEの指定決定)、第5項(VLOP/VLOSEの解除決定)、第6項(指定/解除の決定の通知)
- 第37条:第7項(独立監査の手続的手順、監査方法及び報告様式の策定)
- 第40条:第13項(VLOP/VLOSEのデータのアクセス/共有方法の決定)
- 第43条:監督手数料

参考6. DSAにおける管轄・執行機関

- DSAでは、欧州委員会、加盟各国のデジタルサービス調整官(Digital Services Coordinator)、欧州デジタルサービス会議(European Board for Digital Services)が管轄機関としてそれぞれの役割を果たす。



EC : 欧州委員会(European Commission)

DSC : デジタルサービス調整官(Digital Services Coordinator)

EBDS : 欧州デジタルサービス会議(European Board for Digital Services)

出典: DSA条文に基づき三菱総合研究所作成

参考7. システミック・リスク

- DSAでは、VLOP/VLOSEの「システミック・リスク(systemic risks)」がオンラインの安全性、世論と言説の形成、及びオンライン取引に与える広範かつ強力な影響について大きな懸念を示している。
- システミック・リスクは、VLOP/VLOSEの「広告主導のビジネスモデル」に起因し、その「サービスの設計、機能、使用、及びサービスの受領者による潜在的な誤用から生じる」としており、中でもサービスの「アルゴリズムシステム」を注視している。

DSAで提示されているシステミック・リスク

- 違法コンテンツの流布や、EUや国内の法律で禁止されている製品やサービスの販売などの違法行為が行われることに関するリスク
- 欧州連合基本権憲章で保護されている基本的権利の行使に対する、サービスの実際のまたは予見可能な影響に関するリスク
 - 特に、人間の尊厳に対する基本的権利(憲章第1条)、私のおよび家族生活の尊重に対する基本的権利(憲章第7条)、個人情報保護(憲章第8条)、メディアの自由と多元性を含む表現と情報の自由(憲章第11条)、非差別(憲章第21条)、児童の権利の尊重(憲章第24条)、高水準の消費者保護(憲章第38条)、に対する実際のまたは予見可能な悪影響
- 民主的プロセス、市民の言説、選挙プロセス、および公安に対する実際のまたは予見可能な否定的影響に関するリスク
- 公衆衛生、未成年者の保護、人の身体的・精神的幸福、ジェンダーに基づく暴力の保護に対する、実際のまたは予見できる深刻な悪影響に関するリスク

システミック・リスクの評価

リスク評価において、特に以下の要因が影響しているか考慮する：

- レコメンダーシステム及びその他のアルゴリズム・システムの設計
- コンテンツ・モデレーション・システム
- 利用規約及びその実施
- 広告の選択及び提示システム
- データ取扱いに関する提供者の慣行

- ①サービスの意図的な操作(不正使用、自動的利用)、
 - ②違法コンテンツ・利用規約に違反する情報の増幅及び迅速かつ広範な普及の可能性
- の影響の有無・形態についても分析

特定の地域的または言語的側面も考慮して評価(特定の加盟国固有の場合等)

(DSA序文80～83、第34条に基づいて整理)

参考8. 関連URL

デジタルサービス法(DSA)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)

<https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

未来を問い続け、変革を先駆ける

MRI 三菱総合研究所