L-011

ダークパターン検出に向けた UI 画像データセットの構築

Development of a UI-Based Image Dataset for Detecting Dark Patterns

石井 健太† 武田 利浩†
Ishii Kenta Taketa Toshihiro

1. はじめに

近年、インターネットを介した購買行動が一般化する中で、ユーザーインターフェース（UI）の設計がユーザーの購買行動に与える影響について注目されている。特に、ユーザーが意図しない行動を誘導する「ダークパターン（ディセプティブデザイン）」の存在が問題視[1]されており、社会的にも倫理的な課題となっている。たとえば、定期購入と一回購入の違いが分かりづらい設計や、解約ページへのアクセスが困難な構成、意図しない商品のカート追加など、日常的に多くのユーザーが影響を受けている。これらの設計は、企業の利益を目的としているが、結果としてユーザーの信頼を損ねる可能性がある。

従来の研究では、主にテキストデータを用いたダークパターンの検出が行われてきたが、ボタンの大きさ・色・配置といった視覚的な要素が判断基準となるケースには不十分である。そこで本研究では、ダークパターン検出に向けた UI 画像データセットの構築を目的とする。

2. ダークパターン

2.1 ダークパターンの定義

「ダークパターン」は UX デザイナーHarry Brignull[2]によって 2010 年に「ユーザーが意図していない行動を行わせるウェブサイトやアプリのトリック」と定義された。2022 年頃からは「ディセプティブデザイン」とも呼ばれている。

2.2 関連研究

Mathur[3]らは、2019 年にショッピングサイトの大規模調査を実施し、11,286 件のショッピングページから 1,818 件のダークパターン抽出を行い、「Urgency」「Misdirection」「Social Proof」「Scarcity」「Obstruction」「Sneaking」「Forced Action」の 7 つに分類した。例えば「Urgency」は『〇〇分でセール終了』といったタイマー付きメッセージ（図 1）によってユーザーを焦らせる、「Misdirection」は特定の選択を避けるようにユーザーを誘導する UI 構成である。調査結果を、データセット[4]として GitHub 上に公開した。

図 1 Urgency 例

矢田[5]らは Mathur[3]らの調査結果を基に、テキストベースのデータセット E-Commerce Dark Pattern Dataset を構築し、分類モデルの学習とダークパターンの検出を行った。

しかし、いずれも視覚デザインそのものには着目しておらず、視覚的な特徴を含むダークパターンの検出には限界がある。

3. 構築方法

3.1 分類

Mathur らの分類[6]は学術的信頼性、包括性、実践的適用性、分析的枠組みの面で優れているためこれを採用することとする。ただし、「Sneaking」と「Obstruction」については、以下の理由から UI 画像の自動収集において商品の誤購入の危険性が考えられるため、収集の対象外とする。

- 「Sneaking」：発見のためには商品をカートに追加する必要がある。
- 「Obstruction」：契約画面を表示する必要がある。

したがって、本研究では Mathur らの 7 分類から、上記 2 分類を除外した 5 分類に、「No Dark Patterns」を加えた 6 分類とする。

3.2UI 画像の収集

UI 画像の収集には、スクリーンショット自動撮影プログラムを作成して行う。このプログラムは、Mathur データセット[4](CSV ファイル)に含まれる URL を参照し、ショッピングページの UI 画像を自動で撮影し、フォルダに保存される。

収集できた UI 画像から、データセットとしては扱えない商品ページではない UI 画像や、「Page Not Found」、「404」などが含まれる UI 画像の除外を行う。画像はすべて目視でチェックを行い、手作業で行う。UI 画像の除外結果と URL を、CSV ファイルに自動で記録を行えるようにプログラムを作成する。

3.3UI 画像の分類

UI 画像の分類には、UI 画像分類ツールを作成して行う。このツールは、1 枚の UI 画像と 2.1 で示した 6 分類のチェックボックスで構成され、複数項目のチェックを可能とする。

分類結果を管理できるよう 3.2 で作成した CSV ファイルに、自動で分類結果を書き込まれるようにし、分類ごとのフォルダを作成して、UI 画像が保存されるようにする。

† 山形大学 大学院 理工学研究科
Graduate School of Science and Engineering, Yamagata University

4. 結果

4.1UI 画像の収集

UI 画像の収集は、2024 年 11 月 1 日から 2 日の 2 日間にかけて実施した。対象は、Mathur らのデータセット[4]に含まれる 1,818 件の URL である。

UI 画像の収集には、スクリーンショット自動撮影プログラムを使用して、ショッピングページの UI 画像収集を行った。1,818 件の URL 中、撮影が行えた URL は 1,578 件、サイトが削除された等の理由からエラーが起き、撮影が行えなかった URL は 241 件であった。撮影が行えた URL1,578 件の UI 画像のうち、データセットとしては扱えない商品ページではない UI 画像や、「Page Not Found」といった UI 画像 752 件を除外し、実際にデータセットとして使用可能であった UI 画像は 826 件だった。

4.2 ダークパターンの分類結果

4.1 で商品ページだった UI 画像 826 件に対して、ダークパターン分類に基づいて UI 画像分類ツールを使用して分類を行ったところ、332 件のダークパターンが含まれていた。分類件数は、「Urgency」が 43 件、「Misdirection」が 8 件、「Social Proof」が 29 件、「Scarcity」が 45 件、「Forced Action」が 206 件、「No Dark Patterns」が 494 件だった。最も多かったダークパターンの分類は「Forced Action」で全体の約 62%を占めていた。

4.3Mathur データセット[4]との比較

図 2 に、Mathur データセット[4]における分類数と本研究で得られた分類結果の件数を比較して示す。図からわかるように、「Forced Action」以外の分類は軒並み件数が減少している一方で、「Forced Action」は Mathur データセットでは 5 件であったものが、本研究では 206 件へと大幅に増加している。

また、各分類について Mathur データセット[4]から本研究への分類変遷分析「Mathur→本研究」についても調べた。Mathur データセットでの分類が本研究でもそのまま残っていた分類「あり→あり」が 64 件。逆に、Mathur データセットでは無かったが、本研究で新たに発生した分類「なし→あり」が 268 件だった。特に、分類の発生率が高かったのは「Forced Action」(50.3%)であり、他の分類(1%~3%程度)と比較して非常に高かった。

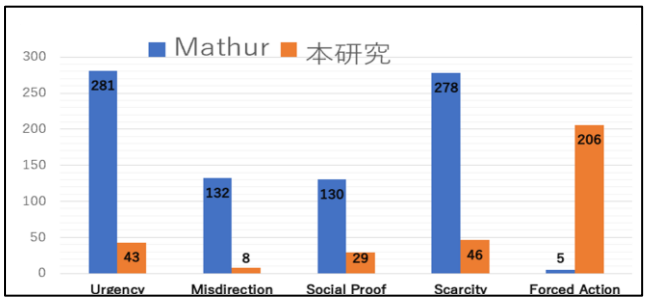

図 2　データセットの比較

5. 考察

ダークパターンの検出数が想定より少なかった要因として、参照元である Mathur データセットが 2019 年以前に収集されたものであり、多くのページが既に削除または、改変された可能性が高い。実際に 1,818 件中 UI 画像収集時点で原型を保っていたのは 64 件(約 3.5%)に過ぎず、ウェブサイトのデザインやダークパターン使用傾向が 5 年間で大きく変化している事が確認された。また、近年の GDPR[7]や CCPA[8]などの法整備の進展により、企業が法的リスクを回避するために UI を修正した可能性も考えられる。特に、Forced Action の増加は、Cookie 同意やアカウント作成を必須とする設計の普及と関連しており、これらは一概に悪意のある設計とは言い切れず、法令遵守やユーザー保護を目的とした正当な設計も含まれている。これにより、近年のダークパターンは「悪意」と「必要性」の境界が曖昧になりつつある点が示唆される。

6. 結論

本研究では、ダークパターン検出に向けた UI 画像データセットの構築を行った(全 332 件)。しかし、学習用データとしては十分な量とは言えず、検出対象も視覚要素に限定されていたため、実用的な汎用モデルの構築には至らなかった。また、参照元の Mathur データセット[4]の多くが、ページ削除・改変により変化していたことから、今後の研究では最新の URL リソースを用いたデータ収集が不可欠である。

今後の課題は、動的なウェブコンテンツへの対応や、最新の UI 設計に即した分類体系の再検討、そして十分な量のデータ収集によるデータセットの拡充を進めることで、より実用性の高い検出モデルの実現である。さらに、テキストやユーザー行動の誘導ロジックなど、視覚以外の要素も複合的に関与するダークパターンを検出するには、HTML 構造やユーザー操作のログなどを統合的に解析するマルチモーダルなアプローチが必要である。

参考文献

[1] Voigt, C., Schlögl, S., & Groth, A. (2021). *Dark patterns in online shopping: Of sneaky tricks, perceived annoyance and respective brand trust*. In F. F.-H. Nah & K. Siau (Eds.), *HCI in Business, Government and Organizations* (Lecture Notes in Computer Science, Vol. 12783, pp. 143–155). Springer.
URL:https://doi.org/10.1007/978-3-030-77750-0_10

[2] H. Brignull, Deceptive Design,
URL:https://www.deceptive.design/

[3] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), Article 81:1–81:32.
URL: https://doi.org/10.1145/3359183

[4] Mathur Dark Patterns Dataset
URL: https://github.com/aruneshmathur/dark-patterns/tree/master

[5] 矢田宙生, 「E コマースサイトにおけるダークパターンの自動検出」, 早稲田大学, 2023

[6] Mathur, A. et al., “Dark Patterns at Scale: Dataset and Classifications,”
URL: https://webtransparency.cs.princeton.edu/dark-patterns/

[7] *Regulation (EU) 2016/679*. Official Journal of the European Union, L119, 1–88.
URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[8] California Office of the Attorney General. (2020). *Final Statement of Reasons: California Consumer Privacy Act Regulations (Title 11, Division 1, Chapter 20)*.
URL: https://oag.ca.gov/privacy/ccpa