Vol.2021-CSEC-94 No.20
Vol.2021-SPT-43 No.20
2021/7/19

アプリのトラッキング許可に対するダークパターン調査

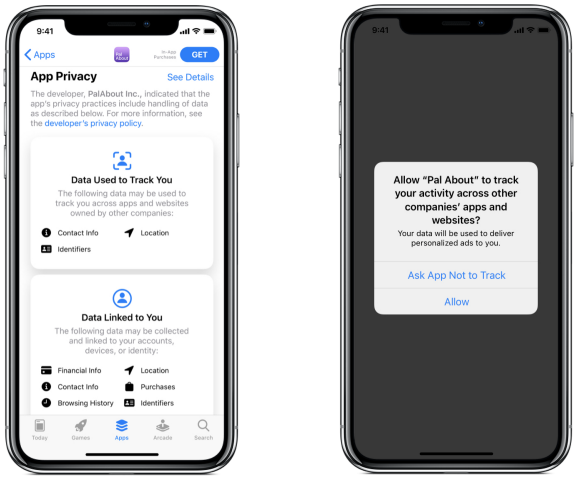
坂本 一仁[1,a)]

概要：Apple 社は iPhone などのモバイル端末 OS である iOS14 からアプリトラッキング透明性 (App Tracking Transparency) を適用し，その一環として広告用識別子の IDFA (Identifier for Advertisers) の利用をユーザのオプトイン形式とした．アプリ事業者は IDFA を利用した複数事業者間での広告測定を行う場合，アプリユーザにトラッキングを許可してもらう必要がある．Apple 社の公式ドキュメントでは，トラッキングの許可を求める画面の前に追加の説明を表示してもよいとしているが，不要なデータアクセスに同意するようユーザを誘導したり，だましたり，強制したりするダークパターンは禁止している．本論文では，Apple のアプリ配信プラットフォームである App Store の日本の無料 Top100 アプリを調査し，IDFA 許可に関する画面においてダークパターンがどの程度存在するかを調査した．調査の結果，35 アプリで IDFA 許可に関する画面が確認され，31 アプリ (88.6%) で少なくとも 1 つのダークパターンが観測された．本論文の貢献として，これまでのダークパターン項目を横断的に整理し，IDFA のオプトイン化に伴うダークパターンの実態を早期に発見し，加えて新たな分類のダークパターンを定義した．

キーワード：ダークパターン，トラッキング許可，IDFA，アプリトラッキング透明性，iOS アプリ

1. はじめに

Apple 社が提供する iPhone は日本のスマートフォン市場において高い普及率を得ている．Apple 社は近年とくに利用者のプライバシー保護に注力しており，特設サイト [1] を設けるなど積極的な施策を打ち出している．Apple 社のプライバシー保護の取り組みの 1 つがアプリトラッキング透明性 (App Tracking Transparency) である．iOS14 からアプリ事業者は，「ユーザのトラッキングに使用されるデータ」や「ユーザに関連付けられたデータ」をアプリ公開時に設定することが義務付けられ，アプリの説明ページに内容が公開されることになった [2] (図 1(a))．また，iOS が広告事業者向けのトラッキング識別子として提供している IDFA (Identifier for Advertisers) の利用がオプトイン形式に変更された．これまで広告事業者はアプリ事業者に提供している広告 SDK (Software Development Kit) 等で単一の識別子である IDFA を利用して事業者横断で利用者をトラッキングしターゲティング広告を配信していた．これまでも利用者は iOS の設定から IDFA に対するオプトアウトや IDFA 値の変更ができるようになっていたが，iOS14.5 からは個々のアプリでダイアログが表示され，アプリ毎にオプトイン形式で IDFA 利用の許諾を取る形に変更された (図 1(b))．



(a) (b)

図 1 Apple のアプリトラッキング透明性の表示例 [2]．(a) はアプリのダウンロード画面に表示される「アプリのプライバシー」で，アプリにおけるデータ利用がラベル形式で表示される．(b) はアプリ利用中に表示される IDFA を使用するためのトラッキング許可選択画面で，一度だけ表示される．

ここで，多くのアプリ事業者は IDFA の許諾を利用者から得るために，IDFA によるトラッキングの許可を求める画面の前に，独自の説明画面を表示するようになった．Apple 社の公式ドキュメントにおいても，トラッキングの許可を求める画面の前に追加の説明を表示してもよいとし

[1] 株式会社 DataSign (DataSign Inc.)
[a)] sakamoto@datasign.jp

ⓒ 2021 Information Processing Society of Japan

ているが，不要なデータアクセスに同意するようユーザを誘導したり，だましたり，強制したりするダークパターンは禁止している [2].

他方，2018 年 5 月に施行された EU 一般データ保護規則 (GDPR: General Data Protection Regulation) [7] では，Cookie のようなオンライン識別子を個人データとして扱い，正当な利益を有しない個人データの利用に対しては自由に与えられた明確な同意を必要とすること，利用者のデータを透明かつ公平な方法で合法的に扱うことなどを事業者へ求めた．具体的に GDPR に適法するためにはいくつかの利用目的に対する Cookie の利用をオプトイン形式で取得する必要があり，多くのサイトで Cookie バナーや CMP (Consent Management Platform) と呼ばれるツールが導入され，Cookie 等のオンライン識別子を利用したトラッキングに対する同意取得が行われている．しかしながら，大半の CMP の UI はダークパターンであり GDPR において有効な同意でないと指摘されている．Utz ら [17] は，クローリングで集めた 5,087 の同意通知から 1,000 をサンプリングして分類し，UI の影響についてユーザスタディを実施しているが，彼らの報告では，ボタン強調や事前チェックといったナッジの応用が利用者の選択に影響があったとしている．Nouwens ら [15] は 680 の CMP 導入サイトを調査し，GDPR 準拠の基準を設定して CMP が GDPR 準拠の同意を実施しているかを調査した．彼らの報告では，12.6%のサイトがすべて許可とすべて拒否が同じぐらい簡単であり，11.8%のサイトのみが GDPR 基準であったと結論付けている．また，8 種類の CMP デザインを利用したダークパターンの影響実験では，「すべて拒否」のボタンを設置しない方が「すべて許可」を選択する傾向が 22%増加するとしている．Machuletz ら [11] は，CMP のダークパターンに焦点を当て，4 つの仮説を検証している．結果として，「すべて許可」ボタンをハイライトしたものは，ハイライトしないものと比べて 4 倍の影響があり，それは必ずしも利用者が納得した上で選択しているものではないことを明らかにしている．

このように，Cookie 利用がオプトイン形式に変わったため，多くの利用者にオプトインを強要させるダークパターンが横行することになった．過去の事例を見るに，今回の IDFA 利用許諾のオプトイン化においてもダークパターンの手法が多く用いられることが予想される．そこで本論文では，Apple のアプリ配信プラットフォームである App Store の日本の無料 Top100 アプリを調査し，IDFA 許可に関する画面においてダークパターンがどの程度存在するかを調査した．ダークパターンの調査には Gray ら [9] のダークパターン分類をベースとして，Mathur ら [12] と，NCC レポート [14] の分類を組み合わせ，IDFA 許可に関する画面がダークパターンに該当するかどうかを判定した．また，既存のダークパターン分類に当てはまらない新たなパターンを定義できるかどうかも分析した．

調査の結果，35 アプリで IDFA 許可に関する画面が確認され，31 アプリ (88.6%) で少なくとも 1 つのダークパターンが観測された．また，16 アプリで IDFA 許可選択画面の前に追加の説明画面が確認されており，8 アプリ (50%) は Apple 社がガイドラインで禁止しているダークパターンに該当する画面内容であった．

本稿の貢献は下記の通りである．

1) IDFA オプトイン化に伴う早期のダークパターン調査を実施し，日本の iOS アプリにおける実態を示した (4.2 節).
2) これまでのダークパターン分類項目を横断的にまとめ，幅広いダークパターン判定に利用できる形とした (表 A·1, A·2).
3) これまでのダークパターン分類にない新たなダークパターンを発見し，新たな定義としてまとめた (4.2 節).

本稿の構成は以下のとおりである．2 章でダークパターンの既存研究や分類について説明する．3 章では調査手法について説明する．4 章で調査結果について示し，5 章で議論を展開する．最後に，6 章にて本稿のまとめとする．

2. ダークパターンとは

ダークパターンは Brignull によって 2010 年ごろに名付けられた概念である [4]．Brignull のウェブサイトではダークパターンを「意図しないことを実行させるトリック」という説明をしているが，今日までの多くのダークパターン研究において，ダークパターンとはどういうものか，様々な定義がされている．

例えば Mathur らの 2019 年の文献では [12]，ダークパターンはユーザにとって潜在的に有害な誘導，強制，騙しの UI と定義している．Geronimo ら [6] においても，ダークパターンは悪意を持って意図しない行動を実行させるものとという強い表現で定義している．一方，ノルウェー消費者委員会 (NCC: Norwegian Consumer Council) のダークパターンに関するレポート [14] では，誤解を招く表現や錯覚を与えるものと説明している．

また，ダークパターンと類似した概念として，BADUI や Sludge と同じ文脈で用いられることがある．BADUI は意図的でなく悪い UI になっているものも含むことがあり，Sludge は Nudge とは反対に行動を思いとどまらせるものと言われるが，ダークパターンは意図的であり Nudge 以外の手法も多く含まれるため，本論文では独立した概念と考える．

以上のように，ダークパターンの概念や定義は文献によって幅があるが，本論文で過去の様々な議論から中立的な解釈を導出して「**あるコンテキストにおいてユーザに深い理解を促さず，ユーザよりも事業者の利益を優先させるように働くもの**」とダークパターンを定義する．

2.1 ダークパターンの既存研究

初期のダークパターン研究として, Brignull は倫理的でない UIUX デザインを分類し，体系化している [4]．Brignull は長らく SNS での報告や通報ベースでダークパターンに対する活動を行なっているが，近年では分類学 (Taxsonomy) として研究が発展している．

Bösch ら [3] は，ダークパターンを定義するテンプレート（ダークパターン名，効果，対策などを記述するための様式）を提案している．Gray ら [9] は，Brignull の分類を拡張してより使いやすい 5 つのカテゴリを定義した．2 ヶ月間ダークパターンを SNS，ブログ，ニュースなどから収集したコーパスを作成し，グラウンデッドセオリーアプローチによって 5 つの主要なダークパターンを特定しカテゴリ化している．Mathur ら (2019)[12] は，ブログや SNS で報告されたダークパターンでは受動的な観測しかできないため，能動的にダークパターンを発見しに行くアプローチをとっている．この論文では Alexa Top Site からショッピングサイト約 11k を抽出し，クラスタリングされた製品ページをサンプリングして調査することで大規模なダークパターン調査を実現している．分類は Gray らの分類をベースにしているが，新たに発見したダークパターンを追加し，7 カテゴリ 15 タイプを報告している．また，ダークパターン実装を提供している 22 のサードパーティライブラリについても言及している．

Geronimo ら [6] は，240 の Android アプリに対してダークパターンを調査している．分類は Gray らの 5 カテゴリを利用し，結果として 240 アプリの 95%に 1 つ以上のダークパターンが存在したと報告している．NCC のレポート [14] では，GDPR 施行後に Facebook, Google, Windows10 の設定画面を分析して消費者のプライバシーにかかわるダークパターンを報告している．GDPR 対応に関連したダークパターンは 1 章で示したように，ユーザに深い理解を与えず同意を取得する目的で問題となっている [11], [15], [17].

最後に 2021 年の Mathur らの論文 [13] では，ダークパターンのレポートや論文の内容を SoK (Systematization of Knowledge) のようにまとめている．これまでの研究では一貫性のある概念基盤が欠けていたとして，ダークパターンをメタ的に大きく 2 つのグループと 6 つの属性に分類している．またダークパターンか否かの判断のために 4 つの視点を開発し，今後のダークパターン判定に貢献するとしている．

2.2 本論文で用いるダークパターン分類

ダークパターンに対する既存の様々な取り組みによって，ダークパターンの分類は明確になってきている．Mathur ら (2021)[13] の分類や判定基準は先進的なものであるが，分類の概念が抽象的で扱いづらく，さらに判定基準を正確に使用するためには倫理や法律に深い造詣が必要とみられる．一方で Gray ら [9] の分類は多くの文献で利用され，分類の抽象度も高くなく扱いやすいため，本論文においても Gray らの分類をベースとする．さらに本論文で Gray らの分類をうまく拡張させている Mathur ら (2019)[12] と，プライバシーに関連するコンテキストを取り扱っている NCC レポート [14] の分類を Gray 分類に追加する．表 A·1, A·2 は，本論文で扱うダークパターン分類項目である．Gray らの分類に Mathur ら (2019) の分類を合わせており，さらに NCC レポートの分類を各カテゴリ下のタイプ追加している．3 つの文献において，いくつかのダークパターンは名称は異なるが同じ内容のものがあるため，同じ内容のものは同じ項目としてまとめている．次章では表 A·1, A·2 のダークパターン分類項目を利用して，アプリトラッキング透明性に対するダークパターンの調査を説明する．

3. 手法

本論文では，Apple 社のアプリトラッキング透明性の一環である IDFA のオプトイン化に焦点を当て，IDFA 利用の許可選択画面の説明文および事前説明内容がダークパターンかどうかを調査する．

調査対象は，2021 年 5 月 14 日時点の App Store 日本無料アプリランキング上位 100 アプリとした．調査期間は，2021 年 6 月 1 日から 2021 年 6 月 11 日である．調査は Geronimo ら [6] の調査手法を参考に，アプリ起動時から IDFA の許可画面または事前説明画面が出現し，選択し終わるまでを画面録画することとした．調査機器は iPhone8 または iPhoneXS を利用した．調査はダークパターンのエキスパート調査として本論文の著者 1 名が実施した．

3.1 ダークパターン判定

調査に使用するダークパターン分類項目は表 A·1, A·2 である．ダークパターンの判定基準としては，表 A·1, A·2 の項目に当てはまるかどうかをまず判定し，当てはまらない場合はダークパターンかどうかを 2 章で示したダークパターンの定義から下記の基準で判定する．

- ユーザに深い理解を促しているか
- 事業者の利益よりもユーザの利益を優先しているか

3.2 内容の正確性判定

さらに IDFA の許可選択画面の文章および事前説明画面の内容が，事業者が公開している「App のプライバシー」およびプライバシーポリシーの内容と相違がないことを確認した．

3.3 内容の公平性判定

IDFA の許可選択画面の文章および事前説明画面の内容が公平であるかどうかを下記の基準で確認した．

- 許可した時の利点、拒否した時の利点の両方が書かれ

表 1 調査結果の概要 (日本の無料 Top100 アプリ中)

項目	アプリ数
調査成功	95
認証機能あり	**93**
├ 必須	43
└ 任意	50
IDFA 許可選択画面	**35**
└ 事前説明画面あり	16

ている

- 許可した時に発生することに関して追加の説明がある

3.4 調査の流れ

調査の流れを下記にまとめる.

事前準備

- 調査機器の設定＞プライバシー＞トラッキング に調査対象アプリが無いことを確認する
- 日本無料アプリランキング上位 100 の調査対象アプリを調査機器にインストールする

調査手順

(1) バックグラウンドで実行しているアプリをすべて終了させる
(2) iOS の画面収録機能を実行し画面録画する
(3) 調査対象アプリを起動する
(4) 調査対象アプリを一定時間操作する
(5) IDFA 許可選択画面が出現し選択完了もしくは一定時間操作して出現しなければ録画を終了する

4. 調査結果

4.1 全体概要

調査結果の全体概要を表 1 に示す．調査対象とした 100 アプリのうち，93 アプリに何らかの認証機能が存在し，43 アプリは会員登録や本人確認または特定サービスの利用者などの何らかの認証を経た後でないと利用ができないアプリであった．本調査では，本人確認および特定サービス利用が不要な会員登録に関しては，会員登録を行いアプリを利用した．本人確認および特定サービス利用が必要なものの例としては，マイナンバーカード利用者を対象としたアプリや，特定モバイル回線利用者を対象としたアプリである．結果として，100 アプリのうち 95 アプリの調査が成功した.

IDFA 許可選択画面が出現し，IDFA 利用が確認されたのは 95 アプリのうち 35 アプリ (約 37%) のアプリであった．その 35 アプリのうちで，IDFA 許可選択画面の前に追加の説明画面を用意しているアプリは 16 アプリ (約 46%) であった.

4.2 発見されたダークパターン

本調査で収集した IDFA を利用している 35 アプリの画面

表 2 ダークパターンの結果 (IDFA 許可選択画面あり 35 アプリ中)

項目	アプリ数
Toying with emotion[9] — Conformshaming[4]	6
Framing[14]	30
False hierarchy[9] — Ease[14]	8
Begging	5

録画内容をもとに, ダークパターン分類表 A·1, A·2 に IDFA 許可選択画面の文章および事前説明画面の内容が当てはまるかどうかを分析した．結果としては，31 アプリ (88.6%) において少なくとも 1 つのダークパターンが観測され，そのすべての内容は Gray らの **Aesthetic Manipulation** のカテゴリに属するものであった．その中でも **Toying with emotion - Conformshaming**，**Framing**，**False hierarchy — Ease** に属するものが全てであった[*1]．さらに，新しい分類として本論文では **Begging** というダークパターンを定義した．結果をまとめたものを表 2 に示し，以降それぞれについて本調査で発見されたダークパターンを記載する.

Toying with emotion — Conformshaming

Gray らの Toying with emotion や Brignull が Conformshaming と呼んでいるダークパターンが 6 アプリで確認された．このダークパターンは，ユーザの感情に働きかけ特定の選択を思いとどまらせようとするものである．例えば，本調査で対象とした IDFA の許可画面では,「(IDFA を許可することは) **サービスを今後も無料で提供する**」ことに協力することであるとユーザの善意に働きかけたり,**「許可をしないとあたなに合わない広告が表示される**」と今後不便になることを連想させたりするものが観測された.

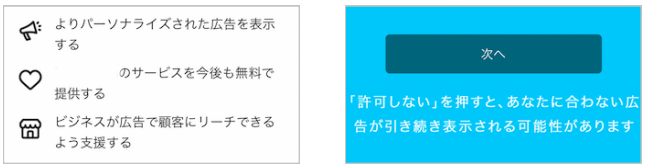
Framing

Framing はフレーミング効果 (Framing Effect) に関するダークパターンである．フレーミング効果は日常的に多くの場面で利用されている認知バイアスの戦略であり，ダークパターンの基準としては厳格なものとなるが，NCC レポートにおいてダークパターンと分類されている．本調査では 35 アプリ中の 30 アプリ (85.7%) という高い割合で観測された．最も多いパターンは「(IDFA を許可することは) **お客様に最適な広告が表示される**」と許可した場合のボジティブな影響のみが強調されている説明である．例えば，許可した場合のネガティブな影響や拒否した場合のポジティブ/ネガティブな影響の説明がない場合，ユーザに認知バイアスを与えている可能性がある.

False hierarchy — Ease

Gray らが False hierarchy，NCC レポートでは Ease と呼んでいるダークパターンである．このダークパターンは片方の選択項目のみを強調させるように表示するものであるため，iOS 標準のダイアログ上では実現できないが，事

[*1] アプリによって複数のダークパターン項目を含むものが多く，1 アプリ 1 ダークパターンに分類されるわけではない.



(a) (b)

図 2 ダークパターン結果: Toying with emotion — Conformshaming
(a) 無料で提供できるようにと善意に働きかけたり，(b) 合わない広告が表示されると不便を連想させる．

(a) (b)

図 3 ダークパターン結果: Framing
iOS 標準のダイアログ上の説明文においても (a) 興味関心にあった情報，(b) 最適な情報を配信，とフレーミング効果が利用される．

前説明画面において観測された．本調査では事前説明画面の存在するアプリが 16 アプリ観測されたが，そのうちの 8 アプリ (50.0%) でこのダークパターンが観測された．

例えば，**「トラッキング許可」の文言を太字**にしたり，「許可」の文字サイズを大きくするなどのハイライトや，IDFA 許可選択画面の絵を表示して，**「許可」ボタンに◯印を付け許可することが正解であるかように認知させる**ものが存在した．このダークパターンは Apple のガイドライン [2] でも禁止されている「ユーザーを誘導したり，だましたり，強制したりする」ものに該当する可能性があり問題が大きい．

Begging

本調査においてユーザへ **IDFA 許可を懇願する表示**が 5 アプリで観測された．2 章で示したダークパターンの概念である「ユーザに深い理解を促さず利用者の利益を優先させる」お願いと判断されるため，ダークパターンと分類した．このダークパターンは Toying with emotion や Framing と類似するが「お願い」という内容が特徴的であるため新たな分類として Begging と名付けた．

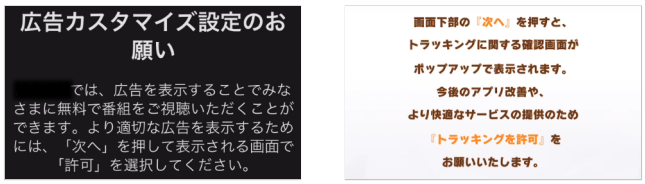
4.3 正確性と公平性

IDFA 許可の画面が存在した 35 アプリにおいて，3.2 節で示した正確性について判定を行なった．11 のアプリは App のプライバシーやプライバシーポリシーと概ね相違のない説明内容であったが，22 のアプリは一部の説明に相違のある状態であり，2 アプリは説明内容が大きく異なるものであった．

また 3.3 節の基準で公平性を判定した結果，27 のアプリ

(a) (b)

図 4 ダークパターン結果: False hierarchy — Ease
追加の説明画面多く見られ，(a) 許可に◯印を付けて正解のように誘導，(b) 許可を強調して誘導している．



(a) (b)

図 5 ダークパターン結果: Begging
(a) お願いというタイトルや，(b) お願いしますという文言でユーザの善意に働きかけている．

で公平や説明内容にはなっておらず，多くは許可した場合の利点のみの説明となっていた．

5. 議論

5.1 考察と発展的調査

本調査で対象とした App Store 日本の無料 Top100 アプリにおいて，IDFA が利用されているものは 35 アプリであった．これは調査前の予想よりも少ない結果となったが，表 1 に記載の通り，ほとんどのアプリに何らかの認証機能が存在していることを鑑みると，IDFA を利用せずに直接ユーザ ID (メールアドレス等) によるトラッキングが既に広く実施されている可能性が考えられる．そのため，サインアップやログインに関してダークパターンを利用した誘導がないかも含め，今後のトラッキングに関する事象に注視する必要がある．

他方，IDFA 利用のアプリを効率的に発見することを考えると，iOS アプリを広くダウンロードし，パッケージ化されているプロパティリスト (Info.plist) を解析して IDFA 許可画面のダイアログ説明文設定有無を確認することで，効率よく IDFA を利用しているアプリを収集し大規模調査を実施できると考える．

5.2 制限事項と研究倫理

本調査では 1 名の著者がダークパターン判定を実施している．2 名以上で判定結果のカッパ係数を測定し，判定

の一致度を測っている文献も多いため，本調査の結果は多少の偏りが存在する可能性がある．また，日本のランキングトップアプリの調査であるため，日本特有の結果であることも考慮される．例えば，本論文で新たに定義した「Begging」というダークパターンは，これまでの既存調査から発見されていないため，日本特有のダークパターンである可能性があり，今後の複数の研究で明らかにされることが期待される．

本稿の調査は，倫理綱領 [19] やチェックリスト [5] を参考に，特定のアプリ事業者へのネガティブな影響を最小化するために，具体的なアプリ名は非公表としている．

5.3 ダークパターン規制

GDPR[7] では「自由に与えられた明確な同意」を必要とし，同意のガイドライン [8], [10] 等でいくつかのダークパターンに該当するものは有効な同意ではないと具体的に記載されている．CCPA (California Consumer Privacy Act) においてもダークパターンに該当するような UIUX 表示が禁止され [16]，ワシントンの法案ではダークパターンという語句が使われ，規制が強化されようとしている [18]．

日本においては明確なダークパターン規制はないが，今後のグローバルな状況に合わせたダークパターンへの規制強化は十分に考えられる．

6. まとめ

本論文では，GDPR でオプトイン化された Cookie 許可におけるダークパターン横行の現状を踏まえ，iOS14.5 における IDFA のオプトイン化に伴うダークパターン発生の早期調査を実施した．App Store 日本の無料 Top100 アプリを対象に調査を実施した結果，35 アプリにおいて IDFA 利用が観測され，IDFA 許可に関する画面においてダークパターン項目に少なくとも 1 つ該当するものは 88.6%であった．また，16 アプリで IDFA 許可選択画面の前に追加の説明画面が確認されたが，8 アプリ (50%) は Apple 社がガイドラインで禁止しているダークパターンに該当する画面内容であった．アプリ事業者は表 A·1, A·2 で記載したダークパターンの存在を理解し，ユーザの利益を優先した倫理的な UIUX をより多くユーザに提供することを期待する．

付　　録

A.1 ダークパターン分類表

参考文献

[1] Apple Inc.: プライバシー，https://www.apple.com/jp/privacy/.
[2] Apple Inc.: ユーザーのプライバシーとデータの使用，https://developer.apple.com/jp/app-store/user-privacy-and-data-use/.
[3] Bösch, C., Erb, B., Kargl, F., Kopp, H. and Pfattheicher, S.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns, *Proceedings on Privacy Enhancing Technologies* (2016).
[4] Brignull, H.: Dark Patterns, https://www.darkpatterns.org/.
[5] CSS2020 研究倫理委員会：サイバーセキュリティ研究における倫理的配慮のためのチェックリスト，https://www.iwsec.org/css/2020/ethics_list.html (2019). (参照 2019-08-20).
[6] Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F. and Bacchelli, A.: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020).
[7] European Union: General Data Protection Regulation (GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[8] European Union: Guidelines on Consent under Regulation 2016/679 (wp259rev.01), https://ec.europa.eu/newsroom/article29/items/623051.
[9] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J. and Toombs, A. L.: The dark (patterns) side of UX design, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018).
[10] Information Commissioner's Office (ICO): Consent, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.
[11] Machuletz, D. and Böhme, R.: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR, *Proceedings on Privacy Enhancing Technologies (PoPETs)* (2020).
[12] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M. and Narayanan, A.: Dark patterns at scale: Findings from a crawl of 11K shopping websites, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3, No. CSCW (2019).
[13] Mathur, A., Kshirsagar, M. and Mayer, J.: What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021).
[14] Norwegian Consumer Council (NCC) / Forbrukerrådet: Deceived by design: How tech companies use dark patternsto discourage us from exercising our rights to privacy, Technical report (2018).
[15] Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, *Proceedings of the ACM on Human-Computer Interaction* (2020).
[16] State of California Department of Justice: Final Regulation Text. California Consumer Privacy Act (CCPA), https://oag.ca.gov/system/files/attachments/press-docs/CCPA%20March%2015%20Regs.pdf (2021).
[17] Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T.: (Un) informed Consent: Studying GDPR Consent Notices in the Field, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (2019).
[18] Washington State Legislature: Bill Information SB 5062, http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062.pdf (2021).
[19] 情報処理学会：情報処理学会倫理綱領，https://www.ipsj.or.jp/ipsjcode.html.

ⓒ 2021 Information Processing Society of Japan

表 A·1 ダークパターン分類表 1

カテゴリ	タイプ	サブタイプ	説明	例
Nagging	Nagging[9]		しつこく都合のよい選択や継続をユーザに求めるもの	タスク中に「Not Now」と「OK」しかないプロンプトを出す．目標にまだ達していないというダイアログを出して継続させるなど
	Forced action and timing[14]		同意の選択をするまで通知が定期的に発生する	タスク中に同意確認を表示させ，同意しなければ煩わしい通知が止められないなど
Obstruction	Roach Motel[4], [9] — Hard to Cancel[12]		入会は簡単だが，退会は難しいもの	サブスク登録は 5 分，解除は 2 日かかる（電話受付のみ）など
	Price Comparison Prevention[4], [9]		価格比較できなくする嫌がらせ	製品名や価格をコピーできないように細工するなど
	Intermediate Currency[9]		課金のクレジットをわかりにくくする	ゲーム内課金量で課金によるクレジットの増加をわかりにくくする（100 円払えば 100 クレジットだけど 1000 円払えば 5000 クレジット）など
Sneaking	Forced Continuity[4], [9] — Hidden Subscription[12]		無料後に確認なしに有料課金が始まる	クレジットカードを登録させておき最初は無料だけど解約しないと有料として課金されるなど
	Hidden Costs[4], [9], [12]		最終価格が最後にわかる	税金，手数料，消費税が最後の確認画面でのみ追加される．商品ページには税抜単価だけの表示など
	Sneak into Basket[4], [9], [12]		オプション商品が勝手に追加される	見つかりにくいように，または最終確認画面でオプション商品が入っており，価格の合計に加えられているなど
	Bait and Switch[4], [9]		特定の操作を続けさせた上で，同一操作で都合のよい選択をさせる	同じ位置，ボタン，色で作業を進める操作をさせて，ある時点で「支払い」に関する決定ボタンになっているなど
Interface Interference	Hidden Information[9]		重要な情報を小さく，または展開式で表示させる	ユーザのデータ販売に関するオプトアウトを小さな文字とチェックボックスで表示するなど
	Preselection[9] — Default settings[14]		直接ユーザの利益にならないオプションが事前に選択されている	メーリングリスト登録やパーソナルデータ収集を事前選択しているなど
	Aesthetic Manipulation[9]	Misdirection[4] — Visual Interference[12]	UIUX で 1 つのものに集中させて他のものから注意をそらせたり，説得させたりする	あたかも記事がペイウォールの後にあるように見えるが，普通にアクセスできるなど
		Toying with emotion[9] — Confirmshaming[4]	かわいい，怖い，健康に悪そうなどの感情に働きかけるもの	料理サイトのサインアップ辞退で「健康に悪い生活を続ける」ことを連想させるコピーを利用するなど
		Framing[14]	倫理的に疑わしいポジティブ/ネガティブな代替説明を表示して選択させる	顔認識の同意で「見知らぬ人による写真利用からあなたを守るため...」などと表示する．「オフにすれば見知らぬ人に使われる...」など表示する
		False hierarchy[9] — Ease[14]	並列のオプションをあえて UI に差異を与えて片方を優良に見せる	選択項目の片方だけ (recommended) としてハイライトする，都合が良い方の選択を目立つボタンにするなど
		Disguised Ad[4]	ユーザの画面内の行動につけ込み選択させる	ダウンロードページで広告内に「ダウンロード」と表示してクリックさせるなど
		Trick Questions[4]	二重否定やわかりにくい表現の質問	二重否定の文言でオプトインではなくオプトアウトのチェックボックスにするなど
		Pressured Selling[12]	一番高い商品がデフォルトで選択されている	価格の低い商品との冷静な比較を難して高い商品を購入させるなど

ⓒ 2021 Information Processing Society of Japan

表 A·2 ダークパターン分類表 2

カテゴリ	タイプ	サブタイプ	説明	例
Forced Action	Social Pyramid[9] — Frend spam[4]		サービス利用のために他のユーザの紹介が必要	オンラインゲームで他のユーザを招待しないとゲームを始められないなど
	Privacy Zuckering[4], [9]		ユーザの意図よりも多くの情報を共有させる	設定を誤られて過剰にデータを共有させるなど
	Gamification[9]		課金しなければ多くの時間がかかるような設計	ゲームに課金する場合に達成できるランクと無課金のままでそのランクに達成する場合に多大な時間がかかるなど
	Forced Enrollment[12]		必要がないのに登録を要求する	利用規約の同意でマーケティングメール送信を強制許可させる，アカウント登録しないと商品情報が見られないなど
	Rewards and punishment[14]		拒否した時の影響があまりにも大きいように設計	新しいプライバシーポリシーに同意しない場合はアカウントの完全削除を強要して今までのアクティビティがなかったことになるなど
Urgency	Countdown Timer[12]		カウントダウンタイマーを表示させて焦らせる	時間限定の割引のように見せるが，タイムアップになってもその割引は有効など
	Limited-time Message[12]		期間限定の割引というメッセージを価格表示にそえる	「セール終了はすぐ」などのメッセージが添えられているが，セールが終了することはないなど
Social Proof	Activity Message[12]		他のユーザのアクティビティを表示するメッセージ	「35 人がこのアイテムをカートに追加」「90 人がこの商品を閲覧中」など，事実でない騙しのものも多いという
	Testimonials[12]		出どころが不明なお客様の声	同じお客様の声の文書が複数のサイトで使われているなど
Scarcity	Low-stock Message[12]		在庫が少ないというメッセージを表示させる	「残りあと 3 つ」などのメッセージ，在庫数が一定時間で減るようになっている騙しのものも多いという
	High-demand Message[12]		需要が高いというメッセージを表示させる	「すぐに売り切れている」などのメッセージをカートの画面で出すなど

ⓒ 2021 Information Processing Society of Japan