Computer Security Symposium 2021
26 - 29 October 2021

# クッキーコンセントバナーにおける ダークパターンの実態調査

永井 達也[1,a)]　高田 雄太[1]　神薗 雅紀[1]

**概要**：各国で個人情報保護に関する法規制が施行され，ウェブサイトではクッキーコンセントバナーを表示することにより，クッキー使用に対するユーザ同意を取得するようになった. しかし，ダークパターンと呼ばれるユーザの意図に反して同意させるよう仕向けるデザインを取り入れたクッキーコンセントバナーの利用が確認されている．ダークパターンによる誘導は，一部の法規制で禁止されているものがあり，ユーザの理解のもと公平に同意を取得する必要がある．本研究では，ダークパターンを利用してしまう原因を探るべく，複数の国のウェブサイトをクローリングし，クッキーコンセントバナーで利用されている5つのダークパターンを調査した．クッキーコンセントバナーの自動生成ツールにおけるデフォルト設定や機能に加え，従来のウェブ開発における知見を適用したクッキーコンセントバナーの独自実装がダークパターンの混入につながることがわかった．ツール提供者やウェブサイト管理者は法規制を正しく遵守し，ユーザからの信頼を損なわないためにも，ダークパターンに関する理解を深めた上でクッキーコンセントバナーをデザインすべきだと考える．

**キーワード**：クッキーコンセントバナー，ダークパターン，プライバシー

# Understanding Dark Patterns in Cookie Consent Banner

Tatsuya Nagai[1,a)]　Yuta Takata[1]　Masaki Kamizono[1]

***Abstract:*** Websites show cookie consent banners to obtain user consent for cookie use due to the privacy regulations in various countries. However, some websites use cookie consent banners with dark pattern design which tricks users to unintentionally give consent. Some dark patterns are forbidden by privacy regulations because they violate user privacy. We must collect user consent fairly with the user's understanding. To investigate why dark patterns are being used, this study analyzes five types of dark patterns used in cookie consent banners by crawling websites in various countries. Our investigation shows that automated banner generation by tool and original implementation of banners lead to the use of dark patterns. We suggest that tool providers and webmasters should understand dark pattern design, and implement cookie consent banners, and comply with privacy laws so as not to damage the trust of users.

***Keywords:*** Cookie Consent Banner, Dark Pattern, Privacy

## 1. はじめに

クッキーを使用したトラッキングに対して，ユーザのプライバシーを保護するための法規制が施行されている．一部の法規制は，クッキー使用に対してユーザへの通知や同意取得を義務付けている．ウェブサイトはクッキーコンセントバナーを表示することにより，上記義務を果たすようになった．ユーザはウェブサイトにおけるクッキーの使用目的を理解した上で，クッキーコンセントバナーを操作することにより，クッキーの使用を同意または拒否することができる．

法規制で求められる要件は国ごとに異なっており，ウェブ

[1] デロイト トーマツ サイバー合同会社
Deloitte Tohmatsu Cyber LLC.
[a)] tatsuya.nagai@tohmatsu.co.jp

サイトはユーザの居住国に応じた対応が必要である．ウェブサイトが各国の法規制すべてに対応することが難しいことから，クッキーコンセントバナーの実装および表示やクッキーの制御に Consent Management Platform (CMP) が利用されている．CMP の導入により，ユーザの居住国によってクッキーコンセントバナーの表示を変えたり，同意に関する詳細な設定方法を提供したりするなど，プライバシーに配慮するとともに法遵守することができる．

一方でウェブサイトは，アクセス解析やコンバージョン計測等のため，ユーザのトラッキングを可能な限り行えるよう同意を得ようとする．その結果，ユーザのプライバシーを尊重しない形で，法規制で求められる要件を無理やり満たすようなクッキーコンセントバナーが確認されている．例えば，ウェブサイトにアクセスするとクッキーコンセントバナーが全面に表示され，ユーザがクッキーコンセントバナーを操作するまでウェブサイトを閲覧できない状態となるバナーがある．ユーザはクッキー使用に対する選択を強制され，ページを閲覧するには同意せざるを得なくなる．

このようにユーザを不当に誘導するデザインはダークパターンと呼ばれる．ダークパターンにより得られた同意は，ユーザがクッキーの使用目的を理解した上で選択したとは言えず，ダークパターンの一部は法規制で禁止されている．したがって，ダークパターンの利用は法違反のリスクがあるとともに，ユーザの信頼を損なう可能性がある．

そこで，本研究ではダークパターンを利用してしまう原因を探るべく，下記 3 つの Research Question (RQ) を設定した．

**RQ1**　クッキーコンセントバナーに適用されるダークパターンの種類や利用率はどれほどか？

**RQ2**　国別の法規制がダークパターンの混入に影響を及ぼすか？

**RQ3**　クッキーコンセントバナーの実装方式がダークパターンの混入に影響を及ぼすか？

上記 RQ を解明するために，複数の国のウェブサイトをクローリングし，クッキーコンセントバナーにおけるダークパターン利用率を調査した．本研究の貢献は以下の通りである．

- 5 種類のダークパターン, Consent Wall, Bad Defaults, Roach Motel，Misdirection Size，Misdirection Color が，それぞれ 1.53%, 56.6%, 8.03%, 8.05%, 40.9% のクッキーコンセントバナーに適用されていることを示す．
- 同意の要件が法規制で指定されている国で，関連するダークパターン利用率が高くなることを示す．
- 独自実装されたクッキーコンセントバナーは，EC サイトやモバイルアプリで利用されているダークパターンの混入が多い一方で，CMP により生成されたクッキーコンセントバナーは，CMP の提供機能によるダークパターンの混入が多いことを示す．

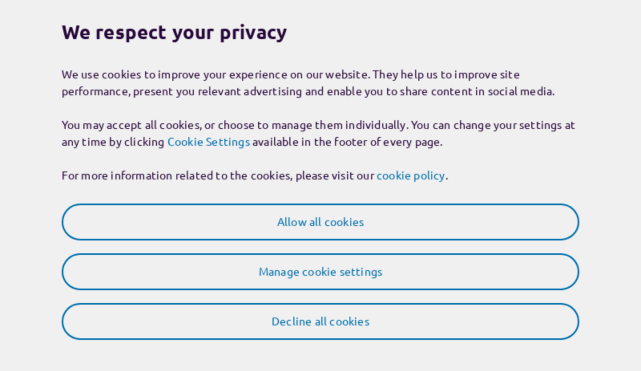


図 1: クッキーコンセントバナーの例

## 2. 研究背景

### 2.1 クッキーコンセントバナー

クッキーコンセントバナーの例を図 1 に示す．クッキーコンセントバナーは一般的に，クッキー使用の通知文，同意や拒否を選択するボタン，詳細設定ボタンで構成されている．通知文は，ウェブサイトがクッキーを使用していることやクッキーの使用目的，ユーザが可能なクッキー制御の方法等について記述されている．同意や拒否ボタンはユーザが押すことでウェブサイトのクッキーを制御することができる．詳細設定ボタンは，クッキーコンセントバナーの表示領域に収まらない機能を提供する場合に，詳細設定を行う画面をポップアップ等で表示させる．詳細設定画面では，クッキーのカテゴリ別同意機能の提供や詳細な利用目的の記述等がされている．

上記の機能を提供するには，クッキーコンセントバナーのデザインに加え，ユーザの選択に応じてクッキーの使用も制御する必要がある．クッキーコンセントバナーは，ウェブサイト管理者が独自に実装する方式や，細やかなクッキー制御やユーザ同意の管理ができる CMP を導入して生成する方式がある．CMP は，ユーザのアクセス元の国に応じて表示するクッキーコンセントバナーを変えるローカライズ機能や，ウェブサイトが使用するクッキーを自動で検出し，ユーザにトラッキング情報を明示した上で同意を求める機能などを備えている．

### 2.2 ダークパターン

ダークパターンは，ユーザの意図に反して特定の行動を起こさせるよう設計されたインターフェースと定義されている [1]．特に，以前より EC サイトや SNS におけるダークパターンの利用が確認されている．例えば EC サイトでは，ユーザが商品を購入したくない場合においてもウェブサイトが商品を購入させようとするページデザインがある．商品を紹介するページでカウントダウンタイマーを表

示し，特定の期限内にしか購入できないとユーザに錯覚させ，商品の購入を強制させる．SNS では，ユーザがプロフィールを公開したくない場合においても，プロフィールを非公開にすることを難しくさせるような設定画面をデザインしている．このように，ウェブサイト側の思惑に偏り，ユーザに誤った判断を促そうとする場面で，しばしばダークパターンが発生する．

クッキーコンセントバナーにおいては，ユーザの同意を取得する場面でダークパターンが利用される．Gray ら [2] はクッキーコンセントバナーの同意フローを (1) Initial framing , (2) Configuration , (3) Acceptance, (4) Revocation の 4 つのフェーズに分けている．Initial Framing はユーザがウェブサイトにアクセスした時にユーザが最初にクッキーコンセントバナーを目にするフェーズである．Configuration はクッキーの使用を同意するか拒否するかであったり，クッキーのカテゴリ別同意のような詳細な設定項目を提供するフェーズである．Acceptance は Configuration で設定した項目を承認するフェーズで，Revocation は同意を撤回するフェーズである．この同意フローにおいて，ユーザに選択を強制させるパターンやユーザの選択を誘導させるパターンが適用可能であると考えられる．他分野で特定されているダークパターンのうち [1][3]，これらのパターンを列挙した結果，表 1 に示す 7 つのダークパターンがクッキーコンセントバナーに適用されうることがわかった．

Consent Wall は，ウェブサイトの全面にクッキーコンセントバナーを表示してウェブサイトを利用できない状態にすることで，ユーザに同意を強制させるパターンである．Bad Defaults は， Configuration フェーズで設定可能なオプションのうち，ユーザにとって不都合なオプションをあらかじめ有効にしておくことで，オプションに対する同意を得やすくするパターンである．Roach Motel は，ユーザが同意を撤回，またはクッキー使用を拒否する際に，複雑な操作を要求し，ユーザに拒否させないようにするパターンである．Misdirection は，同意ボタンを拒否ボタンよりも目立つよう表示させ，同意させやすくするパターンである．Trick Questions は，二重否定語などを利用してユーザが同意と拒否を誤解して選択させるパターンである．Bait and Switch は，ユーザが同意以外の選択をした場合でも，同意とみなすパターンである．Confirmshaming はユーザが拒否する際に，罪悪感を与える文言によって拒否させないよう仕向けるパターンである．

### 2.3 法規制

ダークパターンは，意図せずユーザのプライバシー侵害につながることから，各国で規制する動きが広まっている．EU では 2016 年に GDPR [4] が施行されている． GDPR はクッキーを個人情報とみなしており，クッキー使用にユーザ同意を求めている．同意の取得要件は厳格に定義されており，同意は「自由に与えられ，特定され，事前に説明を受けた上での，不明瞭ではない，意思の表示」と定義されている．2020 年にデータ保護当局が出したガイドライン [5] では法違反になるケースを例示している．例えば，Bad Defaults は暗黙的な同意の取得とみなされており，禁止されている．また，Consent Wall はウェブサイトの利用を制限するようなパターンであることから，ユーザが自由に選択できないため，自由に与えられた同意ではないとされており，禁止されている．

アメリカでは 2018 年に CCPA が施行されている．CCPA は主に個人情報の販売に関する規制がされており，クッキーを使用している場合には，ユーザにクッキー使用の拒否権があることを定義している．ダークパターンに関する規制は 2021 年の改正 [6] で追加されており，個人情報販売を拒否する手続きを複数ステップ要求する Roach Motel が禁止されている．

## 3. 関連研究

### 3.1 ダークパターン

ダークパターンに関する研究はモバイルアプリや EC サイトで行われている．Di Geronimo ら [7] は 240 種類の有名な Android アプリのダークパターンを調査し，平均して 7 種類のダークパターンが適用されていることを示している．また，ユーザ実験を行なっており，ほとんどのユーザはアプリのダークパターンを認識できていないことを示している．Tahaei ら [8] はアプリで利用される 4 つの広告ライブラリについて開発者とユーザに対するダークパターンを調査している．開発者向けのサンプルコードには，ユーザの同意が取得できるまで繰り返し要求メッセージを出す仕組みになっていたり，個人情報提供の要求メッセージに対し同意ボタンしかないことが確認されている．Mathur ら [9] は EC サイトの商品ページをクローリングし，EC サイトに存在するダークパターンを調査している．調査の結果，11,000 件の EC サイトのうち 11.8%がダークパターンを利用していることを示している．また，これらのダークパターンを導入する機能を提供しているツールが 22 個存在することを示している．Gray ら [10] は英語圏と中国語圏のユーザに対してデジタルサービスの利用に関するユーザアンケートを実施し，ユーザがダークパターンを認識しているかについて調査している．ユーザの一部はダークパターンの具体的なテクニックについて理解していることを示している．上記のように，ダークパターンの利用がユーザを誘導して同意率を高くすることが示されている．

### 3.2 クッキーコンセントバナーにおけるダークパターン

クッキーコンセントバナーでは，法規制遵守の観点からダークパターンの利用状況を確認する研究がなされてい

表 1: クッキーコンセントバナーにおけるダークパターン

| ダークパターン種別 | 利用されるフェーズ | 概要 |
|---|---|---|
| Consent Wall | Initial Framing | ウェブサイト全面にクッキーコンセントバナーを表示し，ユーザに操作を強制させる． |
| Bad Defaults | Configuration | オプションをあらかじめ有効にした状態でクッキーコンセントバナーを表示し，オプションを同意させやすくする． |
| Roach Motel | Revocation | 同意は簡単な操作で行えるが，拒否は複雑な操作が必要とし，拒否させづらくする． |
| Misdirecrtion | Acceptance | 同意ボタンを拒否ボタンよりも目立つよう表示し，ユーザに同意させやすくする． |
| Trick Questions | Acceptance | 二重否定語などを利用してユーザが同意と拒否を誤解して選択させるよう仕向ける． |
| Bait and Switch | Acceptance | ユーザが同意以外の選択をした場合でも，同意とみなす． |
| Confirmshaming | Revocation | ユーザが拒否する際に，罪悪感を与える文言によって拒否させないよう仕向ける． |

る．Nouwens ら [11] はユーザ実験を実施しており，Roach Motel パターンを適用した場合に同意率が 22〜23%増加すること， Consent Wall を適用した場合は同意率に影響を与えないものの，ユーザがクッキーコンセントバナーを操作する確率が上がることを示している．Machuletz ら [12] は Misdirection パターンや Bad Defaults パターンがユーザを誘導することを示している．また，Misdirection により誘導されたユーザは自分の選択を後悔し，誘導されたと感じることを示している．Graßl ら [13] はユーザ実験を行い，ダークパターンと拒否させやすくするパターンがユーザを誘導するかどうかについて調査している．ダークパターンによる同意取得率が高い一方で，拒否させやすくするパターンを見たユーザはその後の選択においても拒否しやすくなることが示されている．著者らは，ダークパターンの誘導のせいでユーザが常に同意するよう条件づけられており，プライバシー選択について検討できていない可能性を指摘している．

Soe ら [14] は， EU のウェブサイトのクッキーコンセントバナー 300 件を手動で分析し，ダークパターンを調査している．その結果，Misdirection ， Consent Wall ， Roach Motel および Confirmshaming が利用されていることを示している． Nouwens ら [11] はイギリスのウェブサイト 1 万件をクローリングし，CMP により生成されたクッキーコンセントバナー 680 件に対し GDPR の同意要件を満たしているかどうか調査している．明示的な同意を取得できているかどうかに加え， Roach Motel ， Bad Defaults の使用率を調べており，ダークパターンを利用しないクッキーコンセントバナーは 11.8% しかないことを示している．

ダークパターンの利用率は調査されているが，特定の国のクッキーコンセントバナーに限られており，また，調査対象も各国の法規制に関連するダークパターンに限られている．ユーザのプライバシー保護状況を評価するには，法規制にかかわらずダークパターンの利用を調査することが望まれる．

## 4. 提案手法

図 2 に示すプロセスに従って，クッキーコンセントバナーに適用されるダークパターンを調査する．ユーザの同意フローに沿って各フェーズでダークパターンが適用されるか分析する．クッキーコンセントバナーが提供する機能によって適用可能なダークパターンが異なる．例えば，オプションを提供しないクッキーコンセントバナーは Bad Defaults は適用されない．そのため，ダークパターンの検知はクッキーコンセントバナーの機能を特定したのちに行う．

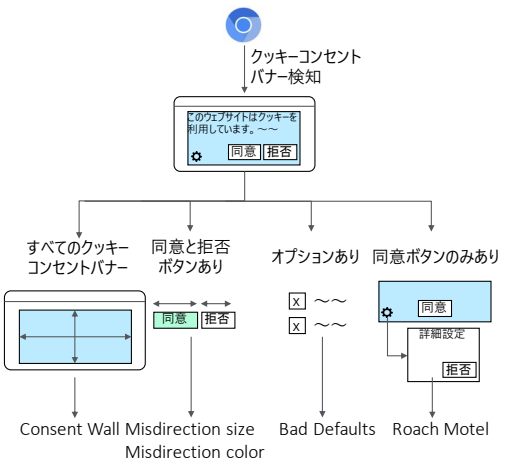


図 2: 調査プロセス

まず，ウェブサイトのトップページにアクセスし，クッキーコンセントバナーが表示されるか確認する．クッキーコンセントバナーが表示された場合，ブラウザの表示サイズとクッキーコンセントバナーの表示サイズを比較し，Consent Wall に該当するか確認する．クッキーコンセントバナーに同意ボタンおよび拒否ボタンが存在する場合，同意ボタンが強調されているかどうかを調べ， Misdirection に該当するか確認する．Misdirection パターンは，ユーザを色で誘導するものと大きさで誘導するものの二通りが確認されている．そのため本調査では，色を強調するパターンを Misdirection Color，大きさを強調するパターンを Misdirection Size として検知する．クッキーコンセントバナーにオプションを選択する機能がある場合，オプションがあらかじめ有効になっているか調べ，Bad Defaults に該当するか確認する．最後に，クッキーコンセントバナーに同意ボタンと設定ボタンがあり拒否ボタンがない場合，設定ボタンを操作することで拒否ができるかどうか調べ，Roach Motel に該当するか確認する．

Confirmshaming および Trick Questions は自然言語に

表 2: ボタン識別のための単語リスト

| ボタン種別 | 単語 |
|---|---|
| 同意 | 同意, 合意, 承認, 承諾, 受け入れる, ok , agree , allow , accept , got it , i understand , approve , confirm |
| 拒否 | 同意しない, 合意しない, 承認しない, 拒否, decline, disagree, reject, no |
| 詳細設定 | 詳細, 設定, setting , more information , show detail , show more |

よりユーザを誘導するパターンである．本研究では国別のダークパターン利用率を調査することから，調査対象となるクッキーコンセントバナーの言語も複数存在する．複数言語の自然言語処理を共通した基準で行えないことから，本研究ではこの二つのパターンを調査対象外とした．また， Bait and Switch はクッキーコンセントバナーに加えウェブサイトのクッキーの送受信を監視する必要があることから，調査対象外とした．

### 4.1 クッキーコンセントバナー検知

独自実装によるクッキーコンセントバナーは法規制や同意に関連する単語が HTML タグの属性に含まれると仮定し，“cookie” や “consent”, “gdpr” が含まれる HTML タグを検知する．CMP により生成されたクッキーコンセントバナーは，バナーへの操作を自動化するツール Consent-O-matic [15] を利用して検知する．どちらの手法による検知でも，バナーの一部分の HTML タグのみを検知することがある．後述するダークパターン検知では，バナーの通知文やボタンの操作を行うため，バナー全体を捉える必要がある．そのため，検知された HTML タグがテキストとクリック可能なタグを持つかどうか確認する．クリック可能なボタンは，`a` タグと `onClick`[16]，`addEventListener` [17] イベントが登録されているタグとした．条件を満たさない場合は検知された HTML タグの親タグを辿る．親タグを辿る過程で，`body` タグやウェブサイト全体を覆うようなタグを参照した場合は，バナーではないと判定する．

次に，バナー内のボタンを識別する．ボタンに含まれるテキストを，表 2 に示す単語リストによって同意，拒否，詳細設定ボタンを分類する．前処理として英語のテキストは小文字に正規化した．`a` タグの `href` 属性に URL が指定されている場合はプライバシーポリシーへのリンクとみなし，分類は行わなかった．

### 4.2 ダークパターンの検知

#### 4.2.1 Consent Wall の検知

クッキーコンセントバナーを操作しないとウェブサイトが閲覧できない状態になっているか確認する．クッキーコンセントバナーがウェブサイト全体を覆っている場合，ウェブサイトの閲覧を妨害しているとして Consent Wall であるとみなせる．つまり，クッキーコンセントバナーを示すタグの領域が `body` タグの領域と同じ大きさでかつ，背景色が透明ではない場合， Consent Wall であると検知する．タグの領域は `getBoundingRect`[18] で取得する．

#### 4.2.2 Misdirection Size の検知

同意ボタンと拒否ボタンを示すタグの面積比から，同意ボタンがユーザを誘導しうるかどうか確認する．本調査では，同意ボタンが拒否ボタンの 1.5 倍以上の面積比を持つ場合に Misdirection Size であると検知する．

#### 4.2.3 Misdirection Color の検知

同意ボタンが見やすい色である，もしくは拒否ボタンが見にくい色であるかどうか確認する．ボタンを見にくくする方法として背景色を同じにする方法が挙げられる．クッキーコンセントバナーの背景色とそれぞれのボタンの背景色を比較し，バナーの背景色と拒否ボタンの背景色が同じでかつ，同意ボタンの背景色が異なる場合に Misdirection Color であると検知する．

#### 4.2.4 Bad Defaults の検知

クッキーコンセントバナーが提供しているオプションが有効になった状態で表示されているか確認する．オプションの設定には `type` 属性が `checkbox` である `input` タグが利用される．一般にはクッキーの使用をカテゴリ別で制御するオプションが提供されることがあるが，ウェブサイト閲覧のために必ず使用されるクッキーは必須カテゴリとして表示される．この場合，必須カテゴリのオプションは有効にされ，ユーザから操作できないよう `disabled` 属性が設定される．このことから，`type` 属性が `checkbox` である `input` タグのうち，`disabled` 属性がなく `checked` 属性があるタグが存在する場合に Bad Defaults であると検知する．

#### 4.2.5 Roach Motel の検知

クッキーコンセントバナーが拒否機能を提供しているにもかかわらず，拒否するために複数の手続きを要求するか確認する．詳細設定ボタンを操作し，ポップアップ画面など新たに表示されたタグから操作可能なボタンが検知できるか確認する．設定ボタンにより新たに表示されるタグの特定には `MutationObserver` [19] を利用し，タグの生成や `display` 属性の変更を監視する．新たに表示されたタグに 4.1 節で述べたボタンの識別を実施し，拒否ボタンが検知された場合，拒否するために 2 回の手続きが必要なため Roach Motel であると検知する．

## 5. 実験

### 5.1 実験環境

複数の国のウェブサイトをクローリングし，ダークパターン利用率を調査する．アクセスするウェブサイトは，日本と海外のウェブサイトを調べるため，ビジネスデータベースである HooversDB [20] から東証上場している企業およびその子会社，海外支店のウェブサイトとした．

表 3: ウェブサイトのアクセス結果

| 結果 | 観測数 |
|---|---|
| アクセス総数 | 30,039 |
| HTTP 200 OK | 26,491 |
| バナー表示サイト (独自検知) | 2,549 |
| バナー表示サイト (CMP 検知) | 551 |
| HTTP エラー | 386 |
| 巡回エラー | 3,162 |

表 4: ダークパターン検知結果

| 種別 | 検知数 | 検知母数 |
|---|---|---|
| Consent Wall | 46 | 3,000 |
| Bad Defaults | 82 | 145 |
| Roach Motel | 25 | 311 |
| Misdirection Size | 12 | 149 |
| Misdirection Color | 61 | 149 |

ウェブサイトにアクセスし，HTTP コンテンツを収集するために， Ubuntu にインストールした Chromium[21] を用いた．コンテンツを読み込んだ後， JavaScript の実行や非同期通信が発生することを考慮し，ネットワーク接続がアイドル状態になるまで待機した．なお，ウェブサイトへのアクセスにおいて，3 分間でコンテンツの読み込みが終わらない場合は，アクセスをタイムアウトした．

### 5.2 データの収集

2021 年 4 月に国内の IP アドレスから URL にアクセスした結果を表 3 に示す．30,039 件中 26,491 件のウェブサイトが HTTP ステータスコード 200 を応答し，アクセスに成功した．そのうち，独自実装と CMP による生成のクッキーコンセントバナーを検知できたウェブサイトは，それぞれ 2,549 件，551 件あった．また，386 件のウェブサイトが HTTP エラーを応答し，3,162 件のウェブサイトにおいて名前解決エラー等の巡回エラーが発生した．

### 5.3 RQ1:ダークパターンの種類および利用率

ダークパターン検知結果を表 4 に示す．検知母数は各ダークパターンを適用するのに必要な機能を提供しているクッキーコンセントバナーの数を示している．Consent Wall は 46/3000(1.53%)，Bad Defaults は 82/145(56.6%)，Roach Motel は 25/311(8.03%)，Misdirection Size は 12/149(8.05%)，Misdirection Color は 61/149(40.9%) のクッキーコンセントバナーに適用されていることがわかった．調査対象となる 5 種類のダークパターンすべてを検知することができ，特に Bad Defaults と Misdirection Color の利用率が高いことがわかる．

### 5.4 RQ2:国ごとのダークパターンの検知数

法規制対象が異なる国で適用されるダークパターンが異なるか確認した．調査対象とした地域は，日本，EU，USA，その他の国とした．それぞれ日本個人情報保護法， GDPR および ePrivacy 法， CCPA に関連してダークパターン利用率が異なるか調べる．ウェブサイトがある国は，D&B Hoovers のデータから取得した．国別にダークパターンの利用率を調査した結果を表 5,6,7 に示す．EU 圏内の国において， Consent Wall および Bad Defaults の検知数が多いことが確認できた．また，アメリカにおいて， Roach Motel の検知数が多いことが確認できた．一方で，日本では上記すべてのパターンの検知数は少なかった．

表 5: 国別の Consent Wall の検知数

| Consent Wall | 日本 | EU | USA | その他 |
|---|---|---|---|---|
| 利用あり | 2 | 23 | 6 | 15 |
| 利用なし | 646 | 804 | 350 | 715 |

表 6: 国別の Bad Defaults の検知数

| Bad Defaults | 日本 | EU | USA | その他 |
|---|---|---|---|---|
| 利用あり | 15 | 41 | 8 | 18 |
| 利用なし | 15 | 20 | 13 | 15 |

表 7: 国別の Roach Motel の検知数

| Roach Motel | 日本 | EU | USA | その他 |
|---|---|---|---|---|
| 利用あり | 0 | 8 | 12 | 5 |
| 利用なし | 65 | 89 | 46 | 86 |

GDPR では Consent Wall および Bad Defaults の利用が禁止されているが，GDPR で求められている同意の取得を優先したために，ダークパターンが混入した可能性が考えられる．CCPA では Roach Motel の利用が禁止されている．CCPA で求められているユーザの拒否権利を表面上用意しているが，実際には拒否されないようにするため，ダークパターンが混入してしまったと考えられる．日本の個人情報保護法ではユーザ同意を必要としていないため，ダークパターンにより同意の取得を誘導する必要性もなく，検知数が低かったと考えられる．

### 5.5 RQ3:CMP ごとのダークパターンの検知数

CMP 別のダークパターン検知数を調査した結果を表 8 に示す．Bad Defaults や Roach Motel は特定の CMP での利用が集中している一方で， Consent Wall , Misdirection size , Misdirection color は独自実装のバナーでの利用が多いことが確認できる．

ダークパターンの混入が，ウェブサイト管理者によるものか CMP の設定によるものかを確認するため，CMP の WordPress プラグインや公式サイトのリファレンスから CMP がダークパターン利用機能を提供しているかどうか調査した．その結果を表 8 に示す．CMP ライブラリ 2 をデフォルト設定で使用しクッキーコンセントバナーを表示した場合，Roach Motel パターンに該当することがわかる．実際に CMP ライブラリ 2 を利用したウェブサイト

表 8: CMP 別のダークパターン検知数および提供機能*

| CMP | 観測数 | Consent Wall | | Bad Defaults | | Roach Motel | | Misdirection Size | | Misdirection Color | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 検知数 | 機能 | 検知数 | 機能 | 検知数 | 機能 | 検知数 | 機能 | 検知数 | 機能 |
| 独自バナー | 2,457 | 44 | ○ | 19 | ○ | 2 | ○ | 12 | ○ | 51 | ○ |
| CMP ライブラリ 1 | 192 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 1 | ○ |
| CMP ライブラリ 2 | 152 | 0 | ◐ | 0 | ○ | 23 | ● | 0 | ◐ | 1 | ◐ |
| CMP ライブラリ 3 | 135 | 1 | ○ | 63 | ◐ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 4 | 62 | 0 | ◐ | 0 | ○ | 0 | ◐ | 0 | ◐ | 8 | ◐ |
| CMP ライブラリ 5 | 16 | 0 | ◐ | 0 | ◐ | 0 | ◐ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 6 | 12 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 7 | 10 | 0 | ◐ | 0 | ◐ | 0 | ◐ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 8 | 8 | 1 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 9 | 8 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 10 | 5 | 0 | ◐ | 0 | ○ | 0 | ◐ | 0 | ○ | 0 | ◐ |
| CMP ライブラリ 11 | 5 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 12 | 3 | 0 | ◐ | 0 | ○ | 0 | ◐ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 13 | 1 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |
| CMP ライブラリ 14 | 1 | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ | 0 | ○ |

(*) ○: ダークパターンの利用なしまたは不明, ◐: 設定によってダークパターン混入, ●: デフォルト設定でダークパターン混入

は Roach Motel パターンが多く観測されており，これらのウェブサイトではダークパターンが意図せず混入してしまっている可能性が高い．また，デフォルト設定ではないものの，ダークパターンが混入する機能を提供している CMP が多く確認できている．ダークパターンの混入が特定の CMP に偏っていることから，CMP が提供する機能によりウェブサイトにダークパターンが混入してしまっていると考えられる．

特定の CMP に利用が集中していたパターンが存在した一方で，Consent Wall, Misdirection Size, Misdirection Color は独自実装のクッキーコンセントバナーに多く適用されていた．これらのパターンは，EC サイトやモバイルアプリでの利用が多く確認されているパターン [7][9] であることから，当該分野での知見をクッキーコンセントバナーの実装に活用している可能性が考えられる．

## 6. 議論

RQ2 の結果から，法規制がある国では関連するダークパターン利用率が高いことを示した．このうち, Bad Defaults はカテゴリ別同意のオプションを持つクッキーコンセントバナー，Roach Motel は拒否機能を持つクッキーコンセントバナーに適用できるパターンである．本来，ウェブサイト管理者は法規制による要件を満たすようなクッキーコンセントバナーを生成するために CMP を導入していると考えられる．CMP を利用するウェブサイトからすると，生成されるクッキーコンセントバナーが法遵守されているかどうかは確認できない可能性が高いと考えられる．CMP 提供者は，ダークパターンとなりうる機能を利用できないようにクッキーコンセントバナーをデザインすべきである．

一方で，Misdirection パターンは独自実装のバナーが多く確認されている．RQ2 にて，EC サイトやアプリ開発の知見を活用していると考えられることを示した．このパターンは法規制とは関係がないことから，ウェブサイト管理者が意図的にダークパターン利用している可能性が高いと考えられる．ウェブサイト管理者は，ダークパターンを利用した不当な同意取得はユーザのプライバシーを侵害することを理解する必要がある．

## 7. 制限事項

本研究で検知されたダークパターンは全体の一部である．Consent Wall パターンの検知はウェブサイトの全体を覆うバナーに着目しているが，半分以上覆うようなバナーであったとしても，十分にユーザを誘導しうるパターンであると考えられる．また， Roach Motel パターンの検知は 2 回の手続きが必要なバナーのみを検知対象としているが，プライバシーポリシーから問い合わせが必要な場合や 3 回以上手続きが必要な場合は検知できていない．したがって，本研究のダークパターン利用率調査の結果は少なく見積もった結果であり，本調査における発見や主張に影響は与えないと考える．

クッキーコンセントバナーの振る舞いはアクセス元 IP アドレスによって制御されている可能性があるため，日本以外のウェブサイトで確認されたクッキーコンセントバナーはダークパターン利用有無が変化する可能性がある．アクセス元 IP アドレスを変えたクローリングを今後の課題とする．

## 8. おわりに

本研究では，複数の国のウェブサイトをクローリングし，クッキーコンセントバナーにおけるダークパターン利用率を調査した．また，実装方式ごとのダークパターンを調査し，ダークパターンの混入がウェブサイト管理者によるも

のか CMP によるものかを考察した．その結果，法規制と関係がないパターンについては他分野におけるダークパターンの知見が混入している可能性がある一方で，法規制に関連するパターンは CMP が提供する機能によりダークパターンが混入していることがわかった．ウェブサイト管理者および CMP 提供者は，ダークパターンの理解を深めた上で，法遵守およびユーザの信頼獲得に向けてクッキーコンセントバナーをデザインすべきである．

## 参考文献


[1] H. Brignull, “Dark patterns,” 2013. https://www.darkpatterns.org/.

[2] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, “Dark patterns and the legal requirements of consent banners: An interaction criticism perspective,” *Conference on Human Factors in Computing Systems - Proceedings*, 2021.

[3] Institute of Distributed Systems, Ulm University, “dark.privacypatterns.eu.” https://dark.privacypatterns.eu/.

[4] Council of European Union, “Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation),,” 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[5] The European Data Protection Board, “Guidelines 05/2020 on consent under regulation 2016/679,” 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[6] State of California, “Attorney general becerra announces approval of additional regulations that empower data privacy under the california consumer privacy act,” 2021. https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-additional-regulations-empower-data.

[7] L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, and A. Bacchelli, “UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception,” *Conference on Human Factors in Computing Systems - Proceedings*, 2020.

[8] M. Tahaei and K. Vaniea, ““ Developers Are Responsible ”: What Ad Networks Tell Developers About Privacy,” *Conference on Human Factors in Computing Systems - Proceedings*, p. 16, 2021.

[9] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, “Dark Patterns at Scale-Findings from a Crawl of 11K Shopping Websites,” *Conference on Human Factors in Computing Systems - Proceedings*, vol. 3, no. November, 2019.

[10] C. M. Gray, J. Chen, S. S. Chivukula, and L. Qu, “End User Accounts of Dark Patterns as Felt Manipulation,” *Journal of Human Technology*, pp. 1–22, 2020.

[11] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, “Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence,” *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–13, 2020.

[12] D. Machuletz and R. Böhme, “Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR,” *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, pp. 481–498, 2020.

[13] P. Graßl, H. Schraffenberger, F. Zuiderveen Borgesius, and M. Buijzen, “Dark and Bright Patterns in Cookie Consent Requests,” *Journal of Digital Social Research*, vol. 3, no. 1, pp. 1–38, 2021.

[14] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, “Circumvention by design – dark patterns in cookie consents for online news outlets,” pp. 1–15, 2020.

[15] “Consent-O-matic.” https://github.com/cavi-au/Consent-O-Matic.

[16] Mozilla, “Globaleventhandlers.onclick.” https://developer.mozilla.org/ja/docs/Web/API/GlobalEventHandlers/onclick.

[17] Mozilla, “Eventtarget.addeventlistener().” https://developer.mozilla.org/ja/docs/Web/API/EventTarget/addEventListener.

[18] Mozilla, “Element.getboundingclientrect().” https://developer.mozilla.org/ja/docs/Web/API/Element/getBoundingClientRect.

[19] Mozilla, “Mutationobserver.” https://developer.mozilla.org/ja/docs/Web/API/MutationObserver.

[20] Dun & Bradstreet, Inc., “D&b hoovers™.” https://www.dnb.com/products/marketing-sales/dnb-hoovers.html.

[21] “The chromium projects.” https://www.chromium.org/Home.