WEBサイト担当・EC担当のための

・個人情報・COOKIEの10のポイント

弁護士　水町雅子

2020.10.23作成中（随時更新予定）

講師略歴

弁護士　　水町雅子　（みずまちまさこ）

http://www.miyauchi-law.com　　メール→osg@miyauchi-law.com

- 東京大学教養学部相関社会科学卒業
- 現、みずほ情報総研入社 ITシステム設計・開発・運用、事業企画等業務に従事
- 東京大学大学院法学政治学研究科法曹養成専攻（法科大学院）修了
- 司法試験合格、法曹資格取得、第二東京弁護士会に弁護士登録
- 内閣官房社会保障改革担当室参事官補佐 マイナンバー制度立案（特にマイナンバー法立法作業、情報保護評価立案）に従事
- 現、個人情報保護委員会上席政策調査員 マイナンバー制度における個人情報保護業務（特にガイドライン、特定個人情報保護評価）に従事
- 首相官邸IT総合戦略本部「パーソナルデータに関する検討会」参考人 個人情報保護改正検討
- 宮内・水町IT法律事務所（旧、五番町法律事務所）共同設立、現在にいたる

その他、東京都都政改革アドバイザリー会議委員や、地方公共団体の情報公開・個人情報保護審査会委員等を務める。

マイナンバー・個人情報に関する著書・論文・講演・TV出演・新聞取材等多数。『１冊でわかる！個人情報保護法』（労務行政、２０１７年）、金融法務事情Ｎｏ.２０４６「改正個人情報保護法と金融機関の実務対応」、労政時報３９１５号「実務に役立つ法律講座（２３）個人情報」、ＮＢＬＮｏ.９４７「ライフログにおける法的問題」等著書・論文多数

- 個人情報保護法は、
  個人情報を入力させるWebサイト・ECサイトだけの問題ではない

- 個人情報を入力させなくても
  Cookie、個人関連情報などの問題を考える必要あり

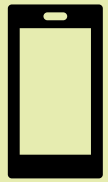
- 本資料では、
  ウェブ・Webマーケティング・ECサイト担当が押さえるべき
  個人情報・Cookieのポイントを10に絞って解説

目次＆ポイント

1. 何が個人情報なのか
   ～Webサイト運営で関係する個人情報は何か
   多岐にわたる（ユーザ入力情報以外にCookie、位置情報、閲覧履歴、購買履歴、自社内で紐づけられる情報等）
   ～メールアドレスやユーザIDは個人情報か
   場合による（次ページ以降参照）。
2. Cookieは個人情報なのか
   場合による。
   デジタル・プラットフォームの場合、独占禁止法に留意。EUは厳格なルール。
3. Cookieポップアップは必要か
   日本法上は義務付けられていない
4. プライバシーポリシーは概ね必須
   不要な場合→個人情報を一切取り扱わない場合
   利用目的等の記載が重要

1.　何が個人情報なのか（例）
～Webサイト運営で関係する個人情報は何か

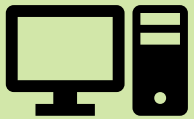
ユーザ側



・ユーザ入力情報
　例）氏名、住所

・Cookie等

サイト側



・ユーザの閲覧行動等

・サイトで生成・出力等する情報
　例）お買い物合計金額
　　性格診断結果

バック

・自社内で保有する個人情報と紐づける
　例）ユーザIDから属性情報・嗜好を引っ張って画面表示等をカスタマイズする
　例）ユーザIDから過去の購買履歴を抽出し、おすすめ商品の掲示等に利用

・他社から取得する情報と紐づける
　例）他社会員であることを確認
　例）遷移元を取得してユーザIDと紐づける

＊上に記載した情報でもそれ以外でも、全く誰かわからなければ個人情報ではないが、情報の履歴や項目数が多くなればなるほど、まったく誰かわからない場合は少ない。詳しくは、次ページ参照。

1.　何が個人情報なのか
～Webサイト運営で関係する個人情報は何か

◆ 個人情報とは、**誰の情報かわかる情報**のこと

〇氏名　　〇住所　　〇電話番号（例外として法人の共用電話番号の場合等、個人情報に当たらない場合も）

- しかし、上記だけではない。匿名SNSでも特定され誰かわかることがあるように、ID・書き込み・出品履歴・購買履歴・位置情報・写真・友達等から、氏名・住所等がなくても誰かわかることはある

◆ 誰かわかる情報と**紐づく情報**は、基本的に全て個人情報

- 下の表で、千葉-市ヶ谷を乗り降りしている人物はA1、すなわち情報太郎であるとわかるので、右の表だけでなく左の表も個人情報になる。さらにA1で管理している別データがあれば、それらも全て個人情報
- 容易照合性
  ＝単体で誰かわからなくても、困難なく照合できる他の情報から、誰かわかれば、全体が個人情報に
- また、仮に左の表だけだったとしても、つぶさな乗降履歴から誰の情報かがわかる場合もあり得る
  例）乗降が少ない駅で乗降が少ない時間帯に乗降している例や、長期間の乗降履歴等

仮名	乗降履歴
A1	2016年6月20日7時32分　千葉駅 2016年6月20日8時38分　市ケ谷駅 2016年6月20日19時55分　市ケ谷駅 2016年6月20日21時3分　千葉駅
B2	2016年6月20日8時35分　新宿御苑前駅 2016年6月20日8時58分　四ツ谷駅 2016年6月20日18時3分　四ツ谷駅 2016年6月20日18時25分　銀座駅 2016年6月20日23時35分　銀座駅 2016年6月20日23時53分　新宿御苑前駅

仮名	実名
A1	情報太郎
B2	難波舞

1.　何が個人情報なのか
～メールアドレスやユーザIDは個人情報か

◆ **メールアドレスは？**

- 個人情報の場合とそうでない場合がある

〇 masako.mizumachi@kitty.or.jpのような氏名入り

✕ 09pika586chew@freemail.comのように誰かわからないメールアドレスで、
メールアドレス単体しか取り扱わない場合。

〇誰かわからないメールアドレスでも、メールアドレス以外から誰かわかる場合
（氏名と紐づいている場合等）

- 個人情報と非個人情報のメールアドレスを明確にシステマチックに切り分けられない以上、メールアドレスは全部個人情報として扱った方が安全である

◆ **ユーザID**は？

→　個人情報の場合とそうでない場合がある

〇実名ID　例）masako.mizumachi

〇有名ID（有名人のSNSアカウント等）

〇上記以外でも、他の情報（購買履歴、位置情報、送り先住所等）から
誰の情報かわかれば個人情報

1.　何が個人情報なのか

- なお、個人情報は、プライバシー情報とは異なる
  - 「個人情報」の定義は、法律で明確に確定されている
  - 人（対象者）によって、個人情報だったり非個人情報だったりしない
    （保有者が企業か自治体か国か独法等かによって個人情報である場合とそうでない場合はある。
    例えば死者情報、事業者情報等は自治体によっては個人情報だったりそうでなかったりする。）
  - 秘密にしたい情報や重要情報が個人情報なわけではない
  - 公知の事実も個人情報である

何が個人情報かについてもっと詳しく知りたい方は、以下の22-32ページをご参照ください。
http://www.miyauchi-law.com/f/170313piikaiseigaiyou.pdf

2. Cookieは個人情報なのか
～Cookieは個人情報か

- **Cookieとは**
  - Webサイトにアクセスしたときなどに PCやスマホなどに保存されるもの
  - そのユーザのブラウザを識別し、ユーザの好みや行動を覚えておく
  - 利用用途は多岐にわたる
    - 何度もログインしなくてよくしたり、お買い物カートの中身を保存したり、アクセスログ・閲覧履歴等を解析するため、広告配信のため等

- Cookieは個人情報か

  → 個人情報の場合とそうでない場合がある

  - Cookieは個人を特定しないでブラウザを特定するものなので、個人情報ではないという人がいる。
    →確かに、業務用の共有PCや家族間共有PC、ネットカフェなどの場合は、ブラウザを複数人で共有する。
    →とはいえ、特定の人に届くであろうと思って、ターゲティング広告等が実施されているとも考えられる？
  - Cookieを元に自社保有の会員情報（氏名・住所等）をたどれたりすれば、Cookieも個人情報に当たる（容易照合性）
  - Cookie情報からたどっても氏名がわからなかったとしても、Cookieと紐づけられる情報によっては（位置情報や購買履歴等）誰の情報かがわかり、そうすると、CookieもCookieと紐づく情報も個人情報に当たる

2. Cookieは個人情報なのか
～Cookieへの法規制はあるのか

- ◆ 日本法とEU法等で、法規制が異なる
  - 日本法では、個人情報保護法と独占禁止法が主に問題となる（場合によっては他法も）

- ◆ 日本の**個人情報保護法**のCookieへの規制
  - 個人情報又は個人関連情報に当たらなければ、原則として特に規制なし
  - 個人情報又は個人関連情報に当たったとしても、Cookie特有の規制ではなく、個人情報保護法上の規制となる（顧客名簿等の通常の個人情報や個人関連情報と同じ規制という意味）
    - 利用目的の特定・通知等、目的外利用規制、第三者提供規制、安全管理措置　などなど
- ◆ 日本の**独占禁止法**のCookieへの規制
  - 公正取引委員会「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」https://www.jftc.go.jp/dk/guideline/unyoukijun/dpfgl.html
  - 「デジタル・プラットフォーム」に関する考え方。一般的企業の公式Web等は含まれない。
    - デジタル・プラットフォームとは、オンラインのサービスの「場」を提供し、そこに異なる複数の利用者層が存在する多面市場を形成し、いわゆる間接ネットワーク効果が働く特徴を有するもの。オンライン・ショッピング・モール，インターネット・オークション，オンライン・フリーマーケット，アプリケーション・マーケット，検索サービス，コンテンツ(映像，動画，音楽，電子書籍等)配信サービス，予約サービス，シェアリングエコノミー・プラットフォーム，ソーシャル・ネットワーキング・サービス(SNS)，動画共有サービス，電子決済サービス等。
  - 個人情報に当たらないCookie等についても、利用目的をユーザに知らせ、目的内利用を厳守し、安全管理措置を講じるべき。不当に個人情報を収集してもいけない。
  - 不利益な取扱いを受けても、ユーザ側としてそのプラットフォーム・サービスを利用するために受け入れざるを得ないような場合（代替可能性のないサービス、事実上乗り換えられないサービス等）。

2.　Cookieは個人情報なのか
～Cookieへの法規制はあるのか

- ◆ 日本の**個人情報保護法改正**でCookieへの規制
  - 個人関連情報規制の創設
    - 提供元基準説の潜脱が禁止される
    - 提供元にとって個人データでなくても、提供先にとって個人データであることが想定されるものを提供する行為が、個人情報保護法によって規制されることに（改正法26条の2）
    - 法23条1項各号（法令に基づく場合等） 又は 本人同意が得られていることを確認した場合（詳細は委員会規則）に提供可
    - 記録・保存義務あり（改正法26条の2第3項で準用される26条3・4項。なお改正法26条の2第3項では26条2項も準用。）
    - 外国への提供であっても同様
  - 令和元年12月13日「個人情報保護法いわゆる３年ごと見直し制度改正大綱 」
    - ここ数年、インターネット上のユーザーデータの収集・蓄積・統合・分析を行う、「ＤＭＰ（Data Management Platform）」と呼ばれるプラットフォームが普及しつつある。この中で、クッキー等の識別子に紐付く個人情報ではないユーザーデータを、提供先において他の情報と照合することにより個人情報とされることをあらかじめ知りながら、他の事業者に提供する事業形態が出現している。
    - ユーザーデータを大量に集積し、それを瞬時に突合して個人データとする技術が発展・普及したことにより、提供先において個人データとなることをあらかじめ知りながら非個人情報として第三者に提供するという、法第23条の規定の趣旨を潜脱するスキームが横行しつつあり、こうした本人関与のない個人情報の収集方法が広まることが懸念される。
    - https://www.ppc.go.jp/files/pdf/seidokaiseitaiko.pdf
  - 改正詳細
    - 水町作成資料　http://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou.pdf
      - 上記PDFを「個人関連情報」で検索

2. Cookieは個人情報なのか
～Cookieは個人情報か

- **EUのCookieへの規制（留意：必ずしも記載が最新でない可能性があります）**
  - ePrivacy指令（Privacy and Electronic Communications Directive）5(3)で事前の同意が必要。同指令に対応する国内法が各国である。
    - イギリス：The UK introduced the amendments on 25 May 2011 through The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
    - フランス：2009年改正Informatique et Libertés法のほか、リコメンデーション。
  - ePrivacy規則（ePrivacy Regulation）が検討されている
- Cookieの機能別に同意不要／要（イギリスの例） https://cyberlawissues.hatenablog.com/entry/2019/04/10/120826
  - 厳に必要なクッキーは同意不要
    - 例えば、通信等のためだけに使われるクッキー
    - ユーザが「カートに入れる」「購入する」ボタンを押した場合に、前のページでユーザが何を選んだかをサイト側が記憶しておくために使うクッキー。
    - セキュリティのためのクッキーや、負荷分散のためのクッキーも。
  - 上記以外の、例えば以下のクッキーなどは説明責任＆同意取得義務あり
    - PVやユニークユーザカウントのための統計目的クッキー
    - 広告のためのクッキー
    - ユーザへのあいさつなど、画面表示のカスタマイズ用のもの
  - 義務がかかるのは、オンラインサービスを運営してクッキーを使っている人（説明責任＆同意取得義務が生じる）。
    - クッキーを発行する人が第一次的にコンプライアンスの責任を負う。
    - サードパーティクッキーの場合は、クッキー発行者とそのサイトの運営者双方が責任を負う。もっとも、ユーザと直接の接点がない第三者の場合は難しいけれども、重要なのは誰が同意を取得するかではなく、よく説明された上で有効な同意が取得されることである
  - 規制に従ったWebサイトは多くないとの報道も

3. Cookieポップアップは必要か

- Cookieポップアップは日本法上は義務ではない
  - 「このサイトはCookieを利用しています　→承諾→拒否→CookiePolicy」といったポップアップ画面のこと
  - もちろん、日本法上Cookieポップアップがあっても良いし、ユーザに説明をして同意を得ることは良いこと

- Cookieウォールでは、ユーザから同意を得たことにならず無効
  - Cookieウォールとは、Cookie利用に同意しなければ、そのWebサイトを閲覧したり利用できないとする仕組み
  - 前記の通り、EUではCookie等に同意が必要だが、Cookieウォールではその同意として無効と、オランダの当局が判断した模様　https://jp.techcrunch.com/2019/03/11/2019-03-08-cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/
  - 欧州データ保護会議（EDPB） もCookieウォールはダメとする
    https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
  - 企業側にしてみればCookie拒否に対応するWebサイト運営の困難性がある？
    EU法にしてみれば、Cookieを拒否すればサービスが利用できない、Webサイトが閲覧できないというのでは、自由にユーザが同意したり拒否したりはできないという意味となってしまい、自由な同意に基づくユーザの選択ではないという意味で、無効
  - なお、EDPBは、画面のスクロールやスワイプをもって、同意とみなすことはできないとする。日本の利用規約では、利用をもって同意とするというのが良く見られるが（継続利用と1スクロールは違うといえば違う）。

- 日本や世界におけるCookie規制の今後
  - Cookie等では、ユーザ側からするとよくわからずに、個人情報等が取得される可能性がある（←ユーザ入力情報であればユーザ側からしても入力していることは明確）。トラッキングの問題も。
  - その透明化の手段としてEUの法制がある。日本でも今後どうなるか。
  - 但し、Cookie等の利用用途が多岐にわたり、厳に必要なものもあるし、個別に事前同意を得ることが現実的に可能かという問題もある。EUでも、Cookie規制の実効性について疑義あり？

4.　プライバシーポリシーは概ね必須

- Webサイトからプライバシーポリシーのリンクは、概ね必須
  - 不要な場合→個人情報を一切取り扱わない場合

- プライバシーポリシーの法的意味
  - プライバシーポリシー自体が法律上要求されているわけではなく、この形式は商慣習的なものともいえる？
  - 利用目的の公表等が法律上要求されていて、多くの企業ではプライバシーポリシーの形態でこの法律上の要求に答えている

- 名称は何でもよい
  - 個人情報保護基本方針、個人情報保護方針、個人情報取扱方針、プライバシーステートメントなどなど
  - なんでも名称は良い

- クリック／タップ数が重要
  - 1クリック程度で開けないといけない（ガイドラインの要請）
  - そのため、多くのサイトでは、常時フッターにリンクを掲示することで、どのページからも1クリックで遷移できるようになっている

- 企業で1つ？　サイトで1つ？
  - どちらでもよい

4.　プライバシーポリシーは概ね必須

- 他サイトのプライバシーポリシーをそのまま真似するのは危険
  - 重要なのは、**利用目的**（個人情報保護法18条）。
    - 他サイトを参考にするのは良い。自社に必要な目的をさらに追加・削除しなければならない。
    - プライバシーポリシーに記載した利用目的通りに利用する必要がある。それを超える利用は、原則違法
      （例外：1仮名加工情報　2個人情報の適法な目的外利用　3個人情報の適法な利用目的の変更）
    - 利用目的に漏れがないように。
    - そして、ユーザから見て理解できるような利用目的にしなければならない。
      漠然とした利用目的は、利用目的の特定違反として個人情報保護法15条1項違反にも。
    - 第三者提供する場合は、その旨を記載する。
  - 個人情報の**外部提供**を共同利用やオプトアウト構成で実施する場合は、その旨も記載する。
  - **開示等の求めに応じる手続**も記載する。
    - 本人から「私の情報を見せてくれ」と言われたら、原則として応じる法的義務がある。本人がそれをどうすれば請求できるか記載する。
  - **問い合わせ先や苦情の受付窓口**も記載する。
  - プライバシーポリシーは、きっちり作りこまなければいけない文書。
  - 参考→　https://cyberlawissues.hatenablog.com/entry/2019/06/12/142251

5.　利用規約が必要な場合

未完成

- ユーザとの約束事を決めるのが利用規約
  - ユーザ側の禁止行為（違法投稿、誹謗中傷の禁止等）
  - 料金・支払（有料サイト等の場合）
  - 利用環境
  - 事業者側の責任　等々
- プライバシーポリシーは、個人情報特有のもの
- 利用規約が必要なサイトとそうでないサイトがある
  - 必要な場合はどういう場合か説明が難しいが、平たくいうと、約束事をしておくべきか否かで判断。

6.　個人情報の使い道（利用目的）を明らかにしているか

未完成

- 取り扱う個人情報を何に使うかを明らかにしているか
- これが足りていないと原則違法になる
- もっとも、仮名加工情報、匿名加工情報、統計情報は別
- サイト側で保存しなければ、個人情報の取扱いが発生していないという誤解
  - サイト側で処理（計算等）したりすれば、個人情報の取扱いあり。例えば、認証用に、メールアドレスや顔画像をユーザに入力/撮影してもらうが、サイト側では保存しないとしても、それらを利用している以上、個人情報の取扱いありとなる。

7.　ユーザから見て不透明な個人情報の収集をしていないか

未完成

- ユーザからすると、自分が入力した情報以外、何がサイト側の手に渡るのかが不透明
- 特に、複数サイトの連携がある場合、バックグラウンド処理がある場合等
  - 例）自社リアル店舗とオンライン店舗のポイント合算
  - 例）自社会員と他社会員の突き合わせ
  - 例）他社から情報を取得し、自社事業に利用
- 個人情報保護法17条1項違反にならないよう留意
- また、同法17条2項違反にならないよう留意

7.　他サイト（自社運営）との連携

未完成

- （作成中）

7.　実店舗（自社運営）との連携

未完成

- （作成中）

7.　他サイト（他社運営）との連携

未完成

- （作成中）

8.　個人関連情報とは何か

未完成

- 参考）以下の右下ページ番号29-35ページ
  http://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou.pdf

9.　外国にサーバや情報移転はないか

未完成

- （作成中）

10.　本人対応の法的重要性

未完成

- （作成中）

個人情報、マイナンバー、医療情報、医療ビッグデータ法（次世代医療基盤法）、
行政ビッグデータ、 DPIA、IT/ICT、契約書・規程策定、国との交渉、企業法務全般、
条例策定支援その他に関するお問い合わせ、ご相談がありましたら、お気軽にどうぞ

http://www.miyauchi-law.com

宮内・水町IT法律事務所
弁護士　水町　雅子
メール→　osg@miyauchi-law.com

※本資料はあくまで当職の意見にすぎず、当局見解と異なる場合があり得ます。
また誤記・漏れ・ミス等あり得ますので、現行法やガイドライン原典に当たるようお願いします。