

資料 4

プラットフォームサービスに関する研究会

利用者情報の通知・同意取得に関する諸外国の事例

株式会社野村総合研究所
コンサルティング事業本部

2020年12月4日

NRI

Share the Next Values!



1. 調査の経緯
2. GDPR : General Data Protection Regulation (一般データ保護規則)
3. Cookie等類似の技術に対する規制
4. CCPA : California Consumer Privacy Act of 2018
5. NIST Privacy Framework
6. ISO/IEC 29184:2020 Online privacy notices and consent

有効な同意の取得やその際の説明の在り方について、さらに検討を深めることを目的に諸外国において通知・同意取得の際に推奨されるルールや事業者の取り組みを調査した。

プラットフォームサービスに関する研究会 最終報告書における記述（抜粋）

第2節 市場環境の変化を踏まえた規律の適用範囲・対象の見直し

2. 今後の検討の具体的な方向性

(1) いわゆる「同意疲れ」への対応

いわゆる「同意疲れ」は、**より多くの利用者情報が利用者から取得されるようになり、また、その活用の方法が複雑かつ多岐にわたるようになり、さらに、その結果同意取得時の説明も複雑で分かりにくくなる**といった事情が相まって生じているものと考えられることから、こうした事情を踏まえて、**有効な同意の取得やその際の説明の在り方について、さらに検討を深める**ことが必要である。

利用者情報の取扱いにあたり、利用者に通知・同意取得を行う際、推奨される又は留意すべき事項について諸外国のルールや事業者の取り組みを調査した。

GDPR : General Data Protection Regulation (一般データ保護規則)

- Guidelines on transparency
- Guidelines on consent under Regulation

概要

- EU※域内の個人データ保護を規定する法として、2016年4月に制定、2018年5月25日施行
- 従前のEUデータ保護指令が、加盟国による法制化を要するのに対し、GDPRはEU加盟国 同一に直接効力を持つ
- GDPRでは個人データの取得にあたり、必ずデータ主体からの同意取得を求めている
- 通知・同意取得にあたり推奨される方法や留意すべき事項はガイドラインで解説される
 - 通知 : Guidelines on transparency
 - 同意取得 : Guidelines on consent under Regulation

※ EU : EU加盟国及び欧州経済領域 (EEA) の一部であるアイスランド、ノルウェー、リヒテンシュタイン

GDPR第12条では透明性について主要な規定を行っている。

- 「データ主体への情報提供」「権利行使に関するデータ主体との連絡」「データ侵害に関する連絡」に関する一般ルール
 - ① 簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式でなければならない
 - ② 明瞭かつ平易な文言が使われなければならない
 - ③ 子どもに情報を提供する際は、明瞭かつ平易な文言という要件が特に重要であり
 - ④ 書面で、又は適切であるときは電子的な手段を含め、その他の方法によらなければならない
 - ⑤ データ主体によって要求された場合は、口頭で提供することができる
 - ⑥ 一般に無償で提供されなければならない

「①簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式」の説明とその実現のために推奨される通知方法・工夫の例示として、ガイドラインでは以下が挙げられている。

「簡潔で、透明性があり、理解しやすく、容易にアクセスできる」の説明

具体的な意味合い

推奨される通知方法・工夫の例

簡潔である

- 主体に情報疲労をさせない為に、情報管理者が情報／通知を効率的かつ簡潔に提示する

- 階層的なプライバシーステートメント／プライバシー通知により、大量のテキストスクロールを不要とする

透明性がある

- データ主体が使われ方を事前に知らなければならない
- リスクを事前に評価し、正しくデータ主体に伝える

- 事前にリスクの有無を丁寧に評価する

理解しやすい

- ごく普通の人でも理解できるようにすることが必要である
- 可能ならば対象者に理解してもらいやすい説明を行うべき

- 理解のしやすさや有効性が分からないときは、公開討論やテストで試行する

容易にアクセスできる

- 必要な情報がどうすれば確認できるかが一目瞭然である

- サイト上に、明瞭に視認できる形でプライバシーステートメント／プライバシーノティスを公表する
- アプリの場合は、ダウンロード前のオンラインストアや、アプリ内から情報に容易に（2タップ以内で）アクセスできるようにする
- 個人データを収集する時点で、プライバシーステートメント／プライバシーノティスへのリンク、又は個人データを収集するのと同じページにその情報を表示する

また、有効な同意としてGDPR第4条においては以下の4要素を満たすことが求められる

有効な同意の4要素

①「自由に与えられる」

- データ主体に選択権・支配権がある
 - ✓ 強制されたと感じない
 - ✓ 同意しなくてもネガティブな結果にならない
 - ✓ 契約等で交渉不可になっていない
- 上記が満たされない場合、同意は無効である

②「特定されている」

- 特定の目的に対応し、同意するかどうかをデータ主体が選べる
 - ✓ 同意の目的は明確に記述する
 - ✓ 同意取得に関係した情報は、他の情報から明確に分離する
 - ✓ 別目的に使う場合は同じデータでも追加の同意が必要である
- 特定の目的に対し、特定の同意を与えられるよう、管理者は個別のオプトインを提供すべきである

③「説明を受けている」

- GDPRでは「同意が説明を受けた上でのものでなければいけない」という要件が強化されている
- 同意を取得する前に、データ主体に情報提供することが必要不可欠である

④「不明瞭ではない」

- 同意は、データ主体が積極的に行動・宣言して与えられるべきである
 - ✓ 契約書への合意やサービス条件の承諾だけでは、積極的な同意とはみなされない
 - ✓ あらかじめチェックの入ったオプトインのチェックボックスやオプトアウトの仕組みも無効
(承諾“しない”ことに行動が必要なため)

GDPR : General Data Protection Regulation (一般データ保護規則)

GDPRを踏まえ、より効果的に通知・同意取得を行うことができる工夫として、ICO※では以下を挙げている。

ICOにおいて推奨される通知・同意取得における工夫

1. 階層的アプローチ (A layered approach)

重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。

2. ダッシュボード (Dashboards)

管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。

3. ジャストインタイム通知 (Just-in-time notices)

個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。

4. アイコン (Icons)

特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。

5. モバイルおよびスマートデバイスの機能性 (Mobile and smart device functionalities)

ポップアップ、音声アラート、モバイルデバイスのジェスチャーなど。

GDPR : General Data Protection Regulation (一般データ保護規則)

階層的アプローチ (A layered approach)

- 重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。
- プライバシー情報の取扱い以外に通知すべき情報があるとき (金融業界における不正利用禁止など) に役立つ。

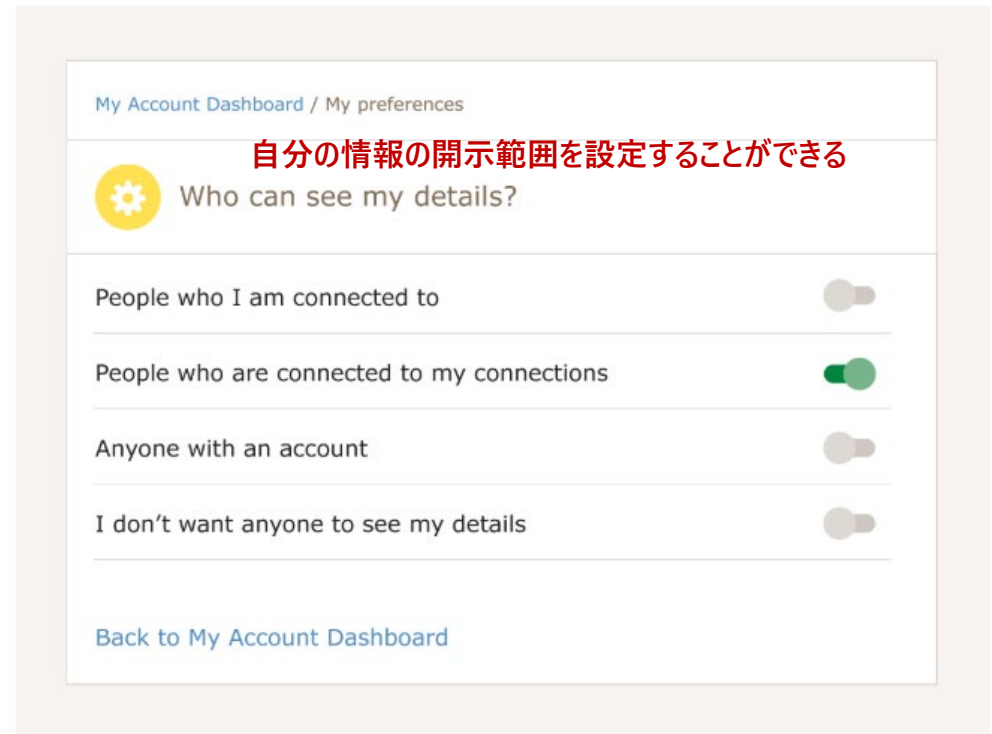
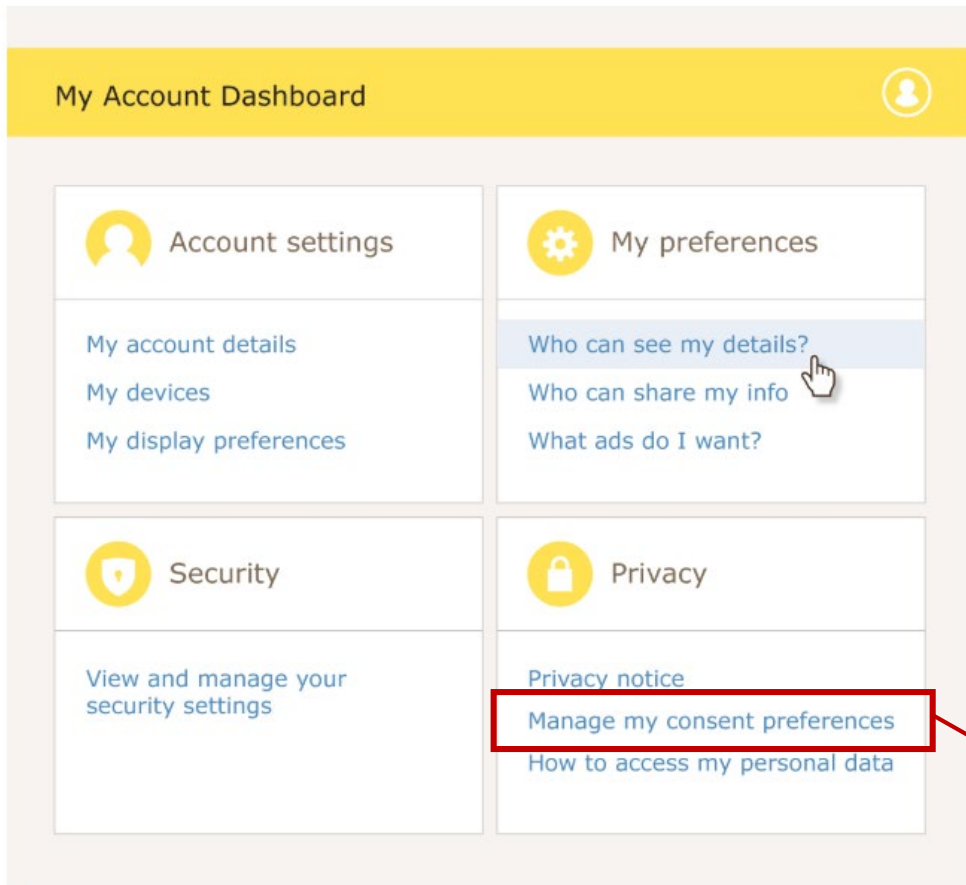
項目を選択すると短文の説明が表示される

短文の説明から更に詳細な説明 (プライバシーポリシー全文等) へ遷移できる

GDPR : General Data Protection Regulation (一般データ保護規則)

ダッシュボード (Dashboards)

- 管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。
- 同意と同程度容易に同意の撤回ができなければならないというGDPRの要件を満たすことに役立つ。



この仕組みを応用する形で、利用目的の種類や第三者提供先について、個別に同意・管理することができるコンセント・マネジメント・プラットフォームサービスが提供され始めている。

ジャストインタイム通知 (Just-in-time notices)

- 個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。
- 収集時に限らず、購入時等異なるタイミングで通知を行うことで、あらかじめ個人が、情報を提供していることを認識するのに役立つ。

Create an account

Title

Mr

Name

Joe Bloggs

Email address



Username

Password

Confirm password

Create account

メールアドレスを登録する際に、利用目的を通知している

We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. [Please follow this link for further information.](#)

アイコン (Icons)

- 特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。
- アイコンを用いることで、データの処理が行われていることを個人にリマインドするのに役立つ。

アイコンの利用方法①

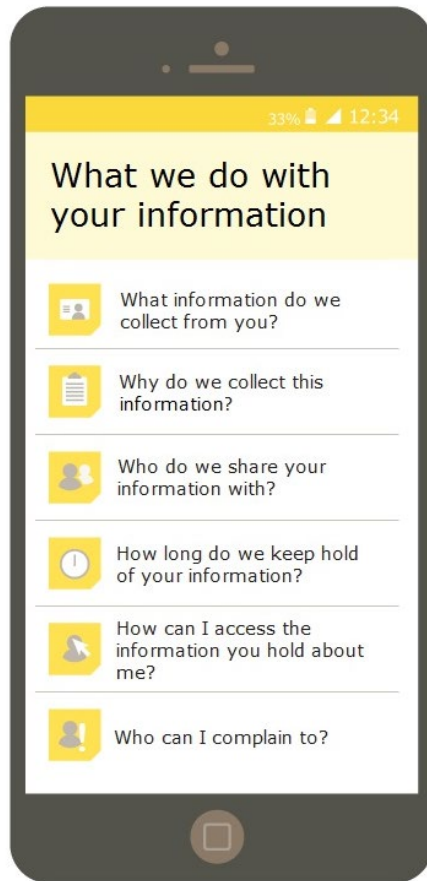
- 個人がオンラインフォームにメールアドレスを入力すると、情報がマーケティングに使用されることを示すアイコンを表示する。アイコンの上にカーソルを置くと、「マーケティング」という言葉が表示され、それをクリックすると、メールアドレスを使って何が行われるかについての、より詳細な説明が表示される。

アイコンの利用方法②

- データ処理が断続的に行われている場合、データ処理が行われていることを示す便利なリマインダーとしてアイコンを使用する。
- このアプローチは特定のアプリが位置情報を処理しているかどうかを示すために、ステータスバーに認識可能なアイコンを配置することで、スマートフォンでよく使用されている。

モバイルおよびスマートデバイスの機能性 (Mobile and smart device functionalities)

- スマートフォンやタブレットなどのモバイル端末は画面の大きさに制約がある反面、ポップアップ、音声アラート、ジェスチャーなどの独自の機能を利用することができる。



【モバイル端末独自の機能を利用した通知・同意取得の例】

- ジャストインタイムの通知を配信するためのポップアップ。
- 音声、音、振動（または触覚フィードバック）による特定のデータ使用を示すアラート（例：wifiや位置情報の追跡）。
- 圧力感知ディスプレイを使用して、個人がそのページを離れることなく、プライバシー情報の追加レイヤーにアクセスできるようにする。
- より詳細な情報を表示したり、データの異なる使用方法を制御したりするために、スワイプ等モバイルデバイスの一般的なジェスチャーを使用する。

Cookie等類似の技術に対する規制

- The Privacy and Electronic Communications Regulations (PECR)
- Guidance on the use of cookies and similar technologies
- CNIL RECOMMENDATION "COOKIES AND OTHER TRACKERS"

概要

- GDPRを踏まえ欧州のデータ保護機関においては、Cookie等の取得・利用に関して通知・同意取得する方法について、ガイドライン等により規定を行っている。
 - イギリス：The Privacy and Electronic Communications Regulations (PECR)
 - 電気通信に関するプライバシー権を整理した英国法
主にマーケティングコール、クッキー、通信サービスのセキュリティ、位置情報の利用を規制している
 - イギリス：Guidance on the use of cookies and similar technologies
 - クッキーおよび類似技術の利用に関して規定する文書
 - フランス：RECOMMENDATION "COOKIES AND OTHER TRACKERS"
 - クッキーおよび類似技術の利用に関して消費者に通知・同意取得する方法について、推奨する方法を提示
 - 2020年10月に採択された
 - ※ 採択された文書は仏語版のみのため、本調査では英語版のドラフトをベースに記載している

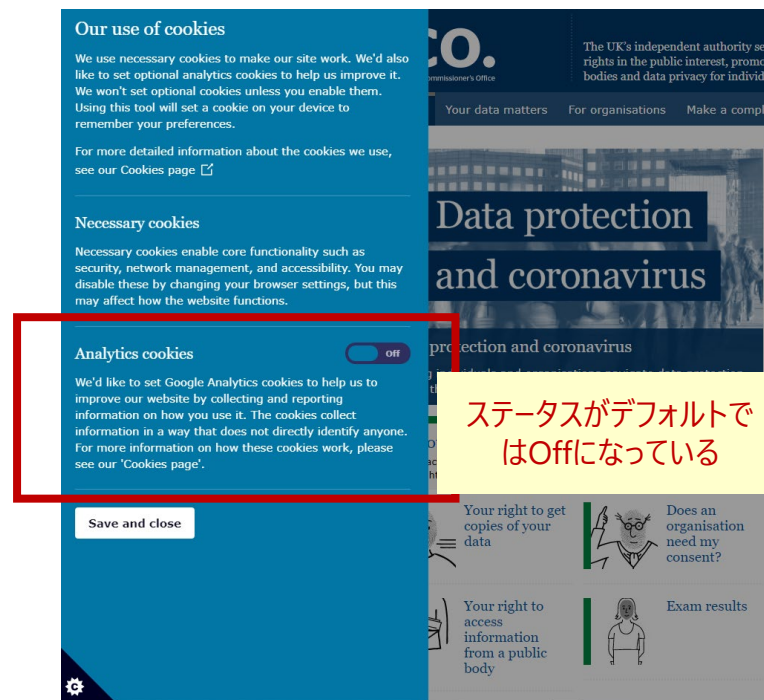
ガイドラインにおいて示されているクッキーの取得・利用に関する主な規定

- ユーザーの同意がない限り、サービスへのアクセスを制限するための包括的なアプローチとしてのクッキー・ウォールを使用することは同意要件を満たしていない。
- 当局（ICO）は、クッキーウォールの使用が、サービスへのアクセスの条件として企業や第三者が個人データを使用することに同意することをユーザーに要求したり、影響を与えたりすることを意図している場合、ユーザーにはクッキーを受け入れる以外に真の選択肢がないため、このアプローチは不適切であると考えます。
- 黙示の同意も認められない。「このウェブサイトの使用を継続することで、クッキーに同意していることとなります」というような文言は、GDPRが求める有効な同意の要件を満たしていないため、使用すべきではない。
- 事前にチェックを入れたボックスや、スライダーのデフォルトが「オン」になっているようなものは、ターゲティング広告用などウェブサイト等の利用に必要な不可欠ではないクッキーの利用には使用できない。
- ユーザーは、ウェブサイト等の利用に必要な不可欠ではないクッキーを制御する必要があり、同意を得る前にランディングページに設定してはならない。
- バナー、ポップアップ、スプラッシュページを使用することは、クッキーの利用を強調して同意を得るための有用な方法に該当するが、ユーザーがページ上の他の場所をクリックしたり、同意ボックスや利用可能なオプションに関与しなかったりした場合に、必須ではないクッキーが設定されている場合は、このようなアプローチは有効ではない。これは、GDPRで求められているように、ユーザーがクッキーに同意するための明確で積極的な行動をとっていないと考えられるためである。ウェブサイト運営者は、必須ではないクッキーを事前に有効にしてはならない。当局（ICO）の見解は、ユーザーが選択を与えられたときに特定の非必須クッキーを選択する可能性は低いかもしれない、あるいはクッキーがプライバシーを侵害するものではないからというだけで、これは事前に有効にする有効な理由にはならないというものである。ユーザーがデバイスに設定される前に積極的な行動を取らずに非必須クッキーを有効にすることは、有効な同意を表すものではない。これを行うことで、ウェブサイト運営者はユーザーから選択権を奪っていることになる。
- 当局（ICO）はユーザーがクッキーを「拒否」または「ブロック」するよりも「同意」または「許可」すべきであることを強調する同意のメカニズムを非準拠とみなしている。当局（ICO）はこれを、ユーザーに「受け入れる」という選択肢に影響を与える「おだて行動（nudge behavior）」と呼んでいる。

ガイドラインにおいて示されているクッキーの取得・利用に関する主な規定

- 最初のバナー/ポップアップアウトやその他のソリューションの一部としてではなく、**「詳細情報」セクションに同意コントロールを組み込む同意メカニズム**も、非必須クッキーが設定される前にユーザーが選択できるようにしていないという理由で**非準拠**とみなされる。
- ターゲティング広告用やサイト内移動の分析用といったクッキーは「ユーザーのウェブサイト利用にあたり、厳密に必要なもの」ではないため、クッキーの同意規則の対象外にはならない。広告用途等のクッキーは、ウェブサイトやモバイルアプリの運営者にとっては、サービスに資金を供給するための収益をもたらすために重要なものかもしれないが、ウェブサイトの利用者の観点からは「厳密に必要な」ではないため、規制の対象となる。
- ウェブサイトが第三者のクッキーを使用している場合、サイト運営者は、通知が提供され、有効な同意が得られるように協力しなければならない。当局（ICO）は、クッキーの設定を希望する第三者、またはクッキーの設定を必要とする製品を提供する第三者は、**クッキーの同意要件が効果的に対処されることを保証する**ために、ウェブサイトの発行者との契約に**契約上の義務を含めることを推奨**している。

ガイドラインがクッキーの利用にあたり適切な同意取得方法として推奨している事例



<https://www.osborneclarke.com/insights/cookies-trackers-cnll-publishes-new-recommendations-launches-public-consultation/>

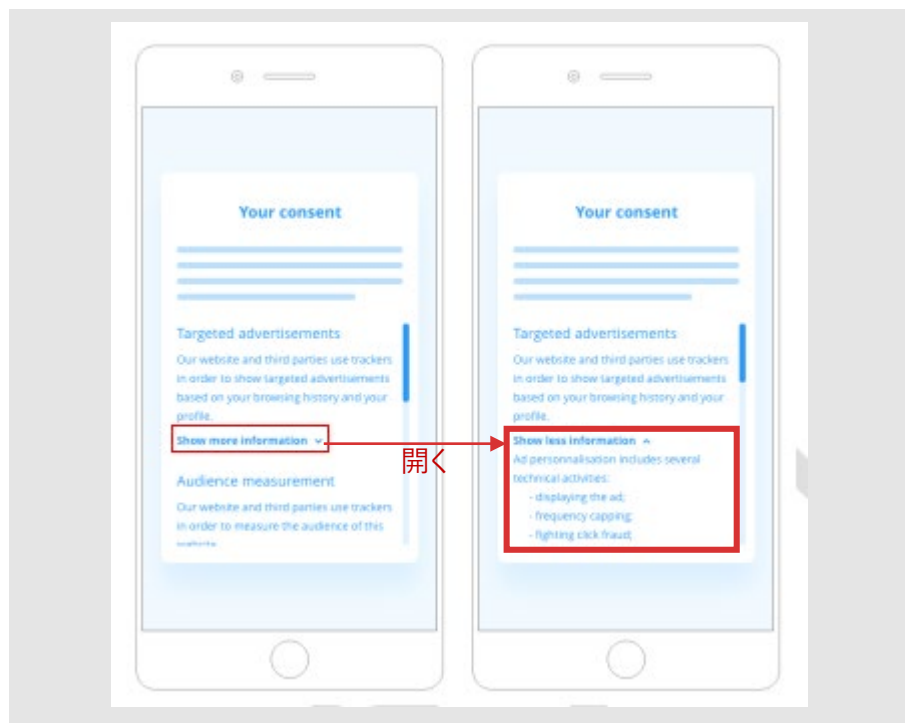
ユーザーによる明示的かつ積極的な行動を必要としている

「通知・同意の情報提示」内では、有効な手法として階層的な表示を推奨している。

階層的な表示のイメージ

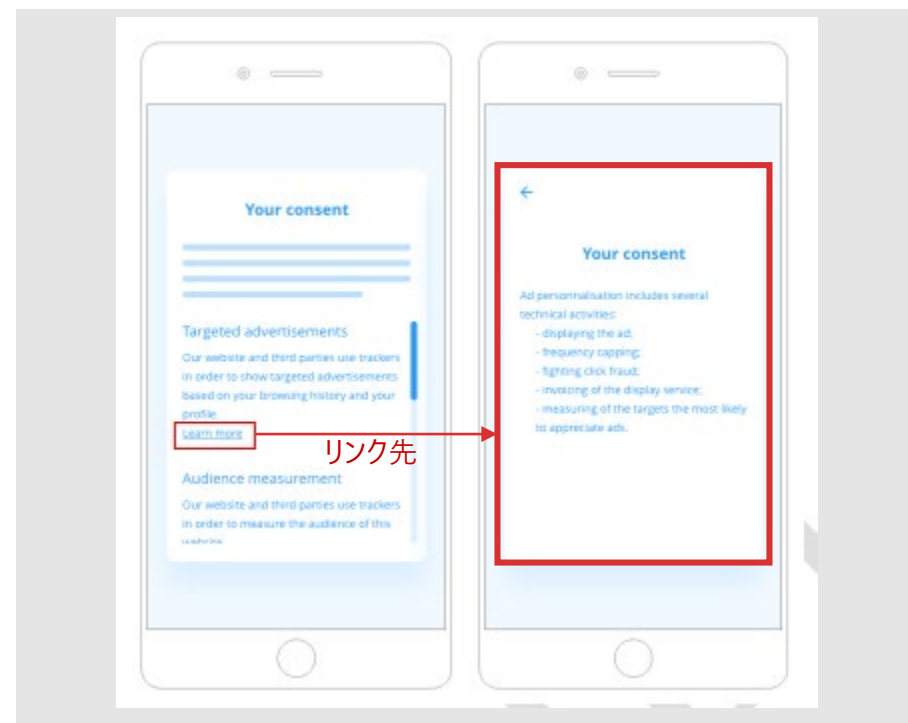
ドロップダウン

- 目的の詳細が、1層目の画面で有効にできるドロップダウンボタンの下に格納されている



ハイパーリンク

- 目的の詳細が、1層目の画面のハイパーリンクをクリックすると確認できる

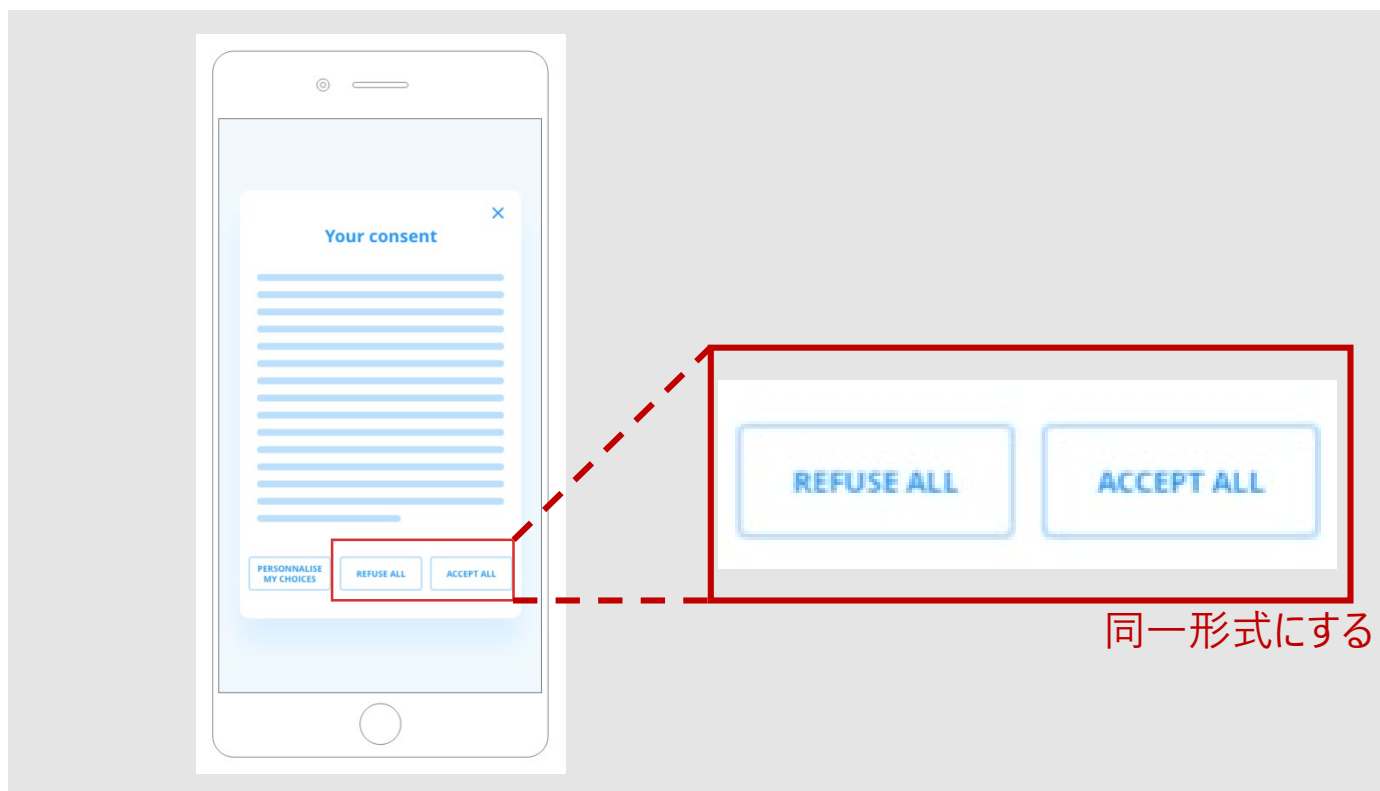


Cookie等類似の技術に対する規制：RECOMMENDATION "COOKIES AND OTHER TRACKERS"

デザインによってユーザーが誘導されないよう、承認/非承認のボタンを提案する際は、同一のサイズ、ハイライト、フォントおよび読みやすいものであることが推奨されている

- 利用者の負担を軽減する為、「すべて承認」「すべて非承認」というボタンを用意し、単一の行動で複数の同意・拒否を行えるように設計することも可能。その際は特に誘導がないように注意する必要がある

ユーザーを誘導しない同一形式のボタン設計



「全て承諾」「全て拒否」と並列でボタンを設定して、ユーザーの目的ごとの承諾内容にアクセスできるように階層化することも一案として提示されている。

- 「全て承認」「全て非承認」と並行してボタンを用意する場合は、同様の情報レベルで作成する
- 目的別の選択ができることが分かるよう、直感的な名称を使用する必要がある

ユーザーを誘導しない同一形式のボタン設計



CCPA : California Consumer Privacy Act of 2018

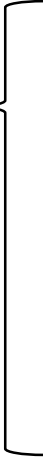
概要

- 2020年1月1日施行済み
- 2020年7月1日当局による執行開始

- CCPA規則は2020年8月14日に発効
 - CCPA規則では通知とプライバシーポリシーを別のものとして規定している

- 2020年11月4日CCPAを改定するCPRA : The California Privacy Rights Act of 2020が成立した
 - CPRAでは個人データの想定する保存期間についても通知項目に含むよう規定している

CCPA規則の構成

- Article 1. GENERAL PROVISIONS
 - **Article 2. NOTICES TO CONSUMERS** —————
 - Article 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS
 - Article 4. VERIFICATION OF REQUESTS
 - Article 5. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE
 - Article 6. NON-DISCRIMINATION
- 
- § 999.304. Overview of Required Notices
 - § 999.305. Notice at Collection of Personal Information
 - § 999.306. Notice of Right to Opt-Out of Sale of Personal Information
 - § 999.307. Notice of Financial Incentive
 - § 999.308. Privacy Policy

CCPA規則では以下 3 つの場合において、プライバシーポリシーの作成・開示とは別に消費者への通知を義務づけている。

プライバシーポリシーとは別に消費者への通知が必要な場合

1. 個人情報の収集に関する消費者への通知
2. オプトアウト権に関する消費者への通知
3. 金銭的インセンティブに関する消費者への通知

CCPA規則で定められている通知を行う際のルール
(規則999.305(a)(2))

- 専門用語を避けた、簡潔でわかりやすい表現を用いる。
- 小さな画面でも読みやすく、目立つ形式を使用する。
- 事業者がカリフォルニア州での事業において通常用いている言語を使用。
- 障害のある消費者も合理的にアクセスできるようにする。

1. 個人情報の収集に関する消費者への通知

#	通知タイミング	通知内容	通知方法
1	個人情報を収集するとき	<ul style="list-style-type: none"> 収集する個人情報の種類一覧 個人情報の種類ごとの、事業上または商業上の利用目的 オプトアウトページのリンク（オフラインの場合はURLの記載） プライバシーポリシーのリンク（オフラインの場合はURLの記載） 	<ul style="list-style-type: none"> オンラインで収集する場合：ウェブサイトのトップページと個人情報を収集するすべてのページで、通知へのリンクを提供する。 アプリで収集する場合：アプリのダウンロードページとアプリ内の設定メニュー等で、通知へのリンクを提供する。 オフラインで収集する場合：収集するフォームや紙で通知する。もしくは、オンライン上の通知場所を案内する。 電話または対面で収集する場合：口頭で通知することも可能である。
2	消費者が想定しない目的で消費者のデバイスから個人情報を収集しようとするとき	<ul style="list-style-type: none"> 収集する個人情報の種類 収集時の通知へのリンク 	収集される個人情報の種類一覧とプライバシーポリシーのリンクを含む通知を即時に提供する。 （例：ポップアップ通知）
3	収集時に通知したもの以外の個人情報を追加で収集するとき	収集する個人情報の種類	追加で収集する個人情報の種類を示す新しい通知を提供する。
4	個人情報を収集する際に消費者に通知したものと、実質的に異なる目的で個人情報を利用するとき	目的外利用	新しい利用目的を消費者に直接通知し、消費者から明示的な同意を得る。
5	雇用関連情報を収集するとき	オプトアウトページとプライバシーポリシーのリンクまたはウェブアドレス（2021年1月1日より有効）	“Do Not Sell My Personal Information” または “Do Not Sell My Info” というタイトルのリンクまたはウェブページのアドレスと、プライバシーポリシーのリンクまたはウェブアドレスを提供する。

CCPAで規定される個人情報の種類（カテゴリ）

- A. 識別子。例えば、実名、別名、郵便住所、一意個人識別子、オンライン識別子であるIPアドレス、Eメールアドレス、アカウント・ネーム、社会保険番号、運転免許証番号、旅券番号、その他の類似の識別子
- B. CA州民法1798.80(e)に規定されるCA州個人情報のカテゴリ（当該個人の名前、サイン、社会保険番号、身体的特徴若しくは記述、住所、電話番号、旅券番号、運転免許証番号、州の識別カード番号、保険証券番号、学歴、雇用、雇用履歴、銀行口座番号、クレジットカード番号、デビットカード番号、その他の財務情報、医療情報、健康保険情報）
- C. CA州法又は連邦法の下で保護された分類の特性
- D. 商業的情報。個人の財産の記録、購入、取得、検討した製品又はサービスの記録、その他の購入又は消費の履歴又は傾向についての記録を含む。
- E. バイオメトリック情報。フェイスプリント、マニキュア・テンプレート（特徴点登録情報）、声紋のような識別テンプレートを抽出できる虹彩、網膜、指紋、顔、手、手のひら、血管パターン及び音声録音の像並びに識別情報を含むタイピング・パターン若しくはリズム、歩行パターン若しくはリズム、睡眠、健康、又は運動データが含まれる。
- F. インターネット又はその他の電子的なネットワーク活動の情報。閲覧履歴、検索履歴、インターネット・ウェブサイト、アプリケーション又は広告との居住者のやりとりの情報を含む。
- G. 地理位置データ
- H. 音声、電子、視覚、温度、嗅覚又は類似の情報
- I. 職業又は雇用に関する情報
- J. 家族教育権とプライバシー法 20 U.S.C. section 1232g, 34 C.F.R. Part 99 に定める公に利用可能な個人識別情報でないと定義される教育上の情報
- K. 居住者についての選好、性格、心理的傾向、性質、行動、態度、インテリジェンス、能力及び素質を反映する居住者のプロフィールを作成するために上記で特定された情報から引き出された推定

2. オプトアウト権に関する消費者への通知

通知タイミング	通知内容	通知方法
常時	<ul style="list-style-type: none"> 個人情報の売却に対する消費者のオプトアウト権の説明 消費者がオンラインでオプトアウト要求を提出できるインタラクティブフォーム（事業者がWebサイトを運営していない場合は、消費者がオフラインでオプトアウトのリクエストをする方法） 消費者がオンラインでオプトアウト要求を提出できるその他の方法の案内 	<ul style="list-style-type: none"> 消費者の個人情報を販売する事業者のウェブサイトのトップページと個人情報を収集する全てのページで通知する。 ウェブサイトのホームページにある“Do Not Sell My Personal Information” または “Do Not Sell My Info” というリンクをクリックして誘導されるウェブページや、アプリのダウンロードページ等で通知する。モバイルアプリケーションを介して個人情報を収集する企業は、アプリケーションの設定メニューなどを通じて、アプリケーション内に通知リンクを設置する。通知リンクの代わりに、通知内容を含むプライバシーポリシーのセクションへのリンクを設置することもできる。 消費者とオフラインで関わる事業者は、オプトアウト権をオフラインで通知する。（例：個人情報を収集する紙のフォームに通知内容を印刷する/通知書を消費者に提供する/オンライン通知への案内を表記する） ウェブサイトを運営していない事業者は、消費者にオプトアウト権を通知する別の方法を確立し、文書化し、遵守する。

3. 金銭的インセンティブに関する消費者への通知

通知タイミング	通知内容	通知方法
<p>消費者が金銭的インセンティブを選択するか決めるとき</p>	<ul style="list-style-type: none"> 当該金銭的インセンティブまたは差異に関する簡潔な概要 当該金銭的インセンティブまたは差異に関する重要な条件の説明 消費者が当該金銭的インセンティブまたは差異に参加する（オプトイン）方法 当該金銭的インセンティブから消費者は、いつでも脱退する権利を有すること、および当該権利の行使方法に関する記載 当該金銭的インセンティブまたは差異が消費者データの価値にどのように合理的に関連しているかの説明（当該金銭的インセンティブまたは差異を提供する根拠となる消費者データの価値の公正な評価および消費者データの価値を算出する方法の説明を含む） 	<p>事業者が金銭的インセンティブをオンラインで提供する場合、プライバシーポリシーの該当セクションへアクセスするためのリンクを通知する。</p>

CCPAに準拠した「個人情報の収集に伴う通知」の例

Los Angeles Times

Los Angeles Timesのウェブサイトトップページ

Copyright © 2020, Los Angeles Times

[Terms of Service](#)

[Privacy Policy](#)

[CA Notice of Collection](#)

[Do Not Sell My Info](#)

ホームページ最下部に利用規約、プライバシーポリシー、CCPA通知、オプトアウトのリンクを分けて記載している

Los Angeles Times PRIVACY POLICY

16.2

California Notice of Collection

プライバシーポリシーのCCPAに関するセクションに遷移する

Do Not Sell My Info

California residents may opt out of the "sale" of their personal information. We sell certain of your information to third parties to provide you with offers and promotions and opportunities that may be of interest to you.

Under the CCPA, sale is defined such that it may include allowing third parties to receive certain information, such as cookies, IP address, and/or browsing behavior, to deliver targeted advertising on the Services or other services. Advertising, including targeted advertising, enables us to provide you certain content for free and allows us to provide you offers relevant to you.

Depending on what Services you use, we may provide the following categories of personal information to third parties for these purposes:

- For online targeted advertising purposes: demographic and statistical information, user-generated content, device information and identifiers, browser and usage data, geolocation, and social media information.
- For sharing with third parties to send you relevant offers, products, promotions and opportunities: contact and registration information, demographic and statistical information, employment and education data, user-generated content, device information and identifiers, and geolocation.

オプトアウト権とメールでオプトアウト要求をする方法について記載している

If you would like to opt out of our use of your information for such purposes that are considered a "sale" under California law, you may do so as outlined on the following page: [Do Not Sell My Info](#). You can also submit a sale opt-out request by emailing us at privacy@latimes.com. Please note that we do not knowingly sell the personal information of minors under 16 years of age without legally-required affirmative authorization.



Los Angeles Times

Notice of Right to Opt-Out

[Opting out of Personalized Advertising](#)

[Opt-Out Tools](#)

Opt-Out Tools

To unsubscribe from Los Angeles Times marketing messages, you can adjust your settings here: <https://membership.latimes.com/settings>.

If you are a California resident, to opt out of the sale of your personal information (and as a result, opt out of personalized advertising), **you must utilize the following toggle (and all 3 tools below)**.

Do Not Sell My Info



ワンクリックでオプトアウトができるようになっている

Save

CCPAに準拠した「個人情報の収集に伴う通知」の例

Miller Toyota of Anaheim (カリフォルニア州で営業するトヨタ自動車のディーラー)

Miller Toyota of Anaheim – Notice at Collection of Private Information

Miller Toyota of Anaheim (“Dealership,” “we,” “us” or “our”) respects the privacy of the information our customers entrust to us. This Notice at Collection applies to both the online and offline collection of information. We share personal information unless you instruct us not to do so by submitting a request a [\(click here\)](#) or by calling 833-220-8200. For more information regarding our privacy practices and consumer rights under the California Consumer Privacy Act, view our Privacy Policy also at [\(click here\)](#).

Categories of personal information we collect from you	The business or commercial purpose(s) for which it will be used:
Identifiers , such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver’s license number, state identification number, military identification number or passport number)	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; complete government forms; confirm your identity and that you are at least 18 years old; and/or confirm you are licensed to drive our vehicles or take delivery of a vehicle you have purchased or leased from us
Other personal information described in Civil Code Section 1798.80(e) , such as: Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information; and/or your signature	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; confirm your insurance coverage; confirm your identity; obtain authorization to collect payment from you; collect payment from you; confirm acknowledgement of receipt of documents
Physical descriptions A photo reveals Driver’s license/state identification card - includes your image, date of birth, physical description and gender Permanent resident card - includes your image, date and place of birth; Social security card - includes your social security number Passport - includes your image, date and place of birth and your nationality Military ID - includes your image and rank Completion of a Translated Contract Acknowledgement or signing of translated documents reveals your primary language	To complete government forms
Commercial information from selling/providing products or services to you , such as: Information, including vehicle information and ownership information, regarding a transaction in which we sell or lease a	To process your transactions; appraise your current vehicle; send you informational and marketing communications; retain records of transactions as required by law; fulfill the terms of a written warranty or product recall; to process warranty, insurance or service contract claims;

オプトアウトのリンク

プライバシーポリシーへのリンク

収集する個人情報の種類 (カテゴリ) の一覧

個人情報の種類ごとの、事業上または商業上の利用目的

CCPAに準拠した「プライバシーポリシー」の例

Miller Toyota of Anaheim (カリフォルニア州で営業するトヨタ自動車のディーラー)

Privacy Policy – Miller Toyota of Anaheim

Effective Date: 1/1/2020

Miller Toyota of Anaheim (“Dealership,” “we,” “us” or “our”) respect the privacy of the information you have entrusted to us. This Privacy Policy (“Policy”) applies to both the online and offline collection of personal information by the Dealership. By using our website and services (collectively, the “Services”), you acknowledge you have read and understand the terms and conditions of this Policy. If you do not agree to the terms and conditions of this Policy, please do not use our Services.

PLEASE NOTE THE ARBITRATION PROVISION SET FORTH BELOW, WHICH MAY, EXCEPT WHERE AND TO THE EXTENT PROHIBITED BY LAW, REQUIRE YOU TO ARBITRATE ANY CLAIMS YOU MAY HAVE AGAINST DEALERSHIP ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE, THE RIGHT FOR A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY.

INFORMATION COLLECTED

Click [here](#) for our Notice at Collection of Personal Information, which lists the categories of personal information we collect from consumers and the purposes for collecting the information.

Below is a chart regarding the personal information we have collected about consumers during the last 12 months:

Category of personal data	Source(s)	Purpose(s)	Disclosure to third parties
Identifiers, such as:	<ul style="list-style-type: none">Directly from consumers	<ul style="list-style-type: none">To respond to consumers' requests and inquiries	<ul style="list-style-type: none">Disclosure for business purposes to internet service providers, analytics providers, payment processors and warranty, insurance or service contract administrators, if applicable to transaction

個人情報の収集に伴う通知のリンク

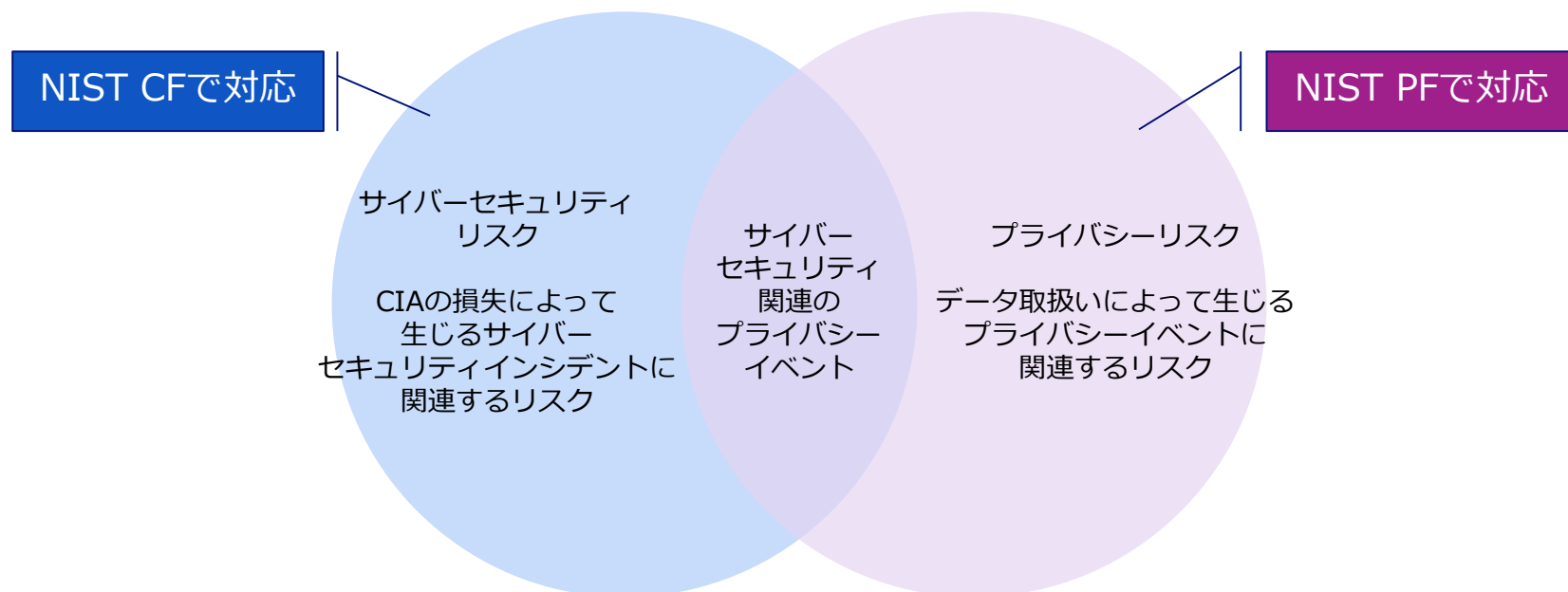
NIST[※] Privacy Framework

※ NIST : National Institute of Standards and Technology (米国国立標準技術研究所)

概要 (1/2)

- NIST Privacy Framework (以下、NIST PF) は組織が個人のプライバシー保護を実現する上で参考にすべきフレームワークとして、米国国立標準技術研究所によって2020年1月にv.1.0が発行された。
 - GDPRやCCPA等の法規とは異なり、強制力を持つものではない。
 - またISO認証規格 (ISMS等) のように基準を示すものではない。
- セキュリティ分野におけるNIST Cybersecurity Framework (以下、NIST CF) の姉妹版という位置づけであり、本フレームワーク自体もNIST CFの構造に準拠して作成されている。
 - NIST CFは2014年に発行、その後わずか2年で、グローバルで35%の企業に採用されるなど、非常に重要視されている。

サイバーセキュリティリスクとプライバシーリスクの関係

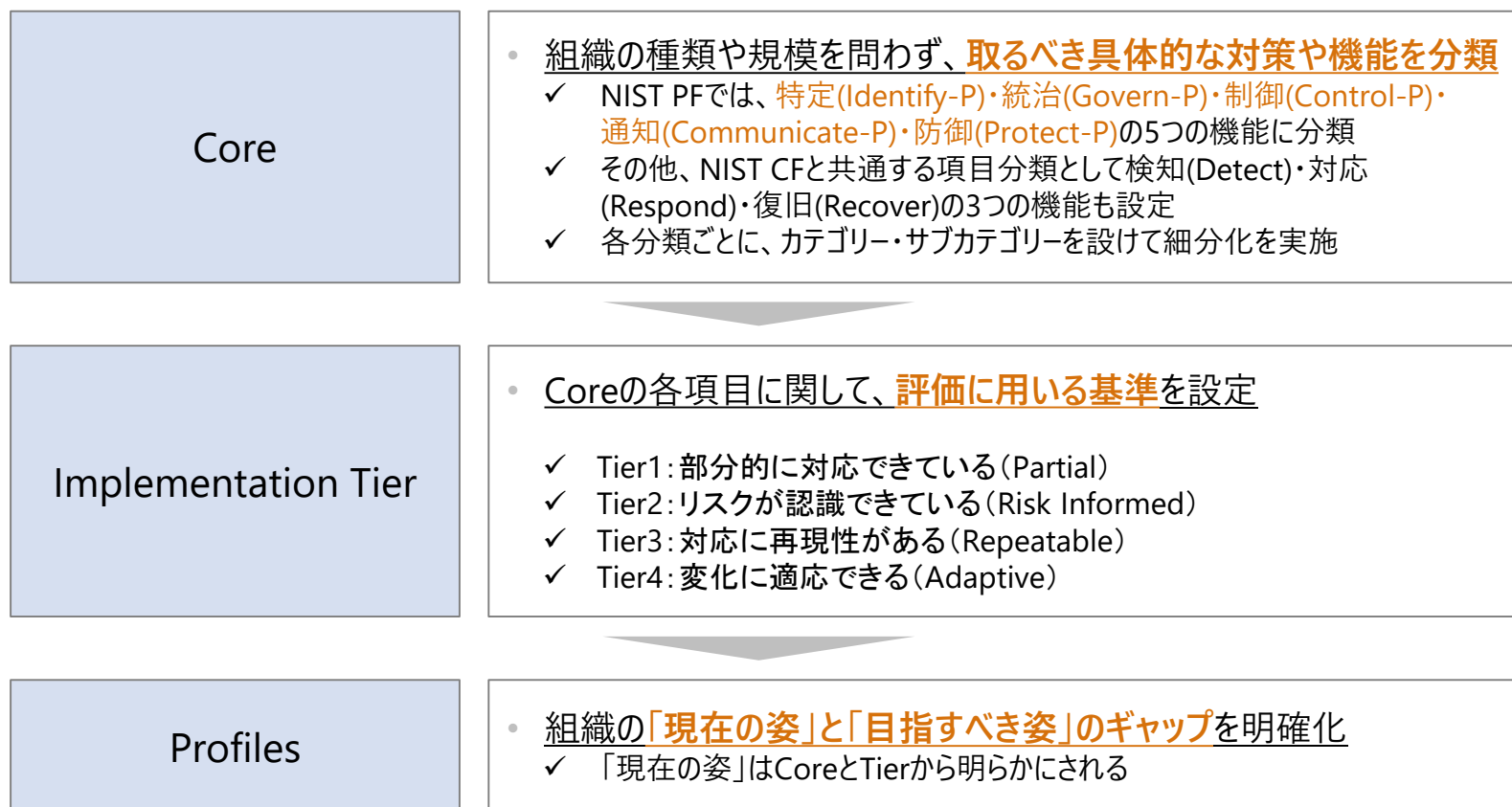


概要 (2/2)

■ NIST PFはCore、Implementation Tier、Profilesの3階層で構成されている。

- 構成や各要素の名称は、先立って作成されたNIST CFを踏襲している。
- 特にTier、Profileの内容はNIST CFと同様である。

各階層の説明



NIST PFでは「Communicate-P」において消費者とやり取りする際に留意すべき点について言及しているが、通知・同意に関する具体的な取り組み方までは示していない。

NIST PFにおいて示されるCore

(プライバシー保護に関して組織の種類や規模を問わず、取るべき具体的な対策や機能)

「Communicate-P」のカテゴリ

(具体的な対策や機能の内訳)

具体的な“機能”	内容
Identify-P (特定)	組織が行っているデータ取扱いに対する理解を深める
Govern-P (統治)	組織のガバナンス構造を構築する
Control-P (制御)	データの取扱いが適切かどうか確認する
Communicate-P (対話)	データ取扱いについて消費者やステークホルダーと対話できる体制を整える
Protect-P (保護)	データの取扱いプロセスを適切に保護する
Detect (検知)	異常を“検知”したり、継続して監視する ⇒NIST Cybersecurity Frameworkで対応
Respond (対応)	分析や改善の方法を構築する ⇒NIST Cybersecurity Frameworkで対応
Recover (復旧)	情報の復旧や、システムエラーからの復旧をする ⇒NIST Cybersecurity Frameworkで対応

コミュニケーションの方針、プロセス、および手順

- 透明性に関するポリシー、プロセス、手順を確立し、導入している
- 役割と責任（広報など）を確立している

データ処理意識

- 個人のデータ処理についての希望や要求に対応するためのメカニズム（通知、内部レポートまたは公開レポートなど）を確立し、導入している
- 個人からフィードバックを得るためのメカニズムを確立し、導入している。
- プライバシー侵害またはイベントの影響を受ける個人や組織には、これらを通知している。

…など

また、NIST CFとNIST PFをシームレスに統合した最新の文書として、SP800-53 Revision5が2020年9月に提示された。

SP800-53 Revision5の目次

- CHAPTER ONE INTRODUCTION
- CHAPTER TWO THE FUNDAMENTALS
- **CHAPTER THREE THE CONTROLS**

- 3.1 ACCESS CONTROL
- 3.2 AWARENESS AND TRAINING
- 3.3 AUDIT AND ACCOUNTABILITY
- 3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING
- 3.5 CONFIGURATION MANAGEMENT
- 3.6 CONTINGENCY PLANNING
- 3.7 IDENTIFICATION AND AUTHENTICATION
- 3.8 INCIDENT RESPONSE
- 3.9 MAINTENANCE
- 3.10 MEDIA PROTECTION
- 3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION
- 3.12 PLANNING
- 3.13 PROGRAM MANAGEMENT
- 3.14 PERSONNEL SECURITY
- **3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY**
- 3.16 RISK ASSESSMENT
- 3.17 SYSTEM AND SERVICES ACQUISITION
- 3.18 SYSTEM AND COMMUNICATIONS PROTECTION
- 3.19 SYSTEM AND INFORMATION INTEGRITY
- 3.20 SUPPLY CHAIN RISK MANAGEMENT

SP800-53 Revision5において示される同意取得を行う際の留意事項（1 / 2）

CHAPTER3 「個人識別可能な情報処理と分散性」>「 CONSENT」

■ 管理：

- 個人のインフォームド・ディシジョン（＝患者が主体的に意思決定して選択を行うこと）を促進するために、個人が個人情報を収集する前に、個人が個人情報の処理に同意するためのツールまたはメカニズムを実装する。

■ 議論：

- 同意を得ることにより、個人は情報の処理に関する意思決定に参加することができ、また、個人を特定できる情報の処理に起因するリスクの一部を組織から個人に移すことができる。
- 同意は、適用される法律、規制、方針、基準、またはガイドラインによって要求される場合がある。そうでない場合は、同意をコントロールとして選択する際に、組織は、個人がその承認から生じるプライバシーリスクを理解し、受け入れることが合理的に期待できるかどうかを検討する。
- 組織は、他の管理策が、単独で、または同意と組み合わせて、より効果的にプライバシーリスクを軽減できるかどうかを検討する。
- また、組織は、システムや組織が行う処理に関して個人の理解や行動に影響を与える可能性のある人口統計学的または文脈的な要因も考慮する。
- 個人から同意を求める場合、組織は、同意の種類（オプトイン、オプトアウトなど）、個人を適切に認証して身元を証明する方法、電子的な手段で同意を得る方法など、同意を得るための適切なメカニズムを検討する。
- さらに、組織は、同意が提供された後、個人が同意を取り消すためのメカニズムを提供することを、適切な場合には検討する。
- 最後に、組織は、個人が同意を提供する際に受け入れられるリスクを理解できるように、平易な言葉を使用したり、専門用語を避けるなど、使いやすさの要素を考慮する。

SP800-53 Revision5において示される同意取得を行う際の留意事項（2 / 2）

CHAPTER3 「個人識別可能な情報処理と分散性」>「 CONSENT」

【管理を強化する手法】：

(1) TAILORED CONSENT：

- 個人が個人情報の要素をどのように処理するかを選択できるようにする。
- 同意をよりカスタマイズすることで、プライバシーリスクを低減し、個人の満足度を高め、製品やサービスの放棄などの不利益な行動を回避することができる場合がある。

(2) ジャストインタイムの同意：

- 組織が定義した同意の仕組みを、定義した頻度で、個人情報の処理に合わせて、個人に提示する。
- ジャストインタイムの同意は、個人にとって最も有用と思われる時点において、または特定の種類のデータ処理に関連して、個人情報がどのように処理されているか確認することを可能にする。
- 個人が最後に同意してから時間が経過している場合や処理の種類によっては、同意内容に対する認識が低下する可能性がある。組織はジャストインタイムの同意の設計にあたり、個人のプライバシーに対する関心や懸念をより深く知り、人口統計、フォーカスグループ、または調査に関する裏付けとなる情報を使用することがある。

(3) 撤回：

- 個人が個人情報の処理に対する同意を撤回できるように、組織が定義したツールまたはメカニズムを実装する。
- 同意の撤回は、状況が変化した場合に、個人が最初の同意の決定をコントロールすることを可能にする。
- 組織は、使いやすい撤回機能を可能にするために、ユーザビリティの要素を考慮する。

SP800-53 Revision5において示される通知を行う際の留意事項（1 / 3）

CHAPTER3 「個人識別可能な情報処理と分散性」>「PRIVACY NOTICE」

■ 管理：個人情報の処理について、個人への通知を行う。

- a. 個人が最初に組織と接触したとき、そしてその後、組織が定義した頻度で通知すること。
- b. 個人情報について平易な言語で、明確かつ分かりやすく表現していること。
- c. 個人情報の処理を許可する権限を識別すること。
- d. 個人情報が処理される目的を特定すること。
- e. 組織で定義された情報を含むこと。

■ 議論：

- 通知は個人情報システムや組織によってどのように処理されているか、個人に知らせるのに役立つ。
- 法律、規則、または方針によっては、通知に特定の要素を含むことや特定の形式で提供されることが要求される場合がある。
- 連邦政府機関の職員は、いつ、どこで、どのような形で通知を提供するか、また、通知に含めるべき要素や要求される形式について、プライバシーに関する上級機関の職員や法律顧問に相談する。
- プライバシーリスク評価は、個人情報の処理に関連するプライバシーリスクを特定し、そのようなリスクを管理するために、組織がプライバシー通知に含めるべき適切な要素を決定するのに役立つ場合がある。
- 自分の情報がどのように処理されているかを個人が理解できるように、組織は分かりやすい言葉で説明し、専門用語を避ける。

SP800-53 Revision5において示される通知を行う際の留意事項（2 / 3）

CHAPTER3 「個人識別可能な情報処理と分散性」>「PRIVACY NOTICE」

【管理を強化する手法】：

(1) ジャストインタイムの通知：

- 個人情報を提供する時に、またはデータアクションに関連して、個人情報の処理を行うことを個人に通知する。
- ジャストインタイムの通知は、そのような通知が個人にとって最も有用であると思われるタイミングに、組織が個人情報をどのように処理するかを通知するものである。
- 組織が最後に通知を提示してから時間が経過した場合や、個人が最後に通知を受けた状況から変化した場合には、個人情報がどのように処理されるかについての個人の想定は、正確または信頼性の高いものではない可能性がある。
- ジャストインタイムの通知は、個人のプライバシーリスクを高める可能性があるとして組織が判断したデータ操作を説明することができる。
- 組織は、特定のデータアクションが発生した際に、それが発生した時点で通知内容を更新したり、個人に思い出させたり、最後に通知を提示した後に発生した特定の変更を強調したりするために、ジャストインタイムの通知を使用することができる。
- ジャストインタイムの通知は、同意が拒否された場合に何が起るかを説明するために、ジャストインタイムの同意と組み合わせて使用することができる。
- 組織は、いつジャストインタイムの通知を使用するかを判断し、ユーザーのプライバシーへの関心や懸念を知るために、ユーザーの人口統計、フォーカスグループ、または調査に関する裏付け情報を使用することができる。

SP800-53 Revision5において示される通知を行う際の留意事項（3 / 3）

CHAPTER3 「個人識別可能な情報処理と分散性」>「PRIVACY NOTICE」

【管理を強化する手法】：

(2) 米国プライバシー法※に関する声明（PRIVACY ACT STATEMENTS）：

- 声明は、情報の提供が強制的か任意か、情報が使用される主な目的、情報が対象となる公表された日常的な使用、要求された情報の全部または一部を提供しない場合の個人への影響、および適切な引用と関連する記録通知システムへのリンクを、個人に正式に通知するものである。
- 連邦政府機関の職員は、声明の規定について、プライバシーに関する上級機関職員および法律顧問に相談する

※ 1974 年米国プライバシー法

Privacy Act (P.L. 93-579), December 1974. (<https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>)

プライバシーに関する重要な要素として、「プライバシー影響評価」への言及も見られた。

CHAPTER3 「リスク評価」>「PRIVACY IMPACT ASSESSMENTS」

■ 管理：システム、プログラム、またはその他の活動について、事前にプライバシー影響評価を実施する。

- a. 個人を特定できる情報を処理する情報技術を開発または調達すること。
- b. 個人を特定できる情報の新たな収集を開始すること。
 1. 情報技術を使用して処理されること。
 2. 連邦政府の機関または職員以外の10人以上の個人に対して同一の質問がなされた場合、または同一の報告要件が課された場合には、特定の個人に連絡を取ること。

■ 議論：

- プライバシー影響評価とは、**個人を特定できる情報がどのように取り扱われているかを分析し、その取り扱いが適用されるプライバシー要求事項に適合していることを確認し、情報システムや活動に関連するプライバシーリスクを決定し、プライバシーリスクを軽減する方法を評価すること**である。プライバシー影響評価は、**分析であると同時に、分析のプロセスと結果を詳細に記述した正式な文書**でもある。
- 組織は、組織がプライバシーを十分に考慮し、組織の活動の初期段階から情報のライフサイクル全体を通じて適切なプライバシー保護を取り入れたことを実証するために、十分な明確さと具体性をもってプライバシー影響評価を実施し、開発する。
- 有意義なプライバシー影響評価を実施するためには、組織のプライバシー担当上級機関職員が、プログラム管理者、システム所有者、情報技術の専門家、セキュリティ担当者、顧問、その他の関連する組織職員と密接に連携して作業を行う。
- プライバシー影響評価は、情報システムや個人を特定できる情報のライフサイクルの、特定のマイルストーンや段階に限定された**時間制限のある活動ではない**。むしろ、プライバシー分析は、**システムや個人を特定できる情報のライフサイクル全体を通して継続される**。したがって、プライバシー影響評価は、情報技術の変更、組織の慣行の変更、またはその他の要因により、そのような情報技術の使用に関連する**プライバシーリスクが変更されるたびに、組織が更新する生きた文書**である。
- プライバシー影響評価を実施するために、組織は、セキュリティおよびプライバシーリスク評価を使用することができる。
- 組織は、プライバシー閾値分析など、異なる名称を持つ他の関連プロセスを使用することもできる。
- プライバシー影響評価は、**組織のプライバシーに関する慣行に係る一般の人々への通知としても機能**する。
- プライバシー影響評価の実施および公表は法律で義務付けられている場合もあるが、適用法がない場合には、組織はそのような方針を策定する場合もある。
 - 連邦政府機関の場合、プライバシー影響評価は[EGOV]によって要求される場合がある。この要求については、プライバシーおよび法律顧問の上級機関職員に相談し、この規定に関連する法令上の例外および OMB のガイダンスに注意する必要がある。

※[EGOV]：Eガバメント法、E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
(<https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf>)

ISO/IEC 29184:2020 Online privacy notices and consent

概要

- ISO : the International Organization for Standardizationの略。各国の標準化団体の世界的な連合
- 『Information technology — Online privacy notices and consent』（オンライン・プライバシー通知と同意）
 - 2014年10月に経済産業省が公表した「消費者向けオンラインサービスにおける 通知と同意・選択に関するガイドライン」をベースとした日本提案の規格案※1で、2020年6月に出版
 - GDPRなどでも言及された同意取得の「高いハードル」を具体的に要件定義し、要件を満たすために必要なアクションを説明
- ISO/IEC 29184の内容※2 :
 - いわゆる「プライバシー・ポリシー」である「プライバシー・ノティス（通知）」に何を書くべきか、
 - 同意を取得するには何をすべきか
 - データの取扱を変更するときには何をすべきか
- ISOでは、より具体的な内容として、同意の証跡（Consent Receipt or Consent Record）に言及しているのも特徴的である

※1：出所) https://www.ppc.go.jp/files/pdf/280426_giziroku.pdf

※2：出所) <https://gihyo.jp/lifestyle/column/newyear/2020/privacy-standards>

『ISO/IEC 29184 オンライン・プライバシー通知と同意』の構成

- Foreword / Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Symbols and abbreviated terms
- 5 General requirements and recommendations
 - 5.1 Overall objective
 - **5.2 Notice**
 - 5.2.1 General
 - 5.2.2 Providing notice obligation
 - 5.2.3 Appropriate expression
 - 5.2.4 Multi-lingual notice
 - 5.2.5 Appropriate timing
 - 5.2.6 Appropriate locations
 - 5.2.7 Appropriate form
 - 5.2.8 Ongoing reference
 - 5.2.9 Accessibility
 - 5.3 Contents of notice
 - **5.4 Consent**
 - 5.4.1 General
 - 5.4.2 Identification of whether consent is appropriate
 - 5.4.3 Informed and freely given consent .
 - 5.4.4 Providing the information about which account the PII principal is using
 - 5.4.5 Independence from other consent
 - 5.4.6 Separate consent to necessary and optional elements of PII
 - 5.4.7 Frequency
 - 5.4.8 Timeliness
 - 5.5 5.5 Change of conditions.
- Annex A : User Interface example for obtaining the consent of a PII principal on PCs and smartphones
- **Annex B : Example of a Consent Receipt or Consent Record ('Note', Clause 5.4.3) .**

通知におけるポイントとして、ISOでは下記の点が記載されている。

- 前提：通知により「データ主体が情報処理の影響や重大性、処理の意図を理解して行動できる」ことが目標である
- 通知に関して求められる主要な要素
 - ① 通知の義務：通知が必要な状況では、いつでも要件を満たした通知をデータ主体に提供する
 - ② 適切な表現：対象にとって明確で理解しやすい方法で提供する
 - ③ 多言語対応：対象の主体に合わせた言語で通知を提供する
 - ④ 適切なタイミング：活動がデータ主体の利益に関連する場合、いつ通知をするべきかを決め、文章で明示する
 - ⑤ 適切な場所：オンラインでの場合も含め、容易に通知を見つけてアクセスできるようにする
 - ⑥ **適切な形態：どのように提供し、アクセスできるようにするかを決定する**
 - ⑦ 継続的な参照：同意した際の通知の最新版などが容易に参照できるよう保管する
 - ⑧ アクセシビリティ：オンラインサービスの技術に適した、主体がアクセス可能な方法で通知を提供する

通知同様、同意におけるポイントとして、ISOでは下記の点が記載されている。

- 同意は「公正で、実証可能で、透明性があり、曖昧さがなく、取消可能（撤回可能）な方法」が必要である
- 同意に関して求められる主要な要素
 - ① 同意の適切さの識別：同意または明示的な同意※1が適切な状況かを特定した上で同意を求める
 - ② 情報提供された自由な同意：
 - 主体が強制や強要を受けず、意図的な行為（チェックボックスのクリックなど）で得られた同意である
 - 十分な情報が提供され、同意の変更や撤回が、同意を与えるのと同じように簡単に行うことができる
 - ③ 対象アカウントの明示：アカウントに関連した同意を収集するときは、どのアカウントに関する内容かを明示する
 - ④ 他の同意からの独立性：プライバシーに関する同意は、他の事項に関する同意と明確に区別して取得する
 - ⑤ 必須/任意の個別同意：必須要素と任意要素が明確に認識され、それぞれについて同意を提供できる仕組みとする
 - ⑥ 適切な間隔：主体が同意疲れを起こさないように、適切な間隔で、既存の同意の確認、もしくは新規の同意取得を行う
 - ⑦ 適時性：適切なタイミングでの同意取得が必要であり、あまり早期に同意を求めることは避ける

※1：明示的な同意：機微な情報や、データ主体にネガティブな影響を与えるリスクがある場合は、より厳しい基準で同意を取得する必要がある

特徴的な点として ISOでは、オンライン上での同意の証左としての同意の証跡の活用と、望ましい同意の証跡の内容について言及している。

- 同意の内容について、一般化したフォーマットを例示
- こうしたレシートを生成して個人提供することで、オンライン上の同意に関するデジタル記録の作成に活用できる点にも言及

Consent Receipt	
Version	KI-CR-v1.1.0
Jurisdiction	Discworld
Consent Timestamp	11/13/2017, 12:00:00 PM EST
Collection Method	Web Subscription Form with opt-in for marketing
Consent Receipt ID	c1befd3e-b7e5-4ea6-8688-e9a565aade21
Public Key	04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1: 40:02:cc:31:b6:4a:77:bf:5e:a0:db:4f:ea:d2:07: c4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01: f4:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2: cc:0b:f8:a1:bf
Language	English

①同意受領書のメタデータ

Consent Parties	
Information Subject	
PII Principle ID	Bowden Jeffries
Information Controller	
PII Controller Name	Ankh-Morpork Times
PII Controller Contact	William de Word, Chief Editor & Data Protection Officer
PII Controller Address	Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld
PII Controller Email	william@example.com
PII Controller Phone	(555) 555-DISC (3429)
PII Controller URL	https://example.com/contact
Privacy Notice	https://example.com/privacy_2017

②同意取引の当事者情報

Data, collection and use				
Service	Digital Subscription and News Alerts			
Purposes for collection and use				
Purpose	Purpose Category	Basis for Processing	PII Categories	Primary purpose?
Fulfil Digital Subscription	Provision of services	Performance of contract	<ul style="list-style-type: none"> Technical Demographics Financial Contact 	TRUE
Marketing	Marketing	Consent	<ul style="list-style-type: none"> Demographics Financial Contact 	FALSE
Financial Record Keeping	Fiduciary obligation	Public task	<ul style="list-style-type: none"> Financial 	FALSE
Law Enforcement	Legal obligation	Legal obligation	<ul style="list-style-type: none"> All 	FALSE
Termination	https://example.com/privacy_2017#termination			
Third Party Disclosure	True			
Third Party Processors	<ul style="list-style-type: none"> Print Shop Fulfillment vendor Bank Law enforcement with subpoena Digital Advertising Agency 			
Sensitive PII	Yes			
Sensitive PII Category	Financial Information			

③利用するデータ・利用方法

The text is framed by two decorative swooshes. The top swoosh is a gradient bar transitioning from blue on the left to red on the right. The bottom swoosh is a solid blue bar.

Share the Next Values!