

プライバシー・バイ・デザインに基づく 適正なパーソナルデータの取り扱い

Appropriate Handling of Personal Data based on Privacy-by-Design

八津川 直伸

要 約 法的な位置づけが不明確なパーソナルデータはビッグデータに大量に含まれ、その取扱いが不適切な場合には、事業者の信用失墜や利用者に対するプライバシー侵害といったリスクが懸念される。しかしその対策については未だ確固たるものが存在しない。これらリスクを回避するためにはプライバシー・バイ・デザインに基づく対応が不可欠であり、ビッグデータビジネスを開始している事業者は早急にその対策を講じる必要がある。本稿はその第一歩として、個人情報保護法の改正動向を踏まえて以下を提言する。

- ①事業者が利用者に提示すべき適切なプライバシーポリシーのあり方
- ②プライバシーポリシーの具体例と提示方法

これら具体例の雛型には、本人の承諾なしにパーソナルデータを第三者提供する場合の対処方法を含み、これは今までのプライバシーポリシーにはなかった大きな特徴である。これらの活用によって、利用者の懸念を払拭するのみならず、事業者のプライバシー侵害リスクを回避することが可能となる。

※本稿は、2014年12月末現在の個人情報保護法改正動向に基づき執筆した。

Abstract Large amount of personal data which orientation in law is uncertain is included in the big data. If the handling of them is inappropriate, privacy infringement against user, and disrepute against company are concerned. However, the steadfast countermeasures do not exist yet. In order to avoid these risks, correspondence based on Privacy-by-Design must be necessary. Then, this paper suggests followings for the first step for the correspondence by Privacy-by-Design.

1. The appropriate concept of the privacy policy which should be presented to the user by company.
2. Specific example and presentation method of privacy policy.

The models of this specific example include how to deal with the case when a company provides the personal data to a third party without the consent of the individual user. This is a great feature which was not included in the past privacy policy. By utilizing these examples, it is possible to avoid not only company's privacy infringement risk but individual user's anxiety.

Note: This paper was written based on the current revision trends for Act on the Protection of Personal Information as of the end of December 2014.

1. は じ め に

ビッグデータビジネスにおいては、個人の行動・状態等に関する「パーソナルデータ」^{*1}の利活用が期待されており、2014年6月24日に決定された「パーソナルデータの利活用に関する制度改正大綱」^[1]（以下、制度改正大綱）においても、その基本方針としてプライバシー保護と利活用の両立が示されている。しかし保護すべきパーソナルデータの範囲が曖昧であり、ま

た制度設計の内容も具体性に乏しいため、データの不適切な取扱いによって個人のプライバシーの侵害やそれに伴う企業信用失墜リスク等（以下、プライバシー侵害リスク）が懸念される。制度改正大綱の内容から察するに、2015年1月の通常国会にて成立予定の改正個人情報保護法においても保護範囲の厳密な定義はなされないものと推測される。2014年12月19日開催の第13回パーソナルデータに関する検討会において公表された「個人情報の保護に関する法律の一部を改正する法律案の骨子（案）」^[2]（以下、改正骨子案）においても新たな保護対象について少数の例示があるのみで、プライバシー性が高いといわれる移動履歴（時間、位置情報含む）や購買履歴、Web閲覧履歴等の情報については依然何も述べられていない。そのため、パーソナルデータ取扱い事業者（以下、事業者）はデータの利活用について、また事業者のサービスを利用する者（以下、利用者）は自身のパーソナルデータを提供することについて、いずれも消極的になる可能性がある。しかしその一方で、各業界ではこれら懸念を抱えながらも、プライバシー侵害リスクへの対応を放置したままパーソナルデータを取扱うビジネスが始まっている。

このような状況に鑑み本稿では、2章で事業者によるパーソナルデータ収集の実態とその取扱いリスクについて述べ、3章で個人情報保護法改正の動向を解説、そして具体性に欠ける制度改正大綱や改正骨子案（以下、制度改正大綱等）の主旨を踏まえつつ、リスク対処を考慮したパーソナルデータの第三者提供スキームを検討する。続いて4章では、事業者が取り組むべき対応としてプライバシー・バイ・デザイン^{*2}の考え方を述べ、そしてその取り組みへの第一歩として5章で、プライバシー侵害リスク回避に向けた利用者への配慮、透明性確保のために必要な事業者が備えるべき適切なプライバシーポリシーのあり方と具体例、ならびにそれらの利用者への提示方法について提言する。

2. パーソナルデータ取扱い上のリスク

本章ではまず、事業者によるパーソナルデータ収集の実態とその取扱いリスクについて述べる。

2.1 パーソナルデータとは

パーソナルデータとは、個人情報保護法に定める「個人情報」に限定されず、広く「個人に関する情報」とされ、例えばスマートデバイスを活用したモバイルネットワーク環境では既に大量のパーソナルデータが収集されている実態がある（図1）。

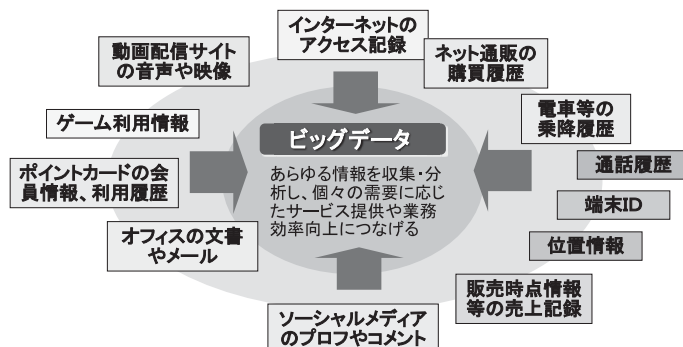


図1 ビッグデータに含まれる様々なプライバシーに係る情報

収集されるパーソナルデータは、主に表1に例示するものだが、これらは直接個人を特定するものではないので現行の個人情報保護法範囲外のグレーゾーンのデータと呼ばれ、利用者がほぼ無意識の間に収集される。

表1 収集されるパーソナルデータの例

区分	情報の種類	含まれる情報
利用者の識別に係る情報	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じて一時的に PC に書込み記載されたデータ（クッキー等）
	契約者・端末固有 ID	OS が生成する ID（Android ID）、独自端末識別番号（UDID）、加入者識別 ID（IMSI）、端末識別 ID（IMEI）、MAC アドレス等
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS 機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォン等で撮影された写真、動画

総務省の“スマートフォン プライバシー イニシアティブ (2012 年 8 月)”^[3]より一部抜粋して作成

パーソナルデータ収集に係る利害関係者（パーソナルデータ取扱い事業者）には図2のように、(1)アプリ提供者、(2)情報収集モジュール提供者、(3)ネットサービス提供者、(4)第三者サービス提供者などがあり、これらは互いに共存しながらビジネスを構成している（表2）。

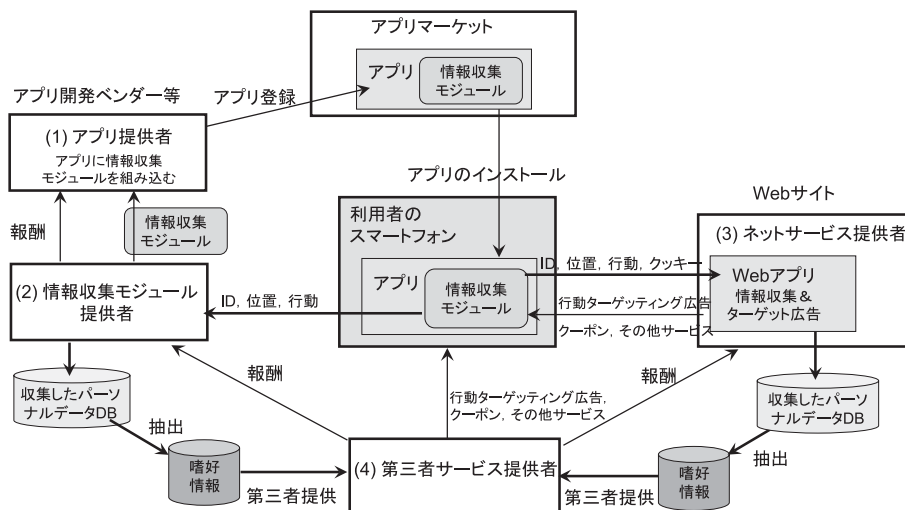


図2 パーソナルデータを取扱う利害関係者

表2 パーソナルデータを取扱う利害関係者の説明

(1)	アプリケーション提供者	アプリを開発しアプリマーケット等でアプリの提供を行う者である。通常アプリはスマートデバイスから取得したパーソナルデータをアプリ自身のサービスのために用いる。また情報収集モジュールを組み込み、収集したパーソナルデータを情報収集モジュール提供者に提供し、その見返りとして報酬を受け取る。特に無料アプリにおいてこの傾向が強い。
(2)	情報収集モジュール提供者	アプリ提供者に情報収集モジュールを提供し、アプリ内に情報収集モジュールを組み込んでもらうことによって、スマートデバイスで取得したパーソナルデータを直接情報収集モジュール提供者が受け取る。収集したパーソナルデータからデータベース等を構築し、それらを解析することにより有用情報を抽出し、それらを第三者サービス提供者に転売し報酬を得る。
(3)	ネットサービス提供者	ネットを通じた Web サイトで各種サービスを提供する者である。スマートデバイスから Web サイトにアクセスがあった際にパーソナルデータを取得し、それを自身の Web サービスのために用いる。また (2) の者と同様にデータベースを構築し、そこから得られた有用情報を活用してスマートデバイス利用者にリーチターゲット広告を出す、あるいはクーポン提供などの利用者指向サービスを提供する。また、有用情報そのものを第三者サービス提供者に転売することもある。
(4)	第三者サービス提供者	(2)または(3)の者より、パーソナルデータそのものあるいはそれらから抽出された有用情報を入手し、それに基づきスマートデバイス利用者にリーチターゲット広告を出し、あるいはクーポン提供などのサービスを行う。広告効果に応じて情報収集モジュール提供者やネットサービス提供者に報酬を支払う。例えば、アプリ内に表示された広告を利用者がタップした場合などに報酬を支払う。

KDDI 研究所によれば、2011 年 8 月に収集したアンドロイド上で動作する 980 個のアプリケーションの利用許諾について分析を行った結果、558 (56.9%) のアプリに合計 1,065 の情報収集モジュールが存在していたとされる^[4]。

利用者情報の収集目的は、一般にサービスの提供・向上や利用者の趣向に応じた広告の表示等とされている。介在するそれぞれの関係者において実際にどのように活用されているかは必ずしも明確ではないが、アプリ提供者が高額の報酬を得る目的で盲目的に情報収集モジュールを組み込み、アプリの趣旨に沿わない情報を取得するケースが多いと言われる。

2.2 プライバシー侵害リスク

プライバシー権とは、一般人の感受性を基準に個人に関する情報を、みだりに第三者に開示または公表されない権利とされる^{*3}。近年、情報通信技術の高度化に伴い、「個人を識別できないデータであっても、ネット上の膨大な情報と照合することで特定の個人が識別される」などのプライバシー侵害リスクが高まっている。特に、パーソナルデータが第三者提供され事業者間を転々とするような場合、当初は個人が識別できなくても、多くの情報が集積・突合・分析されることにより、特定の個人が識別されプライバシー侵害に到る可能性がある。

個人の再特定化の例を図 3 に示す。事業者 A は、収集したパーソナルデータから個人を特定する情報（氏名、郵便番号、住所、メールアドレス、電話番号）を削除（図 3 ①）して事業者 B に転売する。しかし事業者 B は、別途所有する情報から共通項目（性別、年齢、端末 ID、位置情報）を受領データと突合（図 3 ②）、すると受領したデータが誰のものを特定することができてしまう（図 3 ③）。

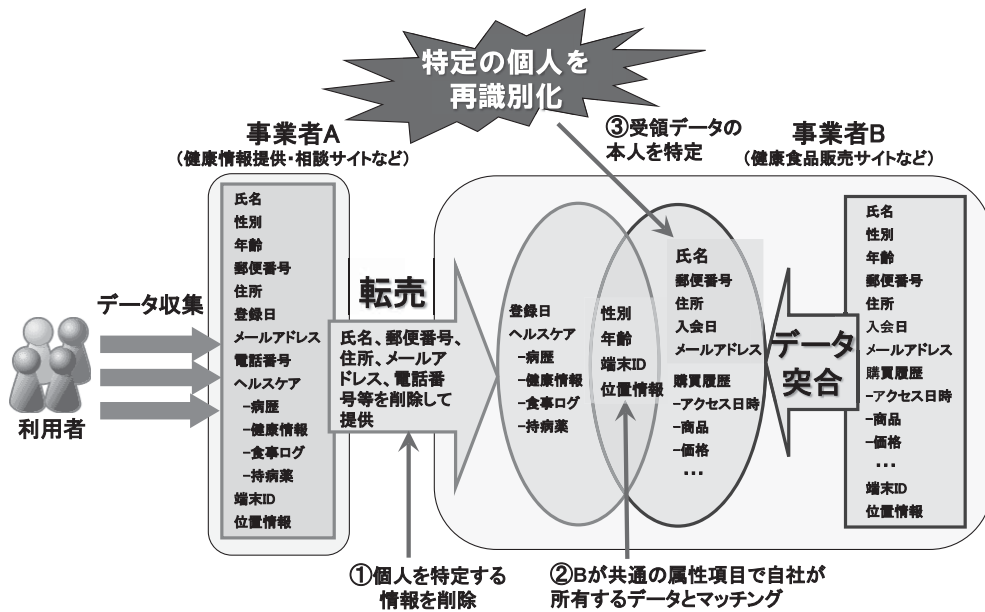


図3 流過程における個人の再特定化の例

このようなことから、利用者には「自己のパーソナルデータが適正に取り扱われているか」という疑念が生じる。この疑念を払拭するには、利用者に対しプライバシーポリシーを提示してデータ取扱いの透明性を確保する必要がある。しかし独立行政法人産業技術総合研究所による国内外の事業者におけるプライバシー対応状況の調査^[6]によると、日本の事業者は、プライバシーポリシーを適切に提示することなく、あるいは提示していても正確な記述を行うことなくパーソナルデータを収集し、自らの事業の用に供している実態が読み取れる。

2013年7月、JR東日本がSuicaの膨大な乗降履歴データを利用者に無断で第三者に販売したところ、利用者からの苦情が相次いだため販売を中止した^{*4}という事件があった。その原因は、JR東日本が、どのようなプライバシー保護施策を講じているのかを明示せず第三者提供したからである。このようなケースでは、データの販売者および購入者は、「収集したデータを利用して特定の個人を再識別化することや営利目的で特定の個人にリーチすること等を行わない」旨をプライバシーポリシーに定め、それを公表すべきである。

3. 個人情報保護法改正の動向

前章で述べたことを背景に、高度情報通信ネットワーク社会形成基本法（平成12年法律第144号）第36条の規程に基づき、首相官邸の高度情報通信ネットワーク社会推進戦略本部に設置された「パーソナルデータに関する検討会」において個人情報保護制度の改正が検討され、まず2014年6月24日に制度改正大綱が決定され、さらに2014年12月19日に改正骨子案が公表された。これらに従い2015年1月の通常国会にて個人情報保護法が改正される見込みである。

3.1 制度改正大綱の概要

本制度改正は、社会全体の利益増進のためにパーソナルデータの利活用を促進することが主

目的であり、プライバシー保護については主眼ではないように感じられる。パーソナルデータの利活用に関する制度改正大綱の大筋は、主に表3のとおりである。また、改正骨子案の概要は表4のとおりである。

表3 パーソナルデータの利活用に関する制度改正大綱の大筋

項番	内容
1	グレーゾーンのパーソナルデータの解消を図り、「利活用の壁」を取り払う。
2	保護されるパーソナルデータの範囲は、政省令、規則及びガイドラインにより定め、その範囲への該当性については、第三者機関が解釈の明確化を図る。
3	本人の承諾なしに個人特定性低減データの第三者提供を容認する。 ここで、個人特定性低減データとは以下を指す。 1) 識別特定情報（個人情報）から個人特定性を低減したデータ 2) 識別非特定情報（グレーゾーンのパーソナルデータ）から個人特定性を低減したデータ
4	マルチステークホルダープロセスの考え方を活かし、民間団体が業界の特性に応じた具体的な運用ルールを定める。
5	第三者機関の体制を整備して実効性のある制度執行を確保するとともに、本制度の国際調和を図る。

表4 改正骨子案の概要

項番	内容
1	第三者機関（個人情報保護委員会（内閣府の外局））の新設。 これはマイナンバー制度の特定個人情報保護委員会を改組するもの。
2	個人情報の定義拡充（グレーゾーンのおおよその範囲を定める）。 生存する個人に関する情報であって、「文字、番号、記号その他の符号のうち政令で定めるものが含まれるもの」を新たに個人情報に加える。 ・特定の個人の身体の一部の特徴を電子計算機の用に供するため変換した符号 （例）指紋データ、顔認識データなど ・個人毎に異なるものとなるように役務の利用、商品の購入または個人に発行される書類に付される符号 （例）携帯電話番号、旅券番号、運転免許証番号など
3	本人の承諾のない第三者提供の容認。 第三者機関で定める基準に従い、個人情報を匿名加工情報 ^(注) に加工することにより、本人の承諾なく匿名加工情報を第三者に提供できる。 （注）制度改正大綱における「個人特定性低減データ」のこと
4	個人情報保護の緩和（利用目的の制限緩和）。 個人情報のオプトアウト方式による利用目的変更を認める。但し、個人情報取得時に本人に予め通知、または公表することに加え第三者機関に届出を要する。
5	個人情報保護の強化。 ・オプトアウト方式による個人情報の第三者提供の規制強化（個人情報取得時に本人に予め通知、または公表することに加え、第三者提供に関する事項を第三者機関に届出なければならない）。 ・第三者提供に係る確認及び記録の作成の義務付け（名簿屋対応）。 ・不正な利益を図る目的による個人情報データベース提供罪の新設（大規模情報漏洩事件対応）。
6	グローバル化への対応。 ・国内企業などが外国で個人情報を取り扱う場合、個人情報保護委員会による命令を除いて個人情報保護法を適用する。 ・外国にある第三者へ提供する場合は、本人同意を得るか、委員会が日本と同等水準の保護制度と認められると定める国が、委員会規則の基準に適合する体制を整備している企業に限る。

3.2 保護されるパーソナルデータとは

いわゆる「グレーゾーンのパーソナルデータ」は広範であり、その取扱いにおいて法制度に抵触するリスクを把握することは大変困難である。その主たる原因は、現行法における「個人情報」の用語定義が明確でないからであり^[7]、特に個人情報に関する個人識別性については「特定」と「識別」に分けて議論しなければならない。

表5 個人識別性・特定性の違いによるパーソナルデータの法的な扱い

項番	データの種別	内容	法的な位置付け	例
1	識別・特定情報	個人が（識別されかつ）特定される状態の情報（それが誰か一人の情報であることがわかり、さらに、その一人が誰であるかがわかる情報）	現行の個人情報保護法に定める個人情報として保護される。	氏名、生年月日その他の記述等により特定の個人を識別することができるもの
2	識別・非特定情報	一人ひとりとは識別されるが、個人が特定されない状態の情報（それが誰か一人の情報であることがわかるが、その一人が誰であるかまではわからない情報）	改正個人情報保護法において、保護されるパーソナルデータ（プライバシーに係る情報）として扱われる予定。いわゆるグレーゾーンのパーソナルデータ。	免許証番号、パスポート（旅券）番号、端末固有ID、MACアドレス、IPアドレス（V6）、メールアドレス、声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、位置情報、Web閲覧履歴など。詳細は表6参照
3	非識別・非特定情報	一人ひとりとは識別されない（かつ個人が特定されない）状態の情報（それが誰の情報であるかがわからず、さらに、それが誰か一人の情報であることが分からない情報）	個人のプライバシーには係わらない情報、即ち、非個人情報として扱われる。	統計情報のような公開情報

第5回パーソナルデータに関する検討会 配布資料2-1 “技術検討ワーキンググループ報告書（2013年12月10日）”^[7]より一部抜粋して作成

表6 グレーゾーンのパーソナルデータの種類と詳細例

項番	情報の種類	グレーゾーンデータの例
1	個人又は個人が使用する通信端末機器等に関するもの	運転免許証番号、パスポート（旅券）番号、健康保険証の記号・番号（健康保険被保険者証記号番号等）、雇用保険被保険者番号、外国人の在留に関する番号（在留カード番号、特別永住者証明書番号、外国人登録証明書番号）、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ユーザID・パスワード（複数事業者、又は一事業者内の複数サービスで共用）、ユーザID・パスワード（一事業者内）、ナンバープレート（自動車登録番号標等）番号、固定電話番号、携帯電話番号、Webフィンガープリント、情報通信端末シリアルナンバー（携帯電話端末シリアルナンバー等）、MACアドレス、情報通信端末ID、ICカードの固有ID、ソフトウェアシリアル番号、不動産番号、IPアドレス（V6）
2	個人の身体的特徴に関するもの	声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、掌形、生体認証で使用されるデータ、歩行パターン、筆跡、性別、肌の色、人種、家族構成、血液型、髪の色、血圧、脈拍、身長、体重
3	上記のほか、特定の個人の識別につながる多量又は多様な情報の収集を可能にするもの	移動履歴（時刻情報を伴う位置情報を含む）、購買履歴、Web閲覧履歴（Cookie含む） ※項番3のこれら三つの項目例は、報告書の最終稿から削除されている。

第10回パーソナルデータに関する検討会 配布資料1-2 “技術検討ワーキンググループ報告書（2014年5月）”^[8]より一部抜粋して作成

個人の識別性/特定性の違いによるパーソナルデータの法的な位置付けを検討した結果を表5に示す。このうち項番2の識別・非特定情報がグレーゾーンのパーソナルデータにあたり、法改正後の制度下において「保護されるパーソナルデータ」となることが予想される。項番2の種類と内容について、その詳細例を文献^[8]に基づき表6に示す。

なお、表5に示すパーソナルデータの包含関係は図4のようになる。



図4 パーソナルデータの包含関係

3.3 パーソナルデータの第三者提供に係るスキーム

本人の承諾のないパーソナルデータの第三者提供は本制度改正の目玉ともいえるが、制度改正大綱等においてはその具体的な方法や例示はほとんど示されず、表7のような内容が記載されているのみである。

表7 制度改正大綱および改正骨子案におけるパーソナルデータの第三者提供に係る記述

取り扱い		制度改正大綱	改正骨子案
加工方法	1	「個人特定性低減データ」への加工方法はデータの有用性や多様性に配慮し一律に定めない。	個人情報から特定の個人を識別することができる記述等の削除（他の記述等に置き換えることを含む）をするなど、当該個人情報を復元することができないようにその加工をしなければならない。
	2	当該加工方法については、民間団体が自主規制ルールを策定する。	匿名加工情報を作成するときは事前に第三者機関（個人情報保護委員会）に届け出る。
	3	第三者機関が当該自主規制ルール又は民間団体の認定を行う。	第三者機関が匿名加工情報へ加工するための基準を定める。
	4	適切な加工方法については、第三者機関、民間団体においてベストプラクティスの共有を図る。	加工に関する情報についての情報漏洩を防止するための安全管理措置を講じなければならない。
第三者提供	1	本人の同意がなくても第三者提供等が可能な枠組みを導入する。	第三者に提供する場合は、その旨の公表と、提供先（受領者）に匿名加工情報であることを明示しなければならない。
	2	個人特定性低減データについて、特定の個人を識別することを禁止する適正な取扱いを定める。	受領者は、加工した方法に関する情報の取得や、匿名加工情報を他の情報と照合してはならない。 なお受領者が、さらなる第三者に転売するときも上記（公表と明示）と同様の措置を採らなければならない。
	3	本人の同意の代わりとしての取扱いに関する規律を定める。	—

これらを踏まえ、事業者A（提供元）から事業者B（提供先）にパーソナルデータを第三者提供するスキームを具体化すると以下ようになる（図5）。

- ① 事業者 A は、匿名加工情報（制度改正大綱における個人特定性低減データのこと）を作成することを予め第三者機関に届け出る。
- ② 事業者 A は、第三者機関が定めた基準に従い、パーソナルデータ（個人情報またはグレー情報）を匿名加工情報に加工する。なお加工方法に関する情報は適切に管理する。
- ③ 事業者 A は、加工によって得られた匿名加工情報を第三者提供する旨を公表し、事業者 B に匿名加工情報であることを明示する。
- ④ 事業者 B は、加工に関する情報を事業者 A から取得してはならない。かつ、受領した匿名加工情報を自身が保有する他の情報と照合してはならない。

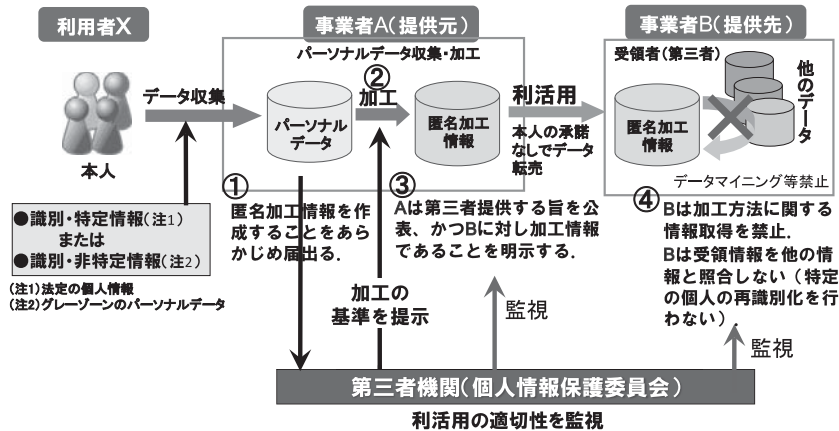
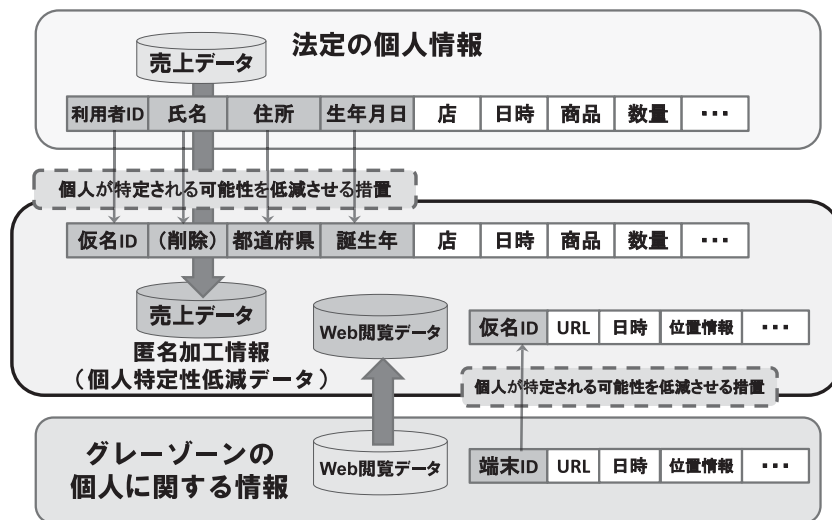


図5 本制度改正の主旨に則ったパーソナルデータの第三者提供に係るスキーム

なお、想定される加工方法の具体例を図6に示す。



首相官邸、第8回パーソナルデータに関する検討会資料(2014年4月24日)を一部修正して作成

図6 匿名加工情報への加工の例

本制度改正の内容は現時点において具体的方法が不明確な部分が多いため、2015年1月の通常国会で改正個人情報保護法が成立した後、施行までには相当の期間を要すると推察される。しかしパーソナルデータを取扱うビジネスやサービスはすでに開始されつつあるので具体的な法制度が整うまでの間、事業者は図5の③④を担保するために制度改正大綱等に述べられている「特定の個人を識別することを禁止する適正な取扱い」を独自に実施する必要がある。

この点につき一歩踏み込んだ具体策としては、米国のFTC3要件^{*5}の考え方が参考となる。特に利用者に対する透明性を確保するため、図5の③④に代えて以下③'および④'の施策が有効と考えられる。

- ③' 事業者Aは加工によって得られた匿名加工情報から特定の個人を再識別化しないことを公表する。

(注) 改正骨子案においては、加工者が匿名加工情報から特定の個人を再識別化することを禁じていないが、加工者も受領者と同様に再識別化を禁止すべきである。

- ④' 事業者Aと事業者Bの間で締結する契約において、匿名加工情報を受領する事業者Bが特定の個人の再識別化を禁止することを定める。

(注) 改正法の施行までの間、匿名加工情報の受領者に特定の個人を再識別化させないことを担保するための手段として有効と考えられる。

これらは、利用者の懸念を払拭するためにプライバシーポリシー（5章で詳述）に提示すべき最も重要なポイントの一つと考えられる。

4. 事業者が取り組むべき対応としてのプライバシー・バイ・デザイン

2.1節で述べたように、利用者が無意識の間にプライバシーに関わる情報を事業者が収集・利用する状況が常態化しているが、収集される情報が利用者にとって許容できるか否かは、各利用者の価値観に依存するため、最終的には利用者の判断によって決まる。

しかし、利用者の判断を可能にするためには、サービスを提供する事業者が、どのような情報をどのように収集し、どう取扱うのかを説明することが不可欠である。

即ち、事業者はプライバシー・バイ・デザイン^[9]の実施体制を構築し、ビジネスを計画・実行する際には、企画・開発・構築・運用においてプライバシー保護のためのチェックポイントを設けることが必要である（図7）。

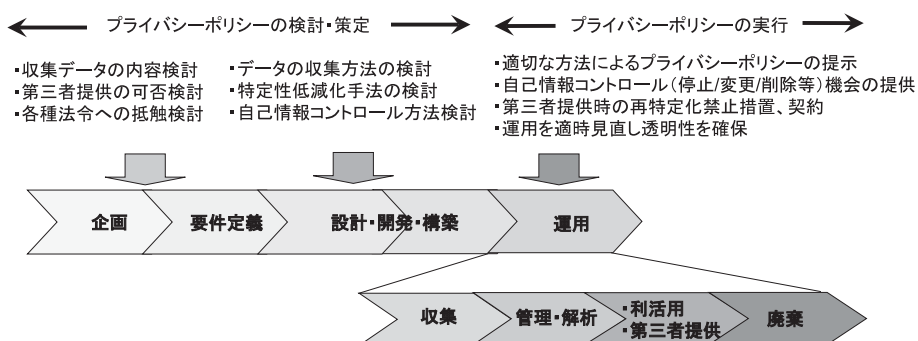


図7 パーソナルデータを利用するビジネスプロセスにおけるプライバシー・バイ・デザイン

そしてビジネス実行時には、利用者に対する透明性を確保し信頼を得るため、

- ・適時に適切な方法によりプライバシーポリシーを提示する
- ・本人の承諾を得ずに匿名加工情報を第三者提供する際の適切な措置を講じる
- ・情報取得の停止、変更、削除等の自己情報コントロールの機会を付与する

ことが必要である。

なお、システム開発ベンダーに対してもプライバシー・バイ・デザインの実施体制が求められることが想定される。例えば特定性低減化手法や自己情報コントロール方法等については、今後設立される予定の第三者機関が認定した規制ルールやガイドラインを注視しつつ、それらを迅速に受託開発プロセス等に取り込む必要があるだろう。

5. プライバシーポリシーの策定と提示方法

本章では、グレーゾーンのパーソナルデータを取扱うにあたり、プライバシー侵害リスク回避のために必要な利用者への配慮、透明性の確保に資するプライバシーポリシーの要件と具体例ならびにその提示方法を検討し、プライバシー・バイ・デザインの第一歩として提言する。

5.1 望ましいプライバシーポリシーの要件

プライバシーポリシー策定に重要な点は、パーソナルデータ取得に係る透明性の確保である。その目的は、利用者のプライバシー保護と事業者リスク回避の両立であり、具体的には表8に示す内容を、利用者が容易に納得（同意）できるようにすることである。

表8 プライバシーポリシーに明記すべき重要事項

項番	内容
1	事業者が取得する情報内容、取得方法、利用目的
2	取得した情報の第三者提供時の対応
3	利用者に対し情報取得の停止、変更、削除等の自己情報コントロールの機会提供

3章で述べたように、制度改正大綱等においては具体的なプライバシー保護ルールがほとんど示されていないため、既存の指針やガイドライン等を参考に基本的な要件を洗い出すこととする。

調査検討の結果、表9に示す二つの文書をプライバシーポリシー要件の基礎とした。特に

表9 プライバシーポリシーの要件検討の基礎とした文書

項番	発行年月日、発行元、名称	検討の基礎とした理由	参考とした内容
1	2012年8月、総務省、「スマートフォンプライバシー イニシアティブ」報告書(SPI) ^[3]	利用者情報の取扱いに係るプライバシー問題等について、国際協調を意識した我が国における先駆的な報告書であり、検討の基礎としては最適と史料。	・6項目の基本原則 ※表10参照 ・プライバシーポリシーに記載すべき8項目 ※表11参照
2	2012年11月13日、モバイル・コンテンツ・フォーラム、「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」 ^[11]	利用者情報の取扱いやプライバシーポリシーの提示方法などにつき、SPIをより具体化した推奨事項が記述されている。	・プライバシーポリシーの実装にあたり推奨される9項目の推奨要件 ※表12参照

表 10 利用者のプライバシー保護のための六つの基本原則

項番	項目	基本原則
1	透明性の確保	事業者等は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。
2	利用者関与の機会の確保	事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。
3	適切な手段による取得の確保	事業者等は、対象情報を適正な手段により取得するものとする。
4	適切な安全管理の確保	事業者等は、取扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。
5	苦情・質問への対応体制の確保	事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。
6	プライバシー・バイ・デザイン	事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようあらかじめ設計するものとする。利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

総務省の“スマートフォン プライバシー イニシアティブ (2012 年 8 月)”^[3]より抜粋して作成

表 11 プライバシーポリシーに記載すべき 8 項目

項番	項目	内容
1	情報を取得する事業者等の氏名又は名称	パーソナルデータを取扱う事業者等の名称、連絡先等を記載する。
2	取得される情報の項目	取得される利用者情報の項目・内容を列挙する。
3	取得方法	利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等を示す。
4	利用目的の特定・明示	・利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。 ・広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。
5	通知・公表又は同意取得方法、利用者関与の方法	・通知・公表の方法、同意取得の方法：プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。 ・利用者関与の方法：利用者情報の利用を中止する方法等を記載する。
6	外部送信・第三者提供の有無、情報収集モジュールの有無	外部送信・第三者提供・情報収集モジュールの組み込みの有無を記載する。
7	問合せ窓口	問合せ窓口の連絡先等（電話番号、メールアドレス等）を記載する。
8	プライバシーポリシーの変更を行う場合の手続	プライバシーポリシーの変更を行った場合の通知方法等を記載する。（当初取得した同意の範囲が変更される場合、改めて同意取得を行う。）

総務省の“スマートフォン プライバシー イニシアティブ (2012 年 8 月)”^[3]より抜粋して作成

表 12 プライバシーポリシーに盛り込むべき推奨要件

項番	項目	内容
1	プライバシーポリシーの名称について	「個人情報保護方針」と混同されないように、「プライバシーポリシー」という表記を採用する。
2	通知又は公表および同意取得等のタイミングについて	最低でも初回起動時に利用者情報を取得する前に閲覧できるようにする。同意が必要な場合には同意の意思を確認できるように、もしくは、個別の情報取得場面で個別の同意を取得。
3	プライバシーポリシーを掲示する場所について	「個人情報保護方針」「サービスの利用規約」等と明確に区別できるようにする。サービスを紹介するスペースに可能な限り掲示する。全文を掲示できない場合には、全文を閲覧できるページへのリンクを掲載し、サービスの紹介ページに可能な限り要約や概要を掲示する。サービス利用中にも、呼び出せるようにする。
4	プライバシーポリシーの変更について	変更前の利用目的と相当の関連性を有すると合理的に認められる範囲で行い、必要に応じて変更箇所や追加内容が理解できるように、通知又は公表すること。利用者が想定することが困難であると認められる利用目的の変更を行う場合には、改めて本人の同意を得ること。
5	同意が得られなかった場合に制限される事項について	同意が得られなかった場合にアプリケーションやサービスの利用が制限される場合は、その旨を説明すること。
6	取得した利用者情報の取扱いについて	取得した利用者情報の保存期間や削除の方針を記載しておくこと。一般的には、一定の保存期間を設定し、その期間を超えて利用が無かった場合には利用者情報を削除することを明記し、利用者にあらかじめ通知又は公表すること。
7	必要要件以外の同意取得について	分かりやすく透明性が高い説明を行うだけでなく有効な選択肢の提供として、「プライバシーポリシー」および「契約者・端末固有 ID 等の取得」については同意を取得すること。
8	日本語以外での説明に対する対応について	情報収集モジュール提供者からプライバシーポリシー等が日本語で提供されていない場合は、情報収集モジュール提供者に日本語での提供を求めること。
9	既存サービスへの対応について	既に提供されているサービスにおいても、可能な限り早く本推奨要件に準拠することを求める。アプリケーションの改修が必要な場合は、改修計画を策定し、着実に実行される体制を整備すること。

モバイル・コンテンツ・フォーラムの「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン (2012 年 11 月)」^[11]を参考に作成

表 9 項番 1 の「スマートフォン プライバシー イニシアティブ」(以下、SPI) は、2013 年 6 月の閣議決定「世界最先端 IT 国家創造宣言」^[10]において先行的なルールとして取り上げられ「その取組みの普及を促進する」とあり、政府方針と合致するなど検討の基礎として最適なものと考えられる。また、項番 2 の「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」は、抽象的な記述の SPI をより具体化しており、プライバシーポリシー策定の参考となり得る。

次節以降では、表 10 と表 11 の基礎資料に記載の推奨事項から得られた要件(表 12)を基礎として、今般の制度改正大綱の主旨に鑑み、事業者が取得したパーソナルデータを第三者提供の際のポリシー、特にデータの利活用を図るために本人の承諾を得ないで第三者提供を行う場合等を想定しながら、利用者に提示すべき適切なプライバシーポリシーの策定を試みる。

5.2 個人情報保護方針とプライバシーポリシーの関係

プライバシーポリシーは、一般の個人情報保護方針と混同されないよう、提供するサービスやアプリケーション毎に策定すべきである（図8）。その理由は、制度改正大綱等の方針では、保護されるパーソナルデータの範囲や第三者提供のための加工方法を一律に定めないで、事業者としては大枠として個人情報の保護方針を定めた上で、サービスやアプリケーション毎にパーソナルデータを扱うためのポリシーを定める必要があるからである。

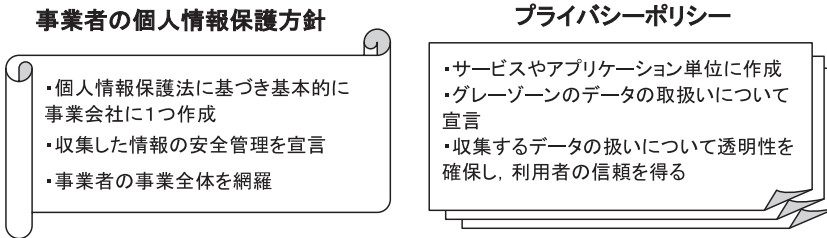


図8 個人情報保護方針とプライバシーポリシーの関係

なお、個人情報保護方針と個々のプライバシーポリシーの内容が異なる場合は、後者が優先する旨を記述することに留意する。

5.3 要件に基づくプライバシーポリシーの策定

ここでは、5.1節の要件に則って検討・作成したプライバシーポリシーの種別およびその雛形を示す。

利用者は、サービスやアプリケーションの利用開始にあたり、プライバシーポリシーのような規約をほとんど読まないことが多いため、プライバシーポリシーは概要版と詳細版を作成することが望ましい。これは利用者へのプライバシーインパクトにつき簡潔明瞭な通知と正確な通知の両立をはかるために必要であり、各々に推奨される記載内容は表13のとおりである。

表13 プライバシーポリシーの概要版と詳細版

種別	推奨される記載内容
概要版	サービスが取得する利用者情報の項目、利用目的、第三者提供、情報収集モジュールの有無等を、ブラウザ等の1画面（スマートフォンにあってはアプリケーションの1画面）で一覧できるよう記載する
詳細版	総務省「スマートフォン プライバシー イニシアティブ」に定めるプライバシーポリシーに記載すべき8項目（表11）に準拠した内容をすべて記載する。 ★スマートフォンのアプリケーションにあってはアプリマーケット等にも概要版を掲載し、そこから詳細版へのリンクを設けることが望ましい

ここまでの検討に基づき策定した概要版の雛形例を表14に、またその詳細版の雛形例を表15に示す。これらには、制度改正大綱を踏まえた本人の承諾のないパーソナルデータの第三者提供スキームを含んでいることが特徴的である。また、パーソナルデータを提供した相手先におけるパーソナルデータの取扱いを契約で規制するなどが従来のプライバシーポリシーにはなかったものである。

表 14 プライバシーポリシー概要版の雛形例

〇〇サービスに関するプライバシーポリシー概要（〇年〇月〇日）		〇〇株式会社
当社（サービス提供者名）が提供するサービスのご利用における利用者情報の取扱いの概要は以下の通りです。詳細につきましては、プライバシーポリシー詳細版（※リンク先を表示）を必ずご確認ください、内容をご理解の上、ご利用ください。なお、当社の個人情報保護方針と内容が相違する場合は本プライバシーポリシーの内容が優先するものとします。		
1. 本サービスで取得する利用者情報と利用目的		
	① GPS による位置情報：本サービスによる利用者への△△機能提供のため ② サービスのログ情報（起動時間、状態情報など）：本サービスの品質改善のため ③ 端末固有 ID、位置情報：当社のプライバシーポリシーに適合することを確認した広告会社が、利用者に広告を表示するため。利用者情報はアプリケーションに組み込んだ情報収集モジュールを通じて取得します。	
2. 利用者情報の第三者提供について		
	取得した利用者情報を第三者に提供する場合には、事前に利用者の同意を取得します。 なお、特定の個人が識別される可能性を低減するよう加工した情報（以下、個人特定性低減データ）を利用者の事前同意を取得せず第三者に提供する場合があります。この場合、当社は以下を公約します。 (1) 当社は加工によって得られた個人特定性低減データを利用して、意図的に特定の個人を再識別化することを行いません。 (2) 個人特定性低減データを提供する第三者（提供先）に対し、提供先が該データを利用して意図的に特定の個人を再識別化することを契約によって禁止します。	
3. 利用の停止等		
	本サービスでは、利用者の操作や申し出により、利用者の情報の全部もしくは一部の取得停止、変更、削除、利用の停止をすることができます。	
4. 利用者情報の廃棄について		
	本サービスは、利用者が本アプリケーションの削除（アンインストール）もしくは〇年以上本サービスを利用されなかった場合に終了するものとし、適正な管理のもと収集した利用者情報を廃棄します。	
5. 問い合わせ窓口等		
	本アプリケーションおよび本サービスにおける利用者情報の取扱いに関するお問い合わせ、ご相談は以下の窓口でお受けいたします。 ■窓口：株式会社〇△□ お客様係 ■お問い合わせ方法：下記のお問い合わせフォームより ■お問い合わせフォーム：http://www.xxxx.co.jp/inquiries/ 詳細は以下よりご確認ください。 ・プライバシーポリシー詳細（※リンク先を再表示） ・個人情報保護方針（※リンク先を表示）	

表 15 プライバシーポリシー詳細版の雛形例 (1/2)

〇〇サービスに関するプライバシーポリシー (〇年〇月〇日 詳細版)		〇〇株式会社																		
第1条 情報を取得する事業者等の氏名又は名称 (※ 本条は表 11 の項番 1 について記載する)																				
本プライバシーポリシーは、[事業者名]が提供するサービス [サービス名称] およびそれに関連するサービス (以下、本サービス)、ならびに本サービスの提供に必要な場合であって利用者の端末上で稼動するアプリケーション (以下、本アプリケーション) (注 1) のご利用における利用者情報の取り扱いを定めたものです。なお、[事業者名] の連絡先は、問い合わせ窓口 (第 10 条) をご覧ください。 (注 1) スマートフォンやタブレット上で稼動するアプリケーション、PC 上で稼動するアプリケーション、あるいは一般ブラウザおよびそれと連動して稼動するプラグインソフトウェアなど																				
第2条 取得される情報の項目、取得方法、利用目的、(※ 本条は表 11 の項番 2, 3, 4 について記載する)																				
1. 利用者ご自身によりご登録いただく個人に関する情報 (※ 利用者に登録してもらう情報がある場合のみ) 本サービスの初回ご利用開始時に、〇〇、△△、□□ (例 1) を登録していただきます。また、任意にご提供いただける場合●●、▲▲について登録いただく場合があります。ご登録いただいた情報については、■● (例 2) の利用目的のために利用させていただき、第 8 条の場合を除き第三者へ提供することはありません。 (例 1) 氏名、生年月日、性別、住所、電話番号、メールアドレス、ユーザー・ネーム、パスワード (例 2) 利用者登録・管理、重要な通知、当社の商品告知などの送付等																				
2. 本サービスのご利用に際して、下表に記載の利用者情報を同表記載の利用目的のために同表記載の方法で取得致します。同意をいただけない場合には、本サービスの機能はご利用いただけません。																				
<table><tr><th>取得する情報</th><th>取得方法</th><th>利用目的</th></tr><tr><td>電話帳情報、端末の位置情報、端末固有 ID (IMEI、IMSI、ICCID、UDID、Android ID 等)、OS が生成する ID、MAC アドレス、IP アドレス</td><td>本アプリケーションによる自動取得</td><td>SNS 連携機能、利用者間での通信および情報共有機能提供のため</td></tr><tr><td>本アプリケーションのシステムログ情報 (起動時間、状態情報など)</td><td>本アプリケーションによる自動取得</td><td>本サービスの障害対応/品質改善/品質向上のため</td></tr><tr><td>本アプリケーションの利用履歴</td><td>本アプリケーションによる自動取得</td><td>本サービス利用者への商品情報提供のため</td></tr><tr><td>本サービスを提供する Web サイトアクセス時のブラウザの種類・バージョン、端末の OS 種別、Web 閲覧履歴、クッキー</td><td>Web サイトによる自動取得</td><td>本サービス利用者のライフスタイル分析を行い、本サービスの機能改善に資するため</td></tr><tr><td>端末固有 ID、MAC アドレス、端末の位置情報</td><td>本アプリケーションに組み込まれた情報収集モジュールによる自動取得</td><td>第三者による利用者への広告表示のため</td></tr></table>			取得する情報	取得方法	利用目的	電話帳情報、端末の位置情報、端末固有 ID (IMEI、IMSI、ICCID、UDID、Android ID 等)、OS が生成する ID、MAC アドレス、IP アドレス	本アプリケーションによる自動取得	SNS 連携機能、利用者間での通信および情報共有機能提供のため	本アプリケーションのシステムログ情報 (起動時間、状態情報など)	本アプリケーションによる自動取得	本サービスの障害対応/品質改善/品質向上のため	本アプリケーションの利用履歴	本アプリケーションによる自動取得	本サービス利用者への商品情報提供のため	本サービスを提供する Web サイトアクセス時のブラウザの種類・バージョン、端末の OS 種別、Web 閲覧履歴、クッキー	Web サイトによる自動取得	本サービス利用者のライフスタイル分析を行い、本サービスの機能改善に資するため	端末固有 ID、MAC アドレス、端末の位置情報	本アプリケーションに組み込まれた情報収集モジュールによる自動取得	第三者による利用者への広告表示のため
取得する情報	取得方法	利用目的																		
電話帳情報、端末の位置情報、端末固有 ID (IMEI、IMSI、ICCID、UDID、Android ID 等)、OS が生成する ID、MAC アドレス、IP アドレス	本アプリケーションによる自動取得	SNS 連携機能、利用者間での通信および情報共有機能提供のため																		
本アプリケーションのシステムログ情報 (起動時間、状態情報など)	本アプリケーションによる自動取得	本サービスの障害対応/品質改善/品質向上のため																		
本アプリケーションの利用履歴	本アプリケーションによる自動取得	本サービス利用者への商品情報提供のため																		
本サービスを提供する Web サイトアクセス時のブラウザの種類・バージョン、端末の OS 種別、Web 閲覧履歴、クッキー	Web サイトによる自動取得	本サービス利用者のライフスタイル分析を行い、本サービスの機能改善に資するため																		
端末固有 ID、MAC アドレス、端末の位置情報	本アプリケーションに組み込まれた情報収集モジュールによる自動取得	第三者による利用者への広告表示のため																		
第3条 取得情報の公開・共有 (※本条は表 11 の項番 5 について記載する)																				
利用者が本サービスを通じて友達や知人と通信による連絡および情報を共有する機能を利用した場合には、本サービスが取得した利用者の位置情報 (位置情報の機能を有効にしている場合)、メッセージに含まれるテキスト、写真、動画、音声、URL のリンクが連絡や情報の共有をしている友達や知人に通知または共有される場合があります。 また、これらの機能を全て公開する設定としていると、本サービスを利用している全ての利用者が閲覧することができます。公開範囲は、本サービスが提供する設定機能から変更することができます。 ※その他、事前に通知が必要あるいは望ましいものについて記載する。また、利用者が誤解や勘違いしやすいものについても補足する。																				
第4条 プライバシーポリシーの提示場所および提示方法 (※本条も表 11 の項番 5 について記載する)																				
当社の個人情報保護方針および本プライバシーポリシーの最新のものは、下記のリンクよりご確認ください。両者が異なる場合には、本プライバシーポリシーが優先するものとします。 ・当社の個人情報保護方針へのリンク http://www.xxxx.co.jp/policy/ ・本サービスのプライバシーポリシーへのリンク http://www.xxxx.co.jp/privacy/																				
第5条 同意取得の方法 (※本条も表 11 の項番 5 について記載する)																				
第5-1条 同意取得の対象、タイミング																				
1. 本サービスは、本プライバシーポリシーをご確認いただき、内容をご理解したうえでご利用ください。本プライバシーポリシーは第 4 条に記載の場所に掲示されており、この掲示をもって公表したものとします。 2. 〇〇 (例 3) の利用目的のために△△ (例 4) の情報を取得する場合には、個別の情報の取得について同意を取得いたします。同意をいただけない場合には、□□の機能はご利用いただけません。 (例 3) 電話帳に登録されている方との通信による連絡および情報の共有、ならびにそれらの方への広告表示 (例 4) 電話帳に登録されている情報 (※電話番号、メールアドレス、住所等、具体的に記載する)、GPS (衛星測位システム) による端末の位置情報など																				
第5-2条 情報の開示、提供																				
当社は、利用者の同意を得ることなく、本サービスにて利用者より取得、保存した情報を、本プライバシーポリシーに明示している第三者以外に開示または提供することはありません。ただし、第 8 条の場合および以下場合は除きます。 1) 法令に基づく場合。 2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難である場合。 3) 国の機関もしくは地方公共団体またはその委託を受けたものが、法令の定めにより遂行することに協力する必要がある場合であって、本人の同意を得ることによりその遂行に支障を及ぼすおそれがある場合。 4) その他、社会通念上、当社が必要と判断した場合であって、本人の同意を得ることが困難である場合。																				

表 15 プライバシーポリシー詳細版の雛形例 (2/2)

第6条 利用者関与の方法（※本条も表11の項番5について記載する。自己情報コントロールの機会付与） 第6-1条 サービス利用中の利用者関与 本サービスでは、利用者の操作やお申し出により、利用者の情報の全部もしくは一部の取得停止、変更、削除、利用の停止をすることができます。（※アプリケーションを使用しながら情報の取得を中止する方法、情報の取得は継続されるがその利用が中止される場合などを分けて記載） 1. 利用者が登録した利用者情報のうち氏名、メールアドレス、ユーザー・ネーム、パスワード、居住地につきましては、利用者情報の確認、変更画面より変更が可能です。 2. 利用者が端末のGPS機能をOFFにすることで、詳細な位置情報の取得が停止できます。この場合も、通信事業者の基地局によるおおまかな位置情報の取得による地図の表示およびナビゲーションはご利用できます。 3. 本サービスにて自動取得した利用者の友達や知人の情報は、本サービスの友達リストの設定より削除、変更が可能です。本アプリケーションにおいて削除した場合には、本サービスのサーバからも適切な管理のもと定期メンテナンス時に消去いたします。 4. 広告を目的とする利用者の情報の取得停止等の取り扱いにつきましては、第9条に記載されている各広告配信事業者のアプリケーション・プライバシーポリシーをご確認ください。 または 本アプリケーションでは、利用者情報の収集を停止する手段を提供しておりません。収集を停止したい場合には、本アプリケーションを削除（アンインストール）してください。 第6-2条 サービス利用終了時の利用者関与 本サービスは、利用者が本アプリケーションの削除（アンインストール）もしくは○年（○ヶ月）以上ご利用されなかった場合には、ご利用を終了されたものとし、（※アプリケーションの削除（アンインストール）や利用しなくなった場合等について記載） 1. 利用者が、本アプリケーションの削除（アンインストール）機能を利用して端末より削除（アンインストール）された場合、利用者より取得、保存した利用者の情報は全て端末より直ちに削除され、本サービス上のサーバからは適切な管理のもと定期的なメンテナンス時に廃棄されます。 または 本アプリケーションは、収集された利用者情報を送信先の収集サーバから削除する手段を提供しておりません。収集サーバからの削除については、第10条の問い合わせ窓口までご連絡ください。 2. 利用者が、本アプリケーションを本アプリケーションの削除（アンインストール）機能を利用せずに端末より削除された場合や端末を交換もしくは廃棄された場合、端末では利用者の情報は削除されませんのでご注意ください。 3. 利用者が、本サービスを○年以上ご利用されなかった場合、当社はご利用を終了されたものとして、利用者から取得、保存した情報を本サービスのサーバ上から適切な管理のもと廃棄いたします。この場合も本アプリケーションおよび端末で保存している利用者の情報は削除されません。
第7条 外部送信の有無（※本条は表11の項番6について記載する） 第2条に基づき取得された情報については、○○○の設置するサーバに転送され、目的の範囲で使用されます。 ※外部送信のない情報へのアクセスについても明確化することが望ましい。 （例）○○については端末内部で△△の目的の範囲で使用されます。
第8条 第三者提供の有無（※本条も表11の項番6について記載する） 第2条の記述に基づき取得された情報は、利用者の同意を取得した上で第三者へ提供される場合があります。 なお、特定の個人が識別される可能性を低減するよう加工した情報（以下、<u>個人特定性低減データ</u>）を利用者の事前同意を取得せずに第三者に提供する場合があります。この場合、当社は以下を公約します。 1) 当社は加工によって得られた個人特定性低減データを利用して、<u>意図的に特定の個人を再識別化することはありません。</u> 2) <u>個人特定性低減データを提供する第三者（提供先）に対し、提供先が該データを利用して意図的に特定の個人を再識別化することを契約によって禁止します。</u>
第9条 情報収集モジュールの有無（※本条も表11の項番6について記載する） 本サービスを無料で提供させていただくために、広告配信を目的として、当社のプライバシーポリシーに適合することを確認した以下の広告配信事業者が、利用者の情報を自動取得します。 （広告配信事業者記載の例） 1) 株式会社XXXX ●●ターゲット広告サービス 取得する情報の項目：○○、△△、×× 利用目的：広告配信 第三者提供の有無：無 アプリケーション・プライバシーポリシー（※リンク先を表示） 2) 株式会社YYYY ▲▲宣伝ネットシステム 取得する情報の項目：○○、△△、×× アプリケーション・プライバシーポリシー（※リンク先を表示） 利用目的：広告配信、市場調査 第三者提供の有無：有（注2） （注2）利用者の同意を取得した上で第三者提供しますが、<u>個人特定性を低減するよう加工した上で利用者の同意を取得せずに第三者提供することがあります。</u>
第10条 問い合わせ窓口（※本条は表11の項番7について記載する） 本サービスにおける利用者情報の取り扱いに関するお問い合わせ、ご相談は以下の窓口でお受けいたします。 ・窓口名称：ZZZZ株式会社広報部 お客様係 ・お問い合わせ方法：下記のお問い合わせフォームより ・お問い合わせフォーム：http://www.xxxx.co.jp/inquiries/ ※お問い合わせフォーム、電話、メール等、連絡先の種類は問わないが、可能な限り利用者からの問い合わせに対応し得る方法を記載する。
第11条 変更（※本条は表11の項番8について記載する。事業者都合によるプライバシーポリシーの変更） 本プライバシーポリシーは改定されることがあります。 1. 本アプリケーションのバージョンアップに伴って、利用者情報の取得項目の変更や追加、利用目的の変更、第三者提供等について変更がある場合には、重要なものについてはインストール前もしくはインストール時にあらかじめ同意を取得させていただきます。 2. その他、利用者情報の取得項目の変更や追加、利用目的の変更、第三者提供等について変更がある場合には、メッセージ機能およびご登録いただいたEメールを通じてお知らせすると同時に、重要なものについてはあらかじめ同意を取得させていただきます。

5.4 プライバシーポリシーの提示方法

適切なプライバシーポリシーの提示とそれに対する利用者の理解（承諾）の目的は、利用者が自身のパーソナルデータを収集されることに対する懸念を払拭するのみならず、事業者によるプライバシー侵害リスクを回避し、双方が安心してパーソナルデータを利活用できるようにすることである。

従って事業者においては、利用者が必ず容易にプライバシーポリシーを参照・理解できるように配慮する必要がある。また、サービスやアプリケーションの利用開始前のみならず、利用開始後であっても利用者が容易に閲覧できるようにすべきである。

図9に示すように、まずは必ず概要版にたどり着くように設置し、利用者が必要に応じて詳細版を参照できるよう配慮する。

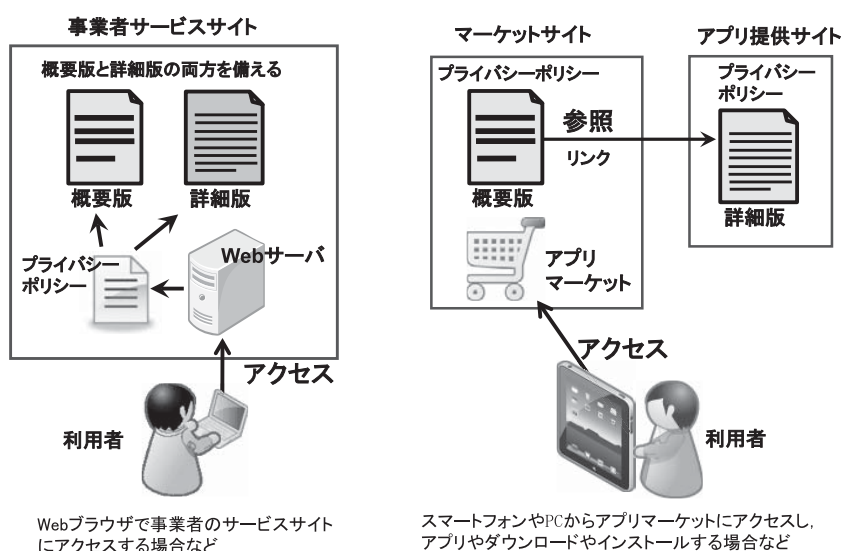


図9 プライバシーポリシーの概要版と詳細版の提示例

また、プライバシーポリシーに関する内容は可能な限りサービスやアプリケーションの利用規約とは別掲示とし、止むを得ず利用規約に含める場合はプライバシーポリシーに係る部分が明確に認識できるようにする。

概要版と詳細版の両方を提示することが望ましいが、少なくとも表14に示したプライバシーポリシーの要点を纏めた概要版だけでも利用者が認識できれば、パーソナルデータ収集における利用者側の不安はかなり解消できると推測され、データ利活用へ向けた事業者の透明性確保に資するものと考えられる。

6. お わ り に

現行の個人情報保護制度では、各省庁が運用基準をおのおの策定しているため、27分野40種類にも及ぶガイドラインが乱立している。事業者は、自らが属する業界のガイドラインを遵守することはもちろん、異業種と協業を行う際には他業界のガイドラインにも配慮しなければならない。

しかし、パーソナルデータの利活用は業界横断的に行ってこそ有用性が発揮されるため、業界個別のガイドラインの存在はむしろビジネス遂行上の障壁となる。従って、パーソナルデータ取扱いについて、基本的な原則を踏まえた雛形があればビジネス遂行上、非常に有益である。

本稿では、事業者がパーソナルデータを取扱うにあたり、どの業界でも応用できるような必要最小限かつ具体的なプライバシーポリシーの雛形について、制度改正大綱の主旨を踏まえて考案し、そしてその適切な提示方法について提言した。パーソナルデータを扱うビジネスでのプライバシー・バイ・デザイン実践に寄与できたら幸いである。

最後に本稿の執筆において協力を頂いた関係各位に感謝の意を表する。

-
- * 1 パーソナルデータとは、個人情報保護法に規定する「個人情報」に限らず、位置情報や購買履歴など、広く個人に関する個人識別性のない情報を含む情報を指す
 - * 2 プライバシー・バイ・デザインとは、プライバシー情報を扱うあらゆる場面において、プライバシー情報が適切に取り扱われる環境を予め作り込むというコンセプトのこと
 - * 3 『宴のあと』事件判決（東京地裁昭和 39 年 9 月 28 日）^[5]
 - * 4 日経新聞、「JR 東日本、「スイカ」履歴外販見送り 法整備まで」、電子版速報、2014 年 3 月 20 日、http://www.nikkei.com/article/DGXNASDZ200DQ_Q4A320C1TJ1000/
 - * 5 米連邦取引委員会（FTC：Federal Trade Commission）がオンラインプライバシーの保護に関するガイドラインとしてまとめた報告書（FTC Report）に記述されたパーソナルデータを第三者提供する際の指針

- 参考文献**
- [1] 首相官邸高度情報通信ネットワーク社会推進戦略本部，“パーソナルデータの利活用に関する制度改正大綱”，2014 年 6 月 24 日
 - [2] 第 13 回パーソナルデータに関する検討会 資料 1，“個人情報の保護に関する法律の一部を改正する法律案の骨子（案）”，内閣官房 IT 総合戦略室パーソナルデータ関連制度担当室，2014 年 12 月 19 日
 - [3] 総務省，“スマートフォン プライバシー イニシアティブ”，利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会 スマートフォンを経由した利用者情報の取扱いに関する WG 最終取りまとめ”，2012 年 8 月
 - [4] 総務省，スマートフォンを経由した利用者情報の取扱いに関する WG，第 1 回会議資料 4，“スマートフォンからの利用者情報の送信～情報収集の実態調査～”，KDDI 研究所，2012 年 1 月
 - [5] 升田 純，“現代社会におけるプライバシーの判例と法理”，青林書院，2009 年 10 月 26 日
 - [6] 独立行政法人産業技術総合研究所，“スマホアプリにおけるアプリケーション・プライバシーポリシー掲載状況の国際比較調査”，SCIS2014，2014 年 1 月
 - [7] 第 5 回パーソナルデータに関する検討会 資料 2-1，“技術検討ワーキンググループ報告書”，技術検討ワーキンググループ，2013 年 12 月 10 日
 - [8] 第 10 回パーソナルデータに関する検討会 資料 1-2，“技術検討ワーキンググループ報告書 ～「(仮称) 準個人情報」及び「(仮称) 個人特定性低減データ」に関する技術的観点からの考察について～”，技術検討ワーキンググループ，2014 年 5 月
 - [9] 堀部政男，JIPDEC，“プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流”，日経 BP 社，2012 年 10 月 29 日
 - [10] 閣議決定，“世界最先端 IT 国家創造宣言について”，2013 年 6 月 14 日，http://www.kantei.go.jp/jp/singi/it2/pdf/it_kokkasouzousengen.pdf
 - [11] 一般社団法人モバイル・コンテンツ・フォーラム，“スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン”，2012 年 11 月

上記脚注ならびに参考文献の URL は 2014 年 12 月 26 日現在での存在を確認。

執筆者紹介 八津川 直 伸 (Naonobu Yatsukawa)

1980 年日本電信電話公社入社，専用回線遠隔試験システムの施設設計，日本縦貫光ファイバー伝送システムの導入計画等を担当。1985 年日本ユニシス株式会社（当時，日本ユニバック株式会社）入社。電気通信事業の企画推進，汎用機の通信制御装置ソフトウェア（DCP/TELCON シリーズ）の開発および保守，セキュリティ商品の開発および保守，法務実務，客先向け J-SOX 対応支援ならびにシステム構築支援等を経て，モバイルセキュリティならびにパーソナルデータ取扱いにおけるプライバシー保護の研究に従事。現在，総合技術研究所インキュベーション室に所属。CISSP。

