国際規格(ISO/IEC)においては、プライバシーのフレームワークが規格化されており、当該規格では、「個人識別可能情報」(personally identifiable information、PII)という用語が使われています(ISO/IEC 29100:2011(Information technology –Security techniques – Privacy framework))。本ガイドラインは国際規格化を目指すものであり、国際規格の用語に従って、本ガイドラインでは「個人識別可能情報」という用語を使っています。個人識別可能情報とは、(1)当該情報に関連する特定の個人を識別するために使用できる、(2)直接的、間接的を問わず、特定の個人に関連し、または関連し得る情報をいいます。なお、本ガイドラインは、パーソナルデータを利活用する際に行う通知等に関しても参照可能なものです。

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

はじめに

ブロードバンド環境等の通信インフラの整備、スマートフォン等の個人の活動から情報を得る端末の普及、情報処理技術の向上等により、多種多様なデータを収集、分析することが可能になっている。このような技術向上を背景に、多種多様なデータを積極的に利活用することで、国民生活の利便性向上、新ビジネス創出、サービスの魅力・付加価値向上等の可能性が高まっている。一方において、近時はプライバシー意識の高い消費者が増加しており、組織による個人識別可能情報の取得や利活用が、プライバシーへの配慮が不十分であるとして批判を受けることがある。

組織による個人識別可能情報の利活用に対する批判は、「このような情報まで取られているとは思わなかった」とか、「このような使われ方をするとは思わなかった」といったことから発生しており、取得段階での個人識別可能情報の取扱いに関する情報提供や説明が、消費者の理解を得る上で、十分に機能を果たしていないことに原因がある。

本ガイドラインは、消費者向けのオンラインサービスを行う組織が、消費者から個人識別可能情報を取得し、利用する際に、消費者との信頼関係を構築する観点から、消費者に対する情報提供、説明の内容の適切性等について、指針を提供することを目的とするものである。本ガイドラインは、消費者の同意を得る様々な場面（個人識別可能情報の取得時、サービス利用開始時、サービス利用中等）において、組織が、消費者に提示すべき情報を消費者に誤解を与えることなく分かり易く提示するために求められる事項についての指針を示している。

本ガイドラインは、ISO/IEC 29100（ISO/IEC 29100:2011 (Information technology - Security techniques - Privacy framework)）におけるプライバシー原則のうち、第 7 原則「公開、透明性及び通知」及び第 1 原則「同意と選択」について、特に消費者向けオンラインサービスの局面に絞って、詳細な指針を提供しようとするものである。

1　適用範囲

本ガイドラインは、消費者向けオンラインサービスにおいて、個人識別可能情報を利用する組織が、消費者本人の同意を取得する際の手続を対象とする。あらゆる業種、規模の組織を対象とするものである。

本ガイドラインは、組織が、消費者本人の意思を有効に確認し、それと整合的に個人識別可能情報を取り扱うために設けるべき消費者の意思確認に関する手続を対象とする。具体的には、本人が自らの選択を行う上で必要な、組織による情報提供の内容やその提供の

仕方等であり、これらには以下のものが含まれる。

- 利用規約又はプライバシーポリシーとして提供される個人識別可能情報の取扱に関する記述内容を消費者にとって分かり易く表現した文書や画面表示
- 同意取得画面の在り方や、その遷移形態といったユーザインターフェース（UI）の観点を含めて、消費者本人の意思を確認するための手続。
- 細かな選択肢の有無、途中からの変更の容易さ、いわゆる「オプトアウト」の容易さなどの消費者本人の意思を事前又は事後に反映させるための手続。

2　用語及び定義

本ガイドラインにおいて使用する用語及び定義は、以下に定めるとおりとする。

2.1

明示的許可

同意を取得するために、同意についての何らかの行為を求めて、その行為があった場合に限って、同意されたものとして取扱う許可（本人の明示的な能動的な行為によって表明される許可）

NOTE:たとえば、「何々について同意（agree）する場合は、このようにしてください」（デフォルトオフで、オン選択など）というようにして取得することである。

2.2

暗黙的許可

同意を取得するために、同意しないための何らかの行為を求めて、その行為がなかった場合に、同意されたものとして取扱う許可

NOTE: たとえば、「何々について同意しない場合は、このようにしてください」（デフォルトオンで、オフ選択など）というようにして取得することである。

3　通知と同意・選択に関する基本的事項

3.1　通知の義務

3.1.1　通知が必要な場合

個人識別可能情報を取得する場合には、3.2 に定める通知内容を適切に通知すること。

3.1.2　適切な認識

本人が認識できるように通知すること。

3.1.3　適切な表現

本人にとって理解できる分かりやすい表現で通知すること。

3.1.4　適切な時

個人識別可能情報を取得する前に通知すること。

3.1.5　適切な箇所

個人識別可能情報を取得する際に本人が気付きやすい箇所で通知すること。

3.1.6　随時の参照

本人に通知した内容を、通知した時以後も本人が容易に参照できるようにすること。

3.2　通知内容

3.2.1　サービスの概要

提供するサービスの概要を通知すること。

3.2.2　取得及び利用主体

個人識別可能情報を取得及び利用する主体を、本人が特定して識別できるように具体的に通知すること。

3.2.3　取得する個人識別可能情報の項目

a) 取得する個人識別可能情報の項目が何であるかわかるように通知すること。取得の状況から取得する個人識別可能情報の項目が何であるか本人にとって自明の場合であっても、その項目を通知すること。

※ 個人識別可能情報の項目とは、個人識別可能情報を項目ごとに分けた氏名、住所、電話番号などのことを言う。すなわち、「個人情報を取得します」ではなく、「氏名、住所及び電話番号を取得します」というように通知する必要がある。仮に、取得の状況から住所だけを取得していることが自明であっても、「個人情報を取得します」ではなく、「住所を取得します」と通知する必要がある。

b) 機微情報を取得する場合は、法的根拠を通知すること。

3.2.4　取得方法

a) 個人識別可能情報の取得方法を通知すること。個人識別可能情報の項目ごとに取得方法が異なる場合には、それを分けて通知すること。

b) 個人識別可能情報の取得方法について、本人にとって分かりにくいものを明確に通知すること。

c) 個人識別可能情報の項目ごとの取得方法のうち、プライバシー・インパクトの異なるものを区分して通知すること。

3.2.5　取得理由

個人識別可能情報を取得する時の状況から判断して、本人にとって気付きにくい利用目的について、その必要性を明確に通知すること。

3.2.6　取得の予定時間

通知から長時間経過してから個人識別可能情報を取得する場合には、個人識別可能情報をいつ取得するのかを通知すること。

3.2.7　利用目的

a) 取得する個人識別可能情報の利用目的を特定し、具体的に通知すること。個人識別可能情報の項目ごとに利用目的が異なる場合には、それを分けて通知すること。取得した個人識別可能情報を利用しない場合には、その旨を通知すること。

b) 個人識別可能情報の利用目的を、個人識別可能情報項目と対応して通知すること。個

人識別可能情報の利用目的のうち、プライバシー・インパクトの大きいものを先に表示して通知すること。

※ 個人識別可能情報の利用目的のうち、本人にとって自明なものは省略して通知することができる。

3.2.8　利用方法

取得する個人識別可能情報を無加工で利用するのか、加工して利用するのかを通知すること。

※ 取得する個人識別可能情報を加工して利用する場合は、その加工方法を通知することが望ましい。

3.2.9　第三者への提供

a) 個人識別可能情報を第三者に提供する場合があるか否かについて通知すること。

b) 個人識別可能情報を第三者に提供する場合には、提供先を通知すること。

※ 提供先を個別に特定して通知することが望ましいが、提供先の範囲を特定して通知することもできる。

c) 個人識別可能情報を第三者に提供する場合には、提供先における利用目的を本人に通知すること。

3.2.10　保存期間、廃棄

a) 個人識別可能情報の廃棄の予定について、

1) 削除の依頼があるまで廃棄しない旨、

2) 保存期間、又は

3) 廃棄期日

のいずれかを通知すること。

3.2.11　本人による関与

a) 個人識別可能情報の開示について本人が依頼できること及びそのための手段を、通知すること。

b) 個人識別可能情報の利用停止について本人が依頼できること及びそのための手段を、通知すること。

c) 個人識別可能情報の訂正について本人が依頼できること及びそのための手段を、通知すること。

d) 個人識別可能情報の削除について本人が依頼できること及びそのための手段を、通知すること。

e) 個人識別可能情報の提供停止について本人が依頼できること及びそのための手段を、通知すること。

f) 同意の撤回について本人が依頼できること及びそのための手段を、通知すること。

g) 本人が組織による個人識別可能情報の取得又は利用・提供の状況を、いつでも確認できることとして通知すること。

h) 本人による同意の状況を、いつでも確認できることとして通知すること。

3.2.12　問合せ先

a) 個人識別可能情報に関する問い合わせ先を通知すること。

3.3　同意及び選択

3.3.1　表示に基づく同意

意思確認をする場合には、意思確認の内容について、本人がわかるように、具体的に表示すること。

3.3.2　主体

意思確認をする場合には、具体的に誰又はどの ID に対して意思確認をしようとしているのか表示すること。

※ 誰として同意しようとしているのかの表示を行うべきである※　昨今のシステムでは、多くの場合、一つのログインクレデンシャルで複数のアカウント／アイデンティティ／立場を使い分けることが多くなってきている。どの立場での同意かというのは非常に重要な事で、これを混同させることによって、不当な同意を取得するような攻撃も考えられる。したがって、「どの立場として」同意しようとしているのかを明示すべきである。

3.3.3　選択

意思確認をする場合には、本人に選択の機会を与え、明示的許可又は暗黙的許可を得ること。

※ 明示的許可を得ることが望ましいが、暗黙的許可を得ることもできる。ただし、何らかの行為による選択の機会を提供せずに、「同意したものとみなします」と記載だけする方法（いわゆる、みなし同意）によっては許可を得たものとして取扱わない。

3.3.4　独立性

意思確認をする場合には、プライバシーに関する事項を独立して許可を得ること。

※ プライバシーに関係しない別のことと一緒に許可を得た場合、プライバシーに関する許可を得たものとして取扱わない。

3.3.5　必然性

意思確認をする場合には、他の内容と比べてプライバシー・インパクトが異なる項目については、個別に意思確認をすること。

※ プライバシー・インパクトが同程度の複数の項目については、まとめて意思確認をすることができる。

3.3.6　頻度

意思確認をする場合には、適切な頻度で意思確認をすること。

※ あまりに頻度の高い状態で意思確認を求めることは、何についての意思確認であるかを本人が見落とす可能性が増す（クリックトレーニングとなる）場合がある。それを防ぐために、不必要に高い頻度で意思確認をすべきではない。

3.3.7　適時性

意思確認をする場合には、適切なタイミングで意思確認をすること。

※ あまりに早い時期に意思確認を求めることは、本人にとって、それが何の意思確認かを推定しにくく事実上は同意をせざるを得ない場合がある。それを防ぐために、あまりに早い時期に意思確認をしてはならない。

3.4　取得時に通知（notice）した内容を変更するために必要な意思確認

3.4.1　サービスの概要

個人識別可能情報を取得するときに本人に通知したサービスの概要を変更する場合には、本人から同意を取得すること。

3.4.2　取得および利用主体

個人識別可能情報を取得するときに本人に通知した個人識別可能情報を取得及び利用する主体を変更する場合には、本人から同意を取得すること。

3.4.3　取得する個人識別可能情報の項目

個人識別可能情報を取得するときに本人に通知した個人識別可能情報の項目を変更する場合には、本人から同意を取得すること。

※ 取得する個人識別可能情報の項目を減らす場合には、その変更について本人から同意を取得する必要はないが、それによってサービスの概要に変更がある場合には、そのサービス概要の変更について、本人から同意を取得する必要がある。

3.4.4　取得方法

個人識別可能情報を取得するときに本人に通知した取得方法を変更する場合には、本人から同意を取得すること。

3.4.5　取得の予定時間

個人識別可能情報を取得するときに本人に通知した取得の予定時間を変更する場合には、本人から同意を取得すること。

3.4.6　利用目的

個人識別可能情報を取得するときに本人に通知した利用目的の範囲外に変更する場合には、本人から同意を取得すること。

※ 利用目的を狭くする場合には、その変更について本人から同意を取得する必要はないが、それによってサービスの概要に変更がある場合には、そのサービス概要の変更について、本人から同意を取得する必要がある。

3.4.7　利用方法

個人識別可能情報を取得するときに本人に通知した利用方法を変更する場合には、本人から同意を取得すること。

※ 無加工で利用するとしていた個人識別可能情報を加工して利用する場合には、その変更について本人から同意を取得する必要はないが、それによってサービスの概要に変更がある場合には、そのサービス概要の変更について、本人から同意を取得する必要

がある。

3.4.8　第三者提供の有無

個人識別可能情報を取得するときに本人に通知した第三者提供に関することを変更する場合には、本人から同意を取得すること。

※ 提供先について個人識別可能情報を取得するときに本人に提供先の範囲を通知しており、その範囲内で提供先だけを変更する場合には、本人から同意を取得しないで変更することができる。

※ 通知した提供先への以後の提供を終了し、または、通知した提供先の範囲を狭くする場合には、その変更について本人から同意を取得する必要はないが、それによってサービスの概要に変更がある場合には、そのサービス概要の変更について、本人から同意を取得する必要がある。

3.4.9　保存期間、廃棄

個人識別可能情報を取得するときに本人に通知した保存期間又は廃棄期日を保存期間が長くなるように変更する場合には、本人から同意を取得すること。

※ 保存期間又は廃棄期日を短くする場合でも、サービスの提供期間中に保存期間又は廃棄期日を迎える場合で、それによってサービス概要の変更があるときは、そのサービス概要の変更について、本人から同意を取得する必要がある。例えば、一定の期間又はサービスの提供終了後にも個人識別可能情報を保存することを契約事項としていた場合やサービス概要として通知していた場合は、その変更がサービス概要への変更であるといえることから、当該サービス概要の変更について、本人から同意を取得する必要がある。

3.4.10　本人による関与項目

個人識別可能情報を取得するときに本人に通知した開示、利用停止、訂正、削除、提供停止及び同意の撤回に関することを変更する場合には、本人から同意を取得すること。

3.4.11　問合せ先

個人識別可能情報を取得するときに本人に通知した問合せ先を変更する場合には、本人から同意を取得すること。

※ なお、問い合わせの方法を変更せずに単にその宛先のみを変更する場合で、本人からのアクセス可能性について変更がない場合（単に問い合わせ先電話番号やメールアドレスを変更する場合など）や問い合わせの方法を変更した場合でも、たとえば、メールでの送信からメールフォームでの送信に変更しそれによって本人からのアクセス可能性に変更がないときは、本人から同意を取得しないで変更することができる。

4　消費者本人の意思確認のためのユーザーインターフェースに関する事項

4.1　全項目通知の方法

4.1.1 表示項目の順序に関する事項

意思確認を得るための通知をする際には、3.2 の各項目を 3.2 の順序で表示すること。表示にあたっては、3.2 の各項目を各行の見出しとして、対応する項目の値とする表形式で表示することが望ましい。

※ 該当する値が無いときには、その行は省略することができる。表示する画面が小さすぎて表形式で重要な事項全てを記載できない時には、テキスト形式で表記することができる。ただし、順序は変えてはならない。

※ 表形式を用いて一定の順序で表示し続けることは、複数の事例の横比較が容易になるメリットが有り、消費者が自らの意志を生成するのに役立つ。

例：

個人識別可能情報利用に係る通知	
サービス概要	移動履歴地図サービス
利用主体	Example 株式会社
提供する個人情報	メールアドレス 位置情報
取得方法	記録ボタンをおした時
利用目的	移動履歴を地図にしてあなたに提供するため
第三者提供	いたしません
保存期間・廃棄	半年間保存の後廃棄
本人による関与	以下から、保存されている情報の参照、訂正他ができます。 http://example.com/maps/
問い合わせ先	Tel: 03-0000-0000 email: info@example.com https://example.com/info/

図 1 － 表形式の通知

例：項目名を省略する場合

図 2 － 項目名を省略した通知

4.1.2　表示量に関する事項

消費者ができるだけ短時間で読むことができる内容を少ない画面数で表示することが望ましい。表示量を押さえる関係上、当該画面には全てを表示することはできないことが想定される。その場合には、要約表示をまず行う必要がある。

取得する個人識別可能情報の項目の表示にあたっては、プライバシーへの影響が異なるものについては、消費者がその違いを明確に意識できるように、プライバシー影響度グループごとに分けて表示することが望ましい。

当該画面で割愛された情報を含む詳細は、その時点で消費者が希望すれば参照できるようにする必要がある。

※ 電子的な通知の場合は、ポップアップ、ドリルダウンなどの方法が考えられる。

※ 消費者に多量の契約文章を読むように仕向けることは難しい。これは、消費者が今まさに何らかの処理を行おうとしている時にはなおさらである。

4.1.3　具体的値の表示に関する事項

可能な場合には、取得する個人識別可能情報の項目の値を通知時に表示すべきである。

※ 例えば、「電話番号」と通知するのではなく、「電話番号：03-1234-5678」と通知する

ことである。具体的値を表示できない場合には、例示をする必要がある。これらの値の表示は、当該画面からのリンクをたどることによって表示される形にしてもよい。

※ 取得する個人識別可能情報の項目名が表示されても、消費者にはそれが何を意味するか理解できない可能性がある。このような状況に対応するために、具体的な値を表示するリンクを各項目に表示することが望ましい。

※ ある処理を許可することによって新たな個人識別可能情報が生成される場合には、同意前に実際の値を表示することは不可能である。その場合は例示を行うのが望ましい。例えば、ショッピングを行った時の購買データを提供するというような場合、消費者が会員になる段階ではショッピングはまだ行っていないので、具体的な購買データは存在しない。そのような場合は、例としての購買データを示し、どのようなものが提供されるのかに関しての消費者の理解を得るのが望ましい。

例：

図 3 － 具体的情報の表示

例：例示を行う場合

お客様にご提供いただくのは、お客様が購入された物品のレシート情報です。

以下の様な情報が弊社に送られます。

```
Example Pharmacy

Date:2014-08-27 15:04:01
Store ID: 1234
Customer ID: 989814501

 Item       Qty     Prc
---------- ---- --------
Rose Soap    10     58.00
SleepNow      1     24.50

Subtotal           82.50
Tax (18%)          14.85
Total              97.35
```

図 4 – 例示を行う場合

4.1.4　機械可読性と表示形式に関する事項

電子的に表示する場合は、表示を担当するソフトウェアが当該条件を読み込んで、消費者の好みに最適化して表示をしたり、消費者の判断を補佐したりすることができるように、機械可読な形式で提供されることが望ましい。これを消費者が理解できる形で表示するにあたっては、画像・アイコン等を援用してわかりやすさを求めることも可とする。

※ 画像等の解釈は文化的背景によって大きく異なる可能性があることに留意すべきである。消費者に混乱を産まないためには、その地域・文化圏における標準を別途定めることが望ましい。

※ このようにすることにより、受け取った機器側で適宜選択して表示するなどということも可能になる。

4.1.5　アクセシビリティに関する事項

表示する際には、消費者の希望によって、ISO/IEC 40500 Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0 にもとづいたアクセシブルな表示を行うことができるようにすることが望ましい。

4.2 差分通知の方法

3.4 にもとづく同意を取得しようとした場合には、前回取得した同意の内容に消費者がその時点でその画面からアクセスできることを条件として、前回との差分のみを通知するこ

とができる。ただし、これにあたっては、消費者を必要な保証水準で認証して消費者を識別し、これに基づき差分を抽出する必要がある。

4.3 同意および選択の方法

4.3.1 同意するものの識別状態の表示

同意を得ようとするものをどのように認識しているかを、消費者にわかりやすく表示すること。

※ どのような同意であっても、それはある一定の立場にもとづいて行われる。その立場毎に、複数の identity を一つのクレデンシャルに紐付けて運用している消費者も多数いる。このような時に、この立場を混同させ、よりプライバシー・インパクトが高くなるような立場での同意を詐取するという攻撃は十分に想定できる。したがって、消費者がどの立場で同意しようとしているのかを、分かりやすい形で明示的に表示するのは重要である。

4.3.2 同意の行為

4.1 で表示した項目に関する明示的許可の取得にあたっては、消費者の能動的な行動によること。同意を取得する画面は、4.1 を通知する画面と同一の画面であるのが望ましい。

※

※ 能動的な行為とは、消費者が自らの意志によって起こさなければならない行為を指す。たとえば、チェックボックスをクリックする、ボタンを押す、スライドバーをスライドする、などのユーザーインターフェースが考えられる。

※ これらの行為を行う画面と、表示が別れてしまうと、消費者は何に対して同意をしているのかが分からなくなるおそれがある。したがって、同意をする対象条件である 4.1 の内容は、同一画面に出すのが望ましい。

4.3.3 同意の独立性

4.1 で表示した項目に関する同意は、他と独立した行為を通じて取得すること。

※ 多数のプライバシー以外の同意項目の中に、プライバシーに関係する同意を紛らせて同意を取得しようとする攻撃は十分想定しうる。これを避けるために、プライバシー関連の同意は、他の同意とは分けて取得すべきである。

4.3.4　同意内容の事後的参照

消費者が同意した内容に希望時に参照できるように、任意の時に参照できるような適切な手段で消費者に通知すること。

※ この際に使う手段は、消費者が、事後的に、任意の時に参照できるような手段を使うべきである。

※ 後から同意が撤回可能な場合は、その手段も合わせて通知すべきである。