# モバイルコンテンツ関連事業者のための
# 個人情報保護ガイドライン

## 第 3 版

2018 年 10 月

一般社団法人モバイル・コンテンツ・フォーラム

本ガイドラインは、モバイルコンテンツ関連事業者において推奨される個人情報の取り扱い並びに保護の方法について記述したものです。一般社団法人モバイル・コンテンツ・フォーラムは、当法人がプライバシーマークの審査を行う際に、本ガイドラインの遵守を条件とします。また、それ以外のモバイルコンテンツ関連事業者においても、本ガイドラインの遵守を推奨します。

本ガイドラインは、下記の各規範（以下、「その他の規範」といいます）を補足するものです。従って本ガイドラインに従う際には、必要に応じて下記の各規範も満たすことを求めるものです。

- 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）最終改正：平成 28 年 5 月 27 日法律第 51 号
- 「政令」 個人情報の保護に関する法律施行令（平成 15 年 12 月 10 日政令第 507 号）最終改正：平成 28 年 10 月 5 日政令第 324 号
- 「基本方針」 個人情報の保護に関する基本方針（平成 16 年 4 月 2 日閣議決定）
- 平成 28 年 10 月 28 日一部変更
- 「規則」 個人情報の保護に関する法律施行規則（平成 28 年 10 月 5 日個人情報保護委員会規則第 3 号）
- 「ガイドライン」個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年 11 月 30 日個人情報保護委員会告示第 6 号）
- 個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）（平成 28 年 11 月 30 日個人情報保護委員会告示第 7 号）
- 個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）（平成 28 年 11 月 30 日個人情報保護委員会告示第 8 号）
- 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）（平成 28 年 11 月 30 日個人情報保護委員会告示第 9 号）
- 電気通信事業における個人情報保護に関するガイドライン（平成 29 年 4 月 18 日総務省告示第 152 号）
- 個人情報保護マネジメントシステムー要求事項（JIS Q 15001：2017）
- プライバシーマーク付与適格性審査基準（2018 年 1 月 (一財)日本情報経済社会推進協会 プライバシーマーク推進センター）
- 特定電子メールの送信の適正化等に関する法律（平成 14 年 4 月 17 日法律第 26 号）
- 不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号）
- 特定商取引に関する法律（昭和 51 年 6 月 4 日法律第 57 号）
- スマートフォン プライバシー イニシアティブ ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー（平成 24 年 8 月 総務省「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（平成 24 年 11 月 13 日 一般社団法人モバイル・コンテンツ・フォーラム）

１）適用範囲

本ガイドラインは、個人情報の定義として個人情報保護法の定義を採用します。
すなわち「生存する『個人に関する情報』であって、『当該情報に含まれる氏名、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（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）』（法第 2 条第 1 項第 1 号）、又は『個人識別符号が含まれるもの』（同項第 2 号）」を個人情報とします。
「個人に関する情報」とは、氏名、住所、性別、生年月日、顔画像等個人を識別する情報 に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問いません。
以下に、モバイルコンテンツ関連事業者の業務内容に関連して個人情報に該当するものと該当しないものを例示します。

【個人情報に該当する事例】
事例 1）本人の氏名
事例 2）生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
事例 3）防犯カメラに記録された情報等本人が判別できる映像情報
事例 4）本人の氏名が含まれる等の理由により、特定の個人を識別できる音声録音情報
事例 5）特定の個人を識別できるメールアドレス（kojin_ichiro@example.com 等のようにメールアドレスだけの情報の場合であっても、example 社に所属するコジンイチロウのメールアドレスであることが分かるような場合等）
事例 6）個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できる場合は、その時点で個人情報に該当する。）
事例 7）官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS（ソーシャル・ネットワーク・サービス）等で公にされている特定の個人を識別できる情報

【個人情報に該当しない事例】
事例１）企業の財務情報等、法人等の団体そのものに関する情報（団体情報）
事例２）記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@xyzisp.ne.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となります)
事例３）特定の個人を識別することができない統計情報（アンケート集計結果など）
事例４）本人が自由に入力することができるニックネームなど（特定の個人を識別できない場合のみ）
事例５）UID／契約者固有番号／端末識別番号、システムログ、IP アドレスなど（他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となります）

２）本人の同意

本ガイドラインは、本人の同意に関してその他の規範と同等の規定を採用します。以下に本人の同意の得ている事例を例示します。

【本人の同意を得ている事例】

事例１）本人からの同意する旨のメールを受信すること。

事例２）本人による同意する旨のウェブ画面上のボタンのクリック

事例３）本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

【推奨される事例】

事例１）子どもまたは事理を弁識する能力を欠く者（未成年者もしくは成年被後見人、被保佐人または被補助人など、その判断力に懸念があると考えられる者）から同意を得る場合には、法定代理人からも同意を得る必要があります。この対策として、登録前の段階で保護者の同意を得るための注意書き（例：「未成年のお客様は保護者の方と一緒に登録してください」「みせいねんのおきゃくさまはほごしゃのかたといっしょにとうろくしてください」）を表示し、本人の目に入るようにすることを推奨します。

３）利用目的の特定

本ガイドラインは、利用目的の特定としてその他の規範と同等の規定を採用します。なお利用目的を特定した場合には、当然ながら、その後その利用目的以外の目的に個人情報を使用することはできません。将来的に自社サービスの告知などを行う予定があるのであれば、「その他の自社サービスの告知のため」などと利用目的に盛り込んでおく必要があります。

４）本人から直接書面によって取得する場合の措置

本ガイドラインは、本人から直接書面によって取得する場合の措置として JIS Q 15001：2017 と同等の規定を採用します。本人から直接書面によって取得する場合には、下記の a)から h)の項目（以下、「個人情報取得時の明示事項」とします）をあらかじめ，書面（電子的方式、磁気的方式など他人の知覚によっては認識することができない方式で作られる記録を含む。以下、同じ）によって本人に明示し，書面によって本人の同意を得なければなりません（JIS Q 15001：2017 における例外事項を除きます）

なお、この場合に下記の a)から h)の項目を含まない個人情報保護方針を明示しているケースが散見されますが、これでは明示したことにはならないので、注意してください。

a) 事業者の氏名又は名称

b) 個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先
c) 利用目的
d) 個人情報を第三者に提供することが予定される場合の事項
－ 第三者に提供する目的
－ 提供する個人情報の項目
－ 提供の手段又は方法
－ 当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性
－ 個人情報の取扱いに関する契約がある場合はその旨
e) 個人情報の取扱いの委託を行うことが予定される場合には，その旨
f) JIS Q 15001:2017 の A.3.4.4.4～A3.4.4.7 に該当する場合には，その請求などに応じる旨及び問合せ窓口
g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果
h) 本人が容易に認識できない方法によって個人情報を取得する場合には，その旨

以下にそれぞれを例示します。

【本人から直接書面によって取得する場合の事例】
事例１）携帯電話のキー操作などの方法により、本人から個人情報を取得する場合

【a)から h)の項目の明示に該当する事例】
事例１）本人がアクセスした自社のウェブ画面上、又は本人の端末装置上に個人情報取得時の明示事項を明記すること（ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等に個人情報取得時の明示事項が本人の目にとまる（個人情報取得時の明示事項が示された画面に１回程度の操作でページ遷移するよう設定したリンクやボタンを含む）ようその配置に留意する必要があります）

【推奨される事例】
事例１）チラシや広告などの文面上にメールアドレスを記載したり、商品に貼付した QR コードから、いわゆる「空メール」で個人情報を取得する場合、事前に個人情報取得時の明示事項を明示することが望ましいが、スペースなどの都合からそれが困難な場合には、空メールを受け付けた後の画面遷移の中で a)から h)の事項を明示し、本人の同意を得ることを推奨します。また、空メールで取得したメールアドレスは一時的な情報として保持し、個人情報取得時の明示事項の明示、ならびに本人の同意を得ることができなかった場合には、その後使用せず、削除することを推奨します。

５）個人情報を本人から直接書面によって取得する以外の方法によって取得した場合の措置

本ガイドラインは、本人から直接書面によって取得する以外の方法によって取得した場合の措置として JIS Q 15001：2017 と同等の規定を採用します。本人から直接書面によって取得する以外の方法によっ

て取得する場合には、あらかじめその利用目的を公表している場合を除き，速やかにその利用目的を，本人に通知し，又は公表しなければなりません。（JIS Q 15001：2017 における例外事項を除きます）

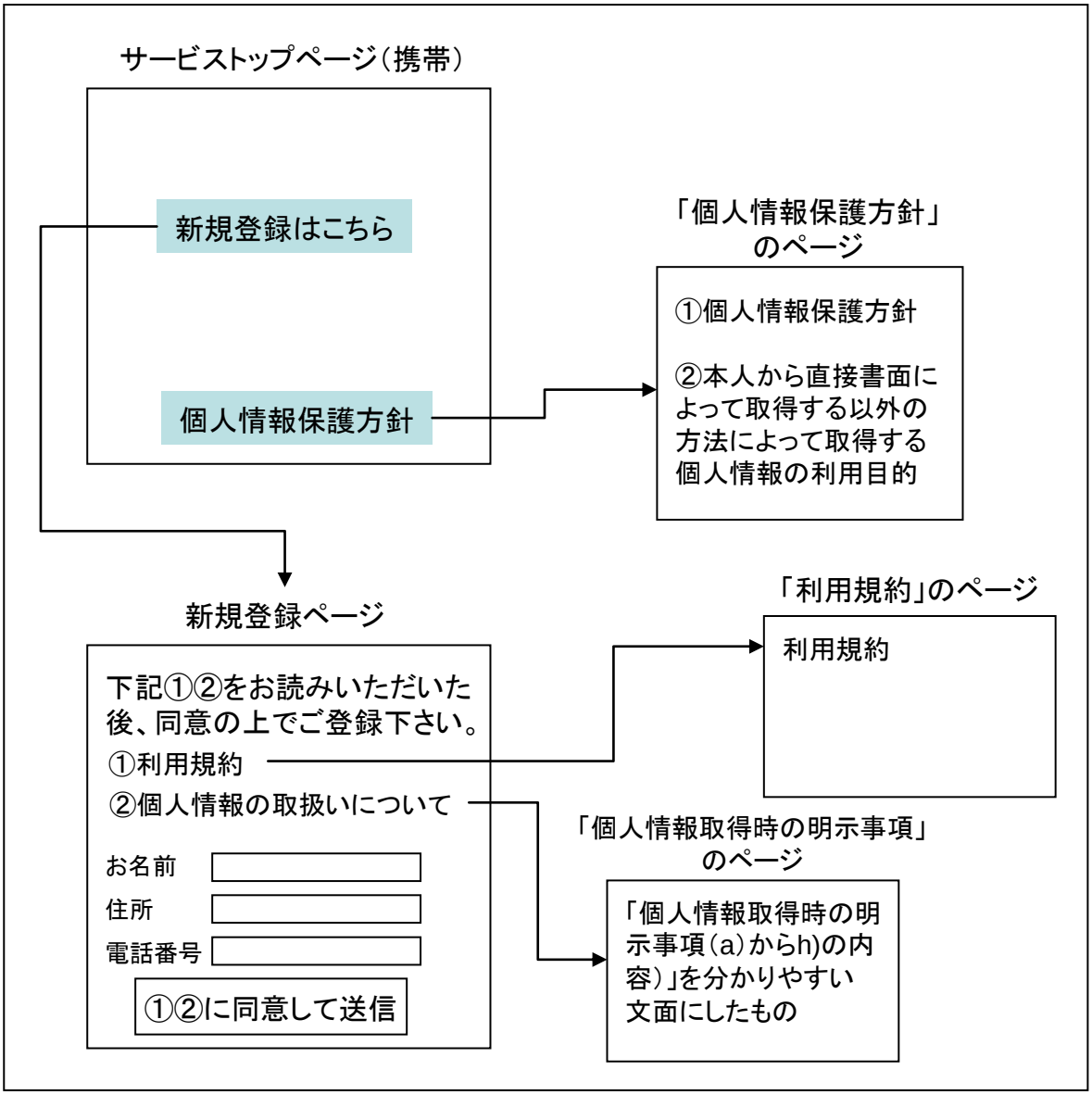
なお、この場合に利用目的を含まない個人情報保護方針を通知または公表しているケースが散見されますが、これでは通知または公表したことにはならないので、注意してください。

【個人情報を本人から直接書面によって取得する以外の方法によって取得する事例】
事例１）インターネット上で本人が自発的に公にしている個人情報を取得する場合
事例２）インターネット、官報、職員録等から個人情報を取得する場合
事例３）電話による問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除きます）
事例４）個人情報の第三者提供を受ける場合
事例５）個人情報の取扱いの委託を受けて、個人情報を取得する場合
事例６）携帯キャリアより受け取る利用料金未払い者の個人情報
事例７）「お友達紹介キャンペーン」などにおいて、既存顧客から知り合いの個人情報を取得する場合
事例８）監視カメラなどで撮影された映像を取得する場合

【本人への通知に該当する事例】
事例１）電子メール等により送信すること。
事例２）郵送物等により通知すること。

【公表に該当する事例】
事例１）自社の携帯サイトのトップページから１回程度の操作で到達できる場所への掲載
事例２）自社のウェブ画面中のトップページから１回程度の操作で到達できる場所への掲載

【４） ５）の規定を満たすための推奨される画面遷移】




注１）「個人情報保護方針」のページの①②の内容は、「公表」することが求められています。「公表（広く一般に知らせる）」の方法は、事業の性質および個人情報の取り扱いの状況に応じ、合理的かつ適切な方法によることが求められており、必ずしも携帯サービスの全てのトップページに記載しなければならないわけではありません。

注２）「利用規約」と「個人情報取得時の明示事項」を一つの文書にまとめることは、「明示（明らかに示す）」の要件を満たさなくなる可能性があるため、「利用規約」と「個人情報取得時の明示事項」は別の文書にすることを推奨します。

６）提供に関する措置

本ガイドラインは、個人情報を第三者に提供する場合の措置として JIS Q 15001:2017 と同等の規定を採

用します。携帯サイトの画面上で他の会員の個人情報を表示させることは、これにあたることが考えられますので、よく注意して対応してください。

モバイルコンテンツ関連事業において、複数社で共同してサービスを運営する場合などにおいて、「個人情報の共同利用」を行う場合があります。この場合には、JIS Q 15001:2017 の 3.4.2.8 の例外事項 f)に従って必要事項を「本人が容易に知り得る状態」に置く（本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置く）必要がありますので、ご注意ください。

７）正確性の確保

本ガイドラインは、正確性の確保の措置としてその他の規範と同等の規定を採用します。以下に正確性の確保が十分な場合を例示します。

【正確性が確保されている事例】

事例１）週に 1 回定期的にメールマガジンを配信している場合、本人からのメールアドレスの変更の連絡があった場合には、最低でも週に 1 回は配信先メールアドレスの洗い替えを行うことで、古いアドレスに配信されることがあったとしてもそれは変更後の１回だけにとどまっている場合。

事例２）パスワード認証を行って本人を認証している場合には、本人がパスワード変更の処理を行った場合には、リアルタイムに認証用データベースに反映することにより、変更の時点から新しいパスワードを使用した認証が行われるようにしている場合。（メンテナンスなどによりサービス自体が停止する場合を除く）

８）安全性の確保

モバイルコンテンツ関連事業者は、自社の提供するモバイルコンテンツサービスで使用する個人情報が漏えいなどする事態を起こさないように、特段の対策を行わなければなりません。そのため、下記のとおり、個人情報保護委員会「個人情報保護法ガイドライン（通則編）」に準拠して安全性の確保の方法を例示します。

安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られません。

なお、中小規模事業者（※1）については、その他の個人情報取扱事業者と同様に、法第 20 条に定める安全管理措置を講じなければなりませんが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るような手法の例を示すこととします。もっとも、中小規模事業者が、その他の個人情報取扱事業者と同様に「手法の例示」に記述し

た手法も採用することは、より望ましい対応であります。

（※1）「中小規模事業者」とは、従業員（※2）の数が 100 人以下の個人情報取扱事業者をいいます。ただし、次に掲げる者を除く。

・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 月以内のいずれかの日において 5,000 を超える者

・委託を受けて個人データを取り扱う者

（※2）中小企業基本法（昭和 38 年法律第 154 号）における従業員をいい、労働基準法（昭和 22 年法律第 49 号）第 20 条の適用を受ける労働者に相当する者をいいます。ただし、同法第 21 条の規定により同法第 20 条の適用が除外されている者は除く。

なお、下記の基準において、モバイルコンテンツサービスの認証やオンライン処理などに利用する個人情報を「サービス用個人情報」といいます。

【望ましい手法の例示】

| 講じなければならない措置 | 手法の例示 | 中小規模事業者における手法の例示 |
|---|---|---|
| 個人データの取扱いに係る規律の整備 | | |
| ○個人データの取扱いに係る規律の整備 | 取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定することが考えられる。なお、具体的に定める事項については、以降に記述する組織的安全管理措置、人的安全管理措置及び物理的安全管理措置の内容並びに情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）は技術的安全管理措置の内容を織り込むことが重要である。 | ・個人データの取得、利用、保存等を行う場合の基本的な取扱方法を整備する。 |
| 組織的安全管理措置 | | |
| （1）組織体制の整備 | （組織体制として整備する項目の例）<br>・個人データの取扱いに関する責任者の設置及び責任の明確化<br>・個人データを取り扱う従業員及 | ・個人データを取り扱う従業者が複数いる場合、責任ある立場の者とその他の者を区分する。 |

| | | |
|---|---|---|
| | びその役割の明確化<br>・上記の従業者が取り扱う個人データの範囲の明確化<br>・法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制<br>・個人データの漏えい等の事案の発生又は兆候を把握した場合の責任者への報告連絡体制<br>・個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化 | |
| (2) 個人データの取扱いに係る規律に従った運用 | 個人データの取扱いに係る規律に従った運用を確保するため、例えば次のような項目に関して、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすることが考えられる。<br>・個人情報データベース等の利用・出力状況<br>・個人データが記載又は記録された書類・媒体等の持ち運び等の状況<br>・個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。）<br>・個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等） | ・あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。 |
| (3) 個人データの取扱状況を確認する手段の整備 | 例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可 | ・あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が |

| | | |
|---|---|---|
| | 能とすることが考えられる。<br>・個人情報データベース等の種類、名称<br>・個人データの項目<br>・責任者・取扱部署<br>・利用目的<br>・アクセス権を有する者　等 | 確認する。 |
| (4) 漏えい等の事案に対応する体制の整備 | 漏えいなどの事案の発生時に例えば次のような対応を行うための、体制を整備することが考えられる。<br>・事実関係の調査及び原因の究明<br>・影響を受ける可能性のある本人への連絡<br>・個人情報保護委員会等への報告<br>・再発防止策の検討及び決定<br>・事実関係及び再発防止策等の公表　等 | ・漏えい等の事案の発生時に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。 |
| (5) 取扱状況の把握及び安全管理措置の見直し | ・個人データの取扱状況について、定期的に自ら行う点検又は他部署などによる監査を実施する。<br>・外部の主体による監査活動と合わせて、監査を実施する | 責任ある立場の者が、個人データの取扱状況について、定期的に点検を行う。 |
| 人的安全管理措置 | | |
| ○従業者の教育 | ・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。<br>・個人データについての秘密保持に関する事項を就業規則等に盛り込む。 | （同左） |
| 物理的安全管理措置 | | |
| (1) 個人データを取り扱う区域の管理 | （管理区域の管理手法の例）<br>・入退室管理及び持ち込む機器等の制限等<br>なお、入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 | ・個人データを取り扱うことのできる従業者<br>及び本人以外が容易に個人データを閲覧等<br>できないような措置を講ずる。 |

| | | |
|---|---|---|
| | （取扱区域の管理手法の例）<br>・壁又は間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止 | |
| (2) 機器及び電子媒体等の盗難等の防止 | ・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。<br>・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。 | （同左） |
| (3) 電子媒体等を持ち運ぶ場合の漏えい等の防止 | ・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。<br>・封緘、目隠しシールの貼付けを行う。<br>・施錠できる搬送容器を利用する。 | ・個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。 |
| (4) 個人データの削除及び機器、電子媒体等の廃棄 | （個人データが記載された書類等を廃棄する方法の例）<br>・焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。<br>（個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例）<br>・情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。<br>・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を | ・個人データを削除し、又は、個人データが記<br>録された機器、電子媒体等を廃棄したこと<br>を、責任ある立場の者が確認する。 |

| | | |
|---|---|---|
| | 採用する。 | |
| 技術的安全管理措置 | | |
| (1) アクセス制御 | ・個人情報データベース等を取り扱うことのできる情報システムを限定する。<br>・情報システムによってアクセスすることのできる個人情報データベース等を限定する。<br>・ユーザーID に付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。 | ・個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。 |
| (2) アクセス者の識別と認証 | （情報システムを使用する従業者の識別・認証手法の例）<br>・ユーザーID、パスワード、磁気・IC カード等 | ・機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。 |
| (3) 外部からの不正アクセス等の防止 | ・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。<br>・情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。<br>・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。<br>・ログ等の定期的な分析により、不正アクセス等を検知する。 | ・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。<br>・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。 |
| (4) 情報システムの使用に伴う漏えい等の防止 | ・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。<br>・個人データを含む通信の経路又は内容を暗号化する。 | ・メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。 |

| | | |
|---|---|---|
| | ・移送する個人データについて、パスワード等による保護を行う。 | |

付則

1. スマートフォン等におけるアプリケーション配信事業に関する付則

スマートフォン等におけるアプリケーション配信事業を行う場合は、以下のように利用者情報の取扱いを行ってください。

スマートフォン等の利用者情報への対応については、関係省庁含め関係機関において普及が進展中であることを考慮して、プライバシーマーク制度においても積極的に情報提供を行い周知していくとともに、審査の際に確認を行います。個人情報保護リスクに対して未対応部分がある場合には残留リスクとして把握し、管理するとともに、個人情報保護リスクの見直しを通じて必要がある場合には、未対応のままとせず、対応に着手してください。

(1) スマートフォン等の利用者情報

スマートフォンは、携帯電話端末として常に電源を入れてネットワークに接続した状態で使用するため、PC に比べて利用者との結びつきが強い。利用者の行動履歴や通信履歴等の多数の情報の取得・蓄積が可能であり、個人を識別できる可能性があるプライバシーに関する情報（以下「利用者情報」）が、非常に詳細なレベルで大量に保存されており、これらがアプリケーションを通じて自動的に取得され外部に送信され得るという、スマートフォンならではのリスク特性があります。

利用者情報は個人情報に該当する情報も含まれますが、具体的に例示すると、個人を識別するための情報として、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）が挙げられます。また、スマートフォンが電話や通信端末として利用されることによる電話番号や電話帳データ（氏名、電話番号、メールアドレス）も該当します。

さらに、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として、GPS 機器等が標準的に搭載されていることから精度の高い位置情報が存在し、通話履歴（通話内容・履歴、メール内容・送受信内容等)、Web ページ上の行動履歴等も存在します。加えて、解像度の高いカメラにより撮影される写真やビデオ、アプリケーションの利用により蓄積される情報やアプリケーションの利用ログ、システムの利用に関するログ等もこの区分に該当します。

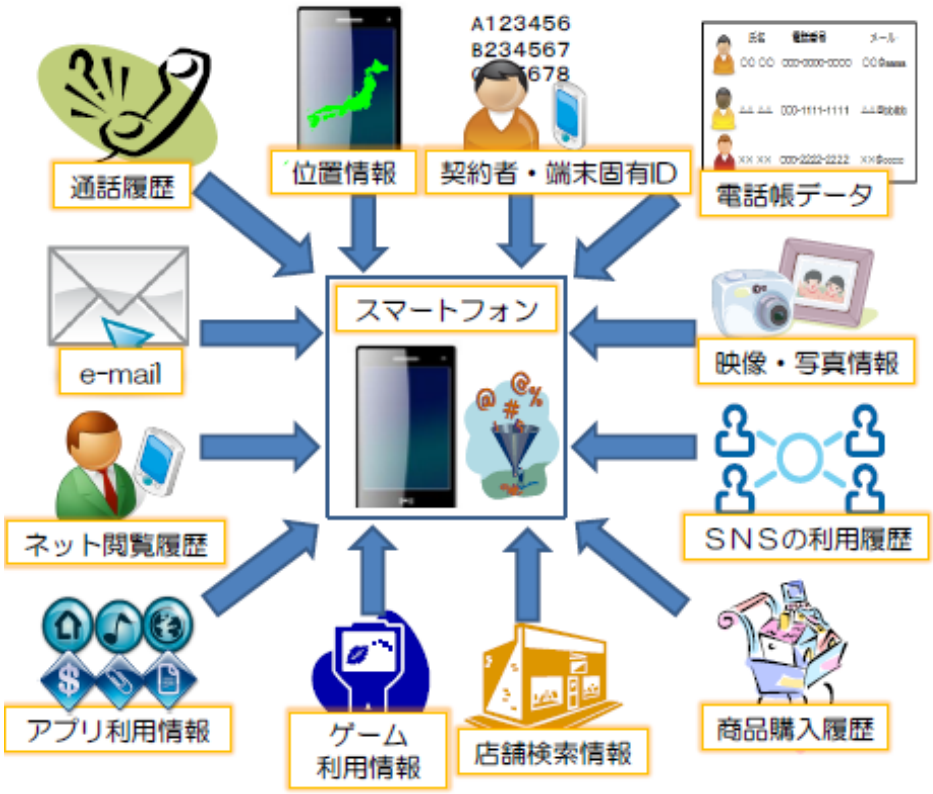



図１　スマートフォンに蓄積される主な利用者情報
出典：総務省「スマートフォン プライバシー イニシアティブ」

(2) 事業における関係者

スマートフォン等関連事業における関係者は多岐にわりますが、本付則の対象となる事業者は、「アプリケーション提供（配信）事業者」と「情報収集モジュール提供事業者」となります。

アプリケーション提供（配信）事業者は、アプリケーションを開発事業者に委託して開発する場合もありますが、広告モデルの場合は情報収集モジュール提供事業者（広告配信事業者等）が提供する情報収集モジュールをアプリケーションに組み込んで、マーケット運営事業者が提供する【アプリ・マーケット】（App Store、Google Play 等）から利用者に対してアプリケーションを配信します。

アプリケーションを受託開発しているだけでアプリケーションを配信していないアプリケーション開発事業者は、利用者情報を取得しないため、本付則の対象外です。

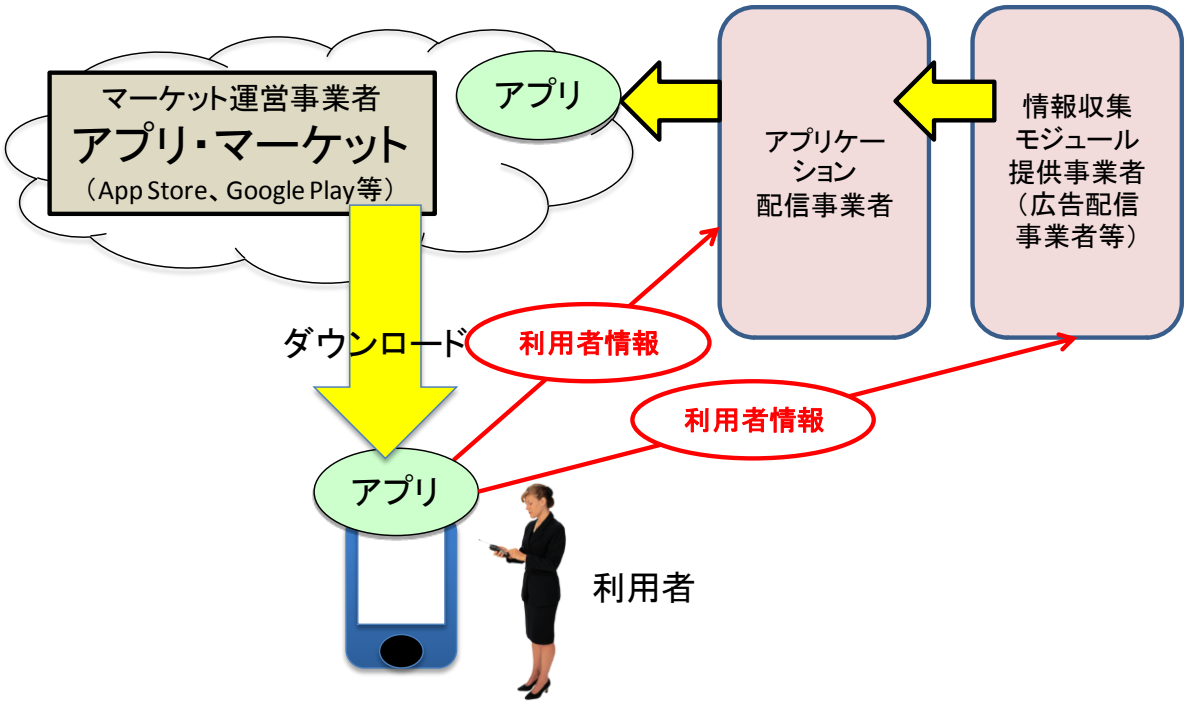



図２　スマートフォン等関連事業における関係者

（3）法令、国が定める指針その他の規範の更新

以下の様な利用者情報に関する法令、国が定める指針その他の規範を特定し参照してください。

①総務省「スマートフォン プライバシー イニシアティブ　ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」

http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html

「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」の 最終取りまとめとして発表されました。スマートフォンにおける利用者情報が安心・安全な形で活用され、利便性の高いサービス提供につながるよう、諸外国の動向を含む現状と課題を把握し、利用者情報の取扱いに関して必要な対応等について取りまとめたものです。

特に、第５章 スマートフォンにおける利用者情報の取扱いの在り方では、「スマートフォン利用者情報取扱指針」としてアプリケーション提供（配信）事業者が対応すべき事項が示されています。

②一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」

http://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf

前記、総務省が示した「スマートフォン利用者情報取扱指針」に沿って「アプリケーション・プライバシーポリシー」の記載方法について推奨事項とモデル案を取りまとめています。

(4) 個人情報の特定とリスク分析

①一般的に特定すべき個人情報

| 情報の種類 | 個人情報の特定 | リスク分析 |
|---|---|---|
| 個人情報に該当する利用者情報(注 1) | 必要 | 必要 |
| 個人情報と同等に扱う利用者情報(注 2) | 不要<br>(但しリスク分析するために管理台帳に登録する。) | 必要 |
| 通信事業者等から取得した決済に関する個人情報（注 3） | 必要 | 必要 |

(注 1) 電話帳、入力フォームから取得する氏名、写真・動画など、特定の個人が識別できる

(注 2) 契約者・端末固有 ID、位置情報、通信履歴、アプリケーション利用履歴などをいう。

(注 3) 氏名、住所、電話番号、メールアドレス、決済金額などをいう。

利用者情報のうち、特定の個人が識別できる個人情報に該当する利用者情報（電話帳、入力フォームから取得する氏名、写真・動画など）は、個別に個人情報の特定を行い、リスク分析（リスクの認識、分析及び対策）を実施してください。

個人情報と同等に扱う利用者情報（契約者・端末固有 ID、位置情報、通信履歴、アプリケーション利用履歴など）については、特定の個人が識別できる可能性があるプライバシー情報であるため、個人情報と同等に取扱い、目的外利用、漏洩、滅失又は毀損を防止するために、管理台帳に「アプリケーションの利用者情報」として 1 つにまとめて登録して、リスク分析を実施してください。

また、有料課金モデルの場合、アプリケーション提供（配信）事業者は、通信事業者や OS 事業者の決済システムを利用する上で、未収債権の回収等のため通信事業者や OS 事業者から個人情報（氏名、住所、電話番号、メールアドレス、決済金額等）を取得することがあるため、個人情報の特定にあたっては対象から漏れないように注意する必要があります。

②リスク分析

特定した個人情報について、その取扱いの局面（取得・入力、媒体の移送、データの送信、利用・加工、保管・バックアップ、消去・廃棄）におけるリスクを認識し、分析し、必要な対策を講じてください。スマートフォンの特性として、アプリケーション内の情報管理の方法（アプリケーションのコーディング方法）によっては、SD カードに個人情報を保管する等、個人情報等漏洩あるいは窃取さ

れるリスクがあるため、アプリケーション内の情報管理方法についてもリスクの認識、分析及び対策を実施する必要があります。なお、個人情報の取扱いの局面と対策例は、個人情報保護委員会の「―個人情報保護法ガイドライン（通則編）」の「8（別添）講ずべき安全管理措置の内容」に記載されていますので、それを参考にしてください。

③安全管理措置

一般的な Web サービスと同様に以下に示すような物理的安全管理措置と技術的安全管理措置をリスクに応じて講じてください。詳細は、本文の 8)安全性の確保を参照してください。

（1）入退館（室）管理の実施（2）盗難等の防止（3）機器・装置等の物理的な保護
（4）個人情報へのアクセス権限の管理（5）個人情報へのアクセスの記録
（6）不正ソフトウェア対策　（7）個人情報の送受信時の対策
（8）個人情報を取扱う情報システムの動作確認時の対策

(5) 個人情報の取得・利用・提供・保管

①利用者情報等の取り扱い

| 情報の種類 | 取得時の措置 | | |
|---|---|---|---|
| | JIS Q 15001:2017 A.3.4.2.5 の措置 | JIS Q 15001:2017 A.3.4.2.4 の措置 | アプリケーション・プライバシーポリシー |
| 個人情報に該当する利用者情報(注 1) | 同意必要 | | 通知または公表が必要 |
| 個人情報と同等に扱う利用者情報(注 2) | 同意不要 | | 通知または公表が必要 |
| 通信事業者等から取得した決済に関する個人情報(注 3) | | 通知または公表が必要 | |

(注 1) 電話帳、入力フォームから取得する氏名、写真・動画など、特定の個人が識別できる情報をいう。
(注 2) 契約者・端末固有 ID、位置情報、通信履歴、アプリケーション利用履歴などをいう。
(注 3) 氏名、住所、電話番号、メールアドレス、決済金額などをいう。

個人情報に該当する利用者情報に関しては、JIS Q 15001:2017 が要求している措置（取得、利用、提供、委託など）の履行とアプリケーション・プライバシーポリシーを通知または公表することを求めます。また、通信事業者や OS 事業者から、未収債権の回収等のため個人情報（氏名、住所、電話番号、メールアドレス、決済金額等）を取得する場合は、A3.4.2.4 の措置が必要です。

個人情報以外の利用者情報（個人情報と同等に扱うもの）に関しては、JIS Q 15001:2017 が要求している措置（取得、利用、提供、委託など）の履行は求めませんが、アプリケーション・プライバシーポリシーを通知または公表してください。

②アプリケーション・プライバシーポリシーについて

「JIS Q 15001:2017 における「個人情報保護方針」は、事業者が個人情報保護に取り組む姿勢や基本的考え方等の個人情報保護の理念を明らかにするものです。一方で「アプリケーション・プライバシーポリシー」は、事業者が透明性の確保を目的として、取得する情報の項目や目的等の事実関係を明らかにするものです。

個人情報保護方針については、原則として 1 社に一つ作成されており、名称としてプライバシーポリシーという文言が用いられ広く普及しています。既に作成されている「個人情報保護方針」と、アプリケーションごとのプライバシーポリシーは記載内容や位置づけが異なるため、実装にあたっては「個人情報保護方針」と混同されないように、「アプリケーション・プライバシーポリシー」という表記を業界団体では推奨しています。なお、表示にあたっては、分けて表示することが望ましいが、プライバシーポリシーとして一体で表示することも許容されます。

記載内容については、アプリケーションが取得する情報や目的に沿って、事業者が判断するものとします。

●「アプリケーション・プライバシーポリシー」に掲載する基本事項としての８項目

①情報を取得するアプリケーション提供者等の氏名又は名称
⇒アプリケーション提供者等の名称、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
⇒利用者情報の利用目的を記載する。
⑤通知・公表又は同意取得の方法、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・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込みの有無を記載する。
⇒広告等のために情報収集モジュールを組込んでいる場合は、情報収集モジュール提供事業者のプライバシーポリシーへのリンクを掲載する。
⑦問合せ窓口
⇒問合せ窓口の連絡先等を記載する。
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。

「アプリケーション・プライバシーポリシー」を掲載する場所は、アプリケーション・マーケット（Google

Play、AppStore 等）やダウンロードページのアプリケーションを紹介するスペースに掲載するようにしてください。
プリインストールアプリケーションやその他の事情により、上記のような掲載場所がない場合や掲示できない事情がある場合等には、インストールの際や初回起動時に、アプリケーションのプログラムでポップアップやページ遷移の工夫を行い、容易に閲覧できるようにしてください。また、アプリケーションに情報収集モジュールを組み込んでいる場合は、各情報収集モジュール提供者のプライバシーポリシーにリンクを張るなどして容易にみられるようにしてください。
情報収集モジュール事業者は、アプリケーション提供（配信）事業者が容易に対応できるようにプライバシーポリシーの内容とリンク先を通知するものとします。


●アプリマーケットの掲載場所（例：Google Play）

以　上

改定履歴

| 版 | 作成／改定年月日 | 内　　容 |
|---|---|---|
| 初　版 | 2010 年 9 月 1 日 | ・新規作成 |
| 第 2 版 | 2013 年 12 月 12 日 | ・その他の規範等の追加修正と付則の追加 |
| 第 3 版 | 2018 年 10 月 12 日 | ・JISQ15001:2017 に対応 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |