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 2 版

2013 年 12 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）
- 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(平成 21 年 10 月 9 日厚生労働省・経済産業省告示第 2 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 16 年 8 月 31 日総務省告示第 695 号）
- 個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2006）
- JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第 2 版―（2010 年 8 月　(財)日本情報処理開発協会　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などに関する法律（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　－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－（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 JIS Q 15001：2006 の定義を採用します。
すなわち「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などによって特定の個人を識別できるもの（他の情報と容易に照合することができ，それによって特定の個人を識別することができることとなるものを含む。）。」を個人情報とします。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）特定の個人を識別できるメールアドレス情報（yamada_taro@abc.co.jp 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、ABC 株式会社に所属するヤマダタロウのメールアドレスであることがわかるような場合等）

事例３）個人ウェブサイト、Blog、プロフィールサイト等で公にされている情報（本人の氏名等、特定の個人を識別できるもの。公開であるかどうかは個人情報であるかどうかには関係がありません）

【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 15001：2006 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、磁気的方式その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）によって本人に明示し，本人の同意を得なければなりません（JIS Q 15001：2006 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 15001:2006 で規定する開示対象個人情報に該当する場合には，開示の求め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 15001：2006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 15001：2006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。

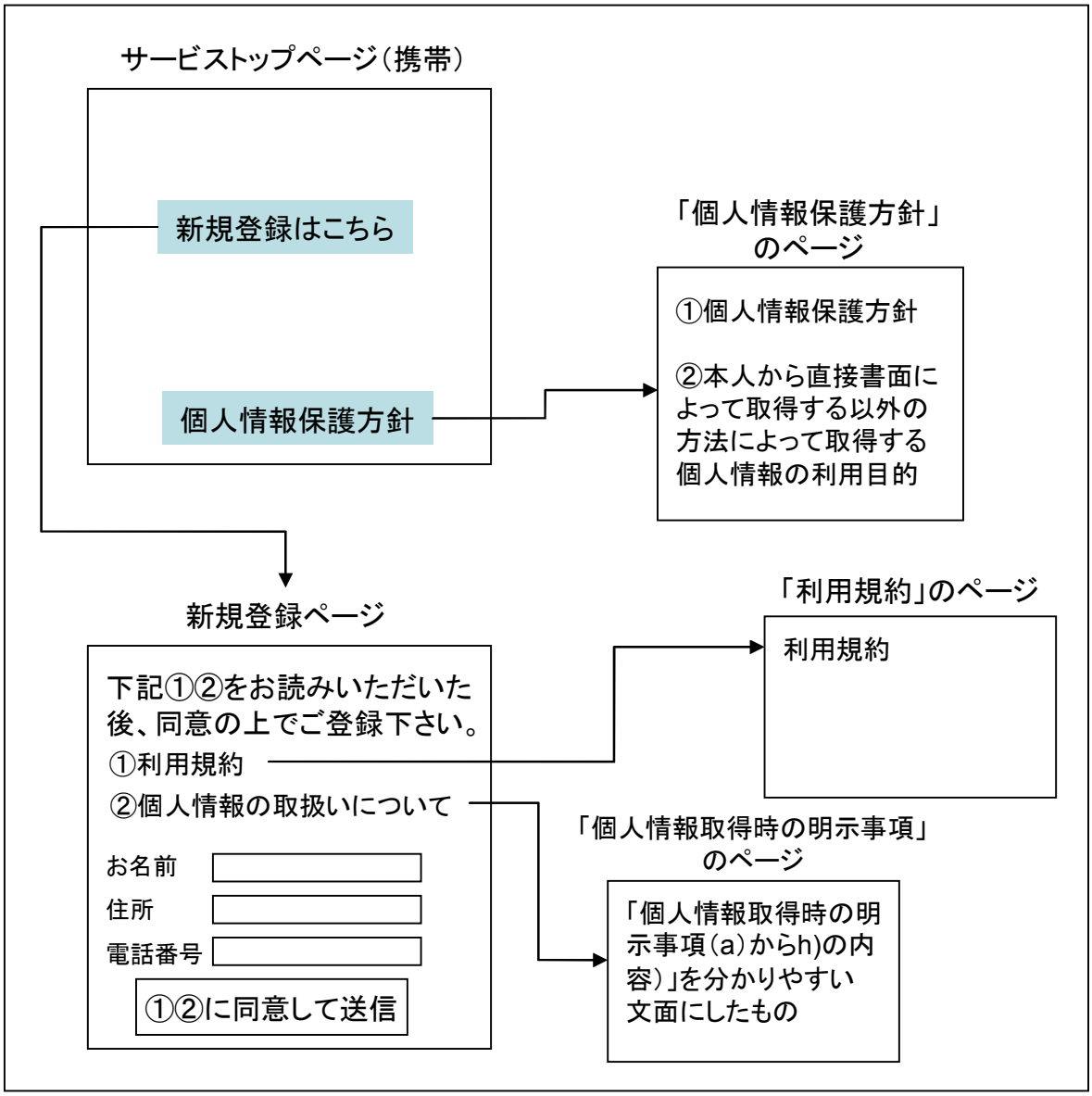
【個人情報を本人から直接書面によって取得する以外の方法によって取得する事例】
事例１）インターネット上で本人が自発的に公にしている個人情報を取得する場合
事例２）インターネット、官報、職員録等から個人情報を取得する場合
事例３）電話による問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除きます)
事例４）個人情報の第三者提供を受ける場合
事例５）個人情報の取扱いの委託を受けて、個人情報を取得する場合
事例６）携帯キャリアより受け取る利用料金未払い者の個人情報
事例７）「お友達紹介キャンペーン」な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

【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 15001：2006 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 15001:2006 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、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」に準拠して安全性の確保の方法を例示します。

安全性の確保は、常にその個人情報の持つリスク（個人情報の漏えい，滅失又はき損，関連する法令，国が定める指針その他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれ）の大きさにより判断するべきであり、実施にあたっては各社の事業の性質および個人情報の取り扱いの状況に応じて定めてください。

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】

<table>
<tr><th>講じなければならない事項</th><th>望ましい手法の例示（具体的な対策の例）</th></tr>
<tr><td colspan="2">1.物理的安全管理措置</td></tr>
<tr><td colspan="2">1.1 入退館（室）管理</td></tr>
<tr><td>①建物、室、マシン室、個人情報の取り扱い場所への入退の制限機構がある。</td><td rowspan="4">●事業所の開錠・施錠時には「それを行った社員の氏名」「日時」の記録を残す。
●個人情報を取り扱う領域に部外者を入れる場合には、「立ち入った人の氏名」「日時」の記録を残す。
●上記の内容が正しく記録されていることを定期的に月に1度程度確認する。</td></tr>
<tr><td>②建物、室、マシン室、個人情報の取り扱い場所への入退が制限されている。</td></tr>
<tr><td>③建物、室、マシン室、個人情報の取り扱い場所への入退の記録が取られ、保管されている。</td></tr>
<tr><td>④建物、室、マシン室、個人情報の取り扱い場所への入退の記録は定期的にチェックされている。</td></tr>
<tr><td colspan="2">1.2 盗難等の防止</td></tr>
<tr><td>①離席時に個人情報を記した書類、媒体、携帯可能なコンピュータ等を机上に放置していない。</td><td rowspan="4">●離席時には個人情報を記した書類、媒体、ノートパソコンなどは机の引き出しなどに入れて施錠する。ノートパソコンに関してそれが難しい際にはワイヤーロックを実施する。
●パスワード付きスクリーンセーバーが一定の時間で自動的に起動する設定とする。
●データの保有期間については、そのサービスでの必要性を考慮して決定する。法律で保管期間が定められているものがあるので、注意する。（取引に関する記録7年間、</td></tr>
<tr><td>②個人情報を取扱う PC の操作において、離席時は、パスワード付きスクリーンセーバーの起動又はログオフを実施している。</td></tr>
<tr><td>③個人情報を記録した媒体（記録媒体、紙）は施錠保管され、あるべきものが全てあることが把握されている。</td></tr>
<tr><td>④個人情報を記録した媒体（記録媒体、紙）の保管場所の鍵は特定者が管理している。</td></tr>
</table>

⑤個人情報を記録した媒体（記録媒体、紙）の廃棄は、再利用できない措置を講じている。	人事・社会保険関係の記録 2～5 年、特定電子メール法における広告宣伝メールを最後に送信した日から 1 ヶ月，特定商取引法におけるメール広告を最後に送信した日から 3 年間など） ●USB メモリ、メモリーカードの廃棄時には物理的に破壊することとする。紙については、シュレッダーを使用するか、機密紙の廃棄サービスを活用する。 ●サービス用個人情報を取り扱うノートパソコンなどの情報機器については、入退室管理の行われた空間のみで取り扱うこととし、持ち出さない。 ●USB メモリ、メモリーカードなどについては会社支給のものを使用することとし、通し番号を付けて、貸出者を台帳で管理する。
⑥個人情報を記録した携帯可能な PC 等の盗難防止措置が施されている。	
⑦FD、MO、CD、USB フラッシュメモリ等の外部記憶媒体の利用はルールに従っている。	
⑧個人情報を取扱う情報システムの操作マニュアルを机上に放置していない。	
1.3 機器・装置等の物理的な保護	
①個人情報を取扱う機器・装置等について、安全管理上の脅威（盗難、破壊、破損等）や環境上の脅威（漏水、火災、停電、地震等）からの物理的な保護装置がある。	●サービス用個人情報を取り扱うオンラインシステムについては、外部のデータセンターに配置するか、サーバー室やサーバーラックなどに施錠保管する。
2.技術的安全管理措置	
2.1 個人情報へのアクセスにおける識別と認証	
①個人情報へのアクセスにおいて、識別情報（ID、パスワード等）による認証が実施されている。	●最低パスワード文字数を決定する。 ●ID と同じパスワードは禁止する。
②個人情報を格納した情報システムは、デフォルトの設定を残していない。	
③識別情報の発行・更新・廃棄は、ルールに従っている。	
④識別情報は平文で記録していない。	
⑤パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止等の措置が講じられている。	

⑥個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等は、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等により、制限されている。	
2.2 個人情報へのアクセス制御	
①個人情報にアクセスできる従業者の数は必要最小限である。	●個人情報にアクセスできる ID、パスワードを複数人で共用することが必要な場合には、共用者を最小限に特定し、利用状況を把握している。
②個人情報にアクセスできる識別情報を複数人で共用していない。	
③従業者に付与するアクセス権限は必要最小限である。	
④個人情報を格納した情報システムの同時利用者数は制限されている。	
⑤個人情報を格納した情報システムの利用時間を制限している。	
⑥個人情報を格納した情報システムを無権限アクセスから保護している。	
⑦個人情報にアクセス可能なアプリケーションの無権限利用を防止している。	
⑧個人情報を取扱う情報システムに導入したアクセス制御機能の有効性を検証している。	
2.3 個人情報へのアクセス権限の管理	
①個人情報にアクセスできる者を許可する権限管理を適切かつ定期的に実施していること。	●退職者のアカウントの削除期限を決定し、期限内に削除されるようにする。 ●社内での共有データへのアクセス権限は、業務内容に基づいて必要な範囲のみに限定する。
②個人情報を取扱う情報システムへのアクセスは必要最小限であるよう制御している。	
2.4 個人情報へのアクセス記録	
①個人情報へのアクセスや操作の成功と失敗の記録を取得し、保管している。	●サービス用個人情報の作成・変更・閲覧のアクセスログの保管期限を決定し、リスク認識に応じてチェックを行い保管する。 ●アクセスログについても定期バックアッ
②取得した記録について、漏えい、滅失及びき損から適切に保護している。	

	プの対象とする。
2.5 個人情報を取扱う情報システムに関する不正ソフトウェア対策	
①ウイルス対策ソフトウェアが導入され、常に最新版が適用されている。	●Web アプリケーションについては、導入時に必ず専門家による脆弱性（SQL インジェクションやクロスサイトスクリプティング、なりすましなど）のチェックを受け、その後も定期的にチェックを実施する。 ●携帯電話のみを対象としたサービスの場合には、アクセスを許可する IP アドレスをキャリアゲートウェイの IP アドレスに限定する、ユーザーエージェントをチェックするなどの対策を実施する。
②OS やアプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆるセキュリティパッチ）を適用している。	
③不正ソフトウェア対策の有効性・安定性を確認している。	
④個人情報にアクセスできる端末にファイル交換ソフトウェア（Winny や Share など）をインストールしていない。	
2.6 個人情報の移送・通信時の対策	
①個人情報の受渡しには授受の記録が残されている。	●フォームに個人情報を入力してもらう際、端末とサーバー間の通信は SSL 等により暗号化を実施する。また、サーバーから担当者にデータをメールにより転送する際にも暗号化するか、必要性を考慮した項目のみに限定する。
②個人情報を媒体で移送する時に、移送時の紛失・盗難が生じた際の対策が講じられている。	
③盗聴される可能性のあるネットワーク（例えばインターネットや無線 LAN 等）で個人情報を送信（例えば本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際に、個人情報の暗号化又はパスワードロック等を実施している。	
2.7 個人情報を取扱う情報システムの動作確認時の対策	
①情報システムの動作確認時のテストデータとして個人情報を利用していない。	●本番データを使用するシステムテストは、テストの最終段階のみに限定し、必ず社員が立ち会う。
②情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことを検証している。	
2.8 個人情報を取扱う情報システムの監視	
①個人情報を取扱う情報システムの使用状況を定期的にチェックしている。	●サービス用個人情報を取り扱うオンラインシステムについては、システムが正常に

②個人情報へのアクセス状況（操作内容を含む。）を定期的にチェックしている。	稼働していることを随時確認して、異常が発生した際にはすぐに担当者に警告が出るようにする。 ●サービス用個人情報を取り扱うオンラインシステムについては、アクセスログを定期的に確認し、不正なアクセスがないことを確認する。

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、当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、未対応な場合は、継続的改善事項として次回更新審査迄に対応を進めてください。

(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。

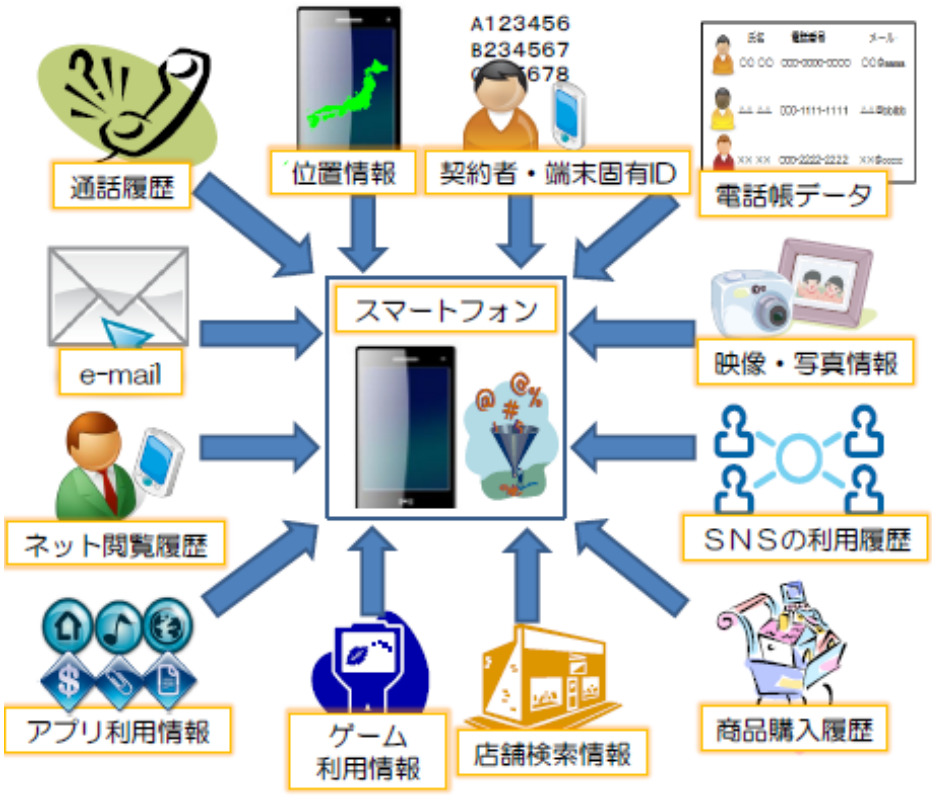


図１　スマートフォンに蓄積される主な利用者情報
出典：総務省「スマートフォン プライバシー イニシアティブ」

(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。

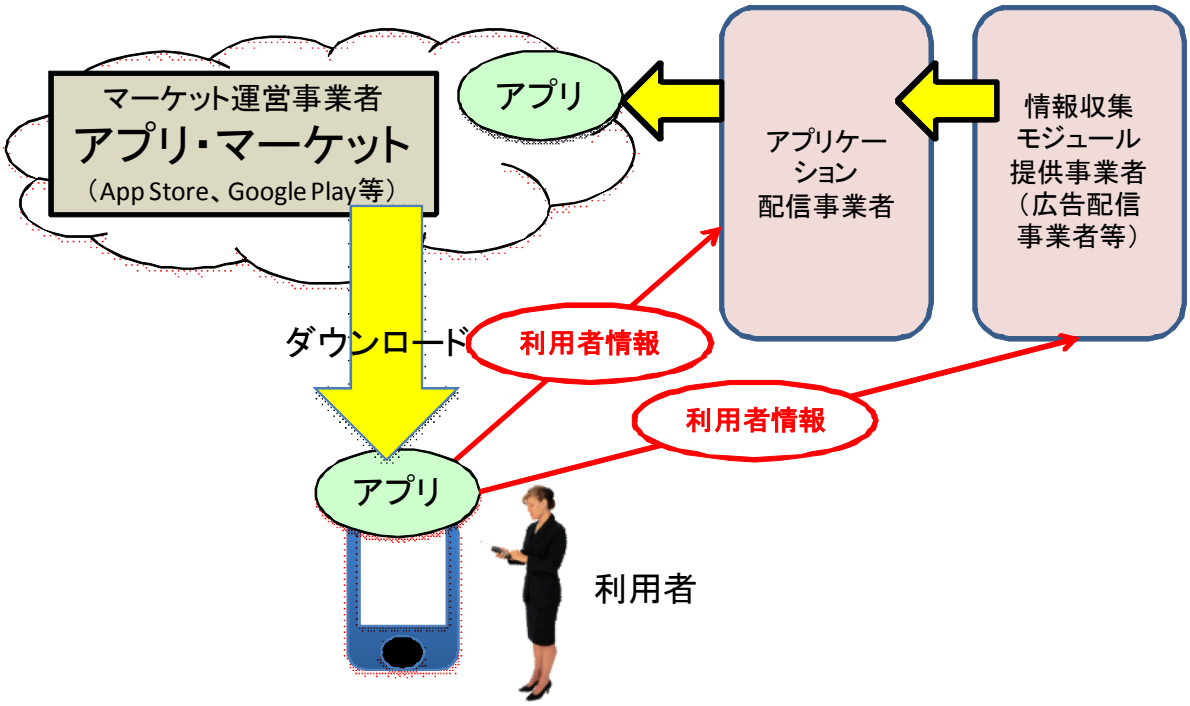


図２　スマートフォン等関連事業における関係者

(3) 3.3.2 法令、国が定める指針その他の規範の更新

「法規等管理台帳」に以下規範を追加して、個人情報保護管理者の承認を得てください。

①総務省「スマートフォン プライバシー イニシアティブ　－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－」

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 (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、「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第 2 版―」の「3.4.3.2　安全管理措置」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 15001:2006 3.4.2.4 の措置	JIS Q 15001:2006 3.4.2.5 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 15001:2006 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、3.4.2.5 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 15001:2006 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 15001:2006 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。

●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