総務省

スマートフォン・プライバシー・セキュリティ・イニシアティブ（SPSI）について

令和7年1月28日

総務省

スマートフォン上の利用者情報の取扱い等に係る総務省の取組の経緯

スマートフォンの普及に伴い、アプリケーション等により取得・蓄積された**利用者情報（アドレス帳、位置情報等）が、本人の意図しないかたちで外部送信されている事案が発覚、社会問題化**したことを踏まえ、**2012年**に、総務省において、**スマホアプリ提供者等の関係事業者が利用者情報を適正に取り扱う上で実施することが望ましい事項（プライバシーポリシーの作成・掲載等）**を**「スマートフォン プライバシー イニシアティブ（SPI）」**としてとりまとめて公表。

2012年８月　**スマートフォン プライバシー イニシアティブ（SPI）**

- スマホアプリ提供者等の関係事業者が利用者情報を適正に取り扱う上で実施することが望ましい事項を示すとともに、利用者のリテラシー向上のための情報提供・周知啓発について提言

2013年９月　**スマートフォン プライバシー イニシアティブⅡ（SPI Ⅱ）**

- SPIで示された利用者情報の適正な取扱いについて実効性を確保するための方策について提言

2017年７月　**スマートフォン プライバシー イニシアティブⅢ（SPI Ⅲ）**

- これまでの報告書の形式から、スマホアプリ提供者等の関係事業者が参照しやすいよう、関係事業者の役割分担を明確化し、プライバシーポリシーの作成等の取組を具体化

2024年11月　**スマートフォン プライバシー セキュリティ イニシアティブ（SPSI）**

- **セキュリティ**の観点から取り組むべき事項を追加
- 電気通信事業法等の国内制度改正を反映するとともに、民間の取組や諸外国制度の動向を踏まえて取組を追記（ダークパターンの回避、センシティブ情報取得時の本人同意等）

現在　**ICTサービスの利用環境の整備に関する研究会　利用者情報に関するWGにおいて更なる検討を開始**

（１）対象スコープ

ウェブサイトや、スマートフォン以外のデバイスについて、対象とすべきか検討

（２）青少年保護

プライバシー、セキュリティに加えて、青少年保護の観点から取り組むべき事項を検討

（３）位置づけ

「実施することが望ましい」事項について、望ましい度合を整理し構造的に示すことを検討

スマートフォン プライバシー セキュリティ イニシアティブ（SPSI）の概要

基本原則

（１）透明性の確保
（２）利用者関与の機会の確保
（３）適正な手段による取得の確保・不適正利用の禁止
（４）適切な安全管理の確保
（５）苦情相談への対応体制の確保
（６）プライバシー・バイ・デザイン/セキュリティ・バイ・デザイン
（７）特定の情報及び利用者への属性に応じた配慮

スマホアプリ提供者の取組（例）

プライバシーポリシーの作成

- プライバシーポリシーをアプリごとに日本語であらかじめ作成することが望ましい。

プライバシーポリシー等の運用

- プライバシーポリシーを公表し、アプリを利用しようとする者が容易に参照できる場所に掲示・リンクを張ることが望ましい。
- 以下のようなプライバシー性が高い利用者情報の取得・利用については同意取得等の適切な対応することが望ましい。
  ①個人情報を含む電話帳情報
  ②人種・信条・病歴等のセンシティブ情報
  （※センシティブ情報を予測・生成するプロファイリングは原則実施しない。実施の場合は同意を取得）
  ③こどもの利用者情報
  （※法定代理人からの同意を取得、こどもの利用者情報のプロファイリングに基づくターゲティング広告は実施しない）
  ④利用者行動のトラッキング
  （※事業者横断的なトラッキングを行うために利用者情報を取得する際には、同意を取得）
  ⑤契約者・端末固有ID
  ⑥GPS等による位置情報
  ⑦通信内容・履歴
  ⑧スマホアプリの利用履歴やスマホ保存の写真・動画
- 利用者が同意した場合であっても、同意の撤回ができる機会を提供し、同意の撤回方法をプライバシーポリシーに記載することが望ましい。

苦情相談への対応体制

- 苦情相談の窓口・連絡先を設置する等体制の整備に努めることが望ましい。

適切な安全管理措置

- 利用者情報が漏えい、滅失又はき損の危険にさらされることがないように、安全管理のために必要な措置を講じることが望ましい。

アプリケーションの開発時における留意事項

- 利用者の個人情報やプライバシーが保護されるように、アプリの企画及び設計の段階から、適切な仕組みを組み込むことが望ましい（プライバシー・バイ・デザイン）。

ダークパターン回避の対応

- 利用者を欺いたり操作する方法又は利用者が自由に決定を行う能力を実質的に歪めたり損なったりする方法（ダークパターン）で利用者情報の取扱いを行わないことが望ましい。

電気通信事業法への対応

- 令和４年改正電気通信事業法で導入された、特定利用者情報規律、外部送信規律の遵守

セキュリティの確保に係る取組

- セキュリティが適切に確保されるよう、アプリの企画及び設計の段階から、適切な仕組みをアプリに組み込むことが望ましい（セキュリティ・バイ・デザイン）。
- アプリに係る脆弱性情報を収集し、窓口・連絡先を設置するなど必要な体制の整備に努める。

アプリストア運営事業者（※）の取組（例）

プライバシーの確保に係る取組

- スマホアプリ提供者がプライバシーに係る左記の事項を実施しているか確認することが望ましい。
- アプリストアへのアプリ登録審査時に、本指針を踏まえた基準等を作成し、あらかじめ公表することが望ましい。
- アプリの掲載を拒否する場合は、その理由についてスマホアプリ提供者に対して適切なフィードバックすることが望ましい。
- 説明や情報提供の方法が適切でないアプリが判明した場合、アプリストアからの削除等を実施し、連絡窓口を設置することが望ましい。

セキュリティの確保に係る取組

- アプリストアで提供されるアプリが満たすべきセキュリティ要件を示し、当該要件を満たしているか審査することが望ましい。
- アプリストアで提供される各アプリが、脆弱性報告のための窓口を有するとともに、アプリ提供者が適切なタイミングで脆弱性を開示するための手続を有していることを確認することが望ましい。
- アプリの掲載を拒否する場合は、その理由について、スマホアプリ提供者に対して適切なフィードバックすることが望ましい。

（※） 既存のアプリストア運営事業者のみならず、今後参入が見込まれる代替アプリストア運営事業者も対象となる

このほか、情報収集モジュール提供者、OS提供事業者、移動体通信事業者、端末製造事業者の取組について記載