スマートフォンアプリケーション開発者の実施規範

～スマートフォンのアプリ開発および提供時に求められる対策について～

【第一版】

2024 年 03 月 08 日

日本スマートフォンセキュリティ協会（JSSEC）
技術部会

文書管理番号　JSSEC-TECA-AP-CP20240305

■制作■

技術部会スマートフォンアプリケーション開発者の実施規範

作成タスクフォース

リーダー	本間 輝彰	KDDI 株式会社
メンバー	上松 晴信	KDDI 株式会社
	小笠原 徳彦	株式会社 SHIFT SECURITY
	小坂 善彦	株式会社 SHIFT SECURITY
	仲上 竜太	ニューリジェンセキュリティ株式会社
	齊藤 義人	株式会社ブロードバンドセキュリティ
	佐藤 竜	株式会社ブロードバンドセキュリティ
	砂川 真範	株式会社ブロードバンドセキュリティ
	横井 宏之	株式会社ブロードバンドセキュリティ
	岸原 孝昌	一般社団法人モバイル・コンテンツ・フォーラム
	木村 芳教	株式会社ラック

（社名五十音順）

文書管理番号 JSSEC-TECA-AP-CP20240305

目 次

1. 実施規範

1.1. 概要

スマートフォン（以下、スマホ）の普及から 10 年以上が経過し、Google Play や App Store などのアプリケーションマーケット（以下、アプリマーケット）では、多数のスマホ向けアプリケーション（以下、アプリ）が提供されています。アプリマーケットは、利用者の安全を確保するために、様々な条件や規制を定めています。しかし、アプリ提供者がアプリのセキュリティに取り組む方法は、明確な手順書やドキュメントが存在していないため、提供者によって異なるのが現状です。本実施規範では、アプリ開発者がアプリ提供に際して利用者を保護するための具体的な手順を定めています。

本実施規範は、世界的に認知されたセキュリティとプライバシーの慣行に基づき、国内の各種法律も考慮に入れています。また、各原則はユーザのセキュリティとプライバシーの保護に重要であることから、特定の優先順位は設けていません。本実施規範内の原則の中には、既に国内の各種法律やアプリストア運営者によって義務付けられているものも含まれています。

本実施規範の遵守により、透明性と安全性を兼ね備えたアプリの提供が可能となり、それによってより安全なアプリが提供されることを期待しています

1.2. 想定読者

本ガイドは、主に以下の読者を対象としています。

(1) アプリ開発者

iOS/iPad アプリ・Android アプリなどスマートフォンアプリケーションの設計、実装、テストを担当するソフトウェア開発事業者・個人

(2) アプリ提供者

iOS/iPad アプリ・Android アプリなどスマートフォンアプリケーションを用いたサービスを提供する事業者・個人

2. 実装ガイドのスコープ

2.1. 本ガイドのスコープ

スマートフォンをとりまくセキュリティ環境には様々な構成要素があり、日本スマートフォンセキュリティ協会（以下、JSSEC と記載）技術部会では、その要素ごとのワーキンググループに分かれています。本ガイドは、スマートフォンアプリケーション開発者の実施規範作成タスクフォースが、実施規範作成にあたって求める事項について、調査等を行い実施規範の作成を行なっています。

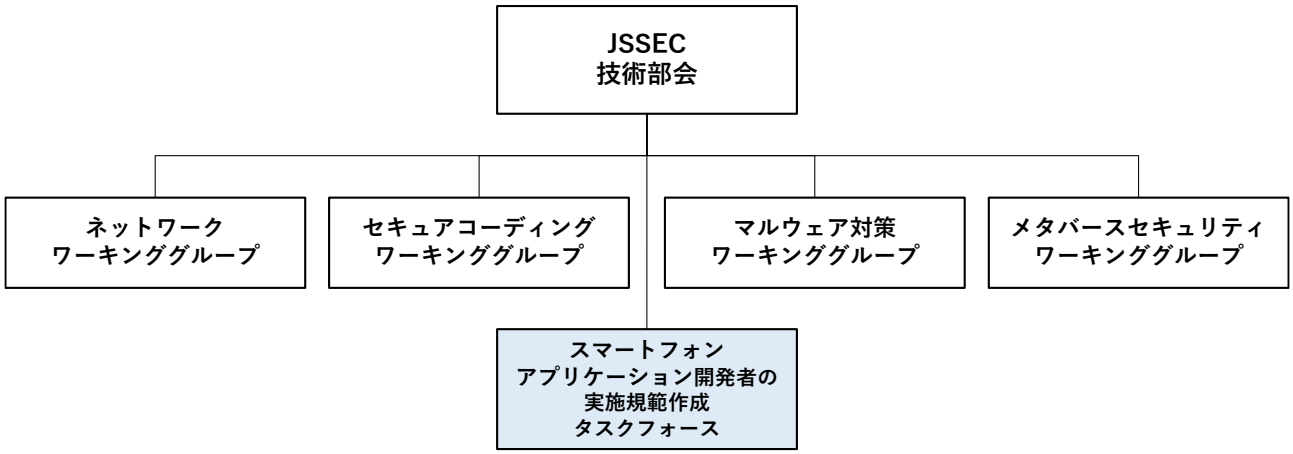


図 2-1　JSSEC 技術部会の組織図と本ガイド執筆組織の位置づけ

2.2. スコープの概念図

サービス事業者などがアプリを提供する際、一般的にはアプリマーケットを経由しての提供が行われます。このプロセスでは、アプリ提供者がアプリ開発者に開発を依頼し、その結果として生じたアプリをアプリマーケットに登録し公開します。なお、アプリ開発者は開発の過程で、3rd Party の SDK（Software Development Kit）を組み込む場合もあります。本実施規範では、アプリ提供者がアプリの開発からアプリマーケットへの登録までの一連の流れにおいて行うべき手順を対象としています。この範囲を整理した概念図を、「図 2-2　検討スコープ」として以下に示します。

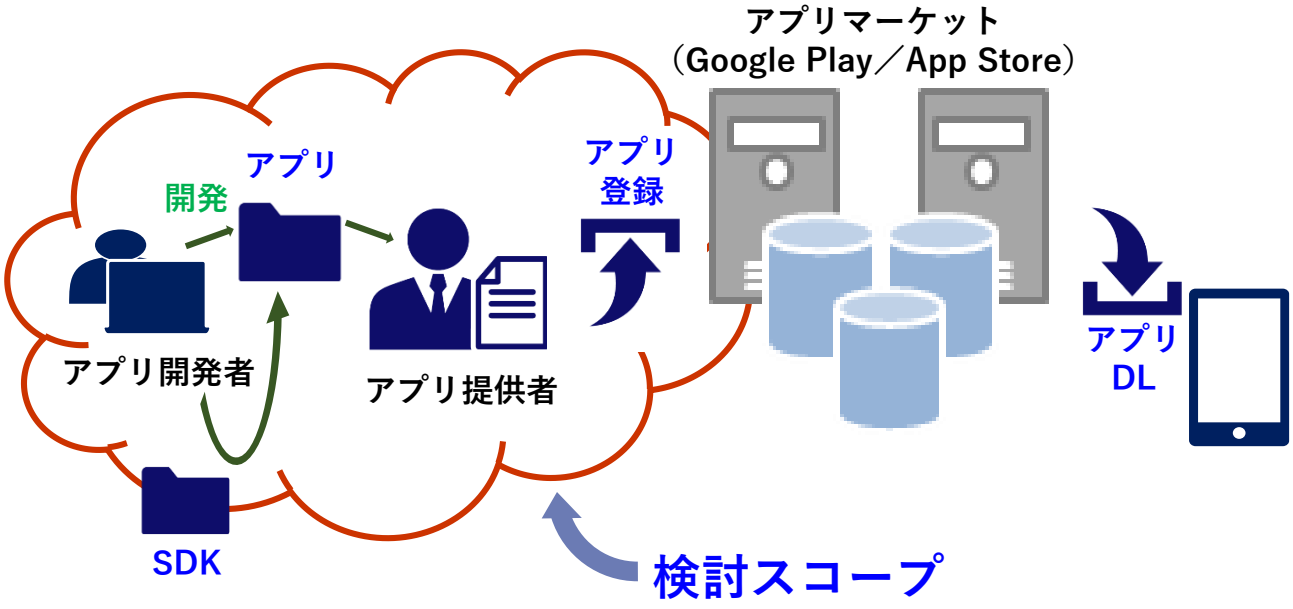


図 2-2　検討スコープ

3. セキュリティとプライバシーの基本要件

一般に公開されたアプリは誰でもアプリマーケットからダウンロード可能であるため、攻撃者がアプリを解析し、脆弱性を見つけて悪用する可能性が存在します。そのため、提供するアプリに対して、セキュリティとプライバシーの基本要件を設け、それに準拠した開発が求められます。

3.1. 準拠すべきセキュリティとプライバシー基本要件

アプリは以下のセキュリティとプライバシーの基本要件に準拠することが必要です。

- アプリ内で業界標準の暗号化を使用する。特に、重要データを端末内や SD など外部メモリに保存する際には、暗号化は必須となる。
  - 暗号技術は時代とともに陳腐化し非推奨になる可能性があるため、最新の業界標準の暗号化を採用することが推奨されます。
- 利用者がアプリのオプション機能や権限・許可の無効化を選択した場合でも、アプリの主要機能が動作することを保証しなければならない。
  - 権限・許可は設定画面などから変更可能であり、利用者が後から許可しないを選択することを想定する必要があります。
- アプリの動作に必要ない許可や権限を要求してはならない。
  - 例えば、アプリが位置情報を利用しないにも関わらず、位置情報収集の権限を要求する行為は不適切です。
- アプリはセキュリティ要件、データ保護法で定められた要件、その他の適切な法律を遵守する措置を講じる必要がある。
  - データを海外に送信する場合には、国内法だけでなく海外の法律にも準拠する必要があります。
- アプリを削除した際には、端末内のデータは全て削除する必要がある。
  - アプリを削除しても、再度アプリをインストールし利用する可能性があるため、サーバで管理するアカウント情報などは削除する必要がありません。
- アプリは収集したデータを削除する仕組みを具備する必要がある。

- アプリから直接収集したデータを削除する機能や仕組みがない場合は、プライバシー要件に記載するアプリプライバシーポリシーに、削除の依頼先を明記することが必要です。なお、収集した個人情報の扱いについては、提供している国の個人情報保護に関する法律に準ずる必要があります。

- アプリ内でアカウントを作成する機能がある場合は、アカウントを削除する機能を具備する必要がある。
  - アカウントを削除した際は、運用上必要な個人情報を除き、サーバから削除する必要があります。なお、アプリ開発やサービス改善のために必要な情報は匿名化し、個人を特定出来ないようにする必要があります。
- アプリにサードパーティの SDK などを組み込む場合、その SDK が利用者にとって不適切な動作をしないこと、またサポート状況や脆弱性がないことを確認する。
  - 特に SDK がアプリ提供者の意図しない情報を収集していた場合、不適切な個人情報収集に該当する可能性があり注意が必要です。
- アプリには難読化を施し、ソースコードが解析されにくいようにする。
  - 攻撃者がリバースエンジニアリングによりソースコードを解析し、悪意のある類似のアプリを作成することを防ぐために難読化を行います。
- パーミッションの同意を得る際には、利用者に対して分かりやすい説明を行う必要があります。
  - アプリが位置情報などを取得する際には、パーミッションの同意が必要となります。その際には、アプリがなぜその情報を必要としているのかを明確に説明し、利用者が納得してアプリを利用できるようにします。
- 平文通信は極力避けて、通信路を暗号化することが推奨されます。
  - アプリがデータを送信する際には通信路を経由しますが、通信路が暗号化されていない場合、平文通信により中間者攻撃によってデータが盗聴される可能性があります。
- ソースコードや設定ファイルの管理にソースコード管理サイトなどを利用する場合は、クレデンシャル情報など重要情報をアップロードしないよう注意する必要があります。
  - パスワードや API キーなどのクレデンシャル情報をソースコードや設定ファイルに明記してアップロードすると、それが不特定多数に共有されてしまう可能性があるため注意が必要です。

3.2. セキュアコーディング

安全なアプリを提供するためには、セキュアコーディングが重要です。以下に示すプロセスを参考にしてアプリの開発を行うことを推奨します。

- アプリ開発に際しては、以下のガイドラインを参考にして必要なセキュリティ要件を定め、それに基づいて実装を行うことをお勧めします。
  - OWASP（Open Web Application Security Project） MASVS（Mobile Application Security Verification Standard）[1]
  - OWASP Mobile Top 10[2]
  - JSSEC（Japan Security Analyst Association） モバイルアプリケーション開発 10 大チェックポイント[3]
- iOS アプリの場合、Apple が開発者向けに提供している「Apple デベロッパーセキュリティ」[4]を参考にしてセキュリティ要件を定め、それに基づいて実装を行うことを推奨します。
- Android アプリの場合、Google が開発者向けに提供している「セキュリティに関するベストプラクティス」[5]や JSSEC が発行している「Android アプリのセキュア設計・セキュアコーディングガイド」[6]を参考にしてセキュリティ要件を定め、それに基づいて実装を行うことを推奨します。

3.3. セキュリティテスト

アプリをセキュリティ上の問題なく開発することは非常に困難です。そのため、開発したアプリに対して適切なセキュリティテストを実施し、問題がないことを確認して提供することが推奨されます。

[1] MASVS： https://mas.owasp.org/MASVS/

[2] Mobile Top10： https://owasp.org/www-project-mobile-top-10/

[3] JSSEC モバイルアプリケーション開発 10 大チェックポイント： https://www.jssec.org/mobile-apps-10checkpoint2023

[4] Apple デベロッパー セキュリティ： https://developer.apple.com/jp/security/

[5] アプリのセキュリティに関するおすすめの方法： https://developer.android.com/topic/security/best-practices?hl=ja

[6] JSSEC Secure Coding ガイド： https://www.jssec.org/dl/android_securecoding/index.html

- セキュリティテストを実施する際には、以下のガイドラインを参考にすることをお勧めします。
  - OWASP MASTG（Mobile Application Security Testing Guide ）[7]
  - OWASP MASDG（モバイルアプリケーションのセキュリティ設計ガイド）[8]
- 脆弱性診断を実施する。
  - 脆弱性診断については、診断の種類によって実施内容が異なるため、アプリの特性などを考慮して適切な診断を行うことが望ましいです。
  - 脆弱性診断はアプリに関するセキュリティ知識が必要となるため、セキュリティベンダーなどの第三者によるセキュリティ診断を実施することが望ましいです。特に、新規開発や大規模な機能追加を行った場合には、厳格な脆弱性診断を実施することが推奨されます。
  - 脆弱性診断は、必要に応じてアプリの対抗側の API についても実施が必要となります。

[7] MASTG： https://mas.owasp.org/MASTG/

[8] MASDG： https://jp-east.mas.scc.lac.co.jp/Android/ja/build/html/index.html

4. アプリ公開後のメンテナンス

アプリを公開した後、利用者からの通報によって不具合やバグが発覚する場合があります。また、アプリマーケットのポリシーやルールが変更された場合、アプリ提供者はそれに準拠する必要があります。したがって、アプリ提供者はアプリ開発者と協力してアプリの保守、運用、メンテナンスを行う必要があります。

4.1. 脆弱性情報の収集

アプリ公開時点では脆弱性が存在しないとしても、その後新たな脆弱性が発見される可能性があります。したがって、アプリ提供者は脆弱性情報を継続して収集する必要があります。

- アプリマーケットに公開しているアプリに脆弱性が存在するか定期的に確認する。
  - アプリ提供者やアプリ開発者は、OS やアプリやアプリ内で使用している SDK に脆弱性がないか定期的に確認します。脆弱性の情報の収集にあたっては、IPA などが公開する脆弱性情報や OS や SDK の提供元の不具合情報などを収集する方法があります。
  - 数多くの SDK を使用しているアプリの場合は、使用している SDK とバージョンを一覧で管理し、定期的に開発元情報をチェックして非推奨になっていないか確認します。
  - アプリの脆弱性を修正できない場合は、利用者にアプリのサポート終了を通知します。サポート終了のアプリについては、配信を停止することが望ましいです。
- 自社で自アプリの脆弱性を発見した際の対応方針を整備準備する。
  - サポートサイトでの公表などの手続きを整備します。ただし、脆弱性の存在が明らかになると攻撃されるリスクがあるため、対応が完了するまで非公開とするのが一般的となります。
  - 深刻な脆弱性の場合は、IPA などの公的機関に報告し、公開することも検討します。公的機関の公表により、より多くのユーザに脆弱性情報が伝わります。
- 外部から脆弱性の申告があった場合の対応方針を整備する。
  - 外部からの申告は、脆弱性関連情報等取扱い方針[9]に基づき IPA や JPCERT から入る場合と発見者から直接来る場合が考えられます。なお、前者の場合は、脆弱性関連情報等取扱い方針に定められたルールに準じて対応が必要となります。

[9] 脆弱性関連情報等取扱い方針： https://www.ipa.go.jp/security/todokede/vuln/policy.html

4.2. 脆弱性の対応

アプリに脆弱性が見つかった場合は、脆弱性の深刻度による利用者やサービスへの影響を鑑みて適切に対応することが求められます。なお、脆弱性があることが外部に知られた場合、攻撃されるリスクが高くなるため、脆弱性の情報の取扱いには十分注意する必要があります。

- 利用者やサービスに重大な影響を及ぼす脆弱性が見つかった場合には、速やかに必要な対応を行う。
  - 利用者に影響等を通知します。なお、通知する方法は、アプリ内での通知やメールなどの通知の他に、HP での公開をする方法などがあります。
  - 脆弱性の対応が完了するまでは、必要に応じて問題のある機能の停止、サービスの一時的な休止、マーケットからのアプリ配信の停止などの対応も検討します。
- アプリでの脆弱性の対応が完了したら、速やかに修正されたバージョンを公開し、利用者にアップデートを要求します。
  - 脆弱性が既知になっていない場合は、不具合改修などと案内し、脆弱性対応であることを案内しないことも多いです。
- アプリでの脆弱性の対応が出来ない場合は、脆弱性の影響を鑑みて、サービスの提供方法の見直しが必要となります。

4.3. アプリの保守・運用

アプリ提供者は、アプリの保守・運用に関して以下の公正を行う必要があります。

- 外部からの申告に備えて、アプリの脆弱性の申告を受け付ける窓口を準備し、申告方法を公開する必要があります。
  - RFC 9116 に準拠した security.txt[10]を使って脆弱性対応窓口を外向けに分かりやすく示しておくことが出来ます。

[10] RFC 9116 A File Format to Aid in Security Vulnerability Disclosure：
https://datatracker.ietf.org/doc/html/rfc9116

- ウェブサイトに問い合わせフォームを設置するなどの方法があります。

- アプリ提供者は、アプリ開発者に脆弱性を修正してもらうための体制を維持する必要があります。
  - アプリリリース後に脆弱性が発覚した場合を考慮して、開発保守体制を維持しておくことが望ましいです。
- 重大な不具合に対応するために、アプリの強制アップデート機能を実装することを推奨します。
  - アプリの起動時に最新バージョンの確認を行い、旧バージョンのアプリでは動作を制限するなどの対策を取る方法があります。
- 利用者からのアプリの不具合について申告窓口を設ける必要があります。
  - 専用の Web サイトを用意するか、アプリのポリシーに申告方法を記載するなどの対応があります。
- アプリに不具合が見つかった場合は、利用者に対して速やかに不具合情報を公開し、対応方針を説明することが望ましいです。
  - 重大な不具合が発生し、アプリ利用者に被害を及ぼす可能性がある場合は、サービスの一時的な中断などの対応も検討する必要があります。
- OS がバージョンアップした場合は、最新の OS での動作を検証し、問題がある場合は必要な対処を行わなければなりません。
  - アプリが新 OS に対応できない場合は、利用者に明確に情報提供する必要があります。
- アプリマーケットの仕様変更情報を定期的に確認し、仕様変更に合わせて対応を行う必要があります。
  - アプリマーケットからの通知を常に確認し、開発者向けのイベントにも参加することが有用です。
- アプリで使用しているサードパーティの SDK のサポート情報を定期的に確認し、問題がある場合には速やかに対処する必要があります。
  - 利用している SDK のサポートが終了した場合には、代替手段を検討することが望ましいです。
- アプリの公開後、2 年以内にアプリのアップデートを行うことが推奨されます。
  - 定期的にアプリをアップデートし、OS のアップデートと同期させることが重要です。
  - Google Play では 2 年以上アップデートされていないアプリは非表示になります。

- App Store では 2 年以上アップデートされていないアプリは削除されます。

- サービスを終了する場合は、利用者に不利益が内容に対応をする。
  - サービスを終了する際には、アプリ内で利用者に対して通知する必要がある。なお、インターネット通信を行わないアプリについては、HP で通知などを行うことが推奨されます。また、終了までにある程度の期間をもって通知することが推奨されます。
  - サービス終了をもって、マーケットのアプリは非公開等にし、ダウンロード出来なくする必要があります。
  - サービス終了後は、アプリ利用時にサービスが終了していることを通知することが推奨されます。
  - サービス終了後には、収集した個人情報も削除する必要があります。ただし、他のサービスと連携している場合などは、サービスに関連した個人情報のみの削除で問題ありません。

5. プライバシーの基本要件

アプリから個人情報を含むさまざまな情報が送信されることがあります。そのため、アプリ開発者およびアプリ提供者は、アプリの利用者に対して送信される情報の開示を行い、アプリの透明性を確保する必要があります。

5.1. アプリマーケットでの対応

アプリマーケットでは、利用者のプライバシーを保護するために、アプリ登録時にさまざまなルールやポリシーが定められています。アプリを公開するためには、アプリ開発者はポリシーに従ってアプリを開発する必要があります。

- Google Play にアプリを登録する際には、Google Play のデベロッパープログラムポリシー[11]に従い、アプリが送信する情報をデータセーフティセクション[12]に開示する必要があります。
- App Store にアプリを登録する際には、App Store のガイドライン[13]および App のプライバシーに関する詳細情報の表示[14]に従い、アプリが送信する情報を申告する必要があります。
- Google Play と App Store の両方で公開するアプリの場合、マーケットに記載する収集項目の内容については、各 OS のみで取り扱う情報以外は、同じ内容を記載する必要があります。
- Google Play および App Store にアプリを登録する際には、プライバシーポリシー（以下、プラポリ）のリンクが必要ですが、リンクするプラポリにはアプリから送信する情報について説明されている必要があります。
- アプリマーケットに申告する内容とプラポリの内容は一致させる必要があります。

5.2. 透明性の確保

アプリは個人情報を含むさまざまなデータを収集し、外部に送信する場合があります。そのため、利

11 デベロッパープログラムポリシー： https://support.google.com/googleplay/android-developer/answer/13837496?hl=ja&visit_id=638294059274498037-630085752&rd=1

12 データセーフティ―セクション： https://support.google.com/googleplay/android-developer/answer/10787469?hl=ja

13 App Store Review ガイドライン： https://developer.apple.com/jp/app-store/review/guidelines/

14 App のプライバシーに関する詳細情報の表示： https://developer.apple.com/jp/app-store/app-privacy-details/

用者に対してプラポを提示することが求められます。

- アプリの初回利用時には、プラポリを表示し、利用者の同意を取得する必要があります。ただし、同意を取得する際には、利用者に負担をかけないように概要版のプラポリを使用し、詳細を確認したい利用者には概要版から詳細版の同意を表示することが望ましいです。
- アプリの機能追加などで、収集するデータが変更される場合には、プラポリの再同意を取得することが推奨されます。再同意を行う際には、利用者に負担をかけないように変更点のみを説明するなどの工夫も考えられます
- アプリから送信するデータとプラポリの内容が一致しているかどうかを確認するために、スマートフォンプライバシーイニシアティブⅡの第 3 章「アプリケーションの第三者検証の在り方」に記載されているように、第三者機関による不正な送信を検証[15]することが望ましいです。
  - アプリには、情報を収集するために第三者が提供する SDK などが組み込まれている場合もあります。これらの SDK はアプリ提供元が認知していないデータを収集している可能性もあるため、SDK が送信している情報を含めて、第三者検証が重要です。
- 2023 年 6 月 16 日施行の電気通信事業法[16]では、電気通信事業を営む者が利用者に関する情報を外部に送信する場合、あらかじめ送信される情報の内容について通知や公表などの措置を講じる必要があることが規定されています。したがって、このルールに従う必要があります。

5.3. アプリプライバシーポリシーの作成

プラポリは、企業が個人情報の取り扱いに関する指針を説明する「企業プライバシーポリシー（企業プラポリ）」、サービス利用時の個人情報の取り扱いに関する詳細情報を説明する「サービスプライバシーポリシー（サービスプラポリ）」、アプリの利用者情報の取り扱いに関する詳細情報を説明する「アプリプライバシーポリシー（以下、アプリプラポリ）」の 3 つのポリシーに分類されます。実際に公開されているプラポリは、企業プラポリとサービスプラポリ、サービスプラポリとアプリプラポリの 3 つが統合されているものや、それぞれ独立しているものなど、さまざまな形態があります。

[15] スマートフォンプライバシーイニシアティブⅡ： https://www.soumu.go.jp/main_content/000358528.pdf

[16] 電気通信事業法（外部送信規律）：
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/gaibusoushin_kiritsu.html

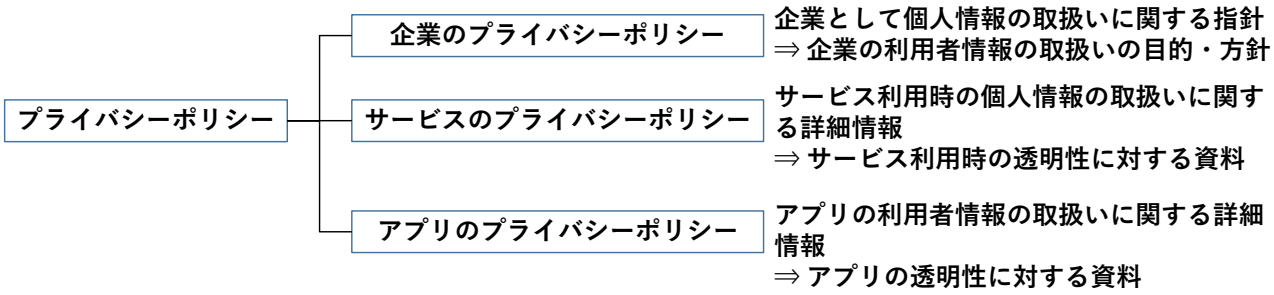


図 5-1　プライバシーポリシーの分類

アプリ利用者は、アプリがどのような情報をどのような目的でどこに送信しているかに関心を持っています。そのため、アプリマーケットでは、アプリから送信される情報を申告するために、アプリプライバポリにリンクすることが推奨されます。アプリプラポリからは、企業プライポリやサービスプラポリへのリンクを行い、企業やサービスごとの情報の取り扱いを説明することが望ましいです。

5.3.1. アプリプラポリに記載すべき項目

アプリプライポリには、「表 5-1　アプリプラポリに記載すべき項目」に示す 10 項目を記載することが推奨されています。これらの項目は、総務省が発行しているスマートフォンプライバシーイニシアティブ（SPI）[17]のアプリプラポリの作成や、電気通信事業者向け個人情報保護ガイドライン（令和４年個人情報保護委員会・総務省告示第４号（最終改正令和５年個人情報保護委員会・総務省告示第５号））の解説[18]で推奨されています。

また、上記の項目に加えて、企業プラポリやサービスプラポリへのリンク、アプリプラポリの作成日や更新日を記載することが推奨されます。

これらの項目を適切に記載することにより、アプリ利用者に対して透明性と情報提供を確保することができます。

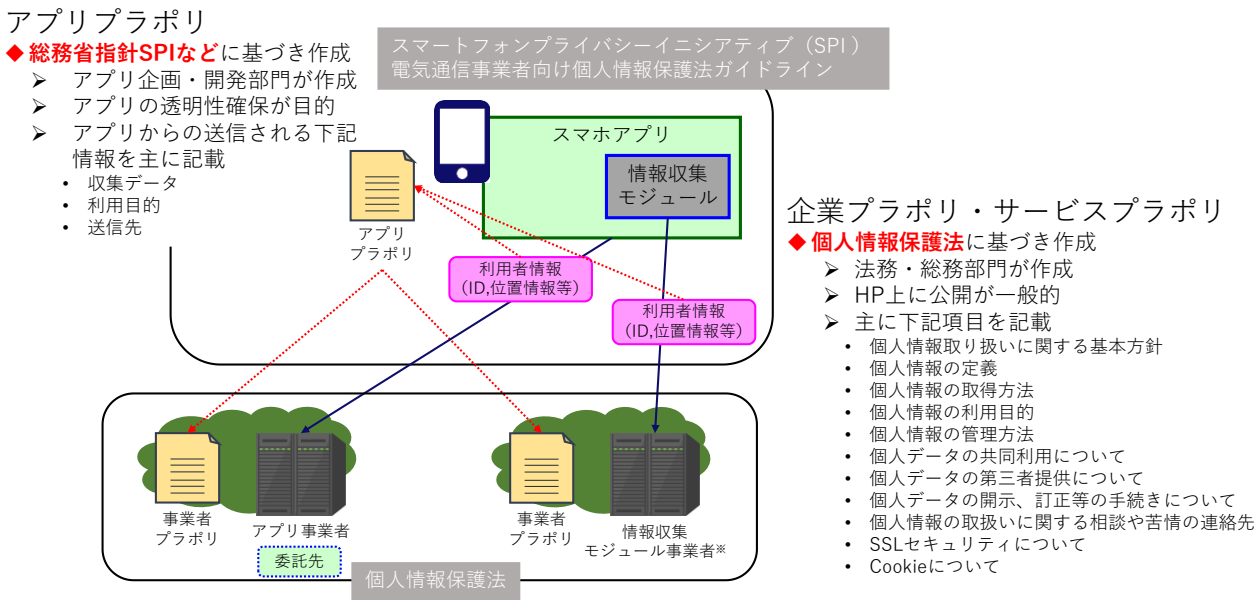
[17] スマートフォンプライバシーイニシアティブ　https://www.soumu.go.jp/main_content/000358525.pdf
[18] 電気通信事業者向け個人情報保護ガイドラインの解説：　https://www.soumu.go.jp/main_content/000805807.pdf

表 5-1　アプリプラポリに記載すべき項目

<table>
<tr><th colspan="2">調査項目</th></tr>
<tr><td colspan="2">① 情報を取得するアプリケーション提供者等の氏名または名称</td></tr>
<tr><td rowspan="2">② 取得される情報の項目</td><td>②-1 取得される項目の記載状況</td></tr>
<tr><td>②-1’取得される項目の詳細</td></tr>
<tr><td colspan="2">③ 取得方法</td></tr>
<tr><td colspan="2">④ 利用目的の特定・明示</td></tr>
<tr><td rowspan="2">⑤ 通知・公表または同意取得の方法、利用者関与の方法</td><td>⑤-1 送信停止の手順の記載状況</td></tr>
<tr><td>⑤-2 利用者情報の削除手順記載状況</td></tr>
<tr><td rowspan="3">⑥ 外部送信・第三者提供・情報収集モジュールの有無</td><td>⑥-1 利用者情報の第三者への送信の有無の記載状況</td></tr>
<tr><td>⑥-2 利用者情報の送信先の記載状況</td></tr>
<tr><td>⑥-3 情報収集モジュールに関する記載状況</td></tr>
<tr><td colspan="2">⑦ 問合せ窓口</td></tr>
<tr><td colspan="2">⑧ プライバシーポリシーの変更を行う場合の手続</td></tr>
<tr><td colspan="2">⑨ 利用者の選択の機会の内容、データポータビリティに係る事項</td></tr>
<tr><td colspan="2">⑩ 委託に係る事項</td></tr>
<tr><td colspan="2">その他：　企業プラポリやサービスプラポリのリンク先
アプリプラポリの作成日や更新日</td></tr>
</table>

アプリから送信されるデータは、アプリ本体だけでなく、組み込まれた情報収集モジュールによっても送信される場合があります。そのため、アプリプラポリでは、情報収集モジュールの名称や送信されるデータを忘れずに記載する必要があります。

「図 5-2　アプリから送信されるデータ」では、アプリから送信されるデータの例が示されています。この図を参考にしながら、アプリプラポリにおいて、具体的な情報収集モジュールの名称や送信されるデータの詳細を記載することが重要です。



※情報収集モジュール事業者：アプリ上に組み込む情報収集モジュールを提供している事業者。

図 5-2　アプリから送信されるデータ

また、アプリプライポリの作成に際しては、モバイル・コンテンツ・フォーラムが作成している「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」[19]を参考にすることが望ましいです。このガイドラインは、アプリプラポリ作成に役立つ指針を提供しています。適切な情報提供と透明性を確保するために、このガイドラインを参考にすることをおすすめします。

[19] 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：
https://www.mcf.or.jp/temp/sppv/mcf_spappp_guidline.pdf

6. 利用規約の基本要件

6.1. 利用規約の基本要件

2020 年 4 月の民法改正により、民法 548 条の 2 第 1 項において、定型約款の合意が義務付けられました。そのため、国内で提供されるアプリに対しては、アプリ利用前に利用規約への同意が必須となります。また、利用規約が変更された場合には、民法に従って適切な対応を行う必要があります。

さらに、アプリは国内利用者以外にも提供される場合があります。このような場合には、各国の法律を確認し、必要な法的同意を得る必要があります。なお、利用規約が日本語で記載されている場合、海外の利用者がその文面を理解することは難しく、同意を取得しても無効とされる可能性があります。そのため、利用規約は提供する国の言語や法律を考慮して作成することが重要です。

また、提供するアプリが日本人のみを対象とする場合は、アプリマーケットに登録する際に、提供先を日本に限定して提供することが推奨されます。

以上の要件に留意しながら、利用規約を作成することで、利用者との関係を明確化し、法的な要件を満たすことができます。

7. ユーザサポート

アプリ提供後に利用者からの問い合わせなどに対応するために、以下の対策が必要です。

7.1. 推奨されるユーザサポート項目

- 利用者が問い合わせできるように、連絡先や問い合わせフォームなどを提供する必要があります。
- 問い合わせ先は、アプリ内で利用できるか、またはアプリからリンクされたウェブページやメールなどを通じて利用できるようにすることが推奨されます。
  - アプリが提供するサービスのウェブサイトでも問い合わせ先を提供することが望ましいです。
- アプリから問い合わせへの遷移は、例えば「メニュー」→「ヘルプ」→「問い合わせ先」といった形で、利用者がイメージしやすく、少ない操作でアクセスできるようにすることが望ましいです。

7.2. 推奨されるユーザサポートセキュリティ項目

アプリ利用時に ID 情報などが不正利用される可能性を考慮し、利用者に必要なセキュリティ対策を提供することが望ましいです。

- アプリ利用時のセキュリティに関する注意事項を提供することが推奨されます。
- アプリで推奨されるセキュリティ設定方法などを公開することが推奨されます。
- 危険な（推奨しない）設定を行う場合には、警告を表示することが望ましいです。
- ID 情報などが漏洩し、不正利用された場合に利用者が実施すべき手順などをまとめて公開することが推奨されます。

以上のユーザサポートの項目を適切に実施することで、利用者からの問い合わせやセキュリティに関する懸念に対応し、より良いユーザーエクスペリエンスを提供することができます。

8. セキュリティインシデント対応

8.1. セキュリティインシデント対応

個人情報漏洩を伴うセキュリティインシデントが発生した場合、迅速に適切な措置を講じる必要があります。

- 個人情報漏洩を伴うセキュリティインシデントが発生した場合、インシデント対応のフローを整備することが推奨されます。
- 個人情報漏洩を伴うセキュリティインシデントが発生した場合、個人情報保護法などに従って速やかに報告する必要があります。
  - 海外でアプリを提供している場合は、各国の法律に準拠した対応が必要です。
- 個人情報漏洩を伴うセキュリティインシデントが発生した場合、影響を受ける利用者に対して迅速に通知する必要があります。
- アプリを通じて個人情報の漏洩が発生した場合、影響を受けるユーザに対して、自己防衛のための対策を案内する必要があります。
- アプリを通じて個人情報の漏洩が発生した場合、アプリの配信停止、利用停止、サービスの停止などを検討する必要があります。個人情報漏洩を伴うセキュリティインシデントが発生した際のインシデント対応フローを整備することが推奨される。

上記のセキュリティインシデント対応を適切に実施することで、個人情報漏洩に対する迅速な対応が可能となり、利用者の信頼を維持することができます。

9. おわりに

本実装規範では、アプリを提供する際に実施すべき対策をアプリ視点でまとめました。すべての対策を実行することは、コストの観点から難しい場合もありますが、提供するアプリが扱う情報や万が一の問題が発生した場合の影響を考慮し、必要な対策を実施することが推奨されます。

また、多くのアプリでは、Web サーバなどと連携してサービスを提供しています。そのため、アプリのセキュリティ対策だけでなく、サーバ側のセキュリティ対策も実施することが推奨されます。

アプリの提供においては、利用者の個人情報やセキュリティに関わる重要な情報を取り扱っていることを念頭に置き、適切な対策を講じることが重要です。利用者の信頼を獲得し続けるために、セキュリティを考慮したアプリの提供を心がけましょう。