スマートフォン上のアプリケーションにおける利用者情報の取扱いに係る調査・分析

～ スマートフォン プライバシー アウトルック Ⅻ （SPO XII）～

2026年03月31日

KDDI株式会社

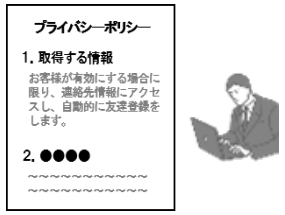
• 【概要】スマートフォンプライバシーアウトルックXII

- 総務省は、令和７年９月、スマートフォン利用者が安心・安全にスマートフォンのアプリを利用できるよう、アプリ提供者やアプリストア提供者等が実施することが望ましい、プライバシー、セキュリティ、青少年保護の確保に向けた事項をまとめたベストプラクティスとして、「**SPSI（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）**」を策定。
- 令和7年度、アプリ提供者やアプリストア提供者における、SPSIの取組状況（セキュリティやプライバシー確保に係る取組の実施状況）について実態を把握するために調査（文献調査と技術的解析）を実施したところ、その結果を「**SPO XII（スマートフォン・プライバシー・アウトルック　XII）**」としてとりまとめ。

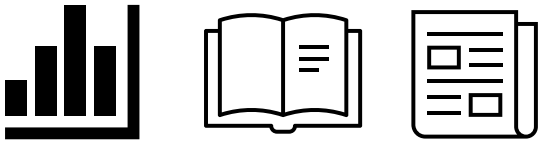
文献調査

- 公式アプリストア及びサードパーティストアのランキング等を基に、選定したアプリに対して、プライバシーポリシーの内容等を確認することにより、アプリによる同意取得状況や利用者への透明性確保の状況を確認
- また、公式ストア及びサードパーティストアの規約・ガイドラインを確認することにより、各ストアのレギュレーション・審査状況を調査

SPSIの各項目と利用者同意の状況・プライバシーポリシーの内容を比較する



アプリストア事業者、OS提供事業者の取り組みをドキュメントベースで調査する

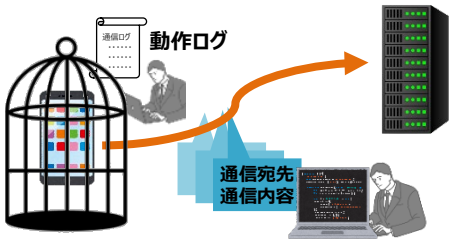


技術的解析

- 公式ストア及びサードパーティストアのランキング等を基に、選定したアプリに対して、第三者による解析等を実施
- **静的解析や動的解析を組み合わせる**ことにより、アプリの脆弱性の有無やセキュリティ・バイ・デザインに関する取組状況を把握

アプリの実行ファイルからソースコードを再構築し、コード内容を分析することでアプリの挙動を把握

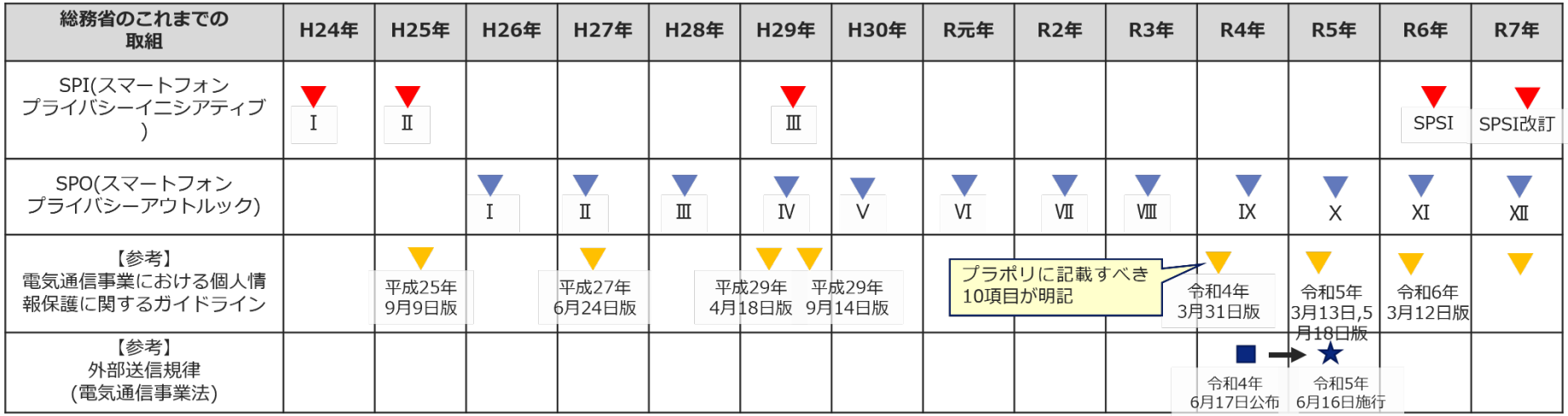
アプリの通信パケットを解析して通信内容を把握



1. 背景

- 十数年前より、スマートフォン上のアプリケーション（以下「スマートフォンアプリ」という。）の利活用の機会が広がり、サービス提供側もスマートフォンアプリを通じて利用者の属性や行動情報等を収集することが容易になったことから、今や、スマートフォンアプリは社会・経済活動において日常的に利活用されている。
- 平成24年頃、スマートフォンに蓄積された利用者情報が、不正なアプリケーションによって外部送信される事例が発生するなどしたことから、スマートフォンの安心・安全な利用環境を整備するため、総務省において、**個人情報及びプライバシーを保護しつつ、アプリケーション提供者等がスマートフォンにおける利用者情報を適切に取り扱うための具体的な指針を定める「SPI (スマートフォン　プライバシー　イニシアティブ）」を公表**した。総務省は、スマートフォンの利用環境の変化に応じてSPIの内容を改定してきており、直近では、**令和７年度９月に「SPSI（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)」として改称・改定**している。
- 加えて、総務省は、平成26年以降、国内外のスマートフォンアプリにおけるプライバシーポリシー（以下、「プラポリ」という。）作成・掲載に係る実態、及び国内外の政府、業界団体、プラットフォーム事業者などの取組動向の定点調査を実施した結果を「SPO (スマートフォン　プライバシー　アウトルック）」として取りまとめてきた。
- 今般、総務省は、令和7年度におけるSPSIの策定を踏まえ、**アプリ提供者やアプリストア提供者における、SPSIの取組状況（セキュリティやプライバシー確保に係る取組の実施状況）について、令和７年度時点の実態を把握すべく調査を実施した。**本「SPO XII（スマートフォン・プライバシー・アウトルック　XII）」は、当該調査結果を踏まえて取りまとめたものである。

<プライバシーポリシーや利用者情報の外部送信に係るこれまでの総務省の取組>



1. 調査手法（アプリの選定、簡易・詳細解析の方法、解析事業者の数など）

- 本調査では、SPSIへの遵守状況を調べるために、アプリ提供者、アプリストア事業者、OS提供事業者について、主に文献調査と技術的解析を実施した。
- 調査対象のアプリは、**公式ストア２つ（App Store、Google Play）**、**サードパーティストア５つ（Aptoide、Uptodown、F-droid、APKPure、HappyMod）**からダウンロード可能なアプリとした。調査対象のアプリストア事業者も同様の２者＋５者とした。なお、App Store以外はAndroid用アプリを対象とした。

文献調査

アプリ提供者のプライバシーポリシーの調査

450個（公式ストアとサードパーティストアについて、各ストア65個程度）のアプリのプライバシーポリシーを調査する。

アプリストア事業者、OS提供事業者のガイドライン等の調査

各アプリストアのガイドラインや規約等からSPSIの各項目の遵守状況を調査する。

技術的解析

”App Store”、“Google Play”、“サードパーティストア”から入手可能な全てのアプリ

↓

- ７つのストアにおける、各ストアのランキング上位100程度のアプリを選定

ツールによる脆弱性診断　対象アプリ：706アプリ

- 解析事業者3社がツールによる自動的な診断を実施し、各アプリのセキュリティスコアを得た。
- １つのアプリについて2社が解析を行うことで1412(=706×2)の結果を得た。

↓

- セキュリティスコアが高い（＝セキュリティレベルが低い）50程度のアプリを選定

詳細な脆弱性解析　対象アプリ：52アプリ（７つのストアから各７個程度のアプリを選定＋α）

- 解析事業者6社により、静的解析及び動的解析を実施した。

各アプリマーケットの概要

マーケット名	主な特徴	主な利用国	ユーザ規模
F-droid	Androidプラットフォーム向けの自由でオープンソースのソフトウェア（FOSS）アプリケーションを集めたインストール可能なアプリマーケット。2010年に設立され、プライバシーに配慮したアプリを提供することを目標としており、約4400のアプリが広告やトラッキングなしで利用可能。	グローバル	中
Aptoide	Google Playとは異なる独立系のAndroidアプリストアで、ユーザーがアプリをダウンロードおよび配布できるプラットフォーム。2009年に設立され、分散型のマーケットプレイスとして開発者が独自のアプリストアを作成・管理できる仕組みを提供している。	グローバル	大
Uptodown	Android APKファイルのダウンロードに特化した独立系プラットフォーム。2002年にスペインで設立され、現在では約400万のAPKファイルをホストしている。	グローバル	中～大
APKPure	Android向けのAPKファイルを提供するサードパーティプラットフォームで、2014年に設立。100万以上のアプリを提供しており、ユーザーに対してGoogle Playでは利用できないアプリへのアクセスを提供している。	グローバル	中
HappyMod	Android向けの代替アプリストアで、主に人気アプリやゲームの改造版提供に特化している。ユーザーに対して、アンロック機能や無制限のゲーム内リソース、広告なしの体験を提供することを目的としている。	アジア	中

SPSI 1.2.1（アプリ提供者における取組）①AppStoreとGooglePlay提供アプリ

- SPSIの項目（例：SPSI 1.2.1.）に沿ってアプリ提供事業者等の取組状況を確認したところ、調査結果概要は以下のとおり。

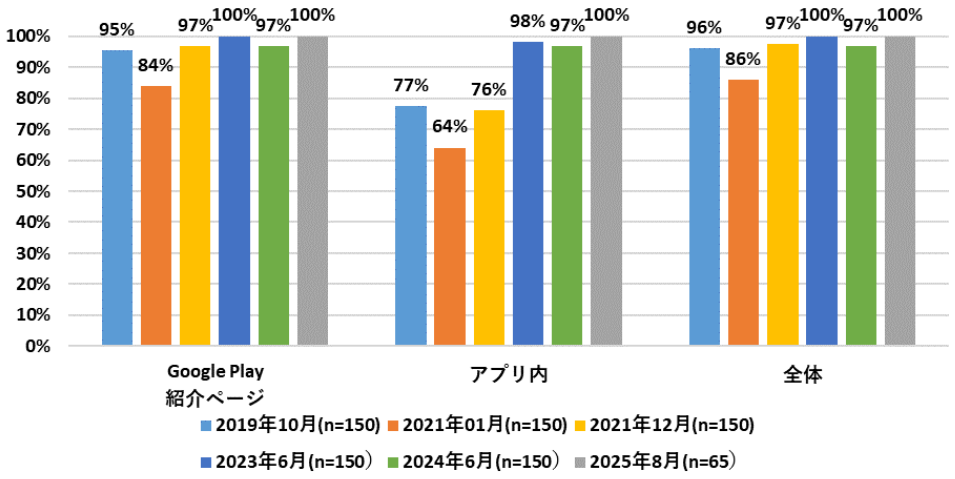
<SPSIの記載（p.18）>

- アプリケーション提供者は、アプリケーションを提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが強く求められる【基本的事項】

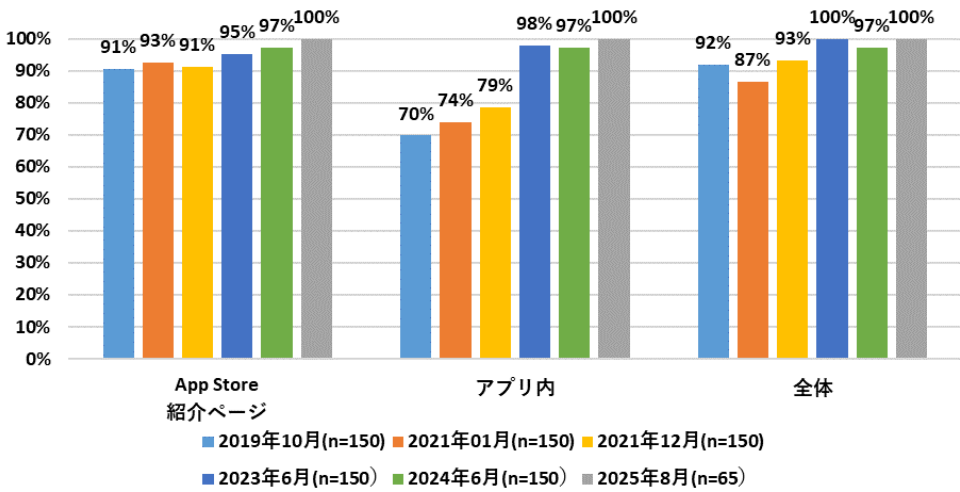
<調査結果概要>

➢ **アプリマーケット運営事業者（Google、Apple）がアプリ紹介ページにプラポリのリンク掲載を義務付けている**ため、**AppStore及びGoogle Playで提供されるアプリの紹介ページにおけるプラポリ掲載率は100%に近い**結果となっている。また、アプリ内でのプラポリ掲載についても100%の結果となっている。

【Android】プラポリの掲載率



【iPhone】プラポリの掲載率



※ 掲載率：以下の「A」から「F」までのうち、「F」判定以外であれば、「プラポリ有り」と判断。
（「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない）
A：個々のスマホアプリ専用のプラポリが用意されている。　B：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある。
C：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がない。　D：一般的なWebサイトのプラポリがあるだけ。
E：会社としての抽象的なポリシー（個人情報保護方針）があるだけ。　**F：日本語もしくは英語のプラポリが記載されていない。**
※ 紹介ページの掲載率：「紹介ページのリンク」か「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。
※ アプリ内の掲載率：「初回起動時」、もしくは、「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。
※ 全体の掲載率：「紹介ページ」、もしくは、「アプリ内」のどちらかが「F」以外の判定となったアプリの割合。

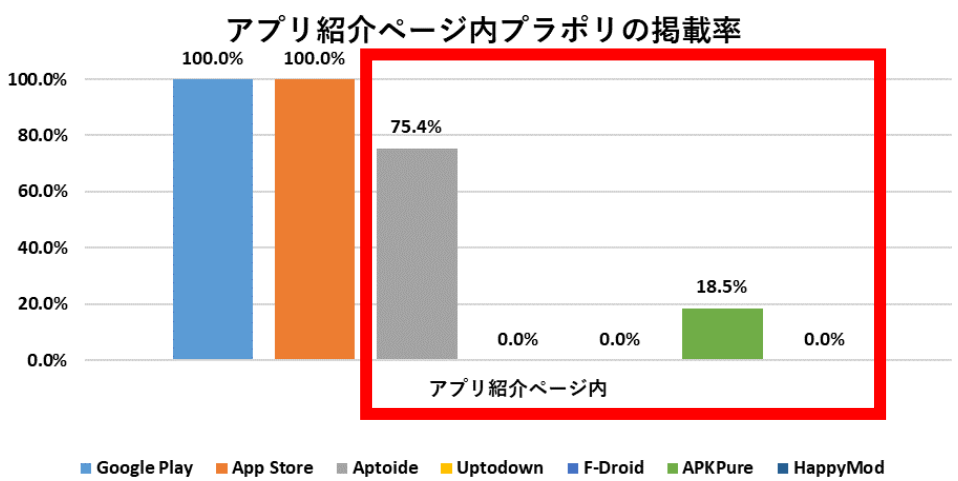
SPSI 1.2.1（アプリ提供者における取組）②サードパーティアプリストア提供アプリ

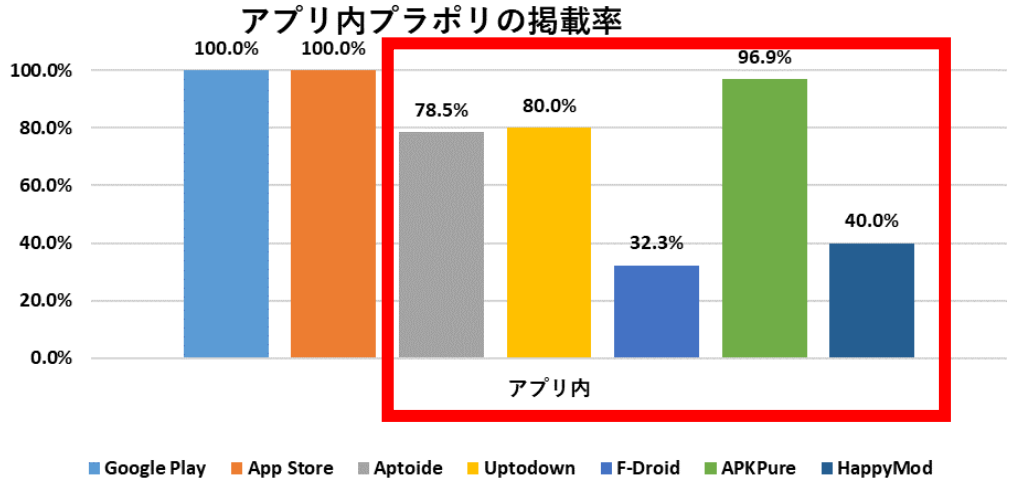
<SPSIの記載（p.18）>

- アプリケーション提供者は、アプリケーションを提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが強く求められる【基本的事項】

<調査結果概要>

- **Aptoide以外のサードパーティストアはアプリの紹介ページにおけるプラポリ掲載率が低かった**。一方で、アプリ内のプラポリ掲載率は、F-Droid、HappyModが50%以下であったが、それ以外のサードパーティストアにおけるアプリのアプリ内プラポリ掲載率は約80%以上と比較的高かった。
- 公式ストア（AppStoreとGooglePlay）とサードパーティストアを比較すると、全体的に公式ストアのプラポリの掲載率が高いことが分かる。
- 全てのサードパーティストアではアプリ紹介ページ内よりもアプリ内の方がプラポリ掲載率が高い傾向があった。公式ストアで配布しているアプリをそのままサードパーティストアで配布しているケースがあると考えられる。





※ 掲載率：以下の「A」から「F」までのうち、「F」判定以外であれば、「プラポリ有り」と判断。
（「個々のアプリに関するプラポリが作成されていること」、「SPI8項目が適切に記載されていること」を示すものではない）
A：個々のスマホアプリ専用のプラポリが用意されている。
B：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある。
C：サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がない。
D：一般的なWebサイトのプラポリがあるだけ。
E：会社としての抽象的なポリシー（個人情報保護方針）があるだけ。
F：日本語もしくは英語のプラポリが記載されていない。
※ 紹介ページの掲載率：「紹介ページのリンク」か「紹介文内での記載」のどちらかで「F」以外の判定となったアプリの割合。
※ アプリ内の掲載率：「初回起動時」、もしくは、「アプリ内のメニューやヘルプ等」のどちらかが「F」以外の判定となったアプリの割合。

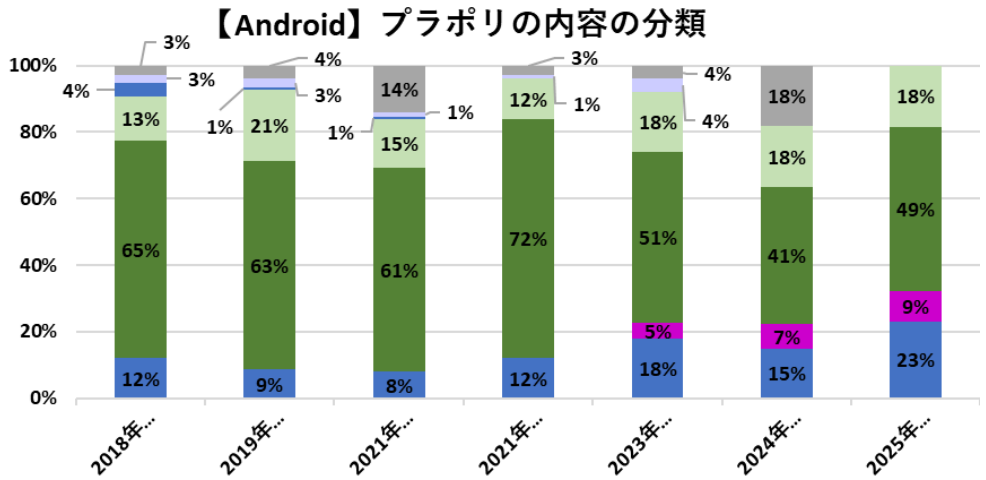
SPSI 1.2.1.1（プライバシーポリシーの作成）①AppStoreとGooglePlay提供アプリ

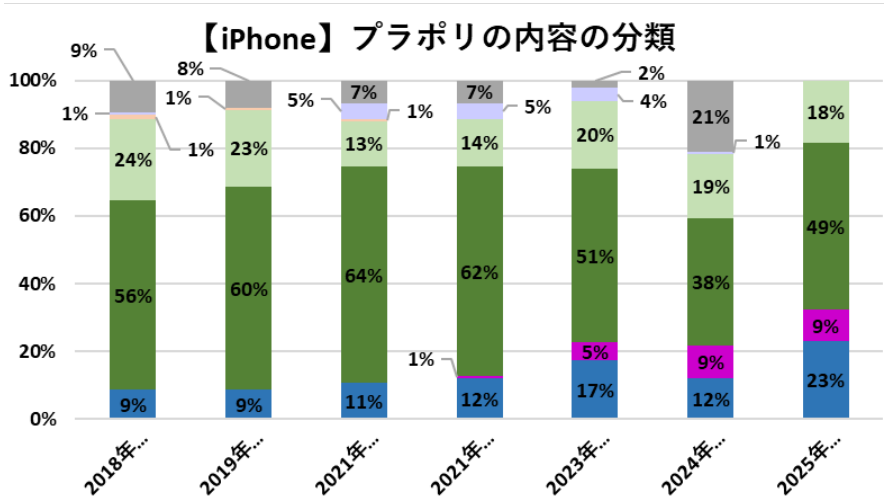
<SPSIの記載（p.18）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
  ① アプリケーション提供者の氏名又は名称及び連絡先等、② アプリケーション提供者が取得する利用者情報の項目等、③ アプリケーション提供者による取得方法、④ 利用目的の特定・明示、⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項、⑥ 同意取得の方法及び利用者関与の方法、⑦ 問合せ窓口 、⑧ プライバシーポリシーの変更を行う場合の手続、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、⑩ 委託に関する事項

<調査結果概要>

- 公式ストアのアプリのプラポリの分類について調査を行った結果は以下の通りである。
- アプリの掲載状況として、【Ｆ】（全く掲載なし）から順に【Ａ】（アプリ専用のプラポリがある）に近い方が望ましい。
- Android・iOSともに、【A】【B】【C-1】【C-2】の合計は、前回調査時よりも増加している。
- 【F】が減少している理由はプライバシーに関する意識が高まっているためと推測される。





【F】日本語もしくは英語のプラポリが記載されていない
【E】会社としての抽象的なポリシー（個人情報保護方針）があるだけ
【D】一般的なWebサイトのプラポリがあるだけ
【C-2】会社・サービス全体のプラポリだけあり、スマホアプリを意識した記載になっていない
【C-1】会社・サービス全体のプラポリだけあり、スマホアプリを意識した記載になっている
【B】会社・サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある
【A】個々のスマホアプリ専用のプラポリが用意されている

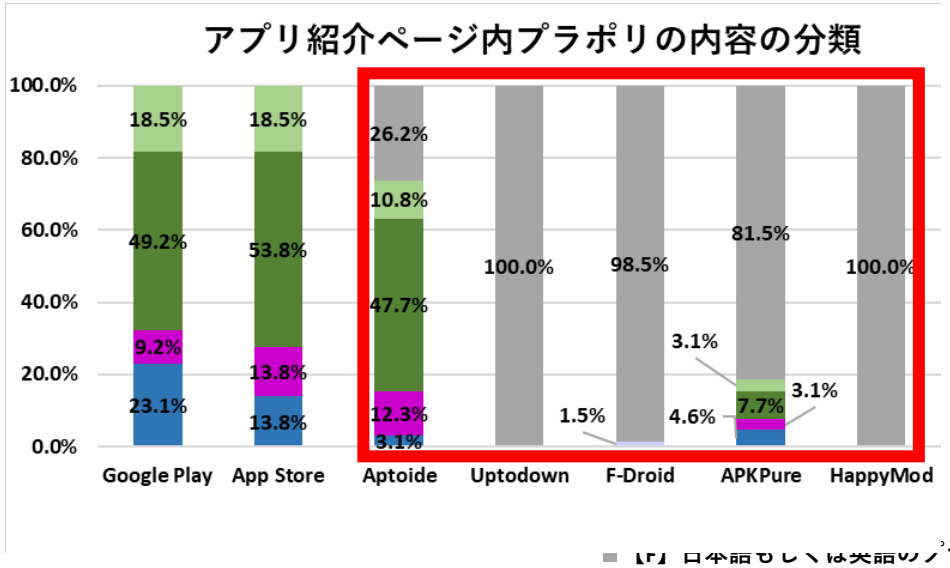
SPSI 1.2.1.1（プライバシーポリシーの作成） ②サードパーティアプリストア提供アプリ

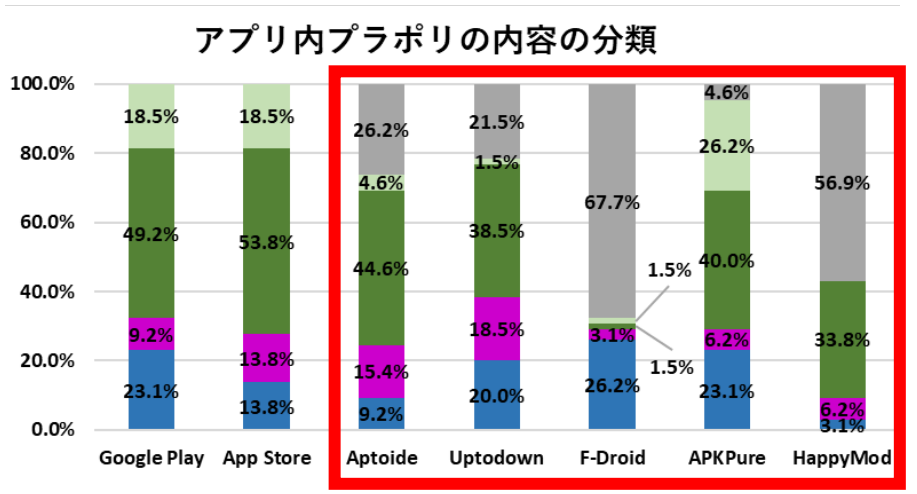
<SPSIの記載（p.18）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
  ① アプリケーション提供者の氏名又は名称及び連絡先等、② アプリケーション提供者が取得する利用者情報の項目等、③ アプリケーション提供者による取得方法、④ 利用目的の特定・明示、⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項、⑥ 同意取得の方法及び利用者関与の方法、⑦ 問合せ窓口 、⑧ プライバシーポリシーの変更を行う場合の手続、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、⑩ 委託に関する事項

<調査結果概要>

- 公式ストアに加えて、サードパーティストアで提供されるアプリのプラポリの分類の調査結果は下記の通りである。
- サードパーティストアではアプリ紹介ページ内において【F】（日本語もしくは英語のプラポリが記載されていない）の割合が多かった。アプリ内プラポリでは【A】【B】【C-1】の合計はサードパーティストアに比べて公式ストアが高い傾向があった。





【F】日本語もしくは英語のプラポリが記載されていない
【E】会社としての抽象的なポリシー（個人情報保護方針）があるだけ
【D】一般的なWebサイトのプラポリがあるだけ
【C-2】会社・サービス全体のプラポリだけあり、スマホアプリを意識した記載になっていない
【C-1】会社・サービス全体のプラポリだけあり、スマホアプリを意識した記載になっている
【B】会社・サービス全体のプラポリがあり、その中に個々のスマホアプリに関する記述がある
【A】個々のスマホアプリ専用のプラポリが用意されている

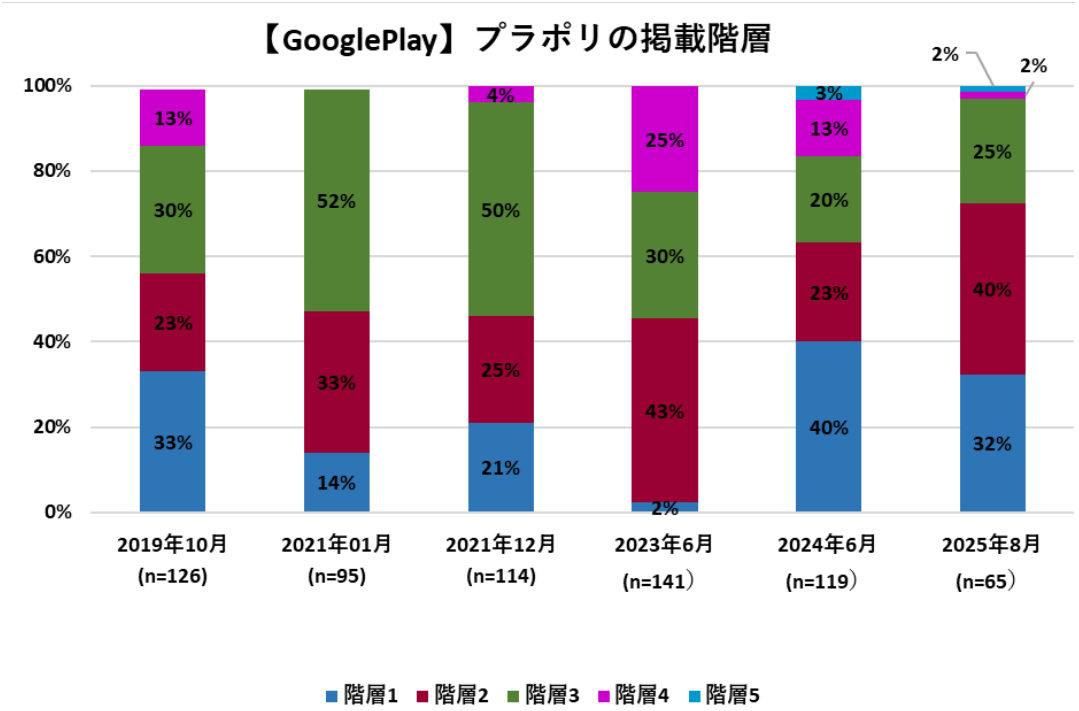
SPSI 1.2.1.1（プライバシーポリシーまでの階層数）①AppStoreとGooglePlay提供アプリ

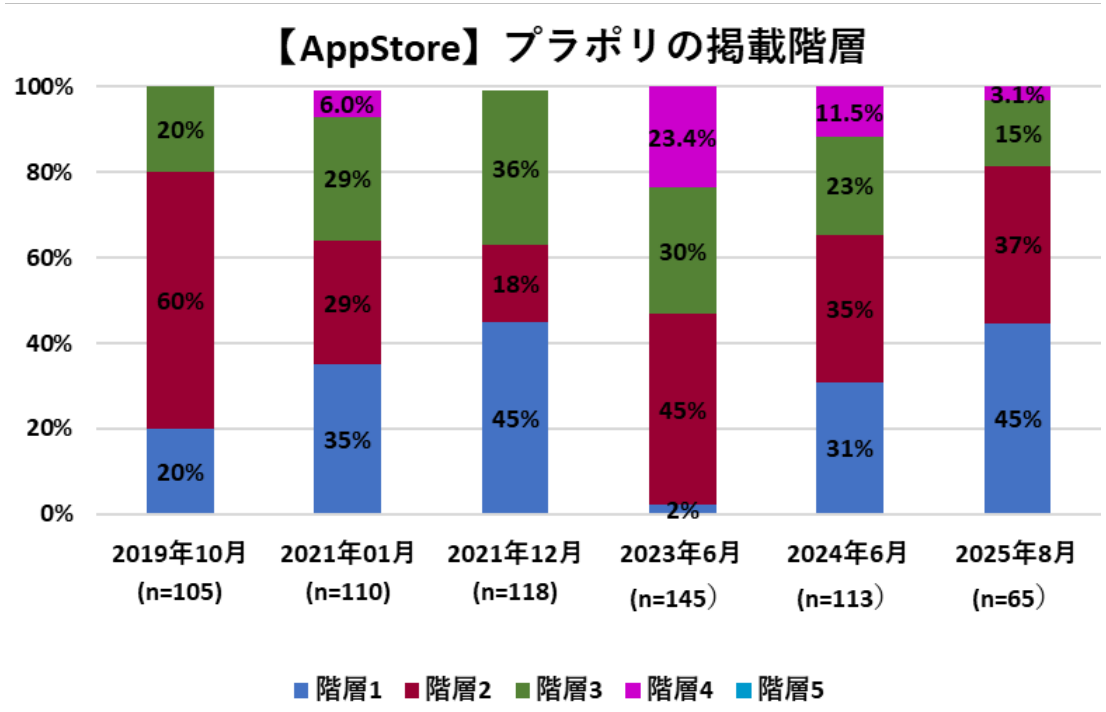
<SPSIの記載（p.18）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
  ① アプリケーション提供者の氏名又は名称及び連絡先等、② アプリケーション提供者が取得する利用者情報の項目等、③ アプリケーション提供者による取得方法、④ 利用目的の特定・明示、⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項、⑥ 同意取得の方法及び利用者関与の方法、⑦ 問合せ窓口 、⑧ プライバシーポリシーの変更を行う場合の手続、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、⑩ 委託に関する事項

<調査結果概要>

- 公式ストアで提供されるアプリのプラポリの掲載階層(プラポリに辿り着くための画面数)について調査を行った結果は以下の通りである。
- 利用者が容易に参照できるように階層数は少ないことが望ましい。
- **GooglePlay、AppStoreともに、3階層以内に掲載されているアプリの割合が増加**している。
  （ただし、この差異は、前回調査と今回調査対象としたアプリが異なることも要因として考えられることに留意が必要）





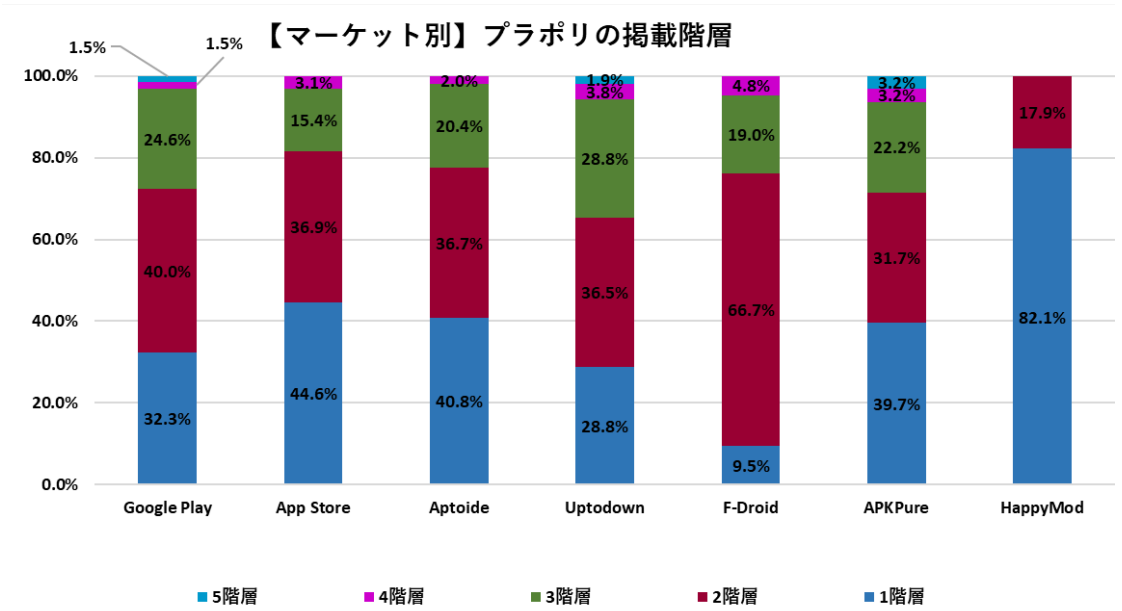
SPSI 1.2.1.1（プライバシーポリシーまでの階層数） ②サードパーティアプリストア提供アプリ

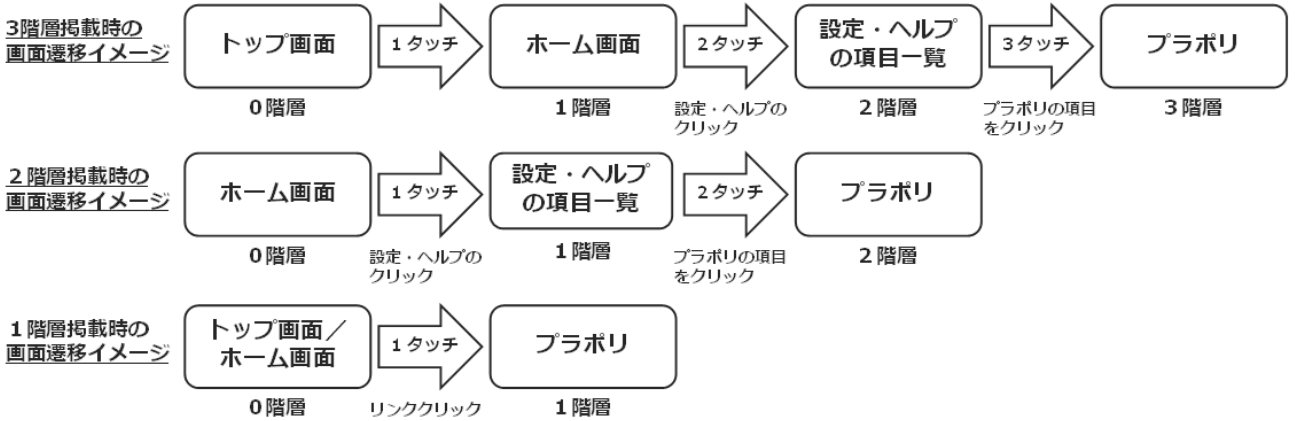
<SPSIの記載（p.18）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
  ① アプリケーション提供者の氏名又は名称及び連絡先等、② アプリケーション提供者が取得する利用者情報の項目等、③ アプリケーション提供者による取得方法、④ 利用目的の特定・明示、⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項、⑥ 同意取得の方法及び利用者関与の方法、⑦ 問合せ窓口 、⑧ プライバシーポリシーの変更を行う場合の手続、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、⑩ 委託に関する事項

<調査結果概要>

- 公式ストアに加えてサードパーティストアで提供されるアプリのプラポリの掲載階層(プラポリに辿り着くための画面数)について調査を行った結果は以下の通りである。
- 利用者が容易に参照できるように階層数は少ないことが望ましい。
- **F-Droidでは他のストアに比べて第二階層の割合が多く**、**HappyModでは第一階層のアプリが多い**結果となった。





SPSI 1.2.1.2（プライバシーポリシーの概要版掲載等）

<SPSIの記載（p.24）>

- アプリケーションをダウンロード又は利用開始しようとする者がスマートフォンの画面上で容易に理解できるように、プライバシーポリシーの分かりやすい概要を作成して利用者が容易に参照できる場所に掲示又はリンクを張る等、利用者にとって分かりやすい方法で示されることが望ましい
- プライバシーポリシーによる通知又は公表あるいは同意取得は、原則として利用者がアプリケーションをダウンロード又はインストールあるいは利用開始しようとする前に行うことが望ましく、それらの時点で行うことが難しい場合には、初回起動時に処理が実行される前に行うことが望ましい

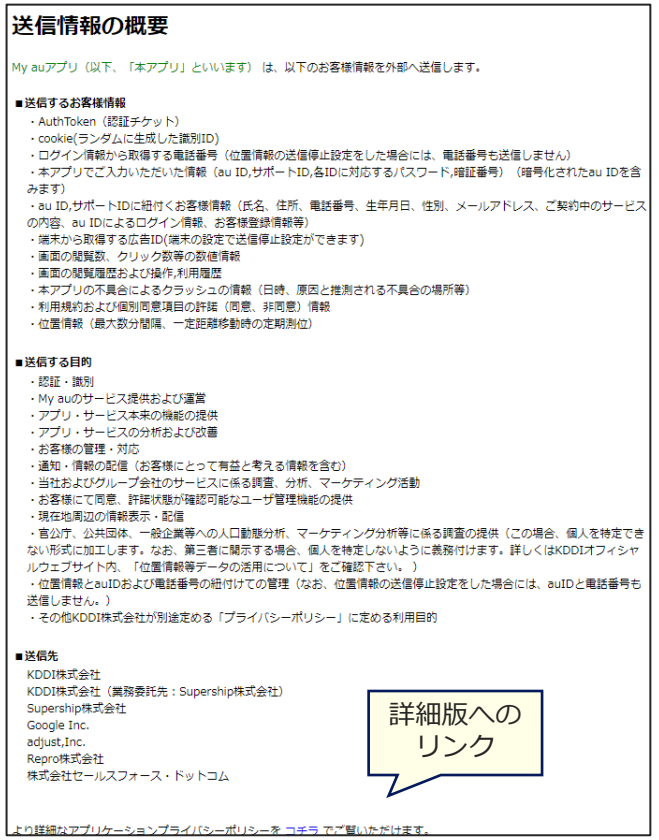
<調査結果概要>

- 公式ストアとサードパーティストアの概要版掲載率について調査を行った結果以下表の通りとなった。
- **概要版の掲載率は公式ストアにおいて3～6%程度、１部のサードパーティストアでは16%程度**確認できた。

<マーケット別のプラポリ概要版掲載率>

	有	無
Google Play	6%	94%
App Store	3%	97%
Aptoide	16%	84%
Uptodown	13%	87%
F-Droid	0%	100%
APKPure	3%	97%
HappyMod	0%	100%

<参考：概要版の事例（出典：My auアプリ）>



送信情報の概要

My auアプリ（以下、「本アプリ」といいます）は、以下のお客様情報を外部へ送信します。

■送信するお客様情報
・AuthToken（認証チケット）
・cookie(ランダムに生成した識別ID)
・ログイン情報から取得する電話番号（位置情報の送信停止設定をした場合には、電話番号も送信しません）
・本アプリでご入力いただいた情報（au ID,サポートID,各IDに対応するパスワード,暗証番号）（暗号化されたau IDを含みます）
・au ID,サポートIDに紐付くお客様情報（氏名、住所、電話番号、生年月日、性別、メールアドレス、ご契約中のサービスの内容、au IDによるログイン情報、お客様登録情報等）
・端末から取得する広告ID(端末の設定で送信停止設定ができます)
・画面の閲覧数、クリック数等の数値情報
・画面の閲覧履歴および操作,利用履歴
・本アプリの不具合によるクラッシュの情報（日時、原因と推測される不具合の場所等）
・利用規約および個別同意項目の許諾（同意、非同意）情報
・位置情報（最大数分間隔、一定距離移動時の定期測位）

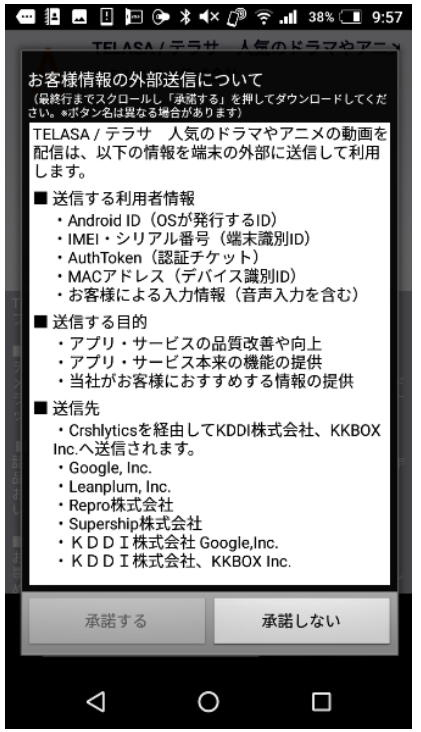
■送信する目的
・認証・識別
・My auのサービス提供および運営
・アプリ・サービス本来の機能の提供
・アプリ・サービスの分析および改善
・お客様の管理・対応
・通知・情報の配信（お客様にとって有益と考える情報を含む）
・当社およびグループ会社のサービスに係る調査、分析、マーケティング活動
・お客様にて同意、許諾状態が確認可能なユーザ管理機能の提供
・現在地周辺の情報表示・配信
・官公庁、公共団体、一般企業等への人口動態分析、マーケティング分析等に係る調査の提供（この場合、個人を特定できない形式に加工します。なお、第三者に開示する場合、個人を特定しないように義務付けます。詳しくはKDDIオフィシャルウェブサイト内、「位置情報等データの活用について」をご確認下さい。）
・位置情報とauIDおよび電話番号の紐付けての管理（なお、位置情報の送信停止設定をした場合には、auIDと電話番号も送信しません。）
・その他KDDI株式会社が別途定める「プライバシーポリシー」に定める利用目的

■送信先
KDDI株式会社
KDDI株式会社（業務委託先：Supership株式会社）
Supership株式会社
Google Inc.
adjust,Inc.
Repro株式会社
株式会社セールスフォース・ドットコム

詳細版へのリンク

より詳細なアプリケーションプライバシーポリシーを コチラ でご覧いただけます。

<参考：概要版プラポリによる同意の例>
(出典：TELASAアプリ)



SPSI 1.2.1.2（OSによるパーミッションの表示）

<SPSIの記載（p.25）>

- アプリケーションに関するOSによるパーミッションは一般にアプリケーションがどのような情報にアクセスするかを示しているが、利用目的やスマートフォン外部への送信・第三者提供・共同利用の有無等の項目の記載がない場合には、OSによるパーミッションのみでは本項に示す通知又は公表あるいは同意取得として十分ではないことに留意することが強く求められる
- OSによるパーミッションが表示される際に別途アプリケーション提供者が作成したプライバシーポリシーのリンク先を示すなどの方法により通知又は公表を行うか、必要に応じて個別の情報に関する同意取得等を行うことが期待される

<調査結果概要>

- 各OSにおけるパーミッションの表示について調査したところ、結果は以下の通りとなった。
- iOS、Androidともに**個人情報や機密情報を扱うアプリに対して、明確な説明と同意取得を求めている。**
- AppStoreのアプリ審査の際には利用者への利用目的の説明が不十分であると拒否される可能性がある。
- iOS、Androidともに**パーミッション表示時にプライバシーポリシーのリンク先を示す仕様にはなっていない。**

SPSI記載項目	iOS	Android
● 情報の利用目的やスマートフォン外部への送信・第三者提供・共同利用について、OSパーミッションにおける表示の仕方	アプリが電話帳などの情報にアクセスする際にパーミッションによるユーザー同意が義務付けられている。**パーミッションによるユーザー同意の際に利用目的を記載する必要があり**、正しく記載しないとAppStoreのアプリの審査の際にリジェクトとなる可能性がある。	Androidアプリでパーミッションをユーザーに説明する際は、Google Playポリシーに準拠した「認識しやすい開示と同意」が求められる。Googleは、ユーザーが予期しない形で**個人情報や機密情報を扱うアプリに対して、明確な説明と同意取得を求めている。**なぜその権限が必要なのか、どのように使われるのか、ユーザーが拒否した場合の影響などの記載が必要。
● OSによるパーミッションが表示される際に別途アプリケーション提供者が作成したプライバシーポリシーのリンク先を示すこと	パーミッション同意画面においては利用目的を記載することが可能であるが、**URLリンクの掲載のためのものではない**のが現状である。	パーミッション同意画面では**文字列の記載ができる仕様にはなっていない。**

SPSI 1.2.1.2（個別の同意取得の状況）

<SPSIの記載（p.25、26）>

- ① 個人情報を含む電話帳情報 アプリケーションが提供するサービスの目的に応じ必要とされる範囲（フィールド）を限定するとともに、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが望ましい
- ② センシティブ情報 不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要する情報を収集する場合については、取得する情報の項目を明示した上で、個別の情報に関する同意取得を行うことが強く求められる【基本的事項】
- ④ 利用者行動のトラッキング プライバシー侵害を回避する観点又は利用者利益の保護の観点から、事業者横断的なトラッキングを実施するために利用者情報を取得する際には、個別の情報に関する同意取得を行う

<調査結果概要>

- 各OSにおける個人情報（電話帳、センシティブ情報、広告ID）の同意取得状況について調査したところ、結果は以下の通りとなった。
- iOS、Androidともに**電話帳情報、センシティブ情報、利用者行動のトラッキングを行う際には同意取得が必要**な状況となっている。

SPSI記載項目	iOS	Android
① 個人情報を含む電話帳情報	電話帳情報にアクセスする際にはなぜ電話帳情報を利用する必要があるのか説明文を記載した上で、**ユーザ同意を得る**必要がある。	電話帳（連絡先）へのアクセス許可は、アプリがユーザーの連絡先情報を利用するために必要な権限である。**アプリが初めて連絡先情報へのアクセスを要求する際、ユーザーは許可または拒否を選択できる。**
② センシティブ情報	iOSでは、**アプリが個人情報にアクセスする際には、ユーザーの許可が必要**となっている。アクセスを許可するかどうかは、設定アプリの「プライバシーとセキュリティ」セクションで管理できる。アプリがアクセスを要求する際には、その理由がユーザーに表示され、許可を求められる。	Android端末における、いわゆる「センシティブ情報」へのアクセスをアプリに許可する際には、**ユーザーの同意が必要**。これは、アプリが連絡先、位置情報、カメラ、マイクなどの個人情報やデバイス機能にアクセスする際に、ユーザーに通知し、許可を求める仕組み。 センシティブ情報には、連絡先、位置情報、カレンダー、ストレージ、マイク、カメラ、SMS、電話帳などが該当する。
④利用者行動のトラッキング 広告ID等の識別子同意取得	iOSの広告ID（IDFA: Identifier for Advertisers）にアクセスするには、まず「設定」アプリを開き、「プライバシー」>「広告」>「広告識別子」の順に選択する。ユーザーは「広告トラッキングを制限」を有効にすることで、**IDFAの利用を制限できる。**	Androidの広告IDに関するパーミッションは、アプリがユーザーの広告IDにアクセスするために必要。ユーザーは、広告のパーソナライズ設定を管理し、広告IDの利用を許可または拒否できる。**アプリは、ユーザーの同意を得た上で、広告IDを送信する必要**がある。

SPSI 1.2.1.2（個別の同意取得の状況）

<SPSIの記載（p.27）>

- ⑤ 契約者・端末固有ID等、契約や端末に対して一義的に指定・作成され、利用者側で変更が困難であるが、幅広い主体により利用される可能性があるものがID等の情報を取得するアプリケーション提供者等において特定の個人の識別性を有する情報と結びつきうる形で利用される場合、同一IDの上に様々な情報が時系列的に蓄積し得ること、当該アプリケーション提供者等又は第三者において特定の個人の識別性を有する可能性があることから、個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱うことが強く求められる
- ⑥ GPS等による位置情報は、アプリケーションが提供するサービスの提供又は機能に直接関連する場合にのみ取得することが強く求められる望ましい【基本的事項】。また、アプリケーション提供者は、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが強く求められる【基本的事項】。

<調査結果概要>

- 各OSにおける個人情報（端末固有ID、位置情報）に関する同意取得状況について調査したところ、結果は以下の通りとなった。
- iOS、Androidともに、**IMEIアクセスに関しては制限がかかっており、位置情報取得を行う際には同意取得が必要**な状況となっている。

SPSI記載項目	iOS	Android
⑤ 契約者・端末固有ID等　個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱うことが強く求められる	iOSアプリが**IMEI(国際移動体装置識別番号)に直接アクセスすることはできない**。iOSのセキュリティポリシーにより、アプリはIMEIのようなデバイス識別子に直接アクセスすることが制限されている。代わりに、UDID (Unique Device Identifier) やVendor Identifierなどの代替手段が提供されているが、これらもプライバシー保護のため、iOSのバージョンによって制限が設けられている。	**Android端末のIMEI（国際移動体装置識別番号）にアクセスするには、特定のパーミッションが必要。**アプリがIMEIにアクセスする必要がある場合、ユーザーはインストール時にその権限を許可するかどうかを求められる。Android 10（API レベル 29）以降、IMEI やシリアル番号など、リセット不可能な ID に関して制限が追加されている。このような ID にアクセスできるのは、デバイス オーナーまたはプロファイル オーナーのアプリや、特別な携帯通信会社パーミッションを持っているアプリ、READ_PRIVILEGED_PHONE_STATE 特権パーミッションを持っているアプリに限られている。
⑥ GPS等による位置情報は、同意取得を行うことが強く求められる。取得する位置情報の粒度や、取得する条件について利用者が設定可能とする	iOS アプリは、許可プロンプトを通じて位置情報へのアクセスを要求する。ユーザーはこのプロンプトを通じてアクセスを許可または拒否することができる。ユーザーは設定アプリで各アプリの**位置情報へのアクセス権限を個別に管理**でき、「許可しない」「次回確認」「この App の使用中のみ」「常に許可」などのオプションを選択できる。また、各アプリの正確な位置情報のオン/オフを切り替えることもできる。	Androidの位置情報の利用を許可するには、「設定」アプリから「位置情報」メニューに移動し、位置情報サービスをオンにする。これによりデバイス全体の現在地取得が可能になり、さらに**特定のアプリに対して「常に許可」「アプリの使用中のみ許可」「許可しない」などの権限を設定できる。** また、特定のアプリにのみ位置情報の利用を許可することが可能。

SPSI 1.2.1.2（個別の同意取得の状況）

<SPSIの記載（p.27）>

- ⑦ 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得 通信相手等の特定の個人の識別性を有する場合があること、及び通信の内容を含むプライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが強く求められる望ましい【基本的事項】。
- ⑧ スマートフォンのアプリケーションの利用履歴やスマートフォンに保存された写真・動画 アプリケーションによるサービス提供のために必要な範囲で用いられる場合を除き、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが望ましい【望ましい事項】。また、アクセス範囲の限定等の設定を可能にする等、取扱いに留意することが望ましい【望ましい事項】。

<調査結果概要>

- 各OSにおける個人情報（メール内容、写真・動画）に関する同意取得状況について調査したところ、結果は以下の通りとなった。
- iOS、Androidともに、**メール内容や写真・動画の取得には同意取得が必要**な状況となっている。
- 写真や動画への**アクセス権限は設定画面から管理することが可能**である。
- 1部の写真のみアクセスするなどのアクセス制限のオプションについても提供されている。

SPSI記載項目	iOS	Android
⑦ 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得	**メールの内容にアクセスするにはアカウント情報が必要**となる。 iOSアプリでメールにアクセスするには、通常、標準の「メール」アプリを使用するか、他のメールアプリをインストールして利用する。標準の「メール」アプリを使用する場合、設定からアカウントを追加する必要がある。	ユーザーのメールアドレスやメール本文は、個人を特定できる情報として個人情報保護法の対象になり、**アプリがこれらを取得・送信・保存・共有する場合、事前にユーザーの明示的な同意が必要。** Google Play Consoleでは、データセーフティセクションに情報を申告する必要がある。
⑧ スマートフォンのアプリケーションの利用履歴やスマートフォンに保存された写真・動画	写真へのアクセスを許可するiOSアプリを管理するには、「設定」>「プライバシーとセキュリティ」>「写真」に進む。「なし」「写真の追加のみ」「制限付きアクセス」「フルアクセス」などのオプションから選択し、各アプリの権限を管理できる。	Androidの「写真・動画の同意」とは、特定のアプリがデバイス内の写真や動画にアクセスする権限を許可する操作を指す。この同意は、各アプリ設定やAndroidのシステム設定から行え、アプリごとに「すべての写真へのアクセス」「一部の写真のみアクセス」「アクセスしない」といった選択肢がある。

SPSI 1.2.1.2（プライバシーポリシーの記載内容）①AppStoreとGooglePlay提供アプリ

<SPSIの記載（p.15、26）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項（※補足※下記表①～⑩を参照）について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
- 利用者情報が、プライバシーポリシーに反して、取得され又は取り扱われていることが明確である場合等については、利用者からの申出を受け利用の停止又は消去を行うことが強く求められる望ましい【基本的事項】。また、その手段についてプライバシーポリシーへ記載する等、利用者にとって参照しやすい方法で情報提供されることが強く求められる【基本的事項】。

<調査結果概要>

- AppStore、Google Playのプライバシーポリシーの内容を調査したところ、結果は以下のとおり。
- Android、iPhoneともに、**⑦問い合わせ窓口・苦情の申出先、⑧プライバシーポリシーの変更を行う場合の手続、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については5%以上増加**している。
- **⑤-1 送信停止の手順の記載率については前回調査よりも低下**していた。

SPSI10項目の記載率（プラポリが存在していたアプリ数を母数として割合を算出。）

	番号	項目		Android				iPhone			
				2021年12月 (n=146)	2023年6月 (n=149)	2024年6月 (n=147)	2025年8月 (n=65)	2021年12月 (n=140)	2023年6月 (n=150)	2024年6月 (n=148)	2025年8月 (n=65)
SPSI	①	情報を取得するアプリ提供者等の氏名又は名称		97%	97%	93%	98%	99%	99%	93%	97%
	②	取得される情報の項目		93%	89%	91%	88%	84%	89%	87%	97%
	③	取得方法		71%	80%	83%	82%	73%	81%	78%	85%
	④	利用目的の特定・明示		95%	97%	95%	94%	95%	99%	97%	95%
	⑤	通知・公表又は同意取得の方法、利用者関与の方法	⑤－１.送信停止の手順の記載（送信停止の手順）	24%	56%	29%	17%	30%	60%	27%	18%
			⑤－２.利用者情報の削除の記載（利用者情報の削除）	61%	83%	85%	88%	76%	85%	81%	95%
	⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	⑥－１.利用者情報の第三者への送信の有無の記載	96%	91%	95%	89%	94%	89%	96%	98%
			⑥－２.利用者情報の送信先の記載	55%	81%	78%	36%	50%	82%	71%	50%
			⑥－３.情報収集モジュールに関する記載	43%	52%	52%	58%	30%	56%	52%	57%
	⑦	問い合わせ窓口・苦情の申出先		84%	94%	93%	98%	81%	99%	92%	100%
	⑧	プライバシーポリシーの変更を行う場合の手続		62%	80%	77%	89%	65%	86%	75%	88%
個人情報保護法	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			77%	77%	82%		76%	76%	86%
	⑩	委託に係る事項			64%	67%	82%		71%	74%	94%

SPSI10項目において、特に重要性が高いと考えられる項目（利用者情報の取扱いにおいて「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の4点は、最低限必要な情報であり、上記10項目の中でも、特に項目①、項目②、項目④、項目⑥はプラポリにおいて特に重要な項目と考えられることから、水色で網掛けしている。）

青字：前回調査から記載率から5%以上増加
赤字：前回調査から記載率から5%以上低下

SPSI 1.2.1.2（プライバシーポリシーの記載内容）②サードパーティアプリストア提供アプリ

<SPSIの記載（p.15、26）>

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩ （※補足※下記表①～⑩を参照）までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し、利用者が容易に参照できる場所に掲示又はリンクを張ることが強く求められる【基本的事項】。
- 利用者情報が、プライバシーポリシーに反して、取得され又は取り扱われていることが明確である場合等については、利用者からの申出を受け利用の停止又は消去を行うことが強く求められる望ましい【基本的事項】。また、その手段についてプライバシーポリシーへ記載する等、利用者にとって参照しやすい方法で情報提供されることが強く求められる【基本的事項】。

<調査結果概要>

- AppStore、Google Play に加え６つのサードパーティストアのプライバシーポリシーの内容を調査したところ、結果は以下のとおり。
- **F-Droidでは全体的に記載率が低い**傾向が見られた。海外のアプリが多いことが原因であると考えられる。
- **⑤-1 送信停止の手順と⑤-2 利用者情報の削除の記載率については公式ストアと比べるとサードパーティストアの記載率が低い**傾向がある。

SPSI10項目の記載率（プラポリが存在していたアプリ数を母数として割合を算出。）

	番号	項目		Google Play (n=65)	App Store (n=65)	Aptoide (n=61)	Uptodown (n=52)	F-Droid (n=21)	APKPure (n=63)	HappyMod (n=28)
SPSI	①	情報を取得するアプリ提供者等の氏名又は名称		98%	97%	97%	96%	71%	98%	100%
	②	取得される情報の項目		88%	97%	95%	96%	62%	79%	96%
	③	取得方法		82%	85%	89%	94%	52%	63%	93%
	④	利用目的の特定・明示		94%	95%	90%	98%	52%	94%	100%
	⑤	通知・公表又は同意取得の方法、利用者関与の方法	⑤－１.送信停止の手順の記載（送信停止の手順）	17%	18%	13%	10%	5%	27%	14%
			⑤－２.利用者情報の削除の記載（利用者情報の削除）	88%	95%	77%	79%	33%	83%	86%
	⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	⑥－１.利用者情報の第三者への送信の有無の記載	89%	98%	93%	90%	48%	94%	100%
			⑥－２.利用者情報の送信先の記載	36%	50%	18%	34%	33%	48%	68%
			⑥－３.情報収集モジュールに関する記載	58%	57%	43%	40%	14%	48%	57%
	⑦	問い合わせ窓口・苦情の申出先		98%	100%	89%	92%	81%	95%	96%
	⑧	プライバシーポリシーの変更を行う場合の手続		89%	88%	84%	88%	71%	81%	82%
個人情報保護法	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		82%	86%	84%	81%	19%	71%	32%
	⑩	委託に係る事項		82%	94%	79%	77%	33%	73%	68%

SPSI10項目において、特に重要性が高いと考えられる項目（利用者情報の取扱いにおいて「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の4点は、最低限必要な情報であり、上記10項目の中でも、特に項目①、項目②、項目④、項目⑥はプラポリにおいて特に重要な項目と考えられることから、水色で網掛けしている。）

赤字：他のストアよりも記載率が低い項目

SPSI 1.2.1.2（プライバシーポリシー等の運用）、 1.2.1.3 (苦情相談への対応体制の確保)

<SPSIの記載（p.26、30）>

- こどもが利用する可能性があるサービスを企画・開発する際には、こどものプライバシーを高い水準で確保するための適切な措置を講じることが望ましい【望ましい事項】。例えば、プライバシーポリシーを簡潔で目立つように、利用者の年齢に適した明確な表現で記載したりすることが考えられる【望ましい事項】。
- 利用者が利用者情報の範囲・取扱方法について同意した場合であっても、その同意の後に、簡単にアクセスでき、かつ、分かりやすい方法で当該同意の撤回等ができる機会を提供し、また、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【望ましい事項】。
- 利用者情報を取得するアプリケーション提供者は、利用者情報の取扱いに関する苦情や相談の適切かつ迅速な処理に努める。具体的には、苦情相談の窓口・連絡先を設置する等必要な体制の整備に努めることが強く求められる

<調査結果概要>

- AppStore、Google Play に加え、6 つのサードパーティストアについて脆弱性の窓口、同意撤回方法、子供向けプライバシーポリシーの有無について調査をしたところ、結果は以下のとおり。
- **脆弱性情報や問い合わせ窓口・苦情の申し出の窓口については各アプリで掲載している割合が高かった**。
- 同意撤回方法の記載については公式ストアとサードパーティストアで大きな差異は見られなかった。
- **子供向けプライバシーポリシーについては公式ストアでは半数程度のアプリが掲載をしていた**。

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=65)	(n=65)	(n=61)	(n=51)	(n=21)	(n=63)	(n=28)
① 脆弱性情報の窓口・連絡先	98%	100%	89%	92%	81%	95%	96%
② 同意撤回方法の記載	14%	18%	36%	12%	5%	16%	21%
③子供向けプライバシーポリシーの有無	52%	51%	62%	51%	19%	37%	71%

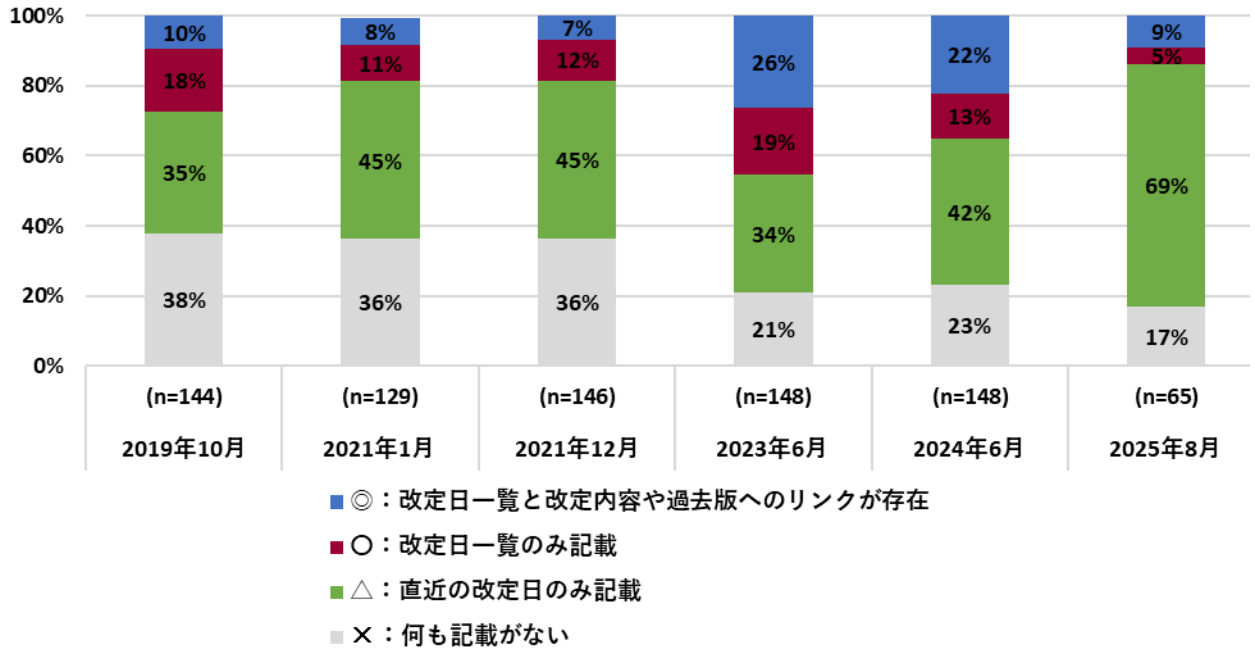
SPSI 1.2.1.2（プライバシーポリシー変更時の対応） ①AppStoreとGooglePlay提供アプリ

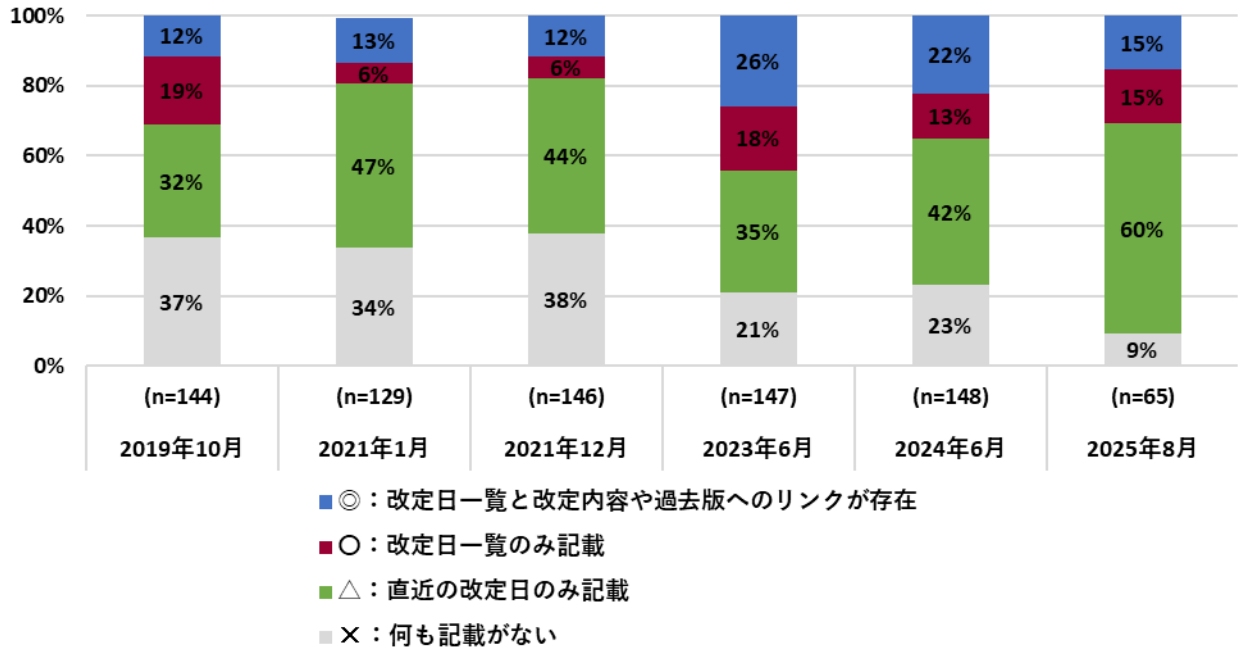
<SPSIの記載（p.30）>

- アプリケーションの更新等によりプライバシーポリシーを変更する場合は、利用者に対し、通知することが強く求められる【基本的事項】。

<調査結果概要>

- AppStore、Google Play で提供されるアプリのプライバシーポリシーの改定履歴の調査をしたところ、結果は以下の通りとなった。
- **AppStore、GooglePlayともに「△：直近の改定日のみ記載」が増加**している。
- **AppStoreでは「〇：改定日一覧のみ記載」が少し増加**している。





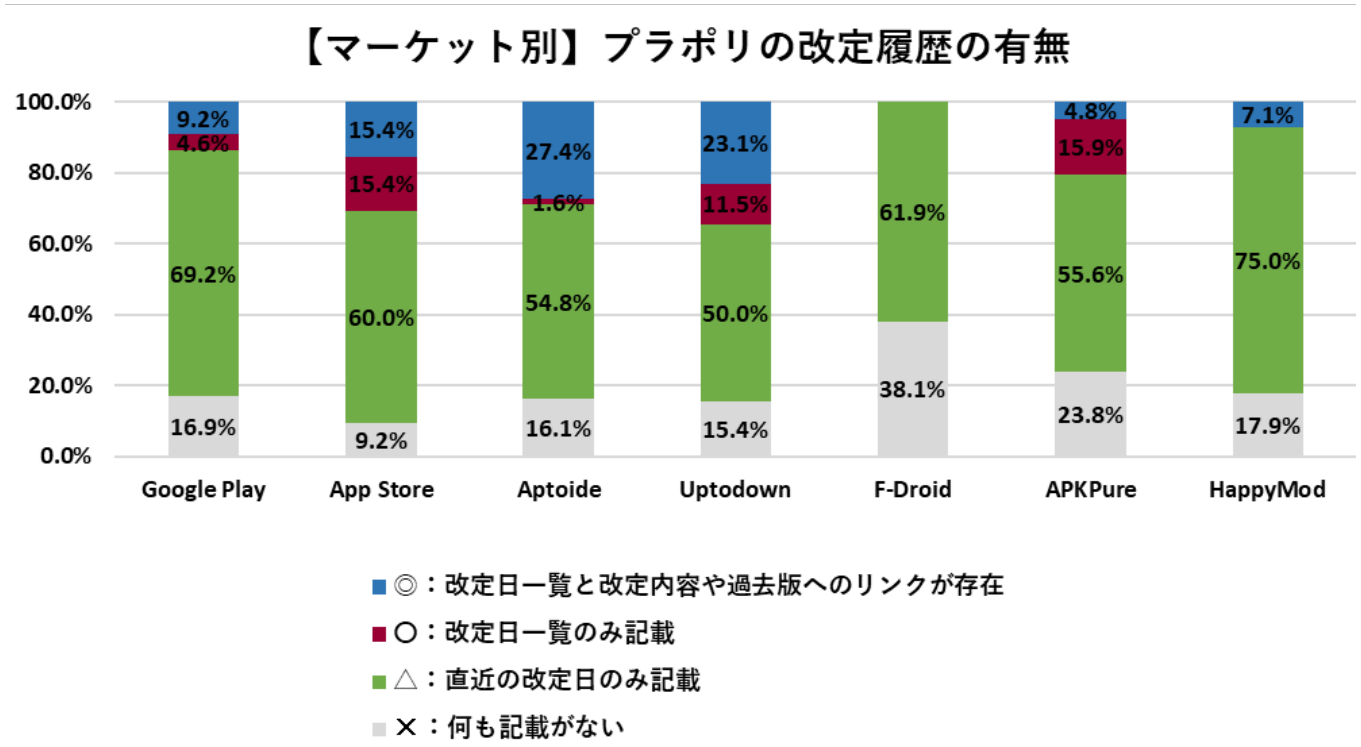
SPSI 1.2.1.2（プライバシーポリシー変更時の対応） ②サードパーティアプリストア提供アプリ

<SPSIの記載（p.30）>

- アプリケーションの更新等によりプライバシーポリシーを変更する場合は、利用者に対し、通知することが強く求められる【基本的事項】。

<調査結果概要>

- AppStore、Google Play 、サードパーティストアで提供されるアプリのプライバシーポリシーの改定履歴の調査をしたところ、結果は以下の通りとなった。
- **AptoideやUptodownでは「◎：改定日一覧と改定内容や過去版へのリンクが存在」の割合が他のマーケットよりも多かった。**
- F-Droidでは「×：何も記載がない」の割合が1番多かった。



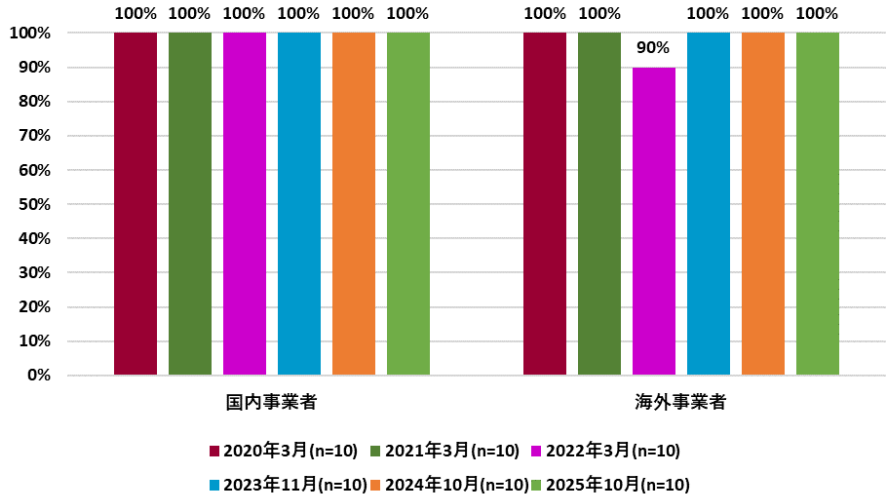
SPSI 1.2.2.1（情報集モジュール提供者の対応）、 1.2.2.2 (プライバシーポリシー等の運用)

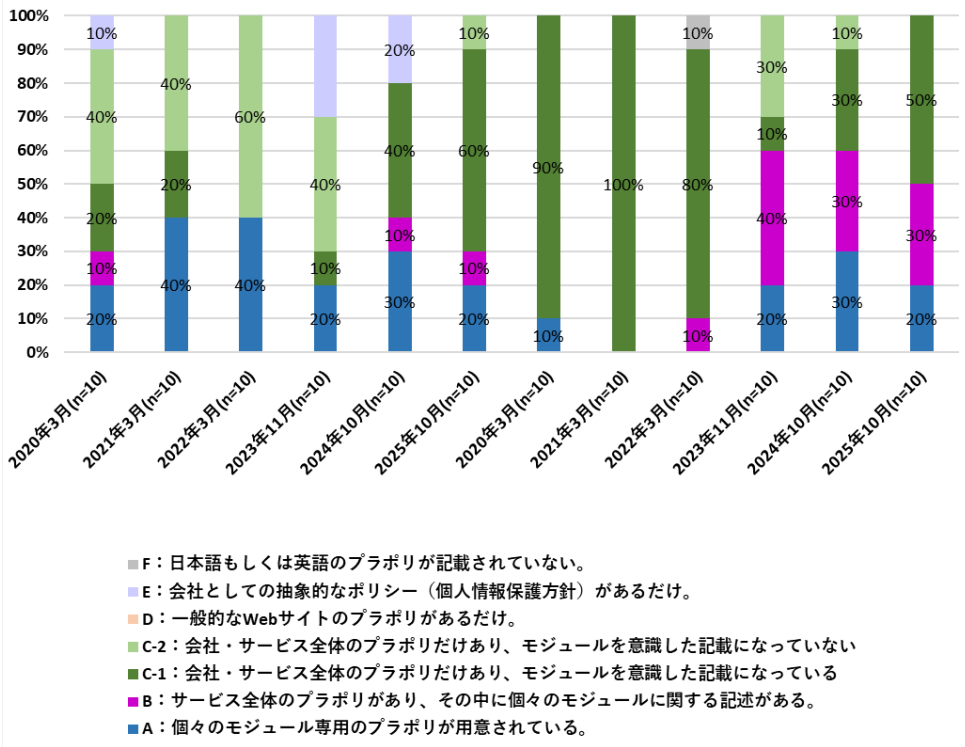
<SPSIの記載（p.33、34）>

- スマートフォンから利用者情報を収集する情報収集モジュール提供者は、1.2.1.1を踏まえ、プライバシーポリシーを作成することが望ましい。
- 情報収集モジュール提供者は、関連する内容を含むプライバシーポリシーを公表し、アプリケーション提供者へ通知することが強く求められる。
- アプリケーションの利用者から、情報収集モジュール提供者に対し、取得した利用者情報に関する問合せ又は取得した利用者情報の消去等の申出があった場合、必要に応じてアプリケーション提供者と協力し、これに応じることが強く求められる

<調査結果概要>

- 情報収集モジュール提供者のプラポリ掲載率を調べた結果は以下の通りとなった。
- **情報収集モジュール提供者のプラポリの掲載率は国内・海外事業者ともに100%となった。**
- 国内事業者のモジュールを意識した記載のプラポリが増加したことで、モジュールを意識した記載のプラポリの割合（【A】【B】【C-1】の合計）は90%となっている。
- 海外事業者ではモジュールを意識した記載のプラポリの割合（【A】【B】【C-1】の合計）は増加していた。





※ 掲載率：プライバシーポリシーや個人情報保護方針やこれらに準ずる記載されたページが事業者のウェブページ上で見つかれば「プラポリ有」と判断。（「個々の情報収集モジュール、もしくは広告ネットワーク等のサービスに関するプラポリが作成されていること」、「SPSI10項目が適切に記載されていること」を示すものではない）

SPSI 1.2.2.3（苦情相談への対応体制の確保）

<SPSIの記載（p.34）>

- 苦情相談への対応体制の確保及び安全管理措置については、1.2.1.3、1.2.1.4及び1.2.1.6を踏まえて取り組むことが強く求められる

<調査結果概要>

- 情報収集モジュール提供者の苦情相談窓口やプラポリの記載内容について調べた結果は以下の通りとなった。
- **情報収集モジュール提供者の⑦（苦情の申出先）は国内・海外事業者ともに100%となった。**
- 昨年度と比較すると、国内・海外事業者ともに④（利用目的の特定・明示）、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）、⑩（委託に係る事項）の割合が高くなっている。これは情報収集モジュールの利用目的、データポータビリティ、委託に関する事項の浸透が進んでいるためと推察される。

番号	項目		国内事業者				海外事業者			
			2022年3月 (n=10)	2023年11月 (n=10)	2024年10月 (n=10)	2025年10月 (n=10)	2022年3月 (n=9)	2023年11月 (n=10)	2024年10月 (n=10)	2025年10月 (n=10)
①	情報を取得するアプリ提供者等の氏名又は名称		100%	100%	100%	100%	100%	100%	100%	100%
②	取得される情報の項目		70%	70%	60%	60%	100%	100%	90%	100%
③	取得方法									
④	利用目的の特定・明示		100%	90%	80%	90%	100%	100%	80%	100%
⑤	通知・公表又は同意取得の方法、利用者関与の方法	⑤－１.送信停止の手順の記載（送信停止の手順）	30%	30%	70%	60%	89%	50%	60%	60%
		⑤－２.利用者情報の削除の記載（利用者情報の削除）	70%	60%	50%	90%	89%	80%	70%	100%
⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	⑥－１.利用者情報の第三者への送信の有無の記載	100%	90%	70%	100%	100%	90%	70%	100%
		⑥－２.利用者情報の送信先の記載	30%	80%	50%	30%	33%	90%	70%	70%
		⑥－３.情報収集モジュールに関する記載								
⑦	問い合わせ窓口・苦情の申出先		100%	100%	100%	100%	100%	60%	70%	100%
⑧	プライバシーポリシーの変更を行う場合の手続		50%	80%	80%	80%	100%	70%	70%	100%
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			80%	0%	60%		80%	40%	90%
⑩	委託に係る事項			90%	40%	100%		20%	20%	100%

SPSI10項目において、特に重要性が高いと考えられる項目（利用者情報の取扱いにおいて「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の4点は、最低限必要な情報であり、上記10項目の中でも、特に項目①、項目②、項目④、項目⑥はプラポリにおいて特に重要な項目と考えられることから、水色で網掛けしている。）

SPSI 1.3.1（アプリストアへのアプリ登録時の審査等）

<SPSIの記載（p.34）>

アプリストアへのアプリケーションの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

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの基準の作成状況を調査したところ、結果は以下のとおり。
- **AppStore、Google Play、Uptodown、F-droidについては開発者に対する審査ガイドラインを公開し公表**している。
- **Aptoideにおいては、マルウェア検知システムを具備するほか、品質管理チームによりアプリを手動でスキャンしてテストするなどの取組が進んでいる**。
- 一方で、APKPure、HappyMod、DMM Gamesについては、アプリの審査基準について公開されていない。

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
App Reviewガイドラインを公開しセキュリティ、安全性の要件を満たしているか審査を行っている。	**Google Playデベロッパープログラムポリシーを公開し、審査**を行っている。	Aptoideでは**マルウェア検出システムを具備**している。また、**品質管理チームによってアプリを手動でスキャンしてテスト**している。**信頼済みのアプリには緑色の信頼済みバッジ**が付いている。	**Uptodown's app publication criteriaが公開**されており、基準を満たさないアプリは拒否される。	アンチ機能と呼ばれる**セキュリティ要件を公開**しスパイウェアやダークパターンを排除している。	アプリの**署名の検証は行っているが、厳格な審査は行っていない。**	MODは、**限定的なウイルススキャンと他のユーザーが機能性・安全性を評価**するため、安全である保障はない。	**明確な技術的審査基準は公開されていな**い。

SPSI 1.3.1（アプリ掲載拒否時の理由通知）

<SPSIの記載（p.35）>

アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して適切なフィードバックを行うことが強く求められる

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアのアプリ掲載拒否時の対応状況を調査したところ、結果は以下のとおり。
- **公式ストアではアプリを拒否（リジェクト）する場合には規約や基準に基づいた拒否理由がフィードバックされる。**

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
AppStoreでアプリが拒否（リジェクト）された場合には**その理由がフィードバック**される。	GooglePlayでアプリが拒否（リジェクト）された場合には**その理由がフィードバック**される。	Aptoideでは自動検証とQAチームによる審査が行われる。**アプリの品質や配信基準に合致していない場合もリジェクトされる**可能性がある。Aptoide Connectを通じて配信するには、Certified Developer Programへの参加が必要。	Uptodownではアプリのリジェクトは公開後でも発生する。アップデートで**基準違反が見つかると、公開済みでも削除される**可能性がある。違反が重大な場合はアカウント停止となる。意図的な回避行為は、開発者アカウントの永久停止対象になる	F-Droidでアプリがリジェクト（却下）される主な理由は、自由でオープンなソフトウェアの原則に反する要素が含まれている場合である。F-DroidはGoogle Playなどの商用ストアとは異なり、完全にオープンソースであることが前提となるため**審査基準も独自かつ厳格。**	APKPureはGoogle PlayやApp Storeでリジェクトされたアプリでも受け入れる傾向があるが、**違法性やセキュリティリスクがあるものは拒否される。**アプリ提出後は「アップロード検証」→「レビュー」→「公開」の流れで、数日以内に結果が通知される。	HappyModの審査は「技術的な動作確認」と「ユーザー評価」に基づくが、MODの**品質が低いと、自動的に非公開になる**こともある。開発者がMODを提出する際は、HappyMod公式サイトから申請可能。	DMM GAMESでアプリ（ゲーム）が**リジェクトされる理由は、合同会社EXNOAが定める開発者向け利用規約と審査基準に基づいて判断される。**

SPSI 1.3.1（アプリストアにおける情報表示場所の提供）

<SPSIの記載（p.35）>

アプリストアの個別のアプリケーションページ上にプライバシーポリシーや取得される情報の概要等の表示場所を提供する、表示すべき事項や標準的なアイコンを示す等、アプリケーション提供者等に対し、適切な対応を行うように支援することが望ましい

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの取得される情報の概要等の表示場所を調査したところ、結果は以下のとおり。
- **AppStore、Google Playではプライバシーポリシーや取得される情報の概要が義務化されている。**
- サードパーティストアでは取得される情報の概要が表示されていない。

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
AppStoreの個別のアプリケーションページではプライバシーポリシーの掲載が義務化されている。また、**プライバシーラベル**と呼ばれる取得される情報を表示する場所が存在する。	GooglePlayのアプリケーションページではプライバシーポリシーの掲載が義務化されている。また、**データセーフティ**と呼ばれる取得される情報を表示する機能がある。	Aptoide Connectを通じてアプリを提出する際、アプリのメタデータ入力フォームに「Privacy Policy URL」の項目がある。ここに、外部サイトに掲載したプライバシーポリシーのURLを入力する必要がある。**取得される情報の概要は表示されない。**	Uptodownではプライバシーポリシーの掲載は必須ではない。**取得される情報の概要は表示されない。**	F-Droidでアプリを公開する際、プライバシーポリシーの掲載は任意。F-Droidは完全にオープンソースであることを前提としたストアであり、メタデータファイルに必要な情報を記述することで、アプリの審査・公開が行われる。**取得される情報の概要は表示されない。**	プライバシーポリシー掲載は義務化されていない。**取得される情報の概要は表示していない。**	プライバシーポリシー掲載は義務化されていない。**取得される情報の概要は表示していない。**	プライバシーポリシー掲載は義務化されていない。**取得される情報の概要は表示していない。**

SPSI 1.3.1（不適切なアプリに関する連絡窓口の設置）

<SPSIの記載（p.35）>

説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応（アプリストアから削除する等）を実施するとともに、連絡通報窓口を設置することが望ましい

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの連絡通報用の窓口を調査したところ、結果は以下のとおり。
- **全てのストアで連絡通報用の窓口は用意されていた。**
- サポートフォームやGithub、ヘルプセンターを通じて窓口機能を提供しているケースがある。
- **HappyModでは72時間以内に回答をすると記載があり開発者に親切な説明をしている。**

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
アプリに関する問題を報告できる**App Store レポートデスク**が存在する。	**アプリに関する問題を報告できる窓口**が存在する。	Aptoideの各アプリページには「**Report Abuse（不正報告）**」ボタンがある。ただし、通報にはAptoideアカウントへのログインが必要。また、Aptoideの公式FAQによると、問題がある場合はサポートフォームから連絡できる。	**Uptodown サポートフォーム**（英語）やアプリページに通報する窓口がある。	公式メール、フォーラム、Githubなど４つの方法で通報することが可能。	公式サイトには明確な「通報窓口」ページは存在しないが、いくつかの方法で**不正なアプリやコンテンツを報告することができる。**	下記の**問い合わせ用のメールアドレスと問い合わせ用のフォーム**がある。 コンタクトフォームでは「すべてのメッセージを読み48-72時間以内に返信をする」と記載されている。	通報窓口にはゲーム内通報機能（相手のプロフィールにある通報するボタン）や**DMM GAMESヘルプセンターからの問い合わせができる。** また、各ゲーム内容に関する問い合わせとして、各ゲームページにあるお問い合わせフォームから直接運営に連絡できる仕組みがある。

SPSI 1.4.1.1（セキュリティ・バイ・デザインを確保するための取組）

<SPSIの記載（p.37）>

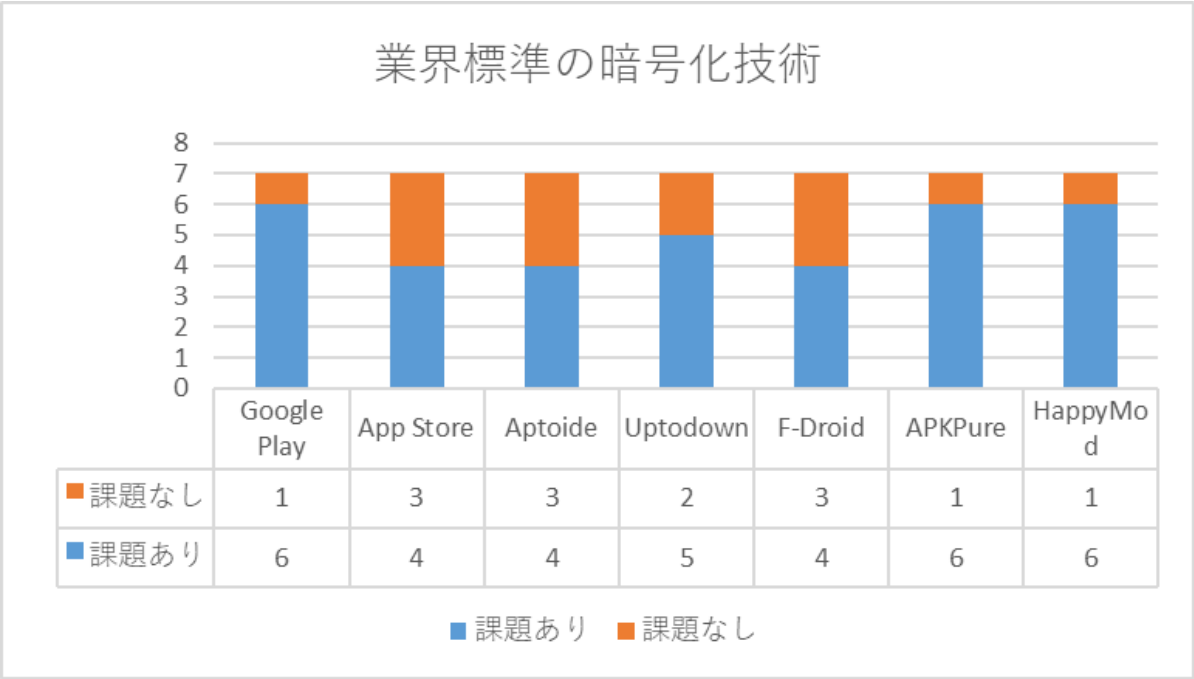
・アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが強く求められる望ましい（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング 等）【基本的事項】。
・アプリケーション提供者は、提供するアプリケーションにおいて使用する情報収集モジュールについて、セキュリティの確保の観点から内容を確認することが強く求められる【基本的事項】。

<調査結果概要>

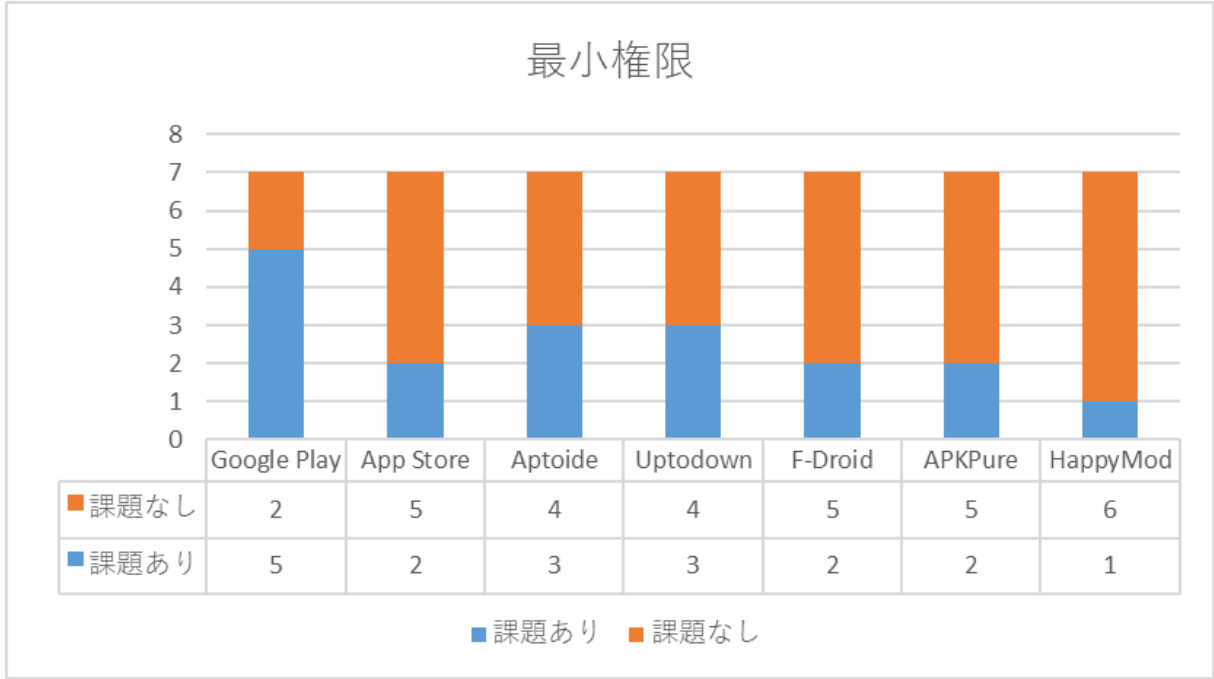
- **業界標準の暗号化技術、最小権限の状況について解析（※）を行った**結果を以下の図に示す。
- **ストア毎に大きな差分は無かったが、暗号化技術の利用、最小権限について課題があるアプリは一定数存在**した。

※ MASVS（モバイルアプリケーションのセキュリティ基準を体系化した国際的なフレームワーク）に沿って調査を実施

<調査結果>



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	1	3	3	2	3	1	1
課題あり	6	4	4	5	4	6	6



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	2	5	4	4	5	5	6
課題あり	5	2	3	3	2	2	1

SPSI 1.4.1.1（セキュリティ・バイ・デザインを確保するための取組）

<SPSIの記載（p.37）>

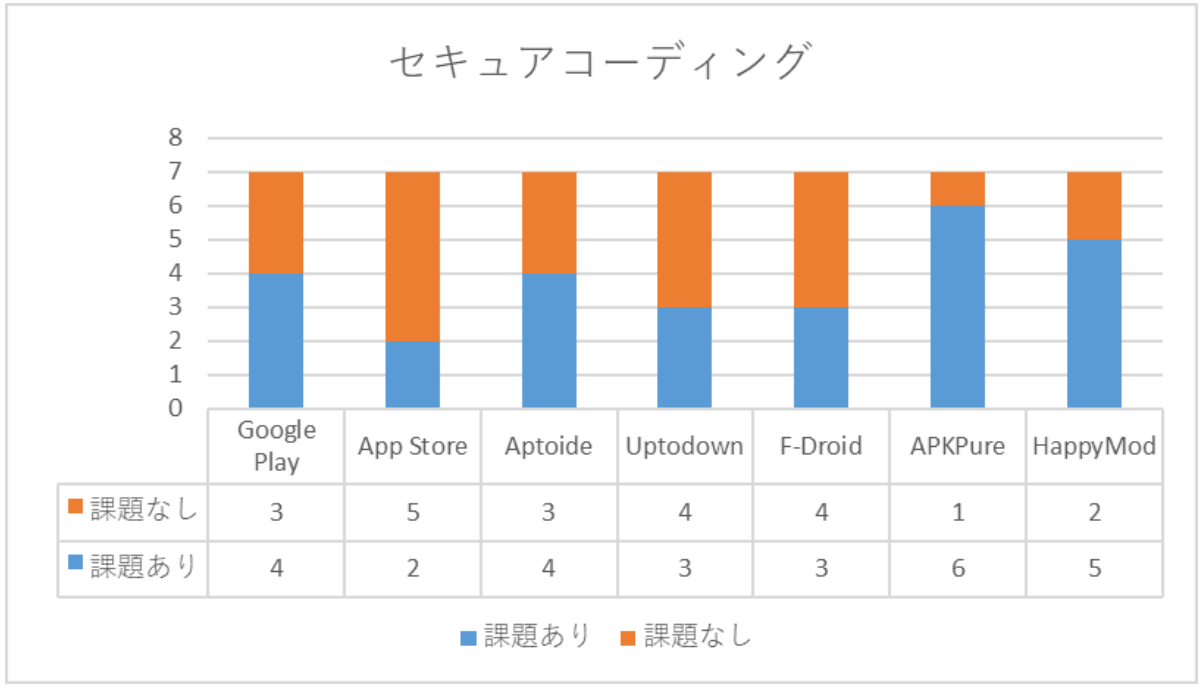
・アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが強く求められる望ましい（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング 等）【基本的事項】。
・アプリケーション提供者は、提供するアプリケーションにおいて使用する情報収集モジュールについて、セキュリティの確保の観点から内容を確認することが強く求められる【基本的事項】。

<調査結果概要>

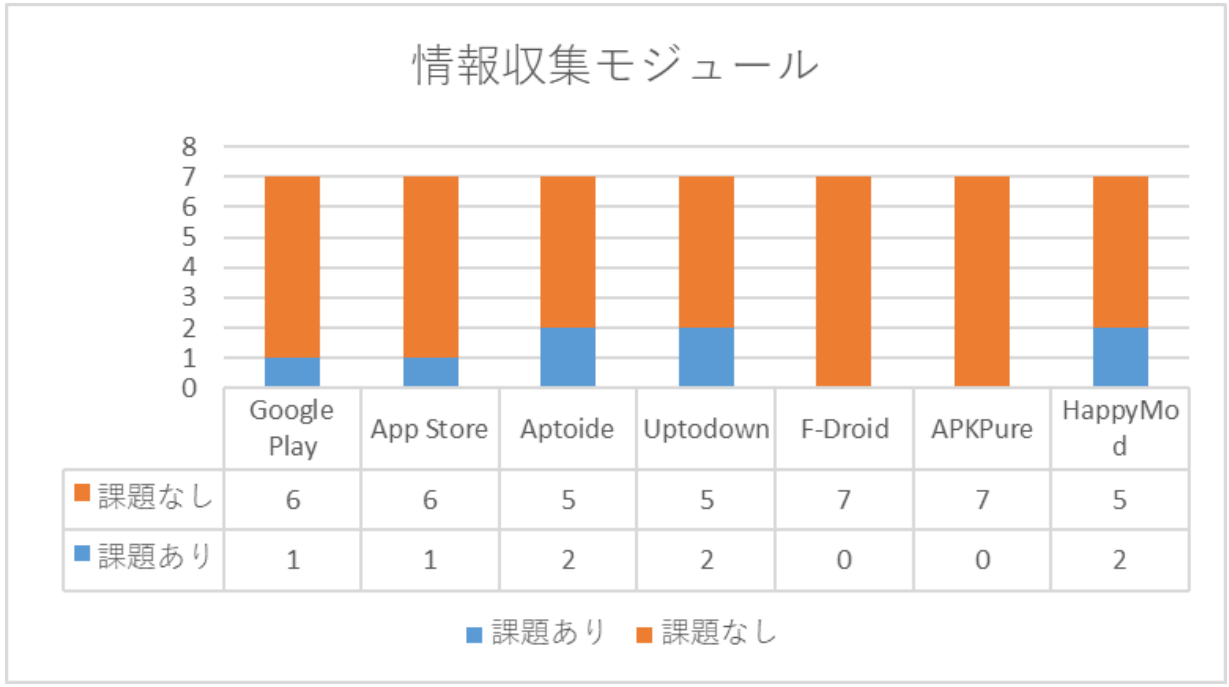
- **セキュアコーディング、情報収集モジュールの状況について解析（※）を行った**結果を以下の図に示す。
- **ストア毎に大きな差分は無かったがセキュアコーディングについて課題があるアプリは一定数存在**した。

※ MASVS（モバイルアプリケーションのセキュリティ基準を体系化した国際的なフレームワーク）に沿って調査を実施

<調査結果>



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	3	5	3	4	4	1	2
課題あり	4	2	4	3	3	6	5



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	6	6	5	5	7	7	5
課題あり	1	1	2	2	0	0	2

SPSI 1.4.1.1（セキュリティ・バイ・デザインを確保するための取組）

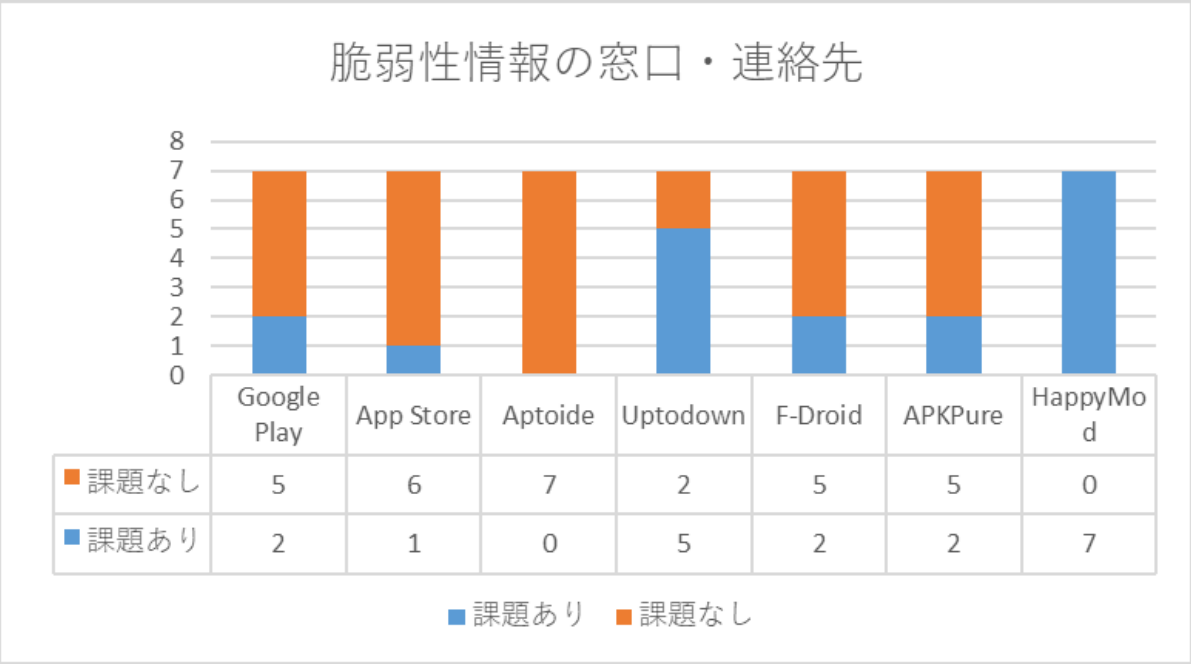
<SPSIの記載（p.37）>

［脆弱性があるアプリケーションへの対応等］
・アプリケーション提供者は、アプリケーションに係る脆弱性情報を継続して収集するとともに、アプリケーション内に発見された脆弱性について適切かつ迅速に報告を受けられるよう、脆弱性情報の窓口・連絡先を設置する等必要な体制をの整備するに努めることが強く求められる【基本的事項】。
・アプリケーション提供者は、アプリケーションを提供する際にはセキュリティの確保に影響を与え得る脆弱性が含まれないようにあらかじめ確認するとともに、セキュリティの確保に影響を与え得る脆弱性が発見された場合には、アプリケーションのアップデートを適切かつ迅速に提供する等、必要な対応を取ることが強く求められる望ましい【基本的事項】。

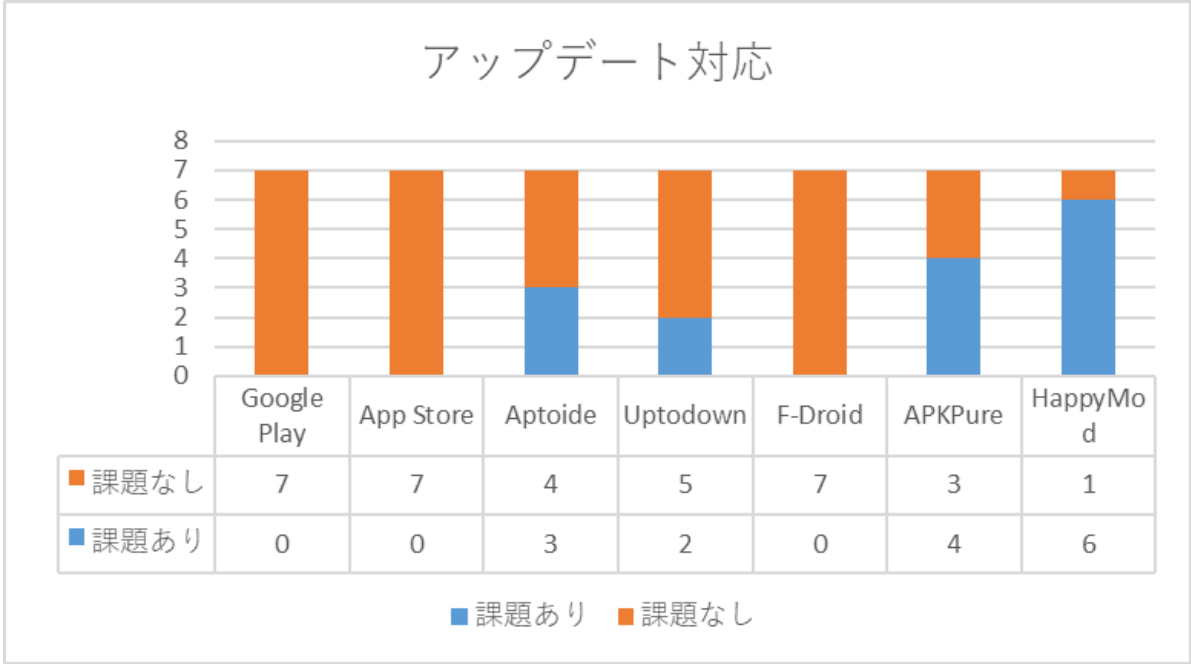
<調査結果概要>

- **脆弱性情報の窓口の設置状況、脆弱性発見時のアップデート対応**について調査を行った結果を以下の図に示す。
- **HappyModでは課題ありの件数が他のストアよりも多かった**ため、アプリの脆弱性やアップデート対応を意識したアプリ開発が求められる。

<調査結果>



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	5	6	7	2	5	5	0
課題あり	2	1	0	5	2	2	7



	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
課題なし	7	7	4	5	7	3	1
課題あり	0	0	3	2	0	4	6

SPSI 1.4.1.1（セキュリティ・バイ・デザインを確保するための取組）

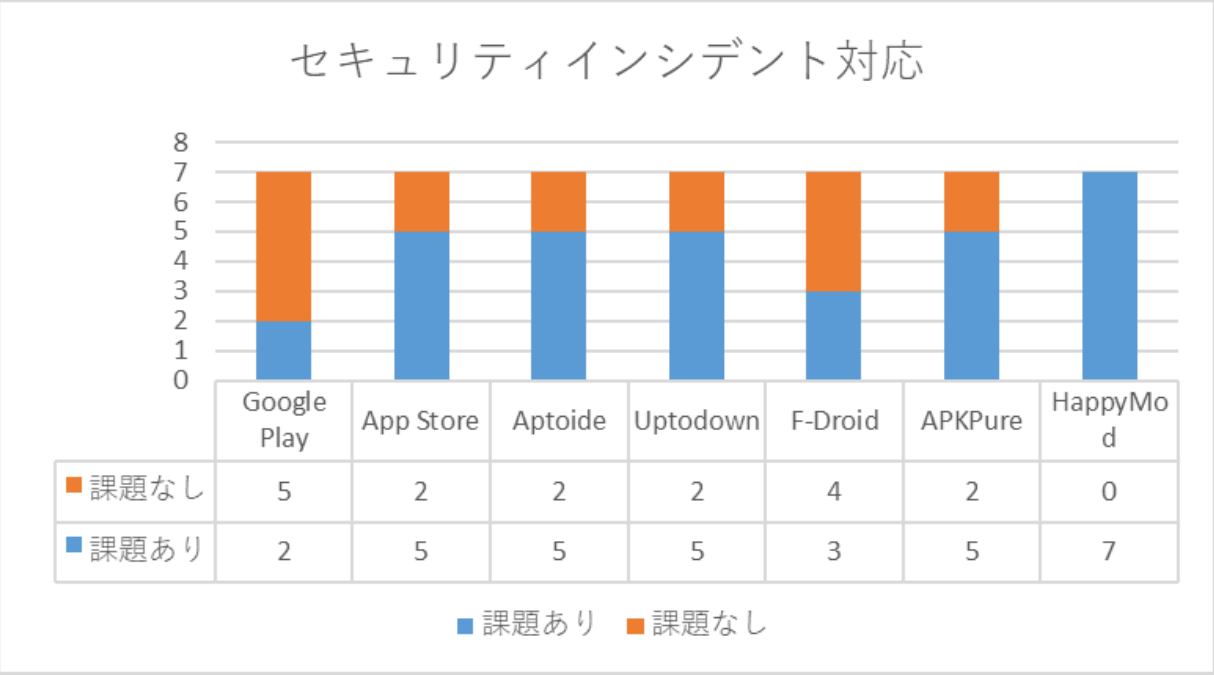
<SPSIの記載（p.38）>

・アプリケーション提供者は、提供するアプリケーションにおいて個人情報漏えい等のセキュリティインシデントが発覚した場合には、関係者に対して適切かつ迅速に周知することが強く求められる【基本的事項】。

<調査結果概要>

- **セキュリティインシデント発生時の対応について調査を行った**結果を以下の図に示す
- **HappyModでは課題ありの件数が他のストアよりも多かった**ため、セキュリティインシデントの発生を意識したアプリの開発が求められる。

<調査結果>



SPSI 1.4.2（アプリ審査におけるセキュリティ要件等）

<SPSIの記載（p.38）>

［アプリストアとしての基本的対応］
① アプリストア内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を審査する（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング 等）ことが期待される【ベンチマーク事項】。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの審査状況を調査したところ、結果は以下のとおり。
- **AppStore、Google Play、Uptodown、F-droidについては開発者に対する審査ガイドラインを公開し、当該ガイドラインの中にセキュリティ要件が示されている**。また、**当該セキュリティ要件を満たしていない場合、申請アプリは拒否される**。
- **Aptoideにおいては、マルウェア検知システムを具備するほか、品質管理チームによりアプリを手動でスキャンしてテストするなどの取組が進んでいる。**
- 一方で、APKPure、HappyMod、DMM Gamesについては、アプリの審査基準について公開されていない。

<アプリごとの調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
App Reviewガイドラインを公開しセキュリティ、安全性の要件を満たしているか審査を行っている。	**Google Playデベロッパープログラムポリシーを公開し、審査**を行っている。	Aptoideでは**マルウェア検出システムを具備**している。また、**品質管理チームによってアプリを手動でスキャンしてテスト**している。**信頼済みのアプリには緑色の信頼済みバッジ**が付いている。	**Uptodown's app publication criteriaが公開**されており、基準を満たさないアプリは拒否される。	アンチ機能と呼ばれる**セキュリティ要件を公開**しスパイウェアやダークパターンを排除している。	アプリの**署名の検証は行っているが、厳格な審査は行っていない。**	MODは、**限定的なウイルススキャンと他のユーザーが機能性・安全性を評価**するため、安全である保障はない。	**明確な技術的審査基準は公開されていな**い。

SPSI 1.4.2（アプリストアにおける利用者情報の取扱い）

<SPSIの記載（p.38）>

②アプリストア内で提供されるアプリケーションについて、利用者情報が保存・処理される法域、利用者情報へのアクセスが許可される者の範囲、利用者情報へアクセスする目的、アップデートの最終更新日等の情報を公開し、利用者が購入及びダウンロードする前に確認可能な場を設けることが望ましい。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの利用者情報の取り扱い方法や公開有無について調査したところ、結果は以下の通りとなった。
- **全てのアプリストアでアップデートの最終更新日については確認が可能**であった。
- 一方で、**アプリのダウンロード前にプライバシーポリシーの掲載がされていないストア（Uptodown、F-Droid、APKPure、HappyMod、DMM Games）では、利用者情報の取り扱いなどを確認することができなかった**。

<アプリごとの調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
AppStoreの個別のアプリケーションページでは、**AppPrivacyという項目があり、開発者はその中で利用者情報の扱われ方について説明を行う**必要がある。	Google Playでのアプリによる利用者情報の取り扱いについて、以下のようなルールと仕組みが定められており、プライバシーポリシーの設置を義務付けている。また、アプリ紹介ページにおいて、アップデートの最終更新日の情報が公開されている。	利用者情報の取り扱いについてはストア内の個々のアプリのページのプライバシーポリシーから確認することができる。リリース日と更新日についても同一ページで確認が可能。	**プライバシーポリシーについては掲載されていない**ため、利用者情報の取り扱いについては不明な場合がある。アップデートの更新履歴についてはストア上から確認ができる。	**プライバシーポリシーについては掲載されていない**ため、利用者情報の取り扱いについては不明な場合がある。アップデートの更新履歴についてはストア上から確認ができる。	**プライバシーポリシーについては掲載されていない**ため、利用者情報の取り扱いについては不明な場合がある。アップデートの更新履歴についてはストア上から確認ができる。	**プライバシーポリシーについては掲載されていない**ため、利用者情報の取り扱いについては不明な場合がある。アップデートの更新履歴についてはストア上から確認ができる。	**プライバシーポリシーについては掲載されていない**ため、利用者情報の取り扱いについては不明な場合がある。アップデートの更新履歴についてはストアからは確認ができなかった。

SPSI 1.4.2（アプリアップデート時の対応）

<SPSIの記載（p.38）>

④アプリケーション提供者からアップデートが提出された場合には、利用者に対してアプリケーションが最新版にアップデートされるよう促す等、必要な対応を取ることが望ましい【望ましい事項】。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアのアプリの最新版へのアップデート通知の有無について調査したところ、結果は以下の通りとなった。
- **アップデート時の通知機能については公式ストアでは用意されている一方でサードパーティストアでは用意されていないケースがあった**。
- **Aptoide、F-Droidではアプリの更新を通知する機能は無いが自動更新機能が存在する。**

<アプリごとの調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
AppStoreでは利用者に通知する仕組みが用意されている。自動アップデートをオンにすると常にアプリの状態が最新の状態になる。	Androidアプリでは個別に更新することも一度にまとめて更新することも、**自動的に更新することもできる。**重大なセキュリティ上の脆弱性を修正するものであると Google において判断された場合は、アプリのアップデートを適用することがある。	ログインしていない状態でアプリの更新を通知する機能はないが、アプリを**自動更新する機能はある。**	アプリのアップデート時にユーザに通知する機能がある。	ログインしていない状態でアプリの更新を通知する機能はないが、アプリを**自動更新する機能はある。**自動更新の間隔設定が可能。	アプリのアップデート時にユーザに通知する機能がある。	通知・更新機能は設定画面では見つけることができない。	通知・更新機能は設定画面では見つけることができない。

SPSI 1.4.2（アプリのサポート状況の確認）

<SPSIの記載（p.38）>

⑤アプリケーションが長期間アップデートされない場合には、アプリケーション提供者にアプリのサポート状況を確認することが望ましい

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストア上のアプリが長時間アップデートされない場合の対応について調査したところ、結果は以下の通りとなった。
- **AppStoreでは削除要件を設定し開発者に通知を送る仕組みを設けている。**
- **６つのサードパーティストアではアップデートを行わないこと自体がポリシー違反とはされていない。**

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
Appleは、以下の条件を満たすアプリを削除対象としている。 **・過去3年間にアップデートされていない** **・過去12カ月間にダウンロードがゼロ、または非常に少ない** このようなアプリに対して、Appleは開発者に通知を送り、最大90日間の猶予期間を与えた上で、アップデートがなければApp Storeから削除される可能性がある。	GooglePlayでは、重大なセキュリティ脆弱性があると判断した場合、ユーザーの設定に関係なく強制的にアップデートを適用することがある。アプリが古いAPIレベル（例：Android 12以前など）にしか対応していない場合、新しい端末では検索結果に表示されなくなることがある。	Aptoideにおいて、アプリ提供者が長期間アップデートを行わないこと自体は、直接的なポリシー違反とはみなされない。ただし、アプリが古いままで既知の脆弱性を含んでいる場合、ユーザーの安全を脅かすとして、Aptoideのマルウェア検出システムにより警告や削除対象になる可能性がある。	Uptodownでは、アプリ提供者が長期間アップデートを行わないこと自体は、公式ポリシー違反とは明記されていない。UptodownはGoogle Playのような厳格な審査制度はなく、アップデートの義務も明確には定められていない。ただし、開発元が不明なアプリや、**更新が止まっているアプリは信頼性が低いとされ、ユーザーに警告されることがある。**	F-Droidでは、アプリ提供者が長期間アップデートを行わないこと自体は、直接的なポリシー違反とはされていない。	アプリ提供者が長期間アップデートを行わないこと自体は、直接的なポリシー違反とはされていない。	アプリ提供者が長期間アップデートを行わないこと自体は、直接的なポリシー違反とはされていない。	アプリ提供者が長期間アップデートを行わないこと自体は、直接的なポリシー違反とはされていない。

SPSI 1.4.2（不正なアプリを発見した際の対応）

<SPSIの記載（p.39）>

⑦不正なアプリを発見した場合には、速やかに当該アプリを削除するとともに、当該アプリケーションを作成したアプリケーション提供者が開発した他のアプリケーションについても調査を行うことが望ましい【望ましい事項】。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストア上の不正アプリの削除事例を調査したところ、結果は以下の通りとなった。
- **AppStoreとGooglePlayでは不正なアプリの削除事例が多数発見された。**
- Aptoideでは数は多くはないが複数の削除事例が発見された。
- Uptodown、F-Droid、APKPure、HappyMod、DMM Gamesでは具体的な削除事例は見つからなかった。

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
海賊版アプリや詐欺的なアプリ、プライバシー侵害など**多数の削除事例があった。**	GooglePlayではセキュリティやコンテンツに問題があり**削除された事例が多数ある。**不正なアプリはPlayプロテクトで削除する仕組みがある。	Aptoideでの**削除事例は複数存在**し、アドウェアやなりすまし、マルウェア感染などでの削除事例がある。	Uptodownはアプリのセキュリティを最優先しており、悪意のあるアプリの削除事例として具体的なアプリ名が公に報じられたケースは見つからなかった。	アプリの削除はコミュニティやユーザーからの報告、ビルドエラー、ポリシー違反の検出によって行われる。削除要求は公式ドキュメントに基づいて処理され、透明性のある手続きが取られる。具体的なアプリ名は見つからなかった。	APKPureの公式アプリにトロイの木馬混入事例が見つかった。	HappyModで具体的な削除事例は見つけられていない。	「不正アプリの削除事例」について公式に公開された具体的な事例は確認されていない。

SPSI 1.5.1（青少年保護に係る取組　アプリケーション提供者）

<SPSIの記載（p.40）>

- アプリケーション提供者は、自ら提供するソーシャルネットワーキングサービスやユーザー生成コンテンツなど青少年と他の利用者の交流などが発生するアプリケーションにおいて、例えば、青少年による利用者情報の発信に係る注意喚起の仕組みや機能、青少年のプライバシーを含む情報など青少年保護の観点から不適切と考えられるコンテンツを報告する機能を備えるなど迅速に対応できる体制、ユーザーが不適切な言動を行うユーザーをブロックする機能などを備えることが望ましい【望ましい事項】。
- アプリケーション提供者は、提供するアプリケーションにおいて、青少年保護の観点から利用者情報の提供や課金の実施などのうち重要な判断が必要になる場合に、保護者の関与に関する仕組みや機能を備えることが強く求められる【基本的事項】。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストア上のアプリの青少年保護の仕組みを調査したところ、結果は以下の通りとなった。
- ①**青少年の利用者情報発信に関わる注意喚起の仕組みについては少ない傾向**であった。
- ②青少年保護の観点から不適切コンテンツを報告する機能（機能有無）、③不適切ユーザーブロック機能については実施しているアプリが一定程度存在することが分かった。

<調査結果>

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=8)	(n=9)	(n=12)	(n=8)	(n=0)	(n=13)	(n=0)
①.青少年の利用者情報発信に関わる注意喚起の仕組み	0%	0%	8%	0%	-	15%	-

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=14)	(n=13)	(n=22)	(n=17)	(n=1)	(n=17)	(n=0)
③不適切ユーザーブロック機能	93%	85%	73%	88%	100%	71%	-

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=14)	(n=13)	(n=22)	(n=17)	(n=1)	(n=17)	(n=0)
②青少年保護の観点から不適切コンテンツを報告する機能（機能有無）	86%	69%	82%	94%	100%	41%	-

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=11)	(n=12)	(n=26)	(n=6)	(n=0)	(n=40)	(n=43)
④利用者情報提供や課金について保護者が関与する仕組み	27%	42%	4%	0%	-	53%	0%

（注）
①：アプリ内/子供向けプライバシーポリシー内に青少年の利用者情報発信に関わる注意喚起の文言が含まれているかを調査している。利用者交流機能が無い場合や子供向けプライバシーポリシーが存在しない場合には対象外とする。
④：ゲームアプリを対象とし利用者情報の提供や課金に関して保護者の関与の仕組みや機能が具備されているかを調査している。

SPSI 1.5.2 (年齢制限限定に関する基準)

<SPSIの記載（p.40）>

アプリストア運営事業者は、運営するアプリストアに掲載する個別のアプリケーションに関して審査を行うことが望ましい【望ましい事項】。
当該審査を行う場合には、年齢制限設定（レーティング）に関する基準を設定し、適切な年齢制限設定が行われるよう確認することが望ましい。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの年齢制限設定に関する基準を調査したところ、結果は以下の通りとなった。
- **GooglePlayやAppStoreではアプリの審査時にIARCなどのレーティングを設定する必要がありレーティングの管理が行われている。**
- サードパーティストア6つはIARCの公式レーティング制度は採用されていないが、一部のアプリでは年齢制限の表示がされる。

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
個別アプリの審査については基準を公開の上実施されている。 **レーティング基準が設定されている。**	個別アプリの審査については基準を公開の上実施されている。 **IARC（International Age Rating Coalition）の年齢レーティング基準を採用している。**	個別アプリの審査については基準を公開の上実施されている。 IARC（国際年齢評価連合）の年齢レーティング基準は採用されていないが、**PEGIのレーティング基準が設定されている。**	個別アプリの審査については基準を公開の上実施されている。 IARC（国際年齢評価連合）の年齢レーティング基準は設定されていないが、**PEGIのレーティング基準が設定されている。**	個別アプリの審査については基準を公開の上実施されている。 **年齢レーティング基準は設定されていない。**	個別アプリの審査については実施されていないと推察される。 **年齢レーティング基準は設定されていない。** アプリごとに年齢制限の表示が無いため、子供が適切なアプリを選択することが難しい。	個別アプリの審査については実施されていないと推察される。 **年齢レーティング基準は設定されていない。** 有料アプリの改造版を無料で提供する非公式ストアのため、著作権侵害やセキュリティリスクが発生する可能性がある。	デベロッパー向けサービス利用規約には、個別アプリの審査については実施されていると記載がある。 **利用規約には18歳以上からのみ**と記載がある。（１部のアプリでは利用目的を考慮し13歳以上から利用可能となる場合がある。）

（参考）各ストアにおけるレーティング・審査の判断基準について

- 各ストアのガイドラインや審査基準から、レーティングをどの機関が担っているか、各ストアがどのようにレーティングを使用しているかを調査した。
- **AppStore、GooglePlayでは年齢制限設定は必須**となっているが、サードパーティストアでは任意となっているケースが確認されている。

Google Play でのアプリとゲームのコンテンツのレーティング

アプリとゲームのコンテンツのレーティングは、アプリの対象年齢を把握するために役立ちます。

レーティングは、アプリのデベロッパーと国際年齢評価連合（IARC）が担っています。韓国では、ゲーム物管理委員会（GRAC）によってレーティングが承認されます。

Google Play でのレーティングの使用方法

Google は以下の目的でコンテンツのレーティングを使用します。

- 不快に感じる可能性のあるコンテンツがアプリに含まれていることをユーザーに伝える。
- 必要に応じて、一部の地域や特定のユーザーに対してコンテンツをブロックまたは除外する。

資料

年齢制限指定の値と定義

年齢制限指定は、アプリ情報の必須フィールドであり、ペアレンタルコントロールで使用されるプロパティです。ペアレンタルコントロールを利用することで、保護者は子どもにとって安全なオンライン環境を構築できます。デベロッパは、各年齢層のユーザに向けて、それぞれの年齢に適した体験を提供することができます。

App Store Connectには、コンテンツの説明、アプリ内コントロール、機能の一覧が用意されており、これを利用することでアプリにおいて特定の要素が表示される頻度やその有無を示すことができます。Appleは、年齢制限指定に関するアンケートへの回答に基づいて適切な年齢制限指定を生成します。アプリの年齢制限指定を設定する方法については、こちらを参照してください。

以下の表に、さまざまな年齢制限指定カテゴリに関する詳しい情報と、地域別の年齢制限指定の値を示します。

注：

- 「審査適応区分外」のアプリは、App Storeで公開することはできませんが、代替アプリマーケットプレイスまたはWebサイトで公開できる場合があります。
- アプリの年齢制限指定は、OSのバージョンによって異なる場合があります。iOS 26、iPadOS 26、macOS Tahoe 26、tvOS 26、visionOS 26、watchOS 26以降を実行しているAppleデバイスの年齢範囲の値について詳しくは、こちらを参照してください。それより前のバージョンのOSを実行しているAppleデバイスについて詳しくは、こちらを参照してください。

情報タブ

- **アイコン**：アプリを識別するアイコンです。正方形のアスペクト比、256x256以上の解像度、PNGまたはJPEGのファイル形式を推奨します。
- **名前**：アプリ名。他のアプリの商標や、SEO向上を目的としているものの、アプリの目的をユーザーに誤解させる可能性のある単語の組み合わせは許可されませんのでご注意ください。
- **オペレーティングシステム**：アプリが実行されるプラットフォーム。Uptodownは現在、Android、Windows、Macをサポートしています。
- **ディレクトリまたはカテゴリ**: アプリの性質に最も適したカテゴリを選択します。
- **パッケージ名**: アプリのパッケージ名またはアプリのアプリケーションID。パッケージ名はアプリ自体に含まれており、ビルドプロセスで追加されるため、Androidアプリをアップロードするとこのフィールドは自動的に入力されます。
- **公式サイト**：アプリの公式サイト、または開発者自身のウェブサイト。ただし、危険、不快、または掲載基準を満たさないコンテンツへのリンクが含まれている場合、編集チームの判断により掲載しない場合がありますのでご了承ください。
- **PEGI (オプション):** Pan European Game Informationコードまたは他の地域の同等のコードに従った推奨年齢範囲。
- **広告**: アプリにアプリ内広告が含まれている場合は、[アプリに広告が含まれています] ボックスにチェックを入れます。
- **国制限**: 選択した国でのアプリの配布を制限します。
- **国籍**: アプリ作成者の国籍。
- **作成者**: アプリを作成した会社、スタジオ、または個人の名前。

Uptodown's app publication criteria

SPSI 1.5.2 (青少年向けカテゴリの有無)

<SPSIの記載（p.40）>

アプリストア運営事業者は、運営するアプリストア内に青少年向けアプリケーションを集めた専用の分類を設けることが望ましい【望ましい事項】。

<調査結果概要>

- AppStore、Google Playに加え、６つのサードパーティアプリストアの青少年向けアプリの分類・カテゴリの設置状況を調査したところ、結果は以下の通りとなった。
- **AppStore、GooglePlay、Aptoideでは教育や子供向けのカテゴリーが存在する。**
- GooglePlayにはGoogleキッズスペースと呼ばれる子供向けのホーム画面機能が用意されている。

<調査結果>

AppStore	GooglePlay	Aptoide	Uptodown	F-droid	APKPure	HappyMod	DMM Games
App Storeには**青少年向けのカテゴリが存在する。** 5歳以下、6～8歳、9～11歳の年齢層別に、知育、ゲーム、パズルなど安全で教育的なアプリを検索可能。 ・教育/知育 ・ゲーム/パズル ・エンターテイメント ・コミュニケーション	Google Playには「ファミリーカテゴリ」と呼ばれる**青少年向けのカテゴリが存在する。** GooglePlayの「子供」を選択すると以下の子供向けのカテゴリが表示される。 ・エンタメ ・テレビ&映画 ・オフラインゲーム ・シミュレーションゲーム	Aptoideではゲーム、アプリ共に**青少年向けのカテゴリが存在する。** ・アプリ ＞ 教育 ・ゲーム ＞ 教育	Uptodownでは、明確な「子供向けカテゴリ」は存在しない。	F-Droidには明確な「子供向けカテゴリ」は存在しない。	明確な「子供向けカテゴリ」は存在しない。	明確な「子供向けカテゴリ」は存在しない。	明確な「子供向けカテゴリ」は存在しない。

SPSI 1.5.3 (ペアレンタルコントロールに係る対応)

<SPSIの記載（p.40）>

OS提供事業者は、アプリストアにおける個別のアプリケーションのダウンロード及び起動の可否、アプリストアの利用制限並びに、アプリストア及び外部ウェブサイトにおける利用者情報の提供及び課金に対する制限等を行うペアレンタルコントロール機能を実施するために必要な役務を提供することが望ましい【望ましい事項】。

<調査結果概要>

- OS提供事業者のペアレンタルコントロール機能について調査を行った結果は下記の通りとなっている。
- **iOSではスクリーンタイムやファミリー共有などの機能を用いてペアレンタルコントロールが可能である。**
- **AndroidではGoogleファミリーリンク機能を提供しておりアプリのインストール制限などが可能である。**

<調査結果>

iOS	Android
・アプリのダウンロードおよび起動の可否 「スクリーンタイム」機能より、アプリのインストール・削除・課金の禁止が可能。 子供がApp Storeでアプリをダウンロードしようとした際に、保護者の承認を必要とするように設定できる。 **・アプリストアの利用制限** [許可されたApp] で、App Storeをオフにすることで、アイコン自体を隠すことが可能。年齢に応じたコンテンツ制限、使用時間の制限なども可能。 **・アプリストア及び外部ウェブサイトにおける利用者情報の提供及び課金に対する制限** iPhoneの「スクリーンタイム」内にある「コンテンツとプライバシーの制限」機能を使用し、個人情報の共有設定やアプリのトラッキングをオフにする。これにより、子供のアカウント（Apple ID）のデータ保護や、年齢に応じたアプリのダウンロード制限が可能。	**・アプリのダウンロードおよび起動の可否** 無料アプリ「ファミリーリンク」を使用することで、親のスマホから子供の端末に対し、アプリのインストール承認が設定できる。 **・アプリストアの利用制限** コンテンツの年齢制限、アプリごとの利用時間制限、アプリの非表示設定などが設定できる。 **・アプリストア及び外部ウェブサイトにおける利用者情報の提供及び課金に対する制限** 子供がGoogleアプリやサードパーティのサービスに対して、デバイスの位置情報、マイク、連絡先へのアクセス権を付与できないように制限することが可能。 「購入の承認」を必須にすることで、有料アプリやアプリ内課金のたびに保護者の許可を求め、子供の勝手な課金を防止可能。

3-1.アプリ開発者の国籍に関する調査（各アプリストアで提供されるアプリの開発者国籍）

＜調査結果概要①：AppStoreとGooglePlayにおいて提供されているアプリの開発者国籍推移＞

- AppStoreにおいて提供されているアプリ（65アプリ）とGoogle Playにおいて提供されているアプリ（65アプリ）について、それぞれアプリ開発者の国籍を整理したところ、下記の通りとなっている。

	GooglePlay			AppStore		
	2023年6月	2024年6月	2025年8月	2023年6月	2024年6月	2025年8月
国内	97	73	30	100	83	38
海外	53	77	30	50	67	27
不明			5			0

＜調査結果概要②： AppStore、GooglePlay、サードパーティストアにおいて提供されているアプリの開発者国籍＞

- AppStore、GooglePlay、サードパーティストアにおいて提供されているアプリ（総数：325アプリ）について、それぞれアプリ開発者の国籍を整理したところ、下記の通りとなっている。
- APKPureを除きサードパーティストアではアプリ開発者の国籍が『海外』の割合が高い傾向がある。

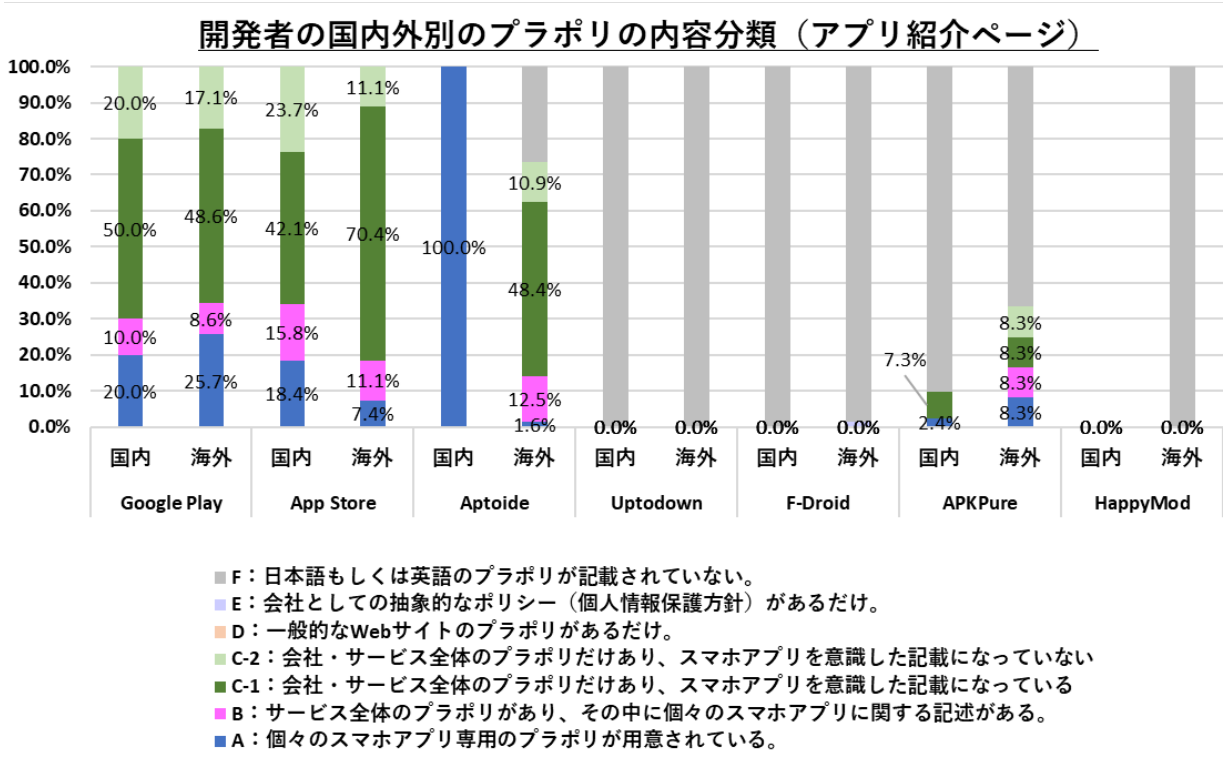
	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
国内	30	38	1	13	2	41	0
海外	30	27	62	37	38	21	56
不明	5	0	1	15	25	3	8

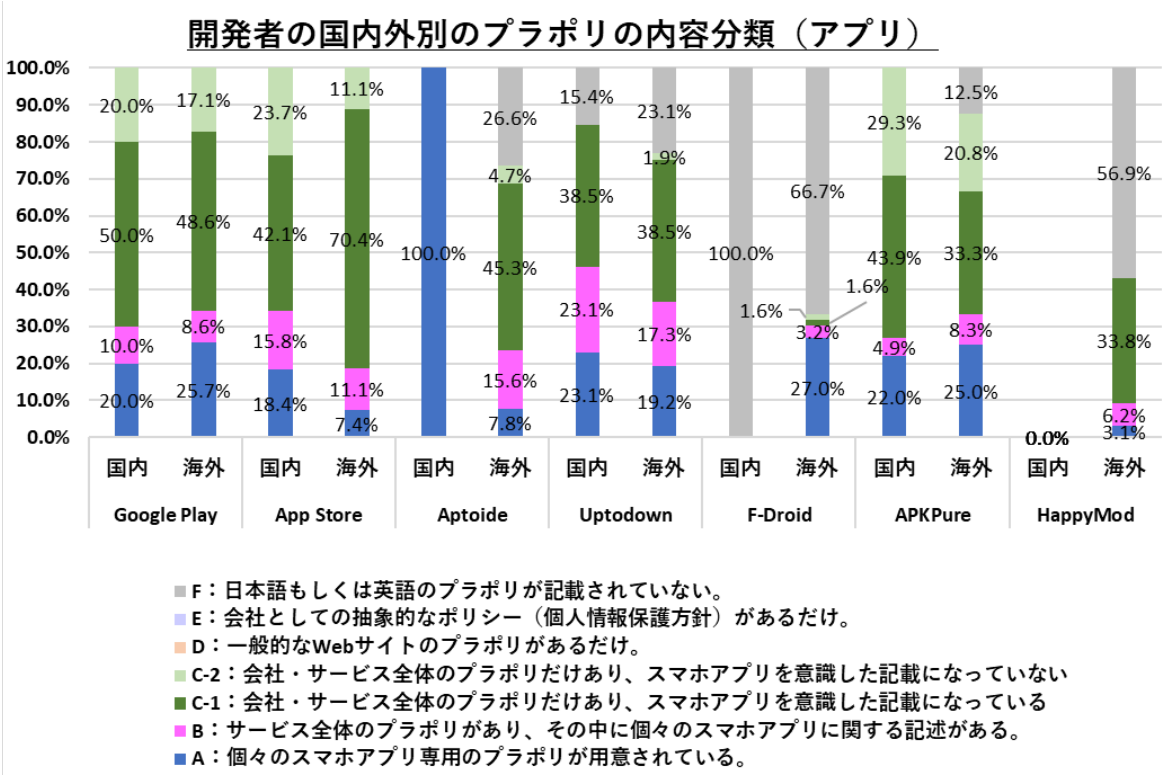
※ 『海外』は、アメリカ合衆国、大韓民国、中華人民共和国、ブラジル、フランス、イギリス、香港、アイルランド、メキシコ、オランダ、パキスタン、ポーランド、スウェーデン、シンガポール、トルコ、台湾（中華民国）、ベトナム、不明（アプリ及びアプリ提供元の情報から判別出来ず）等となっている。

3-1.アプリ開発者の国籍に関する調査　調査結果（プラポリの記載内容の分類）

＜調査結果概要③：AppStoreとGooglePlay、サードパーティストアにおいて提供されているアプリのプラポリの内容の分類＞

- AppStoreとGoogle Play、サードパーティストアにおいて提供されているアプリのプラポリの内容の分類を調査したところ、下記の通りとなっている。
- サードパーティストアではマーケットにプラポリが掲載されてないことを示す【F】の割合が多い。
- 公式ストア（GooglePlay、AppStore）ではプラポリとしてアプリを意識した記載となる【A】～【C-1】まで記載されているアプリは海外アプリの方が高い結果となっている。
- 【D】～【E】までの、プラポリとして必要な項目が記載されていないプラポリは国内・海外で大きな差異はない。





3-1.アプリ開発者の国籍に関する調査　調査結果（SPSI10項目の記載率）

＜調査結果概要④：AppStoreとGooglePlayにおいて提供されているアプリのプラポリのSPSI10項目の記載率＞

- AppStoreとGoogle Playにおいて提供されているアプリのプラポリのSPSI10項目の記載率を調査したところ、下記の通りとなっている。
- **Androidの⑥外部送信・第三者提供の有無、情報収集モジュールの有無の記載率が、海外に比べて国内の方が充実している。**
- iPhoneでは⑧～⑩が何れも国内の方が低い結果となった。

	番号	項目		2024年6月 Android 国内 (n=72)	2024年6月 Android 海外 (n=75)	2024年6月 iPhone 国内 (n=83)	2024年6月 iPhone 海外 (n=65)	2025年8月 Android 国内 (n=30)	2025年8月 Android 海外 (n=35)	2025年8月 iPhone 国内 (n=38)	2025年8月 iPhone 海外 (n=27)
	①	情報を取得するアプリ提供者等の氏名又は名称		100%	89%	95%	94%	100%	97%	100%	93%
	②	取得される情報の項目		90%	96%	84%	94%	87%	89%	95%	100%
	③	取得方法		82%	88%	73%	86%	77%	86%	76%	96%
	④	利用目的の特定・明示		99%	95%	98%	98%	90%	97%	92%	100%
	⑤	通知・公表又は同意取得の方法、利用者関与の方法	⑤－１.送信停止の手順の記載（送信停止の手順）	29%	29%	24%	32%	23%	11%	24%	11%
			⑤－２.利用者情報の削除の記載（利用者情報の削除）	88%	87%	78%	86%	87%	89%	95%	96%
	⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	⑥－１.利用者情報の第三者への送信の有無の記載	99%	96%	98%	97%	100%	80%	97%	100%
			⑥－２.利用者情報の送信先の記載	78%	81%	72%	72%	63%	12%	62%	33%
			⑥－３.情報収集モジュールに関する記載	60%	47%	54%	51%	67%	51%	61%	52%
	⑦	問い合わせ窓口・苦情の申出先		97%	93%	96%	89%	100%	97%	100%	100%
	⑧	プライバシーポリシーの変更を行う場合の手続		74%	84%	72%	82%	83%	94%	82%	96%
	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		83%	73%	76%	78%	83%	80%	76%	100%
	⑩	委託に係る事項		81%	56%	82%	66%	90%	74%	89%	100%

SPSI10項目において、特に重要性が高いと考えられる項目（利用者情報の取扱いにおいて「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の4点は、最低限必要な情報であり、上記10項目の中でも、特に項目①、項目②、項目④、項目⑥はプラポリにおいて特に重要な項目と考えられることから、水色で網掛けしている。）

青字：国内と海外の結果を比較して国内の方が10%以上高い
赤字：国内と海外の結果を比較して国内の方が10%以上低い

3-1.アプリ開発者の国籍に関する調査　調査結果（SPSI10項目の記載率）

＜調査結果概要⑤：サードパーティストアにおいて提供されているアプリのプラポリのSPSI10項目の記載率＞

- サードパーティストアにおいて提供されているアプリのプラポリのSPSI10項目の記載率を調査したところ、下記の通りとなっている。
- **全体的に国内のアプリの方が記載が充実している傾向が見られる。**

番号	項目		Aptoide		Uptodown		F-Droid		APKPure		HappyMod	
			国内	海外	国内	海外	国内	海外	国内	海外	国内	海外
			(n=1)	(n=60)	(n=11)	(n=41)	(n=0)	(n=21)	(n=41)	(n=22)	(n=0)	(n=28)
①	情報を取得するアプリ提供者等の氏名又は名称		100%	97%	100%	95%		71%	98%	100%		100%
②	取得される情報の項目		100%	95%	91%	98%		62%	73%	91%		96%
③	取得方法		100%	88%	82%	98%		52%	56%	77%		93%
④	利用目的の特定・明示		100%	90%	91%	100%		52%	93%	95%		100%
⑤	通知・公表又は同意取得の方法、利用者関与の方法	⑤－１.送信停止の手順の記載（送信停止の手順）	100%	12%	18%	7%		5%	34%	14%		14%
		⑤－２.利用者情報の削除の記載（利用者情報の削除）	100%	77%	82%	78%		33%	78%	91%		86%
⑥	外部送信・第三者提供の有無、情報収集モジュールの有無	⑥－１.利用者情報の第三者への送信の有無の記載	100%	93%	91%	90%		48%	93%	95%		100%
		⑥－２.利用者情報の送信先の記載	0%	18%	73%	23%		33%	56%	33%		68%
		⑥－３.情報収集モジュールに関する記載	100%	42%	91%	27%		14%	56%	32%		57%
⑦	問い合わせ窓口・苦情の申出先		100%	88%	91%	93%		81%	95%	95%		96%
⑧	プライバシーポリシーの変更を行う場合の手続		100%	83%	91%	88%		71%	78%	86%		82%
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		100%	83%	64%	85%		19%	66%	82%		32%
⑩	委託に係る事項		100%	78%	82%	76%		33%	68%	82%		68%

SPSI10項目において、特に重要性が高いと考えられる項目（利用者情報の取扱いにおいて「誰が」、「何の利用者情報を」、「何の目的で取得し」、「どこに送信しているか」の4点は、最低限必要な情報であり、上記10項目の中でも、特に項目①、項目②、項目④、項目⑥はプラポリにおいて特に重要な項目と考えられることから、水色で網掛けしている。）

青字：国内と海外の結果を比較して国内の方が10%以上高い
赤字：国内と海外の結果を比較して国内の方が10%以上低い

3-1.アプリ開発者の国籍に関する調査　調査結果（プラポリ掲載率の比較）

＜調査結果概要⑥：公式ストアにおいて提供されているアプリのプラポリのSPSI10項目の記載率＞

- 公式ストアにおいて提供されているアプリのプラポリのSPSI10項目の記載率を調査したところ、下記の通りとなっている。
- 国内外、プラットフォーム間で差異は見られなかった。
- 国内、海外ともにプラポリの掲載率は前回調査よりも向上している。

項目	Android(2025年8月)		iOS(2025年8月)	
	国内	海外	国内	海外
いずれかに記載	100%	100%	100%	100%
アプリ紹介ページ	100%	100%	100%	100%
アプリ内	100%	100%	100%	100%

＜前回調査の結果＞

項目	人気アプリ(2024年6月)				新着(2024年6月)			
	Android		iOS		Android		iOS	
	国内	海外	国内	海外	国内	海外	国内	海外
いずれかに記載	100%	98%	100%	100%	94%	94%	100%	94%
アプリ紹介ページ	98%	100%	100%	100%	94%	91%	95%	90%
アプリ内	98%	100%	92%	92%	75%	55%	72%	42%

3-2.アプリにおける通知又は公表あるいは同意取得に関する工夫の調査

<調査結果概要①：AppStoreとGooglePlayにおいて提供されているアプリのプラポリの通知又は公表あるいは同意取得に関する工夫>

- AppStoreにおいて提供されているアプリ（65アプリ）とGoogle Playにおいて提供されているアプリ（65アプリ）について、個人情報の利用について説明しているプライバシーポリシーの通知又は公表あるいは同意取得の工夫について調査を実施したところ、下記の通りとなっている。
- 前回調査の結果と比較して、Android、iOSともに①階層的な通知②図・アイコン・動画等の利用の割合が増加している。

<項目の説明>

① 階層的な通知等の内容の表示：プライバシーポリシー等の全文をもって通知を行うのではなく、利用者の関心の範囲や粒度に合わせて通知内容を階層化しているケース（全文とは別に、目次の作成、重要事項や概要版の作成など）

② 図・アイコン・イラスト・動画等の利用：プラポリ内や専用の説明ページ等で、図・アイコン・イラスト・動画を用いて利用者情報の取り扱いを説明しているケース

③ プライバシーポリシーのポップアップでの同意取得：初回起動時などにポップアップ等でプラポリ全文やプラポリのリンクを提示し、同意を取得するケース

項目	2023年10月		2024年6月		2025年8月	
	Android (n=144)	iOS (n=150)	Android (n=147)	iOS (n=148)	Android (n=65)	iOS (n=65)
① 階層的な通知等の内容の表示	16%	15%	16%	21%	42%	40%
② 図・アイコン・動画等の利用	15%	13%	4%	9%	11%	18%
③ プライバシーポリシーのポップアップでの同意	63%	63%	42%	27%	42%	40%

<調査結果概要②： AppStore、GooglePlay、サードパーティストアにおいて提供されているアプリのプラポリの通知又は公表あるいは同意取得に関する工夫>

- AppStore、GooglePlay、サードパーティストアにおいて提供されているアプリについて、個人情報の利用について説明しているプライバシーポリシーの通知又は公表あるいは同意取得の工夫について調査を実施したところ下記の通りとなっている。
- サードパーティストアでは①階層的な通知や②図・アイコンなどの利用をしているストアも一定数みられた。

項目	Google Play	App Store	Aptoide	Uptodown	F-Droid	APKPure	HappyMod
	(n=65)	(n=65)	(n=61)	(n=52)	(n=21)	(n=63)	(n=28)
① 階層的な通知等の内容の表示	42%	40%	41%	44%	10%	27%	25%
② 図・アイコン・動画等の利用	11%	18%	16%	21%	0%	3%	7%
③ プライバシーポリシーのポップアップでの同意	42%	40%	46%	44%	0%	46%	4%