資料５－１

ICTサイバーセキュリティ政策分科会第5回会合

R5年度「通信アプリに含まれうる不正機能の検証に関する実証」について

KDDI株式会社

2024年 4月 5日

1．背景と目的

■ 我が国におけるスマートフォンの個人保有率は77.3%（2022年時点）となる中、スマートフォンは常時ネットワークと接続した状態で利用者に携帯されることから、**利用者の行動履歴や通信履歴等の情報（以下「利用者情報」という。）を多数収集・蓄積すること**が可能となっている。

■ スマートフォンにインストールされたアプリケーション（以下「アプリ」という。）の多くは、スマートフォンに蓄積された利用者情報や端末の機能にアクセスしている。利用者のプライバシー保護の観点からは、利用者情報の利用は適切に管理される必要があるが、利用者にとっては自らが意図しない形での利用者情報の利用があるか否かを直接確認することは難しい。

■ アプリ事業者による**利用者の同意の範囲を超えた利用者情報の収集**や、**アプリの脆弱性を悪用したサイバー攻撃による利用者情報の漏洩**などの懸念が生じたときに、我が国としてアプリの挙動を客観的に把握することが必要になる場合もあると考えられる。

■ 本事業においては、国内解析事業者の**解析能力の水準**を把握するとともに、我が国で普及しているアプリにおけるプライバシーポリシーの策定状況・内容等の調査（「スマートフォン・プライバシー・アウトルック（SPO）」という。）等を含む**利用者情報の取扱慣行やセキュリティ対策の実施状況**を把握する。合わせて、利用者情報の保護のために、アプリ開発者のみならず**サードパーティストアを含めたアプリストア運営者等が果たしうる役割**を整理して、スマートフォン・プライバシー・イニシアティブ（SPI）に盛り込むことが望ましいセキュリティの観点を示す。

2．事業概要

➢ 本事業では、**国内解析事業者の解析能力の水準の把握**や**アプリにおける利用者情報の取扱慣行等を整理**するため、代表的なアプリに対して実際に技術的解析（スクリーニング解析、表層解析、詳細解析）を実施するとともに、利用者の意図しない利用者情報の取扱いの実態や諸外国におけるスマートフォンアプリ規制動向に係る文献調査を実施。

技術的解析

“Google Play”又は”App Store”から入手可能なアプリ

- 売上ランキング、カテゴリー、人気アプリ/新規アプリ等のバランスを考慮して選定

詳細解析対象のアプリ選定

スクリーニング解析　対象アプリ：300アプリ（Android/iOS 150アプリずつ）
➢ ツールを用いた脆弱性に関する総合的評価　等

＋

プライバシーポリシーの確認
➢ SPOに基づいて実施

- スクリーニング解析の結果及びプライバシーポリシーの確認結果を基に、表層解析の対象を選定

表層解析　対象アプリ：100アプリ（Android 50アプリ/iOS 50アプリ）
➢ アプリの通信先の確認　等

- 表層解析の結果を基に、詳細解析の対象を選定

詳細解析　対象アプリ：83アプリ（Android 41アプリ/iOS 42アプリ）
➢ 静的解析及び動的解析の実施

文献調査

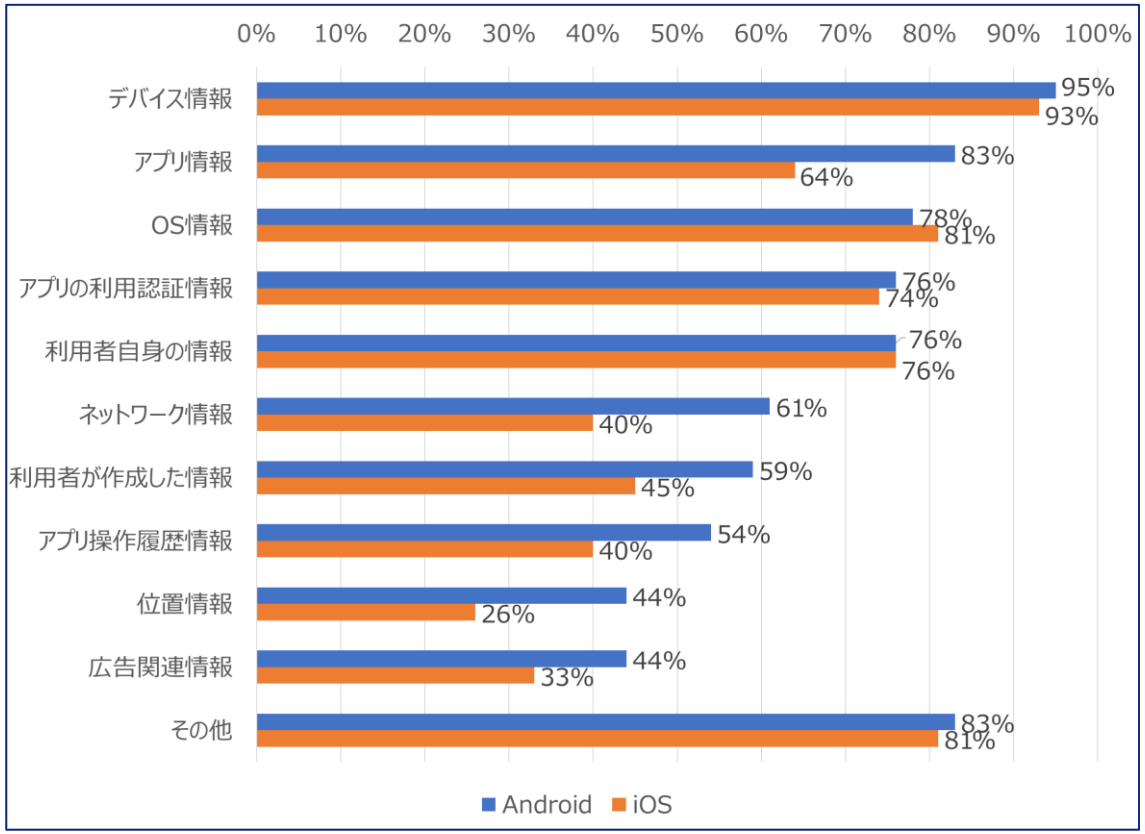
利用者の意図しない利用者情報の取扱いの実態に係る文献調査

諸外国におけるスマートフォンアプリ規制動向に係る文献調査

3．技術的解析（詳細解析結果）

詳細解析によって明らかになった利用者情報の外部送信に係る実態

- 詳細解析の対象であるAndroid 41アプリ、iOS 42アプリにおいて、外部送信される主な利用者情報及び当該利用者情報の外部送信が確認されたアプリの割合は以下のとおり。
- AndroidとiOSは主に同種のアプリを選定しているが、OS情報等を除くいずれの利用者情報においてもAndroidの方が外部送信を確認できた割合が高い。これはAndroidの方が詳細解析によって解析できた範囲が広いことも要因と考えられる。



外部送信される主な利用者情報	具体例
デバイス情報	デバイスID
	メモリ容量
アプリ情報	アプリバージョン
	アプリ設定情報
	SDK関連情報
	インストール日時
OS情報	OS名
	OSバージョン
	言語情報
	国/地域等
アプリの利用認証情報(SNS等の外部連携を含む)	ログインID
	パスワード
利用者自身の情報	メールアドレス
	電話番号

外部送信される主な利用者情報	具体例
ネットワーク情報	Wi-Fi情報
	キャリア情報
	SIM情報
利用者が作成した情報	SDカード内の情報
	ファイル情報
	カメラロールの画像
	録音データ
	アドレス帳情報
	SMSメッセージ
アプリ操作履歴情報	操作ログ
位置情報	
広告関連情報	広告ID
その他	UUID
	Cookie使用可否

4．利用者の意図しない利用者情報の取扱いの実態に係る文献調査

➢ 利用者の意図しない利用者情報の取扱いについて、国内外の事例を基に、その類型を整理するとともに、OS提供事業者やアプリストア運営者による取組を整理する。

利用者の意図しない利用者情報の取扱いが生じるアプリの類型整理

類型①：アプリ開発者の意図したとおりにアプリが動作しているが、プライバシーポリシーの記載が不十分であり、利用者への十分な告知がないまま利用者情報の取扱いがなされているケース
類型②：アプリの脆弱性等を悪用した攻撃が発生し、アプリ開発者や利用者の意図しない利用者情報の取扱いがなされていることが発覚したケース
類型③：利用者に誤認を与える方法等で利用者にアプリをインストールさせ、アプリ開発者の経済的利益等のために利用者情報を収集しているケース

国内外の事例

類型①：透明性が不十分なアプリ
QRコードリーダアプリでQRを読み取ると利用者の許諾なく位置情報をアプリ開発者へ送信。

類型②：脆弱性があるアプリ

メッセージアプリに存在した脆弱性が、相手のスマートフォンにスパイウェアを仕込む目的で利用されていたことが発覚。

類型③：不正なアプリ

「ウイルス対策」などと称した偽のセキュリティアプリをインストールさせ、アドレス帳の情報を抜き取った上で、迷惑メールを送信。

OS提供事業者等による利用者情報保護の取組

【OS提供事業者による取組の例】
✓ 社員向けのプライバシー教育やプライバシーレッドチームの設置。
✓ 未成年者保護の一環として機能制限や通報機能の提供。
✓ プライバシーセンターの設置による利用者への情報提供。

【アプリストア運営者による取組の例】
✓ Googleにおいては「デベロッパープログラムポリシー」及び「デベロッパー販売/配布契約」を定め、Appleにおいては「Apple Developer Program使用許諾契約」及び「App Store Reviewガイドライン」を定めている。

5．まとめ・考察

1．利用者を保護するための第三者検証の必要性

- SPIでも示されているとおり、スマートフォンアプリの第三者検証を実施することで、当該アプリが**プライバシーポリシーに合致した適正な運用がなされているかを客観的に確認**することができ、**利用者がスマートフォンアプリを利用する際の判断基準として有益な情報を提供**することが期待される。

- また、第三者検証の実施を通じて、**スマートフォンアプリに対する信頼が醸成されることで当該アプリの利用促進にも繋がり得ることが期待**されるなど、第三者検証の実施は**アプリ提供者にとっても有益なものとなり得る**。

- このように、スマートフォンアプリに対する第三者検証の実施は、利用者保護の観点からも必要な取組であり、我が国における解析能力を維持・向上させることは重要である。したがって、**今回のような事業の実施を通じて、解析事業者がスマートフォンアプリの解析を実施し、そのノウハウを共有する場を整える**ことが望ましいと考えられる。

2．SPIに基づく取組を進めることの重要性

- 本事業における解析行為やSPOの実施を通じて、今回調査対象となったアプリから外部送信がなされている利用者情報については、概ねプライバシーポリシーにおいて特定されていたが、**一部の利用者情報はプライバシーポリシー上で特定されないまま外部送信**されており、また、特定されている場合でも、**利用目的が明示されておらず利用者への透明性の観点から懸念が生じる**ケースもあった。

- 利用者への透明性の確保の観点からは、プライバシーポリシーの内容を簡潔に示した概要版の作成など、SPIに沿った取組を進めていくことが重要であるが、SPOの結果を踏まえると、これらの趣旨が十分に浸透していない面も確認される。また、SPIで示されているとおり、アプリ提供者のみならず、利用者のリテラシー向上も必要である。

- このような現状を踏まえ、**引き続き、SPIの趣旨の周知徹底を図るとともに、アプリ提供事業者やアプリストア運営者等の関係者においては、SPIを踏まえた適切な対応を取っていくことが重要**であると考えられる。

【アプリプラポリに記載すべき項目】

①情報を取得するアプリ提供者等の氏名又は名称	⑥外部送信・第三者提供・情報収集モジュールの有無
②取得される情報の項目	⑦問合せ窓口
③取得方法	⑧プラポリの変更を行う場合の手続
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
⑤通知・公表又は同意取得の方法、利用者関与の方法	⑩委託に関する事項

3．SPIにおいてセキュリティに係る要件を盛り込む必要性

- 利用者情報の保護のためには、**アプリ開発者のみならず、アプリストア運営者等の関係者も含めて、適切な対応を取ることが重要**である。

- 現行のSPIでは、プライバシーの観点から関係者が遵守すべき方向性を示しているが、脆弱性があるアプリや不正なアプリにおける利用者情報の取扱い等に係る**セキュリティの観点は明示的に含まれていない**。

- 英国のDSITの「Code of practice for app store operators and app developers」も参考に、**セキュリティの観点から、右記の内容をSPIに盛り込むことが望ましい**と考えられる。

- なお、その際、日本スマートフォンセキュリティ協会（JSSEC）が策定した「スマートフォンアプリケーション開発者の実施規範（第一版）（2024年03月08日）」も参考にすることが望ましい。

アプリ開発者

項目	ＳＰＩに盛り込むべき内容
脆弱性がある アプリへの対応	• 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、アプリのアップデートを提供 • 脆弱性情報の窓口や連絡先を設置　等
セキュリティ バイデザイン	• アプリの企画や設計の段階から、セキュリティの確保について適切な仕組みを組み込む　等

※情報収集モジュール提供者も同様

アプリストア運営者

項目	ＳＰＩに盛り込むべき内容
アプリストア としての機能	• 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 • 各アプリについて、利用者情報の取扱い等に関する情報を確認可能な場を設ける • アプリを削除等する場合には、当該アプリの利用者に対して周知 • セキュリティインシデントが発覚した場合には、関係者に対して周知 • アプリの掲載を拒否する場合には、アプリ開発者に対して理由をフィードバック　等
脆弱性がある アプリへの対応	• 各アプリが、脆弱性報告のための窓口を有するとともに、脆弱性開示のための手続を有していることを確認 • 利用者に対してアプリを最新版にアップデートするように促す • アプリが長期間アップデートされない場合には、アプリのサポート状況を確認　等
不正なアプリ への対応	• 利用者が不正なアプリを報告できるよう報告窓口を設置 • 不正なアプリを発見した場合には削除するとともに、当該アプリの開発者が開発した他のアプリも調査　等

※OS提供事業者はアプリストアが上記の取組を進めていることを確認

参考資料

【参考】技術的解析（詳細解析対象のアプリ選定）

詳細解析対象アプリの選定

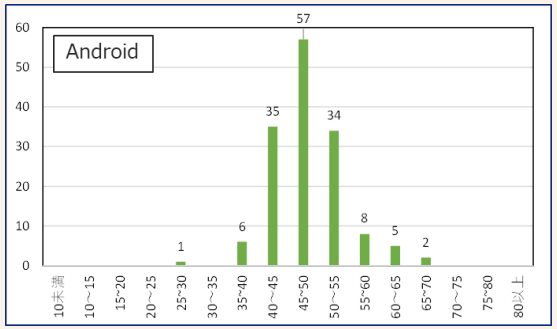
➢ 詳細解析の対象を選定するため、プライバシーポリシーの記載内容の確認に加えて、スクリーニング解析及び表層解析において、脆弱性診断やアプリの通信先等について調査・解析を実施。

プライバシーポリシーの確認（300アプリ）

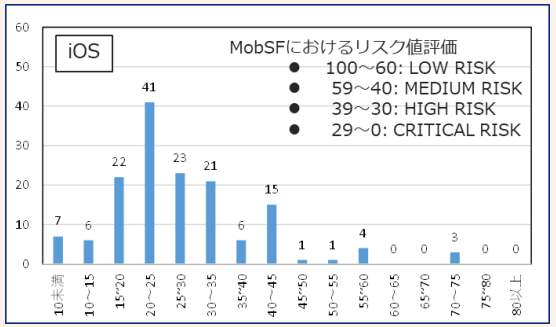
➢ プライバシーポリシーの記載状況等について確認（次頁に結果を記載）。

スクリーニング解析（300アプリ）

➢ 脆弱性診断※1（MobSFを使用）を実施し、セキュリティ上の危険性があることを示すセキュリティスコアの低いアプリは表層解析の対象として選定。



CRITICALに当てはまるアプリが1つ存在



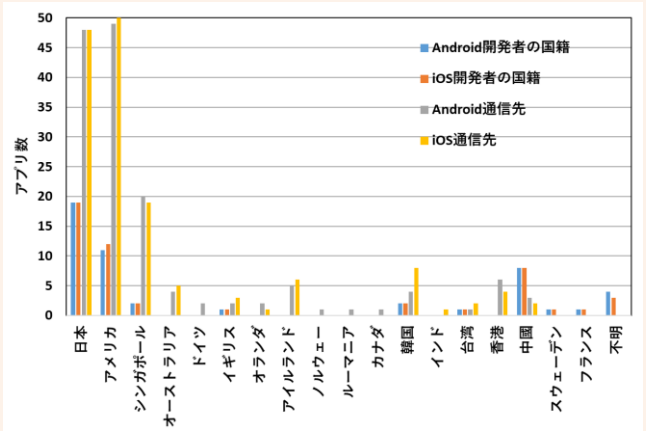
iOSアプリはツールの仕様上スコアが低く算出される

● ● ● プラポリにおいて開発者の国籍が判別できないアプリ
プラポリにおいて個人情報・位置情報を多く扱うことが記載されているアプリ
脆弱性診断でスコアが低いアプリ 等

表層解析（100アプリ）

<通信先の調査>

➢ 大半のアプリが国内又は米国への通信を行っているが、一部のアプリはその他の地域（シンガポール、アイルランド、韓国、香港、中国等）と通信を行っていることを確認。



<スマートフォン機能へのアクセス権限等>

➢ スマートフォン端末内に保存された利用者情報へのアクセス権限等が多数付与されているスーパーアプリ※2は、MobSFのセキュリティスコアが低く算出され、セキュリティ上の危険性が高くなる傾向を確認。

● ● ● 通信先がOSによって異なるアプリ
通信先とプラポリの記載に矛盾があるアプリ
我が国とのデータ移転の枠組みが整備されていない国に通信しているアプリ 等

詳細解析（83アプリ）

➢ 静的解析・動的解析の対象アプリの分類は以下のとおり。

➢ 1アプリ当たり、2つ以上の解析事業者が解析を実施。

アプリ分類	Android	iOS
SNS又はSNSに類するアプリ	16	16
ツール	12	13
ゲーム	6	6
その他	7	7
合計	**41**	**42**

※1：MobSF(Mobile Security Framework)を用いてセキュリティスコアを算出。当該スコアは「セキュリティ上、安全である」という観点で100点満点で算出され、スコアが高いほどセキュリティが確保されていることを示す。

※2：1つのアプリに多種多様な機能が集約されたアプリ

【参考】技術的解析（プライバシーポリシーの確認）

- 総務省では、平成25年度より、アプリケーションにおけるプライバシーポリシーの策定状況・内容等を調査した「**スマートフォン・プライバシー・アウトルック（SPO）**」を公表しており、その最新版となる「SPO Ⅹ」を取りまとめた（詳細は別紙「SPO Ⅹ」を参照）。
- 「SPO Ⅹ」では、本事業においてスクリーニング解析を行った300アプリを対象として調査しており、概要は以下のとおり（調査時点は令和５年６月）。

項　目	調査結果
【1】プラポリの作成・掲載状況	• 紹介ページでのプラポリ掲載率は100%近くであり、アプリ内でのプラポリ掲載率も大幅に上昇。 • 個々のアプリ専用のプラポリが用意されている割合は約20%程度に増加。 • アプリの構造の複雑化等により、アプリのトップ画面等からプラポリ掲載ページまでの操作数は増加。
【2】「電気通信事業における個人情報等の保護に関するガイドライン」で推奨されている10項目の記載状況	• 改正電気通信事業法の外部送信規律施行により、「利用者情報の送信先」に関する記載率が大幅に上昇。 • 10項目を全て記載しているプラポリの割合は、人気アプリで40%程度、新着アプリで25%。
【3】利用者情報の取得に関する状況	• プライバシー性の高い情報（電話番号等）を取得し得るアプリの割合は減少したが、それらのアプリにおいてプライバシー性の高い情報を取得する旨を記載しているアプリの割合は大幅に上昇。
【4】プラポリの概要版作成・公表状況	• 概要版の掲載率は10%以下であるものの、新着アプリにおける掲載率は大幅に上昇。
【5】プライバシーポリシーの改定状況	• 改定内容や過去版へのリンクを掲載しているアプリの割合が大幅に上昇。
【6】アプリ開発者の国籍	• 国内外アプリを比較すると、海外の方がスマホアプリを意識したプラポリとなっている割合が高い。 • 海外アプリの方が「取得される情報の項目」や「利用者情報の送信先」を始め、プラポリの記載内容が充実している傾向。 • 開発者の国籍が不明なアプリを3%程度確認。
【7】アプリにおける通知・同意取得に関する工夫	• アプリで初回起動時等にポップアップでプラポリを表示して同意を取得する等の工夫をしているアプリの割合が大幅に上昇。
【8】利用者の権利・利益保護を妨げるおそれの有無	• 日本語以外の言語でプラポリが記載されているアプリの割合が大幅に低下。

【参考】アプリストア運営者の取組

- アプリストア運営者は、アプリ紹介ページにおいて利用者情報の収集等について公開することを義務付けている。
- Google Playにおいては「データセーフティ」、App Storeにおいては「Appのプライバシー」に収集する利用者情報等が開示される。

項目		Google（デベロッパープログラムポリシーより抜粋）	Apple（App Store Reviewガイドラインより抜粋）※1
対象		全アプリ	全アプリ
公開義務化		2022年7月	2020年12月
表示場所		Google Playの各アプリページ （データセーフティ）	App Storeの各アプリページ （Appのプライバシー）
記載が必要な情報	収集するデータの種類	デベロッパまたはサードパーティパートナーが収集するデータ全て	デベロッパまたはサードパーティパートナーが収集するデータ全て
	収集するデータの用途	必須	必須
	ユーザに紐づけられるデータ	–	必須
	ユーザのトラッキングを行うデータ	–	必須
	プライバシーポリシー	必須	必須

※1 「App StoreでのAppのプライバシーに関する詳細情報の表示」は厳密には「App Store Reviewガイドライン使用許諾契約」に記載されていないが、「App StoreでのAppのプライバシーに関する詳細情報の表示」を掲載している同ウェブページにアプリ公開申請時に必要と記載があるため、ガイドラインの一部として記載

【参考】技術的解析（解析事業者・詳細解析手法・通信先の傾向）

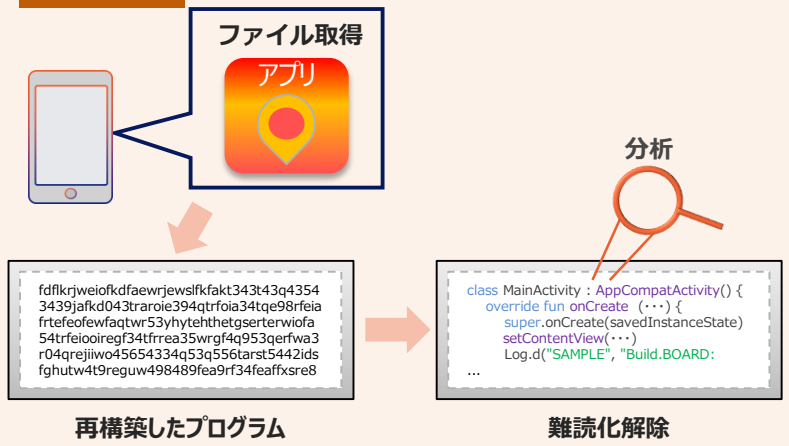
- 表層解析の結果に基づいて、83アプリ（Android 41アプリ/iOS 42アプリ）を選定。
- 「静的解析」と「動的解析」を実施し、利用者情報の外部送信に係る実態等について評価。

詳細解析を実施した解析事業者

事業者名
株式会社ラック
株式会社モノリスワークス
株式会社FFRIセキュリティ
グローバルセキュリティエキスパート株式会社
合同会社エルプラス
GMOサイバーセキュリティbyイエラエ株式会社
株式会社ブロードバンドセキュリティ

詳細解析手法

静的解析



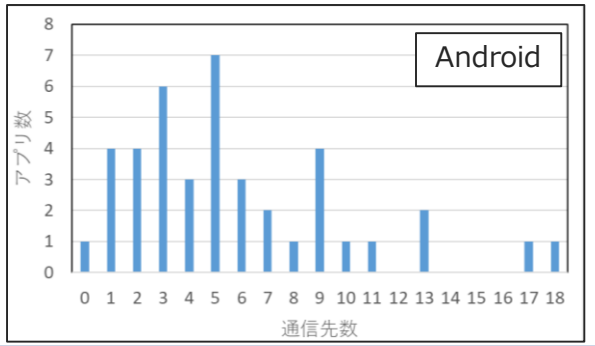
- 再構築したプログラムを分析し、利用者情報の取扱い等について解析。

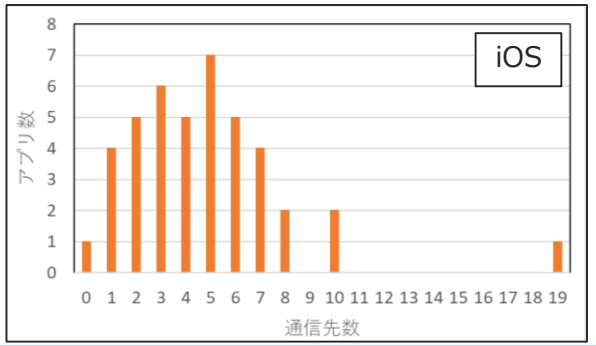
動的解析

- アプリを実際に操作し、通信先・通信内容等について解析。

アプリの通信先の傾向

- 計83アプリの通信先を解析し、Android・iOSごとに1アプリ当たりの通信先数のヒストグラムを右に示す※1。
- 1アプリ当たりAndroidは平均5.7、iOSは平均4.8のドメイン所有者に対して利用者情報を送信していることが判明。
- アプリ開発者のサーバ以外の通信先として、アクセス解析や広告配信等を目的とした情報収集モジュール提供者等にも利用者情報を送信している例を多数確認。





※1：詳細解析の結果に基づいて作成。

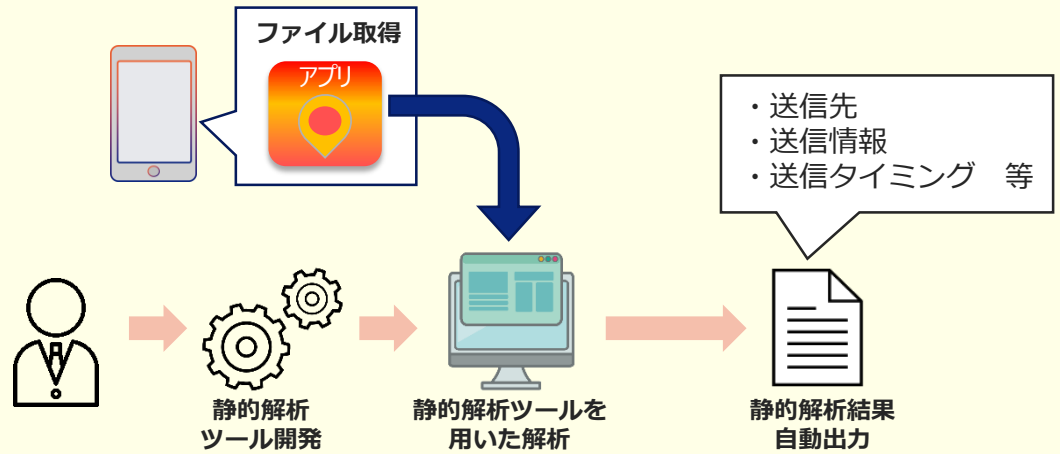
【参考】技術的解析（詳細解析結果）

解析手法について

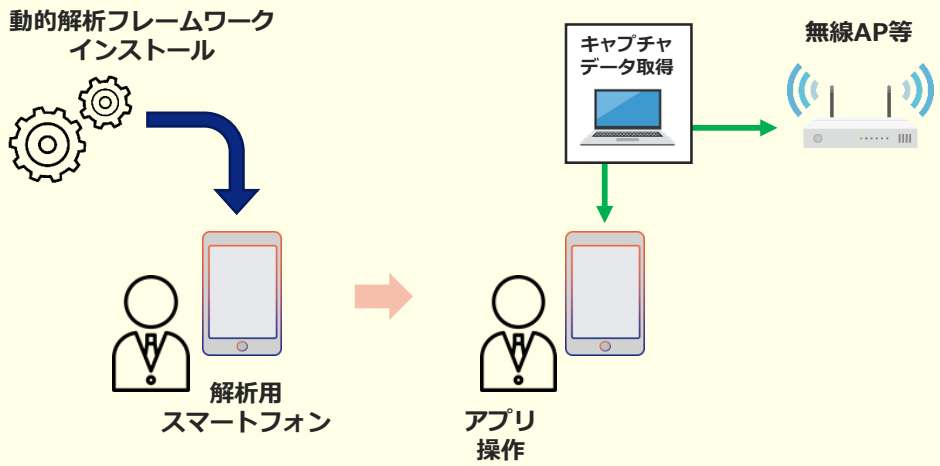
- 本事業での解析に当たっては、解析にかける時間的な制約がある中で、各事業者の解析能力を把握する観点からも、具体的な解析手法については各事業者の裁量に任せた部分が大きかったところ、特に**静的解析の手法を中心に事業者間で大きく差異が見られた**。具体的には、動的解析を一定程度行った上で対象を絞って静的解析を実施している事業者もあった一方、**静的解析用ツールを自社で構築して静的解析を自動化した**事業者もあるなど、事業者による創意工夫が見られたところである。

- また、本事業の解析において、スマートフォンアプリには利用者情報の保護等のセキュリティ対策やチート対策等を実現するため、「難読化処理」、「Jailbreak検知/Rooted検知」、「ピンニング」、「プロキシ検知」及び「暗号化」等の技術が広く利用されていることを確認。

静的解析の一例：静的解析ツールによる自動化



動的解析の一例：動的解析フレームワークを用いた解析



【参考】第三者検証に係る法制度面からの検討

解析事業における法制度面の整理

- 本事業でスマートフォンアプリにおける利用者情報の取扱いに係る第三者検証を実施するに当たって法制度的観点から留意すべき事項について整理するため、法律専門家によって構成される「法的見解整理のための会議」を開催。
- 同会議においては、**本事業でスマートフォンアプリをリバースエンジニアリングすることは著作権侵害には当たらない**こと等が結論として得られた。

「法的見解整理のための会議」における主な議論内容

「論点① 第三者検証（動的解析および静的解析）の実施に際しての著作権法上の検討」への主な指摘（抜粋）

- ✓ 総務省が平成26年度に実施した調査研究においても、一般的な権利制限規定の存在しない当時の著作権法の下でも、著作権法上の支障が生じないように、第三者検証の為の静的解析及び動的解析等を実施することが可能と解するとの結論を得た
- ✓ 「デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方」（文化庁）等においても、サイバーセキュリティ対策の目的やプログラムの調査解析の目的で行われるリバースエンジニアリングが、著作権法第30条の4に規定される権利権限の対象として、著作権侵害にはならないという見解が明記　等

「論点② 第三者検証が利用規約に反する可能性についての検討」への主な指摘

- ✓ リバースエンジニアリング行為が利用規約によって禁止されるとすれば、悪意のあるプログラム開発者に、当該プログラムの不正性の発覚を防ぐ手段を与える
- ✓ 本事業での静的解析・動的解析が規約の違反である旨の訴えが提起されたとしても、静的解析・動的解析行為の差止又は損害賠償を認める可能性は極めて低い（平成26年度に実施した調査研究においても同様の結論を得た）　等

【参考】諸外国における利用者情報の取扱いに係る規制動向に係る文献調査

諸外国の規制動向の現状について

➢ 諸外国における利用者情報の取扱いに係る規制動向として、既存の法令等について調査。

米国（連邦）	➢ 主な枠組み：包括的な個人情報保護の法制度はなく、FTCを中心に分野別（子供・医療・EC等）に規制を行っている。 ➢ 追加的な枠組み：FCCがFTCによる規制が及ばない電気通信事業者に対する規制を担う。
米国（カリフォルニア）	➢ 主な枠組み：個人情報保護に関する包括的な法制度である州消費者プライバシー法が規制の中心的な役割を担っている。 ➢ 追加的な枠組み：州年齢適正設計法、医療情報秘匿法、州不正競争防止法が追加的な枠組みとして機能する。
EU	➢ 主な枠組み：包括的な個人情報保護に関する法律であるGDPRを中心にeプライバシー指令がこの分野の規制の中心を担っている。 ➢ 追加的な枠組み：分野別のAI法案、EHDS法案、DPFを規制するDSAやDMA、EECCによるアプリ規制など関連する制度が整備。
フランス	➢ 主な枠組み：GDPRおよびそれを補完するデータ保護法が中心的な役割を果たしている。 ➢ 追加的な枠組み：DPAであるCNILがアプリ規制に関する勧告案を公表しているほか、警察監視法や子ども分野での個別法がある。
イギリス	➢ 主な枠組み：個人情報保護の包括的な法制度してUK GDPRが中心的な役割を担っている。 ➢ 追加的な枠組み：DCMSによるモバイルアプリ規範、AI規制や消費者保護規制、Ofcomによる有害コンテンツ規制がある。
中国	➢ 主な枠組み：個人情報保護法が包括的な規制、サイバーセキュリティ法等が分野別の規制、各種行政規則が運用ルールとして機能する。 ➢ 追加的な枠組み：アプリのライフサイクルにおける個人情報保護のコンプライアンス監査規制や外資規制が存在する。
韓国	➢ 主な枠組み：包括的な法制度として個人情報保護法が存在する。 ➢ 追加的な枠組み：位置情報法、情報通信法や、新たに子供・青少年分野の個人情報保護法の提案も行われている。

【参考】諸外国における利用者情報の取扱いに係る規制動向に係る文献調査

英国におけるアプリに係る実施規範について

- 英国のDSIT（Department for Science, Innovation & Technology）はアプリに係る実施規範として、「Code of practice for app store operators and app developers」を示し、アプリの利用者情報のセキュリティとプライバシーを保護するために**アプリストア運営者、アプリ開発者及びOS提供事業者が遵守すべき原則**を整理。
- 当該実施規範は８つの原則から構成されており、概要は以下のとおり。

No	Code of Practiceに示された原則	適用者	概要
1	アプリストアのセキュリティとプライバシーに関する要件	アプリストア運営者	■ アプリストア運営者は、アプリに対するセキュリティ及びプライバシーの要件を規定し、アプリ投稿やアップデートを承認する前に当該要件を確認する審査プロセスを実施しなければならない。なお、アプリ審査内容の概要は一般に公開しなければならない。 ■ アプリストア運営者は、悪意あるアプリを報告できる窓口を設けなければならない。明らかに悪質なアプリに対しては、遅くとも48時間以内に当該アプリをアプリストアで利用できないようにしなければならない。 ■ アプリストア運営者は、悪意あるアプリを確認した場合、同じ開発者が制作したアプリについても審査を実施することが望ましい。 ■ アプリストア運営者とアプリ開発者は、アプリのセキュリティとプライバシーについて独立した第三者機関と協力して評価することを検討することが望ましい。
2	アプリの基本的なセキュリティとプライバシーの要件	アプリ開発者 OS提供事業者	■ アプリ開発者及びOS提供事業者は、アプリ内やローカルでデータを暗号化する場合、業界標準の暗号化を使用しなければならない。 ■ アプリ開発者は、利用者がオプション機能を無効化した場合も、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。 ■ アプリ開発者は、アプリが機能的に必要としない権限や特権を要求することは望ましくない。権限や特権を要求する必要がある場合は、アプリストア運営者と共有し、相互に確認できるようにしなければならない。 ■ アプリ開発者は、アプリに簡単なアンインストールプロセスが存在することを確認しなければならない。 ■ アプリ開発者は、アプリの全ての公開バージョンにおいて、既知の脆弱性がないか、監視するプロセスを備えていることが望ましい。 ■ アプリ開発者は、アプリが収集した利用者情報の削除を要求する仕組みを利用者に提供しなければならない。
3	脆弱性の開示プロセス	アプリ開発者 アプリストア運営者	■ 全てのアプリには、連絡先や問い合わせフォームなど、アプリ開発者によって作成・維持される脆弱性開示プロセスを用意しなければならない。また、アプリストア運営者はアプリストアのプラットフォームで見つかった脆弱性を報告できるように連絡先や問い合わせフォームなどの脆弱性開示プロセスを備えていなければならない。 ■ アプリストア運営者は、全てのアプリがアプリストアからアクセス・表示可能な脆弱性開示プロセスを有していることを確認しなければならない。当該プロセスは悪意のある行為者に知られることなく、脆弱性を報告できることを保証しなければならない。

【参考】諸外国における利用者情報の取扱いに係る規制動向に係る文献調査

No	Code of Practiceに示された原則	適用者	概要
4	アプリのアップデート	アプリストア運営者 アプリ開発者 OS提供事業者	■ アプリ開発者は、アプリ内のセキュリティの脆弱性を修正するためのアップデートを提供しなければならない。また、アプリ内で使用しているサードパーティ製ライブラリやSDKがアップデートされた場合、アプリのアップデートを提供しなければならない。 ■ アプリ開発者がアプリのセキュリティアップデートをする場合、アプリストア運営者は利用者にアプリを最新バージョンにアップデートするように奨励しなければならない。なお、アプリストア運営者は、明確な理由なくセキュリティアップデートを拒否してはならない。 ■ アプリが2年間アップデートされていない場合、アプリストア運営者は開発者に連絡して、アプリがサポート中か確認しなければならない。30日以内に応答がない場合、アプリをストアで利用できないようすることを検討することが望ましい。
5	セキュリティやプライバシーに関する情報のユーザへの提供	アプリストア運営者 アプリ開発者	■ アプリストア運営者は、アプリがストアから削除されるか、または、利用できなくなった場合、当該情報を利用者に提供し、利用者が削除する方法に関する手順を示すリンクを提供しなければならない。 ■ アプリストアには、利用者がダウンロードしてインストールしたアプリのうち、アプリストアで利用できなくなったアプリを利用者に情報提供する機能が必要である。 ■ アプリ開発者は、利用者の情報が保存等される場所やその他関連するセキュリティ情報を提供しなければならない。 ■ アプリストア運営者は、全てのアプリについて、セキュリティとプライバシーの専用ページなどで、アクセスする利用者情報やその目的等について情報提供しなければならない。 ■ アプリ開発者は、連絡先、位置情報、デバイスのマイクへのアクセスなど、アプリが要求する可能性のある権限に関する情報とこれらの権限が必要な理由を提供しなければならない。アプリストア運営者は、これらの情報をアプリ購入前に表示しなければならない。
6	開発者向けのセキュリティとプライバシーに関するガイダンスの提供	アプリストア運営者	■ アプリストア運営者は、アプリの投稿に先立ち、当該実施規範をアプリ開発者に提示しなければならない。 ■ アプリストア運営者は、事前にアプリ開発者ガイドライン/ポリシーの変更について公表することが望ましい。 ■ アプリストア運営者は、一般的なサードパーティ製ライブラリやサービスを監視して関連情報を共有し、複数のアプリにまたがる潜在的な脅威を明らかにするなど、アプリ開発者による効果的なサプライチェーン管理の実施を支援することが望ましい。
7	開発者へのフィードバックの提供	アプリストア運営者	■ アプリストア運営者は、アプリの申請を却下した場合、承認するためにどのような変更が必要か明確にし、一貫性のある実用的なフィードバックを提供することが望ましい。
8	個人情報漏洩時の対応	アプリ開発者 アプリストア運営者	■ アプリストア運営者は、個人情報漏洩を伴うセキュリティインシデントを認知した場合、当該アプリ開発者に通知しなければならない。 ■ アプリ開発者は、アプリストア運営者等の利害関係者に通知することが望ましい。 ■ アプリストア運営者は、個人情報漏洩について通知を受けた場合、当該アプリを使用不可とすることを検討することが望ましい。

【参考】スマートフォンアプリケーション開発者の実施規範

概要

- スマートフォンの普及から10年以上が経過し、多数のアプリケーションが提供される中、アプリマーケットは利用者の安全を確保するため様々な条件や規制を定めている。
- 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せず、提供者によって異なるため、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る。

No	実施規範	概要
1	セキュリティとプライバシーの基本要件	• セキュリティとプライバシー基本要件の準拠（業界標準の暗号化の使用等） • セキュアコーディングの実施（アプリ開発に際して参照することが推奨されるガイドライン等） • セキュリティテストの実施（セキュリティテストを実施する際に参考すべきガイドライン、脆弱性診断の実施等）
2	アプリ公開後のメンテナンス	• 脆弱性情報の収集（アプリの脆弱性の定期的な確認等） • 脆弱性の対応（速やかな対応の実施、アップデートの要求等） • アプリの保守・運用（脆弱性申告窓口の設置等）
3	プライバシーの基本要件	• アプリマーケットでの対応（アプリマーケットのポリシー等の遵守等） • 透明性の確保（プラポリの表示、同意の取得等） • アプリプライバシーポリシーの作成（アプリプラポリに記載すべき項目への対応等）
4	利用規約の基本要件	• 利用規約の作成
5	ユーザサポート	• 推奨されるユーザサポート項目（利用者の問い合わせ窓口の設置等） • 推奨されるユーザサポートセキュリティ項目（アプリ利用時のセキュリティに関する注意事項の提供等）
6	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発生時のフローの整備等