資料5

外部送信規律の解説案について

2022年12月2日

日本スマートフォンセキュリティ協会（JSSEC）
技術部会 部会長 仲上竜太
（ニューリジェンセキュリティ株式会社）

外部送信に係る利用者に関する情報の取扱い①
通知又は容易に知り得る状態に置く方法について

JAPAN SMARTPHONE SECURITY ASSOCIATION

基本原則

① 透明性の確保
関係事業者等は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保
関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③ 適正な手段による取得の確保
関係事業者等は、対象情報を適正な手段により取得するものとする。

④ 適切な安全管理の確保
関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤ 苦情・相談への対応体制の確保
関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥ プライバシー・バイ・デザイン
関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。
利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

スマートフォン利用者情報取扱指針：基本原則と改正個人情報を踏まえたプライバシーポリシーの整理

出典：スマートフォン　プライバシー
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html

スマートフォンアプリにおける利用者情報の取り扱いにおいては、「スマートフォン・プライバシー・イニシアチブ(SPI)」（平成24年公表）および改正個人情報法に対応した個人情報に関するガイドライン（令和4年）で規定されたプライバシーポリシーに矛盾なく参照されることが望ましい。

SPI記載内容より引用：
①スマートフォンにおける利用者情報を取得しようとするアプリケーション提供者、情報収集モジュール提供者（これらを提供する広告事業者等を含む）は、個別のアプリケーションや情報収集モジュール等について、以下の①から⑧までの事項について明示するプライバシーポリシー等をあらかじめ作成し、利用者が容易に参照できる場所に掲示またはハイパーリンクを掲載する。

<プライバシーポリシーへの記載事項>
(a) 関係法令・本電気通信事業GL遵守
(b) ガイドラインに定める事項
（ｉ）電気通信事業者の氏名又は名称
（ii）取得される情報の項目
（iii）取得方法
（iv）利用目的の特定・明示
（ｖ）通知・公表又は同意取得の方法及び利用者関与の方法
（vi）第三者提供の有無
（vii）問合せ窓口・苦情の申出先
（viii）プライバシーポリシーの変更を行う場合の手続き
（ix）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
（ｘ）委託に係る事項
(c) 安全管理措置に関する方針
(d) その他利用者の権利利益の保護に関する事項

SPIを踏まえた8項目

デジタル広告市場の競争評価　最終報告等を踏まえた追加事項

出典：JSSEC セキュリティフォーラム2022オンライン・総務省総合通信基盤局電気通信事業部 消費者行政第二課長小川 久仁子様発表資料より抜粋。
https://www.jssec.org/dl/20220324_sf22_ogawa.pdf

外部送信に係る利用者に関する情報の取扱い②
電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報

●-4-1-1 電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報（第●条第 6 項第 1 号関係）

（1）当該電気通信役務において送信する符号、音響又は影像を当該利用者の電気通信設備の映像面に適正に表示するために必要な情報その他当該電気通信役務の提供のために真に必要な情報（第●条第 6 項第 1 号イ関係）

意見）

真に必要な情報とは、利用者が利用者情報の送信のオプトアウトを選択したとしても利用者の期待するサービス提供が可能な情報と定義でき、サービス提供内容に応じてその判断が異なると考える。

例として、案では＜真に必要な情報への該当性＞について「アクセス解析」について「×」と判断されているが、取得される利用者個人の情報をマスキング処置し統計的に処理されたアクセス情報は、サービスの安定的かつ経済的に合理性のある提供を維持するために必要な情報と言え、(5)に示された利用者全体の利用傾向を把握する活動と適切な運用のために必要な情報と分けがたい。

記載方法としては、真に必要な情報への該当ケースを例示しつつ、個別の解説の記載が望ましいと考える。

外部送信に係る利用者に関する情報の取扱い③
電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報

●-4-1-1 電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報（第●条第 6 項第 1 号関係）

（4）当該電気通信役務に対する不正な行為の検知等を行い、又は当該不正な行為による被害の軽減等を図るために必要な情報（第●条第 6 項第 1 号二関係）

意見）

サービスへの攻撃判断に関する情報の一例として、各種セキュリティ対策装置等においてサイバー脅威情報源と照らし合わせて攻撃を検知・遮断する手法が主流である。その際、クラウド形態でセキュリティ対策が行われる事例も普及しつつある現状から、不正行為等の検知のための情報は電気通信役務を利用するために送信することが必要な情報として考えられ、一般的には以下のような情報が該当する。

・IPアドレス
　・IPアドレスより判断可能な国情報、プロバイダ情報などを含む
・利用者のブラウザ環境を含むリクエストヘッダー情報
・アクセス先URL文字列
・リクエストクエリー文字列
・その他セキュリティ装置によって参照されるリクエスト情報

外部送信に係る利用者に関する情報の取扱い④
電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報

●-4-1-1 電気通信役務を適正に表示するために必要な情報その他の電気通信役務を利用するために送信することが必要な情報（第●条第 6 項第 1 号関係）

（５）当該電気通信役務の提供に係る電気通信設備の負荷を軽減させるために必要な情報その他の当該電気通信設備の適切な運用のために必要な情報（第●条第 6 項第 1 号ホ関係）

意見）

通信負荷を軽減させるための情報は、負荷分散装置による機械的な判断による分散のほか、ロケーションによる配信地点の動的な選択、登録時に割り当てられるサーバの分散など複数の観点から動的に操作または調整する必要がある。

利用者から取得する情報としては以下のものが考えられる。

・IPアドレス

　・IPアドレスより判断可能な国情報、プロバイダ情報などを含む

・端末機種種別

・アプリケーション種別（ブラウザ／ネイティブアプリなど）