

利用者に関する情報の外部送信に掛る規律に 関するJSSECの考え方

2022年6月22日

一般社団法人日本スマートフォンセキュリティ協会
技術部会 部会長 仲上竜太

日本スマートフォンセキュリティ協会：JSSECについて



概要

- 名称：一般社団法人日本スマートフォンセキュリティ協会
- 略称：JSSEC / WEB：https://jssec.org
- 代表者氏名:会長 佐々木 良一
- 設立：2011年5月25日（2012年一般社団法人化）
- 幹事会員14社、正会員51社（通信キャリア、メーカー、セキュリティベンダー他）

目的

- 企業・団体における利用者が安心して高度なサービスを受けられるようにする。
- 実装すべきセキュリティレベルの理解を社会に浸透させ、提供者が安心して事業推進を行えるようにする。
- 利用者のセキュリティリテラシー向上のための活動も行い、さらに高度なサービスを受けられるようにする。
- セキュリティを切り口とした「信頼できるニッポン！」を確立しグローバル市場へアピールする。

• 利用部会

- 安心・安全なスマートフォン利用のために情報収集と課題を整理し、情報発信を行う。又、近年のスマートフォン利用形態の変化に合わせ、IoTの導入など利用企業の共通的な経営課題を中心にテーマを選定し、利用事例の調査や新しい技術の調査・研究の成果を発信する。
- 『スマートフォン利用ガイドライン 対策チェックシートⅡ【NIST-CSF対応版】』、『IoTセキュリティチェックシート』

• 技術部会

- スマートフォンを安全に利用するための技術的な調査・研究・議論を行う。具体的には4ワークグループで構成し成果物を公開する事で、日本におけるスマートフォン利用の安全性向上に寄与する。
- 『スマートフォンセキュリティ実装ガイド』『Androidアプリのセキュア設計・セキュアコーディングガイド』『スマートフォン・サイバー攻撃対策ガイド』

• 啓発部会

- JSSECがスマートフォンの安全利用を推進し広く社会に貢献するため、積極的に啓発活動展開を行うことを目的とする。

• PR部会

- JSSECが行うすべての活動について普及啓発するための情報配信を行う

サービスを構成するレイヤー



- スマートフォンアプリのサービスを前提にした場合、プライバシー保護を行ういくつかのレイヤーを対象に考慮する必要があります
- 外部送信の観点では取得する「スマホアプリ」「ウェブアプリケーション」の観点で整理する必要があります
- スマホアプリの中で実装上組み込まれる3rd Partyライブラリで外部送信に関するセキュリティ課題が生じている事例も確認されています
- ウェブアプリケーションの連携する3rd Partyサービスへの送信や外部委託における考え方を整理する必要があります

利用者に関する外部送信の際の措置についての過去の取り組み

- スマートフォンアプリやスマートフォンを対象にしたウェブサービスにおいては総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」が、平成24年8月、利用者が安心安全にアプリを利用できる環境を確保するため、アプリが利用者情報を外部送信又は蓄積を伴う形で取得している場合には、アプリ提供者に対し、アプリごとに当該情報の取扱指針を示したプライバシーポリシーの作成を推奨する「**スマートフォン プライバシー イニシアティブ**」(SPI) が公表されている。
- スマートフォン・プライバシー・イニシアティブII (SPI II) では、第三者の検証を実施し、その結果の蓄積について公表
- SPI, SPI IIの検討結果を踏まえ、スマートフォン・プライバシー・イニシアティブIII (SPI III)、スマートフォン・プライバシー・アウトルックにより利用状況の把握・実証実験が行われた。



JSSECにおいては、SPI、SPI IIに準拠して利用者情報の利用についての同意を得るためのルールをAndroidセキュアコーディングガイドに反映しています
またアプリケーションコードからプライバシーポリシー案を生成するツールなどを開発しました

利用者に関する外部送信の際の措置について

規律の内容

電気通信事業者又は第三号事業を営む者が利用者に対し電気通信役務を提供する際に、利用者の電気通信設備を送信先とする情報の外部送信を指令するための通信（※）を行おうとするときは、当該通信によって送信されることとなる当該利用者に関する情報等を当該利用者に（１）通知又は容易に知り得る状態に置く、（２）同意を取得、（３）オプトアウトのいずれかの措置を取ることとする。

JSSECの考え

- JSSECの見解としては、スマートフォンアプリケーションで行われたプライバシーポリシー実装の議論にもとづき、これらの措置については先のアプリケーションまたはサービスいずれかでの実装において第三者が検証可能な状態であることが必要であると考えます。
- 「（１）通知又は容易に知り得る状態に置く」については、「（２）同意」「（３）オプトアウト」の前提条件となることから（１）は必須であると考えます
- 今後、具体的な検討を進めたいと考えておりますが、その内容に応じて個別に意見をさせていただく機会をいただければ幸いです。

利用者に関する外部送信の際の措置について

【論点1：第27条の12柱書き】内容、利用者の範囲及び利用状況を勘案して利用者の利益に及ぼす影響が少ない電気通信役務

JSSECの考え

①電気通信役務の内容

これらのサービスに加え従来届け出対象となっている「オンラインゲーム」と同類であり、仮想空間上で個人がコミュニケーションが可能な「メタバース」「仮想空間サービス」についても登録・届出の対象とすることで、安全な利用を促すことが可能であると考えます。

②利用者の範囲

I、IIはスマートフォンアプリケーションの多くが内部的にウェブサービスを利用していることから、明確に分けられない場合があると考えます。

③利用状況

すべての情報は安全に扱われるべきという前提に立ちつつ、第三者検証の可能性なども含めた運用を考慮すると、ある程度の定量的な規模を対象に設定することが求められると考えます。

利用者に関する外部送信の際の措置について

【論点2：第27条の12柱書き】 通知又は利用者が容易に知り得る状態に置く際に満たすべき要件

【論点3：第27条の12柱書き】 通知又は利用者が容易に知り得る状態に置くべき事項

【論点4：第27条の12第4号ロ】 オプトアウト措置の際に利用者が容易に知り得る状態に置く事項

JSSECの考え

スマートフォンアプリのセキュリティ実装に関する観点からは、アプリケーション開発の際に省令に基づき開発者に要請する内容があればガイドラインへの反映や開発者への周知などの対応したいと考えています。

利用者に関する外部送信の際の措置について

【論点5：第27条の12第1号】 利用者が電気通信役務を利用する際に送信をすることが必要な情報

JSSECの考え

スマートフォンアプリにおける適切な情報については引き続き会員企業とのコミュニケーションを通して検討を進めたいと考えています。

セキュリティを維持するうえで情報について検討を進めたいと考えています。