

1. アプリケーション提供者等

1-1 アプリケーション提供者

項目	SPIに盛り込む内容
セキュリティ バイデザイン	<ul style="list-style-type: none"> セキュリティが適切に確保されるよう、アプリの企画及び設計の段階から、適切な仕組みを組み込むことが望ましい アプリで使用する情報収集モジュール等について、セキュリティの確保の観点から内容を確認することが望ましい
脆弱性がある アプリへの対応等	<ul style="list-style-type: none"> アプリに係る脆弱性情報を継続して収集するとともに、脆弱性情報の窓口・連絡先を設置するなど必要な体制の整備に努める アプリ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、アプリのアップデートを提供するなど必要な対応を取ることが望ましい 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よう努める

1-2 情報収集モジュール等提供者

- 「1-1 アプリケーション提供者」と同様の取組を行う。

2. アプリストア運営事業者、OS提供事業者

- アプリストア運営事業者は、次に掲げる取組を進めることが望ましい。

項目	SPIに盛り込む内容	
アプリストアとしての 基本的対応	①	<ul style="list-style-type: none"> 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
	②	<ul style="list-style-type: none"> ストア内で提供される各アプリについて、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
脆弱性がある アプリへの対応	③	<ul style="list-style-type: none"> ストア内で提供される各アプリが、脆弱性報告のための窓口を有するとともに、アプリ提供者が適切なタイミングで脆弱性を開示するための手続を有していることを確認する。
	④	<ul style="list-style-type: none"> 利用者に対してアプリが最新版にアップデートされるように促すなど、必要な対応を取る
	⑤	<ul style="list-style-type: none"> アプリが長期間アップデートされない場合には、アプリ提供者にアプリのサポート状況を確認する
不正なアプリ への対応	⑥	<ul style="list-style-type: none"> ストア内において、利用者等が不正なアプリを報告できるよう報告窓口を設置する
	⑦	<ul style="list-style-type: none"> 不正なアプリを発見した場合には、速やかに削除するとともに、当該アプリの提供者が開発した他のアプリについても調査を行う
アプリ削除・掲載 拒否時の対応	⑧	<ul style="list-style-type: none"> アプリの掲載を拒否する場合には、その理由について、アプリ提供者に対して適切なフィードバックを行う

※OS提供事業者は、利用者のためにセキュリティやプライバシーを保護するため、アプリストアが上記の取組を実施することを奨励するとともに、必要な措置を講じることが望ましい。