資料3

生体認証の利用制限方式の検討

2021年7月28日

はじめに

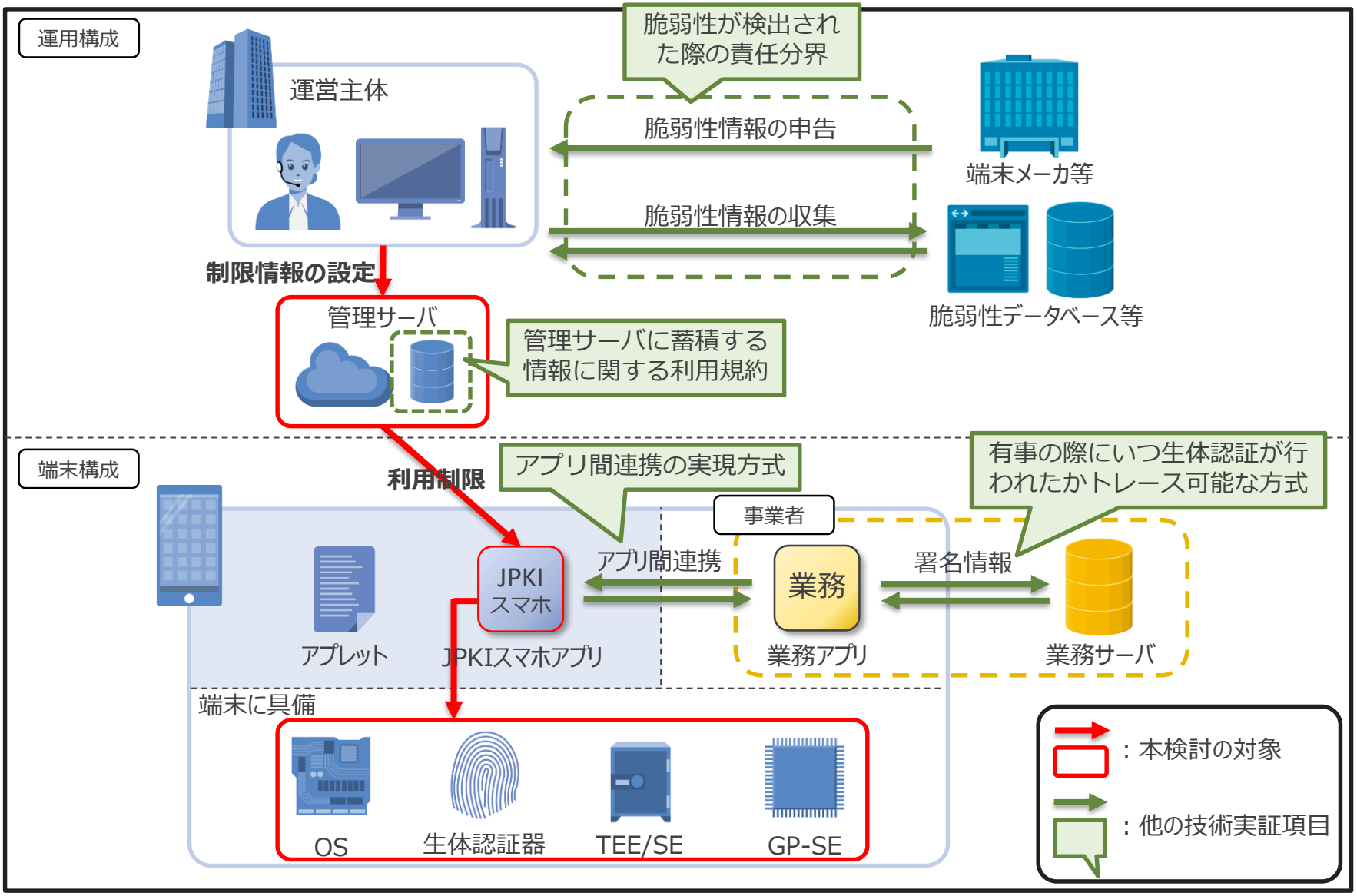
【本検証実施の背景】
　利用者証明用証明書の利用時にAndroid-OSの生体認証機能を用いることで利便性の向上を図る。
　ただし、スマートフォンにおいてOSやICチップ等に脆弱性が検出された際に利用者を保護するため、生体認証機能に限らずJPKI機能を遠隔で制限する方式や運用を検討する。

【本資料の目的】
　JPKI機能及び生体認証機能利用制限の検証を行うにあたり、技術実証用システムで構築予定の利用制限方式やその運用イメージ、処理フローを報告する。
　利用制限の是非や実現方式などについてご意見を頂きたい。

【目次】

1.利用制限の構成図

技術実証対象外の箇所については今後の設計工程等で検討していく必要がある。



2.JPKIスマホアプリに利用制限が必要となるケース

スマートフォンで脆弱性が検出される可能性のある対象について、実施すべき利用制限を検討した。
具体的な過去事例や発生頻度等は今後端末メーカ等へヒアリングを予定している。

想定される脆弱性が見つかる対象		想定する制限
 OS	OSに脆弱性等が検出された場合	・新規インストールの停止(PlayStoreでの制限を想定) ・JPKIスマホアプリの利用を停止
 生体認証器	生体認証器に脆弱性等が検出された場合	・JPKIスマホアプリ上での生体認証機能の登録/利用を停止
 TEE/SE	TEE/SEに脆弱性等が検出された場合	・JPKIスマホアプリ上での生体認証機能の登録/利用を停止
 GP-SE	GP-SEに脆弱性等が検出された場合	・新規インストールの停止(PlayStoreでの制限を想定) ・JPKIスマホアプリの利用を停止

3.利用制限を行う方式

技術実証用システムでは以下の前提条件を満たす2つの方式を構築し、実証後に方式ごとの特徴や課題を整理して報告予定である。

前提条件

- 遠隔での特定機種およびOSバージョンの識別が可能
- 遠隔での利用制限および制限解除が可能
- 利用制限をかける際の反映時間が現実的に運用可能

方式1．独自サーバ上に利用制限端末管理機能を構築

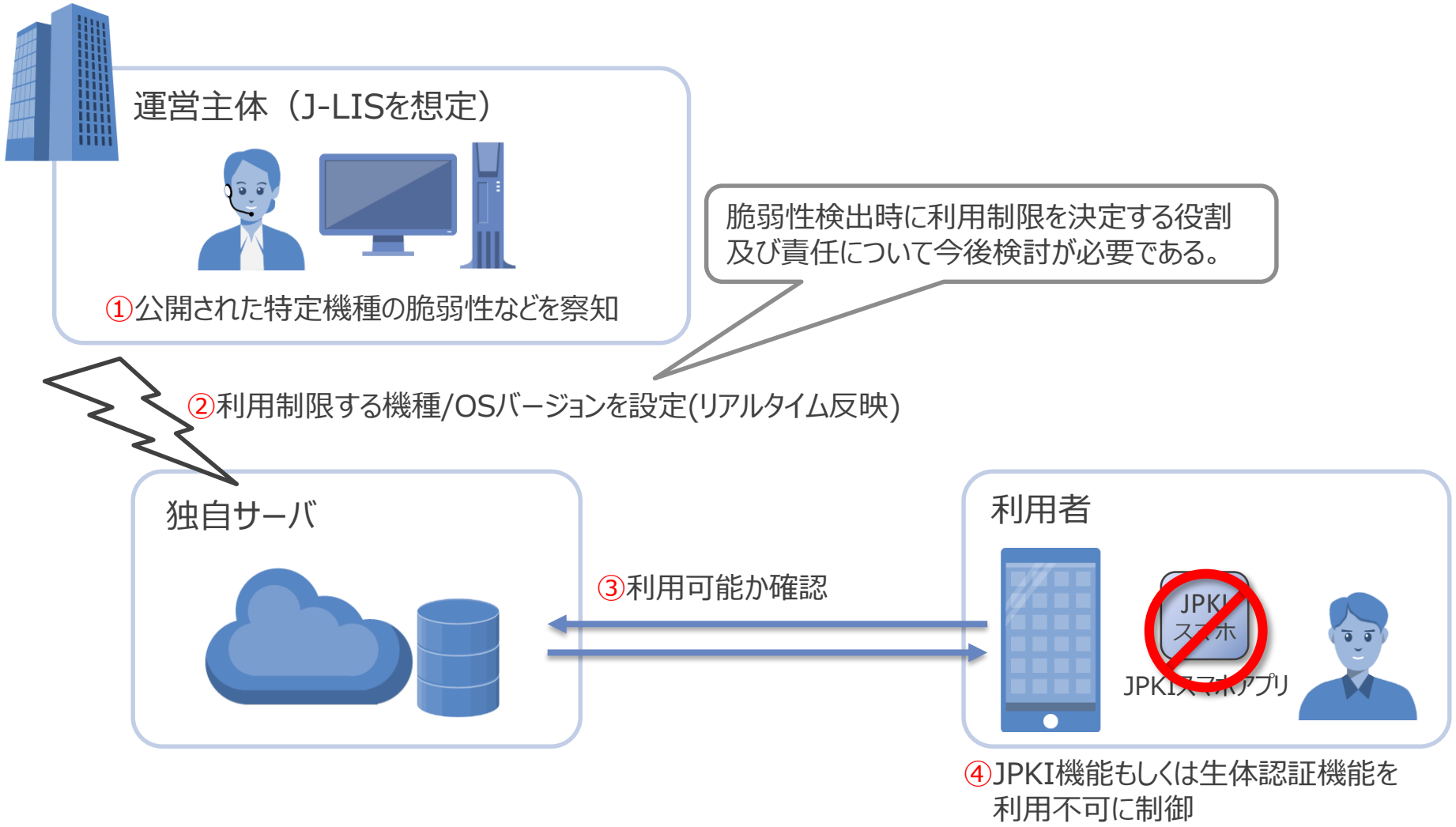
機種、OSバージョンごとに利用可否を管理可能なシステムを構築する。
TSMサーバ上にこの機能を構築する想定である。
JPKIスマホアプリはアプリ起動時や生体認証機能の利用を行う前にサーバにアクセスし、利用可否状態の取得、利用制限を行う。

方式2．汎用サービスを利用して利用制限機能を構築

実証用システムでは構築期間が短いFirebase Remote Config(Firebase)を採用する。
Firebaseのコンソール上で利用制限を行う機種、OSバージョンを指定する。
JPKIスマホアプリは定期的にFirebaseのサーバに利用可否の状態を確認し、利用制限を行う。

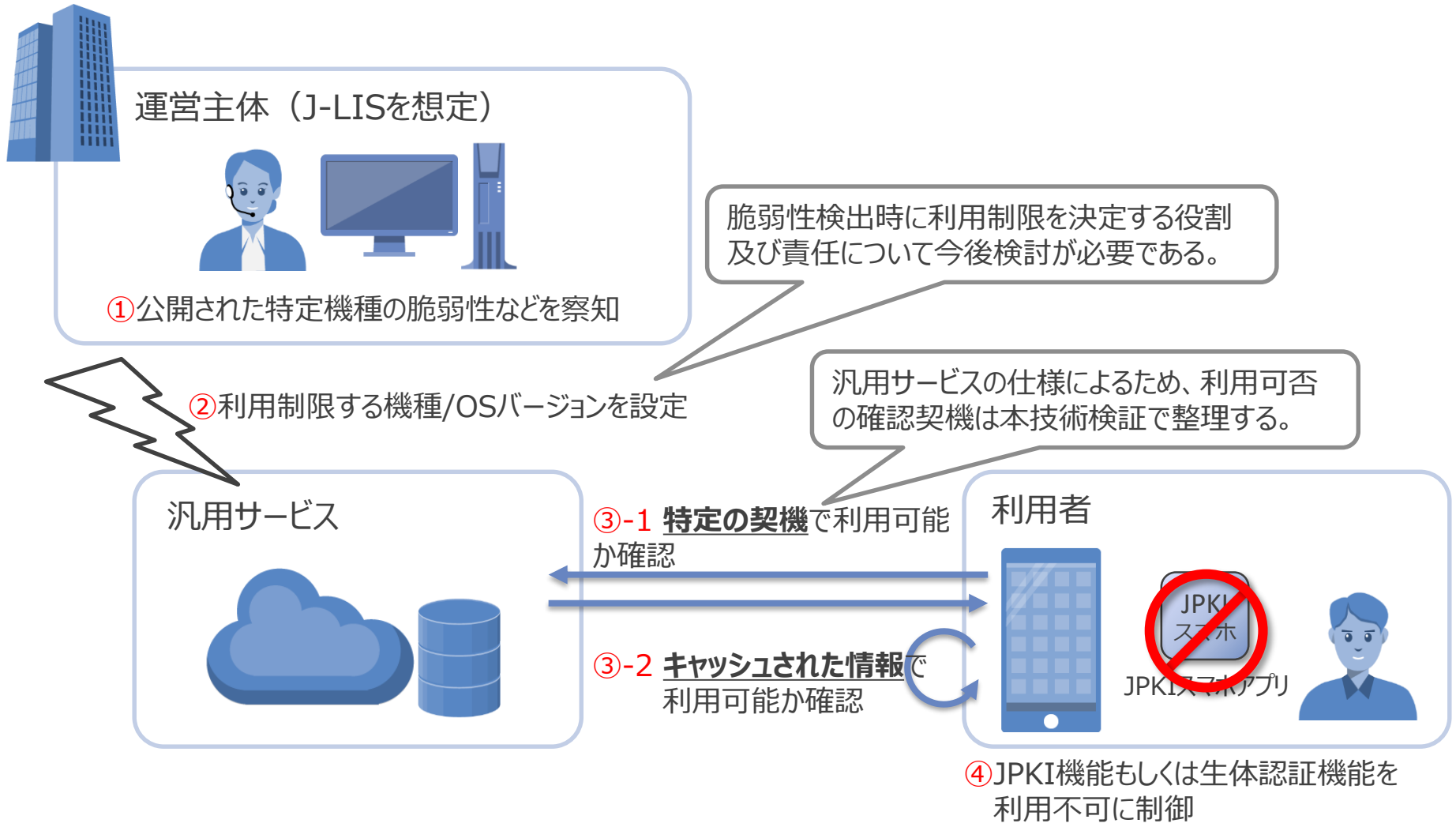
3.1.1. 運用イメージ - 方式1：独自サーバ上に利用制限端末管理機能を構築

方式1(独自サーバ上に構築)は利用制限情報のリアルタイム反映が可能であるが、独自サーバ上に管理機能を構築する必要がある。



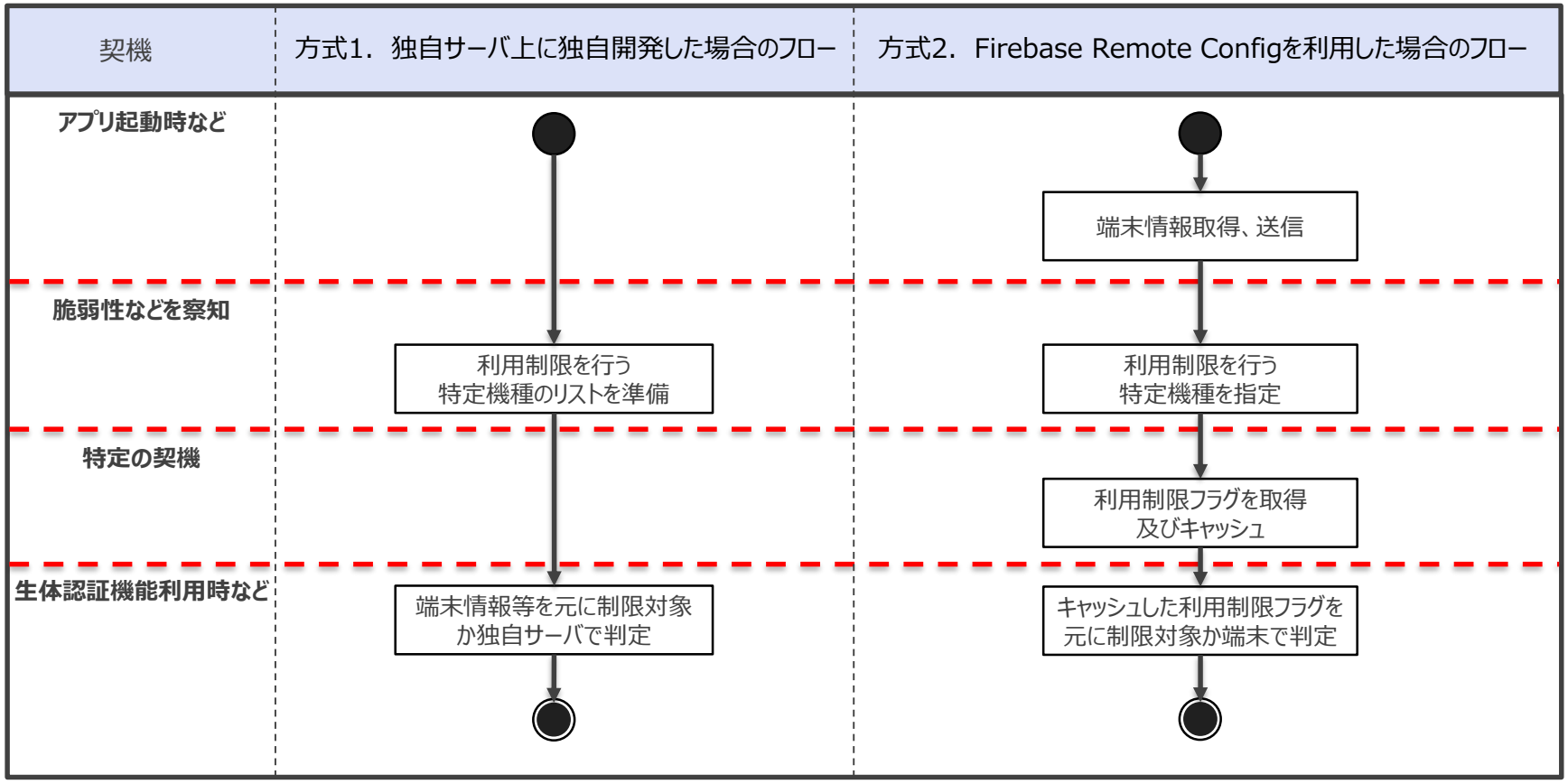
3.1.2. 運用イメージ - 方式2：汎用サービスを利用して利用制限機能を構築

方式2(汎用サービスの利用)は管理機能を無償で利用可能だが利用制限情報の反映までに一定の時間を要する(Firebaseでは最大12時間)。



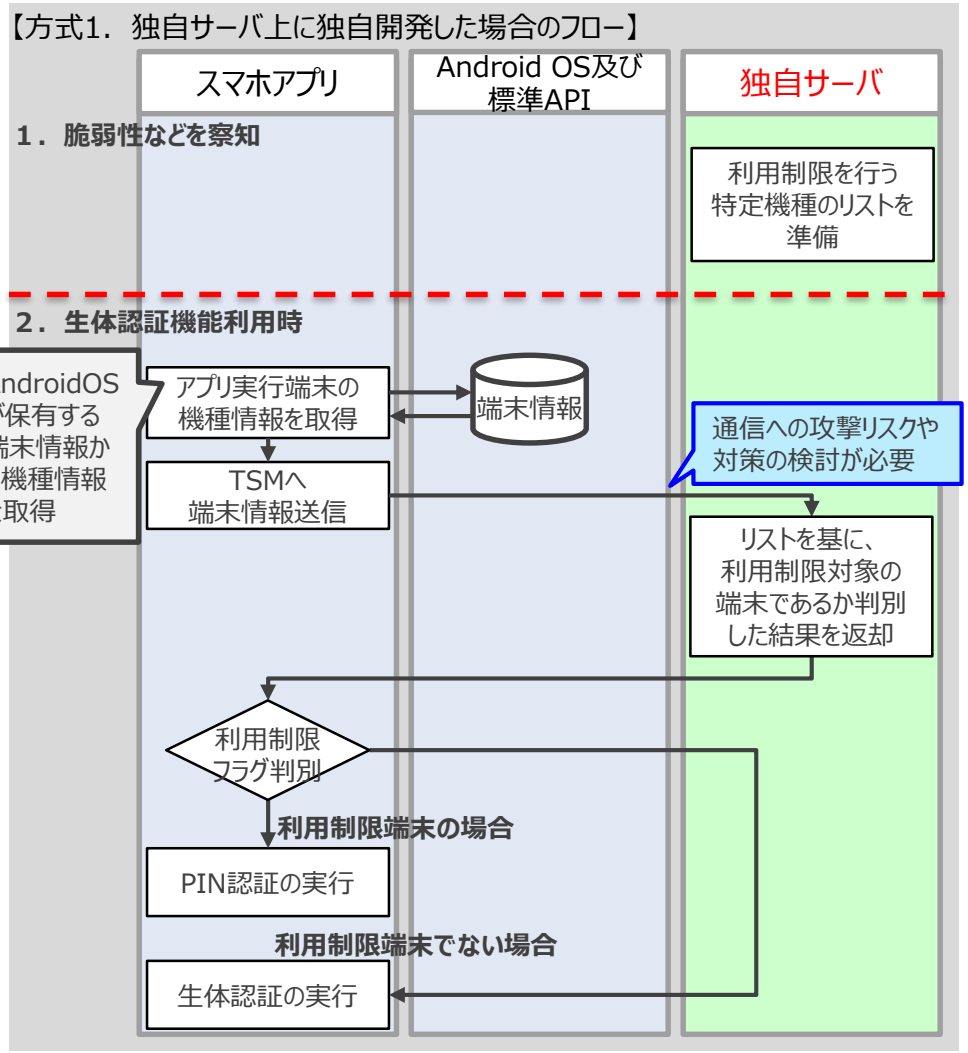
3.2.各方式の処理フロー比較

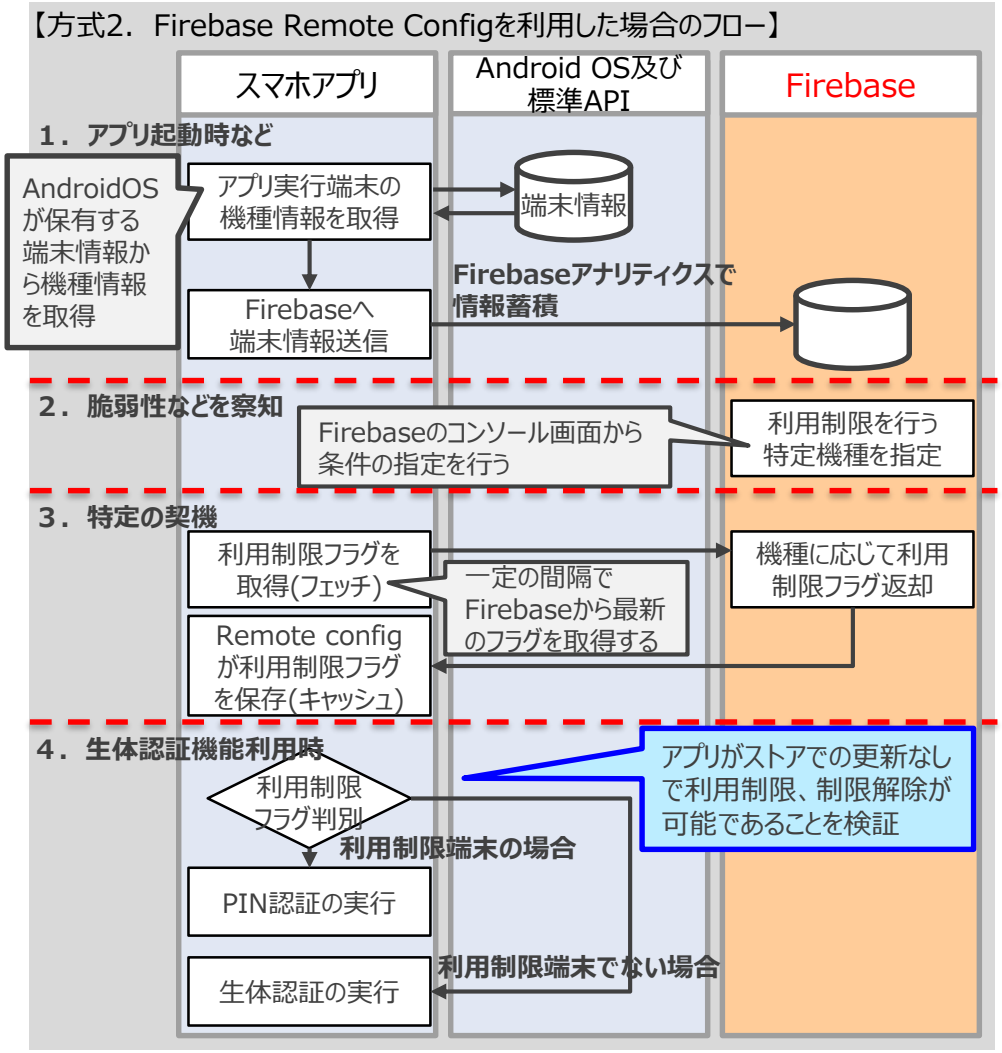
端末情報の送信タイミングや、利用制限対象かどうかをサーバから取得するタイミングが主な差異である。



3.2.各方式の処理フロー比較

下図は生体認証機能に対して利用制限を行う場合の処理フローとなるが、JPKI機能を停止する場合でも処理の流れ自体は変わらない。





3.3.各方式の特徴比較

現時点で判明している各方式の特徴は下表のとおりである。
技術実証用システムでの実機検証を通して再評価を行い、最終的な方式決定に向けて検討を進めていく。

観点		方式1 独自サーバ上に独自開発	方式2 汎用サービスを利用
端末の識別に関する観点	各端末での端末情報取得	○ 情報取得の手法は同一、OS標準のAPIで取得を想定	
	各端末からの情報取集	○	○
利用制限に関する観点	即時性	○	△ 反映までに時間を要する場合がある
	メンテナンス性	○	○ 汎用サービスの仕様が変更される可能性あり
	柔軟性（カスタマイズ性）	◎	○
	開発コスト/運用コスト	○ コンソールなどの開発も必要	◎

方式ごとの特徴を踏まえ、制限対象によって使い分けるハイブリッド案も検討中。

◎：非常に優れている、〇：適用可能なレベル、△：部分的に問題がある