資料4

アプリ間連携の検討

2021年7月28日
株式会社NTTデータ

はじめに

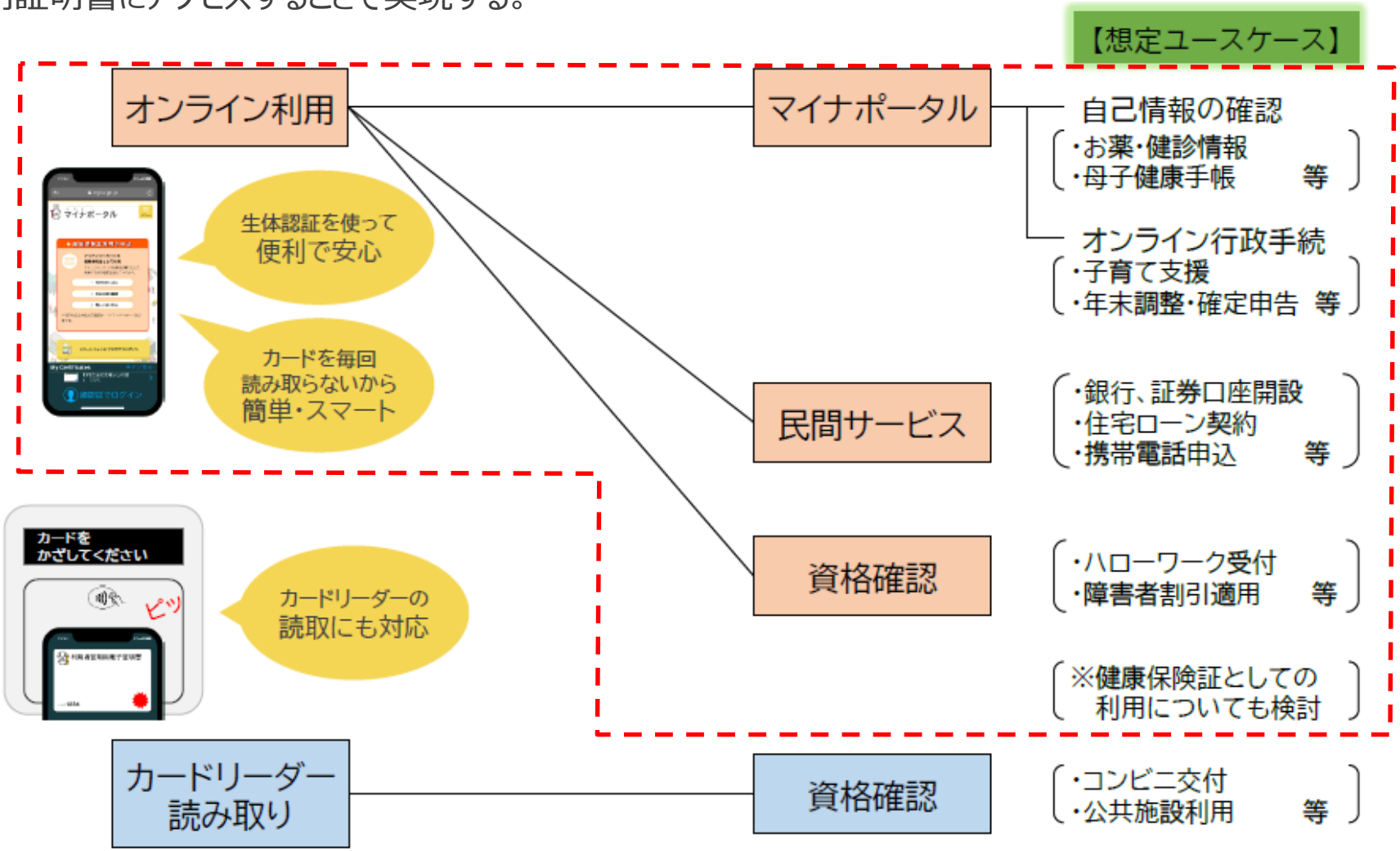
【本検証実施の背景】
　スマホJPKIの幅広い普及を実現するには、民間事業者／公的機関が提供する業務アプリから、スマホJPKIを利用するための連携機能が、安全安心かつ便利に使えることが重要となる。本検討では、多様な業務アプリへの対応を想定して、Androidアプリおよびブラウザを経由したスマホJPKI利用における連携方式について検討する。

【本資料の目的】
　スマートフォンにカードをかざしてJPKIを使用するという既存の体験と、スマートフォンに搭載したJPKIを使用するという新しい体験では、リスクを評価する上で考慮すべき様々な違いがある。この違いを踏まえて、想定されるリスクへの対応方針についてご意見を頂きたい。

【目次】

1．連携機能を活用する範囲

連携機能を活用する範囲として、公的機関/民間事業者が提供する業務アプリからのオンライン利用を対象とする。
オンライン利用は、Androidアプリまたはブラウザ上のサービスから、スマートフォンに格納した利用者証明用証明書／署名用証明書にアクセスすることで実現する。



出典：マイナンバーカードの機能のスマートフォン搭載等に関する検討会　第１次とりまとめ(令和2年12月25日)より抜粋

2．連携時に利用するスマホJPKI機能

オンライン利用では、各業務アプリからスマホJPKIのスマホ証明書利用機能を用いて証明書にアクセスする。
証明書管理機能(発行、失効など)については、連携先業務アプリから使用する必然性のあるユースケースがないため、
連携対象とせず、JPKIスマホアプリ固有の機能とすることが、構築・維持管理コストの観点から望ましいと考える。

ログイン画面 → 認証画面 → ログイン結果画面

No.	分類	機能	ユーザ体験
1	スマホ証明書利用機能	利用者証明用	スマホ(PIN/セキュアロックスクリーン)
2		署名用	スマホ(PIN)
3	スマホ証明書管理機能	発行	カード(PIN)
4		失効	カード(PIN) or スマホ(PIN)
5		更新・再発行	カード(PIN)
6		セキュアロックスクリーン登録	カード(PIN) or スマホ(PIN)
7		PIN変更	スマホ(PIN/セキュアロックスクリーン)
8		PIN閉塞解除(PIN初期化)	カード(PIN) or スマホ(PIN)
9		証明書情報確認	スマホ(PIN/セキュアロックスクリーン)

３．本検討を進める上での前提

本検討を行う上での前提条件と、既存のユーザ体験との相違点について整理した。
ユーザに安心安全に業務アプリからスマホJPKIを利用頂くためには、「スマートフォンアプリでGP-SEのJPKI機能を利用する」という新たなユーザ体験において、既存の体験と比較してどのようなリスクがあるかを考慮することが重要となる。

検討における前提

・連携先のサービスを提供するアクタとして、公的個人認証サービスにおける下記事業者を想定。
　プラットフォーム(PF)事業者：総務大臣認定の設備を所持しており、システムに証明書情報を保存可能
　サービス提供者：自らの設備にはデータを保存できないが、PF事業者に証明書情報の保存を委託可能

・AndroidアプリがGP-SEにアクセスするためには、事前にGP-SEにアプリ署名者証明書を登録する必要があるが、登録に伴う運用の煩雑さとチップ容量の観点から、登録数はなるべく少ないことが望ましい。

新しいユーザ体験で考慮すべきこと

・ユーザ体験の比較
　- 既存体験では、スマホにカードをかざしている間のみJPKI機能へのアクセスが発生する可能性がある。
　- 新しい体験では、常時JPKI機能へのアクセスが発生する可能性がある。

・新しい体験で考慮すべきリスク
　- スマホ内の不正アプリ、および、インターネット経由でアクセスされるリスク
　- ユーザの意識しない所でアクセスされるリスク

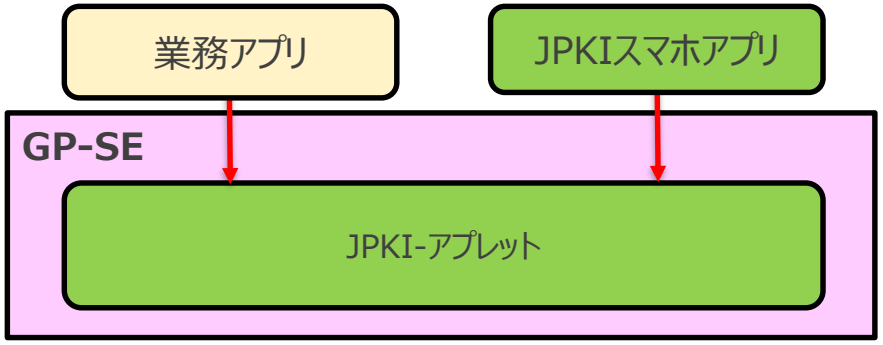
４．スマホJPKIと各業務アプリ連携時の構成

スマホJPKIと各業務アプリを連携する際の構成として、下図に示す2つの構成が考えられるが、構成１については以下の検討ポイントを踏まえ、構成２を採用することとする。

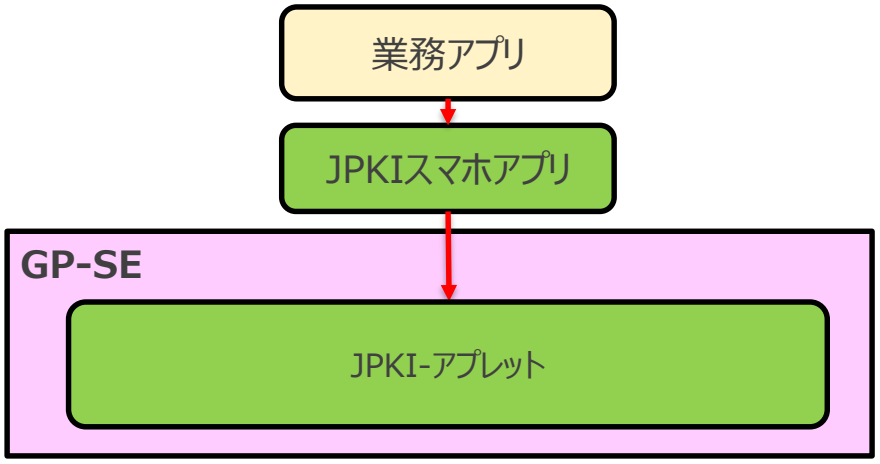
■検討のポイント

○構成1ではGP-SEへのアクセスを民間事業者含めて広く認めることとなるが、これはセキュリティのコアとなる機能にOS経由での直接アクセスを許すことと同義であるため、事業者への機能解放や開示情報のコントロールのしやすさを考えると、構成2のようにアプリを経由する方式とすることが望ましいと考える。

○構成2は、JPKIを利用する業務アプリが発生する度に、GP-SE内のアプリ証明書のハッシュリスト更新が不要である。



構成１． 業務アプリからGP-SEに直接アクセス

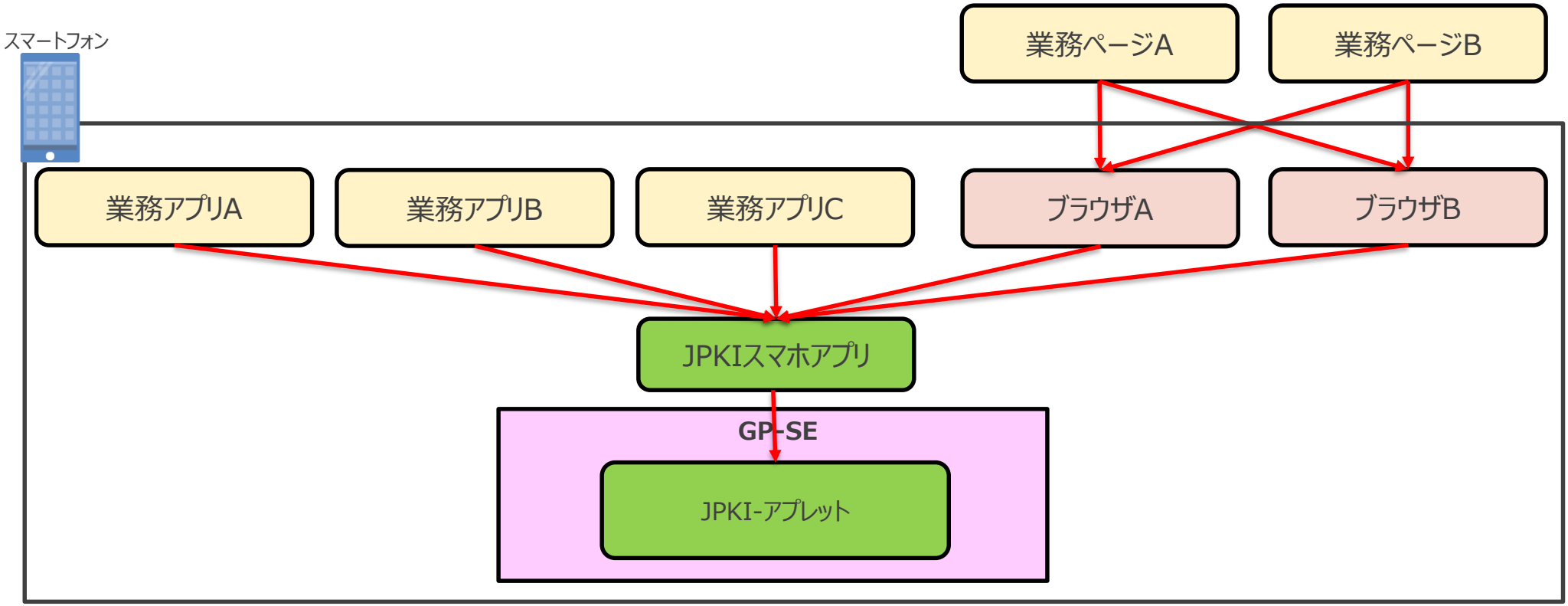


構成2． 業務アプリからスマホJPKIアプリ経由でアクセス

５．本検討における論点

連携方式の検討にあたり、考慮すべき事項が複数存在している。
特に、 安全性対策を重ねるのに反比例して、運用者や事業者の負荷が増大することが普及上の妨げとなることを懸念しており、重層的なセキュリティ対策がどこまで必要なのかという点についてご意見頂きたい。

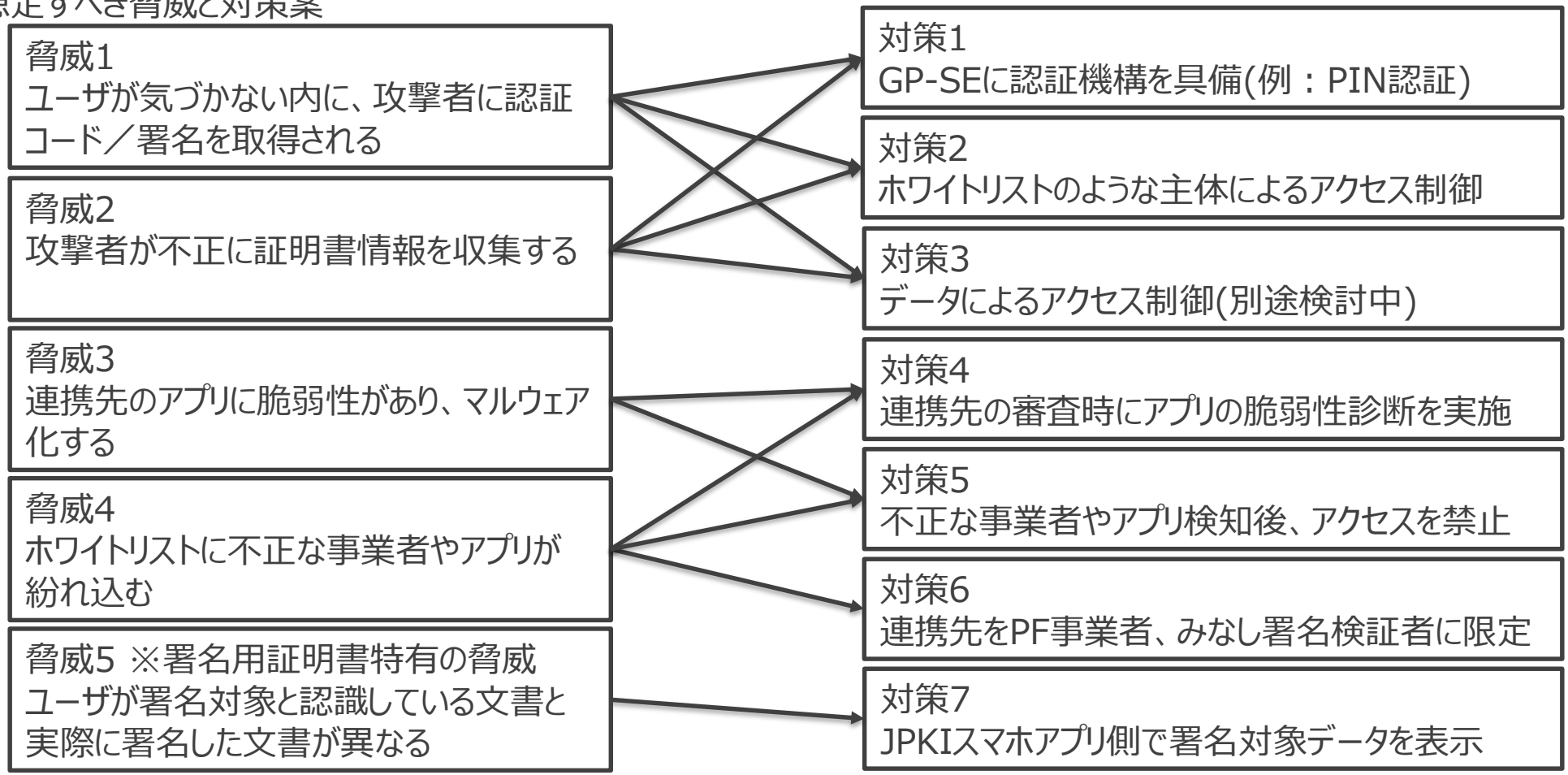
■主な論点
〇複数のアプリやブラウザからインターネット越しにアクセスされるため、アクセスコントロールが必要ではないか。
〇エンドユーザ、業務アプリ提供者、本システムの運用者の運用時の負荷が普及時の妨げにならないか。
〇署名用証明書は、実印相当であり、エンドユーザに安全に使ってもらうにはどうすれば良いか。



６．スマホJPKI利用時に想定されるリスク

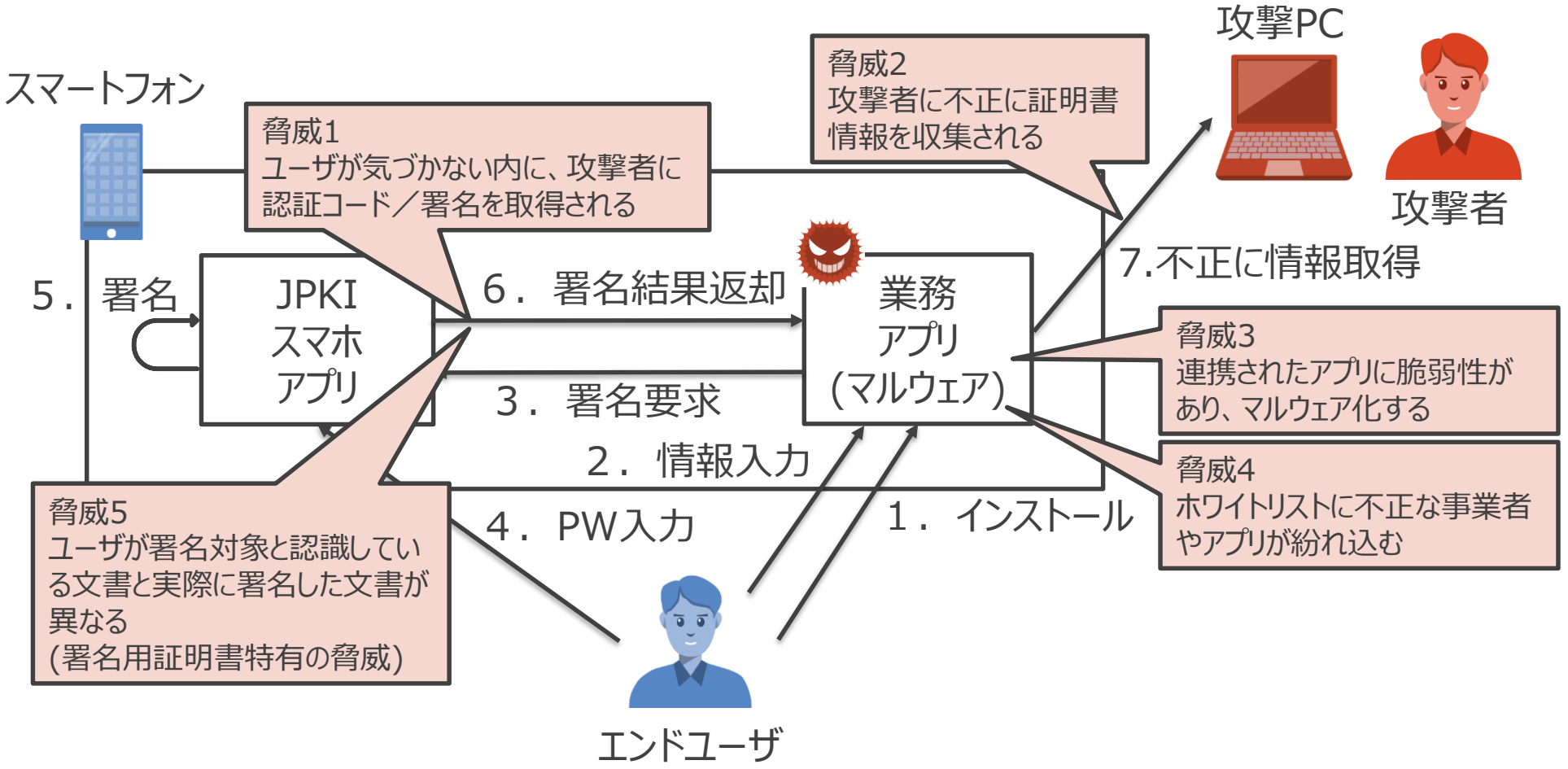
スマホJPKIは、不正利用防止のための認証機構を備えているため、想定される脅威に一定の対処は行われている。
カードと異なり、スマホJPKIが常時インターネットに接続している状態であることを考慮した時に、スマホJPKIとして想定される脅威に対して、認証機構に加える形で重層的な対応を行う必要があるか。
また、対応する必要がある場合、JPKIスマホアプリにアクセス可能なアプリケーションリスト(ホワイトリスト)のような主体によるアクセス制御以外の方法が必要か。※セキュリティ専門家より提案のあったデータによるアクセス制御も検討中。

■想定すべき脅威と対策案



参考：想定すべき脅威の発生個所

構成2を選択した場合に、想定すべき脅威が利用フローのどの部分で発生するかを整理した。
いずれの脅威もJPKIスマホアプリの外側で発生するものである。



７．署名用証明書の重要性を踏まえた対策案

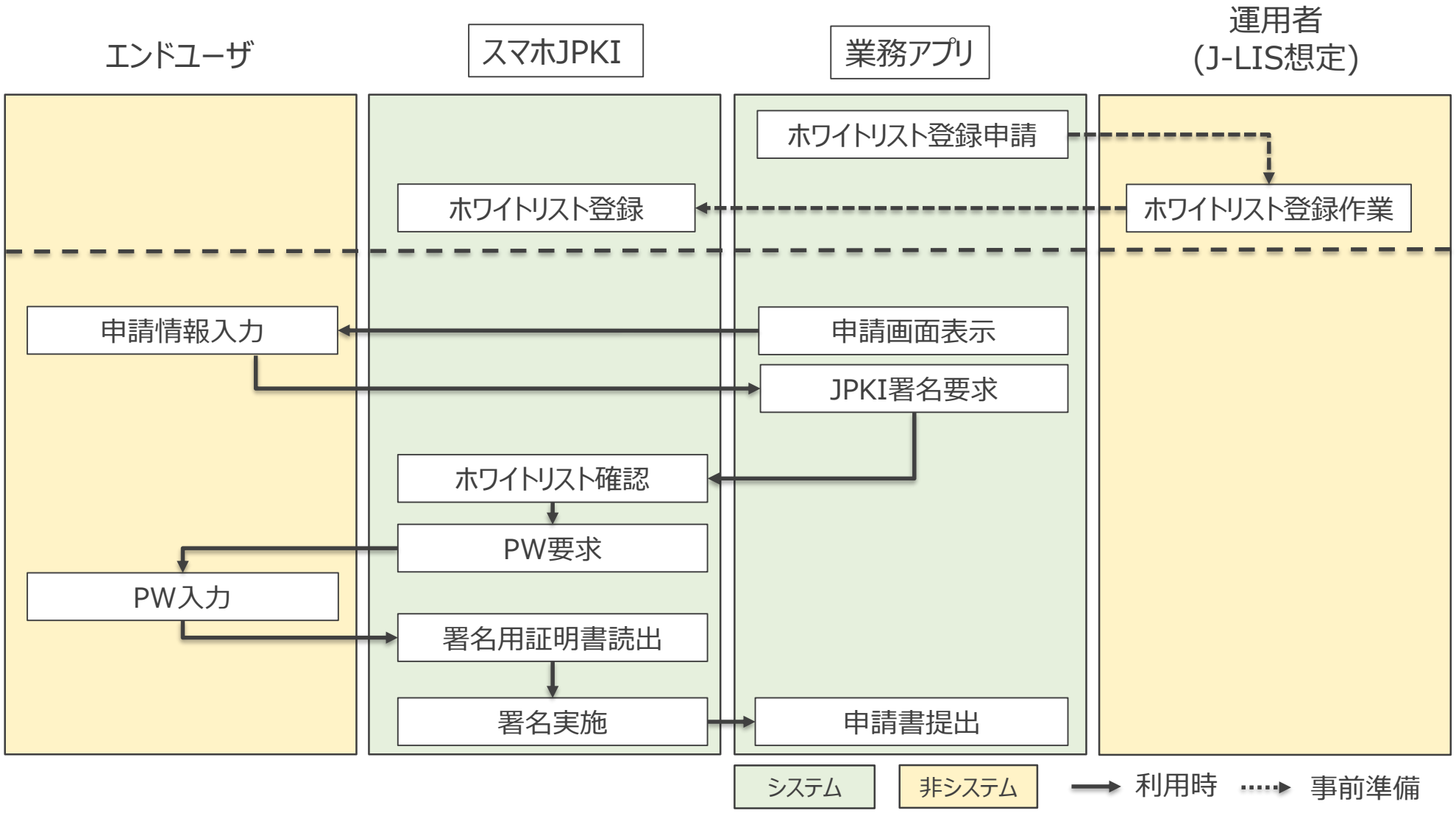
署名用証明書が実印相当であることを踏まえると、アクセス制御の強化やエンドユーザが気づかずに署名するという脅威に対して重層的に追加対策を講じることも考えられる。
この対策についてセキュリティ専門家より提案を受けて検討を行っている。

■データ署名（詳細は14ページ）
・主体によるアクセス制御ではなく、対象データによるアクセス制御を行う。
・署名対象データ／チャレンジに対して、サービス提供者またはPF事業者が署名を行い、JPKIスマホアプリ側で当該署名検証を行うことで、データの完全性を担保する。
・本方式においてサービス提供者には下記の選択肢があるが、最初に検討すべきは(1)、続いて(2)、最後に(3)となる。
  (1) サービス提供者がHSMを準備する
  (2) サービス提供者がソフトウェア署名を実施する
  (3) PF事業者に署名を依頼する

■テンプレート署名（詳細は15ページ）
・エンドユーザが文書の重要性を認識しやすいように、スマホJPKI側で注意を促す。
・改ざん検知用の署名を付与したテンプレート(例：申請書など)を用意し、テンプレートの内容に応じてエンドユーザが署名する際の注意喚起画面の表示を変えることで、確実に確認した上での署名を促す。

参考：署名用証明書を使用する際の処理フロー(ホワイトリスト方式)

署名用証明書を用いて申請を行う場合のフローを以下に示す。



参考：具体的な連携方式の検討

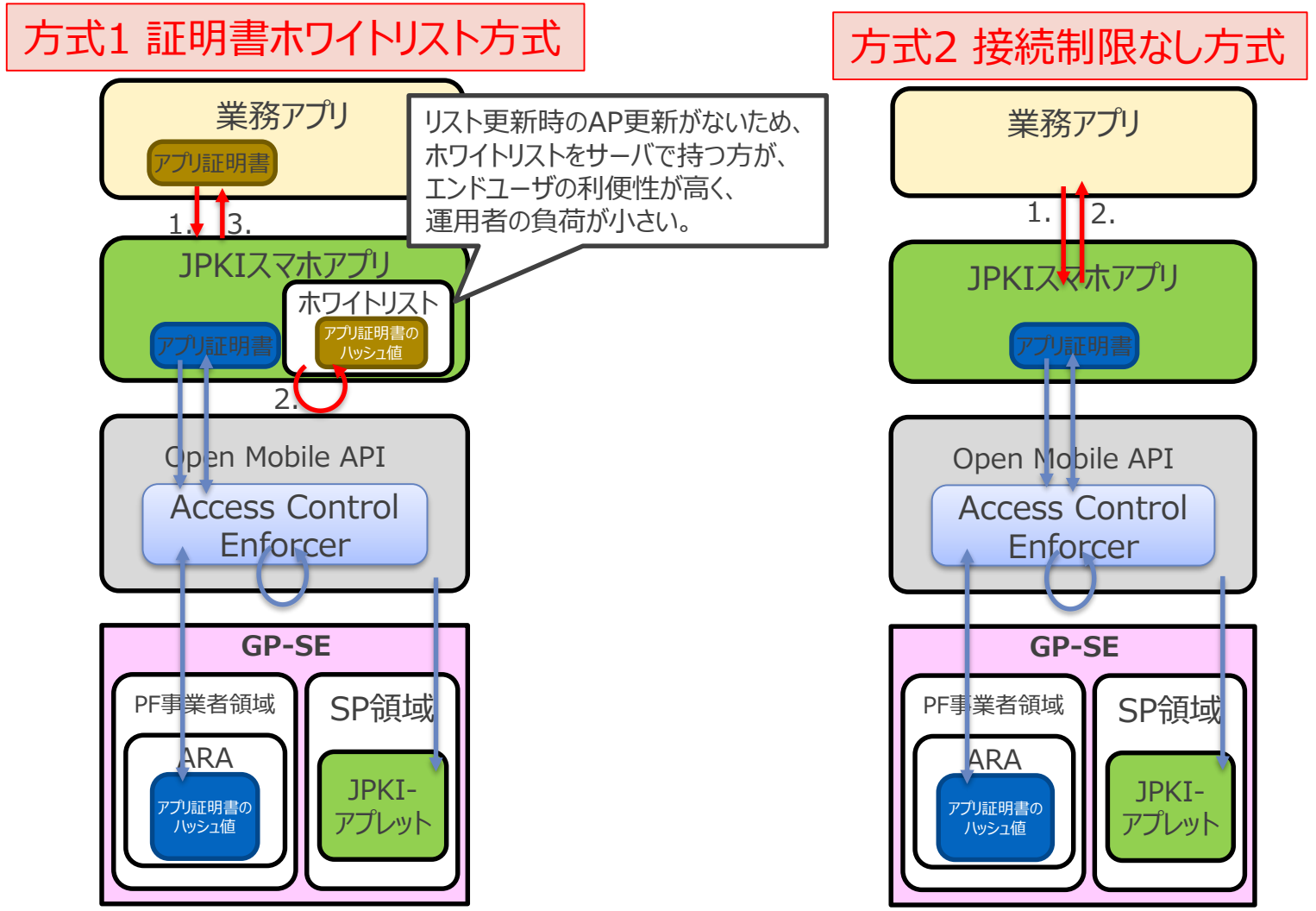
スマホJPKIと各業務アプリの連携方式として5つの方式を検討している。
前述の脅威への対処方針に対するご意見を踏まえて、方式の組み合わせ方を検討していきたい。

ID	方式名	方式の目的	概要	各方式の適用対象		各脅威への効果	
				証明書	連携先	共通(脅威1～3)	署名用特有(脅威5)
方式1	証明書ホワイトリスト方式(Androidアプリ)	ホワイトリストを用いた接続先の限定によるセキュリティ向上	AndroidアプリがJPKIスマホアプリにアクセスする際に、ホワイトリストによるアクセス制限を行う方式	利用者用／署名用	アプリ	○	△
方式2	接続制限なし方式	接続先を限定しないことによる利便性向上	Androidアプリ/ブラウザがスマホアプリにアクセスする際に、制限を行わない方式	利用者用／署名用	アプリ／ブラウザ	△	△
方式3	URLホワイトリスト方式(ブラウザ)	ホワイトリストを用いた接続先の限定によるセキュリティ向上	ブラウザ上のサービスからJPKIスマホアプリにアクセスする際に、要求元のURLをホワイトリストで検証し、検証済みのURLに直接処理結果を返却する方式	利用者用／署名用	ブラウザ	○	△
方式4	データ署名方式	信頼度の高い事業者を経由することによるセキュリティ向上	署名対象データ／チャレンジに対して、サービス提供者またはPF事業者が署名を行い、JPKIスマホアプリ側で当該署名検証を行うことで、データの完全性を担保する方式	利用者用／署名用	アプリ／ブラウザ	○	△
方式5	テンプレート署名方式	署名の重要性を踏まえた注意喚起によるセキュリティ向上	改ざん検知用の署名を付与したテンプレート(例：申請書)を用意し、テンプレートの内容に応じて、エンドユーザが署名する際の注意喚起度を変えて確認を促す方式	署名用	アプリ／ブラウザ	△	○

○：適用可能なレベル、△：部分的に問題がある、×：致命的な問題がある。

参考：スマホJPKIと各業務アプリの連携方式(方式１、方式２)

Androidアプリから、スマホJPKIの証明書を使用する際のアクセス方法を整理した。最新状況についてはJSSEC:『Androidアプリのセキュア設計・セキュアコーディングガイド』を参考とした。連携時の構成についての検討結果を踏まえ、民間サービスでは、JPKIスマホアプリ経由でアクセスを行う「ホワイトリスト方式」、「接続制限なし方式」を候補とした。



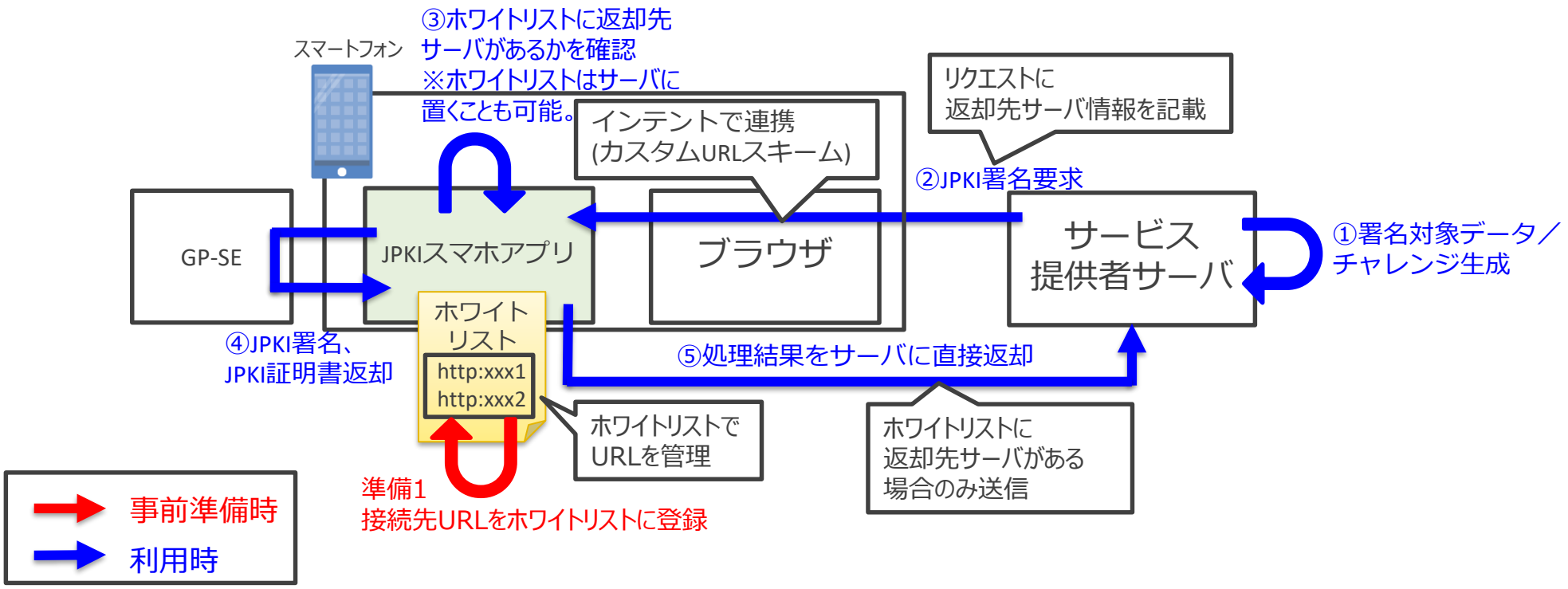
参考：スマホJPKIと各業務アプリの連携方式(方式３)

URLホワイトリスト方式は、ホワイトリストを用いたブラウザ連携方式である。
ホワイトリストに、JPKIスマホアプリへのアクセス元と、処理結果の返却先URLを登録することで不正アクセスを防止する。

■全体の流れ

Step0(準備1)：事前にホワイトリストに接続可能なURLを登録
Step1(①)：署名対象データ／チャレンジ生成
Step2(②～④)： JPKIスマホアプリにて、ホワイトリスト検証実施後に、JPKI署名/認証コードを生成
Step3(⑤)：処理結果を、ホワイトリストで検証した返却先サーバに直接返却

方式3 URLホワイトリスト方式

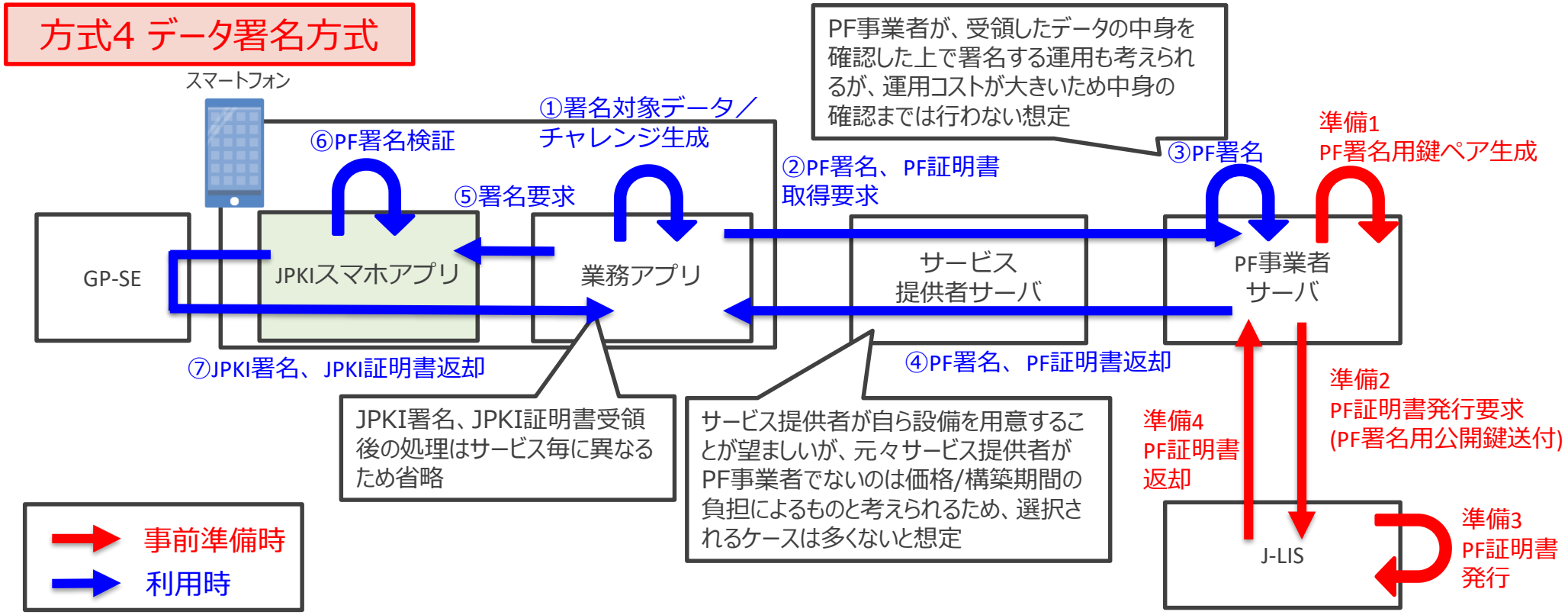


参考：スマホJPKIと各業務アプリの連携方式(方式４)

本方式は、ホワイトリスト方式における脅威への対処を目的として考案された方式であり、対象データをJPKIスマホアプリに送信する前に、サービス提供者またはPF事業者にて署名を行うことで、データの完全性を担保する方式である。
サービス提供者が署名を実施する機能(HSMまたはソフトウェア署名)を用意することが望ましいが、事業者の負担を考慮した時に、より選択される可能性が高いと見込まれるPF事業者の設備で署名を実施する方式を下図で示す。

■全体の流れ

Step0(準備1～4)：事前にJ-LISが発行するPF証明書を準備
Step1(①)：署名対象データ／チャレンジ生成
Step2(②～④)：署名対象データ／チャレンジにPF署名を実施
Step3(⑤～⑦)：JPKIスマホアプリにて、PF署名検証実施後に、JPKI署名/認証コードを生成・返却



参考：スマホJPKIと各業務アプリの連携方式(方式５)

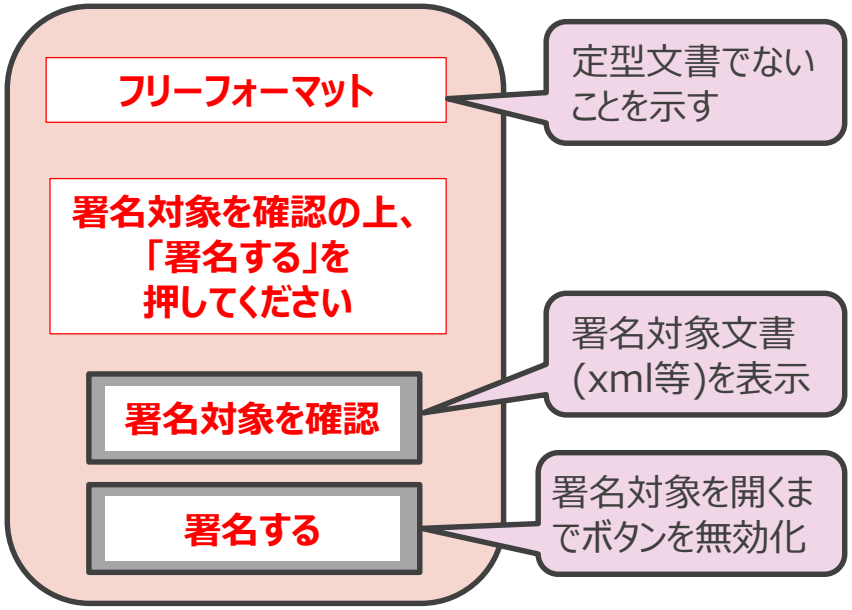
テンプレート署名は、「脅威4：ユーザが署名対象と認識している文書と実際に署名した文書が異なる」に対応するための方式である。この方式では、改ざん防止署名を施したテンプレートを用意しておき、テンプレートの記入欄にエンドユーザが入力したデータを加えて署名対象データを作成させることで、署名時にテンプレートに応じた注意喚起を行う。

方式5 テンプレート署名

テンプレートの登録、審査等の運用イメージは今後整理が必要(残課題)

・J-LISまたは総務省が、JPKI署名用に、JLIS署名付きのテンプレート文書(xml)を用意
・JPKIスマホアプリは、記入済みのテンプレートを受け取り、テンプレートに応じた確認画面を表示する。
・これにより、利用者がきちんと内容を確認した上で署名できるようサポートする。

注意喚起度の高い場合
(フリーフォーマットなど)



注意喚起度の低い場合
(定型文書による行政への申請など)