参考資料2

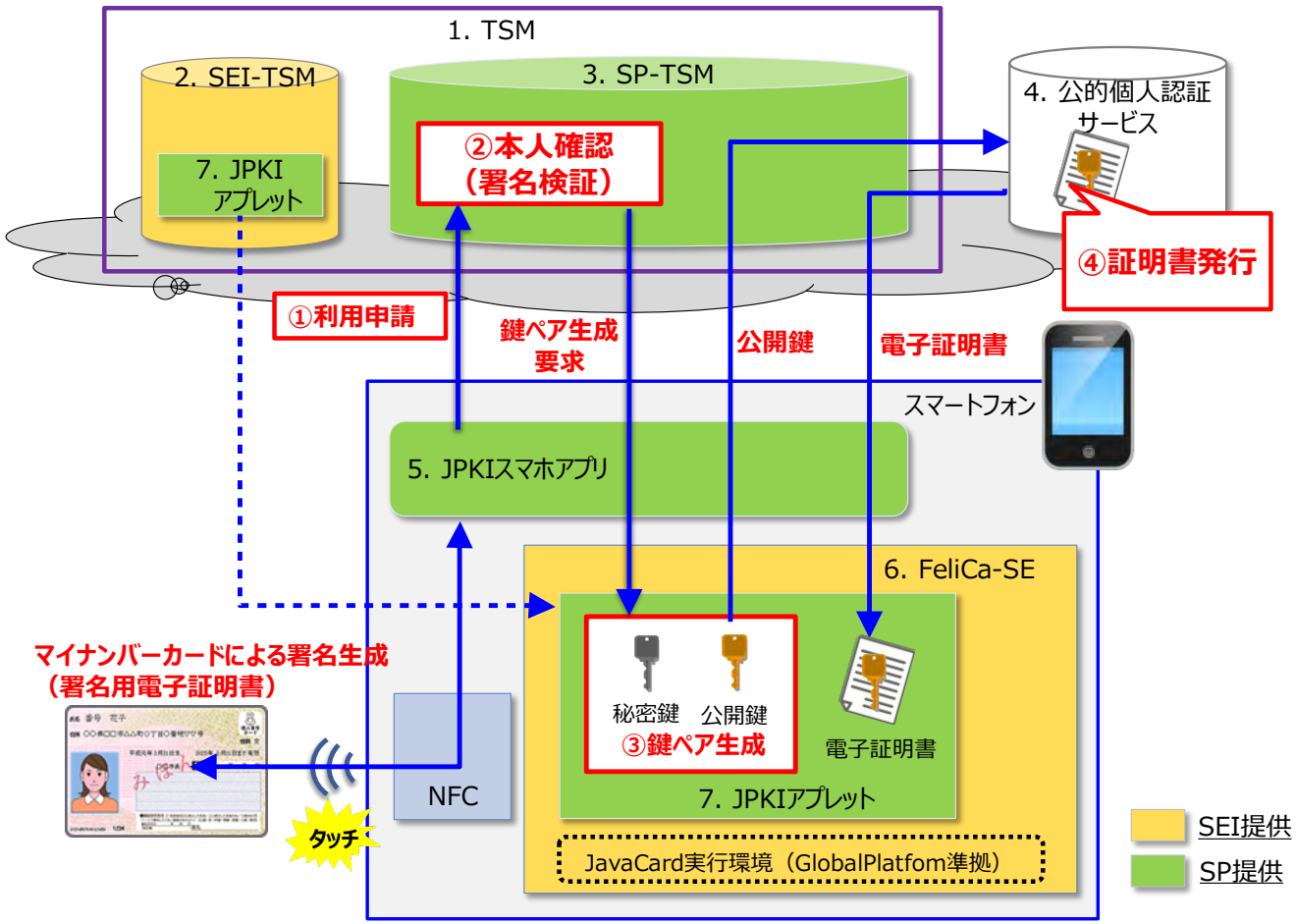
（第1回資料4）

電子証明書のスマートフォン搭載に関するシステム構成と初期発行フロー

2020年11月10日

1．システム構成と用語解説

FeliCa-SEに電子証明書を格納するためのシステム構成およびその用語解説を示す。今回の検討ではFeliCa-SE内で鍵ペア生成を行うものとする。



（補足）上図ではJPKIスマホアプリは利用者によってGooglePlayからダウンロードされた状態を想定。

サーバ側

1. TSM（Trusted Service Manager）
  ・SEI-TSMとSP-TSMで構成される。スマートフォン上のSEへのデータ配信をセキュアに実施する。

2. SEI-TSM
  ・SEの発行者が運営するTSM。
  ・SPのアプレットを預かり、SEにアプレットを格納する役割を担う。

3. SP-TSM
  ・SP（サービス提供者）が運営するTSM。
  ・ユーザの利用申請を受付け、SEのパーソナライズを行う役割を担う。

4. 公的個人認証サービス
  ・J-LISが運営する認証サービス。

スマートフォン側

5. JPKIスマホアプリ
  ・利用申請やサービス利用時に使用するAndroidアプリ。
  ・GooglePlayからダウンロードする。利用申請時やサービス利用時に使用する。

6. FeliCa-SE
  ・Androidスマートフォンに搭載されるSE。
  ・GlobalPlatform仕様に準拠し、Javaアプレットをダウンロードできる。FeliCa機能が標準搭載されていることからFeliCa-SEと呼ぶ。

7. JPKIアプレット
  ・JPKI機能を実装するJavaアプレット。

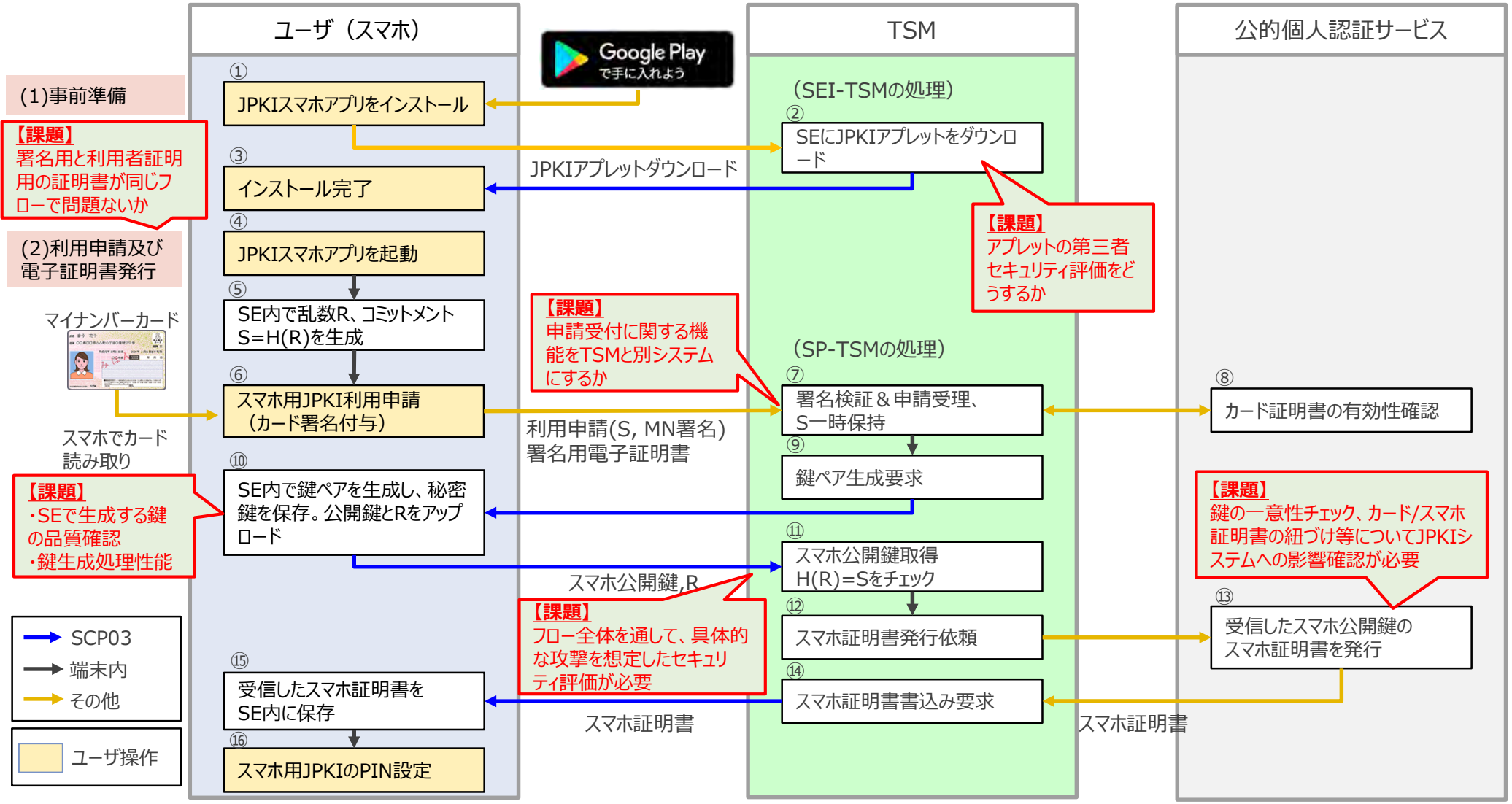
2．今回の検討における前提条件

現時点で想定している電子証明書のスマホ搭載に関する前提条件を以下に示す。

No	分類	No.	前提事項
1	電子証明書	1-1	カードの発行を前提とする（スマホのみの発行を認めない）
		1-2	2種類の証明書格納は未検討のため、1種類の証明書を格納するフローとする ※利用者用・署名用共に、技術的には同一の証明書格納フローが適用可能 ※署名用には特有の課題が存在するため、整理した上でフローへの反映が必要
		1-3	スマホ証明書を同時に格納できる端末は1台のみとする
		1-4	カード／スマホ証明書の有効期限は同一とする
		1-5	JPKIシステムでカード／スマホ証明書の紐づけ管理が行われる
		1-6	カード証明書の失効と連動させてスマホ証明書を失効させる
2	TSMの権限	2-1	SEI-TSMはSE管理者等が運営主体であり、SE内に領域生成する権限を持つ
		2-2	SP-TSMの運営主体であるJ-LISがスマホ内で生成した鍵を登録する権限を持つ
3	セキュリティ	3-1	FeliCa-SEは耐タンパーデバイスである
		3-2	各TSM/FeliCa-SE間はSCP03(GP準拠)を適用する
		3-3	スマホJPKI用のPINはユーザがオフラインで設定する (ユーザ設定前の仮PIN、アプレットライフサイクル等については未検討)

3. 初期発行フロー

・利用者が自身のスマートフォンに公的個人認証サービスを搭載し、利用可能になるまでのフローを以下に示す。
・図中の吹き出しでは、今後の検討課題を示す。



補足資料

「スマートフォンにおける公的個人認証サービスの利活用環境実現に向けた調査研究昨年度の調査研究」（以降、2019年度実証）におけるFeliCa-SE調査結果）

【補足資料1】2019年度実証での検討結果

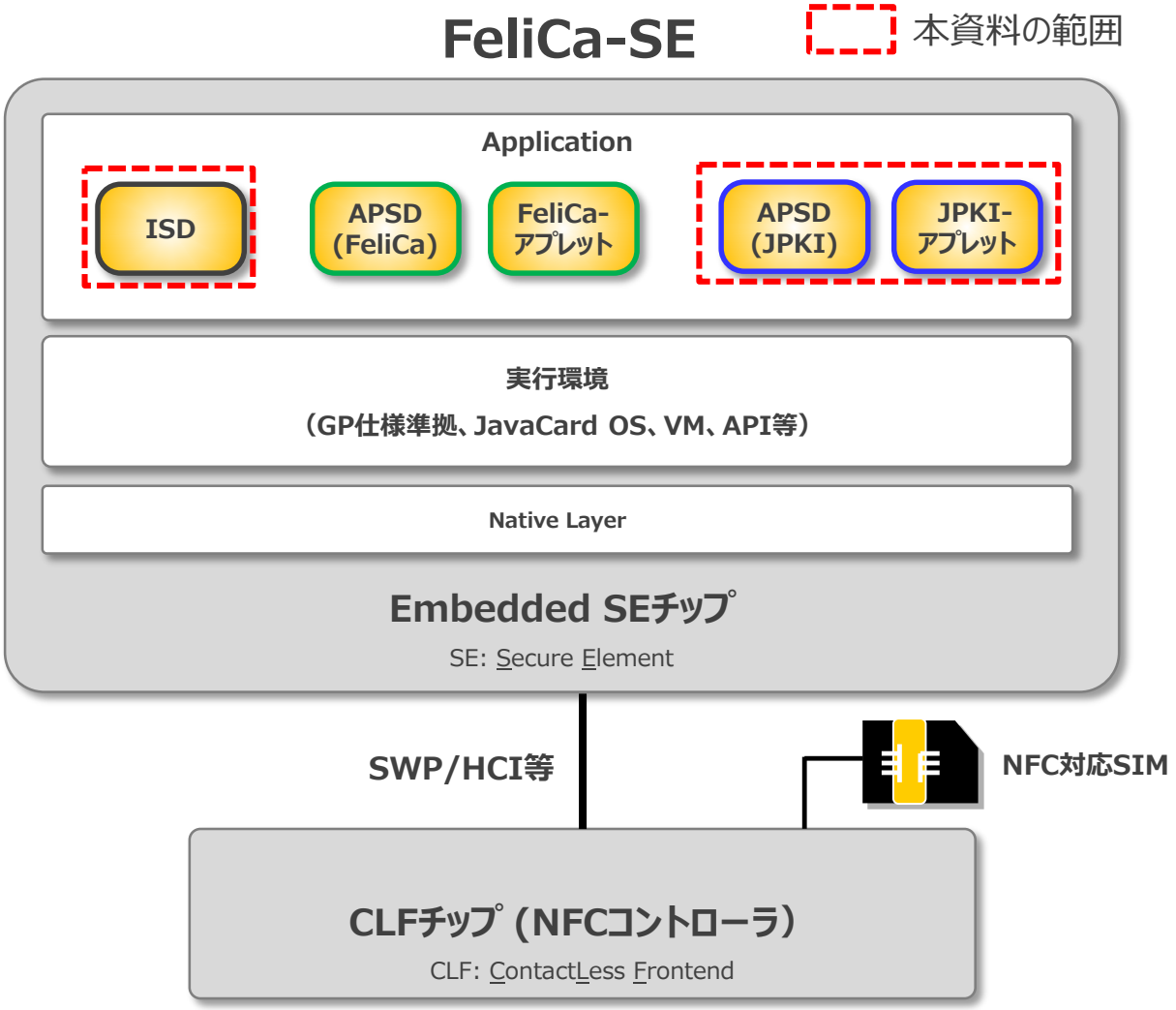
FeliCa-SEを電子証明書の格納媒体とした場合の活用可能性の調査結果及び今後の課題を以下に示す。

○：重要な課題なし　　△：重要な課題あり

#	調査項目	調査内容	調査結果	今後の課題
1	FeliCa-SEの仕様確認	チップ概要とソフトウェア構成 【補足資料2】	・FeliCa-SEチップは、Global Platform仕様対応のJava Card OSを搭載しており、SIM同様JPKI-アプレットが搭載可能な構造である。	
		セキュリティ機能 【補足資料3】	・FeliCa-SEはSCP03（AES）に対応。 電子政府推奨暗号リストに準拠しているため、コンテンツ暗号化は不要である。 ・公開鍵暗号はRSA2048bitに対応している。	
		セキュリティ評価 【補足資料4】	・ICチップ、プラットフォームはFeliCaのセキュリティ評価においてCC認証、またはEMVCoを取得済み。 ・FeliCa-SEとしてICチップ、PFについては第三者評価スキームが定まっており、安全性は高い。	・アプレットを含めた評価方法の検討。 ・セキュリティ評価の有効期間を超えた場合の取り扱いの検討。
2	アプリからFeliCa-SEへのアクセス方式確認	スマホアプリからのアクセス方式 【補足資料5】	・GPで定められた認証により、正当に登録されたJPKI-アプレットのみアプリからアクセス可能であるため、偽造されたアプレットを利用することはできない。	
		業務アプリからのアクセス方式 【補足資料6】	・FeliCa-SEへのアクセスは、JPKI-UIアプリから利用する方式で実現可能である。 ・JPKI-UIアプリ経由でアクセスし、インテントにより業務アプリから実行できる機能は、JPKI-アプレットの「利用」に限られるため、業務アプリのアクセス制御は不要。	
		外部端末からのアクセス方式 【補足資料7】	・NFCを用いたカードエミュレーションモードが利用可能であり、ルーティングによってFeliCa-SEにアクセスできる。	・商用端末での評価要件の提示が今後必要となる。

【補足資料2】チップ概要とソフトウェア構成

チップ概要とソフトウェア構成図を以下に示す。



・ISD(Issuer Security Domain)
　発行者用のSD。主に発行者関連のコンテンツ管理を行う。新たにAPSDを作成したい場合、ISDから承認を受け作成しなければならない。

・APSD（Application Provider Security Domain）
　SEに独自のアプリケーション（左図のFeliCa-アプレットやJPKI-アプレット）をインストールするときに必要なSD。

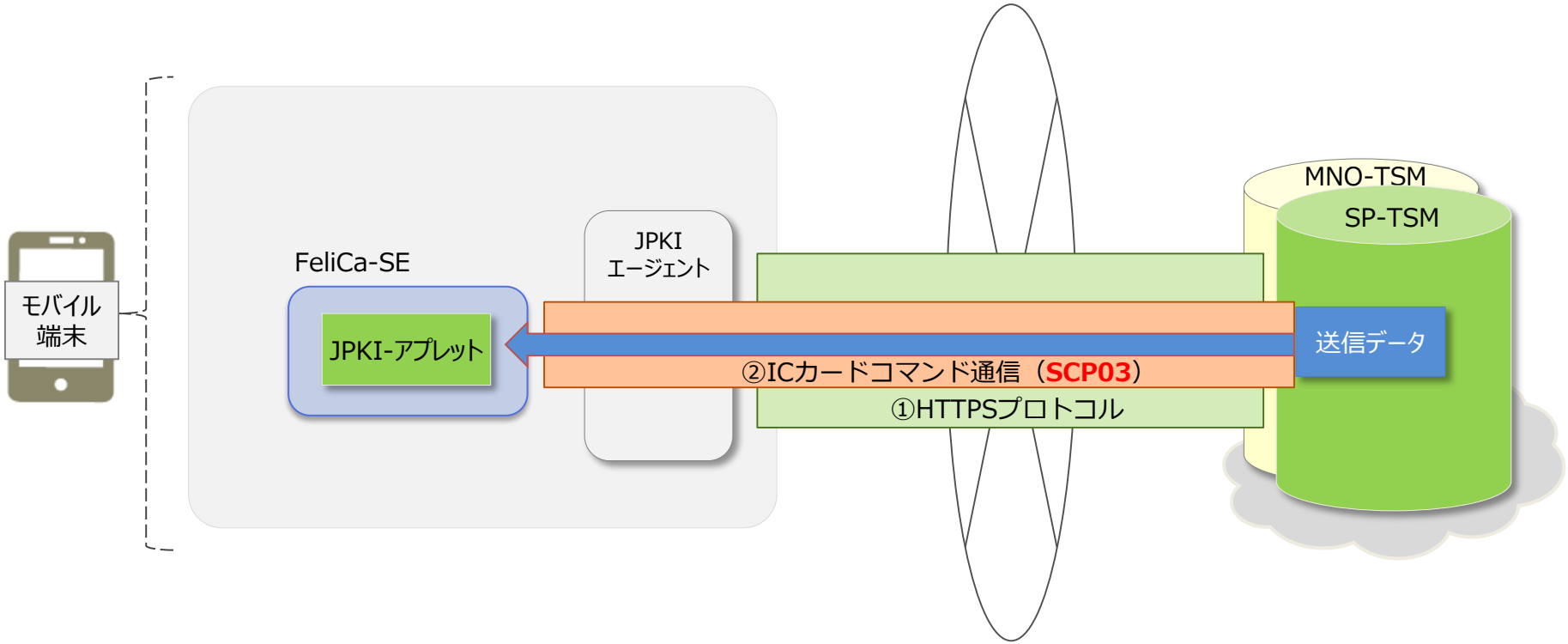
・JPKI-アプレット
　Javaアプリケーション。スマホ用電子証明書・秘密鍵を格納する。

・FeliCa-アプレット
ファイルシステム、コマンド処理、暗号処理等を行う

【補足資料3】セキュリティ機能（セキュアチャネル）

FeliCa-SEとTSM間は、SCP03と呼ばれるセキュアチャネルプロトコルによってデータ通信が実施される。
SCP03は、国際的な標準化団体であるGP（GlobalPlatform）によって定めれた暗号通信プロトコルであり、
FeliCa-SEとTSMの2者間のデータ通信の安全性が確保される。

例えば、SP-TSMからFeliCa-SEへのデータ書込みについては、SP-TSMとスマートフォン間のTLSによる暗号化に
加えて、SCP03による二重の暗号化が実施されることになる。



【補足資料3】セキュリティ機能（セキュアチャネル）

GP（GlobalPlatform）では、TSMとSE間のデータ通信の安全性確保のため、共通鍵暗号ベースのセキュアチャネルプロトコルとして、SCP02とSCP03が定められている。SCP03は電子政府推奨暗号であるAESが採用されている。

項目	SCP02	SCP03
暗号アルゴリズム	T-DES（2Key）	AES
Session keyの生成	GP2.2（SCP02)の仕様に基づき、SP-TSMが保持するマスター鍵を用いてSEごとに異なるT-DES(2Key）のSession Keyを生成	GP2.2（SCP03)の仕様に基づき、SP-TSMが保持するマスター鍵を用いてSEごとに異なるAESのSession Keyを「NIST-SP800-108」のルールに従い生成
MACの生成	MAC session keyとICVを用いて、GPで定められたルールに従いC-MACを生成	MAC session keyを用いて「NIST-SP800-38B」のルールに従いC-MACを生成
暗号化の対象	送信データフィールドに対しENC session keyとICVを用いて、GPで定められたルール（TDES）に従いデータフィールドの暗号化／復号化を行う	送信データフィールドに対しENC session keyとICVを用いて、GPで定められたルール（AES-CBC）に従いデータフィールドの暗号化／復号化を行う
安全性	SCP02 i=55 （送信データフィールドの暗号化およびMAC検証）	SCP03 i=70 （送信データフィールドおよびレスポンスの暗号化およびMAC検証）

【補足資料3】セキュリティ機能（暗号アルゴリズム）

FeliCa-SEでは、公的個人認証サービスで要求される以下の暗号アルゴリズムに対応しており、キャリアSIMと同様に使用できるものと考える。

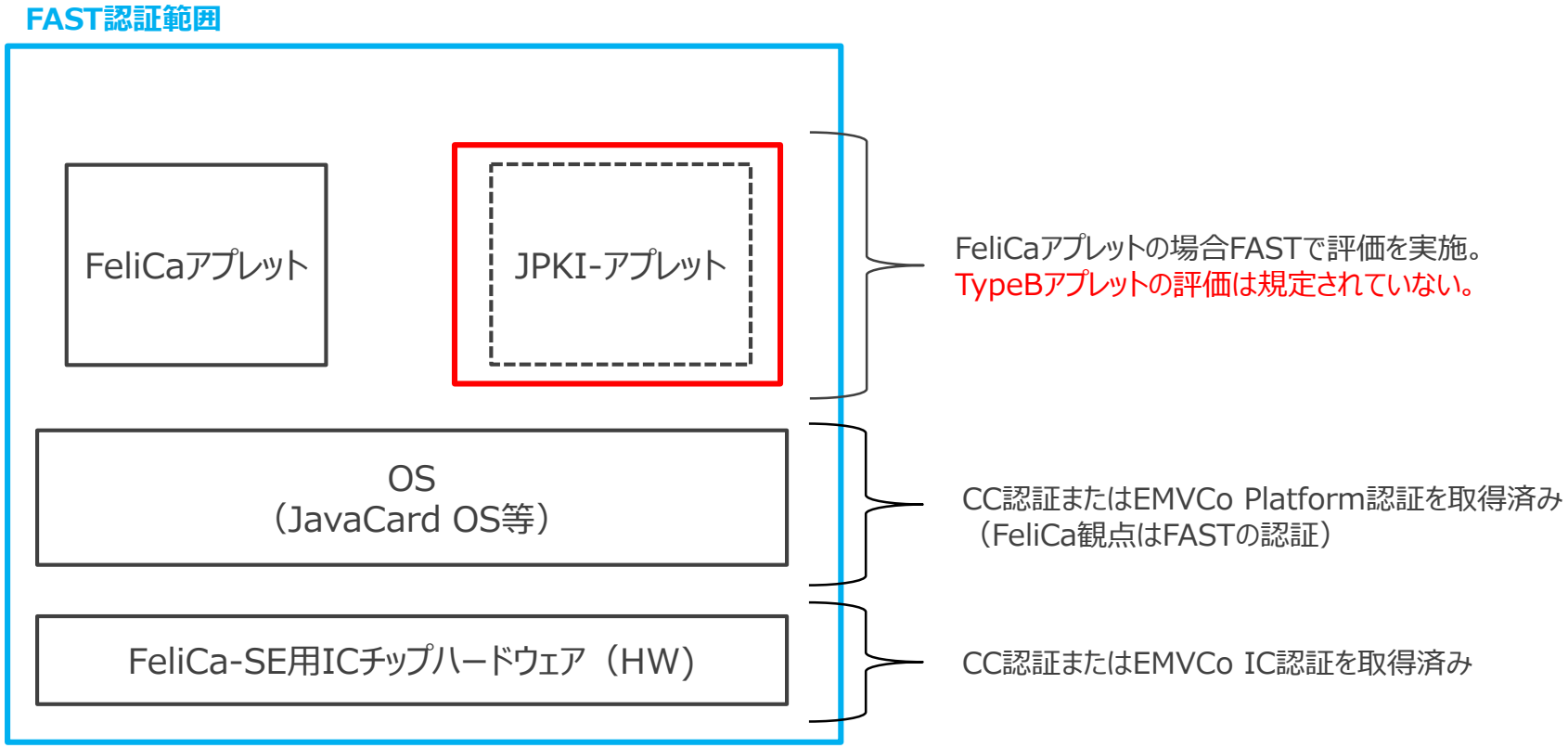
No.	暗号アルゴリズム	利用システム		サポート状況	評価結果	備考
		JPKI-アプレット	FeliCa-SE Platform			
1	RSA2048bit	○	○	○	どちらもマイナンバーカードと同等の安全性を確保している	署名はRSASSA-PKCS#1_v1.5に対応
2	AES128bit	○	○	○	どちらも電子政府推奨暗号リストの推奨暗号に対応している	SCP03の暗号化プロトコル
3	乱数生成	-	○	○	プラットフォームはSCPの内部で必要な処理に対応している	SCPで使用

【評価結果の凡例】
○：該当の暗号アルゴリズムに対応している。
△：該当の暗号アルゴリズムの対応状況は実装によって異なる、または、対応しているが不安要素や課題が残る。
×：該当の暗号アルゴリズムに対応していない。

【補足資料4】セキュリティ評価（FAST）

FeliCa Approval for Security and Trust (FAST)

・FN社が提供するセキュリティ認証プログラム
・SEチップに搭載されるOSのFeliCa機能およびFeliCaアプレットが対象
・Common CriteriaやEMVのセキュリティ評価で実績のある、セキュリティ評価ラボ会社と提携し、FeliCaに関する第三者観点でのセキュリティ評価を実施



【補足資料4】セキュリティ評価（マイナンバーカードとの比較）

・FeliCa-SEのプラットフォーム（HW＋OS）は、FASTというフェリカネットワークス（FN）社で定めたセキュリティルールに基づいて、CC認証、もしくは、EMV認定の取得に加えて、FeliCa機能に関するセキュリティ要件を満たすことが条件となっている。マイナンバーカードにおけるCC認証とは、以下のような相違がある。

項目	マイナンバーカードのセキュリティ評価（CC認証）	FeliCa-SEプラットフォームのセキュリティ評価		
		FAST認定（FeliCa機能観点）		
		CC認証（HW＋OS）	EMV認定（HW+OS）	
セキュリティ要件	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	EMVCoが定めるSecurity Guideline（非公開）EAL4+（AVA_VAN.5）	FNが定めるSecurity Guideline（非公開）EAL4+（AVA_VAN.5）
評価の範囲	製品の評価及びその開発プロセスを含んだ評価	製品の評価及びその開発プロセスを含んだ評価		
脆弱性評価	JIWG文書（※1）で示される攻撃への対抗	JIWG文書（※1）で示される攻撃への対抗		
有効期間	認証取得国による	認証取得国による	1年（再評価後1年、最長6年）	3年（再評価後1.5年）
評価機関	認証機関が認定した評価機関	認証機関が認定した評価機関	EMVCoが認定した評価機関	FNが認定した評価機関
認証機関	認証制度に基づく認証機関（公的機関）	認証制度に基づく認証機関（公的機関）	EMVCo	FNが認定した認証機関

・マイナンバーカードのCC認証及びFeliCa-SEのFAST認定では、脆弱性分析においてはいずれも同一のJIWG文書を参照し、攻撃方法への対抗策が評価されている。参照するJIWG文書は、現在想定されるICカードへの攻撃方法を網羅的に記したものであり、国際的に広く参照されている文書である。

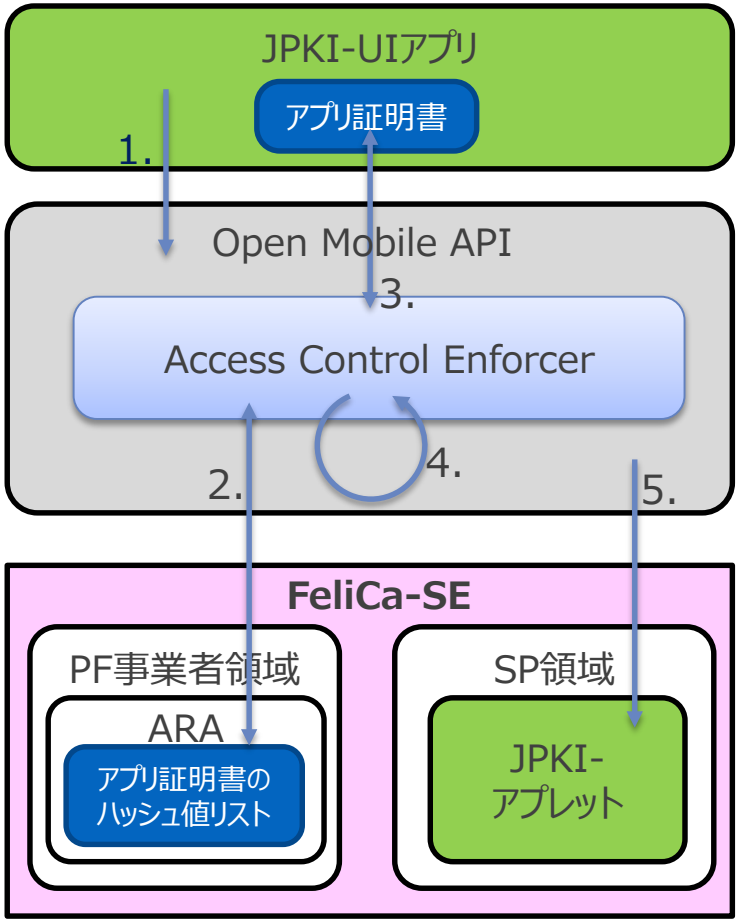
※1 JIL Application of Attack Potential to Smart Cards, version 2.9 Jan 2013

・FeliCa-SEでは、脆弱性分析においては最高レベルであるAVA_VAN.5を取得することが条件となっており、マイナンバーカードと同等の保証レベル（AVA_VAN.5）を要求していることは高く評価できるものと考えられる。

【補足資料5】スマホアプリからのアクセス方式

【内容】

・FeliCa-SE内に格納されたアプレット（JPKI-アプレット）は、下図の仕組みによりアクセス元アプリケーションの認証を行なうことで、正当なAndroidアプリケーション（JPKI-UIアプリ）のみがアクセス可能となっている。



【参考】Global Platform, Secure Element Access Control v1.0

■アプレットにアクセスできるアプリケーションリストの登録方法

1. SPは、JPKI-アプレットにアクセスできるアプリケーションのホワイトリスト（Androidアプリケーションの証明書ハッシュ値リスト）を作成し、SEI-TSMに登録しておく。
2. SEI-TSMがJPKI-アプレットをFeliCa-SEに格納する際に、上記のリストをARA（Access Rule Application）に格納する。

■認証手順（番号は左図に対応）

1. JPKI-UIアプリがOpen Mobile APIにアクセスする。
   ・Open Mobile API： GP仕様に準拠したFeliCa-SE内のセキュアな領域にアクセスするために提供されているAndroid用API
2. Open Mobile API内部のACE(Access Control Enforcer)がPF事業者領域内のARA（Access Rule Application）から、アクセスルールを取得する。
3. ACEは、アクセス元のAndroidアプリケーションに付与されている公開鍵証明書のハッシュ値を算出する。
4. ACEは、手順2と手順3で取得したハッシュ値を比較する。一致した場合は、正しいアプリケーションからのアクセスであると判断する。
5. 手順4で一致した場合は、手順1で要求されたOpen Mobile API処理が実行される。

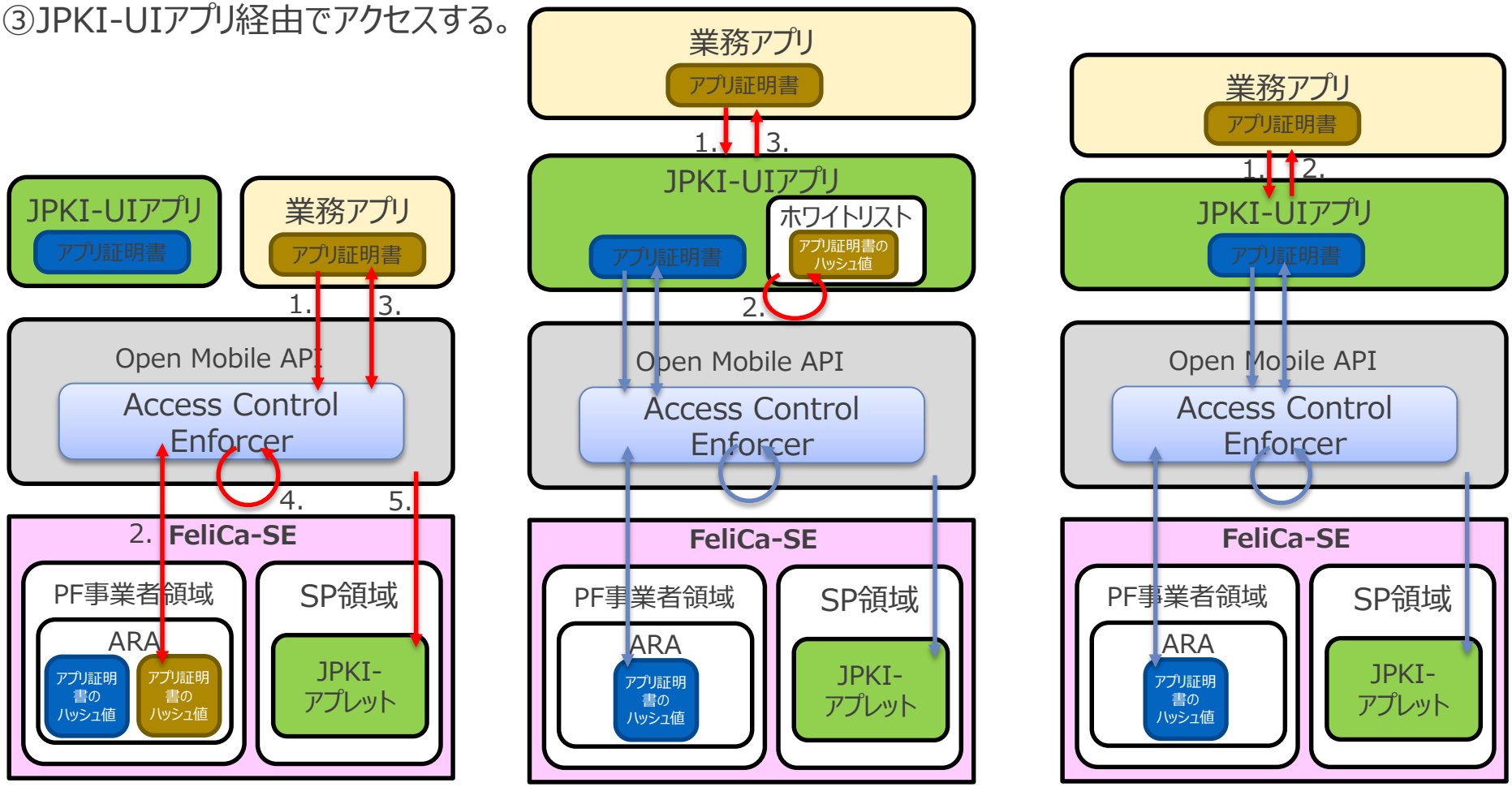
【補足資料6】業務アプリからのアクセス方式

公的個人認証機能を使用する業務アプリからアプレットへのアクセス方法は、以下のようなパターンが想定される。

①直接FeliCa-SEにアクセスする。（FeliCa-SE内でホワイトリスト管理）

②JPKI-UIアプリ経由でアクセスする。（JPKI-UIアプリがホワイトリスト管理）

③JPKI-UIアプリ経由でアクセスする。



【補足資料6】業務アプリからのアクセス方式

パターン比較結果は以下の通り。

【赤枠：推奨案】

項目	パターン①	パターン②	パターン③
概要	直接FeliCa-SEにアクセスする。 （FeliCa-SEがホワイトリスト管理）	JPKI-UIアプリ経由でアクセスする。 （JPKI-UIアプリがホワイトリスト管理）	JPKI-UIアプリ経由でアクセスする。
安全性	○：GP仕様のアクセス制御。許可外アプリからのアプレットアクセスをブロック。（FeliCa-SEのホワイトリストで制御）	○：許可外アプリからの、JPKI-UIアプリのインテント実行をブロック（JPKI-UIアプリのホワイトリストで制御）。 ○：GP仕様のアクセス準拠（JPKI-UIアプリからのアクセスのみ許可）。 △：ホワイトリストはJPKI-UIアプリが保持することになるので、FeliCa-SEと比較するとホワイトリストの格納領域として安全性が劣る	△：許可外アプリからのJPKI-UIアプリのインテント実行はブロックされない。（※） ○：GP仕様のアクセス準拠（JPKI-UIアプリからのアクセスのみ許可）。 ※インテントにより業務アプリから実行できる機能は、JPKI-アプレットの「利用」に限り、「発行」は利用できない（アプレット内のデータが書き換えられることはない）。
審査業務	△：ホワイトリスト登録のための審査業務要	△：ホワイトリスト登録のための審査業務要	○：審査業務を不要にできる
ユーザビリティ	△：業務アプリの利用開始時に、業務アプリ又はJPKI-UIアプリを起動し、ホワイトリストの最新化が必要。	△：業務アプリの利用開始時に、業務アプリ又はJPKI-UIアプリを起動し、ホワイトリストの最新化が必要。	○：業務アプリの利用開始時に、ホワイトリスト最新化の操作が不要。
SP運用負担	△：業務アプリが増える都度、ホワイトリストの最新化の処理が必要 △：SEI-TSMを通じてSIMカード内のホワイトリスト登録が必要。	△：業務アプリが増える都度、ホワイトリストの最新化の処理が必要 △：SPサーバ(SP-TSM等)を通じてUIアプリへのホワイトリスト登録が必要。	○：ホワイトリストの管理が不要。
業務アプリ開発負担	△：FeliCa-SEアクセス機能をモジュール化して提供することで開発負担を軽減できるが、一定の負担がある。	○：FeliCa-SEアクセス機能をAPI化したIF(インテント)を実行する機能の開発は容易。	○：FeliCa-SEアクセス機能をAPI化したIF(インテント)を実行する機能の開発は容易。

【補足資料7】外部端末からのアクセス方式

FeliCa-SE搭載スマートフォンでは、 NFCを用いたカードエミュレーションモードが利用可能であり、カードエミュレーションを実施した際、Manifestファイルに記載されたAIDの情報に従って、FeliCa-SEにルーティングされる。