参考資料2

[別紙]各フローにおける攻撃可能性と対策案の事前検証について

2021年4月21日

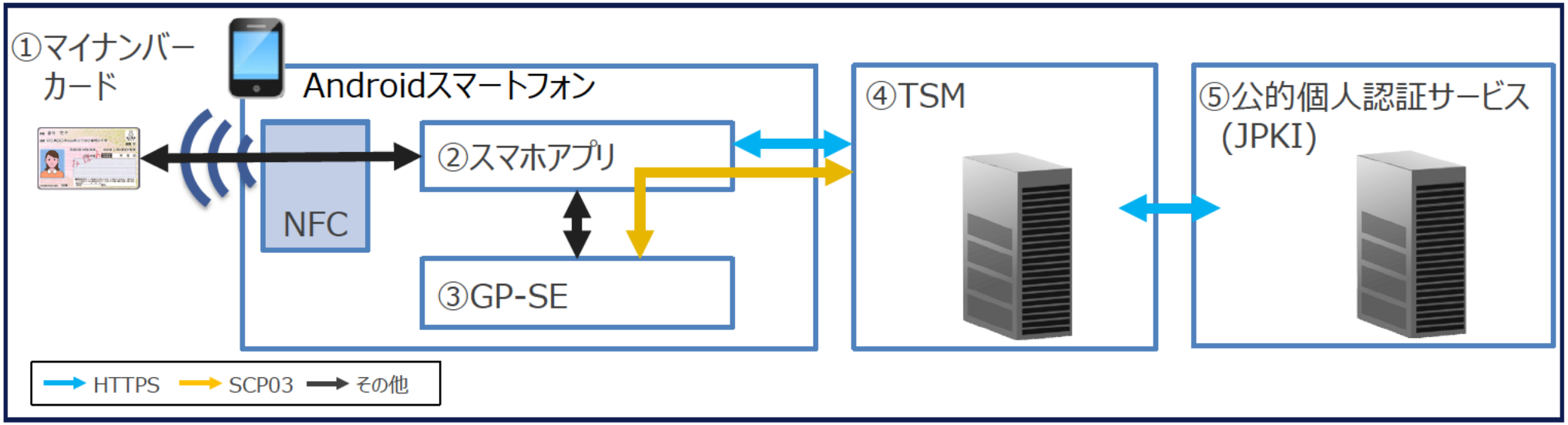
攻撃可能性と対策案についての事前検証概要

第5回検討会にて頂いたご指摘を踏まえて、
各段階における攻撃可能性とその対策案資料におけるセキュリティ機構の一覧化、および、
資料中の攻撃可能性との対応関係の整理を行った。

これらの機構の有効性含め、技術検証におけるセキュリティ面での検証の一部として
第三者機関に依頼する形で検討を進める方針とする。

(1)攻撃可能性への対策について[内部処理]

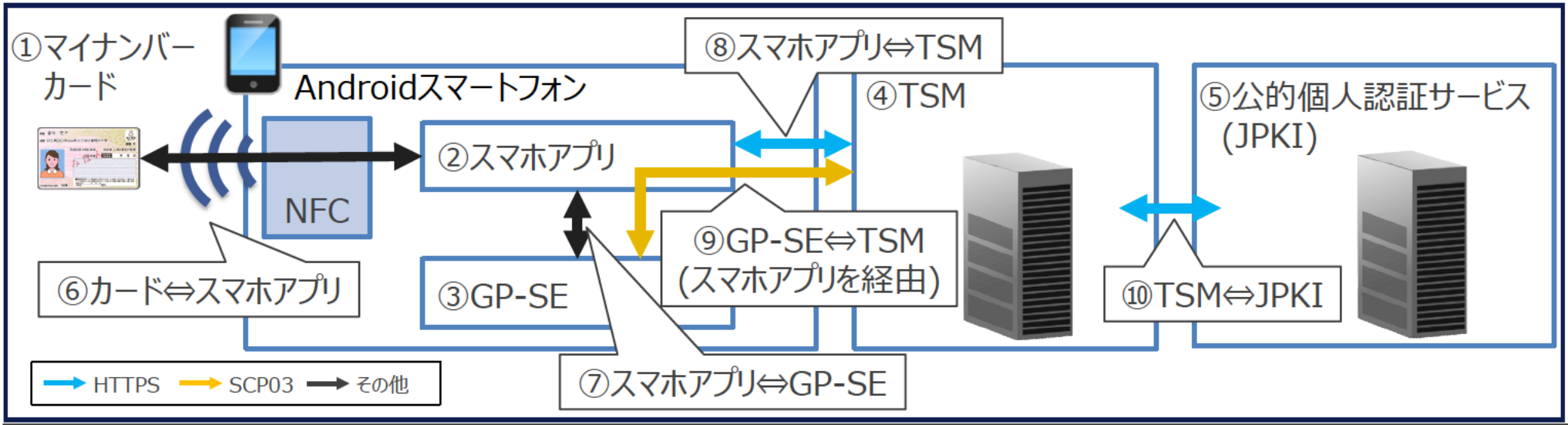
システム構成上、攻撃対象となりうる箇所および対策について、内部処理と外部通信に分類して整理した。



機構	分類	対象	機能/手段	対策	参考資料
機構①	内部処理	カード	耐タンパ性	・耐タンパ性を持つICチップを採用することにより、チップ内での処理が漏洩・改ざんされること防止する。	・参考1:GP-SEのセキュリティ評価 ・参考2:マイナンバーカードによるセキュリティ対策
機構②		スマホアプリ	Androidのセキュリティ機能	・Androidの機能で、パスワードや暗証番号等の知識認証、及び指紋認証等の生体認証により、画面にロックをかけることで、他者による不正操作を防止する。 ・Androidの機能により、アプリが動作する環境の完全性確認、および、動作中の改ざん保護が行われる。	
機構③		GP-SE	耐タンパ性	・スマートフォンに内蔵した耐タンパ性を持つICチップを採用することにより、スマホアプリから情報を取得できず、チップ内での処理が漏洩・改ざんされること防止する。	・参考1:GP-SEのセキュリティ評価
機構④		TSM	セキュアな区画での管理	・セキュリティレベルの高い区画に隔離し、物理的なアクセスが制限される環境に置くことで、処理内容の漏洩・改ざんを防止する。	
機構⑤		JPKI	セキュアな区画での管理	・セキュリティレベルの高い区画に隔離し、物理的なアクセスが制限される環境に置くことで、処理内容の漏洩・改ざんを防止する。	

(2)攻撃可能性への対策について[外部通信]

システム構成上、攻撃対象となりうる箇所および対策について、内部処理と外部通信に分類して整理した。



機構	分類	対象	機能/手段	対策	参考資料
機構⑥	外部通信	カード⇔スマホアプリ	PINロック、NFC通信	・PINを用いた認証を行うことで正当な利用者であることを担保する。 ・マイナンバーカード利用時はスマートフォンにかざす必要があるため、物理的制約により、リモートで攻撃されるリスクが低い。	・参考2:マイナンバーカードによるセキュリティ対策
機構⑦		スマホアプリ⇔GP-SE	Open Mobile API	・Open Mobile APIにより、アクセス元のスマホアプリが正当なアプリかどうかを判断してアクセス制御することで、不正なアプリからのアクセスを防止する。	・参考3:GP-SEのセキュリティ機能①
機構⑧		スマホアプリ⇔TSM	HTTPS、コミットメント	・SSL/TLSプロトコルを用いて、サーバの認証・通信内容の暗号化・改竄検出などを行う ・発行申請時にGP-SEで乱数Rを発生させ、乱数Rのハッシュ値Sをコミットメントとして TSMに送信し、SE-ID読み出し時に取り出した乱数と突合することで、マイナンバーカードの署名生成とSE識別IDが同一スマホで実施されたことを保証する。 これらによって、なりすまし・中間者攻撃・盗聴などの攻撃を防止する。	
機構⑨		GP-SE⇔TSM	SCP03	・SCP03は、GlobalPlatformによって定めれた暗号通信プロトコルであり、GP-SEとTSMの2者間での鍵共有と暗号化されたデータを送受信するため、経路途中の盗聴・改ざんを防止する。（本通信はスマホアプリを経由）	・参考4:GP-SEのセキュリティ機能②
機構⑩		TSM⇔JPKI	閉域網の構築、HTTPS	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または閉域網で繋ぐことで、外部からの侵入を物理的に防止する。 ・通信を暗号化することにより、盗聴・改ざんのリスクを低減させる。	

各段階における攻撃可能性に紐づく対策の整理(1/3)

第5回検討会資料修正

攻撃可能性に紐づく対策案について、以下に整理した。
Androidのセキュリティ機能に加えて、追加対策を施すことでシステム全体の高い安全性を担保している。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
1	なりすまし	(偽)スマホアプリとの通信	GP-SEとのなりすまし通信	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、事前確認を行うことでスマホアプリの正当性が担保されているため、不正なアプリに関してはGP-SEにアクセスできないため実害が発生しない。（機構⑦）	○
2			SP-TSMへのなりすまし通信	・SP-TSMとGP-SE間でSCP03でのセキュアチャネルを確立し、通信を行う。セキュアチャネルを確立できない(偽)スマホアプリや(偽)SP-TSMからはGP-SEにアクセスできないため、公的個人認証サービスへの不正アクセスを防ぎ、実害が発生しない。（機構⑨）	○
3		(偽)SP-TSMとの通信	スマホアプリへのなりすまし通信		
4			公的個人認証サービスへのなりすまし通信	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。（機構⑩） ・SP-TSMと公的個人認証サービスの通信は全て暗号化する。（機構⑩）	○
5		(偽)公的個人認証サービスとの通信	SP-TSMへのなりすまし通信	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。（機構⑩） ・SP-TSMと公的個人認証サービスの通信は全て暗号化する。（機構⑩）	○
6		別端末との通信	・マイナンバーカードによる署名処理を実施したスマホとは別のスマホのGP-SEに鍵ペア生成/鍵登録/SE識別ID認識等を行う	・申請時にGP-SEで乱数Rを発生させ、乱数Rのハッシュ値SをコミットメントとしてTSMに送信し、SE-ID読み出し時に取り出した乱数と突合することで、マイナンバーカードの署名生成とSE識別IDが同一スマホで実施されたことを保証する。(機構⑧) ・SE識別ID読出し時のコミットメントS確認を実施したSCP03のセッションを維持することで、他の後続段階においても署名処理を実施したスマホと同一スマホでの実施が担保できている。(機構⑧、機構⑨)	○
7		(偽)スマホアプリへのなりすまし	・正規のスマホアプリではない(偽)スマホアプリになりすましてフィッシング等を行う	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、対象処理を行う前にスマホアプリの正当性が担保されているため、不正アプリによるGP-SEアクセスは防止される。（機構⑦）	○

各段階における攻撃可能性に紐づく対策の整理(2/3)

第5回検討会資料修正

攻撃可能性に紐づく対策案について、以下に整理した。
Androidのセキュリティ機能に加えて、追加対策を施すことでシステム全体の高い安全性を担保している。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
8	窃取	マイナンバーカードの不正利用	・他人のマイナンバーカードでスマホJPKIの初期設定を行う。 ・マイナンバーカード内の秘密鍵を取り出し複製を行う。	・マイナンバーカードのICチップは耐タンパ性があるため、秘密鍵を取り出し複製することは困難。（機構①） ・マイナンバーカードはPINにより本人にしか利用できず、PINは連続して所定回数失敗するとロックする。（機構⑥）	○
9		他人によるスマホ操作	・他人の端末でPIN設定等の操作を行う	・端末自体のロック操作等により他人によるスマホ操作を防ぐことができる。（機構②）	○
10	盗聴	通信の盗聴	・スマホアプリとGP-SEとの間の通信を盗聴される	・SCP03通信については盗聴が困難なため攻撃についても困難。（機構⑨） ・上記以外の通信でやり取りされる情報は、コミットメント生成コマンドと乱数ハッシュSのみであり、これらが取得されてもコミットメント照合の安全性に影響はない。	○
11			・スマホアプリとSP-TSMとの間の通信を盗聴される	・HTTPS通信については盗聴が困難なため攻撃についても困難。（機構⑧） ・SCP03通信については盗聴が困難なため攻撃についても困難。（機構⑨）	○
12			・SP-TSMと公的個人認証サービスとの間の通信を盗聴される	・SP-TSMの構築先を既存の公的個人認証サービスと同一とする、または、閉域網で繋ぐことで、外部からの侵入を物理的に防ぐ。（機構⑩） ・SP-TSMと公的個人認証サービスの通信は全て暗号化する。（機構⑩）	○

各段階における攻撃可能性に紐づく対策の整理(3/3)

第5回検討会資料修正

攻撃可能性に紐づく対策案について、以下に整理した。
Androidのセキュリティ機能に加えて、追加対策を施すことでシステム全体の高い安全性を担保している。

パターン番号	分類	攻撃可能性	具体的な脅威	対策	評価
13	改ざん	操作の改ざん	・利用者が意図していない操作が行われる。 （利用者が承認していないのに承認の返信を行う等）	・スマホアプリからのGP-SEへのアクセス制御の仕組みにより、GP-SEとの事前確認によりとでスマホアプリの正当性が担保されている。（機構⑦） ・Androidはスマホアプリの動作の完全性が担保する機構が備わっているため、利用者の失効承認等の各種操作は正しく機能すると考えられる。（機構②）	○
14		通信の改ざん	・通信データの改ざんが行われる	・HTTPS通信/SCP03通信は改ざんが困難である。（機構⑧、機構⑨） ・SP-TSMと公的個人認証サービスの通信は全て暗号化する。（機構⑩） ・コミットメント生成コマンドと戻り値である乱数ハッシュSが改ざんされても、コミットメント照合時にエラーとなり、後続のフローは動作しない。（機構⑧）	○
15		業務処理の改ざん	・SP-TSMやGP-SE、公的個人認証サービスの中で実施している業務処理の改ざんが行われる ・SP-TSMの業務処理遷移において改ざんが行われる	・GP-SEの処理はチップ内で閉じているため改ざんは困難である。（機構③） ・SP-TSMの業務処理はサーバ内に閉じているため改ざんは困難である。（機構④） ・SP-TSMの業務処理遷移は単一サーバ内に閉じており外部通信ではないため改ざんは困難である。（機構④） ・公的個人認証サービスの業務処理はサーバ内に閉じているため改ざんは困難である。（機構⑤）	○
16		アプリ処理の改ざん	・スマホアプリ内処理の改ざんが行われる ・スマホアプリ内遷移の改ざんが行われる	・業務処理実行前および完了後の処理および遷移については、業務処理に影響しないため実害が発生しない。 ・失効処理においても業務処理が改ざんされアプレットの残存が考えられるが、実害は発生しない。	○

参考資料

参考１

GP-SEのセキュリティ評価

GP-SEでは、プラットフォーム（HW＋OS）としてCC認証又はEMV認定を取得したICチップが採用されている。マイナンバーカードとGP-SEのセキュリティ評価に関する比較表を以下に示す。

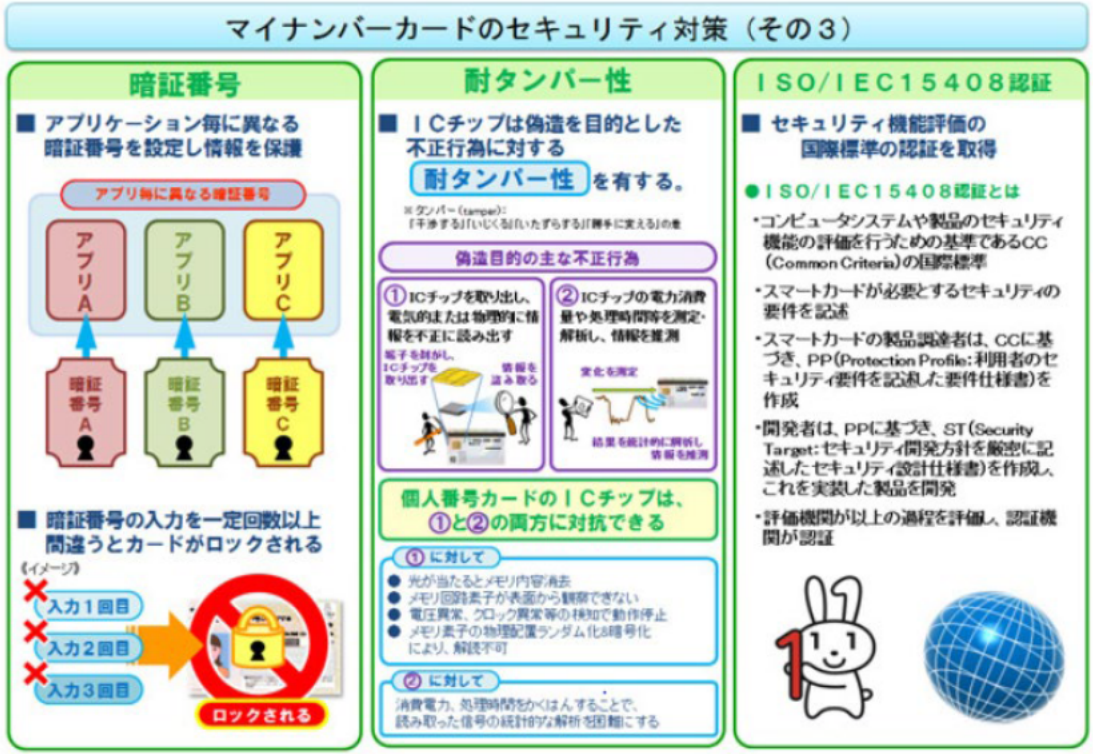
項目	マイナンバーカードのセキュリティ評価（CC認証）	GP-SEプラットフォームのセキュリティ評価	
		CC認証（HW＋OS）	EMV認定（HW+OS）
セキュリティ要件	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	ISO15408に基づいて作成されたプロテクションプロファイル（公開）EAL4+（AVA_VAN.5）	EMVCoが定めるSecurity Guideline（非公開）EAL4+（AVA_VAN.5）
評価の範囲	製品の評価及びその開発プロセスを含んだ評価	製品の評価及びその開発プロセスを含んだ評価	
脆弱性評価	JIWG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）
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
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

GP-SEのCC認証、EMV認定では、脆弱性分析においてはマイナンバーカードと同様に最高レベルであるAVA_VAN.5を達成している。GP-SEはマイナンバーカードと同等レベルの耐タンパー性を有するものと評価できる。

参考２

マイナンバーカードのセキュリティ対策

下記に示す通り、暗唱番号(PIN)および耐タンパ性により外部からの攻撃可能性への対策が実装されている。



（出典：総務省｜マイナンバー制度とマイナンバーカード）
https://www.soumu.go.jp/kojinbango_card/03.html

暗証番号

アプリケーション毎に異なる暗証番号を設定して情報を保護し、また暗証番号の入力を一定回数以上間違えるとカードがロックされる仕組みとなっています。

耐タンパー性

耐タンパー性とは、ICチップ内の情報が不正に読み出されたり解析されようとした場合、自動的に内容が消去される等の対抗措置が講じられる性質のことです。

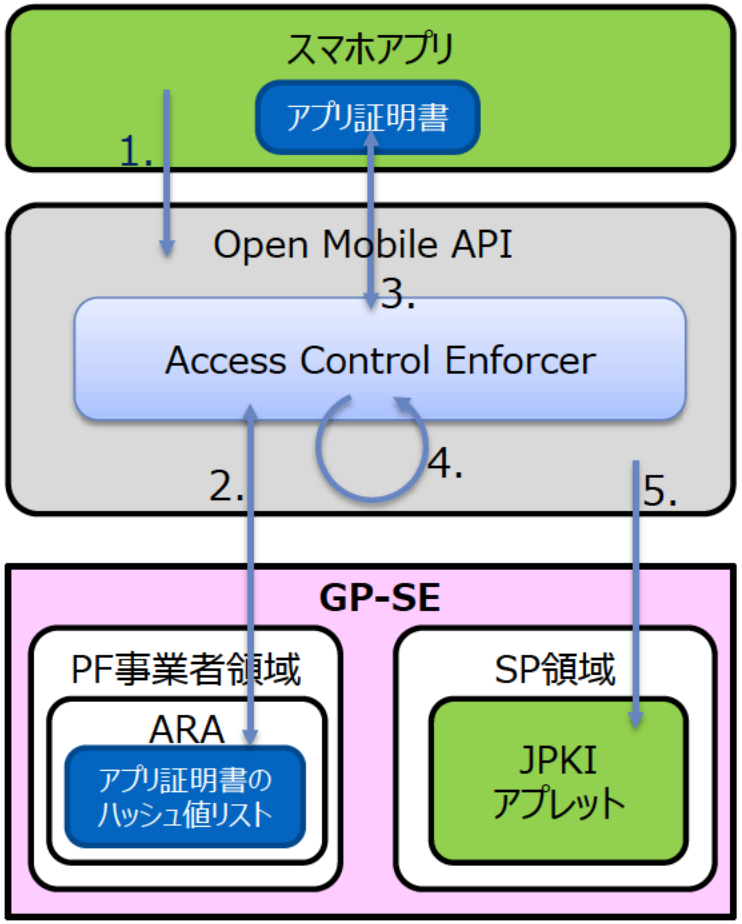
マイナンバーカードのICチップは、こうした偽造目的の不正行為に対する耐タンパー性を有しており、高いセキュリティ性を確保しています。

参考３

GP-SEのセキュリティ機能①

（3）スマホアプリからのアクセスに関するセキュリティ機能

GP-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（スマホアプリ）のみがアクセス可能となっている。この仕組みにより、第三者がGP-SEにアクセス可能なスマホアプリを作ることは極めて困難である。



【参考】GlobalPlatform, 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GP-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）

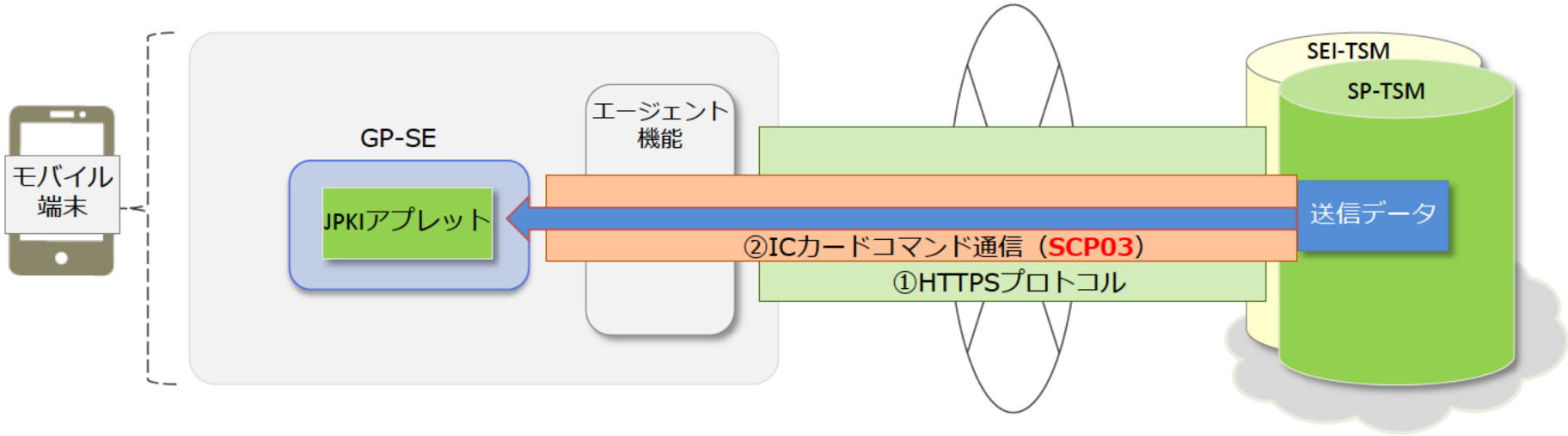
1. スマホアプリがOpen Mobile APIにアクセスする。
   Open Mobile API： GP仕様に準拠したGP-SE内のセキュアな領域にアクセスするために提供されているAndroid用API
2. Open Mobile API内部のACE（Access Control Enforcer）がPF事業者領域内のARA（Access Rule Application）から、アクセスルールを取得する。
3. ACEは、アクセス元のAndroidアプリケーションに付与されている公開鍵証明書のハッシュ値を算出する。
4. ACEは、手順2と手順3で取得したハッシュ値を比較する。一致した場合は、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。

参考４

GP-SEのセキュリティ機能②

（1）セキュアチャネルプロトコル

GP-SEとTSMとの間は、セキュアチャネルプロトコル（SCP03）によってデータ通信が実施される。SCP03は、GlobalPlatformによって定めれた暗号通信プロトコルであり、GP-SEとTSMの2者間での鍵共有と暗号化されたデータを送受信するため、経路途中のデータがスキミングされたとしても解読、改ざんが極めて困難。



（2）GP-SEの暗号機能

GP-SE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いる。また、RSA2048bitの鍵ペア生成も可能となっている。

No.	暗号アルゴリズム	サポート状況	備考
1	RSA2048bit	○	署名はRSASSA-PKCS#1_v1.5に対応
2	AES128bit	○	SCP03の暗号化プロトコル
3	乱数生成	○	SCPで使用