資料5

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基盤構築に向けた調査研究

(概要説明)

株式会社エヌ・ティ・ティ・データ

令和3年5月17日

はじめに（本資料の位置づけ）

本資料は「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基盤構築に向けた調査研究」に関して、弊社が想定している代表的なマイルストン・概要スケジュール及び具体的な検証内容についてまとめたものです。

検証内容の概要及び検証期間について、下記一覧に示します。

＜検証内容及び検証期間　概要一覧＞

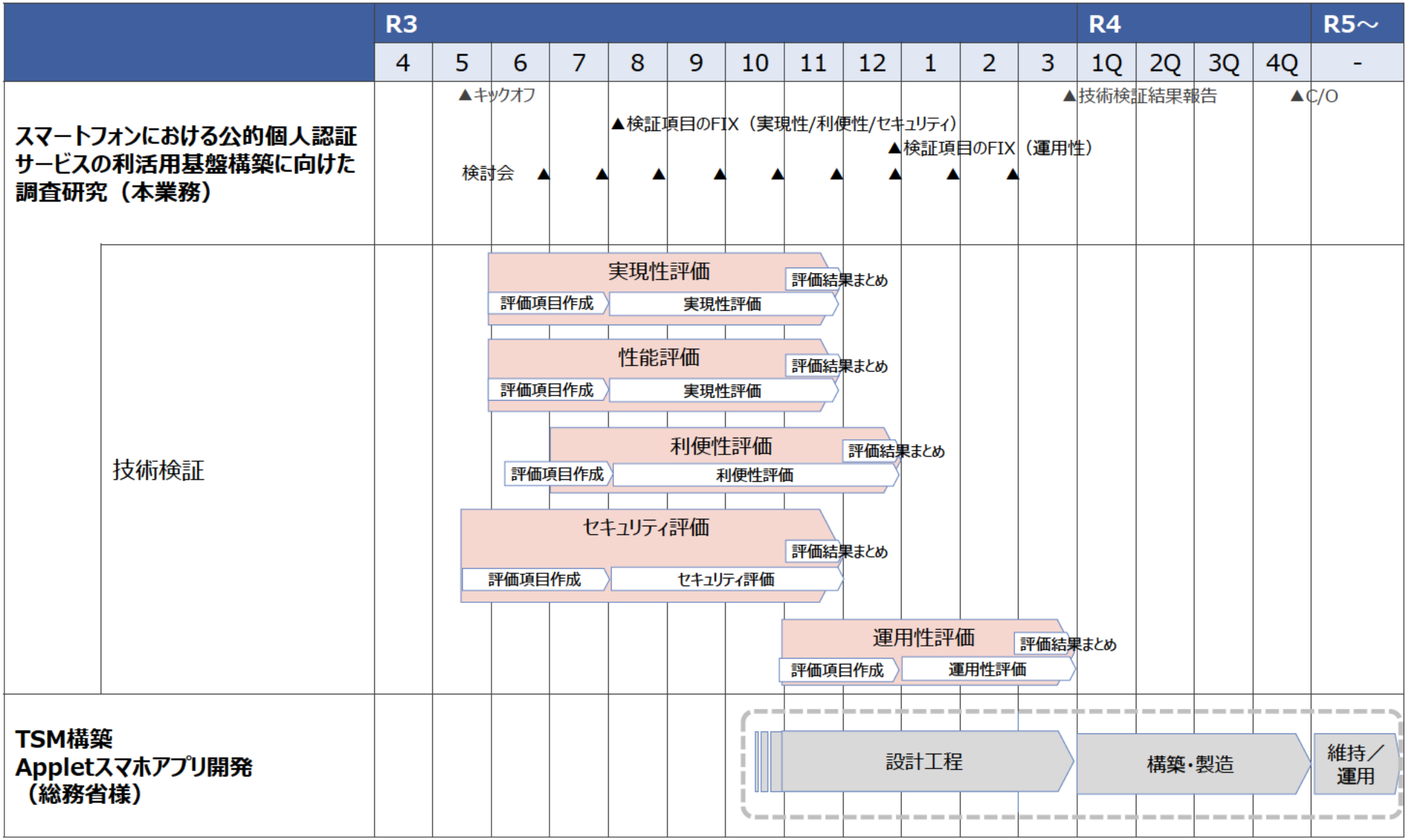
No	検証観点	検証目的	具体的な検証項目	検証期間
1	実現性	これまでの検討結果を実機で検証することによる実現性確認、および課題抽出	・発行、更新等の各フローの実機確認による実現見込の確保 ・実機または実機相当での検証が必要な項目 例）生体認証とGP-SEの連動、SE内の鍵のリモート消去	2021年6月 ～ 2021年11月
2	性能	実機を用いた処理時間計測等による性能確認	・実機での性能確認が必要な項目、製品差が想定される項目 例）GP-SE内の鍵生成処理時間、利用時の処理時間	2021年6月 ～ 2021年11月
3	セキュリティ	フロー全体の安全性および、認証用乱数品質の評価による安全性確認	・技術的な安全性を確認するための評価項目 例）スマホで生成した鍵の品質評価、フローの第三者評価	2021年6月 ～ 2021年11月
4	利便性	スマホならではの使い方やユースケースを踏まえた利便性やUXの確認	・動作における利用時の利便性について検証が必要な項目 例）処理中の通信断/継続、UXに関する実証および評価	2021年7月 ～ 2021年11月
5	運用性	AndroidスマホやGP-SEのライフサイクルを踏まえた運用性の確認	・各種ライフサイクルやユーザサポート観点から確認が必要な項目 例)AndroidOSアップデート	2021年11月 ～ 2022年3月

⇒詳細内容については次ページ以降でご説明いたします。

１．マイルストーン･スケジュール（案）

1. マイルストーン・スケジュール（案）

マスタスケジュール（案）は下記の通り。実現性評価等については、年内に完了予定。



2.前提条件（実証利用スマートフォンについて）

2.前提条件　（利用スマホ種別）

本実証で使用するスマホは以下①～⑤を満たすものとする。

調達仕様書要件詳細
①技術検証は、市販されている端末を利用して実施する。
②AndroidOS搭載スマートフォンを対象とし、OSバージョンは　CryptoObject, BiometricPromptが搭載された9.0もしくは10．0以降を対象とする。
③モバイル通信事業者が提供するモバイルNFCプラットフォームに対応した端末を利用する。
④NFCチップを搭載し、ISO/IEC 14443で規定されるTypeBの通信インタフェースを有するもので実施する。
⑤AndroidOSが持つカードエミュレーション機能、R/Wエミュレーション機能を有する端末であること。

- **GP-SE搭載のスマホ全機種から、端末、OS、GP-SE種類の差分を考慮して検証に使う機種の選択を行っています。**
- **動作検証では市販端末を検証用の設定に変更した上で検証を行う想定です。**
- **選定した機種で実施できない検証項目が生じた場合は、別途評価端末等を新たに用意して実施することも検討いたします。**

3. 検証項目・検証概要

※各検証項目の報告時期について、下記凡例の通り掲載しています。

凡例：

経過報告：〇月　→　任意機種の検証結果の先行報告日　等
検証結果報告：△月　→　全検証完了後の報告（目安）

3． 検証項目･検証概要（サマリ:実現性）

スライドNo	検証項目内容
3	SafetyNet Attestation APIを用いてroot化したスマートフォン等による不正な操作が検出可能か。
4	生体認証時に利用するセキュア領域にて鍵ペアが生成され、GP-SE内に鍵が保存されること。
5	生体認証時に利用するセキュア領域にて本人認証を実施し、実施結果をGP-SE内に連携され、認証できること。
6	特定のスマートフォン機種において生体認証機能に問題/不具合が発生した場合に該当機種を特定して生体認証の利用対象外とすること。
7	アプレットのサイズが64kb上限であるため、サイズ内に収める実装が可能か検証を行うこと。また、アプレットのサイズが64kbを超える場合はその対策を検討すること。
8	GP-SEに対するアクセス元がNFC経由のICカードリーダと電子証明書を活用するためのスマートフォン向けのアプリのどちらであるか識別可能か。
9	GP-SEに残留したJPKIアプレットと失効済の電子証明書等について本人操作ではなくリモートで削除可能か。
10	APK署名、アプリ証明書のハッシュ値リスト等を用いた非正規アプリケーション検出が可能か確認すること。
11	スマートフォンの初期化時にGP-SEの初期化が可能か検討すること。
12	スマートフォンに搭載した電子証明書発行等ができること。
13	スマートフォンに搭載した電子証明書を利用するための生体認証情報登録ができること。
14	オンライン利用（スマートフォンに搭載した電子証明書向けPIN またはパスワード 認証による利用、生体認証による利用、画面ロック解除時の利用）ができること。
15	マイナンバーカードの代わりにNFC経由のICカードリーダへのかざし利用が可能か検証すること。

3．　検証項目･検証概要（サマリ:非機能要件）

スライドNo	検証項目内容
16	･署名用電子証明書と利用者証明用電子証明書2枚向けの公開鍵、秘密鍵の鍵ペア生成を同時に行った際の実機処理時間を計測し、評価すること。 ･電子証明書向けの秘密鍵で署名処理を行った際の実機処理時間を計測し、評価すること。
17	電子証明書の発行、利用におけるターンアラウンドタイムの実機処理時間を計測し、評価すること。
18	かざし利用についてAndroidOSが持つカードエミュレーション機能のTypeB通信における通信性能について評価を行うこと。
19	電子証明書の発行、失効等のフローにおける攻撃可能性への対策の検討及び評価を行うこと。
20	GP-SE、JPKIアプレットの安全性評価スキームの整理を行うこと。
21	電子証明書をスマホ実装したものを用意し、マイナポータルへのログインや各種サービスの電子申請を想定したUX確認を行う。
22	処理中に通信断が発生した場合に中断した処理から再開可能か継続性に関する動作検証を行うこと。
23	Android OSやCDDバージョンアップ時の運用検討、課題抽出を行うこと。
24	Android OSやCDDバージョンアップ時の運用検討、課題抽出を行うこと。
25	GP-SEやアプレットのアップデート、新製品に関する運用課題の抽出及び整理を行うこと。
26	スマートフォン向けアプリの利用者、スマートフォン端末メーカー及び連携先であるJ-LIS様の責任分界を検討すること。
27	スマートフォン向けアプリの利用規約や利用者からの同意取得の方法を検討すること。

3． 検証項目・検証概要
3.1 機能要件

3.1.1 TSM/Android

検証項目

不正利用検出方法の検証において、AndroidOSに具備されているSafetyNet Attestation APIを用いてroot化したスマートフォン等による不正な操作が検出可能か確認すること。

■検証方法

検討会の有識者コメントにあるFIDO2実装の議論を踏まえて、以下の通り検証方法を検討した。検出可能な不正と実装方針を事前に整理し、検証のポイントを明確化することで、効果的な検証を行う。

①事前整理
Safety Net Attestation APIの機能を調査し、検出可能な不正と実装方針を整理する。

②実証用システム構築
Safety Net Attestation APIを用いた不正利用検出を実装する。

③実機検証
実機を用いて、実際に不正な操作を行い検出できるかを確認する。

④検証結果整理
結果をまとめて設計方針として整理する。

経過報告：9～10月
検証結果報告：11月

Point1
SafetyNet Attestation APIの利用シーケンスについて整理し、検証に必要な機能とシーケンスの妥当性を確認する。

Point2
署名済み構成証明(JWS)の判定内容について整理し、不正利用検出の実装方針を整理する。

Point3
スマートフォンのメーカーやOSの種類によってSafetyNet Attestation APIの判定が異なる可能性があるため、複数のGP-SE対応機種を対象として検証を行う。

3．検証項目・検証概要
3.1 機能要件

3.1.2(1) 生体認証とGP-SEの連動(1)

検証項目(1)

生体認証情報の登録について実現可能性を検証するため、生体認証情報向けの公開鍵、秘密鍵の鍵ペア生成を行うこと。生体認証時に利用するセキュア領域にて鍵ペアが生成され、GP-SE内に鍵が保存されること。

■検証方法

検討会で整理した生体認証情報の登録の業務フローを踏まえ、KeystoreとGP-SEの各検証方法を検討した。
運用を想定し、認証パターン、機種・OSパターンの追加検証を行い、網羅性の高い検証結果を提供する。

①Keystore API動作検証
TEE内で鍵生成に用いるAndroid-OSのKeystore APIを実行して、RSA2048bitの公開鍵が出力されることを検討した仕組みを実装し、実機検証する。

②認証パターン検証
鍵生成時の認証としては、生体認証、セキュアロックスクリーンが実施可能なことを検討した仕組みを実装し、実機検証する。

③GP-SE(JPKIアプレット)動作検証
JPKIアプレット仕様を実装し、GP-SEに外部認証用の公開鍵を設定可能であることを検討した仕組みを実装し、実機検証する。

④KeystoreとGP-SE連動検証
KeystoreとGP-SEを連動した処理をGP-SE搭載スマホに実装し、実機検証する。

Point1
生体認証活用の実現方式(KeystoreとGP-SEの連動方式)を理解し、生体認証情報の登録の業務フローを元に、詳細な検証プロセスを整理する。

Point2
鍵生成時の認証パターン検証だけでなく、鍵ペア生成後、指紋追加、指紋全削除、ロック設定(PIN、パスワード、パターン)の変更を実施した場合に鍵が無効化されることを確認する。

Point3
複数OSバージョン、キャリアを整理し、実端末を使用して動作検証を行う。KeystoreとGP-SEのそれぞれのバージョン毎の動作差分を確認する。

経過報告：10月
検証結果報告：11月

3．検証項目・検証概要
3.1 機能要件

3.1.2(2) 生体認証とGP-SEの連動(2)

検証項目(2)

生体認証情報の利用の実現可能性について技術検証するため、生体認証時に利用するセキュア領域にて本人認証を実施し、実施結果をGP-SE内に連携され、認証できること。

■検証方法

検討会で整理した生体認証情報の利用の業務フローを踏まえ、KeystoreとGP-SEの各検証方法を検討した。
認証パターン、機種・OSパターンの追加検証を行い、網羅性の高い検証結果を提供する。

①Keystore API動作検証
GP-SEで生成した乱数とAndroid-OSのKeystore APIを使って、事前に登録した秘密鍵を用いて認証コードを生成可能なことを検討した仕組みを実装し、実機検証する。

②認証パターン検証
認証コード生成時の認証としては、生体認証、セキュアロックスクリーンが実施可能なことを検討した仕組みを実装し、実機検証する。

③KeystoreとGP-SE連動検証
KeystoreとGP-SEを連動した処理をGP-SE搭載スマホに実装し、Keystoreで生成した認証コードをGP-SEに送信し、外部認証が成功することを実機検証する。

Point1

生体認証活用の実現方式(KeystoreとGP-SEの連動方式)を理解し、生体認証情報の利用の業務フローを元に、詳細な検証プロセスを整理する。

Point2

複数OSバージョン、キャリアを整理し、実端末を使用して動作検証を行う。KeystoreとGP-SEのそれぞれのバージョン毎の動作差分を確認する。

経過報告：10月
検証結果報告：11月

3．検証項目・検証概要
3.1 機能要件

3.1.2(3) 生体認証とGP-SEの連動(3)

検証項目(3)

TSMで特定機種による生体認証を利用制限および識別する方法について実機検証するため、特定のスマートフォン機種において生体認証機能に問題/不具合が発生した場合に該当機種を特定して生体認証の利用対象外とすることが技術的に可能か検証すること。

■検証方法

検討会で整理した生体認証情報の利用の業務フローを踏まえ、特定機種に対する生体認証の利用制限の検証方法を検討した。

①特定端末の識別
アプリ実行端末の機種情報を取得する方法を検証する。
端末情報の取得、及び判別の実装方法について、端末情報が偽装されにくい方法かを評価する。

②生体認証機能の制限
(1)で取得したアプリ実行端末の機種情報をTSMサーバに送信し、TSMサーバで生体認証の使用制限対象かを判別する方法を検証する。

Point1　生体認証使用制限の実装方針の整理

アプリ実行端末上で機種情報を取得する方法、TSMサーバ上で生体認証の使用制限対象機種かどうかを判定し、端末での機能制限を実行する方法について整理し、実装方針を整理する。

Point2　複数の機種・OSバージョンでの実機検証

実端末を使用した生体認証の使用制限の動作検証を行い、機種毎・OS毎の動作差分を確認する。

経過報告：10月
検証結果報告：11月

3． 検証項目・検証概要
3.1 機能要件

3.1.3(1) GP-SE(1)

検証項目(1)

JPKI機能を実装させるアプレットのサイズが64kb上限であるため、サイズ内に収める実装が可能か検証を行うこと。また、アプレットのサイズが64kbを超える場合はその対策を検討すること。

■検証方法

①アプレット試作
特定の業務シーケンスが実施できるアプレットを試作し、アプレットサイズを計測する。次ページ以降に記載する業務及び機能を対象とし、その他の機能や異常系処理は対象としない。

②試作に含まない処理に関するサイズの試算
①で実装しない処理(①で対象としないパラメータを指定した機能等)、異常系処理について一部を試作することでアプレットサイズを試算する。

③セキュアコーディングの試算
セキュアコーディングを実装するとアプレットサイズに影響があるため、一部の処理にセキュアコーディングを実装し、アプレットサイズを試算する。

④64kBに収まらない場合の対策検討
アプレットのサイズ低減、及び、アプレットの分割について検討し、アプレットのサイズ制限を回避する方法について検証する。

Point1

マイナンバーカードに関するノウハウを活用し、検討会の議論を踏まえてもれなくコマンド仕様、ファイル仕様、およびデータ構造仕様を検討することで、商用で利用する可能性のあるすべてのコマンド及びファイルを網羅してアプレットサイズを試算する。

Point2

GP-SEの種類により、実装方法が異なる可能性があるため、GP-SEの種類ごとに検証を行うことで、設計工程での手戻りを防ぐ。

Point3

アプレットを分割した際でも外部からのアプレットアクセス時に単一アプレットと見えるような対策を検討し、各システムがアプレットを使用する際に処理が複雑もしくは実現不能となることを回避する。

経過報告:8月
最終報告:11月

3． 検証項目・検証概要
3.1 機能要件

3.1.3(2) GP-SE(2)

検証項目(2)

GP-SEに対するアクセス元がNFC経由のICカードリーダと電子証明書を活用するためのスマートフォン向けのアプリのどちらであるか識別可能か技術検証を行うこと。

■検証方法

①GP-SE機能を用いた通信元識別機能を検討
GP-SEの仕様を調査し、通信元識別機能を実現する方法について検討する。

②通信元識別機能を試作
検討した通信元識別機能を持つアプレットを試作する。

③動作検証
通信元識別機能を持つアプレットの試作品をスマートフォン上で動作させ、通信元を識別できるかどうかを検証する。

④不正アクセスへの別対策の立案
検討会において通信元の識別が不要となった場合、不正アクセスを考慮した対策を検討する。

Point1

GP-SEプラットフォームに実装済の機能を用いて、各通信がスマホアプリ経由なのかNFC経由なのかを識別し、実績のある方法を採用することでより高い確度で実現性の検証を行う。

Point2

GP-SEの種類により、実装方法が異なる可能性があるため、GP-SEの種類ごとに検証を行うことで、設計工程での手戻りを防ぐ。

Point3

現在の検討会の議論では通信元の識別ではなく、生体認証用公開鍵にアクセス権を設定する方式も検討されている。検討会の議論の推移を踏まえ、アクセス権を設定する方針となった際には、アクセス権の設定に対する検証を実施する。

経過報告：8月
検証結果報告：11月

3． 検証項目・検証概要
3.1 機能要件

3.1.3(3) GP-SE(3)

検証項目(3)

電子証明書失効済みのスマートフォンのGP-SEに残留したJPKIアプレットと失効済の電子証明書等について本人操作ではなくリモートで削除可能か検証を行うこと。

■検証方法

①リモートによる削除に必要となる基本方式の検討
利用者がスマートフォンを操作することなく、サーバ側の処理を契機としたGP-SE内のJPKIアプレットおよび失効済の電子証明書を削除するための方式案を検討し、課題抽出を行う。

②課題に対する対応策の検討
①で抽出した課題に対する対応策を検討し、実装すべき範囲を明確にする。加えて、利用シーンを想定し、リモートによる削除が成功するケース、成功しないケースを洗い出す。

③リモートによる削除の動作検証
検証環境を構築し、②で整理した利用シーンにおいて想定通りの実行結果となることを検証する。代表的な機種について検証を実施。

Point1

具体的な電子証明書等の削除の方法として、JPKIアプレットの削除、鍵及び電子証明書の削除の2通りが考えられる。全体のシステム構成、処理時間、コスト等の観点から比較検討し、いずれかを選定する。

Point2

リモート削除の対象となるスマートフォンは譲渡等によって他人が所持していることが想定されるため、発生し得る様々な状況を想定し、想定通りの動作するかを確認する。

検証結果報告：11月

3．　検証項目･検証概要
3.1 機能要件

3.1.4(1)　その他要件(1)

検証項目(1)

APK署名、アプリ証明書のハッシュ値リスト等を用いた非正規アプリケーション検出が可能か確認すること。

■検証方法

①Androidセキュリティ機能の調査
JPKIスマホアプリに関連するAndroidのセキュリティ機能を抽出し、それら機能の詳細、及び実装上の注意点を調査する。

②各機能の実機検証
①で抽出した機能のうち、実機検証が必要となる機能を選定し、それら機能に対して実機検証を実施する。

③アプリの実装方針の整理
①での調査結果、及び②実機検証結果に基づいて、本アプリにおける実装方針の整理を行う。

Point1　主要なAndroidセキュリティ機能を調査

JPKIスマホアプリに関連する主要なAndroidセキュリティ機能を抽出し、それら機能の実装上の注意点を調査する。
（候補： OpenMobileAPIによるアクセス制御機能、APK署名、生体認証機能、業務アプリとの連携機能、等）

検証結果報告：12月

3．検証項目・検証概要
3.1 機能要件

3.1.4(2) その他要件(2)

検証項目(2)

スマートフォンの初期化時にGP-SEの初期化が可能か検討すること。

■検証方法

①現状調査
スマートフォンの初期化時にGP-SEが初期化されるか、実機確認、端末ベンダヒアリング等を実施し、端末初期化の仕組みを調査して整理する。また、類似例（FeliCaサービス）において、GP-SEの初期化がどのように運用されているか調査を行う。

②GP-SEの初期化の実現方式と課題の検討
スマートフォンの初期化時にGP-SEを初期化する方法を検討し、実現に向けて現状と課題を整理する。

③ステークホルダとの課題に対する対応策の検討
②で整理した課題について、GP-SEの初期化の実現に向けて連携が必要となる通信キャリア、端末ベンダ、Google等と協議し、対応方針をまとめる。

Point1

利用者がスマートフォンを初期化する際の導線はAndroid OSに近しいレイヤでのアプリで実現されていることから、実現方式を検討しつつ、通信キャリア・端末ベンダ・Googleなどの関連するステークホルダと協議し、対応方針をまとめる。

Point2

GP-SEの初期化について、できるだけ多くのチャネルで実施できることが望ましいと考えるため、GP-SEの初期化方法について並行して検討を進める。

経過報告：10月
検証結果報告：11月

3． 検証項目・検証概要
3.1 機能要件

3.1.5(1) 業務フロー、基本機能確認(1)

検証項目(1)

スマートフォンに搭載した電子証明書発行等ができること。

■検証方法

検討会で整理した電子証明書に関する業務を踏まえ、業務フローの机上検証、実機検証の各検証方法を検討した。
運用を想定した業務フローの追加検証を行い、また、本番環境に近い環境で実機検証することで、精度の高い評価結果を提供する。

①業務一覧の作成
スマホJPKIに関する想定される業務パターンを整理して、業務一覧を作成する。

②詳細なフローの作成
主要な業務を対象に詳細なフローを作成し、各業務フローの最初から最後まで机上検証する。

③詳細フローに基づいた実機による動作検証
作成した詳細フローを元に、各業務フローの最初から最後まで実機検証する。

④動作検証結果の整理
机上検証、実機検証の結果を元に、実現方式における技術面・運用面の全体的な評価・分析を行う。

経過報告：10月
検証結果報告：11月

Point 1
検討会で整理した電子証明書に関する業務に加え、運用を想定した業務を追加し、業務一覧を作成する。

Point2
検討会で提示された業務フローについて、GP-SE仕様・JPKI仕様を調査し、実現性の評価が可能な詳細な業務フローを作成する。

Point3
試験用マイナンバーカードとJ-LIS様試験環境を利用し、本番環境に近い環境で、業務フローの実機検証を行う。

Point4
GP-SEが搭載されている機種を対象として検証を行う。
また、サポート範囲内の複数OSについて動作検証を行う

3．　検証項目・検証概要
3.1 機能要件

3.1.5(2)　業務フロー、基本機能確認(2)

検証項目(2)

スマートフォンに搭載した電子証明書を利用するための生体認証情報登録ができること。

■検証方法

検討会で整理した生体認証情報の登録の業務フローを踏まえ、業務フローの机上検証、実機検証の各検証方法を検討した。

①詳細なフローの作成
生体認証情報の登録の詳細なフローを作成し、作成した業務フローの最初から最後まで机上検証する。

②詳細フローに基づいた実機による動作検証
作成した詳細フローを元に、各業務フローの最初から最後まで実機検証する。

③動作検証結果の整理
机上検証、実機検証の結果を元に、実現方式における技術面・運用面の全体的な評価・分析を行う。

Point1
生体認証情報の登録の詳細な業務フローを作成し、発行からの一連の業務フローを、最初から最後まで、机上検証、実機検証する。

経過報告：10月
検証結果報告：11月

3． 検証項目・検証概要
3．1 機能要件

3.1.5(3) 業務フロー、基本機能確認(3)

検証項目(3)

オンライン利用（スマートフォンに搭載した電子証明書向けPIN またはパスワード 認証による利用、生体認証による利用、画面ロック解除時の利用）ができること。

■検証方法

検討会で整理した認証方式の併用の考え方を踏まえ、オンライン利用の業務フローの机上検証、実機検証の各検証方法を検討した。

①詳細なフローの作成
オンライン利用の詳細なフローを作成し、作成した業務フローの最初から最後まで机上検証する。

②詳細フローに基づいた実機による動作検証
作成した詳細フローを元に、各業務フローの最初から最後まで実機検証する。

③動作検証結果の整理
机上検証、実機検証の結果を元に、実現方式における技術面・運用面の全体的な評価・分析を行う。

Point1

オンライン利用の詳細な業務フローを作成し、発行からの一連の業務フローを、最初から最後まで、机上検証、実機検証する。

経過報告：10月
検証結果報告：11月

3.1.5(4)　業務フロー、基本機能確認(4)

検証項目(4)

電子証明書を搭載したスマートフォンで、マイナンバーカードの代わりにNFC経由のICカードリーダへのかざし利用が可能か検証すること。

■検証方法

検討会で整理したかざし利用の考え方を踏まえ、かざし利用の業務フローの机上検証、実機検証の各検証方法を検討した。

①詳細なフローの作成
かざし利用の詳細なフローを作成し、作成した業務フローの最初から最後まで机上検証する。

②詳細フローに基づいた実機による動作検証
作成した詳細フローを元に、各業務フローの最初から最後まで実機検証する。

③動作検証結果の整理
机上検証、実機検証の結果を元に、実現方式における技術面・運用面の全体的な評価・分析を行う。

Point1

かざし利用の詳細な業務フローを作成し、発行からの一連の業務フローを、最初から最後まで、机上検証、実機検証する。

経過報告：10月
検証結果報告：11月

3．検証項目・検証概要
3.2 非機能要件

3.2.1(1)(2) 性能確認(1)(2)

検証項目(1)(2)

GP-SE内でスマートフォンに搭載した署名用電子証明書と利用者証明用電子証明書2枚向けの公開鍵、秘密鍵の鍵ペア生成を同時に行った際の実機処理時間を計測し、評価すること。
GP-SE内でスマートフォンに搭載した電子証明書向けの秘密鍵で署名処理を行った際の実機処理時間を計測し、評価すること。

■検証方法

①測定対象の処理が実行できるアプレットの試作・搭載
暗号関連の処理が実行可能なアプレットを試作し、スマートフォンのGP-SEに搭載する。

②SP-TSMからコマンドを送信
測定対象コマンドをSP-TSMから送信し、アプレット上で処理を実行する。

③コマンド送信からレスポンス受信までを計測
コマンド送信からレスポンス受信までに要した時間をTSMクライアント上で計測し、処理時間を出力する。

④処理時間の分析
マイナンバーカードで同様の処理に対して処理時間を計測し、アプレットの処理時間と比較する。マイナンバーカードの代わりにスマートフォンを使用する想定であることから、GP-SEの処理時間とマイナンバーカードの処理時間の比較確認を実施する。

Point1

GP-SEへのコマンド送信からレスポンス受信までの時間を測定することで、GP-SEの処理時間のみを測定することができ、他のボトルネックとなる処理を排除して検討することが可能である。

Point2

GP-SE の種類毎に検証を行うことで、特定のGP-SEの処理時間が遅く運用に耐えられないリスクを排除することが可能である。

経過報告：9月
検証結果報告：11月

3.2.1(3)　性能確認(3)

検証項目（3）

スマートフォンに搭載した電子証明書の発行、利用におけるターンアラウンドタイムの実機処理時間を計測し、評価すること。なお、利用についてはかざし利用についても計測対象とすること。

■検証方法

①実証用システム構築
試験環境に実証用システムを構築し、検証に必要な機能を実装する。

②ターンアラウンドタイム計測
発行、かざし利用、オンライン利用(生体認証)について測定を行う。

③検証結果整理
各機種の処理時間について分析を行い、結果をまとめる。

経過報告:9～10月
検証結果報告:11月

Point1
スマートフォンの機種によって通信特性や処理性能が異なる可能性があるため、GP-SEが搭載されている機種を対象として検証を行う。

Point2
プロファイリングツールを使用してリソース性能をプロファイルする。

検討会における業務フローや実現方式の整理結果を踏まえて、検証方法を検討した。
実機処理時間の計測と併せてリソース性能のプロファイルを行うことで、ボトルネックとなっている処理の特定およびリソースの最適化を行い、本開発に向けた性能課題を整理する。

3.2.1(4)　性能確認(4)

検証項目(4)

かざし利用についてAndroidOSが持つカードエミュレーション機能のTypeB通信における通信性能について評価を行うこと。

■検証方法

①アプレットの試作・搭載
特定の業務シーケンスの処理が実行可能なアプレットを試作し、スマートフォンのGP-SE上に搭載する。

② ICリーダライタとの通信互換性検証
試作したアプレット搭載のスマートフォンをICリーダライタ上に設置し、評価用シーケンスが正常終了することを確認する。

③複数の測定条件で検証
スマートフォンの設置位置、ICリーダライタ、スマートフォン機種といった条件を変更し、検証を行う。

④マイナンバーカードとの比較
マイナンバーカードの測定結果と比較し、分析を行う。

Point1
業務シーケンスに則り通信互換性を検証する。スマートフォンの設置位置や方向については複数種類を対象とする。また、マイナンバーカード対応のICリーダライタのうち、複数種類を対象として検証する。測定結果は、マイナンバーカードの測定結果と比較する。

Point2
スマートフォンをTypeBカードエミュレーションモードで使用した場合について、電気的特性を検証し、ユーザビリティに問題ないことを確認する。

Point3
GP-SEを搭載するスマートフォンのうち、複数機種を対象に評価を実施し、運用上の問題が発生することを未然に防ぐ。

経過報告：9月
最検証結果告：11月

3．　検証項目・検証概要
3.2 非機能要件

3.2.2(1)　セキュリティ確認(1)安全性評価①

検証項目(1)

スマートフォンに搭載した電子証明書の発行、失効等のフローにおける攻撃可能性への対策の検討及び評価を行うこと。なお、評価の実施に当たっては適当な第三者の評価を踏まえること。

■検証方法

①対象とする詳細フロー
本業務では、作成した詳細フローを対象として、攻撃可能性への対策の検討及び評価を行う。主要な業務フローを対象として評価を実施する。

②脅威分析
①で作成した詳細フローをもとに脅威の洗い出しを行う。

③詳細フローの各処理に対応する脅威及び対策の整理
詳細フローの一つ一つの処理に対応する脅威とその脅威に対応する対策案を整理する。

④対策案の妥当性確認
安全性評価の知見を有する事業者の協力を得て、対策案が有効であるかを検証する。脆弱性が検出された場合は、詳細フローの修正など新たな対策を検討する。

検証結果報告：11月

Point1
作成するすべての詳細フローを対象とし攻撃可能性への対策の検討及び評価を行う。

Point2
検討会で示されている各種業務フローをシステム構成要素単位に分解した詳細フローに基づいて、脅威分析及び対策の妥当性検証を実施する。

3.2.2(2)　セキュリティ確認(2)安全性評価②

検証項目(2)

GP-SE、JPKIアプレットの安全性評価スキームの整理を行うこと。

■検証方法

①GP-SEの安全性評価の現状調査
GP-SEにおけるCC認証あるいはEMVCo Platform認証の取得実績、対象範囲等の現状調査を実施する。

②想定される安全性評価スキームの検討
第三者評価の考え方を取り入れ、GP-SEの安全性評価スキーム案を洗い出し、比較検証を行う。

③安全性評価スキームの選定と合意形成
複数の安全性評価スキーム案の中から、セキュリティ評価に関して知見のある評価会社の協力を得て最適なスキームを選定し、関係各所との合意形成を図る。また、実用化に向けてセキュリティ評価の実施時期を検討する。

④セキュリティ要求仕様書とセキュリティ評価項目等の整備
GP-SE（JPKIアプレットを含む）のセキュリティ評価のために必要となるセキュリティ要求仕様書、セキュリティ評価項目等を整備する。

Point1
ICチップ等のセキュリティデバイスのセキュリティ評価の実績のある第三者機関の協力を得て、安全性評価スキームを検討する。

Point2
GP-SEがCC認証あるいはEMVCo Platform認証を取得していることを踏まえ、最適な安全性評価スキームを検討する。

Point3
実用化の際に活用可能となるセキュリティ要求仕様書、セキュリティ評価項目等を整備する。

経過報告：8月
検証結果報告：11月

3.2.3(1)　利便性確認 (1)ユーザテスト/模擬マイナポータルログイン

検証項目

電子証明書をスマホ実装したものを用意し、マイナポータルへのログインや各種サービスの電子申請を想定したUX確認を行う。

■検証方法

①ユーザテストとして実施する内容を具体化し、実行計画を策定する。

②マイナポータルAPを模擬しつつ、今回追加する機能が違和感なく、テストできる環境を構築する。

③会場・ユーザテストのメンバを用意し、ユーザテストの対応者・環境を整備し、ユーザテストを実施する。

④ユーザテストの実施結果をとりまとめ、設計工程に反映できることを意識したスケジュールで、対応すべき課題を整理する。

検証結果報告：11月～12月

Point

マイナポータルAP・マイナポータル画面を使用したスマホJPKIのユーザーテスト環境を用意することで、テストユーザに安心・安全はいままでと同じレベルでありながら、より簡単・便利になったと感じてもらうことを目指す。

3.2.3(2)　利便性確認　(2)個別検証

検証項目

処理中に通信断が発生した場合に中断した処理から再開可能か継続性に関する動作検証を行うこと。

■検証方法

①TSMとアプリ、アプレット、JPKI間で張られるセッション管理方法を整理し、セッション中断時の対応方針を整理する。(最初からやり直すのか／再開するのか等、画面ロック/電池切れ/オフライン等)

②検討会で議論されたスマホJPKIに関連する各業務に対し、セッション中断となるユースケースを抽出し、中断後の状態、および、再開方法・対応策を検討する。

③業務フローを元に、セッション中断後の再開が正常に実行できることを机上で確認する。

④再開方法・対応策を実装し、想定通りの動作となることを実機検証する。

Point1

検討会で提示されたセッションの考え方を詳細検討し、セッション管理方法とセッション中断時の対応方針を整理する。

Point2

スマートフォンの特性とシステム構成から、セッション中断となるユースケースと発生頻度を整理する。

Point3

利用時に特に多く発生すると想定される発行時のスマホ圏外移動によるセッション中断について、中断時の状態と継続性の高い再開方法を整理する。

Point4

セッション中断となるユースケースの実機検証を行い、中断～再開操作(継続性)に関するユーザ利便性を評価する。

検証結果報告：11月

3.2.4（1）　運用性確認 (1)[Android OSアップデート]

検証項目(1)

（１）Android OSやCDD(※)バージョンアップ時の運用検討、課題抽出を行うこと。
※Android Compatibility Definition Document

■検証方法

①事前調査
OSアップデートリリースにより、影響が起こる事象を整理する。

②課題の抽出
調査結果から、OSアップデートに関する課題事項を整理する。

③運用方針検討
抽出した課題に対応するための運用案を検討する。
案の作成については、現行のマイナポータルAPの運用方針を参考にする。

検証結果報告：1月～2月

Point

バージョンアップ時の運用方法について検証を行い、APが利用できなくなるリスクを回避する。

3.2.4(2)　運用性確認 (2) [CDDバージョンアップ]

検証項目(2)

Android OSやCDD(※)バージョンアップ時の運用検討、課題抽出を行うこと。
※Android Compatibility Definition Document

■検証方法

①CDD定義と関連する機能の抽出
検討会での検討結果に基づき、スマホJPKIで利用が想定されるAndroidの機能の一覧を作成し、Android機能に対応するCDDの定義を抽出、CDDがバージョンアップした場合に影響を受ける可能性のある項目を抽出する。

Point1
検討会の議論を考慮して、GP-SE関連の機能だけでなく、生体認証等、スマホJPKIで利用される可能性がある機能についても、対象として調査を行い、網羅的に検証することで、商用工程での手戻りを防ぐ。

②CDDバージョンアップ時の課題の抽出
CDDバージョンアップ時に発生が想定される事象(変更なし、変更、削除、新規定義追加等)をまとめ、対象のCDDの定義毎に、事象によって生じる課題を検討、検討結果を元に、バージョンアップ時に想定される課題をまとめる。

Point2
過去のバージョンのCDDを遡って各定義ごとの変更履歴を調査し、CDD変更時の対応実績を元に今後のCDDバージョンアップ時の対応を検討する。

③CDDバージョンアップ時の運用フロー、課題への対応方針の整理
CDDバージョンアップ時の運用フローを作成し、バージョンアップ時に想定される運用上の対応事項と課題、及び課題への対応方針をまとめる。

経過報告:9月
検証結果報告:11月

3.2.4(3)　運用性確認(3)

検証項目(3)

GP-SEやアプレットのアップデート、新製品に関する運用課題の抽出及び整理を行うこと。

■検証方法

①新製品導入、アップデート時の影響要素の抽出
GP-SE及びスマートフォンの新製品導入、アプレットのアップデート時に影響があるスマホJPKIの構成要素を抽出する。

②新製品導入、アップデート時の確認項目整理
GP-SE及びスマートフォンの新製品導入、アプレットのアップデート時に確認が必要な項目 (かざし利用時の無線通信性能、搭載GP-SE、端末ソフトウェア、セキュリティ実装、JPKI UIアプリの動作等)を整理する。

③ 新製品導入、アップデート時の対応事項と課題の抽出
認項目に関わる対応事項（確認主体、確認基準の策定と運用、評価用サンプル入手等）を整理し、課題を抽出する。

④ 新製品導入、アップデート時の運用課題と対応方針の整理
①②③で整理、抽出した運用上の対応事項に関する課題を整理し、対応方針をまとめる。

Point1

GP-SE、スマートフォン、アプレットと、構成要素(JPKI UIアプリ、SEI-TSM等)を網羅的に組み合わせた表を作成し、影響確認が必要な要素が漏れのないようにすることで商用の設計工程における手戻りを防ぐ。

Point2

現在GP-SEを利用しているサービスのGP-SE新機種投入、スマートフォン新機種投入、アプレット更新のそれぞれの過去実績を参考に、確認項目、対応事項と課題を整理し、運用に関する設計に反映できるようにする。

経過報告:9月
最終報告:11月

3.2.4(4)　運用性確認(4)

検証項目(4)

スマートフォンに搭載した電子証明書を活用するためのスマートフォン向けアプリの利用者、スマートフォン端末メーカー及び連携先であるJ-LIS様の責任分界を検討すること。

■検証方法

①現状の類似APに関する責任分界を調査する。
マイナポータルAPや生体認証機能・ICチップを利用したAPの責任範囲を調査する。

②調査結果を基に責任分界案を作成する。

③作成した責任分界案を基に関係者へヒアリングを行う。
スマートフォン端末メーカーおよび地方公共団体情報システム情報機構へ責任分界の案を提示し、議論を行う。

④ヒアリング結果を基に責任分界案を修正する。
責任分界を確定させた後、利用規約へ免責事項を記載する。

Point1

既存のマイナポータルAPに存在しない機能があるため、運用リスク回避を目的に調査結果整理や追加調査を行う。

Point2

運用開始後のトラブルを回避するため、事前の調査時点では責任が明確になっていない事項を整理する。

検証結果報告：1月～2月

3.2.4(5)　運用性確認(5)

検証項目(5)

スマートフォンに搭載した電子証明書を活用するためのスマートフォン向けアプリの利用規約や利用者からの同意取得の方法を検討すること。

■検証方法

①類似アプリ調査
類似アプリではどのように同意を取っているか調査する。

Point

利用規約の同意に抜けがないよう従来のマイナポータルに無い新規機能の類似アプリを中心に調査し、運用リスク回避につなげる。

②方針案の検討
調査結果を元に方針案を検討する。

③結果のまとめ
方針案を元に議論を行って結果をまとめる。

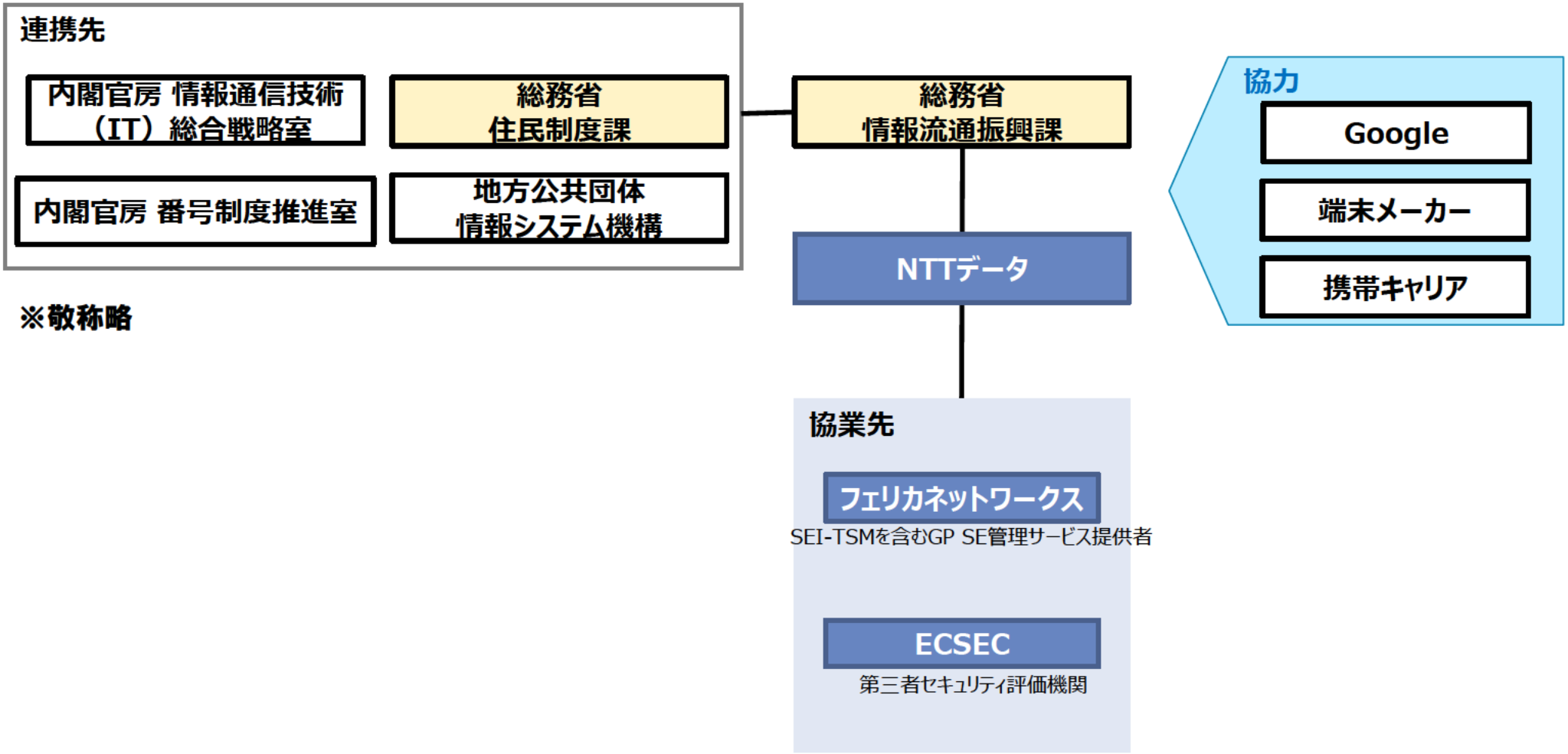
検証結果報告：1月～2月

４.作業の実施体制

4． 作業実施体制

4.1 本調査・検証の実施体制

関係企業・団体の調整を含めて全体管理、調整を行う。下記に全体体制図及び役割を示す。



※敬称略