資料５－１

「公的個人認証サービスのスマートフォンでの利活用の実現に向けた実証」について

平成28年10月25日

NTT DATA

アジェンダ

１．実証事業の全体概要

２．SIMカードへの利用者証明機能の書き込み
- ２－１．検証のポイント
- ２－２．本実証事業で検証するシステムの対象範囲
- ２－３．検証用システムのシステム構成と処理概要
- ２－４．ダウンロード方法に関する安全性の評価
- ２－５．検討会と評価会
- ２－６．検討会及び評価会スケジュール
- ２－７．評価会での検討項目
- ２－８．MVNO事業者による利用者証明機能ダウンロードにおける課題検討

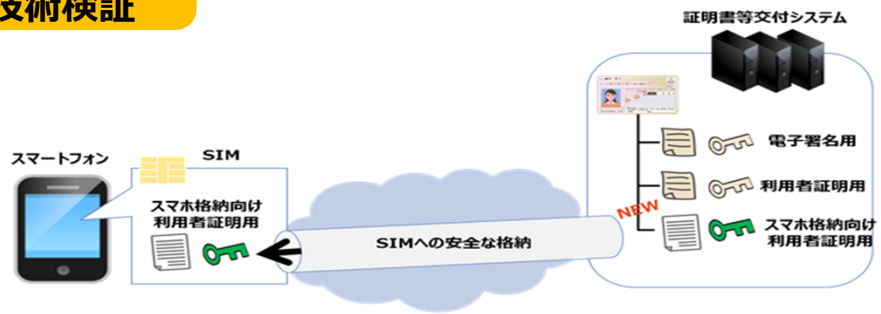
３．iOS搭載スマートフォンによる公的個人認証サービスの活用
- ３－１．検証のポイント
- ３－２．iPhoneにおける利用者証明機能ダウンロードの検証

1. 実証事業の全体概要

本実証事業では、スマートフォンのSIMカードへのセキュアなダウンロードの実現に係る技術検証として「SIMカードへの利用者証明機能の書き込み」「iOS搭載スマートフォンによる公的個人認証サービスの活用」、スマートフォンを活用したユースケース検証として「チケットレス」「インターネットバンキング」の4つの検証を行います。

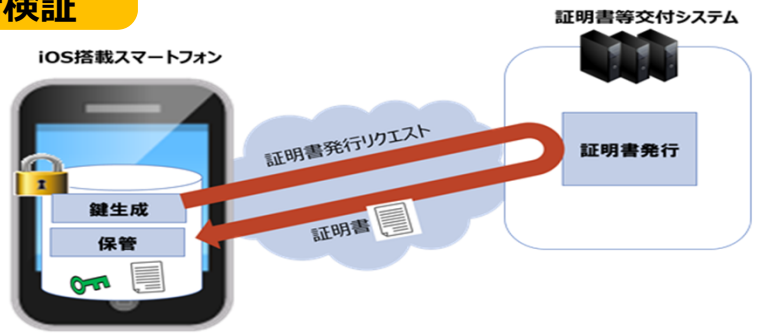
スマートフォンのSIMカードへのセキュアなダウンロードの実現「SIMカードへの利用者証明機能の書き込み」

技術検証



スマートフォンのSIMカードへのセキュアなダウンロードの実現「iOS搭載スマートフォンによる公的個人認証サービスの活用」

技術検証

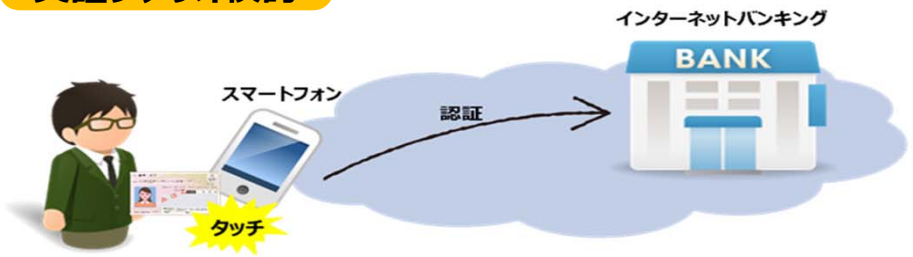


スマートフォンの利活用ユースケースの実現に向けた検討「チケットレスサービス」

ユースケース検証

スマートフォンの利活用ユースケースの実現に向けた検討「インターネットバンキング」

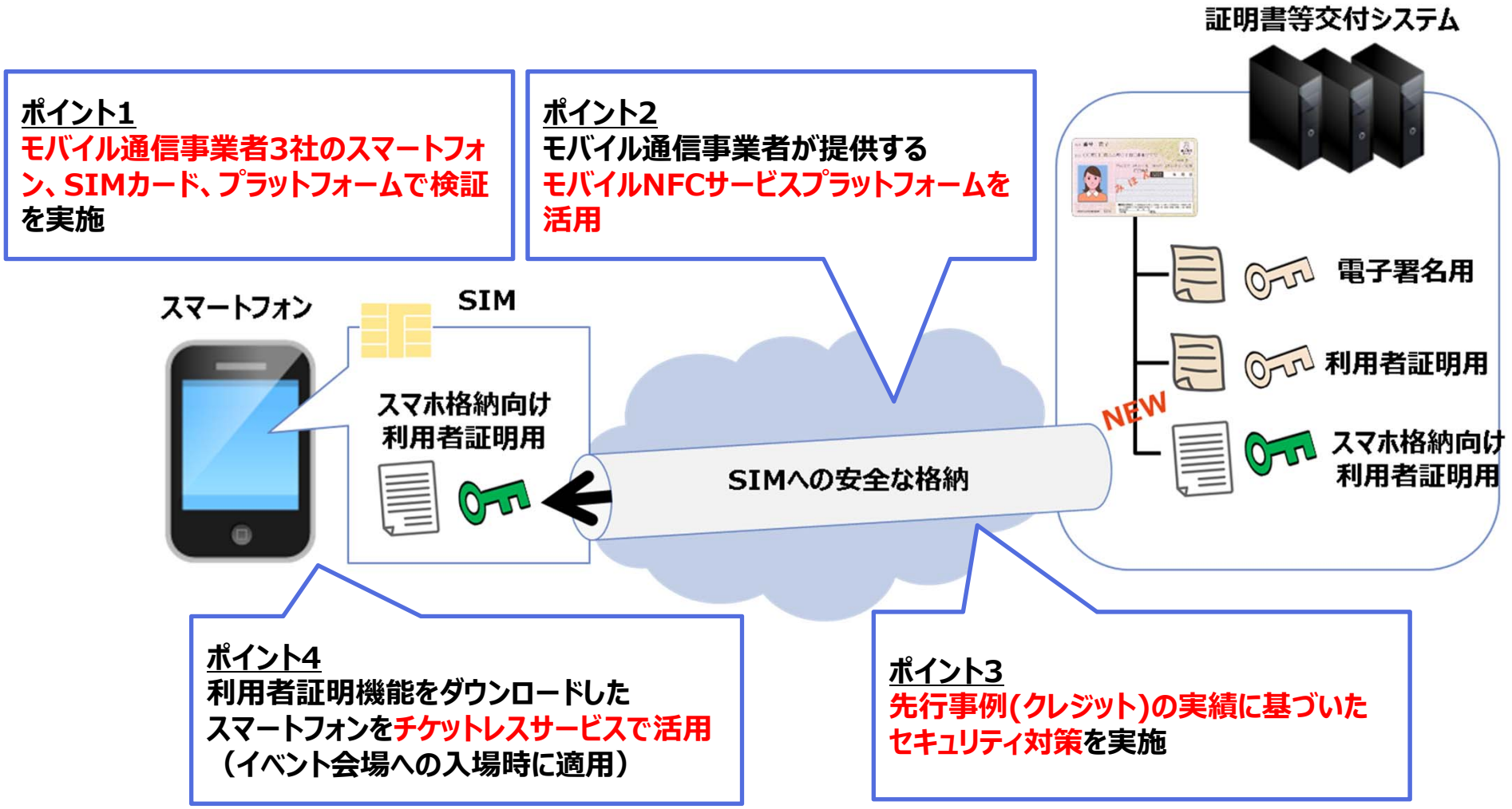
実証シナリオ検討



2. SIMカードへの利用者証明機能の書き込み

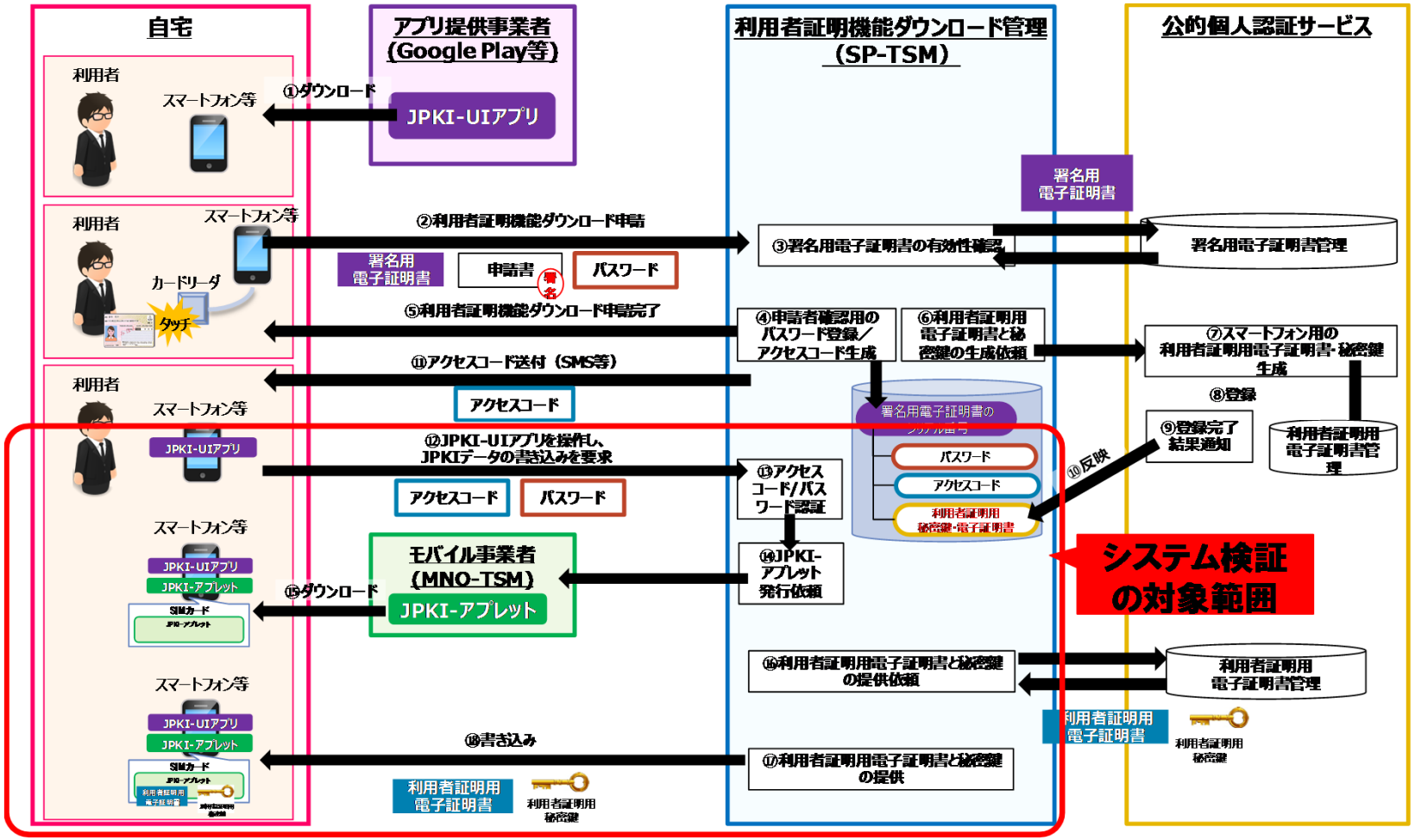
2－1. 検証のポイント

- 利用者のスマートフォン（SIMカード）に利用者証明機能をダウンロードするシステムを開発し、**利用者証明用秘密鍵及び利用者証明用電子証明書の安全な配送方式**を検証を行います。



2－2. 本実証事業で検証するシステムの対象範囲

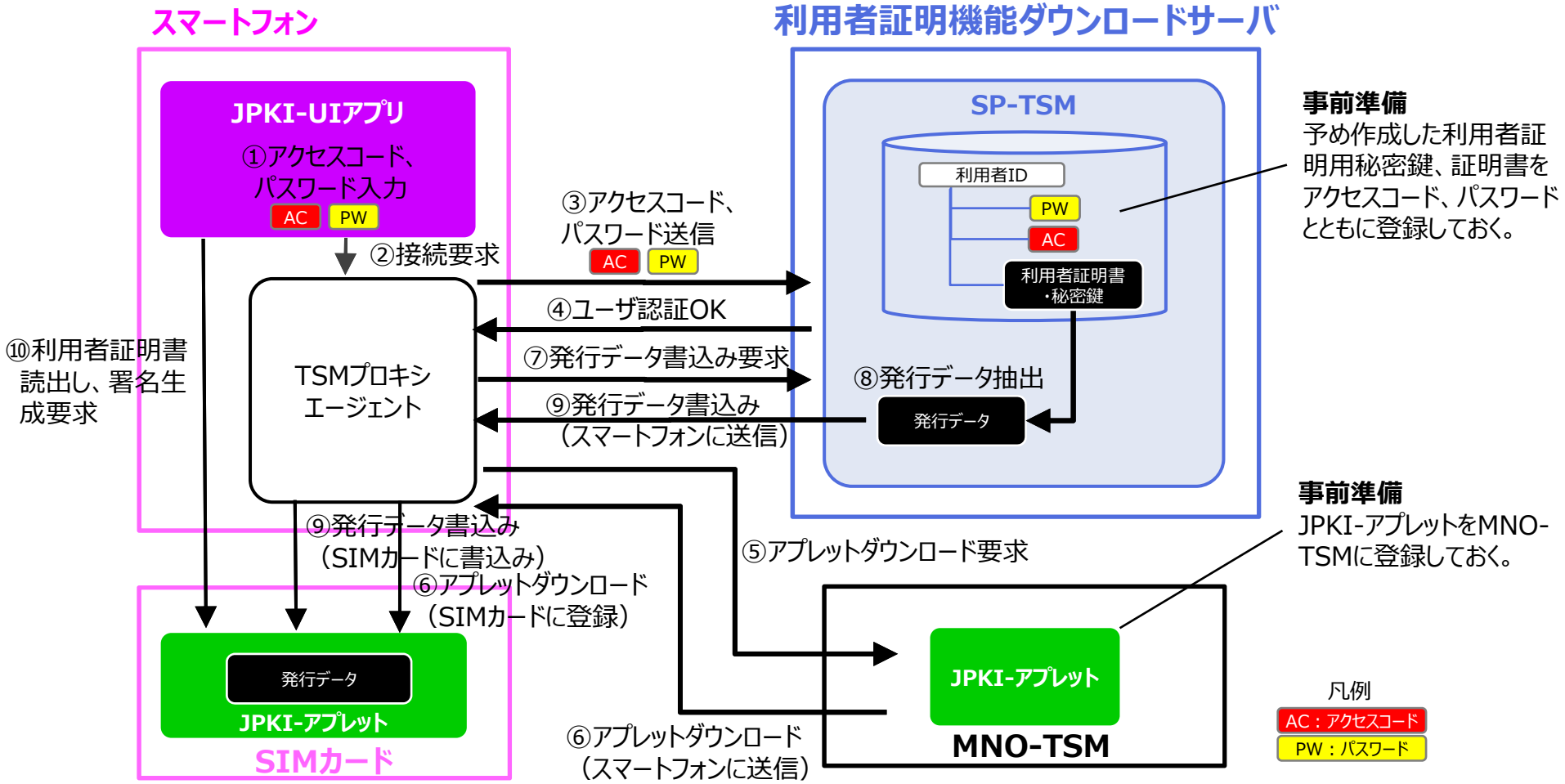
- 利用者のスマートフォン(SIMカード)に利用者証明機能をダウンロードするシステムを開発し、**利用者証明用秘密鍵及び利用者証明用電子証明書の安全な配送方式を検証**を行います。
- 以下に示すように、本実証事業で検証するシステムの対象範囲を以下に示します。



総務省スマートフォンへの利用者証明機能ダウンロード検討SWG(第4回)配付資料より

2－3. 検証用システムのシステム構成と処理概要

- スマートフォン(SIMカード)への利用者証明機能のダウンロードの実現性を検証するため、JPKI-UIアプリ、JPKI-アプレット、SP-TSMを開発します。
- またMNO-TSMについては、モバイル通信事業者3社のMNO-TSMを活用し、JPKI-アプレットのSIMカードへのダウンロードを実施します。



2－4. ダウンロード方法に関する安全性の評価

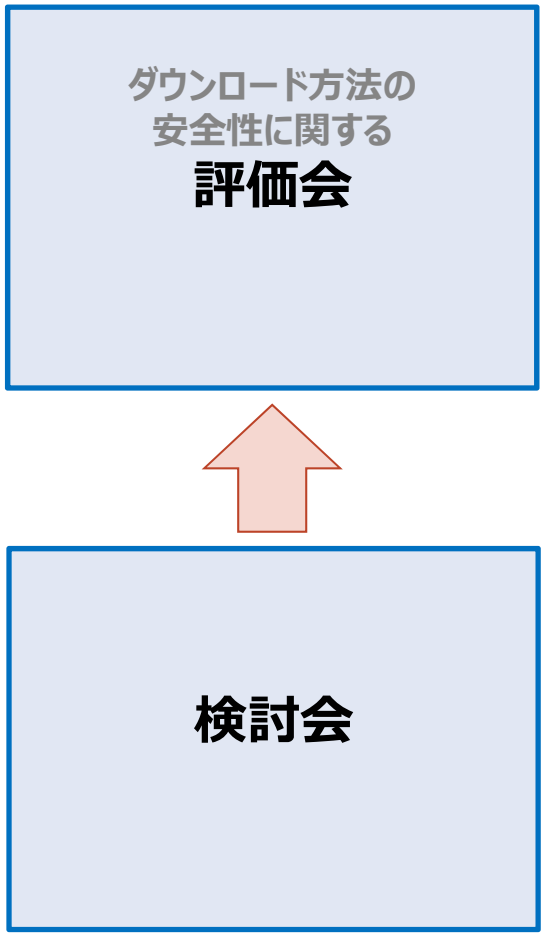
- モバイル通信事業者が提供するモバイルNFCサービスプラットフォームを活用して実現し得るセキュリティ対策の調査及び検討を行い、評価会にて安全性を評価します。

セキュリティ対策の調査及び検討

項番	評価項目（大項目）	評価項目（小項目）	調査及び検討
1	SP領域の安全性	SP領域の生成	・実施権限の確認方法 ・SP領域生成時に設定される情報
2		SP領域の独立性	・特定領域のアプリケーションから他の領域へのアクセス防止 ・他の領域のアプリケーションからのアクセス防止
3		SP領域鍵の運用ルール	・初期設定方法 ・仮SP領域鍵から本SP領域鍵への変更（実施権限の確認方法） ・SP権限での実行機能の範囲
4		SP領域の削除	・実施権限の確認方法 ・削除される情報
5	アプレット配送の安全性	アプレット登録	・実施権限の確認方法 ・アプレット登録時の設定情報
6		セキュアメッセージング方式の安全性	・セキュアメッセージング用鍵の鍵共有方法 ・機密性（暗号化、復号）、完全性（MAC等）の確保方法
7		アプレット内の初期設定データの安全性	・秘密にすべき情報の有無 ・漏洩した場合の影響
8		アプレット削除	・実施権限の確認方法 ・削除される情報
9	秘密鍵配送の安全性	秘密鍵の書込み	・実施権限の確認方法 ・秘密鍵の書込み方法 ・利用者証明用秘密鍵と利用者証明用電子証明書のレベル分け要否
10		セキュアメッセージング方式の安全性	・セキュアメッセージング用鍵の鍵共有方法 ・機密性（暗号化、復号）、完全性（MAC等）の確保方法
11		SP独自の対策	・SP独自の対策の必要性 ・SP独自の対策の実現方法

2－5. 検討会と評価会

- **検証会を開催し、利用者証明秘密鍵等のダウンロード方法に関する安全性評価基準（評価資料）等を作成します。**
- **更に、評価会において有識者、J-LIS様等の関係者にヒアリングを実施し、評価を行います。**



【構成メンバ】
[評価者]有識者（主管課様との協議により決定）
[評価者]J-LIS様、総務省様
[説明者]受託関係者（NTTデータ（請負者）、NTTコミュニケーションズ、DNP）
[オブザーバ]モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）
※モバイル通信事業者については、モバイルNFCサービスプラットフォームに関する各種情報提供、問合せ対応等のため、必要に応じて請負者がオブザーバとして招請するものとします。

【実施内容】
・利用者証明用秘密鍵等のダウンロード方法に関する安全性評価基準（評価資料）の評価
・実用化ロードマップの評価

【構成メンバ】
[資料作成者]受託関係者（NTTデータ（請負者）、NTTコミュニケーションズ、DNP）
[オブザーバ]モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）
※モバイル通信事業者については、モバイルNFCサービスプラットフォームに関する各種情報提供、問合せ対応等のため、必要に応じて請負者がオブザーバとして招請するものとします。

【実施内容】
・利用者証明用秘密鍵等のダウンロード方法に関する安全性評価基準（評価資料）の作成
・システム検証の検討状況や成果等についての意見交換
・実用化ロードマップの検討

2－6. 検討会及び評価会スケジュール

- 検討会及び評価会は以下のスケジュールで開催を予定しています。

#	項目	10月	11月	12月	1月	2月	3月
1	検討会	▲第1回	▲第2回	▲第3回	▲第4回		▲第5回
2	評価会		▲第1回		▲第2回		▲第3回
3	利用者証明機能ダウンロードシステム検証	要件定義/設計	製造/試験/MNO登録			検証	検証済みスマートフォン適用
4	チケットレスサービス実証	要件定義/設計 モニター募集	製造/試験 カード申請 ※クレジットカード申請		カード受取	準備/実証	評価/報告書

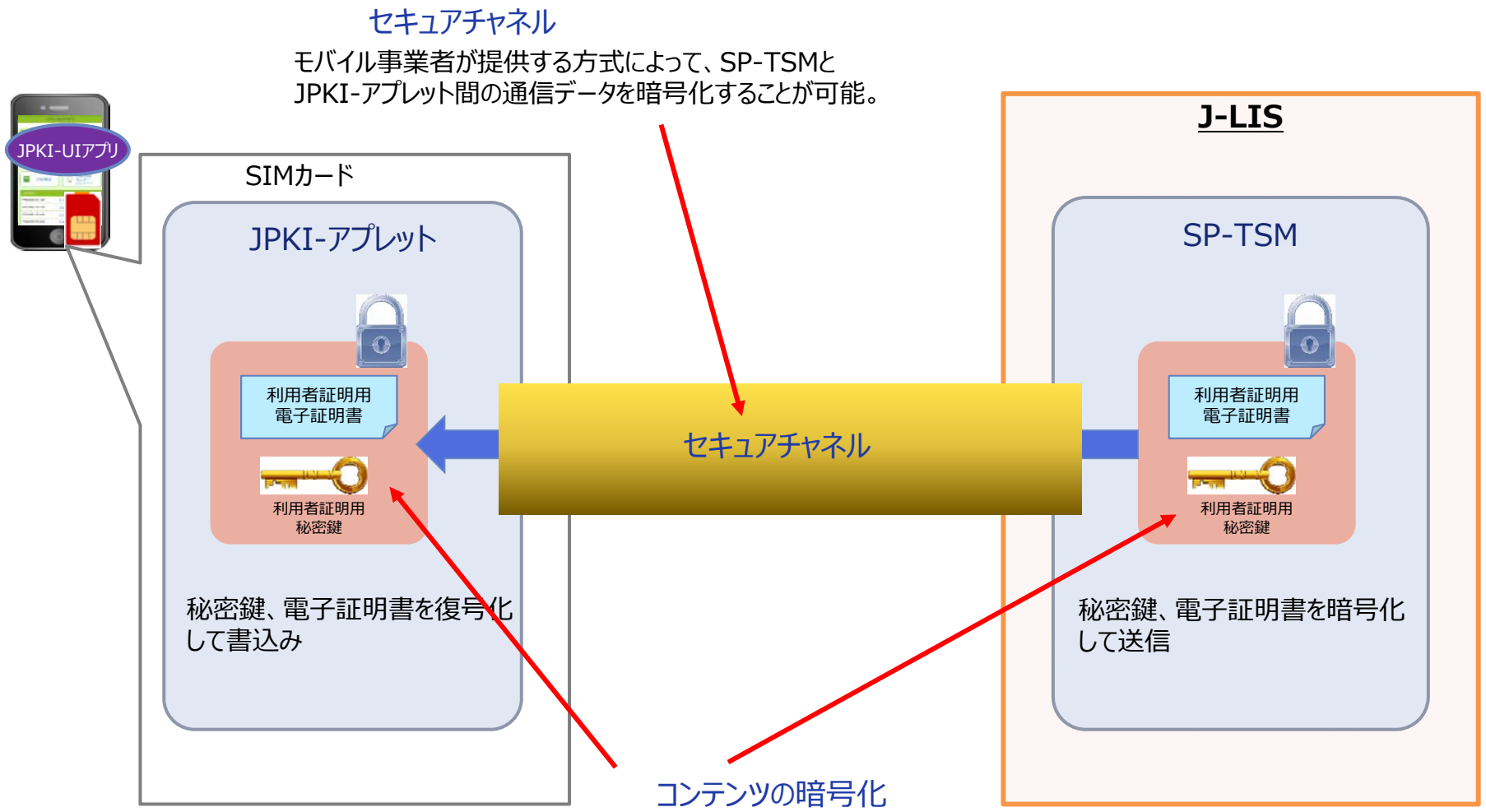
2－7. 評価会での検討項目

- **各回の検討項目を以下に示します。**

回数	検討項目	検討内容	備考
第1回	・アプレット配送の安全性① ・秘密鍵配送の安全性① ・SP領域の安全性① ・SIMカードの機能要件①	・先行事例を参考としたJPKI-アプレットのダウンロード、秘密鍵等の書込み方式について評価する。SP独自のセキュリティ対策の必要性について協議する（別紙1）。 ・SP領域について、SP領域の独立性、SP領域の生成、利用、削除の権限確認方法等などの観点から、安全性を評価する。 ・SIMカードの機能要件を整理するにあたって、調査・検討の進め方について協議する。	提案時に検討した方式についての評価
第2回	・アプレット配送の安全性② ・秘密鍵配送の安全性② ・SP領域の安全性② ・SIMカードの機能要件②	・第1回での評価者からの指摘事項、追加検討事項等を踏まえて検討したJPKI-アプレットのダウンロード、秘密鍵等の書込み方式、SP領域の安全性について評価する。 ・SIMカードの機能要件について、調査・検討結果を踏まえ、機能要件を明確化する。	
第3回	・運用面での課題検討 ・システム検証結果 ・実用化ロードマップ検討	・スマートフォン特有の業務（機種変更、紛失、解約等）及び電子証明書の運用における業務（申請・発行、更新、失効等）の業務フローについて検討する（別紙2）。 ・システム検証結果を課題検討状況を報告する。 ・今後の課題及び解決策の検討状況を踏まえ、実用化に向けたロードマップを作成する。	次年度検証すべき課題の明確化

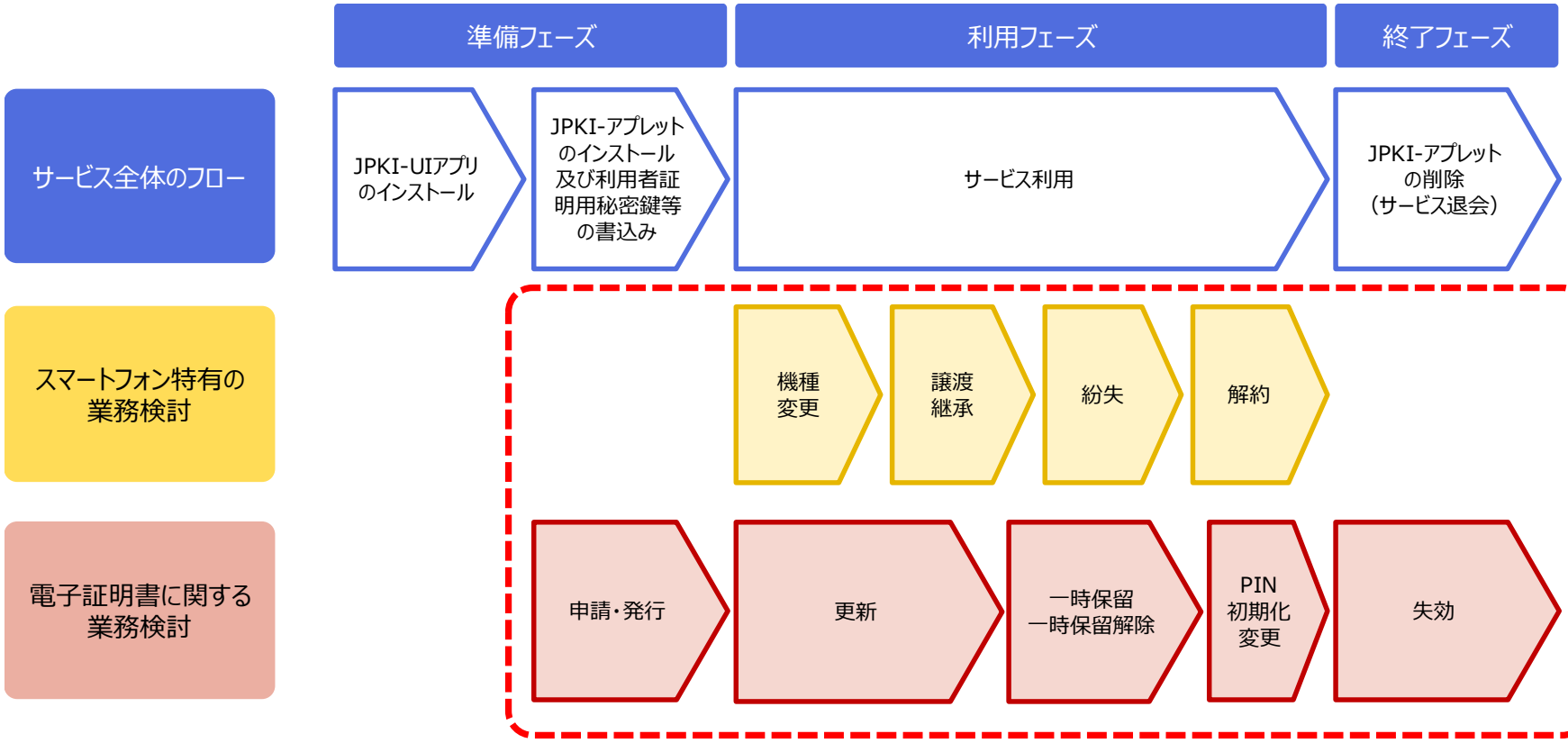
（参考）SP独自のセキュリティ対策

- **SP-TSMとJPKI-アプレット間は、モバイル事業者が提供する方式により、通信データの暗号化を行うことが可能。**
- **更に、秘密鍵、電子証明書の配信におけるセキュリティ対策は強化するため、SP独自の方式によって秘密鍵、電子証明書の暗号化を実施することも可能。**



（参考）運用面での課題検討

- 利用者証明機能をダウンロードするにあたって運用面での課題を整理、検討します。
- スマートフォン特有の業務検討および電子証明書に関する業務検討を実施します。
- 利用者の利便性向上の観点から、マイナンバーカードの署名用電子証明書による署名検証を用いたオンライン本人確認を前提として業務フローを検討し、課題の整理を図ります。



本検討の対象範囲

2－8. MVNO事業者による利用者証明機能ダウンロードにおける課題検討

NTT DATA

- **本実証事業では以下について検討します。**

分類	検討テーマ	概要
技術面	SIMカードとスマートフォンの組合せ調査	MVNO事業者が提供するSIMカード及びスマートフォンを調査し、SIMカードとスマートフォンの組合せ別の課題を整理する。
	MNO既存プラットフォームへの影響範囲	MNO事業者が提供する既存プラットフォーム（MNO-TSMサーバ、SIM、スマホ上のハード／ソフト 等）への影響範囲を整理する。
	サービス事業者側プラットフォームへの影響範囲	サービス事業者が準備すべきプラットフォーム（SP-TSMサーバ、JPKI-UIアプリ、JPKI-アプレット 等）への影響範囲を整理する。
	MVNO事業者側システムへの影響範囲	MVNO事業者が提供するシステム（MVNO-SIM、スマホ上のハード／ソフト 等）への影響範囲を整理する。
	動作保証基準／責任範囲の整理	MNO事業者が提供するモバイルNFCプラットフォームにおける参考として、関係者（利用者、MVNO事業者、MNO事業者、サービス提供者）の動作保証基準/責任範囲を整理する。
	上記課題を踏まえた実現方式の検討	MVNO事業者による実現方式を検討する。
ビジネス面／運用面	MVNO事業者ニーズの分析	MVNO事業者へのヒアリング等を実施し、ニーズを分析する。
	MVNO利用者へのサポート範囲	MVNO事業者、MNO事業者、サービス事業者の責任範囲、サポート範囲を検討する。
	MVNO事業者によるビジネス性の検討	MVNO事業者のニーズを踏まえたビジネス性を検討する。
	運用面の課題検討	上記の検討過程で発生した運用面での課題について検討する。

3. iOS搭載スマートフォンによる公的個人認証サービスの活用

3－1. 検証のポイント

- **iOS搭載スマートフォンへの利用者証明機能ダウンロードを実現する方法を検証**します。

3－2. iPhoneにおける利用者証明機能ダウンロードの検証

- **本実証事業では、以下のiPhoneにおける利用者証明機能のダウンロード方式のうち、②について安全性の確保手段について技術検証を実施する。**
  ①公的個人認証サービスで鍵生成した鍵、証明書を配送する方式
  ②iPhoneで鍵生成する方式