NTT DATA
Global IT Innovator

資料６－４

H28年度「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

2017年7月5日

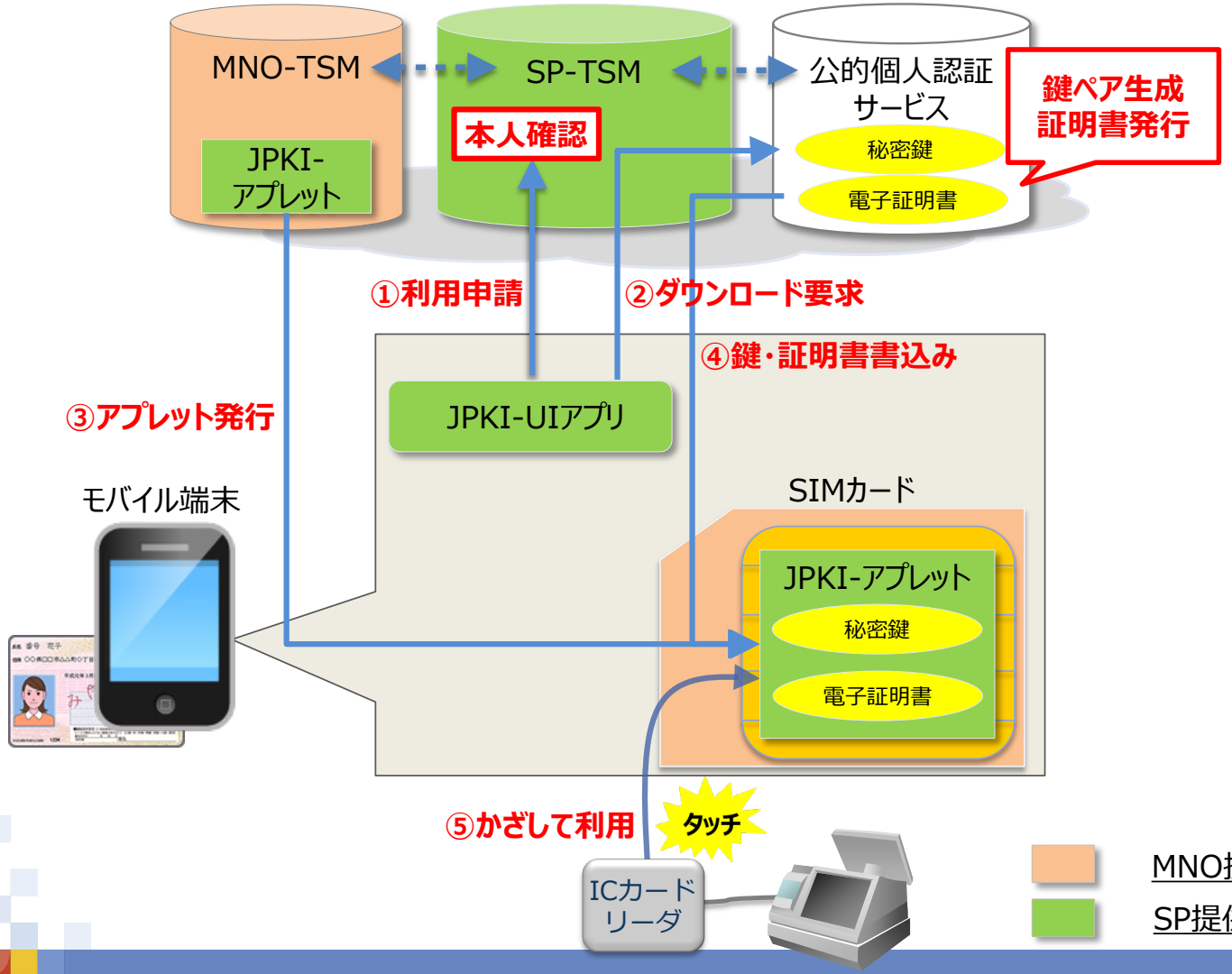
1. 実証内容と実証参加団体

検証項目		実証内容	実証参加団体
技術検証	① SIMカードへの利用者証明機能の書き込み	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。 さらに実用化に向けたビジネスモデルパターン、MVNO事業者展開における課題等を検討	株式会社NTTドコモ KDDI株式会社 ソフトバンク株式会社 地方公共団体情報システム機構 NTTコミュニケーションズ株式会社 大日本印刷株式会社
	② 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	iOSが管理するKeychain領域で鍵ペアを生成し、電子証明書を書き込むことができることを検証	日本IBM株式会社
ユースケース検証	③ チケットレスサービス	チケット申込、購入、入場時の資格確認の一連の手続きにおいて、公的個人認証サービス活用の利便性とニーズを検証	株式会社セブン-イレブン・ジャパン ぴあ株式会社 三井住友カード株式会社 株式会社クレディセゾン NTTコミュニケーションズ株式会社
	④ インターネットバンキング	インターネットバンキングの認証において公的個人認証サービスを提供した実証シナリオを検討	一般社団法人ICTまちづくり共通プラットフォーム推進機構 株式会社群馬銀行

2. 技術検証

2. 1. 技術検証の全体概要
2. 1. 1. Androidスマートフォンへの利用者証明機能ダウンロード（仕組み）

・モバイル通信事業者3社が提供するNFCプラットフォームを活用し、利用者証明機能をスマートフォンにダウンロード。
・公的個人認証サービスで鍵ペア生成、電子証明書発行を行い、SIMカードに秘密鍵及び電子証明書を記録する。



○MNO-TSM※
- MNOの責任範囲の処理を実施するTSMサーバ
- SPのアプレットを預かり、SIMカードへ格納する

○SP-TSM ※
- SPの責任範囲の処理を実施するTSMサーバ(鍵・証明書をアプレットへ書き込む)

○JPKI-UIアプリ
- SPがユーザへ提供するAndroidアプリ
- 利用者が操作し、利用申請等を行う

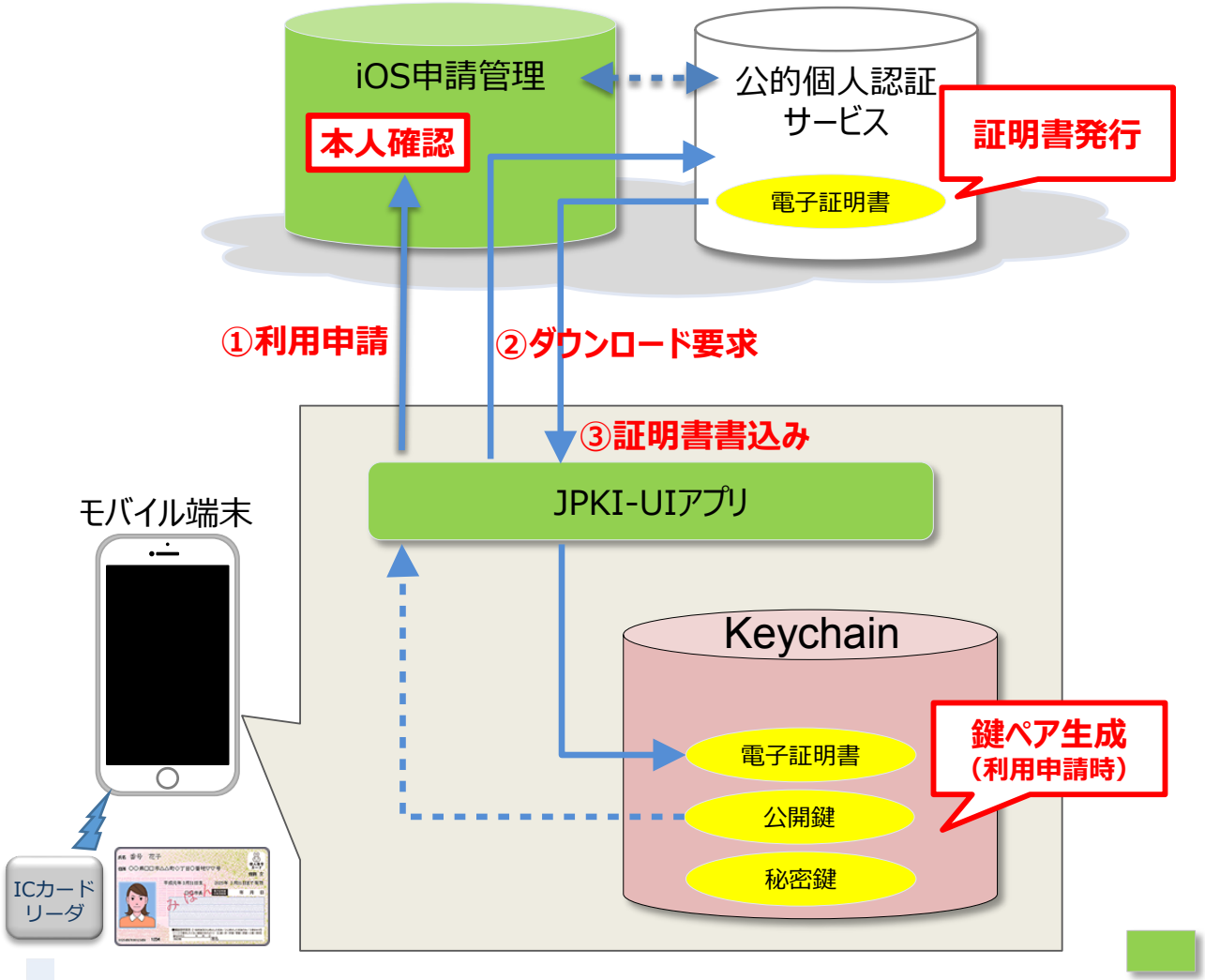
○JPKI-アプレット
- SIMカードに搭載するJavaアプリケーションであり、サービス上必要なSPデータ(鍵・証明書)を保持する

※TSM：Trusted Service Manager

NTT DATA

2. 1. 技術検証の全体概要
2. 1. 1. iOSスマートフォンへの利用者証明機能ダウンロード（仕組み）

・iOSが管理するKeychain領域に秘密鍵及び電子証明書を記録する。
・iOSスマートフォンで鍵ペア生成を行い、公的個人認証サービスで電子証明書を発行する。



○ **iOS申請管理**
- 利用者の申請情報を預かり、公開鍵を公的個人認証サービスに渡す

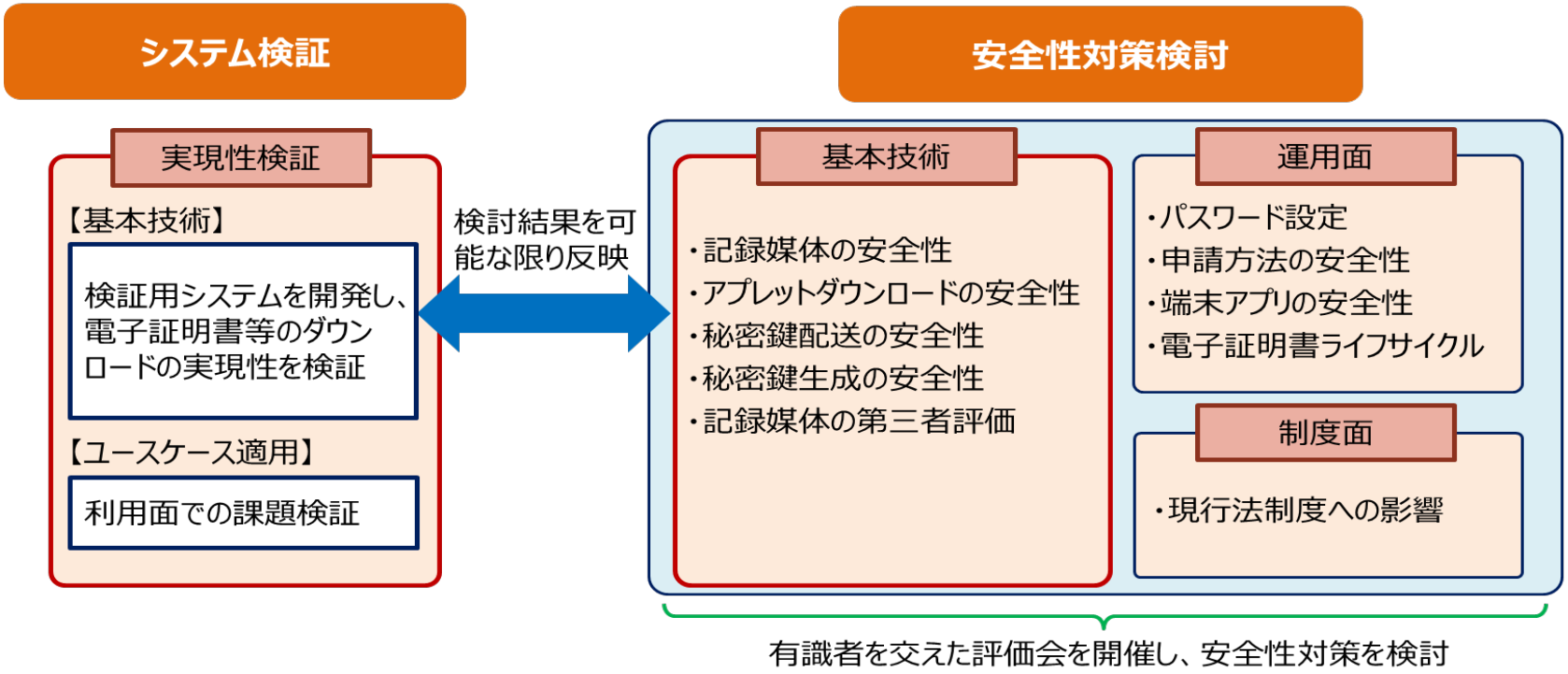
○ **JPKI-UIアプリ**
- SPがユーザへ提供するiOSアプリ
- 利用者が操作し、利用申請等を行う

○ **Keychain**
- iOS内の鍵・証明書の記録領域

SP提供

2. 1. 技術検証の全体概要
2. 1. 3. 検証方法

短期間の実証事業であるため、以下に示す４つの検証作業を並行して進めることとした。



「実現パターンと責任分解」の検討

Androidスマートフォンへの利用者証明機能ダウンロードの実現形態を検討

MVNOによる利用者証明機能ダウンロードにおける課題検討

MVNOがAndroidスマートフォン利用者向けに利用者証明機能ダウンロードサービスを提供するための課題について、ヒアリング及びアンケートを実施し、検討

・SP-TSM、JPKI-UIアプリ、JPKI-アプレットを開発し、システム検証を実施し、ダウンロードの有効性を検証した。
・ユースケースとして、チケットレスサービスの入場時に利用者証明検証を行い、動作検証を実施した。

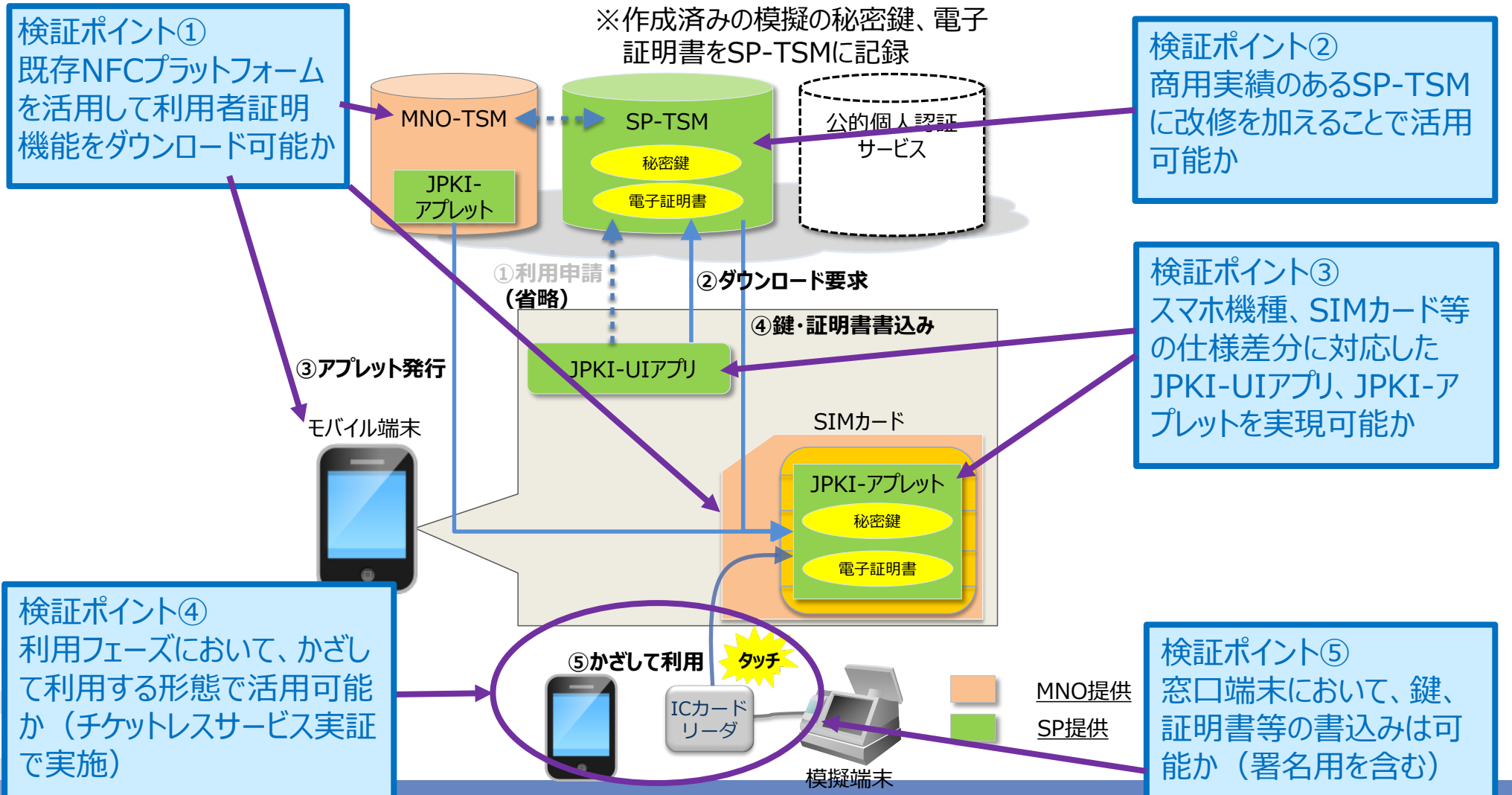
検証ポイント①
既存NFCプラットフォームを活用して利用者証明機能をダウンロード可能か

検証ポイント②
商用実績のあるSP-TSMに改修を加えることで活用可能か

検証ポイント③
スマホ機種、SIMカード等の仕様差分に対応したJPKI-UIアプリ、JPKI-アプレットを実現可能か

検証ポイント④
利用フェーズにおいて、かざして利用する形態で活用可能か（チケットレスサービス実証で実施）

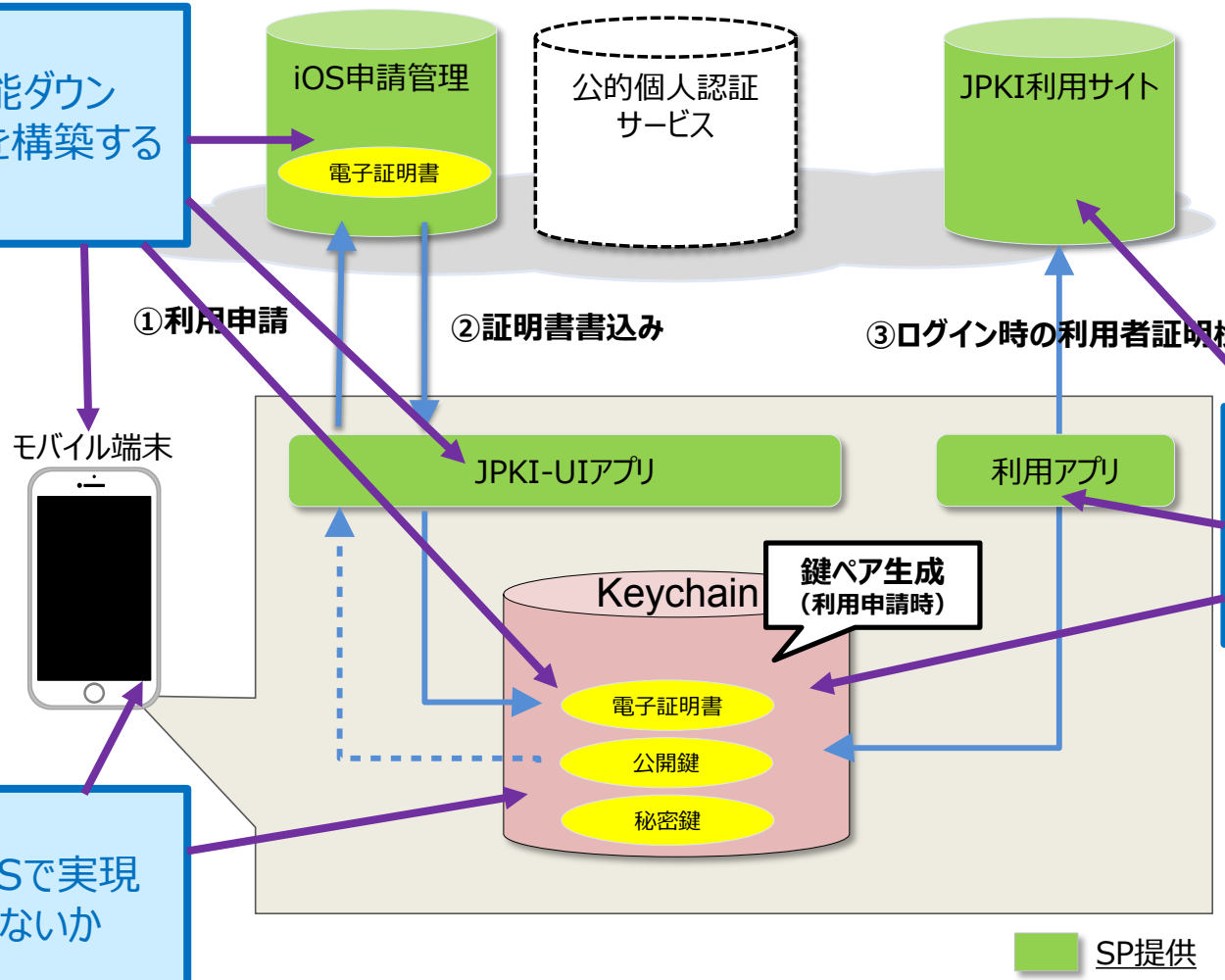
検証ポイント⑤
窓口端末において、鍵、証明書等の書込みは可能か（署名用を含む）



#	検証ポイント	検証結果	今後の課題
①	既存NFCプラットフォームを活用して利用者証明機能をダウンロード可能か	モバイル通信事業者3社のNFCプラットフォームに影響を与えることなく、そのまま活用できた。	特に無し
②	商用実績のあるSP-TSMに改修を加えることで活用可能か	クレジット事例で商用実績のあるSP-TSMに対して、公的個人認証サービスに固有の部分を追加することで利用者証明機能ダウンロードを実現できた。	SP-TSMはSIMカードへのデータ書込み処理に特化しているため、利用申請時の署名検証等、SIMカードへのデータ書込み以外の処理はSP-TSMとは別システムでの実現が望ましい。
③	スマホ機種、SIMカード等の仕様差分に対応したJPKI-UIアプリ、JPKI-アプレットを実現可能か	モバイル通信事業者3社のスマホ（各社1機種）、SIMカード（各社）にて実現性を確認できた。	実用化に向けてはサービス対象とするSIMカード及びスマートフォン機種での動作検証が必要。
④	利用フェーズにおいて、かざして利用する形態で活用可能か（チケットレスサービス実証で実施）	チケットレスサービスの入場時における利用者証明検証について、スマートフォンをかざして利用する形態で実現できた。	かざし位置が利用者にとって分かり難いため、音や触覚（バイブ）の活用等工夫が必要。 現在、窓口端末で使用されている既設ICカードRWとスマートフォンの組合せで動作しないものがあった。 実用化に向けてはサービス対象とするスマートフォン機種での動作検証が必要。
⑤	窓口端末において、鍵、証明書等の書込みは可能か（署名用を含む）	市町村窓口の窓口端末の処理をテスト環境で実施し、スマートフォンのかざして利用する形態で鍵、証明書の書込みが確認できた。 また、利用者証明用電子証明書だけでなく署名用電子証明書等の格納も実現可能であることを確認した。	

・iOS申請管理、JPKI-UIアプリを開発し、システム検証を実施し、ダウロードの有効性及び性能を確認した。
・ユースケースとして、Webサイトのログイン時に利用者証明検証を行うシステムを開発し、動作検証を実施。

検証ポイント①
利用者証明機能ダウンロードの仕組みを構築することは可能か



検証ポイント③
利用フェーズにおいて、ログイン時の利用者証明検証を実現可能か

検証ポイント②
鍵ペア生成をiOSで実現し、性能上問題ないか

#	検証ポイント	検証結果	今後の課題
①	利用者証明機能ダウンロードの仕組みを構築することは可能か	iOS申請管理、JPKI-UIアプリを開発し、iOSスマートフォン内での鍵ペア生成、利用申請、電子証明書ダウンロードの一連の処理が実現できることを確認した。 但し、利用申請時において現状ではiOS用のICカードRWが存在しないため、これに関連する処理は省略した。	実用化に向けてはiOS用のマイナンバーカードに対応したICカードRWが必要。
②	鍵ペア生成をiOSで実現し、性能上問題ないか	iOSの機能を使って、鍵ペアが実用上問題ない時間内で実現できることを確認した。	特に問題なし。
③	利用フェーズにおいて、ログイン時の利用者証明検証を実現可能か	利用サイト、iOS用利用アプリを作成し、Keychain内に秘密鍵、電子証明書が格納された状態で、利用サイトへのログイン処理における利用者証明検証が可能であることを確認した。	業務用アプリからKeychain領域へのアクセス方法について検討する必要がある。 【補足資料B-3:安対03】

2. 3. 利用者証明機能ダウンロードに関する安全性評価
2. 3. 1. 評価会の開催（Androidスマートフォン）

- 評価会を開催し、SIMカードへの利用者証明機能ダウンロードの安全性対策について検討した。
- SIMカードの利用者証明機能ダウンロードでは、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の活用を前提とすることから、モバイル通信事業者から前記プラットフォームの情報提供を受け、評価会参加者とは機密保持契約を締結した上で評価会を実施した。

役割	企業・団体等	作業内容
評価者	・慶應義塾大学　手塚特任教授 ・東京工業大学　小尾准教授 ・地方公共団体情報システム機構	安全性対策の評価
説明者	NTTデータ、NTTコミュニケーションズ、大日本印刷	評価会運営、安全性対策の調査・検討、報告書作成
オブザーバ	総務省、NTTドコモ、KDDI、ソフトバンク	

#	主な議題	開催日時
第1回	・利用者証明機能ダウンロードにおけるSP領域の安全性、アプレットダウンロードの安全性、秘密鍵配送の安全性 ・SP独自の安全性対策（コンテンツ暗号化対策）	2016年11月30日（水） 9：30～12：00
第2回	・申請方法の安全性対策 ・利用者証明用パスワード設定に関する安全性対策 ・SIMカードのセキュリティ評価	2017年1月23日（月） 13：00～15：30
第3回	・端末アプリの安全性対策 ・証明書関連業務及びスマートフォン特有の業務検討 ・法整備に関する論点整理	2017年3月22日（水） 13:00～16:00

2. 3. 利用者証明機能ダウンロードに関する安全性評価
2. 3. 1. 評価会の開催（iOSスマートフォン）

- 評価会を開催し、iOSスマートフォン内の「Keychain」に秘密鍵や電子証明書を保管する際の脅威の洗い出しと対策を検討した。
- 脅威に対してiOSスマートフォン自体、第三者、アプリケーションで実施する安全対策を検討し、その安全対策が利用者証明用電子証明書を利用する為の申請・ダウンロード・利用処理プロセスの中でどの様に有効に作用しているのか検討。

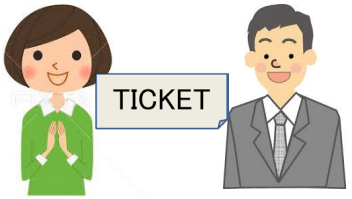
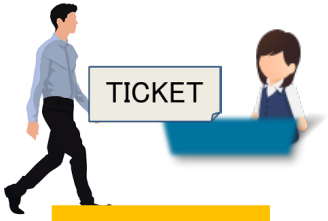
役割	企業・団体等	作業内容
評価者	・慶應義塾大学　手塚特任教授 ・東京工業大学　小尾准教授 ・地方公共団体情報システム機構	安全性対策の評価
説明者	日本アイ・ビー・エム	評価会運営、安全性対策の調査・検討、報告書作成
オブザーバ	総務省、NTTデータ	

#	主な議題	開催日時
第1回	・iOSスマートフォンに公的個人認証情報を保管・利用する際の安全性対策について	2017年1月23日（月） 15:30～17:00
第2回	・iOSスマートフォンにて利用者証明書を利用する為の申請・ダウンロード・利用処理と安全対策との関係について ・公的個人認証法対応について　記録媒体別整理（iOSスマートフォン）	2017年3月6日（月） 9:30～11:30
第3回	・iOSスマートフォンからの申請をAPNsを用いて確認する方法 ・法整備に関する論点整理	2017年3月22日（水） 16:00～17:30

3. ユースケース検証

3. 1. チケットレスサービス
3. 1. 1. 実証背景

- 平成27実証(チケットレスでの入場実証)の課題、①申込から購入、入場の一連の手続き、②同行者へのチケット受渡についてマイナンバーカード、スマートフォンを活用して検証した。

	申込	購入	同行者へのチケット受渡	入場
これまで	パソコンから ID/ﾊﾟｽﾜｰﾄﾞで チケット申込	クレジットカードで 決済	同行者の確認が できていない	チケットと本人確認書類 をスタッフへ提示
				
	チケット申込時の 本人確認の実現	決済時の 強固な本人確認	同行者の 本人確認を実現	スムーズな 入場
これから				
	ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞで チケット申込 (厳格な本人確認)	ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞで 決済	ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞで 本人確認	ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞ/ｽﾏｰﾄﾌｫﾝを 読取機にかざし入場

NTT DATA

3. 1. チケットレスサービス
3. 1. 2. 実証内容

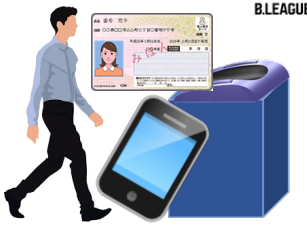
実証内容

- ✓ 申込では、利用者はスマートフォンにマイナンバーカードをかざし、チケットを申込
- ✓ 購入では、コンビニ店舗にてレジのカード読取機にマイナンバーカードをかざし、クレジット決済を実施
- ✓ 利用者は同行者へチケット譲渡を実施、同行者はスマートフォンにマイナンバーカードをかざし、チケットを受け取る
- ✓ 利用者及び同行者は、入場ゲートのカード読取機にマイナンバーカードをかざし、チケット情報を確認し入場
- ✓ また入場では、実証用スマートフォンを入場ゲートのカード読取機にかざし、チケット情報を確認し入場

実証結果

- ✓ チケットの申込、購入、入場の一連の手続きでのマイナンバーカード活用について、利用者ニーズが高いことを確認
- ✓ 同行者についても、譲渡時、入場時にマイナンバーカードによる確実な本人確認ができることを確認
- ✓ マイナンバーカードの利用者証明書をPIN入力をしないでオンラインで検証する本人確認（PINなし認証）を実現
- ✓ マイナンバーカードの代わりにスマートフォンで、利用者証明機能が利用できることを確認（PINあり認証）

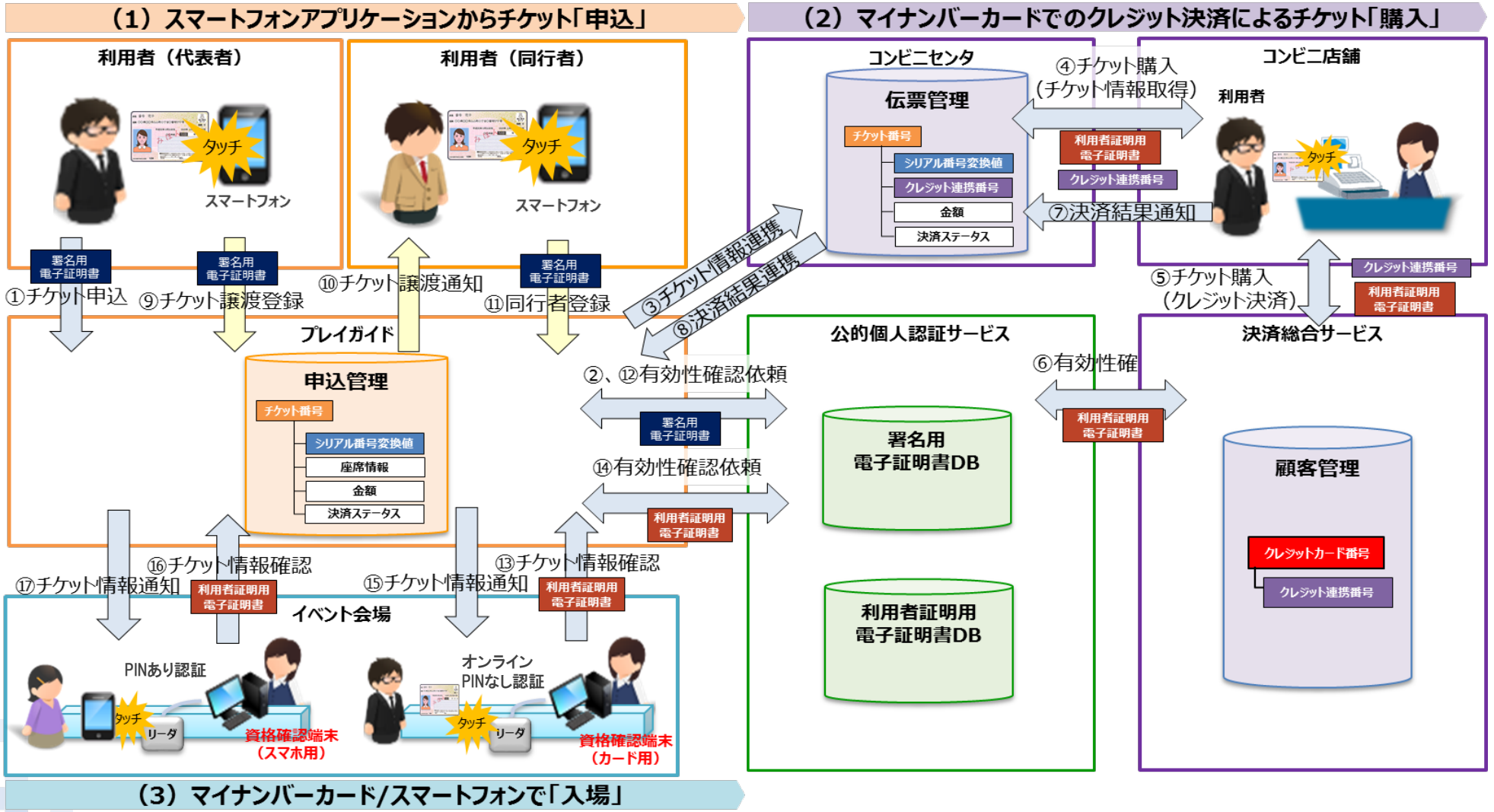
実証イメージ

申込	購入	同行者へのチケット受渡	入場
			
スマートフォンから ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞを使って チケット申込	コンビニ店舗で ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞを使って クレジット決済で チケット代支払い	スマートフォンで ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞを使って チケット受取	ﾏｲﾅﾝﾊﾞｰｶｰﾄﾞ/ｽﾏｰﾄﾌｫﾝを 読取機にかざし入場

フィールド実証	実証場所	モニタ数　※アンケート対象	実証日
申込	ぴあ社会議室	24名　※同行者を含む	2/7（火）
購入	セブン-イレブン店舗（虎ノ門タワーズオフィス店）	11名　※同行者は購入対象外	2/26（日）
入場	代々木第二体育館（Bリーグ　アルバルク東京vs大阪エヴェッサ）	22名	3/11（土）

3. 1. チケットレスサービス
3. 1. 3. 実証フロー

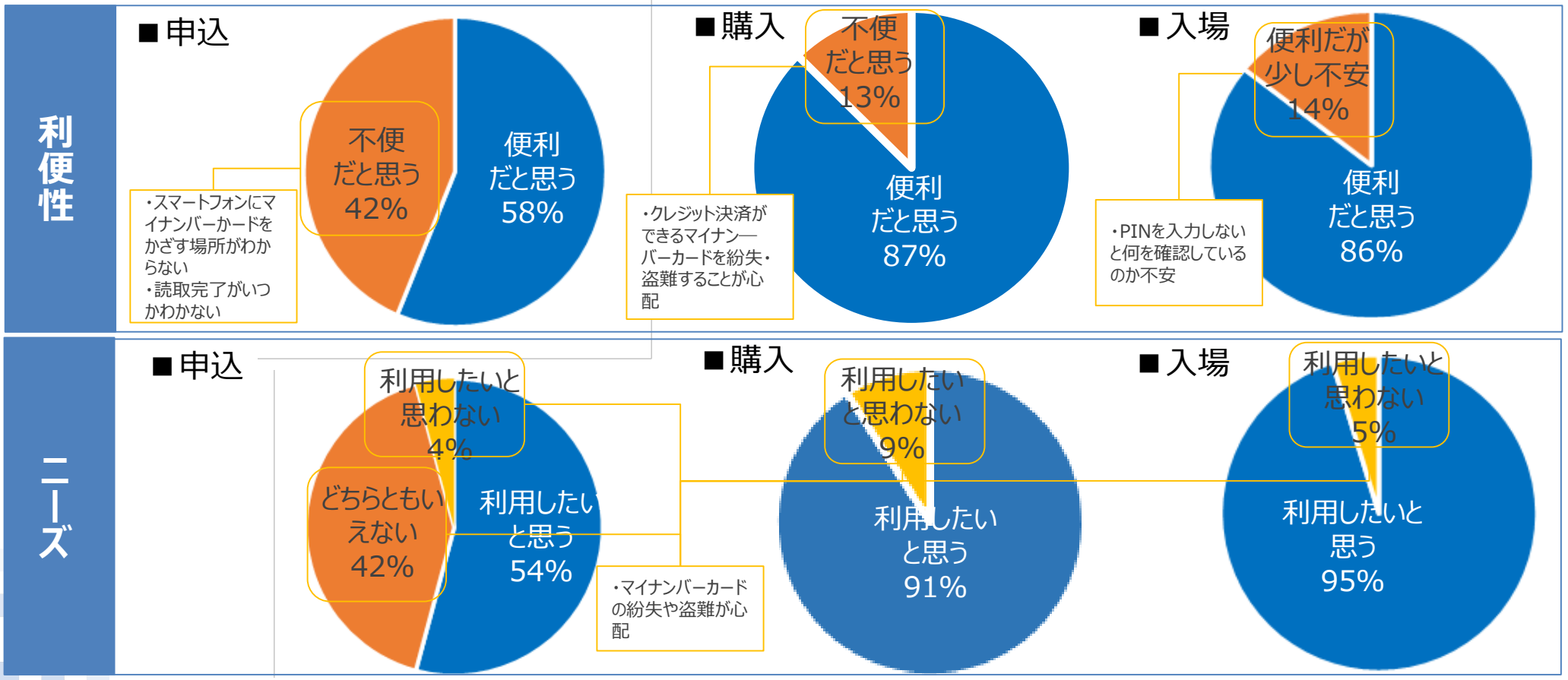
- チケットレスサービスのフローは以下の通り。



NTT DATA

3. 1. チケットレスサービス
3. 1. 4. アンケート結果

- マイナンバーカードを活用したチケットレスサービスについて、購入や入場では多くの利用者が「便利」「利用したい」との評価を得た。
- 実用化に向けた課題は、スマートフォンでマイナンバーカードを読み取るアプリケーションのユーザインタフェースの改善、利用者へのPINなし認証の説明やマイナンバーカード持ち歩きへの不安解消である。



NTT DATA

3. 1. チケットレスサービス
3. 1. 5. 今後の課題

項番	課題	内容
①	スマートフォンでマイナンバーカードを読み取るアプリケーションのユーザインタフェースの改善	スマートフォンにマイナンバーカードをかざす場所や、読取完了の通知など、利用者の利便性を高めたアプリケーションのユーザインタフェースを検討する必要がある
②	利用者へのPINなし認証の説明	PINの保管場所やPINなしで処理されることへの不安の声があった。PINなし認証の利用目的や条件などについて利用者への説明を行う必要がある
③	マイナンバーカード持ち歩きへの不安解消	マイナンバーカードの盗難や紛失への不安が依然として高い。マイナンバーカードの代わりに、普段持ち歩くスマートフォンなどに利用者証明機能を実現したり、マイナンバーカードを持ち歩くメリットを享受できるサービスを実現する必要がある。

3. 2. インターネットバンキング
3. 2. 1. 実証内容

実証内容

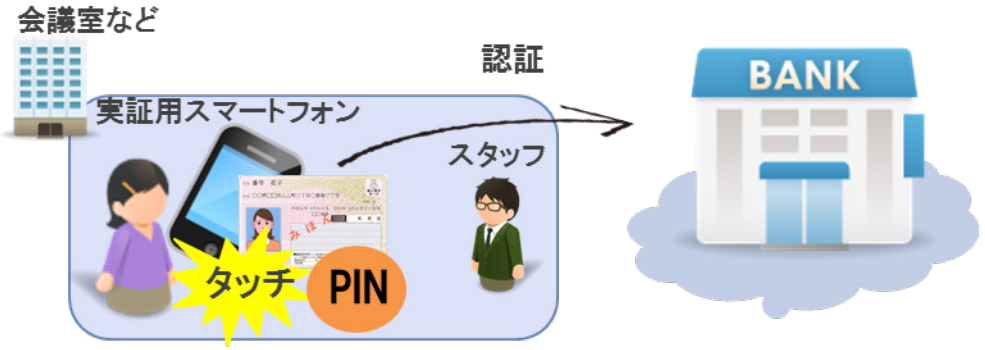
✓ インターネットバンキングへのログインについて、スマートフォンにマイナンバーカードをかざすことで認証できる仕組みを構築するため、利用者の利便性等を検証する実証シナリオを検討

検討シナリオ

実証	実証概要	住民モニター数(予定)
貸出実証	モニターに実証用スマートフォンを貸し出し、日常生活のなかで、実証システムにアクセスし、マイナンバーカードを用いた利用者登録及び認証を体験いただく。 なお実証データ（残高、入出金明細）は貸出実証中に1回更新を行う。	10-20名
会場実証	モニターに実証用スマートフォンを実証会場で操作していただき、マイナンバーカードを用いた利用者登録及び認証を体験いただく。	80-90名

貸出実証
2週間の日常生活の様々なシーンで体験

会場実証
会議室等でスタッフから説明を受けながら体験



検討会	議題	開催日
1回目	・実証スケジュールについて ・実証の内容についての確認 ・課題管理表に基づく課題の共有と確認 ・ワンタイムパスワードとＪＰＫＩのセキュリティ面の比較	12/21（水）
2回目	・平成28年度事業　報告書の確認 ・モニター募集で使用する申込書同意書の確認 ・意見交換	3/3（金）

NTT DATA

Global IT Innovator