

第6回 社会情報流通基盤研究センター・シンポジウム

医療保険の資格確認における 公的個人認証サービスの活用に関する考察

平成28年4月22日

東京工業大学 科学技術創成研究院

社会情報流通基盤研究センター

福田 賢一

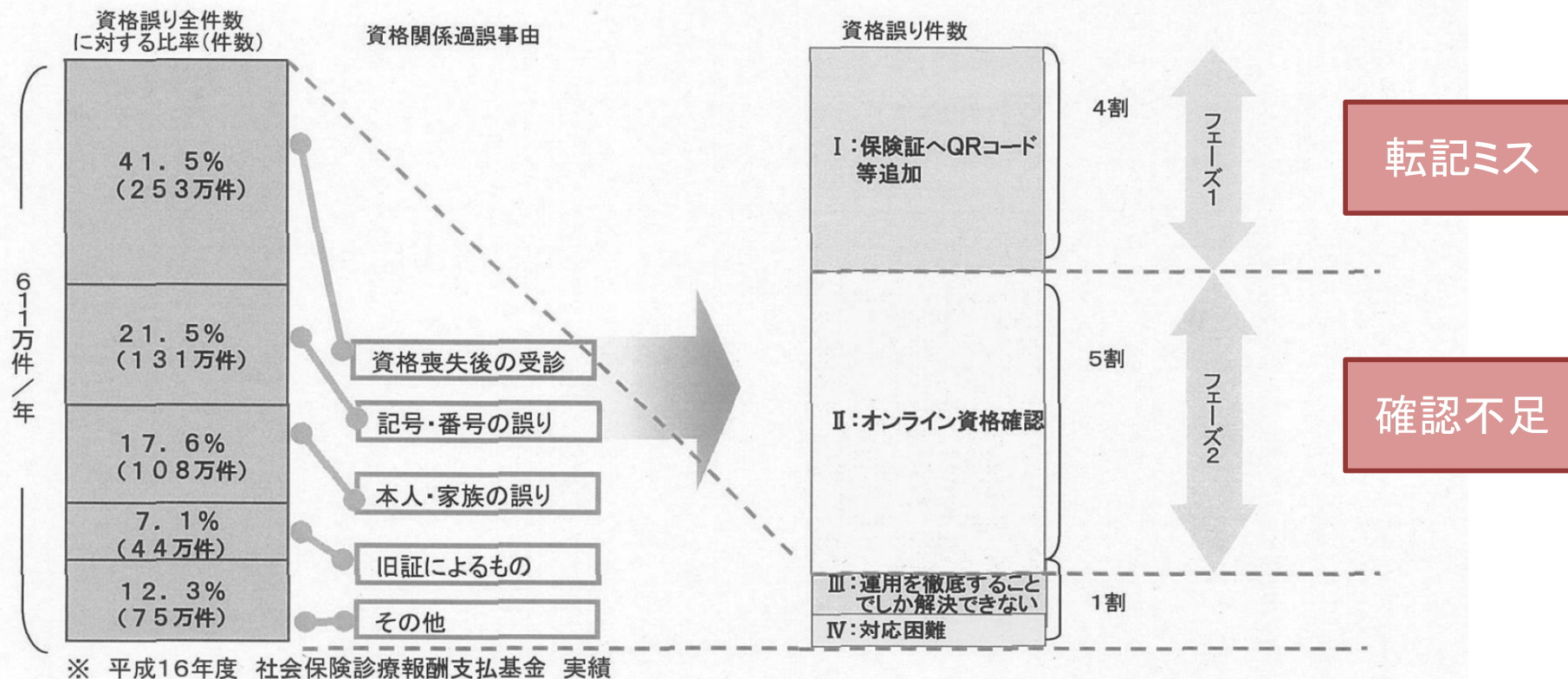
はじめに

- 社会保障・税番号制度が開始。行政の効率化と、国民の利便性を高めることが、その目的。
- 個人番号の医療分野での活用は、健康保険法や介護保険法による保険給付、保険料の徴収等に関する事務等に限定。
(全国健康保険協会、健康保険組合、共済組合等が業務の一部に利用可能。)
- 民間分野への利用の拡大については、マイナンバー法施行後3年を目途に検討することとされているところ。
- 他方、個人番号カードに搭載された新たな公的個人認証サービス(JPKI)は、一定の要件を満たす民間事業者も利用可能。
- これを医療保険の資格確認に用いる方法について考察。

医療保険制度の適正かつ効率的な実施

- 医療保険の資格確認は、国民が円滑かつ確実に保険給付を受けられるための重要な手続き。
- その中心となる機能は、患者個人と、その人に適用される医療保険の資格情報を紐付けること。
 - 個人認証 + 医療保険資格情報データベース
- 医療保険制度を適正に実施するためには、個人認証を厳格に行うことが不可欠。
 - 別途、本人受診のエビデンスを残す用途も考えられる。
- オンラインで行うことにより、リアルタイムでの資格情報反映・取得が可能となり、確実な資格確認が可能。

レセプトの約0.5%が返戻、しかし削減可能



フェーズ1 QRコード等を保険証に追加することにより、資格過誤レセプトは、 **約4割** 削減可能

フェーズ2 被保険者登録状況のオンライン照会の仕組みを構築することにより、資格過誤レセプトは、
約5割 削減可能

具体的な仕組みのイメージ

被保険者証を個人カード化し、その券面に被保険者証の記載事項の一部をコンピュータに簡便に読みとれるように加工したものを共通の仕様により装着する。

資格過誤によるレセプト返戻の解消対策だけを考えて、

- 2次元コード(QRコード)が必要かつ十分な機能を有し、
- ICチップはオーバースペックであるが、
- 医療・介護・年金等を通じた総合的なICチップを装着したカードが導入されるのであれば、このICカードに必要な機能を盛り込めば足りることとなる。

個人番号カード

個人番号カードに搭載された新しいJPKIでは、

- 電子署名用証明書に加え、利用者証明用電子証明書も搭載。
 - 電子署名用証明書には4情報が記されている。
 - 利用者証明用電子証明書には4情報は含まれていない。
- 一定の要件を満たせば、民間企業等も署名検証者になれる。
 - 本年2月12日に民間事業者3社が総務大臣認定を受けた。
- PINなしで利用者証明用電子証明書を利用できる仕組みを搭載。
 - PINありとPINなしを利用場面に応じて選択可能。

厚生労働省が具体的な仕組みを提示

1. 支払基金と国保中央会による資格確認サービスが資格情報を管理。
2. 資格確認サービスは、被保険者の機関別符号を予め取得。
3. 被保険者は受診の際に個人番号カードを提示。
4. 保険医療機関等では、個人番号カードの顔写真と名前により本人確認を行い、電子証明書を資格確認サービスに送付し、資格情報を要求。その際、PINの入力を必要としない本人確認の方法を検討。
5. 資格確認サービスは地方公共団体情報システム機構に対し電子証明書に対応する機関別符号を照会。2.の情報と突き合わせて、電子証明書と対応する機関別符号と資格情報を一対一の関係で管理。
6. 以後、保険医療機関等から資格情報の要求があった場合、地方公共団体情報システム機構に対して電子証明書の有効性のみを照会・確認し、資格情報を通知。

BPMNで可視化

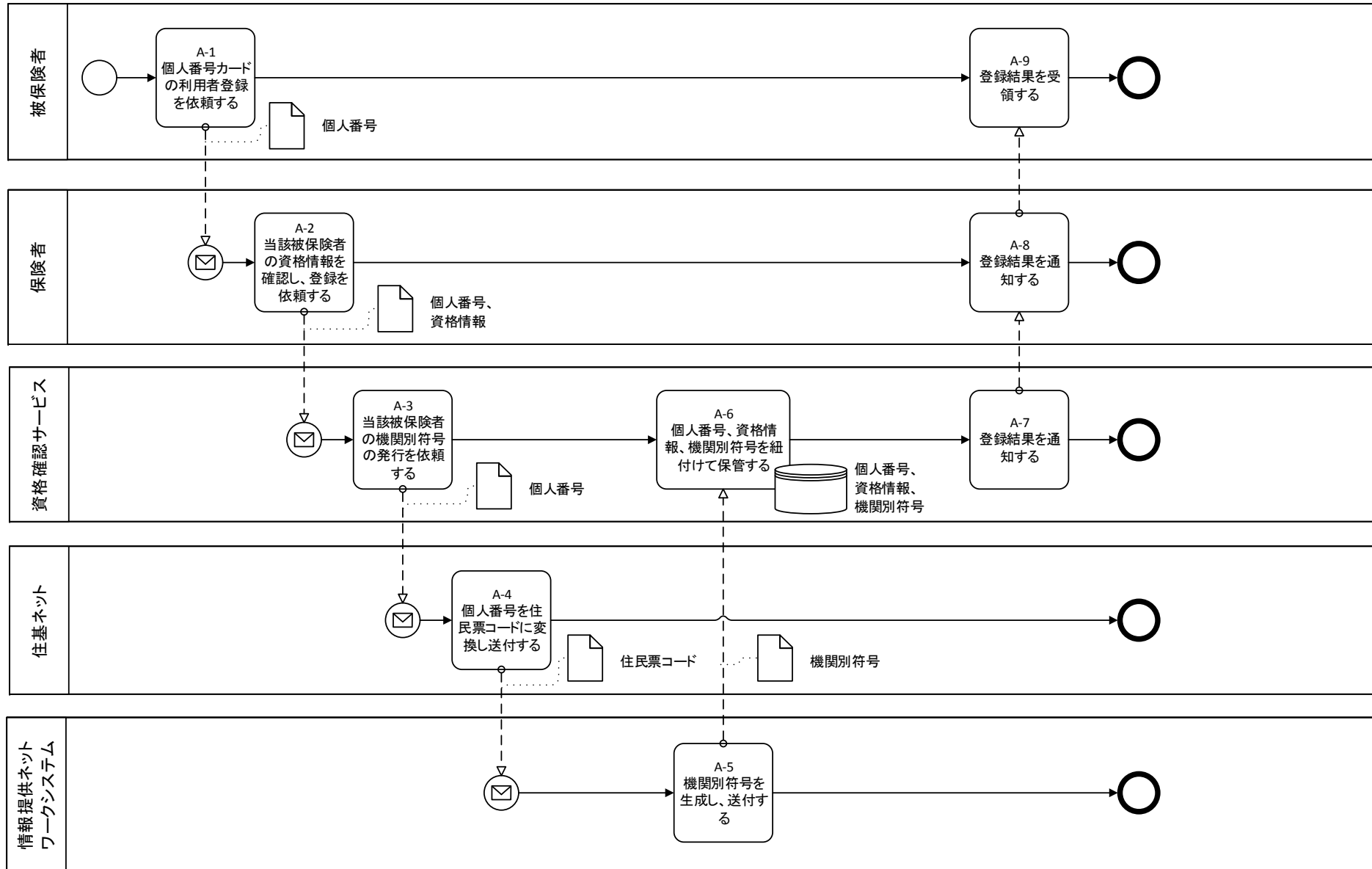
- 今般示されたオンライン資格確認の仕組みについて、手続きの流れを明確にするとともに、改良の余地を議論するため、BPMNで可視化。

(BPMN : Business Process Modeling and Notation)

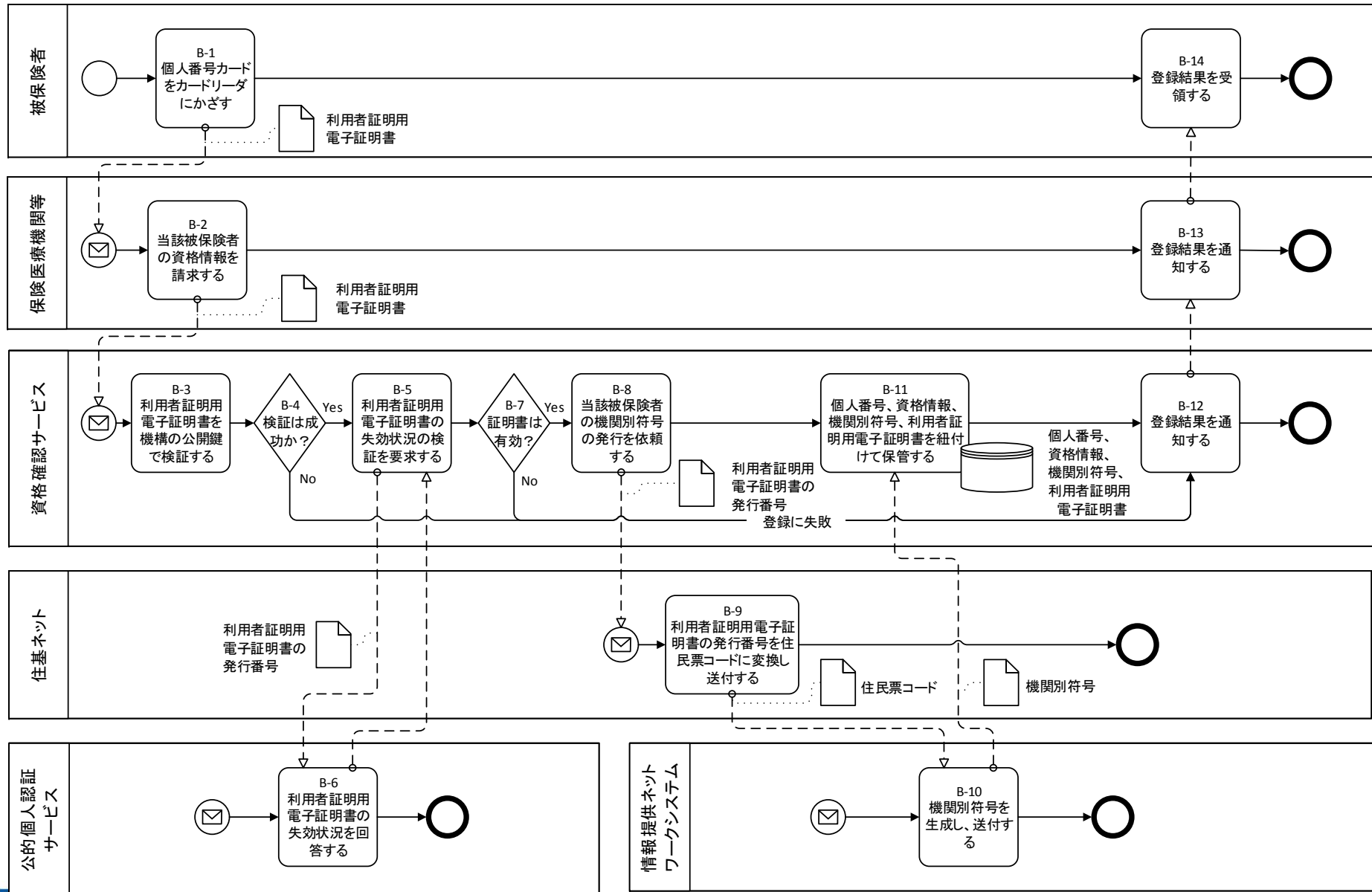
- BPMNを用いた理由は、次の2点。
 - 技術的な専門知識に詳しくない者でも理解しやすいこと。
 - 国際標準として記法が確立しており、調達仕様書での利用に適していること。

(業務フローを明確に示した調達仕様書は、ベンダーロックインの回避、参入機会の拡大、競争促進等に寄与することが期待。)

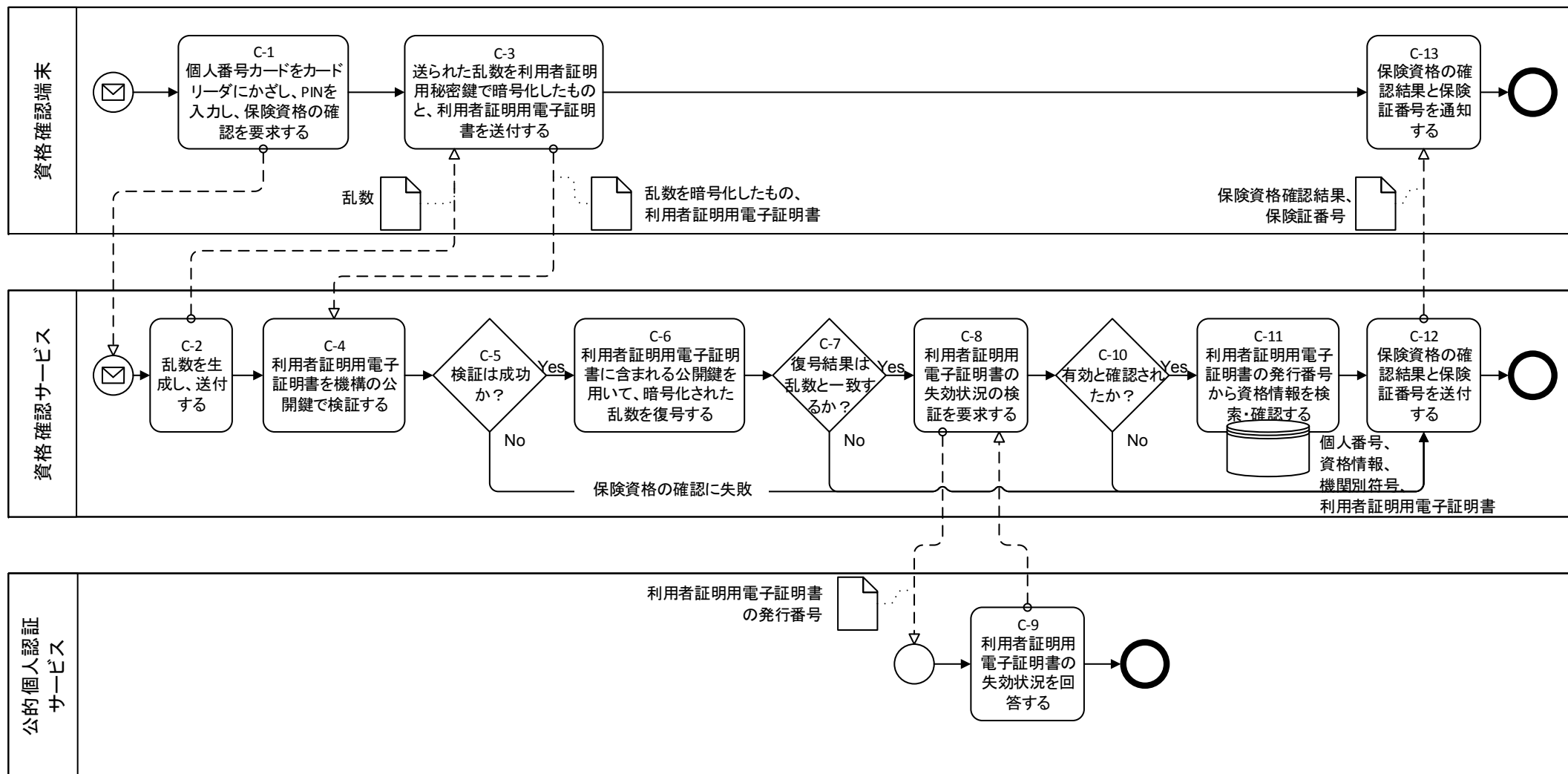
A. 機関別符号の登録



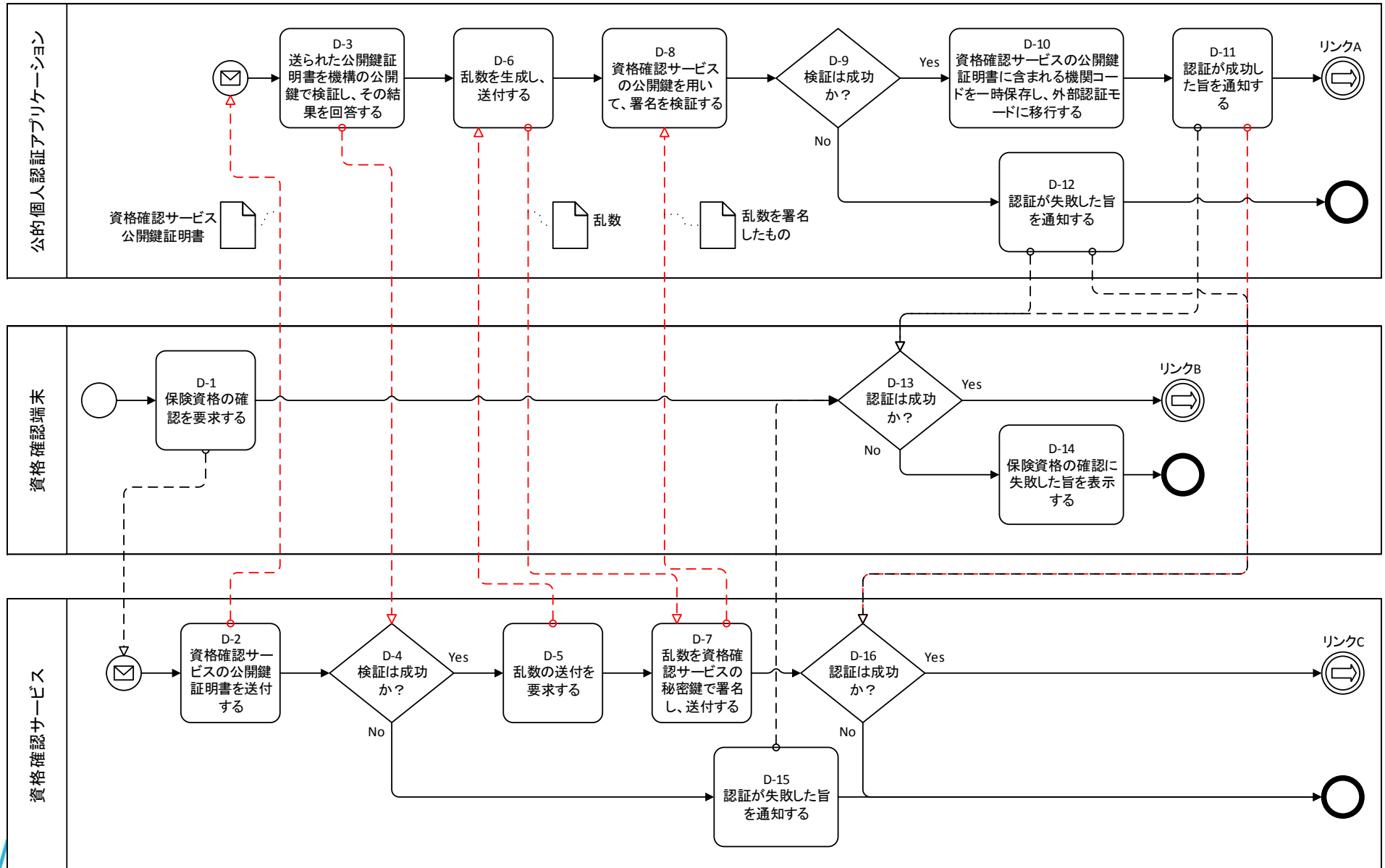
B. 電子証明書と資格情報の突合



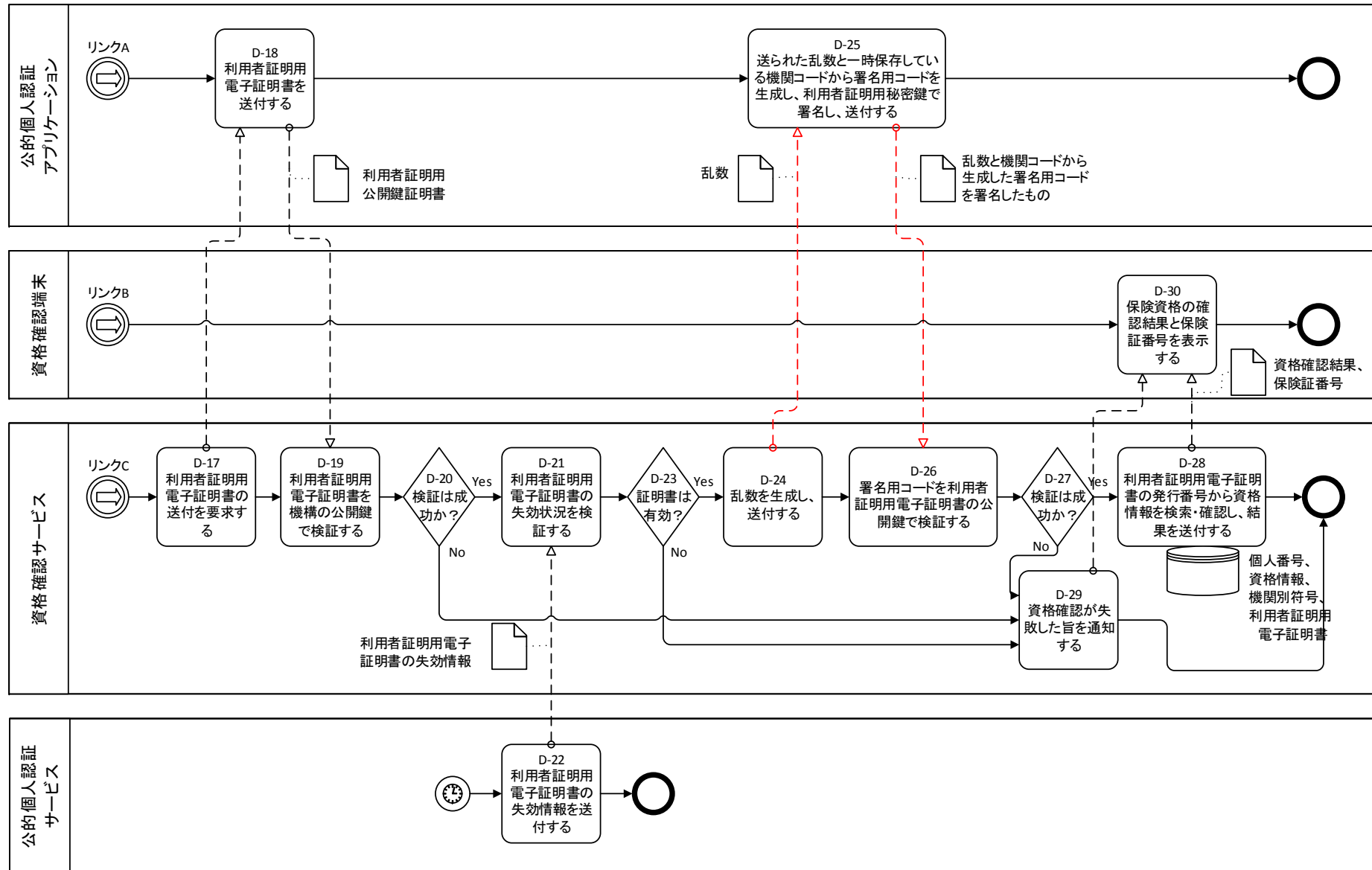
C. 受診時の資格確認



D. 受診時の資格確認: PINなし (1/2)



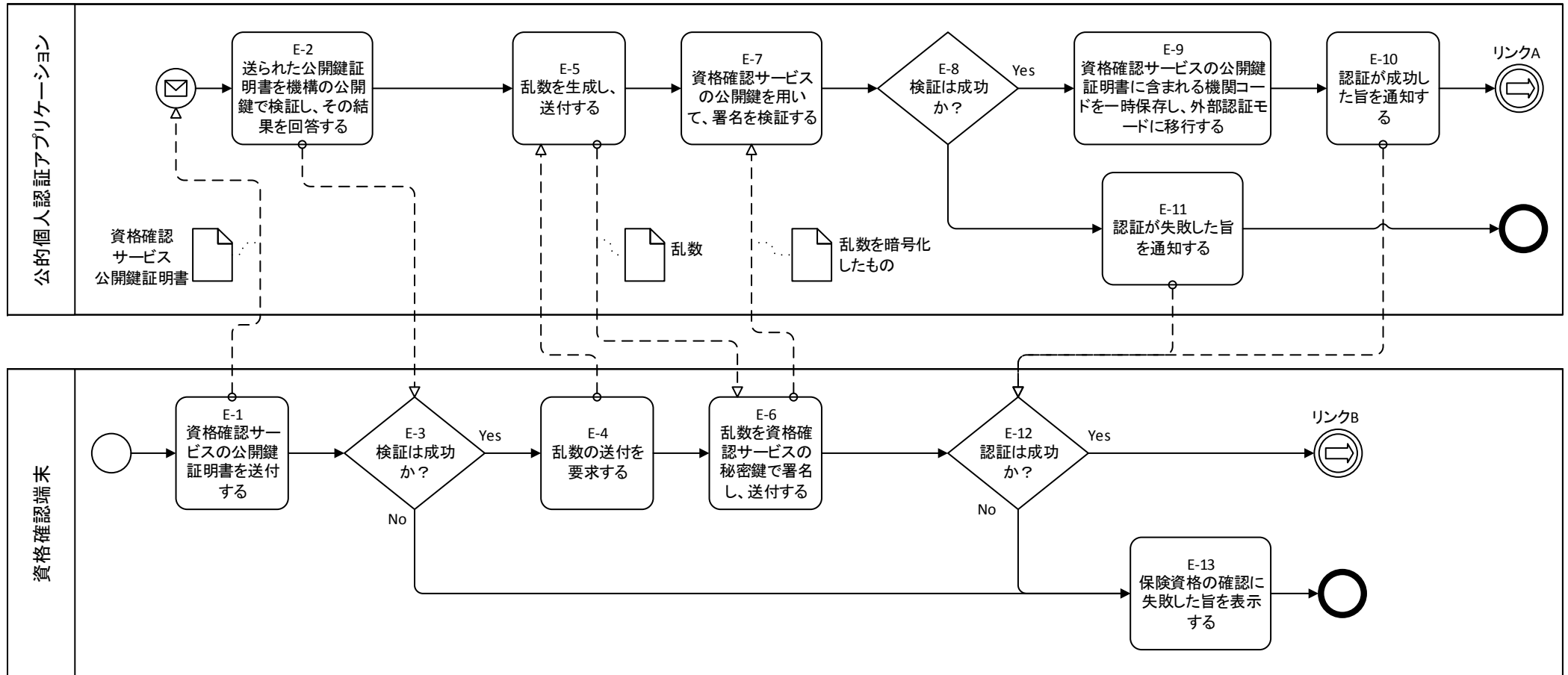
D. 受診時の資格確認: PINなし (2/2)



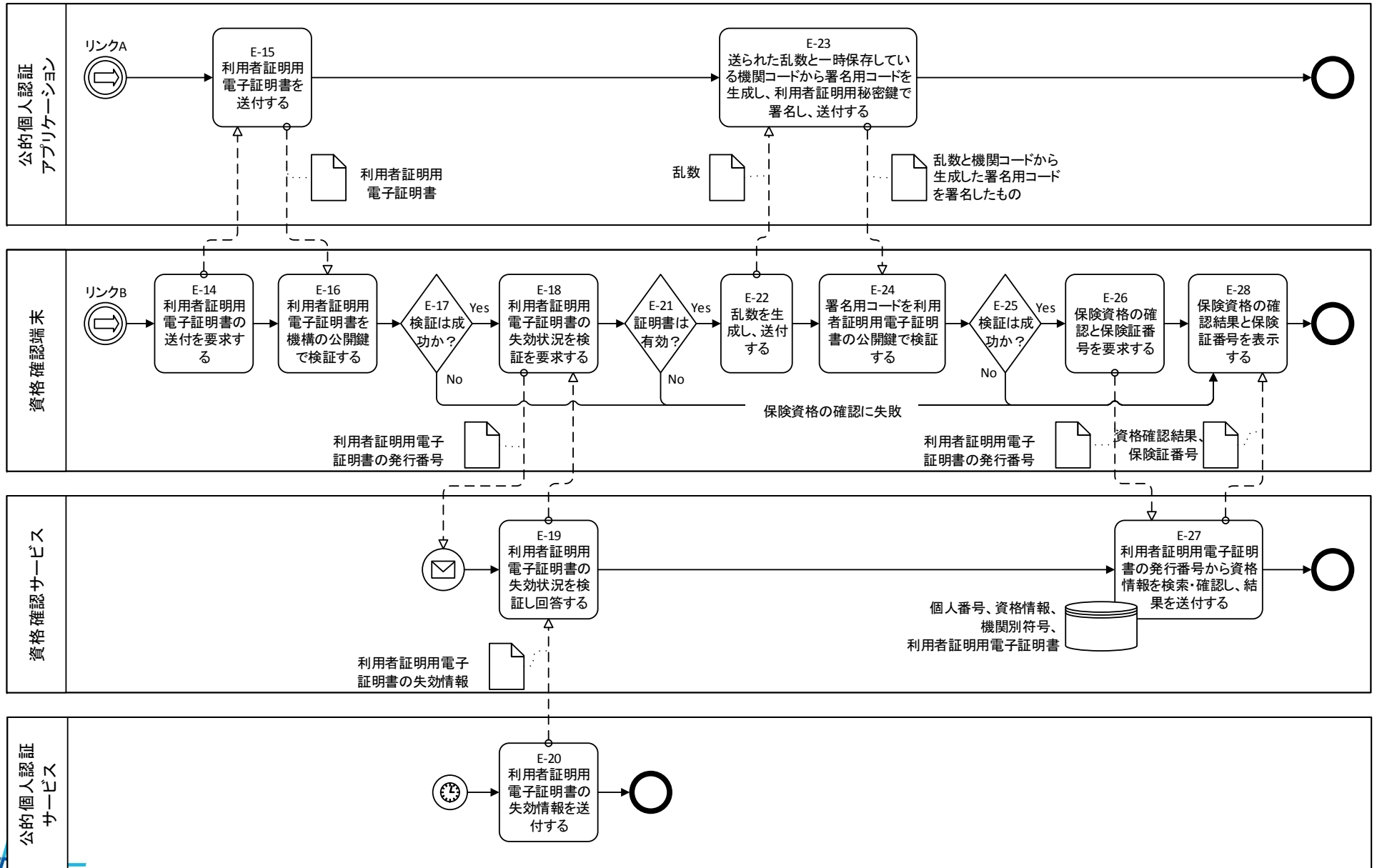
資格確認端末がローカルに処理

- 公的個人認証アプリケーションと資格確認サービスの間で多数回の通信。
 - 資格確認に要する時間が長くなる。
 - 資格確認サービスに多大な処理能力が必要で、コスト高。
 - 通信料金が高額。
- この通信の多くは個人番号カードと資格確認サービスの正当性を確認するためのもの。これを資格確認端末でローカルに実施すれば、通信の削減が可能。
- 資格確認サービスの公開鍵証明書と秘密鍵、機構の公開鍵を資格確認端末に持たせれば、実現可能。

E. 資格確認端末がローカルに処理 (1/2)



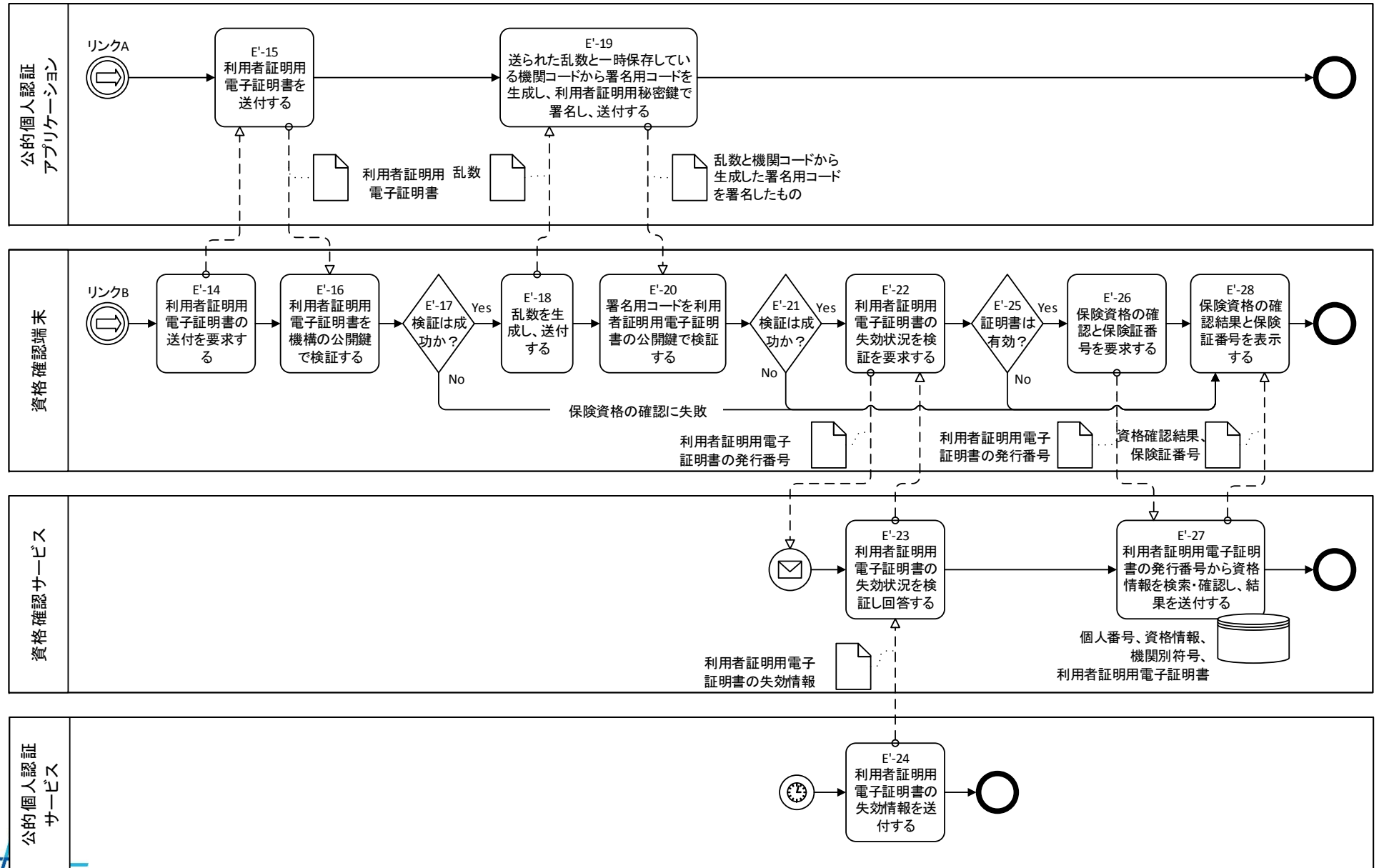
E. 資格確認端末がローカルに処理 (2/2)



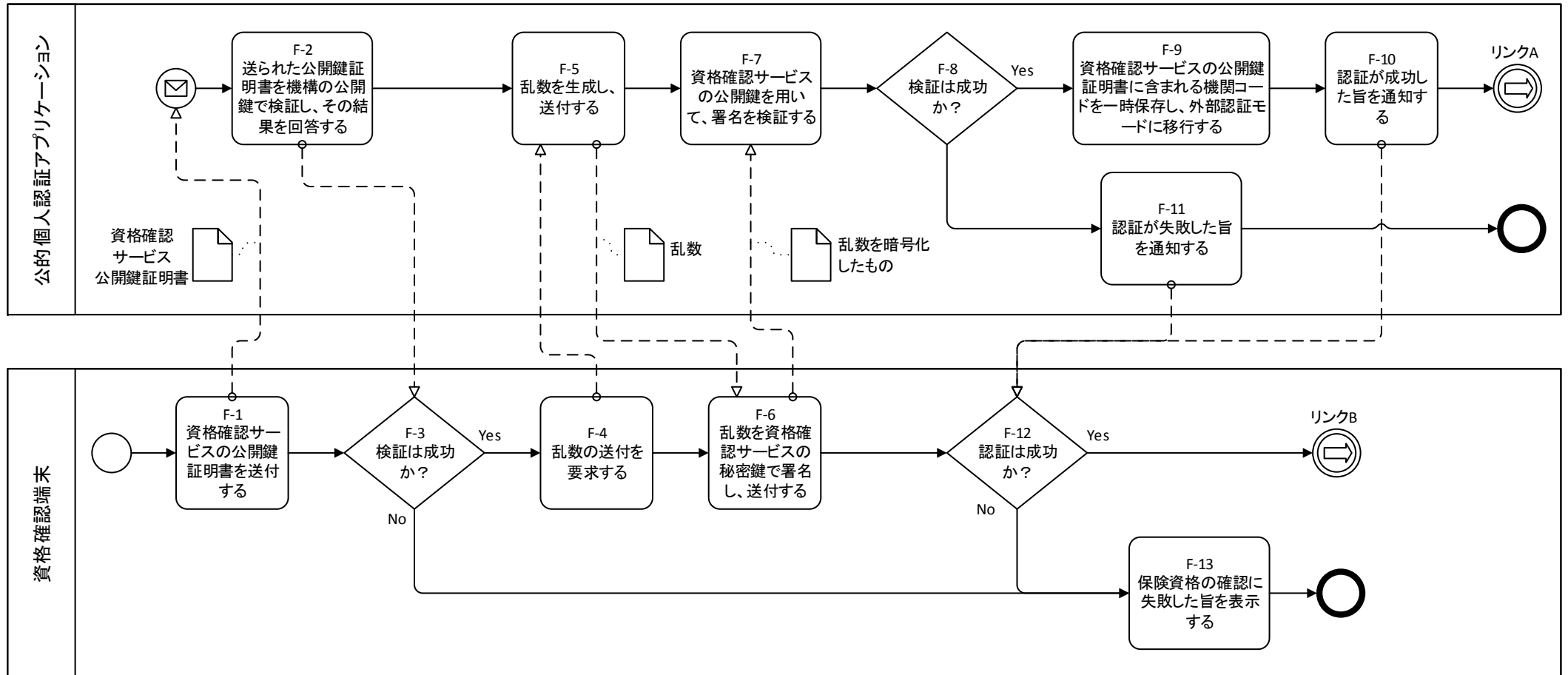
オフライン処理の実現

- 何らかの理由で資格確認サービスが一時的に使えない場合には、次の情報を保存し、資格確認サービスの復帰後、資格確認を行う。
 - 利用者証明用電子証明書
 - 認証を行った時刻
 - 認証の際の付加的な情報
- 偽の情報が資格確認サービスに送られることがないよう、資格確認端末が正規のものであることを確認することが必要。
 - 資格確認端末を資格確認サービスが認証する仕組み
 - 資格確認端末の起動時にHPKIを用いて認証

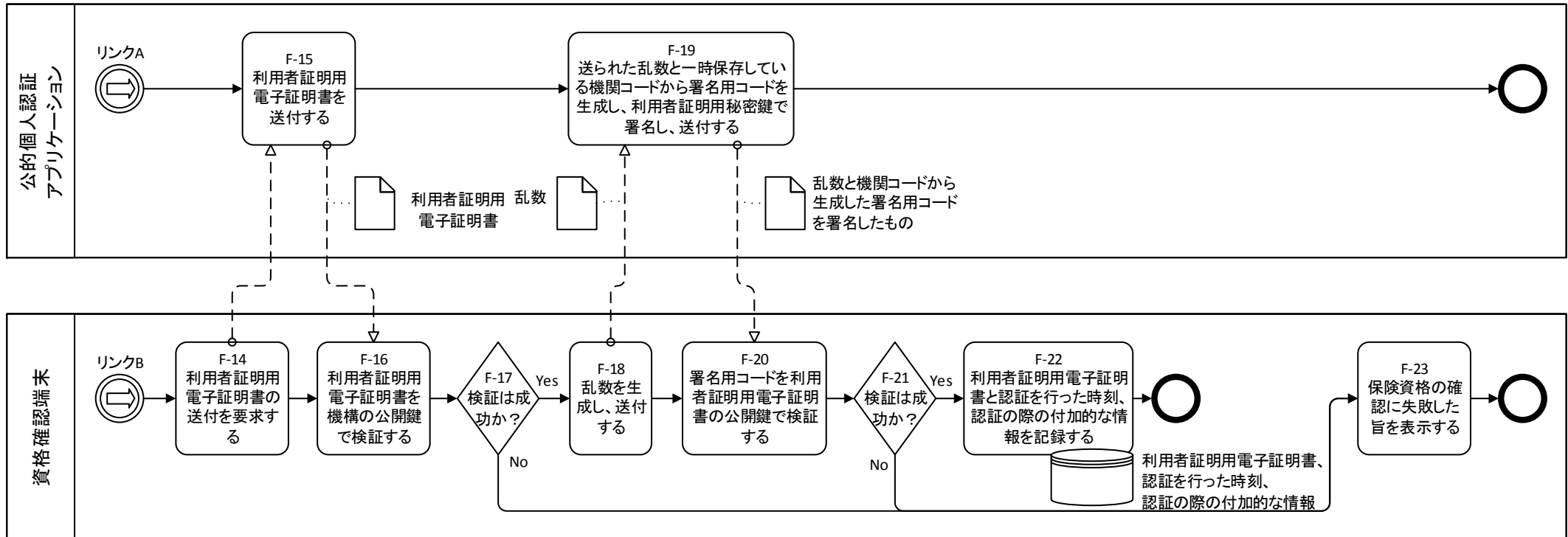
E' . 処理順序を入替え



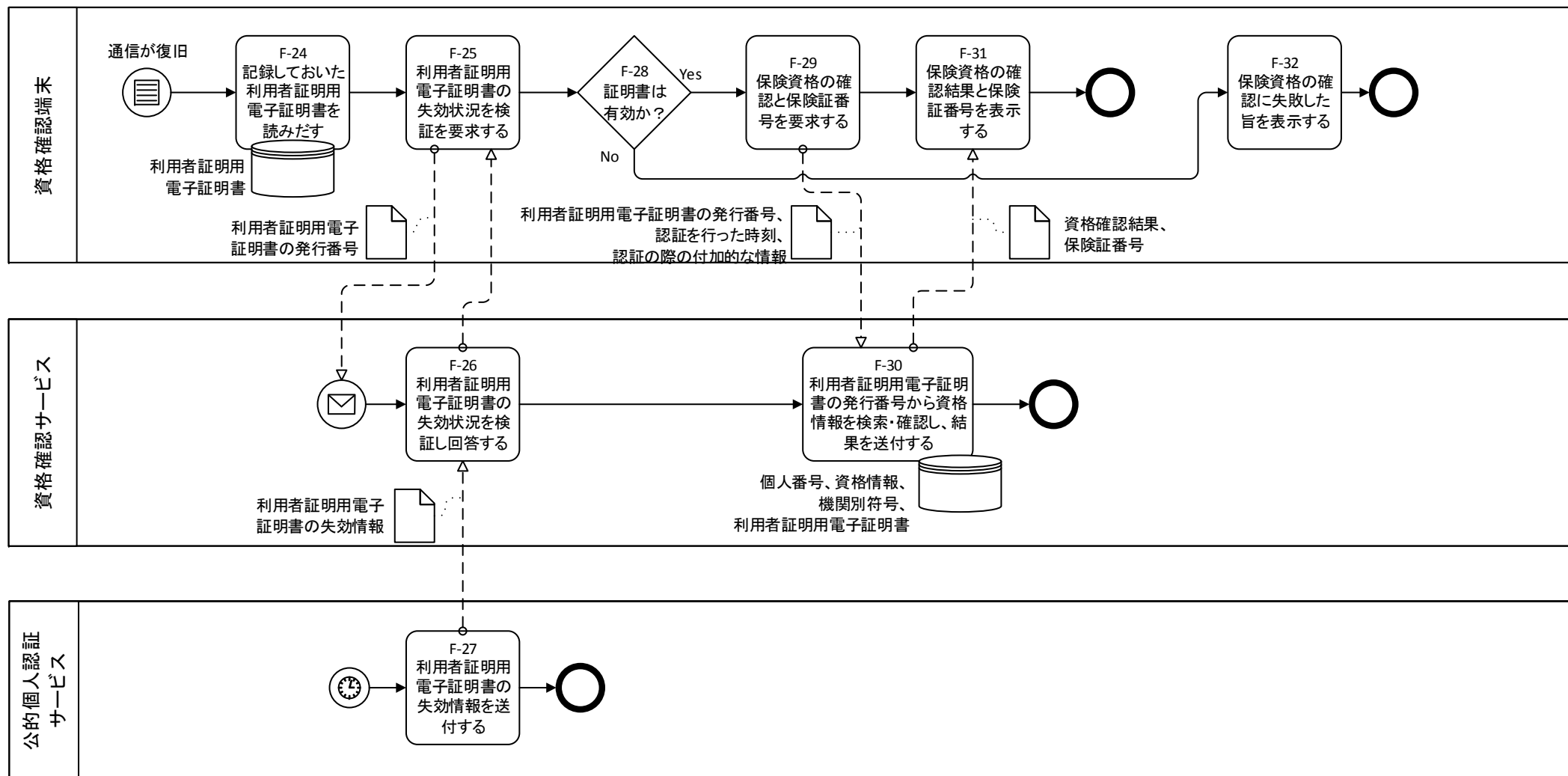
F. オフラインとオンラインを切り分け (1/3)



F. オフラインとオンラインを切り分け（2/3）



F. オフラインとオンラインを切り分け (3/3)



オフラインでの暫定的な資格確認

- 被保険者全員に係る資格情報のデータベースを資格確認端末に載せることは困難。
- 他方、特定の保険医療機関等を過去に受診した経験のある被保険者に限定すれば、データベースの規模を縮減できる可能性。
- 保険医療機関等が、受診した患者についてオンライン保険資格確認を行った際、利用者証明用電子証明書と資格情報のペアをキャッシュ。
- オフラインの場合は、このキャッシュから資格情報を得ることで、暫定的な保険資格の確認が可能。
- 長時間にわたって通信が使えない場合などに適応があるか。

資格確認端末の偽造・盗難

正規の端末

かつ

盗難されていないこと

を確認



- ✓ 電子証明書と秘密鍵を資格確認端末に持たせ、
- ✓ これを資格確認サービス側で認証し、
- ✓ 盗難された端末は失効リストで排除

運用

- 資格確認端末を起動した際に、1回のみ認証
- オフラインになった場合は、オンラインに復帰した際に再度認証
- 電源を入れたままで盗難に遭う可能性のある形態の端末の場合は、資格確認の度に認証

資格確認サービスの秘密鍵の盗難

秘密鍵を安全な場所に格納すること

- ICカードのような耐タンパ性のメディアに格納
- 端末内のセキュアエレメントに格納

秘密鍵を用いた処理を安全な場所で行うこと

- 通常のOS配下の領域から切り離されたセキュアな領域で処理を実施

過去の資格情報の保持

オフライン処理とオンライン処理を切り分けた場合、

照会日よりも前の日付の資格情報が必要となる場合あり



- ✓ 資格確認端末で受診日を記録し、
- ✓ 資格情報照会の際は、受診日も送付し、
- ✓ データベースでは過去の資格情報も保持しておく

備考

- どの程度過去の情報まで保持しておくかは、実務等も精査して決定

まとめ

- 厚生労働省が提示したオンライン保険資格確認の仕組みを基に、手続きの詳細を可視化した。
- 手続きの際に必要なとなる通信の量を減らすために資格確認端末で可能な限りローカルに処理を行う方法と、オフラインでも可能な範囲の手続きを行う方法を示した。
- 実運用に際して留意すべき課題について考察した。
- JPKIの活用は、医療保険の資格確認にとどまらず、確実な本人認証が可能である特徴を活かして本人受診のエビデンスを残す用途や、個人の医療・健康情報の収集・保存・活用の用途にも広げていくことが期待される。