NRI SECURE

認証認可の調査研究

最終報告書 概要版

2020年09月25日

NRIセキュアテクノロジーズ株式会社

認証認可技術は技術進化が進む中で様々な選択肢が増えている。そこで、本調査研究では2018年度調査研究の結果も踏まえ、認証認可技術に係る追加調査を実施した。

背景

- 日本国においては、世界に先駆けて急速な少子高齢化が進行している。このような中で国民一人ひとりの健康寿命を延伸するとともに、多忙を極める医療や介護現場において、サービスの質を維持・向上しつつ、その効率化や生産性の向上を含めたあらゆる手段を講じることにより、社会保障の持続可能性を確保することが求められている。
  厚生労働省では、平成29 年(2017 年) 1 月に厚生労働大臣を本部長とする「データヘルス改革推進本部」を立ち上げ、健康・医療・介護データの有機的な連結やその利活用の推進に向けた取組を進めてきた。
- データヘルス改革において実現を目指す各プロジェクト等において各々に必要となる認証認可の仕組みについて、できるだけ共通化し集約することが、保護すべき情報に対してのセキュリティ強度を高め、また全体でのコストに対して効果が高いと考えられる。厚生労働省では、認証認可に係る事業として、「医療等分野のネットワーク接続の機関認証に関する調査・研究」（2017 年度）および「利用者認証に関する調査研究」（2018 年度）を実施している。
- 「利用者認証に関する調査研究」（2018 年度）の調査研究の結果、提供されるサービスの内容や利用場所、利用者の属性、閲覧される（保護すべき）情報の機微性などによって異なる認証方式を用いる必要があることが整理された。
  また、**それらすべての認証方式を提供するために、ユーザ/管理者画面・認証API・FIDOサーバ・認証局（OpenID）・HPKI/JPKI/外部ID 認証基盤との連携、などを今後さらに検討する必要があることが導出された。**

調査研究の目的

- 認証認可に関連する技術について、モダンIT 化が進む中、様々な選択肢が増えている。上記の背景と技術進化の状況を踏まえ、**本調査研究では、認証認可技術に係る追加調査を行う。その結果として、今後の認証基盤の設計時の有用な参考情報を提供することを目的としている。**

調査研究の目的を踏まえ、「認証認可技術の基本的情報および動向に関する調査」と、「認証認可構成の要素技術についての一部実証」を実施した。

本調査研究の調査テーマは以下の通り。

OpenID FoundationとFIDO Allianceの基本的情報の整理

- 認証認可に関する国際団体であるOpenID FoundationとFIDO Allianceについて、策定している規格を含めた基本的情報を整理する。

外部認証基盤との属性情報交換（JPKI/HPKI）についての机上検討

- 外部認証基盤との属性情報交換（JPKI/HPKI）について、実現方法と課題の机上検討を行い、その活用可能性について検討する。

OpenID ConnectとFIDOを活用した認証認可構成の検討および一部実証

- OpenID Connect CIBAとFIDOを組み合わせて、特定のシーンに特化しない医療情報交換においての認証・認可の構成について、全体像を検討する。
- 検討した認証認可構成において、要素となる一部の新しい技術(CIBAおよびFIDO)について、クラウド環境にて実証環境の構築を行い、機能面の実現性を実証する。

普及している認証基盤の活用に関する調査

- OpenID ConnectまたはFIDOを実装し、一般的に普及している認証基盤の活用に関して調査する。

同意の表現方法に関する調査

- 同意の表現方法、電子的な形で本人同意を取得する場合の法的な裏付け等について調査する。

OpenID ConnectやFIDOは認証機能の要素技術として十分に活用できるものである。JPKI/HPKIは、認証基盤での身元確認、当人認証手段の1つとして活用が考えられる。

本調査研究では以下のテーマについて調査検討を行い、知見を得た。

本研究で明らかにすべきこと	調査検討結果のポイント
認証認可に関する国際団体であるOpenID FoundationとFIDO Allianceについて、策定している規格を含めた基本的情報を整理する。	• **OpenID Connectは、認証基盤において管理されるIDの連携をセキュアに行うための規格**であり、複数のサービスに対して利用者認証および認可の機能を提供する手法として広く活用されている。 • 直近では、OpenID Connect Client Initiated Backchannel Authentication (CIBA)プロファイルの発行により、リソースオーナーの認証・同意に基づき、第三者がそのリソースオーナーの持つリソースアクセスを認可するユースケースへの適用が可能となっている。 • **FIDOは公開鍵暗号方式を利用した認証技術**であり、セキュリティと利便性を両立させる次世代の認証方式として活用されている。主要なデスクトップOSやスマートフォンでFIDO規格のサポートが進んできており、普及の環境が整いつつある。 • デジタルアイデンティティに関するガイドラインとして、米国国立標準技術研究所(NIST)が発行するNIST SP800-63-3があり、認証基盤に求められる保証レベル等が定められている。OpenID ConnectおよびFIDOにおいても、本ガイドラインに記載事項に沿う機能を提供している。 • **OpenID Connect および FIDO は技術的な仕組みとしてセキュリティ等が考慮され、前者に関しては形式的検証を通じて安全性が確認されたものであり、世界各国の有識者により国際的な規格として検討されたものである。今後の認証基盤の要素技術として、十分に信頼、活用できるものである。**
外部認証基盤との属性情報交換（JPKI/HPKI）について、実現方法と課題の机上検討を行い、その活用可能性について検討する。	• **認証基盤におけるJPKIの活用用途としては、認証基盤のID申請、登録を行う際のオンライン身元確認の手段の1つとして利用することが考えられる。また、認証基盤で当人認証を行う際の認証手段の1つとして利用することが可能である。** • マイナポータルでは、行政機関等が保有する自己情報（所得、世帯など）を確認できるサービスとして、自己情報取得APIを公開している。JPKIによる当人認証を介して、認証基盤またはサービスが、認証した者の自己情報を取得することが可能となっている。 • HPKIの活用用途としては、医師等保健医療福祉分野の従事者が、利用する認証基盤においてID登録を行う際の資格情報の確認方法として利用する用途が考えられる。

OpenID Connect CIBAおよびFIDOにより、利用者のリアルタイムな認証と同意の下に、第三者に対する利用者への情報提供が技術的に可能であることを確認した。

本調査研究では以下のテーマについて調査検討を行い、知見を得た。

本研究で明らかにすべきこと	調査検討結果のポイント
OpenID Connect CIBAとFIDOを組み合わせて、特定のシーンに特化しない医療情報交換においての認証・認可の構成について、全体像を検討する。	• **検討にあたっては患者の所有する端末での認証、同意のもとに、医師等の第三者に対して患者の医療・健康情報アクセスを認可するユースケースを仮定し、そのユースケースの実現方式について、OpenID Connect CIBA および FIDO の組み合わせが適用し得ることを確認した。** • 患者に対する都度の同意を省略するケースにおいては、事前の同意の取得の他、初回同意時に取得した医療・健康情報アクセス用のトークンを有効活用する、医師が患者の当人認証を行っていることを担保するためのサービス・認証基盤間のトラストフレームワークを構成する等、その方法および運用について検討が必要となる。 • **代理人の同意に基づくリソースアクセスの認可については、代理人が適切であることの管理およびその検証方法、連携方式がユースケースにより多様となることが想定され、今後の検討課題となる。**
検討した認証認可構成において、要素となる一部の新しい技術(CIBAおよびFIDO)について、クラウド環境にて実証環境の構築を行い、機能面の実現性を実証する。	• **前項で検討したユースケースについて、OpenID Connect CIBA および FIDO を組み合わせることにより機能的に実現可能であることを、評価環境での実機検証によって確認した。** • OpenID Connect CIBAにおいては、認証デバイスへの通知を起点とした認証処理が行われる。認証デバイスへの通知方式、認証デバイスにおける認証手段については複数の方法が考えられるため、認証基盤を構築する組織において今後の検討課題となる。

OpenID ConnectやFIDOは大規模な認証基盤においても活用され、運用されている。同意取得の具体的な方法等は、国際規格として整理されてきている。

- 本調査研究では以下のテーマについて調査検討を行い、知見を得た。

本研究で明らかにすべきこと	調査検討結果のポイント
OpenID ConnectまたはFIDOを実装し、一般的に普及している認証基盤の活用に関して調査する。	• **OpenID ConnectとFIDOは、行政機関、民間企業が運営する大規模な認証基盤の認証技術として活用され、運用がなされていることを確認した。** • **各認証基盤においては、提供するサービスの性質および関連法制度に応じて、当該サービスの利用者のIDが満たすべき身元確認レベル・当人認証レベルを定め、運用が行われている。** • マイナポータルにおいては、その認証手段となるJPKIについて、法的根拠（マイナンバー関連法）に基づく運用がなされている。 • 銀行業、携帯電話事業においてもJPKIと同様に、IDの取得にあたって求められる要件を犯収法、携帯電話事業者法等により法制度として定め、各事業者に対して適切な運用を求めている。
同意の表現方法、電子的な形で本人同意を取得する場合の法的な裏付け等について調査する。	• **個人情報保護法および関連ガイドラインでは個人データの第三者提供における同意取得を求めている。**一方で、これらのガイドラインにおける規定の内容は同意取得に関する指針であり、**同意取得を技術的に実現する際の具体的な方法および項目の詳細については規定しておらず、その運用は各事業者に委ねられている状況にある。** • 国外においても、同意の具体的な取得方法、管理方法を定めている例は少数である。同意内容の管理方法に関する事例としては、インドのAadhaar(国民識別番号制度)における “Data Empowerment and Protection Architecture” の中で定められている Electric Data Consentが挙げられる。 • **同意取得時の表現に関する国際規格として、ISO/IEC 29184が2020年6月に発行されている。**ISO/IEC 29184では、オンラインにおけるプライバシー通知の内容と構造を決定する方法、個人を特定できる可能性のある情報を収集および処理することへの同意を求めるプロセスについて定めている。

OpenID Foundationは分権的な認証プロトコルのオープンスタンダードである OpenID技術の標準化団体であり、世界中の主要IT企業が参加している。

OpenID Foundationの概略

- OpenID Foundationは、OpenID技術（サイト間のID連携、API連携など）の実現、促進、保護に取り組む個人や企業の非営利国際標準化団体である。
- 2007年6月に財団が設立され、開発者、ベンダー、ユーザーのオープンなコミュニティを代表する信頼のおける組織として機能している。
- 世界中のデジタルID業界の大企業や個人が協力して仕様の策定を行い、OpenIDのアプリケーションの採用を推進している。

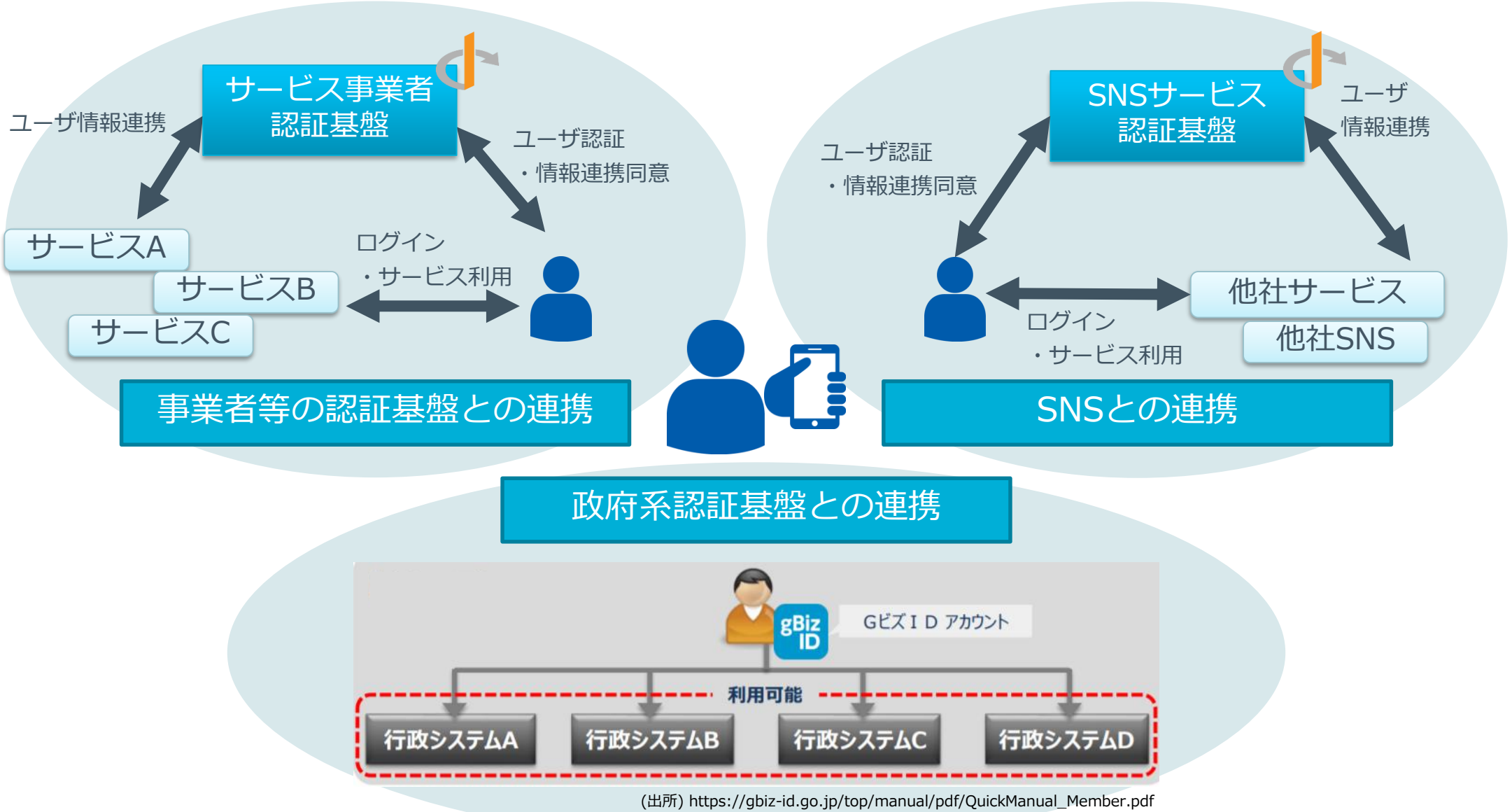
参加企業・団体 (2020年9月時点)

- Sustaining Corporate Members（ボードメンバー）

Akamai	Google	KDDI
Microsoft	NRI SecureTechnologies	Ping Identity
Verizon	Verizon Media	

- Corporate Members（59団体）
- Non-Profit Members （16団体）

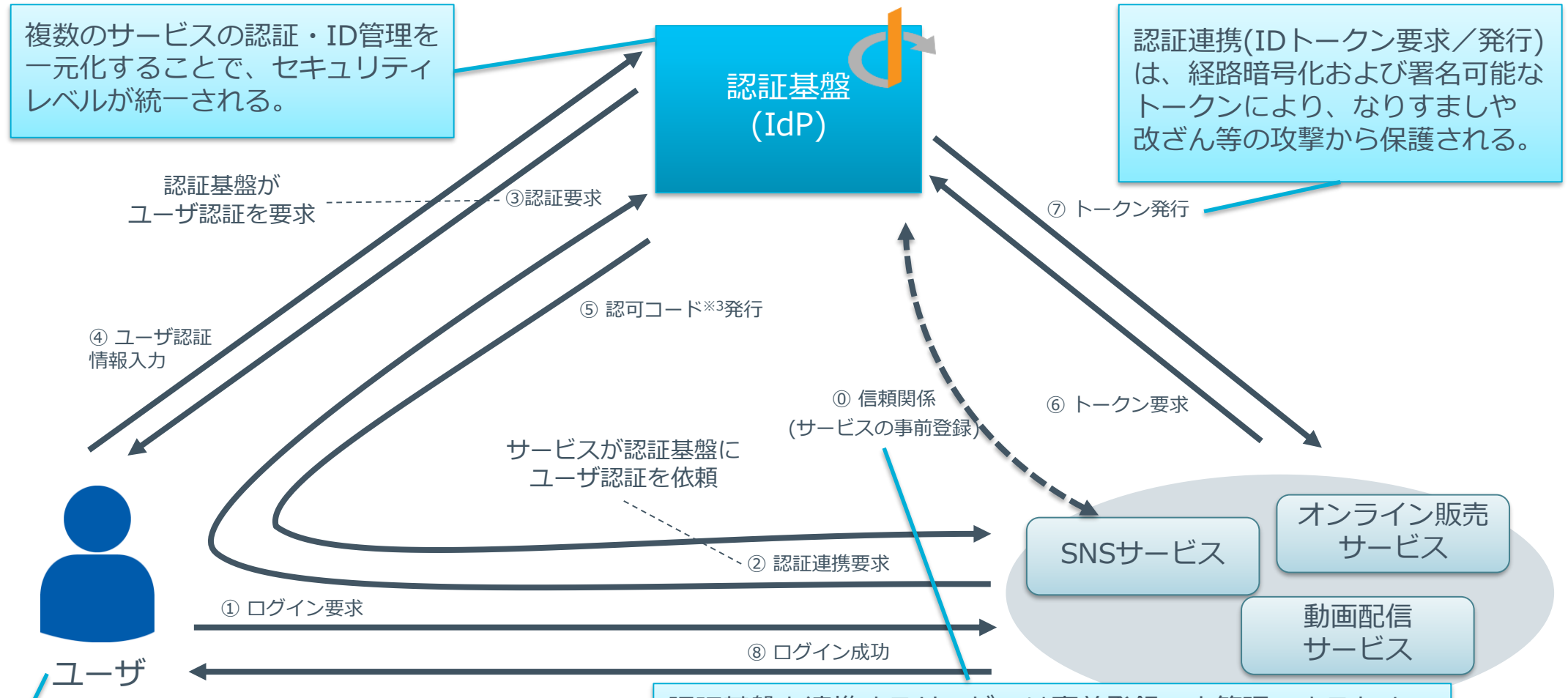
OpenID Connectは、IDサービスのアカウント情報を利用したサービスログインや、ID情報連携の手法として広く活用されている。



(出所) https://gbiz-id.go.jp/top/manual/pdf/QuickManual_Member.pdf

OpenID Connectによる認証連携はセキュリティ専門家の議論、意見が集約されたデファクトスタンダード※1であり、セキュリティ面で優れている※2。

- OpenID ConnectにおけるAuthorization Code Flowの処理フローイメージと特徴を以下に示す。



※注1：Sign in Apple, Google Sign-in, Microsoft Azure App SigninはいずれもOpenID Connectの実装。
また、ベルギーなどの国民ID基盤としても利用されている。
※注2：形式的検証により安全性が確かめられている。
※注3：OpenID Connectは認可の規格であるOAuthをベースにしているため、用語に「認可」が使われている。

FIDO Allianceはパスワードへの過度な依存を減らすための標準規格としてFIDOの普及を目指している標準化団体であり、世界中の主要IT企業が参加している。

FIDO Allianceの概略

- 認証技術「FIDO」の仕様策定および普及活動を行う非営利国際標準化団体である。
- FIDO導入製品に対する認定プログラムを提供している。

沿革

- 2012年7月：PayPal、Lenovo、Nok Nok Labs等6社がFIDO Allianceを設立
- 2013年2月：正式にFIDO Allianceが発足
- 2014年2月：パスワードレスプロトコルのUAF 1.0および2要素認証プロトコルのU2F 1.0を公開
- 2018年4月：W3CとFIDO AllianceがFIDO2を正式発表

参加企業・団体（2020年9月時点）

- Board Level Members（42社）
  - Google, Apple, Facebook, Amazon, Microsoft, NTT docomo, LINE, Yahoo! Japan 等
- Sponsor Level Members（59社）
  - Alibaba Group, Twitter, ebay, 富士通, 日立, KDDI, NRI SecureTechnologies 等
- Government Level Members（7団体）
- Associate Level Members （140団体）

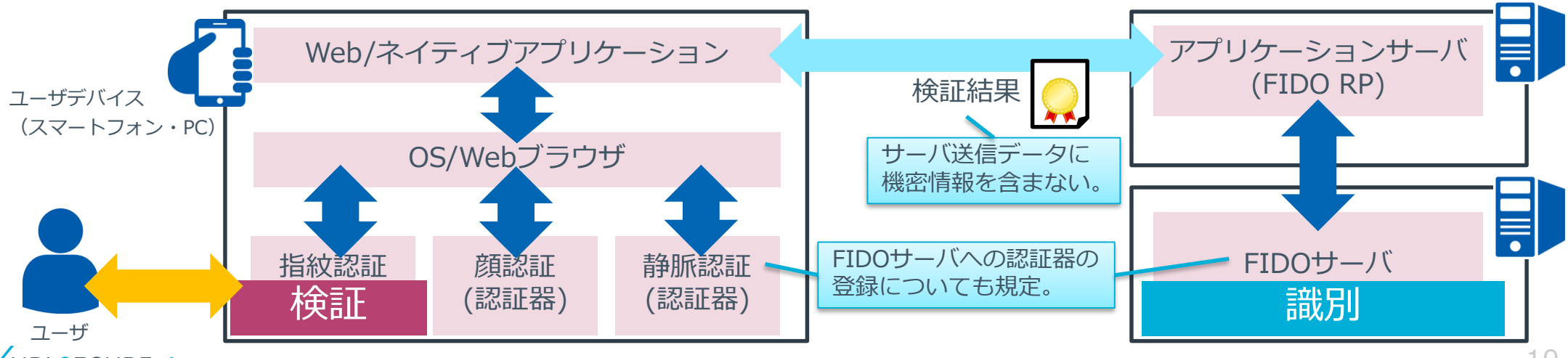
FIDO認証モデルでは従来サーバ側で実施していた本人の検証と識別のうち、本人の検証をユーザデバイス側で実施することでセキュリティを向上させている。

従来の認証モデル

- 当人認証は本人の検証(本人であることの確認)および本人の識別(サービス中のどのIDに紐づくか確認)から成る。
  それらをサーバ側で行うため、検証のための機密情報(パスワード・生体情報)をネットワーク経由で送信する。

FIDO認証モデル

- 本人の検証をユーザデバイス内の認証器で実施するため、**機密情報をネットワーク上に流すことがない**。
  また、検証結果は**電子署名により改ざんやなりすましから保護される**。
- FIDOではFIDOサーバへの認証器の登録についても規定している。**身元確認済みのユーザがFIDO認証の登録を適切に行うことで、その後の当人認証をシンプルで非常に堅牢なものとすることができる。**



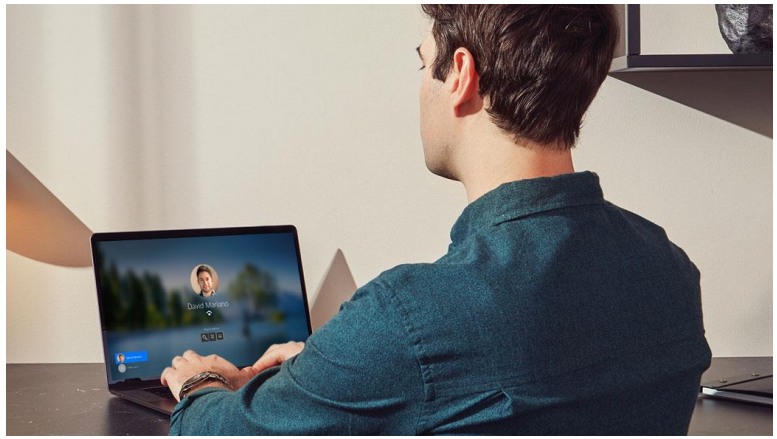
FIDO認証はWebサービス側だけでなく、ユーザデバイス側においてもOS標準でサポートが進み、より広くFIDO認証を利用できる環境が整ってきている。

Webサービス側におけるサポート状況

- GoogleやYahoo! Japan、LINEなどの国内外の主要サービス事業者がユーザ認証方法としてFIDO認証をサポート。
- NTTドコモやKDDIといった国内主要キャリアが自社サービスのユーザ認証(dアカウント、au ID)でFIDO認証をサポート。

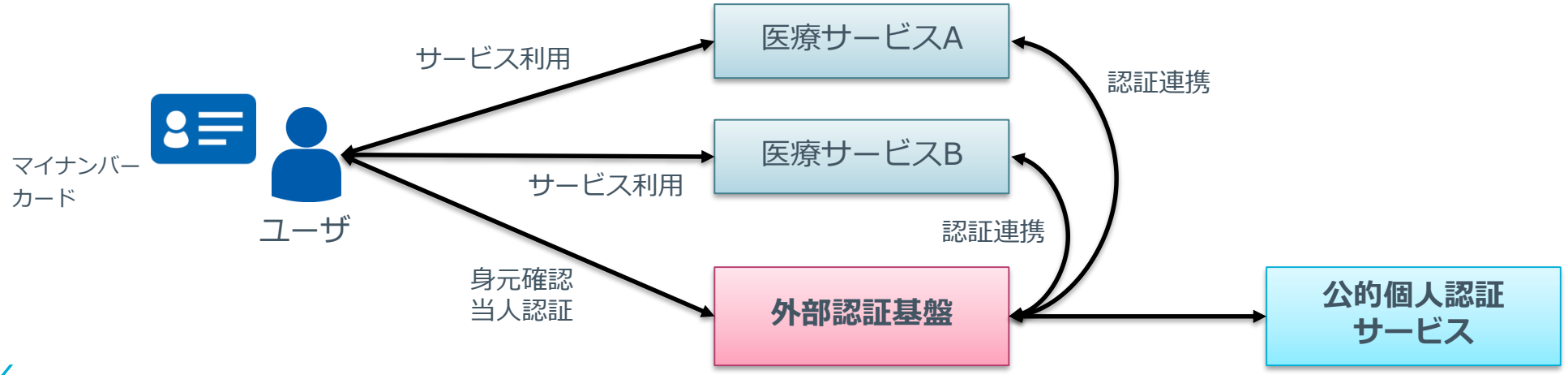
ユーザデバイス側(スマートフォン・PC)におけるサポート状況

- Google Chrome, Mozilla Firefox, Microsoft Edgeなどの主要ブラウザでFIDO認証をサポートしており、Webアプリケーションはパスワードレス認証を利用することができる。
- **iOSやmacOS上の標準ブラウザであるSafariも2020年9月リリースのiOS14およびmacOS Big Surに入るSafari14でWebAuthnに対応することを発表。** WebアプリケーションはTouchIDやFaceIDによる認証が可能になる。
- Windows 10では、FIDOをベースとしてPCに内蔵されている指紋認証や顔認証デバイスを使ったパスワードレス認証機能であるWindows Helloをサポートしている。
- スマートフォンOSであるAndroidはFIDO2認定を取得しており、Androidアプリケーションはスマートフォンに内蔵されている指紋認証や顔認証機能を利用したパスワードレス認証を利用することができる。



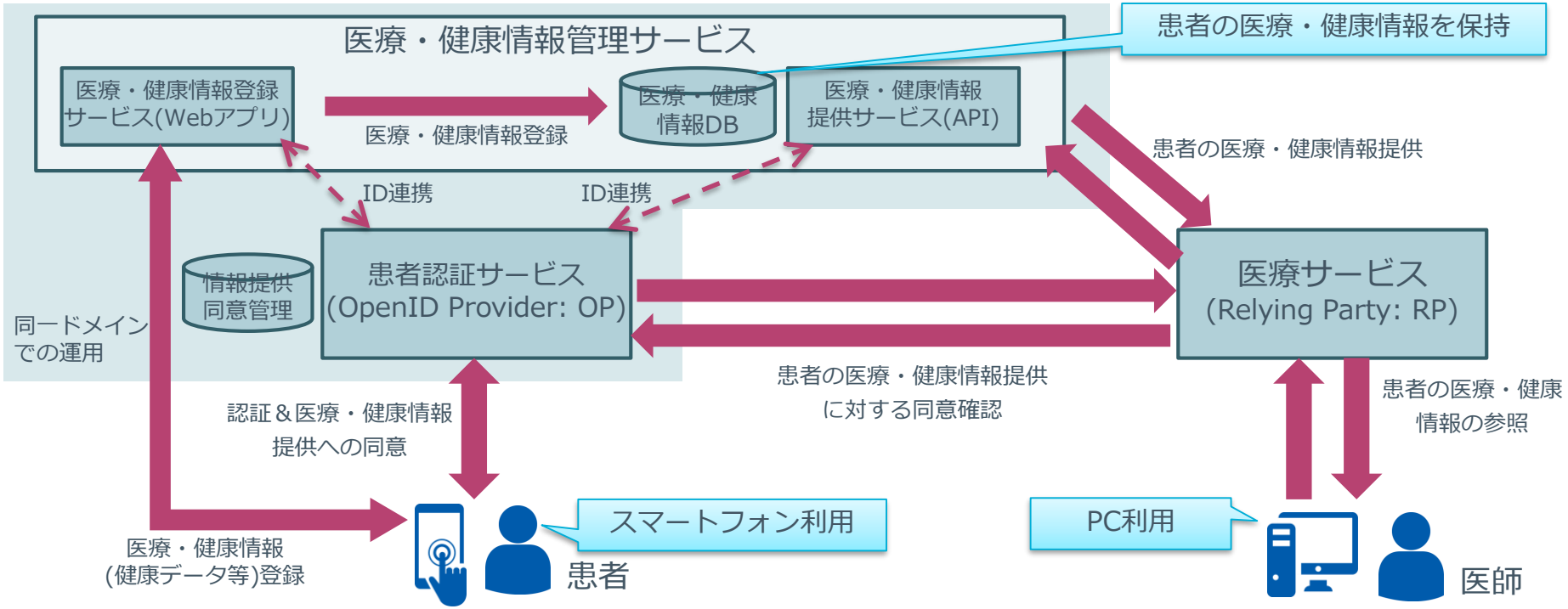
JPKIが提供する基本4情報は地方公共団体で確認済である信頼性の高い情報であり、医療分野向け外部認証基盤での身元確認に活用することが考えられる。

- 医療福祉分野における一部のサービスでは、個人の検診情報など要配慮個人情報に相当する情報を扱うことが想定される。この場合、ユーザ登録時における身元確認やサービス利用時の当人認証には高いレベルが求められることが考えられる。
- 身元確認の方法としては顔写真付き公的証明書を使った確認などいくつかの方法が存在するが、**認証基盤でのユーザ登録に関して、セキュリティレベルの高い身元確認および当人認証を実現する方法の1つとして、公的個人認証サービス(JPKI)を活用することが考えられる。**
- マイナンバーカードは、署名用電子証明書に基本4情報と呼ばれる氏名・性別・生年月日・住所の情報を保持している。この基本4情報を利用した、サービスへのユーザ登録時における身元確認の実現方式、具体的な処理内容、実装・運用時において想定される課題について机上検討を行った。
- また、認証・ID管理機能を各サービスで実装することについては、セキュリティレベルが各サービスの実装に依存し、サービス間で統一されない可能性があるリスクがある。各サービスが利用可能な、認証・認可機能を提供する信頼できる外部認証基盤を用意し、外部認証基盤においてJPKIとの連携を実装することで、各サービスがJPKIによる身元確認、当人認証の機能を実装する負担を軽減することができると考えられる。



患者の同意が得られた場合のみ患者の医療・健康情報にアクセスするユースケースを仮定し、OpenID Connect および FIDO を活用した際の実現性を実証する。

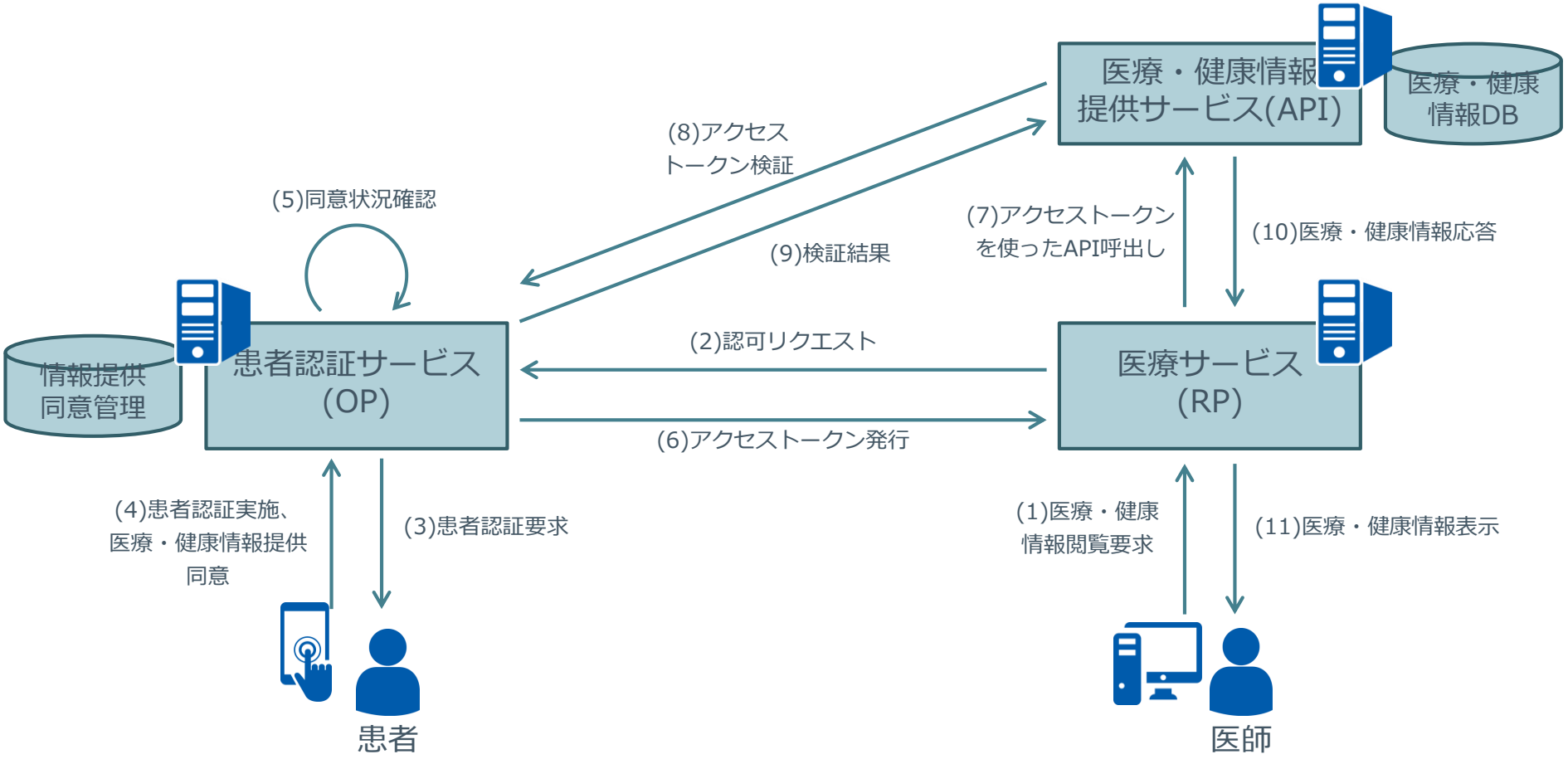
- シナリオ実現の前提として、以下の構成を想定する。



No.	システム・サービス	説明
1	医療サービス	各種医療サービス提供のために主に医師が利用するサービス。本サービス利用時の患者の認証や患者の医療・健康情報へのアクセス認可は患者認証サービスから実施する。 なお、本検討では医師の認証は何らかの手段(医師認証サービス等による)で完了していることを前提としている。
2	患者認証サービス	患者の本人認証を実施し、複数の医療サービス向けへ認証情報連携を行うサービス。認証の他、外部の医療・健康情報提供サービスに保管されている患者の医療・健康情報へのアクセス認可の管理を行う。
3	医療・健康情報管理サービス	患者または診療所等で登録された医療・健康情報を管理するサービス。医療・健康情報提供APIの他、患者または診療所からのデータ登録サービスも有する。医療・健康情報提供は、患者認証サービスで発行されたアクセストークンを基に行われる。

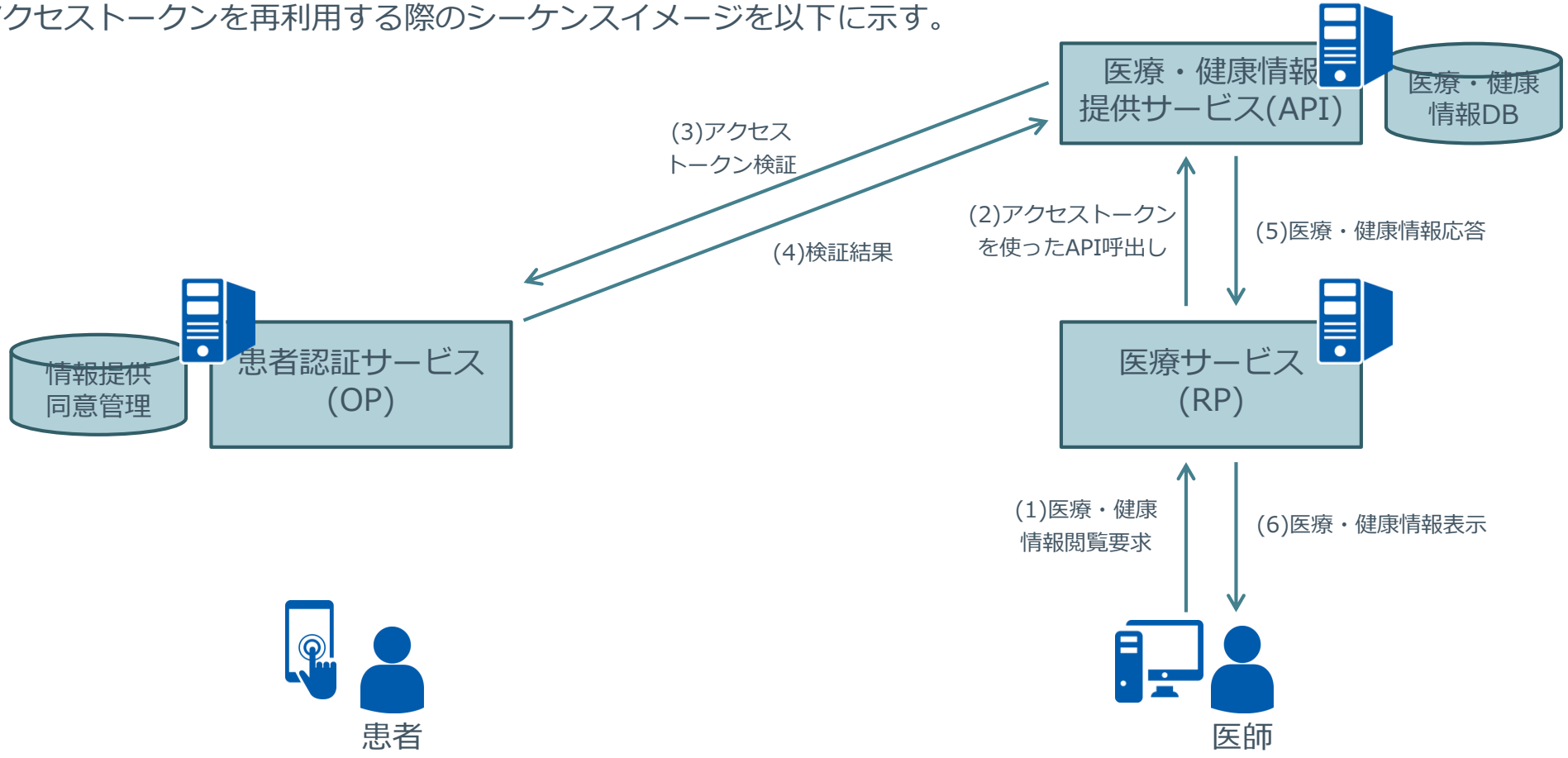
患者が自分のデバイスで認証および医療・健康情報提供の同意を行った上で、医師が医療・健康情報にアクセスするケースを基本シナリオとして設定した。

- 医療サービス(RP)からの認可リクエストを受けて、患者認証サービス(OP)はOpenID Connect CIBAの仕様に基づき患者のデバイスにプッシュ通知で認証要求を送る。
- 患者は認証実施後に医療・健康情報提供への同意を行い、その後医療サービスにアクセストークンが発行される。
- 医療サービスはそのアクセストークンを使って医療・健康情報提供サービスに医療・健康情報をリクエストする。



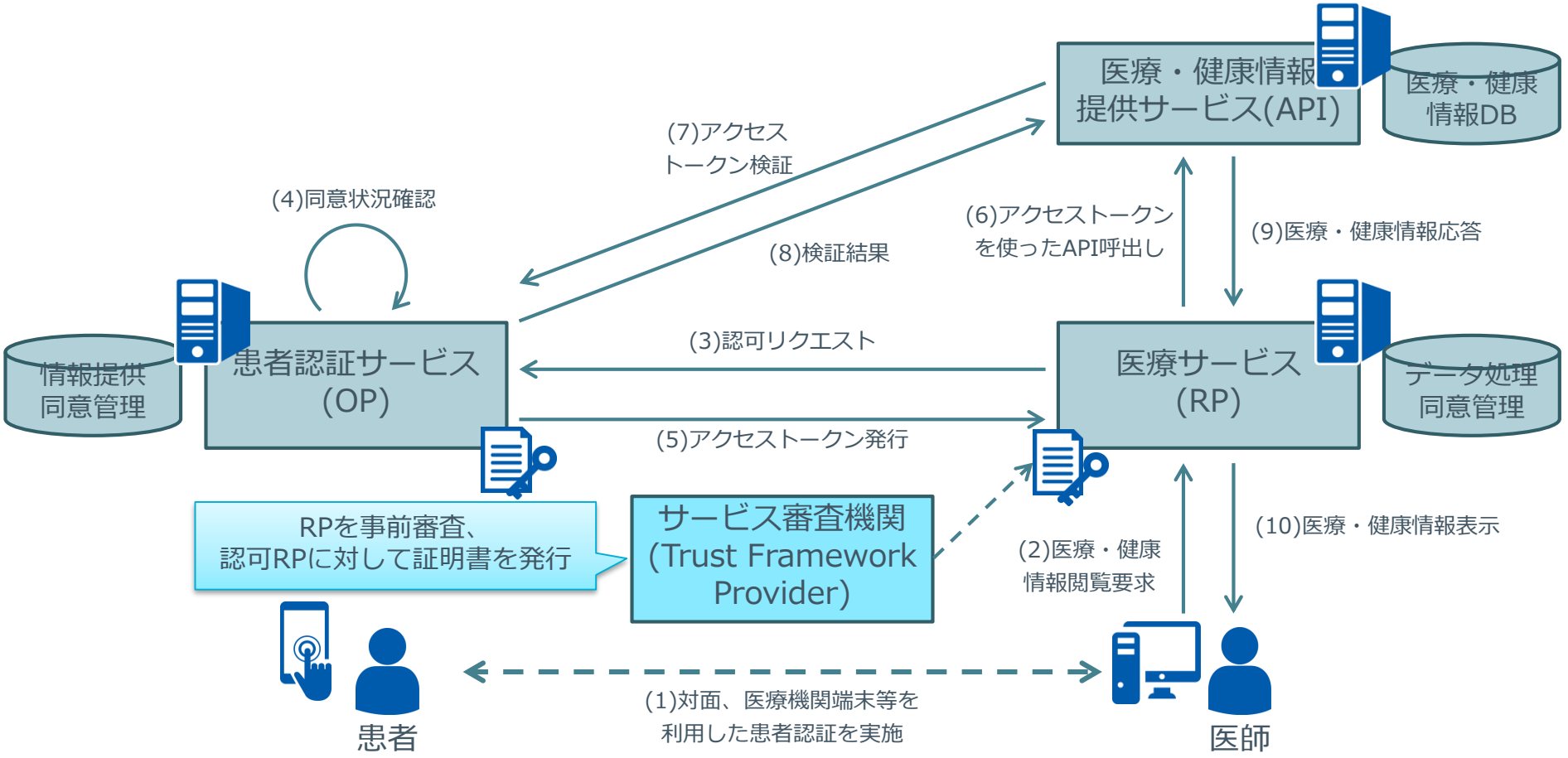
医療・健康情報提供への同意を一度実施したユーザについて、患者認証および情報提供同意を再利用して医療・健康情報取得を行う方法について検討を行った。

- 患者認証・同意処理を都度求めることは患者の負担となり得るものと想定し、基本シナリオの派生シナリオの1つとして、患者認証および情報提供同意を再利用し、画面等での都度の同意取得を求めずに医療・健康情報取得を行うことについて、技術的な方法を検討した。対応の考え方として、大きく以下の2通りの方法が考えられる。
  - 取得したアクセストークンを再利用する。
  - 改めて医療サービスから認可リクエストを行い、アクセストークンを取得する。
- アクセストークンを再利用する際のシーケンスイメージを以下に示す。



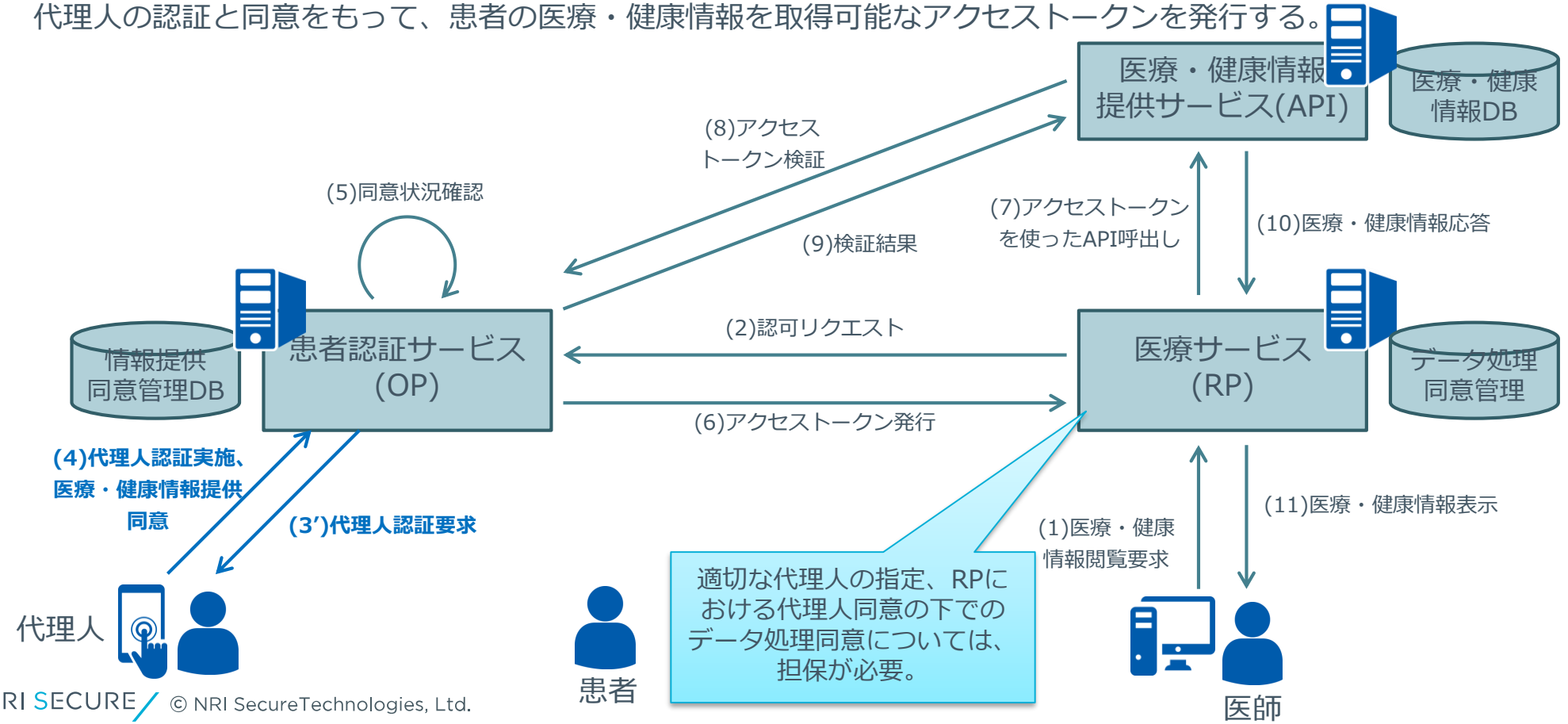
同意省略の方策の1つとして、医療サービスと患者認証サービス間の信頼関係担保を前提として、医師側にて患者の認証を行う方式が考えられる。

- 医療サービスが信頼できることを確認可能な、第三者となるサービス審査機関を設ける。
  - 医療サービスと患者認証サービスを含むトラストフレームワークを構成する形となる。
- サービス審査機関は、RPの事前審査を行い、認可したRPに対して証明書を発行する。
- 対面、医療機関端末等を利用した患者認証を実施した前提のもとに、患者認証サービスは、医療サービスの認可リクエストを受けつけ、患者の認証処理を省略してアクセストークンを発行、返却する。



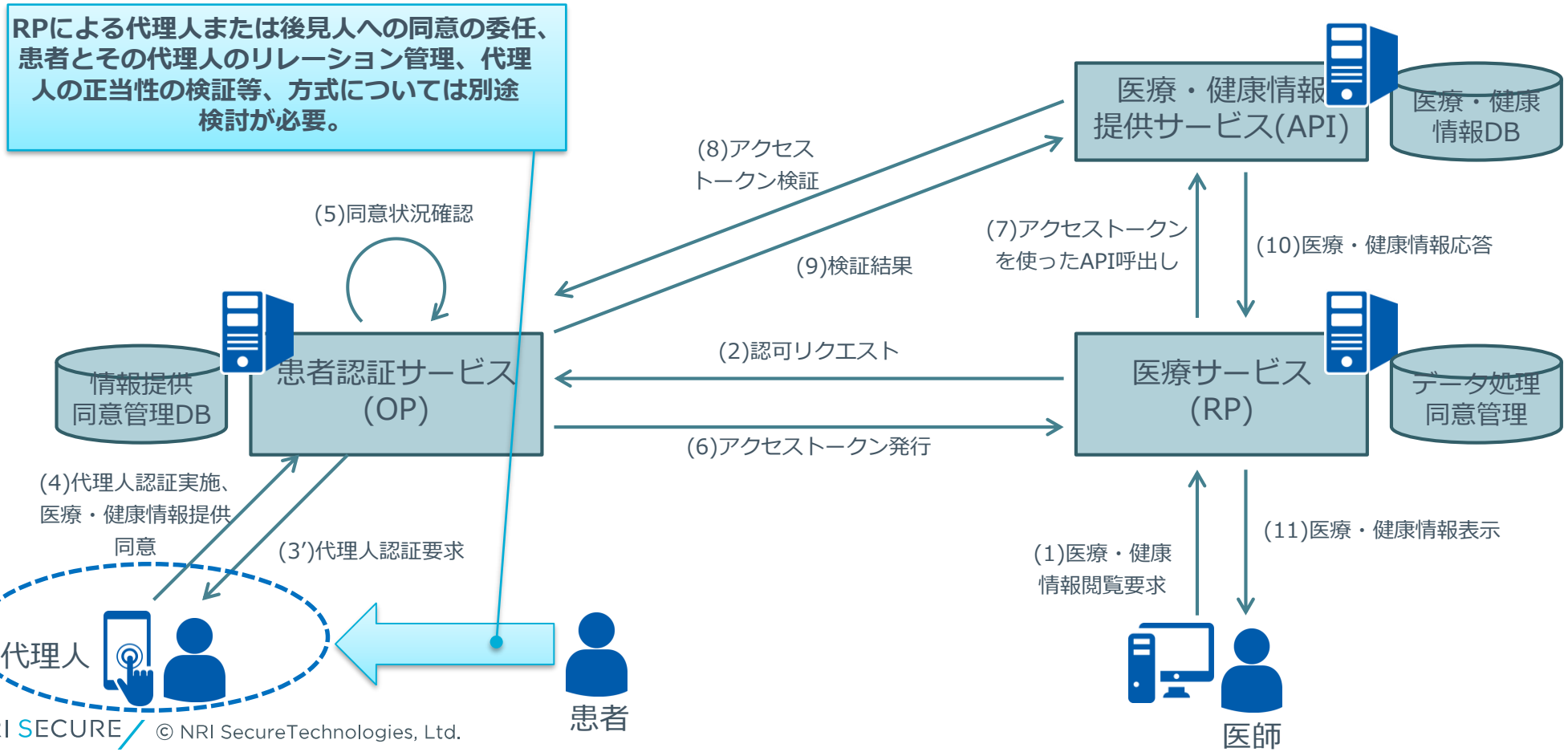
代理人同意のケースでは、医療・健康情報提供同意が可能な代理人を事前登録の上、代理人による同意手続により患者の情報を得るトークンを発行する方式が考えられる。

- 医療福祉分野においては、患者自身による情報提供同意の意思表示が困難な場合に、後見人もしくは代理人が情報提供同意を行うケースが想定される。2件目の派生シナリオとして、代理人により患者の医療・健康情報へのアクセスを許可する方法について検討する。
- このケースでは、OpenID Connect CIBAの仕様に基づき、医療サービス(RP)からの認可リクエストを受けて、代理人の認証デバイスにプッシュ通知で認証要求を送信する方法が考えられる。
  - 医療サービス(RP)において代理人が適切であることの確認および代理人によるデータ処理の同意が適切であることを担保する必要がある。
- 代理人の認証と同意をもって、患者の医療・健康情報を取得可能なアクセストークンを発行する。



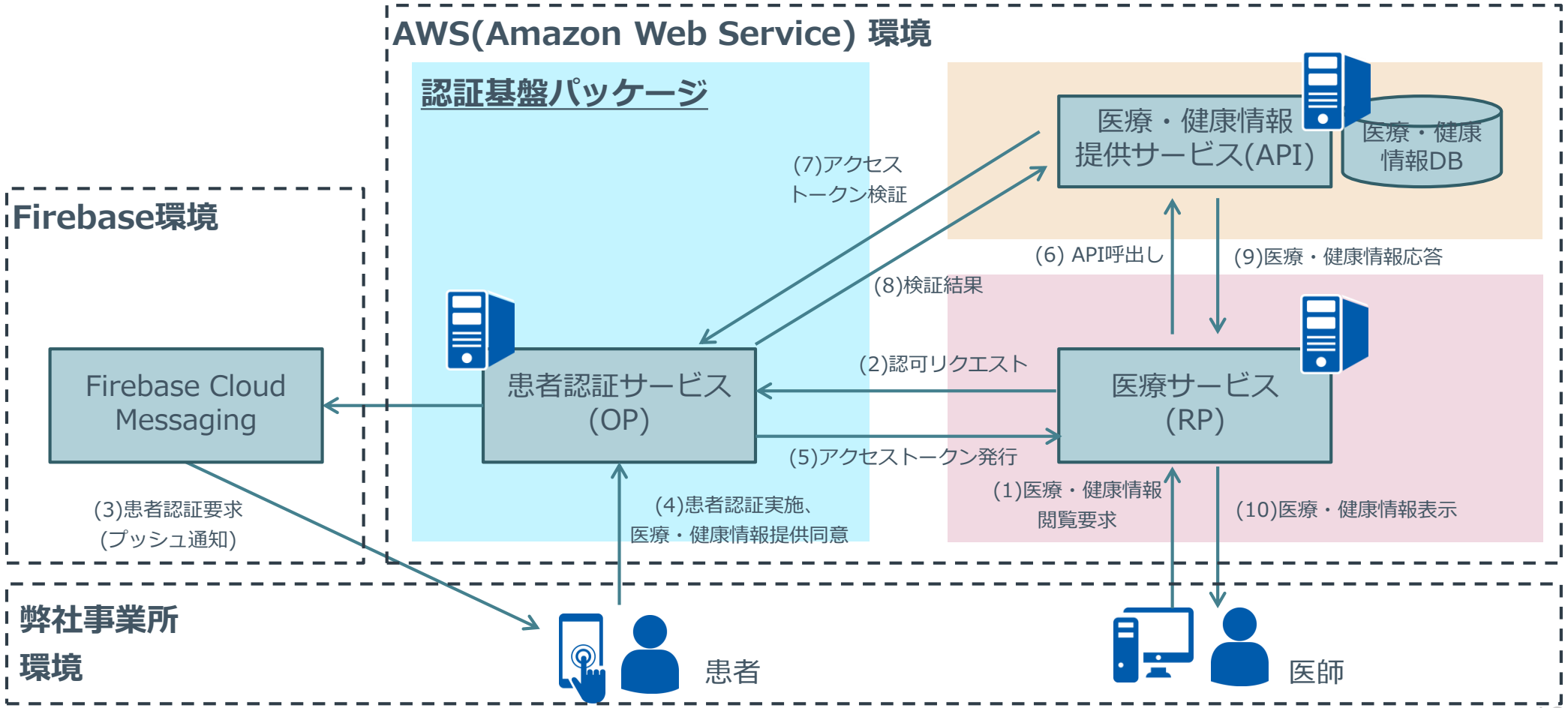
適切な代理人のリレーション管理、代理人の検証については、ユースケースと関連法制度を踏まえた検討が必要である。

- 前述の方式は、適切な代理人がRPによりリレーション管理のもとに識別され、検証されていることが前提となる。
- 代理人または後見人への同意の委任に関しては、様々な業務ユースケースおよび関連法制度があり、それぞれのケースに応じた技術的な処理方式については別途検討が必要である。



実証環境は、クラウド環境上にOpenID ConnectやFIDO等の規格に標準対応する認証基盤パッケージを利用することで実現した。

- 患者認証サービスには、 OpenID ConnectやFIDO等の規格に標準対応する認証基盤パッケージを適用した。
  - 本検証では、NRIセキュアテクノロジーズ製品の「Uni-ID Libra」を利用した。
- 医療サービスおよび医療・健康情報提供サービスについては、検証用の簡易なモックアップアプリケーションを実装した。
- 患者認証要求時のメッセージ通知(プッシュ通知)には、Firebase Cloud Messagingを利用した。



認証基盤の評価項目を定め、5つの認証基盤を中心に具備する機能の調査および評価を実施した。

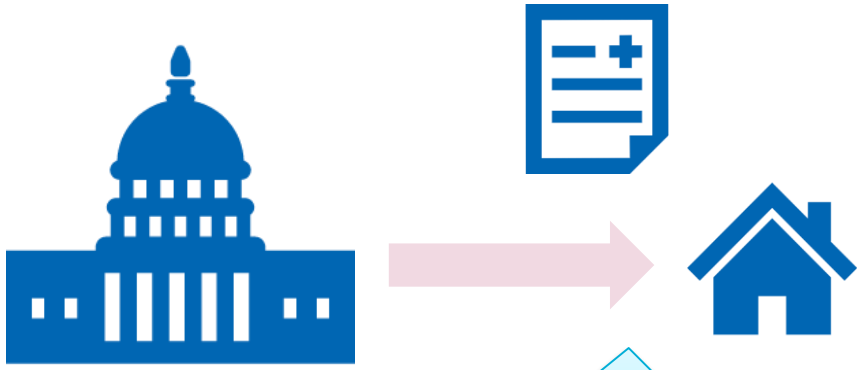
- 別添資料3に、評価項目と各認証基盤の機能、評価を一覧化した。

大項目	中項目	小項目	マイナポータル	gBizID	LINE ID	Value Direct	dアカウント
登録	ID数		2033万 （令和2年4月1日時点のマイナンバーカード発行数）	13万	月間アクティブユーザ数8300万※ （※LINE利用ユーザの92%はスマホアプリを利用、またLINEアカウントは複数アカウント持つことができる）	非公開	7000万以上 （回線契約をしてなくてもアカウント作成可能）
	ID管理	情報更新	マイナンバーの情報を更新する際には、官公署発行の写真付き本人確認書類または、市区町村長が適当と認めるもの2点を使って、対面での身元確認を実施。	基本項目はマイページより変更可能。ただし法人の代表者氏名の変更は、申請書をgBizID運用センターに送付する必要がある。	マイページ上で変更可能。	住所・氏名はマイページより変更可能。ただしローンや投資信託などを利用している場合は、郵送での手続きとなる。	マイページサイトから変更可能。ただし氏名と生年月日は本人確認書類のアップロードが必要。
		利用不能時のリカバリー方法	複数回連続でパスワードを間違えるとアカウントがロックされ、市区町村窓口に出向いてアカウントのロック解除が必要になる。	利用不能時のリカバリー方法：パスワード忘れまたはアカウントロックがされた場合は、アカウントに登録しているメールアドレスに送信されるメールから、パスワードの初期化を行う。	アカウントロック時には、登録している電話番号を使ってSMS認証、FacebookとLINEアカウントを紐づけている場合はFacebookアカウントで復旧可能。	専用窓口でキャッシュカードの情報と電話取引用暗証番号を伝え、再設定を行う。	パスワード忘れで携帯回線未契約時には、IDに登録されているメールに仮パスワードが発行され、そのパスワードを使ってログインを実施、パスワードの再設定を行う。 携帯回線契約時には、契約回線での通信をONにして、dアカウントのサイトから携帯回線契約時に設定したパスワードを入力することで、dアカウントに設定したパスワードを確認することができる。
		紛失時	マイナンバーカード紛失時は、警察署で遺失物届の手続きを行い、市区町村窓口に出向いて再発行を行う。	-	-	-	-
		失効・退会	本人の死亡や国外への転出に伴い、住民票から削除された場合は、マイナンバーカードが失効する。	マイページ上より退会可能。	LINEアプリのアカウント削除を実行することで退会が可能。	窓口または郵送にて、必要書類を提示して退会手続きが可能。	回線契約している場合：ｄアカウントの削除を行っても、電話番号と紐づいて情報が残るため、再度作成することで削除前に戻すことができる。 回線未契約時：一度削除すると、削除前に戻ることができない。
	ID登録・身元確認	公的証明書を用いた身元確認なし	-	・gBizID エントリー：誰にでも作成できるアカウントで、審査なしで即日アカウント作成可能。（メールアドレスと、法人の場合は法人番号の確認は行う。） ・gBizID プライム：利用者が法人代表者又は個人事業主本人であることを確認したアカウント。アカウント作成には審査が必要となる。 ・gBizID メンバー：組織の従業員用のアカウント。gBizID プライムによって作成される。	・ID登録：アカウント作成のために、電話番号登録と確認が必須。（2020年4月までは、facebookアカウントを利用してのアカウント作成を可能としていた。） ・年齢確認：青少年保護の観点から一部LINEの機能を利用できるようにするために、通信キャリアの契約情報を使って年齢確認を実施している。	-	いずれかの方法でdアカウントを作成し、回線契約との紐づけ、または身分証明書のアップロードを行わなかった場合。 ・Web ・スマートフォンアプリ
		公的証明書を用いた身元確認あり	マイナンバーカードを受け取る際に、官公署発行の写真付き本人確認書類（住民基本台帳カードや運転免許証など） または、市区町村長が適当と認めるもの2点を使って、対面での身元確認を実施。	・gBizID プライム：利用者が法人代表者又は個人事業主本人であることを確認したアカウント。アカウント作成には審査が必要となる。 ・gBizID メンバー：組織の従業員用のアカウント。gBizID プライムによって作成される。	・身元確認（LINE Payのみ）：LINE Payで送金等の機能を使う際には、身元確認(eKYC)が必要。	登録の申請を行うと、インターネットバンキングサービス用のアカウントと銀行口座の作成が行われる。 ・インターネット：運転免許証と健康保険証の2点の画像を使って身元確認を実施。 ・郵送：下記の2種類の1~5の書類から2種類を使って身元確認を実施。 1：運転免許証コピー 2：マイナンバーカードコピー、住基カードコピー、住民票の写し 3：印鑑登録証明書原本 4：公共料金領収書・請求書原本 ・店舗：対面で運転免許書等の本人が確認できる書類を使って、身元確認を実施。	いずれかの方法でdアカウントを作成し、回線契約との紐づけ、または身分証明書のアップロードを行った場合。 ・Web ・スマートフォンアプリ ・店頭
認証	認証方法	ID/PWによる認証	-	・gBizID エントリー：ID/パスワードでの認証	【LINEログイン(外部サイトとの認証連携)】 ・ブラウザ：ID/パスワードによる認証 【LINEアプリへのログイン】 ・デスクトップアプリ：ID/パスワードによる認証	-	・パスワード認証
		多要素認証	・ICカードリーダライタでのログイン： ICカードリーダライタにマイナンバーカードをセットし、利用者証明用電子証明書パスワードを入力。 ・2次元バーコードでのログイン: マイナポータルAP（スマートフォンアプリ）でバーコードを読み取り、スマートフォンでマイナンバーカードを読み取り、利用者証明用電子証明書パスワードを入力。 ・スマートフォンでのログイン： スマートフォンでマイナンバーカードを読み取り、利用者証明用電子証明書パスワードを入力。	・gBizID プライム：ID/パスワードに加え、スマートフォンアプリまたはSMSでワンタイムパスワード ・gBizID メンバー：ID/パスワードに加え、スマートフォンアプリまたはSMSでワンタイムパスワード	【LINEアプリへのログイン】 デスクトップアプリ：初回のみ ID/PW+LINEをインストールしているスマートフォン上でPINコード入力	・ログイン時：ID/パスワードに加えて、登録している端末以外からのログインなどリスクが高いと判定された場合は、合言葉による追加の確認。	・パスワード＋PIN（メール） ・パスワード＋PIN（SMS）
		その他の認証	-	-	【LINEアプリへのログイン】 ・スマホアプリ：端末認証 ・デスクトップアプリ：QRコード認証	・振込処理時：アプリのワンタイムパスワードまたは乱数表による認証	・FIDO認証 ・回線認証
認証連携	IDプロトコル		非公開	OpenID Connect（認可コードフロー）	OpenID Connect（認可コードフロー）	-	OpenID Connect（認可コードフロー）
	連携しているサービス		国税電子申告納税システム（e-Tax）、ねんきんネット、MyPost(日本郵便)、e-私書箱（野村総研）、総務省 電波利用 電子申請・届出システムLite	社会保険手続きの電子申請、IT導入補助金2020、農林水産省共通申請サービス等20システム	主にB to Cビジネスを展開している多種多様な業界・サービスと連携している。	-	自社サービス、Jリーグオンラインストア、gaccoなど
	認証連携の同意・情報提供の管理等		サービス連携時の同意取得 エンドユーザのマイページから外部サイトに連携した履歴の確認および取り消しの実行	利用規約の同意取得等	サービス連携時の同意取得 マイページより連携しているサービスの解除可能	サービス利用時の同意の取得	自身のデータの提供に関して、どのデータを誰に提供するのか管理できる。 マイページから外部サイトに情報を連携した履歴の確認および取り消しの実行。 パーソナルデータ憲章と、プライバシーポリシーを定め、プライバシーの保護とパーソナルデータを活用する際の利用目的を明示。
関連法制度・ガイドライン等	関連法制度		・行政手続における特定の個人を識別するための番号の利用等に関する法律 ・行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則	・情報通信技術を活用した行政の推進等に関する法律 ・各省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則	犯罪収益移転防止法	犯罪収益移転防止法	携帯電話不正利用防止法 犯罪収益移転防止法
	関連ガイドライン	NIST SP800-63A	アイデンティティ保証レベルIAL3に相当	・gBizID プライム・メンバー アイデンティティ保証レベルIAL2に相当 ・gBizID エントリー アイデンティティ保証レベルIAL1に相当	・通常のLINEアカウント作成時 アイデンティティ保証レベルIAL1に相当 ・LINE Payで身元確認を実施した場合 アイデンティティ保証レベルIAL2に相当	アイデンティティ保証レベルIAL2に相当	・対面で回線契約をしているアカウント アイデンティティ保証レベルIAL3に相当 ・ネット上で回線契約をしている、または身分証明書のアップロードをして本人確認済みのアカウント アイデンティティ保証レベルIAL2に相当 ・回線契約をしておらず、本人確認もしていないアカウント アイデンティティ保証レベルIAL1に相当

マイナンバーは住民票が登録されている住所に通知され、マイナンバーカードを受け取る際には対面で身元確認を行うため、カード発行におけるなりすましは困難である。

マイナンバー法※1 第７条に該当

住民票に住民票コードを記載したときは、
その者に対して、速やかに個人番号通知書
を送付しなければならない。



住民票に登録されている住所に個人番号通知書が送付されるので、**必ず本人に届く。**

マイナンバー法 第17条に該当

市町村が備える住民基本台帳に記録されている者に対し、
その者の申請により、その者に係る個人番号カードを交付する。
当該市町村長は、その者から通知カードの返納及び
前条の主務省令で定める書類の提示を受け、
又は同条の政令で定める措置をとらなければならない。

官公署発行の本人確認書類
・運転免許証
・パスポート
・在留カードなど

マイナンバー法 主務省令※2 第1条に該当

「氏名・生年月日」または
「氏名・住所」が記載され、
市区町村長が適当と認めるもの2点
・健康保険証
・年金手帳
・学生証など

官公署発行の顔写真付きの本人確認書類
または複数の本人確認書類を用いて**対面で**
身元確認を行うため、**なりすましが困難。**

※1 行政手続における特定の個人を識別するための番号の利用等に関する法律
※2 行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則

マイナンバー法では、マイナンバーカードの不正取得や詐欺行為等でマイナンバーを取得した場合の罰則規定が定められている。

第75条 通知カード及び個人番号カードの不正取得

偽りその他不正の手段により通知カード又は
個人番号カードの交付を受けた者は、
六月以下の懲役又は五十万円以下の罰金に処する。

・**他人になりすまして**その者の個人番号カードを取得する行為、**虚偽の請求事由**を記載して個人番号カードの再交付を受ける行為を行った場合適用される。
・人を欺く行為、暴力・脅迫の手段によってこれを取得した場合は、第70条の適用もされる。

第70条 詐欺行為等による情報取得

人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為、その他の個人番号を保有する者の管理を害する行為により、個人番号を取得した者は、三年以下の懲役又は百五十万円以下の罰金に処する。

・**個人番号利用事務等の職員を装って**本人から個人番号を聞き出したり、**暴行、脅迫などの手段**によって相手方の意思に反して個人番号を聞き出す、**個人番号が記録された書面**を盗む行為等を行った場合適用される。

個人情報保護法および関連ガイドライン上では個人データの第三者提供における同意取得を求めているが、具体的な同意取得内容については示されていない。

- 個人情報保護法では個人データの第三者提供における同意の必要性のみ定めている。
- ガイドライン上では同意取得時の指針として同意にあたって判断に必要な情報を「合理的かつ適切な範囲を明確に示すこと」との記載があるが、その指針に沿う具体的な同意取得方法の詳細までは定められていない。運用は各事業者の判断に委ねられており、事業者はガイドライン中の以下事例を参考にするなどして対応しているのが実状である。

個人情報保護法

第二十三条（第三者提供の制限）

個人情報取扱事業者は、次に掲げる場合を除くほか、**あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。**
・・・

個人情報保護法ガイドライン(通則編)

3-4-1.第三者提供の制限の原則

・・・同意の取得に当たっては、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に応じ、**本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示さなければならない。**
・・・

- 個人情報保護法ガイドライン(通則編)における本人の同意を得ている事例（2-12 「本人の同意」）
  - 事例 1）本人からの同意する旨の口頭による意思表示
  - 事例 2）本人からの同意する旨の書面（電磁的記録を含む。）の受領
  - 事例 3）本人からの同意する旨のメールの受信
  - 事例 4）本人による同意する旨の確認欄へのチェック
  - 事例 5）本人による同意する旨のホームページ上のボタンのクリック
  - 事例 6）本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ 等による入力

ISO/IEC 29184では、オンラインにおけるプライバシーと同意を保護するためのガイドラインを提供している。

ISO/IEC 29184の概要

- 2020年6月発行のISO/IEC規格。ISO/IEC 29100 において定められているプライバシー原則のうち、「原則1:同意と選択」および「原則7:開放性、透明性、通知」の実施に関する詳細に相当する。
- オンラインにおけるプライバシー通知の内容と構造を決定する方法、個人を特定できる可能性のある情報を収集および処理することへの同意を求めるプロセスについて定めている。

主な規程事項

- 通知に関する事項
  - 対象者に適切な方法かつ認識しやすい場所で、事前の同意への通知とその補足情報へのアクセスを提供するための考慮事項を記載している。
- 通知の内容に関する事項
  - 対象者が、個人情報がどのように処理され、対象者がどのような権利を有しているかを理解するために、同意への通知内に十分な情報を与えることについての考慮事項を記載している。
- 同意に関する事項
  - 対象者からの同意を、組織が公正かつ撤回可能な方法で取得するための考慮事項を記載している。
- 条件の変更に関する事項
  - 取得した同意に関する事項に重大な変更があった場合に、対象者が再同意する機会を確保するための考慮事項を記載している。

認証基盤の保証レベルを定めるための影響評価基準については検討が求められる。ID連携の活用には、安全性の理解等を含めた普及活動も肝要と考える。

- 認証認可に関する今後の要検討課題について以下の通り整理した。

課題	内容	解決の方向性	主体	時期
保証レベル決定のための影響評価の基準に関する検討	認証基盤において求められる身元確認、当人認証、連携の各保証レベルの決定には、各機能が侵害された場合のサービスへの影響評価が必要であるが、各ガイドラインに示された評価基準は具体性を欠くものとなっている。	• 今後の調査研究において、認証基盤の侵害時の影響評価基準の参考として、典型的なユースケースにおける影響評価事例の調査等を検討する。	情報化担当参事官室	2021年度以降
外部IDの活用のための国民のリテラシー向上と仕様設計	OpenID Connectをサポートする外部ID基盤とのID連携は、今後構築される認証基盤における認証方法の有用な選択肢の1つとなり得る。一方で、外部IDの活用は、そのリスクを十分に理解し、国民が自身の責任において選択することが前提となる。	• 国が主体となって、国民のITセキュリティリテラシー向上のためのガイダンスを行う。 • 国民が自己判断を行うことが出来るよう、外部IDを選択することのメリットに加え、リスクについても十分な説明を行うことが望ましい。	情報化担当参事官室	2022年度以降

医療・健康情報の交換における認証基盤とサービス間のトラストフレームワークの運用、同意における後見人・代理人の認証基盤上の扱いについては、さらなる検討が望まれる。

- 認証認可に関する今後の要検討課題について以下の通り整理した。

課題	内容	解決の方向性	主体	時期
認証基盤とサービス間のトラストフレームワークの具体的な運用に関する検討	医療・健康情報の取得における同意省略の検討において、認証基盤とサービス間のトラストフレームワークが必要となる可能性を確認した。実現に向けては、トラストフレームワークの具体的な運用について検討が必要となる。	• 今後の調査研究において、トラストフレームワークの運用主体、具体的な対象サービス、連携技術方式等の審査事項について検討する。	情報化担当参事官室	2021年度以降
後見人・代理人の同意に関する検討	医療福祉分野においては後見人、代理人等、第三者が当人の情報提供や行為に対する同意を行うケースが多岐に渡り存在する。 同意を行う者が、正しい後見人・代理人であることをどの組織が管理し、その正当性の検証をどのように行うべきか、さらなる検討が必要である。	• 今後の調査研究において、典型的なユースケースにおける後見人・代理人による権限移譲の際の後見人・代理人の表現方法、検証方法について検討する。	情報化担当参事官室	2021年度以降

OpenID Connect CIBAの各種パラメータは、ユースケースに応じた設計検討が必要。電子的な同意に関する運用等の詳細については検討の余地がある。

- 認証認可に関する今後の要検討課題について以下の通り整理した。

課題	内容	解決の方向性	主体	時期
OpenID Connect CIBAの適用シーンおよび各種パラメータの検討	本調査研究では、患者の同意に基づく第三者への医師への医療・健康情報提供におけるCIBAの適用について検証を行った。認証主体を指定するパラメータの選定方法等の一部パラメータについては、ユースケースおよび前提システム構成に基づくパラメータ検討が必要となる。	• 今後、認証基盤を構築する組織において、要件定義および設計工程にて具体的な仕様を検討する。	認証基盤構築組織	2021年度以降
同意の行為を裏付ける法制度およびガイドラインの検討	現行法制度では、個人情報の第三者提供の同意について、具体的な取得方法、管理項目等については明確には定められていない。各認証基盤やサービス間の情報交換の仕組みが今後整備普及する場合、同意に関する運用等の詳細を具体的に示すことについて検討の余地がある。	• 既存の運用やガイドライン等を踏まえ、同意が必要となるケースを整理すると共に、その具体的な提示方法、管理方法等を定める。	情報化担当参事官室	2021年度以降

NRI SECURE