認証認可の調査研究

最終報告書

2020年09月25日

NRIセキュアテクノロジーズ株式会社

目次

1. はじめに
2. 調査研究の概要
3. OpenID FoundationとFIDO Allianceの基本的情報の整理
4. 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
5. 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
6. 普及している認証基盤の活用に関する調査
7. 同意の表現方法に関する調査
8. おわりに

© NRI SecureTechnologies, Ltd.

1. はじめに

© NRI SecureTechnologies, Ltd.

本報告書について

本報告書は、令和二年度厚生労働省委託事業「認証認可の調査研究」（以下、本調査研究）の成果をとりまとめたものである。本調査研究では、医療福祉分野におけるITおよびデータ利活用の推進状況および直近の認証認可技術の進展を踏まえ、近年普及が進んでいる認証および認可の技術規格であるOpenIDおよび FIDOを中心に調査検討を実施した。

本報告書の構成を以下に示す。

１．はじめに

本報告書の構成と各章の記載事項の概要を示す。

２．調査研究の概要

本調査研究の背景、目的、調査事項の概要を示す。

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

OpenID および FIDO 規格の標準化団体および主な規格について示す。

４．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

既存の認証基盤として運用されている公的個人認証基盤（JPKI）および保健医療福祉分野公開鍵基盤（HPKI）の概要および活用方法、属性情報交換に関する技術的観点での机上検討内容を示す。

５．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

個人の認証および同意を通して、第三者に対して個人の属性情報を提供するユースケースについて、OpenID Connect および FIDO を利用した実現方式の検討および一部機能実証について示す。

© NRI SecureTechnologies, Ltd.

本報告書について

６．普及している認証基盤の活用に関する調査

既に世の中に普及している認証基盤について、具備している機能、関連する法制度、ガイドラインの概要を示す。

７．同意の表現方法に関する調査

同意に関する現行の国内外の法制度およびガイドラインの調査内容、オンラインにおいて同意を取得する際の同意表現方法に関する規定等の調査結果を示す。

８．おわりに

各調査テーマの調査結果のポイントおよび今後に向けた課題と解決の方向性について示す。

© NRI SecureTechnologies, Ltd.

2. 調査研究の概要

© NRI SecureTechnologies, Ltd.

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。**

© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

各団体が策定している認証認可に関する規格のうち、今後の認証認可機能の整備に向けて特に有用と考えられるものについて整理を実施した。

OpenID Foundation の概要

- OpenID関連技術の有効化、促進、保護に取り組む個人および企業の非営利国際標準化組織。
- 規格の拡張や各業種での活用について検討する複数のワーキンググループが活動しており、医療ドメインでの適用については、HEART (Health Relationship Trust) ワーキンググループ がその役割を担っている。

主な調査対象規格

規格	概要	調査の効果
OpenID Connect Core 1.0	OpenID Connectの基本的なアクターや処理シーケンスを規定。	OpenID Connectに基づく認証認可の仕組みを実現するベースとして活用する。本調査研究における機能実証の対象として、理解を深める。
OpenID Connect Security Consideration	OpenID Connectを実装する際の一般的なセキュリティ考慮事項をガイドする。	OpenID Connectベースのシステム間連携のセキュリティを高めることが可能となる。
OpenID Connect Client Initiated Backchannel Authentication Flow (CIBA)	クライアントが起点となり、ユーザー認証を経てクライアントに対するリソースアクセスを可能とする処理仕様を規定。	医師が患者の情報にアクセスする際に、患者の認証・同意にもとづき情報を提供する仕組みを実現する方式として活用する。本調査研究における機能実証の対象として理解を深める。
Health Relationship Trust Profile for OAuth 2.0	OpenID Connectの土台となっているOAuth2.0仕様を医療ドメインに適用する場合のプロファイルおよび考慮事項について規定。 HEARTワーキンググループにて策定。	OpenID Connectを医療ドメインでの活用に最適化することが可能となる。

© NRI SecureTechnologies, Ltd.

各団体が策定している認証認可に関する規格のうち、今後の認証認可機能の整備に向けて特に有用と考えられるものについて整理を実施した。

FIDO Alliance の概要

- 端末認証など、ID・パスワードに依らない認証手段を提供するFIDO規格を策定する非営利国際標準化組織。

主な調査対象規格

規格	概要	調査の効果
FIDO2	デバイスの組み込み認証システムなどを使用して、Webシステムにおけるパスワードレス認証、二要素および多要素認証をサポートする仕様。	FIDOに対応するWebブラウザおよび端末によるパスワードレス認証を実現する。本調査研究における機能実証の対象として理解を深める。
FIDO UAF	FIDO UAFをサポートするデバイスにより、パスワードレスの認証をサポートする仕様。	ユースケースや仕様について、FIDO2との差異を明らかにする。
FIDO U2F	Webサービスでユーザーログインに強力な第2要素認証を追加するための仕様。	ユースケースや仕様について、FIDO2との差異を明らかにする。

© NRI SecureTechnologies, Ltd.

JPKI・HPKIに関して、属性情報連携および認証機能の利用、認証フェデレーション機能の利用の両面において、適用する場合の実現方法を机上検討した。

本テーマについては以下のとおり調査、検討を行った。

JPKI・HPKIの基本情報の整理

- JPKI、HPKIの概要と主な提供機能について整理する。

JPKI・HPKIの適用検討

- JPKI、HPKIの提供機能に基づき、医療・介護の現場で適用可能なユースケースを検討する。
- 想定したユースケースにおける属性情報交換の方式（処理シーケンス等）について検討する。
- 検討した方式の実装および運用上の課題について考察する。

JPKIの適用仮説

- JPKIでは、マイナンバーカード内の電子証明書から基本4情報(氏名、住所、性別、生年月日)を取得するAPIインターフェースを提供している。また、マイナポータルでは、行政機関が保持する情報を提供する「自己情報取得API」を提供している。これらのAPIを活用したID登録時の本人確認、ユーザー認証の実現性について検討する。

HPKIの適用仮説

- HPKIは、SAML(※)による認証連携の仕組みを提供している。医療福祉事業者の認証においてSAMLを適用することを想定し、実装・運用上の考察を行う。

(※)SAML：Security Assertion Markup Language の略。インターネット上のサイト間でユーザー認証を行うための標準規格の1つ。

© NRI SecureTechnologies, Ltd.

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、全体像の検討および実機実証を行った。

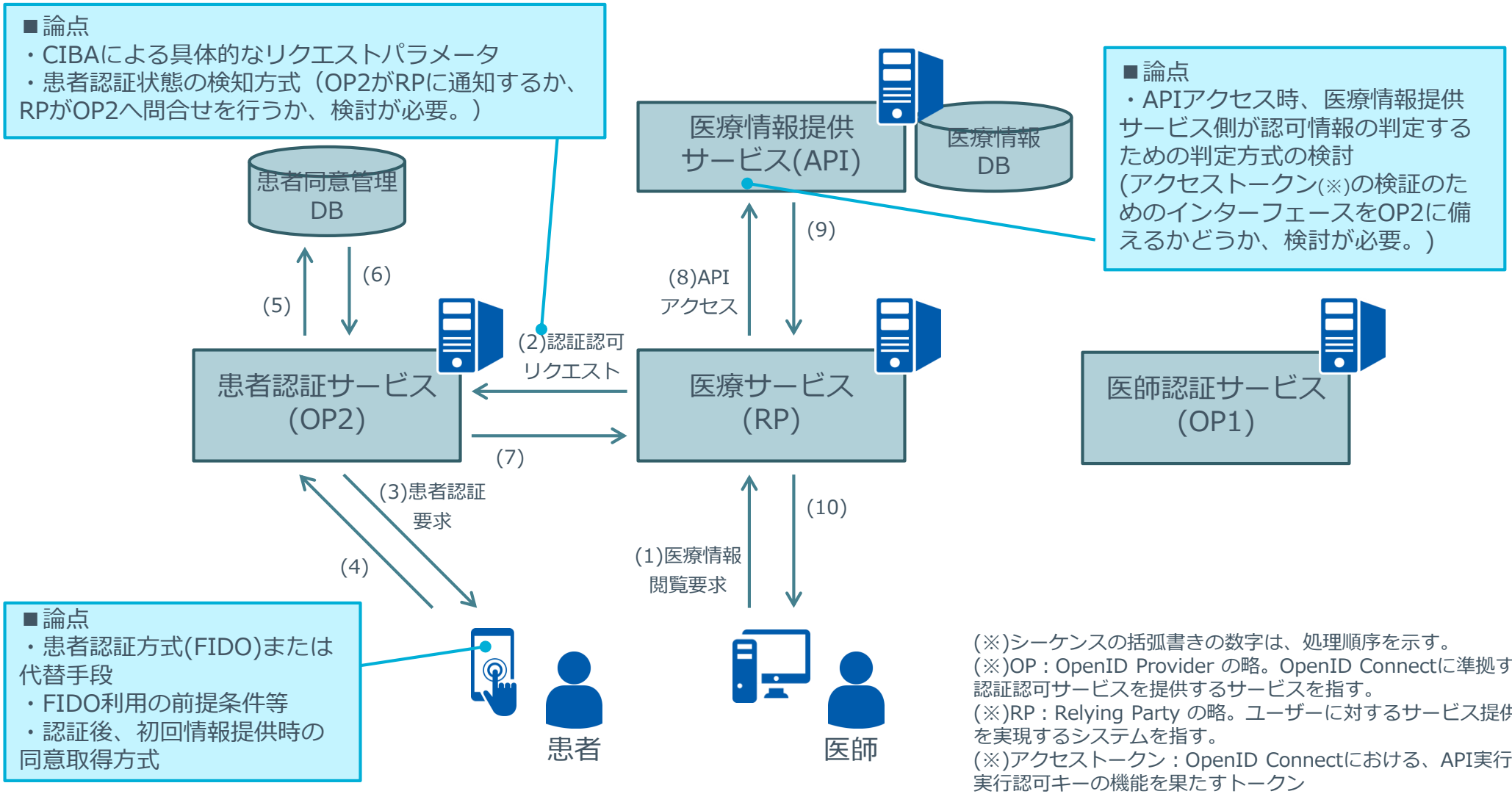
本テーマについては以下のとおり調査、検討を行った。

- 「OpenID FoundationとFIDO Allianceの基本的情報の整理」において調査したOpenID Connect、CIBA および FIDO の仕様に基づき、構成要素、処理シーケンス、適用パラメータを整理する。
  - OpenID Connect および CIBAは、ある医療サービスと、医師または患者のユーザー認証サービス間のセキュアな連携、医療情報取得(API実行)のための認可機能を実現するために適用することを想定する。
  - FIDOは、患者が認証を求められた場合の認証手段として利用することを想定する。
- 処理シーケンスや、適用パラメータの検討にあたっては、OpenID FoundationのHEARTワーキンググループが発信している考慮事項や、患者に対する同意取得の方法に関しても考慮する。
- 検討した構成については、標準規格の策定団体（OpenID Foundation およびFIDO Alliance）の有識者への確認を行った。
- 整理した構成、シーケンス、適用パラメータに基づき、前頁の実証シナリオを検証可能な実証環境を実装した。

© NRI SecureTechnologies, Ltd.

検討済の全体構成、処理シーケンスにおいて、複数の論点があると想定し、本検討活動を通して、機能実現に最適かつ検証に必要な情報を整理した。

構成検討イメージ(医師ログイン後、患者認証～医療情報取得)と主な論点



(※)シーケンスの括弧書きの数字は、処理順序を示す。
(※)OP：OpenID Provider の略。OpenID Connectに準拠する認証認可サービスを提供するサービスを指す。
(※)RP：Relying Party の略。ユーザーに対するサービス提供を実現するシステムを指す。
(※)アクセストークン：OpenID Connectにおける、API実行の実行認可キーの機能を果たすトークン

© NRI SecureTechnologies, Ltd.

普及している複数業種の認証基盤について、デスクトップ調査・ヒアリング調査を通して運用の現状を整理した。

本テーマについては以下のとおり調査、検討を行った。

調査方法

- デスクトップ調査：Web・書籍等の公開情報を元に調査を実施。
- ヒアリング調査（必要に応じて実施）：各システムの運用担当者等、有識者にヒアリングを実施。

調査対象システム

調査対象システム	業界	選定理由
マイナポータル	官公庁	日本国民に発行されるマイナンバーカードを使ってアクセスする、政府が運営するオンラインサービスであり、子育てや介護などの行政手続きができるなど、G to Cで影響度が大きいサービスであるため。
gBizID	官公庁	法人や個人事業主向けに発行されるIDで、様々な行政サービスを利用する際に使うことができるなど、G to Bで影響度が大きいサービスであるため。
LINE ID	IT	日本国内だけで8300万人以上の月間アクティブユーザ数が存在する国内有数のSNSであるため。
Value direct	金融	野村総合研究所が開発したインターネットバンキングシステムで、信用金庫や地方銀行など多数の採用実績があるため。
dアカウント	通信	国内最大手の通信事業であるNTTドコモが発行する共通IDであるため。

© NRI SecureTechnologies, Ltd.

調査システムの概要、システムの機能と運用、法制度とガイドラインとの関連性について合わせて調査を行った。

調査項目

- 調査システムの概要、利用システム普及の状況（登録ID数等）
- システム機能、運用
  - ID登録、身元確認（KYC有無等）の運用方式
  - 認証手段（ID/パスワード、2段階認証等）
  - ID管理に関する事項（情報更新、利用不能時のリカバリー方法、ID削除方法等）
  - セキュリティ向上のための機能（ログイン日時表示、ログインアラート等）
- 具備する機能と関連法制度・ガイドラインの関連について

© NRI SecureTechnologies, Ltd.

電子的な形で本人同意を取得に関連する現行法制度についてデスクトップ調査を行い、具体的な同意取得シナリオとの関連を整理した。

本テーマについては以下のとおり調査、検討を行った。

想定する調査対象法制度

- 改正個人情報保護法
- GDPR (EU一般データ保護規則)
- eプライバシー規則
- CCPA (カリフォルニア州消費者プライバシー法)
- India Stack DEPAにおける Electronic Consent Framework

調査方法

- 法制度、同意取得シナリオは、デスクトップ調査を行う。
- 調査した法制度、同意取得シナリオに基づき、関連を考察し、整理する。
  - 調査結果は、後続工程における利用者認証基盤の同意取得方式検討に活用できるよう考慮する。

調査項目

- 法制度の概要
- 各法制度において同意を求める対象、同意の取得方法
- 実在する同意取得シナリオと法制度における同意取得規定の関連の整理
  - ID連携における属性（個人情報）提供の同意取得
  - 医療・介護等の現場での同意取得
  - 他業種（金融業等）での同意取得

© NRI SecureTechnologies, Ltd.

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

© NRI SecureTechnologies, Ltd.

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）

© NRI SecureTechnologies, Ltd.

OpenID Foundationでは様々な作業部会(Working Group)が存在し、それぞれの団体や業界に適したOpenID Connect仕様のプロファイルの策定が行われている。

作業部会 (2020年9月時点)

- AB/Connect
  - OpenID Connectに関する主要な仕様（**OpenID Connect Core 1.0**など）の策定を行っている。
- Mobile Operator Discovery、Registration & autheNticAtion（MODRNA）
  - RPにIDサービスを提供する移動体通信事業者や、それらのサービスを利用するRPを対象に、それらに適したOpenID Connectのプロファイル(**Client Initiated Backchannel Authentication (CIBA)**)の策定を行っている。さらにOpenID Connectの拡張仕様として、の仕様策定を行っている。
- HEART（Health Relationship Trust）
  - 個人が健康に関するデータ共有のためのAPIのアクセス権限を管理すること可能にするための、プライバシーとセキュリティに関するプロファイル(**Health Relationship Trust Profile for OAuth 2.0**)の策定を行っている。
- International Government Assurance Profile（iGov）
  - OpenID Connectのセキュリティとプライバシーのプロファイルを作成し、ユーザーが認証を行い、同意を得た属性情報を世界中の公共部門サービスと共有することを可能にするOpenID Connectのセキュリティとプライバシーのプロファイル策定を行っている。
- Financial-grade API (FAPI)
  - アプリケーションが金融機関口座と連携できるようにするため、セキュリティとプライバシーに関する推奨事項とプロトコルを提供するための活動を行っている。

© NRI SecureTechnologies, Ltd.

OpenID Foundationでは様々な作業部会(Working Group)が存在し、それぞれの団体や業界に適したOpenID Connect仕様のプロファイルの策定が行われている。

作業部会 (2020年9月時点)

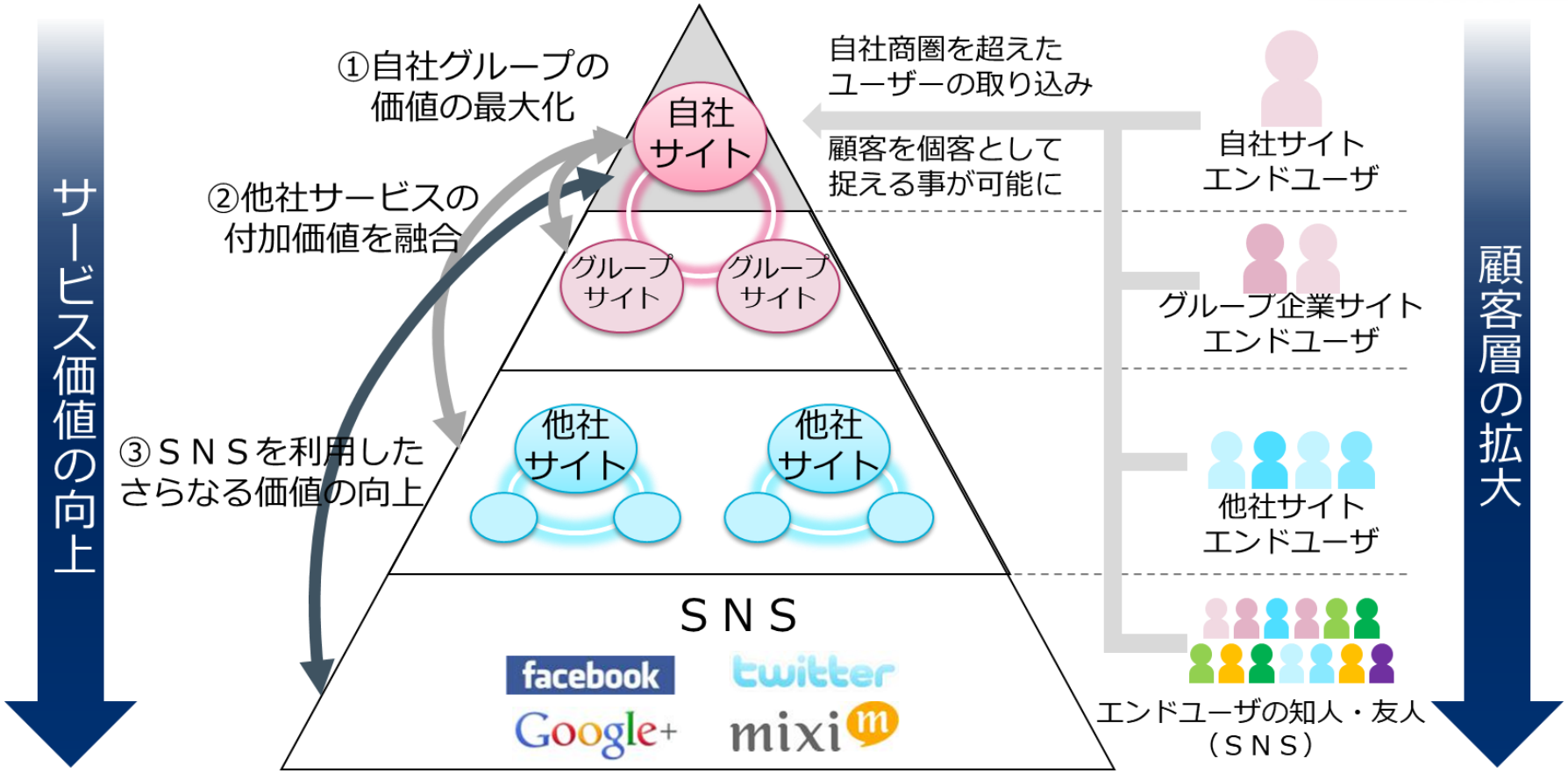
- Enhanced Authentication Profile (EAP)
  - ユーザーが強度の高い認証仕様を使用して、OpenIDプロバイダへの認証を可能にするための、OpenID Connectのセキュリティおよびプライバシープロファイルの策定を行っている。OpenID ConnectでのIETFトークンバインディングの使用、およびFIDOや他の強度の高い認証仕様との統合を行ったプロファイル策定を行っている。
- eKYC-IDA
  - RPにアイデンティティ情報（検証されたクレーム、およびそれらのクレームをいつ、何を、どのように、どのようなルールに従って、どのような証拠を使用したかなど、検証状況の情報）を提供するためのOpenID仕様の開発を行っている。
- FastFed
  - 管理者がOpenID Connect、SAML、SCIM を1つ以上をサポートするIDプロバイダとアプリケーションを連携させて、ID プロバイダとホストされたアプリケーション間で設定変更のための通信ができるようにするための、メタデータ文書仕様、API、およびワークフローを開発を行っている。
- Research & Education (R&E)
  - 研究・教育 (R&E) セクターにおける OpenID Connect の採用を容易にするために、OpenID Connect 仕様の一連のプロファイルの開発を行っている。
- Shared Signal & Events
  - セキュリティイベント、状態変化、およびその他のシグナルを、関連するシステムや依存するシステム間で共有して、リソースへのアクセス管理、悪意のあるアクターがシステムやリソースに不正アクセスすることを防止する、エンドユーザー、管理者、サービスプロバイダーが連携してインシデントを検出できるようにすることを目指している。

© NRI SecureTechnologies, Ltd.

OpenID Connectは、ID連携とAPI連携をセキュアに行うための規格。自社のみのサービス提供から、様々な企業を巻き込んだサービス提供が可能になる。

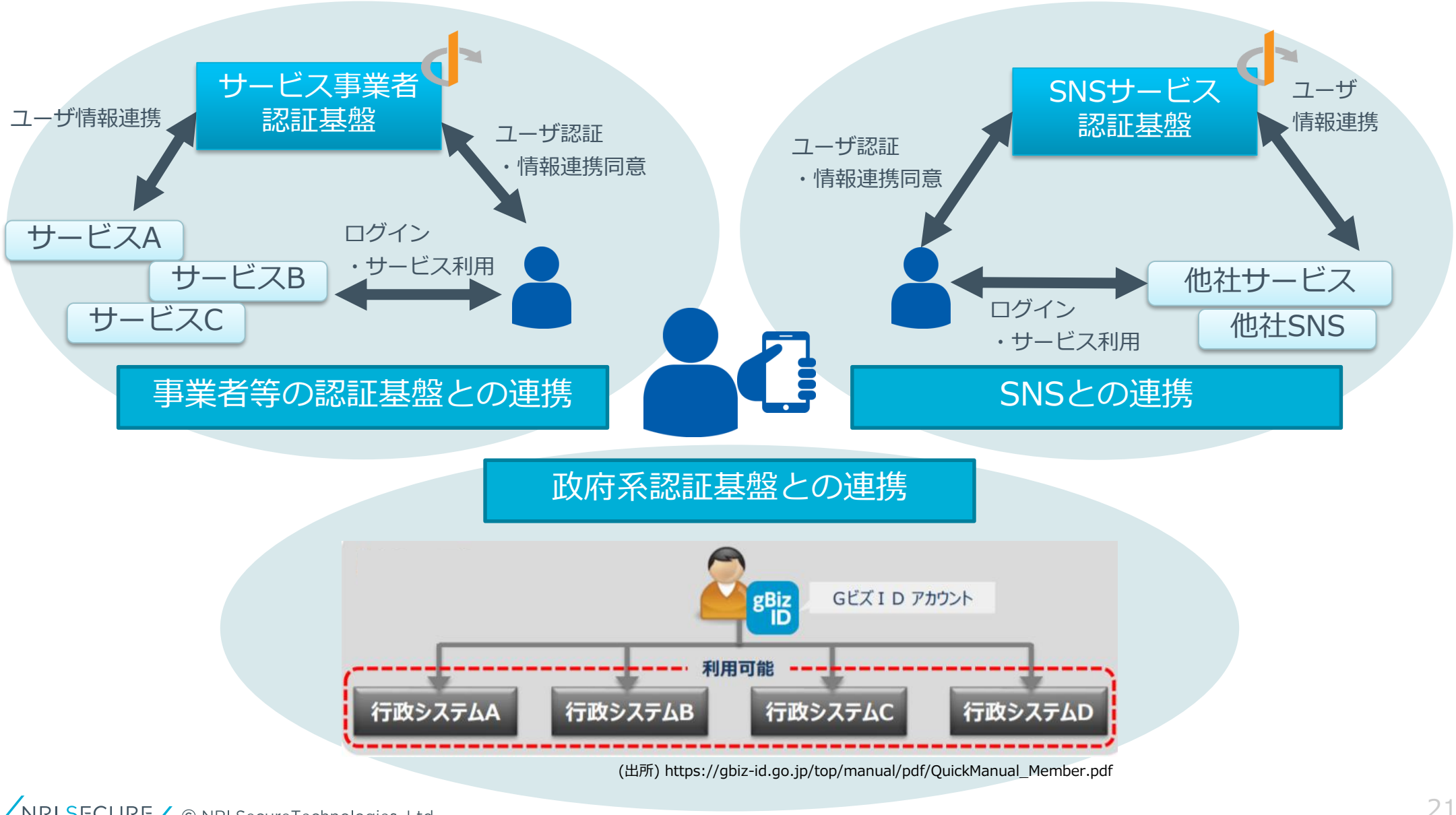
- OpenID Connectを使うことで、自社サイトだけでなく他社サイトとの連携もすることができ、より多くのエンドユーザに自社サイトを使ってもらうことができるようになる。

引用元：https://openid.net/



© NRI SecureTechnologies, Ltd.

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

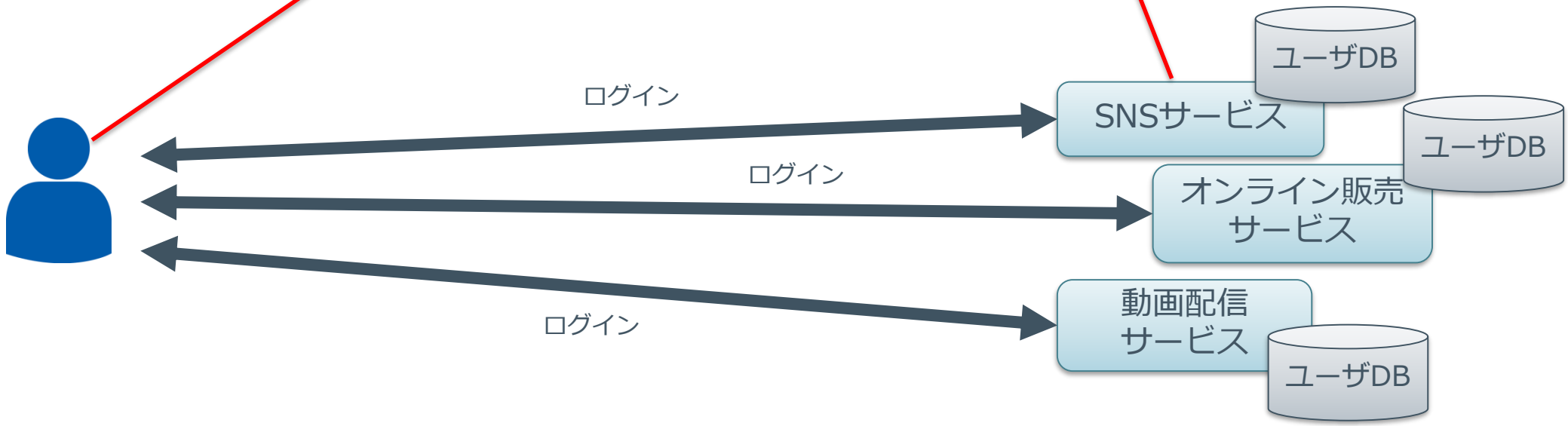
© NRI SecureTechnologies, Ltd.

近年では1ユーザが複数のサービス/アプリケーションを利用することが一般的となり、認証連携の仕組みを利用しない場合にセキュリティ面での課題が発生する。

- OpenID Connectなどの認証連携を利用しない場合、ユーザはサービスごとに認証情報を登録の上で管理する必要がある。その結果、ユーザ側及びサービス側のそれぞれについて以下の課題が発生する。

【ユーザ側の課題】
ユーザがサービスごとに認証情報(ID/パスワード等)を覚える必要がある。
→覚えやすい(推測されやすい)パスワードを使うことで、攻撃者にパスワードを推測されるリスクがある。

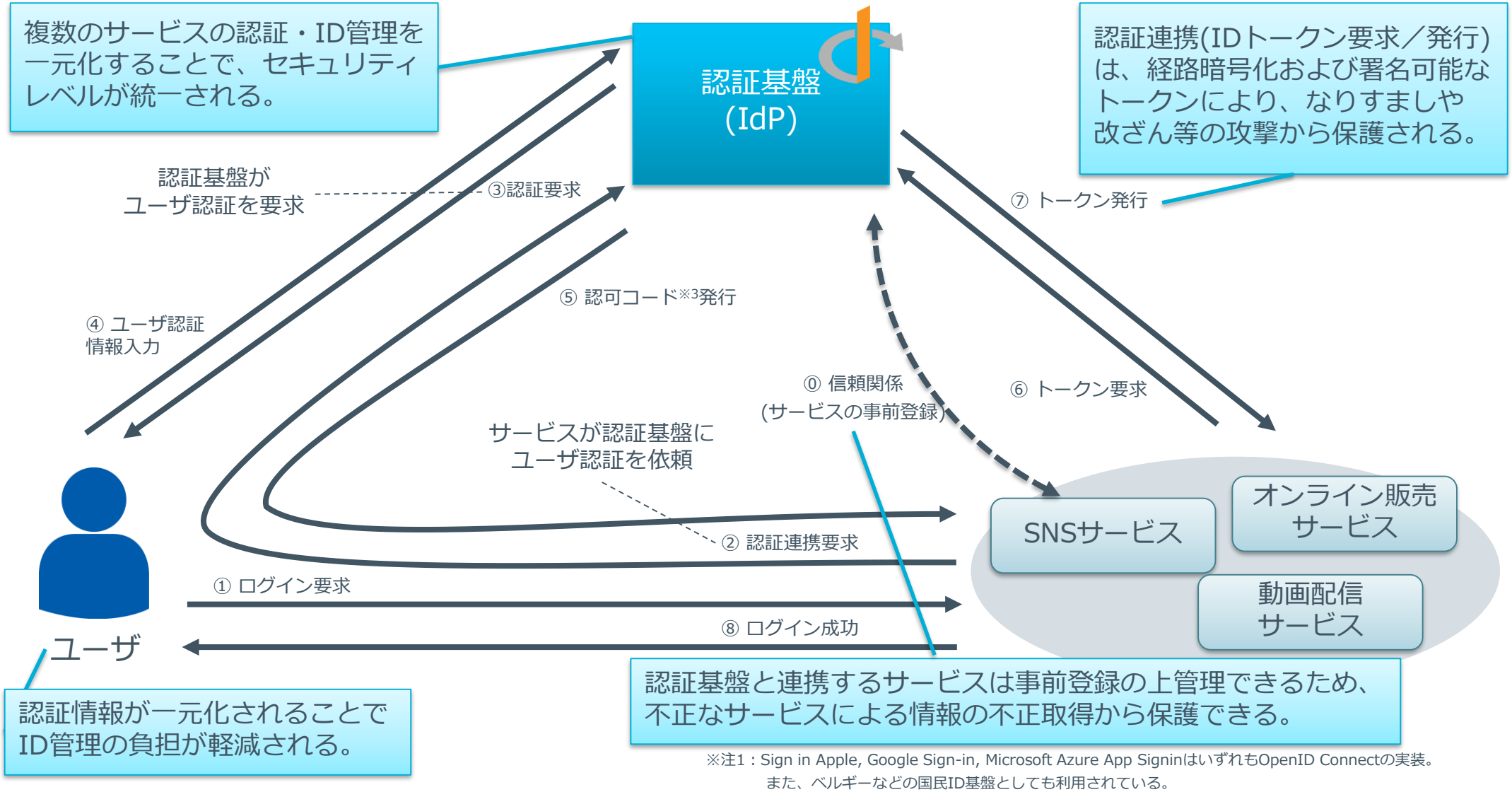
【サービス側の課題】
認証・ID管理を各サービスが実装することで、セキュリティレベルがバラバラになる。
・ID管理手法(データ暗号化、運用など)
・サポートするユーザ認証方式
（ID/パスワード認証のみ・OTP認証・生体認証など）



© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

異なるサブシステム間でのID連携、API連携プロトコルにおいて「標準」を使うことは以下のような意義があり、保健医療分野においても活用する価値がある。

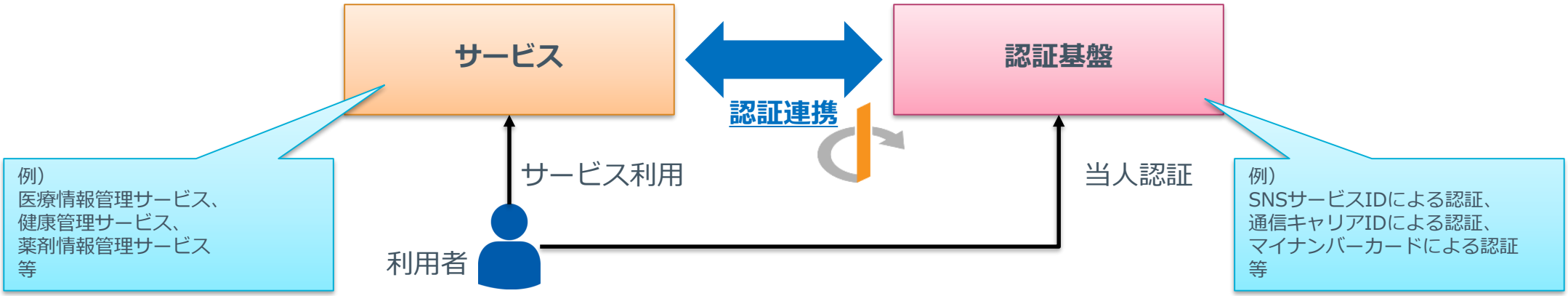
標準的なプロトコルを使うことの意義として、以下のポイントが挙げられる。

- **セキュリティ・プライバシー対策と答責性**
  - 認証サーバ、認可サーバ、クライアントの成りすまし、中間者攻撃、再生攻撃、トークン置換攻撃等各種攻撃に対する耐性を考慮された設計となっている。
  - プライバシーコントロールを考慮してプロトコルユースケースの設計が行われている。（同意管理、スコープ管理）
  - 外部に対してセキュリティ標準を遵守していること、一定のセキュリティ対策水準を満たしていることのアカウンタビリティ。
- **ユースケースの拡張性**
  - デバイスタイプ、アプリケーションタイプの拡張性を意識した設計となっている。
  - サードパーティー（信頼度の下がるクライアント）からのサービス連携に対して適切な最小限の認可範囲、有効期限をグラントするための枠組みを有する。
- **テストツールの利用可能性**
  - OpenID ConnectやFIDOについては、それぞれの仕様を策定しているOpenID FoundationおよびFIDO Allianceより実装が仕様通りに行われているか確認するためのテストツールが提供されている。テストツールを活用することで、接続システム間の相互接続性を確保するとともに、テスト工数と時間を大幅に削減することができる。
- **相互接続の容易性**
  - 標準であるため、仕様がオープンであり多くの製品ライブラリが対応しているため、サードパーティーからの接続性を確保しやすい。また、接続容易性は相互セキュリティ維持につながる。（カスタム仕様の場合、誤認識、誤用途による脆弱性を生む可能性がある。）
- **実装コストの削減**
  - 仕様がオープンであり、多くの製品やライブラリが対応している。それらを活用することで、仕様をゼロからスクラッチで実装する場合と比較して、実装にかかるコストを抑えることができる。

© NRI SecureTechnologies, Ltd.

保険医療福祉分野のサービスにおいても、OpenID Connectを通して普及している認証基盤(外部ID)との認証連携によりサービス提供も可能である。

- サービスを患者が利用するにあたり、普及し多くのユーザに利用されている認証基盤とOpenID Connectを利用した認証連携を行うことで、ユーザは自分が日頃利用している認証基盤の認証方式を使い医療サービスへのログイン及びサービス利用を行う。
  - 利用者にとっては、普段活用しているIDを利用することで、サービスの利用開始の登録手続きの負担や認証情報管理の負担が軽減される。
  - サービスにとっては、認証基盤およびID管理の実装負荷を一部軽減することができる。
- OpenID Connectが正しく利用されているシステムにおいては、サービスと認証基盤は一定のセキュリティをもって連携がなされるため、外部IDと連携する前提であっても、安心してサービスを利用することができる。一方で、認証基盤が何らかの理由で利用できなくなることにより、利用者の医療サービス利用に影響が出る等のリスクもゼロではないため、利用者は、その利用のリスクを正しく理解した上で外部IDを利用することが期待される。
- サービスの利用者が、外部ID連携も含めて安心してサービスを利用することは、サービスと認証基盤が適切なIDの保証レベルの下で運用されていることが前提となる。**サービスと認証基盤には、サービス提供に必要かつ適切なIDの保証レベルを定め、運用することが求められる。**
  - ID連携における適切な保証レベルの担保については、NIST SP800-63-3Cの「5.1.3 Federation Authorities」にて言及されている。



© NRI SecureTechnologies, Ltd.

インターネットセキュリティにおいては、「認証」と「認可」の概念は明確に区別されており、OpenID Connectの活用の際にはこれらの理解が必要である。

- インターネットセキュリティにおいては、「認証」と「認可」は以下の通り区別される。

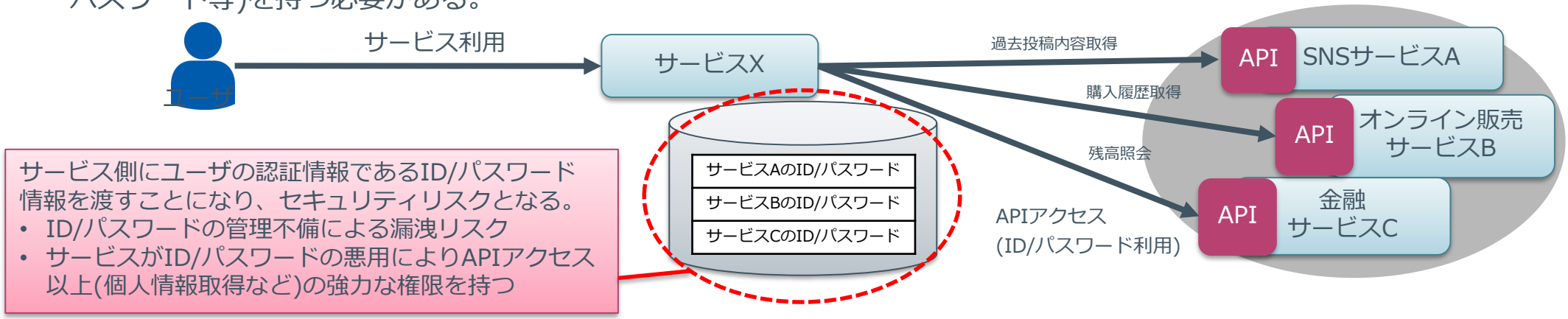
用語	説明	例	主な規格
認証	相手が誰（何）であるか確認すること。	SNSサービスが、アクセスしてきたユーザについて入力されたID/パスワードを基にユーザAであると識別する。	OpenID Connect、SAML
認可	特定のリソースへのアクセスを許可すること。	SNSサービスが、別サービスに対してユーザAの個人情報へのアクセスを許可する。	OAuth 2.0

- 一般的には認可を行う際には誰のリソースへのアクセスを許可するか識別するためにユーザの認証処理が行われる。
  - 認証を行わずに認可を行うケースも存在する。（例：特定のIPアドレスからのアクセスはどのユーザであっても許可する場合など）

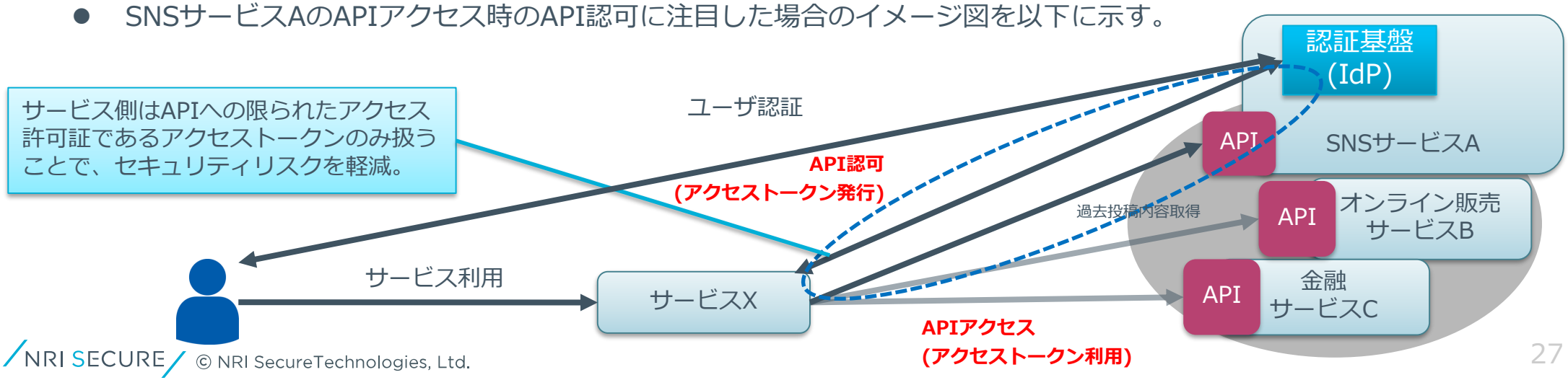
© NRI SecureTechnologies, Ltd.

近年のオンラインサービスではAPIを通した別サービスとの連携(マッシュアップ)が増えている。APIアクセス制御においてもOpenID Connectの仕組みが活用できる。

- 複数サービスのAPIを呼び出す場合、サービスXは各サービスのAPI呼出しのためにユーザの各サービスでの認証情報(ID/パスワード等)を持つ必要がある。



- OpenID Connect(およびそのベースとなるOAuth 2.0)の活用により、安全に認証連携およびAPI認可を行うことが可能となる。
  - SNSサービスAのAPIアクセス時のAPI認可に注目した場合のイメージ図を以下に示す。



© NRI SecureTechnologies, Ltd.

OpenID Connectを同じ認証連携の規格であるSAMLと比較した場合、サービス側での実装しやすさやAPI認可への対応の観点でOpenID Connectの利用が適している。

- OpenID ConnectとSAMLに関して、「認証連携」、「API認可」、「サービス(RP)側の実装容易性」の観点から比較した表を以下に示す。

方式	認証連携	API認可	サービス(RP)側の実装容易性
OpenID Connect	認証結果の連携やセキュリティ対応(署名・暗号化)について一通りサポート。**Webアプリの他にスマートフォンアプリケーションにも広く利用**されている。	OpenID Connectのベースとなっているの OAuth 2.0の利用により**API認可もサポート**	Webアプリ、スマートフォンアプリにおいて**汎用的なデータ形式であるJSON/REST形式を採用**し、実装は容易
SAML 2.0	認証結果の連携やセキュリティ対応(署名・暗号化)について一通りサポート。仕様上Webアプリ以外にも対応可能だが、現状ではWebアプリの利用が中心。	SAMLは認証連携の規格であるため、単独ではAPI認可はサポートしない。	XML/SOAP形式を採用しているため、一般的に実装の際にはSAML処理ライブラリやミドルウェアの導入が必要となる

© NRI SecureTechnologies, Ltd.

OpenID Connect Core は、OpenID Connectの骨子となる仕様を定めている。現在の最新版は1.0であり、2014年11月に策定されている。

- OpenID Connect Coreの仕様目次を以下に示す。
- 青字でタイトルを記載している章は、詳細を別添資料1に記載している。

章番号	タイトル	概要
1	**Introduction**	OpenID Connect Core 1.0仕様の紹介。Open ID Connectは、OAuth2.0のプロトコル上に、アイデンティティレイヤーを付与したことを述べている。
2	**ID Token**	IDトークンは、OpenID ConnectがOAuth2.0に追加する最大の拡張機能であり、ユーザの認証情報を持ったトークンであることを述べている。
3	**Authentication**	OpenID Connectで定義している認証フローである、認可コードフロー、インプリシットフロー、ハイブリットフロー、についての説明を行っている。
4	Initiating Login from a Third Party	ログイン主体がRPからでなく、3rd Partyから開始する際のフローについて規定している。
5	**Claims**	クライアントが、エンドユーザと認証に関するイベントで、ユーザ属性の種類とを取得方法について定義している。
6	Passing Request Parameters as JWTs	認可要求に、署名及び暗号化を可能にするための仕様を定義している。
7	Self-Issued OpenID Provider	自己署名つきの ID トークンを発行し、self-hostedなOPをサポートするための仕様について規定している。
8	Subject Identifier Types	Subject Identifierは、クライアントによって利用されるエンドユーザの識別子で、その仕様について定義されている。
9	**Client Authentication**	クライアントがトークンエンドポイントにアクセスする際に、認可サーバで自身を認証するための方法を定義している。

© NRI SecureTechnologies, Ltd.

OpenID Connect Core は、OpenID Connectの骨子となる仕様を定めている。現在の最新版は1.0であり、2014年11月に策定されている。

- OpenID Connect Coreの仕様目次を以下に示す。
- 青字でタイトルを記載している章は、詳細を別添資料1に記載している。

章番号	タイトル	概要
10	**Signatures and Encryption**	JSON Web Signature(JWS)とJSON Web Encryption(JWE)をつかって、コンテンツの暗号化と署名を行うための仕様について記載されている。
11	Offline Access	OAuth2.0 リフレッシュトークンの発行要求するためのscope値に関して定義している。
12	**Using Refresh Tokens**	認可サーバが、リフレッシュトークンを受け取った際の挙動について定義されている。
13	Serializations	メッセージをシリアライズする方法の構文について定義されている。
14	String Operations	OpenID Connectのメッセージを処理する際に、メッセージの中の既知の値を比較することが求められるが、その際の手順について定義されている。
15	**Implementation Considerations**	RPとOPの両者によって使用される機能について定義されている。
16	**Security Considerations**	RFC6750、6819、ISO/IEC29115を参照して、実装者が考慮すべきセキュリティ事項に関して説明されている。
17	**Privacy Considerations**	OpenID Connectのフローにおいて、個人情報保護の観点から考慮すべき事項について述べられている。
18	IANA Considerations	OpenID Connectで定義しているJWTのクレーム、OAuthのパラメータ、エラー種別を、JWT及びRFC6749に登録するということが述べられている。

© NRI SecureTechnologies, Ltd.

MODRNA WGでは通信キャリア向けに仕様書やプロファイルの策定を行っており、その中の1つにCIBAがある。

MODRNA（Mobile Operator Discovery, Registration & autheNticAtion）の活動

- MODRNA WGは、RPにIDサービスを提供する通信キャリアや、それらのサービスを利用するRPを対象に、それらに適したOpenID Connectのプロファイルの策定を行っている。
- MODRNA WGで策定されている仕様書（実装者ドラフト版）は下記の4つであり、その中にCIBAも含まれる。
  - OpenID Connect MODRNA Authentication Profile
  - OpenID Connect Account Porting
  - OpenID Connect User Questioning API
  - **OpenID Connect Client Initiated Backchannel Authentication Flow – Core**

© NRI SecureTechnologies, Ltd.

OpenID Connect CIBAは、サービス利用と認証・認可を行うデバイス・ユーザーを分離したいというユースケースを実現するための考え方である。

OpenID Connect CIBAができた背景

- OpenID Connect Coreでは認可、認証の代表的なフローとして認可コードフローが多く使われているが、サービスを利用するユーザー自身が認証・認可を行う流れとなっている。
- 認可コードフローは、**多様なデバイス（例えば、スマートスピーカーやIoT、POSなど）への対応や、第三者がユーザーの同意に基づいてAPIを実行できるような仕様にはなっていない。**
- そこで、サービス利用と認証/認可を行うデバイス・ユーザーを分離したいというユースケースを実現するために生まれた考え方がOpenID Connect CIBAである。

OpenID Connect CIBAのユースケース例

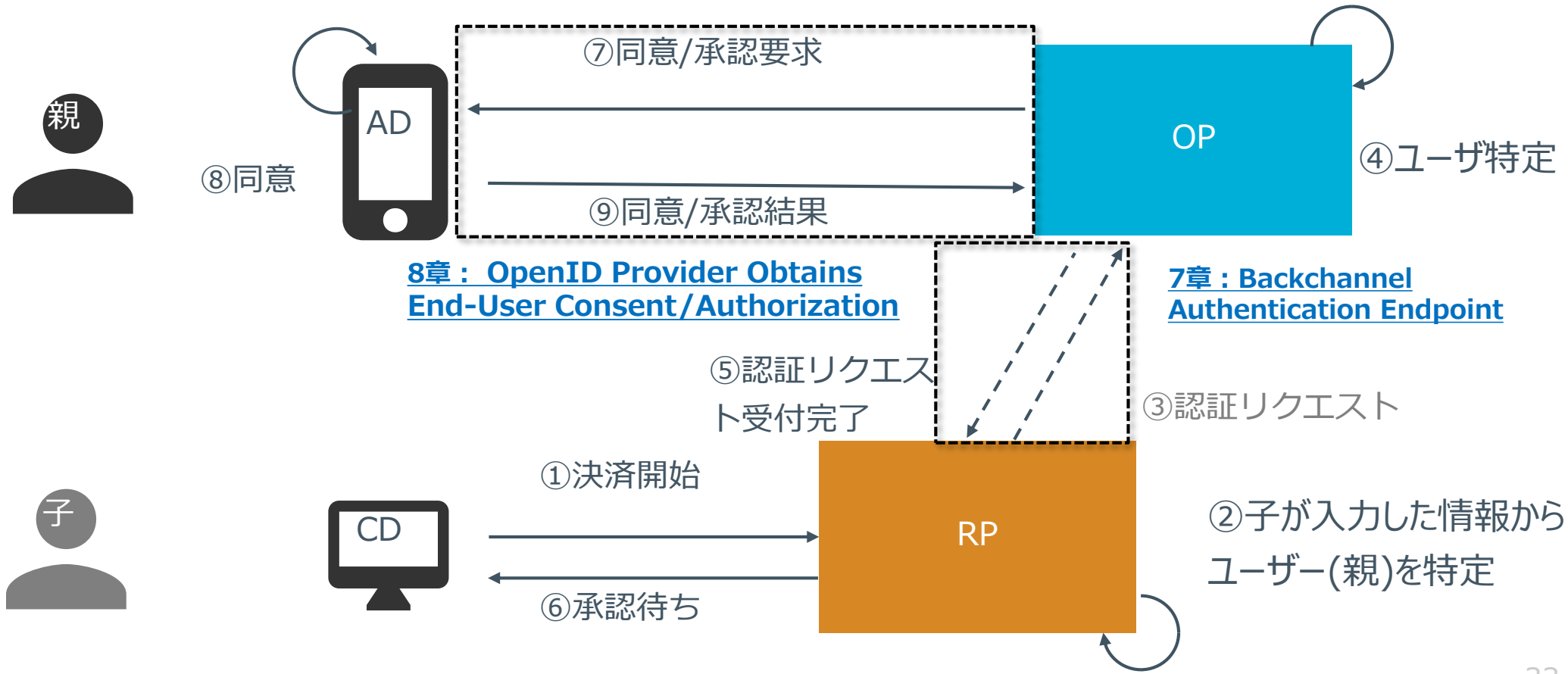
- 銀行窓口処理を、Web上でユーザーの同意を得て、受付担当者に実行させたい。
- POS端末での決済を、ユーザーのスマートフォン上で許可したい。
- 子の（親のカードを使った）支払いを、親がスマートフォン上で許可したい。

© NRI SecureTechnologies, Ltd.

CIBAフロー例として、ECサイトにおいて子が親のクレジットカードで決済しようとし、親のデバイスで親から承諾を得て決済が行われるシナリオが挙げられる。

CIBAフロー例

- ここでは決済の開始から、親の持つ認証デバイスで同意をして、OPに同意結果を返却するまでのフローを示している。（図中の章記載は、CIBAで記載されている各章を示す。）

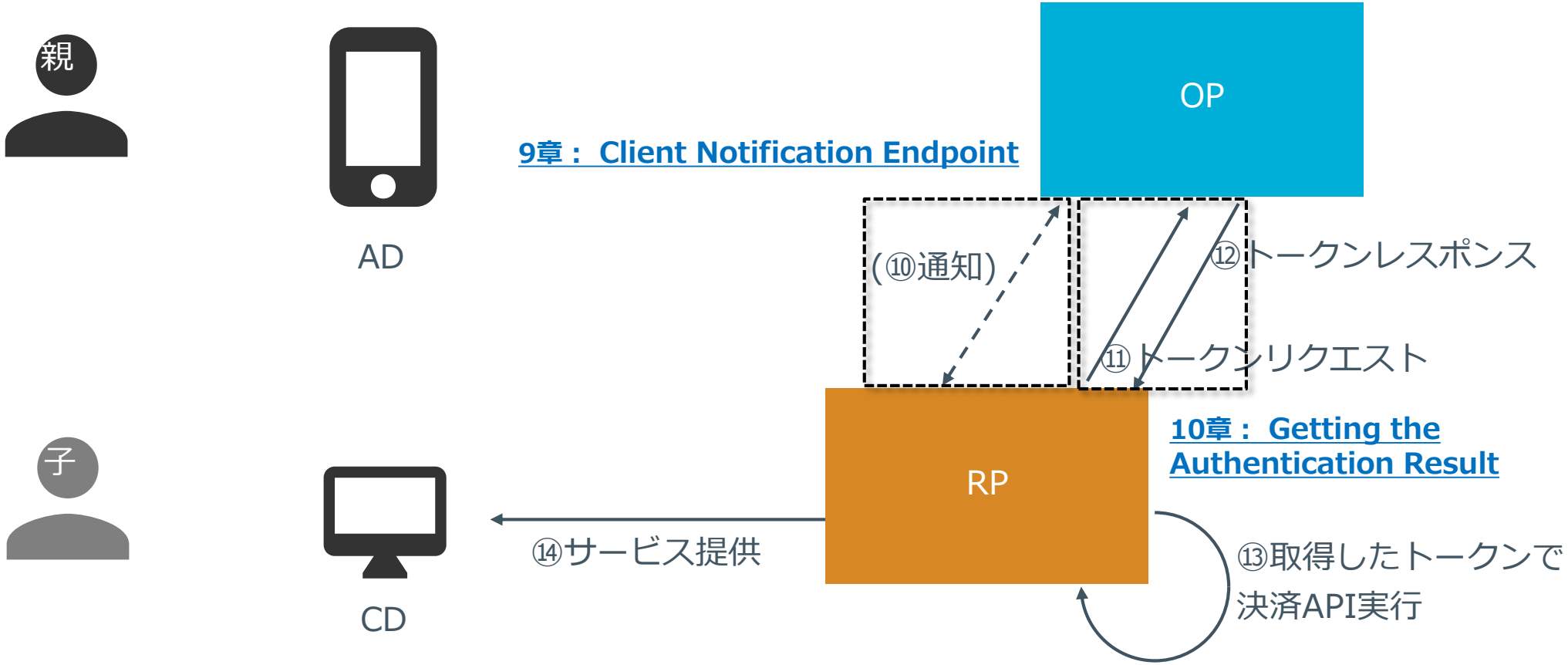


引用：https://www.secure-sketch.com/blog/openid-connect-ciba-implementation

© NRI SecureTechnologies, Ltd.

CIBAフロー例として、ECサイトにおいて子が親のクレジットカードで決済しようとし、親のデバイスで親から承諾を得て決済が行われるシナリオが挙げられる。

- ここでは、親から承認が得られてOPに承認結果が通知されるところから、子にサービスが提供されるまでのフローを示している。



© NRI SecureTechnologies, Ltd.

引用：https://www.secure-sketch.com/blog/openid-connect-ciba-implementation

HEART WGではヘルスケア領域のプロファイルの策定を行っており、2020年6月現在では、4つの仕様書を公開している。

HEART (Health Relationship Trust) WGの活動

- HEART WGは、患者がいつ、どのように、だれと、どのように臨床データを共有するかをコントロールするプロファイルの策定を行っている。

- 上記の他に、FHIR（Fast Healthcare Interoperability Resources）、OAuth、OpenID Connect、UMA（User-Managed Access）に準拠した、患者のヘルスケアデータを交換するシステムのためのプロセスを定義している。

- HEART WGで策定されている仕様書（実装者ドラフト版）は下記の4つである。
  - **Health Relationship Trust Profile for OAuth 2.0**
  - **Health Relationship Trust Profile for Fast Healthcare Interoperability Resources (FHIR) OAuth 2.0 Scopes**
  - Health Relationship Trust Profile for User-Managed Access 2.0
  - Health Relationship Trust Profile for Fast Healthcare Interoperability Resources (FHIR) UMA 2 Resources

© NRI SecureTechnologies, Ltd.

Health Relationship Trust Profile for OAuth 2.0は、OAuth 2.0 のWeb認可フレームワークに対するRESTful APIの安全性を確保するためのプロファイルである。

HEART for OAuth 2.0 策定の背景

- OAuth 2.0 の仕様は、異なるタイプのソフトウェアクライアントでの使用を想定して、さまざまなセキュリティとユーザビリティを考慮した幅広い実装に対応している。
- 上記より、標準では多くのセキュリティ制御をオプションにしており、最小限のセキュリティ対策のみでは既知の攻撃を防ぐことができない。
- **実装の容易さと機能性を維持しつつ、幅広いユースケースに適したセキュリティのベースラインセットの策定と、機密性の高いユースケースのためにより高度なセキュリティ制御リスト提供を行うことを目的**としてHEARTの仕様が策定された。
- 本プロファイルは、医療ドメインだけでなく他の事業ドメインでも利用されることを想定している。

HEART for OAuth 2.0 のプロファイル構成

- 本プロファイルでは大きく分けて下記の3つの観点から、それぞれが準拠すべき考慮事項がまとめられている。
  - OAuthグラントタイプに基づく、クライアントタイプ（2章）
  - 認可サーバ（3章）
  - 保護されたリソース（4章）

© NRI SecureTechnologies, Ltd.

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）

© NRI SecureTechnologies, Ltd.

FIDO Allianceでは国や業界ごとにWorking Group(作業部会)が存在し、それぞれの国や業界に適した仕様やプロファイルの策定が行われている。

Technical Working Groups

- FIDO2
  - デバイス、クライアント、サーバ間の認証エコシステム内での広範な相互運用性を確保することを目指している。
- Internet of Things (IoT)
  - RPとIoTデバイス間の相互運用性を可能にするためのIoTデバイス認証/認証プロファイル等の、ユースケース、ターゲット・アーキテクチャ、の仕様を開発を行っている。
- Metadata Service
  - FIDOメタデータ・サービスを管理するとともに、技術要件・セキュリティ要件について各ワーキンググループとの調整を行い、メタデータに必要な変更が加えられるようにし、メタデータ・サービスの利用を促進している。
- Universal Authentication Framework (UAF)
  - デバイス、クライアント、サーバ間の認証セキュリティエコシステムの実現可能性と広範な相互運用性を確立し、それに必要なFIDO技術仕様を策定することを目指している。

© NRI SecureTechnologies, Ltd.

FIDO Allianceでは国や業界ごとにWorking Group(作業部会)が存在し、それぞれの国や業界に適した仕様やプロファイルの策定が行われている。

Certification, Security, Privacy and Identity focused Working Groups

- Certification
  - FIDOの技術仕様に沿って開発された製品の認証のための戦略、プロセス、および支援プログラムを開発し、試験プロトコルとFIDOブランドへの影響の調和を確保することにより、IDOアライアンスの目標を支援している。
- Identity Verification & Binding
  - 所持ベースの ID 検証（およびバインディング）の性能要件を確立し、これらの要件に対する認証評価基準を策定し、これらの要件および認証基準の適合を支援する白書とその他の資料を作成するために設立された。
- Security & Privacy Requirements
  - プライバシー、セキュリティ要求事項・脅威を継続的に評価されるFIDO実装のプライバシーとセキュリティを評価するための方針とプロセスを定義する。

© NRI SecureTechnologies, Ltd.

FIDO Allianceでは国や業界ごとにWorking Group(作業部会)が存在し、それぞれの国や業界に適した仕様やプロファイルの策定が行われている。

Adoption Working Groups

- Consumer Deployment
  - FIDOのソリューションの展開に影響を与える問題について、FIDOアライアンス内の専門家および内部アドバイザーとして活動する。
- Enterprise Deployment
  - エンタープライズレベルでのFIDOソリューションの展開に影響を与える問題について、FIDOアライアンス内の専門家および内部アドバイザーとして活動する。
- Government Deployment
  - 政府によるFIDOソリューションの展開に影響を与える問題について、FIDOアライアンス内の専門家および内部アドバイザーとして活動する。

Regional Working Groups

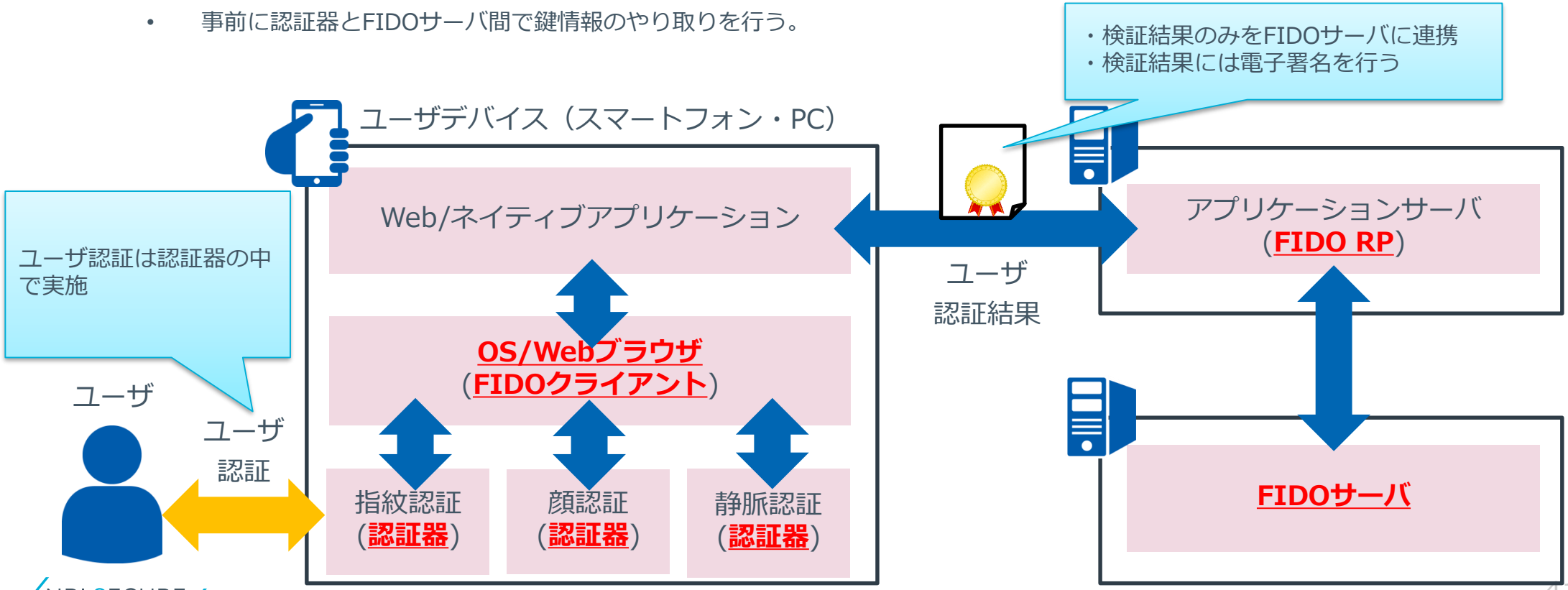
- 下記の国や地域において、それぞれの作業部会がFIDOの知名度向上や展開の促進を行っている。
  - FIDO China
  - FIDO Europe
  - FIDO India
  - FIDO Japan
  - FIDO Korea

© NRI SecureTechnologies, Ltd.

ユーザ認証において公開鍵暗号方式を利用することでサーバとユーザデバイス間での秘密情報のやり取りを不要とした認証技術として「FIDO」規格を策定している。

FIDO概要

- **ユーザ認証はユーザデバイス中の認証器(指紋認証デバイス等)で行われる。**
- FIDOサーバへは検証結果のみが送信され、FIDOサーバは認証結果を検証する。
  - **ネットワーク上をID/パスワードや生体情報といった機密情報が流れないため安全性が向上する。**
- 検証結果に公開鍵暗号方式を用いた**電子署名を行うことで改ざんやなりすましを防ぐ。**
  - 事前に認証器とFIDOサーバ間で鍵情報のやり取りを行う。



© NRI SecureTechnologies, Ltd.

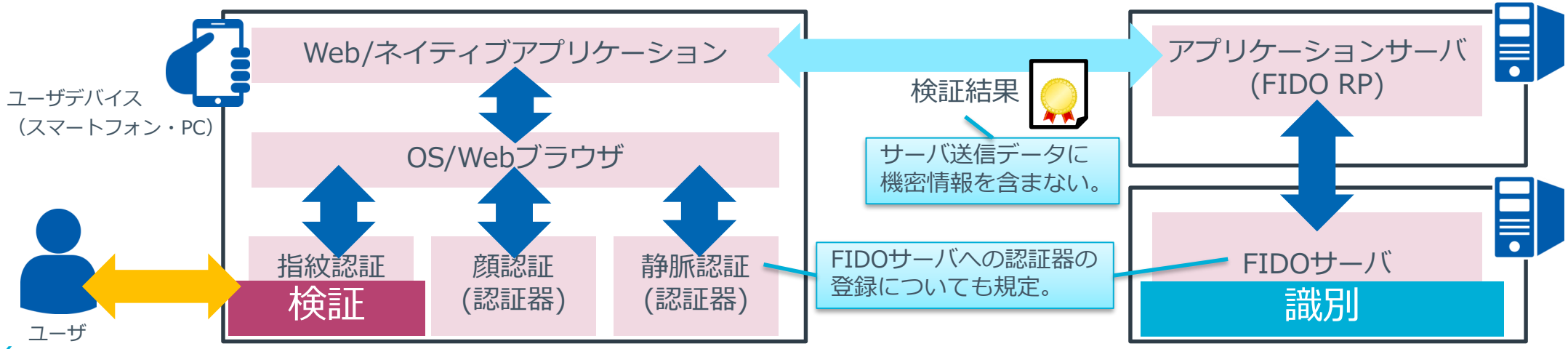
FIDO認証モデルでは従来サーバ側で実施していた本人の検証と識別のうち、本人の検証をユーザデバイス側で実施することでセキュリティを向上させている。

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。

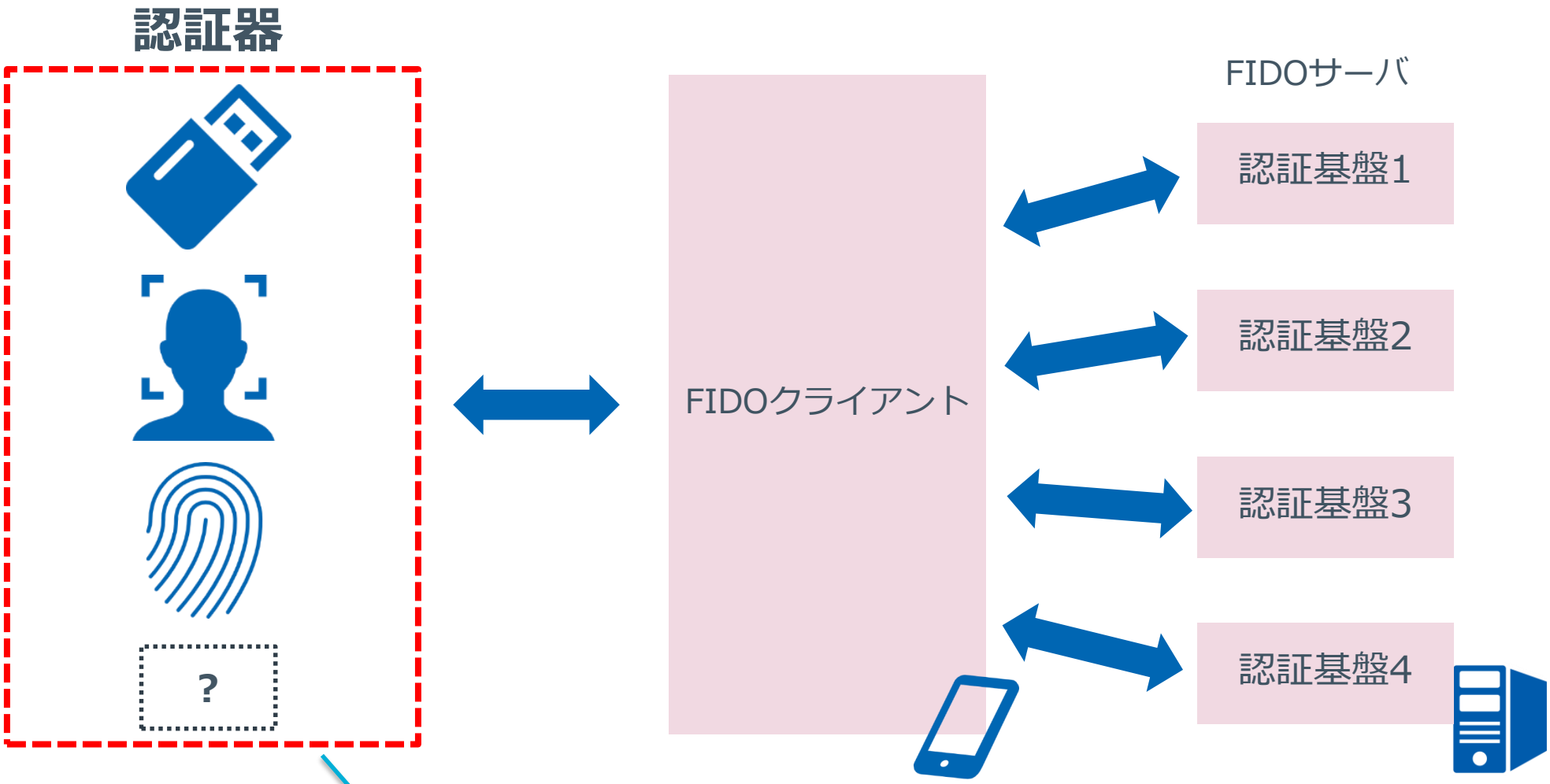
FIDO認証モデル

- 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。**



© NRI SecureTechnologies, Ltd.

FIDOは認証器を部品化することにより、FIDOをサポートしている多種多様なデバイスが生体認証などの認証機能を容易に利用することができる。



- FIDOの認証器は部品化されているため、FIDOの仕様に従う様々な認証器を容易に利用することが可能となる。
- 将来において新しい認証手段が出た場合でもFIDO標準に従うことでいち早く利用可能となる。

© NRI SecureTechnologies, Ltd.

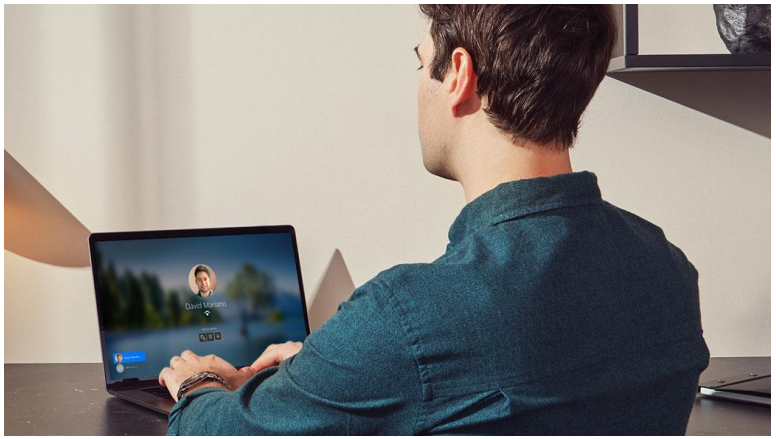
FIDO認証はWebサービス側だけでなく、ユーザデバイス側においてもOS標準でサポートが進み、より広くFIDO認証を利用できる環境が整ってきている。

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。

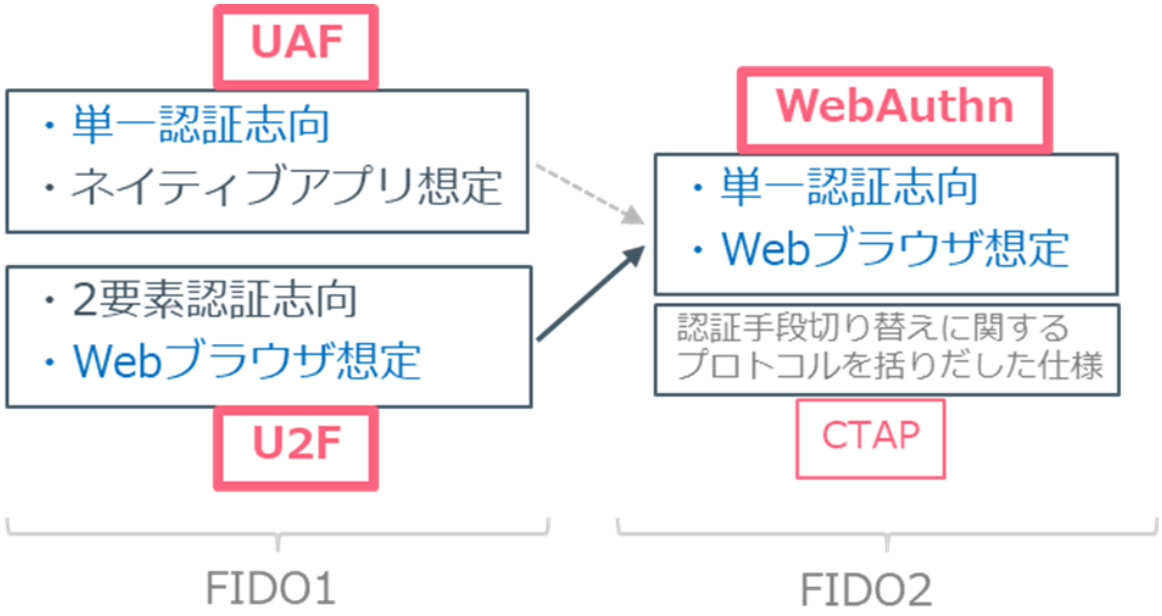


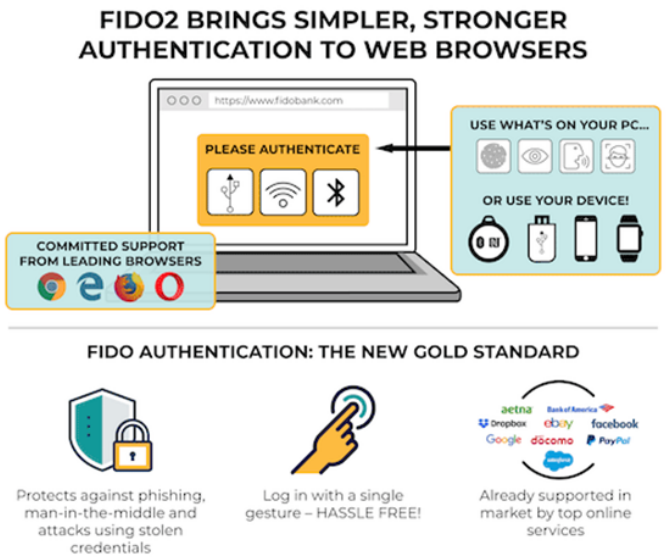
© NRI SecureTechnologies, Ltd.

FIDO仕様として、最初に策定されたFIDO1ではユースケースに応じてFIDO UAFとFIDO U2Fで分派していたが、FIDO2では1つの仕様として統合された。

FIDOの規格の推移

- FIDO1.0ではパスワードレス規格であるFIDO UAF、「認証の二要素目」としての用途であるFIDO U2Fで分派していた。FIDO2ではこれらの仕様が統合され、また標準Web API仕様として Web Authentication API (WebAuthn) が策定された。
- WebAuthnはWebブラウザからFIDO認証器(指紋認証デバイスなど)にアクセスするためのAPI仕様が策定されている。これにより、Webブラウザ上で指紋認証や顔認証、USBキーといった端末側の認証機器を使用できるようになる。





https://www.w3.org/2018/04/pressrelease-webauthn-fido2.html.ja より引用

© NRI SecureTechnologies, Ltd.

FIDOにおける認証は、登録、認証、登録解除の3つの処理から構成される。これらの処理はFIDO UAF/U2FおよびFIDO2のいずれの仕様でも行われる。

登録

- FIDO認証を行う前に1度だけ実施する。
- FIDOクライアント、ユーザ、認証器のペアに対して秘密鍵＆公開鍵を作成し、FIDOサーバに公開鍵を登録する。
- Challenge-Response形式のやり取りを実施する。

認証

- ユーザが認証器を用いて認証を実施すると、 FIDOクライアントが認証結果を秘密鍵で署名しFIDOサーバに渡す。
- FIDOサーバはその内容を検証する。
- Challenge-Response形式のやり取りを実施する。

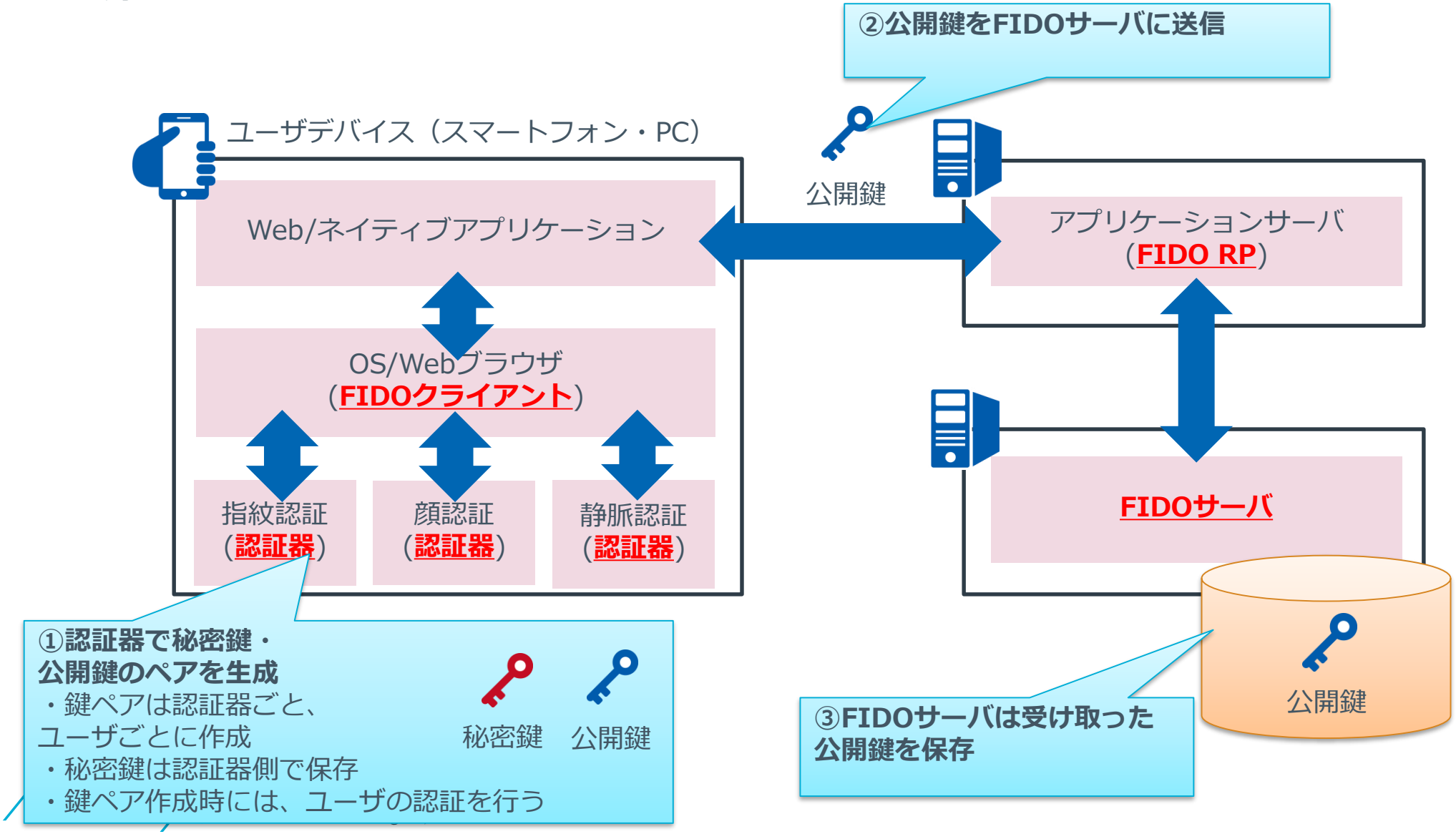
登録解除

- FIDO認証を行わなくなった場合(ユーザID削除時など)に実施する。
- FIDOサーバに登録されている公開鍵情報を削除する。

© NRI SecureTechnologies, Ltd.

登録処理では、認証器が検証結果に用いる秘密鍵・公開鍵のペアを作成し、公開鍵をFIDOサーバに連携する。

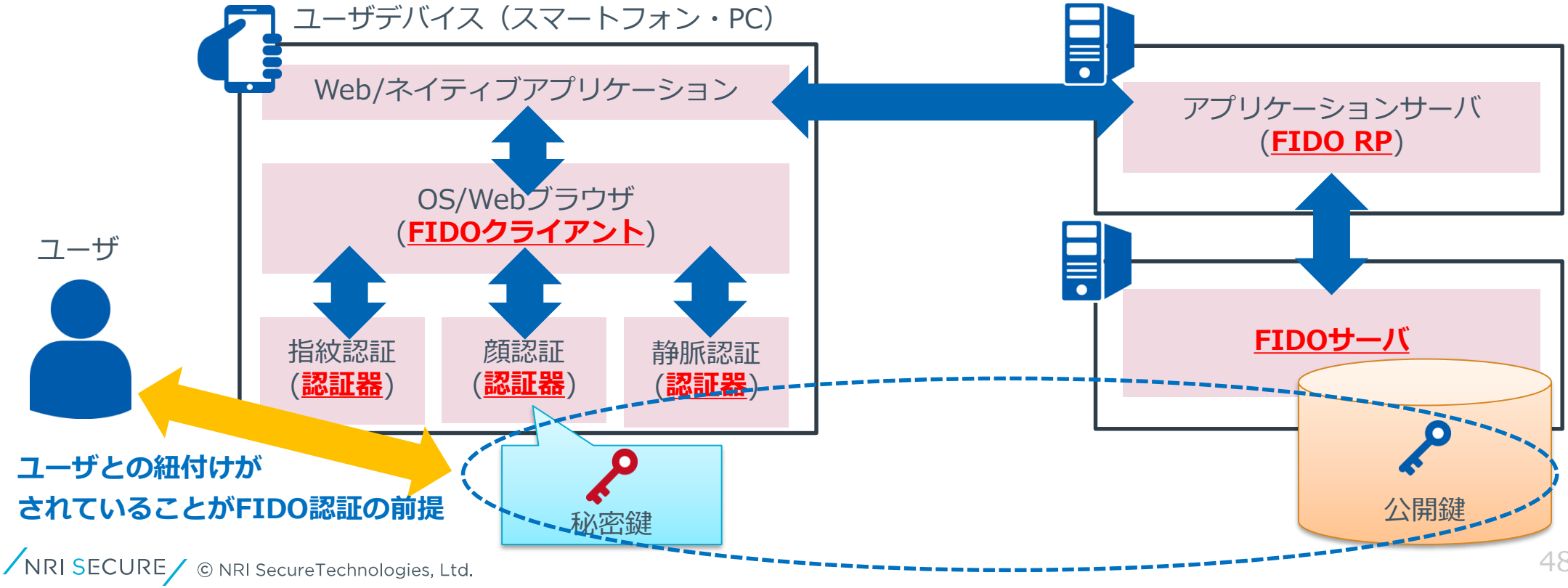
登録



FIDO認証の仕組みにおいて、登録処理においてユーザと認証器との紐付け(バインディング)が実施されることがセキュリティ上重要である。

登録処理におけるバインディングの重要性

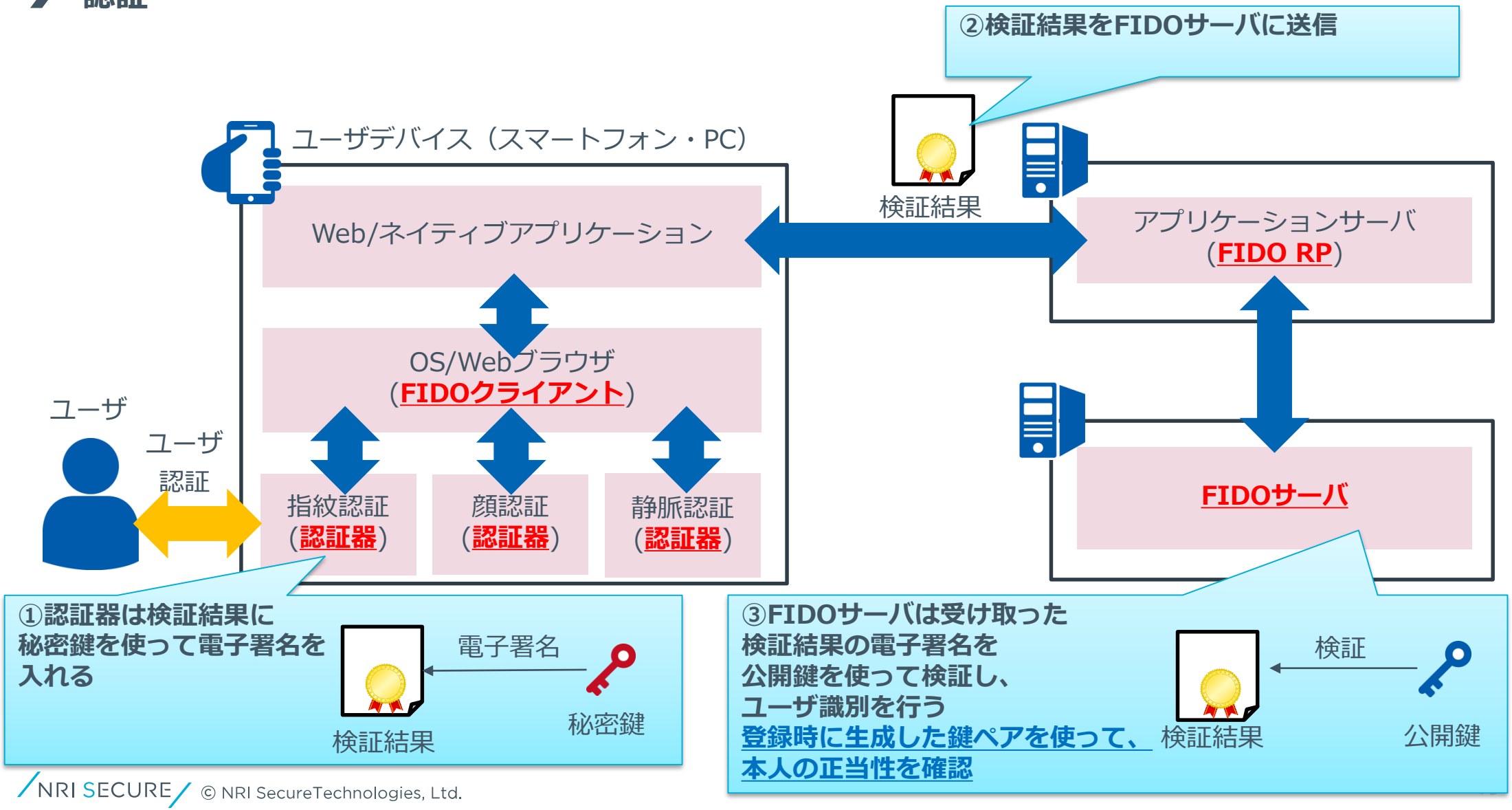
- 登録処理においては、ユーザデバイス側でユーザに紐づく秘密鍵・公開鍵のペアを作成し、これらの鍵ペアを利用した公開鍵認証を実施する。
- **鍵ペアがそのユーザに紐付けられたものであることがFIDO認証の大前提であり、登録処理として事前に身元確認済みのユーザと鍵ペアとの紐付けを適切に行うことが重要となる。**ユーザの身元確認から認証器の適切な登録を一貫して行うことにより、その後の当人認証をシンプルかつ堅牢なものとすることが可能となる。
  - ユーザと認証器(鍵ペア)との紐付けの重要性についてはNIST SP800-63-3Bの「6.1 Authenticator Binding」にて言及されている。



© NRI SecureTechnologies, Ltd.

認証処理では、認証器が検証結果に電子署名を行い、FIDOサーバがその電子署名を検証し、ユーザの識別を行う。

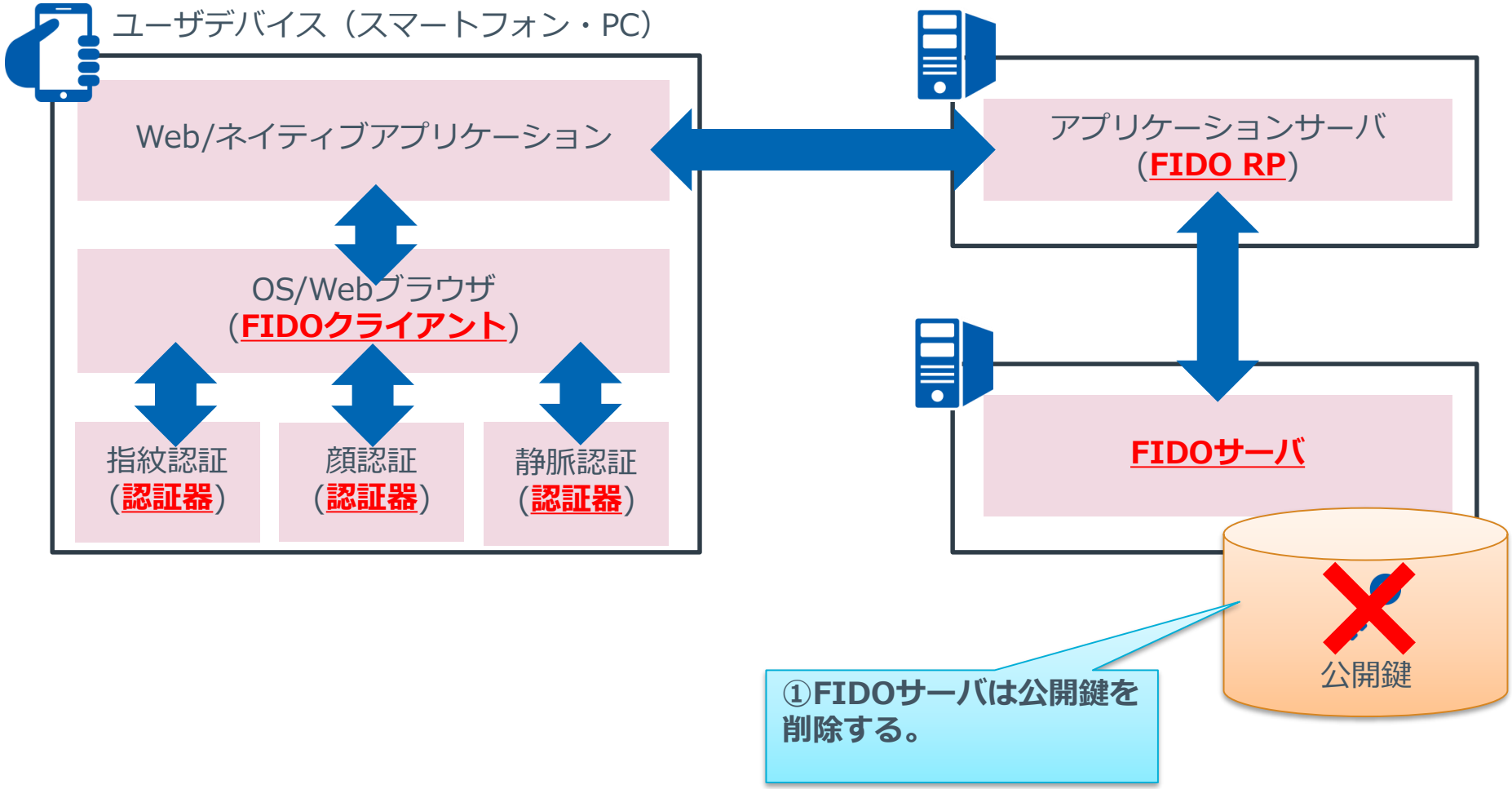
認証



© NRI SecureTechnologies, Ltd.

登録解除処理は、サービスユーザ退会時などにFIDOサーバが該当するユーザの公開鍵情報を削除する。

登録解除

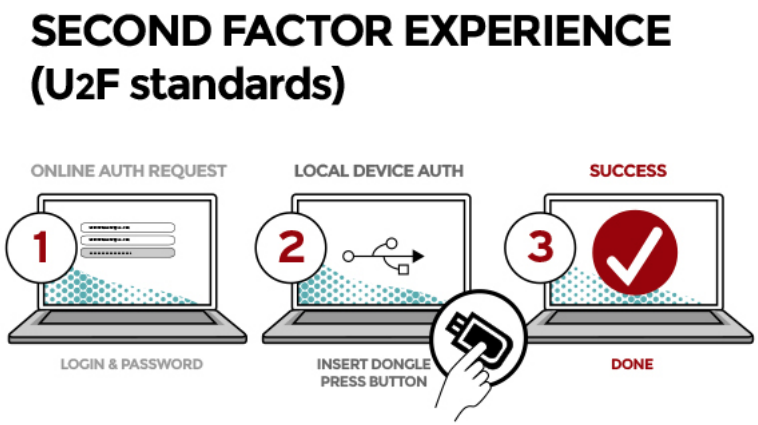


© NRI SecureTechnologies, Ltd.

FIDO U2Fは、Webアプリケーションを主な対象として既存のID/パスワード認証に加えて2要素目の認証をサポートするための仕様として策定されている。

FIDO U2F 概要

- オンラインサービスはユーザーログインに対して堅牢な第2の認証要素を追加することで、既存のパスワード基盤のセキュリティを強化できる。
- ユーザーは、まず今までと同様に、ユーザー名とパスワードでログインする。サービスは、さらに任意のタイミングで、ユーザーに2段階認証デバイスの提示を求めることができる。
- 堅牢な2段階認証を使用することで、サービスはセキュリティレベルを下げることなく、パスワードを簡素化できる（4桁の暗証番号など）。



FIDO U2Fの特徴

- 主に、**Webブラウザでパスワード認証を要するアプリケーションに対して、2段階認証機能の追加しての利用**が想定されている。
- 利用のためには、専用デバイスの追加が必要となる。

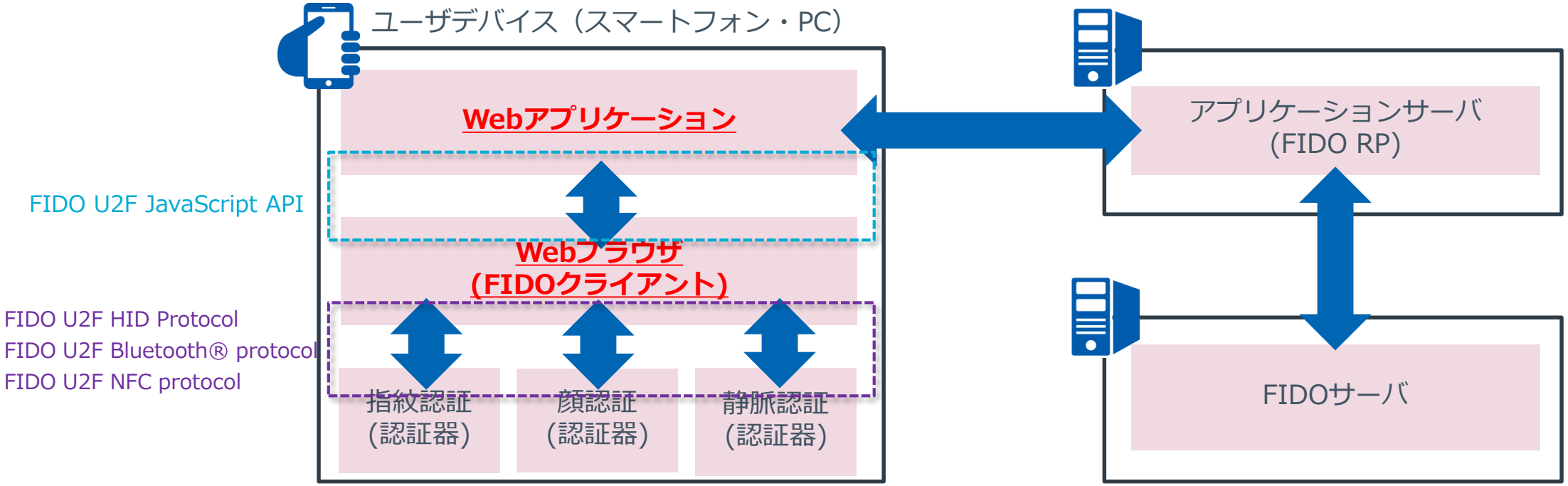
(引用元) https://fidoalliance.org/%E3%82%A2%E3%83%97%E3%83%AD%E3%83%BC%E3%83%81%E3%81%A8%E3%83%93%E3%82%B8%E3%83%A7%E3%83%B3/
https://www.mhlw.go.jp/content/10800000/000537436.pdf p152

© NRI SecureTechnologies, Ltd.

FIDO U2Fでは、WebブラウザがFIDOクライアントとして動作することを前提に、Webアプリケーションや認証器との通信に関する仕様を用意している。

FIDO U2F 構成要素と対応する仕様

- WebアプリケーションとWebブラウザ間の通信仕様としてU2F Javascript APIを定義
- Webブラウザと認証器間の通信仕様としてU2F HID/Bluetooth/NFC protocolを定義
- これらの通信でやり取りされるメッセージ仕様としてU2F Raw Message Formatsを定義



© NRI SecureTechnologies, Ltd.

参考：FIDO U2F 仕様一覧

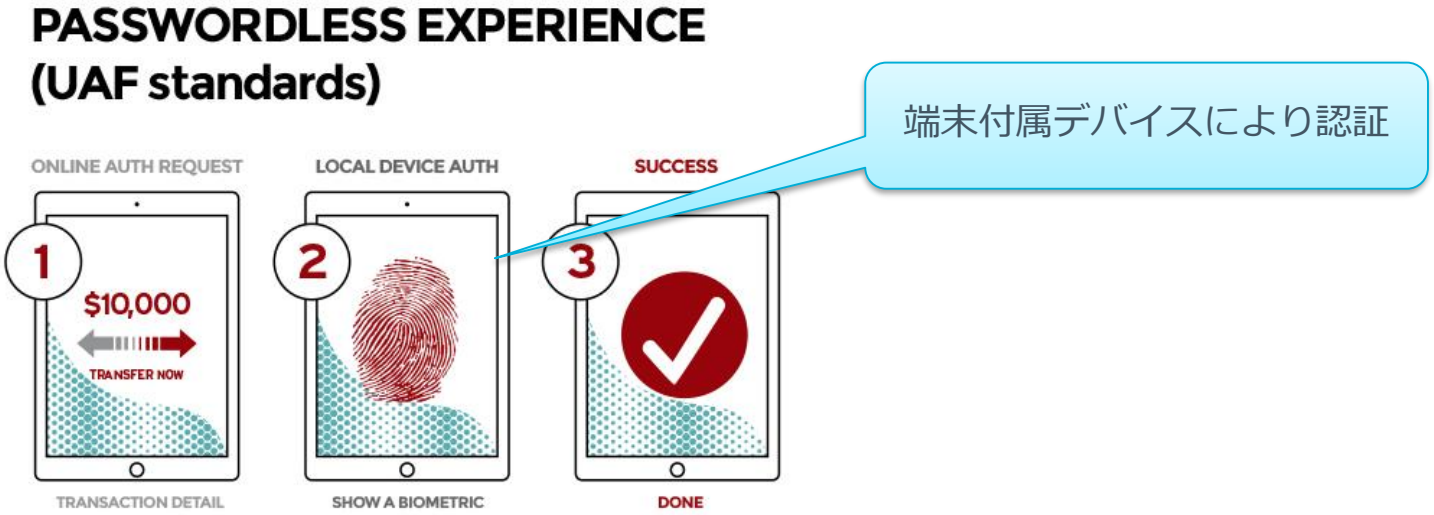
仕様書名	内容
FIDO U2F Architectural Overview	プロトコルを詳細に記述するための様々な設計上の考慮事項を説明し、ユーザフローを詳細に記述している。この仕様書を通じて、プロトコル設計における様々なプライバシーへの配慮について説明している。
FIDO U2F Javascript API	U2FにアクセスするためのWebブラウザのクライアントサイドのAPIについて説明されている。 オンラインサービスやウェブサイトは、クライアント側でこのAPIを使用し、サーバー側でU2Fメッセージを検証できるサーバーとペアリングすることで、U2Fを活用することができる。
FIDO U2F Raw Message Formats	FIDO U2FサーバとFIDO U2Fトークン間でのバイナリ形式のメッセージに関して説明されている。
FIDO U2F HID Protocol Specification	FIDOクライアントから USB U2Fトークンに送信されるメッセージが、USB HIDを介してどのように形作られているかを説明している。
FIDO U2F Implementation Considerations	U2Fデバイスの作成者および U2F サポートをするRPのための実装に関する考慮事項および推奨事項を記述。
FIDO AppID and Facet Specification	U2Fプロトコルは、発信元のfoo.com が U2F トークンによって foo.com のために発行された鍵のみを行使できることを保証する。この文書では、foo.com の様々な実施形態が (ブラウザ内、モバイル OS 内などで) トークンと同じ発行元を安全に主張する方法を説明する。
FIDO Common Header Files u2f.h	FIDO U2F Raw Messagesや FIDO U2F HID Protocol Specificationで参照されているシンボリック定数やデータ構造の値を定義している。
FIDO Bluetooth Specification	U2F プロトコルが FIDO クライアントと Bluetooth Low Energy FIDO認証機能との間でどのように実行されるべきかを記述している。
FIDO NFC Specification	FIDO クライアントとNFC FIDO認証機能との間で U2F プロトコルがどのように実行されるべきかを記述。

© NRI SecureTechnologies, Ltd.

FIDO UAFは、ネイティブアプリを対象としてユーザデバイス付属の生体認証デバイス等を用いることでパスワードを使わず認証を行う仕様として策定されている。

FIDO UAF（Universal Authentication Framework）概要

- UAFでは、指紋の読み取り、カメラでの顔の撮影、マイクでの発話、PINコードの入力するなどのクライアントデバイス上での認証メカニズムをユーザーが選択することで、ユーザーのデバイスをオンラインサービスへ登録する。
- UAFプロトコルでは、サービスがユーザーに対してどの認証メカニズムを提示するかを選択できる。



FIDO UAFの特徴

- 主に**スマートフォンのネイティブアプリケーションにおいて、スマートフォンの付属デバイスを活用した認証**が想定されている。
- **アプリケーション側でのパスワードレスを想定**して、所有物（スマートフォン）を用いて生体認証や画面ロック解除等による認証を行う。

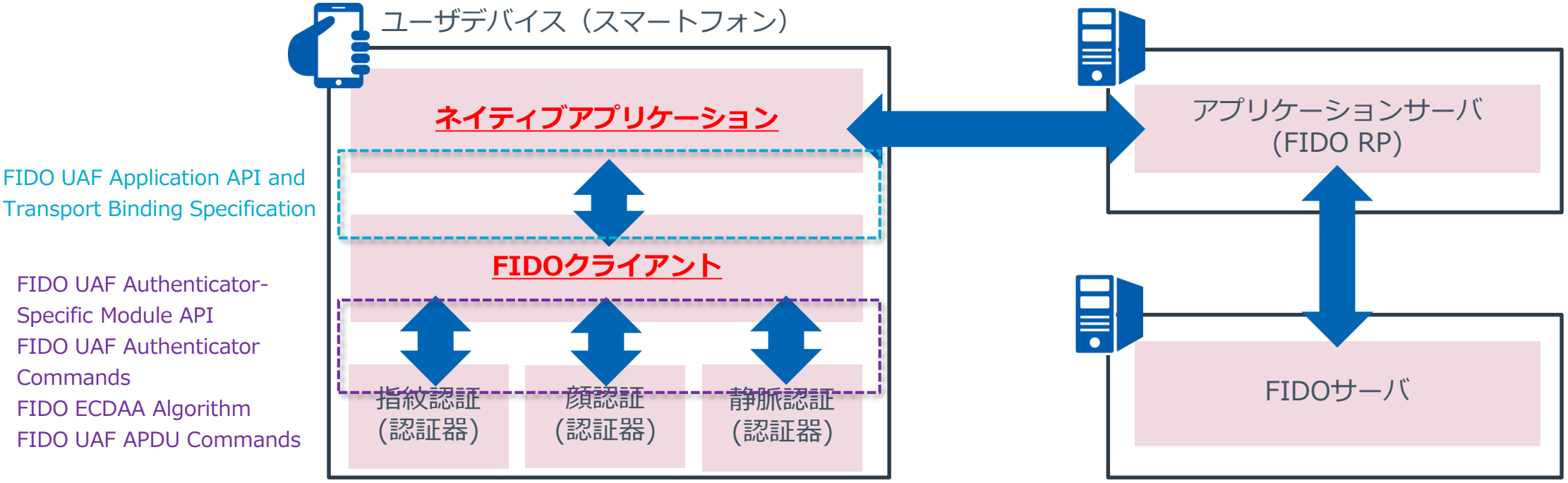
(引用元) https://fidoalliance.org/%E3%82%A2%E3%83%97%E3%83%AD%E3%83%BC%E3%83%81%E3%81%A8%E3%83%93%E3%82%B8%E3%83%A7%E3%83%B3/
https://www.mhlw.go.jp/content/10800000/000537436.pdf p153

© NRI SecureTechnologies, Ltd.

FIDO UAFでは、ネイティブアプリケーション向けであることを前提に、ネイティブアプリケーション-FIDOクライアント-認証器間の通信に関する仕様を用意している。

FIDO UAF構成要素と対応する仕様

- ネイティブアプリケーションとFIDOクライアント間の通信仕様としてUAF Application APIを定義
- FIDOクライアントと認証器間の通信仕様としてUAF Authenticator-Specific Module APIおよびUAF Authenticator Commands等を定義
- これらの通信でやり取りされるメッセージ仕様や処理方式としてUAF Protocol Specificationを定義



© NRI SecureTechnologies, Ltd.

参考：FIDO UAF 仕様一覧

仕様書名	内容
FIDO UAF Architectural Overview	プロトコルを詳細に記述するための様々な設計上の考慮事項を説明し、ユーザフローを詳細に記述
FIDO UAF Protocol Specification	すべてのUAFプロトコルメッセージのメッセージフォーマットと処理ルールを定義
UAF Application API and Transport Binding Specification	FIDO UAFを利用するクライアントアプリのためのAPIと相互運用性プロファイルについて説明
FIDO UAF Authenticator-specific Module API	認証器固有のモジュールと、ASMがFIDOクライアントに提供するAPIを定義
FIDO UAF Authenticator Commands	UAF認証器がUAFプロトコルをサポートするために実装すべき低レベルの機能について記述
FIDO ECDAA Algorithm	認証器のためのセキュアでプライベートな認証の形態として、楕円曲線直接匿名認証を使用する方法について説明
FIDO UAF APDU Commands	セキュアな要素に基づく UAF認証器を促進するためにFIDO UAF 認証器コマンドのアプリケーション・プロトコル・データ・ユニット（APDU）へのマッピングを定義
UAF Registry of Predefined Values	UAF プロトコルで予約されたすべての文字列と定数を定義

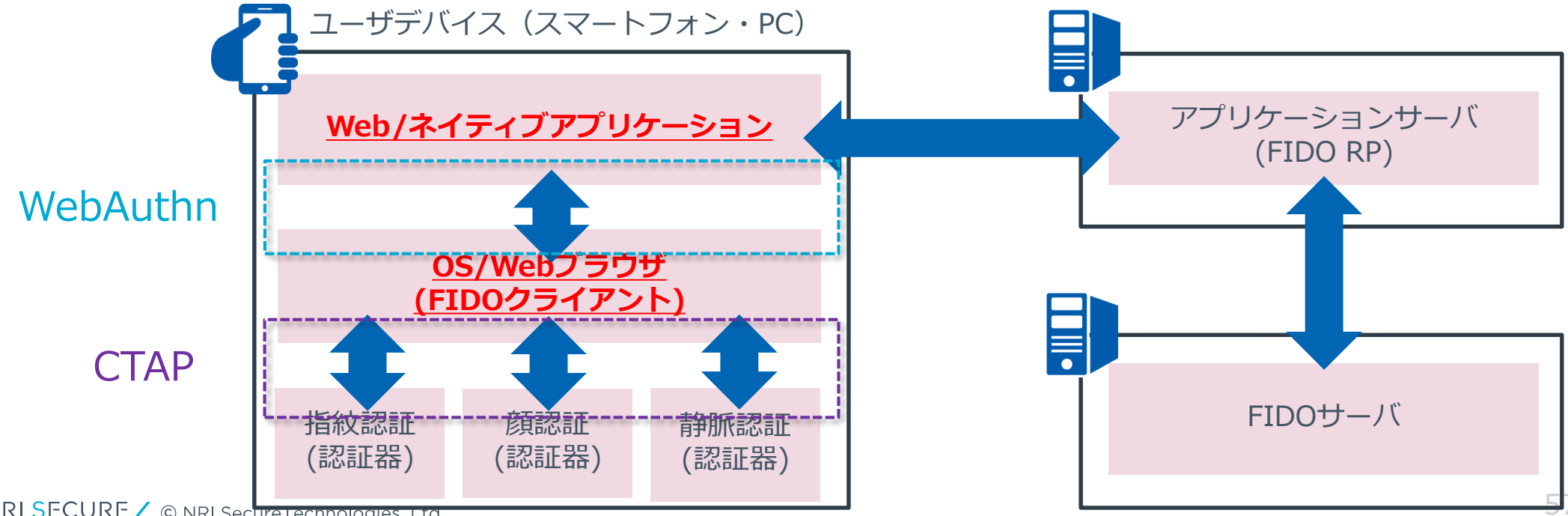
© NRI SecureTechnologies, Ltd.

FIDO2は、WebAuthnとCTAPの2つの仕様から構成され、WebAuthnはW3C標準規格とすることで幅広いOS/Webブラウザでのサポートを目指している。

FIDO2の特徴

- **FIDO U2F および UAF に不足する仕様を補完し、統合**するための認証仕様群。
  - FIDO2の登場により、FIDO UAFやU2Fでは標準でサポートしていなかったWebブラウザでのパスワードレス認証が可能に
- FIDO2を構成する大きな仕様として、**Web Authentication API (WebAuthn)とCTAP**が存在。

WebAuthn	Webブラウザ(FIDOクライアント)が提供するWeb認証のための標準化されたJavascript API群。2019年3月にW3Cにおける正式な勧告(仕様)となった。
CTAP	FIDOクライアントと認証器間の通信仕様であり、FIDO U2Fの仕様を拡張。

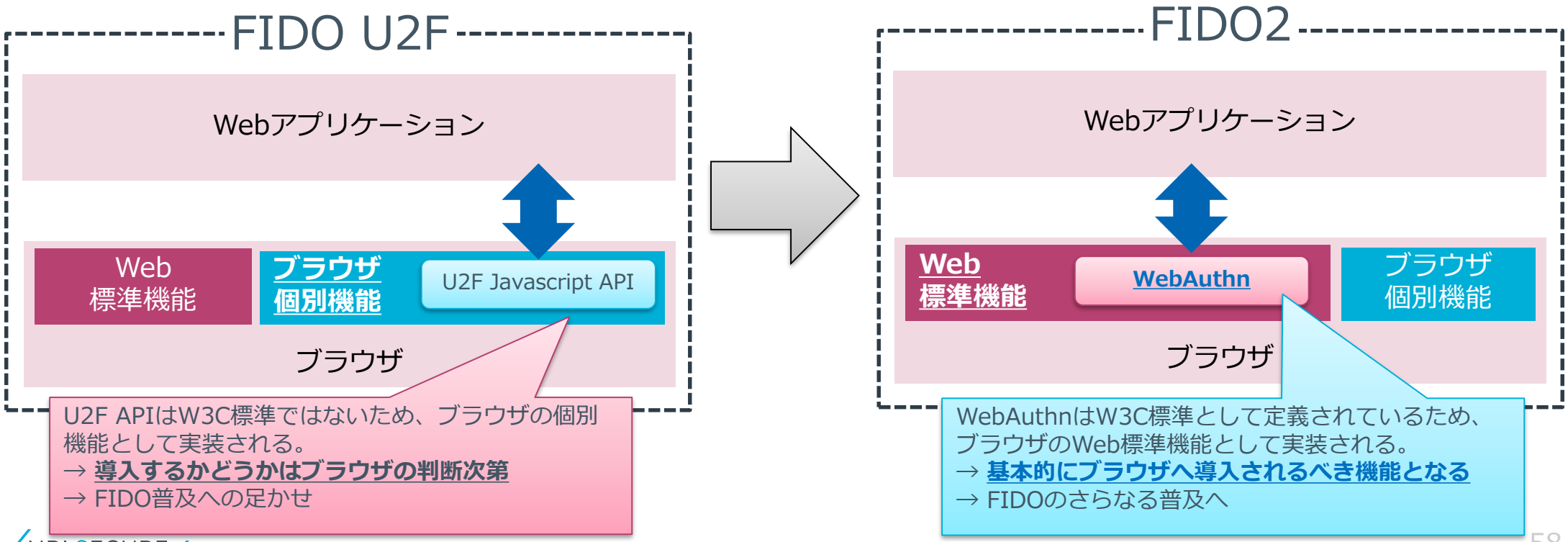


© NRI SecureTechnologies, Ltd.

FIDO2ではWebブラウザがサポートすべきAPI仕様(WebAuthn)がW3C標準として定義され、ブラウザへの普及が急速に進んでいる。

WebAuthn 概要

- WebAuthnはW3C(World Wide Web Consortium)標準として仕様策定が進められ、2019年3月にW3Cにおける正式な勧告(仕様)となった。
- W3C標準となることで、ブラウザ側の対応としても以前のようにブラウザ個別機能としてブラウザ側の判断による導入から、Web標準機能として基本的に導入すべき機能として重要度が上がり、ブラウザへの普及が進んでいる。
- ブラウザだけではなく、Windows 10のようにOS/プラットフォーム側への導入も進んでいる。

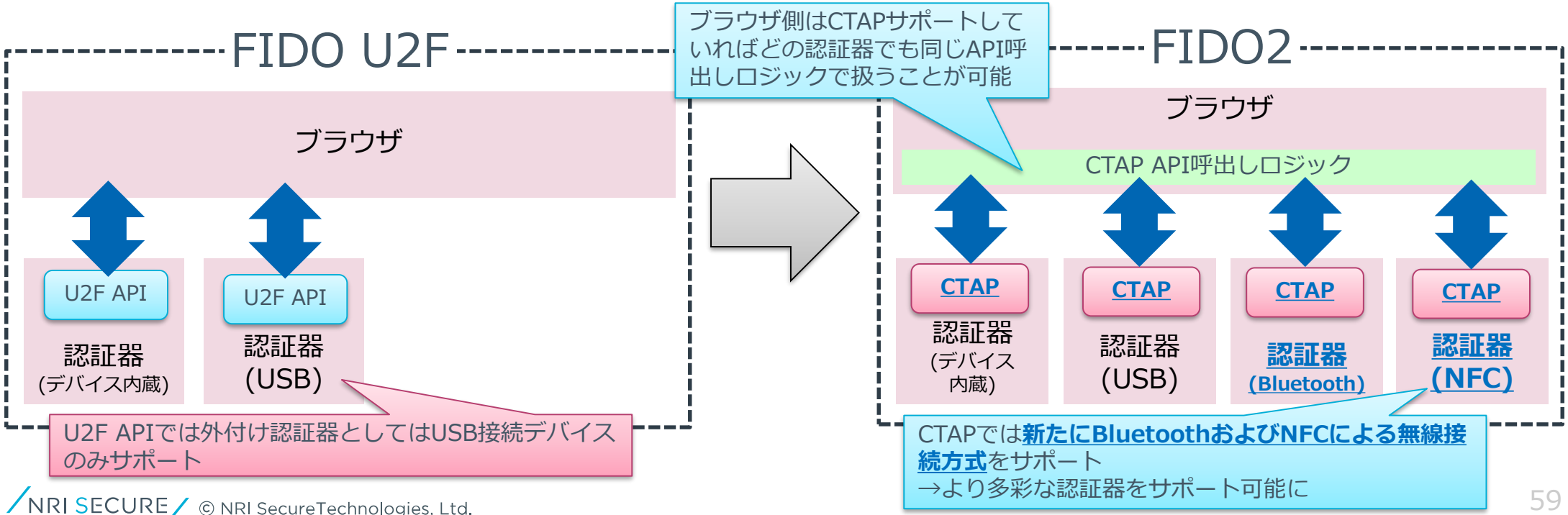


© NRI SecureTechnologies, Ltd.

認証器がサポートすべきAPI仕様(CTAP)はU2Fの仕様から拡張され、新たにBluetoothやNFCによる無線通信もサポートできるようになった。

CTAP 概要

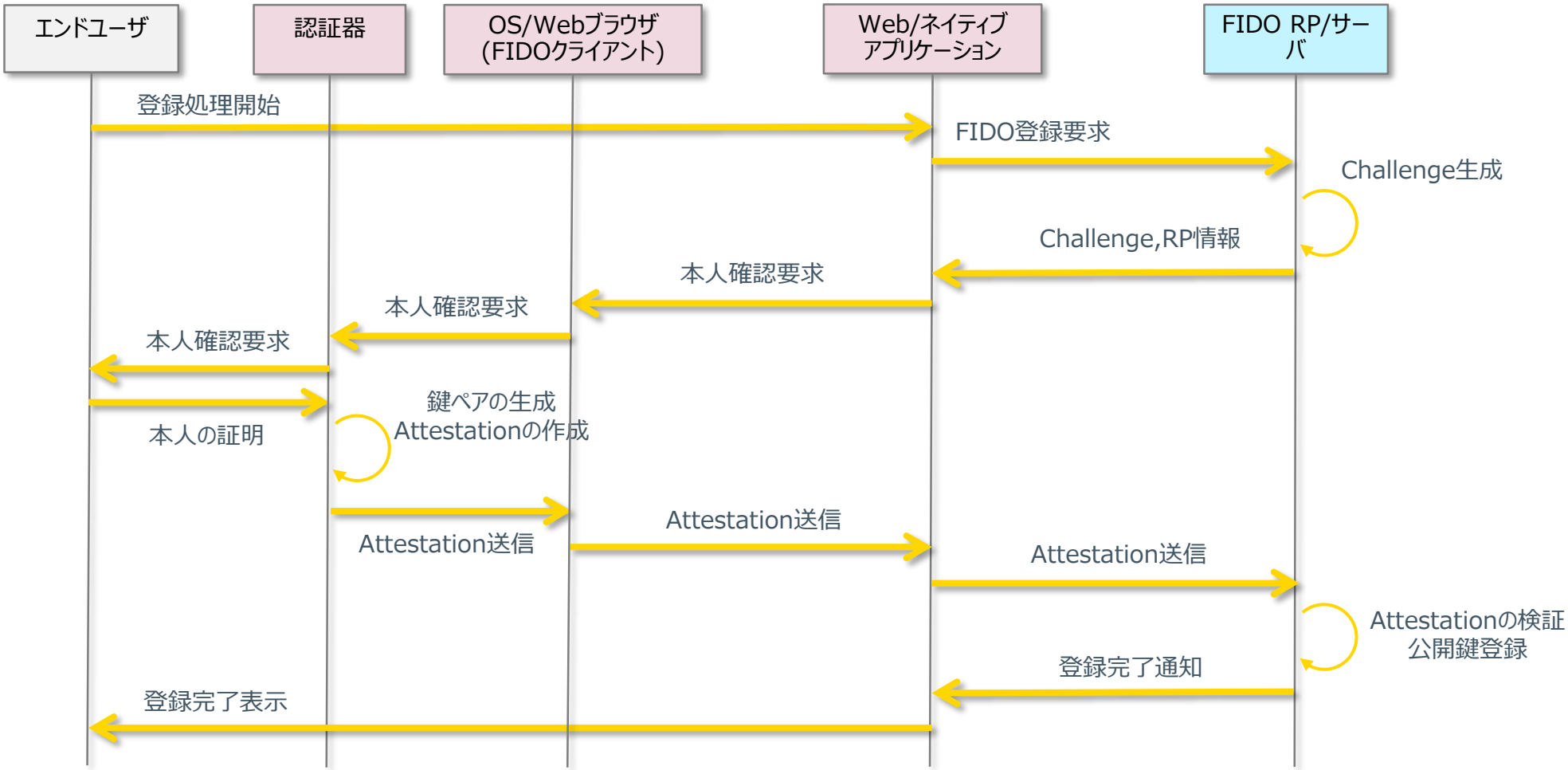
- CTAPはFIDO U2F仕様を拡張し、新たにBluetoothやNFCといった無線接続による認証器の接続も可能とした。
- CTAPはU2Fとの互換性を持つCTAP1および、CTAP1の仕様をさらに改善したCTAP2の2つから構成される。
- CTAPは電気通信の標準化団体であるITU-T(International Telecommunication Union Telecommunication Standardization Sector)により標準規格(勧告ITU-T X.1278)として採択されている。



© NRI SecureTechnologies, Ltd.

FIDO2における登録シーケンスでは、認証器で鍵ペアを作成したうえで公開鍵をFIDOサーバに送信する。

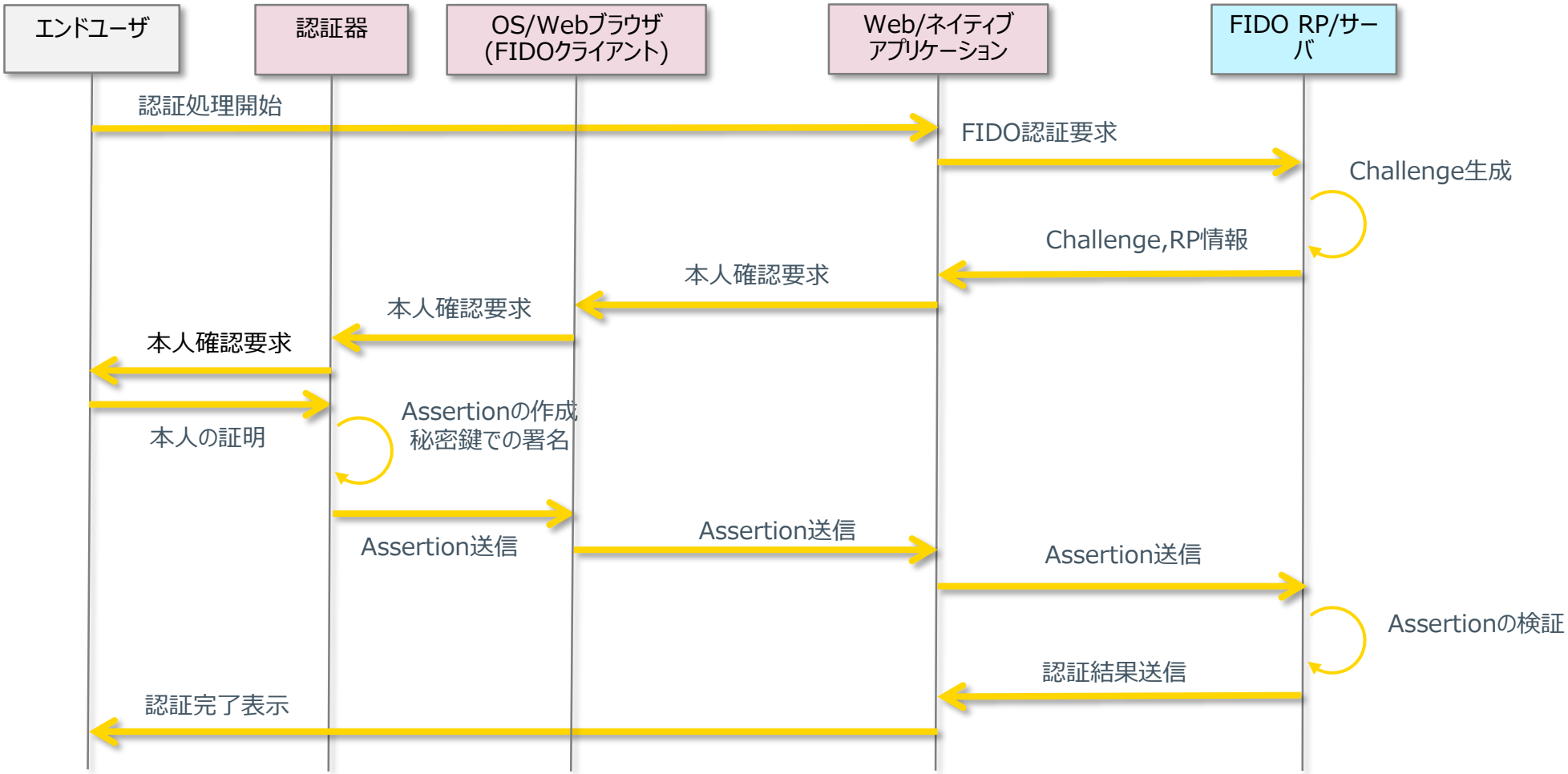
- 生成された公開鍵情報は<u>Attestationと呼ばれる認証器情報</u>に含められ、FIDOサーバに送信される。



© NRI SecureTechnologies, Ltd.

FIDO2における認証シーケンスでは、検証結果を秘密鍵で署名した上でFIDOサーバに送信する。

- 認証器での検証結果はAssertionと呼ばれ、FIDOサーバに送信される。

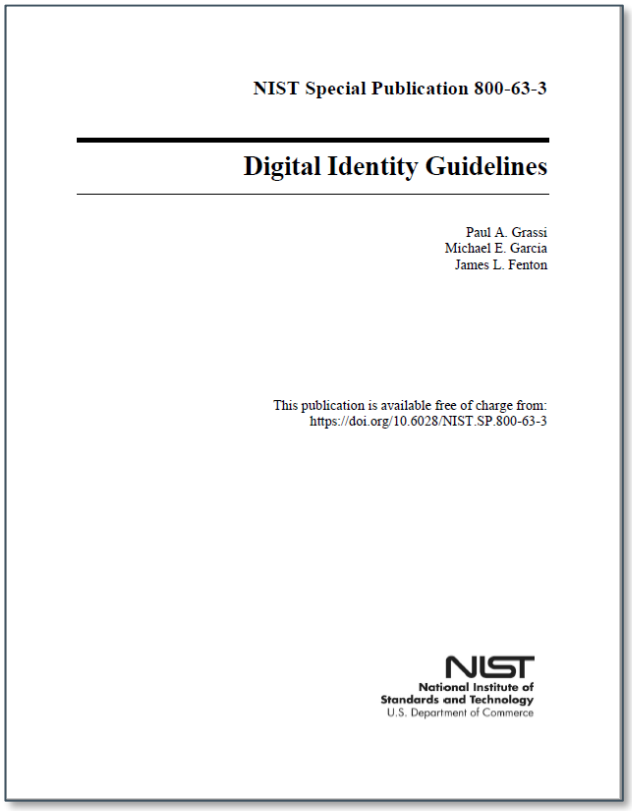


© NRI SecureTechnologies, Ltd.

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)は SP800-63-3を発行している。

NIST SP800-63-3 概要

- 米国国立標準技術研究所(NIST：National Institute of Standards and Technology)が発行しているデジタルIDに関するガイドライン。ID管理、認証、フェデレーションなどIDにかかわる包括的なガイドラインとして最も権威のあるドキュメント。2017年6月に第3版が公開。


NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

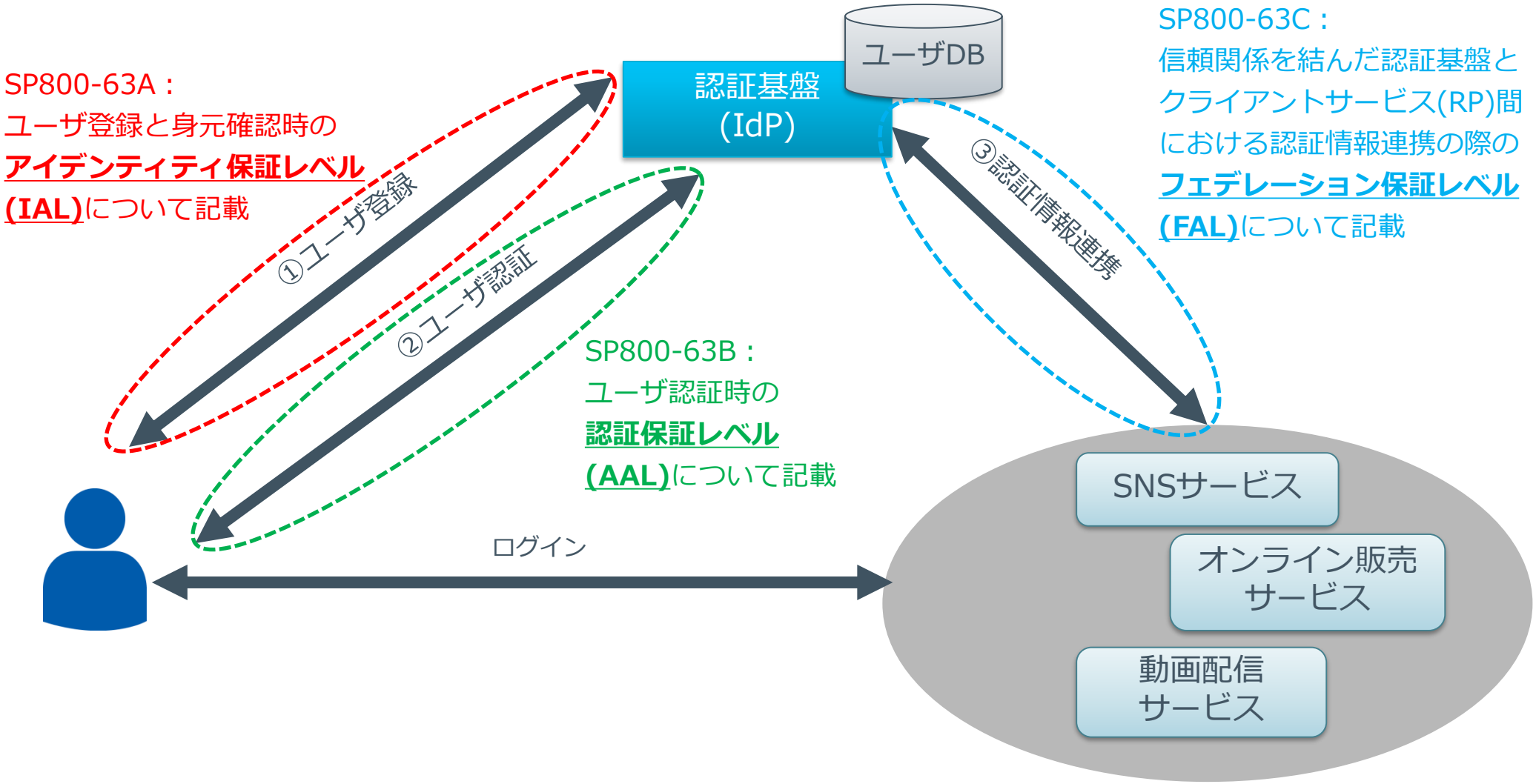
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

全体の文書構成

文書番号	タイトル	記述内容
SP 800-63-3	Digital Identity Guidelines	**IDフレームワークの全体の概要**、リスクに応じた保証レベルの選択
SP 800-63A	Enrollment and Identity Proofing	**ID登録と身元確認におけるアイデンティティ保証レベル**の定義
SP 800-63B	Authentication and Lifecycle Management	**認証保証レベルの導入**と各認証方式に求められる要件、脅威/プライバシー/ユーザビリティ面での考慮ポイント
SP 800-63C	Federation and Assertions	信頼関係を結んだシステム間での**認証連携（フェデレーション）におけるフェデレーション保証レベルの導入**と各レベルに求められる要件、プライバシーに考慮した属性連携

© NRI SecureTechnologies, Ltd.

NIST SP800-63-3では、ID管理・認証に関して「①ユーザ登録」、「②ユーザ認証」、「③認証情報連携」の3つの各ケースについてガイドラインを作成している。



© NRI SecureTechnologies, Ltd.

NIST SP800-63-3の各ガイドラインではID登録・認証・認証連携のそれぞれについて保証レベルを定義している。

ガイドラインで記載されている保証レベルの種別

- IAL（Identity Assurance Level）：ID自体の確からしさを決めるプロセスにおける、確からしさの保証レベル
- AAL（Authenticator Assurance Level）：認証のプロセスおよび、認証結果の確からしさの保証レベル
- FAL（Federation Assurance Level）：IDフェデレーションのプロトコルおよび、属性情報に関する保証レベル

ガイドラインで記載されている各保証レベルに必要な要件

保証レベル		概要
IAL	1	IDを人物と紐付ける必要がなく、申請のみによるものとする。
	2	対面または非対面で、エビデンスによりIDと人物とを紐付けていることを証明する。
	3	対面で、エビデンスによりIDと人物とを紐付けていることを代理人が検証する。
AAL	1	単一要素または多要素の認証により利用者が認証情報を持つことを、ある程度の管理統制の元に保証する。
	2	多要素または二要素の認証により、利用者が認証情報を持つことの高い確実性を、一定の管理統制の元に保証する。
	3	指定された要素を組み合わせた認証により、利用者が認証情報を持つことの高い確実性を、高い管理統制の元に保証する。
FAL	1	SAML、OIDC等の標準的なプロトコルをもちいたアサーションであり、IdPの署名を必要とする。
	2	FAL1に加えて、暗号化した通信を用いる。
	3	FAL2に加えて、Cryptographic Authenticator等で利用者側がそのアサーションに紐付く鍵の所有を証明する。

(出所) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

© NRI SecureTechnologies, Ltd.

適切な保証レベルを選択するためには、サービスごとにデジタルアイデンティティに関する潜在的なリスクを評価する必要がある。

リスク評価と保証レベルの決定

- 今日のデジタルサービスでは、Identity Proofing と Authenticator と Federation の各要件をひとくくりにすると、意図しない結果が生じる要因となるため、個別に失敗時のリスクと影響を評価する必要がある。
- NIST SP 800-63-3 ではIAL,AAL,FALを決定するために、下記の被害カテゴリーに対して潜在的な影響度を評価を行い、それに対応した保証レベルを選択する手順について記載されている。

	保証レベル		
被害カテゴリー	1	2	3
不便, 苦痛, または社会的地位やレピュテーションの毀損	Low	Mod	High
経済的損失または機関の負債	Low	Mod	High
機関のプログラムや公共の利益への損害	N/A	Low/Mod	High
Authorize のないセンシティブ情報の公開	N/A	Low/Mod	High
個人の安全	N/A	Low	Mod/High
民事または刑事上の違反	N/A	Low/Mod	High

(出所) https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

© NRI SecureTechnologies, Ltd.

各被害カテゴリーの潜在的影響と影響レベルの関係は相対的なものとなっており、各サービスにおいてどの影響レベルにあたるか慎重な検討が必要となる。

- 被害カテゴリーと潜在的影響、影響レベルの関係性を以下に示す。
- 影響レベルを決定する影響の度合いは相対的なものとして定められており、影響レベルの決定にあたっては、ユースケースに基づき、慎重な検討が必要になる。

被害カテゴリー	潜在的影響	影響レベル
不便, 苦痛, または社会的地位やレピュテーションの毀損に関する潜在的影響	最悪でも, 任意の主体に対する, 限定的かつ短期間の不便, 苦痛, 困難.	Low
	最悪でも, 任意の主体に対する, 相当かつ短期間ないしは限定的だが長期間の不便, 苦痛, 社会的地位やレピュテーションの毀損.	Moderate
	任意の主体に対する, 重度または重大かつ長期的な不便, 苦痛, 社会的地位やレピュテーションの毀損. これは通常, 特に重大な影響を及ぼしたり, 多くの個人に影響を及ぼす可能性のある状況を想定したレベルである.	High
経済的損失に関する潜在的影響	最悪でも, 任意の主体に対する, ささいで取るに足らない経済的損失ないしは機関の負債	Low
	最悪でも, 任意の主体に対する, 相当な経済的損失ないしは機関の負債	Moderate
	任意の主体に対する, 重大または致命的な経済的損失ないしは機関の負債	High
機関のプログラムや公共の利益への損害に関する潜在的影響	最悪でも, 組織の運用や資産, 公共の利益への限定的な悪影響. 限定的な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の低下による組織の主たる機能の処理効率の目に見えた低下, (ii) 組織資産または公益への軽微な損害, などがある	Low
	最悪でも, 組織の運用や資産, 公共の利益への相当な悪影響. 相当な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の著しい低下による組織の主たる機能の処理効率の著しい低下, (ii) 組織資産または公益への著しい損害, などがある	Moderate
	組織の運用や資産, 公共の利益への重大または致命的な悪影響. 重大または致命的な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の重大な低下や喪失による組織の主たる機能の処理不能, (ii) 組織資産または公益への深刻な損害, などがある	High

(出所) https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

© NRI SecureTechnologies, Ltd.

各被害カテゴリーの潜在的影響と影響レベルの関係は相対的なものとなっており、各サービスにおいてどの影響レベルにあたるか慎重な検討が必要となる。

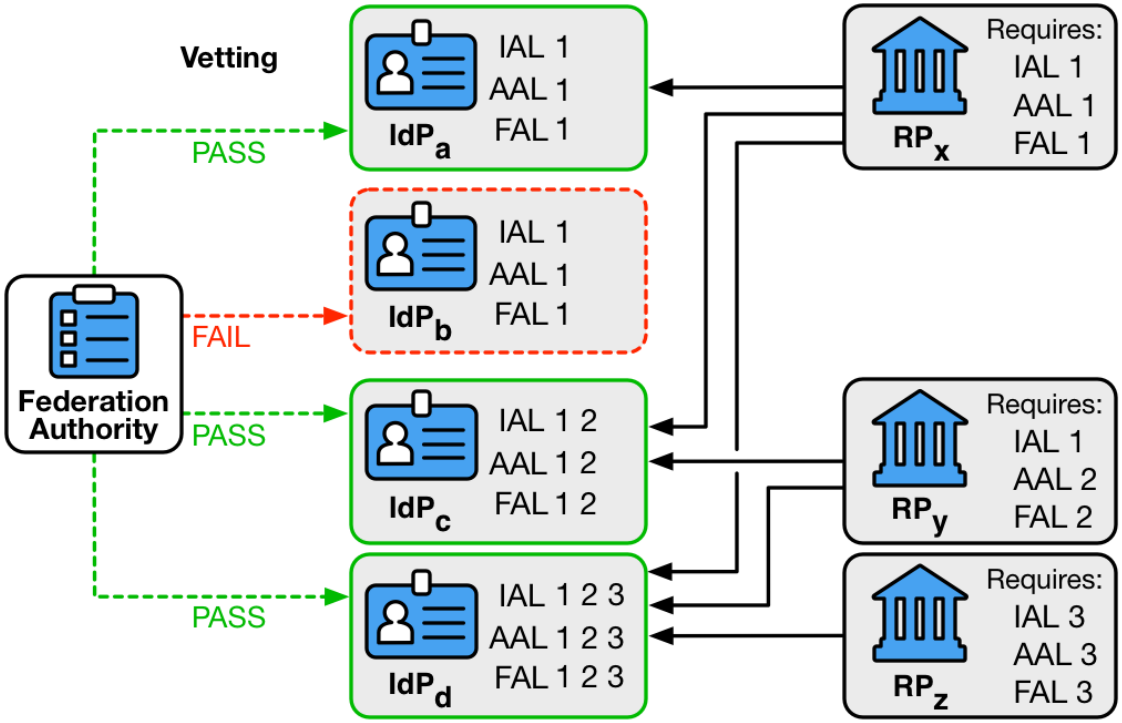
被害カテゴリー	潜在的影響	影響レベル
Authorize のないセンシティブ情報の公開に関する潜在的影響	最悪でも, FIPS 199 で定義された低インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開	Low
	最悪でも, FIPS 199 で定義された中インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開.	Moderate
	FIPS 199 で定義された高インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開.	High
個人の安全に関する潜在的影響	最悪でも, 治療を必要としない軽傷	Low
	最悪でも, 軽傷に関する中程度のリスク, ないしは治療を必要とする怪我に関する限定的リスク	Moderate
	重大な傷害または死亡に関するリスク	High
機関のプログラムや公共の利益への損害に関する潜在的影響	最悪でも, 通常は執行努力の対象とはならない種類の民事または刑事上の違反のリスク	Low
	最悪でも, 執行努力の対象とりうる民事または刑事上の違反のリスク	Moderate
	執行プログラムにとって特に重要な民事または刑事上の違反のリスク	High

(出所) https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

© NRI SecureTechnologies, Ltd.

ID連携を行うにあたっては、サービスが求める保証レベルと認証基盤が提供する保証レベルが適切であることを検証することが求められている。

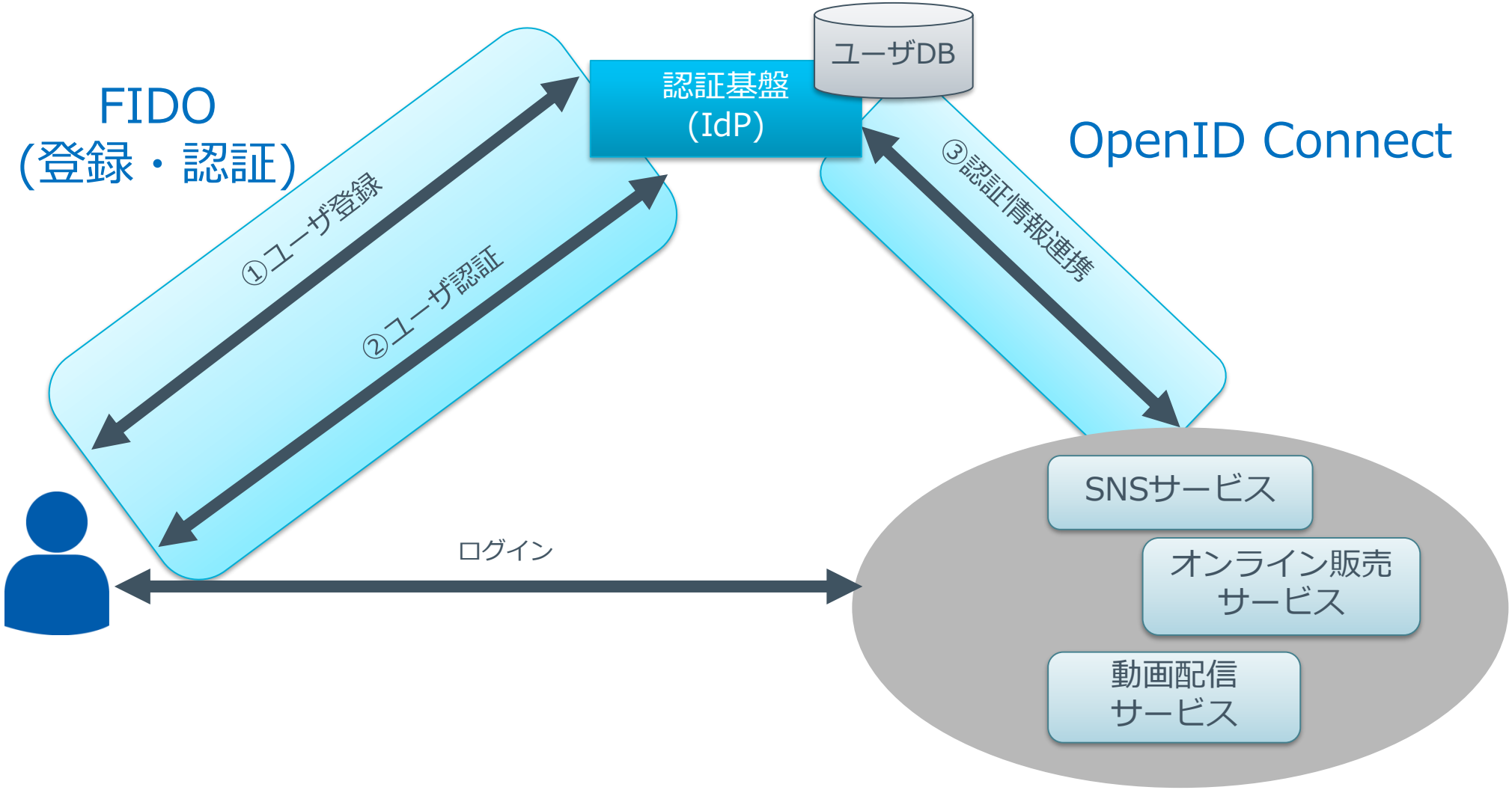
- NIST SP800-63-3Cにおいて、ID連携を行う際のFederation Authorityの概念が示されている。以下にそのモデルを示す。
  - Federation Authorityは、IdPが特定のIAL、AAL、FALで運営することを承認する。
  - Federation Authorityは、対象のID連携に関して, 期待され受入可能なIAL、AAL、FALに関するパラメータを規定すること、また、ID連携への参加者を審査し、期待されるセキュリティ、アイデンティティおよびプライバシー基準に準拠しているかを判断することが求められている。



(出所) https://openid-foundation-japan.github.io/800-63-3-final/sp800-63c.ja.html

© NRI SecureTechnologies, Ltd.

OpenID Connect及びFIDOはNIST SP800-63-3の各ガイドラインが想定する各ケースをカバーしている。



© NRI SecureTechnologies, Ltd.

認証レベルについて定義されているNIST SP800-63Bでは、認証の際に用いられる認証要素が定義されている。

カテゴリ	認証手段	内容	具体例
知識認証	記憶シークレット	ユーザーの記憶を使用した認証	パスワード、PIN
所有物認証	参照表	ユーザーと認証側で共有されている参照表を使ったチャレンジレスポンス型の認証	乱数表
	経路外認証デバイス	認証とは別のチャネルで通信可能な物理デバイスを使用した認証	SMS/プッシュ通知での携帯電話へのOTP
	単一要素OTPデバイス	OTP生成デバイスを使って生成したOTPをユーザーが入力することで行う認証	ハードウェアOTPトークン、 スマートフォンにインストールされたOTPアプリケーション
	単一要素暗号ソフトウェア	ストレージ上に格納された秘密鍵によって行う認証	クライアント証明書
	単一要素暗号デバイス	暗号鍵を格納したデバイスによって行う認証	ICカード、USB認証キー
所有物認証 ＋ （知識認証 または 生体認証で有効化する）	多要素OTPデバイス	知識認証または生体認証によって有効化されるOTPデバイス	PIN入力で正しいOTPを表示するハードウェアトークン 所有者の指紋入力でロック解除されるスマートフォン上のOTPトークン
	多要素暗号ソフトウェア	ストレージ上に格納され、知識認証または生体認証によって有効化される秘密鍵	PIN入力や指紋入力で有効化されるクライアント証明書
	多要素暗号デバイス	知識認証または生体認証によって有効化される暗号鍵を格納したデバイスによって行う認証	所有者の指紋で有効化されるUSB認証キー

© NRI SecureTechnologies, Ltd.

SP800-63-3B認証要素とFIDOで利用されるデバイス・認証器との関連は以下の通りとなる。

カテゴリ	認証手段	内容	具体例
知識認証	記憶シークレット	ユーザーの記憶を使用した認証	パスワード、PIN
所有物認証	参照表	ユーザーと認証側で共有されている参照表を使ったチャレンジレスポンス型の認証	乱数表
	経路外認証デバイス	認証とは別のチャネルで通信可能な物理デバイスを使用した認証	SMS/プッシュ通知での携帯電話へのOTP
	単一要素OTPデバイス	OTP生成デバイスを使って生成したOTPをユーザーが入力することで行う認証	ハードウェアOTPトークン、スマートフォンにインストールされたOTPアプリ
	単一要素暗号ソフトウェア	ストレージ上に格納された秘密鍵に 認証	
	単一要素暗号デバイス	暗号鍵を格納したデバイスによって行う認証	ICカード、USB認証キー
所有物認証 ＋ （知識認証または生体認証で有効化する）	多要素OTPデバイス	知識認証または生体認証によって有効化されるOTPデバイス	PIN入力で正しいOTPを表示するハードウェアトークン
	多要素暗号ソフトウェア	ストレージ上に格納され、知識認証 認証によって有効化される秘密鍵	
	多要素暗号デバイス	知識認証または生体認証によって有効化される暗号鍵を格納したデバイスによって行う認証	所有者の指紋で有効化されるUSB認証キー

FIDO U2F用のUSBドングル

FIDO対応スマートフォン
（生体認証・PIN認証・画面ロック解除あり）

© NRI SecureTechnologies, Ltd.

認証基盤の運用においては、認証器のバインディングをはじめとした認証器のライフサイクル管理、IDライフサイクル管理も重要となる。

- NIST SP800-63-3Bにおいては、認証要素を実現する認証器(Authenticator)のライフサイクル管理についても言及されている。
- 認証器のライフサイクル管理のアクションとして、以下が挙げられている。
  - 認証器のバインディング（認証器とユーザを紐づける初期登録作業）
  - 認証器の紛失、盗難、破損、不正な複製
  - 有効期限切れ
  - 失効と解約

- NIST SP800-63-3における直接的な言及はないが、**一般に、認証基盤およびID管理基盤としてはIDライフサイクル管理は重要な機能として求められる。**
- IDライフサイクルについては、ISO/IEC 24760 A framework for identity managementにおいて、登録、アクティベーション、停止、削除等、IDの状態遷移のモデルが示されている。認証基盤には、それらのIDライフサイクル管理を適切に行うための機能を備えることが必要となる。

© NRI SecureTechnologies, Ltd.

NIST SP 800-63Cでは定義されているフェデレーション保証レベル(FAL)と各レベルにおいてOpenID Connectが準拠すべき内容について記載されている。

- フェデレーション(認証連携)における各保証レベル(FAL)とOpenID Connect利用の際に対応すべき内容について以下に示す。

保証レベル	OpenID Connectで準拠すべき内容
FAL1	特に機能追加の無い OpenID Connect Basic Client プロファイル
FAL2	FAL1の要件に加え、IDトークンをRPの公開鍵で暗号化する必要がある。 (IDトークンの暗号化についてはOpenID Connect Coreの「10. Signatures and Encryption」で定義)
FAL3	FAL2の要件に加え、サブスクライバ(エンドユーザ)がIDトークンに紐づく鍵の所有証明を行う(Token Binding)必要がある。 (IDトークンのToken Binding仕様としてはOpenID Connect Token Bound Authentication 1.0が存在)

- OpenID ConnectにおけるImplicit Clientプロファイルのようにに IDトークンが一度サブスクライバ(ユーザのブラウザ)を経由するFront-channel提示手法においては、IDトークンの内容がブラウザや他者への漏洩を防ぐためにFAL2以上が必要と記載されている。

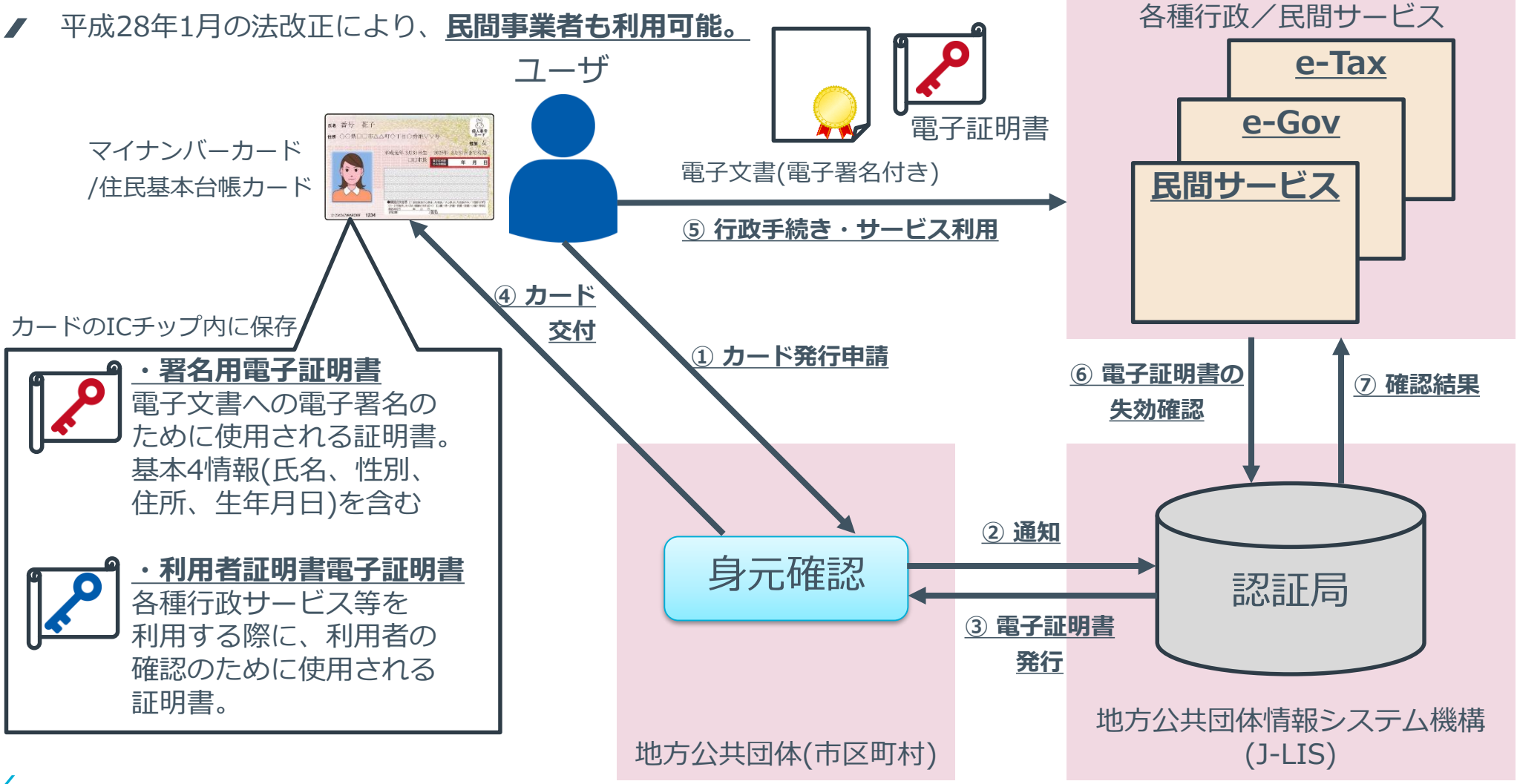
© NRI SecureTechnologies, Ltd.

4. 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

© NRI SecureTechnologies, Ltd.

公的個人認証サービス(JPKI)は、公開鍵暗号方式に基づく電子証明書を使った電子署名・本人確認機能を提供する。

- インターネット上での行政手続きを安全に行うために、公開鍵暗号方式に基づく電子証明書を使った電子署名・本人確認機能を提供する。
- 平成28年1月の法改正により、**民間事業者も利用可能。**



© NRI SecureTechnologies, Ltd.
https://www.soumu.go.jp/main_content/000400619.pdf を基にNRIセキュアテクノロジーズ作成

公的個人認証サービス(JPKI)は電子文書への署名/検証機能の他、利用者証明や基本4情報提供の機能も提供している。

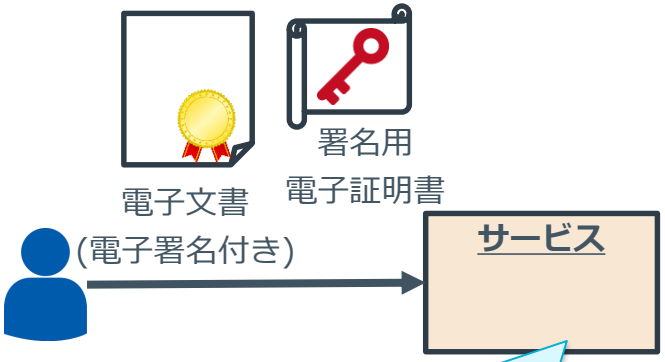
JPKIでは大きく3つの機能を提供している。

① 電子文書への署名および検証

② 利用者証明

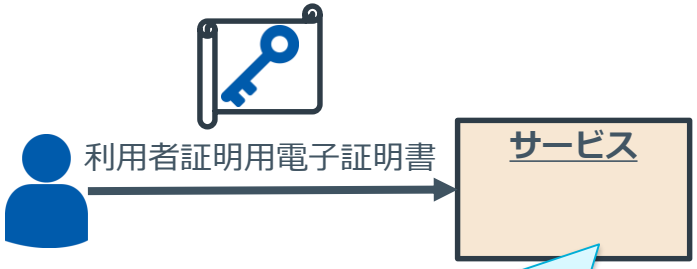
③ 基本4情報(氏名、性別、住所、生年月日)の参照

① 電子文書への署名および検証



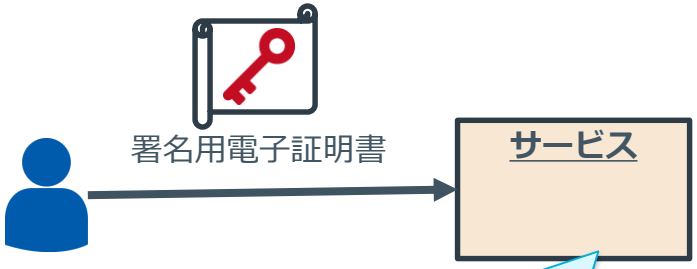
サービスは電子証明書に含まれる公開鍵を使って電子署名を検証することで、電子文書が改ざんされていないことを確認

② 利用者証明



サービスは電子証明書に含まれる公開鍵を使って利用者本人であることの検証を行う。

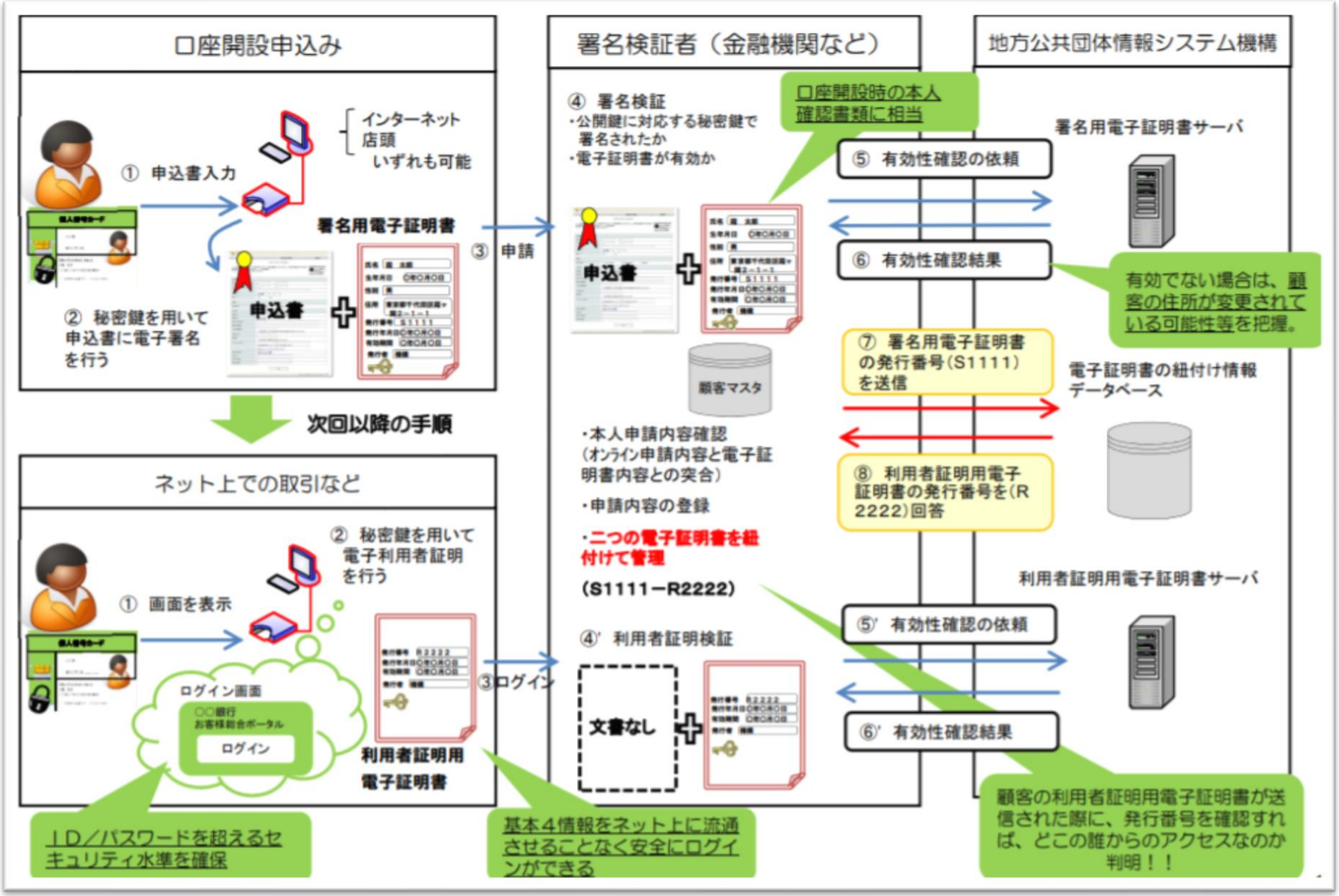
③ 基本4情報の参照



サービスは電子証明書に含まれる基本4情報を参照する

© NRI SecureTechnologies, Ltd.

公的個人認証サービス(JPKI) 活用例として、金融サービスにおけるユーザ登録・認証での利用が挙げられている。

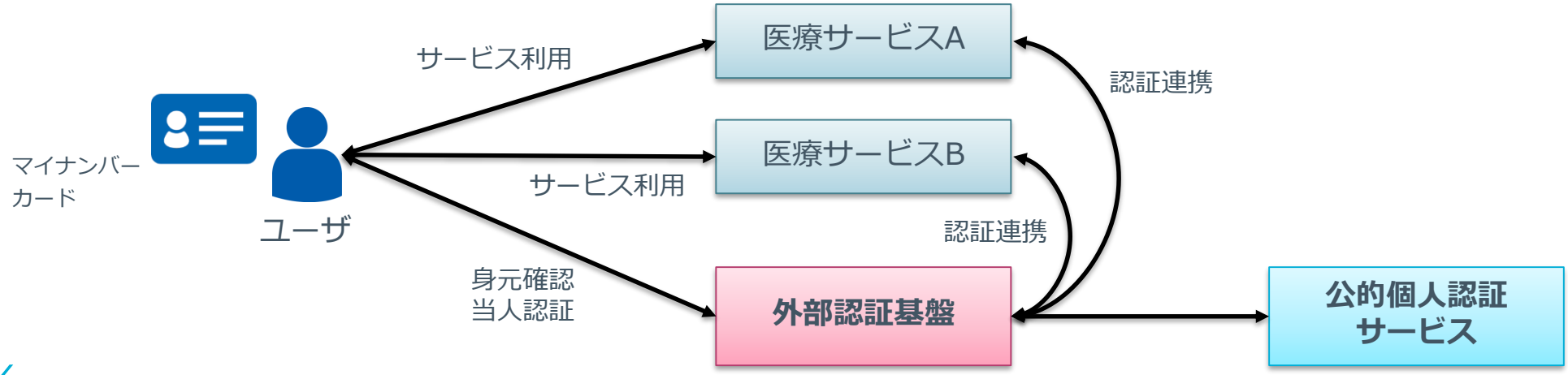


参照元：https://www.soumu.go.jp/main_content/000324414.pdf

© NRI SecureTechnologies, Ltd.

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。

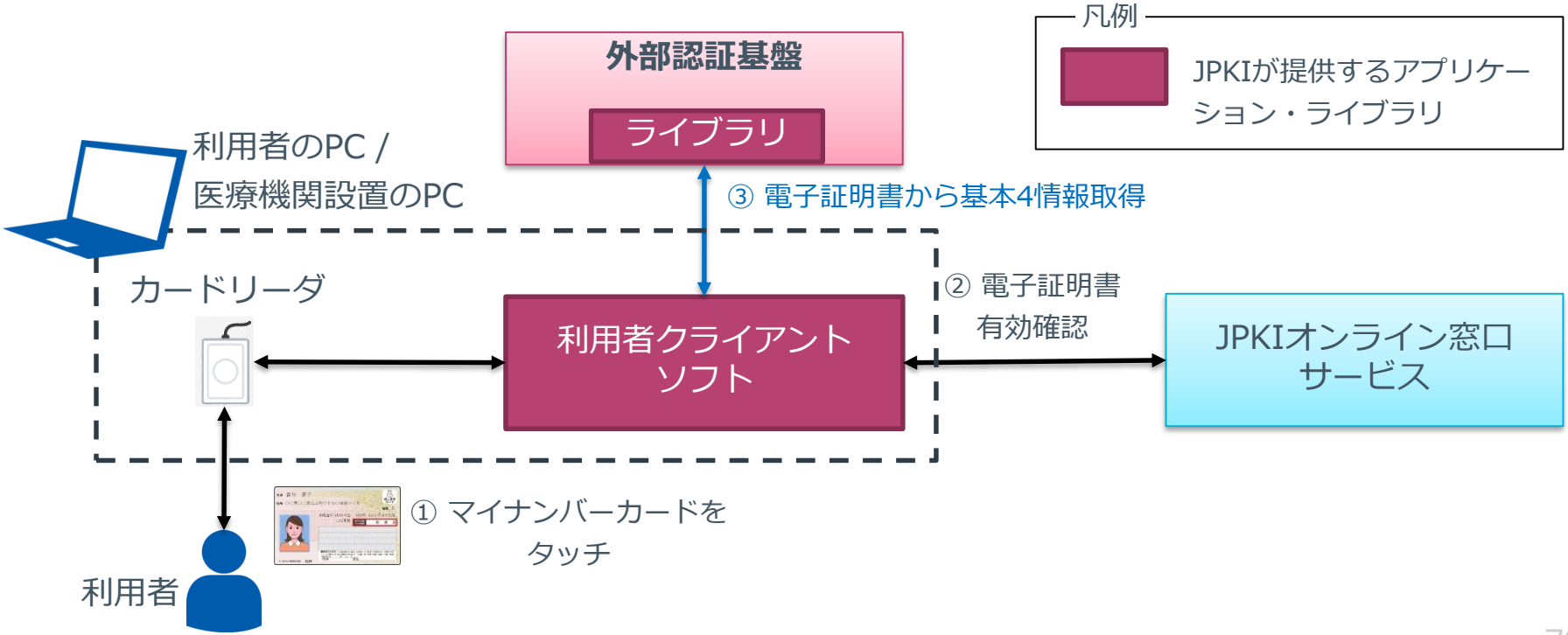
- 医療福祉分野における一部のサービスでは、個人の検診情報など要配慮個人情報に相当する情報を扱うことが想定される。この場合、ユーザ登録時における身元確認やサービス利用時の当人認証には高いレベルが求められることが考えられる。
- 身元確認の方法としては顔写真付き公的証明書を使った確認などいくつかの方法が存在するが、**認証基盤でのユーザ登録に関して、セキュリティレベルの高い身元確認および当人認証を実現する方法の1つとして、公的個人認証サービス(JPKI)を活用することが考えられる。**
- マイナンバーカードは、署名用電子証明書に基本4情報と呼ばれる氏名・性別・生年月日・住所の情報を保持している。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。



© NRI SecureTechnologies, Ltd.

外部認証基盤は、JPKI側が提供するライブラリを組み込むことで、マイナンバーカード／住民基本台帳カードから基本4情報を取得できる。

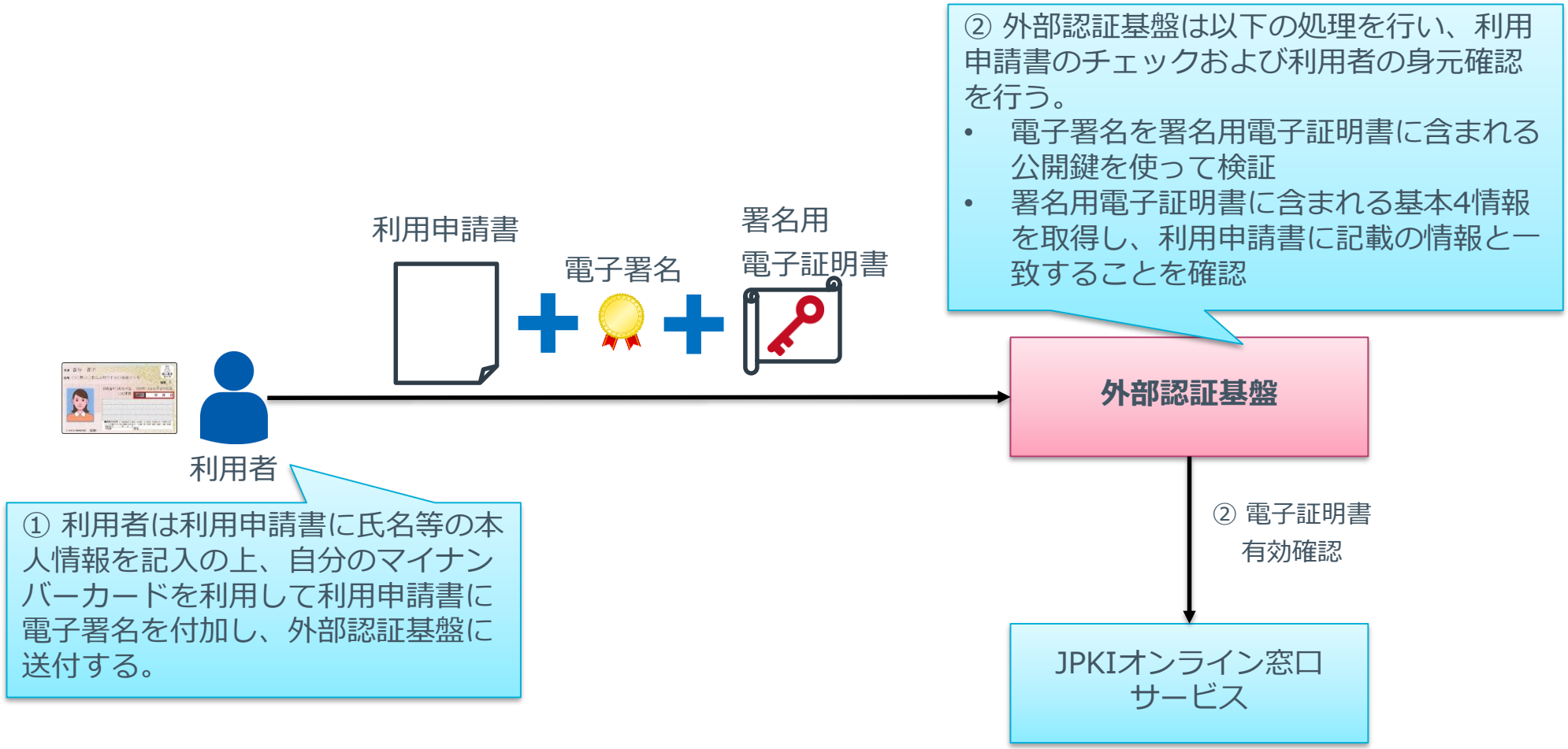
- JPKIで利用される署名用電子証明書の中には、基本4情報と呼ばれる氏名・性別・生年月日・住所の4情報が含まれており、マイナンバーカードや住民基本台帳カードのICチップに格納されている。
- **基本4情報については、カード発行申請時に地方公共団体によって確認された情報であり、信頼性が高い情報として利用できる。**
- JPKIではクライアントアプリケーション向けに署名用電子証明書から基本4情報を取得するなどの各種操作のためのライブラリを提供しており、外部認証基盤にこのライブラリを組み込むことで基本4情報を取得できる。これらの情報確認により身元確認を行うことができる。



© NRI SecureTechnologies, Ltd.

外部認証基盤では、JPKIを利用して利用申請書などの電子文書の署名検証および基本4情報による身元確認を行う方式が考えられる。

- 外部認証基盤の利用申請時など、利用者の身元確認が必要となるケースにおいて、JPKIの署名用電子証明書による電子署名の検証および基本4情報の取得による身元確認の流れは以下の通りとなる。
  - 以下は、外部認証基盤利用申請時の身元確認時の例となる。



© NRI SecureTechnologies, Ltd.

JPKIを使った身元確認については、犯罪による収益の移転防止に関する法律施行規則においても身元確認方法の1つとして規定されている。

- 犯罪による収益の移転防止に関する法律施行規則（以降、犯収法）は2018年11月の法改正によりオンラインで完結する身元確認方法が規定された。
- **JPKIを活用した身元確認については、現在の犯収法の第六条一項「ワ」で以下の通り定義されている。**

ワ　当該顧客等から、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成十四年法律第百五十三号。以下この号において「公的個人認証法」という。）第三条第六項の規定に基づき**地方公共団体情報システム機構が発行した署名用電子証明書及び当該署名用電子証明書により確認される公的個人認証法第二条第一項に規定する電子署名が行われた特定取引等に関する情報の送信を受ける方法**（特定事業者が公的個人認証法第十七条第四項に規定する署名検証者である場合に限る。）

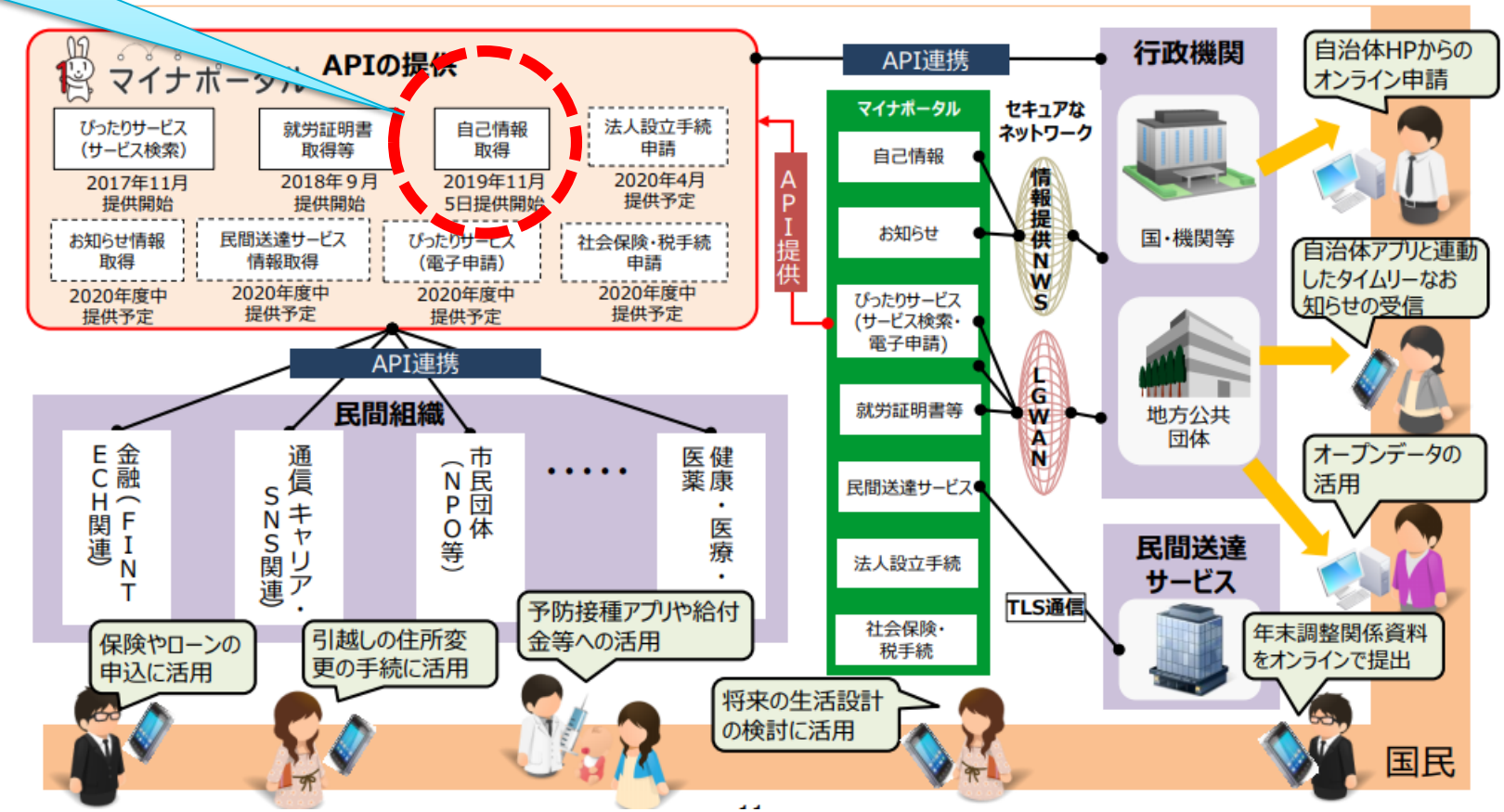
© NRI SecureTechnologies, Ltd.

マイナポータルでは、利用者の自己情報をAPIの形で提供する仕組みを用意しており、外部認証基盤においても活用が可能であると考えられる。

行政機関が保持する
自己情報を提供するAPI

マイナポータルで提供する機能を、行政機関だけではなく企業や市民団体等の民間組織に対してもAPIとして提供することで、自己情報や検索機能を活用した新たな行政サービス・民間サービスの開発につながることが期待されます。

※ APIとは、アプリケーション・プログラミング・インターフェースの略。マイナポータルのAPIの提供は、外部のWEBサービスのシステムからマイナポータルにアクセスしてその機能を活用できるように必要な仕様等を作成し、一定の要件の下で公開するものです。

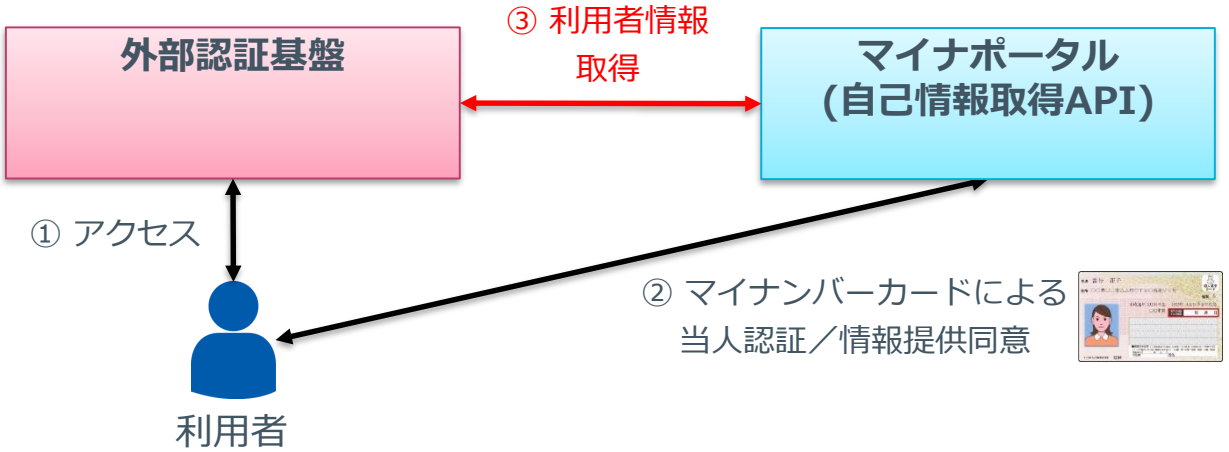


参照元：https://www.mhlw.go.jp/content/12401000/000610530.pdf

© NRI SecureTechnologies, Ltd.

外部認証基盤は、マイナポータルが提供する自己情報取得APIを呼び出すことで、行政機関が保持する利用者情報を取得できる。

- 外部認証基盤は利用者の利用登録このAPIを呼び出すことで自己情報にアクセスでき、これにより利用者への属性提供や当人認証に活用することができる。

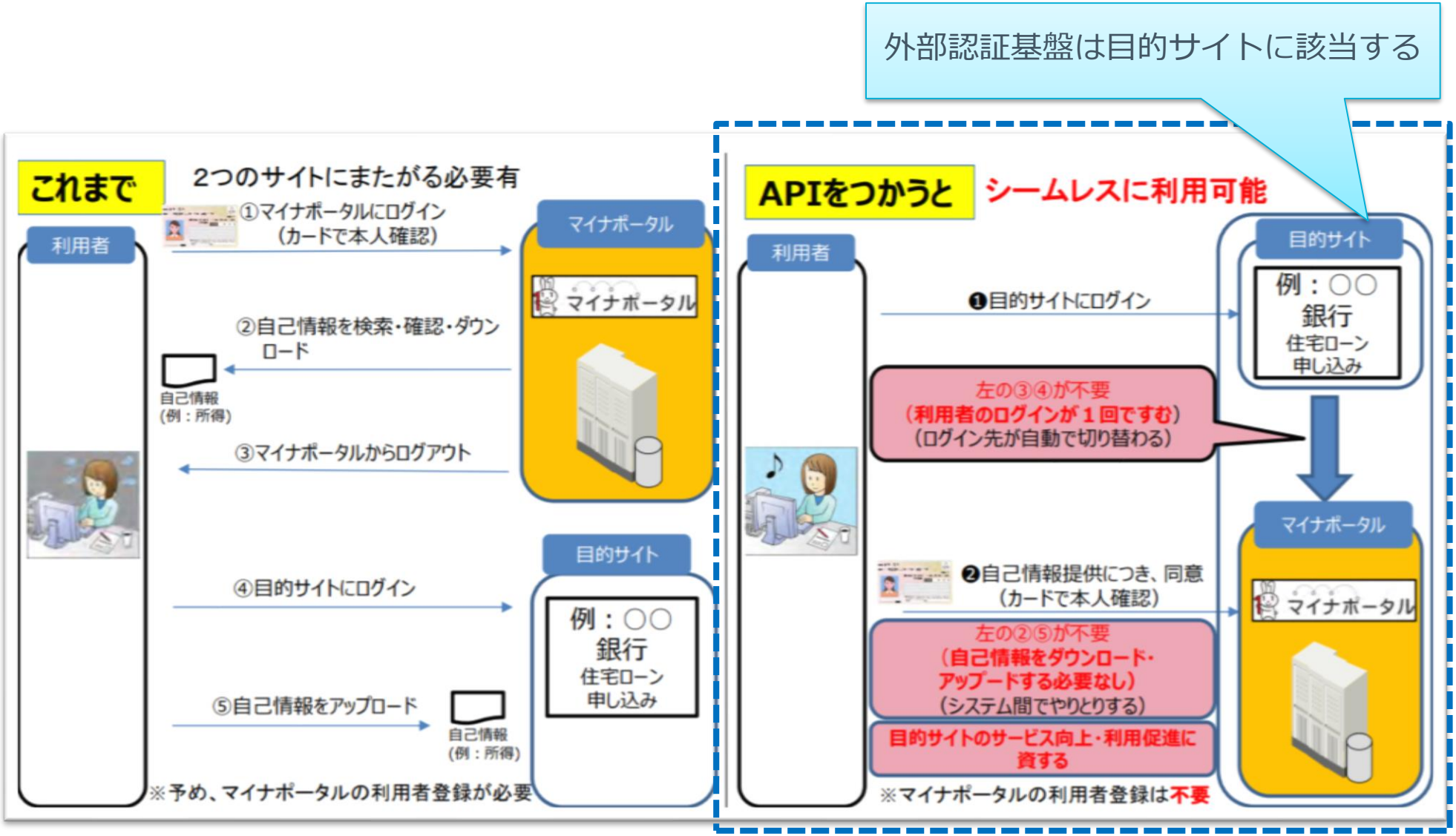


- 自己情報取得APIで取得可能な情報の分野名および分野詳細名(2020年3月時点)はそれぞれ以下の通り。

No.	分野名	分野詳細名
1	世帯	世帯
2	税	地方税
3	社会保障(健康・医療)	医療保険、予防接種、健康・医療その他
4	社会保障(子ども・子育て)	子ども・子育て支援、母子家庭等関係、母子健康、教育・就学支援、子ども・子育てその他
5	社会保障(福祉・介護)	障害保健福祉、生活保護・福祉一般、中国残留邦人等支援、介護・高齢者福祉
6	社会保険(雇用・労働)	雇用、労災補償
7	社会保険(年金)	年金・日本年金機構関係

© NRI SecureTechnologies, Ltd.

外部認証基盤における本人確認に自己情報取得APIを活用した場合のシーケンスイメージは以下の通り。



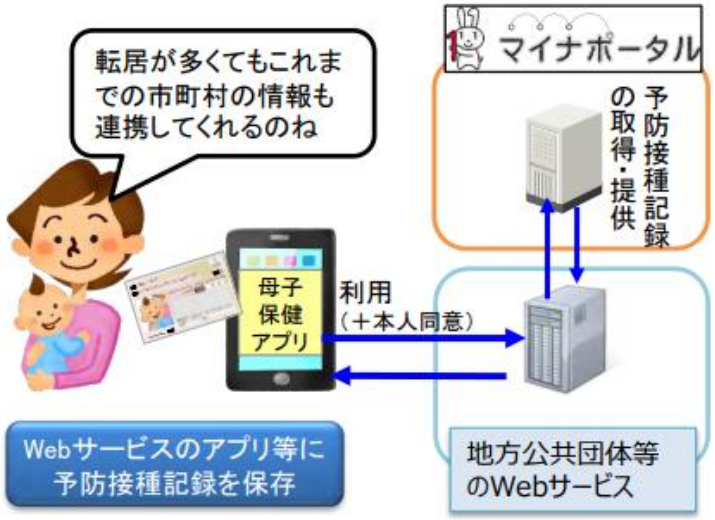
参照元：https://www.cao.go.jp/bangouseido/pdf/api_notice.pdf

© NRI SecureTechnologies, Ltd.

神奈川県が開発した健康増進アプリの「マイME-BYOカルテ」は、マイナポータルが提供している自己情報取得APIを利用して、予防接種記録の取得を行っている。

マイME-BYOカルテの概要

- 神奈川県が開発した健康増進アプリ。
- 歩数の自動記録、服薬情報、母子健康手帳、健診情報の登録と確認を行うことができる。
- 歩数計アプリ、血液検査アプリ、健康増進アプリなどの民間サービスのアプリとも連携を行っている。
- マイナポータルが提供している自己情報取得APIを利用して、予防接種記録の取得を行い、アプリ上から予防接種履歴の確認を行うことができる。



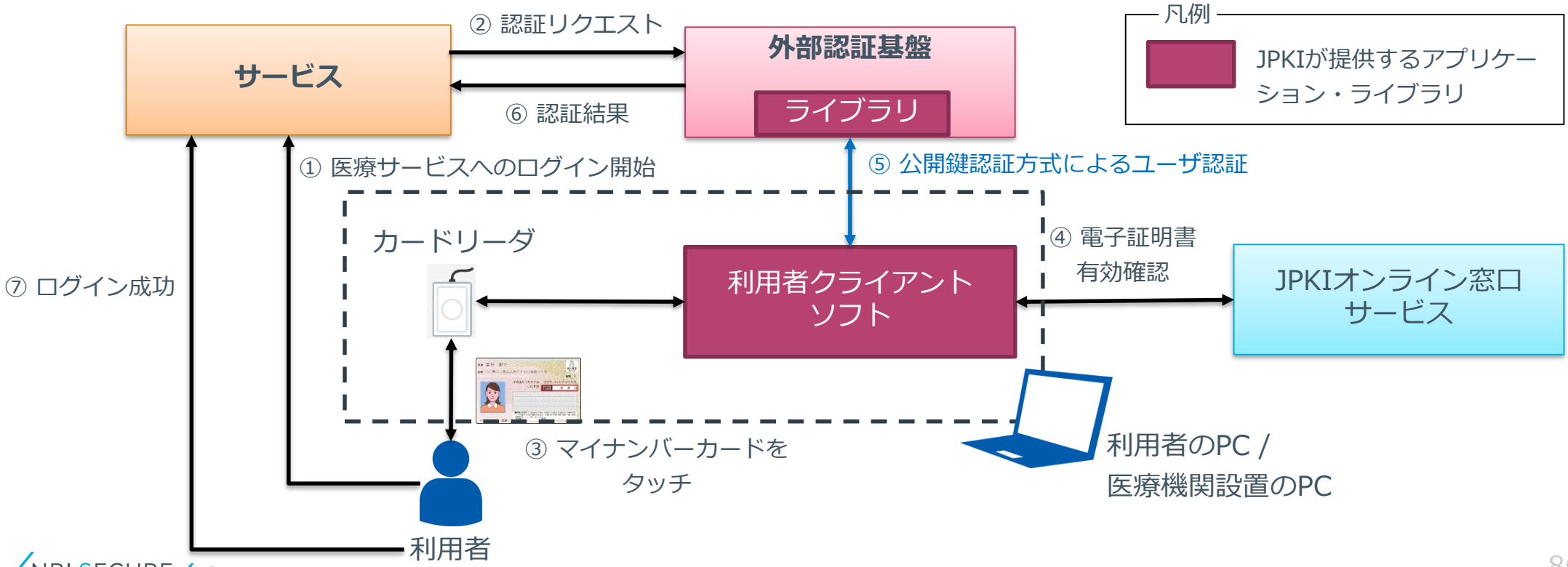
予防接種履歴の連携

※参照元：https://www.pref.kanagawa.jp/docs/mv4/cnt/f532715/p991437.html
https://www.cao.go.jp/bangouseido/pdf/myna20191021.pdf

© NRI SecureTechnologies, Ltd.

JPKIが提供する公開鍵認証方式による利用者証明機能を活用することで、外部認証基盤でのユーザ認証にJPKIを活用することが考えられる。

- 外部認証基盤へのJPKIの適用について、属性情報交換による身元確認の他に、JPKIが提供する利用者証明機能を利用したサービスへのログイン時のユーザ認証への活用が考えられる。
- JPKIではユーザ認証のために利用者証明用電子証明書を提供しており、マイナンバーカード内に含まれる秘密鍵および電子証明書内の公開鍵を使った公開鍵認証方式による認証が行われる。
- **外部認証基盤において、このJPKIの利用者証明用電子証明書を利用したユーザ認証機能を導入することで、利用者は自分のマイナンバーカードで複数のサービスにログインできるため、セキュリティおよび利便性でのメリットがある。**



© NRI SecureTechnologies, Ltd.

外部認証基盤における本人確認にJPKIを活用した場合の実装・運用面での考慮事項として、利用者クライアントソフトの利用に伴う制限が挙げられる。

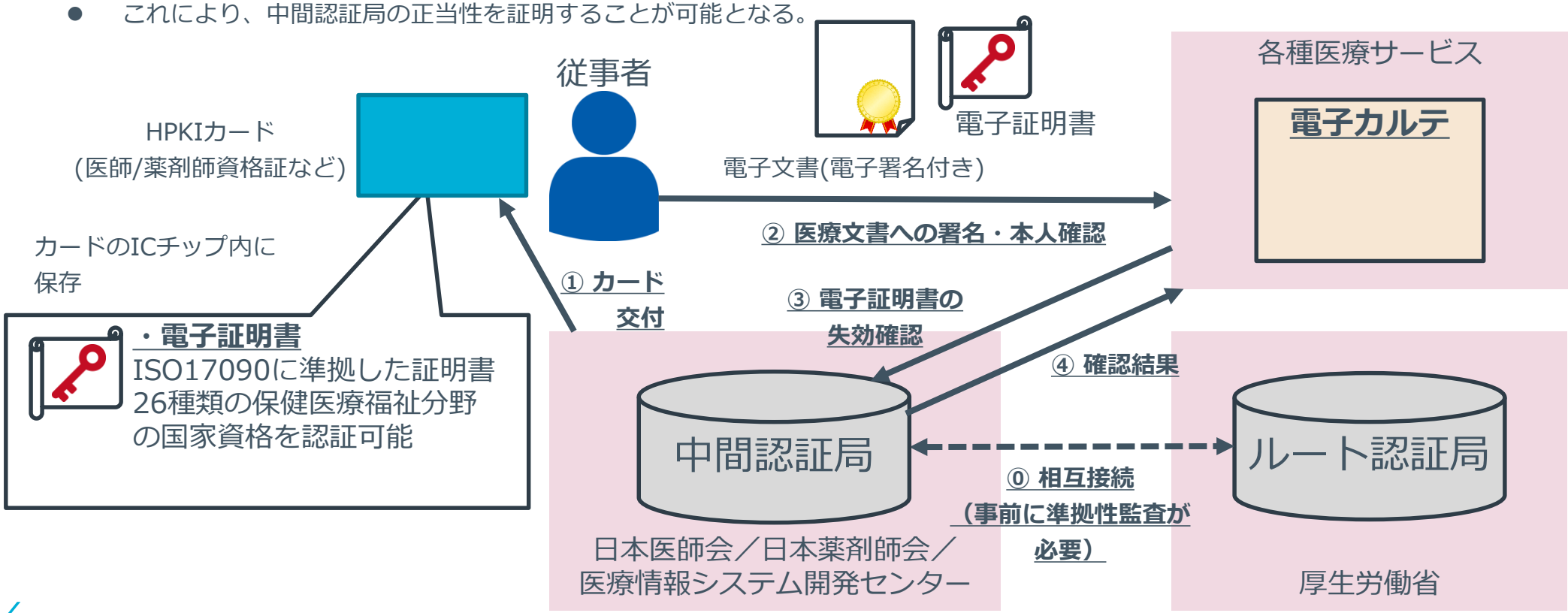
JPKI 利用者クライアントソフトの動作環境による制限

- マイナンバーカードからの基本4情報取得のために利用する利用者クライアントソフトの動作環境は、2020年3月時点では以下の通りとなっており、**利用できるブラウザやOSに制限がある**。よって、利用者が自宅からオンラインで本人確認をできるようにする場合には利用者に事前準備手順など適切な情報の提供を行う必要がある。
  - Windows 8.1 / Windows 10 : Internet Explorer 11
  - macOS v10.14 / v10.15 : Safari 13
  - Android OS
  - iOS

© NRI SecureTechnologies, Ltd.

保健医療福祉分野公開鍵基盤(HPKI)は、保健医療福祉分野の従事者を主な利用者とする公開鍵基盤である。

- インターネットを介して医療情報などをやり取りする際に、医療従事者へのなりすましやカルテ等の医療文書やデータの改ざんを防ぐために保健医療福祉分野に適用される公開鍵基盤（PKI）。
- 2005年3月にISO17090（Health Informatics -Public Key Infrastructure）で定義された「hcRole（healthcare Role）」に準拠した証明書ポリシーとして厚生労働省にて「保健医療福祉分野 PKI 認証局証明書ポリシ（以下、共通ポリシ）」を策定。
- 厚生労働省によるポリシーの準拠性監査に合格することで、厚生労働省のHPKIルート認証局と相互接続することができる。
  - これにより、中間認証局の正当性を証明することが可能となる。



http://www.medis.or.jp/8_hpki/conceptual-scheme.html を基にNRIセキュアテクノロジーズ作成

© NRI SecureTechnologies, Ltd.

保健医療福祉分野公開鍵基盤(HPKI) は、JPKIと同様の電子文書への署名/検証機能の他、当人認証及び保健医療福祉分野の国家資格証明機能を提供する。

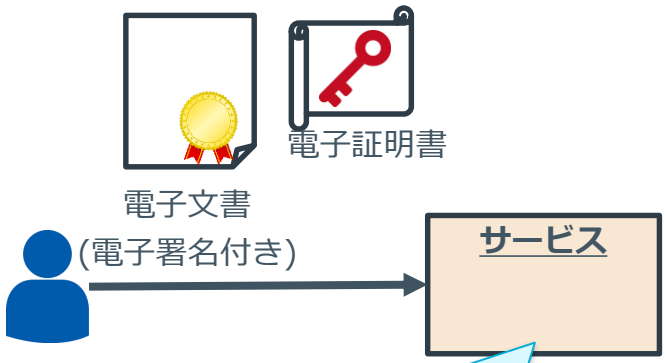
HPKIでは大きく3つの機能を提供している

① 電子文書への署名および検証

② 当人認証

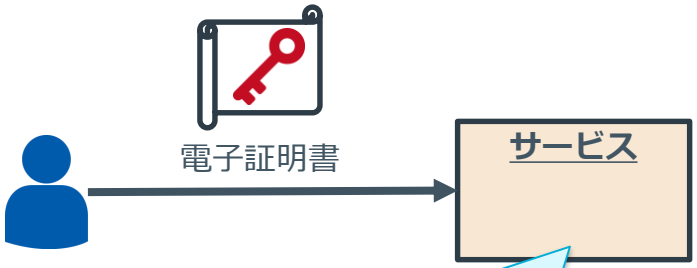
③ 26種類の保健医療福祉分野の国家資格および5種類の管理者資格の証明

① 電子文書への署名および検証



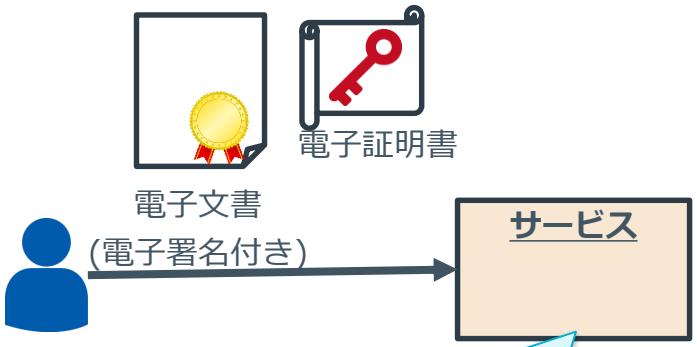
サービスは電子証明書に含まれる公開鍵を使って電子署名を検証することで、電子文書が改ざんされていないことを確認。

② 当人認証



サービスは電子証明書に含まれる公開鍵を使って利用者本人であることの認証を行う。

③ 保健医療福祉分野の国家資格および管理者資格の証明



サービスは電子証明書のhcRole（医療従事者の資格）項目を確認することで国家資格や管理者資格を認証する。

© NRI SecureTechnologies, Ltd.

保健医療福祉分野公開鍵基盤(HPKI) 活用例として、紹介状作成時の医療資格者の署名付与が挙げられる。

- 島根県のまめネット(しまね医療情報ネットワーク)では、従来の紙に押印した紹介状に代わってHPKI認証局が発行する電子証明書を使って紹介状に電子署名を付与。
- 紹介状の正当性を確保しつつ紹介状作成や送付における利便性向上を達成している。

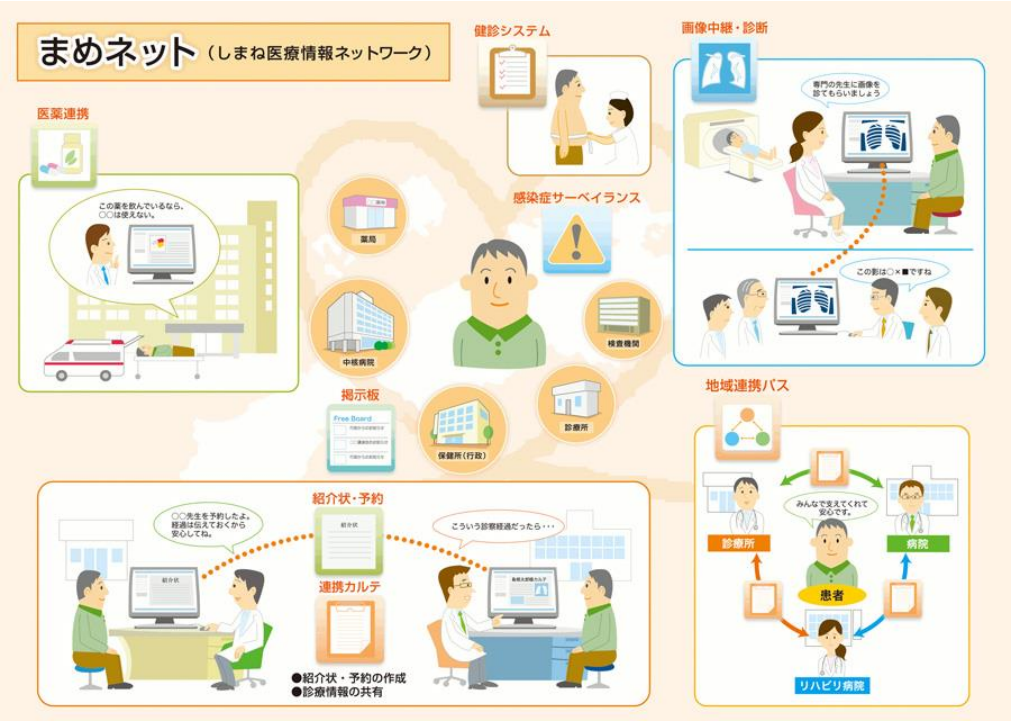
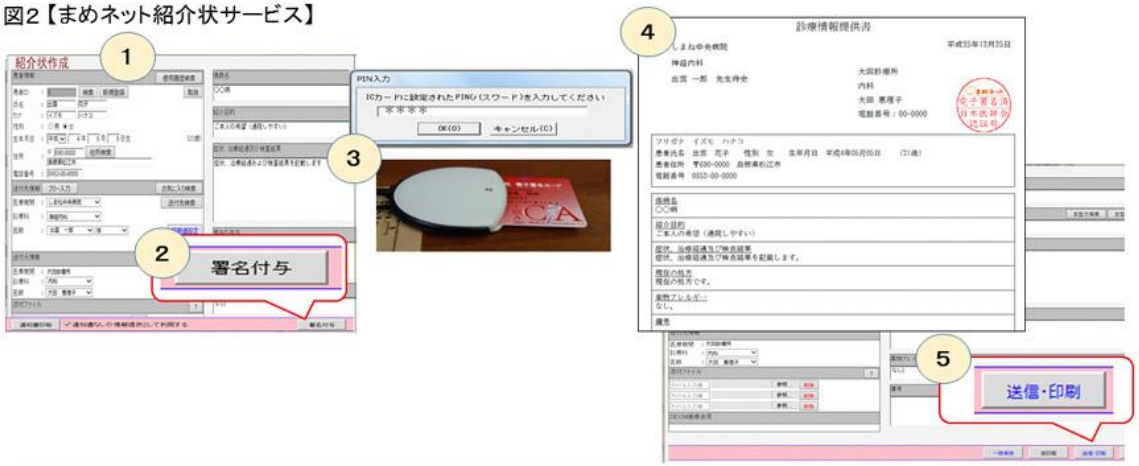


図2【まめネット紹介状サービス】



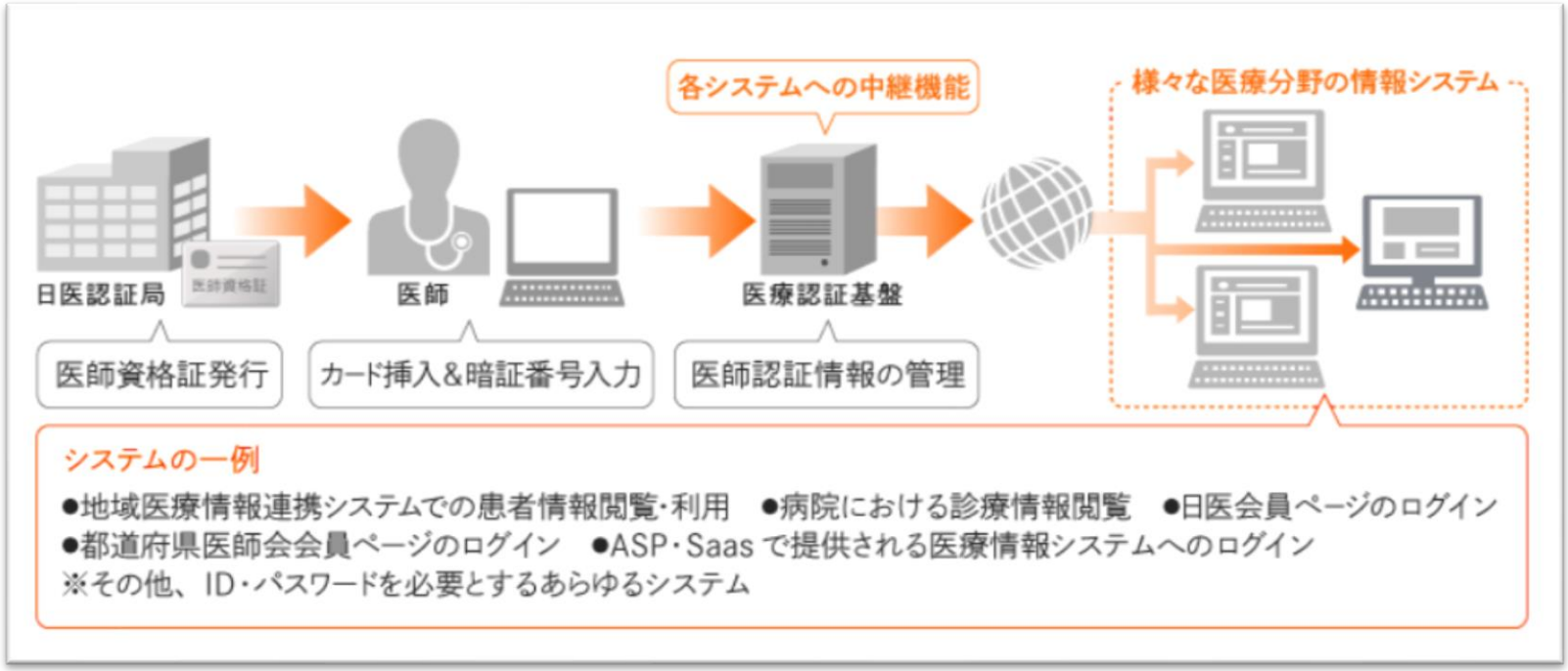
①まめネットの紹介状サービスで、紹介状を作成します。
②「署名付与」ボタンを押すと、パスワード入力画面がでます。
③医師資格証をカードリーダにセットしてパスワードを入力します。
④電子署名を付与した紹介状を作成します。この時、日医認証局に問い合わせを行い、署名の検証を行います。
⑤署名付与した紹介状を、紹介先へ送信します。

参照元：https://www.jmaca.med.or.jp/hpki/case/example02.html

© NRI SecureTechnologies, Ltd.

医療従事者向け認証基盤については、HPKIのSAMLを活用した認証および属性情報交換が考えられる。

- 医療向け認証基盤では、患者だけでなく医師などの医療従事者の認証および医療情報アクセス認可を行う必要がある。
- 医師の当人認証や属性情報（資格情報等）取得のためにHPKIを活用できる。
- 日本医師会では医療認証基盤を構築しており、医療サービスに対してHPKIによる認証結果をSAML(Security Assertion Markup Language)によって連携する仕組みを提供している。

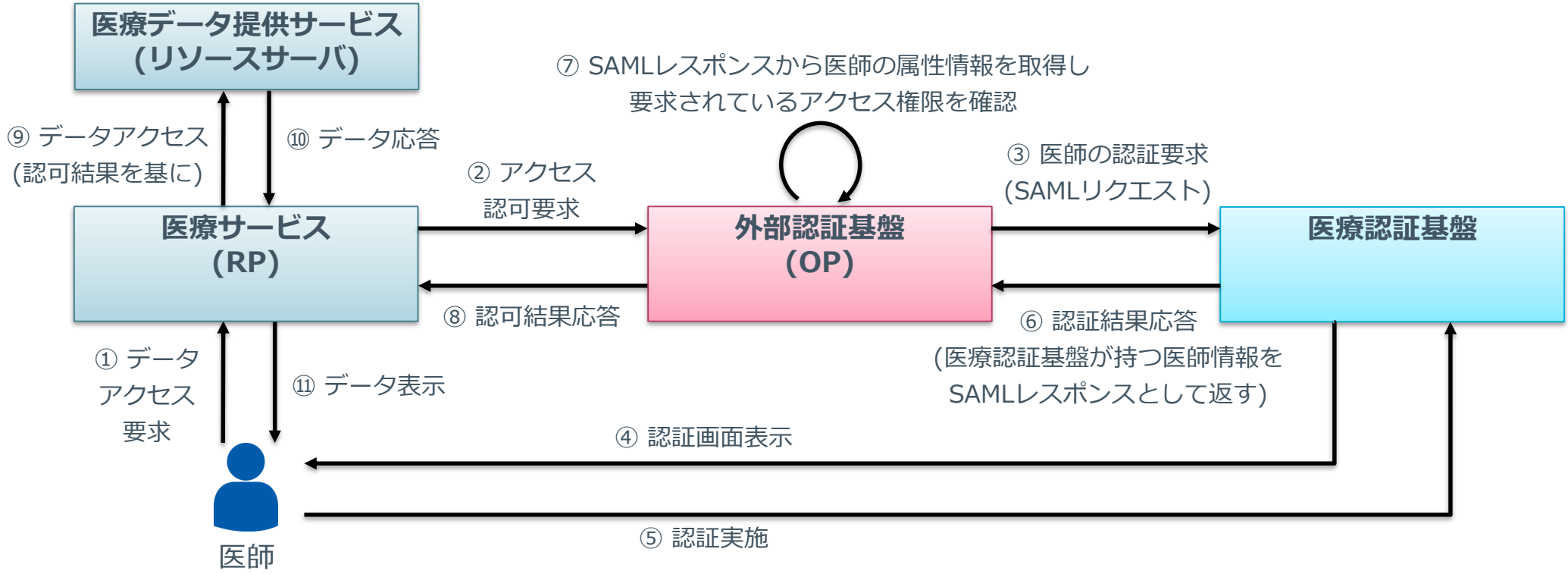


参照元：https://www.jmaca.med.or.jp/hpki/role/sso.html

© NRI SecureTechnologies, Ltd.

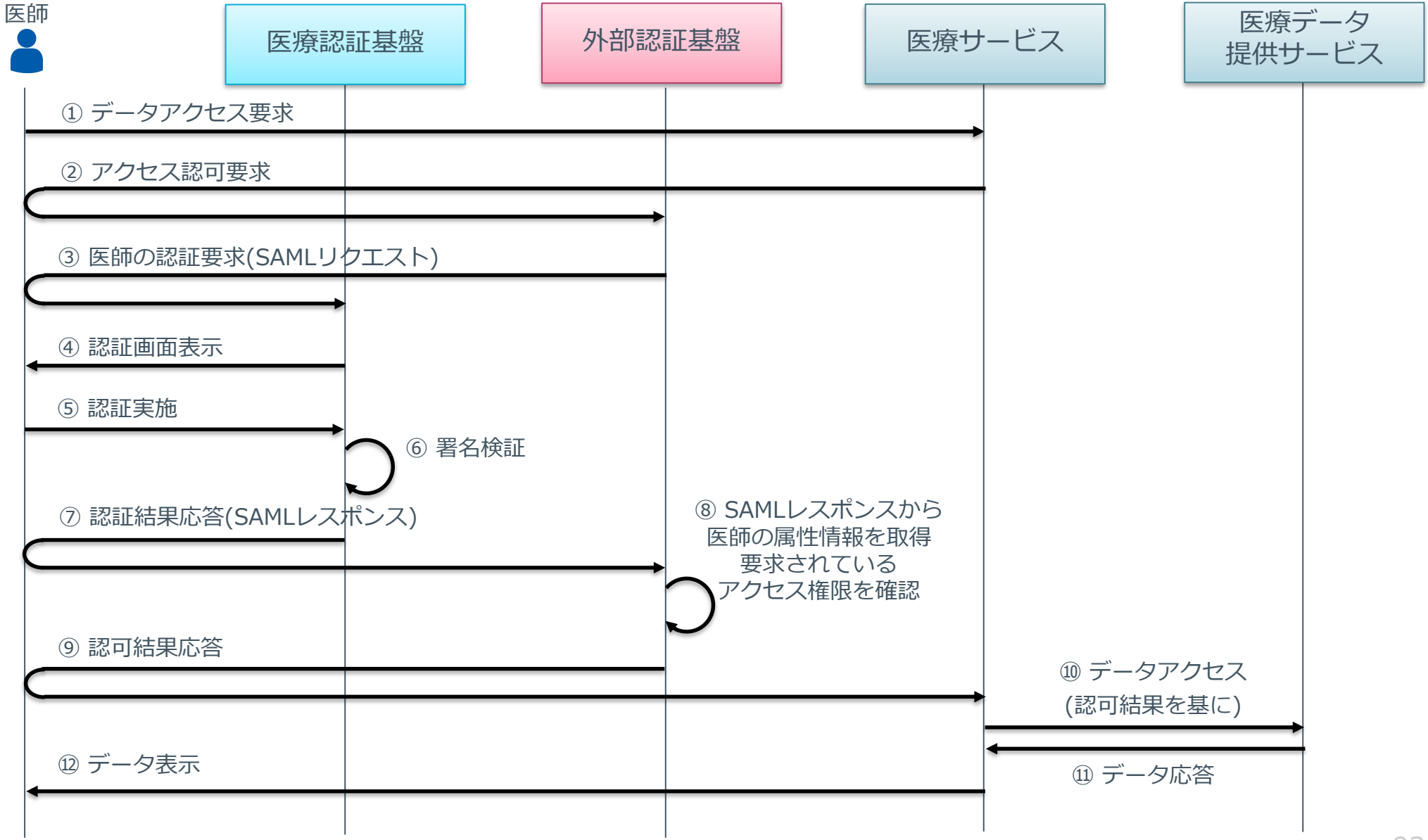
医療認証基盤の活用方法の1つとして、外部認証基盤の認証手段として連携することで医療従事者の認証を行うことが可能である。

- 外部認証基盤は医療サービスからの医療情報アクセス認可要求を受け、医療認証基盤とSAMLによる認証連携を行うことで医師の認証および医師の属性情報取得を行う。取得した属性情報を基に医療情報アクセスの許可／不許可を判断し、医療サービスに認可結果を返す。
- 医療サービスと医療認証基盤との間に外部認証基盤を挟むことで、以下の利点がある。
  - 外部認証基盤－医療サービス間のやり取りにOpenID Connect/OAuth2.0 を利用することで、SAMLだけでは対応できない認可要求処理への対応を行うことができる。
  - 今後医師以外の医療従事者向け認証基盤と連携することで、医師以外も対象とすることができる。



© NRI SecureTechnologies, Ltd.

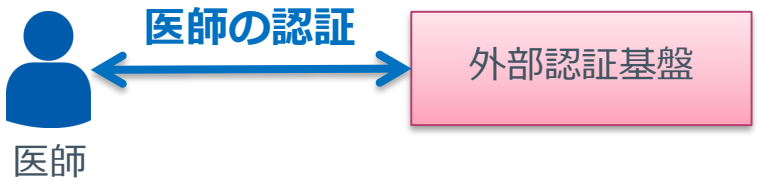
医療サービス利用時の医師の医療情報アクセス認可処理における、医療認証基盤との連携による属性情報交換のシーケンスを検討した。



© NRI SecureTechnologies, Ltd.

医療認証基盤から返却される情報を基に、外部認証基盤では医師の認証や医療情報へのアクセス認可判定等を行うことが考えられる。

- 医療認証基盤からは、認証結果応答(SAMLレスポンス)として認証された医師に関する以下の情報が返される。
  - 医籍番号
  - hcRole（health care role、HPKIで定義されている保健医療福祉分野の国家資格情報26種および管理者等資格5種）
- 外部認証基盤は、上記の情報を以下の処理に活用することが考えられる。



- また、今後医療認証基盤側で認証結果応答により多くの医師の属性情報(氏名等)を返すよう拡張がなされる場合には、外部認証基盤において以下のように初期登録時等における医師のオンライン身元確認への活用も考えられる。

- SAMLは認証連携に関する仕様であり、以下のような医療情報アクセスの認可判定はサポートしないため、外部認証基盤側で独自に実装する必要がある。

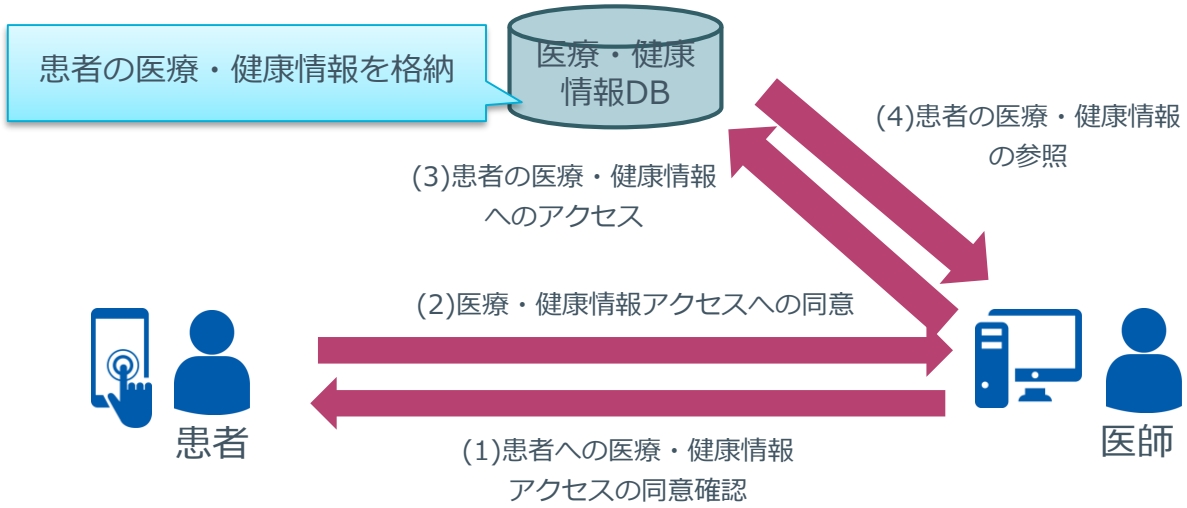
© NRI SecureTechnologies, Ltd.

5. 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

© NRI SecureTechnologies, Ltd.

診察時において医師が認証済みかつ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できるというシナリオの実現性を実証した。

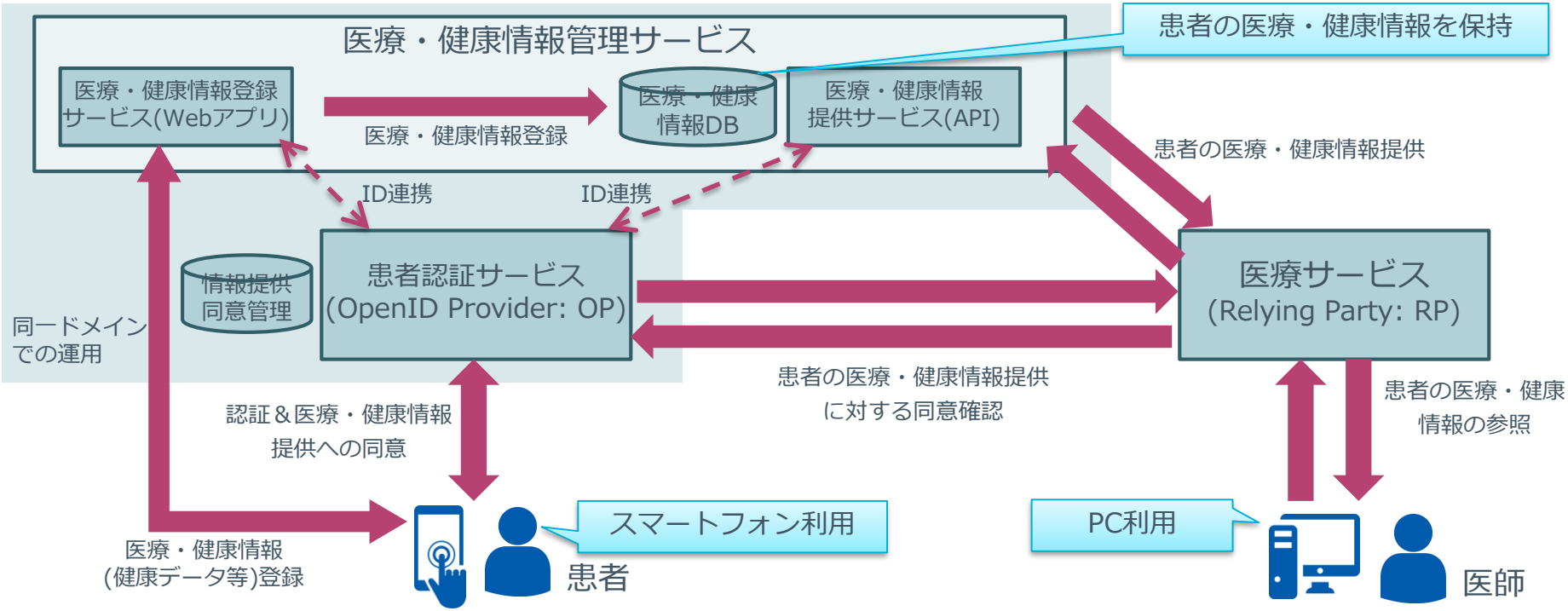
- 具体的なユースケースとして、以下を想定した。
  - 医師が診察を行うにあたって、医療サービス（電子カルテシステム等）を使って患者の医療・健康情報を閲覧・作成している。
  - 個人が記録する健康データや別の病院での過去の診察記録など、医療サービス上に存在しない医療・健康情報は、オンライン上の医療・健康情報DBに格納され、取得用のAPIインターフェースが提供されている。
  - 医師は、医療・健康情報DB上の患者の医療・健康情報を参照する場合には、患者に医療・健康情報へアクセスすることへの同意依頼を患者に行う。
  - 患者は、同意依頼をスマートフォンへの通知で受け取り、本人であることを認証したうえで医療・健康情報アクセスの同意を行う。
  - 患者の同意後に、医師は、医療サービスを通して医療・健康情報DBのAPIにアクセスし、医療・健康情報を取得、参照する。



© NRI SecureTechnologies, Ltd.

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。

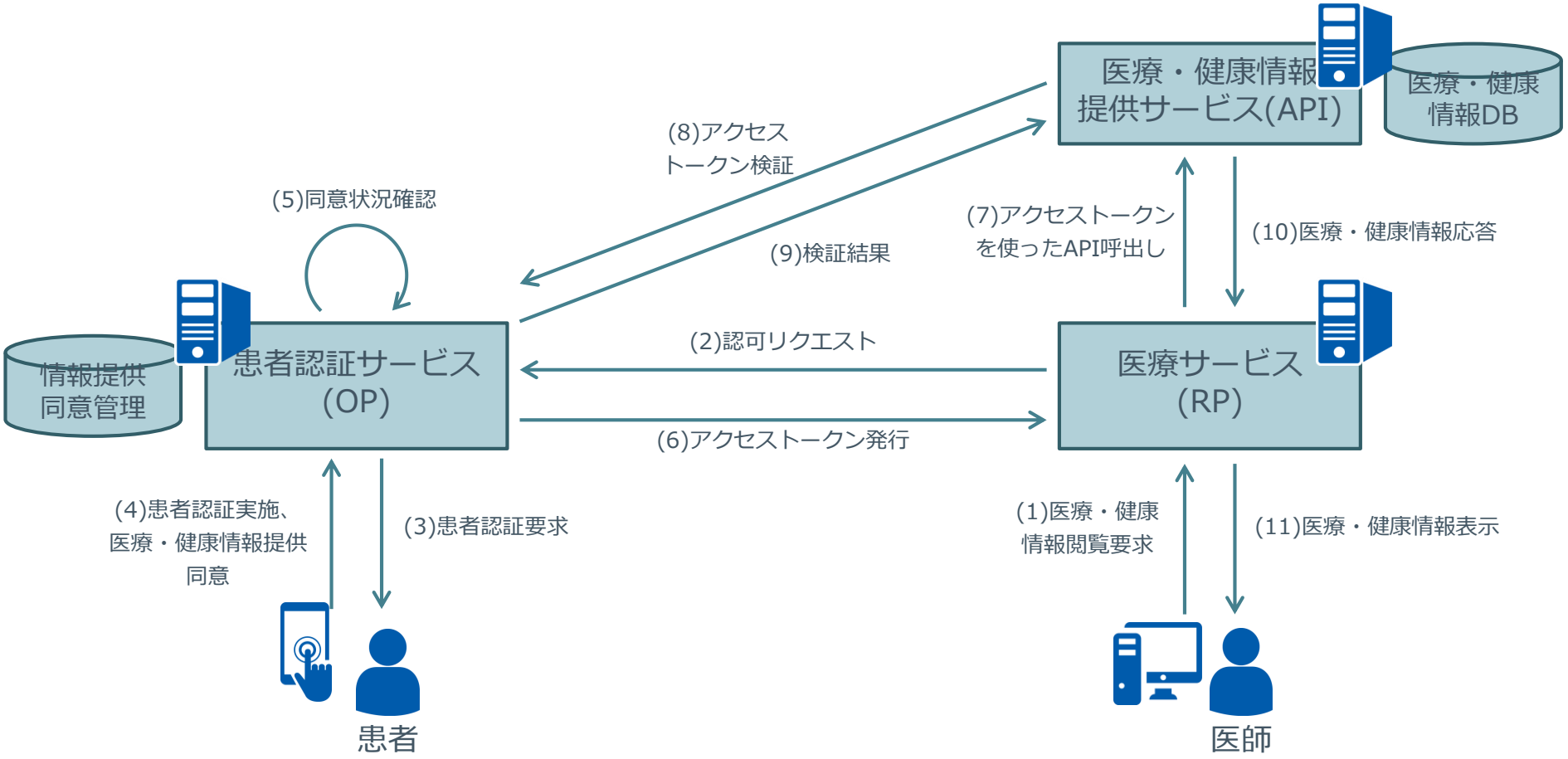


No.	システム・サービス	説明
1	医療サービス	各種医療サービス提供のために主に医師が利用するサービス。本サービス利用時の患者の認証や患者の医療・健康情報へのアクセス認可は患者認証サービスから実施する。 なお、本検討では医師の認証は何らかの手段(医師認証サービス等による)で完了していることを前提としている。
2	患者認証サービス	患者の本人認証を実施し、複数の医療サービス向けへ認証情報連携を行うサービス。認証の他、外部の医療・健康情報提供サービスに保管されている患者の医療・健康情報へのアクセス認可の管理を行う。
3	医療・健康情報管理サービス	患者または診療所等で登録された医療・健康情報を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

© NRI SecureTechnologies, Ltd.

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。

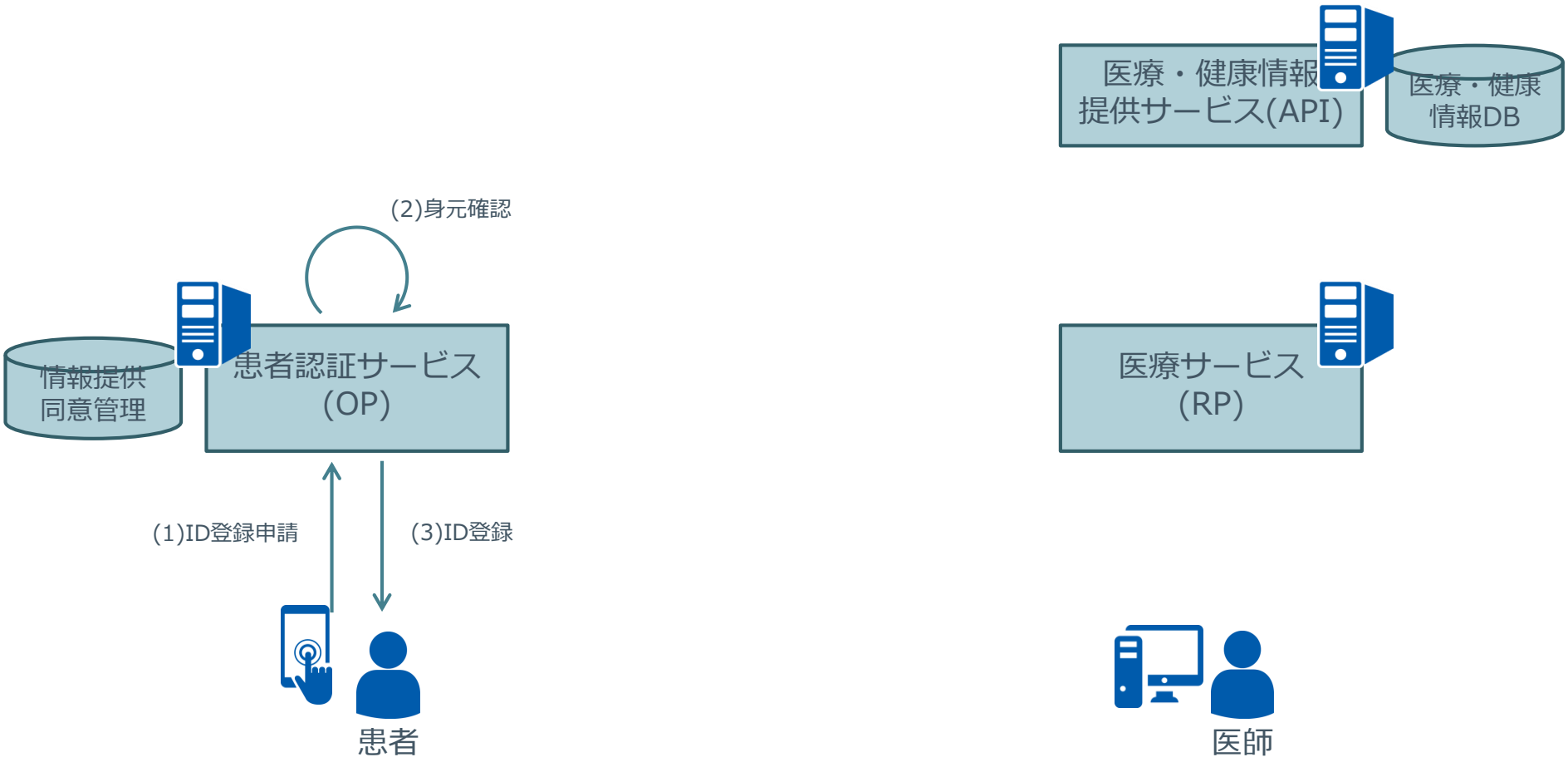
- 医療サービス(RP)からの認可リクエストを受けて、患者認証サービス(OP)はOpenID Connect CIBAの仕様に基づき患者のデバイスにプッシュ通知で認証要求を送る。
- 患者は認証実施後に医療・健康情報提供への同意を行い、その後医療サービスにアクセストークンが発行される。
- 医療サービスはそのアクセストークンを使って医療・健康情報提供サービスに医療・健康情報をリクエストする。



© NRI SecureTechnologies, Ltd.

基本シナリオの１点目の事前処理として、患者認証サービスへの患者IDの新規登録が必要となる。

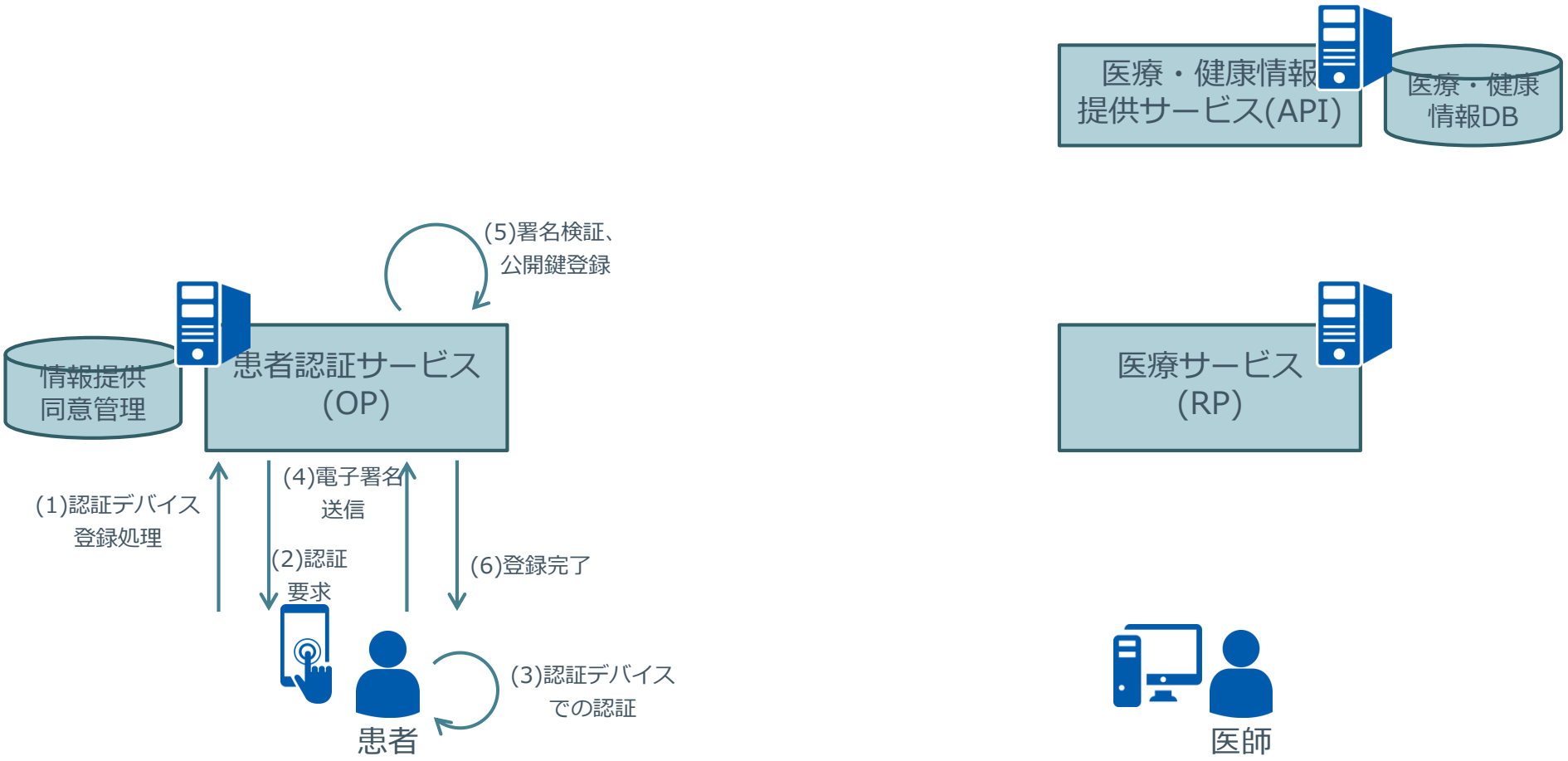
- 基本シナリオを実現する事前処理として、患者は、認証サービスへのID登録が必要となる。
- データとして要配慮個人情報に相当する情報が扱われる可能性があると想定し、ID登録においては身元確認が行われることを想定している。
- ID登録後、患者は患者認証サービスからのプッシュ通知を受信するため、認証デバイスにネイティブアプリケーションをインストールする。



© NRI SecureTechnologies, Ltd.

２点目の事前処理として、患者認証サービスへの患者認証デバイスの新規登録が必要となる。

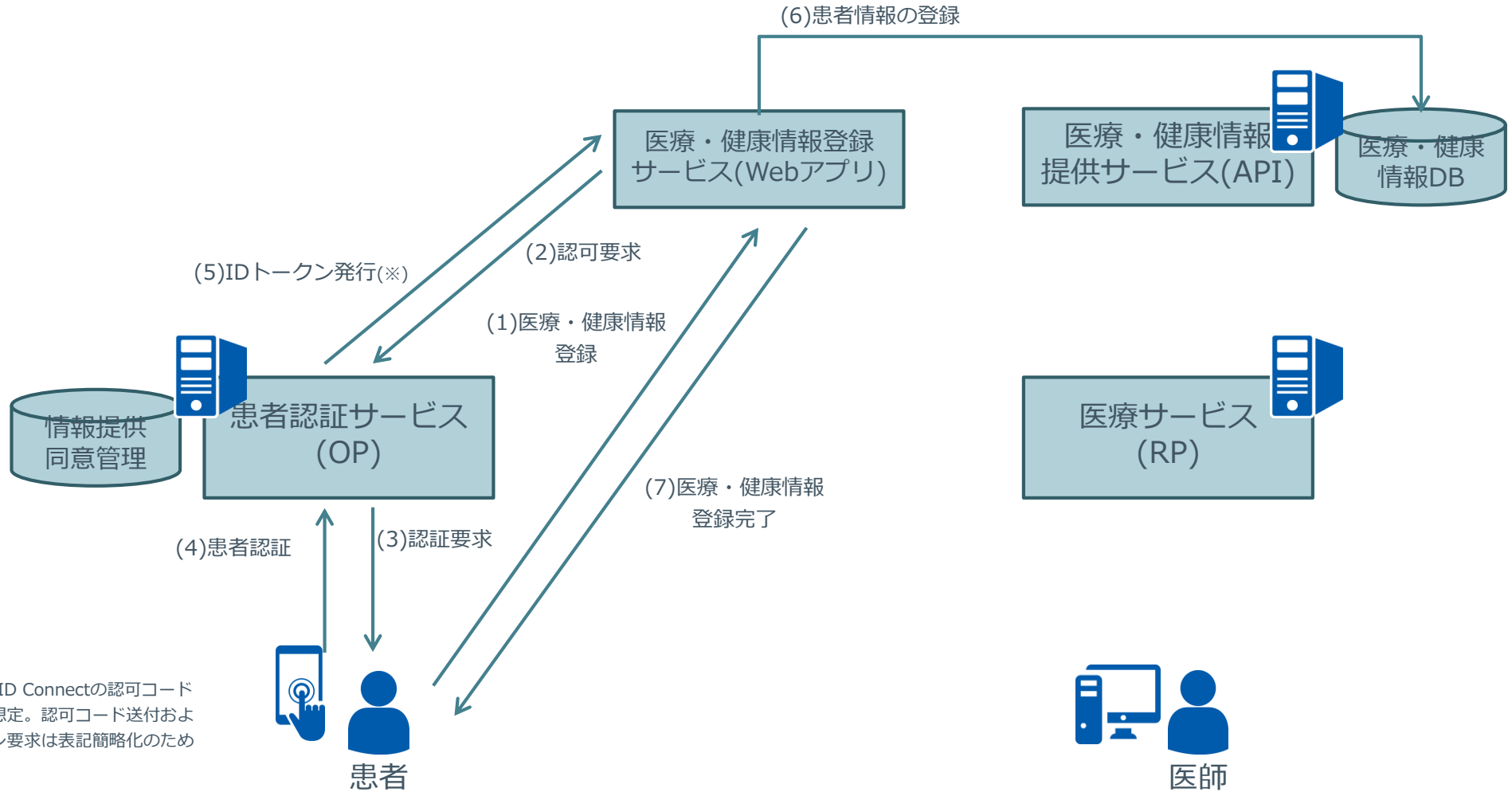
- FIDO認証による患者認証を行うためには、認証サービスへの認証デバイスの登録が必要となる。



© NRI SecureTechnologies, Ltd.

３点目の事前処理として、医療・健康情報管理サービスへの患者の医療・健康情報登録が必要となる。

- 医療・健康情報提供サービスにおいてRPからの患者の医療・健康情報提供リクエスト時の患者識別を行うため、医療・健康情報提供サービスでの利用登録が必要となる。

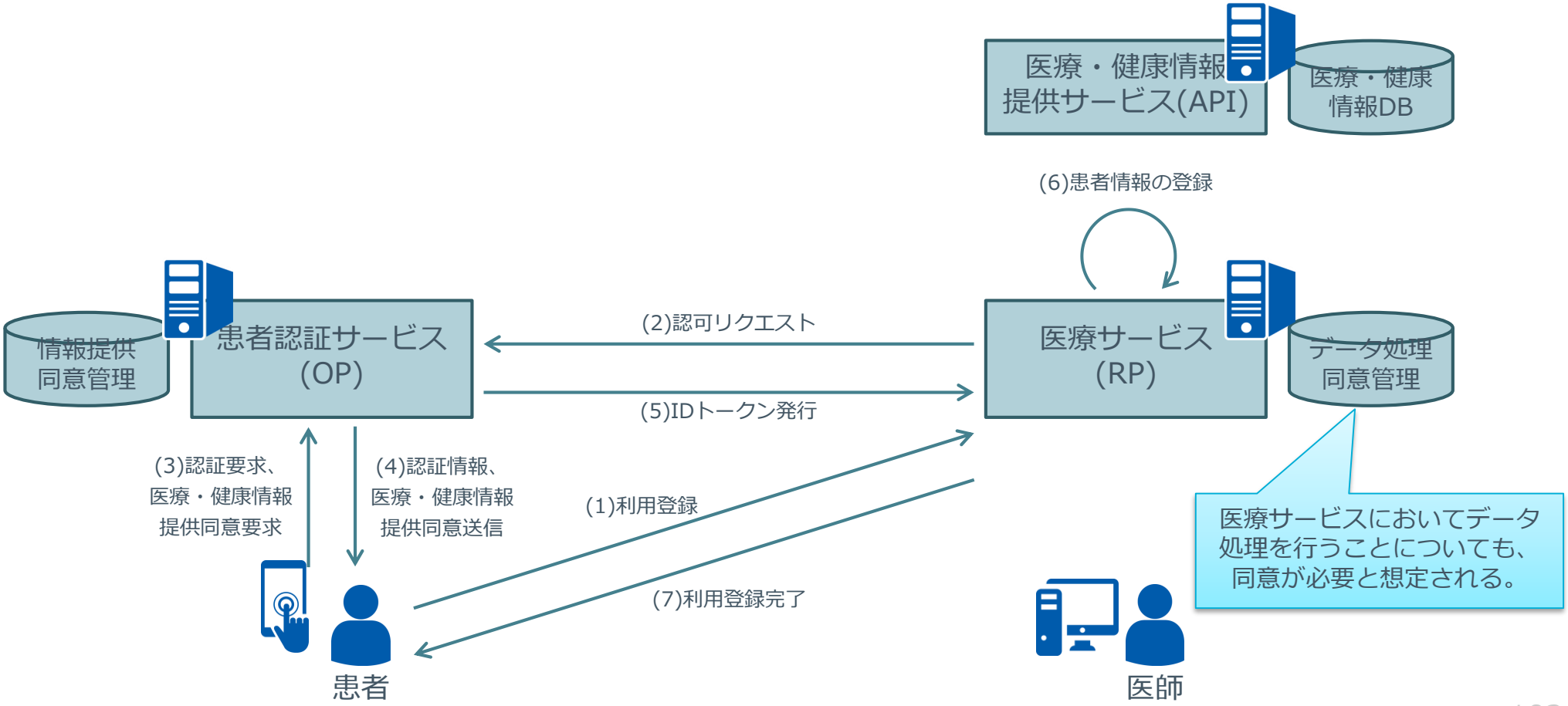


(※)OpenID Connectの認可コードフローを想定。認可コード送付およびトークン要求は表記簡略化のため記載省略。

© NRI SecureTechnologies, Ltd.

４点目の事前処理として、医療サービスへの患者識別情報の通知が必要となる。

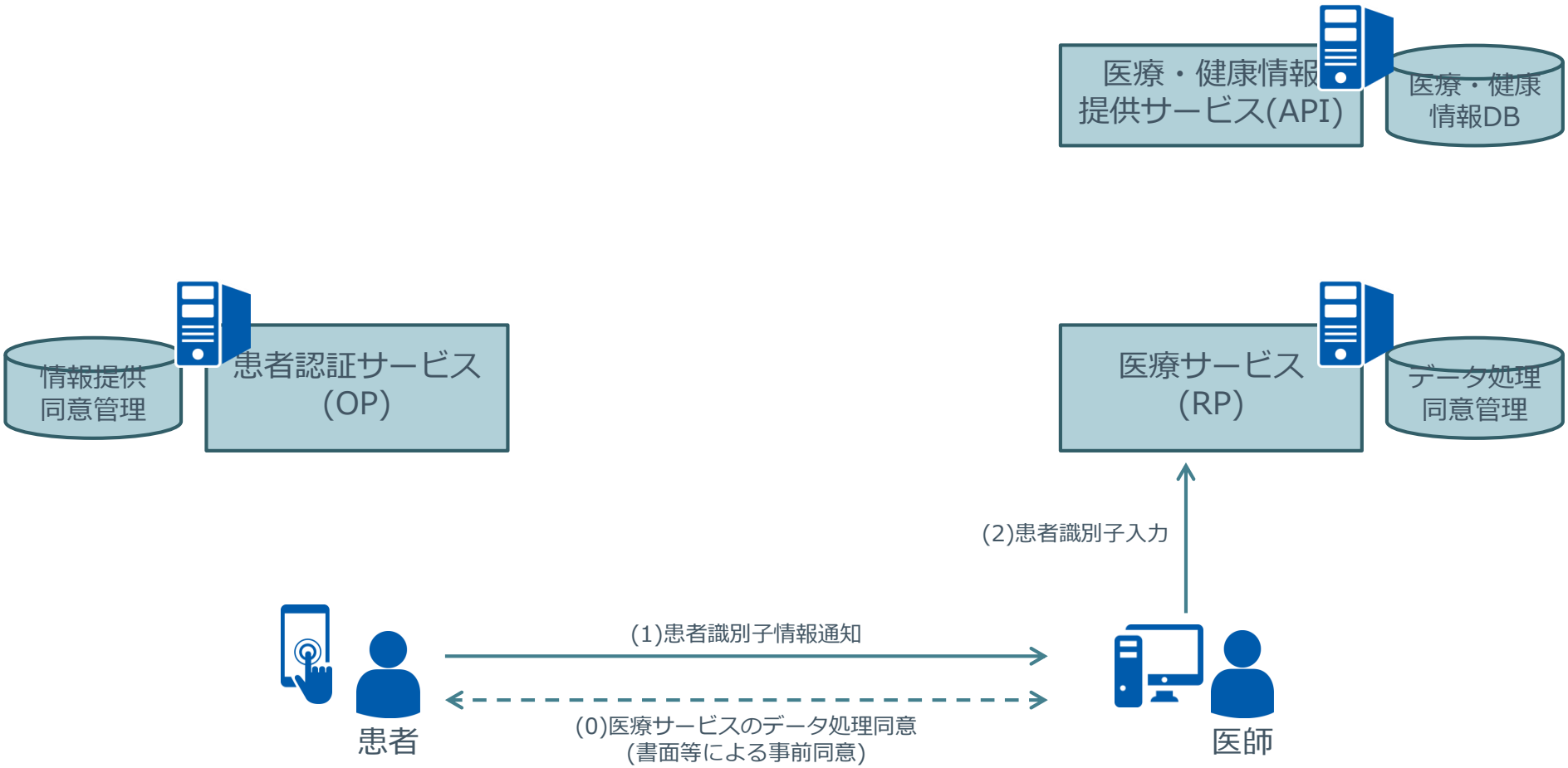
- OpenID Connect CIBA仕様に基づく認可リクエストおよび患者の情報提供同意を求める際の患者識別子の送付形式は、3通りのパターンが存在する。(id_token_hint, login_hint_token, login_hint)
- 下記は、患者識別子の送付形式として患者認証サービスが払い出すIDトークンを利用する場合の処理を示す。この場合は、医療サービスでの患者の利用登録、認証要求が必要となると想定される。
  - このケースでは、医療サービス利用登録時に医療サービス(RP)における患者情報のデータ処理同意も電子的に取得が可能となる。



© NRI SecureTechnologies, Ltd.

４点目の事前処理については、医療サービスへの患者識別情報の通知をもって処理する方式も考えられる。

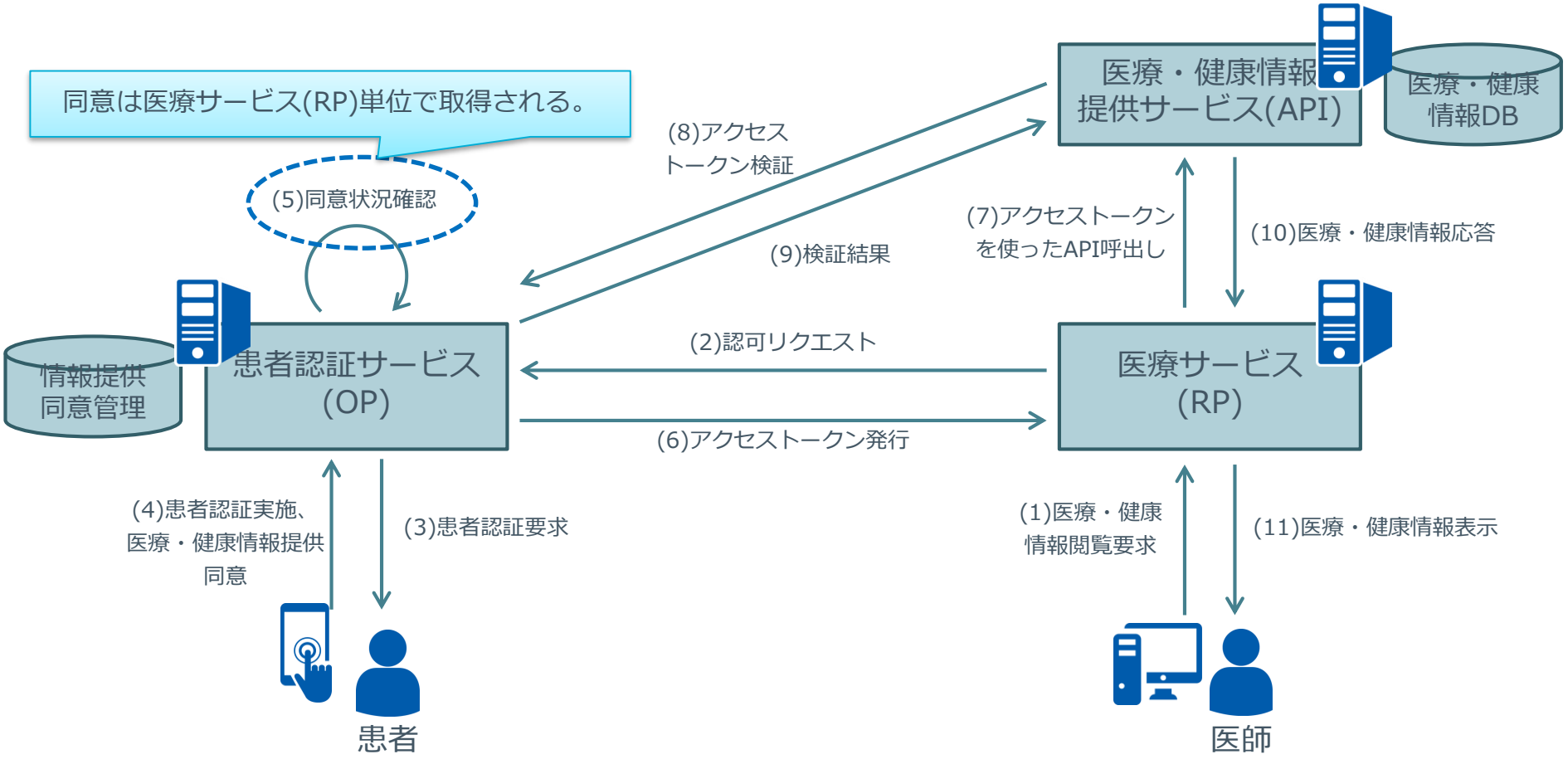
- 患者認証サービスが患者を一意に識別可能な識別子情報(保険者番号、患者認証サービスログイン用ID等)を医師に通知、または医療サービスに入力する方式も考えられる。
  - このケースでは、医療サービスでのデータ処理については事前での書面等による同意取得が前提となると想定される。



© NRI SecureTechnologies, Ltd.

患者への情報提供同意は、医療サービス単位で取得することが必要と想定される。

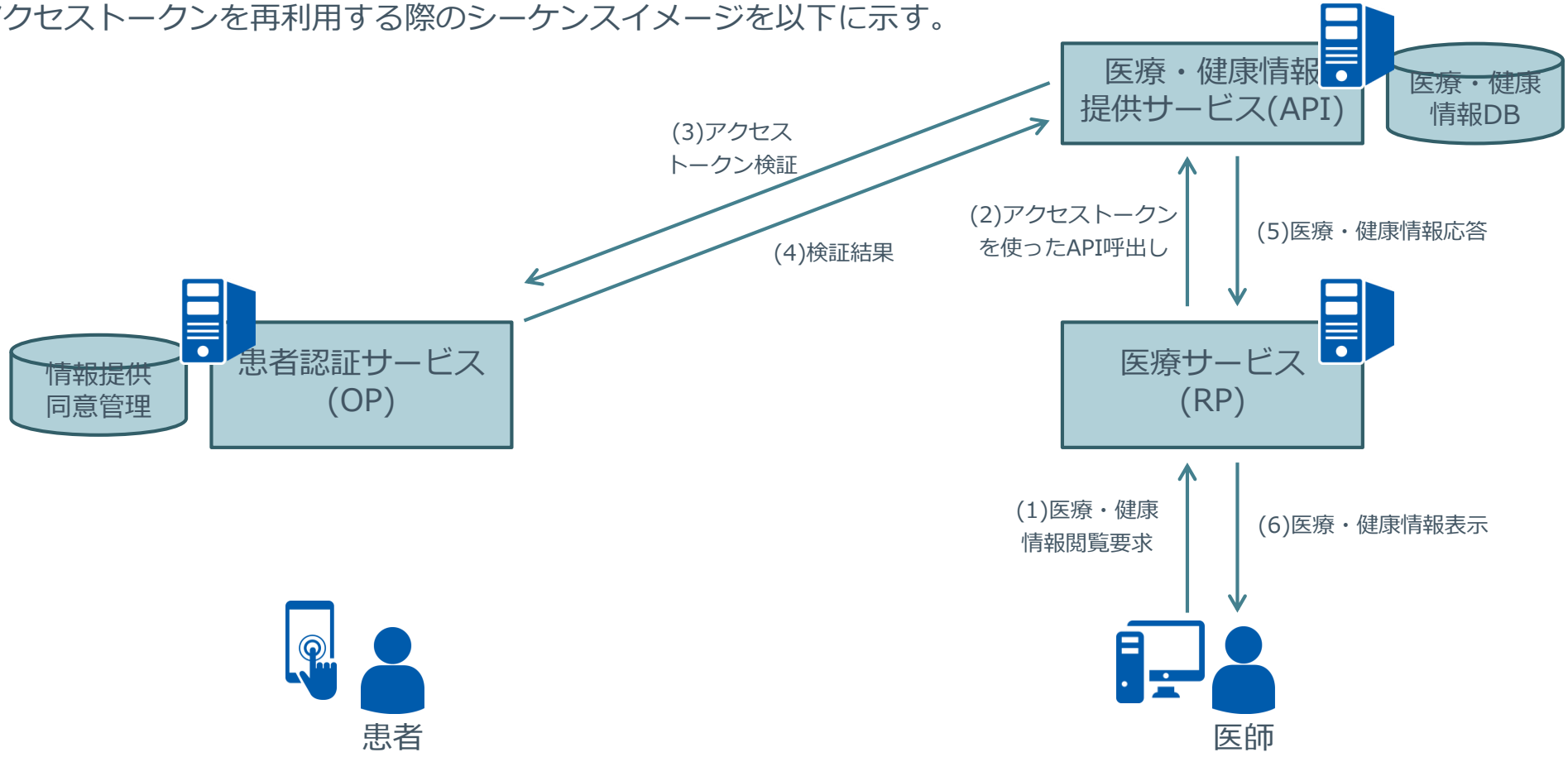
- 情報提供の同意は、医療サービス(RP)単位で取得することが望ましいと想定される。同じ医師と患者であった場合においても、利用する医療サービスが異なる場合は改めて同意取得が必要となる。
- 本実証検討では医療・健康情報という機微な個人情報を扱う性質上、患者からの医療・健康情報提供同意の取得が医療・健康情報へのアクセスの都度必要とするケースも想定し、都度同意取得を行う。



© NRI SecureTechnologies, Ltd.

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。

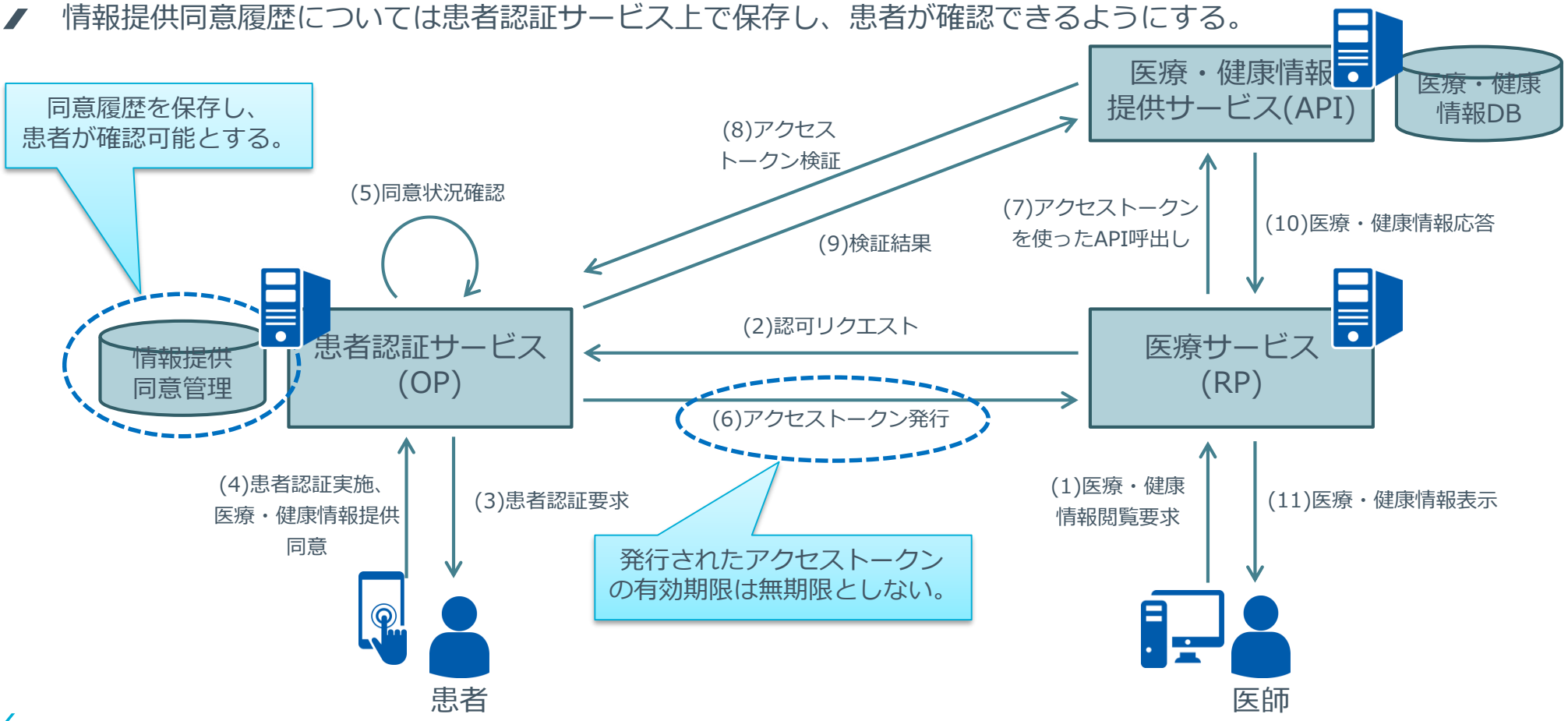
- 患者認証・同意処理を都度求めることは患者の負担となり得るものと想定し、基本シナリオの派生シナリオの1つとして、患者認証および情報提供同意を再利用し、画面等での都度の同意取得を求めずに医療・健康情報取得を行うことについて、技術的な方法を検討した。対応の考え方として、大きく以下の2通りの方法が考えられる。
  - 取得したアクセストークンを再利用する。
  - 改めて医療サービスから認可リクエストを行い、アクセストークンを取得する。
- アクセストークンを再利用する際のシーケンスイメージを以下に示す。



© NRI SecureTechnologies, Ltd.

アクセストークンを再利用する場合は、セキュリティリスクを考慮してアクセストークンの有効期限を適切にして運用することが望ましい。

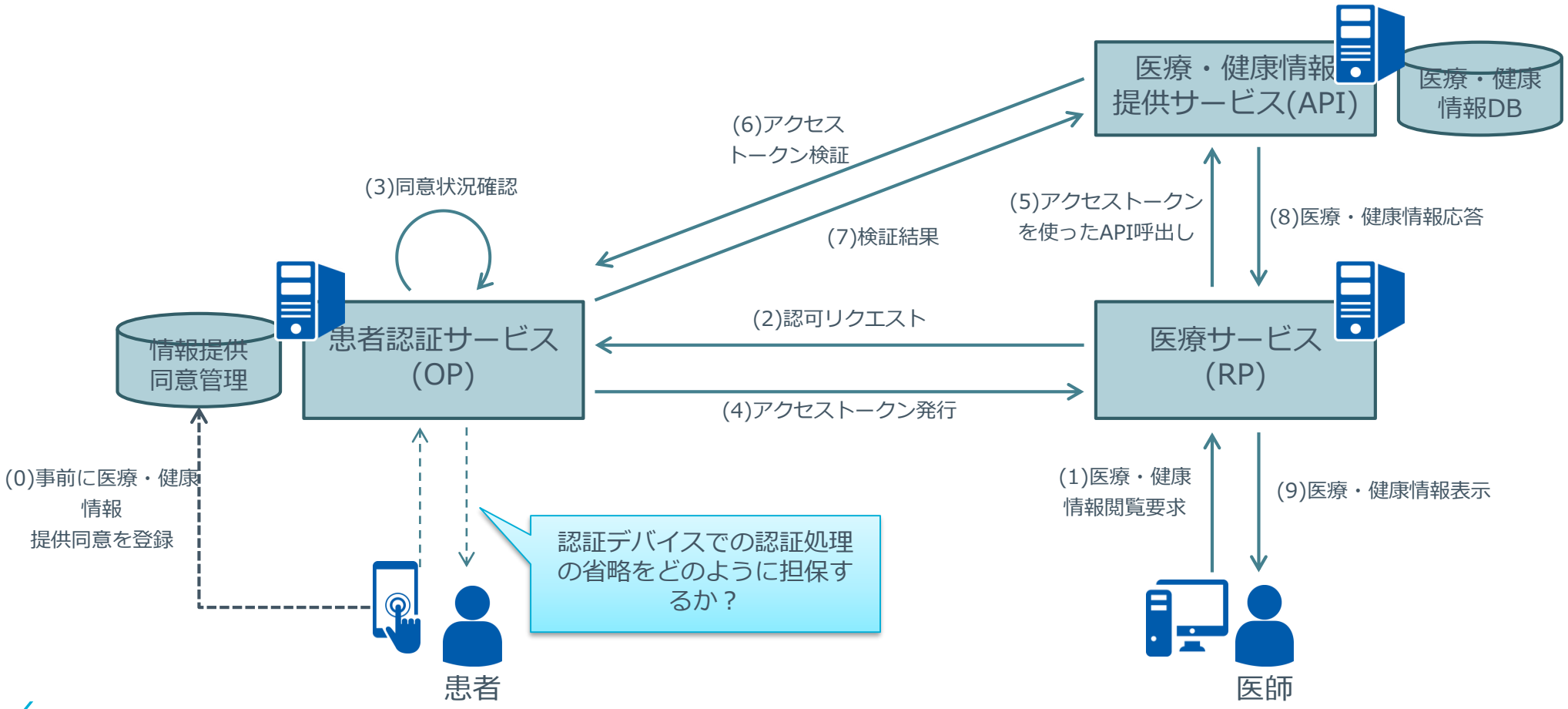
- アクセストークンについては、万一の漏えい等のセキュリティリスクをゼロにすることはできないこと、患者の医療・健康情報提供同意が破棄される可能性があることから、アクセストークンの有効期限を無期限とする運用は推奨されない。
  - 一定期間トークンを再利用する場合は、リフレッシュトークンを用いたアクセストークンの更新運用を行うことが望ましい。
  - OpenID Connect のリフレッシュトークンを利用することで、患者の認証および同意を都度行うことなく有効なアクセストークンを取得することが可能。
- 情報提供同意履歴については患者認証サービス上で保存し、患者が確認できるようにする。



© NRI SecureTechnologies, Ltd.

医療サービスから再度認可リクエストを行いアクセストークンを取得する場合では、患者認証をどのように担保するか、考慮が必要となる。

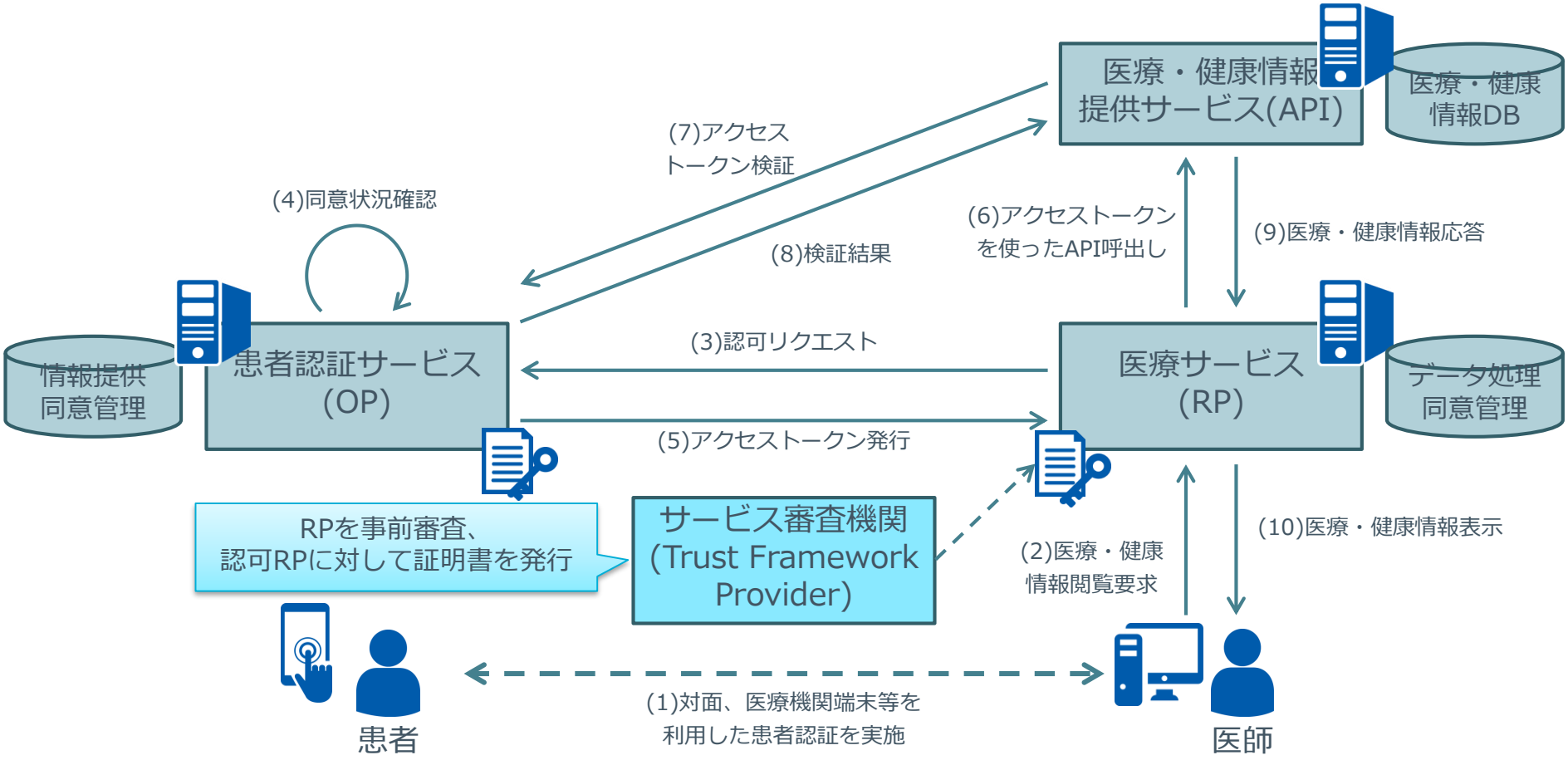
- OpenID Connect CIBAの仕様においては、認可リクエストを受信したOpenID Providerは、認証する者の認証デバイスに対して通知し、認証を行うこととされている。
- そのため、本ケースでは、患者認証サービス(OP)が管理する情報提供に事前に同意している場合においても、患者の認証を何らかの形で担保する必要があると考えられる。



© NRI SecureTechnologies, Ltd.

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。

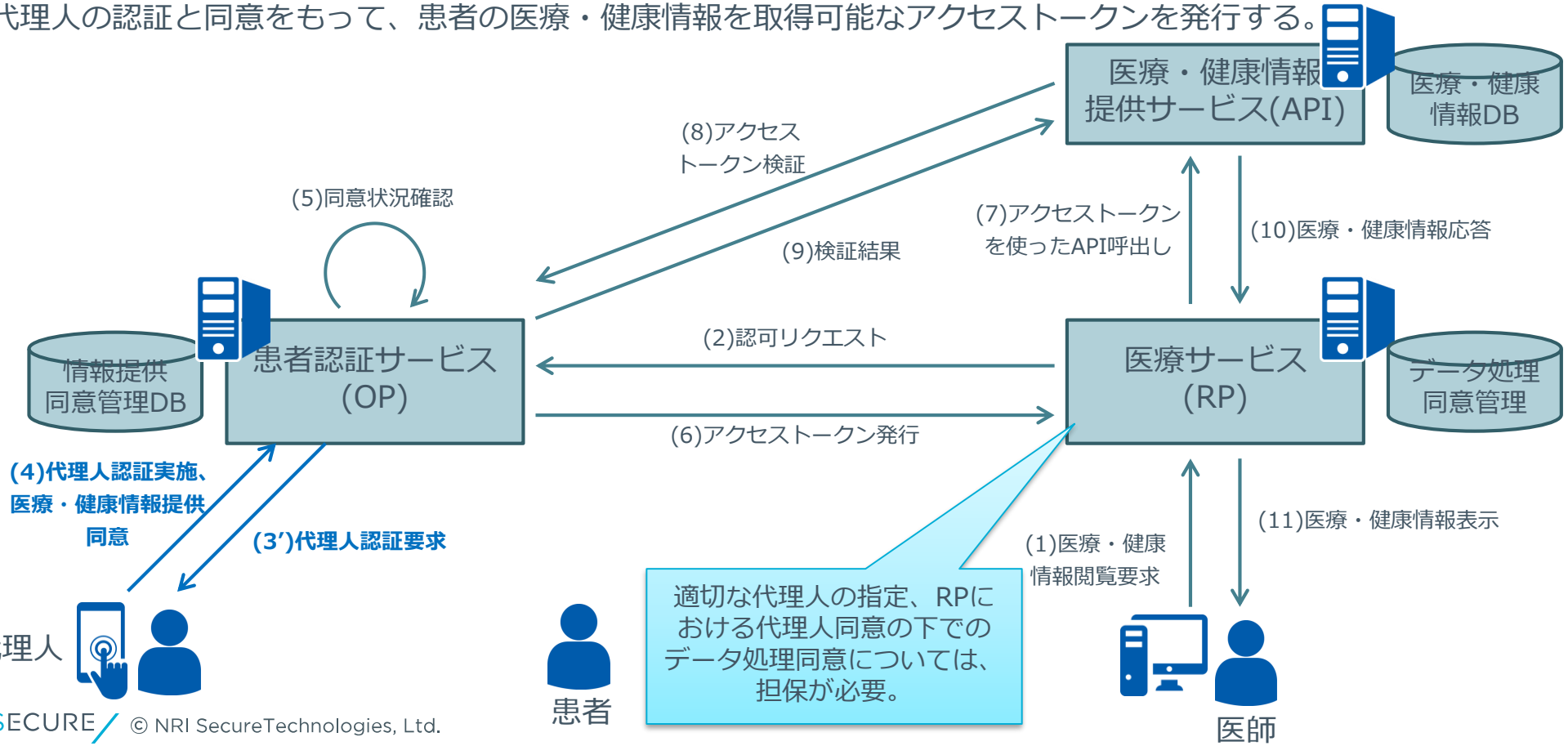
- 医療サービスが信頼できることを確認可能な、第三者となるサービス審査機関を設ける。
  - 医療サービスと患者認証サービスを含むトラストフレームワークを構成する形となる。
- サービス審査機関は、RPの事前審査を行い、認可したRPに対して証明書を発行する。
- 対面、医療機関端末等を利用した患者認証を実施した前提のもとに、患者認証サービスは、医療サービスの認可リクエストを受けつけ、患者の認証処理を省略してアクセストークンを発行、返却する。



© NRI SecureTechnologies, Ltd.

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。

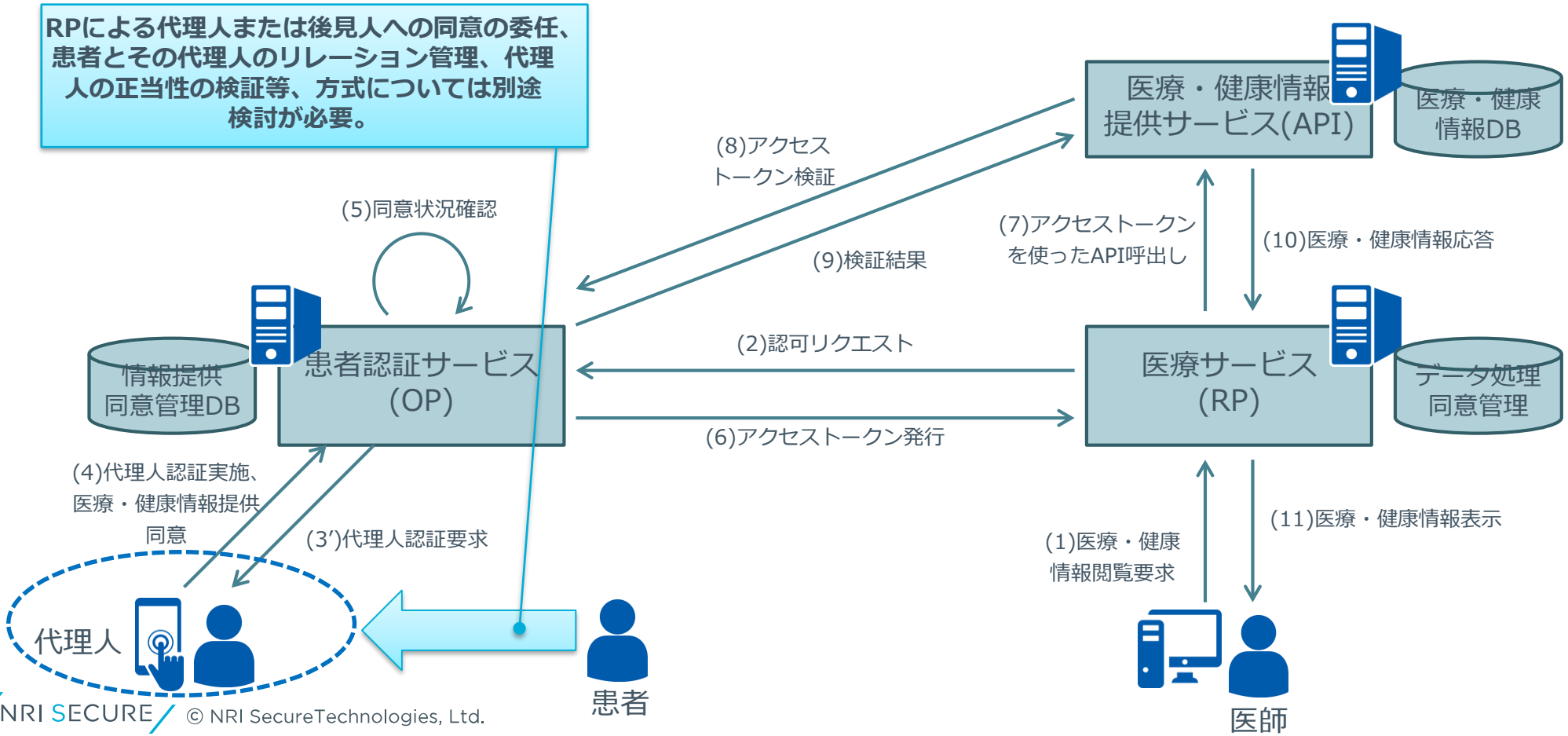
- 医療福祉分野においては、患者自身による情報提供同意の意思表示が困難な場合に、後見人もしくは代理人が情報提供同意を行うケースが想定される。2件目の派生シナリオとして、代理人により患者の医療・健康情報へのアクセスを許可する方法について検討する。
- このケースでは、OpenID Connect CIBAの仕様に基づき、医療サービス(RP)からの認可リクエストを受けて、代理人の認証デバイスにプッシュ通知で認証要求を送信する方法が考えられる。
  - 医療サービス(RP)において代理人が適切であることの確認および代理人によるデータ処理の同意が適切であることを担保する必要がある。
- 代理人の認証と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



© NRI SecureTechnologies, Ltd.

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。

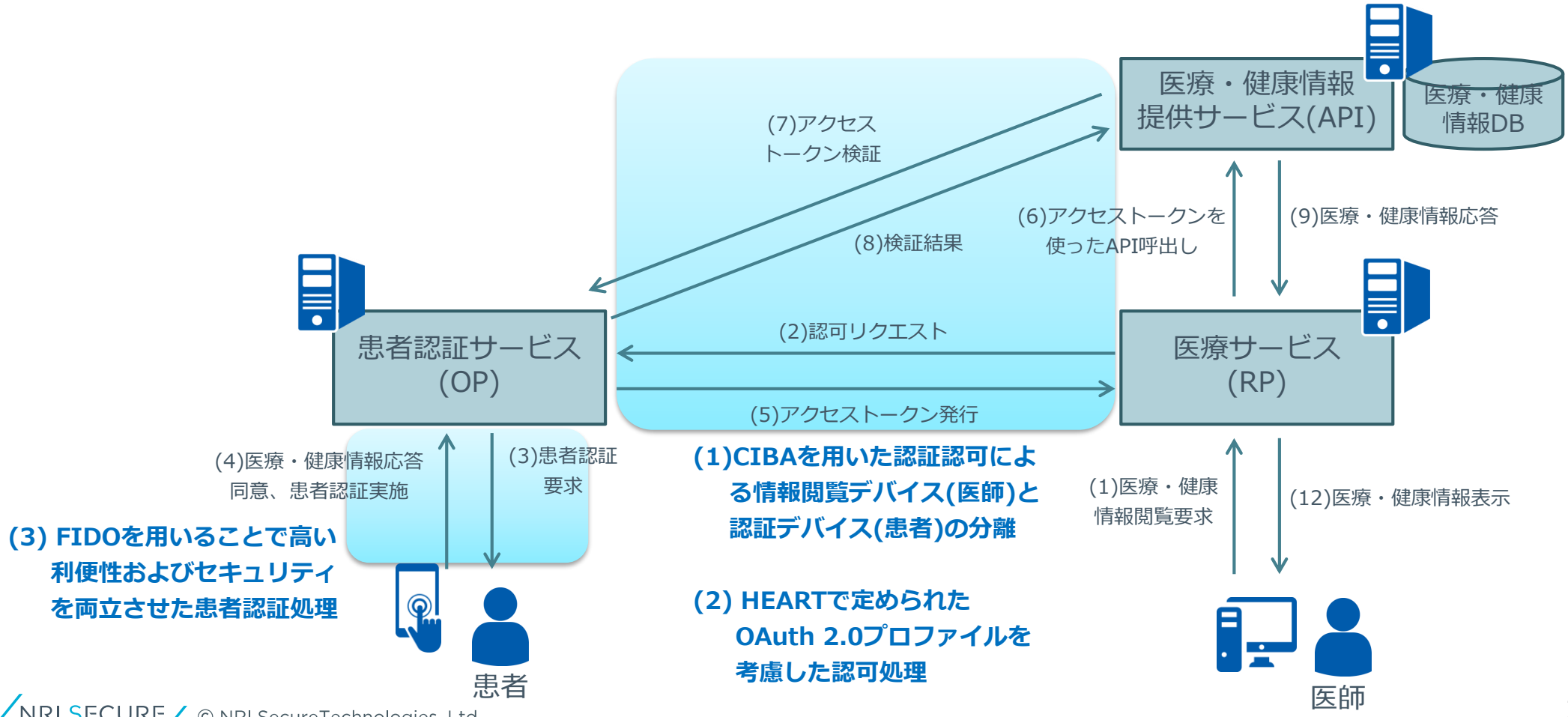
- 前述の方式は、適切な代理人がRPによりリレーション管理のもとに識別され、検証されていることが前提となる。
- 代理人または後見人への同意の委任に関しては、様々な業務ユースケースおよび関連法制度があり、それぞれのケースに応じた技術的な処理方式については別途検討が必要である。



© NRI SecureTechnologies, Ltd.

機能実証では、前述の基本シナリオについて、「OpenID FoundationとFIDO Alliance の基本的情報の整理」の調査結果を踏まえ構成要素を検討した。

- 前に示した基本シナリオについて「OpenID FoundationとFIDO Allianceの基本的情報の整理」において調査したOpenID Connect CIBA および FIDOの仕様に基づき、処理シーケンス・適用パラメータを整理した。
- 整理した結果に基づき、シナリオを検証可能な実証環境を構築した。



© NRI SecureTechnologies, Ltd.

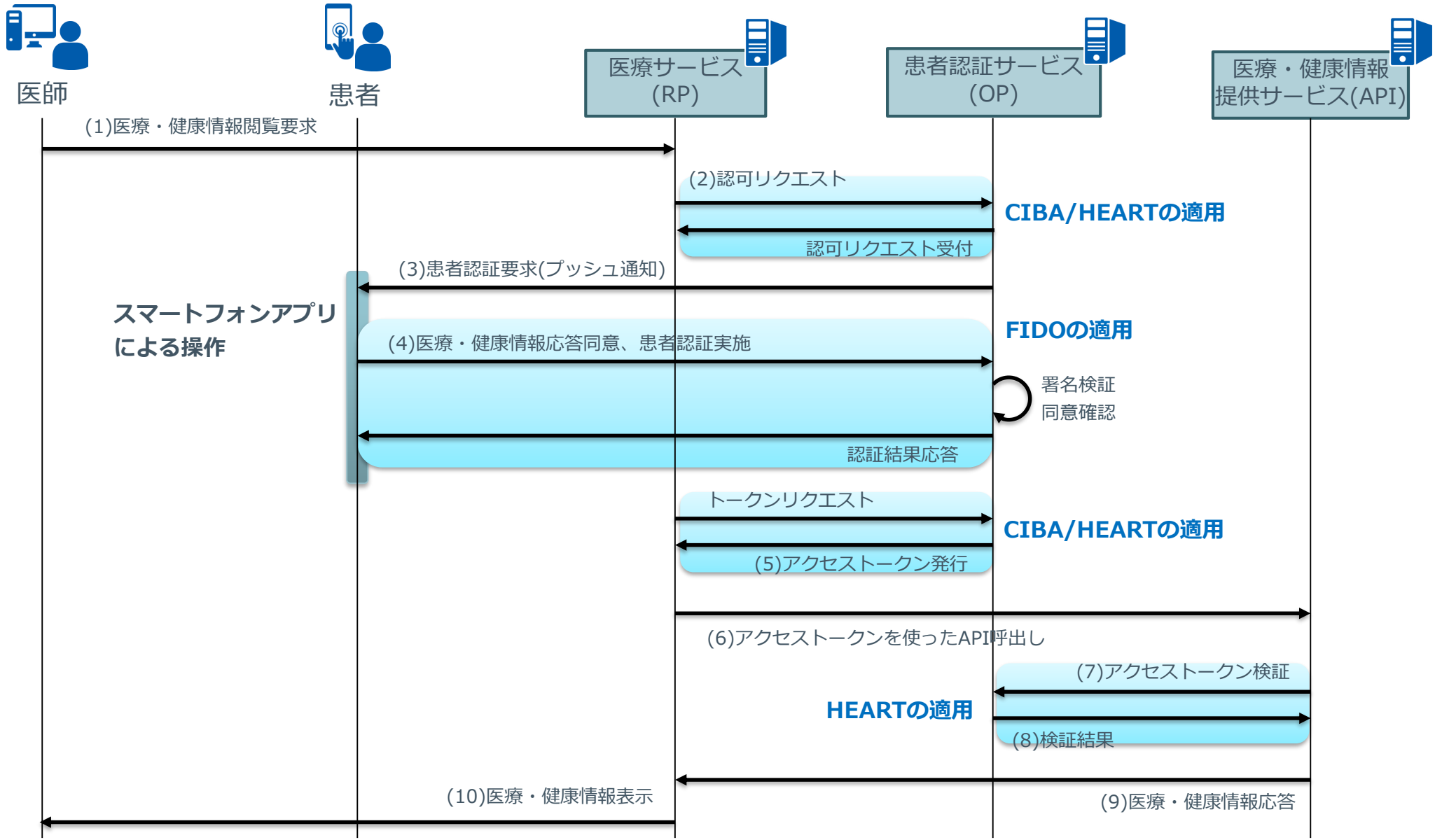
実機実証の構成の前提事項は以下の通り。

実機実証の構成の前提事項を以下に示す。

- 整理した構成、シーケンス、適用パラメータに基づき、前頁の実証シナリオを検証可能な実証環境を実装する。
  - 2件の派生シナリオについては、机上の構成検討までとし、実証実装の対象外とした。
  - 医療サービスにおける医師の認証は、何らかの方法で認証完了している前提とし、実証の対象外とした。
- 本調査研究では、処理性能に関する実機検証、基盤運用など運用に関する実機検証は想定しない。
- OpenID Connect および FIDO の仕様に定められている各機能をスクラッチ開発する場合、実装期間、実装コストが大きくなると考えられる。そのため、本実機実証ではOpenID Providerは、OpenID Foundation および FIDO Allianceの認証を取得しているパッケージを利用することとする。
- Relying Party および医療・健康情報提供APIについては、簡易なモックアップアプリケーションの実装を想定する。
- 基盤は実装期間短縮のため、クラウド環境利用とする。
- 実証環境はセキュリティに配慮し、弊社および貴省担当者が許可する環境からのみアクセス可能とする。
  また、実証用データは仮想のテストデータを利用し、実在の個人情報は利用しない。

© NRI SecureTechnologies, Ltd.

前項で示した構成における認証認可の処理シーケンスは以下の通りとなる。



© NRI SecureTechnologies, Ltd.

「(2)認可リクエスト」のパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

- 患者の医療・健康情報に対する認可リクエストは、情報閲覧デバイス（医師）と認証デバイス（患者）が異なるため、CIBAの仕様に沿った認可リクエストを行う。
- 現行のHEART OAuth 2.0 ProfileにおいてはCIBA仕様までは考慮されていないため、パラメータの検討においては主にCIBAのSecurity Considerationを参考とした。
- 上記を踏まえて検討した結果のパラメータを次ページに記載する。

© NRI SecureTechnologies, Ltd.

「(2)認可リクエスト」のパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

No.	エンドポイント名	説明
(2)	バックチャネル認証エンドポイント	CIBAによる認証リクエストを受け付けるエンドポイント

パラメータ	必須	設定値／方針	説明／設定根拠
scope	必須	“openid”および認可要求対象操作に応じたスコープの値を指定する。	スコープについてはHEART FHIR OAuth 2.0 Scopesの記載も踏まえて設計する。
acr_values	任意	FIDO認証を指定するパラメータとして、”urn:cibatest:auth:fido”を指定する。	RP側が認証レベルを指定したい場合に使用されるパラメータ。本実証では医療・健康情報という機微情報を扱うため、認証強度の高い認証を行うことができるFIDO認証を必須とする。
client_notification_token	特定条件下で必須	本パラメータは使用しない。	本パラメータはPing, PushモードにおいてRPにコールバックする際のクライアント認証で使用するベアラートークンの値であるが、今回はPollモードで実施する想定のため使用しない。
login_hint_token id_token_hint login_hint	何れか必須	id_token_hintとして、患者が医療サービス利用時に患者認証サービスから取得したIDトークンを指定する。	login_hintはユーザを一意に識別するためのメールアドレスやユーザ名を指定する。そのために個人情報を扱うケースも想定されるため、本パラメータを利用する場合は、セキュリティ観点での設計検討が必要。
binding_message	任意	仕様上は必須ではないが、本検証においては指定する。また、比較的短く、限られた文字セットから成る文字列を指定することとする。	攻撃者からの意図しない認証リクエストを患者が誤って認証しないように本パラメータを指定する。 値の指定の際はデバイスの制約上長い文字列や特定の文字セットを表示できない可能性を考慮する。
user_code	任意	本パラメータは使用しない。	主にlogin_hintを指定する場合に、認証リクエストが一方的に送信されることを防ぐために使用されるが、今回はlogin_hintを使用しない想定のため使用しない。

© NRI SecureTechnologies, Ltd.

「(2)認可リクエスト」のパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

No.	エンドポイント名	説明
(2)	バックチャネル認証エンドポイント	CIBAによる認証リクエストを受け付けるエンドポイント

パラメータ	必須	設定値／方針	説明／設定根拠
requested_expiry	任意	本パラメータは使用しない。	認可リクエストの有効期限を設定。今回の実証では患者認証サービスが持つ有効期限のデフォルト値を使用する。
client_id	必須	医療サービスのクライアントIDを指定	患者認証サービスが払い出す値を設定する。
client_secret	必須	医療サービスのクライアントシークレットを指定	患者認証サービスが払い出す値を設定する。

© NRI SecureTechnologies, Ltd.

acr_values パラメータについては、具体的な値をサービスごとに検討し、定義する必要がある。

- acr_values の定義
  - 要求された認証コンテキストクラス参照(acr：Authentication Context Class Reference) の値。
  - 実行された認証によって満たされた認証コンテキストクラスは、IDトークンのacrクレーム値として返される。

- acr の定義 (OpenID Connect Core 1.0 において記載)
  - 実施された認証処理が満たす Authentication Context Class を表す Authentication Context Class Reference 値を示す文字列。
  - この値の意味するところはコンテキストによって異なる可能性があるため、この Claim を利用する場合は, 関係者間で値の意味するところについて合意しておく必要がある。acr は大文字小文字を区別する文字列である。
  - 英 Open Banking における acr 定義の例 (Open Banking Security Profile - Implementer's Draft v1.1.0 において記載)
    - urn:openbanking:psd2:sca　：PSD2 RTSで義務付けられているとおりに認証を行う必要があることを示す。
    - urn:openbanking:psd2:ca　：SCAを使用せずに認証を要求する（許可されている場合）ことを示す。

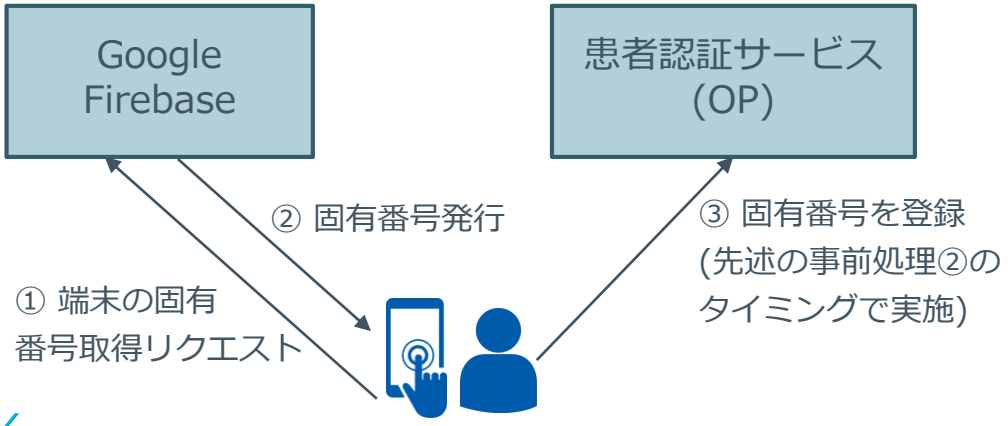
- 本格的に認証サービスを構築する際の acr_values の値の定義および運用については、構築する認証サービスと提供機能の目的、業務要件に基づき検討が必要となる。

© NRI SecureTechnologies, Ltd.

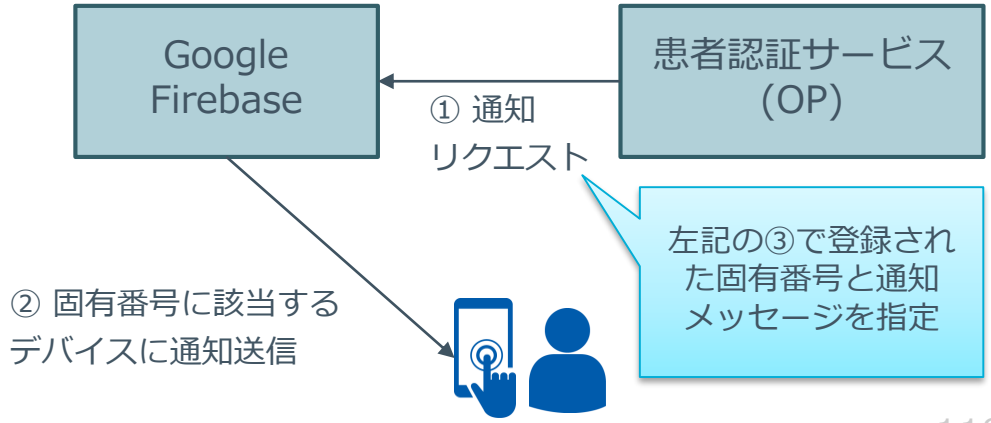
「(3)患者認証要求」における患者の持つデバイスへの通知については、普及している既存のモバイルバックエンドサービスを活用して実現した。

- mBaaS (mobile Backend as a Service)
  - スマートフォンなどを対象としたモバイルアプリケーションにてよく利用される汎用的な機能をクラウドから提供するサービスとしてmBaaS(mobile Backend as a Service)が存在する。
- 患者のデバイスへのプッシュ通知の仕組み
  - サービス利用前の事前準備として、**患者の認証デバイス(スマートフォン)にあらかじめ患者認証サービスからの通知の受信とその後のユーザ認証を行うためのスマートフォンアプリケーションをダウンロードの上インストールする。**
  - 実証では、mBaaSの一つであるGoogle Firebase が提供するプッシュ通知サービスを活用することで、患者認証サービスから患者の端末内のアプリケーションに向けて同意依頼の通知を送信することとした。具体的な通知の流れは以下の通り。
    - 通知先デバイスの紐付けは、アプリケーションインストール後の初期設定の中でGoogle Firebaseから端末に向けて発行する固有番号を患者認証サービスのユーザ情報と紐づけることで実現している（端末変更時は旧端末の固有番号紐付け解除＆新端末での紐付けを別途実施）。このように**ユーザに紐づくプッシュ通知先の担保についてはプッシュ通知の実現方式に合わせて検討が必要**である。

アプリケーションインストール後の初期設定時



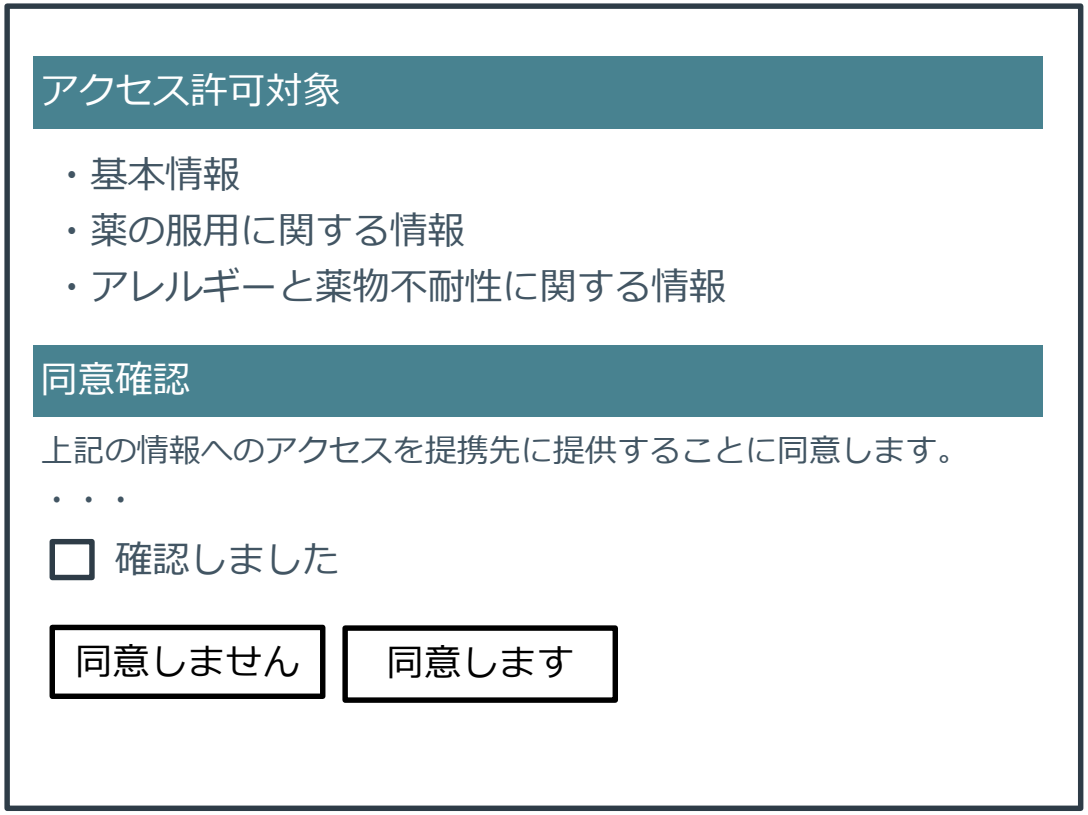
医療サービスからの患者認証要求時



© NRI SecureTechnologies, Ltd.

「(4)医療・健康情報応答同意、患者認証実施」における情報提供同意の方式は、法制度や既存サービスの同意取得方法調査結果に基づき定めた。

- 医療・健康情報提供の同意確認については、患者の認証処理完了後に以下の情報を提供する画面を表示し、その画面でユーザが明示的に同意表示を行うことができるようにする。
  - 医療・健康情報の提供先サービス名
  - 提供する個人情報や医療・健康情報の内容
    - 情報の分類についてはFHIR OAuth 2.0 Scopesにおいて定義されているリソースタイプの分類を参考にした。
  - 同意撤回方法についての記載



© NRI SecureTechnologies, Ltd.

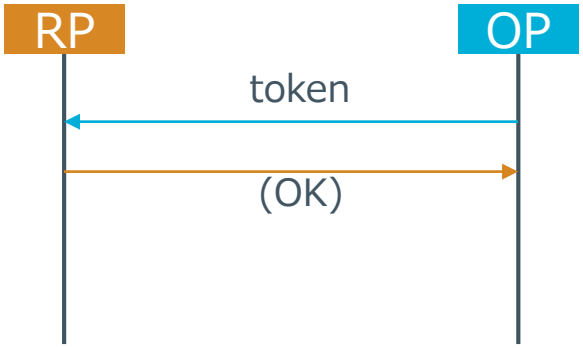
「(4)医療・健康情報応答同意、患者認証実施」におけるFIDO認証規格として、ネイティブアプリケーション向けのFIDO UAFを用いた。

- 利用するFIDO認証規格
  - 患者認証については、医療・健康情報という個人情報を扱うという高いセキュリティが求められる点と、子供からお年寄りまで幅広い層にとって利用しやすいという利便性が求められる点より、ユーザのデバイスがサポートする生体認証・デバイスロック解除機能を利用したFIDO認証を行う。
  - FIDO認証規格として、主にWebアプリケーション向けの二段階認証を可能とするFIDO U2F、FIDO2とスマートフォンアプリケーションなどのネイティブプリケーションを主眼としているFIDO UAFがある。
  - 本実証では、患者のデバイスへの通知の受信とその後のユーザ認証処理をスマートフォン向けアプリケーションから行うこととするため、FIDO UAFを用いることとした。
- FIDO認証における各種パラメータの検討
  - パラメータの検討においては、主にFIDO規格中のSecurity Considerations および Privacy Considerationsを参考に決定した。

© NRI SecureTechnologies, Ltd.

「(5)アクセストークン発行」におけるトークンリクエストのパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

- CIBAではトークン受信のモードとしてPoll, Ping, Pushの3つのモードをサポートしている。

モード	Poll	Ping	Push
概要	RPはトークンエンドポイントに対してポーリング(定期的にリクエスト)を行うAD(患者側の認証端末)上でユーザ同意が完了した後にリクエストを行うと、トークンが返却される	AD上でユーザの同意が完了すると、OPはRPに対して、完了通知を送る 通知を受け取ったRPはトークンリクエストを行う	AD上でユーザの同意が完了すると、OPはRPに対してトークンを返却する
イメージ			

- CIBAの仕様上およびHEARTの各仕様上では医療サービス向けの推奨モード等は明記されていない。そこで、医療サービスと同様に高いセキュリティを要求される金融サービス向けのCIBA設定(プロファイル)について定めた「Financial-grade API: Client Initiated Backchannel Authentication Profile」（以降、FAPI-CIBA）を参考とした。
- **FAPI-CIBA上では、モードについては以下の点が定義されているため、本検証ではPollモードを利用する。**
  - Pushモードをサポートしてはならない (shall not)
  - Pollモードをサポートすべきである (shall)
  - Pingモードをサポートしてもよい (may)

© NRI SecureTechnologies, Ltd.

「(5)アクセストークン発行」におけるトークンリクエストのパラメータとして、HEART OAuth 2.0 Profile の内容を考慮して定めた。

- 前ページの内容に加えて、HEART OAuth 2.0 Profile中の「2.2.2. Requests to the Token Endpoint」にて記載されているトークンエンドポイントへのアクセスにおける記載事項についても考慮した。

No.	エンドポイント名	説明
(5)	トークンエンドポイント	アクセストークン、IDトークン、リフレッシュトークンを取得する

パラメータ	必須	設定値／方針	説明／設定根拠
grant_type	必須	グラントタイプを指定。CIBAの場合は「urn:openid:params:grant-type:ciba」で固定	OpenID Connect CIBA プロファイルで指定の値を設定する。
auth_req_id	必須	「(2)認可リクエスト」のレスポンス中のauth_req_idの値	OpenID Connect CIBA プロファイルの仕様に基づき設定する。
client_id	必須	医療サービスのクライアントIDを指定	患者認証サービスが払い出す値を設定する。
client_secret	必須	医療サービスのクライアントシークレットを指定	患者認証サービスが払い出す値を設定する。

© NRI SecureTechnologies, Ltd.

「(7)アクセストークン検証」のパラメータとして、HEART OAuth 2.0 Profileの内容を考慮して定めた。

- HEART OAuth 2.0 Profile中の「3.2.2. Introspection」にて記載されているトークンイントロスペクションエンドポイントにおける記載事項について考慮した。

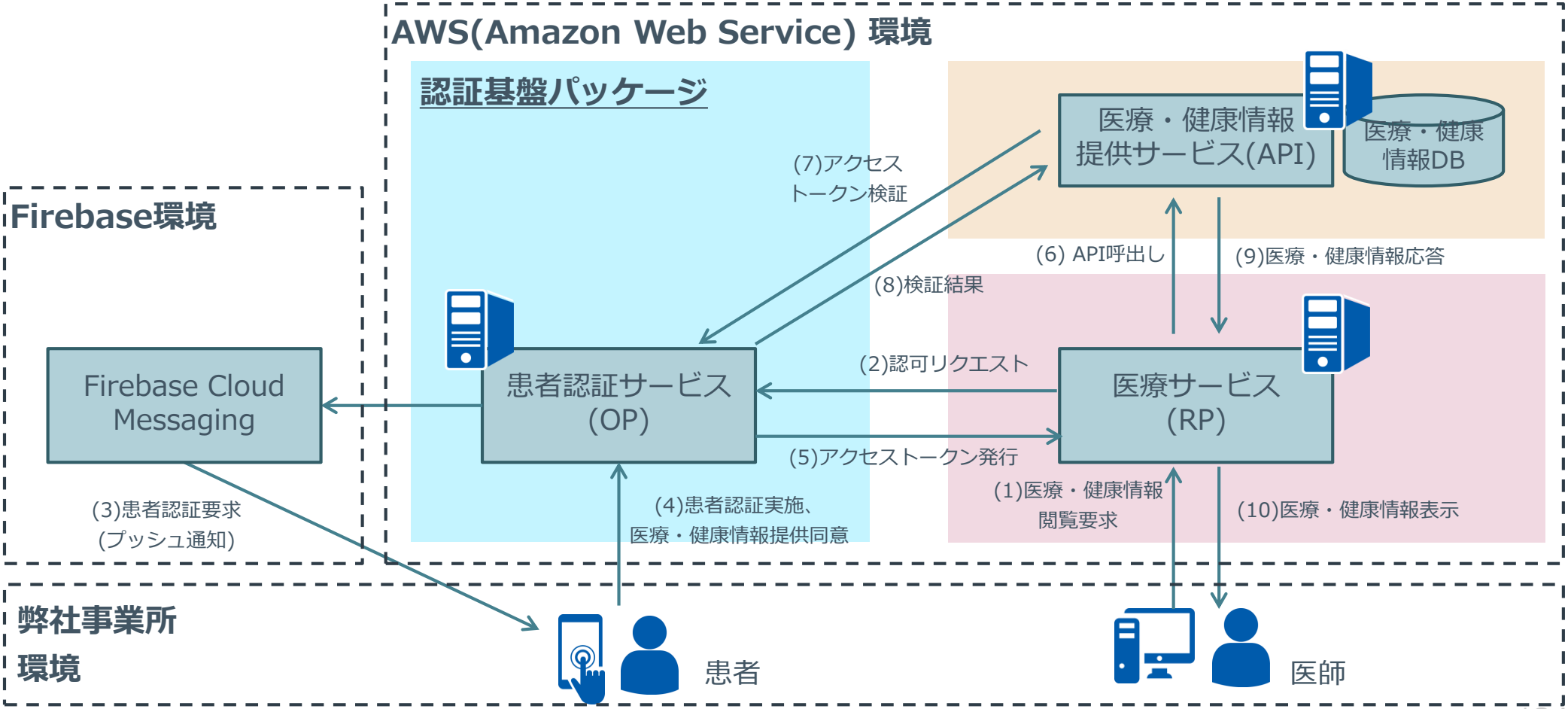
No.	エンドポイント名	説明
(7)	トークンイントロスペクションエンドポイント	アクセストークンの内容を検証する（有効状態、対応するスコープ等）

パラメータ	必須	設定値／方針	説明／設定根拠
token	必須	トークンを指定。	患者認証サービスが払い出す値を設定する。
token_type_hint	任意	本実証においては特に指定しない。	任意パラメータのため。
client_id	必須	医療・健康情報提供サービスのクライアントIDを指定	患者認証サービスが払い出す値を設定する。
client_secret	必須	医療・健康情報提供サービスのクライアントシークレットを指定	患者認証サービスが払い出す値を設定する。

© NRI SecureTechnologies, Ltd.

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。



© NRI SecureTechnologies, Ltd.

実証結果として、OpenID Connect CIBA/FIDOを活用することで患者個人の同意を経て医療従事者が患者の医療・健康情報を取得する仕組みを構築できることを確認した。

実証結果およびその考察を以下に示す。

- OpenID Connect CIBA活用による患者個人の同意による医療・健康情報提供の仕組みの実現
  - OpenID Connect CIBAの活用により、患者の医療・健康情報にアクセスする医師の端末と、医療・健康情報提供に同意する患者のデバイスを分離することができ、患者個人の同意を経て医療従事者が患者の医療・健康情報を取得する仕組みを機能的に実現可能であることが確認できた。

- FIDO活用によるユーザ認証の利便性・セキュリティ向上
  - FIDOの活用により、患者はユーザ認証の方法として、患者自身が利用するスマートフォン等のデバイスを用いたセキュアな認証方式を利用できることを確認した。医療・健康情報のような機微な情報を扱う際においても、FIDOの活用により高い利便性とセキュリティを確保できると考えられる。

- 患者認証サービス導入による医療サービス開発者および患者への負担軽減
  - 本実機実証では、患者の認証および医療・健康情報提供同意の確認を患者認証サービスに一元化する構成とした。これにより、医療サービス開発者視点からは、患者の認証と医療・健康情報の同意確認処理を個別に実装する負担が減り、患者視点からは、医療サービスごとにIDおよびパスワード等の認証情報を持つ必要がなくなり、情報管理の負担が軽減できると考えられる。

© NRI SecureTechnologies, Ltd.

今回の実証を通して、実証内容を実際に導入する際におけるユースケースに応じたパラメタ検討や、代理人による同意の正当性担保など今後の検討が必要な事項が確認された。

今後検討すべきと考えられる事項について以下に示す。

ユースケースに応じたOpenID Connect CIBAパラメータの検討

- 実機実証では、患者の認証連携および認可においてOpenID Connect CIBAを活用している。CIBA利用にあたっての各種パラメタの検討にあたっては、CIBA仕様ドキュメントに記載されているSecurity Considerationなどを参考にしている。
- 一方で、以下のパラメタについては利用されるユースケースや前提システム構成に基づくパラメタ検討が必要であり、今後認証基盤の設計・構築にあたっては実装者において検討が必要である。
  - 患者認証サービスへの認可リクエスト時に認証主体を指定するパラメタ
  - 患者認証サービスへの認可リクエスト時に必要とする認証レベルを指定するパラメタ

FIDO連携方式

- 今回の実機実証ではFIDO認証にFIDO UAFを利用したが、FIDO2を利用した実装も考えられる。例えば、GoogleはAndroid上で動作するネイティブアプリケーション向けに、FIDO2の機能を実行するためのAPIを提供している。この点についても、認証基盤の実装者において検討が必要である。

代理人・後見人による同意の正当性担保

- 医療福祉分野においては、患者の病状による要因や患者が乳幼児であるなどの様々な理由により、患者本人による認証や医療・健康情報提供の同意が困難なケースが想定される。
- そのような場合への対応ケースとして今回の実証では代理人による同意を設計したシステム構成に組み込む方式の検討を実施した。
- しかし、実際に代理人や後見人による同意を行う場合には、正当な代理人・後見人であることの確認・管理および同意の正当性の担保などについて、業務ユースケースと関連法制度を踏まえて技術的な方式の検討が必要である。

© NRI SecureTechnologies, Ltd.

6. 普及している認証基盤の活用に関する調査

© NRI SecureTechnologies, Ltd.

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。

調査対象システム

調査対象システム	業界	選定理由
マイナポータル	官公庁	日本国民に発行されるマイナンバーカードを使ってアクセスする、政府が運営するオンラインサービスであり、子育てや介護などの行政手続きができるなど、G to Cで影響度が大きいサービスであるため。
gBizID	官公庁	法人や個人事業主向けに発行されるIDで、様々な行政サービスを利用する際に使うことができるなど、G to Bで影響度が大きいサービスであるため。
LINE ID	IT	日本国内だけで8300万人以上の月間アクティブユーザ数が存在する国内有数のSNSであるため。
Value direct	金融	野村総合研究所が開発したインターネットバンキングシステムで、信用金庫や地方銀行など多数の採用実績があるため。
dアカウント	通信	国内最大手の通信事業であるNTTドコモが発行する共通IDであるため。

調査項目

- 調査システムの概要、利用システム普及の状況（登録ID数等）
- システム機能、運用
  - ID登録、身元確認（KYC有無等）の運用方式
  - 認証手段（ID/パスワード、2段階認証等）
  - ID管理に関する事項（情報更新、利用不能時のリカバリー方法、ID削除方法等）
  - セキュリティ向上のための機能（ログイン日時表示、ログインアラート等）
- 具備する機能と関連法制度・ガイドラインの関連について

© NRI SecureTechnologies, Ltd.

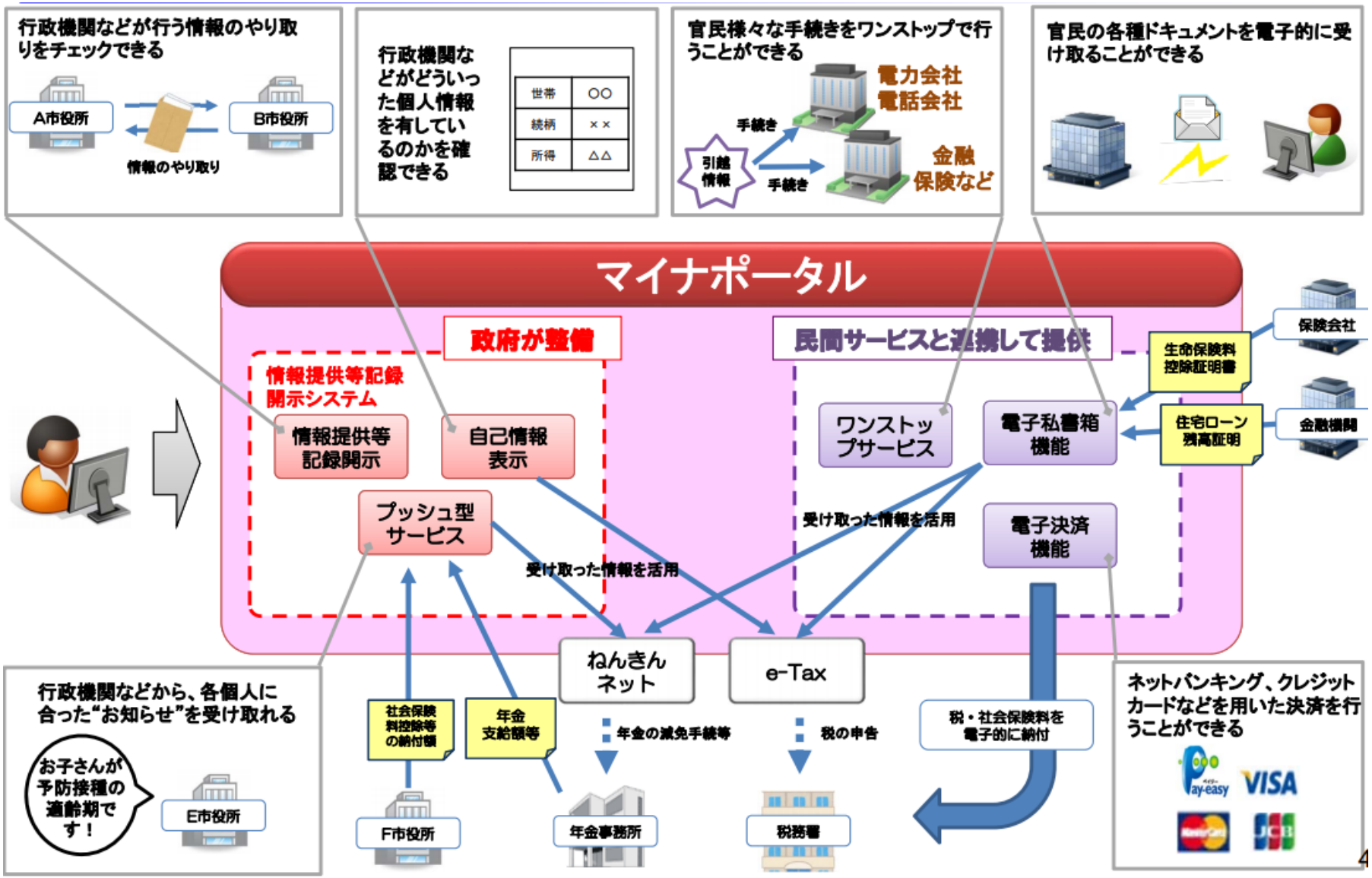
認証基盤の評価項目を定め、5つの認証基盤を中心に具備する機能の調査および評価を実施した。

- 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ることができる。 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。）	・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連携プロトコル		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

© NRI SecureTechnologies, Ltd.

マイナポータルは、政府が運営するオンラインサービス。子育てや介護などの行政手続き、公金決済、外部連携などサービスを提供している。



※参照元：https://warp.da.ndl.go.jp/info:ndljp/pid/11126101/www.meti.go.jp/policy/it_policy/id_renkei/150917_1_METI.pdf p4

マイナポータルに関する調査結果を以下に示す。

調査項目		説明
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）
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。
	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。
	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。
ID登録・身元確認	公的証明書を用いた身元確認なし	-
	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。
認証方法	ID/パスワードによる認証	-
	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。
	その他の認証	-

© NRI SecureTechnologies, Ltd.

マイナポータルに関する調査結果を以下に示す。

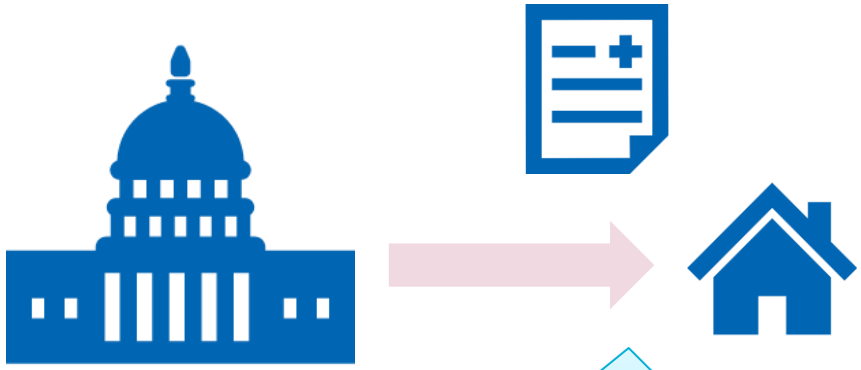
調査項目		説明
ID連携プロトコル		非公開
連携しているサービス		国税電子申告納税システム（e-Tax）、ねんきんネット、MyPost(日本郵便）、e-私書箱（野村総研）、総務省 電波利用 電子申請・届出システムLite
認証連携の同意・情報提供の管理等		サービス連携時の同意取得 エンドユーザのマイページから外部サイトに連携した履歴の確認および取り消しの実行
関連法制度		・行政手続における特定の個人を識別するための番号の利用等に関する法律 ・行政手続における特定の個人を識別するための番号の利用等に関する法律施行規則
関連ガイドライン	NIST SP800-63A	アイデンティティ保証レベルIAL3に相当
	NIST SP800-63B	認証保証レベルAAL3に相当
	NIST SP800-63C	非公開
	その他	行政手続におけるオンラインによる本人確認の手法に関するガイドライン
セキュリティ向上のための施策	ログイン履歴	利用履歴より確認可能
	ログインアラート	ログインするたびに指定したメールアドレスへの通知が可能。
	ログインセッション	なし
	その他	重要な手続きをする際に、認証の際に使われる利用者証明書電子証明書ではなく、署名用電子証明書を用いて、送信内容が改ざんされないようにする。

© NRI SecureTechnologies, Ltd.

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

×2

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

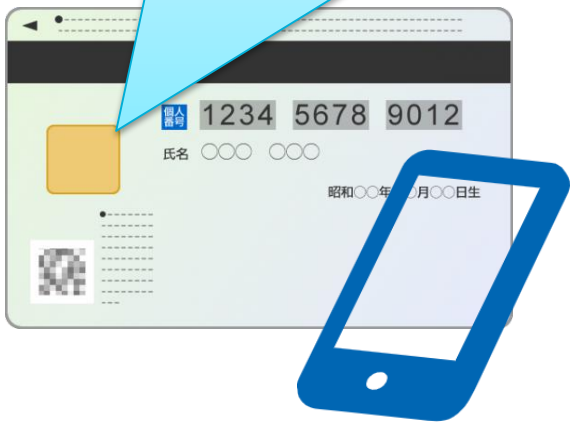
© NRI SecureTechnologies, Ltd.

マイナポータルにログインをする際には、マイナンバーカードのICチップにある利用者証明書電子証明書とパスワードが必要となり、セキュリティ強度が高いのが特徴である。

・ICチップに利用者証明用電子証明書が格納されている。
・取り出すには**パスワードの入力**が必要。
・**対タンパー性**を有するため、ICチップ内の情報を外部から不当に改ざん・読取りができない。

利用者証明書電子証明書

マイナポータルにログインするには、
・マイナンバーカード（所持認証）
・利用者証明書電子証明書パスワード（記憶認証）
の**二要素認証**が必要となる。**（セキュリティ強度が高い）**



利用者証明書電子証明書の送付

ログイン

マイナポータル

電子証明書の照会

照会結果の通知

公的個人認証サービス（JPKI）

・マイナンバーカードのICチップを読取り、利用者証明書電子証明書のパスワード入力し、電子証明書を取り出す。

© NRI SecureTechnologies, Ltd.

行政手続におけるオンラインによる本人確認の手法に関するガイドラインに記載されている保証レベルと比較すると、保証レベル3に該当する。

	ガイドラインにおける保証レベル3の要件	マイナンバーカードとマイナポータルにおける身元確認と認証の要件
登録	・対面で、公的な写真付き身分証明書１種の提示 ・申請情報の公的な台帳照合 ・重複登録ではないことの確認	・対面で官公署発行の本人確認書類1種の提示、または市区町村長が適当と認めるもの2点
発行・管理	・手渡しによるトークン発行 ※本人限定受取郵便基本型及び これと同等の手段は対面として扱う	・市区町村窓口において、マイナンバーカードを発行
トークン	・記憶された秘密、認証デバイス、生体認証の中から複数の認証要素を利用すること。 ・耐タンパ性が確保された ハードウェアトークンを利用すること。	・記憶された秘密（利用者証明用電子証明書）と認証デバイス（マイナンバーカード）を用いて、認証をする。 ・電子証明書が保存されているマイナンバーカードのICチップは、耐タンパ性を有する。
認証プロセス	・オンライン上の推測、リプレイ攻撃、盗聴、セッション・ ハイジャック、中間者攻撃、フィッシングの脅威に対する耐性	・オンライン上の推測：認証回数の制限（アカウントロック） ・リプレイ攻撃：認証要求ごとにランダムなデータを含める ・盗聴：通信の暗号化 ・セッションハイジャック：推測困難なセッションIDの利用、認証後に新たなセッションIDの払い出しを行う ・中間者攻撃：正当なサービス提供者に接続したことをOpenID Connectの認証プロセスで確認 ・フィッシング：EV-SSL証明書を利用
署名等プロセス	・電子政府推奨暗号リストに記載の電子署名 ・電子署名用の証明書の用途は電子署名限定	・地方公共団体情報システム機構から発行された電子署名を用いる。 ・署名用電子証明書の用途は、電子署名に限定。

※https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf
を基にNRIセキュアテクノロジーズ作成

© NRI SecureTechnologies, Ltd.

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

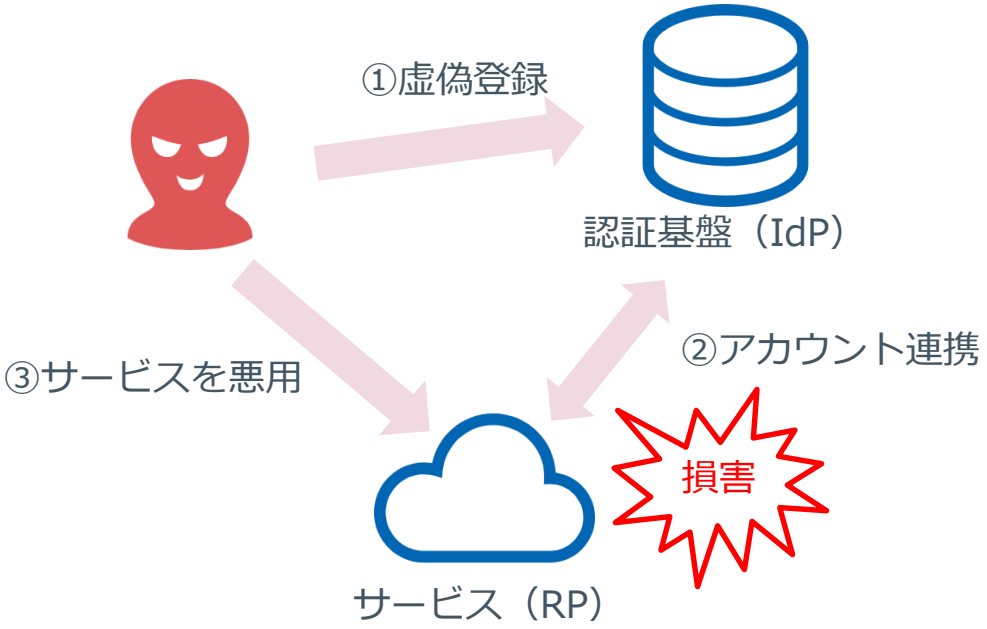
人を欺き、人に暴行を加え、若しくは人を脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為、その他の個人番号を保有する者の管理を害する行為により、個人番号を取得した者は、三年以下の懲役又は百五十万円以下の罰金に処する。

・**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。

© NRI SecureTechnologies, Ltd.

認証基盤に登録された虚偽情報をもとにサービスの提供を行い、サービスで損害が発生した場合の責任分担は、ユースケースや各地域の運用次第である。

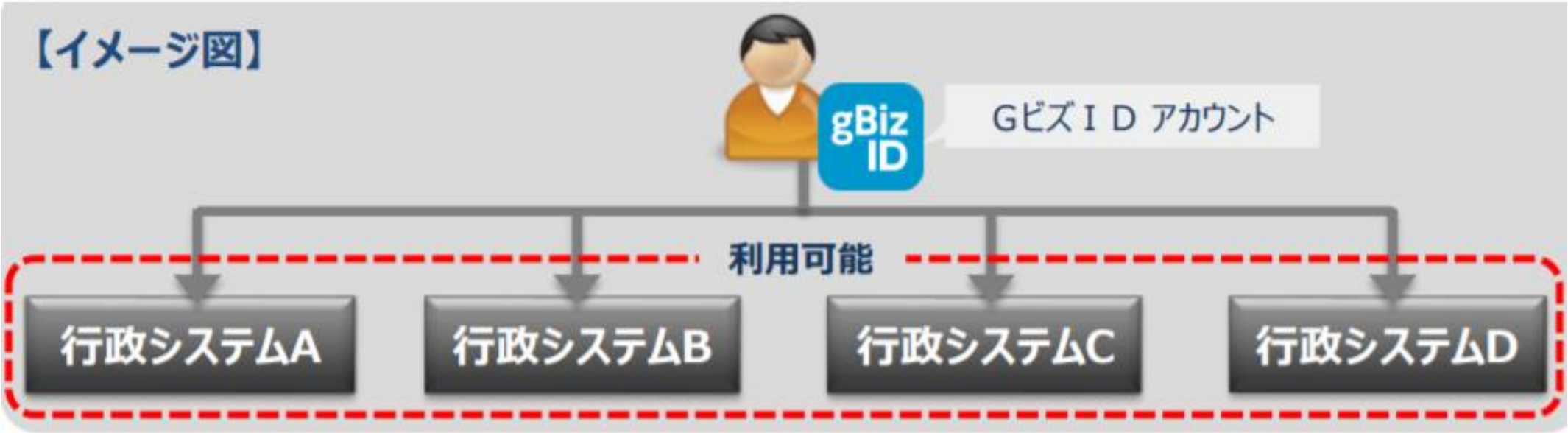
- 認証基盤(IdP)に登録されている虚偽情報をもとにサービス(RP)がサービスの提供を行い、サービスで損害が発生してしまった場合の責任分担は、ユースケースや各地域の運用次第である。
- 例えば、英国Open Bankingでは、サービス側の事業規模が小さいケースが多数であることもあり、IdPとなる銀行が一旦その負担を引き受けて、RPと結んでいる利用規約によって、責任の分担を行うモデルにより運用されている。
- アメリカのバージニア州では、IdP側のクレデンシャル情報の提供をもとに発生した訴訟に伴い、IdP側に重大な過失がない場合はIdPを免責とする法律改正案を提出する動きがみられた。※



※参照元：https://lis.virginia.gov/cgi-bin/legp604.exe?111+ful+HB2259&111+ful+HB2259/

© NRI SecureTechnologies, Ltd.

gBizIDは、法人番号を活用し、1つのアカウントで複数の行政サービスにアクセスすることができる認証システムである。



※参照元：https://gbiz-id.go.jp/top/manual/pdf/QuickManual_Member.pdf

© NRI SecureTechnologies, Ltd.

gBizIDに関する調査結果を以下に示す。

調査項目		説明
ID数		13万
ID管理	情報更新	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。
	利用不能時のリカバリー方法	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。
	紛失時	-
	失効・退会	マイページ上より退会可能。
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。）
	公的証明書を用いた身元確認あり	・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。
認証方法	ID/パスワードによる認証	・gBizID エントリー：ID/パスワードでの認証
	多要素認証	・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ワンタイムパスワード
	その他の認証	-

© NRI SecureTechnologies, Ltd.

gBizIDに関する調査結果を以下に示す。

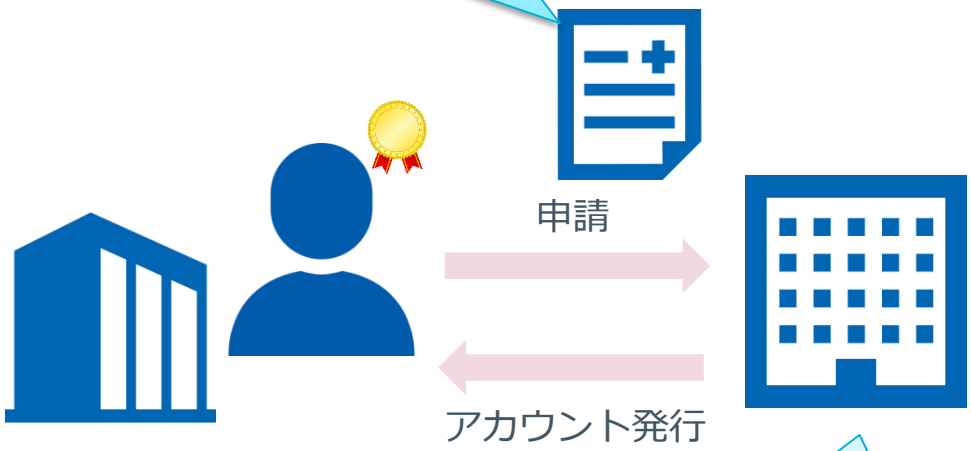
調査項目		説明
ID連携プロトコル		OpenID Connect（認可コードフロー）
連携しているサービス		社会保険手続きの電子申請、IT導入補助金2020、農林水産省共通申請サービス等20システム
認証連携の同意・情報提供の管理等		利用規約の同意取得等
関連法制度		・情報通信技術を活用した行政の推進等に関する法律 ・各省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
関連ガイドライン	NIST SP800-63A	・gBizID プライム・メンバー 　アイデンティティ保証レベルIAL2に相当 ・gBizID エントリー 　アイデンティティ保証レベルIAL1に相当
	NIST SP800-63B	・gBizID プライム・メンバー 　認証保証レベルAAL2に相当 ・gBizID エントリー 　認証保証レベルAAL1に相当
	NIST SP800-63C	認証連携における保証レベルFAL1
	その他	行政手続におけるオンラインによる本人確認の手法に関するガイドライン
セキュリティ向上のための施策	ログイン履歴	ログイン履歴等を取得
	ログインアラート	一度もログインしたことのない端末からログインがあった場合、SMSまたはメールで通知する。
	ログインセッション	なし
	その他	-

© NRI SecureTechnologies, Ltd.

gBizプライムのアカウント作成をする際に、運用センターで申請の審査が実施される。また、gBizプライムとメンバーがgBizIDを利用する際には2要素認証が要求される。

gBizプライムの発行

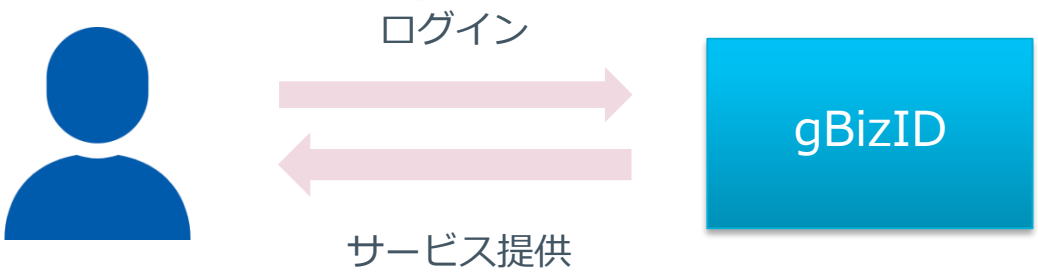
申請書に押印をし、印鑑登録証明書とともに送付をする。



ＧビズＩＤ運用センターにて、申請内容の審査が行われる。

gBizプライム・メンバーの認証

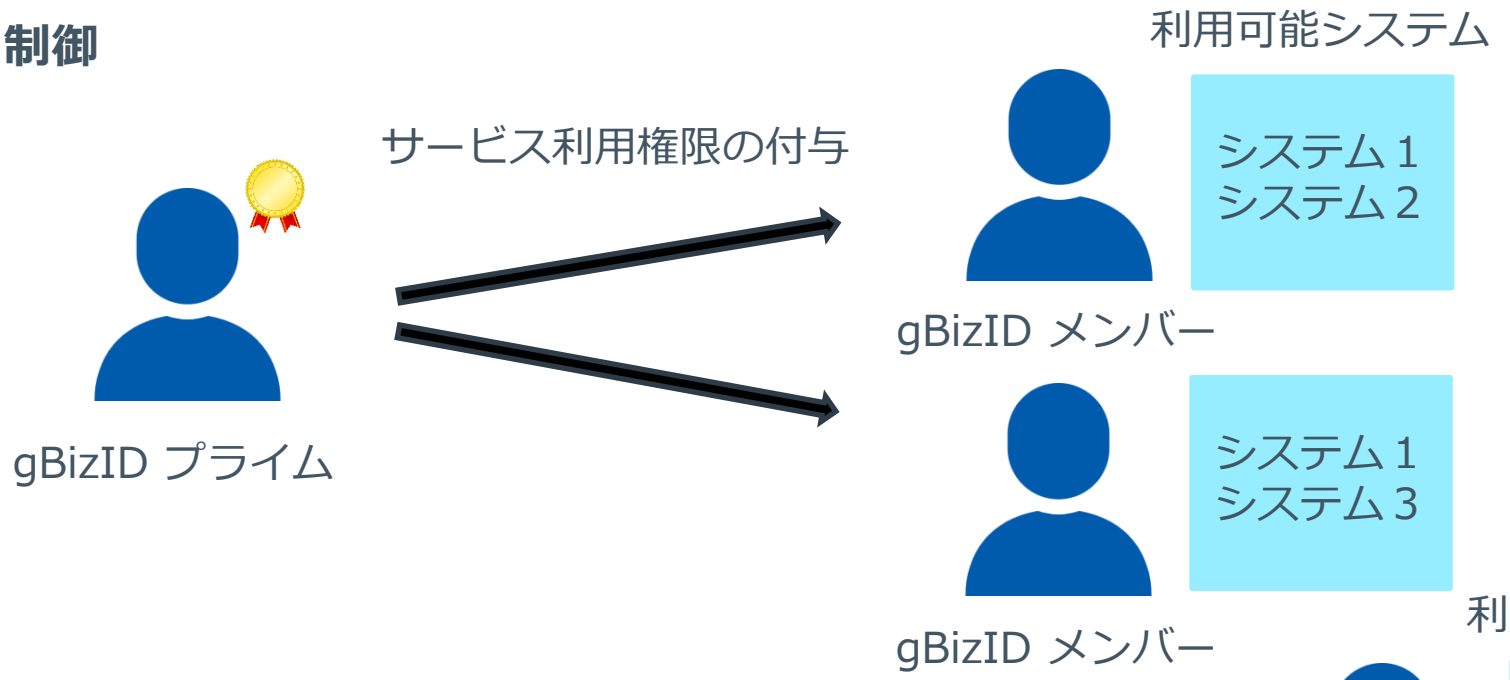
必ず2要素による認証を行う必要がある。
・ID/パスワード
・SMSワンタイムパスワード、またはスマートフォンアプリによるパスコード認証または生体認証



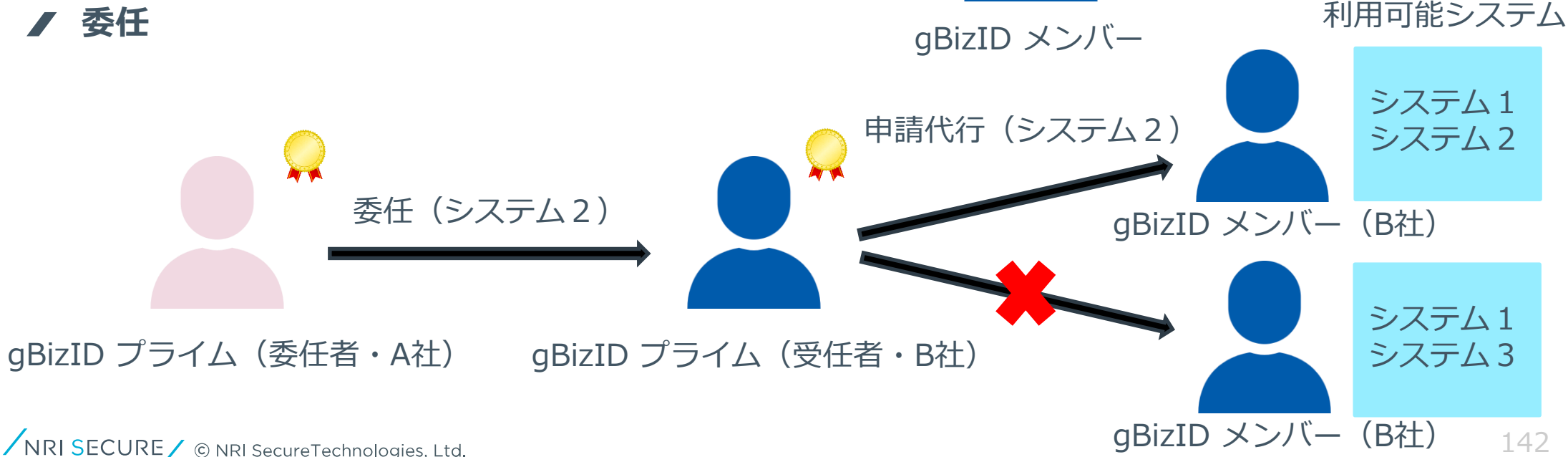
© NRI SecureTechnologies, Ltd.

gBizID プライムはgBizID メンバーを作成を行い、一部サービスの利用を許可することができる。また、代理申請に会社間で委任関係を登録することができる。

サービス利用制御



委任



© NRI SecureTechnologies, Ltd.

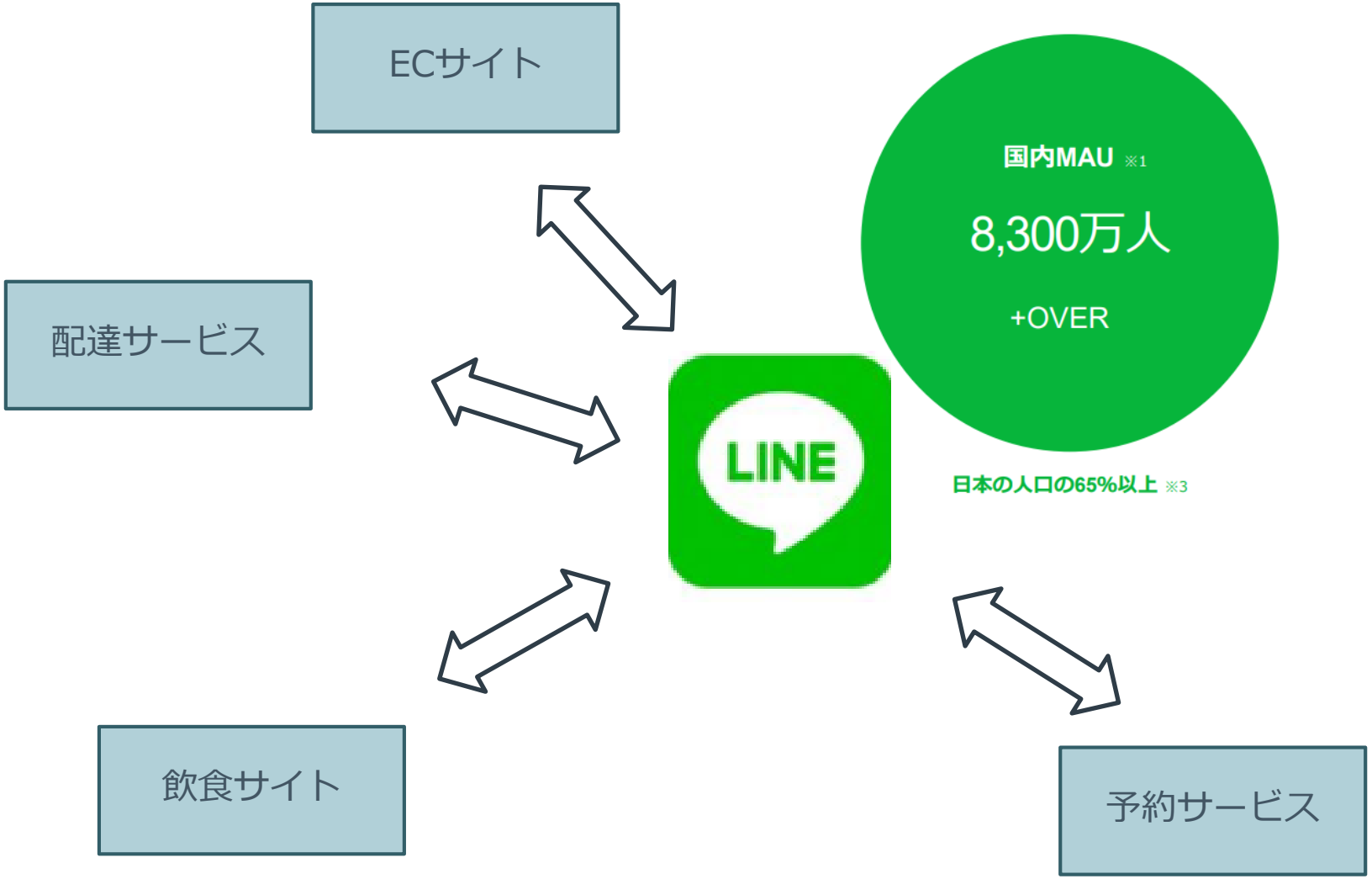
行政手続におけるオンラインによる本人確認の手法に関するガイドラインに記載されている保証レベルと比較すると、保証レベル2に該当する。

項目	ガイドラインにおける保証レベル2の要件	gBizプライムのアカウントを対象とした際の、gBizIDにおける認証と身元確認の要件
登録	（対面の場合） ・公的な写真付き身分証明１種（又は他２種）の提示 ・申請情報の台帳（又は公的証明書）照合 **（郵送又はオンラインの場合）** **・申請書に対する電子署名（郵送の場合は署名又は捺印）** **・申請情報の台帳（又は添付の公的証明書）照合**	申請書を記入して押印後、印鑑（登録）証明書とともに郵送を行い、審査後が行われる。
発行・管理	・手渡しによるトークン発行、本人限定受取郵便基本型及びこれと同等の手段、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、**携帯電話の番号検証＋ダウンロードによるトークン発行**	メールで通知されるURLにログインをし、SMS番号に発行されるワンタイムパスワードを入力することで、アカウントが発行される。
トークン	・記憶された秘密、認証デバイス、生体認証の中から複数の認証要素を利用すること	ID/パスワード＋スマートフォンアプリまたはSMSワンタイムパスワードで認証
認証プロセス	・オンライン上の推測、リプレイ攻撃、盗聴、セッション・ ハイジャック、中間者攻撃、フィッシングの脅威に対する耐性	・オンライン上の推測：認証回数の制限（アカウントロック） ・リプレイ攻撃：認証要求ごとにランダムなデータを含める ・盗聴：通信の暗号化 ・セッションハイジャック：推測困難なセッションIDの利用 ・中間者攻撃：正当なサービス提供者に接続したことをOpenID Connectの認証プロセスで確認 ・フィッシング：EV-SSL証明書を利用
署名等プロセス	・電子政府推奨暗号リストに記載の電子署名	該当する署名を利用

※https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf
を基にNRIセキュアテクノロジーズ作成

© NRI SecureTechnologies, Ltd.

LINEは月間8300万のアクティブユーザ数がある、国内有数のSNSサービスで、様々なコンシューマ向けサービスとLINE IDを用いた連携を行っている。



https://www.linebiz.com/system/files/jp/download/LINE%20Business%20Guide_202001-06.pdf
を基にNRIセキュアテクノロジーズ作成
※1 LINEアプリ 月間アクティブユーザー 2019年12月末時点

© NRI SecureTechnologies, Ltd.

LINE IDに関する調査結果を以下に示す。

調査項目		説明
ID数		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)
ID管理	情報更新	マイページ上で変更可能。
	利用不能時のリカバリー方法	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。
	紛失時	-
	失効・退会	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。
ID登録・身元確認	公的証明書を用いた身元確認なし	・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。
	公的証明書を用いた身元確認あり	・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。
認証方法	ID/パスワードによる認証	【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
	多要素認証	【LINEアプリへのログイン】 デスクトップアプリ：初回のみ ID/パスワード+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
	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

© NRI SecureTechnologies, Ltd.

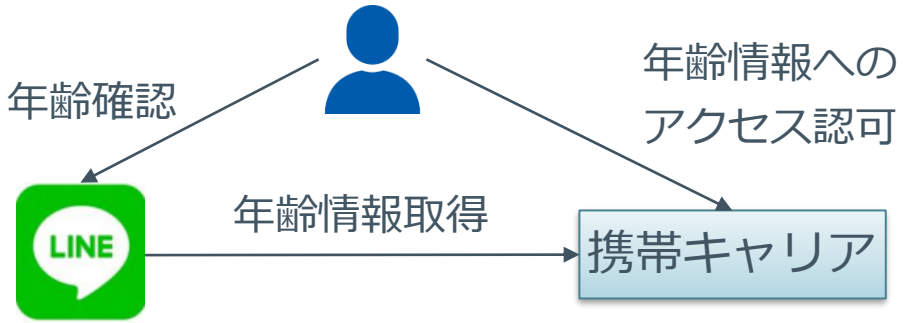
LINE IDに関する調査結果を以下に示す。

調査項目		説明
ID連携プロトコル		OpenID Connect（認可コードフロー）
連携しているサービス		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。
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 マイページより連携しているサービスの解除可能
関連法制度		犯罪収益移転防止法
関連ガイドライン	NIST SP800-63A	・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
	NIST SP800-63B	・LINE PayのFIDO認証：認証保証レベルAAL3に相当 ・デスクトップアプリのLINE初回認証時：認証保証レベルAAL2に相当 ・それ以外：認証保証レベルAAL1に相当
	NIST SP800-63C	認証連携保証レベルFAL2に相当
	その他	-
セキュリティ向上のための施策	ログイン履歴	なし
	ログインアラート	デスクトップアプリとブラウザ上でログインした際には、アプリ上で通知される。
	ログインセッション	デスクトップアプリとブラウザからのログインセッションの取り消しができる。
	その他	-

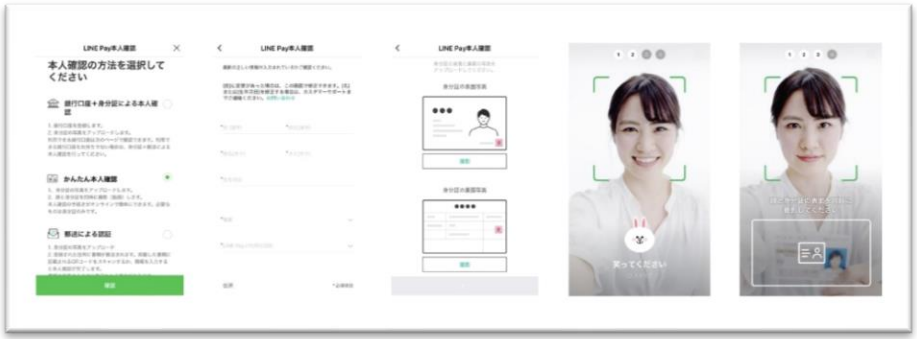
© NRI SecureTechnologies, Ltd.

LINE ID登録の際は、ユーザが持つ電話番号との紐付けやキャリアと連携した年齢確認を行っている。また、特定サービス利用にあたっては身元確認も実施。

- LINE IDの新規登録時においては以下2点の確認を実施している。
  - 電話番号紐付け：入力された電話番号宛にSMSもしくは電話で6桁の確認コードを送付し、そのコードを確認することでアカウントに疎通確認された電話番号を紐づける。複数のアカウントで同じ電話番号を紐づけることはできない。
  - 年齢確認：ユーザのアクセス認可を受けてキャリア側に登録されている年齢情報を取得し年齢確認(18歳以上であること)を実施。



- モバイル決済サービスであるLINE Payでは、身元確認手法として銀行口座登録による確認に加え、2018年に改正された犯罪収益移転防止法施行規則に基づき、本人確認書類によるオンラインでの身元確認に対応している。

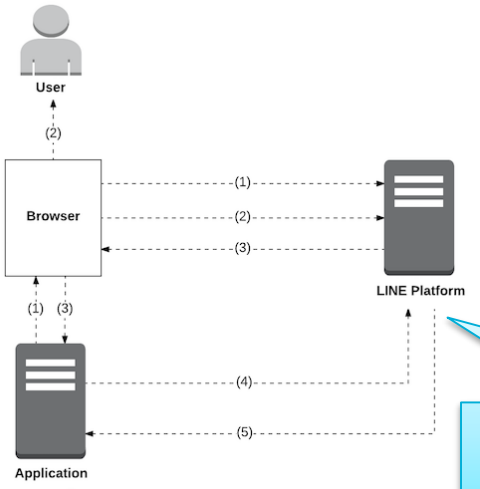


※参照元：https://linecorp.com/ja/pr/news/ja/2019/2688

© NRI SecureTechnologies, Ltd.

認証連携サービスLINEログインでは、外部サービス向けにOAuth2.0 および OpenID Connect プロトコルに基づく認証連携機能を提供している。

- LINE ログインにおけるWebアプリケーションとの認証連携の処理シーケンスおよびインターフェース仕様は、OpenID Connectに基づくものとなっている。



1. LINEログイン画面がブラウザで開き、ユーザーはログインして認証を受ける。LINEプラットフォームでユーザーの認証情報が検証された後、ユーザーはアプリから要求される権限を付与することに同意する必要もある。
2. 必要なクエリパラメータを使用して、アプリからLINEログインの認可URLにユーザーを誘導する。
3. LINEプラットフォームからアプリに、redirect_uri を介してユーザーをリダイレクトする。このとき、認可コードとstateを含むクエリ文字列もアプリに送信される。
4. アプリは、認可コードを使ってエンドポイントURLにアクセストークンを要求する。
5. LINEプラットフォームがアプリからのリクエストを検証し、アクセストークンをアプリに返す。

LINEプラットフォーム
(OpenID ConnectにおけるOpenID Provider)

外部サービスWebアプリケーション
(OpenID ConnectにおけるRelying Party)

(※)https://developers.line.biz/ja/docs/line-login/integrate-line-login/を基にNRIセキュアテクノロジーズ作成

- スマートフォンネイティブアプリに対しては、LINEログインを利用する外部サービスに対して、連携用SDK(Software Development Kit)を提供している。
  - SDKにより、OpenID Connect における Relying Party の実装の検討負荷を軽減することができる。外部サービス側の開発負荷を低減するとともに、認証連携のセキュリティを一定以上に保つことが可能となる。

© NRI SecureTechnologies, Ltd.

LINE IDを利用したユーザ認証方法として、LINEアプリとの連携による認証など多彩な認証方式をサポートしており、一部サービス向けにはFIDO認証もサポートしている。

- LINEログインでは、以下の認証方式をサポートしている。

認証方法	説明
自動ログイン	同一スマートフォン(Android/iOS端末)内のLINEアプリケーションにログインしている場合にユーザの操作なしでログインする
メールアドレスログイン	LINEに登録したメールアドレスとパスワードを入力してログインする
QRコードログイン	LINEログイン画面に表示されたQRコードを、スマートフォン版LINEアプリケーションのQRコードリーダーでスキャンしてログイン
SSO(シングルサインオン)によるログイン	以前にLINEログインした場合に作成されるCookieが存在する場合にログインボタンをクリックするだけでログイン

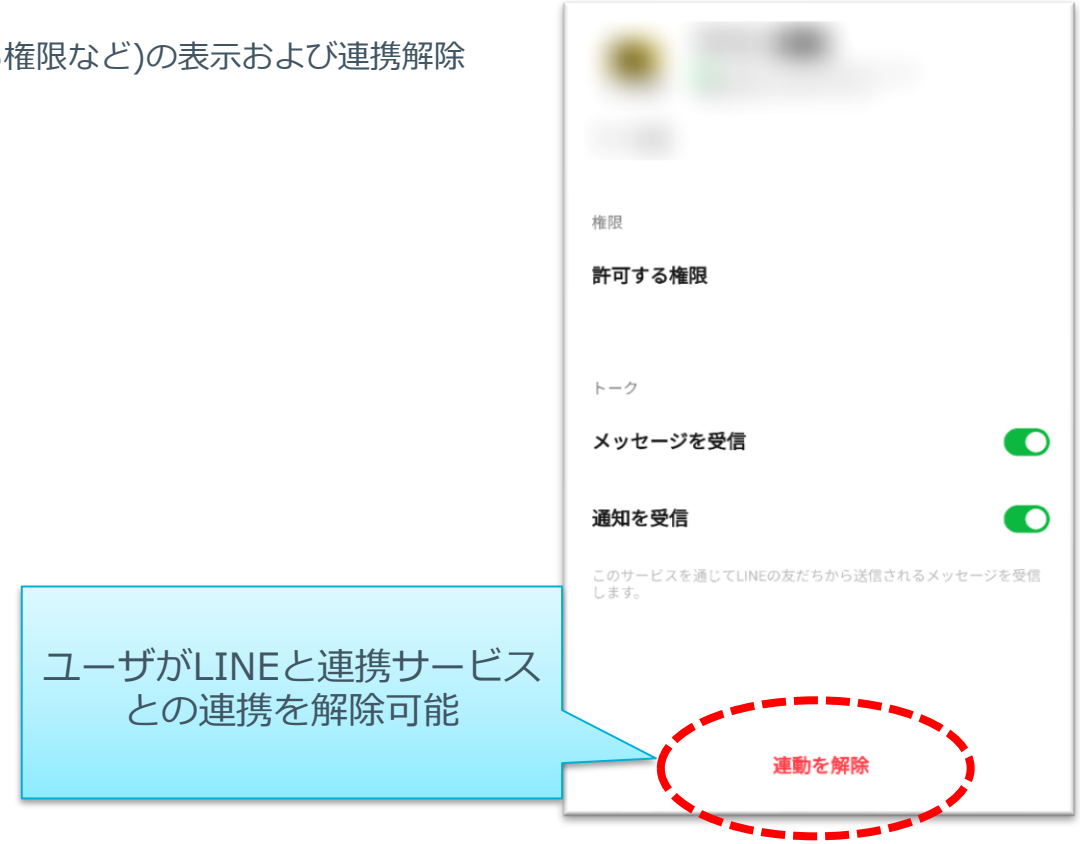
- さらに、高いセキュリティが求められるモバイル決済サービスであるLINE PayではFIDO認証を導入しており、今後FIDO認証はLINEの他サービス向けにも導入されていく予定※。
  - LINE認証サーバは、2019年にFIDO AllianceのFIDO Universal Server認証を受けている。

※参照元：https://www.slideshare.net/FIDOAlliance/2019-fido-tokyo-seminar-line-payfido2

© NRI SecureTechnologies, Ltd.

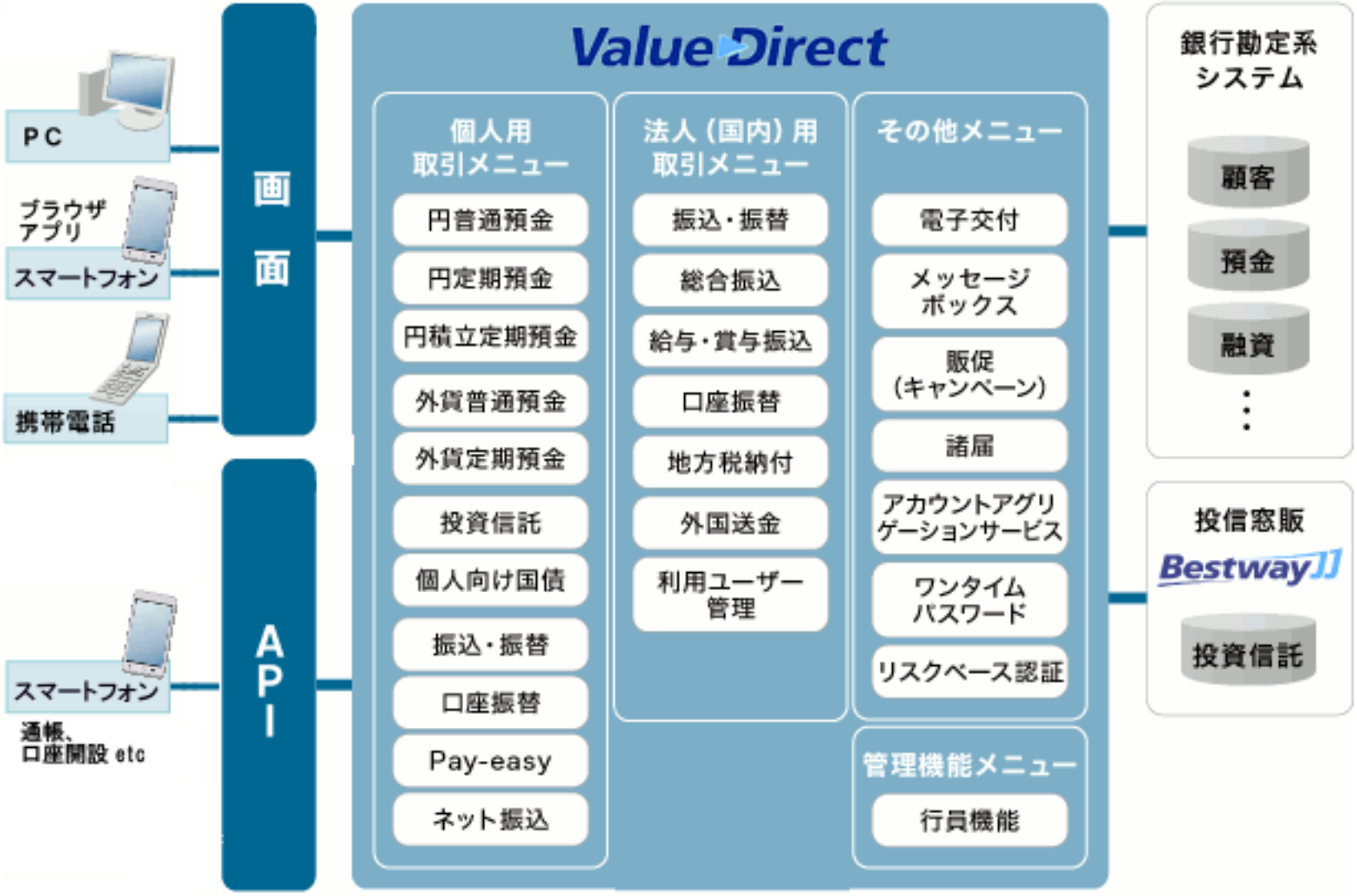
LINEとの連携サービスについて、ユーザ向けに一覧表示や連携を解除するための機能を提供することで、ユーザが意図しない情報連携を防ぐことが可能となっている。

- サービス連携時にはユーザに対して連携するサービス名およびそのサービスに許可する権限（ユーザ情報の参照など）を表示の上同意を得て初めて連携される。
- 連携されたサービスについてはユーザ向けに一覧の表示およびサービス連携解除の機能を提供する。
  - 右図に連携サービスの詳細(そのサービスに許可している権限など)の表示および連携解除のための画面イメージを示す。



© NRI SecureTechnologies, Ltd.

Value Directはインターネットバンキングの共同利用型サービス。地方銀行や信託銀行等に導入されている。



※参照元：https://www.nri.com/jp/service/solution/fis/value_direct

© NRI SecureTechnologies, Ltd.

Value Directに関する調査結果を以下に示す。

調査項目		説明
ID数		非公開
ID管理	情報更新	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。
	利用不能時のリカバリー方法	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。
	紛失時	-
	失効・退会	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。
ID登録・身元確認	公的証明書を用いた身元確認なし	-
	公的証明書を用いた身元確認あり	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。
認証方法	ID/パスワードによる認証	-
	多要素認証	・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。
	その他の認証	・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

© NRI SecureTechnologies, Ltd.

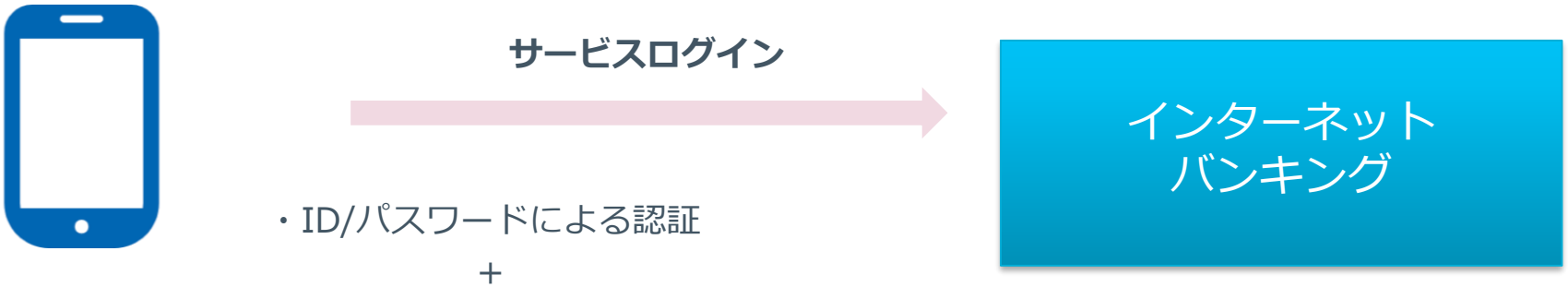
Value Directに関する調査結果を以下に示す。

調査項目		説明
ID連携プロトコル		-
連携しているサービス		-
認証連携の同意・情報提供の管理等		サービス利用時の同意の取得
関連法制度		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IAL2に相当
	NIST SP800-63B	・サービスログイン時 認証保証レベルAAL1 ・重要取引時 認証保証レベルAAL2
	NIST SP800-63C	-
	その他	-
セキュリティ向上のための施策	ログイン履歴	マイページから確認することができる。
	ログインアラート	なし
	ログインセッション	なし
	その他	-

© NRI SecureTechnologies, Ltd.

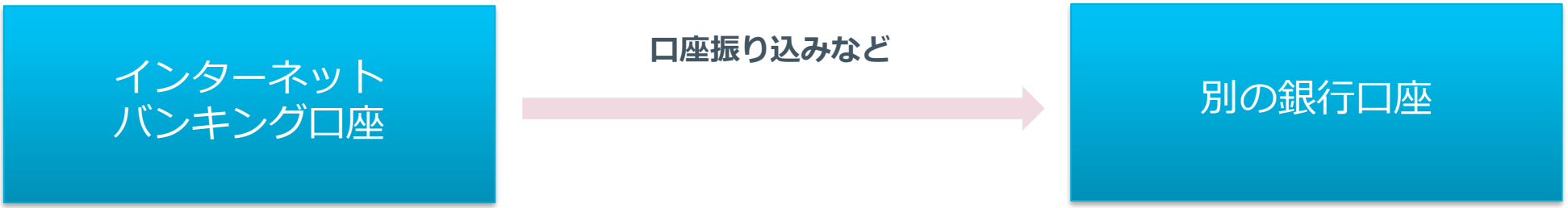
インターネットバンキングでは、オプション機能としてワンタイムパスワード認証機能、リスクベース認証機能を提供している。

サービスログイン



・ID/パスワードによる認証
＋
・リスクベース認証（高リスクの場合、追加で秘密の質問による認証）

重要取引時の追加認証

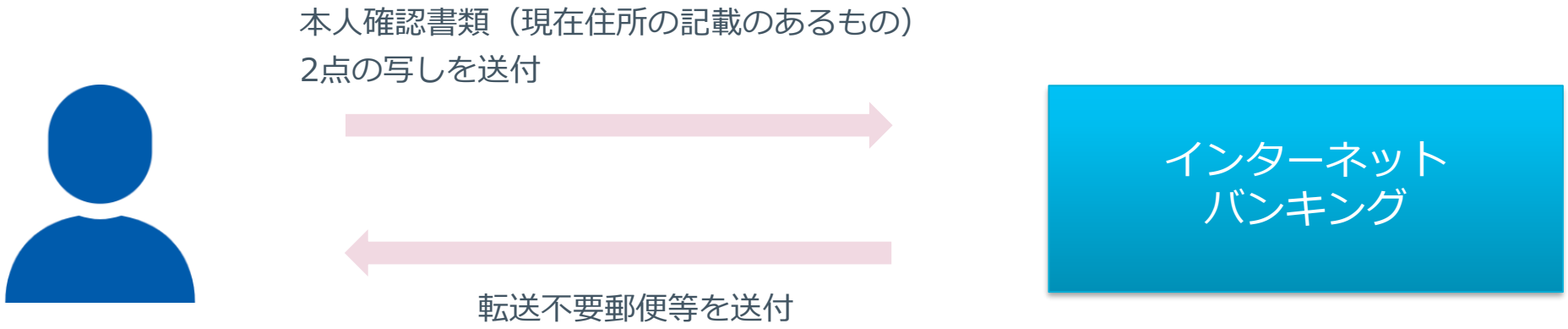


・アプリ型ワンタイムパスワードまたは、乱数表を使って、追加でパスワードを入力する。

© NRI SecureTechnologies, Ltd.

インターネットバンキングで口座開設をする際に、犯罪による収益の移転防止に関する法律施行規則の第６条第１項第１号リに基づく身元確認を実施している。

身元確認



本人確認書類

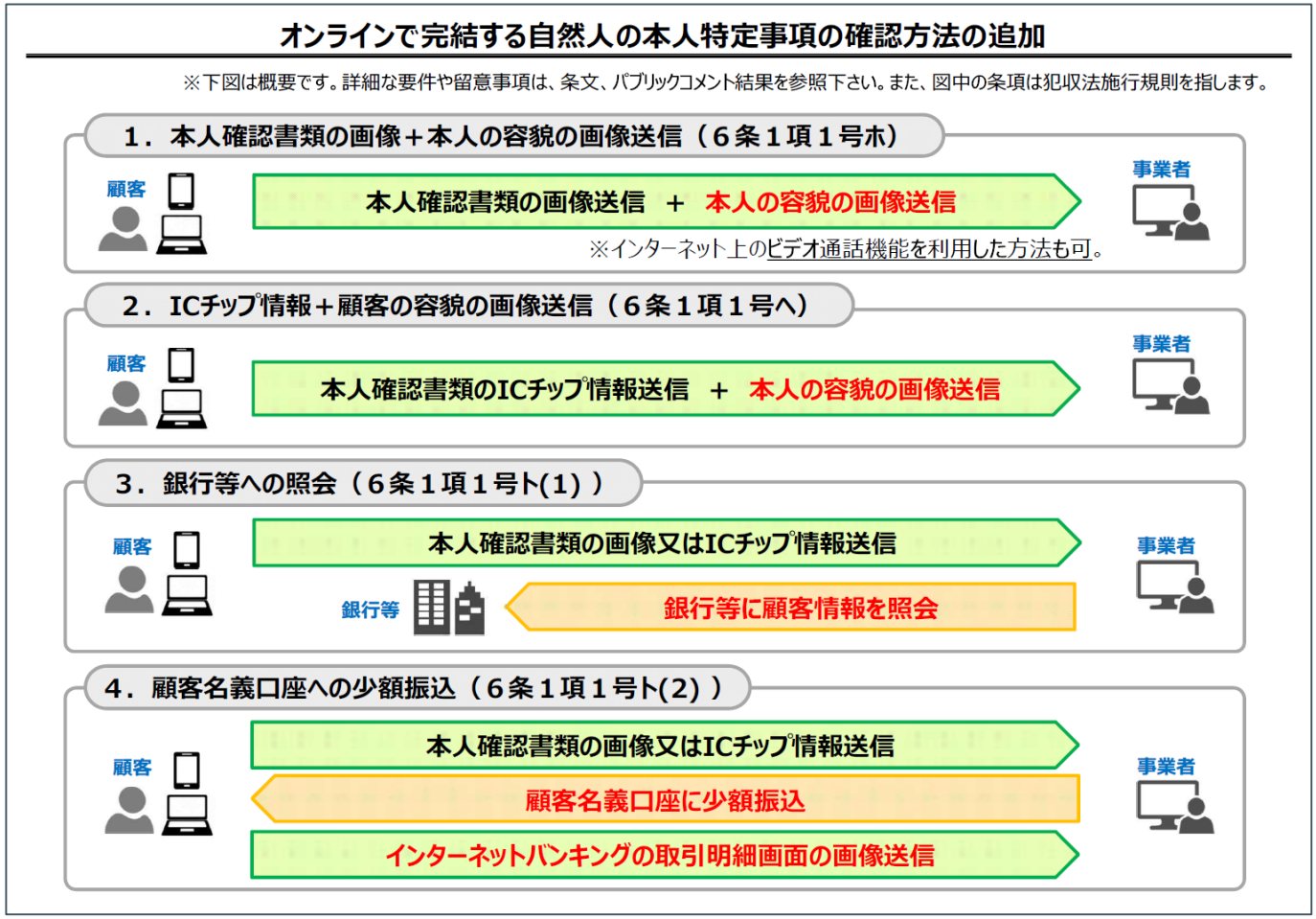
- インターネット経由による書類送付、身元確認(eKYC)にも対応している。

送付方法	本人確認書類
インターネット	運転免許証と健康保険証
郵送	下記の1~4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

© NRI SecureTechnologies, Ltd.

犯罪による収益の移転防止に関する法律施行規則では、オンラインで完結する身元確認方法として、複数の方法が追加された。

- 平成30年11月にオンラインで完結する自然人の本人特定事項の確認方法の追加として、以下の方法が追加された。
- これにより、JPKI等の電子証明書および署名を利用する方法の他、本人確認書類の画像等を利用した身元確認方法も認められるようになっている。



※参照元： https://www.fsa.go.jp/news/30/sonota/20181130/01.pdf
「オンラインで完結する自然人の本人特定事項の確認方法の追加」

© NRI SecureTechnologies, Ltd.

犯罪収益移転防止法では、取引確認時の身元確認の情報の偽造やなりすましを想定し、不正に預貯金通帳・カードの提供・交付を受けた場合の罰則が規定されている。

第27条

顧客等又は代表者等の**本人特定事項を隠蔽**する目的で、第四条第六項の規定に違反する行為
（取引確認時にかかる事項を偽る行為）をした者は、
一年以下の懲役若しくは百万円以下の罰金に処し、
又はこれを併科する。

・口座開設等の際に行われる**取引確認時に**、本人特定事項を偽ると適用される罰則。

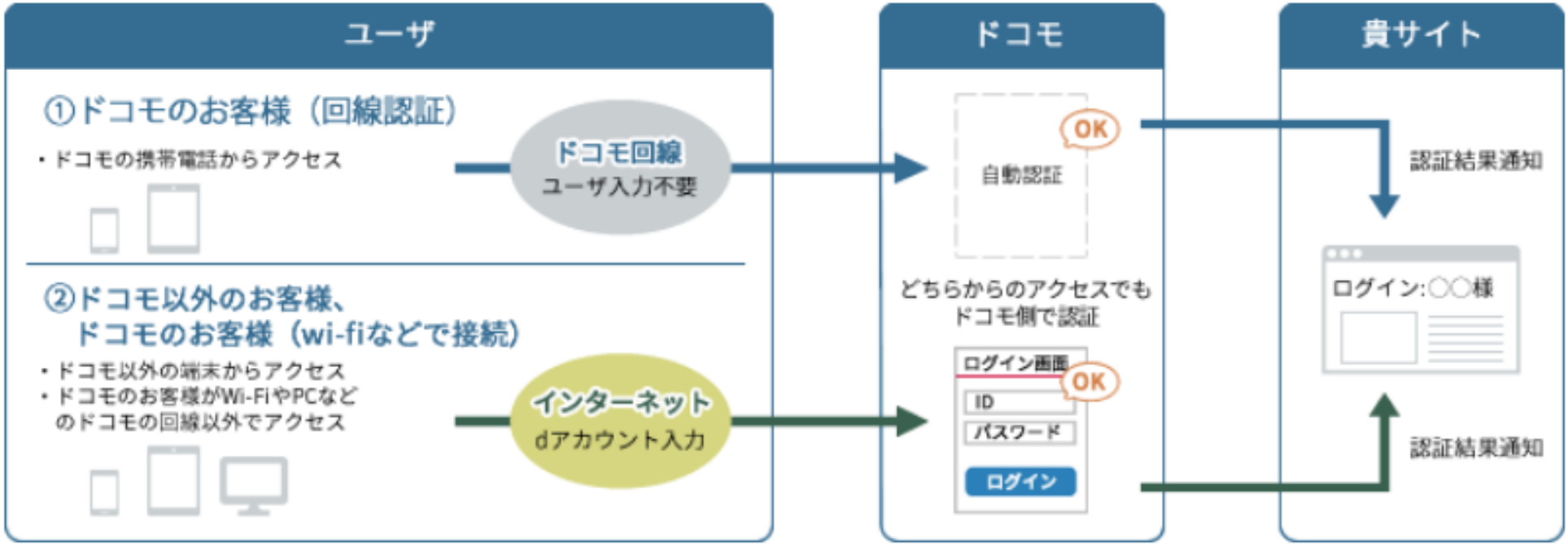
第28条

他人になりすまして特定事業者との間における預貯金契約に係る役務の提供を受けること又はこれを**第三者にさせることを目的**として、当該預貯金契約に係る預貯金通帳、預貯金の引出用のカード、
（中略）の交付を受け、又はその提供を受けた者は、一年以下の懲役若しくは百万円以下の罰金に処し、又はこれを併科する。

・**他人になりすまし**をして、銀行と預貯金の契約を結ぶまたは、第三者にさせることを目的として預貯金通帳・カードの交付を受けた場合に適用される罰則。

© NRI SecureTechnologies, Ltd.

dアカウントはNTTドコモが提供しているIDで、ドコモグループだけでなく教育サービスやスポーツチケット予約サイト等のサービスと連携をしている。



※参照元： https://id.smt.docomo.ne.jp/src/dlogin/ctop_method.html

© NRI SecureTechnologies, Ltd.

dアカウントに関する調査結果を以下に示す。

調査項目		説明
ID数		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	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	-
	失効・退会	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	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	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
認証方法	ID/パスワードによる認証	・パスワード認証
	多要素認証	・パスワード＋PIN（メール） ・パスワード＋PIN（SMS）
	その他の認証	・FIDO認証 ・回線認証

© NRI SecureTechnologies, Ltd.

dアカウントに関する調査結果を以下に示す。

調査項目		説明
ID連携プロトコル		OpenID Connect（認可コードフロー）
連携しているサービス		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		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		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	・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
	NIST SP800-63B	・FIDO認証でログイン 認証保証レベルAAL3に相当 ・回線認証、ID/パスワード+スマホアプリ操作 認証保証レベルAAL2に相当 ・ID/パスワード、ID/パスワード+メール 認証保証レベルAAL1に相当
	NIST SP800-63C	非公開
	その他	-

© NRI SecureTechnologies, Ltd.

dアカウントに関する調査結果を以下に示す。

調査項目		説明
セキュリティ向上のための施策	ログイン履歴	利用履歴より確認可能
	ログインアラート	普段利用しない環境からログインがあった場合にはログイン通知メールが送付される。
	ログインセッション	なし
	その他	パスワードレス認証設定をすることで、フィッシング詐欺やリスト型アカウントハッキング等を防ぐことができる。

© NRI SecureTechnologies, Ltd.

大手携帯電話事業者においては、各社ともOpenIDおよびFIDOに対する取り組みを行っており、実運用が行われている。

KDDI

- 2015年11月より、OpenID Foundation のボードメンバーとして参画。
- FIDO Japan Working Group 参加メンバーとして参画(2020年1月時点)
- au IDにて、OpenID および FIDO を活用した認証連携機能を提供。

ソフトバンク

- FIDO Japan Working Group 参加メンバーとして参画(2020年1月時点)
- スマートフォンアプリ「My SoftBankプラス」(※)にFIDO認証でのログイン機能を追加。

※2020年3月サービス終了、以降はMySoftbankに機能統合。

© NRI SecureTechnologies, Ltd.

携帯音声通信事業者は、回線契約を行う際に携帯電話不正利用防止法に基づく身元確認を実施する必要がある。

確認項目

下記の事項の確認を
行わなければならない。
・氏名・住所・生年月日

携帯電話不正利用
防止法
第3条に該当

本人確認書類

・運転免許証、旅券、
マイナンバーカード等
・健康保険証、介護保険の被保険者証
等
・国民年金手帳、母子手帳等
・印鑑登録証明書、住民票の写し等

主務省令
第５条に該当

確認方法

・顔写真付きの公的証明書原本の提示
・公的証明書やその写しを送付し、
転送不要郵便の送付または事業者が
出向いて電話番号等を交付
・ソフトウェアを通じて顔画像を送信
し、写真付き本人確認書類のICの情
報または、画像を送信する。

主務省令
第３条に該当

© NRI SecureTechnologies, Ltd.

携帯電話不正利用防止法では、回線契約時に行う身元確認の情報を偽ったり、自身が契約者になっていないSIMカードを他人に譲渡した場合の罰則規定が定められている。

第19条

本人特定事項を隠ぺいする目的で、第三条第四項（通信事業者と回線契約を行う際の身元確認で身元特定事項を偽ってはいけないことを定めている条項）の規定に違反した者は、五十万円以下の罰金に処する。

・**他人になりすまし**をしたり、**身元確認の際に情報を偽って**回線契約を行った場合に適用される罰則。

第21条

自己が契約者となっていない役務提供契約に係る通話可能端末設備等を他人に譲渡した者は、五十万円以下の罰金に処する。**相手方が**通話可能端末設備等に係る役務提供契約の**契約者となっていないこと**の情を知って、その者から当該通話可能端末設備等を譲り受けた者も、前項と同様とする。

・**自分が契約していない通信可能端末**を他人に譲渡したり、**相手が契約者となっていないことを知りながら**通信可能端末を受け取ると適用される罰則。

© NRI SecureTechnologies, Ltd.

回線認証やFIDO認証をサポートすることにより、利用環境によりパスワードレスでログインすることができる。

回線認証

ドコモの回線を契約しているユーザがドコモのネットワークを通してdアカウントへアクセスする際は、回線認証によってログインすることができる。

ログイン

FIDO認証

ログイン

dアカウントではFIDO認証をサポートしているため、FIDO利用登録を行った端末では、パスワードを入力することなく認証を行うことができる。

d アカウント

認証連携

連携サービス

© NRI SecureTechnologies, Ltd.

dアカウントでは専用のアプリでFIDO認証の端末登録を行うことができ、端末を紛失した場合でも、契約した回線で認証することで、FIDO認証の再設定を行うことができる。

端末登録

dアカウントのアプリ上でFIDO認証登録を行いたいdアカウントの認証を行う。

①アプリとdアカウント紐づけ

指紋や顔認証等などを実行し、FIDO認証の端末の登録を行う。

②端末の登録

dアカウント

端末紛失

紛失時は、端末を新たに準備してSIMカードの再発行を行い、契約回線で認証することで、FIDO認証の再設定をすることができる。

①紛失手続き

②SIMカード再発行

ドコモ
お客様サポート

③契約回線で本人確認

④FIDO認証再設定

dアカウント

※参照元：https://www.nttdocomo.co.jp/binary/pdf/corporate/technology/rd/technical_journal/bn/vol28_1/vol28_1_004jp.pdf

© NRI SecureTechnologies, Ltd.

パーソナルデータダッシュボードでは、ユーザの同意内容の一覧や誰にどのようなデータを提供しているのか、管理を行うことができる。

パーソナルダッシュボード

情報提供の管理

	グループ	加盟店	その他
基本情報	✓	✓	✓
利用情報	✓	✓	✓
位置情報	✓	✓	✓
医療健康情報	✓		

どの提供先にどのような情報を提供するのか、ユーザ自身で管理することができる。

※参照元：https://datadashboard.front.smt.docomo.ne.jp/

© NRI SecureTechnologies, Ltd.

7. 同意の表現方法に関する調査

© NRI SecureTechnologies, Ltd.

同意の表現方法調査における調査対象の法制度として、国内外の個人情報保護に関連する法制度の他、インドのデータ利活用基盤であるIndia Stackも対象とした。

- 同意の表現方法に関する法制度調査として、日本における個人情報取り扱いに関する法律である「個人情報の保護に関する法律」（個人情報保護法）を対象とした。

- 上記に加え、海外事例として、特に個人情報保護の意識が高い欧米諸国における取組の調査として個人情報およびプライバシー保護に関連するEUのGDPR、ePrivacy規則およびカリフォルニア州で最近施行されたCCPAを調査することで同意の表現方法の参考とした。

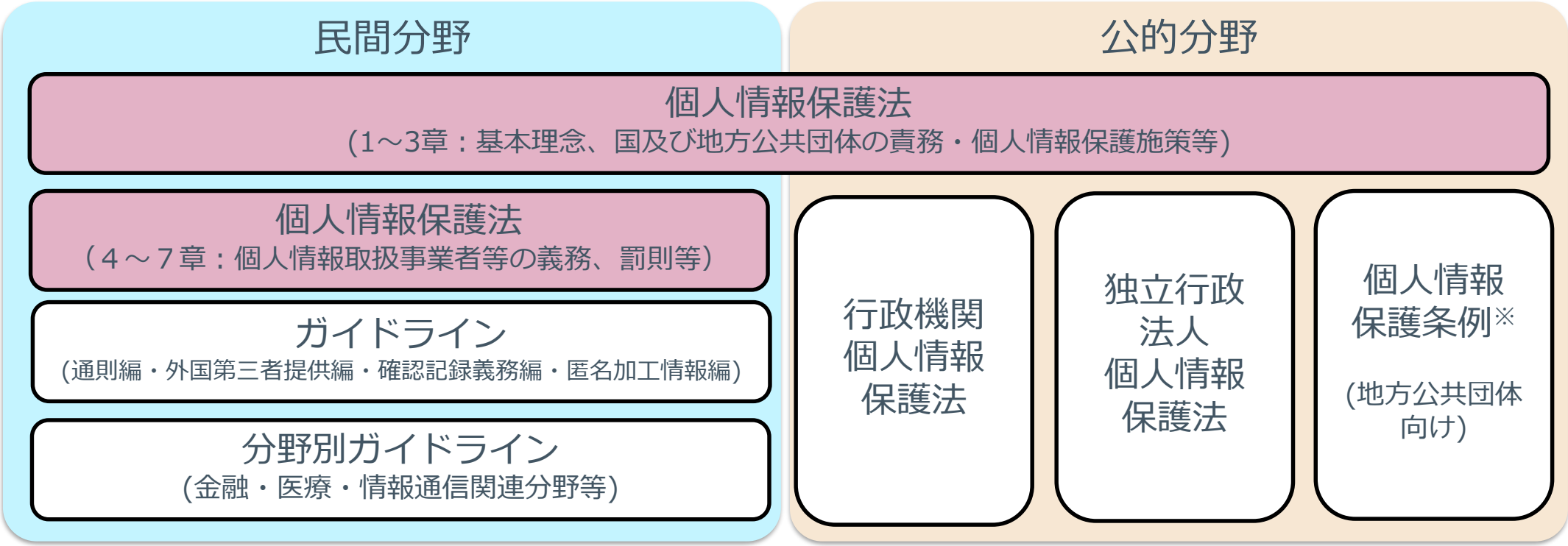
対象国・地域	法制度
欧州連合(EU)	• GDPR(General Data Protection Regulation：EU一般データ保護規則) • ePrivacy規則
カリフォルニア州 (アメリカ合衆国)	• CCPA(California Consumer Privacy Act：カリフォルニア州消費者プライバシー法)

- さらに、法制度だけではなく実際に構築された大規模なデータ利活用基盤における同意の表現方法の調査として、インドで政府主導で構築されてたデータ利活用のためのAPI基盤であるIndia Stackも調査対象とする。India Stackの中でも特にデータ保護のためのアーキテクチャであるDEPA(Data Empowerment and Protection Architecture)を中心に調査を実施した。

© NRI SecureTechnologies, Ltd.

個人情報保護法の法制度概要の概要を以下に示す。

- 個人情報の保護に関する法律(以下、個人情報保護法)は、個人情報の取り扱い方法を定めた法律であり、2003年5月に成立し2005年4月に施行された。
- 個人情報保護法は個人情報の保護に関する基本方針（1～3章）及び個人情報取扱業者等を対象とした義務、罰則（4～7章）から構成される。個人情報保護に関する法律・ガイドラインの体系上の位置づけは以下の通りとなる。



※個人情報保護条例の中には、公的分野における個人情報の取扱いに関する各種規定に加えて、事業者の一般的責務等に関する規定や、地方公共団体の施策への協力に関する規定等を設けているものもある。

参照元：https://www.ppc.go.jp/files/pdf/personal_framework.pdf

© NRI SecureTechnologies, Ltd.

個人情報保護法の法制度概要の概要を以下に示す。

- その後、情報通信技術の発展や事業活動のグローバル化等の急速な環境変化により、個人情報保護法が制定された当時は想定されなかったパーソナルデータの利活用が可能となったことを踏まえ、2015年9月に改正個人情報保護法が公布され2017年5月に施行された。主な変更点は以下の通り。
  - 個人情報取扱事業者の監督権限を個人情報保護委員会に一本化した。
  - 個人情報取扱事業者の対象として個人情報の件数が5,000人分以下の事業者（小規模取扱事業者）も含められた。
  - 個人情報の定義を明確化し、匿名加工情報については一定の規律の下での同意なしでの第三者への提供等の利活用が可能となった。
  - 個人情報の第三者提供に関する各種規則の追加を行った。

© NRI SecureTechnologies, Ltd.

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

© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

GDPR(General Data Protection Regulation : EU一般データ保護規則)の法制度の概要を以下に示す。

概要

- GDPRは欧州における個人データ保護規約であり、2018年5月より施行される。**企業の所在地に依らず欧州域内の居住者に関する個人データの収集/処理に際して順守すべきルールが規定**されており、違反すると多額の罰則金（最も重いケースでグローバル売上の4%または2,000万ユーロのどちらか高い方）を科される。
- GDPRの主なポイント
  - 個人データの収集/処理には本人による明示的な同意が必要。**同意はデータの利用目的ごとに個別に行われなければならず**、いつでも撤回可能でなければならない。
  - 個人データは本人による利用停止、データ削除やデータ持ち出しが任意に行えるようにしなければならない。
  - 個人データは目的に対して必要な最小の範囲/期間でしか取り扱ってはならず、同意の撤回や目的に照らし合わせて不要になった場合は速やかに削除しなければならない。
  - 事業者は個人データの管理責任者(DPO)を任命しなければならず、欧州各国当局の監督・指示に従わなければならない。
  - データ取扱い業務のリスクが高い場合は、データ保護の影響評価アセスメントを実施しなければならない。
  - データ漏えいが発生した場合は72時間以内に当局に報告しなければならない。

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

参照元：http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

© NRI SecureTechnologies, Ltd.

GDPR上では同意の定義および同意に関する要件が定められている。また16歳未満の子どもの場合の同意取得についても別途定められている。

GDPRにおける同意の定義(第4条より)

(11) データ主体の「同意」とは、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する。

同意の要件(第7条より)

#	要件	条文中の記載
1	同意の証明	取扱いが同意に基づく場合、管理者は、データ主体が自己の個人データの取扱いに同意していることを証明きるようにしなければならない。
2	目的別の同意取得	別の事項とも関係する書面上の宣言の中でデータ主体の同意が与えられる場合、その同意の要求は、別の事項と明確に区別でき、理解しやすく容易にアクセスできる方法で、明確かつ平易な文言を用いて、表示されなければならない。
3	同意の撤回	データ主体は、自己の同意を、いつでも、撤回する権利を有する。

子どもの同意に適用される用件（第8条）

- 16歳未満の子どもに対しての同意については、**その親権者の同意も与えられた場合のみ適法**となる。

© NRI SecureTechnologies, Ltd.

GDPRでは同意に関するガイドラインが作成されており、その中では同意についてより具体的な説明がされている。

- GDPRでは同意に関してのガイドラインとして「Guidelines on consent under Regulation 2016/679」が作成されている。特に以下の章で同意に関しての具体的な構成要素や条件が記載されている。
  - 第3章：Elements of valid consent (有効な同意の要素)
  - 第4章：Obtaining explicit consent (明示的な同意の取得)
  - 第5章：Additional conditions for obtaining valid consent (有効な同意を得るための追加的条件)

© NRI SecureTechnologies, Ltd.

ガイドラインでは有効な同意を構成する要素として4つの要素を挙げている。

- 同意に関するガイドラインの第3章に、以下の通り記載がある。

freely given (自由に与えられている)

- ✓ データ主体に同意する／しないの真の選択権があること。
- ✓ データ主体が同意を強制されたと感じる場合にはその同意は無効である。
- ✓ データ主体は不利益を被らずに同意拒否／撤回できる必要がある。

specific (特定されている)

- ✓ データ主体の同意が「一つ又は複数の特定の」目的に関係して与えられなければならず、またデータ主体はそれら個々に関して自由に選べること。

informed (説明を受けている)

- ✓ 同意の取得に先立ってデータ主体に情報を提供することは、データ主体による、情報に基づく意思決定を可能とし、何について承諾しているかを理解できるようにし、また、たとえば同意を撤回する権利を行使できるようにするために不可欠である。

unambigious indication of wishes (不明瞭でない意思表示)

- ✓ 同意は常に積極的な行動又は宣言によって与えられなければならない。（例：あらかじめチェックの入った同意のチェックボックスは無効。）
- ✓ 同意が、契約書に合意すること又はサービスの一般的な条件を承諾することと同じ行為によっては得られない。

© NRI SecureTechnologies, Ltd.

同意を構成する要素の1つであるfreely given(自由に与えられている)を阻害する要素として4つの点が挙げられている。

imbalance of power (力の不均衡)

- 公的機関や雇用主などが管理者の場合にデータ主体と関係に力の不均衡がある。

conditionality (条件性)

- 契約の条件とサービス提供に必要ではない個人データ取り扱いの同意を抱き合わせる。

guranularity (粒度)

- 複数の目的をひとまとめにして同意を取ろうとする 。(目的ごとに同意する/しないの選択ができない。)

detriment (不利益)

- 同意の拒否や撤回をすることで不利益を得る。（例：サービスのグレードが下がる等。）

© NRI SecureTechnologies, Ltd.

ガイドライン上では、同意がinformed(説明を受けている)を満たすために必要最小限の要件が定義されている。

- ガイドラインにおける「3.3.1.　同意が「説明を受けた」うえでのものとなる最小限の内容の要件」より、同意が説明を受けたものとなるためには以下の情報が必要と記載している。

#	情報	備考
1	管理者の身元	
2	同意が求められるそれぞれの取扱業務の目的	
3	収集され利用されるデータ（そのタイプ）	
4	同意を撤回する権利の存在	
5	関連する場合、第 22 条(2)(c)に従い自動化された意思決定のためのデータ利用についての情報	GDPRの第22条(2)(c)では、データ主体の明示的な同意がある場合には、自動化された意思決定を行ってもよいと記載
6	十分性認定及び第 46 条で述べられる適切な保護措置がないことによるデータ移転の起こりうるリスクについて	GDPRの第46条は適切な保護措置に従った移転について記載

© NRI SecureTechnologies, Ltd.

ガイドライン上では、明示的な同意が必要とされるケースおよび同意の取得するために必要な内容の例をまとめており、医療データも明示的な同意が必要なケースとなる。

- ガイドラインの第4章では明示的な同意が必要なケースを「重大なデータ保護のリスクが出現する状況」と記載しており、具体的な例として以下の3つを挙げている。その中には医療データも含まれる。

GDPR中の記載箇所	ケース
第9条	特別な種類のデータの取扱い (人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、**遺伝子データ**、自然人を一意に識別することを目的とする生体データ、**健康に関するデータ**、又は、自然人の性生活若しくは性的指向に関するデータ)
第49条	十分な保護措置を持たない第三国又は国際組織へのデータ移転
第22条	プロファイリングを含む個人に対する自動化された意思決定

- 明示的な同意を取得するために管理者が実施すべき内容の例について以下の通り記載されている。
  - データ主体による署名のある書面による声明。
  - 電子的な書式へ書き込みに、データ主体の署名付きスキャン文書もしくは電子署名を加える。
  - 選択についての情報が公正、明瞭かつ明白であり、また、データ主体からの明確な確認を求めるものである場合における（たとえば、ボタンを押すこと又は口頭の確認を行うこと）電話での会話を通しての陳述。
  - 二段階の同意
    - 例：管理者が特定目的のための特定情報の利用について同意を求めることをeメールで説明し、データ主体は承諾する旨をメールで返信し、さらにその承諾を証明するために追加で証明用のリンクをクリックもしくはSMSで受け取った証明コードを入力する。

© NRI SecureTechnologies, Ltd.

ガイドライン上では、有効な同意を得るための追加条件として同意の証明と同意の撤回の2つが挙げられている。

同意の証明

- 同意の証明についてはGDPRの第7条で記載されているが、具体的な手法については定義されていない。本ガイドラインでも具体的な手法ではなくいくつかの事例の提示のみにとどまっている。
  - 管理者がデータ主体から受け取った同意の陳述を記録。
  - オンラインの場合はセッション時の同意作業の文書化、同意が表明されたセッションに関する情報およびデータ主体に提供した情報の写しの保存。
- 同意の証明のために十分なデータは保持すべきだが、必要以上に多くの情報を収集すべきではない。
- 該当するデータ取り扱い期間中は同意を証明できなければならない。取扱期間が終了した後は同意の証拠も保持されるべきではないが、法的義務の順守や訴訟の提起、攻撃防御のために必要な同意の証拠は保持されるべき。

同意の撤回

- GDPRの第7条では「同意の撤回が、同意を与えた時と同様に簡単またはいつでも可能であることを確保しなければならない」と記載があるが、ガイドラインではさらに具体例として、電子的手段を用いる場合は同意の取得時と同じユーザインタフェースを用いて同意の撤回もできるべきと記載している。
  - 例：電子メールで同意取得する場合は、同意の撤回も電子メールで実施できるべき。
- 管理者はデータ主体に同意を求める前に、同意撤回の権利に関する情報をデータ主体に提供しなければならない。

© NRI SecureTechnologies, Ltd.

ePrivacy規則の法制度の概要を以下に示す。

- ePrivacy規則は電子通信におけるプライバシー保護のための規制である。EUにて2017年1月に提案され、その後何度か修正案が公表されているが、2020年5月時点ではまだ採択プロセス中である。

- ePrivacy規則の概要
  - 対象事業者：インターネット事業者
  - 対象データ：通信コンテンツとメタデータ（例えば、通話時間と場所）のプライバシーが保証される。メタデータは高いプライバシー要素を持ち、課金にデータが必要でない限り、ユーザーが同意しなかった場合には匿名化または削除する。
  - クッキーに関するルール：クッキーの提供により、インターネットユーザーの同意の要求が合理化。ブラウザの設定では、Cookieやその他の識別子のトラッキングを簡単に許可または拒否できるため。.
  - 新しいビジネスチャンス：従来の通信事業者は、処理される通信データ（コンテンツおよび/またはメタデータ）の処理に一度同意すると、追加のサービスを提供し、ビジネスを開発する機会が増える。
  - 迷惑メールからの保護：電子メール、SMS、自動発信機による迷惑な電子通信を禁止。国によって、デフォルトNGであったり、ユーザの反応によってはOKをNGに変更するなどの方式に差あり。

EUROPEAN COMMISSION
Press Release Database

European Commission › Press releases database › Press Release details

Latest updates | Related links | Contact | Search | Login | Subscribe

Other available languages: FR DE DA ES NL IT SV PT FI EL CS ET HU LT LV MT PL SK SL BG RO HR

Back to the search results | Expand | Share | PDF

European Commission - Press release

Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions

Brussels, 10 January 2017

The Commission is proposing new legislation to ensure stronger privacy in electronic communications, while opening up new business opportunities.

The measures presented today aim to update current rules, extending their scope to all electronic communication providers. They also aim to create new possibilities to process communication data and reinforce trust and security in the Digital Single Market – a key objective of the Digital Single Market strategy. At the same time, the proposal aligns the rules for electronic communications with the new world-class standards of the EU's General Data Protection Regulation. The Commission is also proposing new rules to ensure that when personal data are handled by EU institutions and bodies privacy is protected in the same way as it is in Member States under the General Data Protection Regulation, as well as setting out a strategic approach to the issues concerning international transfers of personal data.

First Vice-President **Timmermans** said: *"Our proposals will complete the EU data protection framework. They will ensure that the privacy of electronic communications is protected by up to date and effective rules, and that European institutions will apply the same high standards that we expect from our Member States."*

Andrus **Ansip**, Vice-President for the Digital Single Market said: *"Our proposals will deliver the trust in the Digital Single Market that people expect. I want to ensure confidentiality of electronic communications and privacy. Our draft ePrivacy Regulation strikes the right balance: it provides a high level of protection for consumers, while allowing businesses to innovate."*

Věra **Jourová**, Commissioner for Justice, Consumers and Gender Equality said: *"The European data protection legislation adopted last year sets high standards for the benefit of both EU citizens and companies. Today we are also setting out our strategy to facilitate international data exchanges in the global digital economy and promote high data protection standards worldwide."*

Better online protection and new business opportunities

The proposed Regulation on Privacy and Electronic Communications will increase the protection of people's private life and open up new opportunities for business:

- **New players:** 92% of Europeans say it is important that their emails and online messages remain confidential. However, the current ePrivacy Directive only applies to traditional telecoms operators. Privacy rules will now also cover new providers of electronic communications services, such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber.
- **Stronger rules:** By updating the current Directive with a directly applicable Regulation, all people and businesses in the EU will enjoy the same level of protection for their electronic communications.Businesses will also benefit from one single set of rules across the EU.

Documents
- ePrivacy Factsheet.pdf
- international transfert data Factsheet.pdf
- data_protection_regulation-09 revised.pdf

参照元：http://europa.eu/rapid/press-release_IP-17-16_en.htm

© NRI SecureTechnologies, Ltd.

ePrivacy規則では、同意に関する規定はGDPRの規則が適用される。

- ePrivacy規則(2018年10月の修正案)では、第4a条で同意について記載されており、その中の第1項で同意に関する規定はGDPRの規則が適応されることが記載されている。
- 第4a条では、他にユーザ端末上のデータや通信データの処理に関しての同意について記載されている。

項	記載内容
第1項	GDPRの規則中における同意の規定は個人、そして必要な変更を加えて法人に適用される。
第2項	第8条(1)の(b)(ユーザ端末からの情報の処理、蓄積に関する同意)に関して、同意はインターネット中の情報を検索そして表示といった電子通信を許可するソフトウェアの適切な技術的設定を使い表現することができる。
第3項	第6条(2)の(c)(通信メタデータの処理)や第6条(3)の(a)もしくは(b)(通信コンテンツの処理)に関してエンドユーザが同意を与えた場合は、少なくとも12か月ごとに同意が撤回できることのリマインドをされること。

© NRI SecureTechnologies, Ltd.

CCPA(California Consumer Privacy Act：カリフォルニア州消費者プライバシー法)の法制度の概要を以下に示す。

- CCPAはカリフォルニア州民の個人情報保護を目的とした法律で、2020年1月に施行。

- CCPAの主なポイント
  - 以下の条件を満たす事業者がCCPAの対象となる。

✓ カリフォルニア州で営利目的の事業を行っている
✓ カリフォルニア州民の個人情報を収集または処理している

＋

以下のいずれかに該当

✓ 年間総売上が2,500万ドル以上
✓ 年間5万件以上のカリフォルニア州の消費者のデータを購入・取得・販売している
✓ カリフォルニア州の消費者データを販売することで売上の50%以上を得ている

  - カリフォルニアに在住している消費者および従業員がCCPAの保護対象であり、事業者が持つ従業員の情報（求職者の情報、従業員の緊急連絡先等）も保護対象となる。
  - 個人だけでなく、世帯の情報も対象となる。
  - 個人データの第三者提供については、個人情報保護法やGDPRが本人の事前同意（オプトイン）を求めているのに対し、CCPAは消費者から提供停止の要請があった場合に対応（オプトアウト）することを求めている。
  - 事業者は、消費者からの開示・削除等の問い合わせがあった場合（直近12カ月の期間に収集、販売、処理された情報が対象）、45日以内に対応することが求められる。
  - 違反があった場合、消費者からの請求1件あたり最大2,500ドル（故意による違反の場合、最大7,500ドル）の罰金が科せられる。

© NRI SecureTechnologies, Ltd.

CCPAでは、個人データの第三者提供時における要求事項は個人情報保護法やGDPRとは異なっている。

- CCPAでは個人データの第三者提供においては、個人情報保護法やGDPRのように事業者に事前の同意(オプトイン)を求めるのではなく、消費者による提供停止の要求(オプトアウト)への対応を求めている。

法制度	第三者提供時の同意方式
個人情報保護法	オプトイン、オプトアウト(届出制)
GDPR	オプトイン
CCPA	**オプトアウト**

  - 個人情報保護法でもオプトアウト方式での個人データの第三者提供については第23条第2項で定義されている。条文ではオプトアウト方式での第三者提供を行う事業者は事前に個人情報保護委員会への届出が必要と記載されている。

- 具体的なCCPAでの個人データの第三者提供において求められる事項は以下の通り。
  - プライバシーポリシーに提供する個人データの種類を開示。
  - 消費者が自身の個人データの第三者提供を停止するためのリンク(“Do Not Sell My Personal Information”リンク)をウェブページに公開する。

- ただし、16歳未満の子どもの個人データについては以下の通り事前の同意(オプトイン)が求められる。

対象の年齢	必要な同意
16歳未満13歳以上	本人の同意
13歳未満	親権者、保護者の同意

© NRI SecureTechnologies, Ltd.

India Stackの概要を以下に示す。

- India Stackは、インド政府の主導により構築された複数のオープンAPIから成るデータ利活用基盤である。
- インド政府が2015年に始めたデジタル化政策であるDigital India実現のための基盤であり、これらの基盤を政府／企業／スタートアップ／開発者に広く利用してもらうことで各種ビジネスや手続きの非対面化、ペーパーレス化、キャッシュレス化を推進することを目的としている。
- India Stackを構成する主要な機能として以下の５つが存在する。

#	機能	説明
1	Aadhaar	Aadhaarはインドにおける国民識別番号制度の名称。すでに10億人以上のインド国民に対してAadhaar番号が発行されている。Aadhaarでは個人情報の他に指紋や光彩といった生体情報も一緒に登録されており、IndiaStackではAadhaarを利用した個人認証のためのAPIを提供する。
2	eKYC	Aadhaar認証を通して、電子的に身元確認(Know Your Customer : KYC)を行うためのAPIを提供する。
3	eSign	電子ドキュメントへの電子署名を行うためのAPIを提供する。署名者の身元確認にeKYCを利用する。
4	DigiLocker	電子的な文書や証明書の発行、検証、保管のためのプラットフォームである。インド国民にAadahaar番号に紐づくクラウド上のストレージスペースが用意され、そこで電子文書/証明書を保管する。紙の文書/証明書をスキャンしてeSignで署名の上アップロードすることも可能。
5	UPI	Unified Payment Interfaceの略であり、銀行口座保有者間での送金処理などのキャッシュレス決裁を行うためのAPIを提供する。

参照元：https://www.indiastack.org/

© NRI SecureTechnologies, Ltd.

IndiaStackは4つのレイヤーから構成されており、同意についてもそれ単独で1つのレイヤーを構成している。

- IndiaStackを構成するレイヤー(階層)は以下の通り。

#	レイヤー	説明	対応する機能
1	Presenceless Layer （非対面レイヤー）	デジタル化された生体情報に基づく個人識別により、インド国内のどこにいても本人確認を行うことが可能	Aadhaar認証
2	Paper-less Layer （ペーパーレスレイヤー）	個人に紐づく各種電子記録を扱うことができる機能を提供することにより、紙による手続き、保管を減らす	eKYC、eSign、DigiLocker
3	Cashless Layer （キャッシュレスレイヤー）	電子的な支払いや口座間取引のインタフェースを統一することでキャッシュレス経済を実現する	UPI,AEPS(Aadhaar Enabled Payment System), APB(Aadhaar Payments Bridge)
4	Consent Layer （同意レイヤー）	個人データのやり取りを自由に、かつセキュアに実施するためのフレームワークを提供する。	DigiLocker, **DEPA(Data Empowerment and Protection Architecture)**

- 同意に関するConsent Layerを実現するための機能の1つとして、DEPA(Data Empowerment and Protection Architecture)と呼ばれるアーキテクチャが存在する。

参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

© NRI SecureTechnologies, Ltd.

DEPA(Data Empowerment and Protection Architecture)概要および対象とするデータ種別を以下に示す。

- DEPAは「個人からデータ収集時の同意」および「収集したデータの第三者への共有時の同意」を実現するために利用されるツール及びユーティリティであり、大きく以下の3つの機能から構成される。
  - eKYC
  - DigiLocker
  - EDC (Electric Data Consent)
- 上記の3つのツールのうちEDCが同意取得処理において使用される最も主要なツールである。
- EDCにおける同意取得の対象となるデータ種別は以下の赤色部分で記載された3つの種別となる。

データ種別	Non Sharable (共有不可)	Personal Data (個人情報)	Generated Data (生成されたデータ)	Derived(Intelligence) (派生データ)	Anonymous Dataset (匿名化されたデータセット)	Public Dataset (公共のデータセット)
データ例	生体情報	KYC関連情報, 運転免許証	位置情報, 銀行取引履歴	個人に最適化されたキーボード辞書, クレジットスコア	匿名化された	data.gov.inで公開されているデータ
ユーザ同意	–	必要	必要	必要	–	–
下流への共有	–	制限あり (Limited)	制限あり (restricted)	禁止 (Barred)	禁止 (Barred)	–
規制者	法による規制	無償での共有 or 価格規制	無償での共有 or 価格規制	市場価格次第	市場価格次第	法による規制
取扱時に使用されるツールおよび規格	生体情報セキュリティ	eKYC, DigiLocker, Electric Data Consent (EDC)	Electric Data Consent (EDC)	Electric Data Consent (EDC)	匿名化に関する各種規格	オープンデータに関する各種規格

参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

© NRI SecureTechnologies, Ltd.

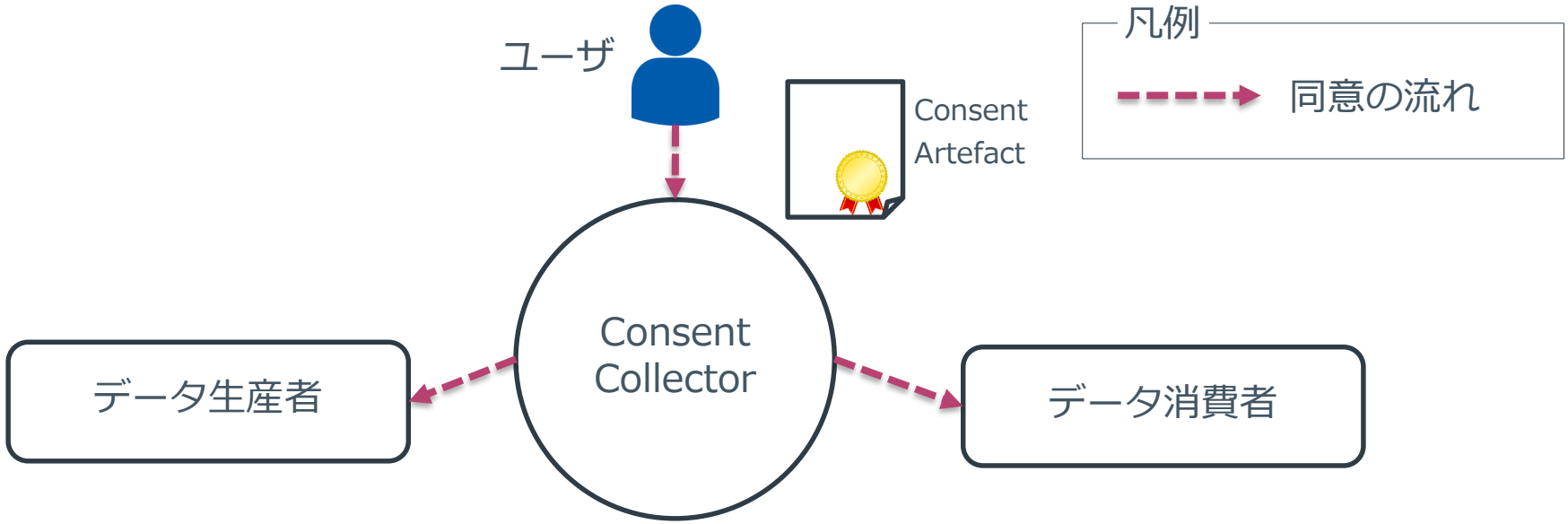
EDCにおいては、Consent Collectorと呼ばれる機能がユーザ・データ生産者・データ消費者の間に入ってデータ提供における同意処理を制御する。

- EDCでは、Consent Collectorと呼ばれる機能が以下の3者の間に入り、ユーザが与えた同意に基づく処理を制御する。

項目	説明
ユーザ	同意を与える対象のデータの所有者
データ生産者	ユーザデータを生産・所有する者
データ消費者	ユーザデータを利用してサービスを提供する者

  - 例：「ある金融会社がユーザへのローンを許可するかどうか判断するために銀行口座情報を参照する」ケースの場合、銀行がデータ生産者（ユーザの銀行口座情報を扱う）、金融会社がデータ消費者となり、ユーザが銀行口座情報参照同意を与えることとなる。

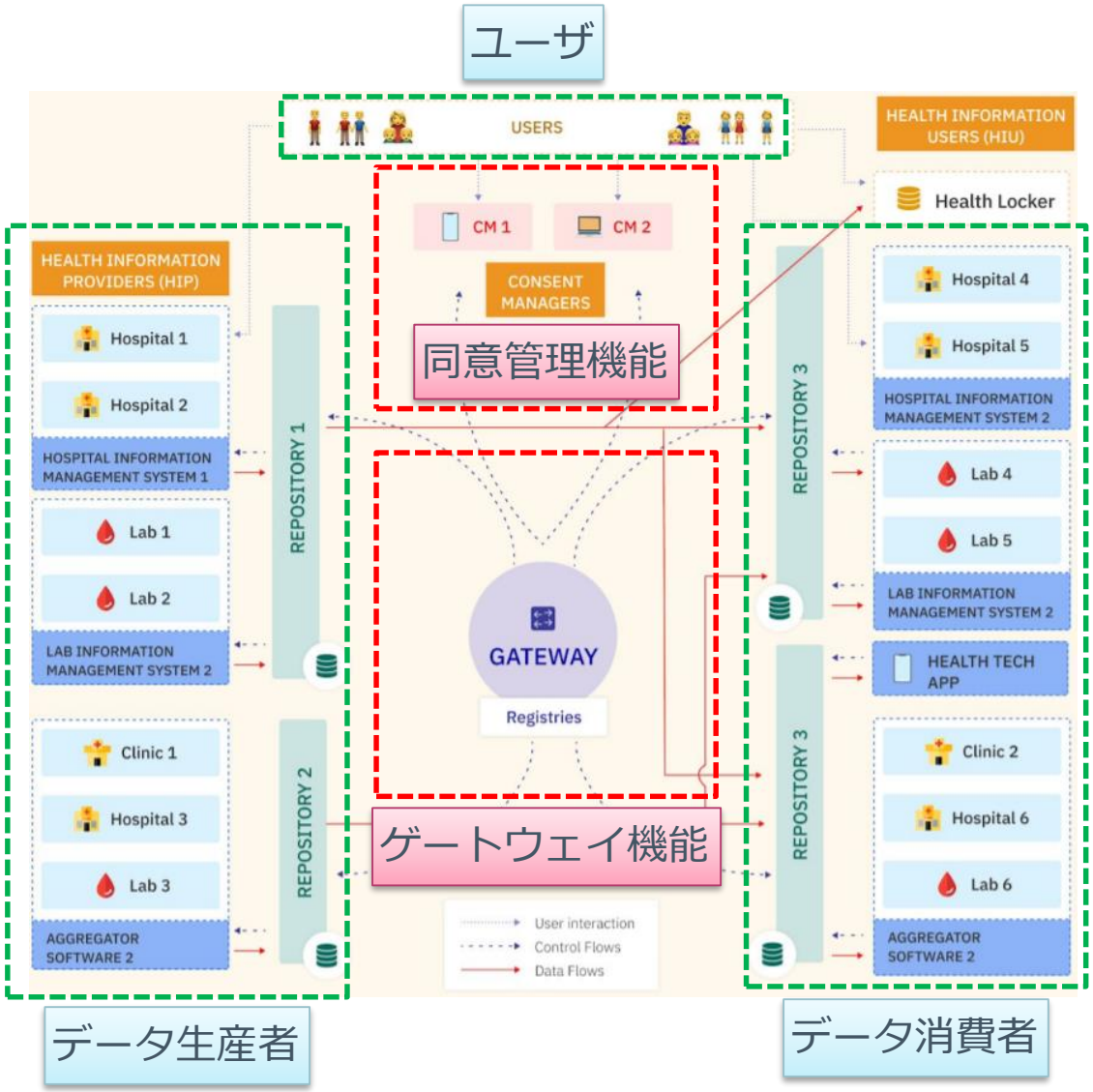
- 同意情報は**Consent Artefactと呼ばれる電子署名付きのXML形式ファイル**で表現される。



参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

© NRI SecureTechnologies, Ltd.

Consent Collectorはデータ生産者と消費者をつなぐゲートウェイ機能とユーザの同意管理機能から構成される。



- 左記の図は医療向けの同意管理であるHealth Information Flowに関する図である。左図におけるConsent Controllerは以下の2つの機能から構成される。
- **ゲートウェイ機能**
  - データ生産者、データ消費者および同意管理機能の間に入り、データおよび同意情報のやり取りを行う。
  - データ生産者、データ消費者および同意管理機能それぞれに向けたAPIを用意しており、データのやり取りはそのAPIを通して行う。
- **同意管理機能**
  - データ生産者が持つユーザデータのうち、管理対象となるデータを管理する。
    - 実際のデータはデータ生産者側で保存されており、同意管理機能側ではその情報のラベル情報のみ記録。
  - データ消費者側からユーザデータへのアクセス要求があった場合に、ユーザに通知する。
    - ユーザはWebアプリやスマホアプリで同意する／しないを選択する。
  - ユーザからの同意取り消しをゲートウェイ機能を通してデータ生産者やデータ消費者に送信する。

参照元：https://www.slideshare.net/ProductNation/health-information-flows-technical-standards-v-05

© NRI SecureTechnologies, Ltd.

Consent Artefactを通して、ユーザ同意情報に対象データや提供期間の他に様々な要素を表現することが可能となる。

- Consent ArtefactはXML形式で以下のデータ構成をとっており、同意に関する様々な情報を表現することが可能である。
  （以下はMeitY(インド電子情報技術局)におけるConsent Artefact形式の例）

```
<consentcollector> CC </consentcollector>
<dataconsumer> DC </dataconsumer>
<dataproducer> DP </dataproducer>

<user type="UID"> 123412341ABC </user>
```

Identifier Section

同意の対象となるユーザ、データ生産者およびデータ消費者の情報

```
<datatype type="transactional">
    <attribute-list> … </attribute-list>
    <duration> 6 months </duration>
    <datalife> 10 days </datalife>
    <frequency> YEARLY </frequency>
    <revocable> YES </revocable>
    <access> VIEW| STORE| QUERY </access>
</datatype>

<datatype type="profile"> </datatype>
```

Data Section

同意対象データに関する情報
- 具体的な属性名
- 同意期間
- データの有効期間
- 同意破棄の可否
- データアクセス種別

```
<loggingInfo> … </loggingInfo>

<purpose code=""> LOAN </purpose>

<signature> #@%%#@$$##$@  </signature>
```

Logging Section — ログ出力(監査時に利用)

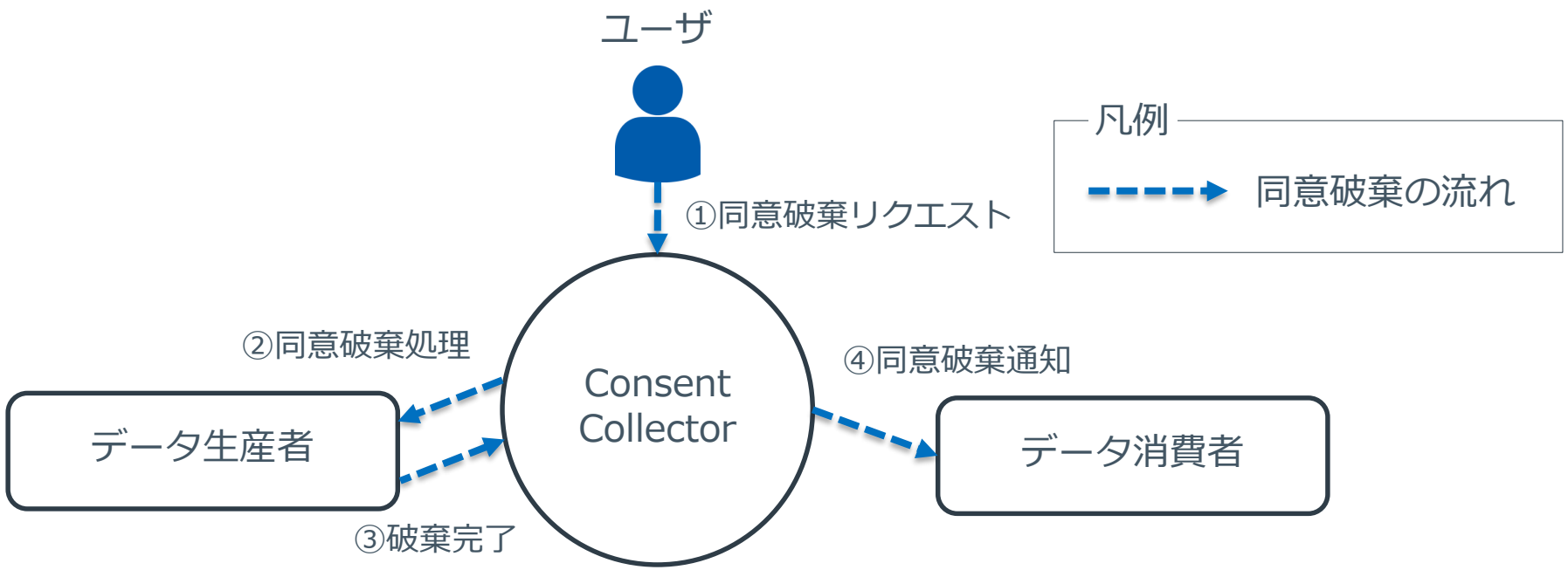
Purpose of Data Access — データアクセスの目的

Signature Section — 電子署名

© NRI SecureTechnologies, Ltd.
参照元：https://www.slideshare.net/ProductNation/data-empowerment-protection-architecture-depa

Consent Artefactを用いることで、同意の破棄や監査といったことも可能となる。

- EDCでは、Consent Collectorを仲介して一度与えた同意の破棄の仕組みも備えている。



- Consent Artefactではロギング(ログ出力)の指定も可能であり、出力されたログ情報を用いた監査も可能である。

© NRI SecureTechnologies, Ltd.
参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

EDCを使ったデータ提供同意のユースケースを以下に示す。

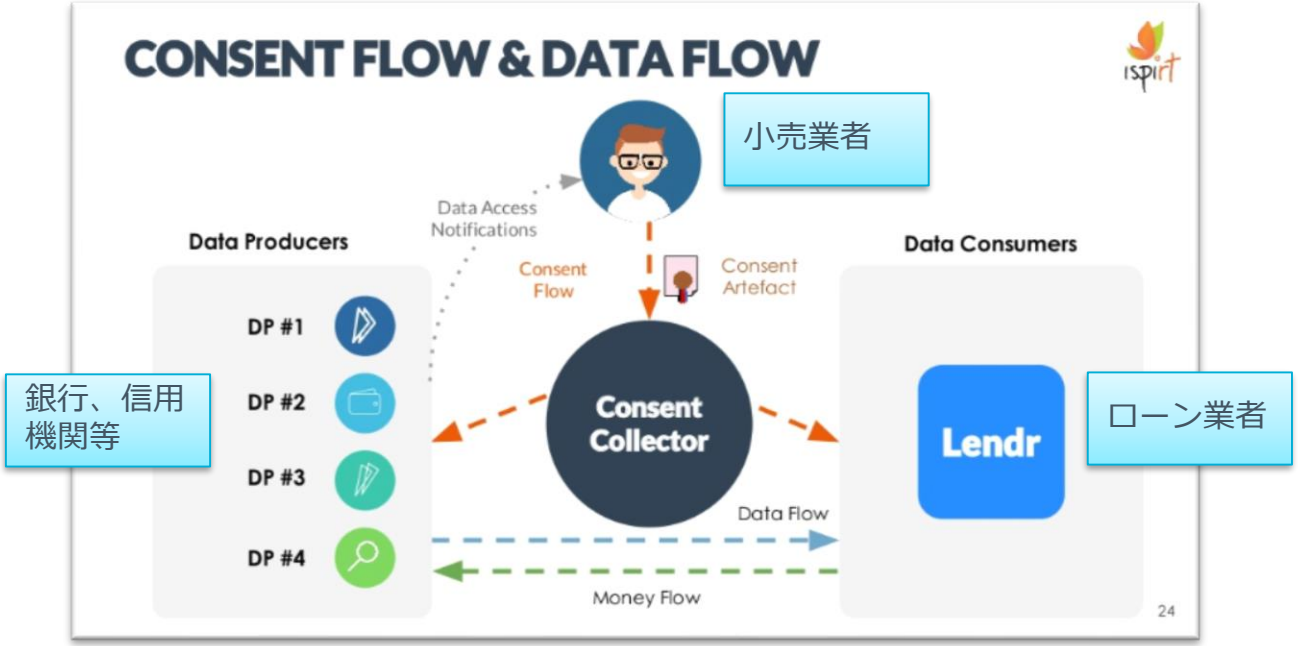
EDCを使ったデータ提供同意のユースケース

① ある小売業者がローンを借りるにあたり、ローン業者に向けて自分の銀行口座情報などのローン審査に必要な情報へのアクセスを許可する

② ある患者が医療機関で診察してもらうにあたり、医療機関に対して自分の過去の診断結果情報へのアクセスを許可

③ ある農業従事者が今後の農家向けサービス改善のために、政府農業機関、銀行、保険会社および農業用品製造業者などに農作業において生成される各種データ（農地の位置・サイズ、土壌データ、収穫時期・量など）へのアクセスを許可

① 小売業者がローンを借りる際の情報提供同意

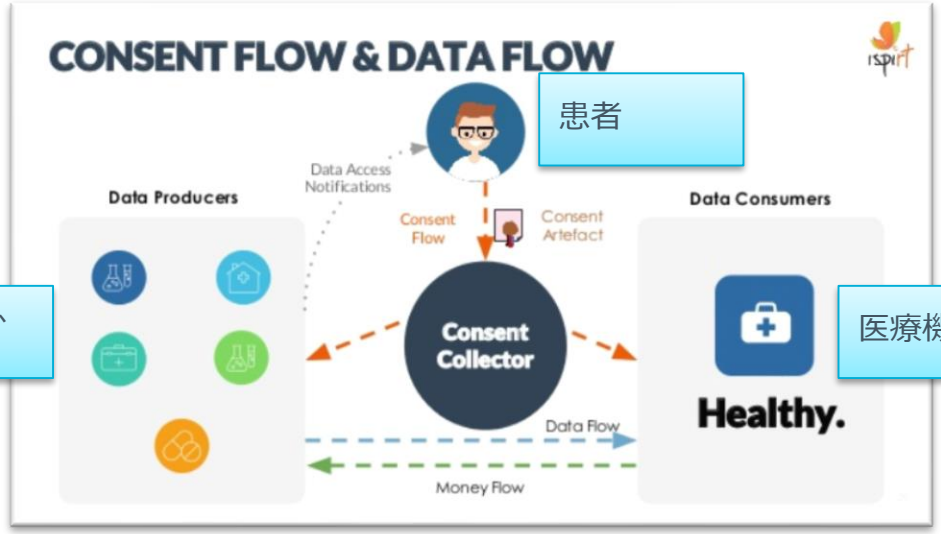


参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

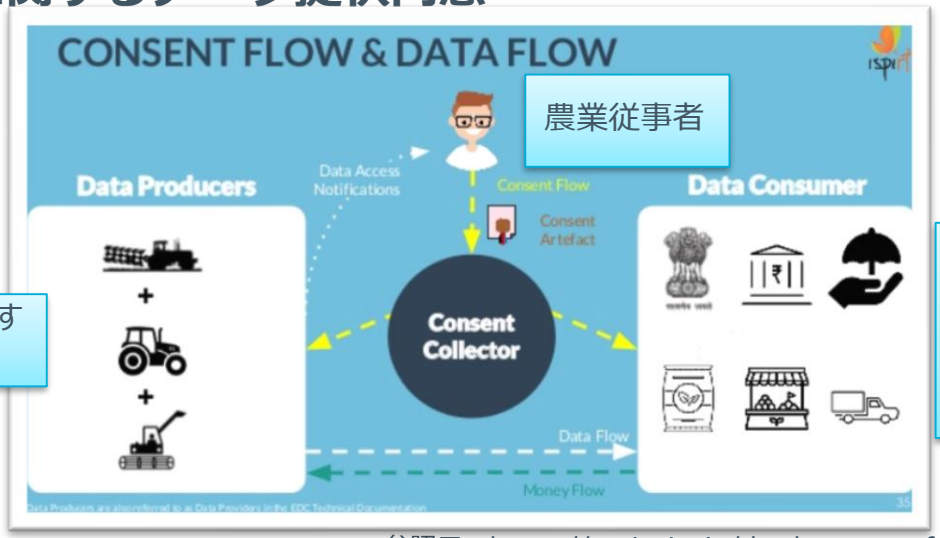
© NRI SecureTechnologies, Ltd.

EDCを使ったデータ提供同意のユースケースを以下に示す。

② 患者が医療機関に受診する際の診察結果情報提供同意



③ 農業従事者が農作業に関するデータ提供同意



・政府農業機関
・銀行
・保険会社
・農業用品製造業者

参照元：https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/

© NRI SecureTechnologies, Ltd.

実在するサービスにおける個人情報収集や第三者提供の際の同意取得シナリオと法制度における同意取得規定の関連をサービスの公開情報を基に整理する。

- 実在するサービスとして以下のサービス・アプリケーションについて個人情報の収集および第三者提供における同意方法の調査を実施した。

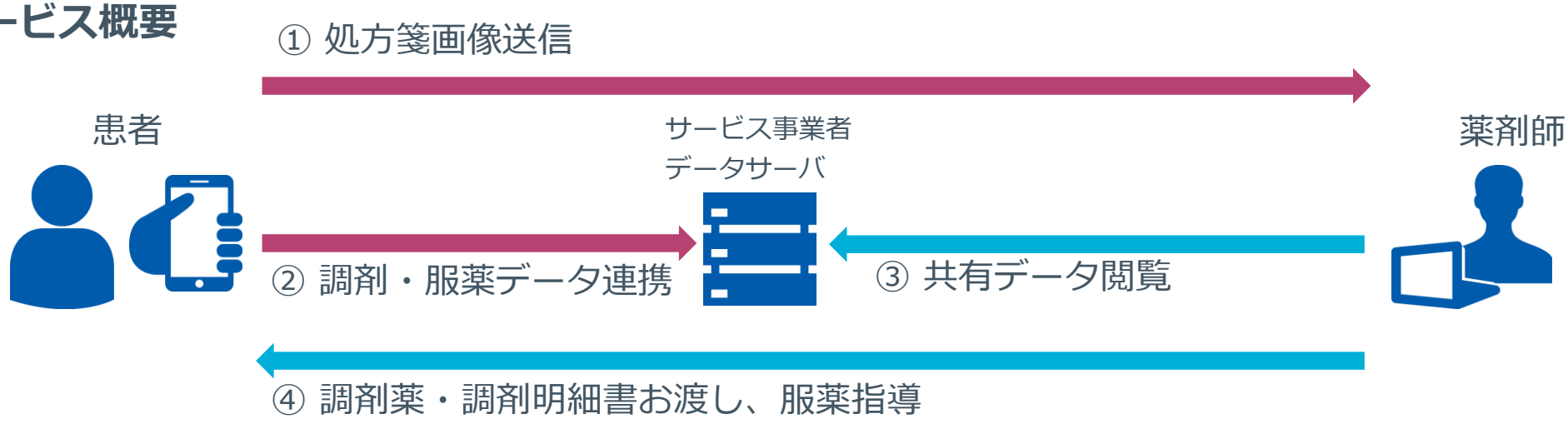
No.	サービス名	サービス概要
1	お薬手帳アプリケーション	患者向けにスマートフォン上で調剤情報や服薬情報を管理することができるアプリケーションを提供する。保存された情報は薬局側も患者の同意のもと服薬情報を参照し服薬指導に役立てることができる。
2	女性向け体調管理サービス	女性向けに基礎体温や生理日の情報を入力することで体調管理を行うサービスを提供する。保存された情報は利用者の同意のもと提携する婦人科の医師が参照し診断に役立てることができる。
3	SNSサービスの個人情報連携	SNSサービスが連携するサービス向けに、ユーザの属性情報（氏名、住所、電話番号等）をAPIを通して連携する。
4	銀行の取引情報サービス連携	銀行が提携先企業向けに、ユーザの取引情報（口座残高情報や入出金情報など）をAPIを通して連携する。

- 調査方法としては、各サービス・アプリケーションにおいてマニュアルやFAQなどの一般に公開されている情報を基にした机上調査を実施した。

© NRI SecureTechnologies, Ltd.

事例調査１：お薬手帳アプリケーション

サービス概要



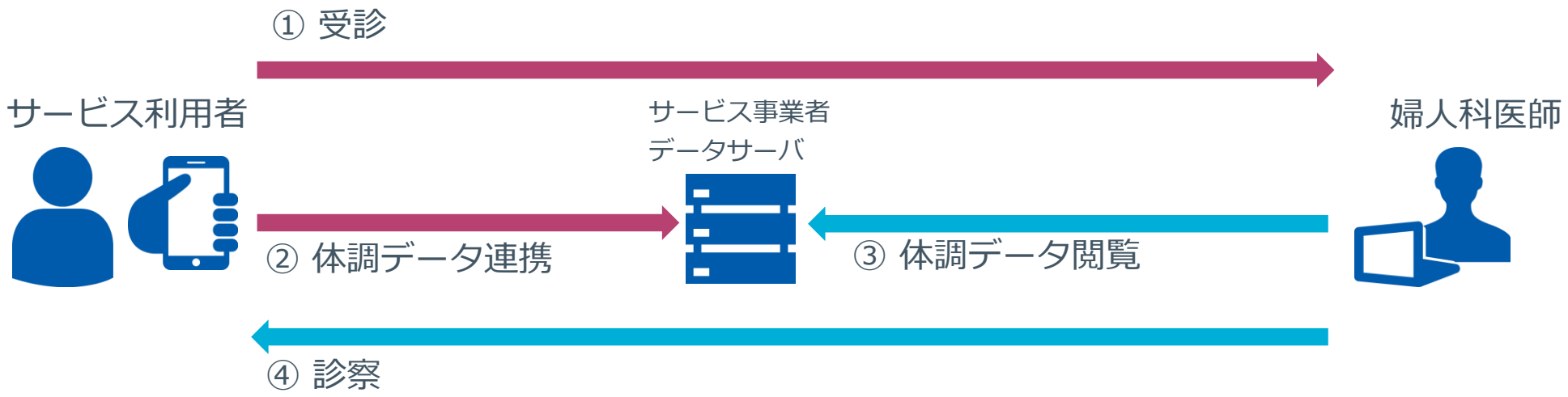
同意取得方法

- 「③共有データ閲覧」において患者が薬剤師に対して自分の調剤・服薬データを閲覧することへの同意を与える必要がある。
- 本サービスでは患者が薬剤師に共有データを閲覧させる際に**アプリケーションから発行されるワンタイムコードを直接薬剤師に伝える**必要があり、患者が自主的にワンタイムパスワード発行および薬剤師への通知を行う行為を通して個人情報保護法の第二十三条に記載の「個人データ提供における同意」を与えている。

© NRI SecureTechnologies, Ltd.

事例調査２：女性向け体調管理サービス

サービス概要（婦人科受診サポート機能）



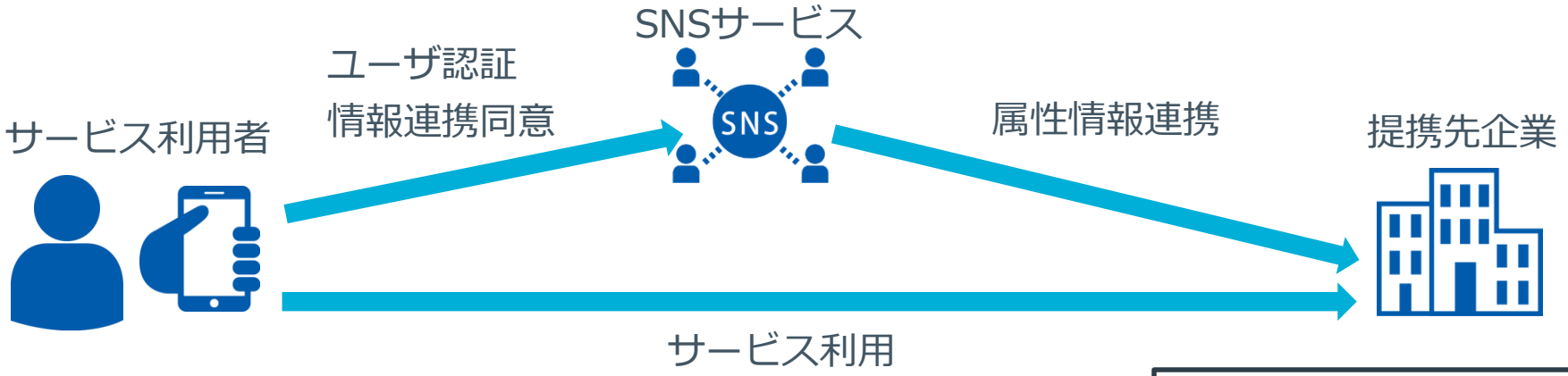
同意取得方法

- 「③体調データ閲覧」においてサービス利用者が婦人科医師に対して自分の体調データを閲覧することへの同意を与える必要がある。
- 本サービスではサービス利用者が婦人科医師に共有データを閲覧させる際に**アプリケーションから発行される6桁のデータ番号を直接婦人科医師に伝える**必要があり、サービス利用者が自主的にワンタイムパスワード発行および婦人科医師への通知を行う行為を通して個人情報保護法の第二十三条に記載の「個人データ提供における同意」を与えている。

© NRI SecureTechnologies, Ltd.

事例調査３：SNSサービスの個人情報連携

サービス概要（取引情報サービス連携）



同意取得方法

- 提携先企業のサービスがそのユーザの属性情報をAPI経由で取得する前に、サービス利用者は自分の属性情報をそのサービスに提供する同意を与える必要がある。
- SNSサービス側が表示する同意確認画面では、提携先企業に連携を許可する情報と同意ボタンが表示される。ユーザは同意内容を確認した上で同意ボタンをクリックする行為を通して個人情報保護法の第二十三条に記載の「個人データ提供における同意」を与えている。

情報提供先のサービス

XXXサービス

提供する情報

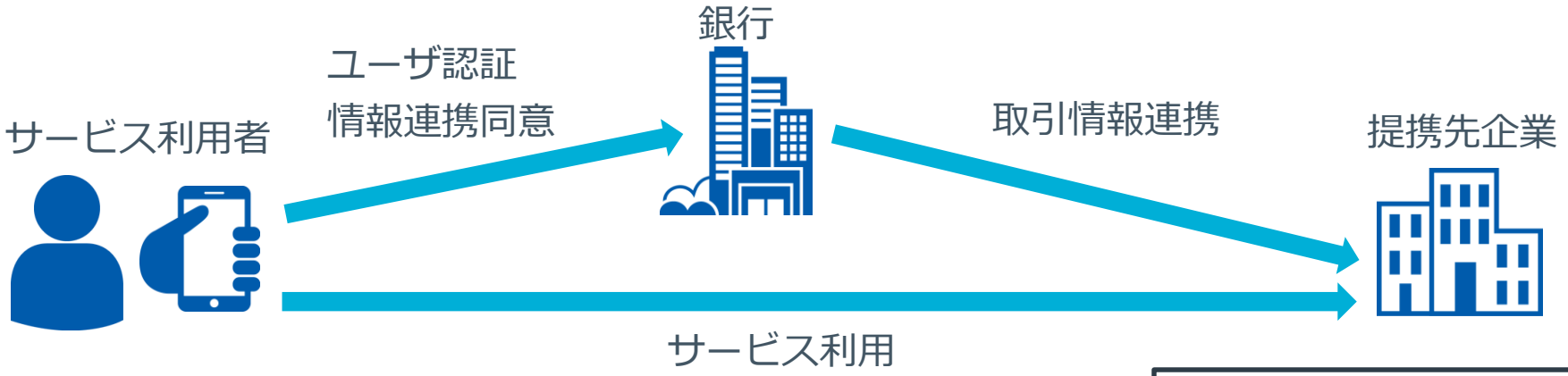
・ユーザ識別子
・姓名、年齢、性別
・メールアドレス

同意しません　同意します

© NRI SecureTechnologies, Ltd.

事例調査４：銀行の取引情報サービス連携

サービス概要（取引情報サービス連携）



同意取得方法

- 提携先企業のサービスがそのユーザの銀行取引情報をAPI経由で取得する前に、サービス利用者は自分の取引情報をそのサービスに提供する同意を与える必要がある。
- 銀行側が表示する同意確認画面では、提携先企業に連携を許可する情報・サービスと同意確認のためのチェックボックスが表示される。ユーザは同意内容を確認した上でチェックボックスにチェックする行為を通して個人情報保護法の第二十三条に記載の「個人データ提供における同意」を与えている。

アクセス許可対象

・残高照会
・入出金明細照会

同意確認

上記の情報へのアクセスを提携先に提供することに同意します。
・・・

☐ 確認しました

同意しません　同意します

© NRI SecureTechnologies, Ltd.

8. おわりに

© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

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。

© NRI SecureTechnologies, Ltd.

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

© NRI SecureTechnologies, Ltd.

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

© NRI SecureTechnologies, Ltd.

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 SecureTechnologies, Ltd.

NRI SECURE