野村総合研究所

利用者認証に関する調査・研究事業一式

～最終報告資料～

2018年09月28日

株式会社野村総合研究所

〒100-0004
東京都千代田区大手町1-9-2 大手町フィナンシャルシティ グランキューブ

最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

本事業は、データヘルス各サービス及び全国保健医療情報ネットワークにおける個人認証方式を検討するための参考情報をとりまとめることを目的とする

■ 背景

世界に先駆けて超高齢化社会に直面する日本では、「国民一人一人の健康寿命を延伸」と「良質で安心なサービスの提供」への実行的な施策の実施が急務となっており、その歩みを大きく進めるためにICTインフラの整備を通じたデータの利活用の推進が不可欠と考えられている。

厚生労働省では、平成29年1月12日に「データヘルス改革推進本部」を立ち上げ、健康・医療・介護のデータの有機的な連結に向けた「ICTインフラの抜本改革」や「ゲノム解析やAI等の最先端技術の医療への導入」の具体化に着手しており、7月4日に「国民の健康確保のためのビックデータ活用推進に関するデータヘルス改革（以下データヘルス改革推進計画）」を作成している。データヘルス改革推進計画では、全国保健医療情報ネットワークを整備し、具体的に以下のサービスの提供を検討している。

① 全国的な保健医療情報ネットワークを整備し、医療関係者等が円滑に患者情報を共有できるサービス
② 医療ケア児(者)等の救急時や予想外の災害、事故に遭遇した際に、医療関係者が、迅速に必要な患者情報を共有できるサービス
③ 健康に関するデータを集約・分析し個人や事業主に健康情報を提供jするサービス
④ 健康・医療・介護のビッグデータを個人単位で連結し、解析できるようにするサービス
⑤ 介護の科学的分析のためのデータを収集し、最適サービスを提供
⑥ がんゲノム情報の収集、医療関係者等が利活用できるサービス
⑦ AI開発基盤をクラウドで研究者や民間等へ提供するサービス

■ 目的

本事業では、上記7つのサービスにおける認証方式の具体化に向けた整理を行い、データヘルス各サービス及び全国保健医療情報ネットワークの設計時の参考情報とすることを目的としている。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

データヘルスにおける健康医療情報の活用において、それを支えるための認証技術や実現方式を、直近の社会的・技術的動向を踏まえて整理する必要がある

- 政治的背景
  - データヘルス改革推進計画において検討されているサービスには、「健康に関するデータを集約・分析し個人や事業主に健康情報を提供するサービス」などをはじめとして、医療関係者だけではなく、国民など広範囲の利用者に対する情報共有サービスが想定されている。
- 社会的背景
  - 2017年に施行された改正個人情報保護法においては、「健康診断等の結果」など、要配慮個人情報と位置付けられる情報が定義された。要配慮個人情報を扱う手続きには十分な検討が求められる状況にある。
- 技術的背景
  - 従来、ID/パスワードなどの記憶情報による認証や、ICカードなどの所有物による認証などの認証方式が存在していたが、技術進展に伴い、スマートフォン端末などを活用して生体認証を実現可能なFIDOなどの技術が登場している。
  - 最近の技術動向と並行して、NIST（米国国立標準技術研究所）のNIST 800-63をはじめとして、電子認証におけるガイドラインについても更新が進められている。

データヘルスにおける「認証」に関する課題（弊社認識）

利用者が、データヘルスにおける健康医療情報の利活用を行うために最適な認証技術・方式について、最新の動向を踏まえた検討ができていない状況である。
加えて、健康医療情報の利活用を実現するための認証基盤の青写真が描けていない。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

課題認識を踏まえ、「認証技術及びサービス動向の調査」と、「利用者及びユースケースを踏まえた認証方式、製品に関する整理」を実施する

【ステップ1】認証技術及びサービス動向の調査

■調査検討の概要
- 一般に普及している認証およびフェデレーションの技術を整理する。
- 認証の対象となる主体（デバイス、組織・個人、システム等）と、操作種別（データ参照、データ更新等）に関する想定を整理する。
- アクセス可能となる情報の性質（センシティビティ、緊急時でのデータの要否、他サービスで集積された情報のシステム間共有の要否等）を整理する。
- PKI含めた証明書の利用も含め、技術を実現する製品・仕組みについて調査する。
- 医療業界、金融業界を主として、認証基盤を実現している事例について調査する。

【ステップ2】利用者及びユースケースを踏まえた認証方式、製品に関する整理

■調査検討の概要
- ステップ1の結果をもとに、データヘルスにおけるサービスと認証基盤の構成について検討する。
- NIST 800-63などの各種規格・標準の内容およびデータヘルスにおける健康医療情報の利活用のユースケースに照らして、認証基盤として提供すべき認証のレベル（物理的、論理的な認証方法の組み合わせ）および方式を整理する。
- 検討した製品（または製品の組み合わせ）の認証方式案の検討について、導入・運用に関する検討事項を整理する。必要に応じて実効性の検証を行う。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

3. 本事業の全体像

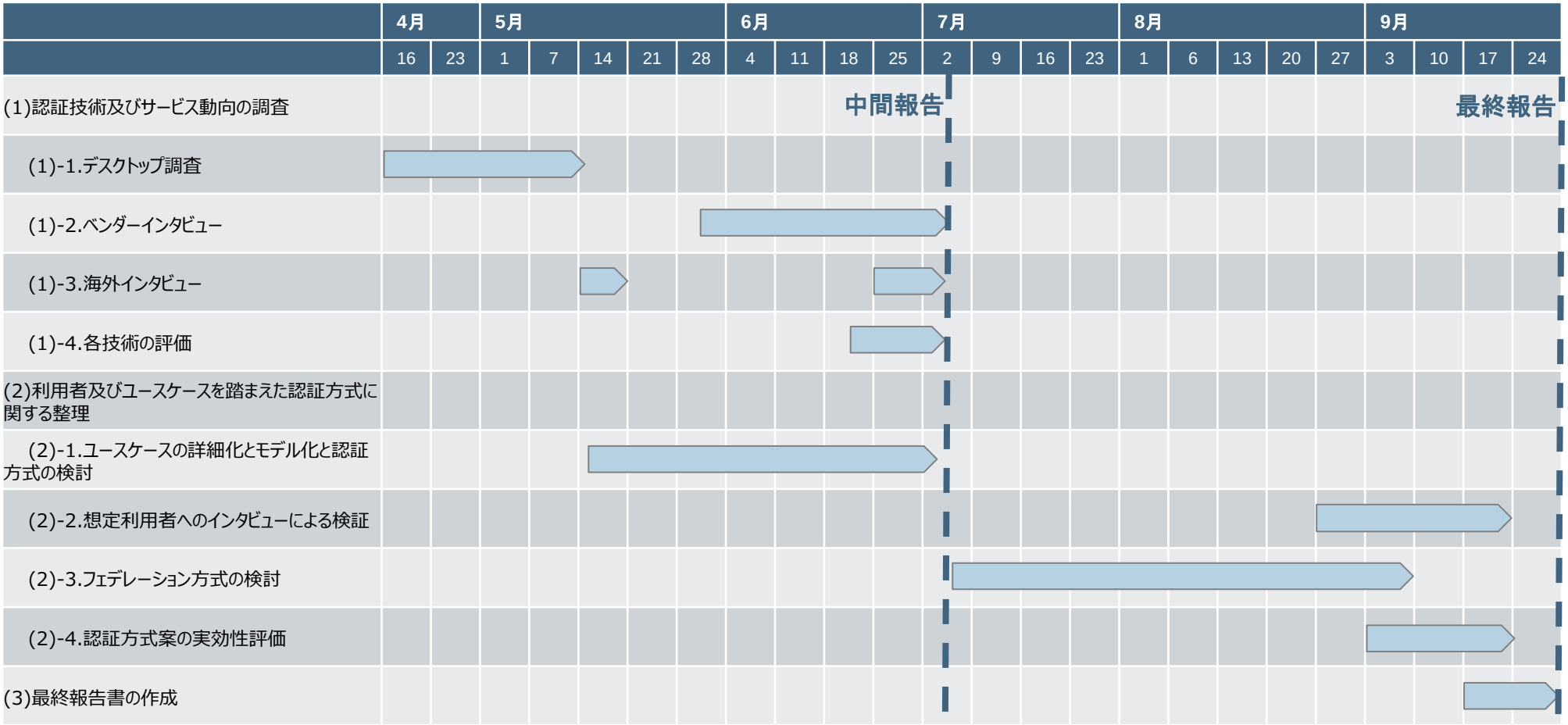
全国保健医療情報ネットワークの認証基盤の構想のために以下の内容について調査研究を行った

実施項目		本研究で明らかにすべきこと
(1)認証技術及びサービス動向の調査	(1)-1.デスクトップ調査	国内外の動向踏まえ、どのような認証技術が利用可能か。
	(1)-2.ベンダーインタビュー	医療従事者へ広く普及するために、認証技術についてどのような要件が考えられるか。
	(1)-3.海外インタビュー	国内外の動向踏まえ、どのような認証技術が利用可能か。
	(1)-4.各技術の評価	各認証技術はどのようなユースケースに適しているか。
(2)利用者及びユースケースを踏まえた認証方式に関する整理	(2)-1.ユースケースの詳細化とモデル化と認証方式の検討	全国保健医療情報ネットワークにより提供されるサービス内容や求められる要件はなにか。 (1)-4の評価を踏まえ、どのような認証技術を採用すべきか。
	(2)-2.想定利用者へのインタビューによる検証	認証方式案について、利用者側からどのようなニーズがあるか。
	(2)-3.フェデレーション方式の検討	各サービスを連携していくために、どのようなフェデレーション方式が考えられるか。
	(2)-4.認証方式案の実効性評価	検討した認証方式案について、実効性はあるか。どのような課題が考えられるか。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

3. 本事業の全体像

（1）デスクトップ調査、インタビューにより認証技術や医療現場でのニーズなどを調査。（2）調査結果を踏まえ、ユースケースごとの認証方式、フェデレーション方式の案を作成



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

デスクトップ調査により、金融、医療分野の認証関連技術や製品の事例と、ベンダーとその提供製品の全体像を把握した

■ 調査内容

1. 事例調査　　・・・金融、医療分野でのユースケースについて、想定ニーズ、認証技術、製品の例など調査をした。
2. ベンダー調査 ・・・インタビュー候補を幅広く把握するため、金融、医療分野のベンダーとその提供製品を調査した。
(参考資料参照)

■ 結果概要

- 金融分野では、ネットバンキング、クレジットカードの明細参照、公的個人認証を用いた口座開設の事例を調査した。
- 医療分野では、電子カルテ、地域医療連携システム、EDC、PHR、地域医療連携システム、公的個人認証を用いたHPKIカード発行の事例を調査した。
- 金融、医療ともに、記憶、所持、生体認証の3点それぞれの技術を用いた製品が流通しており、HPKIや公的個人認証を用いた製品も新たに登場しつつあった。
- 医療においても、クライアント証明書、USBトークン、OTP、パスロジック方式OTP、静脈、顔、指紋などの生体認証を利用した多彩な製品が発売されている。
- 一方、日本医師会総合政策研究機構の調査などによると、実際の医療現場ではID、パスワードでの運用が大多数を占めており、HPKIや生体認証などの導入はまだ僅かであると考えられた。
- 多様な技術や製品例が流通しているにも関わらず、実際の導入はID, パスワードに限局している背景に、医療現場特有のニーズや導入障壁が存在している可能性が考えられ、ベンダーインタビューを通じてその点を明らかにすることとした。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ネットバンキング、クレジットカード明細参照、マイナンバーカードの電子証明書を利用した事例を調査した

No.	分野	事例			想定利用規模		利用者					利用シーン		その他要件			調査対象
		toC /inB /toB	項目	内容	利用者数（万人）	利用頻度	国民（患者）	医療従事者	介護従事者	研究者等	金融機関従業員	日常	緊急	モバイル利用	認証連携	生体認証、FIDO等の利用度	
1	金融	toC	銀行口座開設	銀行口座の新規開設手続を行う。	*	低	○	–	–	–	–	○	–	–	–	–	○
1	金融	toC	ネットバンキング（参照・振込）	インターネットバンキングシステム経由で口座金額を参照、他口座への振込みを行う。	*	中	○	–	–	–	–	○	–	○	–	○	○
3	金融	toC	ネットバンキング（利用登録）	インターネットバンキングの初回利用登録を行う。	*	低	○	–	–	–	–	○	–	–	–	○	○
4	金融	toC	家計簿アプリ参照	スマートフォン利用で家計簿アプリから各種明細を確認する。	*	中	○	–	–	–	–	○	–	○	○	○	
5	金融	toC	クレジットカードの登録	クレジットカードの利用登録を行う。	*	低	○	–	–	–	–	○	–	–	–	–	
2	金融	toC	クレジットカード明細参照	インターネット経由でクレジットカードの利用明細の参照を行う。	*	中	○	–	–	–	–	○	–	○	–	○	○
			クレジットカード	インターネット経由で獲得ポイントの交換利							–	○	–	○	–	○	
3	マイナンバーカードの電子証明書を利用した銀行口座の開設手続き																
8	金融	toC	株式購入	インターネット経由で株式購入を行う。	*	中	○	–	–	–	–	○	–	○	–	○	
9	金融	toC	銀行ATM利用	銀行ATM利用で現金の引き出しを行う。	*	中	○	–	–	–	–	○	–	–	–	○	
10	金融	inB	オフィス入館	従業員が業務オフィスに入館する。	*	高	–	–	–	–	○	○	–	–	–	–	
11	金融	inB	システム運用端末室入室	システム担当従業員が運用端末室に入室する。	*	高	–	–	–	–	○	○	–	–	–	○	
12	金融	inB	業務端末利用	従業員が業務用端末にログインする。	*	高	–	–	–	–	○	○	–	–	–	○	

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

toC:個人向け、toB:法人向け、inB:業務利用

事例1:ネットバンキング（参照・振込）

事例1	インターネットバンキングシステム経由で口座金額を参照、他口座への振込みを行う。
ニーズ	・国民が広く利用するため、簡便性が必要。 ・金額情報を取り扱うため、高いセキュリティが求められる。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	日立製作所	FINEMAX	・パスワード	・乱数表 ・ワンタイムパスワード	-	・インターネットやモバイルなどのネットワークを利用して提供するインターネットバンキングサービスの共同利用型のアウトソーシングサービス。 ・ワンタイムパスワード、リスクベース認証、乱数表認証など、さまざまなセキュリティ対策機能を保持。
2	NTTデータ	AnserParaSOL	・パスワード	・ワンタイムパスワード	-	・最新鋭のインターネットバンキングサービスを個人向けに提供できる共同利用型のサービスです。 ・パスワード認証に加え、ワンタイムパスワード、リスクベース認証機能を保持。
3	NRI	ValueDirect	・パスワード	・ワンタイムパスワード	-	・インターネットバンキングの共同利用型サービス。 ・普段利用していないPC、スマホからログオンしようとした場合の追加認証（リスクベース認証）や、振込などの機能において、通常利用パスワードに加え、メールを利用した期限付きパスワード（＝メール通知パスワード）を必要とする認証を実装。
4	RSA Security	RSA SecurID Access	-	・ワンタイムパスワード（ハードトークン）	-	・時刻同期方式のワンタイムパスワードを生成する認証デバイス。 ・トークンに表示される 60 秒毎に変わるトークンと、カードの所有者を示す PIN 番号 (暗証番号)を組み合わせて、その時の自分のパスワードとして使用。
5	Symantec	VIP Access	-	・ワンタイムパスワード（スマートフォン）	-	・30秒間毎に更新される使い捨てのワンタイムパスワードを生成するアプリケーション。
6	富士通	Finplex オンライン認証サービス for FIDO	-	・スマートフォン	・虹彩 ・指紋 ・顔	・『Finplex オンライン認証サービス for FIDO』は、次世代オンライン認証規格FIDOに準拠したオンライン認証サービス。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

事例2：クレジットカード明細参照

事例1	インターネット経由でクレジットカードの利用明細の参照を行う。
ニーズ	・国民が広く利用するため、簡便性が必要。 ・金額情報を取り扱うため、高いセキュリティが求められる。 ・API提供の場合、フェデレーション技術として、OAuth2、OpenID Connectへの対応が求められる。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	ヒューレット・パッカード	Icewall SSO	・パスワード	-	-	・利便性の高い快適なセキュリティ環境を実現するWebシングルサインオン ソリューション ・スマートフォンやタブレット等のモバイルデバイスからのアクセスにも、セキュアで利便性の高いシングルサインオン環境を提供。
2	日立製作所	金融API連携サービス	・パスワード	・乱数表 ・ワンタイムパスワード	-	・「FINEMAX API連携サービス」では、インターネットバンキングの契約者IDに紐づく普通預金、定期預金、外貨預金などの口座情報の参照を可能にします。（FINEMAX契約行向けのサービス）
3	日本電気	API連携プラットフォームサービス	・パスワード	-	・顔	・金融機関のオープンAPI(注2)対応で求められる認証機能やセキュリティ対策を提供することで、金融機関の社内システムを安全に他の事業者システムと連携。 ・顔認証をはじめとする生体認証やAI・IoT等の先端ICT技術を活用したオプションサービスも提供。
4	NRIセキュアテクノロジーズ	Uni-ID	・パスワード	・ワンタイムパスワード ・SMS	-	・顧客IDをセキュアに統合・連携・管理するConsumer IAM（Identity and Access Management）パッケージソリューション。

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

事例3：金融機関の口座開設時に犯罪収益移転防止法や番号法上の本人確認を行う

事例	金融機関の口座開設時に犯罪収益移転防止法や番号法上の本人確認を行う
ニーズ	・非対面（オンライン）で口座開設完結 ・本人確認書類の郵送不要化および口座開設に関わる期間短縮

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	野村総合研究所	e-NINSHO	マイナンバーカードの暗証番号	マイナンバーカード	-	公的個人認証サービスにおける総務大臣認定事業者。 金融機関の口座開設時にマイナンバーカードを利用して犯罪収益移転防止法や番号法上の本人確認を行った上で、4情報（氏名・住所・生年月日、性別）や個人番号を取得するサービス。 マイナンバー保管・管理サービス（e-BANGO）との連携により、マイナンバーの収集から保管・管理まで一気通貫で行うことができる。

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

マイナンバーカードを利用した事例を含む計10事例を調査した

No.	分野	事例			想定利用規模		利用者					利用シーン		その他要件			調査対象
		toC/inB/toB	項目	内容	利用者数(万人)	利用頻度	国民(患者)	医療従事者	介護従事者	研究者等	金融機関従業員	日常	緊急	モバイル利用	認証連携	生体認証、FIDO等の利用度	
1	医療	inB	電子カルテの閲覧・更新	医療従事者等が電子カルテにログインし、閲覧・更新を行う。	*	高	−	○	○	−	−	○	○	−	○	○	○
18	医療	inB	病院の入退館	医療従事者等が病院職員エリアへ入退館を行う。	*	高	−	○	○	−	−	○	−	−	−	−	
19	医療	inB	検査機器の使用	検査機器システムへログインし、検査を行う。	*	高	−	○	○	−	−	○	−	−	−	−	
20	医療	toC	来院窓口での本人確認	来院窓口での本人確認	*	高	○	−	−	−	−	○	−	−	−	−	
21	医療	toC	健康保険被保険者資格の確認	来院窓口での健康保険の有資格者であることを確認する。	*	高	○	−	−	−	−	○	−	−	−	−	
2	医療	toB	製薬企業等による閲覧	臨床研究・治験を目的に、製薬企業やCRO担当者が診療情報を閲覧する。	*	高	−	−	−	○	−	○	−	−	○	−	○
3	医療	toB	製薬企業等との共有(EDC)	臨床研究・治験を目的に、製薬企業やCRO担当者と診療情報の一部を共有する。	*	低	−	−	−	○	−	○	−	−	−	−	○
4	医療	toB	地域医療連携システム(EHR)	医療従事者等が、診療情報を閲覧・更新する。	*	高	−	○	○	−	−	○	○	○	○	○	○
5	医療	toC	地域医療連携システム(EHR)	患者が、診療情報の確認・更新を行う。	*	高	○	−	−	−	−	○	−	○	○	○	○
6	医療	toC	PHRサービス	患者が、診療情報の確認・更新を行う。(PHR)	*	中	○	−	−	−	−	○	−	○	−	−	○
7	医療	toB	PHRサービス	医療従事者等が、診療情報を閲覧・更新する。(PHR)	*	中	−	○	○	−	−	○	−	○	−	−	○
8	医療	toB	PHRサービス	医療従事者等が、PHRサービスの初回登録を行う。(PHR)	*	低	−	○	○	−	−	○	−	○	−	−	○

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

toC:個人向け、toB:法人向け、inB:業務利用

マイナンバーカードを利用した事例を含む計10事例を調査した

No.	分野	事例			想定利用規模		利用者					利用シーン		その他要件			調査対象
		toC /inB /toB	項目	内容	利用者数（万人）	利用頻度	国民（患者）	医療従事者	介護従事者	研究者等	金融機関従業員	日常	緊急	モバイル利用	認証連携	生体認証、FIDO等の利用度	
9	医療	toC	PHRサービス	患者が、PHRサービスの初回登録を行う。（PHR）	*	低	○	－	－	－	－	○	－	○	－	－	○
30	医療	toC	遠隔医療システム	患者が遠隔医療システムの初回登録を行う	*	低	○	－	－	－	－	○	－	○	○	○	
31	医療	toB	遠隔医療システム	医療従事者等が遠隔医療システムの初回登録を行う	*	低	－	○	○	－	－	○	－	○	○	○	
32	医療	toB	遠隔医療システム	医療従事者等が診療情報の閲覧・更新を行う。	*	高	－	○	○	－	－	○	－	○	○	○	
33	医療	toC	遠隔医療システム	患者が診療情報の閲覧・更新を行う。	*	中	○	－	－	－	－	○	－	○	○	○	

10 マイナンバーカードの電子証明書を利用した事例

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

toC:個人向け、toB：法人向け、inB:業務利用

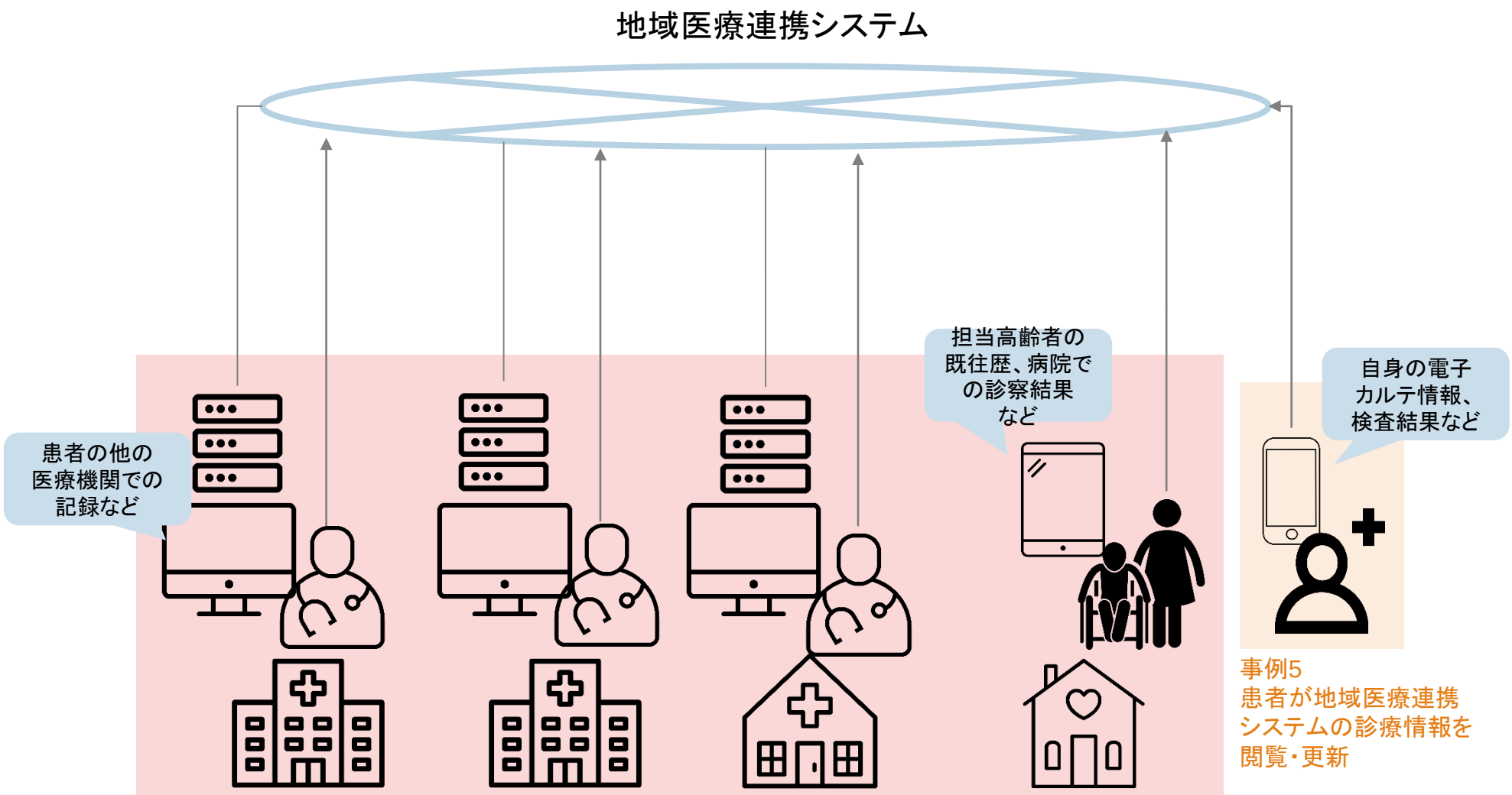
事例1:医療従事者が日常的に院内のカルテを閲覧する

事例1	医療従事者が日常的に院内のカルテを閲覧する。
ニーズ	・利用頻度が高いため、簡便性が必要。 ・ガイドライン上は2要素認証が求められる。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	イードクトル	Taikoban	-	・HPKIカード ・スマートフォン	-	HPKIカード、スマートフォン、および位置情報を利用した多要素認証ソリューション。 利用する電子カルテなどの端末のカードリーダーにHPKIカードをかざすと利用開始端末をサーバーに通知する。続いて利用者が持っているNFC（近距離無線通信の一規格）対応のスマートフォンにHPKIカードをかざすと、外部認証局（日医認証局など）に問い合わせて本人確認（資格確認）を実施。同時にスマートフォンはサーバーに位置情報を通知する。この一連の操作によって端末が利用できるようになる。
2	ジャパンシステム NTTデータ NTT西日本	ARCACLAVIS Ways	・ワンタイムパスワード	・ICカード	・指紋 ・指静脈 ・顔	多要素認証・マルチプラットフォームに対応した認証セキュリティー製品。ID/パスワードによる認証を、ICカードや生体情報、ワンタイムパスワードによる多要素認証に置き換え、認証セキュリティを強化する。また、シングルサインオン機能により、業務アプリケーションのID/パスワードの自動入力を可能にする。
3	日立ソリューションズ	静紋	-	-	・指静脈	指静脈認証。静紋にて正規のユーザを判別し、正規のユーザと確認された場合のみ、PCの利用と電子カルテのログオンが可能となり、不正なログオンによる電子カルテシステムの不正利用や情報漏洩を防ぐ。
4	富士通フロンテック	PalmSecure	-	-	・手のひら静脈	手のひら静脈認証。手のひら静脈認証は、認証率が良いため失敗が少なく、かつレスポンスが良いため、ログオンにかかる時間が大変短くなった。認証サーバ（PalmSecure LOGONDIRECTOR）で生体情報を一元管理することで、職員は何も携帯せずに、どの端末からでも手のひら静脈認証でシステムへログオンすることが可能。
5	PASSLOGY	Pass Logic	・パスロジック方式（トークンを利用しないワンタイムパスワード）	・クライアント証明書	-	クライアント証明書をインストールした端末だけがログイン可能となる「物理認証」と、トークンレスワンタイムパスワード認証の併用による「記憶認証」の2要素認証が可能。 トークンレスワンタイムパスワードとは、毎回異なる乱数表を用いることで、ユーザーがマス目の位置と順番の「パターン」を覚えるだけで認証が可能となる方式。ハードウェアトークンや、指紋や顔認証などの生体認証に必要な読み取り機器（リーダー）、ICカード＆リーダーといった認証用の物理デバイスを必要としないため、導入や管理コストが削減されるのが特徴となる。

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

地域医療連携システムの概要



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

地域医療連携システムにおける認証の状況

図 2.8-16 医療機関・薬局ログインセキュリティの採用状況（予定含む）

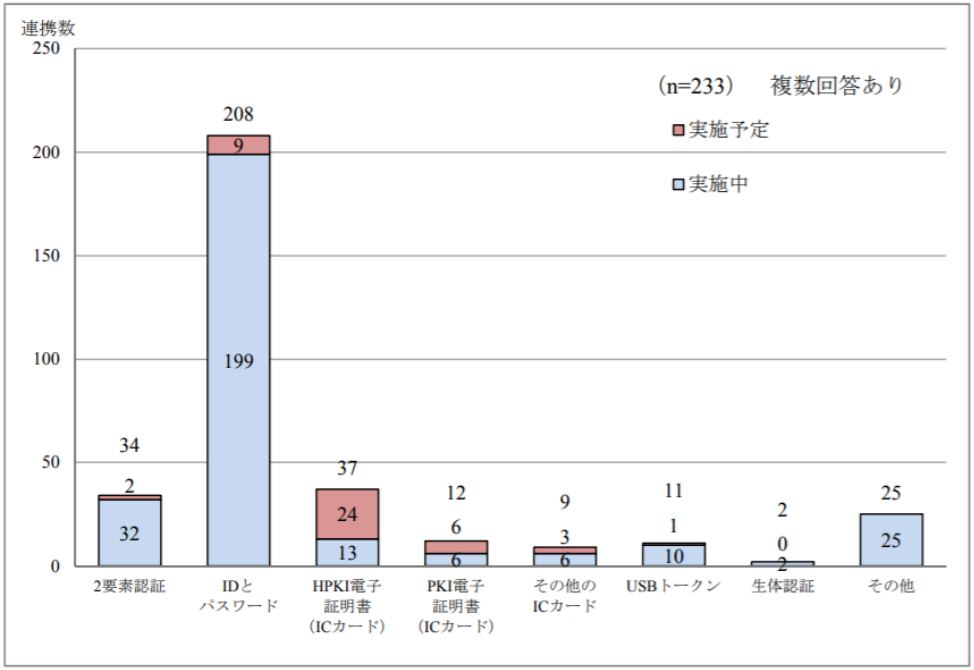
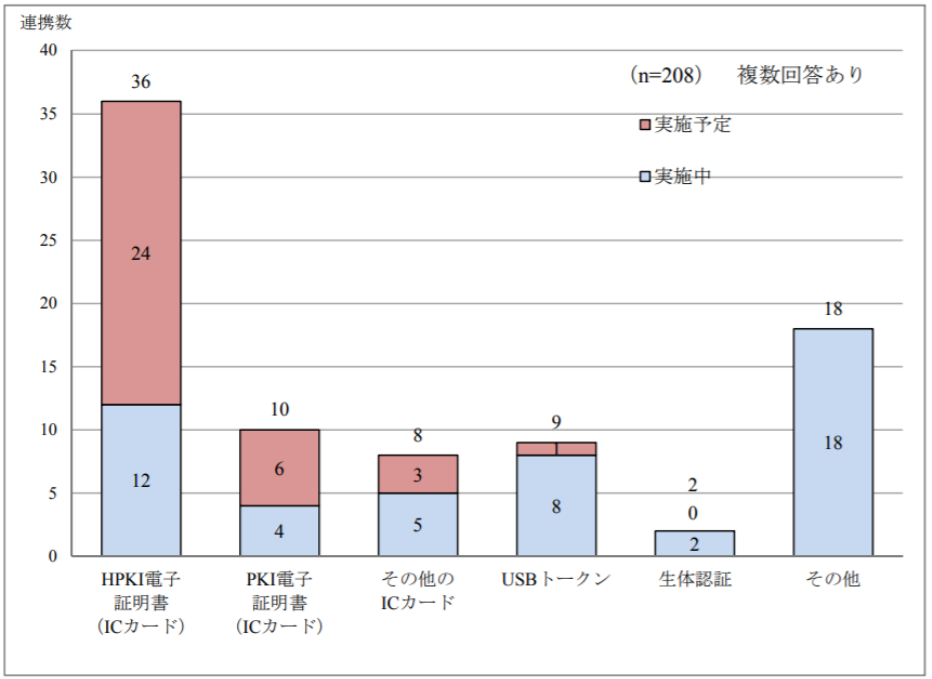


図 2.8-17 医療機関・薬局「ID とパスワード」と組合せのログインセキュリティ（予定含む）

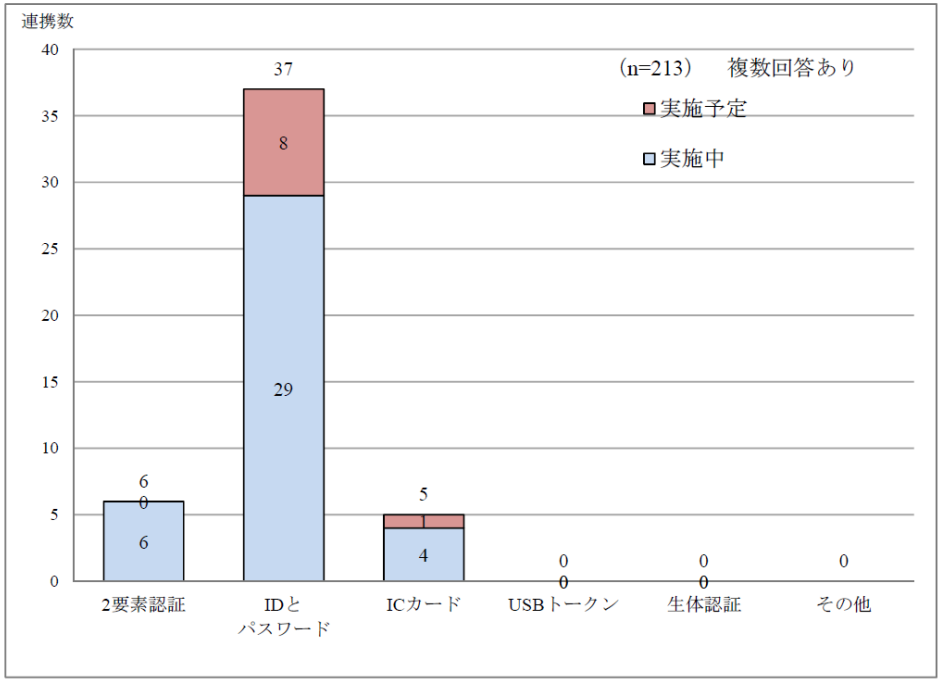


出所）日医総研ワーキングペーパー　ICTを利用した全国地域医療連携の概況（2016年度版）

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

地域医療連携システムにおける認証の状況

図 2.8-19 患者ログインセキュリティの採用状況（予定含む）



出所）日医総研ワーキングペーパー　ICTを利用した全国地域医療連携の概況（2016年度版）

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

事例2:臨床研究・治験を目的に、製薬企業やCRO担当者が電子カルテを閲覧する
事例3:臨床研究・治験を目的に、製薬企業やCRO担当者がEDCシステムを閲覧する

事例2	臨床研究・治験を目的に、製薬企業やCRO担当者が電子カルテを閲覧する。
ニーズ	・同意と取得できた患者の情報のみ、一定期間のみ、など活用範囲を限定した認証が求められる。 ・院内の電子カルテ情報を病院外へ提供するため、個人認証の強度は院内よりも強固であるべきである。 ・現状は、閲覧のたびに対面による本人確認が行われており、モバイル閲覧の許容度は低い。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	富士通	HOPE／EGMAIN-GX V05	・IDとパスワード		*	・利用者の職種によってアクセス権限が与えられており、一部の患者の閲覧のみ等、権限を越える操作ができない。 ・国立がんセンターで採用、訪問による院内閲覧のみ可能であり、対面による本人認証が行われている。
2	NEC	Mega Oak-HR	・IDとパスワード		*	・利用者の職種によってアクセス権限が与えられており、一部の患者の閲覧のみ等、権限を越える操作ができない。 ・旭川医科大学で採用、訪問による院内閲覧のみ可能であり、対面による本人認証が行われている。

事例3	臨床研究・治験を目的に、製薬企業やCRO担当者がEDCシステムを閲覧する。
ニーズ	・数百人規模での閲覧者が存在、数ヶ月-1,2年単位で担当者の変更、削除が頻繁に発生する。 ・役職や所属組織によって、アクセス範囲や編集権限の設定が必要。 ・格納データは、匿名化されており、個人認証の強度が院内にくらべて強度である必要はなく、モバイル閲覧は許容されている。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	富士通	DDworks21/EDC plus	・メールアドレスとパスワード	-	-	国内治験で比較的普及度の高いクラウド型ソリューション
2	NTTデータ/DataTrak	DataTrak One	・メールアドレスとパスワード	-	-	国内治験で比較的普及度の高いクラウド型ソリューション
3	イートライアル	Medidata	・メールアドレスとパスワード	-	-	グローバル治験などで、利用実績の高いクラウド型ソリューション

事例4:医療従事者等が地域医療連携システム(EHR)の診療情報を閲覧・更新する

事例4	医療従事者等が地域医療連携システム(EHR)の診療情報を閲覧・更新する。
ニーズ	・利用頻度が高いため、簡便性が必要。 ・ガイドライン上は2要素認証が求められる

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	富士通	すずらんネット（市立札幌病院地域医療情報ネットワークシステム）	・施設ID ・ユーザーID・パスワード	・デジタル証明書（端末の認証）	-	情報参照施設の端末から接続する際は３つの認証を必要とする構成になっている。
2	メディオ・テック	TOMA-NET	・IDとパスワード	・HPKI(ICカード)	-	-
3	エスイーシー（運営主体） NEC（システム）	道南MedIka	・ユーザーID・パスワード	・デジタル証明書	(連携する電子カルテは指紋認証)	-
4	アルム	-	・ユーザーID・パスワード	・デジタル証明書	-	-
5	ビーミック	bmicZR	・ユーザーID・パスワード	・ICカードまたは二次元バーコード	-	-
6	ウエルエス	まごころネット	・ユーザーID・パスワード	・ICカード ・USBトークン	-	患者にもICカードを配布。救急搬送時に患者がICカードを持っていれば、救急車内でパソコンからまごころネットにアクセスすることで、迅速な診療情報収集が可能になる。
7	名古屋掖済会（えきさいかい）病院	エキサイネット	・ユーザーID・パスワード	・USBトークン	-	JCCH・セキュリティ・ソリューション・システムズが提供するインターネットの標準技術である PKI によるクライアント認証が可能となる JS3 のプライベート CA Gléas（認証局）および USBトークン（Gemalto .NET キー）を採用。電子証明書をUSBトークンに格納し、二因子認証を実現した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

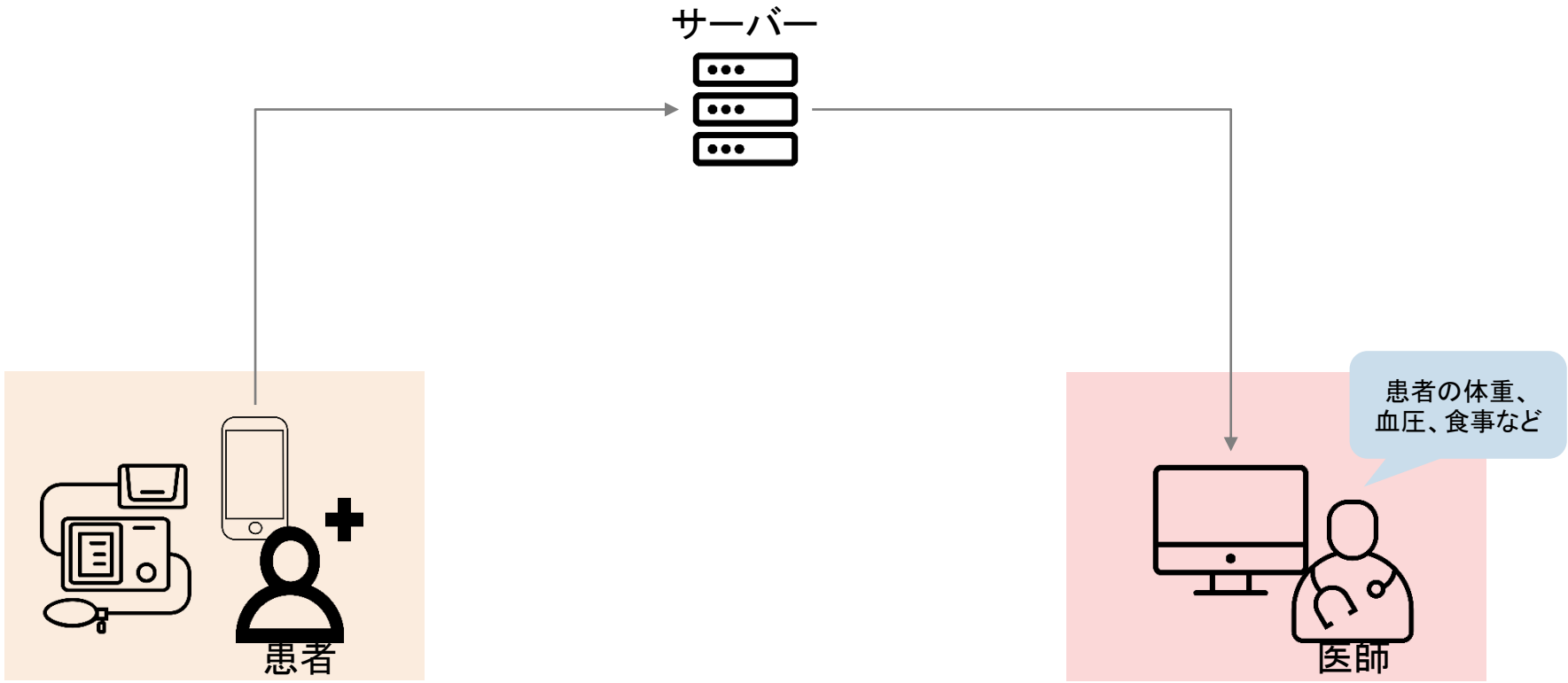
事例5:患者が地域医療連携システム(EHR)の診療情報の確認・更新を行う

事例5	患者が地域医療連携システム(EHR)の診療情報の確認・更新を行う。
ニーズ	・簡便性が必要 ・高価な機器は導入できない。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	アルム	-	・ユーザーID・パスワード	・デジタル証明書	-	-
2	ビーミック	bmicZR	・ユーザーID・パスワード	・ICカードまたは二次元バーコード	-	-
3	加古川総合保険センター	加古川地域保健医療情報システム	・ユーザーID・パスワード	・KINDカード	-	患者側にインターネットに接続できる環境とカインドカードリーダライタ（カインドカード読取装置）が必要。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

PHRの概要



事例6
患者がPHRの生体情報等を閲覧・更新

事例7
医療従事者がPHRの生体情報等を閲覧・更新

事例8
患者がPHRサービスの初回登録を行う

事例9
医療従事者がPHRサービスの初回登録を行う

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

事例6:患者がPHRの生体情報等を閲覧・更新する
事例7:医療従事者等がPHRの生体情報等を閲覧・更新する

事例6	患者がPHRの生体情報等を閲覧・更新する。
ニーズ	・継続性が重要であるため、簡便性が重視される。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	ウェルビー	Welbyマイカルテ	・メールアドレスとパスワード	-	-	-

事例7	医療従事者等がPHRの生体情報等を閲覧・更新する。
ニーズ	・利用頻度が高いため、簡便性が必要。 ・ガイドライン上は2要素認証が求められる

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	ウェルビー	Welbyマイカルテ	・メールアドレスとパスワード	-	-	-

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

事例8:患者がPHRサービスの初回登録を行う(PHR)
事例9:医療従事者等がPHRサービスの初回登録を行う(PHR)

事例8	患者がPHRサービスの初回登録を行う(PHR)。
ニーズ	・利用頻度が高いため、簡便性が必要。 ・ガイドライン上は2要素認証が求められる。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	ウェルビー	Welbyマイカルテ	・メールアドレスとパスワード	・端末認証	-	患者情報とメールアドレスを登録後メールアドレスに認証コードが送付され、それを登録画面で入力することで初回登録が可能となる。

事例9	医療従事者等がPHRサービスの初回登録を行う(PHR)。
ニーズ	・利用頻度が高いため、簡便性が必要。 ・ガイドライン上は2要素認証が求められる

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	ウェルビー	Welbyマイカルテ	・メールアドレスとパスワード	・端末認証	-	医師の情報や医療機関の情報等を登録後認証コードが送付され、それを登録画面で入力することで初回登録が可能となる。 申し込み情報と医師データベースとを照合し、所属等の確認を行う。状況により、電話、郵送による確認を行う。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

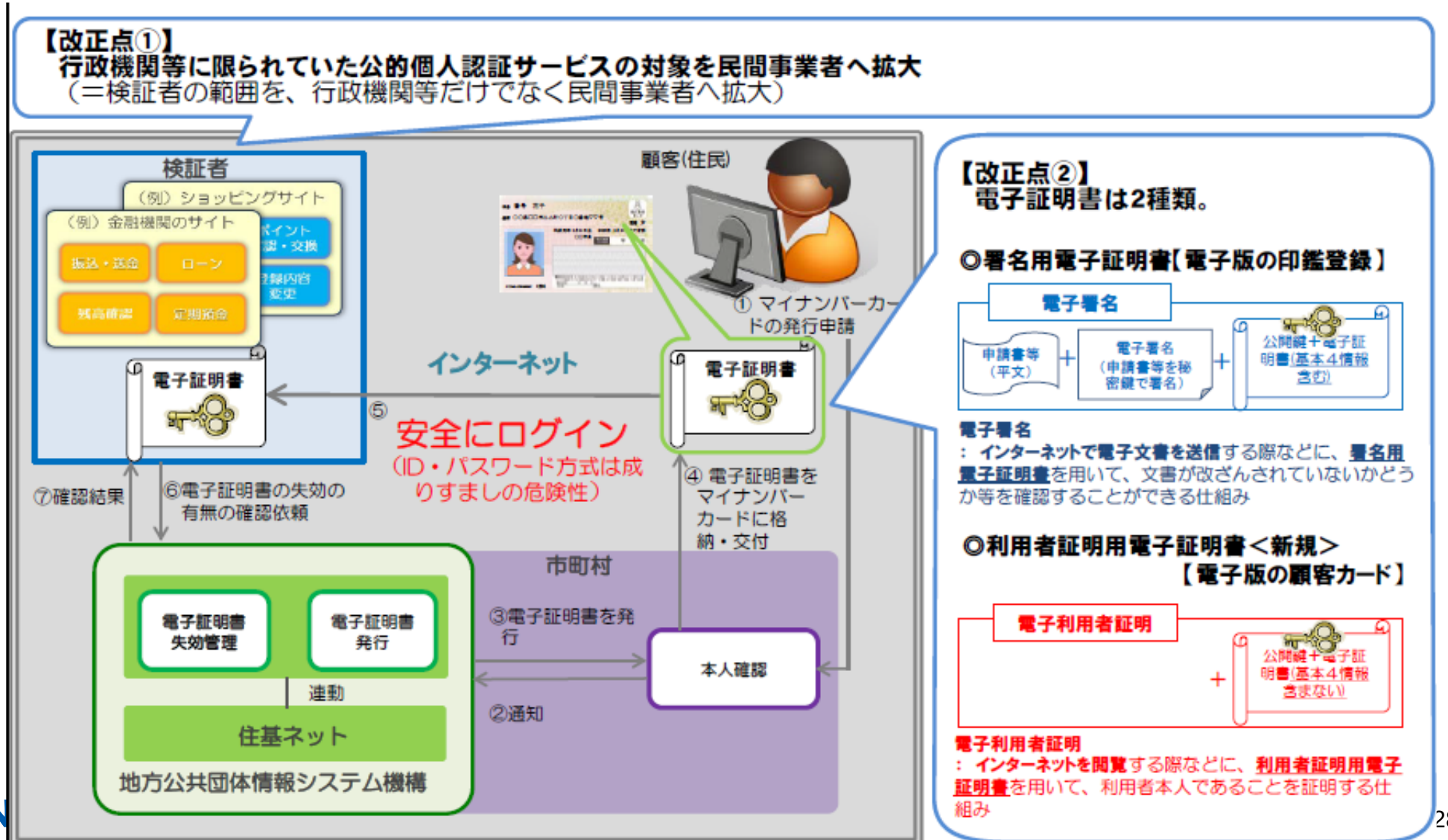
事例10：マイナンバーICを用いた個人認証の事例

事例	医師が医師資格証(HPKIカード)の新規発行時になりすまし防止のために本人確認を行う。
ニーズ	・非対面（オンライン）で発行手続完結。 ・本人確認書類の郵送不要化およびカード発行に関わる期間短縮。

	企業名	製品名	認証技術			特徴
			記憶	所持	生体	
1	日本医師会	-	マイナンバーカードの暗証番号	マイナンバーカード	-	公的個人認証サービスにおける総務大臣認定事業者。 医師がHPKIカードの発行を申請する時に、マイナンバーカードによる電子署名によって手続を行う。

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

ご参考：公的個人認証サービスのイメージと制度改正（平成28年1月）



ご参考：マイナンバーカードを利用した公的認証サービス（JPKI）導入に伴うHPKIカード発行手続きの変化

現状

医師

・発行申請書
・医師免許証のコピー
・住民票の写し
・身分証のコピー
・顔写真

申請（郵送）

日本医師会

発行

マイナンバーカード活用後

各種申請書類の用意、郵送が不要

受付事務の効率化

医師

・発行申請フォーム
（医籍登録番号と医籍登録年月日を含む）
・医師免許証のコピー
・顔写真データ
・JPKIで電子署名

電子申請

日本医師会

証明書
有効性確認

JPKIセンタ

署名用
電子証明書
管理ＤＢ

発行

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ベンダーインタビュー概要

■ 医療系ベンダーインタビューの目的

- 現在医療・介護の現場で使われている認証技術や、現場のニーズを把握し、全国保健医療情報ネットワークでの認証技術に求められる要件を検討した。
- 全国保健医療情報ネットワークに接続することになる既存の医療システムの概要やそれらの認証方式を確認し、医療現場のニーズにあった認証方式の検討材料とした。

■ ヒアリングの対象

	インタビュー先	提供するサービスの特徴							
		電子カルテ			介護システム	地域(広域)医療連携	他職種連携システム	薬歴レセコン	救急・災害システム
		大病院	中小病院	診療所					
1	A社	●							
2	B社	●				●			
3	C社		●			●			
4	D社					●			
5	E社			●				●	
6	F社			●	●				
7	G社				●		●		
8	H社		●						
9	I社								●

■ 調査結果の概要

- 医療・介護の現場では業務負荷やコストの観点から、ID・パスワードによる認証が選択されている。それ以外の認証強度の高い認証方式を導入する場合は、業務負荷やコストについて慎重に考慮する必要がある。
- 救急隊員は迅速性を重視するため、認証は極力軽くし、システム上アクセスできる情報を制限するなどの工夫が必要。
- 災害時に他県から来たDMAT(災害派遣チーム)が情報を見られるような対応をする必要がある。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

医療・介護の現場では業務負荷やコストの観点から、ID・パスワードによる認証が一般的であり、それ以上高いセキュリティに対しての反発が強い

	自社製品で利用する認証技術	当該認証技術選択の背景・ニーズ
A	• ID・パスワード。 • 一部院内システムの利用に際して生体認証を行っている医療機関もある。 • 地域医療連携ネットワークではHPKIの認証を行っている地域もある。	—
B	• ID, パスワード。 • 指紋認証、IC認証、顔認証は実証実験中、虹彩認証は実績がない。	• 薬局や診療所など、ID, パスワードにも慣れておらず、教育が必要な場合もある。 • 使って頂くことが最も重要なので、実用性を重要視。
C	• IDとパスワード。 • 指静脈とパスワード、Felica認証とパスワードという2要素の組み合わせはわずかながら実績がある。	• 認証に関しての強い声は聞かない。 • 指認証やFelicaは医療機関側の要求仕様に対応するためにカスタマイズした。
D	• 院内端末→院内NW:個人認証（LDAP認証、BASIC認証等） • 院内端末→地連ポータル：拠点認証（ODVPNアダプタ）、個人認証（ID/パスワード） • 地域医療連携ポータル→ASPサービス：SSO（ID/パスワード）	• セキュリティポリシーは施設ごとに異なるため、連携システムの認証は簡易にし、ポリシーに応じた厳格化は施設側の運用に任せる方が良い。 • 地域医療連携では、AP毎のアカウント入力作業や認証手続きが煩雑となるため、SSOによる連携ニーズが高い。
E	• IDとパスワード。	• セキュリティを強くしたいというニーズがない。 • 診療に専念したいという思いから、離席時のロックですら敬遠される。 • 以前は指認証を導入していたが、接触型は好まれなかった。
F	• 介護請求システムの基本設定はUSBデバイス認証とWindowsAD認証で、強化のニーズがある場合はID・パスワードを利用。iphone・iPadの場合はID・パスワードと施設キーが全てが揃って接続可。 • 医療はIDとパスワードが基本設定で、指静脈認証も接続可能。	• 介護の現場では以前よりはリテラシーがあがってきており、ID・パスワードを望むケースも増えてきている。 • 静脈認証はコストがかかるためになかなか受け入れられない。
G	• 基本はIDとパスワード。施設のセキュリティポリシーにあわせて指紋認証や指静脈認証・OTPが追加されることもある。	• 医師・看護師・介護士などの利用者に応じて認証形態を変える必要はない。 • 利用するデバイスの種類も認証形態の選択には影響しない。 • コストが重視されるため、おのずとID・パスワードになる。 • 静脈は手が冷えるとエラーが出やすい。指紋は心理的な抵抗も強い。
H	• 基本はIDとパスワード。 指紋認証や指静脈認証も一部ある。	• 電子カルテはクローズなシステムであるので、ID, パスワードで十分であり、それ以外の認証技術はコスト負担のデメリットが大きくなる。 • 生体認証は、10年前に流行り、その継続が一部あるが、近年はあまり要望はない。

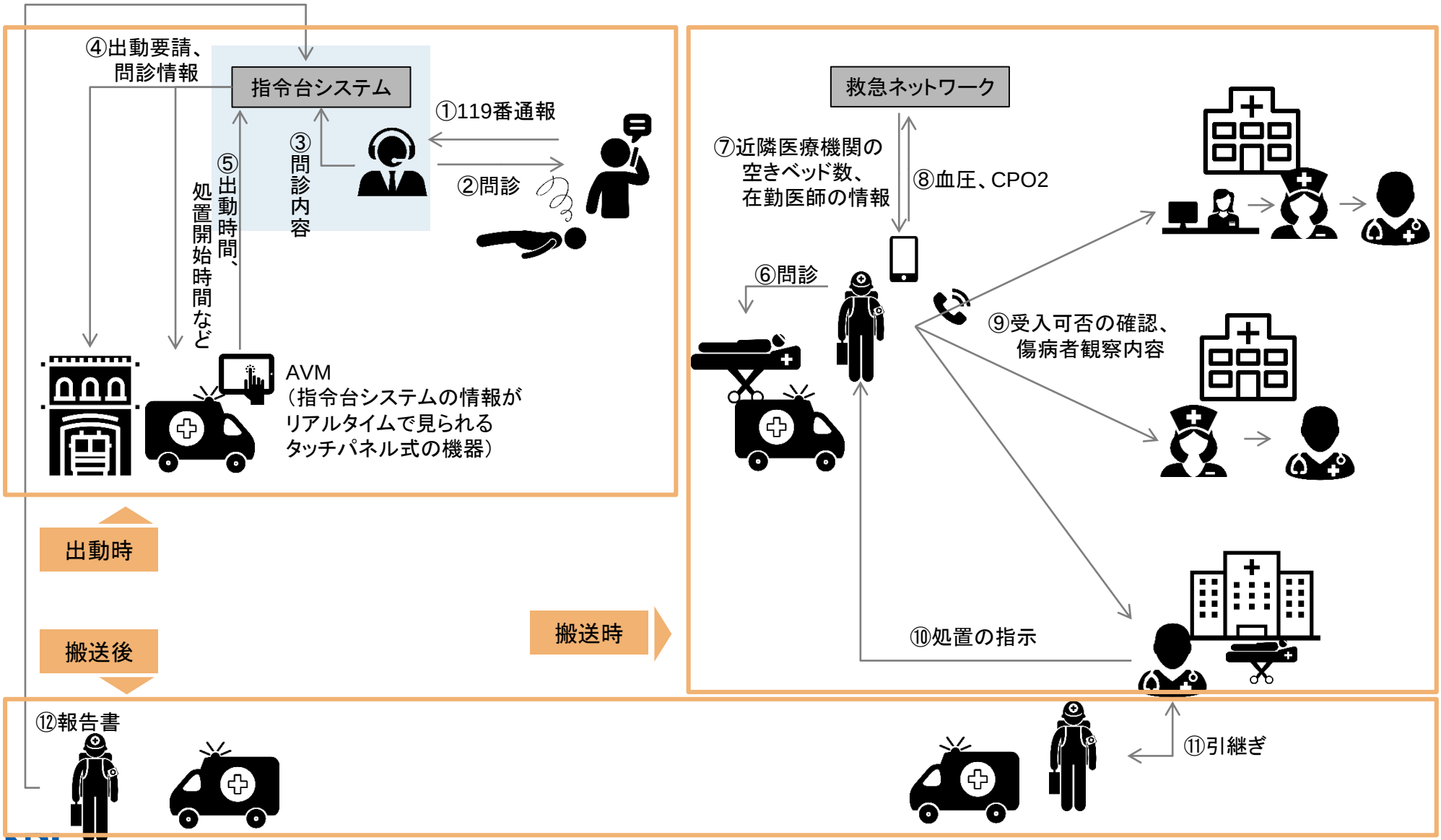
閲覧範囲の設定やIDの管理などは医療・介護施設へ任せることができる。ただし、システムの知識を持つ人がいないことも多く、ベンダーが代理で行うケースも多いと思われる。

	認証情報の登録・変更・削除などの運用方法	権限設定
A	—	—
B	• 院内に担当者をおいてもらい、職員の情報を集約したマスタを管理していただいている。人事的な管理もなされているそのマスタを、電子カルテの認証に利用している。 • 多い施設では、500~1000程度のユーザー管理	—
C	• 院内SEがIDとパスワードの発行、初期登録などをする。 • パスワードを何にするかは病院のルール次第。パスワードを最初から期限切れの状態にしておいて、職員が最初にログインするときに自身で設定するケースも多い。	• 職種単位で何ができるかの権限はシステム上で設定できる。
D	• 利用施設は、利用を希望する者の職種・氏名・性別・年齢・連絡先等を記した申請書を、ファックス若しくは郵送で地域連携システムの協議会へ提出することにより、個別の利用者ID及びパスワードを生成・付与される。 • ID・パスワードの管理については利用施設の責任で管理。	—
E	• IDとパスワードは医療機関側が設定する。 • ただし、クリニックはシステムに詳しい人がいるとは限らないので、代理店のインストラクターに任せているケースも多い。	• 職種ごとに参照可能範囲を変えているが、現場からは同じにしてほしいと言われる。
F	• 介護はデバイス認証なので、管理が必要になるケースはほとんどない。 • 電子カルテはIDとパスワードの管理は病院内の管理者が行う。	• 介護の場合はアプリの中で閲覧可能範囲を設定できる。 • 権限設定は病院側に任せている。組織の担当者レベルで判断している。 • 医療の場合、VIP患者のカルテは特定の職員だけ見られるようにするなども可能。
G	• 院内の担当者が管理する。小規模な病院では医師が担当していることもある。 • 勤怠管理などの業務システムとID管理を連動させており、職員の退職による権限の削除などは業務システムを正しく使っていれば自動で反映される。	• 認可範囲は患者ごと、項目ごと、閲覧または更新などの要素ごとに個別に設定でき、これらの管理更新も院内の担当者に行ってもらっている。
H	• 院内の職員マスタを紐づけて、ID管理をしている。 • パスワードは、数ヶ月に一回変えるなど、院内運用を行っている。	• 医師やコメディカルなど職種だけでなく、個人別でアクセス制限を設定している。 • VIPの患者などプライバシー保護のため、アクセスできる医師を制限するなどのニーズがある。

利便性の観点から、シングルサインオンなどの認証連携は求められる一方で、芋づる式に情報が漏洩するリスクに対しての懸念の声も一部聞かれ、連携しない場合もある

	フェデレーション技術	フェデレーション技術を選択した理由・利用しない理由
A	• 院内システムなので特にない。	—
B	—	—
C	• 自社システムから他社のサービスを呼び出す場合に、ログイン情報をお渡しする。バックヤードで同期を取っていることが多い。 • トークンや識別子を渡している訳ではない。	• 医療系のシステムベンダー間での連携をする中で一般的になっているからこの形式をとっている。
D	• シングルサインオン認証。	—
E	• シングルサインオン認証はしていない。 • 患者のIDは連携するが、システムのログインはそれぞれ行う。	• シングルサインオン認証は芋づる式にデータが取れてしまうので避けている。
F	• 他社システムへの接続の際のシングルサインオン認証は個別に対応している。自社システム間はオートログインが可能。	• 他社のPACSや検査システムとの連携は求められている。
G	• 院内ポータル等からのアクセスを受けてSSO対応はしている。 • 介護情報の地域連携の機能でTポイント加算がたまる取り組みをしており、そこでID連携に対応している。	—
H	• 院内では、患者には患者ID、職員番号がそれぞれ一つであるので、それを統一IDにしているので、ID連携は必要ない場合がほとんど。 • 院外とのID連携では、ID-LINKとHuman-Bridgeが2大勢力といえる。	—

現状の救急時の情報のやり取りのフロー



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

救急隊員は迅速性を重視するため、認証は極力軽くし、システム上アクセスできる情報を制限するなどの工夫が必要

現状の救急ネットワークの認証

- 基本的にはID・パスワードのみ。
  - システム上個人情報を保有していないため、一度ログインするとずっとログインした状態になっている。
- IDは隊（3人一組）ごとに1つ付与。

現状の救急現場における課題

- 問診に時間がかかる。
- 問診内容を医療機関に伝達するのに時間がかかる。

現場のニーズ

- 認証の形式について
  - 迅速性が問われる場なので、認証の負担は軽くする必要がある。
  - 持ち運ぶ備品が多いため、機材を増やすのはハードルが高い。
  - グローブをしているため指紋認証は受け入れがたい。虹彩認証、顔認証などなら良いだろう。
  - HPKIの普及率は低いが、救急隊は規則に縛られるため、国や自治体がルールを定めてしまえば持つだろう。
- 連携する情報について
  - 医療機関に受け入れてもらうために、細かな情報収集が求められる。
  - 特に保険加入の有無は重要。その他患者の属性や既往歴、禁忌薬の有無jなどの治療に役立つ情報があると良い。
  - ただし、医療機関が把握しているならば、必ずしも現場で救急隊員が把握する必要はないため、救急隊員は鍵のみ取得し、それを搬送先医療機関に伝達する形式でもかまわない。

その他

- 災害時に他県から来たDMAT（災害派遣チーム）が情報を見られるような対応をする必要がある。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

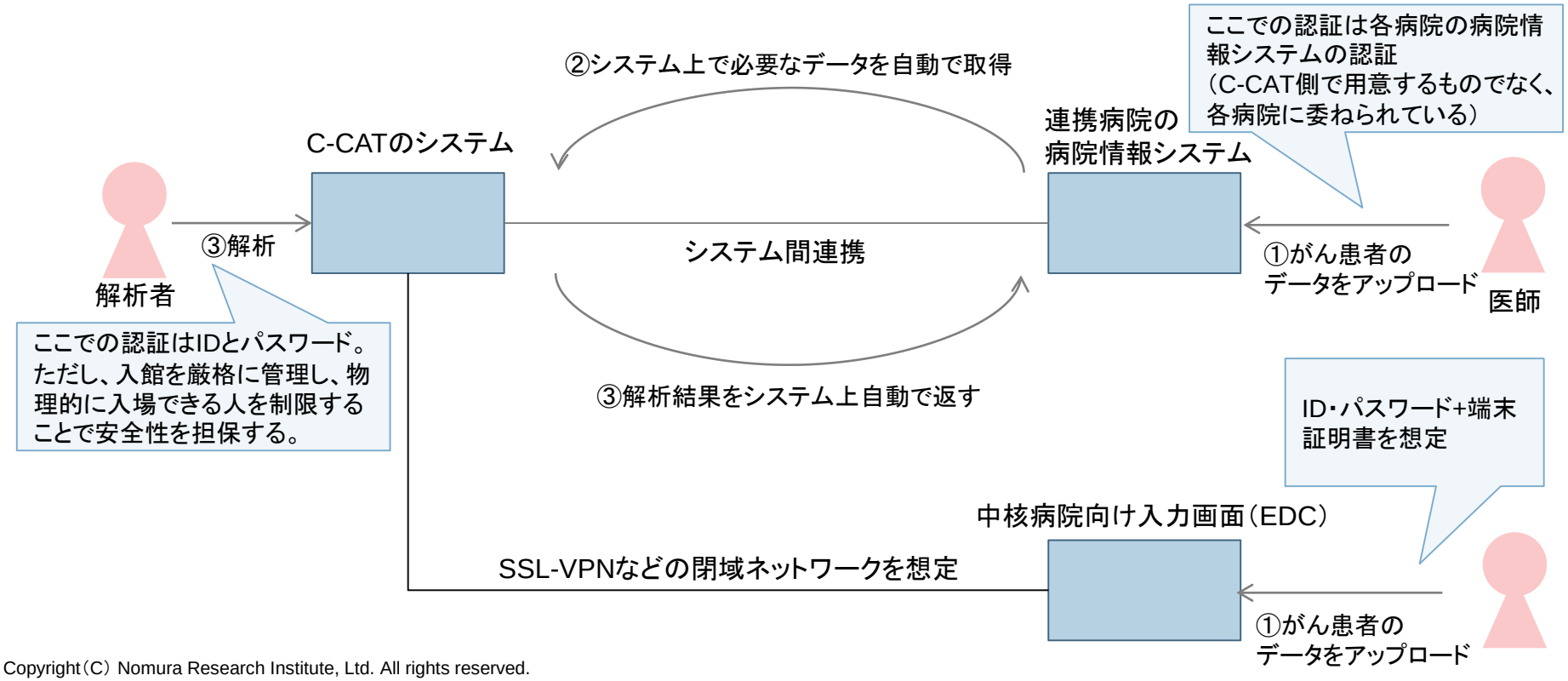
最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

C-CATでは、すでにシステムの調達が進んでおり、連携病院とはシステム間連携を行う想定。ただし、中核病院はEDCと呼ばれるWeb型の入力画面を作成する

■ 現状の想定（病院とのデータのやり取り）

- すでにC-CATのシステムの調達は進んでいる。
- C-CATと連携病院との間で想定されるデータのやり取り
  - 連携病院とのやり取りはシステム間連携のため、ユーザーを介さない。そのため、利用者の認証も行わない。
  - システム間連携の対応が出来ない中核病院などは、C-CAT側でEDCというWeb型の入力画面を作成する予定。
    - ここでの認証方式は具体的には決まっていないが、ID・パスワードと端末証明書などを使うことを想定している。



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

機微度が高いゲノムデータを扱う場合、利用できる人の審査を厳重にすることが重要。研究データなど、個人情報がないものについては、簡易に認証できる仕組みを検討すべき

現状の想定（ゲノムデータの利活用）

- C-CATに蓄積されたがんゲノムデータを利用する場合
  - 解析者とは明確に場所を分けた上で物理的に入れる区域を制限する。
  - 利用できる人の審査を厳格に行うため、電子的な認証はID・パスワードやカードなど簡易なものにする想定でいる。

将来的な構想

- 将来的には、すでに国内外で公開されている研究データ（個人情報のない情報）をデータベースにまとめて公開したい。
  - ただし、この蓄積は日本の宝なので、誰でも利用できるのではなく、事務局に登録してもらってIDとパスワードを発行することを想定している。
- 将来的な拡張性
  - 将来的にはゲノムのデータだけでなく、がん登録や検診の情報などと紐付けていきたい。
  - ＝拡張性のあるシステムの構築が重要。
- 利用者の拡大も考えると研究者個人ではなく、C-CATは組織単位での管理にとどめ、各研究者の管理は組織に委ねることも考えられる。
  - 権限の委譲についても今後検討していく必要はあるだろう。

課題

- 検査会社から直接データをやり取りする仕組みが定まっておらず、中核病院を経由しなければならない。
  - 現状検査会社は数社程度なので、検査会社から直接C-CATにデータをやり取りできる環境を整備するよう国から促してほしい。
- がん登録などは法律上使える範囲が限られるため、紐付けができない。
  - →将来的な利用を考えて法律の改正なども必要になるだろう。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

本人確認・個人情報に関する課題感を背景として、デジタルアイデンティティが検討された

■ 本人確認・個人情報の扱いに関する課題感。

カナダ政府

- 公的手続きでの各種身分証明書の確認のコスト。
- 本人確認のための窓口の運用・管理の維持。

銀行

- マネーロンダリング対策に向けた取り組み、kyc※の効率。
- 偽装された身分証明書による手続きの防止。

※ Know Your Customer：新規に口座開設する際に銀行側から要求する、顧客の身元確認における書類手続きの総称

ヘルス

- 緊急時の患者レコード・患者管理システム へのアクセス含めた、委託コストの削減。
- 現場で必要な個人情報の取り寄せの煩雑さ。

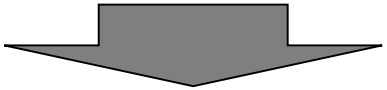
■ 以下のようなデジタルアイデンティティが検討された。

- 実在の個人に紐づいた1つのものであること。
- 不正を許さないものであること。
- 個人情報の連携が安価であること。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

個人がコントロール主体となる、デジタルアイデンティティの仕組みをデザインしている

- 一方で、国民は個人情報を企業や組織間が融通する取り組みに懐疑的。
  - 78%の顧客が企業による個人情報の活用・連携に不信感があるとの調査結果もある。

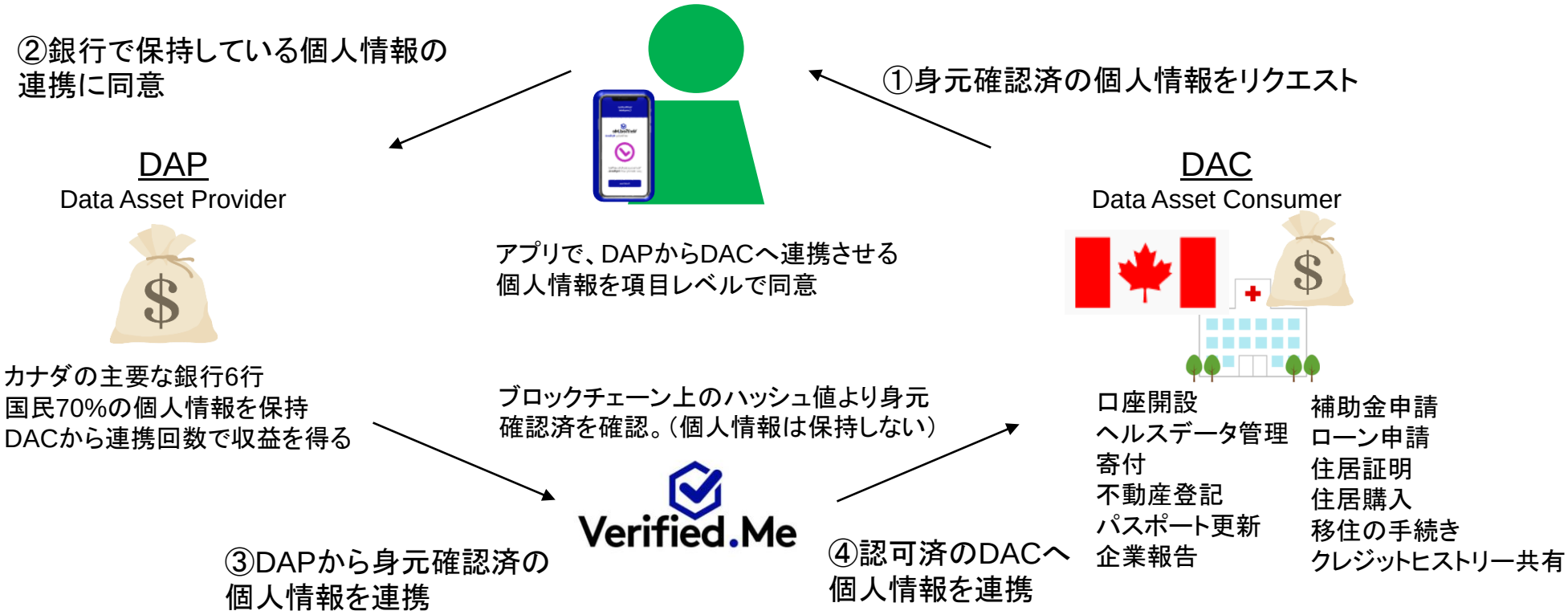


- デジタルアイデンティティの構築には、以下のような仕組みが求められた。
  - セキュリティとプライバシーを個人自身でコントロールできること。
  - データ項目を個人自身が選択できること。
  - 企業ではなく、個人が自身の個人情報に対してオーナーシップを発揮できること。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

分野を横断した、デジタルアイデンティティの活用を実証実験で検証している

- 以下の概念で、実証実験。連携済の個人情報の精度（住所変更が反映されていない等）、DAC向けの個別のポリシーの整備が課題。



- 個人情報を扱う業務プロセスのある各分野を横断し、経済へのデジタルアイデンティティの取り込みを目指している。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

Windows Helloの進展によりデファクトスタンダードのアップデートが考えられる

- 知識認証のうちのパスワードは、認証手段として最も普及しているが、紛失・盗難・推測への懸念は未解決。

- 所有物認証・生体認証の組み合わせによりそれを解決したのが、WebAuthn。各ブラウザも対応を開始。
  - W3CとFIDO Allianceが普及を進めるFIDO2の認証技術。
  - 参考）生体認証については、現在の技術では認識精度や認証情報が漏えいした場合の対処に限界があるため、単一の認証要素ではなく、多要素認証の中の一要素として扱うことが一般に推奨されている。

認証の種別	内容
知識認証 （Something you know）	パスワード等、本人しか知りえない情報を利用した認証
所有物認証 （Something you have）	IDカード、暗号鍵等、本人しか所有していない物を使用した認証
生体認証 （Something you are）	指紋、指の静脈、掌形、光彩、声紋、筆跡、動作の癖、等の本人の生体に関する電子情報

- Windows10 搭載の生体認証機能・Windows Hello においても、生体認証のI/F未対応の端末・オフィスの共有端末を想定し、OSログイン時に、USBに差し込んで指紋認証でロックを外すデバイスの検証が進んでいる。

- Windowsの対応により、パスワードレスが将来的なベストプラクティスになる可能性がある。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

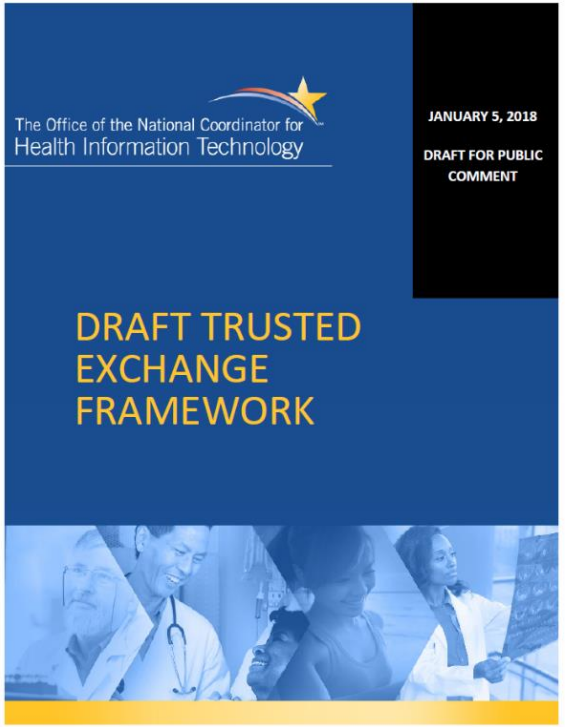
個人の健康情報を相互交換するためのフレームワーク(TEFCA)が検討されている

背景

- アメリカ保健福祉省 国家医療IT調整室(Office of the National Coordinator for Health Information Technology)において、個人の電子健康記録(EHR)を相互交換するためのフレームワークとして、TEFCA:Trusted Exchange Framework and Common Agreement の策定が進められている。
- 現在、米国には多くの保健情報交換ネットワークが存在するものの、これらのネットワーク間の相互運用性は限られており、個人のEHR活用に限界がある状態となっている。これを解決するために、TEFCAの検討が開始された。

概要

- TEFCAでは、健康情報交換ネットワーク相互接続のための標準化された方法を満たすネットワークをQHIN:Qualified Health Information Networks として定め、各ネットワークに対して参加を求める。(参加は任意)。
- TEFCAでは、以下の2パートに分けてQHINに求める要件を記載している。
  - パートA:信頼できる交換の原則
  - パートB:信頼できる取引の最低限必要な条件



検討スケジュール

- ドラフトが2018年1月5日に公開され、パブリックコメントが集められた。
- 2018年後半の確定を目指している。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

TEFCA構成要素として、複数のQHINと参加するPARTICIPANTSが存在する

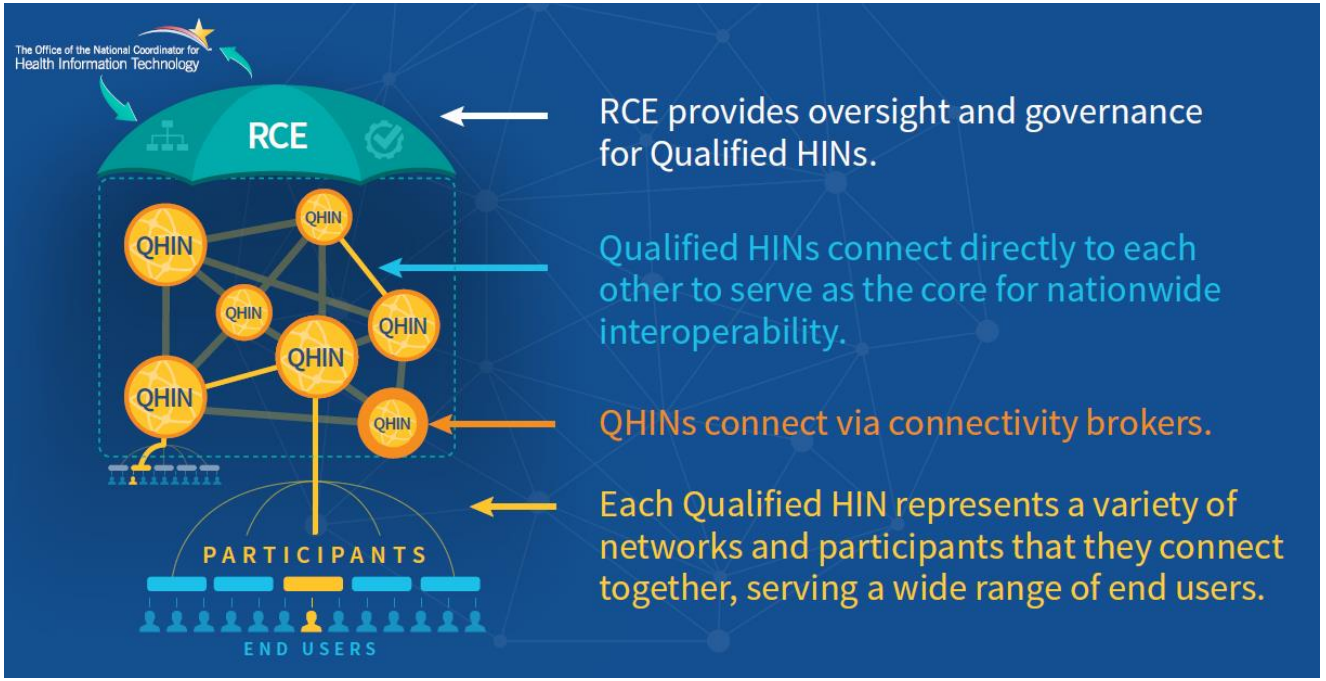
■ TEFCAを構成する要素

① RCE:TEFCAで定められた要件をQHINに対して課し、QHINを管理するエンティティ。

② QHIN:EHRなど医療データ交換を扱うネットワークのうち、TEFCAの規定する基準を満たすもの。
QHINは相互に直接的に通信を行う。

③ Participant:あるQHINに参加するエンティティ。EHRベンダ、病院組織などが該当する。

④ End User:Participantが提供するサービスを利用する利用者。医者、看護師などが該当する。
また、Participant に属する患者やその代理人を Individual と表現する。



（出所）https://www.healthit.gov/sites/default/files/draft-guide.pdf

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

TEFCAにおけるID登録では、NIST800-63のIAL2以上を満たす本人確認を求めている

■ ID登録に関する要件

- QHINは、ID登録およびクレデンシャルの発行に先立ち、個人の身元証明を少なくともIAL2で要求するものとする。
- 要件の詳細については、パートB 6.2.4項、9.1.4項（Paticipant観点）、10.1.4項（End User観点）に記載されている。

■ 要件の概要（※）

- 各 Paticipant は、QHINへアクセスするための資格証明を発行する前に、最低限IAL2で End User および Individual の本人確認を行う。
- Individual の本人確認にあたっては、 Paticipant のスタッフは権威ある審判員として、登録に先立って収集した個人の身元の知識（運転免許証やパスポートなどの法的写真身分証明書、または従業員または学校の身分証明書との物理的比較など）を使用して、情報を補完することができる。
- 参加者のスタッフまたはQHINによって収集されるすべての個人識別可能な情報は、一意のIDを解決するために必要な最小限のものに限定する必要がある。

（※）「https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf」6.2.4項、9.1.4項、10.1.4項を元に記載。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

TEFCAにおける認証では、NIST800-63のAAL2以上を満たす認証レベルを求めている

■ 認証に関する要件

- QHINは、個人の身元証明を少なくともAAL2で要求するものとする。
- また、FAL2あるいはFAL3をサポートしなければならない。
- エンドユーザー認証を必要とするFHIR APIベースのトランザクションの場合は、OpenID Connect を使用するための SMART App Authorization GuideのIDデータスコープを指定する。
- 要件の詳細については、パートB 6.2.5項、9.1.5項（Paticipant観点）、10.1.5項（End User観点）に記載されている。

■ 要件の概要（※）

- 各 Paticipant は、End User および Individual が QHIN へアクセスするための認証を、最低限AAL2で行う。
  → すなわち、2要素認証が必要となる。
- 2要素認証の認証要素として認められるものは、NIST 800-63Bに記載されているものと同じ。
  → 多要素認証デバイスまたはソフトウェアか、パスワードなどの記憶シークレットと単要素の認証デバイス またはソフトウェアの組み合わせが求められる。

（※）「https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf」6.2.5項、9.1.5項、10.1.5項および「https://www.healthit.gov/sites/default/files/draft-guide.pdf」を元に記載。

■ ヒアリングにおける補足事項

- ID登録および認証に求められる要件はTEFCAで定めているが、具体的な実現方法については言及していない。
- 有識者ヒアリングにおいて、この要件を実現する要素技術としてFIDOには注目している、とのコメントがあった。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

認証方法の議論の進め方

■ 以下の流れに沿って、認証方法の議論を進める

4.(1)認証技術及びサービス動向の調査 | 各技術の評価

- A) 認証の考え方の方針
- B) 認証技術(単一)の評価
- C) 認証技術の組み合わせの評価

5.(2)利用者及びユースケースを踏まえた認証方式に関する整理にて後述

- D) 認証技術のサービスへの適応
  - i. モデル毎の認証の要素数の考え方
  - ii. サービス①～⑦の認証、その構成案

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

A) 認証の考え方の方針・評価軸　サマリ

■ 認証の考え方の方針

関連するガイドラインを踏まえて、以下のように認証の考え方の方針をまとめた。

- ユーザの自己申告のみで発行したIDではなく、そのサービスの特性として人物とIDの紐付が求められる場合は、対面または非対面で、個人を特定できるエビデンスによりIDと人物とを紐付けていることを確認する。

- 上記の場合、単一要素の組み合わせ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の高い確実性を、一定の管理統制の元に確認する。

- 医療現場では、業務区域への入場ないし端末利用時に何らかの認証がなされていることが想定される。利用者の利便性確保のため、それらの認証を前提として、利用者認証基盤側で1要素の認証を適応することで、全体として2要素認証となるように検討する。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

NIST Special Publication 800-63-3で定義される認証の保証レベルを考慮した

- NIST SP 800-63 の概要
  - NIST SP 800-63は、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のことで、IDを処理するシステムを実装する際に米国連邦政府が満たすべき要求項目を記載している。その内容により、米国政府だけでなく民間企業や教育機関などを含めて世界中で幅広く参照され、ID登録時の身元確認や複数システム間の認証連携（フェデレーション）など、IDの取り扱い全般に関する包括的な文書となっている。第3版（NIST SP 800-63-3）が、2017年に正式に発表された。
- 本検討に求められる認証の保証レベル
  - アプリケーション利用のための初期登録に求める確からしさとして、ユーザの自己申告と申請のみで発行したIDではなく、そのサービスの特性として人物とIDの紐付が求められる場合は、NIST Special Publication 800-63-3 のうちの保証レベル（後述）より 、IAL2となる。
  - 初期登録に求める確からしさとしてIAL2を想定とした場合に、認証に求める確からしさの保証レベルの組み合わせも合わせて定義がなされていることを受けて、認証のプロセスの保証レベルとしてAAL2またはAAL3が求められる。

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	単一要素の組み合わせ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、暗号化した通信をもちいる
	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

本検討で考慮すべき認証の保証レベル

※RP（ Relying Party ）がリスクに基づいて選ぶべき、三つのプロセスに関する保証レベルがまとめられている。
- 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

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

医療情報システムの安全管理に関するガイドライン第5版を考慮し、2要素認証を前提とした

- 本ガイドライン「6.5 技術的安全対策 D.推奨されるガイドライン」に記載された、情報システムへアクセスする際の認証に関する記載事項を想定とした（以下抜粋）。これにより、アプリケーション利用のみならず、利用端末へのOSログイン・利用端末の所在する場所への入場も含めての2要素認証を仮定した。

> 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又はIC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように2つの独立した要素を用いて行う方式（2要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に2要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め2要素以上（記憶・生体計測・物理媒体のいずれか2つ以上）の認証がなされていれば、2要素認証と同等と考えてよい。

出典：「医療情報システムの安全管理に関するガイドライン第5版」

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

その他、以下のガイドラインを参照し、認証技術の評価を行った

- 前項の他、本検討で参照したガイドライン類
  - JAHIS HPKI 電子認証ガイドラインVer1.1
  - JAHIS シングルサインオンにおけるセキュリティガイドラインVer1.0
  - PCI-DSS v3.2.1
  - JIS Q 15001
  - ISO/IEC27033、ISO/IEC27017
  - クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版
  - オンライン診療の適切な実施に関する指針

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

B) 認証技術 (単一) の評価　サマリ

■ 評価方法

- 知識認証、所有物認証、生体認証の技術それぞれ4種類ずつ取り上げ、以下の観点から1~3点の3段階のスコアで評価を行った。
  - 機能の信頼性
  - 性能や負荷耐性
  - 管理負荷の低減
  - 緊急対応の実施
  - アフォーダンス
  - 実績

■ 評価結果

- 知識認証、所有物認証、生体認証のそれぞれにおいて、総合的に評価の高かった認証技術は以下の通りとなった。
- 最もスコアが高くなったのはPIN認証とパスワード認証であった。PIN認証は、その推測可能性から利用者本人の端末での利用が妥当と考えられるが、パスワード認証では業務端末利用も想定しやすい。よって、単一の認証技術をユースケースに適応する場合には、パスワード認証が最も望ましい、と考えられた。

No.	分類	認証技術	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績	スコア
1	知識認証	パスワード認証	3	2	3	1	2	3	14
4		PIN認証	3	3	1	1	3	3	14
7	所有物認証	クライアント証明書認証	3	2	1	3	1	3	13
9	生体認証	指紋認証	1	2	1	3	3	3	13

単一技術の評価で総合スコアが最も高いのは、パスワード認証となった。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

評価は、以下の一般的な認証技術を対象とした

■ 評価対象とした認証技術

No.	分類	認証技術	概要
1	知識認証 (Something you know)	パスワード認証	ユーザの入力値と、検証者が保持している情報を、照合する。
2		事前登録知識認証	ユーザが事前に登録しておいた問いかけの部分集合に対して適切な応答を返す、または選択肢の中から該当する画像を選択する等し、検証者が保持している情報と、照合する。
3		情報探索認証	ユーザと検証者間で共有して保持されている1つ以上の情報をもちいる。認証時には、検証者からの問いかけに対してユーザが情報を検索し、その入力値とで照合する。
4		PIN認証	デバイス等の操作制限や機能制限の解除時に、暗証番号をもとに、照合する。それらの情報はあらかじめデバイス内に保存がなされる。
5	所有物認証 (Something you have)	経路外認証	ユーザの所有する物理装置またはシステムに対して、電子認証の主たるチャネルとは分離された通信によって認証コードを送付する。装置に送られた認証コードは時限付きかつ1回限り有効なものとする。それを踏まえた、ユーザの入力値をもとに、照合する。
6		ワンタイムパスワード認証	ワンタイムパスワードを生成するデバイスを用いて、1回限り有効なパスワードを生成し認証にもちいる。ソフトウェア、ハードウェアの二種類があり、パスワードの生成にあたってPINなどの活性化情報の入力を要求するものもある。
7		クライアント証明書認証	ソフトウェアまたはハードウェアにあらかじめ格納した暗号鍵。暗号鍵の利用にあたっては、PINなどの活性化情報の入力を要求するものもある。モバイルのSIMカードに保持するケースもある。
8		ICカード認証	ICチップがはいったICカードをもちいる。電子証明書や、認証・決済に関する情報などを保存し、リーダーに読み取らせて利用する。クライアント証明書が保存されていたり、利用にあたってPINなどの活性化情報の入力を要求するものもある。
9	生体認証 (Something you are)	指紋認証	人物の生体的な特徴、特性を秘密情報とする。指紋、静脈、顔、虹彩など本人の肉体に付随しているものや、音声、署名など、本人の行動により生成されるものが挙げられる。生体認証のうちの一般化してきた技術、またはマスクやグローブを着用している医療現場のシーンで利用しやすいと考えられる技術について、評価を行う。また、FIDO準拠のものを想定して評価した。
10		静脈認証	
11		顔認証	
12		虹彩認証	

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

評価軸として、以下の6つの項目を設定し、スコア化した

- 認証技術に対する評価の調査観点として、本調査の目的を鑑み、下記6種類の観点を用いた。
- 高く評価できるものから順に3点、2点、1点と評価区分を点数で表現した。
- 評価区分が2つの場合には、3点と1点に振り分けた。

No.	調査観点	概要	評価区分
1	機能の信頼性	利用技術の動作の確かさについて確認する。具体的には、通常利用時に、不具合なく目的の結果が得られるものほど良いと評価する。	3点:ユーザが正しく利用すれば、正しい認証結果が返る
			2点:(区分分けなし)
			1点:ユーザが正しく利用しても、誤った認証結果が返る場合がある
2	性能や負荷耐性	利用技術の処理負荷について確認する。具体的には、目的の結果を得られるまでに処理・通信がなされるシステム上の構成の規模が少ないほど良いと評価する。	3点:処理がデバイスに閉じておりネットワークを経由しない
			2点:インターネット上のサーバで照合する処理及び通信が必要であるもの
			1点:2点の内容に加えて、認証要求とは別の回線に関する処理が必要であるもの
3	管理負荷の低減	利用技術に関するデータやデバイスの管理負荷について確認する。システムの提供側において見込まれるメンテナンスの量が少ないほど良いと評価する。初回の認証に関する管理負荷ではなく、運用に見込まれるものを想定して評価する。	3点:システム運用者側での管理が不要のもの
			2点:システム運用者側で管理が必要で、決まった時期に対応が必要となるもの
			1点:システム運用者側で管理が必要で、ユーザ毎に都度対応が必要となるもの

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

評価軸として、以下の6つの項目を設定し、スコア化した

No.	調査観点	概要	評価区分
4	迅速な緊急対応の実施	緊急時(救急対応、災害時対応など)に、利用者の迅速な対応を損なうことなく認証を行うことが可能か確認する。損ないにくいものほど良いと評価する。	3点:ユーザの状況を問わないで緊急対応が可能となるもの
			2点:(区分分けなし)
			1点:ユーザの状況によっては緊急対応ができないもの
5	利用者のアフォーダンスなどの利用性	認証技術の利用者が、利用方法の理解、習得、利用をスムーズに行えるものかを確認する。スムーズに行えると考えられるものほど良いと評価する。	3点:デバイスに搭載されるなど一般的で、直感的なIFで利用されているもの
			2点:3点のようには一般的ではないが、直感的なIFで利用されているもの
			1点:利用やその設定にある程度のITリテラシーを要するもの
6	利用実績	当該技術が実際に運用されているサービス、ユースケースについて確認する。具体的には、金融分野のオンラインバンキングや、ヘルスケア分野の本案件との類似ユースケースでの利用実績があるほど良い評価とする。	3点:オンラインバンキング、ヘルスケア分野での利用製品で利用実績があるもの
			2点:(区分分けなし)
			1点:3点の内容にならないもの

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

評価結果(1/2):各項目のスコアをその判断理由と共に記載

No.	認証技術	機能の信頼性		性能や負荷耐性		管理負荷の低減	
1	パスワード認証	3	単純なデータの照合であるため	2	認証サーバでデータを照合する処理及び通信が必要であるため	3	利用者によるパスワード再発行の機能を実装すればよい
2	事前登録知識認証	3	同上	2	同上	1	利用者が登録した情報を失念した場合の措置が必要
3	情報探索認証	3	同上	2	同上	1	乱数表等の紛失や交換についての措置が必要
4	PIN認証	3	同上	3	デバイス内のみで照合するため	1	利用者が登録した情報を失念した場合の措置が必要
5	経路外認証	3	同上	1	上述のものに加えて、電話回線の通信が挟まるため	2	電話回線の利用の外部委託の維持が必要
6	ワンタイムパスワード認証	3	同上	2	認証サーバでデータを照合する処理及び通信が必要であるため	1	ハードは紛失や交換についての措置が必要
7	クライアント証明書認証	3	同上	2	Webサーバで証明書を照合する処理及び通信が必要であるため	1	クライアント証明書の再発行・失効・有効期限切れへの措置が必要
8	ICカード認証	3	同上	2	認証サーバでデータを照合する処理及び通信が必要であるため	1	ICカード(保存している情報)の再発行・失効・有効期限切れへの措置が必要
9	指紋認証	1	本人拒否率及び他人受入率が見込まれる場合があるため	2	デバイス内での照合結果をサーバで処理する通信が必要であるため	1	本人拒否に関する問い合わせへの措置や利用機器のメンテナンスが必要
10	静脈認証	1	同上	2	同上	1	同上
11	顔認証	1	同上	2	同上	1	同上
12	虹彩認証	1	同上	2	同上	1	同上

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

評価結果(2/2):各項目のスコアをその判断理由と共に記載

No.	認証技術	迅速な緊急対応の実施		アフォーダンスなどの利用性		調査済製品での利用実績	
1	パスワード認証	1	利用者がパスワードを失念し自身で再発行する場合があるため	2	直感的なデザインであるわけではないものの、認証技術の中でも一般に広く認識されているIFともいえるため	3	多数あるため略
2	事前登録知識認証	1	利用者が登録した情報を失念する場合があるため	1	直感的なIFではないため	1	なし
3	情報探索認証	1	利用者が携帯していない場合があるため	1	直感的なIFではないため	3	FINEMAX(乱数表)
4	PIN認証	1	利用者が登録した情報を失念する場合があるため	3	キャッシュカードに利用されたり、デバイスに搭載される等一般的かつ直感的なIFが多いため	3	e-NINSHO(マイナンバーカード)、Taikoban(HPKIカード)等
5	経路外認証	1	利用者が携帯していない場合があるため	1	直感的なIFではないため	3	Uni-ID(SMS利用)
6	ワンタイムパスワード認証	1	同上	1	直感的なIFではないため	3	RSA SecurID Access(ハード)、VIP Access(ソフト)等
7	クライアント証明書認証	3	インストール済の端末が利用できれば問題ない	1	直感的なIFではなく設定にある程度のリテラシを要する	3	Pass Logic
8	ICカード認証	1	利用者が携帯していない場合があるため	2	直感的なIFであるため	3	e-NINSHO(マイナンバーカード)、Taikoban(HPKIカード)等
9	指紋認証	3	本人拒否率の吟味は要するが、本人の身体に問題なければ問題ない。	3	デバイスに搭載される等一般的かつ直感的なIFが多いため	3	Finplex
10	静脈認証	3	同上	2	直感的なIFが多いため	3	静紋、PalmSecure
11	顔認証	3	同上	2	直感的なIFが多いが、最新のデバイスに限り搭載されている点から3点とはしなかった	3	Finplex、API連携プラットフォームサービス
12	虹彩認証	3	同上	2	直感的なIFが多いため	3	Finplex

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

IF:インターフェイス

知識認証の評価結果への見解

■ 評価結果への見解

- 知識認証では全体に、緊急対応の実施について低い評価となったものの、平常時であれば利用しやすい技術であるといえる。緊急時への適応を考えるには、失念した利用者向けの対応を検討する必要がある。
- 単独で認証技術を利用する場合には、パスワード認証が適すると考える。

No.	分類	認証技術	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績	スコア
4	知識認証	PIN認証	3	3 ①	1	1	3	3	14
1		パスワード認証	3	2	3 ②	1	2	3	14
3		情報探索認証	3	2	1	1	1	3	11
2		事前登録知識認証	3	2	1	1	1	1	9

- ①PIN認証
  - 本人が入力値を失念した場合に、デバイス等の設定値のリセットが必要となるため、管理負荷の低減、緊急対応の実施の項目が低い評価となった。配布時にPINコードの個人での保管に関する事前周知を行うなど、緊急時への適応には、リスクに留意した対応が必要と考える。
  - PIN認証のみでの利用は、その推測可能性の面から、共用端末ではなく、利用者本人の端末においての利用を対象とするのが妥当と考える。
- ②パスワード認証
  - アプリ側でパスワードの再発行を実装可能ではあるものの、これにより緊急時の対応スピードを損なう。またアフォーダンス等のデザイン面については、普段からWebを利用する一般の利用者には、認証のフローに関する認識も比較的定着しているためにあまり問題とならない場合も考えられる。
  - 共用端末において認証を行う場合は、パスワードポリシーを十分複雑にすれば、PIN認証よりも推測困難となるためPIN認証よりも優れていると考える。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

知識認証の評価結果への見解

- 評価結果への見解
  - その他
    - 情報探索認証では探索の元となる物を不所持の場合、認証を行うことができない。近年では、探索の元となる乱数表等の並びの情報が、不審な電話を経て奪取される被害も所有者あり、ワンタイムトークンへ移行するケースも見受けられる。
    - 事前登録知識認証では登録済のQAを失念した場合、認証を行うことができない。NIST SP800-63Bでは親しい人物による推測の可能性により認証技術として認めないという見解もある。加えて運用側への失念の問い合わせが頻発するとの声もあり実装が減ってきている。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

所有物認証の評価結果への見解

■ 評価結果への見解

- 所有物認証では、知識認証と同様に管理負荷の低減や緊急対応の実施などの項目で1点の評価が多く見受けられたが、全体的に製品の実績があり、比較的スコアのばらつきが少なかった。それぞれの技術特性への理解を深め、利用シーンに応じて使い分ける必要がある。

No.	分類	認証技術	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績	スコア
7	所有物認証	クライアント証明書認証	3	2 ①	1	3	1	3	13
8		ICカード認証	3	2 ②	1	1	2	3	12
5		経路外認証	3 ③	1	2	1	1	3	11
6		ワンタイムパスワード認証	3	2 ④	1	1	1	3	11

- ①クライアント証明書認証
  - 緊急対応の実施について生体認証を除いて、本技術が最も高いスコアとなった。アフォーダンスの項目の評価が低く運用面への懸念はあるものの、医療施設の業務用として管理可能な端末を対象として、セットアップ済の端末を利用者に配布できる組織での利用を想定する場合やITリテラシーがある程度見込まれる利用者を対象として手順書を配布する等を行う場合は問題なく活用できると考える。
- ②ICカード認証
  - 管理負荷や緊急対応の実施など、運用面への懸念はあるものの、JPKI、HPKI及び社員証や入館証等の既存の仕組みがあるものを利用することで、普及の難易度がある程度下がると考える。
  - ただし緊急時に利用する端末においてカードリーダーが利用可能な状況にあるのかは業務内容を踏まえて検討する必要がある。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

所有物認証の評価結果への見解

- 評価結果への見解
  - ③経路外認証
    - 電話やSNSが利用可能な状況であれば特別なデバイスを必要としない技術となる。ただし複数経路を利用するために、他社の管轄内において障害があると認証ができなくなるリスクが考えられるため緊急時というよりは、平常時に利用しやすいものと考える。
    - Yahooなど一般でも使われており、認証方法として一般に受け入れやすいものと考えられる。
  - ④ワンタイムパスワード認証
    - 管理負荷や緊急対応、及びアフォーダンスの点で低い評価となっており、ワンタイムパスワードの生成機器の不所持や交換への懸念はある。ただし、スマホ利用者向けにGoogle Authenticator の利用を検討するなどでこれらの懸念点をカバーすることも可能と考える。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

生体認証の評価結果への見解

■ 評価結果への見解

- 生体認証では、知識認証および所有物認証とは異なる評価の傾向となり、機能の信頼性、管理負荷の低減では低い評価となったものの、アフォーダンス、緊急対応の実施、は高い評価となった。認証の精度について検討の余地があるものの、認証失敗時の代替方法の検討や技術の進歩や他の認証方法との組み合わるなどの工夫により低い評価を補い、高い評価となった部分を活かすことが可能と考える。

  ※NIST SP800-63B より、現在の技術では認識精度や認証情報が漏えいした場合の対処に限界があるため、単一の認証要素ではなく、多要素認証の中の一要素として扱うこととされている。

No.	分類	認証技術	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績	スコア
9	生体認証	指紋認証	1 ①	2 ②	1 ③	3 ④	3	3	13
10		静脈認証	1	2	1	3	2	3	12
11		顔認証	1	2	1	3	2	3	12
12		虹彩認証	1	2	1	3	2	3	12

- ①機能の信頼性
  - 現状では全体に低い評価となったが、一般に実証実験も進められているため、この点への理解を深めるためにも今後の技術動向の把握は有用であると考える。
- ②性能や負荷耐性
  - FIDO準拠の技術を想定して評価した。これは生体情報を個別のサーバに集約して保存しネットワーク経由で照合する場合よりは、FIDO準拠により照合自体はデバイス側で処理する場合のほうが、性能面で優れていると考えられるため、そのような前提で評価を行った。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

生体認証の評価結果への見解

- 評価結果への見解
  - ③管理負荷の低減
    - 一般に生体認証を導入しようとすると、利用機器のメンテナンスが煩雑となる。しかし、広くデバイスにカメラが搭載され、Touch ID・Face ID・Windows Hello等の一般利用も進みつつあることから、今後の技術動向も踏まえて機能を利用することができれば、管理負荷を低減することも可能となる。
  - ④緊急利用の実施、アフォーダンス
    - アフォーダンスの面からは、デバイスへの機能搭載が比較的進んでいる指紋認証が特に高い評価となった。また静脈や顔、虹彩など他の方式についても、緊急利用やアフォーダンスともに知識認証、所有物認証に比べて高い評価となった。
    - よって、ユーザビリティが他の認証技術の分類群よりも高く、利用者のITリテラシーへの懸念も少ないことが生体認証の特徴と言える。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

C) 認証技術の組み合わせの評価　サマリ

- 2要素認証を考慮した場合、医療従事者、介護従事者が利用する業務用端末からのアクセスには、緊急対応などスピード感に優れたクライアント証明書認証＆生体認証の組み合わせでの利用者認証が最も適切と考えられた。
  - 生体認証の導入が現場にて現実的ではない場合には、パスワード認証＆クライアント証明書認証の組み合わせが推奨となる。
  - 加えてID登録時には、オンラインでの資格・本人確認の方法として、HPKIの活用が望ましい。
  - 介護従事者など国家資格ではない利用者については、所属組織の妥当性によって利用者IDの登録を可能とすることが可能と考える。

- 2要素認証を考慮した場合、患者の私用端末からのアクセスには、総合評価が最も高いパスワード認証＆指紋認証が利用が適切と考えられた。
  - 加えてID登録時には、オンラインでの本人確認の方法として、公的個人認証の活用が望ましい。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせを評価するための前提事項

- 利用者へ要求する認証技術の組み合わせを検討することを目的として、評価した認証技術の組み合わせを検討した。
- 組み合わせは、知識認証・所有物認証・生体認証、のうちから2種類の分類を満たすようにした。また、評価には各認証技術の評価結果のスコアを参考値として利用した。
- 認証技術ごとに考慮した前提事項を以下にまとめる。

No.	認証技術	組み合わせを検討する際の前提事項
2	事前登録知識認証	認証技術の評価結果を踏まえて、他の認証技術と組み合わせた利用について、これらの技術の利用は考慮しない
3	情報探索認証	
4	PIN認証	・一般にトークン・ICカード・クライアント証明書に本機能が組み込まれていることを踏まえて検討する ・その他、一般にスマホ等のデバイスにも設定可能ではあるが、その場合にはMDMを導入することでデバイスのポリシーを制御し、設定を強制させる必要がある
7	クライアント証明書認証	他の認証技術とは異なり、その特性により、個人である証明というよりも、認められた端末であることの証明にもちいられる技術であることを踏まえて検討する
8	ICカード認証	・一般に、ICカードには、機能解除時にPIN設定があるものとないものがある ・JPKIについて検討が進められている”PINなし認証”は、組み合わせについて考慮しない
9	指紋認証	・生体認証の実際の導入については、技術評価の結果を踏まえて、技術動向により取り入れる時期感に留意する必要があるが、組み合わせの検討のなかではそれを考慮しない ・指紋認証、顔認証、虹彩認証は、専用デバイスの他、PCやスマホに必要な機器が付属するなどで一般化しつつある。一方で静脈認証は読み取り用のデバイス機器が外付けで必要となる点が異なる
10	静脈認証	
11	顔認証	
12	虹彩認証	

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせの評価結果

- 認証技術の組み合わせを、スコアの和とともにマトリックスにまとめた。
- 内訳を次頁以降に、評価項目毎に6点満点の指数で示すが、欠点のない組み合わせはなく、技術毎の特性と評価結果を踏まえつつ、利用イメージをもとに、組み合わせを吟味する必要がある。

分類	認証技術		知識		所有				生体			
			PIN認証	パスワード認証	クライアント証明書認証	ICカード認証	経路外認証	ワンタイムパスワード認証	指紋認証	静脈認証	顔認証	虹彩認証
		スコア	14	14	13	12	11	11	13	12	12	12
知識	PIN認証	14										
	パスワード認証	14										
所有	クライアント証明書認証	13	27	27								
	ICカード認証	12	26	26								
	経路外認証	11	25	25								
	ワンタイムパスワード認証	11	25	25								
生体	指紋認証	13	27	27	26	25	24	24				
	静脈認証	12	26	26	25	24	23	23				
	顔認証	12	26	26	25	24	23	23				
	虹彩認証	12	26	26	25	24	23	23				

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせの検討結果と利用イメージ（総合スコア　降順）

No.	スコア	知識	所有	生体	利用イメージ					
						私用端末	業務用デバイス	業務用PC	平常時	緊急時
1	27	PIN認証	クライアント証明書認証	–	・ブラウザからアプリへアクセス時にクライアント証明書を選択、PINで機能を解除 ・MDMでデバイスの認証をポリシーで管理、クライアント証明書を設定		●	●	●	
2	27	PIN認証	–	指紋認証	・指紋認証のデバイス機器をPINで機能解除 ・MDMでデバイスの認証をポリシーで管理、アプリ起動時に指紋認証を求める		●	●	●	
3	27	パスワード認証	–	指紋認証	・指紋認証のデバイス機器を利用し、フォームへパスワードも入力	●	●	●	●	
4	27	パスワード認証	クライアント証明書認証	–	・クライアント証明書が設定された端末から、フォームへパスワードを入力		●	●	●	

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせの検討結果と利用イメージ（総合スコア　降順）

No.	スコア	知識	所有	生体	利用イメージ					
						私用端末	業務用デバイス	業務用PC	平常時	緊急時
5	26	–	クライアント証明書認証	指紋認証	・クライアント証明書が設定された端末で、指紋認証のデバイス機器を利用		●	●	●	●
6	26	PIN認証	–	静脈認証	・生体認証向けの機器を利用し、PINで機能解除			●	●	
7	26	PIN認証	–	顔認証	・同上			●	●	
8	26	PIN認証	–	虹彩認証	・同上			●	●	
9	26	パスワード認証	–	静脈認証	・フォームへパスワードを入力、デバイス機器で静脈認証			●	●	
10	26	パスワード認証	–	顔認証	・フォームへパスワードを入力、カメラにより顔認証	●	●	●	●	
11	26	パスワード認証	–	虹彩認証	・フォームへパスワードを入力、カメラにより虹彩認証	●	●	●	●	
12	26	PIN認証	ICカード認証	–	・PINが設定されたICカードをリーダーへかざす	●	●	●	●	
13	26	パスワード認証	ICカード認証	–	・ICカードをリーダーへかざし、フォームへパスワードを入力	●	●	●	●	

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせの検討結果と利用イメージ（総合スコア　降順）

No.	スコア	知識	所有	生体	利用イメージ					
						私用端末	業務用デバイス	業務用PC	平常時	緊急時
14	25	–	ICカード認証	指紋認証	・ICカードをリーダーへかざし、デバイス機器より指紋認証			●	●	
15	25	PIN認証	経路外認証	–	・MDMでデバイスの認証をポリシーで管理、SMSや電話で通知されたコードを、フォームへ入力		●※	●※	●	
16	25	PIN認証	ワンタイムパスワード認証	–	・トークンをPINコードで有効化、表示されたワンタイムパスワードをフォームへ入力		●	●	●	
17	25	–	クライアント証明書認証	静脈認証	・クライアント証明書が設定された端末で、デバイス機器より静脈認証			●	●	●
18	25	–	クライアント証明書認証	顔認証	・クライアント証明書が設定された端末で、カメラにより顔認証		●	●	●	●
19	25	–	クライアント証明書認証	虹彩認証	・クライアント証明書が設定された端末で、カメラにより顔認証		●	●	●	●
20	25	パスワード認証	経路外認証	–	・パスワードをフォームへ入力し、画面遷移後電話やSNSで通知されたコードも入力	●	●	●	●	
21	25	パスワード認証	ワンタイムパスワード認証	–	・パスワードをフォームへ入力し、画面遷移後ワンタイムパスワードも入力	●	●	●	●	

- No.15は、医療現場で緊急の電話をかけているときなど、経路外に電話を利用することは難しい。一方、一般の私用端末での経路外認証の利用では、PIN認証を強制することが難しい。私用端末では業務用スマホ等のようにMDMの導入でこれを強制することができないためである。これを受けて、業務用端末でSNSにコードを通知するか、PIN認証等が強制された業務用デバイスに電話でコードを受け取り、ログイン自体は業務用PCで行うイメージが想定される。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証技術の組み合わせの検討結果と利用イメージ（総合スコア　降順）

No.	スコア	知識	所有	生体	利用イメージ					
						私用端末	業務用デバイス	業務用PC	平常時	緊急時
22	24	–	経路外認証	指紋認証	・MDMでデバイス認証をポリシー管理、SMSや電話からの通知コードを、フォームへ入力		●	●	●	
23	24	–	ワンタイムパスワード認証	指紋認証	・トークンを指紋認証で機能解除し、ワンタイムパスワードをフォームへ入力	●	●	●	●	
24	24	–	ICカード認証	静脈認証	・デバイス機器より静脈認証後、リーダーにICカードをかざす			●	●	
25	24	–	ICカード認証	顔認証	・カメラにより顔認証後、リーダーにICカードをかざす			●	●	
26	24	–	ICカード認証	虹彩認証	・カメラにより虹彩認証後、リーダーにICカードをかざす			●	●	
27	23	–	経路外認証	静脈認証	・SNSで通知されたコードを入力、デバイス機器より静脈認証			●	●	
28	23	–	経路外認証	顔認証	・SNSで通知されたコードを入力、デバイス機器より顔認証	●	●	●	●	
29	23	–	ワンタイムパスワード認証	静脈認証	・ワンタイムパスワードをフォームに入力し、デバイス機器より静脈認証			●	●	
30	23	–	ワンタイムパスワード認証	顔認証	・ワンタイムパスワードをフォームに入力し、カメラより顔認証	●	●	●	●	
31	23	–	経路外認証	虹彩認証	・SNSで通知されたコードを入力、カメラにより虹彩認証	●	●	●	●	
32	23	–	ワンタイムパスワード認証	虹彩認証	・ワンタイムパスワードをフォームに入力し、カメラにより虹彩認証	●	●	●	●	

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

医療従事者、介護従事者が利用する業務用端末からのアクセスに適した認証方法

- 医療従事者、介護従事者が利用する業務用端末からのアクセスには、クライアント証明書認証＆生体認証の組み合わせでの利用者認証が最も適する。
  - 医療従事者、介護従事者が業務用端末から個人情報へアクセスする場合、平常時と緊急時といった場面を問わず、医療業務のスピード感を損なわない組み合わせであることが望ましい。
  - よって、緊急対応の実施で最も高い評価となったクライアント証明書＆生体認証の組み合わせ(次スライド参照)が適していると考えられた。
  - また、医療従事者はゴーグル・マスク・手袋などを装着しているケースも考えられるため、生体認証を用いる場合は指紋や静脈認証よりも、顔認証または虹彩認証が比較的現場の動きを妨げにくいものと考える。ただし、カメラを利用できない環境など、顔や虹彩認証が難しいケースでは、指紋認証または静脈認証に切り替えられるようにしておく方法も考えられる。
- 次点として、パスワード認証＆クライアント証明書認証の組み合わせが適切と考えられた。
  - 緊急対応の実施で2番目に高い評価となったのは、PIN認証＆クライアント証明書認証の組み合わせであった。ただし、クライアント証明書認証は端末の識別となっており、個人の専用端末であればこの組み合わせで問題ないが、共用端末であればPINのみの認証となり、本人認証は強度に欠けるものと考える。
  - 生体認証を除いてかつ次に高い評価であったパスワード認証＆クライアント証明書認証の組み合わせの方がPIN認証よりも望ましいと考える。ただし、クライアント証明書認証のアフォーダンスの評価が低い点は、利用手順の周知などにより対応を要するものと考える。
- 最終的に生体認証と、知識認証のどちらをクライアント証明書認証と組み合わせるのかは、実際の現場でのニーズも考慮に入れて使い分けることが望ましい。
- また、これらの組み合わせでは資格認証を行うことが出来ないため、上記の検討結果にHPKIをどう組み入れていくか検討する必要がある。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

【参考】認証技術の組み合わせの検討結果(緊急対応の実施、スコア降順)

＊スコア内訳は、6点満点の指数で記載

No.	スコア計	知識	所有	生体	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績
1	26	–	クライアント証明書認証	指紋認証	0.7	0.7	0.3	1.0	0.7	1.0
2	25	–	クライアント証明書認証	静脈認証	0.7	0.7	0.3	1.0	0.5	1.0
3	25	–	クライアント証明書認証	顔認証	0.7	0.7	0.3	1.0	0.5	1.0
4	25	–	クライアント証明書認証	光彩認証	0.7	0.7	0.3	1.0	0.5	1.0
5	27	PIN認証	クライアント証明書認証	–	1.0	0.8	0.3	0.7	0.7	1.0
6	27	PIN認証	–	指紋認証	0.7	0.8	0.3	0.7	1.0	1.0
7	27	パスワード認証	–	指紋認証	0.7	0.7	0.7	0.7	0.8	1.0
8	27	パスワード認証	クライアント証明書認証	–	1.0	0.7	0.7	0.7	0.5	1.0
9	26	PIN認証	–	静脈認証	0.7	0.8	0.3	0.7	0.8	1.0
10	26	PIN認証	–	顔認証	0.7	0.8	0.3	0.7	0.8	1.0
11	26	PIN認証	–	光彩認証	0.7	0.8	0.3	0.7	0.8	1.0
12	25	–	ICカード認証	指紋認証	0.7	0.7	0.3	0.7	0.8	1.0
13	26	パスワード認証	–	静脈認証	0.7	0.7	0.7	0.7	0.7	1.0
14	26	パスワード認証	–	顔認証	0.7	0.7	0.7	0.7	0.7	1.0
15	26	パスワード認証	–	光彩認証	0.7	0.7	0.7	0.7	0.7	1.0
16	24	–	経路外認証	指紋認証	0.7	0.5	0.5	0.7	0.7	1.0
17	24	–	ワンタイムパスワード認証	指紋認証	0.7	0.7	0.3	0.7	0.7	1.0
18	24	–	ICカード認証	静脈認証	0.7	0.7	0.3	0.7	0.7	1.0
19	24	–	ICカード認証	顔認証	0.7	0.7	0.3	0.7	0.7	1.0
20	24	–	ICカード認証	光彩認証	0.7	0.7	0.3	0.7	0.7	1.0
21	23	–	経路外認証	静脈認証	0.7	0.5	0.5	0.7	0.5	1.0
22	23	–	経路外認証	顔認証	0.7	0.5	0.5	0.7	0.5	1.0
23	23	–	ワンタイムパスワード認証	静脈認証	0.7	0.7	0.3	0.7	0.5	1.0
24	23	–	ワンタイムパスワード認証	顔認証	0.7	0.7	0.3	0.7	0.5	1.0
25	23	–	経路外認証	光彩認証	0.7	0.5	0.5	0.7	0.5	1.0
26	23	–	ワンタイムパスワード認証	光彩認証	0.7	0.7	0.3	0.7	0.5	1.0
27	26	PIN認証	ICカード認証	–	1.0	0.8	0.3	0.3	0.8	1.0
28	25	PIN認証	経路外認証	–	1.0	0.7	0.5	0.3	0.7	1.0
29	25	PIN認証	ワンタイムパスワード認証	–	1.0	0.8	0.3	0.3	0.7	1.0
30	26	パスワード認証	ICカード認証	–	1.0	0.7	0.7	0.3	0.7	1.0
31	25	パスワード認証	経路外認証	–	1.0	0.5	0.8	0.3	0.5	1.0
32	25	パスワード認証	ワンタイムパスワード認証	–	1.0	0.7	0.7	0.3	0.5	1.0

緊急対応の実施では、クライアント証明書x生体認証が最も優れる

生体認証以外では、クライアント証明書xパスワードが緊急対応に優れている

私用端末からアクセスする場合に適した認証方法

- 私用端末からのアクセスには、パスワード認証＆指紋認証が適する。
  - デバイスの台数が非常に多く組織的な管理の難しい私用端末からのアクセスには、端末の設定に依存するようなPIN認証・クライアント証明書認証の利用は不向きである。また全国民への普及度や導入コストを考慮すると、特別な外付けデバイスを要するもの、新規のトークンやICカードの配布を要するものも、不向きである。
  - 総合スコアが最も高いパスワード認証＆指紋認証が適すると考えられた(次スライド参照)。
    - ただし、パスワード認証＆指紋認証では、指紋認証に対応したデバイス機器が必要である。しかしながら、近年のモバイル端末には指紋認証の機能が搭載済のものも増えつつあることを受けて、特にスマホのネイティブアプリで利用する組み合わせとして適するものと考える。
    - ただし、この組み合わせでは、本人確認や資格の確認はできない。これには、既存の公的個人認証の活用を別途検討する必要がある。

- 次点として、PIN認証＆ICカード認証（マイナンバーカードを想定した場合に利用可能）が適していると考えられる。
  - ICカードの配布を行う必要があるが、これはマイナンバーカードの活用を想定することで導入コストを軽減できる。
  - また、個人が自身の医療情報にのみアクセスする場合には、ID登録時に本人確認が済めば以降の確認は不要となるため、ログイン時にマイナンバーカードを都度利用せずとも、パスワード認証＆指紋認証でサービスを利用させると、認証強度を満たしつつユーザビリティを高められるものと考える。

- その他、それ以降のスコア合計の順で、汎用的な組み合わせを考えた場合には、パスワード認証＆経路外認証の組み合わせが適する。これは、Yahoo、Googleなどの一般のWebサービスでも実績のある組み合わせとなる。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

5.(2) 利用者及びユースケースを踏まえた認証方式に関する整理 C) 認証技術の組み合わせの検討

＊スコア内訳は、6点満点の指数で記載

【参考】認証技術の組み合わせの検討結果(スコア合計の降順)

No.	スコア計	知識	所有	生体	機能の信頼性	性能や負荷耐性	管理負荷の低減	緊急対応の実施	アフォーダンス	調査済製品の実績
1	27	PIN認証	クライアント証明書認証	–	1.0	0.8	0.3	0.7	0.7	1.0
2	27	PIN認証	–	指紋認証	0.7	0.8	0.3	0.7	1.0	1.0
3	27	パスワード認証	–	指紋認証	0.7	0.7	0.7	0.7	0.8	1.0
4	27	パスワード認証	クライアント証明書認証	–	1.0	0.7	0.7	0.7	0.5	1.0
5	26	–	クライアント証明書認証	指紋認証	0.7	0.7	0.3	1.0	0.7	1.0
6	26	PIN認証	–	静脈認証	0.7	0.8	0.3	0.7	0.8	1.0
7	26	PIN認証	–	顔認証	0.7	0.8	0.3	0.7	0.8	1.0
8	26	PIN認証	–	光彩認証	0.7	0.8	0.3	0.7	0.8	1.0
9	26	パスワード認証	–	静脈認証	0.7	0.7	0.7	0.7	0.7	1.0
10	26	パスワード認証	–	顔認証	0.7	0.7	0.7	0.7	0.7	1.0
11	26	パスワード認証	–	光彩認証	0.7	0.7	0.7	0.7	0.7	1.0
12	26	PIN認証	ICカード認証	–	1.0	0.8	0.3	0.3	0.8	1.0
13	26	パスワード認証	ICカード認証	–	1.0	0.7	0.7	0.3	0.7	1.0
14	25	–	クライアント証明書認証	静脈認証	0.7	0.7	0.3	1.0	0.5	1.0
15	25	–	クライアント証明書認証	顔認証	0.7	0.7	0.3	1.0	0.5	1.0
16	25	–	クライアント証明書認証	光彩認証	0.7	0.7	0.3	1.0	0.5	1.0
17	25	–	ICカード認証	指紋認証	0.7	0.7	0.3	0.7	0.8	1.0
18	25	PIN認証	経路外認証	–	1.0	0.7	0.5	0.3	0.7	1.0
19	25	PIN認証	ワンタイムパスワード認証	–	1.0	0.8	0.3	0.3	0.7	1.0
20	25	パスワード認証	経路外認証	–	1.0	0.5	0.8	0.3	0.5	1.0
21	25	パスワード認証	ワンタイムパスワード認証	–	1.0	0.7	0.7	0.3	0.5	1.0
22	24	–	経路外認証	指紋認証	0.7	0.5	0.5	0.7	0.7	1.0
23	24	–	ワンタイムパスワード認証	指紋認証	0.7	0.7	0.3	0.7	0.7	1.0
24	24	–	ICカード認証	静脈認証	0.7	0.7	0.3	0.7	0.7	1.0
25	24	–	ICカード認証	顔認証	0.7	0.7	0.3	0.7	0.7	1.0
26	24	–	ICカード認証	光彩認証	0.7	0.7	0.3	0.7	0.7	1.0
27	23	–	経路外認証	静脈認証	0.7	0.5	0.5	0.7	0.5	1.0
28	23	–	経路外認証	顔認証	0.7	0.5	0.5	0.7	0.5	1.0
29	23	–	ワンタイムパスワード認証	静脈認証	0.7	0.7	0.3	0.7	0.5	1.0
30	23	–	ワンタイムパスワード認証	顔認証	0.7	0.7	0.3	0.7	0.5	1.0
31	23	–	経路外認証	光彩認証	0.7	0.5	0.5	0.7	0.5	1.0
32	23	–	ワンタイムパスワード認証	光彩認証	0.7	0.7	0.3	0.7	0.5	1.0

PIN認証、クライアント証明書認証、PIN認証、ICカード認証を除外した場合、パスワード認証x指紋認証、が最も優れた候補となる。

JPKIの利用を想定する場合、PIN認証、ICカード認証も選択できる

PIN認証、クライアント証明書認証、PIN認証、ICカード認証を除外した場合、パスワード認証x経路外認証が次点となる。

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ユースケースの詳細化およびモデル化、は以下のようなプロセスで実施した

- 各サービスの想定
  - 認証方式を検討するためには、全国保健医療情報ネットワークの7つのサービスについて、そのサービスの内容や全体のシステム構成を考慮することが望ましい。
  - しかしながら、各サービスにおいてのこれらの内容は検討段階にあり、現時点で確定していること、未確定である部分に対する現状の想定などを整理し、認証方式等を検討材料とする必要がある。
  - そのため、各サービス内容に関する公開情報及びサービス関係者へのヒアリング、及びそれらを参考としたNRI想定も含め、想定されるサービス内容を整理した。

- ユースケースの洗い出しとモデル化
  - 各サービスの想定の結果を踏まえ、各サービスのユースケースを洗い出した上で“扱う情報”、“ネットワーク”、“使用端末”、“認証される者”の観点から12のモデルに分類し、認証方式の検討材料とした。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

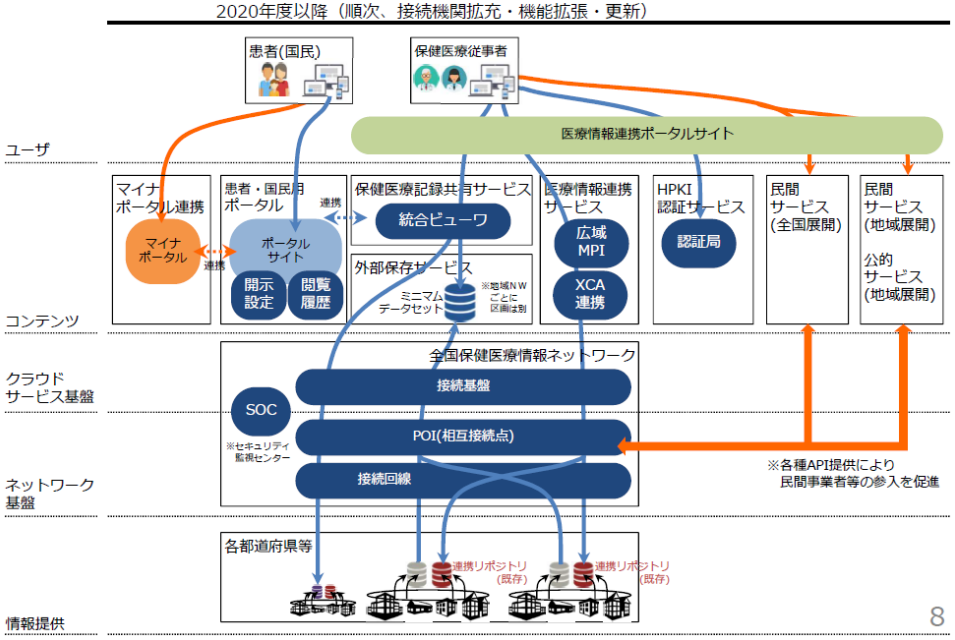
認証技術の検討には、ポータルサイトからのログイン、早いレスポンス、2要素認証、HPKIやマイナポータル活用、情報の機密性の高さ、私用スマホ利用等を考慮する必要がある

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

本格的高齢社会の到来にふさわしい健診内容の見直し、電子カルテの全国的統一化や介護分野における科学的かつ統一的な記録の在り方の開発、確立を図りながら、全国的な保健医療情報ネットワークを整備し、保健医療情報関係者等が、円滑に国民、患者等の健康情報を共有できるようになる。これによって、今まで保健医療データの利活用が出来なかった地域を含めて、初診時などに、保健医療関係者が患者の状況を把握し、過去の健診データや治療履歴等を踏まえた最適な診断や診療の選択肢を提供できるようにすることを目指す。

サービスの構造

医療情報連携ポータルサイトから、保健医療記録共有サービス(総合ビューワ)へログインし、必要な医療情報を閲覧する。患者は、ポータルサイトからログインし、総合ビューワの設定ができる(次スライド)。



サービス想定(NRI)

■ 利用者(規模)
- 医師、薬剤師、看護師等の医療従事者(約250万人)
- 介護従事者(約100万人)
- 患者、患者家族(約250万人)*閲覧履歴確認、開示設定のみ
- 各施設の規模は参考資料参照。

◆閲覧される情報の機密性
- 診療記録など要配慮個人情報を含み、機密性は高い。

◆ネットワーク
- 公衆ネットワークを想定。

◆システムの管理主体
- 国から民間へ委託を想定。

◆デバイス
- 院内PC、タブレット、患者私用のスマホ、タブレット等。

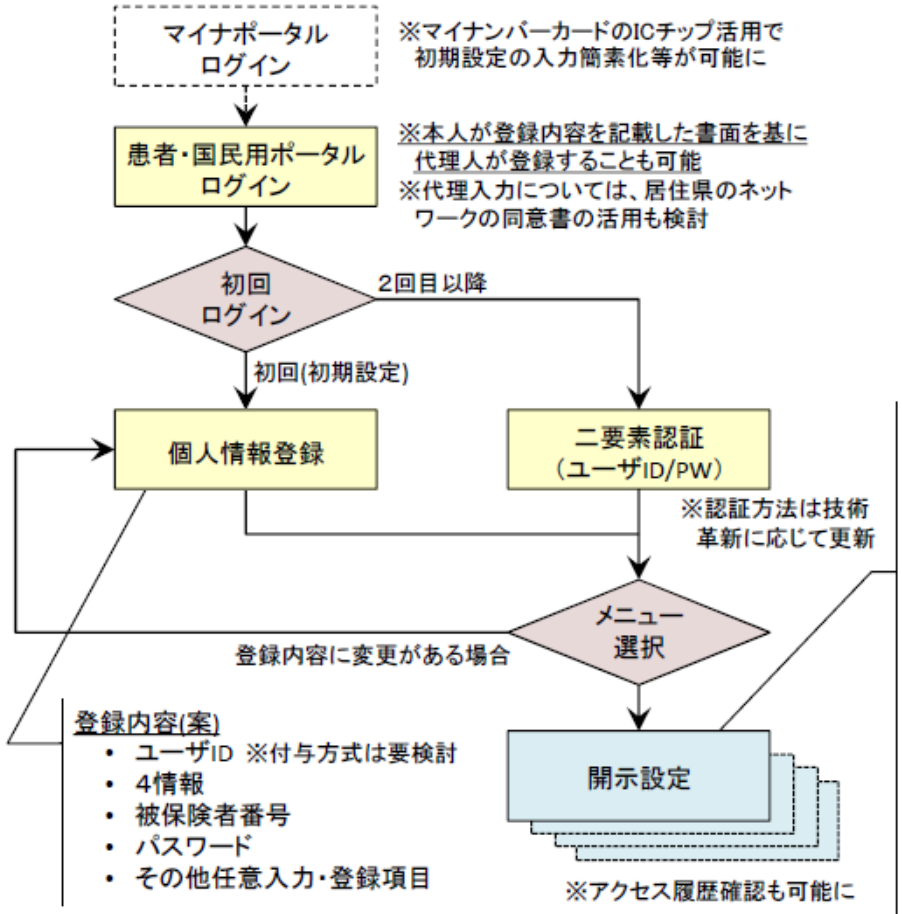
◆認証技術の要件
- 緊急性が高く、数秒以内にレスポンスが得られる必要がある。
- ポータルサイトからのSSOでのログイン、2要素認証。
- 目的の患者のみを閲覧できるよう認可範囲の設定が必要。
- 医療従事者はHPKIによる認証、患者はマイナポータルを活用した認証も想定される。
- HPKIのような資格認証が整備されていない介護従事者の認証について別途検討する必要がある。

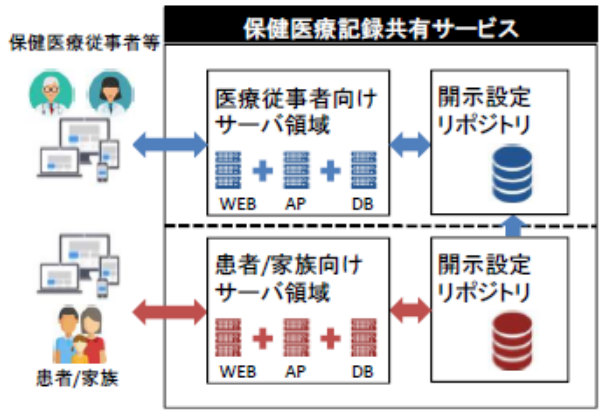
厚生労働省,全国保健医療情報ネットワークと保健医療記録共有サービスの課題と対応(案) 180524より作成

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

患者・国民用ポータルの概要

■ 患者・国民本人がポータル経由で保健医療記録共有サービスの情報開示設定やアクセス履歴確認を可能とする。
■ 初期登録項目は4情報（氏名、性別、住所、生年月日）、被保険者番号、パスワード等を想定。
※その他、任意に入力・登録可能な項目・データは要検討 （例：電話番号、メールアドレス、かかりつけ医情報、写真データ等）
■ 本人同意があれば代理人（家族、病院の地域連携室事務職員等）による登録も可能とする。
■ マイナンバーカードの普及を踏まえ、マイナポータルからシングルサインオンでログインする方式への拡張も想定。





開示設定項目(案)　※患者・国民の入力負荷の少ない設定を要検討

- 共通設定分類
  - ・圏域（県域）別：居住県⇒過去2年の居住県⇒それ以前の居住県
  - ・施設別：県別（又は2次医療圏別）に、病院/診療所/薬局/その他
  - ・保健医療従事者資格別：
    医師 / 歯科医師 / 薬剤師 / 看護師 / 事務職 等
- 個別設定

※収集元は被保険者番号（履歴）で利用実績のある施設のみ表示
※開示先は個別設定（例：居住2次医療圏内は包括同意、それ以外は個別同意など）

【イメージ】
- 病院　（3）：☑○○病院、☑○○病院・・・
- 診療所（5）：☑○○医院、□○○クリニック、☑○○歯科・・・
- 薬局　（8）：☑○○薬局、☑○○薬局、□○○薬局・・・

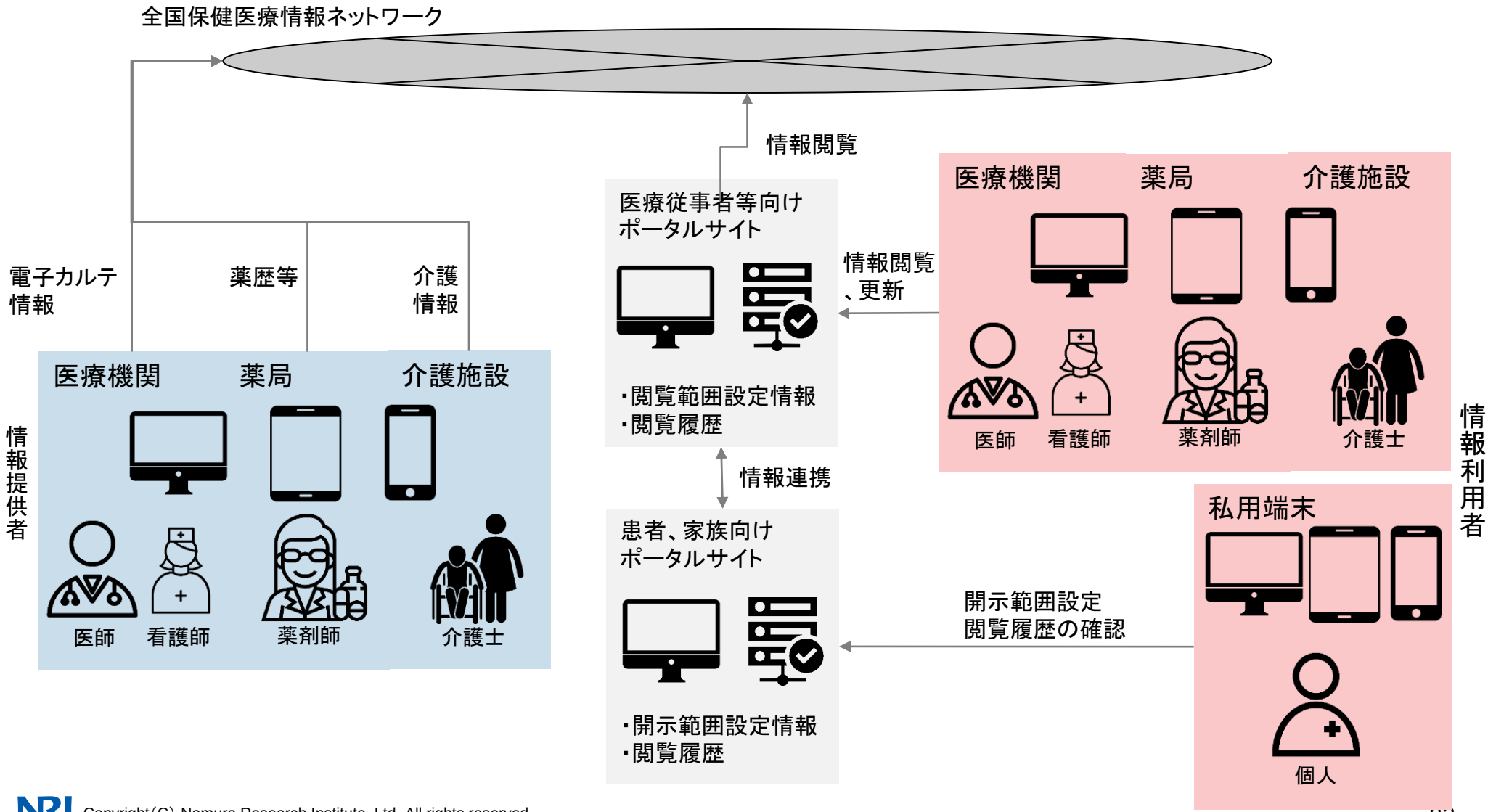
※1クリックでチェックを「つける」又は「はずす」程度の操作を想定

9

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

厚生労働省,全国保健医療情報ネットワークと保健医療記録共有サービスの課題と対応（案） 180524より作成

医師、看護師、薬剤師、介護士が、PC、タブレット、スマホなど多様なデバイスからポータルサイトを介して全国保健医療情報ネットワークへアクセスする



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

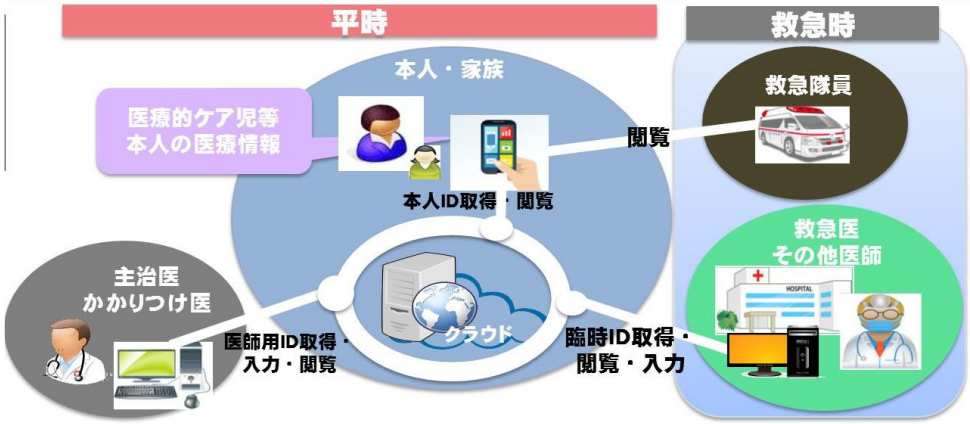
認証技術の検討には、早いレスポンス、2要素認証、HPKI活用、情報の機密性の高さ、私用スマホ利用等を考慮する必要がある。また災害時の対応は救急とは分けて検討が必要

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

医療的ケア児等の救急時や予想外の災害、事故に遭遇した際に、医療関係者が、処置に必要な患者情報を迅速に共有することで、どのような状況下においても、国民、患者に対して適切な治療等を遅滞なく提供できるようにする。これによって、医療的ケアが必要な障がい児などが安心して外出できるような環境を整備するとともに、災害時などへの備えに万全を期すことを目指す。

サービスの構造

平時には、かかりつけ医が、医療情報を入力・閲覧、本人・家族が自身の医療情報を閲覧する。救急時や災害時には、救急隊員による閲覧、救急医への臨時IDの発行などが行われる。



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定（NRI）

■ 利用者（規模）
- 救急隊員　（約6万人）
- 救急医　（約3000人）
- 患者、家族（約250万人～全国民）*医療的ケア児に限らない
- かかりつけ医（30万人）

◆閲覧される情報の機密性
- 診療記録など要配慮個人情報を含み、機密性は高い。

◆ネットワーク
- 公衆ネットワークを想定。

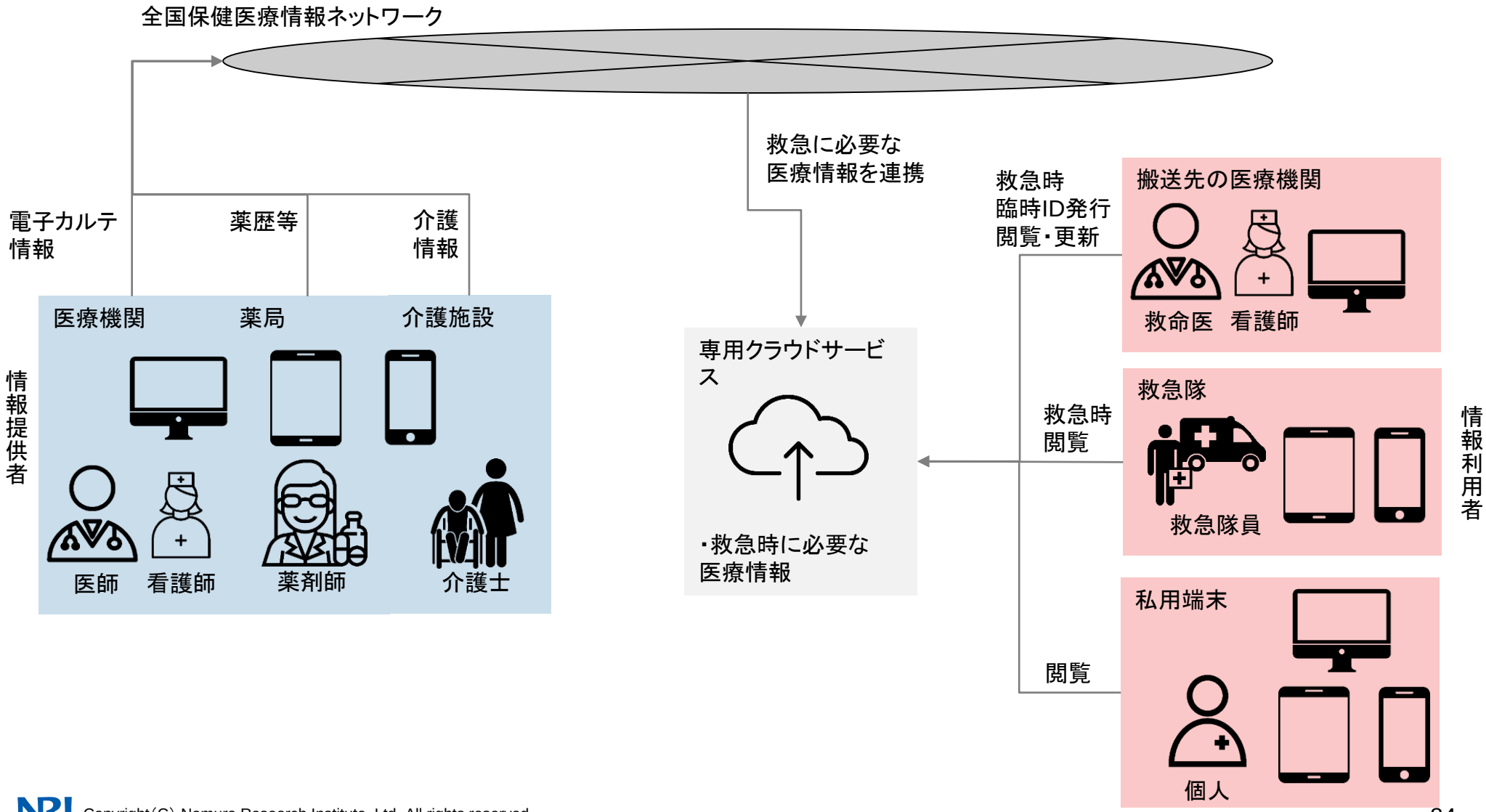
◆システムの管理主体
- 国から民間へ委託を想定。

◆デバイス
- 院内PC、タブレット、患者私用のスマホ、タブレット等。

◆認証技術の要件
- 緊急性が高く、数秒以内にレスポンスが得られる必要がある。
- 医師、救急隊員は、HPKI認証、2要素認証が望ましいが、救急時の素早い対応のための配慮が必要。
- 目的の患者のみを閲覧できるよう認可範囲の設定が必要。
- 災害時には、他地域から被災地へ不特定多数の医師や救急隊員が参加するため、認可範囲を広く開放する必要がある。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

平時には、かかりつけ医が医療情報を入力・閲覧、本人・家族が自身の医療情報を閲覧する。救急時や災害時には、救急隊員や救急医が患者情報を閲覧する



NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

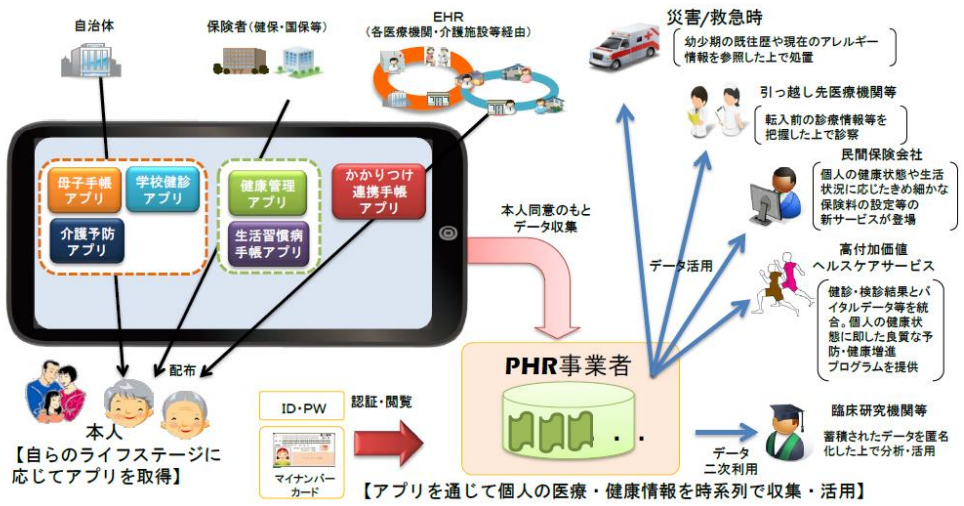
認証技術の検討には、全国民が広く利用する点、情報の機密性の高さ、私用スマホ等による利用等を考慮する必要がある

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

個人の健診データや医療情報をサマリーか、ヒストリー化して、個人にわかりやすく提供し、自らの健康管理・予防行動に繋げられるようにする（PHR）。

サービスの構造

①妊娠・出産、②疾病・介護予防、③生活習慣病重症化予防、④医療・介護連携にかかるPHRサービスモデルの開発、サービス横断的にデータを管理できる連携基盤を開発。



未来投資会議構造改革徹底推進会合「健康・医療・介護」第1回,,①データ利活用基盤の構築 171027より作成

サービス想定（NRI）

■ 利用者（規模）
- 国民　（最大1億3千万人,又は高齢層7~8万千人）

◆閲覧される情報の機密性
- 診療情報などの要配慮個人情報を含むため機密性は高い。

◆ネットワーク
- 公衆ネットワーク
- 私用スマホ等によるアクセスを前提とするため、公衆ネットワークが前提となる。

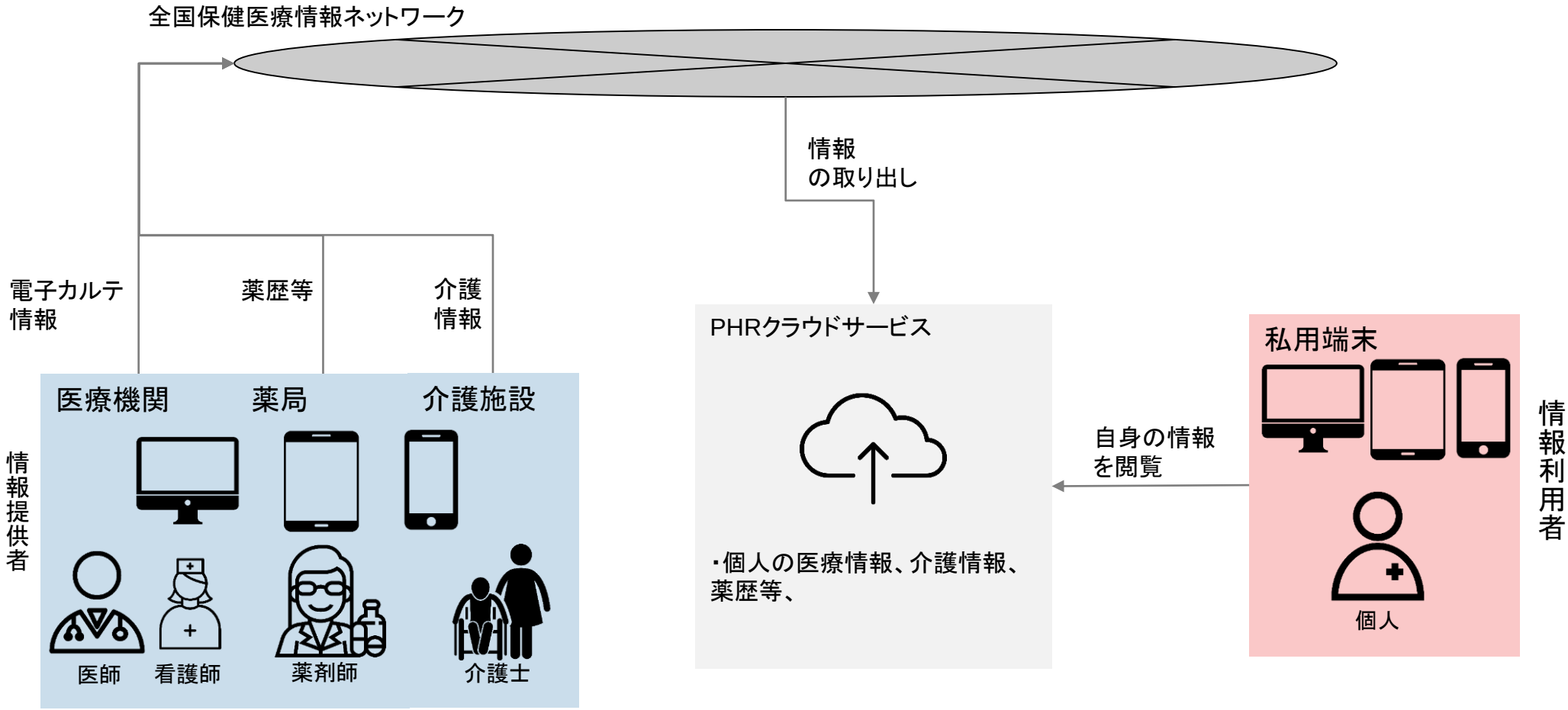
◆システムの管理主体
- 国から民間へ委託を想定。

◆デバイス
- 私用スマートフォン、タブレット。個人がPHRアプリを通じて自身の健康情報をクラウド上へ蓄積していく前提。

◆認証技術の要件
- 緊急性はないが、多くの国民が日常的に閲覧するため、使いやすく、安価なものが望ましい。
- 複数のアプリへ連携するため、SSOなどのフェデレーションが必要。
- 国民規模での認証となるため、マイナポータルやGoogle ID等の外部IDの活用が望ましい。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

PHRサービスを介して、全国保健医療情報ネットワークにある自身の医療情報等をスマートフォン等で閲覧する



NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

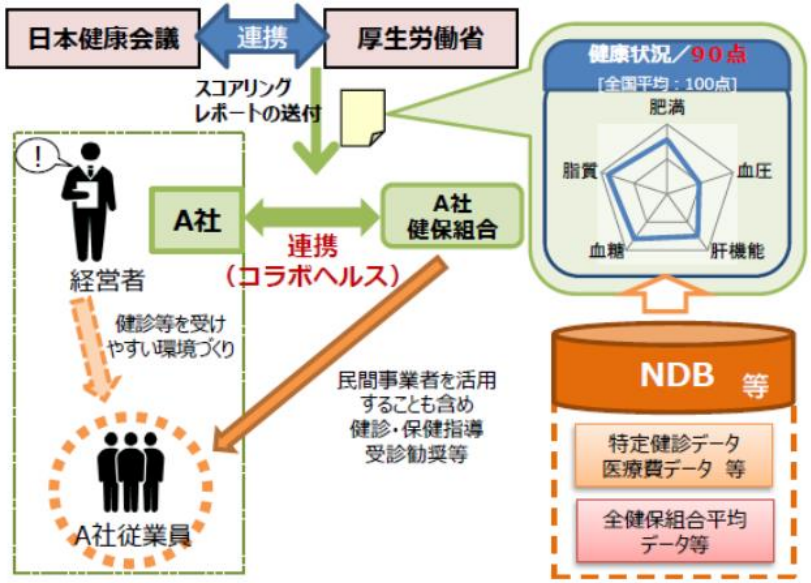
情報の機密度は低く、使用頻度も低いため、認証技術として特別な要件はないと想定。使用が容易で、安価な技術が想定される

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

保険者が保有する「加入者の健康管理に関するデータ」を集約・分析し、個人情報の確実な保護を前提としつつ、保険者や保健に加入する事業者に対して、その保険者や事業所全体の「全国平均と比較した場合の健康傾向に関する情報」や「必要な健康行動についての情報」を提供する。(健康スコアリング)

サービスの構造

NDB等の既存DBからデータを集約・分析した健康スコアリングレポートを提供するサービスを厚生労働省と日本健康会議が連携して構築する。企業の人事職員や産業医は、スコアリングレポートを受領する。



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定(NRI)

■ 利用者(規模)
- 企業の人事職員(50万人程度：小規模企業除く企業数)
- 企業の産業医(1000人程度：平成26 年現在産業医数)
- 健康スコアリングレポートを受領するのみでDBの集約分析は日本健康会議と厚労省が行う。

◆閲覧される情報の機密性
- 匿名化かつ加工後のデータのため情報の機密性は低い

◆ネットワーク
- 公衆ネットワーク
- スコアリングレポートは現状郵送配布されているが、本調査ではネットワーク上での提供を想定。

◆システムの管理主体
- 厚生労働省、日本健康会議

◆デバイス
- 専用の固定端末PC。組織毎に必要なときに分析を行う程度であり、屋外やモバイルでアクセスするニーズはないと想定。

◆認証技術の要件
- 機密性は比較的低く、高い認証強度は求められない。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

健康スコアリングレポートのイメージ：企業ごとに匿名個人データを集計、加工したものと想定し、他のサービスに比べ、情報の機微性は比較的低い

○○○○健保組合　様
貴健保組合の健康スコアリングレポート

■我が国は既に人口減少、超高齢化社会に突入し、深刻化する人手不足に加え、従業員の平均年齢の上昇による健康リスクの増大、生産性低下といった構造的課題に直面しています。
■従業員がいつまでも元気で働き続けられる環境づくり、予防・健康づくりなくして、企業における持続的成長の実現は困難です。
■そのためには、健保組合と事業主（企業）が連携し、一体となって予防・健康づくりの取組を進める必要があります。
■本レポートでは、事業主と健保組合のコミュニケーションの一助となるよう、予防・健康づくりの取組状況や健康状況等を可視化しています。経営者においては、企業の財産である従業員等の健康を守るために、健保組合と連携した従業員等の予防・健康づくりの取組のさらなる推進にご活用ください。なお、健康状況等に関する詳細情報は健保組合にお問い合わせください。

健保組合の保健事業が健康課題の解決策に！

少子高齢化の進展や定年延長といった社会環境の変化に伴い、労働者の平均年齢の上昇に加えて、健保組合における医療費も増加を続けています。こうした中で、従業員等に対する予防・健康づくりの取組をより一層進めるために、事業主と健保組合による協働が求められています。

■就業者の平均年齢の推移

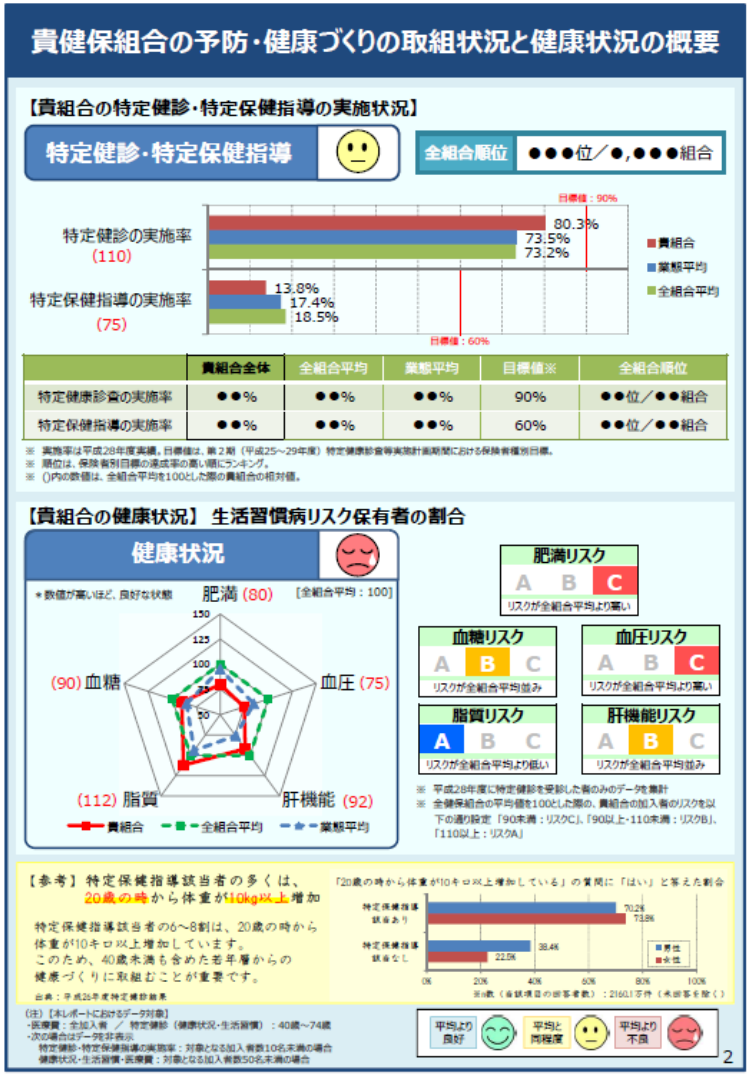
※総務省統計局「労働力調査」に基づく推計（5歳階級の中央の年齢に就業者数を乗じた値を積み上げ、全就業者数で除する方法で算出）

■健保組合の総医療費の推移

※厚生労働省「医療保険に関する基礎資料～平成27年度の医療費等の状況～」に基づき作成。医療費は全健保組合の総額。

【本レポートで使用する用語の定義】「組合」及び「全健保組合」：健康保険組合　／「全組合」：全健康保険組合　／「医療費」：平成28年度年間医療費　／「特定健診」：特定健康診査　／「業態」：健康保険組合における業態（29分類）

1



貴健保組合の予防・健康づくりの取組状況と健康状況の概要

【貴組合の特定健診・特定保健指導の実施状況】

特定健診・特定保健指導

全組合順位　●●●位／●,●●●組合

	貴組合全体	全組合平均	業態平均	目標値※	全組合順位
特定健康診査の実施率	●●%	●●%	●●%	90%	●●位／●●組合
特定保健指導の実施率	●●%	●●%	●●%	60%	●●位／●●組合

※　実施率は平成28年度実績、目標値は、第2期（平成25～29年度）特定健康診査等実施計画期間における保険者種別目標。
※　順位は、保険者別目標の達成率の高い順にランキング。
※　()内の数値は、全組合平均を100とした際の貴組合の相対値。

【貴組合の健康状況】生活習慣病リスク保有者の割合

健康状況

肥満リスク　A　B　C　リスクが全組合平均より高い
血糖リスク　A　B　C　リスクが全組合平均並み
血圧リスク　A　B　C　リスクが全組合平均より高い
脂質リスク　A　B　C　リスクが全組合平均より低い
肝機能リスク　A　B　C　リスクが全組合平均並み

※　平成28年度に特定健診を受診した者のみのデータを集計
※　全健保組合の平均値を100とした際の、貴組合の加入者のリスクを以下の通り設定（「90未満：リスクC」、「90以上・110未満：リスクB」、「110以上：リスクA」）

【参考】特定保健指導該当者の多くは、20歳の時から体重が10kg以上増加

特定保健指導該当者の6～8割は、20歳の時から体重が10キロ以上増加しています。このため、40歳未満も含めた若年層からの健康づくりに取組むことが重要です。

出典：平成28年度特定健診結果
当該データ：2160.1万件（未回答を除く）

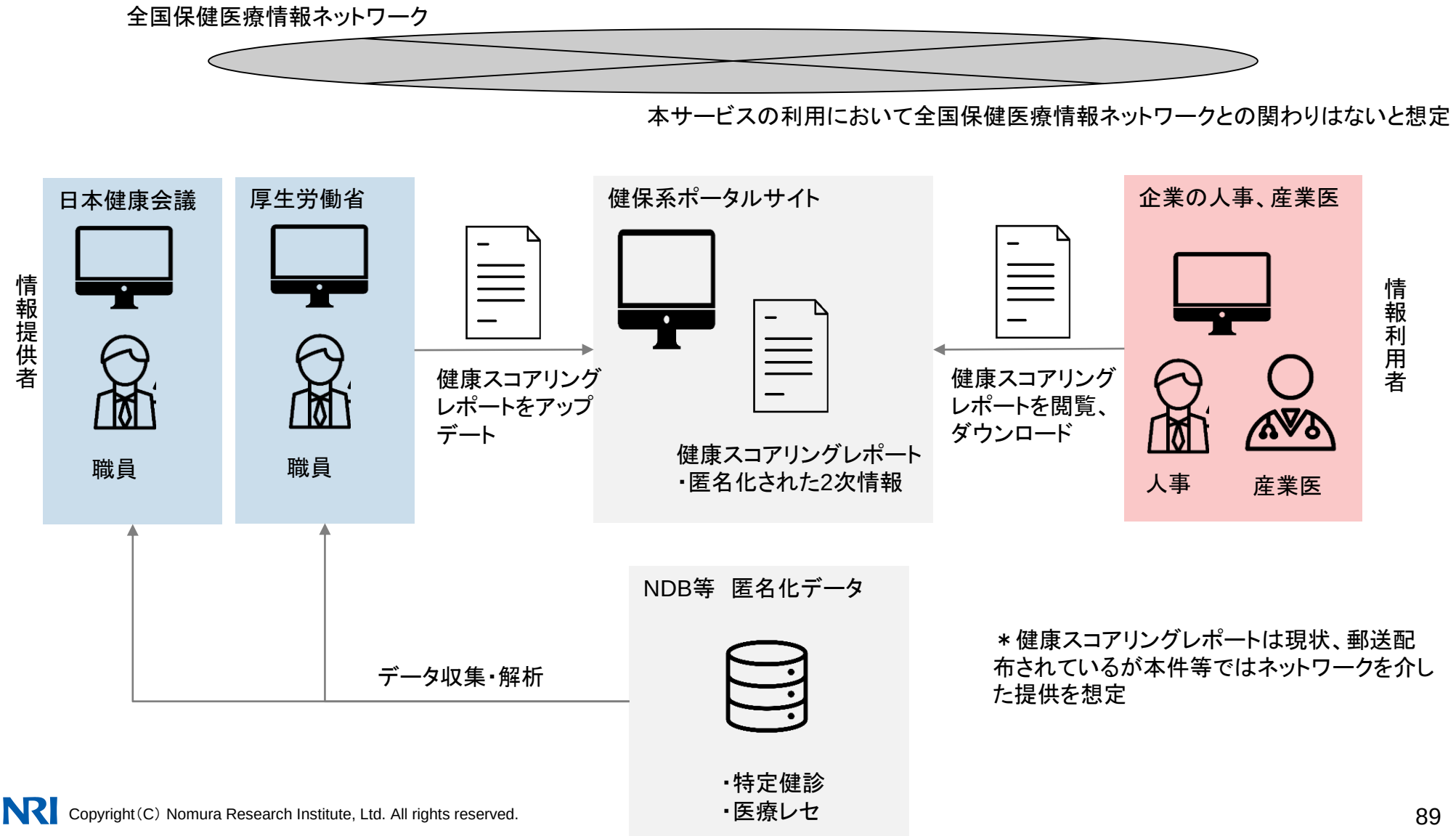
(注)【本レポートにおけるデータ対象】
・医療費：全加入者　／　特定健診（健康状況・生活習慣）：40歳～74歳
・次の場合はデータ化非表示
特定健診・特定保健指導の実施率：対象となる加入者数10名未満の場合
健康状況・生活習慣・医療費：対象となる加入者数50名未満の場合

平均より良好　平均と同程度　平均より不良

2

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

日本健康会議と厚生労働省が連携し、健康スコアリングレポートを作成、企業の人事担当者や産業医へ提供する



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

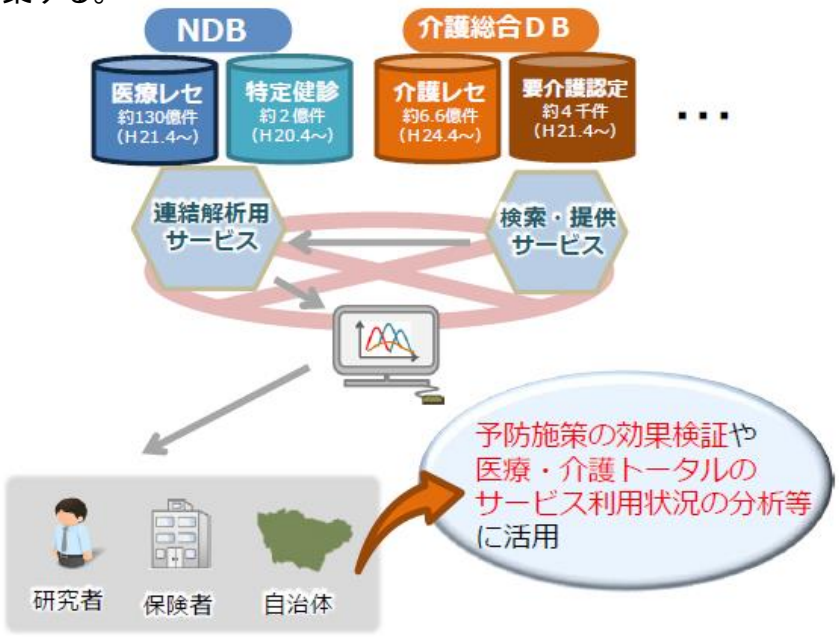
情報の機密度は低く、使用頻度も低いため、認証技術として特別な要件はないと想定。使用が容易で、安価な技術が想定される

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

国民の健康・医療・介護、各々の分野で抱える課題の解決に際してエビデンスとなる、科学的な分析に必要なビッグデータと匿名化して収集の上、個人単位で連結・解析可能とし、保険者や研究者、民間企業等が、今まで以上に、保健医療分野で精密な研究・開発や実行性のある施策の実施に活用できるようにする。早期の予防施策の展開、治験・臨床研究の患者アクセス向上、新たな治療法の開発、創薬等のイノベーションの活性化、科学的介護の実現等を目指す。

サービスの構造

NDB,介護総合DB等の匿名DB(既存)を連結・解析するサービスを新たに構築する。



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定（NRI）

■ 利用者（規模）
- 保険者　（生命保険会社数約40社）
- 同分野の研究者　（保健・医学・薬学：約13万人）
- 同分野の民間企業（製薬約70社、医療機器約3000社程度）

◆閲覧される情報の機密性・規模
- 匿名化データのため情報の機密性は低い。
- 一度に、最大で患者240万人、要支援・要介護者640万人のデータを閲覧・解析。

◆ネットワーク
- 公衆ネットワーク

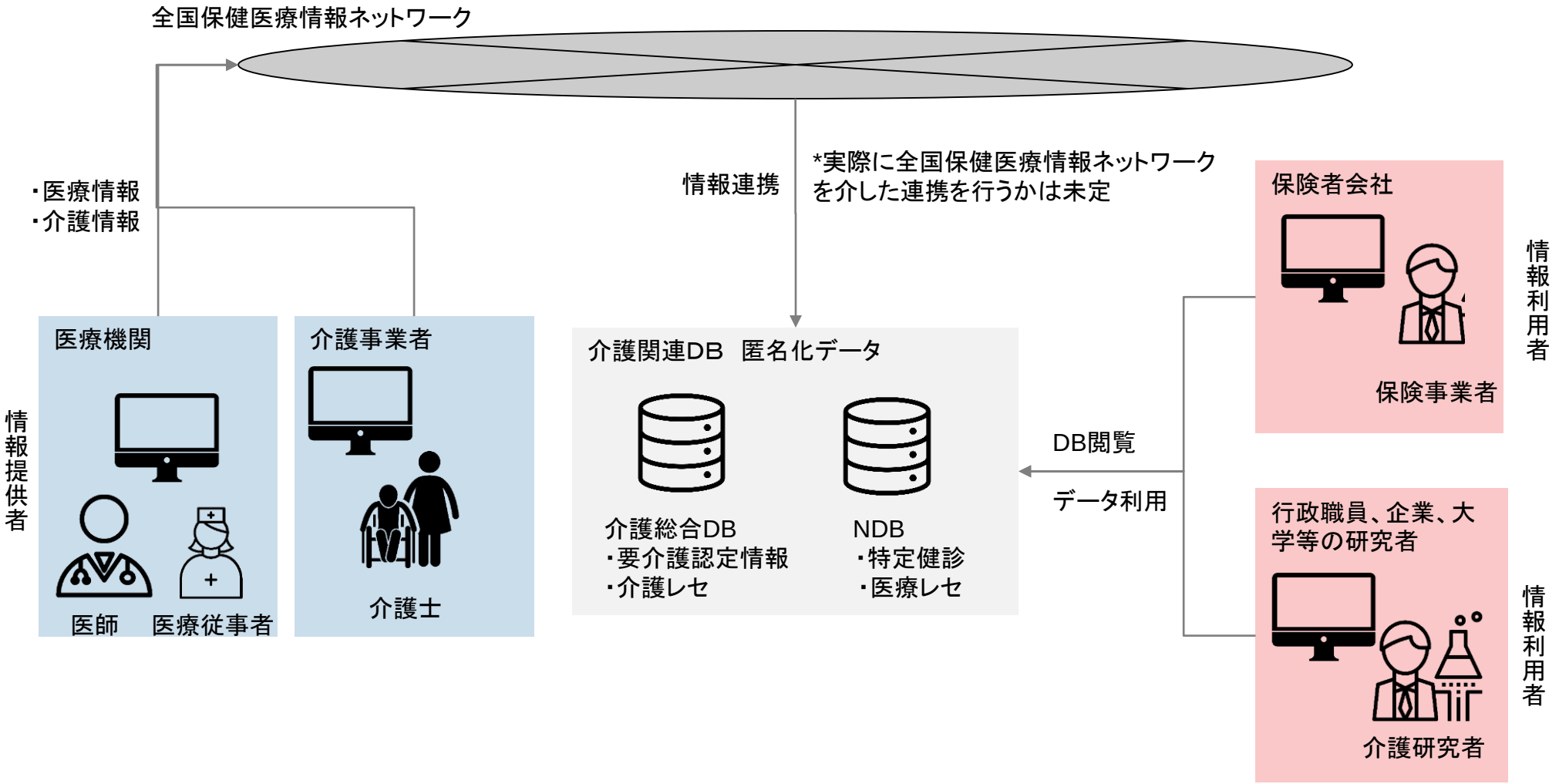
◆システムの管理主体
- 国から民間へ委託を想定。

◆デバイス
- 専用の固定端末PC。組織毎に必要なときに分析を行う程度であり、施設外やモバイルでのアクセスするニーズはない。

◆認証技術の要件
- 研究目的の利用であり、緊急性はなく、時間的制限は少ない。
- 必要データ以外は閲覧できないよう認可設定が必要。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

介護総合、NDB等のデータベースを、保険者や行政職員、研究者がデータヘルスに関する調査、研究に活用する



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

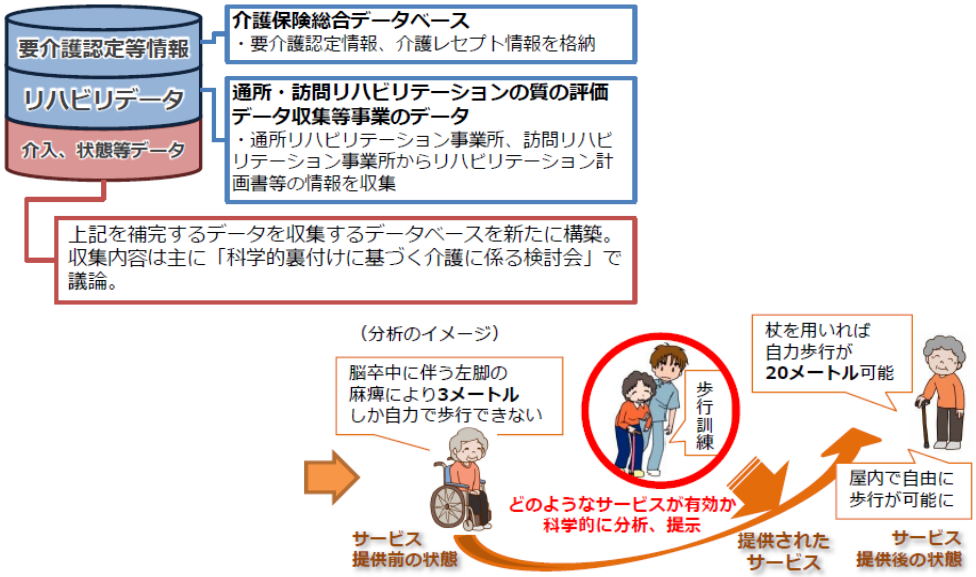
現状のサービス想定やサービス担当者へのヒアリングにより、利用者認基盤証の利用は現状予定されていないと考えられる

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

自立支援や認知症等の治療やケアにおける科学的効果に裏付けされた介護を実現するために、科学的分析に必要なデータ(日常の生活行動、リハビリテーション、栄養摂取、医学的な診断情報等)を収集しつつ、データベースの構築とその有効活用を推進し、保健、医療、介護の現場や研究者等に提供する。

サービスの構造

介護保険総合DB、通所・訪問リハビリテーションの質の評価データ収集等事業のDB(VISIT)の既存DBに加え、介入や状態等のデータを収集したDB(CHASE)を構築する。



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定(NRI)

■ 利用者(規模)
- 保健、医療、介護の職員によるデータ登録(350万人)
- 同分野の研究者による情報活用(約13万人)

◆閲覧される情報の機密性・規模
- 匿名化データのため情報の機密性は低い。

◆ネットワーク
- 公衆ネットワーク(データ登録)
- 電子媒体(情報活用)

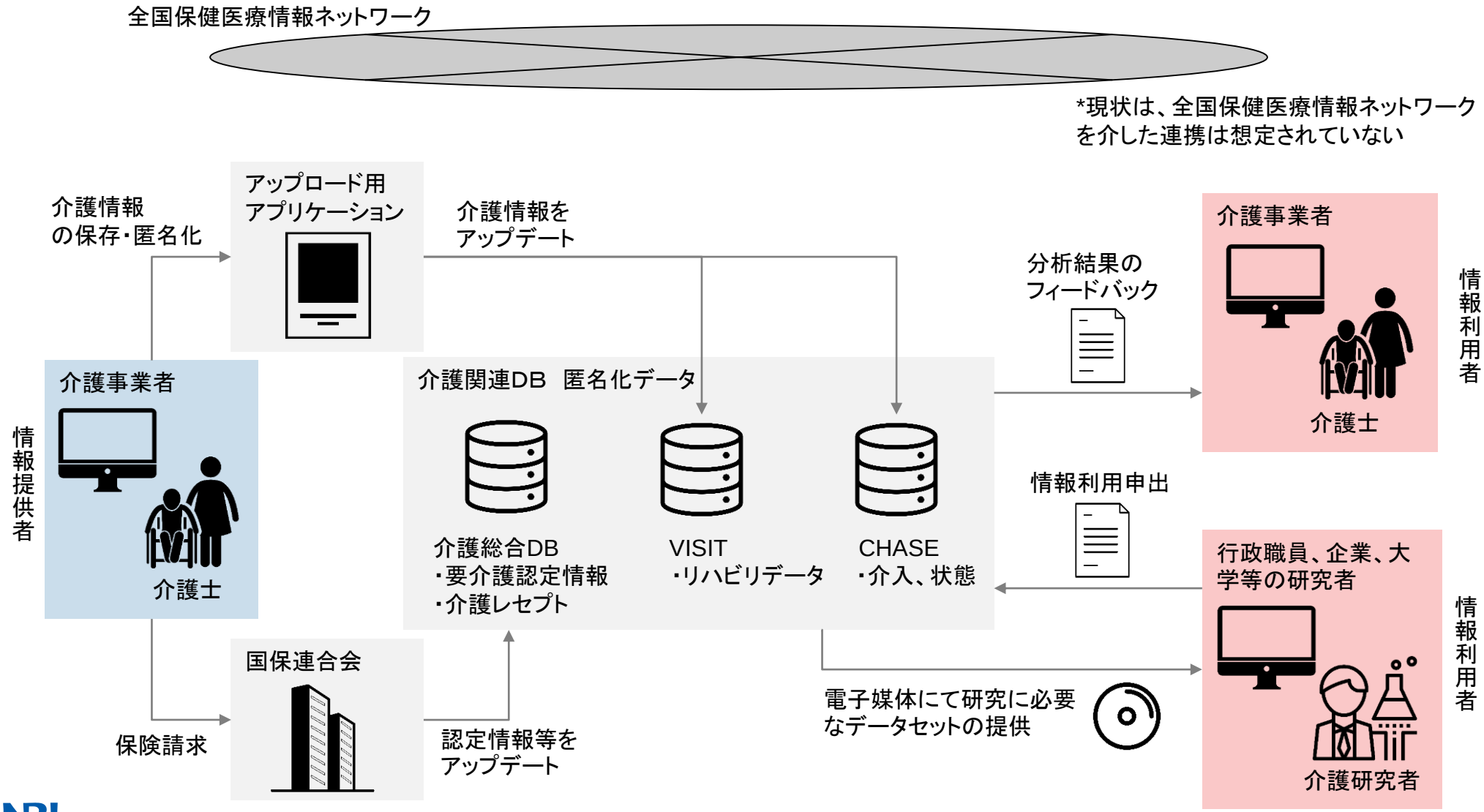
◆システムの管理主体
- 国による運営を想定。

◆デバイス
- 専用の固定端末PC。組織毎に必要なときに分析を行う程度であり、施設外やモバイルでのアクセスするニーズはない。

◆認証技術の要件
- 厚生労働省内サービス担当者へのヒアリングにより、現状は介護事業者がDBへ直接ログインする想定はなく、現時点では認証は不要と想定される。
- データの活用についても、現状は電子媒体での提供が予定されており、現状では認証は必要性は低いと考えられる。
- 今回の検討では、ネットワークを介した場合を想定して認証方式を検討した。

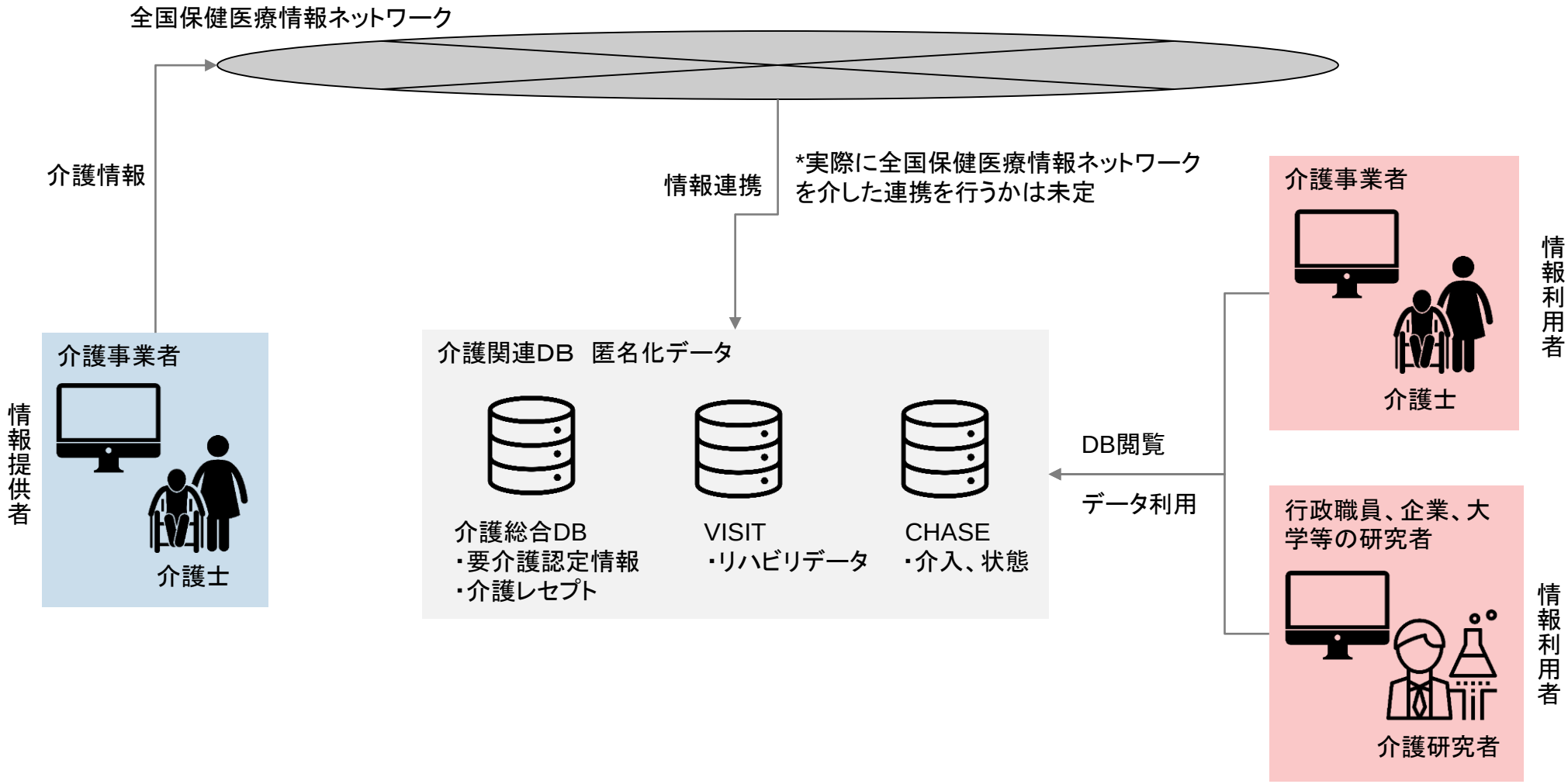
NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

介護総合、VISIT、CHASEの三つのデータベースを、介護事業者や行政職員、研究者が介護に関する調査、研究に活用する



NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

本検討では、ネットワーク経由で、DBの情報利用が行われる場合を以下のように想定し、認証方式を検討した



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

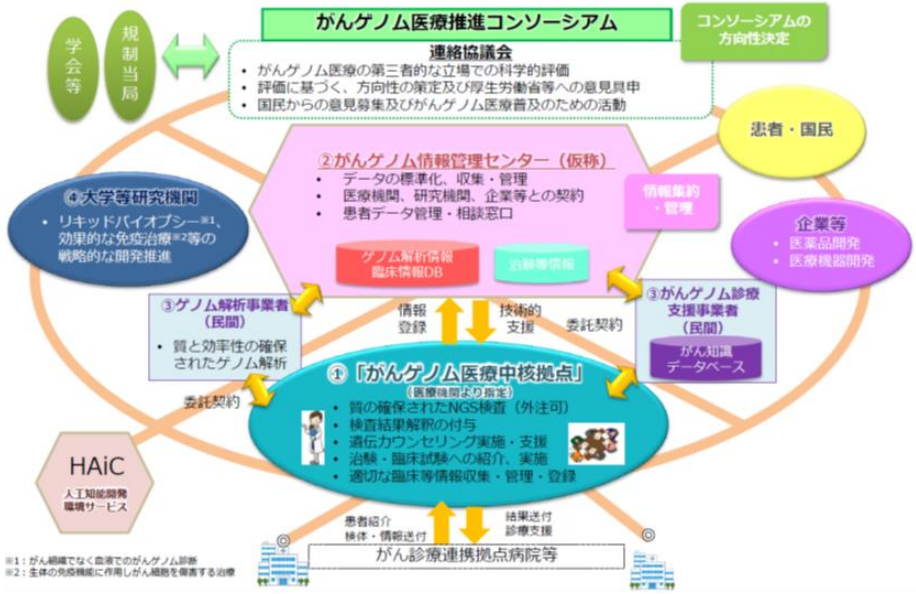
認証技術の検討には、情報の機密性の高さを考慮すべき。また、情報へのアクセス可能者を制限する必要性も高いと考えられる

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

国民、患者の意向に十分配慮した上で、がん患者に関するゲノム情報、診療及び治療に関する最新の情報、治験情報等を効率的に収集し、医療関係者や研究者等に提供し、新たな治療法の開発や創薬につなげる。これによって、国民、患者は、最適で効率的かつ個別化された医療を享受することができる。

サービスの構造

がんゲノム医療中核拠点で収集された情報をがんゲノム情報管理センターへ登録。データの標準化と管理を行う。医療機関、研究機関、企業はがんゲノム情報管理センターと契約し、情報を活用する。



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定（NRI）

■ 利用者（規模）
- 医薬品、医療機器を開発する企業（製薬約70社、医療機器約3000社程度）
- がんゲノムの解析事業者、診療支援事業者
- がんゲノム医療中核拠点の医師、医療スタッフ（11箇所：H30時点）

◆閲覧される情報の機密性・規模
- A：個人のゲノム情報であるため、機密性が非常に高い。

◆ネットワーク
- 閉域ネットワーク:専用回線

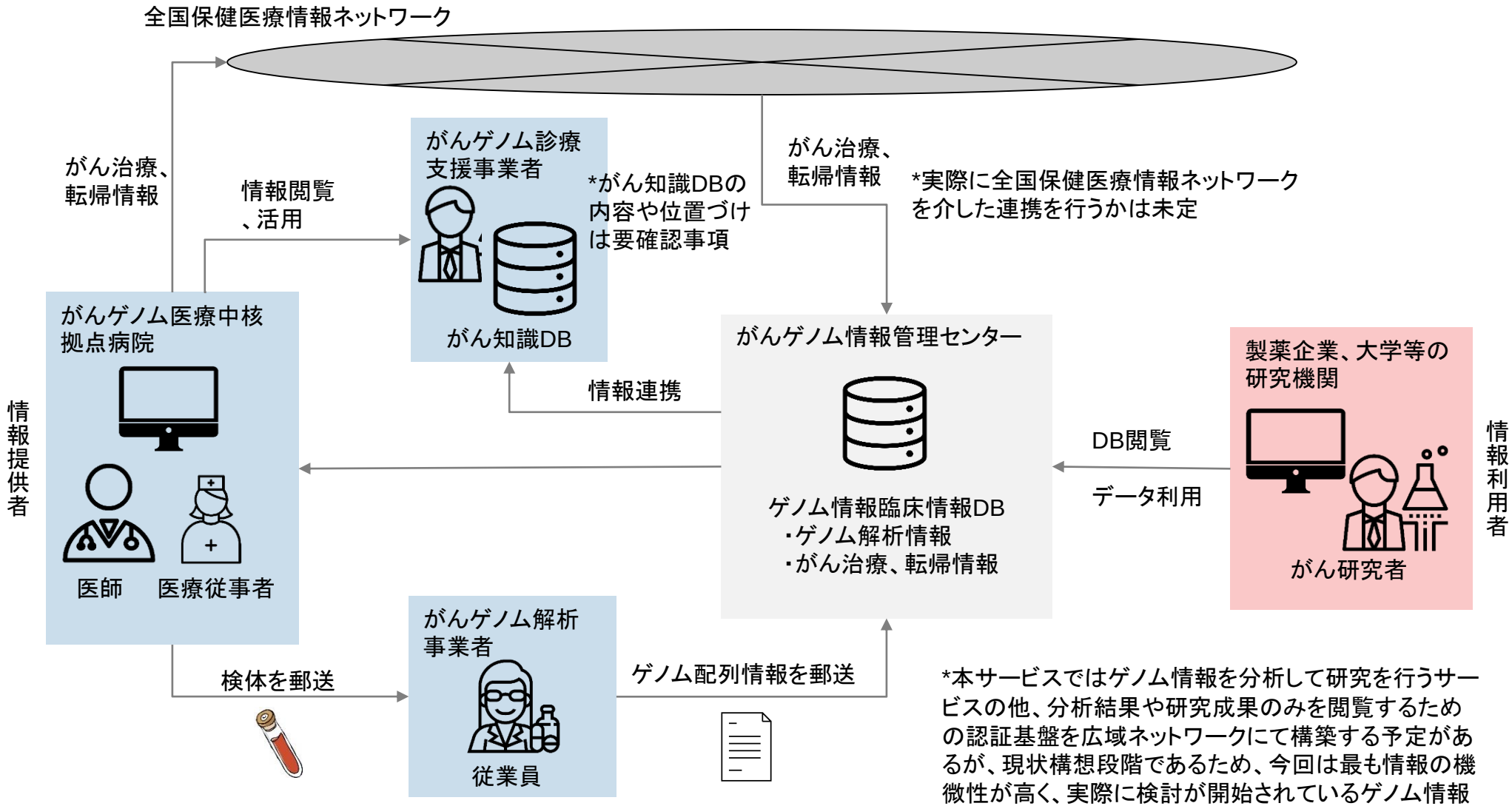
◆システムの管理主体
- 公的機関（がんゲノム情報管理センター）

◆デバイス
- 専用の固定端末PCを想定。組織単位で必要なときに分析を行う程度であり、施設外やモバイルでのアクセスするニーズはない。

◆認証技術の要件
- 研究目的の利用であり、緊急性はなく、時間的制限は少ない。
- 機密性の高い情報を大量に扱うため、認証の必要性が高い。
- 認可により、必要最低限の閲覧者とすることも考慮すべき。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

がんゲノム情報管理センターへ、患者のゲノム情報及びがん治療、転帰情報を集約、DB化される。DBの情報は、がん研究に活用される



*本サービスではゲノム情報を分析して研究を行うサービスの他、分析結果や研究成果のみを閲覧するための認証基盤を広域ネットワークにて構築する予定があるが、現状構想段階であるため、今回は最も情報の機微性が高く、実際に検討が開始されているゲノム情報へアクセスするユースケースについて検討した。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

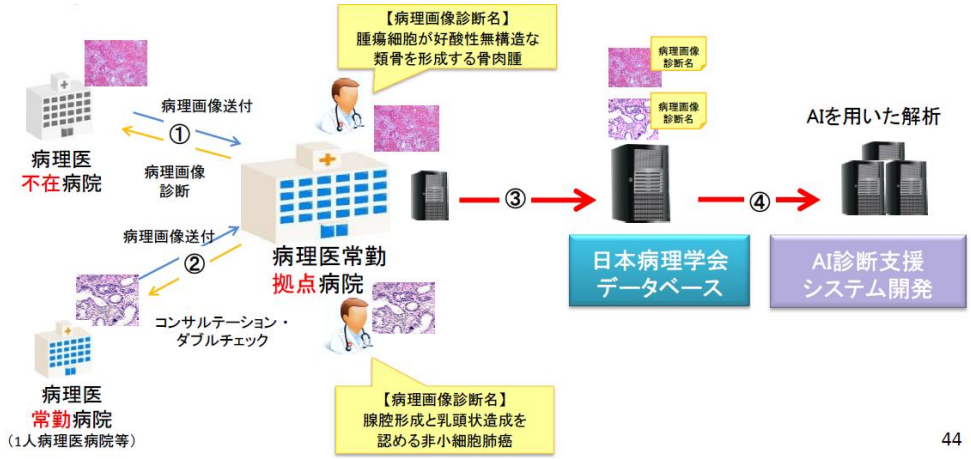
情報の機密度は低く、認証技術として特別な要件はないと想定。使用が容易で、安価な技術が想定される

サービスの説明(2017年7月4日　データヘルス改革推進計画より)

文献読み込み等による診断補助などあらゆる臨床行為はもとより、レセプト審査や、医療、介護における予防策の因果関係解明など、広く保健医療分野において、クラウドコンピューティングを含めたAIのフル活用を促進する。これにより、保健医療分野におけるAI開発を促進し、がん等の診断制度の向上や不足する病理医の負担軽減など、患者に対する最適な医療・ケアの選択肢の提供、並びに医療関係者の負担軽減を目指す。

サービスの構造

①病理医不在病院あら、病理医常勤拠点病院に対し画像データを送付
②病理医常勤病院から、病理医常勤拠点病院に対しコンサルテーション・ダブルチェックシステムにより画像データを送付
③拠点病院は、正確な診断名のついた病理画像データをデータベースに保存
④保存された教師付データを用いてAIの開発を推進



厚生労働省,データヘルス改革に関する平成30年度予算案等について　1801より作成

サービス想定(NRI)

■ 利用者(規模)
- 医師(30万人)
- AI研究者

◆閲覧される情報の機密性・規模
- D:匿名化された画像データであり、機密性は低い。
- 一度に数十万人分の病理検体を分析。

◆ネットワーク
- 公衆ネットワーク

◆システムの管理主体
- 日本病理学会

◆デバイス
- 専用の固定端末PC。組織単位で必要なときに分析を行う程度であり、施設外やモバイルでのアクセスするニーズはない。

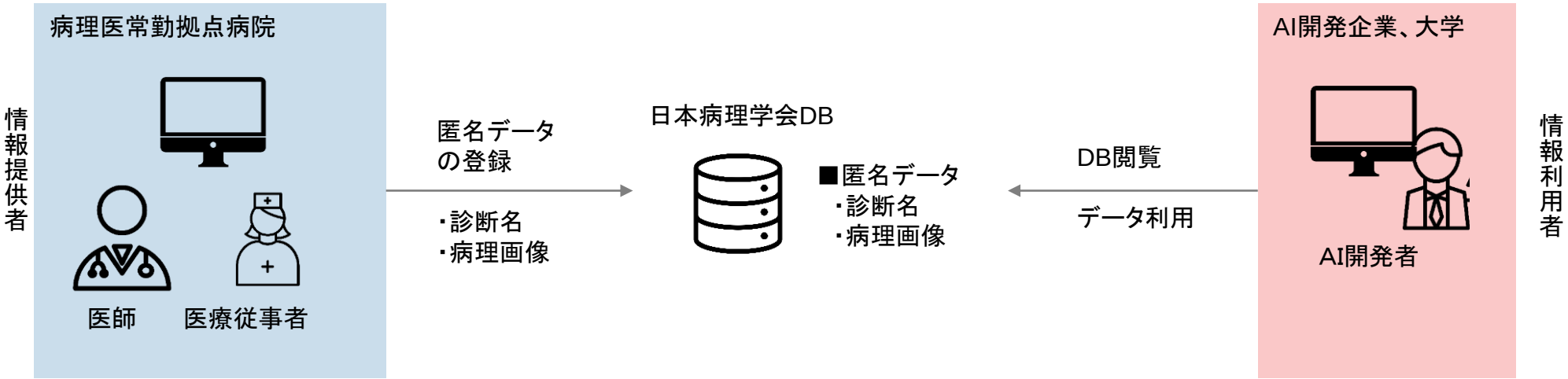
◆認証技術の要件
- 研究目的の利用であり、緊急性はなく、時間的制限は少ない。
- 電子カルテなどと同様、診断をした医師の電子署名などの認証が必要。

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

日本病理学会DBにおいて、診断名及び病理画像の匿名化データを蓄積、AI開発に活用する

全国保健医療情報ネットワーク

本サービスの利用において全国保健医療情報ネットワークとの関わりはないと想定



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

画像診断を含め、6分野での検討が進められているが、画像診断以外の概要は現在検討中であり現時点では具体的な想定を置くことは難しく、本研究では対象としない

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

厚生労働省,データヘルス改革に関する平成30年度予算案等について 1801より作成

各サービスのユースケースを洗い出し、分類、モデル化した。（別紙参照）

サービス	ユースケースNo.	誰が		いつ	どこで			なんの情報を					どのように		どうする	モデル番号	認証技術の要件	
		職種	対象人数の規模	状況	アクセスする場所	ネットワーク	閲覧文書の保存先	情報の持ち主	種類	情報の機密度	一度に閲覧される規模	認可の範囲	デバイス	専用・私用	目的		時間的制限	その他
①保健医療記録共有サービス	①-2	医師	約30～40万人	初診・他院からの患者受け入れ時	病院	公共（暗号化あり）	他の病院の電子カルテシステム	新規の患者	電子カルテ	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	院内のパソコン	専用	閲覧のみ	①-a	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・医師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-3	医師	約30～40万人	介護師との連携が必要な高齢者担当時	病院	公共（暗号化あり）	他の施設の介護業務システム	担当患者	介護記録	C	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	院内のパソコン	専用	閲覧のみ	①-b	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・医師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-6	看護師	約160～170万人	初診・他院からの患者受け入れ時	病院	公共（暗号化あり）	他の病院の電子カルテシステム	新規の患者	電子カルテ	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	院内のパソコン	専用	閲覧のみ	①-a	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・看護師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-7	看護師	約160～170万人	介護師との連携が必要な高齢者担当時	病院	公共（暗号化あり）	他の施設の介護業務システム	担当患者	介護記録	C	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	院内のパソコン	専用	閲覧のみ	①-b	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・看護師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-10	訪問看護師	約4～5万人	訪問時	訪問先	公共（暗号化あり）	他の病院の電子カルテシステム	新規の患者	電子カルテ	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	タブレット	専用	閲覧のみ	①-a	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・看護師の資格認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術
	①-11	訪問看護師	約4～5万人	訪問時	訪問先	公共（暗号化あり）	他の施設の介護業務システム	担当患者	介護記録	C	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	タブレット	専用	閲覧のみ	①-b	診療の合間に発生するため、目安として10秒程度のレスポンスが求められる	・看護師の資格認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術
	①-15	介護従事者	約90～100万人	通常サービス提供時(施設系)	施設	公共（暗号化あり）	医療機関の電子カルテシステム	担当高齢者	電子カルテ	B	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	施設内のパソコン	専用	閲覧のみ	①-c	介護業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・介護士の個人認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当高齢者の特定（認可範囲の設定） ・利用者側に負担なく簡単に利用できるもの（介護従事者のITリテラシーに配慮）
	①-16	介護従事者	約90～100万人	通常サービス提供時(施設系)	施設	公共（暗号化あり）	医療機関の電子カルテシステム	担当高齢者	電子カルテ	B	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	タブレット	専用	閲覧のみ	①-c	介護業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・介護士の個人認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当高齢者の特定（認可範囲の設定） ・利用者側に負担なく簡単に利用できるもの（介護従事者のITリテラシーに配慮）
	①-19	訪問介護士	約13～14万人	通常サービス提供時(訪問系)	訪問先	公共（暗号化あり）	医療機関の電子カルテシステム	担当高齢者	電子カルテ	B	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	スマートフォン	専用	閲覧のみ	①-c	介護業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・介護士の個人認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当高齢者特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの（介護従事者のITリテラシーに配慮）
	①-20	訪問介護士	約13～14万人	通常サービス提供時(訪問系)	訪問先	公共（暗号化あり）	医療機関の電子カルテシステム	担当高齢者	電子カルテ	B	1名～担当患者数百人程度	担当患者（患者自身がポータルサイトで閲覧許可）	タブレット	専用	閲覧のみ	①-c	介護業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・介護士の個人認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当高齢者特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの（介護従事者のITリテラシーに配慮）
	①-22	薬剤師	約16～17万人	処方箋受付時	薬局	公共（暗号化あり）	他施設の薬歴システム	来局患者	薬歴	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	施設内のパソコン	専用	閲覧のみ	①-a	業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・薬剤師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-23	薬剤師	約16～17万人	疑義照会時	薬局	公共（暗号化あり）	医療機関の電子カルテシステム	来局患者	電子カルテ	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	施設内のパソコン	専用	閲覧のみ	①-a	業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・薬剤師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定）
	①-24	訪問薬剤師	約３～４万人	訪問時	訪問先	公共（暗号化あり）	自施設の薬歴システム	担当患者	薬歴	B	1名～数名	担当患者（患者自身がポータルサイトで閲覧許可）	タブレット	専用	閲覧・更新	①-a	業務の合間に発生するため、目安として10秒程度のレスポンスが求められる	・薬剤師の資格認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術
	①-34	患者	約200～250万人	閲覧履歴の確認、開示範囲を設定	自宅	公共（暗号化あり）	ポータルサイトの設定リポジトリ	本人	閲覧歴、開示範囲設定情	B	1名	自身の情報	個人のタブレット・スマートフォン	私用	閲覧・更新	①-d	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・個人単位の認証 ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの ・認可範囲の設定（家族の情報のみ）
	①-35	患者家族	約200～250万人	患者に代わり、閲覧履歴の確認、開示範囲を設定	自宅	公共（暗号化あり）	ポータルサイトの設定リポジトリ	家族	閲覧歴、開示範囲設定情	B	1名	自身又は患者	個人のタブレット・スマートフォン	私用	閲覧・更新	①-d	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・個人単位の認証 ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの ・認可範囲の設定（家族の情報のみ）
②救急時医療情報共有サービス	②-2	かかりつけ医	約30万人	通常診療時に緊急時の対応を確認する	病院	公共（暗号化あり）	他の医療機関の電子カルテシステム	担当患者	電子カルテ	B	1名～担当患者数百人程度	担当患者	院内のパソコン	専用	閲覧のみ	①-a	救急救命を行うため、通常診療よりも時間的制限は大きい。（10秒未満）	・医師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定） ・私用端末でも利用できるソフトウェアトークンなど。
	②-3	救急搬送先の医師	約3000人	緊急搬送時に患者の基礎データや既往歴等を確認する	病院	公共（暗号化あり）	他の医療機関の電子カルテシステム	来院患者	電子カルテ	B	1名	搬送された患者	院内のパソコン	専用	閲覧のみ	②-a	救急救命を行うため、通常診療よりも時間的制限は大きい。（10秒未満）	・医師の資格認証 ・二要素認証（入場時・端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲の設定） ・私用端末でも利用できるソフトウェアトークンなど。
	②-5	救急隊員	約6万人	救急搬送中の患者情報の確認	救急車	公共（暗号化あり）	他の医療機関の電子カルテシステム	搬送患者	電子カルテ	B	1名	搬送された患者	救急車内のタブレット端末など	専用	閲覧のみ	②-a	救急救命を行うため、通常診療よりも時間的制限は大きい。（10秒未満）	・薬剤師の資格認証 ・二要素認証（端末利用時を含めて二要素以上の認証が行われていれば二要素認証同等） ・担当患者の特定（認可範囲設定） ・持ち運び可能で、外出先でも認証可能な技術
	②-6	患者	約200～250万人	自身の医療情報を医師や救急隊員に見せる	病院・救急車内	公共（暗号化あり）	他の医療機関の電子カルテシステム	本人	電子カルテ	B	1名	自身の情報	個人のスマートフォン・タブレット	私用	閲覧のみ	②-b	救急救命を行うため、通常診療よりも時間的制限は大きい。（10秒未満）	・個人単位の認証 ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの
	②-7	患者家族	約200～250万人	家族の医療情報を医師や救急隊員に見せる	病院・救急車内	公共（暗号化あり）	他の医療機関の電子カルテシステム	家族	電子カルテ	B	1名	自身又は患者	個人のスマートフォン・タブレット	私用	閲覧のみ	②-b	救急救命を行うため、通常診療よりも時間的制限は大きい。（10秒未満）	・個人単位の認証 ・持ち運び可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの ・認可範囲の設定（家族の情報のみ）

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

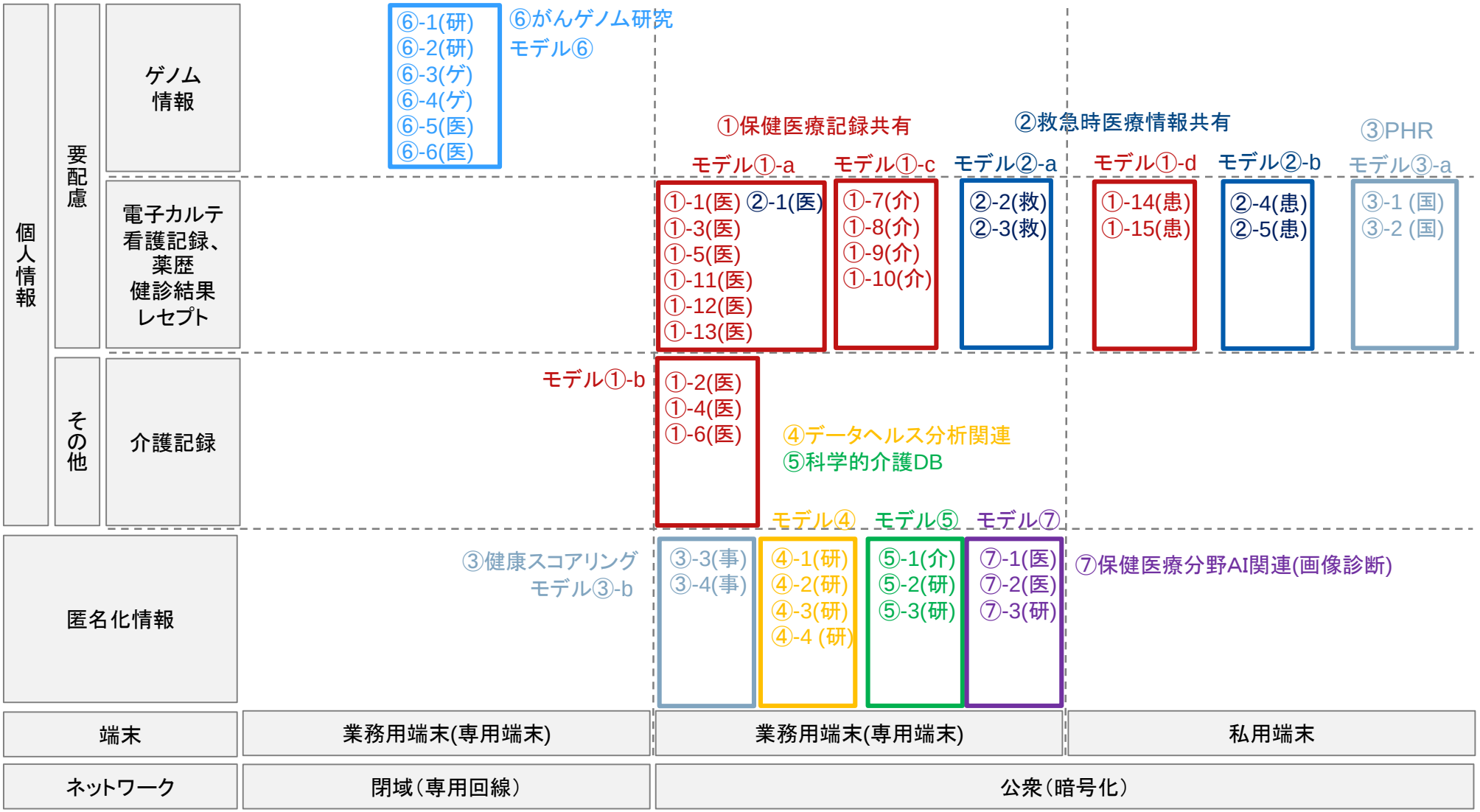
各サービスのユースケースを洗い出し、分類、モデル化した。（別紙参照）

サービス	ユースケースNo.	誰が		いつ	どこで			なんの情報を					どのように		どうする	モデル番号	認証技術の要件	
		職種	対象人数の規模	状況	アクセスする場所	ネットワーク	閲覧文書の保存先	情報の持ち主	種類	情報の精密度	一度に閲覧される規模	認可の範囲	デバイス	専用・私用	目的		時間的制限	その他
③個人や事業主に健康情報を提供するサービス	③-1	個人	数千万人～全国民	自身の健康診断結果を確認する	自宅	公共（暗号化あり）	PHRクラウド	本人	①妊娠・出産、②疾病・介護予防、③生活習慣病重症化予防、④医療・介護連携などの情報	B	1名	自身の情報	個人のパソコン	私用	閲覧のみ	③-a	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・個人単位の認証 ・持ち運び好可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの
	③-2	個人	数千万人～全国民	自身の健康診断結果を確認する	自宅	公共（暗号化あり）	PHRクラウド	本人	①妊娠・出産、②疾病・介護予防、③生活習慣病重症化予防、④医療・介護連携などの情報	B	1名	自身の情報	個人のタブレット・スマートフォン	私用	閲覧のみ	③-a	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・個人単位の認証 ・持ち運び好可能で、外出先でも認証可能な技術 ・利用者側に負担なく簡単に利用できるもの
	③-7	事業主（人事職員）	約50万人	健康スコアリングレポートを確認する。	事業所内	公共（暗号化あり）	日本健康会議、又は厚労省のシステム内？	従業員	健康スコアリングレポート（匿名化された加工された健診、医療費情報）	D	数百～数線人（匿名化）	自社の情報	職場のパソコン	専用	閲覧のみ	③-b	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・個人単位の認証 ・従業員の特定（認可範囲の設定）
	③-8	事業主（産業医）	約1000人	健康スコアリングレポートを確認する。	事業所内	公共（暗号化あり）	日本健康会議、又は厚労省のシステム内？	従業員	健康スコアリングレポート（匿名化された加工された健診、医療費情報）	D	数百～数線人（匿名化）	自社の情報	職場のパソコン	専用	閲覧のみ	③-b	医療処置を行う目的ではないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・個人単位の認証 ・従業員の特定（認可範囲の設定）
④健康・医療・介護のビッグデータを個人単位で連結し解析できるサービス	④-1	研究者（アカデミア）	約13～14万人（アカデミア以外も含む）	研究時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	数万～数千万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	④	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	④-2	研究者（製薬企業など）	約3000人社	製品開発時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	数万～数千万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	④	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	④-3	行政	検討中	統計解析時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	数万～数千万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	④	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	④-4	サービス開発者（民間）	約13～14万人（アカデミアも含む）	サービス開発時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	数万～数千万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	④	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
⑤科学的介護のデータベース活用	⑤-1	介護事業者	約90～100万人	自社の介護の効果検証時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	自社の顧客	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	最大で650万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	⑤	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑤-2	行政	検討中	介護の効果についての調査時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	最大で650万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	⑤	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑤-3	研究者	約13～14万人（アカデミアも含む）	介護の効果についての研究時	事業所内	公共（暗号化あり）	NDB、DPC、介護レセ、電子カルテなど様々なデータベース	国民	NDB、DPC、介護レセ、電子カルテなど様々なデータベースに保存された情報を匿名化したもの	D	最大で650万人（匿名化）	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	⑤	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
⑥がんゲノム情報の利活用サービス	⑥-1	研究者(大学、製薬等)	検討中	統計解析時	研究施設内	閉域	がんゲノム情報管理センター内、がんゲノム情報レポジトリ	国民	ゲノム情報、がんの治療履歴、転帰情報	A	数十万人～数百万人	すべてのデータ又は研究に必要な範囲のみ	施設内のパソコン	専用	閲覧のみ	⑥	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑥-2	ゲノム解析事業者	検討中	ゲノムシークエンス実施時	事業所内	閉域	がんゲノム情報管理センター内、がんゲノム情報レポジトリ	国民	ゲノム情報	A	数十万人～数百万人	すべてのデータ又は研究に必要な範囲のみ	事業所内のパソコン	専用	閲覧・解析・ダウンロード	⑥	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑥-3	がんゲノム診療支援事業者	検討中	統計解析時	事業所内	閉域	がんゲノム情報管理センター内、がんゲノム情報レポジトリ	国民	ゲノム情報、がんの治療履歴、転帰情報	A	数十万人～数百万人	すべてのデータ又は研究に必要な範囲のみ	事業所内の（専用）パソコン	専用	閲覧・解析・ダウンロード	⑥	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑥-4	医師	1000~5千人程度	データ登録時	がんゲノム医療中核拠点病院	閉域	がんゲノム情報管理センター内、がんゲノム情報レポジトリ	国民	がんの治療履歴、転帰情報	A	数十万人～数百万人	登録用の入力部分のみ	職場のパソコン	専用	閲覧・更新	⑥	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑥-5	看護師等、医療スタッフ	5000～2.5万人程度	データ登録時	がんゲノム医療中核拠点病院	閉域	がんゲノム情報管理センター内、がんゲノム情報レポジトリ	国民	がんの治療履歴、転帰情報	A	数十万人～数百万人	登録用の入力部分のみ	職場のパソコン	専用	閲覧・更新	⑥	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
⑦ＡＩ開発基盤に必要なデータを収集し、利活用できるサービス	⑦-1	医師	検討中	データ登録時	病理医常勤拠点病院	公共（暗号化あり）	日本病理学会データベース	国民	匿名化された、診断名、画像データ	D	数十万人～数百万人	登録用の入力部分のみ	職場のパソコン	専用	閲覧・更新	⑦	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑦-2	看護師等、医療スタッフ	検討中	データ登録時	病理医常勤拠点病院	公共（暗号化あり）	日本病理学会データベース	国民	匿名化された、診断名、画像データ	D	数十万人～数百万人	登録用の入力部分のみ	職場のパソコン	専用	閲覧・更新	⑦	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）
	⑦-3	AI研究者	検討中	統計解析時	研究施設内	公共（暗号化あり）	日本病理学会データベース	国民	匿名化された、診断名、画像データ	D	数十万人～数百万人	すべてのデータ又は研究に必要な範囲のみ	職場のパソコン	専用	閲覧のみ	⑦	医療処置を行う目的ではなく、使用頻度も少ないため、医療処置の場合（10秒程度）よりも時間的制限は小さい。	・事業者単位の認証 ・研究者個人単位の認証 ・対象者の特定（認可範囲の設定）

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

ユースケースの詳細化：ユースケースの整理とモデル化

洗い出した各サービスのユースケースを以下のように分類、モデル化した。



（）は認証される者
医：医療従事者　介：介護従事者　患：患者又は患者家族　救：救急医、救急隊員
国：国民　事：事業主　研：大学や企業等の開発者又は研究者　ゲ：ゲノム解析事業者等

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

D) 認証技術のサービスへの適応　サマリ

i. モデル毎に、アクセスがなされる情報の機微度に応じて、必要な認証の要素数を決定した。

ii. モデル毎に、サービス利用のうえで必要な利用者に関する情報を整理した。

- 利用者のサービスへのアクセス環境と、その周辺の構成案
- 利用者認証基盤側で利用者に関して特定すべき事項
- 利用者のID登録時に、その特定すべき事項を満たすための要素
- 利用者に求める、認証の要素数
- 前項B)、C)の結果を踏まえて、利用者のログインに適した認証技術の設定
- その他、サービス提供のために有用と考えるシステム的な制限事項

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

【参考】モデル化の前提について

- 認証後に利用されるデータは、個人情報ないし要配慮情報とし、それらが不要な場合には匿名化されたものと想定した。

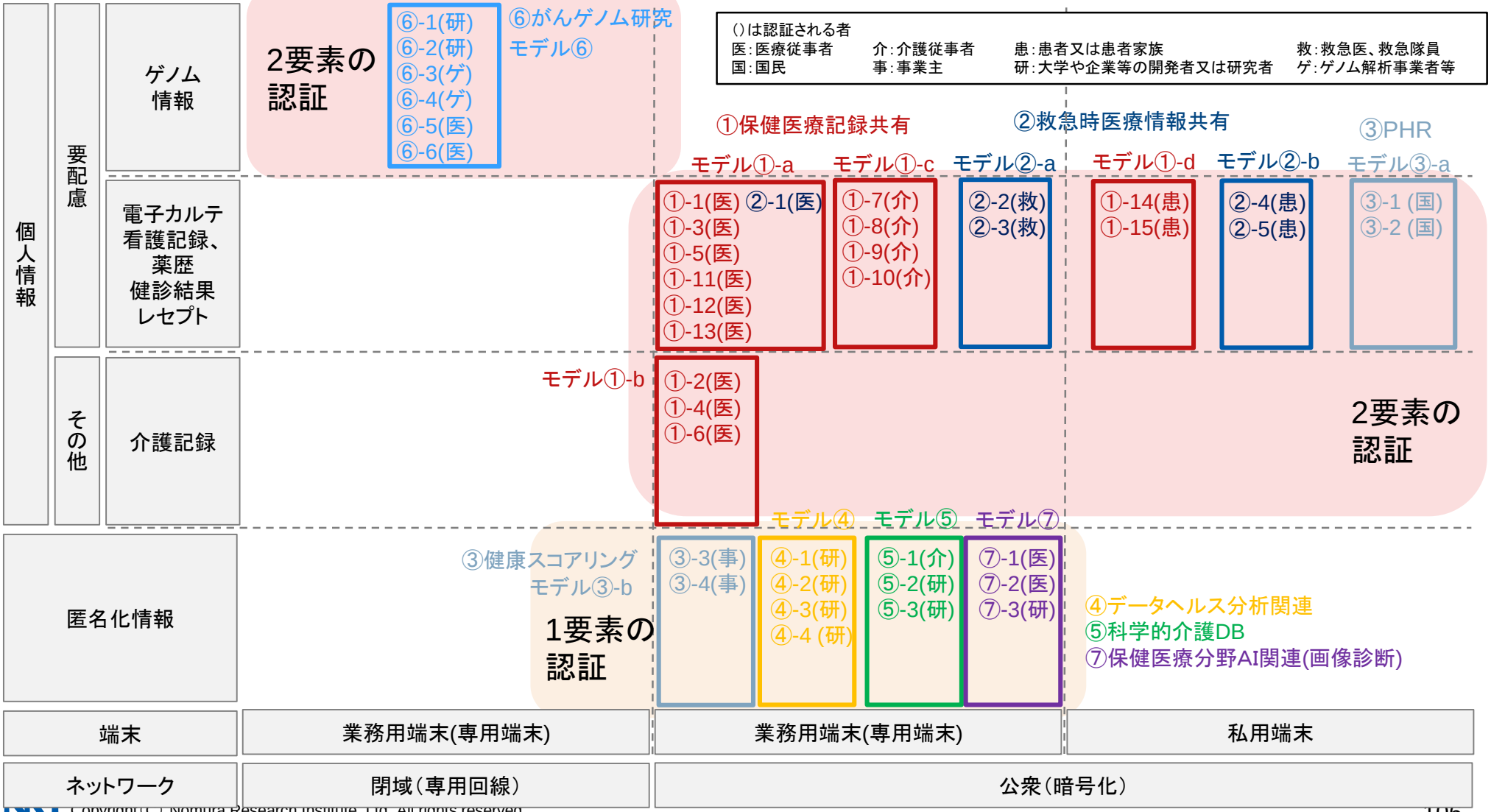
- 認証後に利用可能となる各種データについては、ログインした当該アカウントの利用に対して適切なデータが処理可能であるものとする。
  - 例）サービス②救急時医療情報共有サービスにおいて患者本人が、自身の電子カルテを閲覧するが、認証情報をもとに電子カルテのデータのなかから患者本人のデータが特定できるように整理されている。

- ログイン後に利用されるデータには、必要なものには既に電子署名がなされている前提であり、サービス側での認証後に利用者が医療情報に対して電子署名を施す機能は想定しない。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ⅰ. モデル毎の認証の要素数の考え方

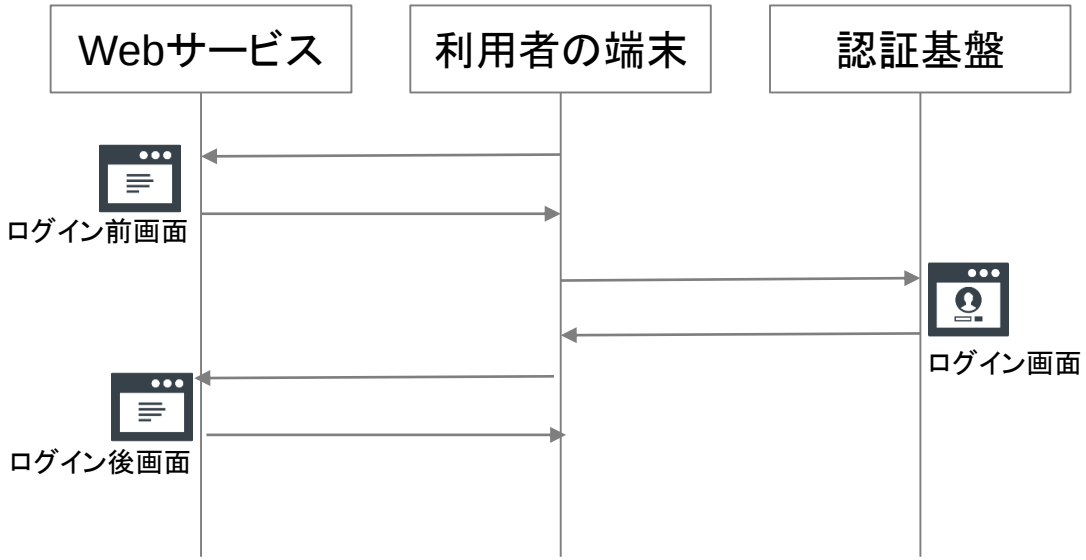
■ 各ユースケースで扱う情報に応じて、個人情報を扱う場合は2要素認証、匿名化情報を扱う場合には1要素認証と設定した。



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

【参考】構成案の見方

- 参考に利用者認証基盤を使ったWebサービスへのアクセスのイメージを、一般的な認証基盤での利用者からのアクセスを踏まえて次頁以降に、アクセス先・アクセス元の概観をサービス毎にまとめた。



- 表記のうちの一部の記号について、意味を以下にまとめる。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.①保健医療記録共有サービスの認証方式案

■ サービス全体

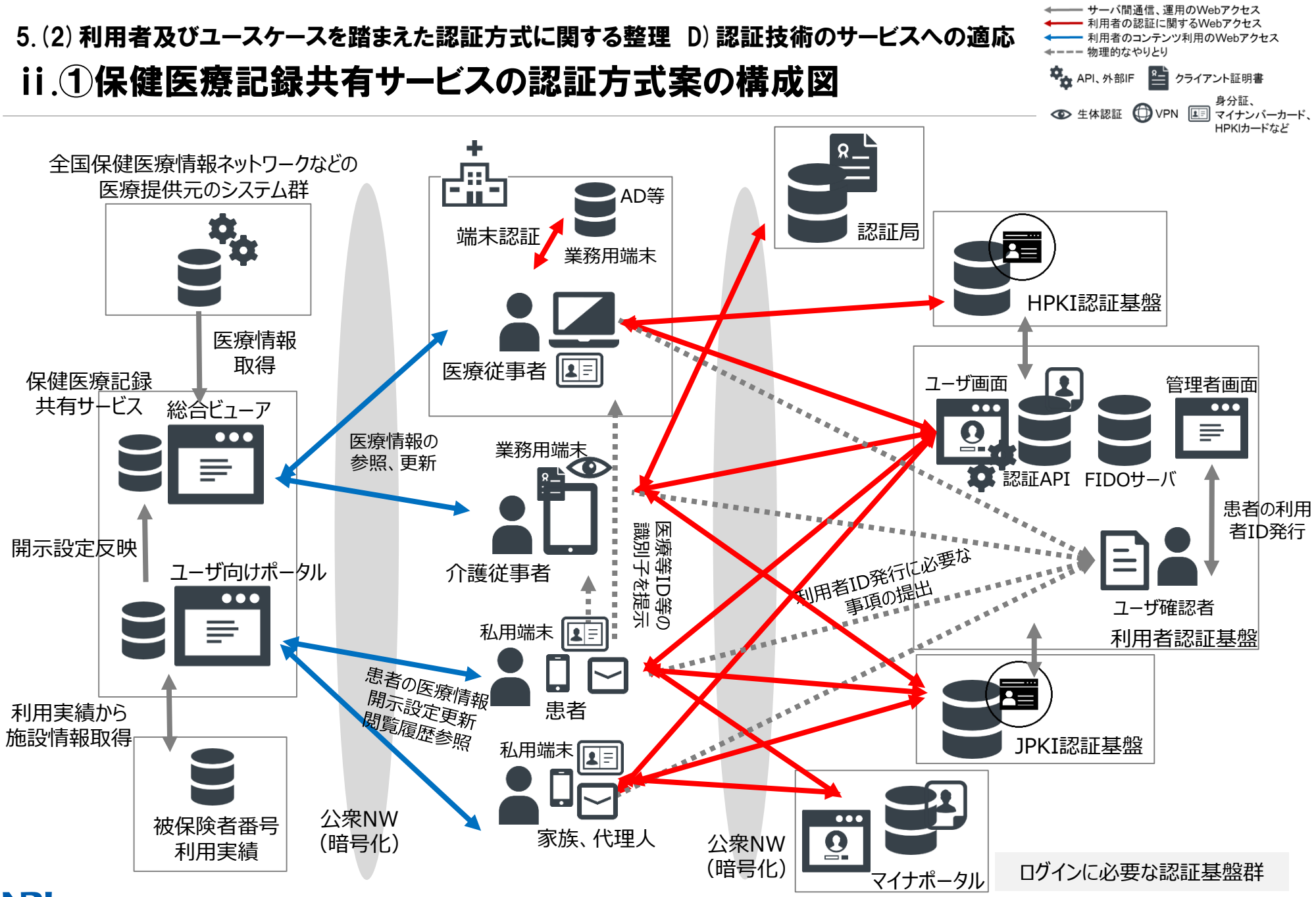
取り扱う情報	必要な認証数	その他
個人情報	2	なし

■ モデルごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
①-a/b	医師、薬剤師、看護師等の医療従事者	業務用端末	資格の確認要	・HPKIカード ・顔写真付きの身分証 ・資格を示す情報	・施設管理下の認証（入退室,端末等） ・パスワード	前述の技術評価より、1要素認証に適するものを選定
①-c	介護従事者	業務用端末	資格の確認が難しいため、組織の確認要	・組織ID ・公的個人認証 ・組織ID ・顔写真付きの身分証	・クライアント証明書 ・生体	・所属する組織を登録制とし、組織IDを事前に発行。組織IDと利用者IDを紐付ける ・前述の技術評価より、業務用端末向けの組み合わせとして適すると選定
①-d	患者	私用端末	なし	・公的個人認証 ・顔写真付きの身分証	・パスワード ・指紋	前述の技術評価より、私用端末向けの組み合わせとして適すると選定
	患者の家族、代理人	私用端末	なし	・公的個人認証（自身・患者の両方） ・家族・代理人は同意 ・顔写真付きの身分証（自身・患者の両方） ・家族・代理人は同意書	・パスワード ・指紋	・前述の技術評価より、私用端末向けの組み合わせとして適すると選定

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.①保健医療記録共有サービスの認証方式案の構成図



NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.①保健医療記録共有サービスの認証方式案の説明

- 想定する利用者は、医療従事者、介護従事者、患者、患者の家族・代理人となる。またログイン後の機能により医療従事者、介護従事者と患者の紐付け、家族・代理人と患者の紐付けを、医療等ID等をもちいて行うことを前提とした。
- 医療従事者、患者、家族・代理人のID登録の方法については、利用性の面から、既に整備されている公的個人認証やHPKIの活用が望ましいが、現状普及度が十分とは言えないため、それらを用いない方法も検討し、以下の2通りとした。
  - オンラインでの公的個人認証またはHPKIカードの利用（加えて、必要であれば患者本人の同意書のアップロード）、自身でのID登録
  - 顔写真付きの身分証（または、加えて職種を示す情報、患者の同意書）を郵送等で提出、ユーザ確認者が確認。運用者側でID登録し、利用者（または家族、代理人）へ初期パスワードとともに通知
- 介護従事者はHPKIのような資格確認のシステムが整備されていない。このため、利用する必要性が認められる組織を登録制とし、利用組織ID等の組織を示す情報を発行するものとした。介護従事者は、この利用組織IDを添えて、利用者ID登録を行うこととした。利用者ID登録の方法は、患者と同様に上述の2通りとする。
- 医療従事者は、所属の施設管理下での入退室の認証・端末認証等を2要素認証の内の1要素と見込み、パスワード認証のみをもちいることで、認証方式が業務負担とならないよう配慮した。
- 介護従事者は、業務用端末利用に適したクライアント証明書認証＆生体認証をもちいることとした。これにより、その組織が管理する業務用端末を利用してのみ、サービスを利用できるようになる。
- 患者、患者の家族、代理人は私用端末を利用することから、5.各技術の評価にて私用端末の利用に適すると評価されたパスワード認証＆指紋認証をもちいることとした。なお、国民にとっての利便性や普及度の向上を鑑みGoogle ID, Yahoo IDなどの外部IDの活用も検討すべきと考える。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

【参考】HPKIカードを使った資格・本人確認の頻度に関する考え方

- HPKI認証基盤側では、認証にHPKIカードをもちいることで、認証の都度、資格・本人確認も行っている。
- 一方で、本研究で提示した利用者認証基盤側の認証方式案では、現状のHPKIの普及度や利用性の確保などを考慮し、HPKIカードをもちいた資格・本人確認をID登録時にのみに求め、認証時には求めないこととした。
- 医療従事者や救急隊員が利用者認証基盤を利用する際には、以下に示すように、業務用端末を利用するには医療施設への入館又は施設の業務用端末の利用が前提となり、この際に認証が行われることで、医療施設の医療従事者であることをある程度担保することができると考えられる。よって、本研究で示した案も採用可能であると考えられた。
  - 業務用端末には、クライアント証明書をインストール済であることが前提となる。

利用時の前提条件	医療従事者	救急隊員
業務用端末を要する	●	●
施設入館を要する	●	

- ただし、今後、HPKIの普及度などの課題の改善を見据えた場合、HPKIを用いて認証の都度資格認証を行うことも想定できると考えられる。
- これを踏まえ、後述のフェデレーション及び処理イメージの検討（グループA’）では、HPKIを都度認証に用いた場合についても検討を行っている。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.①保健医療記録共有サービスの認証方式案

●:必須、1・2はどちらかが必須　○:任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種(資格)	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
医師、薬剤師、看護師等の医療従事者	ID登録	–	–	–		●			●		1●			1●			2●				
	ログイン	2	1	1					●						●						
介護従事者	ID登録	–	–	–	●				●	●				1●		2●					
	ログイン	2	0	2					●									●	●		
患者	ID登録	–	–	–					●					1●		2●					
	ログイン	2	0	2					●						●				●		
患者の家族、代理人	ID登録	–	–	–			○	○	●			○	○	1●		2●					
	ログイン	2	0	2					●						●				●		

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.②救急時医療情報共有サービスの認証方式案

■ サービス全体

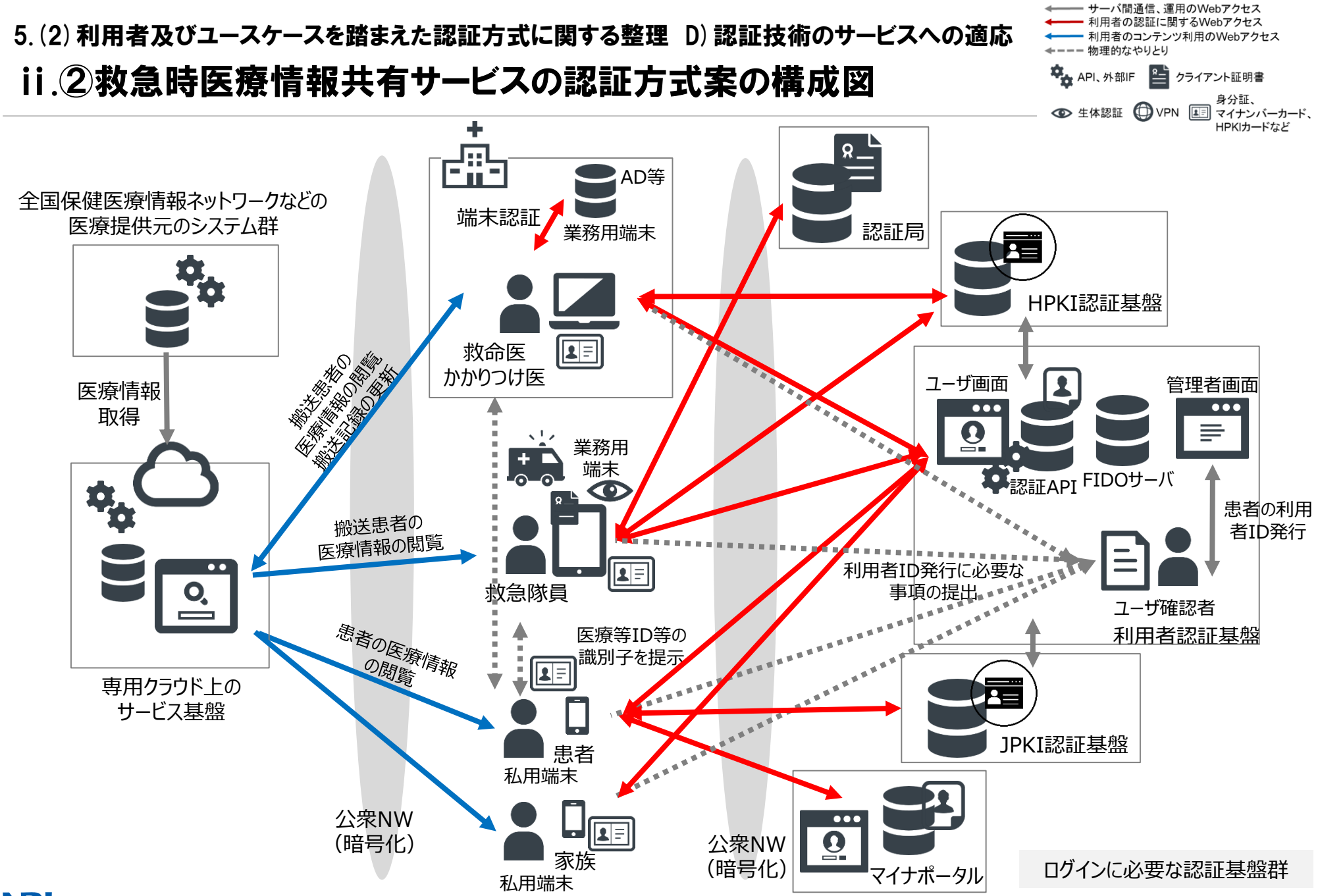
取り扱う情報	必要な認証数	その他
個人情報	2	なし

■ モデルごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
②-a	救急隊員	業務用端末	資格の確認要	・HPKIカード ・顔写真付きの身分証 ・資格を示す情報	・クライアント証明書 ・生体	前述の技術評価より、業務用端末向けの組み合わせとして適するものを選定
①-a	救急医、かかりつけ医	業務用端末	資格の確認	・HPKIカード ・顔写真付きの身分証 ・資格を示す情報	・施設管理下の認証（入退室,端末等） ・パスワード	前述の技術評価より、1要素に適するものを選定
②-b	患者	私用端末	なし	・公的個人認証 ・顔写真付きの身分証	・パスワード ・指紋	前述の技術評価より、私用端末向けの組み合わせとして適するものを選定
	患者の家族	私用端末	なし	・公的個人認証 ・本人の同意書 ・顔写真付きの身分証 ・本人の同意書	・パスワード ・指紋	前述の技術評価より、私用端末向けの組み合わせとして適するものを選定

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.②救急時医療情報共有サービスの認証方式案の構成図



NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.②救急時医療情報共有サービスの認証方式案の説明

- 想定する利用者は、救急隊員、救急医、かかりつけ医、患者、患者の家族とした。またログイン後の機能により、救急隊員、救急医、かかりつけ医と患者の紐付け、患者の家族は自身と患者の紐付けは、医療等ID等をもちいて行われることを前提とした。
- サービス①と同様に理由にて、ID登録の方法を以下の2通りとした。
  - オンラインでの公的個人認証またはHPKIカードの利用、自身でのID登録。
  - 顔写真付きの身分証（または、加えて職種を示す情報）を郵送等で提出、ユーザ確認者が確認。運用者側でID登録し、利用者へ初期パスワードとともに通知。
    - なお、現状、普及度は高くないものの、救急救命士もHPKIカードを利用可能であるため、資格認証のためにもちいることとした。
- 救急隊員は、5.各技術の評価にて緊急時の業務用端末利用に適したクライアント証明書認証＆生体認証をもちいることとした。
- 救急医、かかりつけ医は、所属の施設管理下での入退室の認証・端末認証等を見込み、パスワード認証のみをもちいることとし、認証方式が業務負担とならないよう配慮した。
- 患者、患者の家族は私用端末を利用することから、5.各技術の評価にて私用端末の利用に適すると評価されたパスワード認証＆指紋認証をもちいることとした。なお、国民にとっての利便性や普及度の向上を鑑みGoogle ID, Yahoo IDなどの外部IDの活用も検討すべきと考える。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.②救急時医療情報共有サービスの認証方式案

●：必須、1・2はどちらかが必須　○：任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種（資格）	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
救急隊員	ID登録	–	–	–		●			●		●			1●			2●				
	ログイン	2	0	2					●									●	●		
救急医、かかりつけ医	ID登録	–	–	–		●			●		●			1●			2●				
	ログイン	2	1	1					●						●						
患者	ID登録	–	–	–					●					1●		2●					
	ログイン	2	0	2					●						●				●		
患者の家族	ID登録	–	–	–			○		●			○		1●		2●					
	ログイン	2	0	2					●						●				●		

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.③PHRサービスの認証方式案

サービス全体

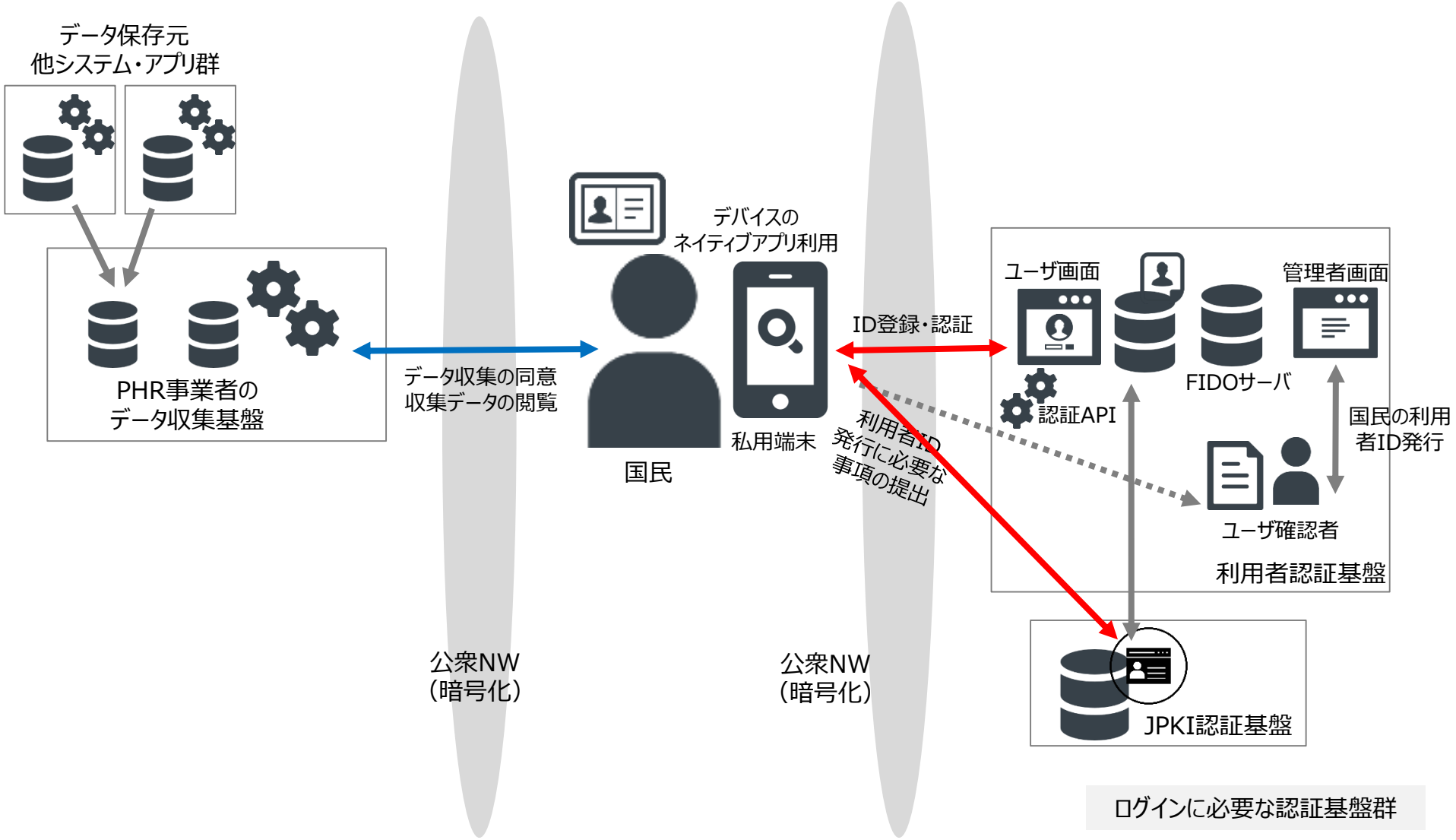
取り扱う情報	必要な認証数	その他
個人情報	2	なし

モデルごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
③-a	国民	私用端末	なし	・公的個人認証 ・顔写真付きの身分証	・パスワード ・指紋	前述の技術評価より、私用端末向けの組み合わせとして適するものを選定

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.③PHRサービスの認証方式案の構成図



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.③PHRサービスの認証方式案の説明

- 想定する利用者は、国民である。
- スマホ向けネイティブアプリからのサービス利用を想定した。
- サービス①と同様に公的個人認証の活用が望ましいが、それらの普及度が十分でないことを考慮し、公的個人認証を用いない方法も検討し、ID登録の方法を以下の2通りとした。
  - オンラインでの公的個人認証の利用、自身でのID登録。
  - 顔写真付きの身分証を郵送等で提出、ユーザ確認者が確認。運用者側でID登録し、利用者へ初期パスワードとともに通知。
- 利用者によるログインには、5.各技術の評価にて私用端末の利用に適すると評価されたパスワード認証＆指紋認証をもちいることとした。なお、国民にとっての利便性や普及度の向上を鑑みGoogle ID, Yahoo IDなどの外部IDの活用も検討すべきと考える。

●：必須、1・2はどちらかが必須　○：任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種（資格）	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
国民	ID登録	–	–	–					●					1●		2●					
	ログイン	2	0	2					●						●				●		

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.③健康スコアリングサービスの認証方式案

サービス全体

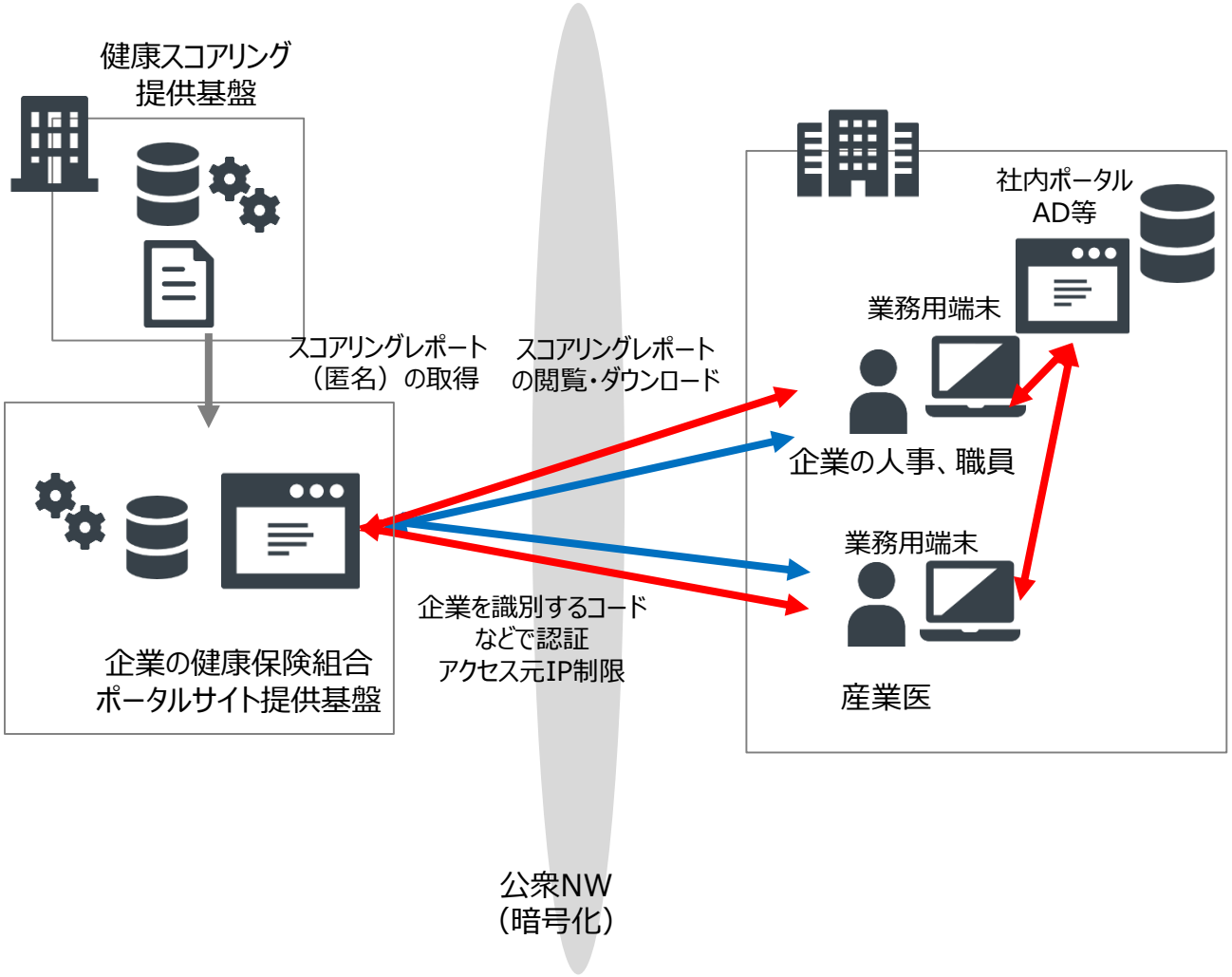
取り扱う情報	必要な認証数	その他
匿名化情報	1	利用者認証基盤を利用しないで企業の既存の仕組みを利用することを想定

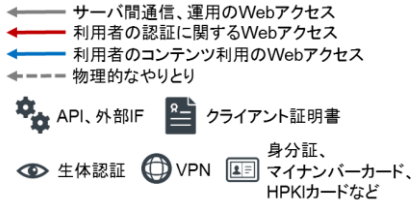
モデルごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）確認	認証方法		
				ID登録	ログイン時	選定の経緯
③-b	企業の人事、職員	業務用端末	なし	企業保有のADないし、既存の企業の保険組合ポータルサイトの利用に必要な仕組み		前述のサービス想定の検討により、左記の方法が簡便であると考えた
	産業医	業務用端末	なし	企業保有のADないし、既存の企業の保険組合ポータルサイトの利用に必要な仕組み		前述のサービス想定の検討により、左記の方法が簡便であると考えた

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.③健康スコアリングサービスの認証方式案の構成図





Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

ii.③健康スコアリングサービスの認証方式案の説明

- 想定する利用者は、企業の人事職員、産業医となる。
- 企業の健康保険組合のポータルサイトで、スコアリングレポートを閲覧・ダウンロード可能とすることを前提と置き、健康スコアリング提供基盤から、ポータルサイトへサーバ間通信にてスコアリングレポートを連携する形を想定した。
- スコアリングレポートは匿名化情報であるために、利用者のアクセスに必要な認証は1要素で良いと考える。
- 想定されるサービス内容では、利用者は健康保険組合のポータルサイトへの既存のログイン方法によるサービス利用が可能と考えられた。よって、新たな利用者認証基盤の検討は不要と考えられた。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.④データヘルス分析サービスの認証方式案

サービス全体

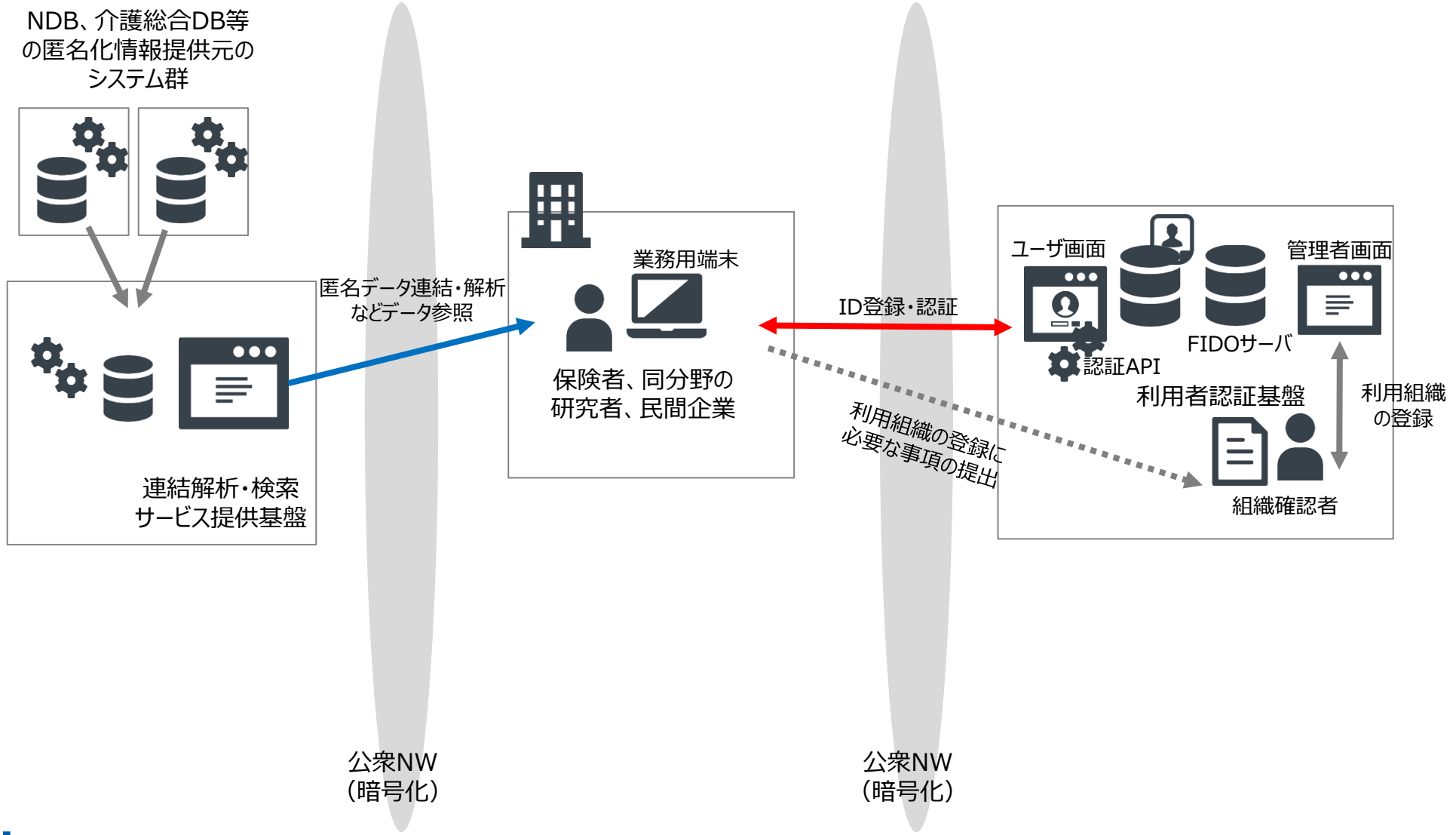
取り扱う情報	必要な認証数	その他
匿名化情報	1	登録していない組織（アクセス場所）からのサービス利用を避けるためにIP制限を想定

モデルごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
④	保険者、同分野の研究者、民間企業	業務用端末	組織の確認要	・組織ID	・パスワード	・利用者IDは、利用組織のIDとともにオンラインで本人が登録人物との紐付けは考慮しない

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.④データヘルス分析サービスの認証方式案の構成図



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.④データヘルス分析サービスの認証方式案の説明

- 想定する利用者は、保険者、同分野の研究者、民間企業とした。
- 業務用端末からの利用が想定され、研究目的に沿った組織に属する職員の利用が想定される。利用する必要性が認められる組織を登録制にすることとし、登録により利用組織ID等の組織を示す情報を発行する。研究者個人レベルの認証は不要とした。このような運用とすることで、組織レベルでの利用者の妥当性を確保しつつ、個人ごとの運用負担を軽減し、普及度を確保できると考える。
- 利用者IDはパスワード、利用組織のIDとともにオンラインで本人が登録、利用者はパスワード認証を行う。
- なお、今後のサービスの仕様の変更などにより、2要素認証を要する場合は、所有物認証又は生体認証の併用が選択肢となりえる。所有物認証では5.各技術の評価の結果よりクライアント証明書の選択肢となるが、この場合、各端末ごとのインストールが必要となる。一方、生体認証ではFIDOサーバの導入を前提する限り利用者側での負担なく利用できる。よって、本研究では生体認証の併用を選択することとした。

●:必須　○:任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種（資格）	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
保険者、同分野の研究者、民間企業	ID登録	–	–	–	●					●											●
	ログイン	1	0	1						●					●				○		●

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑤科学的介護サービスの認証方式案

■ サービス全体

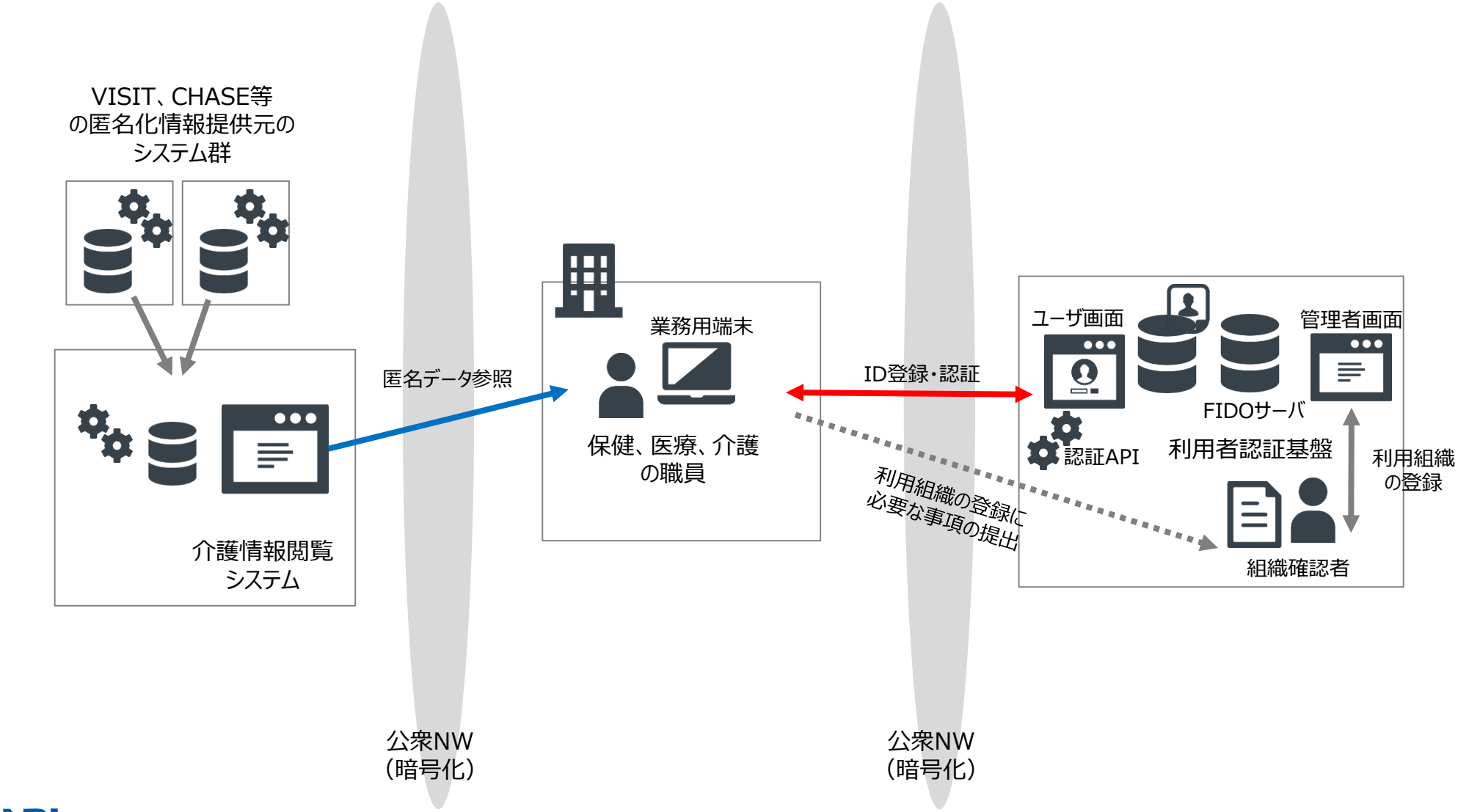
取り扱う情報	必要な認証数	その他
匿名化情報	1	登録していない組織（アクセス場所）からのサービス利用を避けるためにIP制限を想定

■ 利用者ごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
⑤	保健、医療、介護の職員	業務用端末	組織の確認要	・組織ID	・パスワード	・利用者IDは、利用組織のIDとともにオンラインで本人が登録。実在のその際、人物との紐付けは考慮しない。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.⑤科学的介護サービスの認証方式案の構成図（公衆NWを介して情報を利用すると想定した場合）



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑤科学的介護サービスの認証方式案の説明

- 想定する利用者は、保健、医療、介護の職員とした。
- サービス⑤と同様の理由により、利用する必要性が認められる組織を登録制にすることとした。利用登録により利用組織ID等の組織を示す情報を発行する。
- 利用者IDはパスワード、利用組織のIDとともにオンラインで本人が登録、利用者はパスワード認証を行うこととした。
- なお、今後のサービスの仕様の変更などにより、2要素認証を要する場合は、サービス④と同様に理由により生体認証の併用を選択することとした。

●:必須　○:任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種（資格）	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
保健、医療、介護の職員	ID登録	–	–	–	●					●											●
	ログイン	1	0	1	●										●				○		●

NRI Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑥がんゲノム医療サービスの認証方式案

サービス全体

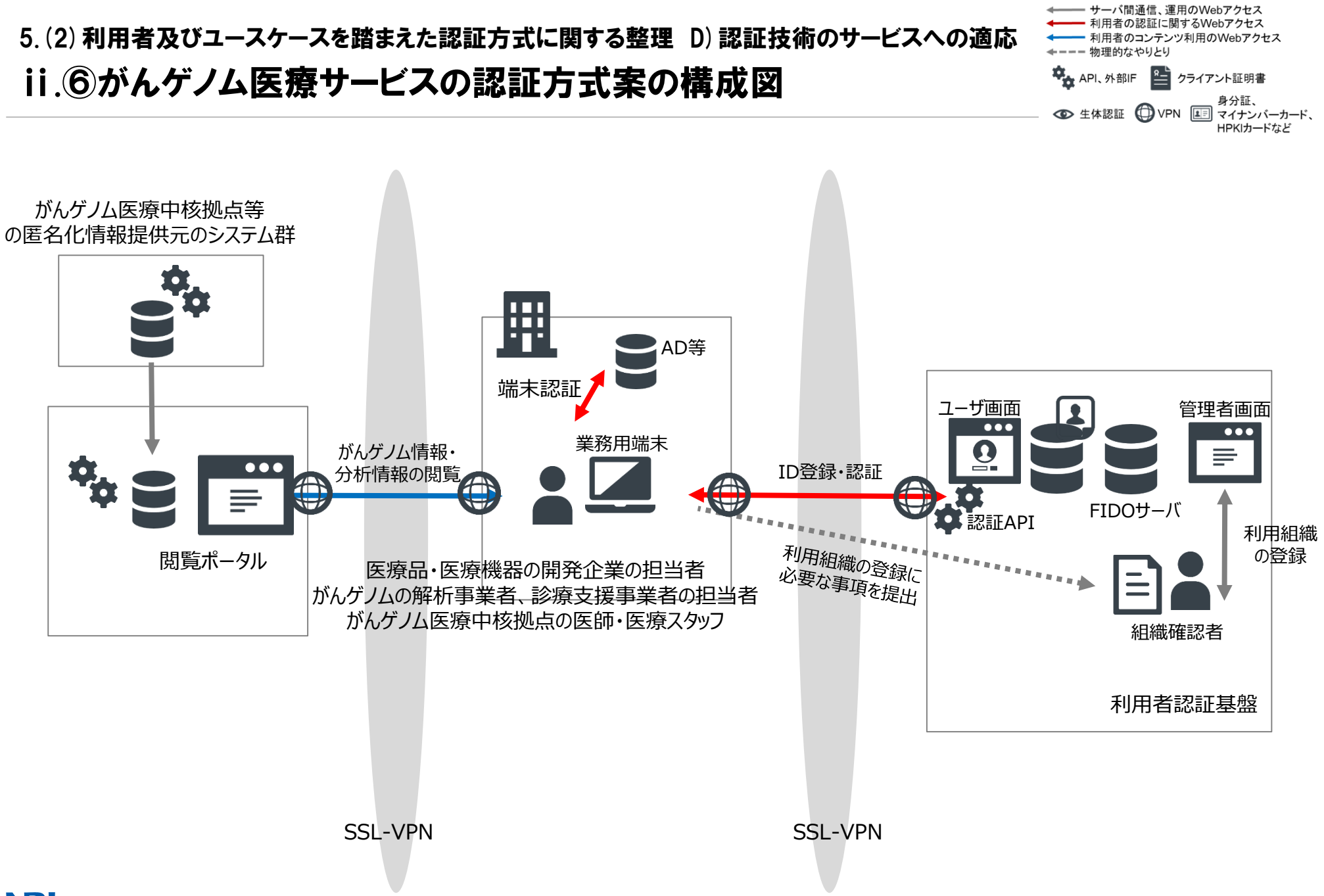
取り扱う情報	必要な認証数	その他
個人情報	2	情報の機微性により閉じたネットワークでのサービス利用を想定

利用者ごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種（資格）の確認	認証方法		
				ID登録	ログイン時	選定の経緯
⑥	関連企業、事業者、医療スタッフ	業務用端末	組織の確認要	・組織ID	・施設管理下の認証（入退室,端末等） ・パスワード	・利用者側の組織において業務用端末向けにAD等の端末認証や、施設入館の認証が導入済であると想定 ・前述の技術評価より、1要素に適するものと選定

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

ii.⑥がんゲノム医療サービスの認証方式案の構成図



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑥がんゲノム医療サービスの認証方式案の説明

- 想定する利用者は、医薬品・医療機器を開発する企業、がんゲノムの解析事業者、診療支援事業者、がんゲノム医療中核拠点の医師、医療スタッフとした。
- 以下の点より、他サービスとは独立したネットワーク（SSL-VPN）でのサービス提供とし、利用する必要性が認められる組織を登録制にすることとした。利用登録により利用組織ID等の組織を示す情報を発行する。
  - 他サービスに比べて利用者数少ない。
  - サービス利用場所が、物理的に限られる。
  - 漏洩に関するリスクをみたときに機密性が高いとされる生体情報を扱う。
- がんゲノムデータへのアクセスには2要素の認証が必要と考える。ここでは、利用者側の所属組織において業務用端末向けにAD等の端末認証が導入済のことを想定し、利用者認証基盤側では1要素の認証を求める前提とする。
- 利用者IDは利用組織のIDとともにオンラインで本人が登録、利用者はパスワード認証を行う。なお、今後のサービスの仕様の変更などにより、さらなる認証を要する場合は、サービス④と同様の理由により生体認証の併用を選択することとした。

●：必須　○：任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種（資格）	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
関連企業、事業者、医療スタッフ	ID登録	－	－	－	●					●										●	●
	ログイン	2	1	1	●										●				○	●	●

ii.⑦保健医療分野AI(画像診断)の認証方式案

■ サービス全体

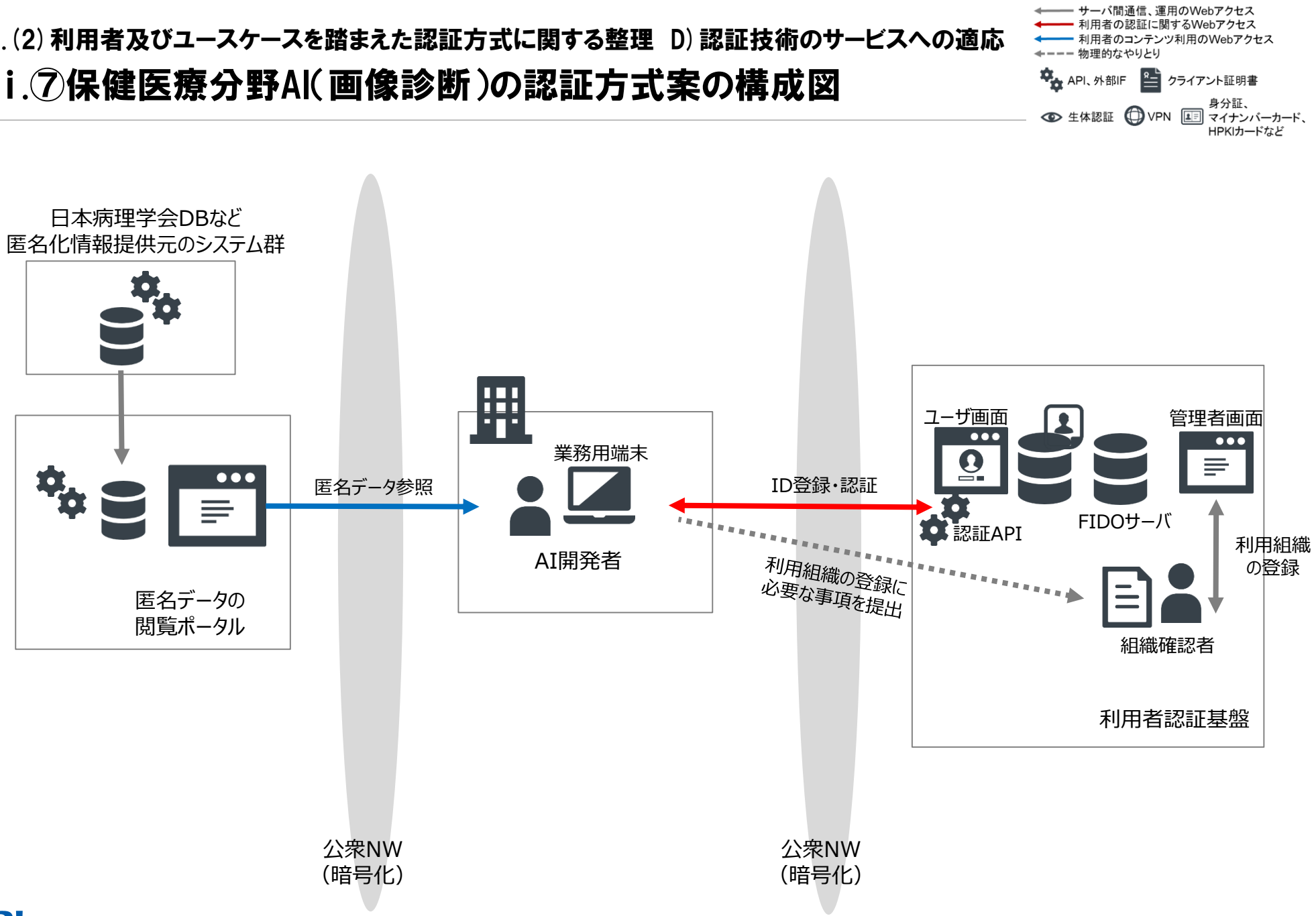
取り扱う情報	必要な認証数	その他
匿名化情報	1	登録していない組織(アクセス場所)からのサービス利用を避けるためにIP制限を想定

■ 利用者ごとの想定、認証方式案の検討

モデル番号	想定利用者	使用端末	組織、職種(資格)の確認	認証方法		
				ID登録	ログイン時	選定の経緯
⑦	AI開発者	業務用端末	組織の確認要	・組織ID	・パスワード	・利用者IDは、利用組織のIDとともにオンラインで本人が登録。実在のその際、人物との紐付けは考慮しない

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑦保健医療分野AI(画像診断)の認証方式案の構成図



Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ii.⑦保健医療分野AI(画像診断)の認証方式案の説明

- 想定する利用者は、AI開発者とした。
- サービス④と同様の理由により、サービスを利用する組織を登録制にするとする。利用登録により利用組織ID等の組織を示す情報を発行する。
- 利用者IDは利用組織のIDとともにオンラインで本人が登録、利用者はパスワード認証を行う。なお、今後のサービスの仕様の変更などにより、2要素認証を要する場合は、サービス④と同様の理由により生体認証の併用を選択することとした。

●:必須　○:任意

利用者	操作	認証の要素数の合計	利用者の組織の管理下	利用者認証基盤側	特定事項					必要な情報										制限	
					組織	職種(資格)	世帯	代理人	本人	組織を示す情報	職種を示す情報	世帯を示す情報	代理を示す情報	ICカード以外の身分証	パスワード	マイナンバーカード	HPKIカード	クライアント証明書	生体	VPN利用	IP制限
AI開発者	ID登録	–	–	–	●					●											●
	ログイン	1	0	1	●										●				○		●

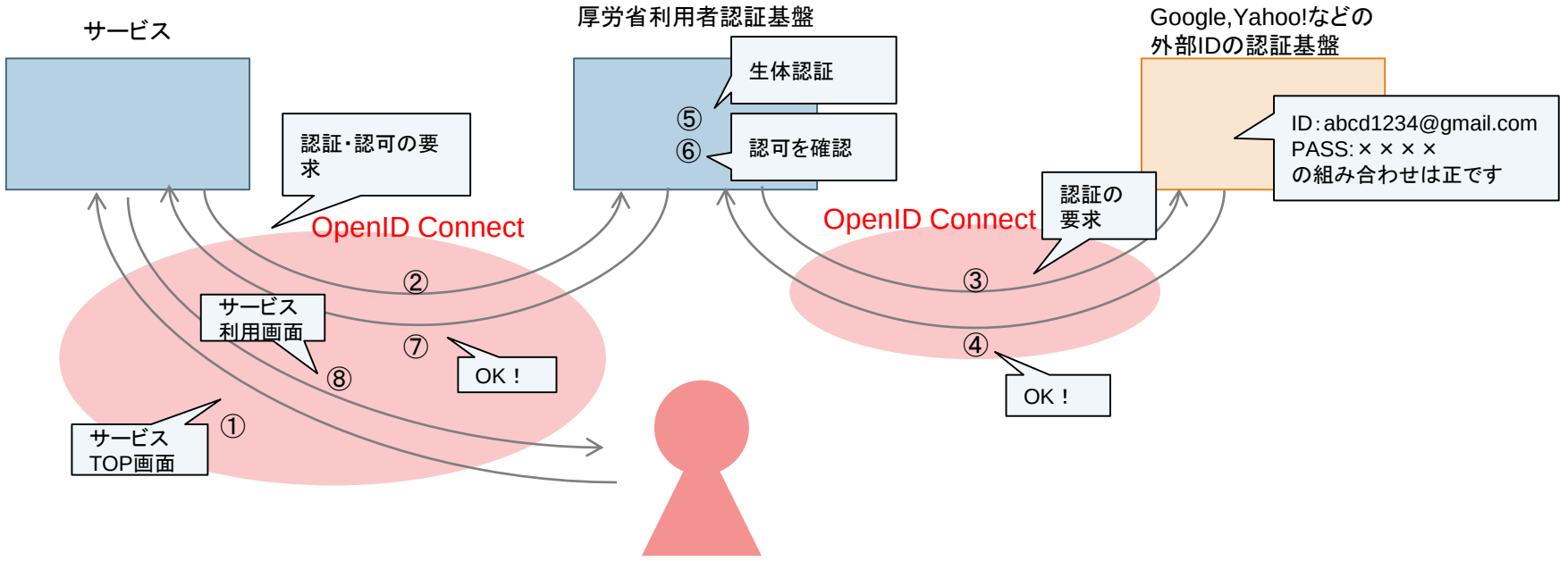
Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

OpenIDとは、業界では一般的にOpenID Connectという認証連携方式を指し、必ずしもGoogleやYahoo!などの外部IDの利用を前提としない

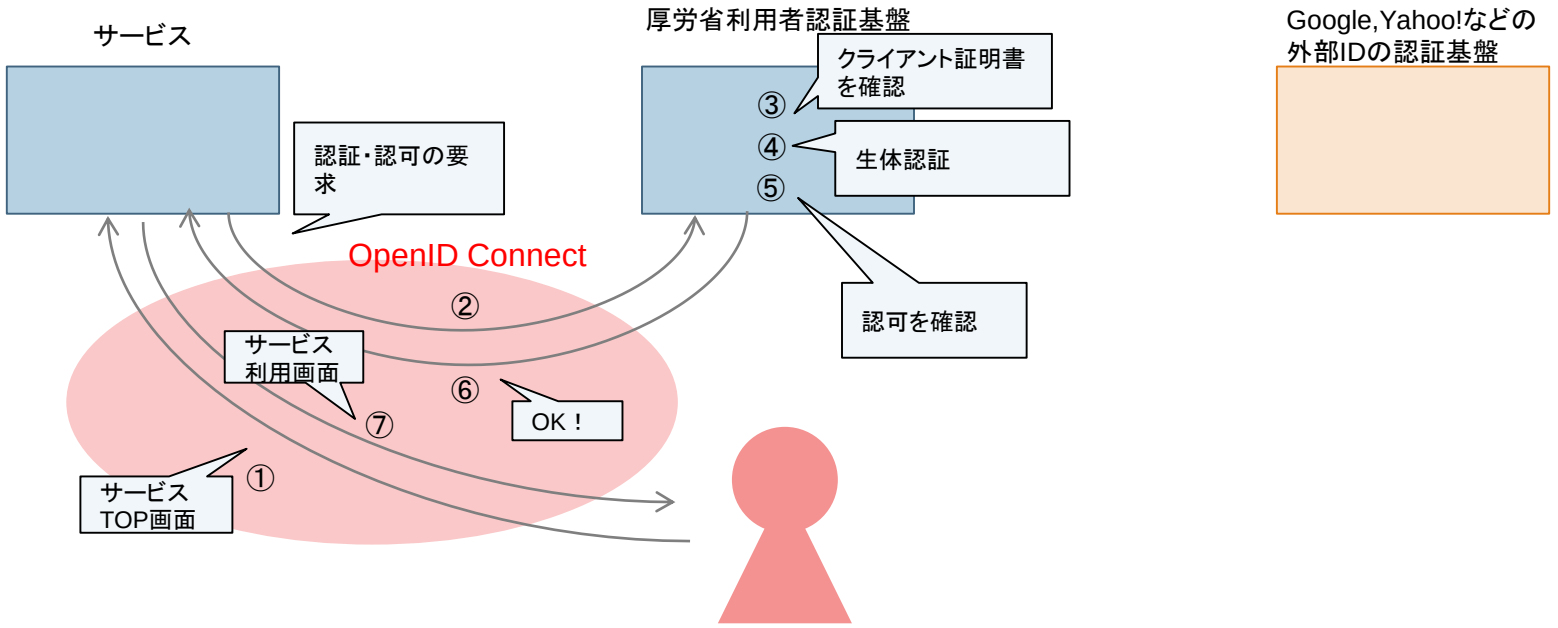
- OpenID Connect
  - インターネット上にある様々なWebサイトや、モバイルアプリなどを利用する際に一つのIDで認証を実現できるようにするID連携の仕組み。
  - GoogleやYahoo!もOpenID Connectの仕様をサポートしているため、OpenID Connectを用いた認証連携が出来るサービスの一部にあたる。Open IDとの区別のため、本事業においてはこれらのIDを「外部ID」と呼ぶ。
  - OpenID Connectは必ずしもこれらの外部IDの利用を前提としない（下図の右のオレンジの箱がない場合にも成立する、後述）。



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

【参考】OpenID Connectを認証連携方式として利用しつつ、GoogleやYahoo!などの外部IDを利用しない場合もある

- OpenID Connectに対応しつつ、外部IDを利用しない場合の例
  - 前述のフェデレーショングループAのうち、介護従事者の利用時に業務用端末よりクライアント証明書＆生体認証によりサービスを利用する場合を例示する。
  - 業務用端末が共用端末であると想定されること、また生体認証のみを求める外部IDの認証基盤が現状存在しないことを踏まえると、外部IDを利用は想定されない。よって、外部ID基盤側による認証ではなく、利用者認証基盤側で認証を行うこととなる。
  - 上記の前提でフェデレーション技術としてOpenID Connectを利用する場合には、サービスと厚労省利用者認証基盤の間のID連携を行うのみとなる。OpenID Connectではこのような活用の仕方も想定される。



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

Googleなどの広く普及した外部IDでの認証は、ユーザーの利便性を高めるほか、サービス利用のハードルを下げることで、サービスの普及率向上に貢献する

- 全国保健医療情報ネットワークでは、国民や医療従事者に広く普及されることが重要と考えられ、その促すための工夫が必要となる。
- Googleなどの広く普及した外部IDで認証を行うことは、サービスの普及面で以下のようなメリットが考えられ、各サービスの普及に貢献するものと思われる。
- よって、活用において後述する課題はあるものの、全国保健医療情報ネットワークへの外部IDの活用を検討する価値があると考える。

1. ユーザーの利便性が高い
   - 使い慣れたログイン方法で利用が可能になる。
   - 多くのインターネットサービスを利用する現代社会において、ユーザーのID管理をしやすくできる。
   - ID・パスワードを忘れにくい。

2. サービスの普及率向上
   - 使用頻度の低いサービスであってもIDを忘れることがなく、気軽にサービスを利用できる。
   - 使いやすさ自体が、ID登録のインセンティブになる。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

全国保健医療情報ネットワークにおいて、患者（本人）及び患者・代理人からの利用時にGoogleやYahoo!などの外部IDの活用が可能と考える

- 外部IDを使った認証について、全国保健医療情報ネットワークへの適応可否について考え方を以下に示す。
  - 閉域のネットワークにおける認証基盤ならびにサービス利用が想定される場合には、外部IDの利用は適当ではない。利用する外部IDのドメインなどについて通信を許可する設定が必要となるため現場での運用が難しいものと考える。
  - 業務用端末からの認証基盤ならびにサービス利用が想定される場合には、外部IDの利用は適当ではない。例えば、医療現場における業務用端末は他の職員・従業員との共用端末である可能性があり、外部IDを利用すると外部ID側の認証基盤におけるログアウトも必要となるため現場での運用が難しいものと考える。
  - 外部IDのそれ自体は基本的に個人が自己申請に基づいて発行したものであり、本人確認が成されているとは言いがたく、IAL2を満たすとは限らない。この対策のために、本人確認が公的個人認証基盤でなされたあとに、その本人により利用者認証基盤において、外部IDの紐付がなされる必要がある。

フェデレーショングループ	利用者	ネットワーク	利用端末	外部ID利用の可否
A ①保健医療記録共有 ②救急時医療情報共有 ③PHR	医療従事者	公共（暗号化）	業務用端末	否
	救急隊員			
	介護従事者			
	患者（本人）		私用端末	可
	家族・代理人			
B⑥がんゲノム医療	利用者（名称略）	閉域	業務用端末	否
C⑦保健医療分野AI（画像診断）	AI開発者	公共（暗号化）		

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

外部IDの利用には下記のような課題をクリアする必要がある。フィッシングなどの危険もあることから、リスクを十分に理解した上で活用する必要がある

	課題	対応策
1	Googleなどの外部ID基盤側で、本人確認がきちんとできない。（偽のアカウントを作ることも可能）	利用者認証基盤側で登録の際にきちんと本人確認を行ったうえで、Googleなどの外部IDと紐付ければ問題なく対応可能。
2	外部IDの認証基盤の利用では2要素認証が、ユーザ自身の設定によるものであるため確保できない。（ガイドライン上2要素認証が必要とされているものについての対応が必要）	外部IDの正誤に追加して、利用者認証基盤側で指紋などの2要素目の認証を組み合わせることで対応可能。
3	外部IDとの連携に伴い、システム上の仕様の設計に時間がかかる。	どの外部IDで認証を行うかの選定と、実証等を通じて仕様を固めるなどの対応が考えられる。また、外部IDによる認証の機能をあとから追加するなどの段階的な実装も考えられる。
4	ネットワークへの接続が求められるため、閉域での実装には適さない。がんゲノムや閉域ネットワークで稼動している医療機関の端末などでは利用できない。	他人の情報を閲覧できる医師従事者・介護従事者などの利用では現状採用しない。 本人が自己の責任において自身の情報を見るPHRなどのサービスに絞り、新規IDを発行する方法と選択制にすることで、利便性の向上と安全性のバランスをとる。 また利用に当たってのリスクや留意点などについて、国民に対し十分なガイダンスを行う必要がある。
5	外部IDはあちこちのサービスで利用されているため、フィッシングなどにより認証情報が奪取されるリスクが高くなる。利用者認証基盤側でも認証を行うことで、直接悪用されづらいものの、利用者がそれらのリスクを十分に理解して選択する必要がある。	

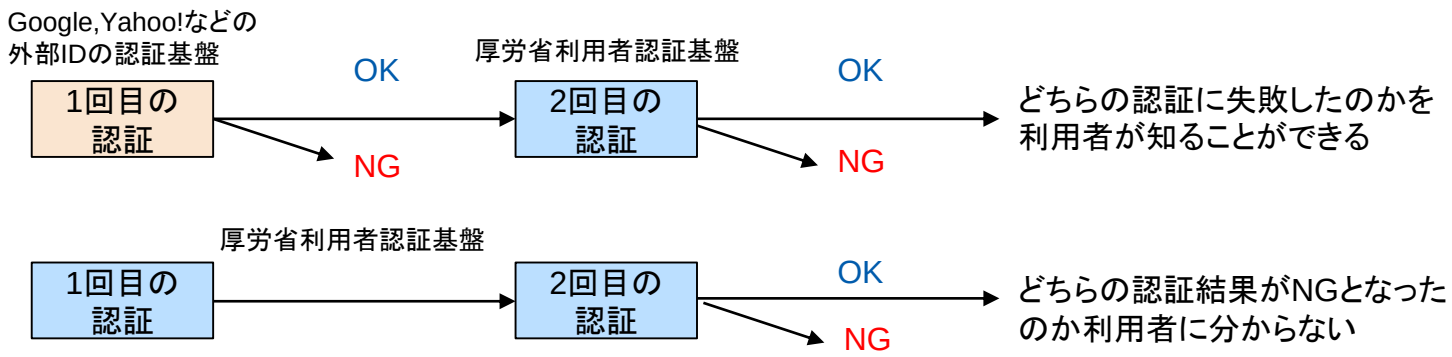
NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

その他、外部IDで認証を行う場合の一般的な留意点をまとめる

- 外部IDの認証基盤において、システムが機能しなくなっている場合には（システム障害の発生、一時的なアクセスの急増、DoS攻撃など）、利用ができない。オンラインでの利用経路を確保する場合、複数の外部IDで認証できる実装としておく、利用者認証基盤側で発行したIDでも認証ができるようにしておく必要がある。

- 外部IDの認証基盤における技術仕様や認証方式の影響を考慮する必要がある。例えばパスワード認証を将来的に取りやめる、技術仕様のうちのエラーハンドリングの仕方がアナウンスなしに変更になるといったケースも考えられる。その場合に、利用者認証基盤側での対応を検討する必要性がでてくる。

- 外部IDを用いる場合、認証基盤を個別に分けて利用することとなる（下図上段）。このような認証方式は医療情報システムの安全管理に関するガイドライン第5版では許容されており問題ない。ただし、2要素認証は一つの認証基盤で行われることが望ましい（下図下段）とされているため、外部IDを用いる場合は厳密な意味での2要素認証に比べて、認証の強度が劣ることを理解しておく必要がある。



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

OpenID Connect ＝ OpenID ＋ OAuth

- ID連携機能を提供するOpenID2.0と、API連携のためのアクセス制御機能を提供するOAuth2.0が合わさって、OpenID Connectの仕様が策定された。

ID連携

ID情報（認証結果と属性情報）を、安全にサービス間でやりとりするための仕様

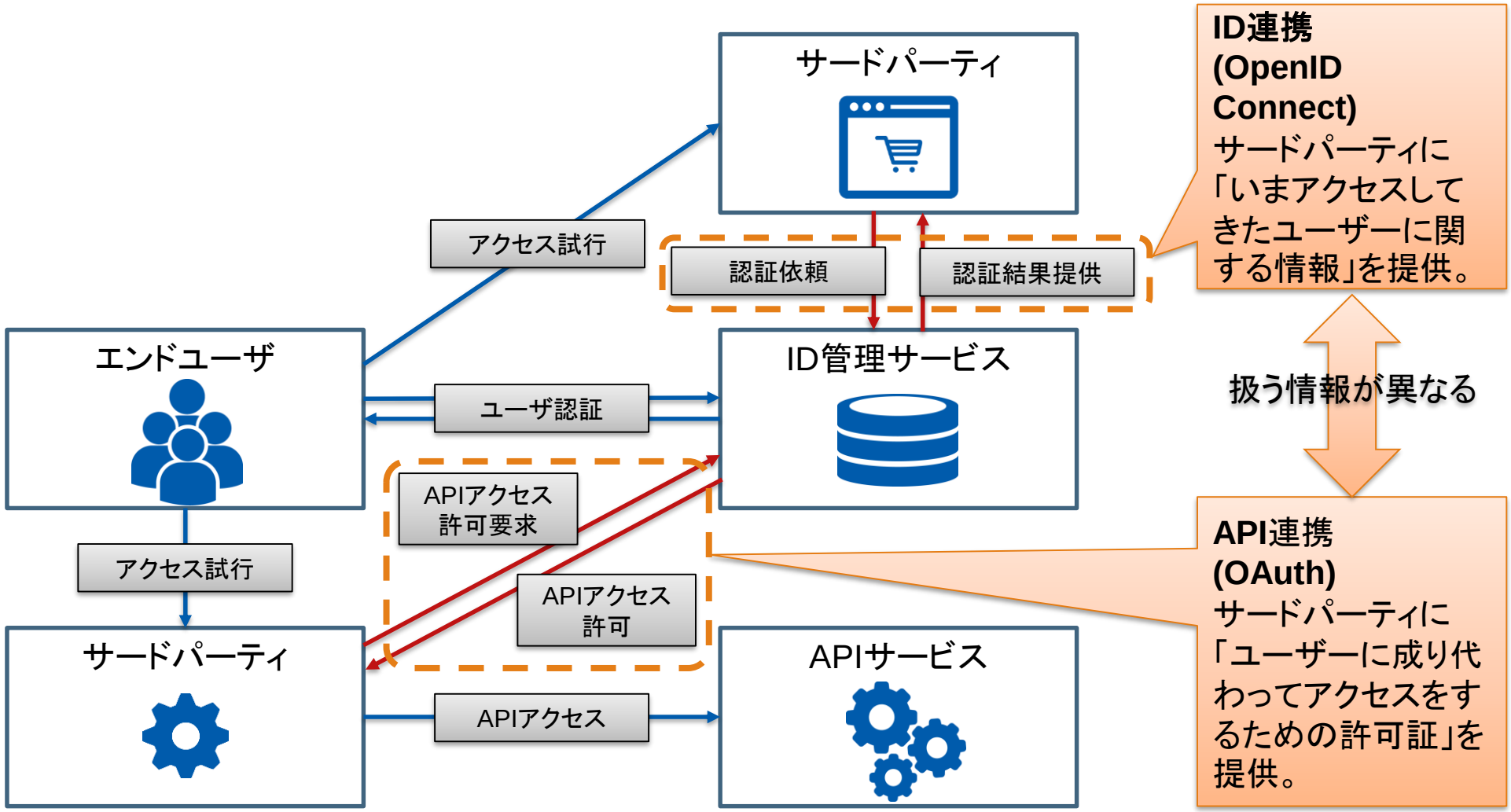
API連携

あるサービスのAPIアクセスの許可を、別のサービスに安全に与えるための方法

OpenID 2.0 ＋ OAuth 2.0 ＝ OpenID Connect

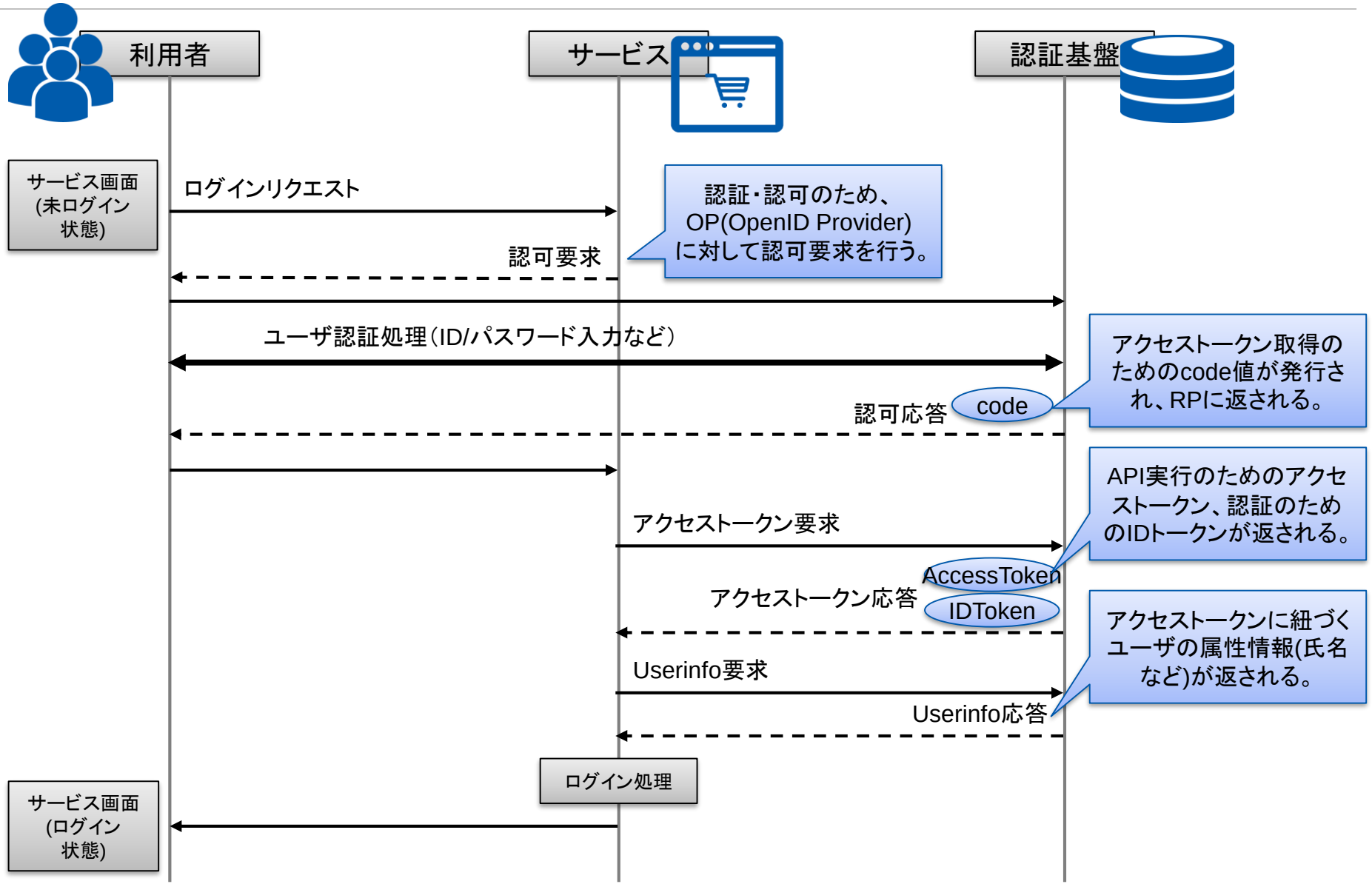
Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

OpenIDとOauthの役割の違い



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

OpenID Connect（認可コードフロー）シーケンス



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

（２）利用者及びユースケースを踏まえた認証方式に関する整理｜OpenID Connectの活用と留意点

ID連携とAPI連携の双方を提供するならば、OpenID Connectの利用が最も適している

		比較項目＼仕様	SAML 2.0	OpenID 2.0	OAuth 2.0	OpenID Connect
ID提供側（IDP）	ID連携	認証結果の連携	○	○	×（仕様外であり、OAuth採用事業者の独自拡張が乱立）	○
		属性情報の連携	○	○	×（仕様外であり、OAuth採用事業者の独自拡張が乱立）	○
		認証結果・属性情報への署名や暗号化	○	△（共有鍵による署名のみ可能。暗号化は仕様のスコープ外）	×（仕様のスコープ外）	○
		サイト間のセッション管理	○	×（仕様のスコープ外）	×（仕様のスコープ外）	○
		Webブラウザ以外（デスクトップアプリ、スマートフォンアプリなど）への対応	△（仕様上はWebブラウザ以外にも対応可能だが、実際に広く利用されているのはWebSSOのみ）	×（Webブラウザのリダイレクト機能に依存したプロトコルであり、Webブラウザ以外への対応は不可能）	○	○
	API連携	APIアクセス認可（アクセストークン配布）への対応	×	△（OAuth 1.0とのハイブリッドにより対応）	○	○
		複数のアクセストークンへの対応	×	×（仕様のスコープ外）	×（仕様のスコープ外）	○
		PC以外のデバイス（スマートフォン等）への対応	×	×	○	○
ID受入側（RP）		ID受け入れ側（リライングパーティ）の実装・運用の容易さ	××（XMLやSOAP、PKIなどのスキルが必要であり、通常はSAML処理ライブラリやミドルウェアの導入が必須）	△（鍵交換や署名処理が必要であり、通常はOpenID処理ライブラリなどの導入が必須）	○（ライブラリ等の導入が不要）	○（ライブラリ等の導入が不要）
特徴、懸念点			さまざまなユースケースに適用可能なフレームワークである。 しかし、それゆえに複雑であり、結果的には歴史的経緯による企業向けSaaSのSSOや、同一サービス内でのID連携に利用されるにとどまっている。	Webサイト間の認証結果・属性情報の交換に特化したプロトコルであり、従前の仕様（SAML 2.0)に比較して単純なプロトコルである。 しかし、鍵交換や署名処理など、まだ実装が容易ではない点が残る。	OAuth 1.0をベースに、より容易に実装できるように仕様を簡略化。 Web APIのアクセス認可フレームワークとして広く普及。 しかしI、D連携に関してはスコープ外であり、独自仕様が乱立している。	OAuth 2.0をベースに、ID連携のためのプロトコルを定義。OAuth 2.0の実装のしやすさを活かしつつ、ID連携に十分な機能を定義している。 しかし、技術仕様の各パラメータに設定すべき値やユースケースごとにどのシーケンスを適用すべきかについては定められていないため、個別に検討が必要となる。

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、全国保健医療情報ネットワークにおいても活用する価値がある

- 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。

- 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が確保しやすい。
  - 接続容易性は、相互セキュリティ維持性につながる。（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。）

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

OpenID Connectの活用においては、技術仕様のパラメータ設定の必要性やセキュリティレベルの確保などの留意点が挙げられる

- OpenID Connect の仕様においては、APIのリクエスト、レスポンスパラメータの定義、IDP、RPが実装すべき処理については定められているが、リクエスト、レスポンスの各パラメータに設定すべき具体的な値や、ユースケースごとにどのシーケンスを適用すべきかについては定められていない。

- OpenID Connectを正しく使い、認証基盤としての高いセキュリティを確保するためには、OpenID Connect仕様に対応済の製品を利用することに加えて、技術仕様のうちの各パラメータの設定、使い方に関する理解を深め、具体的な設定を検討することが必要となる。
  - http://openid-foundation-japan.github.io/openid-connect-core-1_0.ja.html#Security
    - 16. Security Considerations
  - https://tools.ietf.org/html/rfc6819

- より高いセキュリティレベルを確保するには、FAPIの参考が有効である。
  - 昨今、金融業界では顧客情報や取引に関する機能をAPI化して公開し、サードパーティからの利用を可能とする取り組みが進められている。そのためのより高いセキュリティレベルを確保する使い方について、国際標準化団体 OpenID Foundation のワーキンググループ主体となり金融API（Financial API）に関する標準仕様FAPIの策定が進んでいる。
  - Part1, Part2 のドラフト版が公開済。英OpenBankignがPart2を採用、米FS-ISACがPart1の採用を検討中である。
    - FAPI Part 1 Read Only API Security Profile
      http://openid.net/2017/02/19/fapi-part-1-implementers-draft-approved/
    - FAPI Part 2 Read and Write API Security Profile
      http://openid.net/2017/07/24/fapi-part-2-implementers-draft-approved/

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

FAPIの概要

- 金融機関でのAPI公開のためのOpenID Connectの使い方について、Part1 では参照系APIを対象として、Part2ではPart1の対応を前提として更新系APIを対象としてまとめられている。Part3～5はAPI仕様に関する記載となっている。

- これら自体はOpenID Connectのセキュリティ面への懸念を示唆するものではなく、例えばOpenID Connectについて誤った使い方をしていた場合にサービスとして悪意のあるアプリケーションが紛れ込むようなケースがあった場合、あるいは他のレイヤーの問題といえるネットワークの盗聴と処理シーケンスへの介入があった場合等に、それらを成立させないような、より厳格なセキュリティレベルを確保する使い方をまとめたものである。

- サービスと認可サーバとのシーケンスを成立させるためのいくつかの既存の方法（例えば、APIキー、リダイレクトURI、秘匿された情報であるシークレットなどのパラメータの検証）に加えて、一部に署名を付けて検証を行うようにする、認証認可の結果により発行されるトークンのエントロピーを引き上げる、シーケンスにおいて引き換えるトークン同子の紐付けとしてハッシュ値の埋め込みを既存のものに加えてさらに追加する、といった方法により、サービスと認可サーバとのシーケンスの正当性を高く確保するという内容が含まれる。

- その他、認可の結果、サービス側へ発行されるトークン自体が、サービス側から何らかの方法で奪取された場合には、そのトークン自体ではなく、そのトークン自体とクライアント証明書の紐付けを検証するトークンバインディングを実装する、あるいは、なりすましの対策としてユーザ認証にLoA3（※）レベルで多要素認証を求めるといった、実装面からも厳しい内容を含むものとなっている。

  ※ ITU-T X.1254（ISO/IEC 29115）で定義されたID管理を行う組織の運用管理基準に求めるレベル（Level of Assurance）の4段階のうちの1つ。NIST SP 800-63 においてLoA3は、IAL2、AAL2 FAL2と対応付けされている。

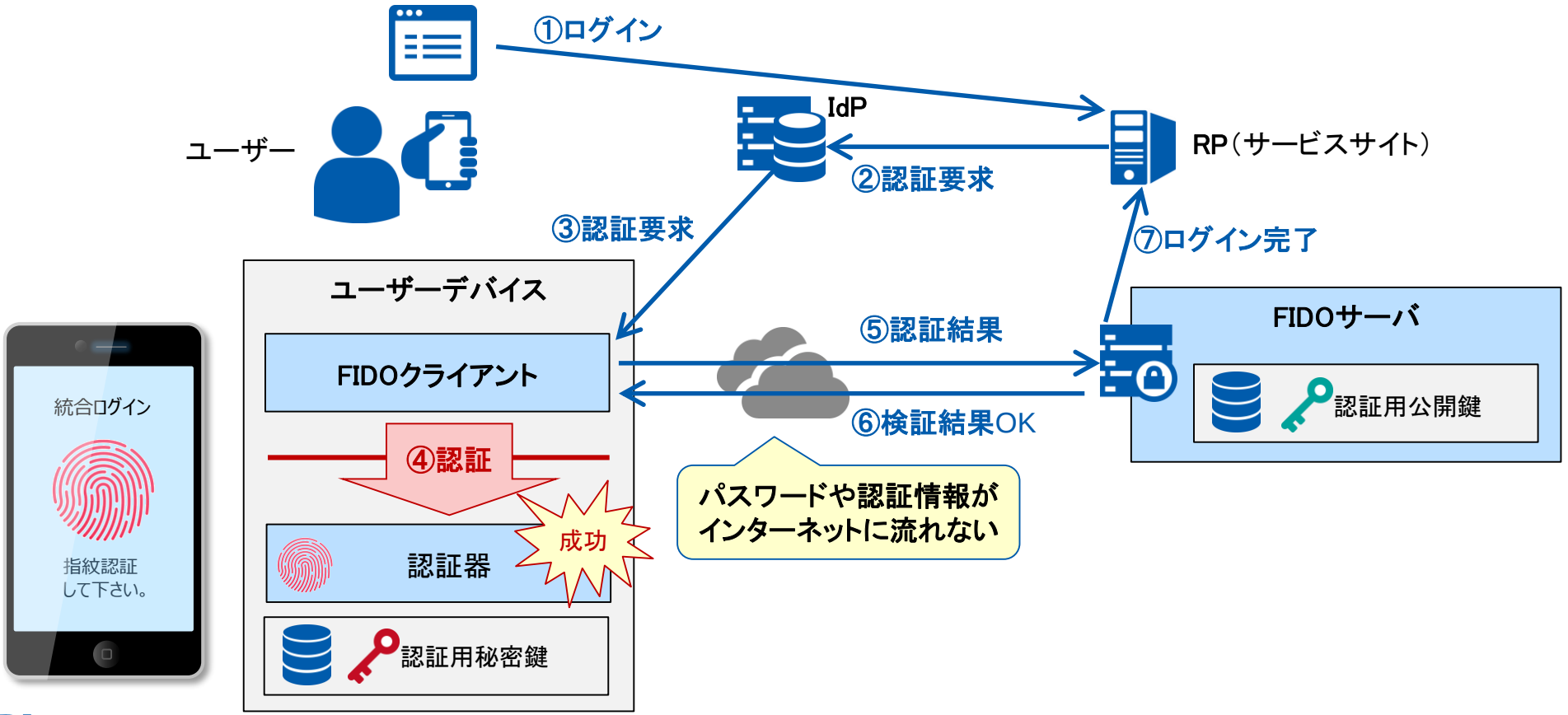
NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証のための秘密情報を伝送しない認証技術として、「FIDO」が存在する。

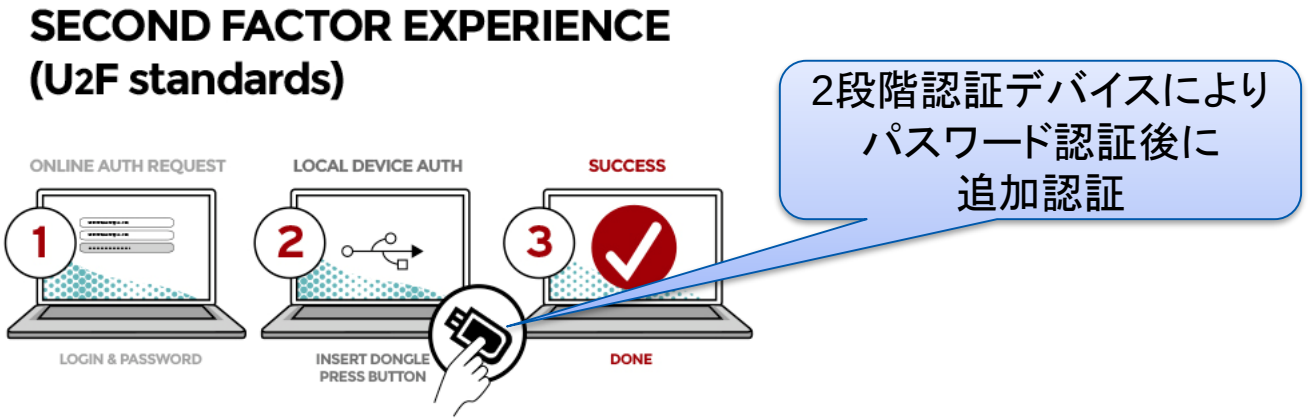
- FIDO（Fast Identity Online）認証は、公開鍵暗号方式を用いた認証方式の一種である。**認証に必要な秘密情報は認証を行う端末側のみに保存され、ネットワーク上での伝送やサーバー側での保存の必要がない**ことを特徴とする。
- Webブラウザの2段階認証を想定したFIDO U2F、モバイル端末付属の認証器（認証を行うためのデバイス）利用を想定したFIDO UAFが規定されている。



NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

FIDO U2Fは、追加デバイスによる2段階認証をサポート

- FIDO U2F（Universal Second Factor）の概要
  - 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）。



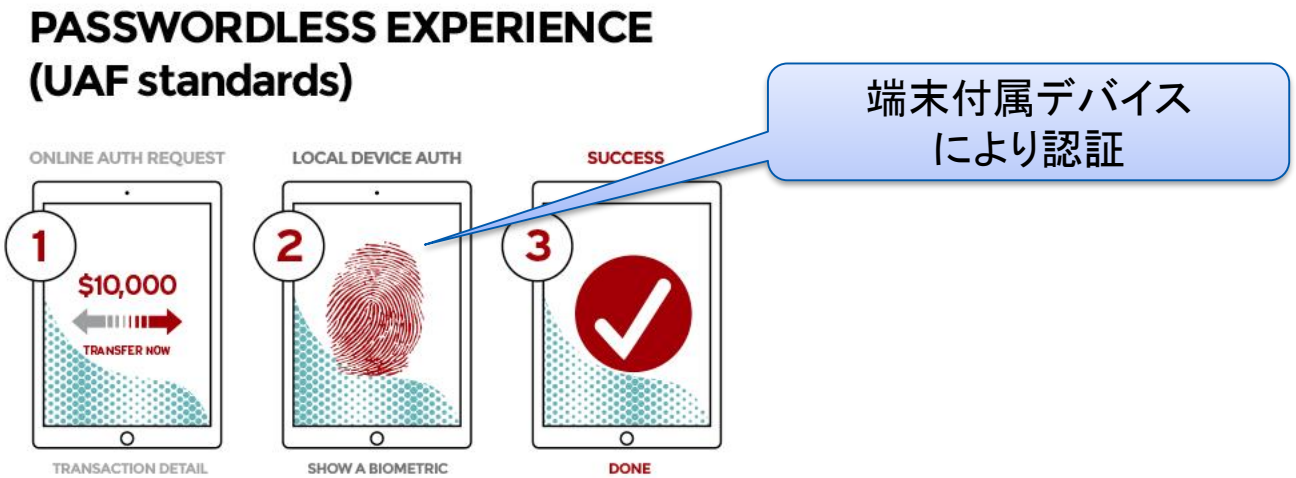
(引用元)「https://fidoalliance.org/%E3%82%A2%E3%83%97%E3%83%AD%E3%83%BC%E3%83%81%E3%81%A8%E3%83%93%E3%82%B8%E3%83%A7%E3%83%B3/」

- U2Fの特徴
  - 主に、PCの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。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

FIDO UAF は、パスワードレスな2要素認証をサポート

- FIDO UAF（Universal Authentication Framework）の特徴
  - 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。



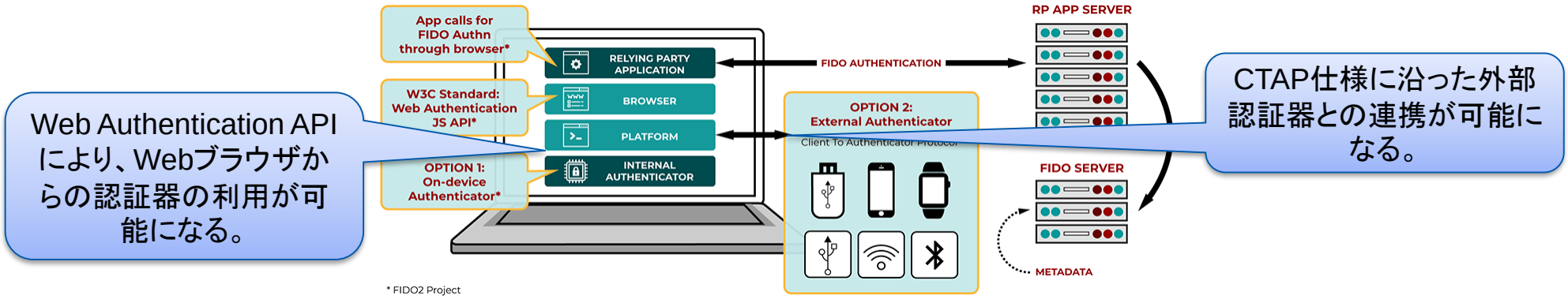
(引用元)「https://fidoalliance.org/%E3%82%A2%E3%83%97%E3%83%AD%E3%83%BC%E3%83%81%E3%81%A8%E3%83%93%E3%82%B8%E3%83%A7%E3%83%B3/」

- 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。
  - パスワードレスを想定しているため、事実上、所有物（スマートフォン）と生体による認証となる。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

FIDO2.0は、WebAuthentication、CTAPの2つの規格からなる

- FIDO 2.0の特徴
  - 広範なプラットフォームでFIDO認証機能を提供することを目的として、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。
  - 大きな仕様として、Web Authentication APIとCTAPが存在。



(引用元)「https://fidoalliance.org/fido2/」

- Web Authentication API (WebAuthn)
  - WebサイトがWebブラウザのJavascriptを介して認証器の情報にアクセスできるようにするインターフェースを定義。
  - 2018年4月、W3Cにおける勧告候補の仕様となった。

- CTAP(Client To Authenticator Protocol) 2.0
  - プラットフォーム(OS)やWebブラウザと、FIDO Authenticator(認証器)間の通信プロトコルを定義。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

FIDO2.0の実現により、広範な環境でパスワードレス認証が実現可能となる

- Webブラウザを利用したパスワードレス認証
  - 以下のいずれかの方法での認証が可能になる。
    - 1要素認証（USBキーなど）による認証
    - 多要素認証
  - 従来のFIDO U2F仕様では、パスワード認証＋追加認証の構成が前提となっているが、その制約がなくなる。

- 無線通信によるAuthenticator利用
  - CTAP2.0の実装により、従来のU2F対応デバイスに加え、無線通信を介した認証デバイス利用が可能となる。
    →スマートフォン、スマートウオッチなどを利用した認証が見込まれる。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

現時点では普及度やコストの課題はあるものの、FIDOは利便性とセキュリティをともに高める認証技術として注目をあびており、中長期視点では活用を想定すべき技術と考えられる

■ FIDOの適用に関する期待

- パスワードレス認証を実現するためには、従来カードリーダや生体認証器を用意する必要があった。
  これに対し、FIDO技術により、広く普及しているスマートフォンデバイスを認証器としてパスワードレス認証を実現できるようになることから、次世代の認証技術として注目されている。
- 認証情報をネットワーク上に流さないため、セキュアな方式と考えられている。また、事実上所有物認証と生体認証をかねるため、高いAALを確保できる。
- 実装面では、Android OSやWindows OS、WebブラウザについてはGoogle、Mozilla、Microsoftが順次FIDO対応を進めており、今後FIDO認証を使ったサービスが増えていくものと予想される。

■ FIDOの適用に関する課題

- 市場への普及の観点では、FIDO認証は黎明期であり、FIDOサーバ（およびFIDOクライアント）の実装コストは、メーカーによるものの現時点では安価とは言い難い状況にある。今後、製品の市場価格も含めた構想が必要となる。
- 日本で広く普及するiPhoneを提供するApple社はiOSのFIDOへの対応を明言していない。
  （※）FIDO UAFと類似の機能を提供するTouch ID、Face IDは、FIDOに必ずしも準拠しない独自仕様で構成。
  アプリケーション実装において、端末別の検討が必要になる。

■ FIDOの適用に関する今後の展望

- 現時点では普及度やコストの課題はあるものの、利便性とセキュリティをともに高める認証技術として注目をあびており、中長期視点では、全国保健医療情報ネットワークへの適用を想定すべき技術と考えられる。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フェデレーションの導入により、サービス利用時において、利用者はID連携・シングルサインオンの利用が可能となる

■ フェデレーションの考え方

- フェデレーション方式や実現するためのプロトコルには複数の種類があるが、利用者・認証基盤・サービスの3者間の一般的な関係を示した図式は以下の通りとなる。
- フェデレーションの考え方に共通する基本的な考え方をまとめる。
  - 認証基盤側からサービス側へ、ユーザ情報を連携（ID連携）する仕組みである。
  - 一般に、認証基盤側の認証結果でもってサービス側ではSSOの利用が可能となる。

5 Federation

This section is normative.

Federation プロトコルでは, Figure 5-1 に示すように Subscriber, IdP, RP の3者の関係が構築される. 各プロトコルによってどのタイムングでどの主体の間でどんな情報がやりとりされるかは異なる. Subscriber は通常ブラウザーを介して IdP と RP の両方とコミュニケーションをとる. RP と IdP の間のコミュニケーション方法は2通りある.

- *Front Channel*, Subscriber を介したリダイレクトを通じたコミュニケーション
- *Back Channel*, Subscriber を介さず RP と IdP の直接のコネクションを通じたコミュニケーション

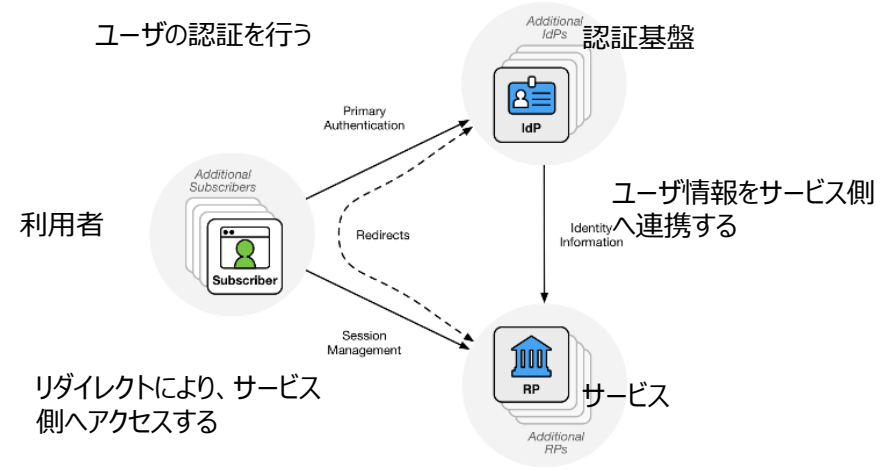


Figure 5-1 Federation

Subscriber は IdP に対して Authenticate し, Authentication イベントの結果が RP に対して Network 経由で提示される. この Transaction において, IdP は SP 800-63B にあるように Credential の Verifier として振る舞う. IdP はこのプロセスにおいて Subject に関する Attribute ステートメントを作成することも可能である. Attribute と Authentication イベントの情報は, Section 6 にあるように Assertion を通じて RP に伝送される. さらなる Attribute が Authorized Credential で保護されたセカンダリープロトコルを通じてやりとりされることもある (MAY).

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

Copyright（C） Nomura Research Institute, l

サービス毎の利用者に求める認証強度、ネットワークの条件を踏まえて、フェデレーションの範囲を検討する必要がある

フェデレーションの範囲に関する考え方の前提

- フェデレーションの実装に関するガイドライン・標準化仕様は一般に存在しているが、フェデレーションの範囲の考え方を示したものは、本研究において整理を行う。
- サービス③健康スコアリング、④データヘルス分析、⑤科学的介護については公開資料や企画者へのヒアリングから利用者認証基盤の利用が予定されていないと考えられたことから、本検討の対象には含めないこととした。
- フェデレーションの範囲の前提となる考え方は以下の通りとした。
  - 認証基盤には、ユーザの属性情報については最も新しいものが保持されている。
  - 認証基盤および各種サービスは、それぞれ異なるドメインのシステムとなっている。
  - 各種サービス間で認証やID連携に関する通信は、発生しない。

フェデレーションの範囲とするサービスや、その認証基盤に関する考え方

- 以上を踏まえて以下を前提としてこれ以降の検討を行った。
  - 認証基盤は、保守運用・構築・ユーザの最新の属性情報を保持する必要性から、数が少ない程良いものとする。
  - サービス利用時のネットワーク（閉域、公共）で、利用する認証基盤を分けるものとする。
  - フェデレーションに参加する各サービスは、ID登録時の本人確認の厳密さに差があってはならない。
  - フェデレーションに参加する各サービスは、ID連携によって認証基盤より取得したユーザ情報をもちいて、利用者の認証・同意結果に関わらずサービス利用可否（ユーザ利用の妥当性）の判定を行うものとする。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

対象となる5つのサービスを、想定されるネットワークの種類、求める認証の強度の観点から3つのグループに分類し、フェデレーションの検討を行った

- ①認証方式の検討内容を踏まえて、検討対象のサービスを以下の2つの観点から、A, B, Cの3つのフェデレーションのグループに分類した。
  - サービスの利用に想定されるネットワークの種類。
  - 認証基盤側でサービス利用のために求める認証の強度(ID登録の際の利用者IDと本人との紐付の確認の要否、および認証の要素数の合計)。

サービス	ネットワーク	認証の強度		フェデレーションのグループ
		利用者の本人確認	要素数	
①保健医療記録共有サービス	公衆（暗号化）	要	2	A
②救急時医療情報共有	公衆（暗号化）	要	2	
③PHR	公衆（暗号化）	要	2	
⑥がんゲノム医療	閉域	否	2	B
⑦保健医療分野AI（画像診断）	公衆（暗号化）	否	1	C

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

5.（2）利用者及びユースケースを踏まえた認証方式で示した認証方式案に基づき、フェデレーションのグループ毎に想定される処理イメージを整理した

- フェデレーションのグループ毎に、ID登録からログインを経てサービスを利用する流れの処理イメージを、その処理の主体となるシステムとともに整理した。
- ①認証方式の検討内容のうち、利用者自身による電子的なID登録・ログインを、整理の対象とした。窓口担当者が、本人・資格・組織などの確認を行い、管理者機能からID登録を行うケースは整理の対象外とした。
- 利用時の処理の流れを↓で表記した。空欄は、その利用者では不要な処理となる。
- 処理イメージと、その処理の主体となるシステムの関係は●で対応付けた。

例）一部項目など省略

処理順	処理イメージ	利用者	各サービス管轄	認証基盤管轄	その他
1	サービスTOP画面返却	↓	●		
2	認証基盤へリダイレクト	↓	●		
3	クライアント証明書確認	↓			●
4	ログイン画面返却	↓		●	
5	……	……	……	……	……

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

①保健医療記録共有、②救急時医療情報共有、③PHRの認証基盤の利用イメージ

- ①保健医療記録共有、②救急時医療情報共有、③PHRの利用者は、以下の流れで認証基盤を利用する　※個所の説明は、後述の緊急時の利用イメージ補足へ記載
- 医療従事者の1要素目の認証は、施設入館又は業務端末へのログインを想定している。
- 患者・家族代理人の利用については、外部IDの活用を前提としている。

青字個所：認証の要素数

処理順	処理イメージ	ID登録	ログイン	利用者（名称を一部略）					患者・家族代理人の外部ID利用	処理の主体		
				医療従事者	救急隊員	介護従事者	患者（本人）	家族代理人		各サービス	認証基盤	他システム
1	利用端末へログイン			↓1								●
2	サービスTOP画面返却			↓	↓	↓	↓	↓		●		
3	認証基盤へリダイレクト			↓	↓	↓	↓	↓		●		
4	クライアント証明書の確認				↓1	↓1					●	
5	ログイン画面返却			↓	↓	↓	↓	↓			●	
6	新規登録画面へ遷移			↓	↓	↓	↓	↓	左記に同じ		●	
7	所有する資格・本人確認			↓	↓	↓	↓	↓				●
8	同意書のアップロード							↓			●	
9	ID登録			↓	↓	↓	↓	↓			●	
10	ID登録完了画面返却			↓	↓	↓	↓	↓			●	
11	ログイン画面へ遷移			↓	↓	↓	↓	↓			●	
12	外部IDの認証基盤へ認証の要求								↓		●	
13	外部IDで認証　パスワードの照合								↓1			●
14	利用者認証基盤へリダイレクト								↓			●
15	利用者認証基盤での認証　パスワードの照合			↓2	※	↓	↓1	↓1			●	
	利用者認証基盤での認証　生体認証結果の検証				↓2	↓2	↓2	↓2	↓2		●	
16	同意画面返却			↓	↓	↓	↓	↓			●	
17	同意			↓	↓	↓	↓	↓			●	
18	サービスへリダイレクト			↓	↓	↓	↓	↓			●	
19	ユーザの認証・認可の結果の検証			↓	↓	↓	↓	↓	左記に同じ	●		
20	ユーザの属性情報取得の要求			↓	↓	↓	↓	↓		●		
21	ユーザの属性情報の返却			↓	↓	↓	↓	↓			●	
22	サービス利用可否の判定			↓	↓	↓	↓	↓		●		
23	利用者向けサービスの画面返却			↓	↓	↓	↓	↓		●		

①保健医療記録共有、②救急時医療情報共有、③PHRの認証基盤によるID連携のイメージ

- ①保健医療記録共有、②救急時医療情報共有、③PHRについて利用者とサービス利用のために必要と想定されるデータ内容の紐付けを、属性情報の項目毎に整理した。利用者の種類により認証基盤側で取得されない属性情報は、含めないこととした。
- 医療従事者においては、資格ごとの利用範囲の設定は各サービス側で設定されることが想定されるため、その所有する資格の種類に応じて、サービス側でサービス利用可否が判定されることとした。

※患者（本人）、家族代理人をシステム上区別する場合、その区別に必要な項目がID連携される属性情報に追加となる。またこの場合に、PHRサービスにおいて家族代理人による患者（本人）情報の閲覧を認めない設計とする場合は、家族代理人の認証は通ったとしても、サービス側の利用可否の判定により利用不可となる。

利用サービス	属性情報	利用者（名称を一部略）と、必要なデータ内容の紐付け				
		医療従事者	救急隊員	介護従事者	患者（本人）	家族代理人
①保健医療記録共有サービス	・ログインID	●		●	●	●
	・所有する資格に関する情報	●				
	・組織ID			●		
	・本人データと紐付く内部的な識別子				●	●
	・氏名	●		●	●	●
②緊急時医療情報共有	・ログインID	●	●		●	●
	・所有する資格に関する情報	●	●			
	・本人データと紐付く内部的な識別子				●	●
	・氏名				●	●
③PHR	・ログインID				●	※
	・本人データと紐付く内部的な識別子				●	※
	・氏名				●	※

①保健医療記録共有、②救急時医療情報共有、③PHRの認証基盤によるSSOのイメージ

- 1.ユースケースの詳細化とモデル化での検討内容を踏まえ、①保健医療記録共有、②緊急時医療情報共有、③PHRについて、SSOが想定されるサービスを利用者別に整理した。
- 医療従事者においては、認証結果が正であったとしても、所有する資格でのサービス利用が認められていない場合は、サービス側によりサービス利用不可の判定がなされる。

  ※患者（本人）、家族代理人をシステム上区別する場合、その区別に必要な項目がID連携される属性情報に追加となる。またこの場合に、PHRサービスにおいて家族代理人による患者（本人）情報の閲覧を認めない設計とする場合は、家族代理人の認証は通ったとしても、サービス側の利用可否の判定により利用不可となる。

利用サービス	利用者（名称を一部略）				
	医療従事者	救急隊員	介護従事者	患者（本人）	家族代理人
①保健医療記録共有サービス	●		●	●	●
②緊急時医療情報共有	●	●		●	●
③PHR				●	※

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

サービス②救急時医療情報共有の災害時の利用イメージ

- サービス②救急時医療情報共有では、救急時に加えて災害時の利用想定が含まれているため、本項で検討した。
- 災害時の利用者認証を切り出して検討すると、災害時の状況に応じて、利用者認証基盤を利用する場合と、利用しない場合の2つの利用方法が考えられた。

No.	利用者認証基盤	認証方法	考え方	利用者認証基盤側のシステムのイメージ例
1	利用する	・救急隊員は、2つ目の認証に生体認証ではなくパスワード認証を利用する（前項※個所） ・その他の利用者（医療従事者、患者本人、家族代理）の認証は変更なし。	・5.(2)で検討の検討結果より、救急隊員による利用では、グローブ・マスクの着用やカメラの動作に悪影響のでるコンディションの悪い外環境での利用が想定され、生体認証の利用に支障が出る可能性がある。 ・これにより救急隊員の業務端末利用時の認証方法は、次点であったパスワード認証＆クライアント証明書の組み合わせが妥当となる。	・利用者認証基盤側では、クライアント証明書＆生体認証ならびに、クライアント認証＆パスワードの両方を実装しておく。 ・利用者が認証処理を行う際に、2つめの処理を生体認証とパスワードのどちらを利用するか画面で選択できるようにする。
2	利用しない	既存の災害時向けシステムを利用する。	・システム側でその利用時が”災害時” か”平常時” かは判別できないため、利用者が”災害時”に利用することに対してシステム側が対応する必要がある。 ・そのため災害時の利用が既に浸透している既存のシステム等を活用することも考慮する必要がある。	-

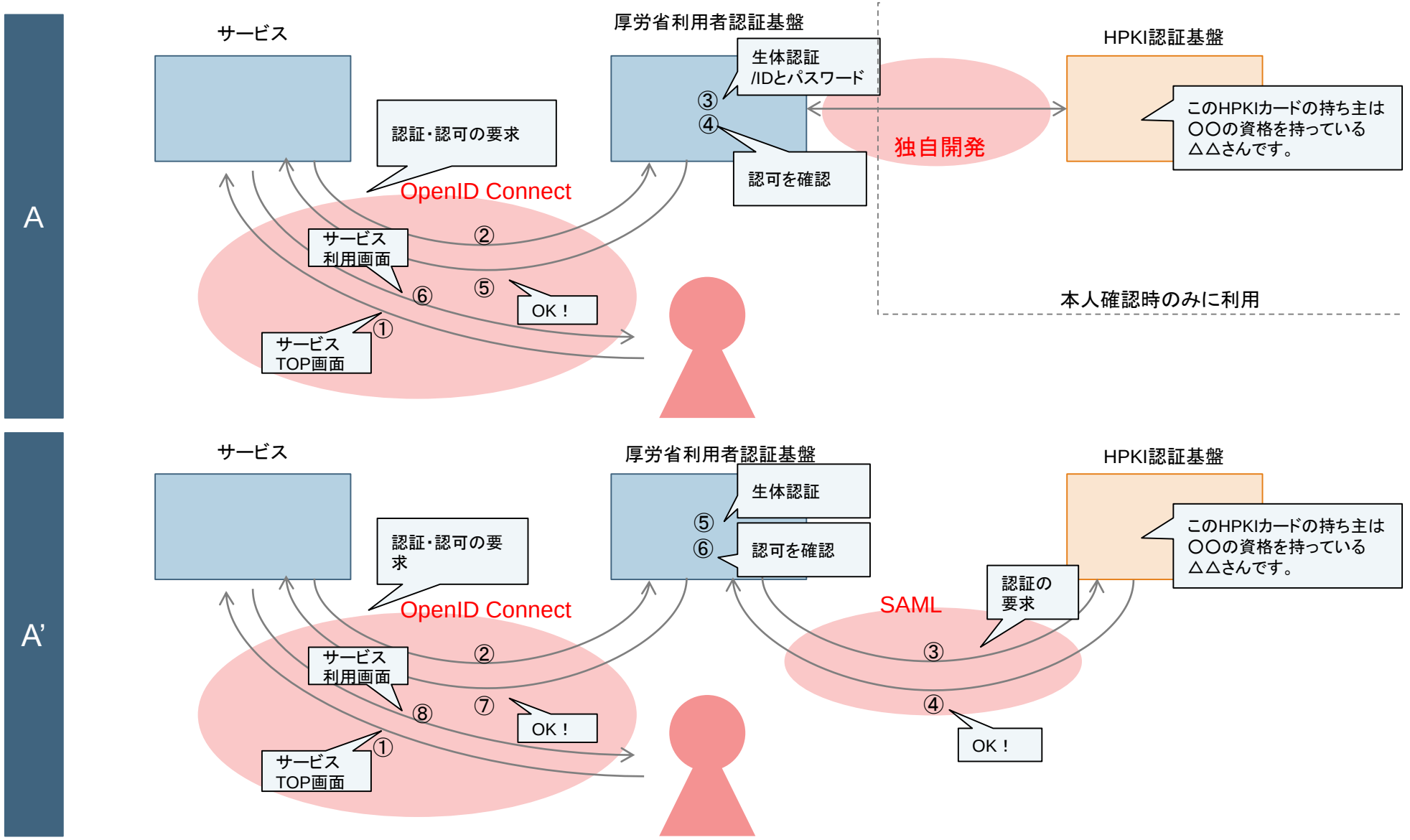
NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

HPKIカードを使った本人確認と認証に関する考え方

- 前述のグループAのうち、医療従事者においては資格の確認が必要であり、資格の確認にはHPKI認証基盤への問い合わせが必要となる。この際、HPKI認証基盤と利用者認証基盤の機能のすみわけを整理する必要がある。
- 本研究では、前述のグループAは資格・本人確認のみをHPKI認証基盤で管轄することとしたが、それに対し、資格・本人確認と認証にHPKI認証基盤を用いる案を新たにグループA'とした。
- グループAのように、利用者認証基盤側で認証を行う場合には、ID登録時において既存のHPKI認証基盤側へHPKIカードをもとに所有資格と本人確認を行うための新規IFが必要となる。認証自体は利用者認証基盤側で行うために、所有資格と本人性を書面等で確認済であれば（5.(2) D参照）、HPKI非保持者であってもサービス利用可能である。
- グループA'のように、HPKI認証基盤を認証基盤としても利用する場合には、利用の度に資格確認を行うことになるため、厳密な認証が可能となる点でグループAと比べ、優れた選択肢なり得る。ただし、サービス利用のために、HPKIの保有が必須となるため、医療従事者への広い普及が課題となる。また技術面では、HPKIアプリケーション利用時の適切な認可を利用者認証基盤側で設定する前提であることから、HPKI認証基盤側での認証結果を利用者認証基盤側で受け取る仕組みが必要となる。

No.	必要なプロセスの管轄			補足	実現するためのシステムに関する追加イメージ	課題
	資格・本人確認	認証	認可			
A	HPKI認証基盤	利用者認証基盤	利用者認証基盤	・前項までで検討した認証方式を利用する ・認証にHPKIカードを用いず、利用者認証基盤側で保持するID/パスワードを用いる ・HPKIカード非保持の医療従事者であっても、利用者認証基盤の利用が可能（所有資格と本人性を書面等で確認した場合）	・HPKI認証基盤側で、サーバ間通信による資格及び本人確認のための新規IFが必要。	・HPKI認証基盤側への新規IF追加に関する実現性 ・
A'	HPKI認証基盤	HPKI認証基盤	利用者認証基盤	・前項までで検討した認証方式ではなく、HPKI認証基盤側の認証方式を利用する。 ・認証にHPKIカードとカードリーダーが必須となる。	・HPKI認証基盤側から利用者認証基盤へのつなぎ込みが必要 ・HPKI認証基盤側と利用者認証基盤側とで、ある利用者の認証・認可の状態を同期させる仕組みが必要	・ヒアリングなどであがっていた既存の問題（HPKIカードの普及率・性能懸念・高利用費）への対処が必要 ・救急隊員利用への普及

HPKIを用いた本人確認と認証に関する考え方



Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

HPKIを認証にも用いる場合（前項A’案）の各種認証基盤の処理イメージ

- ①保健医療記録共有サービス、②救急時医療情報共有について、前項で示したグループA’の処理イメージを以下に示す。
- HPKIカードが発行済であることを前提とするため、新たなID登録の処理は不要とした。
- 今回は資格認証を重視し、救急隊員向けについてもHPKI利用を想定したが、前述のインタビュー結果によると、救急の現場では装備が多く、なるべく持ち物が増えない認証方式が望ましいというニーズがあった。よって、業務用タブレット端末で外付けのカードリーダ等を使ったHPKIカード利用が救急の現場に許容できるか否かは今後引き続き検討が必要と考えられる。
- 認証方式としては、グループA’では利用のたびに資格認証を行いかつPIN認証も含めると実質3要素認証と捉えることができ、グループAに比べ、より強度の高い認証となる。

青枠個所：認証の要素　緑箇所：A案との違い

処理順	処理イメージ	ログイン	利用者（名称を一部略）					処理の主体			
			医療従事者	救急隊員	介護従事者	患者（本人）	家族代理人	各サービス	利用者認証基盤	HPKI認証基盤	他システム
1	利用端末へログイン		↓ 1								●
2	サービスTOP画面返却		↓	↓				●			
3	利用者認証基盤へリダイレクト		↓	↓				●			
4	クライアント証明書の確認		↓	↓ 1					●		
5	HPKI認証基盤へリダイレクト		↓	↓					●		
6	ログイン画面返却		↓	↓						●	
7	ログイン PINの照合		↓ 2	↓ 2						●	
	ICチップの情報の検証		↓ 3	↓ 3						●	
8	認証結果をつけて利用者認証基盤へリダイレクト		↓	↓						●	
	ユーザの属性情報の要求		↓	↓	Aに同じのため割愛				●		
	ユーザの属性情報の返却		↓	↓						●	
9	同意画面返却		↓	↓					●		
10	同意		↓	↓					●		
11	サービスへリダイレクト		↓	↓					●		
12	ユーザの認証・認可の結果の検証		↓	↓				●			
13	ユーザの属性情報取得の要求		↓	↓				●			
14	ユーザの属性情報の返却		↓	↓					●		
15	サービス利用可否の判定		↓	↓				●			
16	利用者向けサービスの画面返却		↓	↓				●			

⑥がんゲノム医療サービスの認証基盤の処理イメージ

- ⑥がんゲノム医療サービスの利用者は、以下の流れで認証基盤を利用する。
- 今後のサービス内容の検討により、フェデレーション先となるサービスが将来的に増えないことが想定される場合には、利用サービス側において認証機能を実装する等の案も考えられる。

青字個所：認証の要素数

処理順	処理イメージ		ID登録	ログイン	利用者（名称を一部略）	処理の主体		
						サービス	認証基盤	他システム
1	利用端末へログイン				↓ 1			●
2	利用端末のVPN接続				↓			●
3	サービスTOP画面返却				↓	●		
4	認証基盤へリダイレクト				↓	●		
5	ログイン画面返却				↓		●	
6	新規登録画面へ遷移				↓		●	
7	ID登録				↓		●	
8	ID登録完了画面返却				↓		●	
9	ログイン画面へ遷移				↓		●	
10	ログイン	パスワードの照合			↓ 2		●	
		生体認証結果の検証			↓ 3(任意)			
11	同意画面返却				↓		●	
12	同意				↓		●	
13	サービスへリダイレクト				↓		●	
14	ユーザの認証・認可の結果の検証				↓	●		
15	ユーザの属性情報取得の要求				↓	●		
16	ユーザの属性情報の返却				↓		●	
17	サービス利用可否の判定				↓	●		
18	利用者向けサービスの画面返却				↓	●		

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑥がんゲノム医療サービスの認証基盤によるID連携のイメージ

■ 現状は連携が必要なサービスは想定されていないが、今後のサービス追加を想定して認証基盤を構築する場合には、⑥がんゲノム医療サービス向けに、以下の属性情報を認証基盤より連携することが考えられる。

利用サービス	属性情報	利用者（名称を一部略）と、必要なデータ内容の紐付け
⑥がんゲノム医療サービス	・ログインID	●
	・組織ID	●
	・氏名	●

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑥がんゲノム医療サービスの認証基盤によるSSOのイメージ

- 1.ユースケースの詳細化とモデル化での検討内容を踏まえ、利用者ごとにSSO可能となるサービスを整理した。ただし、現状は、連携が必要なサービスは想定されていない。

利用サービス	利用者（名称を一部略）
⑥がんゲノム医療サービス	●

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑦保健医療分野AI（画像診断）の認証基盤の利用イメージ

- ⑦保健医療分野AI（画像診断）は、以下の流れで認証基盤を利用する。
- 今後のサービス内容の検討により、フェデレーション先となるサービスが将来的に増えないことが想定される場合には、利用サービス側において認証機能を実装する等の案も考えられる。

青字個所：認証の要素数

処理順	処理イメージ		ID登録	ログイン	AI開発者	処理の主体		
						各サービス	認証基盤	他システム
1	サービスTOP画面返却				↓	●		
2	認証基盤へリダイレクト				↓	●		
3	ログイン画面返却				↓		●	
4	新規登録画面へ遷移				↓		●	
5	ID登録				↓		●	
6	ID登録完了画面返却				↓		●	
7	ログイン画面へ遷移				↓		●	
8	ログイン	パスワードの照合			↓1		●	
		生体認証結果の検証			↓2(任意)			
9	同意画面返却				↓		●	
10	同意				↓		●	
11	サービスへリダイレクト				↓		●	
12	ユーザの認証・認可の結果の検証				↓	●		
13	ユーザの属性情報取得の要求				↓	●		
14	ユーザの属性情報の返却				↓		●	
15	サービス利用可否の判定				↓	●		
16	利用者向けサービスの画面返却				↓	●		

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑦保健医療分野AI（画像診断）の認証基盤によるID連携のイメージ

■ 現状は連携が必要なサービスは想定されていないが、今後のサービス追加を想定して認証基盤を構築する場合には、⑦保健医療分野AI（画像診断）向けに、以下の属性情報を認証基盤より連携する。

利用サービス	属性情報	AI開発者と、必要なデータ内容の紐付け
⑦保健医療分野AI（画像診断）	・ログインID	●
	・組織ID	●
	・氏名	●

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑦保健医療分野AI（画像診断）の認証基盤によるSSOのイメージ

- 1.ユースケースの詳細化とモデル化での検討内容を踏まえ、利用者ごとにSSO可能となるサービスを整理した。ただし、現状は、連携が必要なサービスは想定されていない。

利用サービス	AI開発者
⑦保健医療分野AI（画像診断）	●

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証基盤の認証方式案の検討を実現する製品組み合わせ例について、想定される機能要求、非機能要求の机上評価を実施した

- 機能要求の評価
  - 認証基盤に求められる機能（認証機能、ユーザ登録機能など）を整理し、製品機能で実現可能であること（または個別開発が必要となること）を確認した。

- 非機能要求の評価
  - 非機能要求については、「非機能要求グレード2018」の項目を評価軸とし、認証方式案の検討において対応困難な要求の有無を整理した。
  - 評価基準とする要求レベルは、非機能要求グレード内で参照例として示されている要求レベルとした。
    各フェデレーショングループのシステム分類は、「社会的影響が極めて大きいシステム」とした。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

機能要求の評価項目は、認証およびID管理システムに一般に求められる機能とした

■ 機能要求の項目サマリ

項目	説明	要求の例
認証	IDとそれに紐づくユーザの正当性を確認するための要求	・パスワード認証 ・ICカード認証
ID連携	あるシステムにおけるIDを他システムに連携し、他システムでも活用するための要求	・OpenID Connect連携 ・シングルサインオン
ID管理	ユーザに紐づくID、クレデンシャル、属性といった情報の登録、参照、変更を行うための要求	・ユーザ新規登録 ・パスワード変更

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

機能要求の評価項目の詳細は以下の通りとした

項番	大項目	小項目	メトリクス（要求指標）
1	認証	記憶認証	ID/パスワード認証
2		所有物認証	クライアント証明書認証
3			ICカード認証
4			ワンタイムパスワード認証
5			経路外認証
6		生体認証	指紋認証
7			静脈認証
8			顔認証
9			虹彩認証
10		その他認証機能	多要素認証制御
11			ログアウト
12	ID連携	ID連携	OpenID Connect連携
13			OpenID Connect Userinfo API
14			SAML連携
15			外部IDP認証連携
16			シングルサインオン
17	ID管理	ID管理	ユーザ新規登録
18			ユーザ情報参照
19			ユーザ情報更新
20			クレデンシャル変更
21			ユーザ削除
22			ユーザ退会

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

非機能要求の評価項目は、「非機能要求グレード2018」であげられている重要項目を対象とした

- 非機能要求グレードとは
  - 「非機能要求グレード」は、「非機能要求」についてのユーザと開発者との認識の行き違いや、互いの意図とは異なる理解を防止することを目的とし、非機能要求項目を網羅的にリストアップして分類するとともに、それぞれの要求レベルを段階的に示したもの。

    (※)IPAサイト(https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html)より引用
- 非機能要求の項目サマリ

項目	説明	要求の例
可用性	システムサービスを継続的に利用可能とするための要求	・運用スケジュール ・障害、災害時における稼働目標
性能・拡張性	システムの性能、および将来のシステム拡張に関する要求	・業務量および今後の増加見積り ・システム化対象業務の特性（ピーク時、通常時、縮退時など）
運用・保守性	システムの運用と保守のサービスに関する要求	・運用中に求められるシステム稼働レベル ・問題発生時の対応レベル
移行性	現行システム資産の移行に関する要求	・新システムへの移行期間および移行方法 ・移行対象資産の種類および移行量
セキュリティ	情報システムの安全性の確保に関する要求	・利用制限 ・不正アクセスの防止
システム環境・エコロジー	システムの設置環境やエコロジーに関する要求	・耐震/免震、重量/空間、温度/湿度、騒音などシステム環境に関する事項 ・CO2排出量や消費エネルギーなど、エコロジーに関する事項

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

非機能要求の評価項目の詳細は以下の通りとした（１/３）

項番	大項目	小項目	メトリクス（要求指標）
A.1.1.1	可用性	運用スケジュール	運用時間（通常）
A.1.1.2			運用時間（特定日）
A.1.1.3			計画停止の有無
A.1.2.1		業務継続性	対象業務範囲
A.1.2.2			サービス切替時間
A.1.2.3			業務継続の要求度
A.1.3.1		目標復旧水準 （業務停止時）	RPO（目標復旧地点）
A.1.3.2			RTO（目標復旧時間）
A.1.3.3			RLO（目標復旧レベル）
A.1.4.1		目標復旧水準 （大規模災害時）	システム再開目標
A.1.5.1		稼働率	稼働率
A.4.2.1		可用性確認	確認範囲
B.1.1.1	性能・拡張性	通常時の業務量	ユーザ数
B.1.1.2			同時アクセス数
B.1.1.3			データ量
B.1.1.4			オンラインリクエスト件数
B.1.1.5			バッチ処理件数
B.1.2.1		業務量増大度	ユーザ数増大率
B.1.2.2			同時アクセス数増大率
B.1.2.3			データ量増大率
B.1.2.4			オンラインリクエスト件数増大率
B.1.2.5			バッチ処理件数増大率
B.1.3.1		保管期間	保管期間
B.2.1.1		オンラインレスポンス	通常時レスポンス順守率
B.2.1.2			ピーク時レスポンス順守率
B.2.2.1		バッチレスポンス（ターンアラウンドタイム）	通常時レスポンス順守度合い
B.2.2.2			ピーク時レスポンス順守度合い
B.3.1.1		CPU拡張性	CPU利用率
B.3.1.2			CPU拡張性
B.3.2.1		メモリ拡張性	メモリ利用率
B.3.2.2			メモリ拡張性

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

非機能要求の評価項目の詳細は以下の通りとした（２/３）

項番	大項目	小項目	メトリクス（要求指標）
C.1.1.1	運用・保守性	運用時間	運用時間（通常）
C.1.1.2			運用時間（特定日）
C.1.2.2			外部データの利用可否
C.1.2.3			バックアップ利用範囲
C.1.2.4			バックアップ自動化の範囲
C.1.2.5			バックアップ取得間隔
C.1.2.6			バックアップ保存期間
C.1.3.1		運用監視	監視情報
C.1.3.2			監視間隔
C.2.1.1		計画停止	計画停止の有無
C.2.2.1		運用負荷削減	保守作業自動化の範囲
C.4.1.1		開発用環境の設置	開発用環境の設置有無
C.4.2.1		試験用環境の設置	試験用環境の設置有無
C.4.3.1		マニュアル準備レベル	マニュアル準備レベル
C.4.4.1		リモートオペレーション	リモート監視地点
C.4.4.2			リモート操作の範囲
C.4.5.1		外部システム接続	外部システムとの接続有無
C.5.1.1		保守契約（ハードウェア）	保守契約（ハードウェア）の範囲
C.5.2.1		保守契約（ソフトウェア）	保守契約（ソフトウェア）の範囲
C.5.3.1		ライフサイクル期間	ライフサイクル期間
C.6.1.1		内部統制対応	内部統制対応の実施有無
C.6.2.1		サービスデスク	サービスデスクの設置有無
D.1.1.1	移行性	移行のスケジュール	システム移行期間
D.1.1.2			システム停止可能日時
D.1.1.3			並行稼働の有無
D.2.1.1		システム展開方式	拠点展開ステップ数
D.2.1.2			業務展開ステップ数
D.3.1.1		移行設備	設備・機器の移行内容
D.4.1.1		移行データ量	移行データ量
D.4.1.2			移行データ形式

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

非機能要求の評価項目の詳細は以下の通りとした（３/３）

項番	大項目	小項目	メトリクス（要求指標）
E.1.1.1	セキュリティ	情報セキュリティに関するコンプライアンス	順守すべき社内規程、ルール、法令、ガイドライン等の有無
E.2.1.1		セキュリティリスク分析	リスク分析範囲
E.3.1.1		セキュリティ診断	ネットワーク診断実施の有無
E.3.1.2			Web診断実施の有無
E.5.1.1		認証機能	管理権限を持つ主体の認証
E.5.2.1		利用制限	システム上の対策における操作制限度
E.6.1.1		データ暗号化	伝送データの暗号化の有無
E.6.1.2			蓄積データの暗号化の有無
E.7.1.1		不正監視	ログの取得
E.7.1.2			ログ保管期間
E.7.1.3			不正監視対象（装置）
E.7.1.4			不正監視対象（ネットワーク）
E.7.1.5			不正監視対象（侵入者・不正操作等）
E.8.1.1		ネットワーク制御	通信制御
E.8.2.1		不正検知	不正通信の検知範囲
E.8.3.1		サービス停止攻撃の回避	ネットワークの輻輳対策
E.9.1.1		マルウェア対策	マルウェア対策実施範囲
E.10.1.1		Web実装対策	セキュアコーディング、Webサーバの設定等による対策の強化
E.10.1.2			WAFの導入の有無
F.1.1.1	システム環境・エコロジー	構築時の制約条件	構築時の制約条件
F.1.2.1		運用時の制約条件	運用時の制約条件
F.2.1.1		ユーザ数	ユーザ数
F.2.2.1		クライアント数	クライアント数
F.2.3.1		拠点数	拠点数
F.2.4.1		地域的広がり	地域的広がり
F.2.5.1		特定製品指定	特定製品の採用有無
F.3.1.1		製品安全規格	規格取得の有無
F.3.2.1		環境保護	規格取得の有無
F.4.1.1		耐震/免震	耐震震度
F.4.2.1		スペース	設置スペース制限(マシンルーム)
F.4.2.2			設置スペース制限(事務所設置)

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

フェデレーションのグループ毎の製品例

- ②フェデレーション及び処理イメージで示した内容をもとに、それを実現するための認証基盤側の製品例を、4.(1)の調査結果をもとにまとめた。
- 構成例は、それぞれのコンポーネント例や一般的な範囲で推測できる場合に参考として併記した。
- 機能例へは認証方式のうちのアプリケーション側の関係部分（内部的なものを除く）のみを記載した。アプリケーションへのWebアクセスまでの関係部分は対象外とした。

- 製品構成例の考え方
  - 製品は、デスクトップ調査およびベンダーヒアリングから得られた製品から選定した。
  - 認証基盤で備えるべき機能は、可能な限り製品として備える機能を利用して実現する。機能例としては、以下の通りとした。
    （製品機能の活用により、個別の作り込みを極力削減し、構築コストの削減を図る。）
    - ID/パスワード認証
    - 生体認証（FIDO+FIDO対応認証器によるものを含む）
    - OpenID Connect対応
    - SAML対応
  - 認証基盤に必要な認証方式がID/パスワード認証に限られる場合は、個別開発による対応も検討することとした。

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

フェデレーションのグループ毎の製品例

赤字：利用者認証基盤側で独自の作り込みが必要となる可能性が高い機能

グループ	共通の機能例 認証方式の関係部分のみ	個別に必要な機能例 認証方式の関係部分のみ	製品構成例
A	【フロント】 ID登録・管理 同意管理 パスワード認証 生体認証 【管理者】 ID登録・管理 サービス管理 利用量確認 認証ポリシーの管理 【DB】 （割愛）	【フロント】 外結先HPKI利用による資格確認 または外結先HPKI認証基盤側での認証結果の受け入れ 外結先JPKI利用による本人確認 フェデレーション SSO スマホアプリ対応	【要件】 OpenID Connectに対応可能であること。 SAML対応が可能であること。(HPKI接続) FIDO対応が可能であること。 ・Icewall SSO + Icewall MFA ・Uni-ID Libra
A’		【フロント】 外結先HPKI認証基盤との連携（SAML） 外結先JPKI利用による本人確認 フェデレーション SSO スマホアプリ対応	Aと同じ
B		【フロント】 ID登録時の組織IDの確認	・製品利用なし（サービスの１機能としてID/パスワード認証機能を実装） ・Aの製品例のいずれか
C		【フロント】 ID登録時の組織IDの確認 生体認証のオプション利用	Aと同じ

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

SAML連携やHPKI/JPKI連携には個別開発が必要となる。非機能要求実現に向けては、特段の制約はない見込み

- 製品構成に関する前提事項
  - 認証基盤製品としてUni-ID Libraを利用し、Webアプリケーションで機能を実現することを前提とする。
- 評価サマリ（詳細は参考資料参照）

項目		評価	説明
機能	認証	△	製品機能でID/パスワード認証、FIDO利用の生体認証に対応可能。クライアント証明書による認証、HPKI連携、JPKI連携は個別開発（カスタマイズ）が必要。
	ID連携	△	SAML連携機能については、個別開発が必要。
	ID管理	○	製品標準機能で、ID登録、属性参照、ID削除が可能。
非機能	可用性	○	適切な基盤構成を取ることにより、各要求とも実現可能と想定される。
	性能・拡張性	○	適切なサイジングを行うことにより、各要求とも実現可能と想定される。
	運用・保守性	○	適切な監視運用設計を行うことにより、各要求とも実現可能と想定される。 製品ライフサイクルについては調整が必要となる可能性あり。
	移行性	○	新規システムであり、机上では移行（リリース）に関し大きな課題は想定されない。
	セキュリティ	○	NIST 800-63-3の要件を満たす形での構成が可能。基盤機能やWebアプリケーションファイアウォールなどの他製品も組み合わせて実現される想定。
	システム環境・エコロジー	○	各種ガイドラインを確認したうえでの構成であり、各要求とも実現可能と想定される。

（凡例）○：実現可能に向けて特段の課題が見受けられない
△：実現可能であるが、軽微な課題がある
－：評価の対象外

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

HPKI/JPKI連携には個別開発が必要。利用者向けID管理機能は要否含めて今後要検討。非機能要求実現に向けては、特段の制約はない見込み

- 製品構成に関する前提事項
  - 認証基盤製品としてUni-ID Libraを利用し、Webアプリケーションで機能を実現することを前提とする。
- 評価サマリ（詳細は参考資料参照）

項目		評価	説明
機能	認証	△	製品機能でID/パスワード認証、FIDO利用の生体認証に対応可能。クライアント証明書による認証、HPKI連携、JPKI連携は個別開発（カスタマイズ）が必要。
	ID連携	△	OpenID Connect連携については、個別開発が必要な可能性あり。
	ID管理	△	利用者によるID登録、属性参照、ID削除機能は、製品標準機能としては備えていない。
非機能	可用性	○	適切な基盤構成を取ることにより、各要求とも実現可能と想定される。
	性能・拡張性	○	適切なサイジングを行うことにより、各要求とも実現可能と想定される。
	運用・保守性	○	適切な監視運用設計を行うことにより、各要求とも実現可能と想定される。 製品ライフサイクルについては調整が必要となる可能性あり。
	移行性	○	新規システムであり、机上では移行（リリース）に関し大きな課題は想定されない。
	セキュリティ	○	NIST 800-63-3の要件を満たす形での構成が可能。基盤機能やWebアプリケーションファイアウォールなどの他製品も組み合わせて実現される想定。
	システム環境・エコロジー	○	各種ガイドラインを確認したうえでの構成であり、各要求とも実現可能と想定される。

（凡例） ○：実現可能に向けて特段の課題が見受けられない
△：実現可能であるが、軽微な課題がある
－：評価の対象外

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

がんゲノム医療においては、Web3層構造のアプリケーション実装を行うことで、各要求は実現可能と想定される

- 製品構成に関する前提事項
  - 製品利用は行わず、Web3層構造によるWebアプリケーションで機能を実現することを前提とする。
- 評価サマリ（詳細は参考資料参照）

項目		評価	説明
機能	認証	△	パスワード認証画面をアプリケーションとして実装する必要がある。
	ID連携	-	ID連携の要求がないため、評価対象外とする。
	ID管理	△	ID登録画面やパスワード変更画面をアプリケーションとして実装する必要がある。
非機能	可用性	○	適切な基盤構成を取ることにより、各要求とも実現可能と想定される。
	性能・拡張性	○	適切なサイジングを行うことにより、各要求とも実現可能と想定される。
	運用・保守性	○	適切な監視運用設計を行うことにより、各要求とも実現可能と想定される。
	移行性	○	新規システムであり、机上では移行（リリース）に関し大きな課題は想定されない。
	セキュリティ	○	閉域網での運用であり、ネットワーク経由での攻撃リスクは低いため、各要求の実現はインターネット向けシステムと比較して容易。
	システム環境・エコロジー	○	各種ガイドラインを確認したうえでの構成であり、各要求とも実現可能と想定される。

（凡例） ○：実現可能に向けて大きな課題がない
△：実現可能であるが、軽微な課題がある
-：評価の対象外

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

⑦保健医療分野AI（画像診断）の製品評価は、グループAの製品評価内容に準じる

- 製品構成に関する前提事項
  - (グループA)参照
- 評価サマリ
  - (グループA)参照

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

最終報告　目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

認証基盤の検討材料として、記憶、所持、生体といった認証方式、HPKI等の既存インフラの活用などが挙げられる。また医療現場の業務負荷やコストに十分配慮する必要がある

■ 全国保健医療情報ネットワークの認証基盤の構想を描くため、本調査研究では以下の論点について検討した。

本研究で明らかにすべきこと	方法	分かったこと
国内外の動向踏まえ、どのような認証方式が利用可能か	• デスクトップ調査 • 海外インタビュー	• 現状では記憶、所持、生体の3点それぞれを用いた製品が利用可能。 • HPKIやマイナンバーカードなどが整備されており、それらも活用できる。 • 海外では、データ項目やセキュリティ、プライバシーなど個人でコントロールし、国や企業ではなく、個人が自身の情報に対してオーナーシップを発揮することが求められている。
医療介護現場へ広く普及するために認証技術に求められる要件は何か	• ベンダーインタビュー • 利用者インタビュー	• 医療介護現場への普及には、業務負荷やコストに十分に配慮した認証方式を用いる必要があり、パスワード認証が最も用いられている。 • ID管理は、医療施設の従業員マスタと連携して行われていることが多く、医療施設で管理できる体制が比較的整っている。 • 救急の現場では、特に迅速性が求められ、IDを隊で共有するなど簡便な認証が求められる。 • 災害の現場では、他県からの支援チームが素早く情報を確認できる工夫が必要となる。 • また災害時と平常時を区別するため、システムを分けておくことも検討する必要がある。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

医療情報やゲノム情報を扱う場合は2要素認証が必要となる。また、国民へ広く普及させる工夫として、マイナンバーカードやGoogle ID等外部IDの活用も検討すべき

■ 全国保健医療情報ネットワークの認証基盤の構想を描くため、本調査研究では以下の論点について検討した。

<table>
<tr><th>本研究で明らかにすべきこと</th><th>方法</th><th colspan="2">分かったこと</th></tr>
<tr><td>どのようなユースケースが考えられるか</td><td>・ユースケースの詳細化</td><td colspan="2">代表的なユースケースとして以下のような場合が想定された。
• 医療・介護従事者が、業務用端末から、患者の医療・介護情報を閲覧する。救急時は屋外からの利用が想定される（①保健医療記録共有、②救急時医療情報共有）。
• 国民が私用端末（スマホ、PC等）から自身の医療情報を閲覧、又は閲覧範囲の設定をする（①保健医療記録共有、②救急時医療情報共有、③PHR）。
• アカデミア、企業などの職員が研究を目的に、匿名化されたデータを閲覧、分析を行う（④データヘルス分析、⑤科学的介護、⑦保健医療分野AI）。
• アカデミアの研究者が、研究を目的に患者のゲノム情報にアクセスし、分析を行う。SSL-VPN利用などによる閉域のネットワークで利用される。ゲノム解析を行う場所は限定され入退室は厳格に管理される予定（⑥がんゲノム研究）。</td></tr>
<tr><td rowspan="2">想定されるユースケースでは、どのような要件が求められるか</td><td rowspan="2">• ユースケースの詳細化
• 各技術の評価</td><td>共通</td><td>医療情報やゲノム情報を扱う場合には、2要素認証が望ましい。</td></tr>
<tr><td>国民</td><td>• 国民が広く利用するため、大規模なID発行、管理が想定される。
• 私用端末による利用が想定されるため、個別端末の設定に依存せず、特別な外付けデバイスなどを要しない方式が望ましい。
• 普及度の向上やコスト軽減のため、マイナンバーカードの活用や指紋認証などスマホ搭載済の認証、Google ID等外部IDなどを活用も検討することが望ましい。</td></tr>
</table>

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

医療従事者では、資格認証を組み入れることが望ましい。また、利便性やコストの観点から施設への入退室時の認証などを認証要素に含めることも検討すべき

■ 全国保健医療情報ネットワークの認証基盤の構想を描くため、本調査研究では以下の論点について検討した。

本研究で明らかにすべきこと	方法	分かったこと	
想定されるユースケースでは、どのような要件が求められるか	• ユースケースの詳細化 • 各技術の評価	医療・介護従事者	• 適切な資格認証の導入が必要であり、HPKIの活用を検討すべき。 • HPKIの活用では、現状普及率が高くないこと等の課題を考慮する必要がある。 • HPKIのような認証システムのない介護従事者については、資格の確認が難しい。これにより所属する組織と本人確認をすることが望ましい。 • 緊急性の高い場面も多く、利用者のスピード感を損なわないことが必要である。 • ゴーグルやマスク、手袋などを装着しているケースも多く、生体認証を検討する場合は、指紋や静脈認証だけでなく、顔、虹彩など幅広く認証方式を考慮する必要がある。 • 医療現場では、入退室管理など既に用いられている認証方式が存在するため、利便性やコストの観点からはこれらを考慮することが望ましい。
		研究者	• 研究目的の場合は、緊急性や迅速性の重要性は低く、情報の機微度に応じた方式を選択することが望ましい。 • 情報の利用範囲はその研究目的の範囲に留めることが望ましく、研究組織ごとの登録制なども検討すべき。 • ④データヘルス分析、⑤科学的介護、⑦保健医療分野AIでは、匿名化情報を扱うため、認証強度の要求性は比較的低い。 • ⑥がんゲノム医療では、機微性の高いゲノム情報を扱うため、医療情報と同様に厳格な認証が必要となる。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

1要素認証では、パスワード認証が総合的に高い評価となった。2要素認証では、利用者の属性や使用する端末によって、望ましい組み合わせが異なる

■ 全国保健医療情報ネットワークの認証基盤の構想を描くため、本調査研究では以下の論点について検討した。

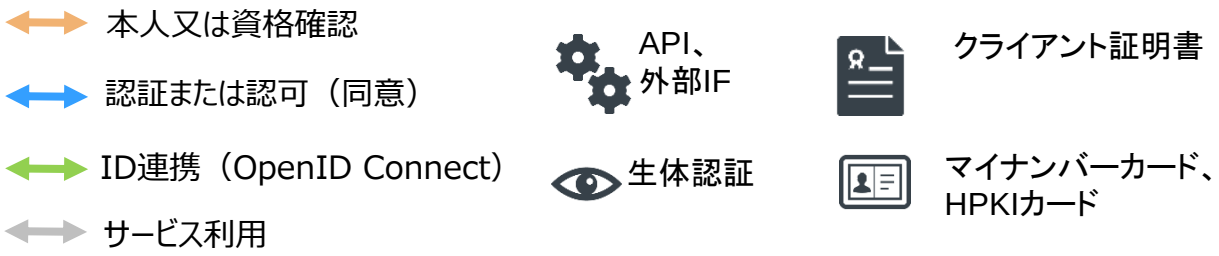
本研究で明らかにすべきこと	方法	分かったこと
各認証技術はどのようなユースケースに適しているか	• 各技術の評価	代表的な認証技術について、機能の信頼性、性能や負荷耐性、管理負荷の低減、緊急対応の実施、アフォーダンス、実績をスコア化し、評価した結果、以下のような特徴が明らかとなった。 • 1要素認証で用いる場合は、知識認証ではパスワード認証、所有物認証ではクライアント証明書、ICカード認証、生体認証では指紋認証が総合的に高い評価となり、全体ではパスワード認証が総合的に高い評価となった。 • 2要素認証で用いる場合、医療従事者等が業務用端末からアクセスするユースケースでは緊急対応の実施の観点から、クライアント証明書及び生体認証、パスワード認証及びクライアント証明書の組み合わせが高い評価となった。また、私用端末からアクセスするユースケースには、パスワード認証及び指紋認証、PIN認証及びICカード認証などが高い評価となった。
フェデレーション方式としてどのような選択肢があるか	• フェデレーション及び処理イメージの検討	• フェデレーション方式として、SAML2.0、OpenID2.0、OAuth2,0、及びOpenID Connectが想定される。 • ID連携とAPI連携（サービス側のスマホアプリ提供に必要）の双方を提供する手段として、OpenID Connectが最も優れている。
Google IDなどの外部IDやFIDOの活用可能性	• Google ID, Yahoo ID等の外部IDの活用と留意点 • FIDOの活用と留意点	• 外部IDは、国民の利用時において活用可能。外部IDの活用によって、利便性を高め、普及度が向上されることが期待できる。 • 現時点では普及度やコストの課題はあるものの、FIDOは利便性とセキュリティをともに高める認証技術として注目をあびており、中長期視点では活用を想定すべき技術と考えられる。

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

前述までの調査結果を踏まえ、全国保健医療情報ネットワークに望ましい認証基盤の構成について提言する

- 本調査結果を踏まえ、全国保健医療情報ネットワークに望ましい認証基盤の構成を以降に示す。
  - Webアクセスおよびサーバ間通信について、本人・資格確認、認証認可に関するものの概観を図示した。加えてフェデレーションの標準技術により対応可能な範囲と、独自開発により対応可能なものを色分けした。
  - Webアクセスおよびサーバ間通信は概念を示すものであり、実際のリダイレクトを含めたシーケンスの概観とは必ずしも一致しない。シーケンスの概観については、別頁フェデレーション及び処理イメージに処理順を記載した。
  - サービス側で想定する構成については記載を簡略化しており、個別には別頁認証技術のサービスへの適応へ記載する。
  - 書面による本人確認並びに管理者によるID発行といったフェデレーションとは関係のない運用フローは記載しない。
  - ①保健医療記録共有、②救急時医療情報共有など医療従事者の認証が関わるサービスについては、ID登録のみにHPKIを活用する案とID登録と認証の双方にHPKIを用いる案を検討した。
  - なお、④科学的介護、及び⑤データヘルス分析については、公開情報や企画者へのヒアリングにて、利用者認証基盤の利用を予定していないと考えられたため、今回の検討の対象には含めないこととした。

- 表記のうちの一部の記号について、意味をまとめる。



Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

サービス①～③については、認証要素数は2が望ましい。また利用者によって認証方式を分けるべきと考える

参考とした主な事実・要件

1. 医療情報を扱う場合には、2要素認証が望ましい。

2. 医療介護現場への普及には、業務負荷やコストに十分に配慮した認証方式を用いる必要があり、パスワード認証が最も用いられている。
3. 利便性やコストの観点から、入退室管理など既に用いられている認証方式を2要素の内、1要素に考慮することが望ましい。
4. 1要素認証では、パスワード認証が総合的に高い評価となった。
5. 適切な資格認証のため、HPKIを活用すべきだが、現状普及率が高くないこと等の課題を考慮する必要がある。

6. 救急時は屋外からの利用が想定される。
7. 2要素認証の場合、医療従事者等が業務用端末からアクセスするユースケースでは緊急対応の実施の観点から、クライアント証明書及び生体認証が最も高い評価となった。
8. FIDOは利便性とセキュリティをともに高める生体認証技術として注目をあびており、中長期視点で活用を想定すべき技術と考えられる。
9. 救急救命士はHPKIの対象資格であり、上記⑤は同様に当てはまる。

認証基盤の構成に関する提言

認証要素数		2	
認証方式	プロセス	ID登録	認証
	医療従事者	以下のいずれか ・HPKIカード ・顔写真付き身分証及び資格を示す情報	[HPKIを用いない場合]* ①施設管理下の認証(入館・端末等) ②パスワード認証
			[HPKIを用いる場合]* ①施設管理下の認証(入館・端末等) ②HPKIカード（PIN認証及びICカード認証）
	救急隊員	以下のいずれか ・HPKIカード ・顔写真付き身分証及び資格を示す情報	[HPKIを用いない場合] * ①クライアント証明書 ②生体認証(FIDO活用)
			[HPKIを用いる場合]* ①施設管理下の認証(端末等) ② HPKIカード（PIN認証及びICカード認証）

*HPKIカードの普及度が高くないことや利便性など考慮し、現状は認証にHPKIを用いない場合を推奨する。ただし、HPKIの将来の広い普及を想定し、HPKIを認証に用いる場合も合わせて記載した。

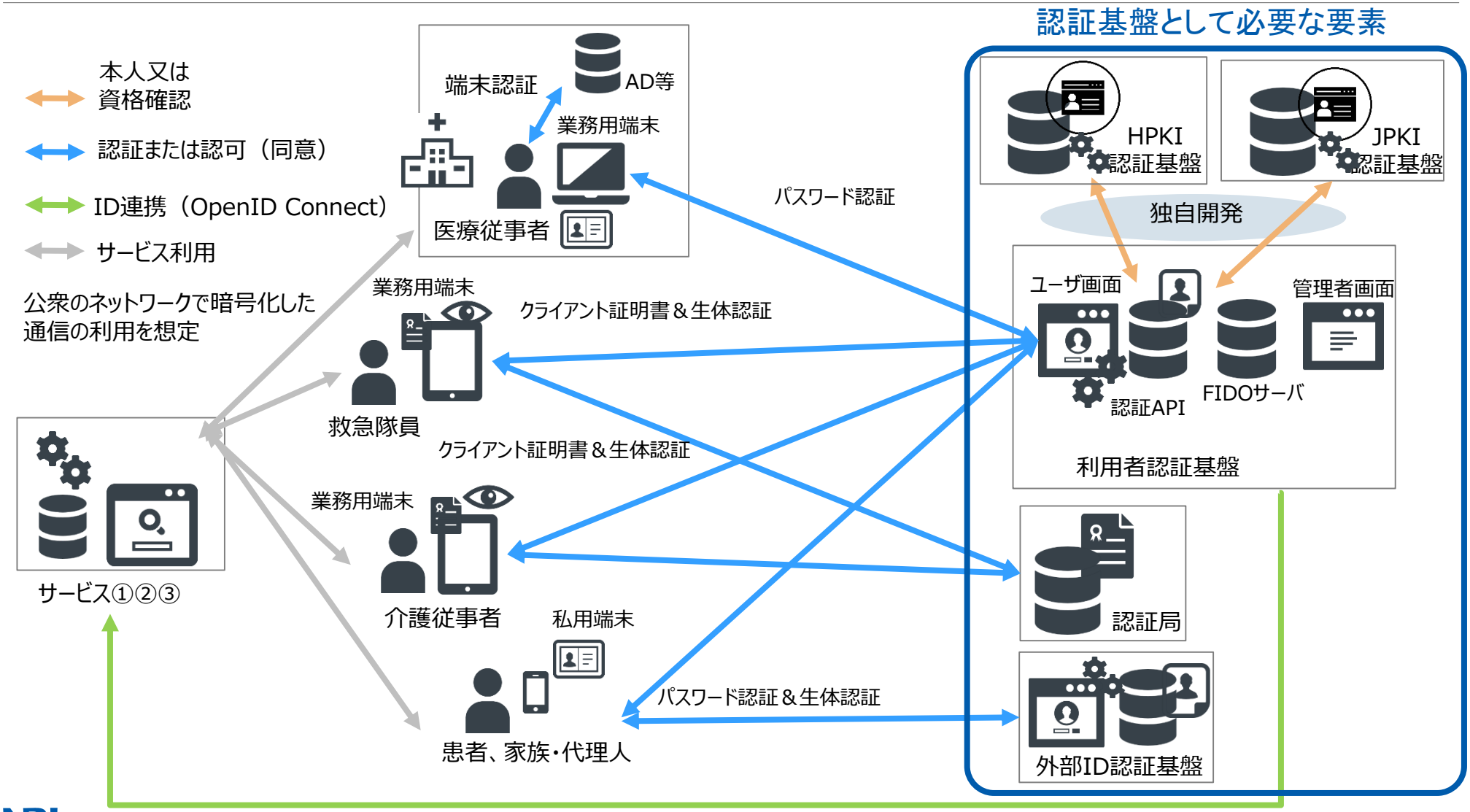
NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

患者・家族又は代理人については、普及度の向上やコスト軽減のため、生体（指紋）認証や外部IDの活用を検討すべきと考える

参考とした主な事実・要件	認証基盤の構成に関する提言			
		プロセス	ID登録	認証
10. HPKIのような資格認証システムのない介護従事者については、資格の確認が難しく、所属する組織と本人確認をすることが望ましい。 11. 2要素認証の場合、医療従事者等が業務用端末からアクセスするユースケースでは緊急対応の実施の観点から、クライアント証明書及び生体認証が最も高い評価となった。 12. FIDOは利便性とセキュリティをともに高める生体認証技術として注目をあびており、中長期視点で活用を想定すべき技術と考えられる。	認証方式	介護従事者	以下のいずれか ・組織ID及び公的個人認証 ・組織ID及び顔写真付き身分証	①クライアント証明書 ②生体認証(FIDO活用)
13. 私用端末による利用が想定される。 14. 2要素認証で私用端末からアクセスする場合では、パスワード認証及び指紋認証が総合的に最も高い評価となった。 15. 普及度の向上やコスト軽減のため、公的個人認証の活用や指紋認証などスマホ搭載済の認証、Google ID等外部IDなどを活用も検討することが望ましい。		患者・家族又は代理人	以下のいずれか ・公的個人認証 (家族・代理人は同意書) ・顔写真付き身分証 (家族・代理人は同意書)	①パスワード認証(外部ID活用) ②生体認証

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

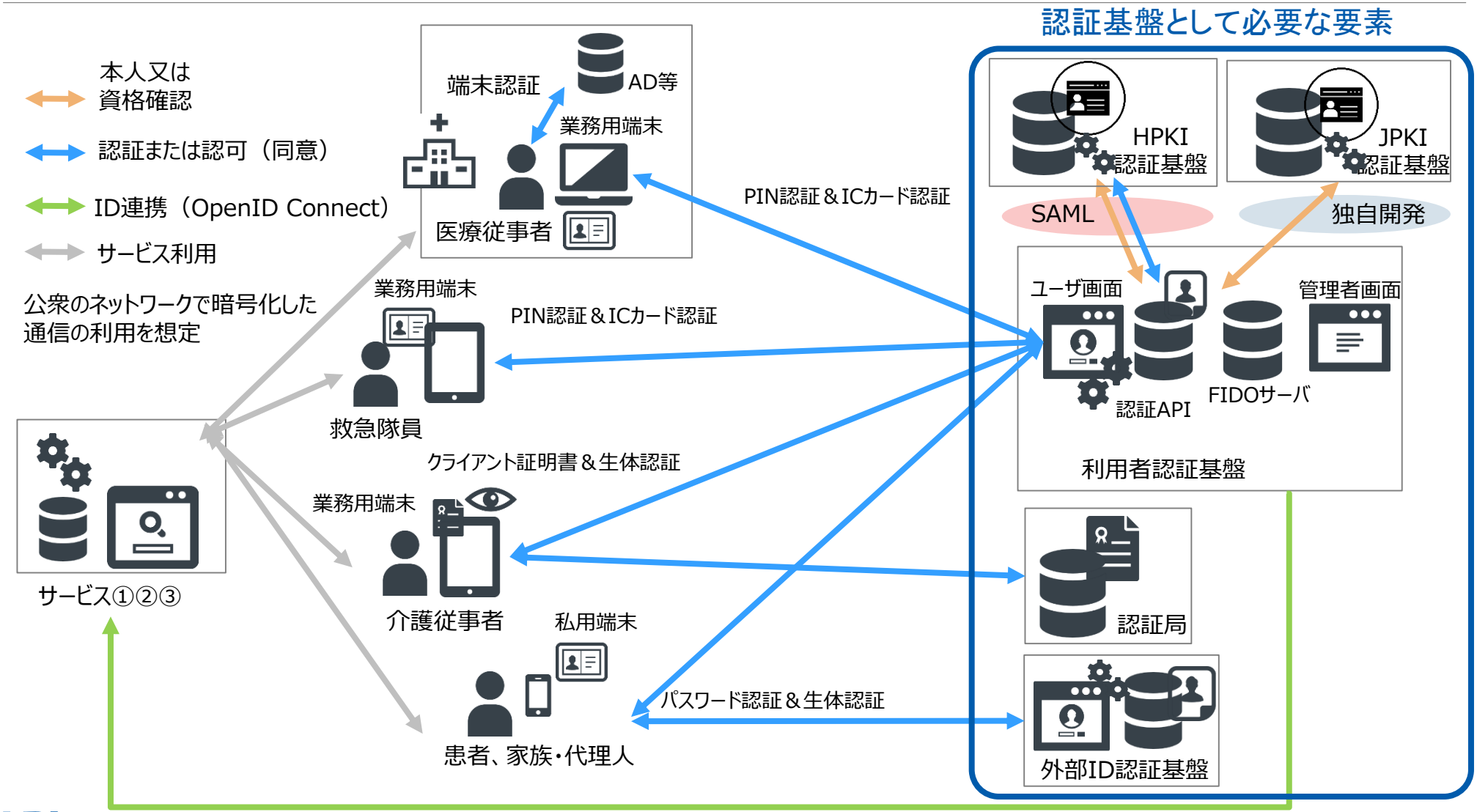
以上をまとめると、サービス①～③を提供するための認証基盤はHPKIやJPKI及び外部IDの認証基盤との連携やFIDOサーバといった機能を備える必要がある



NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

画面、API、サーバ等の構成は、その認証を行うために必要なものの一般的な概観を示した。

なお、HPKIを医療従事者のID登録と認証の双方に用いる場合は、SAMLを用いたHPKI認証基盤とのコミュニケーションが発生する



Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

画面、API、サーバ等の構成は、その認証を行うために必要なものの一般的な概観を示した。

サービス⑥については、情報の機微性の高さから認証要素数は2、利便性やコストの観点から施設管理下での認証とパスワード認証を用い、必要に応じて生体認証を検討すべき

参考とした主な事実・要件

1. ゲノム情報を扱う場合には、2要素認証が望ましい。

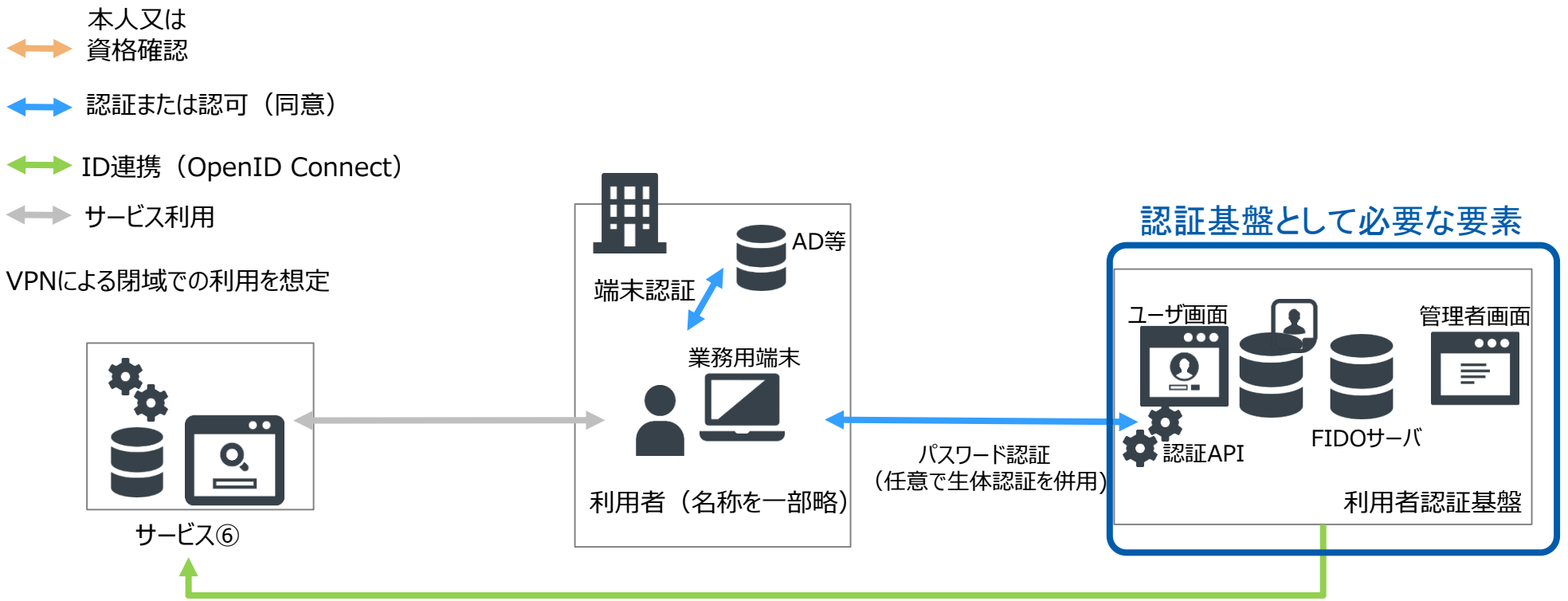
2. 情報の利用範囲はその研究目的の範囲に留めることが望ましく、研究組織ごとの登録制なども検討すべき。
3. SSL-VPN利用などによる閉域のネットワークで利用される。
4. ゲノム解析を行う場所は限定され入退室は厳格に管理される予定（施設入館の認証が導入されると想定）。
5. 利便性やコストの観点から、入退室管理など既に用いられている認証方式を2要素の内、1要素に考慮することが望ましい。
6. 1要素認証では、パスワード認証が総合的に高い評価となった。
7. 今後サービス仕様の変更により、認証要素を追加する場合は、本研究の技術評価より、生体認証(FIDO活用)が適している。

認証基盤の構成に関する提言

認証要素数		2	
認証方式	プロセス	ID登録	認証
	利用者	以下のいずれか ・組織ID	①施設管理下の認証(入館・端末等) ②パスワード認証 （③生体認証（必要な場合））

NRI Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

以上をまとめると、サービス⑥を提供するための認証基盤は認証APIに加え、FIDOサーバ等の機能を備える必要がある



Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

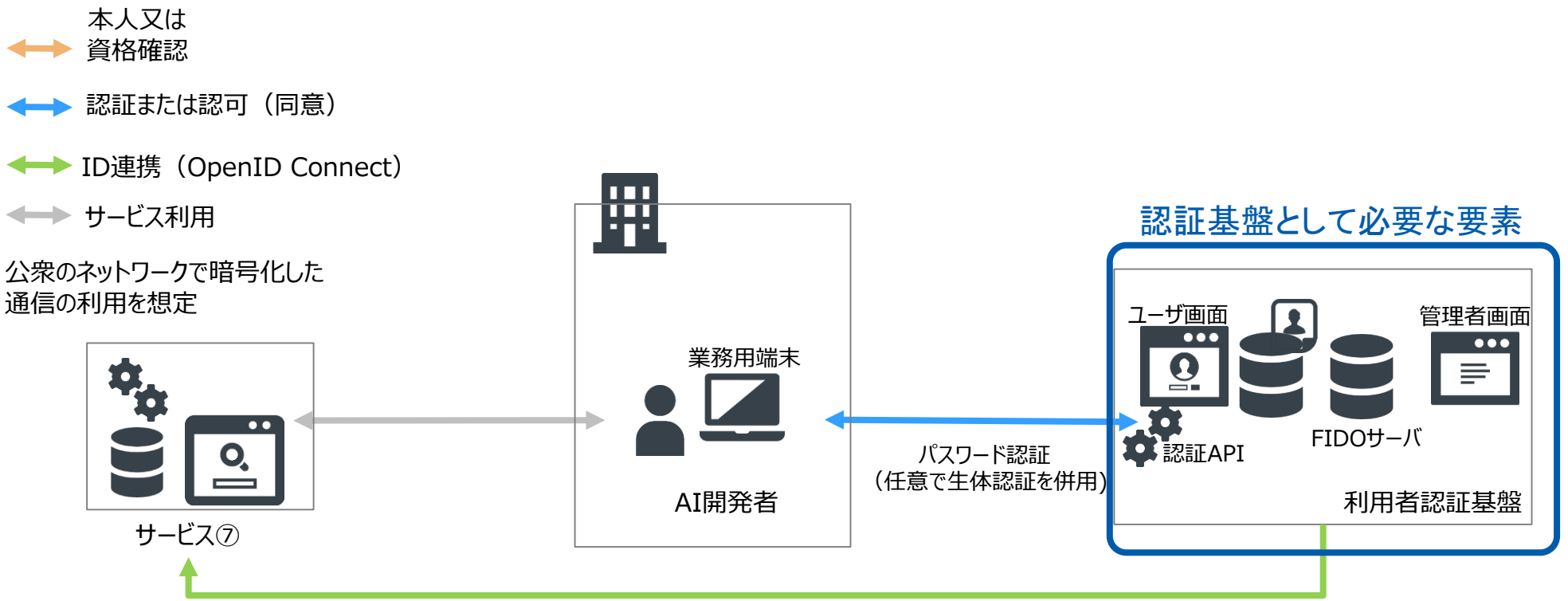
画面、API、サーバ等の構成は、その認証を行うために必要なものの一般的な概観を示した。

サービス⑦については、匿名化情報を扱うことから認証要素数は1、利便性やコストの観点からパスワード認証を用い、必要に応じて生体認証を検討すべき

参考とした主な事実・要件	認証基盤の構成に関する提言			
1. 匿名化情報が対象であり、扱う情報機微性は低い。	認証要素数		1	
2. 情報の利用範囲はその研究目的の範囲に留めることが望ましく、研究組織ごとの登録制なども検討すべき。 3. 1要素認証では、パスワード認証が総合的に高い評価となった。 4. 今後サービス仕様の変更により、認証要素を追加する場合は、本研究の技術評価より、生体認証(FIDOサーバ)の活用が適している。	認証方式	プロセス	ID登録	認証
		利用者	以下のいずれか ・組織ID	①パスワード認証 （②生体認証（必要な場合））

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

以上をまとめると、サービス⑦を提供するための認証基盤は認証APIに加え、FIDOサーバ等の機能を備える必要がある



Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

画面、API、サーバ等の構成は、その認証を行うために必要なものの一般的な概観を示した。

以上をまとめると、今回想定した①・②・③・⑥・⑦のサービスの提供に向け、認証基盤はFIDOサーバや認証局、他の認証基盤との連携など7つの機能を備える必要がある

- 全国保健医療情報ネットワークでは、提供されるサービスや利用者の属性、閲覧される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。
- それらすべての認証方式を提供するため、全国保健医療情報ネットワークの認証基盤は、以下の機能を備える必要がある。
  1. ユーザ/管理者画面
  2. 認証API
  3. FIDOサーバ
  4. 認証局
  5. HPKI認証基盤との連携機能
  6. JPKI認証基盤との連携機能
  7. 外部ID認証基盤との連携機能

Copyright（C） Nomura Research Institute, Ltd. All rights reserved.

HPKIやJPKIの認証基盤との連携機能について個別開発が必要。また、外部IDを適切に用いるため、セキュリティ上のリスクなどについて国民の理解を高めることが求められる

課題	内容	解決の方向性	主体	時期（優先度）
提供されるサービス内容の詳細化	本調査研究時点では、全国保健医療ネットワークのサービス内容が検討段階の部分が多く、今後の具体化に合わせて、認証方式も再考の余地がある。	• 各サービス企画者を含めた検討委員会を設定するなど、サービスの進捗状況に合わせた継続的検討が必要。	情報化担当参事官室	2018年度（高）
個別開発の検討	実効性の評価を行った結果、HPKIやJPKIとの連携などについて、個別開発が必要と考えられたため、これらの検討が求められる。	• 今後の実証研究において、HPKIやJPKIとの連携を踏まえた検討を行い、個別開発に必要な仕様の設計を行うこと必要がある。	情報化担当参事官室	2018年度（高）
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	本研究の認証方式では、国民の利用時には利便性の高い利用方法として、Google IDなどの外部IDの活用を挙げた。しかし、これは外部IDのセキュリティリスクを十分に理解し、国民自らが自身の責任において選択することが前提となる。このような国民自身によるセキュリティコントロールは海外では広まりつつある考え方であるものの、国内では浸透しているとは言いがたい。 また外部IDの活用を踏まえた仕様設計も必要となる。	• 今後の実証研究において、外部IDで認証することを検討する必要がある。	情報化担当参事官室	2018年度（高）
		• 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必要がある。 • 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	2020年度以降(中)

NRI Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

FIDOの活用に関する実証研究や導入時期の検討、公的個人認証のさらなる普及策の検討などが課題となる

課題	内容	解決の方向性	主体	時期（優先度）
FIDOの活用時期の検討	本研究の認証方式では、FIDOの活用を挙げた。しかし、FIDOサーバのコストは現状安価とは言いがたく、国内普及度の高いiOSやSafariブラウザなどの対応も不明である。よって、これらの市場価格や各社の動向を踏まえて導入時期を検討する必要がある。	• FIDOサーバの市場価格、FIDOの普及度を踏まえた導入可能範囲の検討が必要。 • FIDO活用、FIDOサーバの設置を踏まえた実証研究を行う必要がある。	情報化担当参事官室	2018年度（中）
公的個人認証の普及度の向上	国民に対し、広くID管理を行う基盤として、公的個人認証の活用は利便性、コストの観点から有用と考えるが、現状では、国民に広く普及しているとは言いがたい。	• 公的個人認証や全国保健医療情報ネットワークについて、国民にとってのメリットを整理し、公的個人認証への登録を継続的に訴える必要がある。 • 例えば、一定期間に、登録者への減税、医療費の控除などのインセンティブを設けるなど、医療従事者だけでなく、国民のメリットに訴えることが最も重要となる。	総務省	2020年度以降（中）

NRI Copyright（C）Nomura Research Institute, Ltd. All rights reserved.

医療従事者の資格認証のためには、HPKIの広い普及が鍵となる。HPKIが医師以外も含めた医療従事者へ広く普及させるための対策を検討する必要がある

課題	内容	解決の方向性	主体	時期（優先度）
HPKIの普及度の向上	資格認証の必要性を考慮すると、HPKIを活用した認証は必須と考えるが、現状では十分に普及しているとは言いがたく、普及度の向上が必要となる。本来、HPKIをID登録と認証の双方に活用し、利用の都度資格認証を行うことが認証強度の面から望ましい。しかし、本研究ではHPKIの普及度が低いこと等から、HPKIをID登録時のみに用いる案を推奨した。今後普及が進んだ場合、HPKIを認証に用いる案を選択可能となる。	• 日本医師会と協力し、普及に向けた対策の検討が必要。 • 全国保健医療ネットワークへのHPKI活用の重要性を考慮し、段階的に医療従事者のHPKI登録を必須としていくことも検討すべきと考える。	MEDIS 日本 医師会等	2020年度以降 （中）
がんゲノム医療データベースの認証方式の多様化	本研究では、がんゲノム情報を格納されるデータベースへのアクセスを想定して認証方式を検討したが、サービス企画者へのインタビューによると今後は、分析結果のみの閲覧など、情報の機微性の異なる複数の階層が形成される見込みとなっている。	• がんゲノム医療データベースの階層構造の検討進捗把握とそれらに合わせて認証方式の検討が必要。	C-CAT	サービスの進捗に応じて （低）

Copyright（C）Nomura Research Institute, Ltd. All rights reserved.


NRI
未来創発
Dream up the future.