オフライン資格確認用スマート医療端末及び
その実証環境の開発
仕様概要書

平成 29 年 8 月

一般財団法人　ニューメディア開発協会

１ 件名

オフライン資格確認用スマート医療端末及びその実証環境の開発に関わる請負

２ 背景・目的

政府では、マイナンバーの利用範囲の見直しや医療保険者の保険料徴収等の事務の共同委託等の内容を含む、番号法等の改正案と国民健康保険法等の改正案を平成27年通常国会に提出し、同国会で成立した。また、日本再興戦略改訂2015（平成27年6月閣議決定）では、次のことが示されている。

・公的個人認証やマイナンバーカードなどマイナンバー制度のインフラを活用して、医療等分野における番号制度を導入することとし、これを基盤として、医療等分野の情報連携を強力に推進する。具体的にはまず、2017年7月以降早期に医療保険のオンライン資格確認システムを整備し、医療機関の窓口においてマイナンバーカードを健康保険証として活用することを可能とし、医療等分野の情報連携の共通基盤を構築する。

・地域の医療情報連携や研究開発の促進、医療の質の向上に向け、医療等分野における番号の具体的制度設計や、固有の番号が付された個人情報取扱いルールについて検討を行い、本年末までに一定の結論を得て、2018年度からオンライン資格確認の基盤も活用して医療等分野における番号の段階的運用を開始し、2020年までに本格運用を目指す。

一方、保険医療機関等では、マイナンバーカードの顔写真と名前により本人確認を行い、同じマイナンバーカードの電子証明書を資格確認システムに送付し、資格情報を要求することが検討されている。

この処理はマイナンバーカードと資格確認システムの正当性を確認するためのものであるが、業務開始時間等、国内の保険医療機関に設置する資格確認端末が一斉に資格確認システムに接続する場合、ネットワークや資格確認システムへの影響が懸念される。

このように、何らかの理由で資格確認システムが一時的に使えない場合でも、ローカルの情報を利用し、資格確認システムの復帰まで暫定的な資格確認を行う方法を実証する。

以上のことを踏まえ、オフラインによる資格確認用医療端末及びその実証環境の開発を行う。

３ 事業の概要

個人生涯健康医療管理システム[1]の実現に向けた取り組みとして、オフライン資格確認用スマート医療端末（以下、スマート端末）及びこれを用いる実証環境の開発を行う。

また、開発した機器をネットワーク上で動作させ、医療保険の資格確認情報を活用するアプリケーションと組み合わせて実証を行う。

３．１ 前提条件

（１）開発の対象

本開発は、マイナンバーカードに搭載されるJPKIアプリケーションである特定機関認証を実行できるよう、スマート端末向けのオフライン機能を開発し、NFCインタフェースにより対応可能とするものである。

医療機関における保険資格確認や全国的な受診履歴管理サービスでの適用を意識したものであるが、保険資格確認PFあるいは受診履歴管理サービスはまだ確立されていないため、開発するスマート端末の開発実証環境として、外部のサーバ上に想定される保険資格確認PF機能及び受診履歴管理サービス機能の一部を模擬的に開発する。また、開発実証に使うマイナンバーカードは実際のものと同等なJPKI機能を備えた模擬カードを用意する。マイナンバーカードCAについても、公開鍵のペアとその証明書の発行を担う模擬機能を用意するが、ネットワーク接続による連携は行なわない。

これらの環境を前提に対応するスマート端末のアプリケーションとしては、保険資格確認をオンライン／オフラインで利用する機能、および資格確認の証跡を活用して受診履歴管理サービスに記録する機能を開発構成する。

また、オプションとして複数の科を持つ中・大病院を想定し、スマート端末と機能分担する院内中継サーバ方式も開発対象として考慮する。

（２）標準技術の採用

原則、OS、ミドルウェア、データベース、開発言語は一般的に広く使用されている標準技術を用いる。

（３）拡張性

アプリケーションフレームワークを採用する場合は、オープンソースソフトウェアを極力採用し、拡張・変更時の追加ライセンスを発生させないこと。

システムに変更を加える際の影響範囲を局所化できる構成を検討する。

３．２ 実証環境の構成

本実証において開発する基本的な実証システム構成イメージを、図３．１に示す。なお、ここにおける職域カードはスマート端末の運用者（オペレータ）の認証のために使われる（以下、オペレータカードと呼ぶ）。

以下、主な構成要素について簡単に説明する。

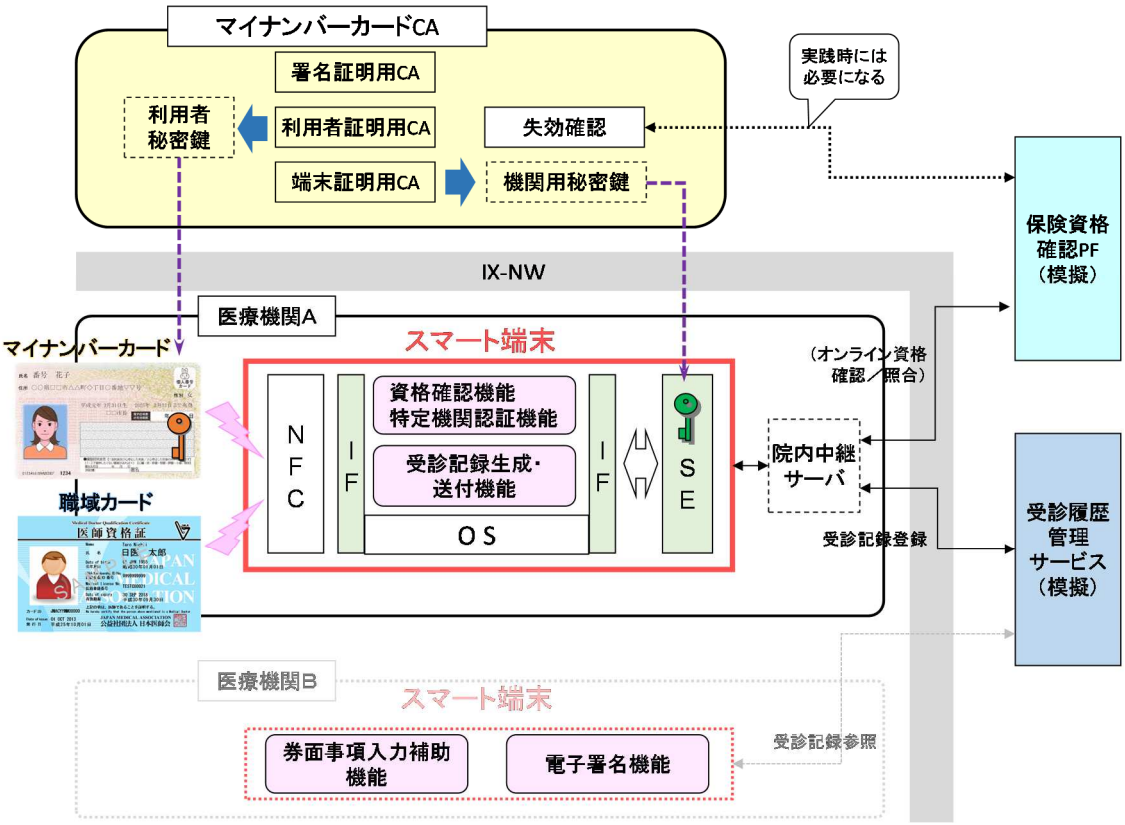


図３．１　基本的な実証システム構成イメージ

（１）マイナンバーカード CA

マイナンバーカードの JPKI アプリケーションにおける特定機関認証機能に対応した CA 機能であり、開発実証環境においては秘密鍵発行等の模擬 CA としての機能を提供する。

（２）院内機器

ア．スマート端末

マイナンバーカードによる特定機関認証機能に対応できるスマート端末（NFC搭載）を開発する。マイナンバーカードCAで生成した秘密鍵は、スマート端末等により管理されるSE（Secure Element）に格納する。

スマート端末はオペレータカードが持つカード保有者の電子認証機能を使うことで、利用権限の制約を可能とする（ログイン機能）。また、患者のマイナンバーカードが搭載する前述の特定機関認証機能を使って証跡性のある資格確認記録を生成・保持する（受付機能）。スマート端末に一時保存された患者の資格確認記録は、最終的に保険資格確認PFにオンライン接続して照合される（オンライン照合）。

さらに資格確認証跡を含む受診記録情報は担当医が操作して生成し、受診履歴管理サービスに送信・登録を行う（受診記録情報登録）。

なお、他の医療機関Ｂにて操作されることになる受診記録参照スキームの部分については、開発実証環境としては用意しない。

イ．院内中継サーバ（オプション）

複数の科を持つ中・大病院ではSEやいくつかの機能を中継サーバに実装し、端末とWi-Fi等で接続する方式が考えられる。以下の院内中継サーバを用いる方式は、いずれも医療機関側における機能分散実装のためのオプション形態になる。

医療機関用の秘密鍵および公開鍵証明書を院内中継サーバ配下で管理し、スマート端末と連携して認証処理を支援する。院内中継サーバはスマート端末から送付される資格情報および受診記録を一時蓄積する。患者の資格情報を基にIX-NWを経由して資格確認PFに接続し事後にオンライン保険資格照合を行なう。同様に受診記録については受診履歴管理サービスへ転送・登録を行う。各処理結果は院内記録として保存する。

（３）ネットワーク

本開発実証におけるネットワーク環境としては、一般的なLANを使用して機器間を接続し、インターネット等への外部接続は行わない。なお、実証環境として想定する構築中のIX-NW[2]ではVPN接続が前提であり、今回開発する機器類では、IX-NWでの対応も想定し、必要な接続手順を組み込めるよう設計上の配慮を行う。

（４）マイナンバーカード、およびオペレータカード

開発実証のために準備するマイナンバーカードにて利用者証明用電子証明書と署名用電子証明書、および特定機関認証の機能を搭載して利用できるようにする。なお、券面事項入力補助機能により基本４情報も電子的に利用できるようにする。

またオペレータカードにおいても、利用者証明用電子証明書と署名用電子証明書の機能が利用されることから、これらの機能を搭載したICカードを準備する。

以下に、本実証で利用するこれら２種類のICカードに共通する基本仕様を示す。

a. 形状とサイズ

・ISO/IEC7816に準拠

b. インタフェース

・コンビネーション型（接触・非接触型両用タイプ）

・接触インタフェースは、ISO/IEC 7816に準拠

・非接触インタフェースは、ISO/IEC 14443 Type-Bに準拠

c. セキュリティ

・暗号方式：RSA2048ビット、AES、SHA-256
・ＩＣチップこじ開けなど、物理的・電気的攻撃によりカード内の情報を読み出そうとする行為に対し、情報読み出し、又は解析されないような耐タンパ性

d. カードアプリケーション
・マルチアプリケーションカード
・今後の検討により設計するカードアプリケーションを実装可能

（５）保険資格確認 PF（模擬）

オフラインで認証された保険資格の結果照合を行う場合には、医療機関のスマート端末から送付されたデータに基づき保険資格確認を行い、記録を残すとともに、結果を医療機関側へ返却する。マイナンバーカードとオンラインで接続される場合にはこのPFにおいて通常の特定機関認証の手順による保険資格確認を行う。(ただし、開発実証環境では失効情報をオンラインでCAと連動させ確認することは行わない)

（６）受診履歴管理サービス（模擬）

院内中継サーバ経由で送付された受診記録を受診履歴管理サービスへ登録する。また、登録した結果を院内中継サーバへ返却する。開発実証では登録の機能のみとし、スマート端末からの参照機能は実装せず、登録状況は直接サーバ内のデータを表示して確認する。

３．３ 開発対象と機能要件

（１）セキュアエレメント

スマート端末もしくはスマート端末と通信を行う機器内に実装されるセキュアエレメントとして具備すべき機能とその概要を以下に示す。

表 3-1　セキュアエレメントが具備すべき機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
1	セキュアエレメント	①セキュアエレメント	・機関用公開鍵証明書など、スマート端末内アプリケション処理で必要なデータの一部を保持し、提示する機能 ・特定機関用秘密鍵を保持し、暗号演算を行う機能 ・エレメントモジュールが挿抜可能な構造

			では、取り外し時の機能を制限するなど、脅威を軽減する対策を検討すること ・携帯電話機の SIM 形状と物理的に互換性があること

（２）スマート端末のハードウエア／ファームウエア

スマート端末のハードウエア／ファームウエアとして具備すべき機能とその概要を以下に示す。

表 3-2　スマート端末のハードウエア／ファームウエアが具備すべき機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
2	ハードウエア／ファームウエア	①セキュアエレメント(SE)制御機能	スマート端末でアプリケーション領域とは分離されたセキュアエレメント機能もしくはスマート端末と通信を行う機器に実装されたセキュアエレメント機能を活用し、セキュアエレメント内の秘密鍵と暗号演算機能を利用して秘密鍵を保管して暗号演算を制御する機能
		②NFC 機能	スマート端末として NFC 機能を具備し、マイナンバーカードと非接触通信を行う機能（APDU のコマンド長として 400byte 以上を送ることができること）

（３）スマート端末内アプリケーション

スマート端末内アプリケーションとして具備すべき機能とその概要を以下に示す。

表 3-3　スマート端末内アプリケーションが具備すべき機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
3	スマート端末内アプリケーション	①オペレータ認証処理	提示されたオペレータカードを認証する機能
		②オペレータ情報取得処理	オペレータカード内に格納されているオペレータの情報（ID 等）を読み取る機能
		③特定機関認証処理	・SE と連動してカードの特定機関認証処理を実行する機能 ・上記プロセスの証跡を記録する機能

		④署名生成・検証	カードで署名を行い、またその署名に対して署名検証を行う機能
		⑤保険資格確認・照合・記録機能	利用者シリアルナンバーにより保険資格確認 PF に資格の状況を照会し、結果を記録する機能
		⑥受診記録生成・送付機能	受診記録を生成し、受診履歴管理サービスへ送付登録する機能

（４）保険資格確認ＰＦ（模擬）

開発実証用の保険資格確認 PF（模擬）が具備すべき機能とその概要を以下に示す。

表 3-4　保険資格確認 PF（模擬）が具備すべき機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
4	保険資格確認 PF	①保険資格確認機能	マイナンバーカードとのオンライン相互認証により、紐づけ ID（※注１）をキーに保険資格を確認し、返却する機能
		②保険資格照合機能	医療機関側での特定機関認証シーケンスにより生起された利用者証明の証跡を元に、事後に保険資格の照合を行い、医療機関側に確認情報を返却する機能

注１：マイナンバーカードの利用者シリアルナンバーと保険資格IDとを紐づけるもので、開発実証においては事前にデータセットを準備する。

（５）受診履歴管理サービス（模擬）

開発実証用の受診履歴管理サービス（模擬）が具備すべき機能とその概要を以下に示す。

表 3-5　受診履歴管理サービス（模擬）が具備すべき機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
5	受診履歴管理サービス	①受診記録登録機能	・紐づけ ID をキーに受診記録を受診履歴管理サーバに書き込み登録する機能 ・登録受診記録の状態表示機能

（６）院内中継サーバ（オプション）

院内中継サーバとして考えられる機能とその概要を以下に示す。

表 3-6　院内中継サーバが担う機能とその概要

項番	機能名（大分類）	機能名（中分類）	概要
6-1	保険資格確認機能	①保険資格確認抽出機能	スマート端末経由で院内中継サーバに保管された患者情報から、資格確認が必要な被保険者を抽出する機能
		②保険資格確認の問い合わせ機能	抽出した被保険者番号の資格を保険資格確認 PF に照会し、結果を返却する機能
6-2	受診記録転送機能	①受診記録転送機能	スマート端末経由で院内中継サーバに保管された受診記録を受診履歴管理サービスへ転送・書き込みする機能
		②受診記録の更新機能	転送が完了した受診記録を一定時間の経過により削除する機能

（７）マイナンバーカード CA（模擬）・IC カード

開発実証用のマイナンバーカード CA（模擬）と IC カードが具備すべき機能とその概要を以下に示す。

表 3-7　CA・IC カードが具備すべき機能とその概要

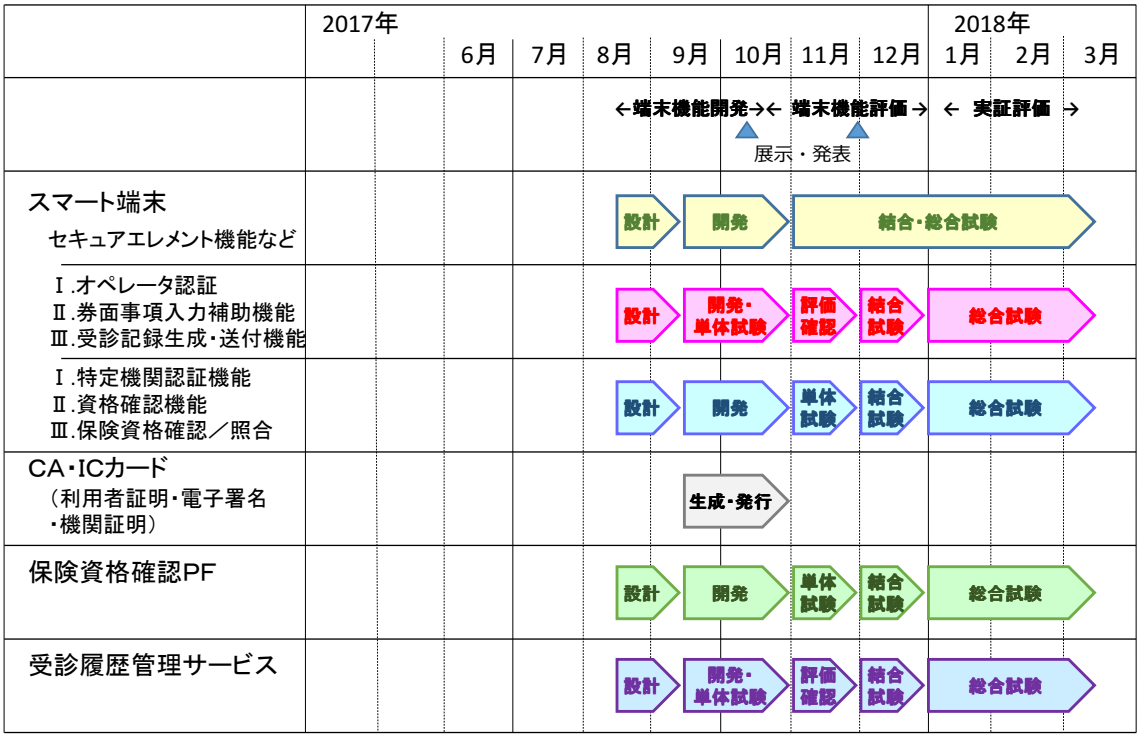
項番	機能名（大分類）	機能名（中分類）	概要
7	CA・IC カード	①PKI セット生成	マイナンバーカード、オペレータカード、スマート端末、および保険資格確認 PF（模擬）それぞれが保持する秘密鍵、公開鍵と公開鍵証明書を生成と保持
		②IC カード	・マイナンバーカードとしての PKI 証明書機能 ・オペレータカードとしての PKI 証明書機能

３．４ インタフェース仕様

各インタフェースは今後詰めていくこととする。なお、開発した各インタフェースについては、基本的に開示していくことを前提とする。

３．５ スケジュール

本開発実証に係る想定スケジュールは以下の通りとする。



４．納入等

４．１ 納入成果物

納入成果物は、書面により提出するほか、同内容を記録した電子媒体（CD-R 又はDVD-R）により、それぞれ正副二式ずつ納入すること。スマート端末については、OS、アプリケーション、秘密鍵等を搭載した状態で動作確認の検証を受けたものであること。

納入成果物の形態、記載内容の詳細、納入方法及び納入期限等については、事前に当協会と協議し、承認を受けた上で決定すること。

また、電子媒体の納入については、以下のとおりとすること。

- 納入のファイル形式は、「Microsoft Word 2010」、「Microsoft Excel 2010」「Microsoft Power Point 2010」、「PDF1.7」以降の版とし、参照・編集可能な形式とする。ただし、当協会が他の形式による提出を求める場合にはこれに応じること。
- 納入に当たっては、事前に最新のウィルス定義パターンによる検疫を必ず実施すること。
- 納入成果物は納入後に改変が可能となるよう、図表等の元データも併せて納

入すること。

・ 特別なツールを使用する場合は、事前に承認を得ることとし、ツールも併せて納入すること。

本開発実証の実施に係る主な納入成果物を以下に示す。

項番	成果物	数量	備考
1	設計書	紙（２部）及び電子媒体（２式）	
2	実証結果報告書		
3	操作マニュアル		
4	システム接続の手引書		
5	プログラムファイル	１式	電子媒体
6	スマート端末	５台	アプリケーション等、機能搭載のこと

４．２ 納入期限

平成３０年３月３０日（金）

４．３ 納入場所

東京都中央区日本橋小舟町３番２号　リブラビル
ニューメディア開発協会

５．特記事項

５．１応募者の条件

（１） 実績

本業務は、マイナンバーカードの利用を前提とするシステムの開発であることから、受託者はこれまでにマイナンバーカードあるいはマイナンバーカードを扱うシステムについて開発・運用、または機器開発において実績を有すること。

（２） 参加要件

応募者は３．３に示す本開発における開発対象と機能要件の項番のうち、一つあるいは複数項目について実現できることを示す提案を行うこと。ただし連携する項番4～6については必ず一括で提案を行うこと。また、項番3の提案に当たっては、適用を想定するスマート端末に関して動作環境を明示すること。

複数の事業者が共同提案する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、代表者が本業務にかかる連絡調整等

を行うこと。その際は、代表者を中心に、各共同提案者が協力して業務を遂行すること。各共同提案者間の調整は、その当事者となる事業者間において行うこと。

また、共同提案するすべての事業者が、前記５.１（１）の要件を満たすこと。

５．２ 再委託

受託者は、受託業務の全部又は一部を第三者に委託することはできない。ただし、受託者があらかじめ、再委託先の名称、住所、再委託する理由およびその業務の範囲、その他協会が求める情報について記載した書面及び再委託に係る履行体制図を提出して再委託の申し出を行い、協会が承認した場合にはこの限りではない。

受託者は、この受託契約により生じる権利又は義務を第三者に譲渡又は継承させてはならない。

なお、第三者に再委託する場合は、その最終的な責任を受託者が負うこと。

５．３ 著作権等の帰属

本開発における知的財産権等の扱いを以下に示す。

① 本件に関する新たな成果物に関し、著作権法（昭和45年5月6日法律第48号）第21条、第26条の3、第27条及び第28条に定める権利を含むすべての著作権を協会に譲渡し、協会は独占的に使用するものとする。なお、受託者は協会に対し、一切の著作権人格権を行使しないこととし、第三者をして行使させないものとする。また、受託者が本契約の納入成果物に係る著作権を自ら使用し、又は第三者をして使用させる場合、協会と別途協議するものとする。

② 成果物に第三者が権利を有する著作物および工業所有権が含まれている場合は、協会が特に使用を指示した場合を除き、受託者は当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。なお、この場合、受託者は当該権利者の仕様許諾条件につき、協会の了承を得ること。

③ 本件の作業に関し、第三者との間で著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら協会の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、協会は係る紛争の事実を知ったときは、受託者に通知することとする。

５．４ 機密保持

受託者は、本調達を実施するに当たり、入手した資料等については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。

① 貸与された書類等は指定された期日までに協会に返納すること。

② 本調達の完了後、上記に記載される情報を削除又は返却すること。

③ 受託者は、本調達に関して入手した情報等（公知の事実等を除く。）及び業

務遂行過程で生じた納入成果物等に関する情報を本業務の目的以外に使用又は第三者に開示若しくは漏えいしないものとし、そのために必要な措置を講ずること。

④ 受託者の責任に起因する情報の漏えい等により損害が発生した場合は、それに伴う弁済等の措置はすべて受託者が負担すること。

⑤ この項目について受託者は、契約期間の終了後においても同様とする。

５．５ その他

本仕様書に記載なき事項にあっても本業務の実施に必要と認められる事項に関しては、その取扱いについて別途当協会と協議を行うこと。

---

1) 個人生涯健康医療管理システムとは、平成 28 年度に当協会にて開催した委員会において、将来構想として調査検討を行ったシステムの名称。
<http://www2.nmda.or.jp/mainproject/project0202/>

2) IX-NW とは総務省が構築中の医療等分野における高精細映像等データ共有基盤のことであり、今年度での実証を経て、平成 30 年度からは医療等分野専用ネットワークとして全国の地域医療情報連携ネットワーク間を接続する役割を担う。