URL　https://journal.ntt.co.jp/article/29830
DOI　https://doi.org/10.60249/24105003

6G/IOWN時代の信頼できるアイデンティティデータ流通を実現するSSI基盤

ユーザのアイデンティティに関するデータを標準化されたフォーマットでデジタル化し，多様なサービスで活用できるようにするというデジタルアイデンティティに関する動きが加速しています．デジタルアイデンティティを取り巻く世の中の動向に合わせ，NTTネットワークサービスシステム研究所ではインクルーシブコアの要素技術として，ネットワークサービスとデジタルアイデンティティの連携を実現するSSI（Self-Sovereign Identity）基盤の研究開発に取り組んでいます．本稿では，SSI基盤の持つセキュアIDウォレットを中心とする技術について述べた後，同時に進めているSSI基盤をメタバースに適用するユースケース実証について紹介します．

キーワード：#デジタルアイデンティティ，#自己主権型，#移動固定融合

松本　存史（まつもと　ありふみ）
肥後　直樹（ひご　なおき）
NTTネットワークサービスシステム研究所

デジタルアイデンティティとは

免許証などの資格情報や大学在籍情報，TOEICのスコアに至るまで，さまざまな個人・法人にかかわるデータを標準化されたフォーマットでデジタル化し，それをさまざまなサービスで活用できるようにするというデジタルアイデンティティに関する動きが加速しています．デジタルアイデンティティとは，個人を他と区別するために用いる個人の属性情報の集合といえます．なぜ，今このデジタルアイデンティティが注目を集めているのでしょうか．リアルな空間では相手の顔を見て識別したり，身分証のカードを提示して特定の国籍を持っていることを証明したり，資格を持っていることを証明していたりしたものが，デジタル空間でサービスを提供する際にはデジタル化された個人の属性情報を用いて制御を行う必要があります．さまざまなサービスをオンライン上で提供したいというデジタル化のニーズと，デジタル空間上で提供されるサービスをより安全または便利に使うために，各個人の属性や資格を確認したいというニーズにこたえるため，デジタルアイデンティティが注目されているのだと考えています．

本稿では，デジタルアイデンティティを取り巻く世の中の動向について述べた後，NTTネットワークサービスシステム研究所で取り組んでいるインクルーシブコアの要素技術であるSSI（Self Sovereign Identity）＊1 (1)基盤について紹介します．

デジタルアイデンティティに関する動向

デジタルアイデンティティについては，欧州連合（EU）圏において特に法整備やサービス提供に向けたプロダクト開発，標準規定の策定が進んでいます．

■電子身分証明（eIDAS規則）の普及

EUでは，eIDAS（Electronic IDentification, Authentication and trust Services）＊2が導入され(2)，異なるEU加盟国で発行された電子身分証明書を相互に認証可能にする枠組みが整備されています（**図1**）．これにより，EU市民は国境を越えて安全にデジタルサービスを利用することができます．特にeIDAS2.0と呼ばれるアップデートにおいて，ユーザ自らが自身のデジタルアイデンティティに関する情報の管理を行えること，またそれをEUDIW（European Digital Identity Wallet）と呼ばれるウォレットサービスによって実現することが提案されており，2024年2月にこのアップデートが正式に承認されました．

■電子パスポートの導入

多くのEU加盟国では，電子パスポートが発行されており，バイオメトリクスやRFID（Radio Frequency IDentifier）チップを利用してデジタル化された個人情報を保持しています．これにより，国境通過やオンラインサービスの利用が簡便化されています．

■eIDの利用拡大

多くのEU加盟国では，税務申告や行政手続きなどでeID（Electronic IDentification）を使用することが一般的になっています．これにより，EU加盟国間で国をまたいで，個人が安全にオンライン上で身分を証明し，取引を行うことが可能です．

また，北米においても以下のようなデジタルアイデンティティに関する動向があり，世界中から注目を集めています．

■デジタル身分証明の推進

米国では，州ごとに運転免許証や身分証明書のデジタル化が進んでいます．一部の州では，モバイルアプリを通じてデジタル運転免許証を利用できるようになっており，オンラインでの身分証明が容易になっています．

■デジタルヘルスパスポートの導入

新型コロナウイルスのパンデミックによ

＊1 SSI：自己主権型アイデンティティ．SSIは，個人が自分自身のデジタルアイデンティティを所有し，コントロールすることを可能にするWeb3.0にかかわる技術コンセプトです．SSIは中央管理者や認証機関に頼る必要がなく，ユーザが自分の情報を安全に管理できる仕組みを提供します．
＊2 eIDAS：EU政府による電子的な認証および信頼に関する規則．

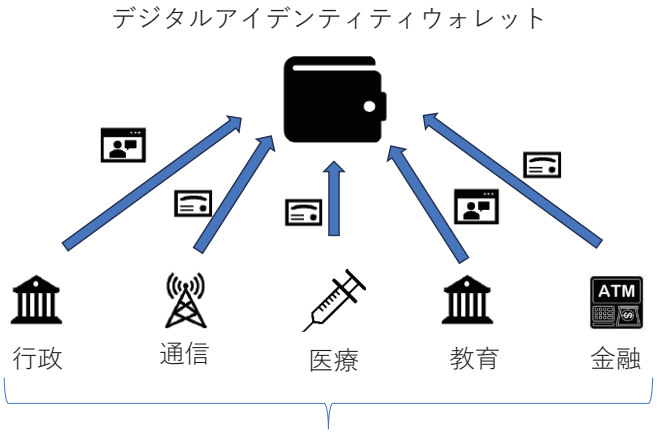

図1　EU圏での動向

り，デジタルヘルスパスポートの需要が高まっています．米国では，ワクチン接種証明書や健康ステータスを電子的に管理・証明する取り組みが進められています．

日本国内におけるデジタルアイデンティティに関連する動向としては近年さまざまな動きがあります．

■マイナンバーカードの普及

日本では，マイナンバーカードが国民1人ひとりに割り当てられており，個人番号（マイナンバー）を持つことが法律で義務付けられています．このカードは，オンラインでも利用できるようになっており，各種行政サービスの利用や電子申請が可能となっています．

■電子証明書の普及

企業や行政機関において，電子証明書が広く利用されています．電子証明書は，デジタル署名やオンライン手続きの際に使用され，法的な効力を持ちます．電子署名や電子契約，ソフトウェアの偽造防止のための証明書などにより，紙の証明書からデジタル化への移行が進んでいます．

これらの動向により，日本においてもデジタルアイデンティティの普及が進み，その利便性を認知されつつあり，さまざまな行政サービスや日常生活の中でアイデンティティのデジタル化が進んでいることが確認されます．

デジタルアイデンティティの技術トレンド

次に，最近のデジタルアイデンティティに関する技術的な動向として重要なトピックについて触れます．

■セルフソブリンID（SSI：Self-Sovereign Identity）の普及

セルフソブリンとは自己主権型という意味で，セルフソブリンIDは，ユーザが自らのアイデンティティを制御することを可能にするコンセプトです．このアプローチにより，個人は中央管理者や第三者に依存せず，自己のデジタルアイデンティティ，すなわち個人識別子（ID）とそれに紐付く属性情報や各種証明書などの個人情報を持つことができます．

■分散型IDの台頭

分散型ID（DID：Decentralized Identifier）*3は，中央集権的なシステムではなく，ユーザ自身が管理する形態のデジタルIDです(3)．ブロックチェーンなどによる分散型台帳技術（DLT：Distributed Ledger Technology）をベースとすることが多く，ユーザが自分のデータを所有し，管理することが可能となり，SSIを実現するための要素技術といえます．分散型IDはW3C（World Wide Web Consortium）などの標準化団体が関連規格を策定し，普及が進んでいます．

■VCの発展

VC（Verifiable Credentials）*4は，さまざまな機関やサービスが発行する証明書や情報を，安全に受け取り，自己のデジタルアイデンティティに結びつける仕組みです．例えば，学位証明書や医療記録，会員証などがVCとして発行され，必要なときに第三者に提出することができます．これにより，データの所有権やプライバシーがユーザ自身によって管理される仕組みが強化されています．DIDを連携させて利用されることが多く，こちらもSSIのコンセプトを実現するための要素技術です．

図2のように，従来は中央集権型のアイデンティティプロバイダー（IdP）によって，ID情報やそれに紐付くデータが管理され，データの授受もIdPからそのデータを利用するサービス事業者に提供されていました．分散型のアイデンティティ管理においては，データはユーザ自らが管理し，ユーザが利用するサービス事業者に自ら提示するというデータの流れに変わります．ユーザデータが1カ所に集まらず，ユーザ各自が管理するため分散型のアイデンティティ管理と呼ばれており，ユーザのプライバシー情報の漏洩を防ぎつつデジタルアイデンティティ情報の流通・活用を促進する方式として注目を集めています．

デジタルアイデンティティと6G/IOWN時代のネットワークサービス

これらの法制度やビジネス化の動向，および標準化等の技術確立の進展に合わせて，DIDとVCを活用したさまざまなユースケースの検討や実証が行われています．特に現在は業界ごとにDID/VCをはじめとするデジタルアイデンティティの活用方法について検討が進められています．しかし，デジタルアイデンティティの活用は各業界に閉じたものではなく，業界を横断して進めてこそ利便性の向上や業務効率の向上など，より大きな効果をもたらすものです．つまり，各業界でどのようなデジタルアイデンティティの発行や利用が可能であるかを決め，各業界から発行される情報を業界横断で活用していくことになり，和算ではなく積算によって利用シーンが広がっていくことが期待できます．

＊3 DID：分散型識別子は，SSIの基盤となる要素で，一意なデジタル識別子です．DIDは中央の機関に依存せず，ブロックチェーンなどの技術を使用して，ユーザが自分自身を一意に識別できるようにします．

＊4 VC：検証可能な資格証明．個人が所有するスキル，資格，属性などの情報をデジタル形式で表現したもので，信頼性を確認するための証拠を提供します．VCはDIDと結びついて使用され，信頼性のある方法で資格情報を共有できるようにします．

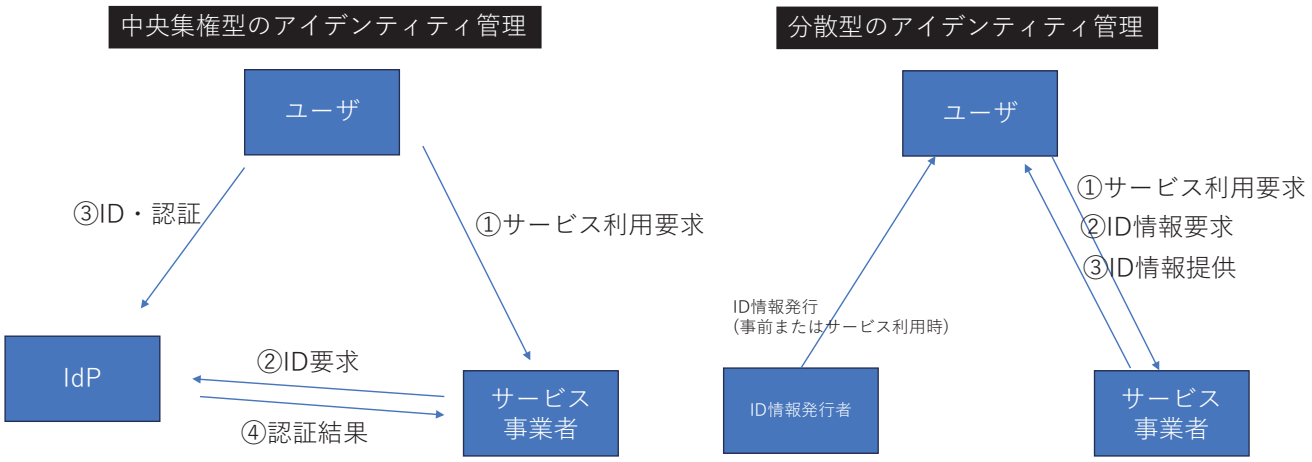

図2　分散型のアイデンティティ管理へのシフト

ネットワークキャリアのデジタルアイデンティティに関する動向は，まだいくつかの団体で検討が始まったばかりという状況です．デジタルアイデンティティを流通することの効果をより大きなものにし，より便利で安全なデジタル社会を創造していくためには，ネットワークキャリアの果たすべき役割は大きなものであるといえます．NTTネットワークサービスシステム研究所では，ネットワークキャリアとして，デジタルアイデンティティの発展すなわちデジタルアイデンティティ情報流通の実現やそれに基づくサービスの展開に貢献していくという取り組み，また社会に流通するデジタルアイデンティティ情報を用いたネットワークサービスの展開などについて検討を行っています．以下にその検討状況について述べます．

■デジタルアイデンティティ情報の発行

移動固定を問わず，ネットワークキャリアはデジタル社会においてさまざまな役割を果たしています．データ通信や電話などの通信サービスの提供が主たる提供サービスであることは言わずもがなですが，それらのサービスを提供する際には，本人確認（KYC：Know Your Customer）や居住地の確認等を実施することにより，正しいユーザに間違いなく通信サービスが提供できるようになっています．また，電話サービスの利用者に対しては電話番号を割り当て，その契約者がその電話番号を利用できることを保証しています．また，携帯電話ユーザについては，ユーザの居場所を把握していなければ，通信サービスを提供できませんので，ユーザが通信可能な所にいる限り，常にユーザの居場所を把握している必要があります．

契約情報やサービス提供において必要となる情報は，通常はネットワークキャリアが内部で保持・管理している情報です．これらの情報をユーザや他のサービス事業者に対し再利用可能なかたちで発行することにより，さまざまな利用価値をもたらす可能性があります（**図3**）．例えば，電話番号所有証明を前述のVCとして発行することにより，現在さまざまなサービスを利用する際に連絡先の入力が求められていますが，この連絡先情報として高い信頼性のある検証可能な証明書として提供することができるようになります．電話番号に限らず，通信サービスを契約する際にネットワークキャリアに提示した情報であれば，同様にネットワークキャリアが確認を行ったユーザのデジタルアイデンティティ情報として発行・流通が可能となるわけです．また，ユーザの位置情報については，例えばATMで銀行口座から預金の引き出しを行いたい場合，ATMを操作している人が本当にその場所にいるのか，あらかじめ銀行口座と携帯電話の契約を紐付けておけば確認することができ，本人以外がお金を引き出している場合にそれを防ぐことが可能になります．

このような取り組みはすでにGSMA（Global System for Mobile Communications Association）等の団体で議論が開始されており[4]，今後ますますさまざまなネットワークキャリアによるデジタルアイデンティティ証明書の発行が加速していくと思われます．NTTネットワークサービスシステム研究所では，各種ネットワークキャリアが発行可能な証明書の標準化や，それを用いたユースケースの実証に取り組んでいきます．

■セキュアIDウォレットの提供

デジタルアイデンティティ情報は，ユー

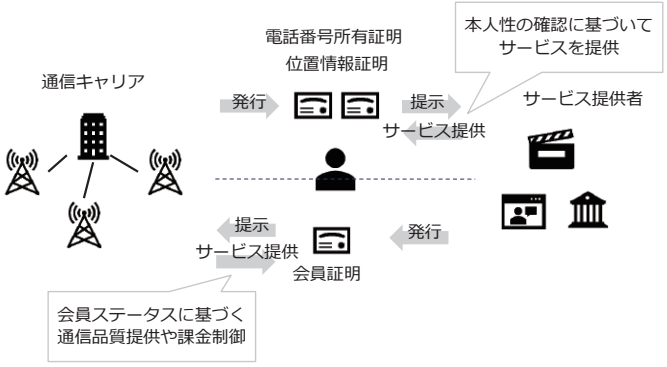

図3　キャリアによるアイデンティティ発行

ザ自らが管理し，提示先や提示内容などをユーザ自らが決定することが基本であるため，従来ではユーザが管理する端末にデータを格納することが一般的でした．しかし，デジタルアイデンティティ情報はユーザにとっても，またそれを利用するサービス事業者にとっても重要な情報であり，データの漏洩や改ざん，またユーザ自らによって不正に複製・譲渡などの悪用を防ぐことが求められます．そのため，データを格納する端末に悪意のあるソフトウェアがインストールされていて，端末内のウォレットのデータを盗み見るなどの攻撃からデータを守る仕組みが必要となります．また，ユーザが端末を紛失した場合に，データが遺失してしまうリスクにも対処が必要となります．

NTTネットワークサービスシステム研究所ではこれらの攻撃やリスクへの対策として，デジタルアイデンティティを格納するウォレットを，専用のセキュリティモジュールを具備したクラウドで提供するセキュアIDウォレットの検討を進めています（**図4**）．セキュアIDウォレットでは，TEE（Trusted Execution Environment）[*5]等のハードウェアで実装されたセキュリティモジュールを用いて，ウォレットソフトウェアをクラウドのサーバ上の隔離された実行環境において実行させることにより，その処理中のメモリの内容や，永続化されるデータが暗号化されること（秘匿性）を保証しています．さらには，ウォレットを実現しているソフトウェアに改変が加えられてしまうと，メモリやデータが暗号化されていたとしても，データの漏洩や改ざんなどが可能となってしまうため，Remote Attestation（RA）[*6]という仕組みで，ソフトウェアが改ざんされていないこと（完全性）を利用者などがシステムの外部から検証できるという特長を持っています．

ウォレットから外部サービスにデジタルアイデンティティ情報を提示する際のセキュリティの確保も，重要な課題となります．提示するデータに記載されているDIDの匿名化・ワンタイム化に加えて，開示するデジタルアイデンティティ情報に記載された複数の属性のうち，サービス利用に必要な最低限の属性のみを開示する選択的開示などの技術が検討され，標準化も進んでいます．これらの技術は，サービス事業者の名寄せによるユーザプロファイリングや，プライバシー情報の漏洩などのリスクを回避するために有用です．しかし，こういったデータの内部に記載されている情報だけでなく，ユーザのウォレットにアクセスする際のURLやIP（Internet Protocol）アドレスなどのエンドポイントの情報についても対策を講じなければ，プライバシーリスクの対策としては不完全です．NTTネットワークサービスシステム研究所では，ユーザウォレットのエンドポイントアドレスの名寄せ対策として，ワンタイムエンドポイント方式や，外部サービスにエンドポイントアドレスを開示しないVCの提示方法などの検討を行っています．

また，このセキュアIDウォレットをさらに利便性高く利用する方法として，ユーザの所有する端末に挿入されているSIMカードに記録された認証のための鍵などの情報を用いて，セキュアIDウォレットに安全かつ便利に接続可能とさせる認証連携や，サービスによって複数のウォレットを使い分けるような利用シーンを想定して，他のウォレットサービスと連携して動作する連携機能などについても検討を進めています．

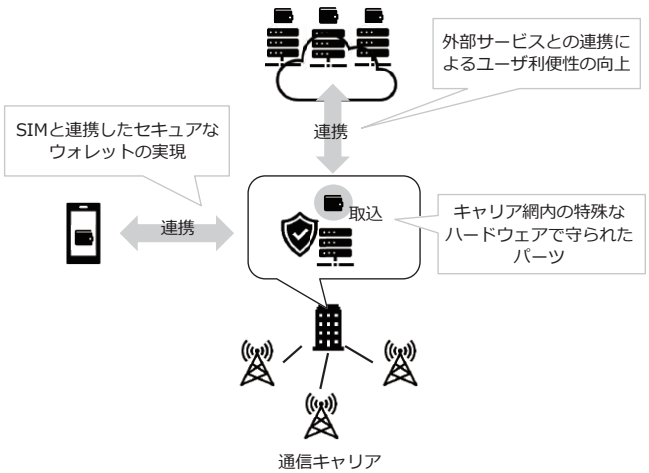

図4　セキュアIDウォレットサービス

デジタルアイデンティティを活用したネットワークサービス提供

次にデジタルアイデンティティ情報流通を用いたネットワークキャリアサービスの提供に関する検討内容について説明します．

アイデンティティ情報がデジタル化されることで，サービス事業者はユーザのアイデンティティ情報をより動的・柔軟に扱うことができるようになります．ネットワーク接続サービスにおいても同様に，ユーザのデジタルアイデンティティ情報を用いて，より柔軟で多様なネットワーク接続サービスが可能となることが想定されます．

例えば，提示されるデジタルアイデンティティ情報によって，緊急車両や緊急呼，医療サービス関連など緊急性の高い通信を識別し，ネットワーク内部の通信リソースを優先的に割り当てる制御を行うなどの利用方法が考えられます．また，特定のサービス利用時の通信料金を，ユーザに代わってそのサービス事業者などの他者が負担するような仕組みをVCによって実現することも可能と思われます．

こういった取り組みは，まだ研究段階という状況ですが，NTTネットワークサービスシステム研究所としてもより利便性の高いネットワークサービスの実現に向けて，検討を進めていきます．

メタバースを用いたユースケース実証

NTTネットワークサービスシステム研

＊5　TEE：ハードウェア上の安全な隔離実行環境を指し，メモリを暗号化した状態でデータを処理する秘密計算技術．
＊6　Remote Attestation：プラットフォームやアプリケーションの完全性をリモートから検証するための仕組み．

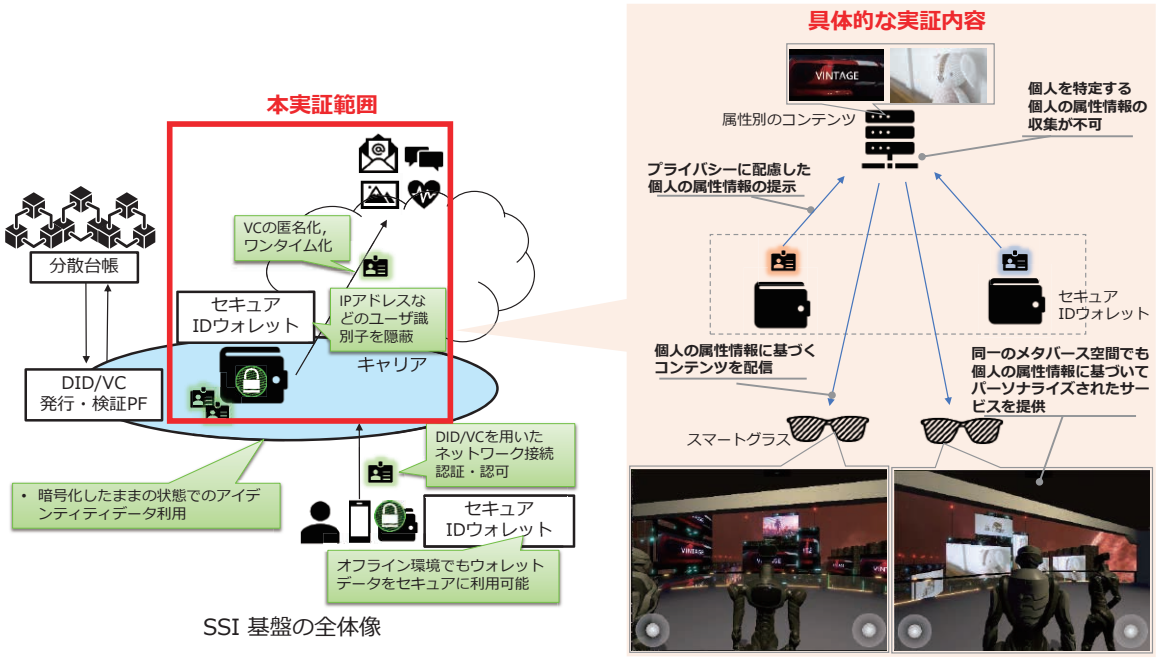

図5　メタバースをユースケースとした実証

究所では，ここまで紹介した技術の方式検討と並行して，実装を用いた技術の実現可能性の検証も行っています．2023年度のNTT R&Dフォーラムでは，SSI基盤をコアネットワークへ具備することを想定した実装を行い，それをメタバースサービスに適用するユースケース実証を行い，実証内容について報道発表を行いました．

本実証では，メタバース空間上でさまざまなサービス事業者が独自のサービスを提供しており，サービス事業者はユーザ1人ひとりに合ったパーソナライズされたサービスを提供するため，ユーザの個人情報を必要としているという状況を想定しました．必要以上のプライバシー情報の開示を防ぐために，SSI基盤をメタバースサービスに適用することで，ユーザのウォレットから必要最低限の情報（年齢情報）を提供するだけで，提供コンテンツのパーソナライズが可能となることを実証しました．ユーザのウォレットは前述のセキュアIDウォレットであり，サービス事業者に開示するデータの内容以外に，ウォレットのエンドポイント情報についてもワンタイム化することで名寄せリスクを回避する方式を実装し，さらには，インクルーシブコアにおいてインネットワークコンピューティングを実現するISAP（In-network Service Acceleration Platform）*7とも連携し，ISAP上にセキュアIDウォレットを実装しインスタンスの管理を行うことで，ユーザの位置やサービス利用状況に合わせてウォレットサービスを提供できることを実証しました（**図5**）．

今後の展望

EU圏での2025年のeIDAS2.0に関する各種サービス本格開始に向け，今後デジタルアイデンティティに関するサービス提供や技術開発はますます世界的にも加速することが予想されます．NTTネットワークサービスシステム研究所ではこれらの動きと歩調を合わせながら，デジタルアイデンティティ情報流通によるさまざまな社会課題の解決に向け，他の通信キャリアと連携しながら標準化や技術確立に向けて検討を進めていきます．

■参考文献

(1) A. Preukschat and R. Drummond：“Self-sovereign identity,” Manning Publications, 2021.
(2) https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
(3) O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and Manu Sporny：“Decentralized identity：Where did it come from and where is it going?,” IEEE Communications Standards Magazine, Vol.3, No.4, pp.10-13, 2019.
(4) https://www.gsma.com/about-us/regions/europe/gsma_resources/mobile-number-as-a-verifiable-credential-in-eidas-2-0-wallets/

*7 ISAP：ネットワークキャリア内部のGPUやDPUなどのハードウェアを含む計算リソースを外部のアプリケーションサービスに利用させるための基盤．

（左から）松本　存史／ 肥後　直樹

デジタルアイデンティティの社会実装と，それによるさまざまな社会課題の解決に向け，ネットワークキャリアとしても貢献していきます．そのための要素技術や標準化活動などを展開していきます．

◆問い合わせ先
NTTネットワークサービスシステム研究所
ネットワークアーキテクチャプロジェクト
E-mail　nea-mgr @ ntt.com