URL　https://journal.ntt.co.jp/article/36084
DOI　https://doi.org/10.60249/25095104

デジタル価値社会の実現に向けて――個人起点の情報流通

個人主導の情報流通による「デジタル価値社会」の実現に向け，NTTではデジタル情報の信頼性確保，暗号化などの制御の実現，安全な活用手法に関する研究開発を行っています．情報の真正性・制御性・安全性を三本柱としてデジタルIDウォレットや分散型トラスト，秘密計算等を通じて，信頼可能かつプライバシー保護された情報活用を可能とする基盤技術の構築をめざしています．

キーワード：＃情報の信頼確保，＃情報の暗号化・復号制御，＃情報の安全な利活用

横関　大子郎（よこぜき　だいごろう）／藤村　滋（ふじむら　しげる）
伊藤　宏樹（いとう　ひろき）／田中　政志（たなか　まさし）
張　一凡（ちょう　いいふぁん）

NTT社会情報研究所

はじめに

世界中のすべての情報がデジタル化される時代が到来しつつあります．買い物，移動，医療，教育，エンタテインメントといった人間のあらゆる営みがデジタル情報として記録され，その情報の集合が私たちの“もう1つの姿”をかたちづくるようになってきました．

この莫大なデジタル情報を活用するには，信頼性を保ちつつ，安全に流通させる仕組みが不可欠です．ところが現実には，フェイクニュースや生成AI（人工知能）による情報の氾濫，個人情報の囲い込み，プライバシー漏洩のリスクといった課題があります．

誰もが自分の情報を活用し，価値を得ることができる「デジタル価値社会」の実現に向けて，情報を信頼できるようにするデジタル信頼性確保技術と，そのうえでのデータ暗号化制御技術，データ活用技術の3つの柱（**図1**）で取り組みを進めています[(1), (2)]．

デジタル情報を信頼できるようにする

デジタル情報が社会の基盤となる中，その「真正性」を担保する技術が求められています．私たちは，人・法人・モノ・AI（人工知能）・データ等，あらゆる情報の出所や内容の正しさを保証する「トラストが保証された次世代のインターネット」の構築をめざしていきます．

これにより，国や業界，企業を横断した信頼ネットワークが形成され，安全に情報が流通し，価値を生み出すことが可能です．

また，個人・法人などのバーチャル空間上，リアル空間上のすべての活動履歴や取引情報を一元的に記録・管理できる「デジタルIDウォレット*1」の実現をめざしています．ウォレットは，いわば個人や法人の分身（デジタルツイン）といえ，それを学習したパーソナルAIが，自身の嗜好や行動を理解し，食事の好みや旅行先，金融や健康面での最適な提案まで行うなどの応用が期待されます．

こうした「デジタルIDウォレット」が社会基盤として広く普及するためには，そのウォレットに格納される情報の真正性と信頼性をいかに確保するかが重要です．ウォレット内の情報が信頼できなければ，パーソナルAIによる提案やサービス連携の土台が崩れ，結果として社会全体の情報流通に対する信頼が損なわれてしまいます．そのため，私たちは「信頼できる情報を誰

＊1　デジタルIDウォレット：個人・法人の資格やデータ流通の記録・証明を一元管理し，必要に応じて開示できるデジタル情報管理ツール．プライバシー保護と利便性を両立します．

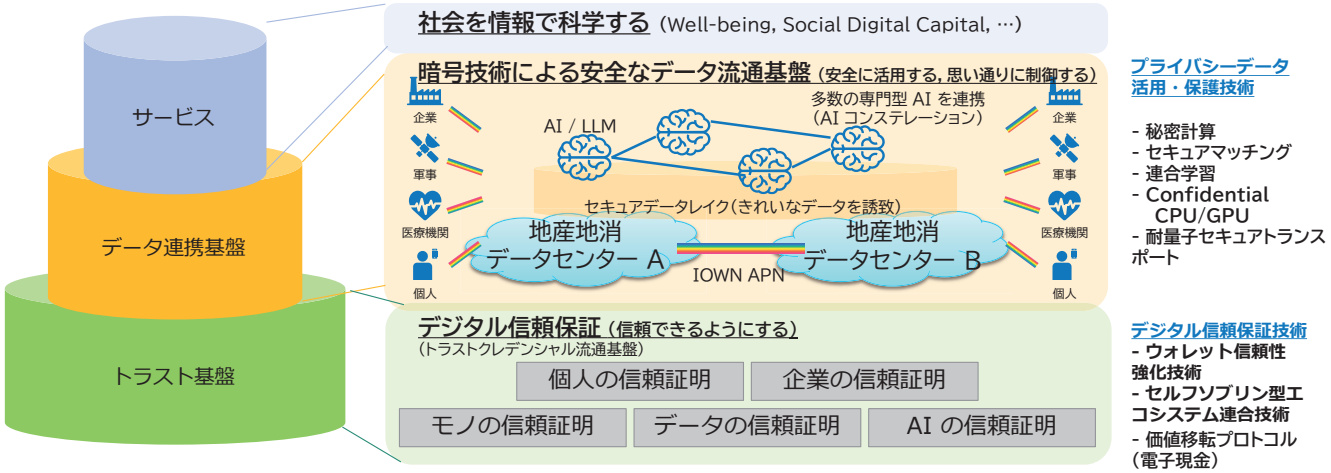

図1　デジタル情報基盤アーキテクチャ

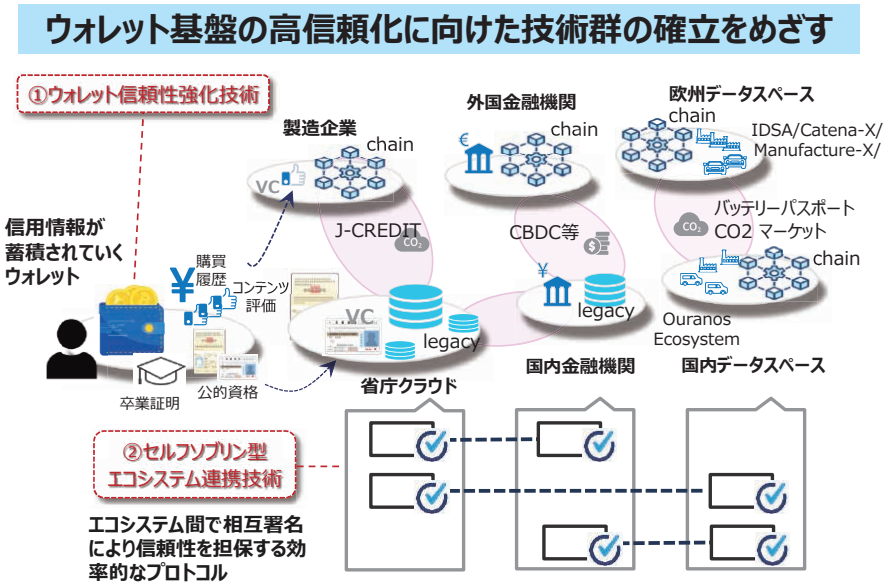

図 2　デジタル情報の真正性を担保するための 2 つの要素技術

が，どのように所有・管理・提示し，第三者がどのように検証できるか」を体系的にとらえ直す必要があります．

このような観点から，私たちはデジタル情報の真正性を担保するための 3 段階のステップを描いています．

第 1 のステップは，情報そのものに「証明可能な形式」を与えることです．個人や法人，サービス提供者などが発行する資格情報や取引証明，認証結果などを，改ざん不可能なデジタルクレデンシャルとして流通させる仕組みが必要です．デジタルクレデンシャルとして，内容の正当性は発行者の署名により保証し，真正性や信頼性を受け取り手が検証可能な構造を志向しています．

第 2 のステップは，それらの証明情報を「利用者が自律的に管理・提示できる仕組み」を構築することです．ここで中心的な役割を果たすのが，前述の「デジタル ID ウォレット」です．これは単なる情報保管庫にとどまらず，利用者自身が必要な場面に応じて，適切な証明情報を選び，開示できるプライバシー・バイ・デザインのプラットフォームです．ウォレットは，個々人の情報的自立性と，サービス提供側の検証容易性とを両立させるものです．

第 3 のステップは，証明情報の発行者・検証者・保管者を支える「分散型トラスト基盤[*2]」の構築です．デジタルクレデンシャルの検証には，発行者の公開鍵やスキーマ定義，失効情報などを格納・参照する仕組みが必要ですが，単一のルートオブトラストを世界中で共有するのは困難です．そこで私たちは，複数のトラストドメインが互いに相互運用可能であり，信頼関係を接続可能な構造を持つべきです．これにより，国家や業界を越えたグローバルな信頼ネットワークが形成され，分散型のデジタルクレデンシャル流通が可能になります．

これら 3 つのステップを実現するために，私たちは基盤技術として 2 つの要素技術に取り組んでいます（**図 2**）．

1 つは，秘密分散技術を応用した MPC（Multi-Party Computation）型の「ウォレット信頼性強化技術」です．デジタルクレデンシャルの提示や署名に必要な秘密鍵の安全な管理は，ウォレットの信頼性に直結する要素です．単一の端末やサーバに鍵を集中させる方式では，不正アクセスや紛失に対して脆弱です．そこで私たちは，秘密鍵を複数の分散的な要素に分け，協調的に署名を実行する MPC 技術に加えて，ソーシャルリカバリー機能を備えることで，利用者が信頼する人や別デバイスを鍵再構成の一部とする仕組みを実装し，セキュリティと利便性の両立を図っています．

もう 1 つは，エコシステム間の相互連携を可能とする「セルフソブリン型エコシステム連携技術」です．私たちは，世界に 1 つの中央集権的なレジストリではなく，国や業界が独自に構築したエコシステムどうしが，互いに認証や信頼の橋渡しを行えるような構造をめざしています．この構造により，多様なステークホルダがエコシステムをまたぐかたちでの参加が可能となり，将来的には分散型かつ多元的なトラスト・ネットワークが形成されていきます．

私たちは，以上のようなステップと技術要素を通じて，「真正性」が保証されたデジタル情報の世界を実現していきます．それは単なるセキュリティの強化にとどまらず，情報社会における信頼のあり方を根本

＊2 分散型トラスト基盤：国家や組織間で相互に信頼性を検証し合える仕組みで，特定の中央管理者に依存せずに情報の真正性を担保する基盤のこと．

から再定義し，すべての人とAIが安全・効率的に共存する次世代インターネットの基盤となることをめざし，取り組みを進めています．

デジタル情報を思いどおりに制御する

デジタル情報は一度自身の手を離れると，どのように使われるか分からないのが現状です．本来，デジタル情報はその本人が主体的に管理すべきものであり，データが所有者の期待したとおりに処理されることを保証する仕組みが不可欠です．

NTTはこの課題に対し，ユーザが自らの情報利用を制御できる仕組みとして，ポリシーに基づいたアクセス制御，情報使用履歴の可視化，第三者による証明・検証といった機能の研究開発を進めています．

さらに，ウォレット内の情報が他者に漏洩しない設計や，プラットフォーム事業者としてのNTT自身も個々のユーザが所有するデータの中身にアクセスできない仕組みを構築することで，真の意味での「データ主権（Data Sovereignty）*3」の実現をめざしています．これは，安心して情報を流通させ，AIなどによってその価値を享受するための土台です．

NTTが考える「データ主権」，ユーザのデジタル情報が「自身の手を離れた」場合であっても，ユーザが自らデジタル情報の利用を制御できている，「データ主権」のある状態とは，どのような状態でしょうか．

一般に，データはその生成から消滅（消去）に至るまで，そのライフサイクルを通じて，蓄積，伝送，計算とさまざまな処理が繰り返し行われます．NTTが考える「データ主権」では，この過程を通じて，データが常に暗号化されている状態であること，およびデータは，それを利用する権限を持つ者以外がデータの閲覧，加工，複製，再利用等できる機会を最小化されていること，の2点を必要とします．すなわち，悪意を持った攻撃者だけでなく，適切な権限を持たない当事者による意図しないデータ取得が可能な機会を最小化することを必要とします．

これは，データはデータライフサイクルを通じて一貫して暗号化され，ユーザにより認められた当事者が，認められた条件に基づいた場合だけ復号可能とすること，データを暗号文のまま分析処理可能なフレームワークを必要とすること，あるいはそのデータを活用した処理結果の利用もユーザにより認められた条件に基づく場合に限られること，などデータが必要な状況以外は常に暗号化され，秘匿とされる世界，「平文のない世界」を必要とします．

NTTが考える「データ主権」では，こうしたデータの利用を適切に管理可能な機能を持つプラットフォームが，データ処理を行うクラウドなどの外部の計算基盤や，その計算基盤が構築されているデータセンタを含め，その安全性が当事者や監査者などの第三者に対し証明可能である状態，すなわち暗号技術，権限管理によりデータが適切に保護されたコンピューティング空間にある状態を，「データが安全な金庫にある状態」と表現しています．

NTTが考える「データ主権」は，前述の技術群を組み合わせることで実現します．ここでは，「第三者による証明・検証」「情報が他者に漏洩しない，NTT自身も情報にアクセスできない設計」の2点の技術を概観します．

まず「第三者による証明・検証」は，データ流通にかかわるシステムが適切に設計，構築，運用されていることを，当事者や第三者に対して検証可能な様態で証明するものです．

例えば，あるシステムが対向するシステムと接続し，機微なデータの授受を行うに際し，当該システムは，対向システムをいかに信頼しデータ授受が適切か判断できるでしょうか．一般的には定期的に外面的な監査を行い，システムが適切に設計，構築，運用されていることを第三者がお墨付きを与えることが考えられますが，それによって保証できる真正性には限りがあります．

これに対し，NTTでは「相互アテステーション*4」と呼ばれる考え方を提唱しています．

ここでいう「アテステーション」とは，あるシステム（ソフトウェア，ハードウェア，設定等）が正当かつ改竄されていない状態であることです．例えば特定バージョンのOSやアプリケーションで動作していることを示す証跡（測定値）を用いて，接続しようとするシステム間で相互に信頼可能かを判断する際に利用します．

次に，「情報が他者に漏洩しない，NTT自身も情報にアクセスできない設計」は，データが，その生成から消滅（削除）に至るまで常に暗号化された状態で管理，運用されることの保証をめざしたシステム設計の考え方です．具体的にはデータの復号は，必要最小限のタイミングで行われること，復号されたデータ（いわゆる生データ）は，必要最小限の相手に対し必要最小限の権限で開示されることを定めます．これにより，データの意図しない他者への提供や，データの受領者を経由した他者への漏洩リスクを可能な限り低減します．

その具体例として，NTTでは“Confidential Remote CPU/GPU”と呼ぶフレームワークを提唱しています．このフレームワーク技術の特徴は，TEE（CPU内部のハードウェア的に隔離しメモリ暗号化を行うセキュアな処理環境）を中心としたConfidential Computing（秘匿計算）*5技術と，量子計算機時代に発生する高度な攻撃耐性と高い可用性を実現するエンド・ツー・エンドのネットワーク暗号化機能を中心とした耐量子セキュアトランスポート技術[3]を組み合わせることを特徴とします．

その構成では，秘匿計算環境であるTEE上の仮想マシン各々に耐量子セキュアトラ

＊3 データ主権：データの収集・保管・利用を当事者自身が制御できるという原則．組織や個人の主権的立場を反映する概念．
＊4 相互アテステーション：システム間でお互いに正当な状態であることを検証し合う仕組み．信頼実行環境（TEE）を活用します．
＊5 Confidential Computing：実行中のデータを保護するための計算技術．主にCPU内の隔離領域（TEE）で処理を行います．

ンスポート技術を用いたネットワーク接続機能を実装することで，秘匿計算空間どうしを耐量子セキュアなネットワークで保護します．これにより，別々に設置された複数の秘匿計算環境の間を通信レベルで安全に接続できます．Confidential Remote CPU/GPU技術は，例えば分散データセンタ構想に基づき，高速大容量低遅延を特徴とするIOWN（Innovative Optical and Wireless Network）APN（All-Photonics Network）で相互接続された複数のデータセンタ上に遍在する複数の秘匿計算空間を仮想的に統合し，単一の大規模な秘匿計算空間として活用することが考えられます．

今後，AIにおけるモデル生成などを中心に，現在よりはるかに多くのデータを，現在よりはるかに高度な計算環境で処理し，新たなデータを生成することにより，活用する需要が高まることが想定されます．今回紹介した2つの技術を軸とするデジタル情報の利活用に関する技術の社会実装を進捗させることで，NTTではデータ主権が担保された高度かつセキュアなデジタル情報の利活用の実現をめざしていきます．

デジタル情報を安全に活用する

デジタル情報を社会全体で共有できれば，より豊かな「共有知」を創出することができます．しかしその際には，プライバシーや機密性といった課題を同時に克服する必要があります．

私たちは，秘密計算*6，連合学習，セキュアマッチングなどの先端的な技術を活用し，情報を「見せずに使う」ことを可能にする仕組みを開発しています．

情報を「見せずに使う」社会では，あらゆる情報が常に暗号化された状態で安全に流通し，個人や組織が信頼や同意に依存せずとも情報提供や分析を行うことが可能です．そういった社会をめざし，実現のための仕組みとして新しい情報流通基盤の確立を進めていきます．この理想的な社会では，情報の利用過程においても情報の機密性や提供者のプライバシーが技術的に担保されるため，安心して知見を共有し，豊かな共有知の創出が可能になります．

現在，情報の安全性は法制度によって支えられており，個人情報保護法をはじめとする法律では安全性を守るため，機微情報の取り扱いにおいて利用目的の明確化や本人同意の取得，安全管理措置の徹底などが実施されています．しかし，情報提供者の同意取得や組織内部での管理・監査対応などには多大なコストと手間がかかり，特に複数組織間でのデータ連携や広域な分析においては利活用の大きな障壁となっています．

こうした課題を克服するため，技術的手段によって制度が求める安全性を担保・補完しようとする動きが推進されています．法律に基づく形式的な信頼だけに頼るのではなく，そもそも漏洩のリスクが生じないような安全性を実現しようとするアプローチです．しかし，こうした情報社会の理想形をすぐに実現することは困難であり，法的枠組みの整備，社会的な受容性の獲得，そして高い計算コストを伴う先進技術の実装など，まだまだ時間と段階的な進展が必要です．

その中で，統計情報の利活用は，比較的早期に技術的実装が進みつつある分野の1つです．特に個人情報を識別できないかたちに加工し，分析や意思決定へ活用する事例に対しては，法制度に準拠したうえでの技術の社会実装が現実味を帯びてきています．

このような段階的実現の第一歩として，いくつかの実装可能な技術として秘密計算などが注目されています．

秘密計算などの技術は，データを見せずに処理することを実現しており，統計処理やAI活用において法的・倫理的リスクを最小化する鍵となる技術です．今後は，これら技術の高度化とともに，制度，社会側の理解と信頼の醸成が不可欠です．

デジタル価値社会の実現に向けて

医療機関や自治体，交通事業者がデータを掛け合わせることで，病気の早期発見，渋滞の予測・緩和，フードロスの削減といった高度な社会最適化が実現します．

私たちは，「人と人」「人と地域」が信頼に基づいてつながる，“分かり合える社会”の実現をめざし，信頼ある情報流通の仕組みに関する研究を進めています．日本を真のデジタル立国とする「デジタル価値社会」，すべての人が自らの情報を活かし価値ある選択ができる社会――それが私たちのめざす「個人起点の情報流通」の姿です．

■参考文献

(1) https://www.rd.ntt/sil/project/iown-pets/iown-pets.html
(2) 鈴木・横関：“IOWN時代のデータ流通を実現するデータガバナンス”，NTT技術ジャーナル，Vol. 34，No.2，pp.36-40，2023.
(3) https://www.rd.ntt/iown_tech/post_52.html

（上段左から）横関 大子郎／ 藤村 滋／ 伊藤 宏樹
（下段左から）田中 政志／ 張 一凡

誰もが自らの情報を安心して活用できる社会をめざし，NTTはデータの信頼性確保・データ保護の実現・安全な活用による情報流通の信頼性・安全性・利便性の提供をめざしていきます．本稿を通じ，実現の方向性と意義を感じ取っていただければ幸いです．

◆問い合わせ先

NTT社会情報研究所
社会情報流通研究プロジェクト

＊6 秘密計算：データを暗号化したまま処理を行う技術で，第三者に中身を知られることなく分析や演算を可能にするプライバシー保護の技術．