安心・安全な価値創造プロセスを実現するデータ流通・利活用技術

Society 5.0の実現には組織や業種・業界を超えたデータの利活用が必須ですが，期待されるほどには行われていません．本稿では，その障壁となっているデータ授受に伴うリスクとその原因について概説します．そして，この問題の解決に向けたNTTのセキュリティR&Dの取り組みとして，「データ処理の管理・制御」というデータ流通の新しいパラダイムと，これを実現するために研究開発中のプラットフォームや要素技術を紹介します．

鷲尾 知暁（わしお ともあき）
森田 哲之（もりた てつし）
森村 一雄（もりむら かずお）
折目 吉範（おりめ よしのり）
千田 浩司（ちだ こうじ）
大嶋 嘉人（おおしま よしひと）
NTTセキュアプラットフォーム研究所

Society 5.0とクロスドメインデータ流通

経済発展と社会的課題の解決を両立した将来の社会像として，サイバー空間とフィジカル空間とを高度に融合させたシステム「Society 5.0」が提唱され[(1)]，その実現に向けた取り組みが盛んに行われています．Society 5.0では，さまざまなデータを駆使することで現状認識や課題発見，未来予測や最適解導出などが可能となり，それらが経済の発展と社会的課題の解決をもたらすとされています．言い換えると，組織や業種・業界を超えたデータの利活用（これをクロスドメインデータ流通と呼ぶことにします）が活発に行われることがSociety 5.0の生命線であるといえます．

クロスドメインデータ流通を阻む障壁とその原因

しかし，クロスドメインデータ流通，特に，機密性や希少性の高いデータの流通は，思うほどには進んでいません．その最大の障壁は，データ提供者とデータ利用者の双方に存在するリスクです．

データ提供者は，提供したデータが漏洩してしまったり，予期せぬ方法で利用されて自らや第三者に損害を与えたりするリスクを負います．一方のデータ利用者は，提供されたデータの守秘管理に伴うリスクや，提供されたデータの適法性に関するリスクを負います．

別の観点では，データ利用者は提供されたデータが従前期待していたような結果や価値を生み出さなかったり，データの提供に伴い課せられた条件（例えば，支払う対価）に見合わなかったりするリスクを負います．一方のデータ提供者は，提供したデータが想定以上の価値を生み出す（受領する対価が過小である）リスクを負いますし，逆に想定した価値を生み出さないことでデータ提供の目的（例えば，得られた結果の共有や社会への還元など）が果たされない場合があります．

上記のリスクが生じる根本的な原因は，従来のデータ流通の方法がデータそのものを渡してしまう・受け取ってしまうものであったことにあります．データは使い方次第でさまざまな価値や問題を生み出す可能性があり，それらすべてをあらかじめ見定めることは困難です．このような不透明性や不確実性が存在していては，クロスドメインデータ流通が活発に行われるはずがありません．

データ処理の管理・制御という新たなパラダイムへ

この問題を解決するには，データそのものを授受してしまう「データ参照の管理・制御」という従来のパラダイムから，「データ処理の管理・制御」という新たなパラダイムにシフトすることが必要です．この新たなパラダイムでは，データ最小化の原則に則り，データそのものではなくデータに対して合意した（データ利用者が望み，データ提供者が認めた）処理を行った結果のみをデータ利用者に渡します．こうすることで，そのデータ利用で生じ得

る価値も問題も限定的で予見しやすくなり，前述したリスクも大きく低減されるのです（**図1**）．

クロスドメインデータ流通プラットフォームの概観

私たちは，上記の新パラダイムに基づいた，信頼できる*1クロスドメインデータ流通のプラットフォームを実現し，そこに参画するあらゆるデータ提供者・利用者があらゆるデータを安心して共有し利活用できるようにすることをめざしています．同プラットフォームの主要な要件には，①データを保護しつつ必要な処理を加えられること，②データの提供者と利用者の合意内容や法に従ってデータ処理を制御できること，③扱うデータやその処理について透明性を確保すること，の3点があります（**表**）．

このプラットフォームは以下の3つの機構から構成されます（**図2**）．

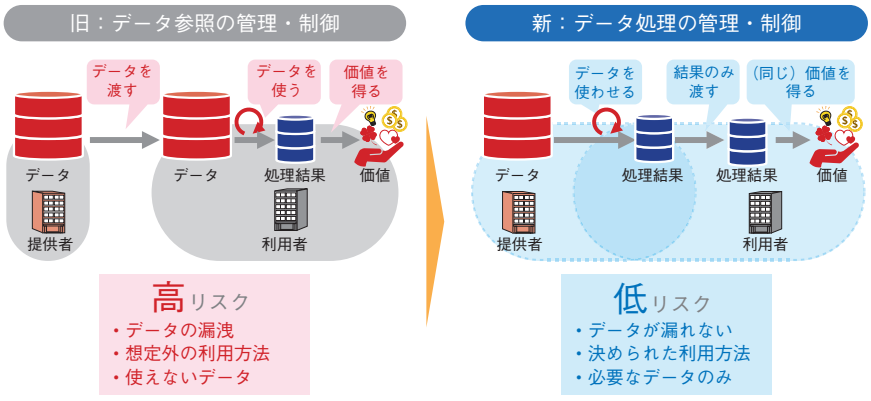

図1　データ流通方法のパラダイムシフト

表　クロスドメインデータ流通プラットフォームの主要要件

区分	主な要件
データの保管と処理の保護	データについて，その機密性や完全性を高度に保ちながら，利用者が望むさまざまな分析・加工等の処理を実行できること
	データ処理の結果（派生データ）についても，上記のように扱えること
	プラットフォームの運用者であってもデータや派生データを参照したり書き換えたりできないこと
データ処理権の管理と制御	提供者と利用者が合意したデータ処理のみを実行すること
	対象のデータや派生データに応じて必要な法（個人情報保護法など）に適合した処理のみを実行すること
	処理にかかわるデータ提供者や利用者，対象データなどについて正確かつ詳細に把握したうえで実行の可否を判断すること
データやデータ処理の透明性確保	データや派生データの特徴や出自について，データ利用者が確認できるようにすること
	データや派生データに対して実行された処理の事実や履歴について，データ提供者やデータ利用者が確認できるようにすること
	データの保管や処理にかかわるプラットフォームの動作について，データ提供者や利用者が確認できるようにすること

(1)　データ保護・活用機構

・　データ（派生データ*2を含みます．以下同様）を秘匿したまま，データ利用者が必要とするさまざまな分析・加工等の処理を実行します．

・　認可機構が許可した処理のみが許可したとおりに実行されることを保証し，また，処理の事実や履歴，派生データの出自を証明します．

(2)　データ処理認可機構

・　データ保護・活用機構へのデータ処理の要求について，データ提供者が定めたデータ利用ポリシー*3やデータの提供者と利用者とが合意した内容に従い，また，適法性も加味し，その実行の可否を判断します．

・　データの提供者や利用者，あるいは，対象データについて，トラストデータ管理機構からの情報を基に正確かつ詳細に確認したうえで可否を判断します．

(3)　トラストデータ管理機構

・　データの提供者や利用者，あるいは，対象データに関する属性（トラストデータ）を管理し，認可機

＊1　信頼できる（プラットフォーム）：データの提供者や利用者が期待するとおりに動作し，その役割を的確に果たしていることをプラットフォーム自らが示し，データの提供者や利用者からの信頼を獲得できるものであることを指します．

＊2　派生データ：データ提供者からプラットフォームに託されたデータを処理した結果を指します．派生データを処理した結果も含みます．

＊3　データ利用ポリシー：どのようなデータ利用を許すか・許さないかをあらかじめ規定したもの．対象のデータ，利用を要求する主体，利用の内容（データ処理の方法）などを用いて認可対象を指定し，それに対して許可・不許可や，許可時に満たすべき条件などを定めます．

※データの検索やマッチング，課金や決済などの機能は省略しています．

図２　クロスドメインデータ流通プラットフォームのアーキテクチャ

構や必要とする者に提供します．

・　データ保護・活用機構によるデータ処理の事実や履歴，派生データの出自を証明する情報もトラストデータとして管理し，必要とする者に提供します．

クロスドメインデータ流通の要素技術

前述の各機構を実現する要素技術のうち主要なものについて，その概要を以下に示します．

■秘密計算技術

秘密計算技術は，データを暗号化したまま一切復号することなく計算できる技術です．これにより，プライバシにかかわる情報や企業の機密情報など機微なデータの安全な利活用が可能となります．また，他組織に開示することが難しいデータを持ち寄った分析が可能となり，分析対象データの種類や量の増加による新たな価値の引き出しが可能になると期待されます．秘密計算技術では安全性はもちろん，処理の性能と多様性が重要です．NTTセキュアプラットフォーム研究所はこれまで，世界最高速レベルでの統計処理が可能な秘密計算システムを実用化しました[(2)]．現在はディープラーニングの学習や予測を暗号化したまま行える秘密計算AI（人工知能）技術の開発を進めており[(3)]，画像データなど大規模データを扱うためのさらなる高速化，必要とされるAIアルゴリズムの拡充などに取り組んでいます．

■データ処理機密性・真正性保証技術

クロスドメインデータ流通ではさまざまなステークホルダの計算環境でデータが処理されるため，データのアクセス制御（機密性を保証すること）やデータ処理結果の真正性を保証することは容易ではありません．しかし前述のとおり，クロスドメインデータ流通プラットフォームが信頼され，広く利用されるにはこれらの要件を満たすことが必要です．具体的には，①提供データが許可された範囲でのみ利用されているかをデータ提供者が確認可能であること，②データ処理結果が要求どおりの正しい結果であるかをデータ利用者が確認可能であること，の２つの要件が特に重要と考えています．私たちはこれら要件を実現するため，TEE（Trusted Execution Environment）と呼ばれるセキュアな実行環境[(4)]を援用した安全な処理手続き（プロトコル）の確立に取り組んでいます．

■属性ベース認可技術

プラットフォームには大量のデータが次々と登録されますし，登録されたデータを誰が利用しようとするのか事前には分かりません．そのため，データ利用ポリシーを「どのような属性を持つデータをどのような属性を持つ主体が利用できるか」というかたちで規定しておき，認可判断の際にはそこに対象データやデータ利用者の属性値を当てはめて評価する，属性ベースの認可が有効です．例えば，データ利用者が有する資格（例：ISMS認証，Pマーク認証）を必要な属性としてデータ利用ポリシーで指定するといったことです．

属性ベースの認可自体は新しい考え方ではありませんが，後述するように適法性を考慮した認可判断を行うには，データ利用ポリシーにかかわらず，データの特性に応じて所定の属性の有無や値を確認して判断することなどが必要です．また，誤った認可判断を回避するために，データ利用ポリシーで指定された属性の有無およびその真正性（第三者機関による証明有無など）を厳格に判断することが必要です．さらに，データ利用の認可判断においては，許可・不許可の二値だけではなく条件付きで許可するなどの柔軟性も必要と考えています．例えば，要求され

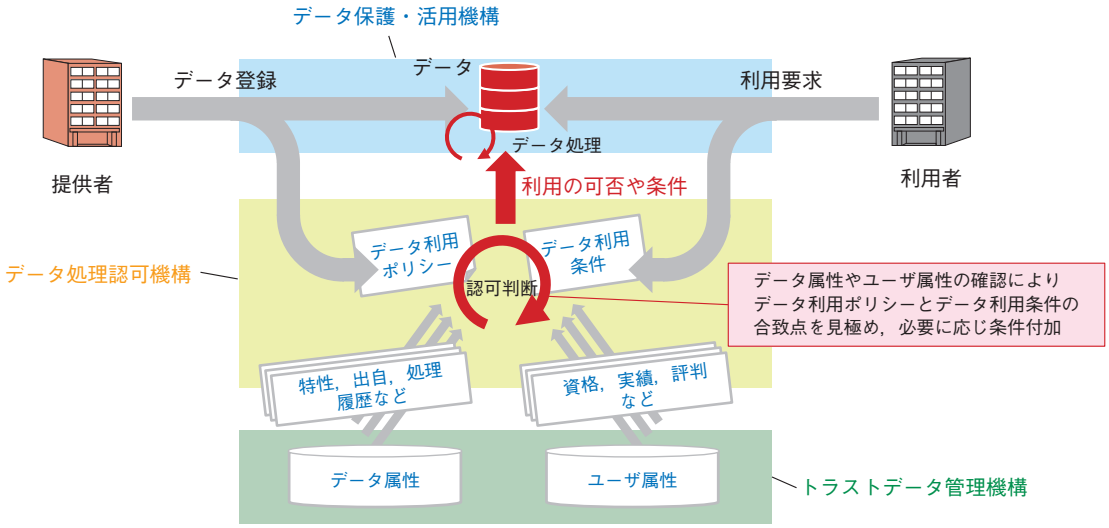

図 3　属性ベースの認可判断

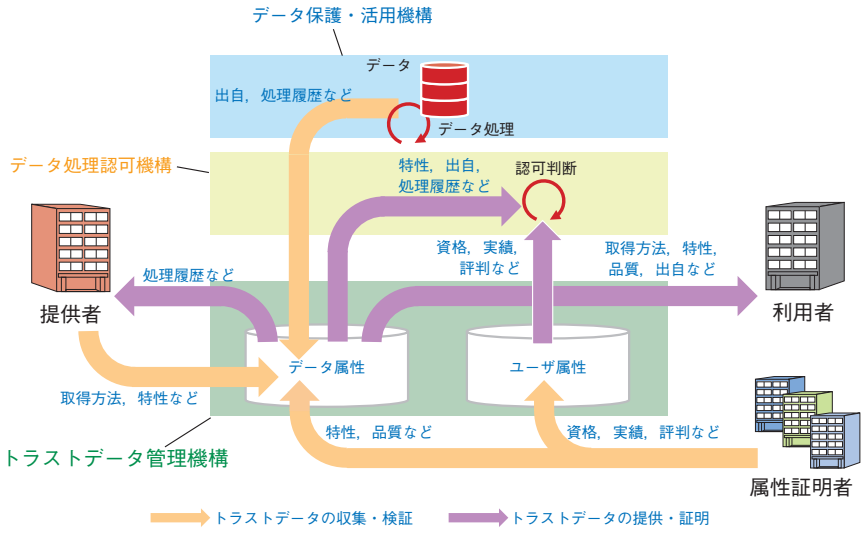

図 4　トラストデータの流れ

たデータそのものの利用は認められないが，匿名加工したものであれば許可するなどです．データの提供者と利用者の双方の要求を調整しながら柔軟な認可判断を行うことで，データの流通機会の拡大に資すると考えています（**図 3**）．

■トラストデータ管理技術

トラストデータ管理機構は，データの提供者や利用者などプラットフォームのユーザの属性（資格や実績，評判など）や，プラットフォームで扱われるデータの属性（種別，項目，収集方法などのデータ特性や，出自，処理履歴など）を収集，管理し，ユーザやデータがどのようなものであるかを確認する際の信頼の拠り所となる情報「トラストデータ」としてデータ処理認可機構やデータ提供者・利用者などに提供します（**図 4**）．

トラストデータは信頼の拠り所となるため，その確からしさを保証できる多様な主体により証明されていることや，その内容の正しさを検証できるようにする必要があります．一方で，トラストデータ自体が機密性を持つ場合もあり，いつ・誰に・どの部分までを開示して良いかを適切に判断する必要があります．さらに，必要とするときにいつでも利用できる可用性も求められます．これらさまざまな要求にこたえるトラストデータ管理技術とその仕組みを実現していきます．

■トラストデータと認可判断における法的要求事項の実装

データの提供者や利用者は，授受するデータに関する適法性についても配慮しなくてはなりません．データがどのように取得されたかをデータ利用者が把握することは難しく，違法に取得されたデータが紛れていても気付けない可能性があります．また，個人情報

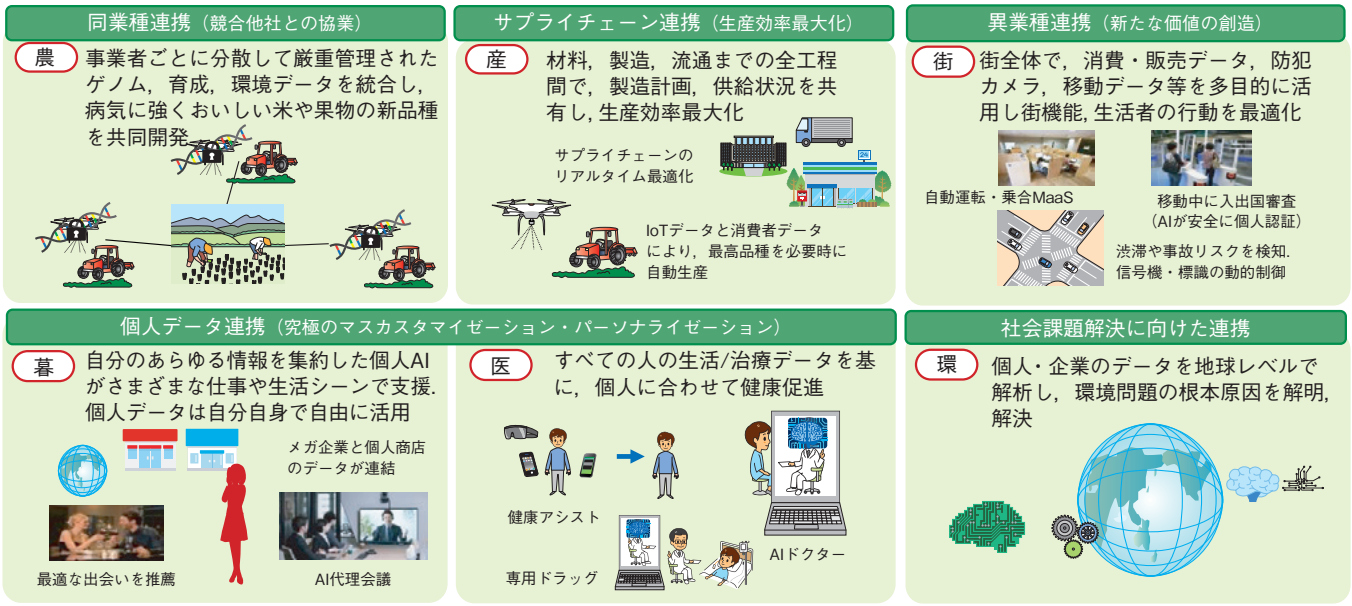

図 5　クロスドメインデータ流通が実現する世界

にあたるデータについては，取得時に本人に示した利用目的の範囲外で使用することや，本人の同意を得ずに第三者へ提供することなどが個人情報保護法で禁じられており，これを守るためにデータの提供者も利用者も多くの注意を払う必要があります．

このような適法性への配慮の負担を軽減するため，データと合わせて法的要求事項を実装した属性データを付与し，トラストデータとして管理し認可判断の際に確認する方法についても検討しています．

今後に向けて

信頼できるクロスドメインデータ流通プラットフォームにより，これまで困難だった同業種・異業種間での協業や連携が加速され，新たな価値の創造や大きな社会課題の解決が可能になると考えています（**図 5**）．

その実現に向け，私たちは，要素技術の研究開発だけではなく，クロスドメインデータ流通を志向するパートナーと連携した仮説検証や，国際標準化活動，社会受容性の確保に向けた活動などを加速していきます．

■参考文献

(1) https://www8.cao.go.jp/cstp/society5_0/
(2) https://www.ntt.co.jp/news2018/1808/180808a.html
(3) https://www.ntt.co.jp/news2019/1909/190902a.html
(4) https://globalplatform.org/specs-library/?filter-committee=tee

（上段左から）鷲尾 知暁／ 折目 吉範／ 森田 哲之
（下段左から）千田 浩司／ 森村 一雄／ 大嶋 嘉人

私たちは，本稿で紹介したクロスドメインデータ流通プラットフォームの研究開発を通じてIOWN上に新たな価値創造のプロセスを構築し，Society 5.0/Smart Worldの実現に貢献していきます．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
E-mail　scpflab＠hco.ntt.co.jp