2.4.6 データ・コンテンツのデジタルトラスト

（1）研究開発領域の定義

サイバー空間とフィジカル空間を高度に融合したシステムによるSociety5.0では、データは価値の源泉である。本領域は、データを扱う人やモノの真正性やデータの非改ざん性に関する信頼性を保証する研究開発を行う。

（2）キーワード

デジタルトラスト、トラストサービス、デジタルアイデンティティー、デジタル署名、電子署名、タイムスタンプ、eシール、eデリバリー、eIDAS（electronic Identification and Authentication Service）規則、FICAM（Federal Identity, Credential and Access Management）

（3）研究開発領域の概要

［本領域の意義］

サイバー空間とフィジカル空間を高度に融合したシステムによるSociety5.0の中核となるデータ駆動型社会では、人だけでなく、モノもインターネットに繋がる。そこで得られた膨大なデータは価値の源泉となるものであり、社会で活用し、社会問題の解決や経済の発展に寄与することが期待されている。一方で、このデータを扱う人やモノのなりすましや、データの改ざんが行われると、データの価値が失われることに繋がる。また、急速な情報化社会に伴う市民活動、経済活動、行政活動のデジタル・トランスフォーメーション（DX）は、人々にさまざまな恩恵を与えており、例えば、マイナンバーカードは、コンビニエンスストアでの各種行政証明書の取得やe-Taxによる確定申告、健康保険証としても利用することが可能であり、その利便性が拡大している。一方で、マイナンバーカードの所有者本人以外による利用や、データの改ざんは、利用者に不安や不信を与えるだけでなく犯罪にも繋がる。このため、データ駆動型社会の発展やDXの推進のためには、データを扱う人やモノの真正性（本人、本物であること）や、データの非改ざん性を保証することが非常に重要である。このように、Society5.0におけるデータ駆動型社会やDXを推進していく上で、基礎となる人やモノの真正性やデータ・コンテンツの非改ざん性を保証するデータ・コンテンツのデジタルトラストは、今後のデジタル社会の発展に必要不可欠なものである。

［研究開発の動向］

米国の心理学者であるデニース・ルソーは「他者の意図または行動に対する肯定的な期待に基づいて脆弱性を受け入れる意図からなる心理的状態」とトラストを定義している[1)]。このようにトラストとは、個人の心理状態を示す言葉であり、データやコンテンツをトラストするかどうかは、個人の主観的な判断によるものである。その判断要因の一つとなるものが、人やモノが本人・本物であること、扱うデータ・コンテンツが改ざんされていないことを保証するデータ・コンテンツのデジタルトラストと考えることができる。

データ・コンテンツのデジタルトラストは、一般には、「トラストサービス」と呼ばれており、データ・コンテンツと個人、組織との結び付きを技術的・法的に保証する形でそのトラストを確立している。トラストサービスは、2016年に欧州で施行されたeIDAS規則[2)]で初めて定義され、トラストサービスの法的要件、技術的要件、第三者評価の枠組みが整備された。 eIDAS規則では、トラストサービスとして、電子署名、タイムスタンプ、eシール、eデリバリーなどを定義している。技術的要件については、技術的中立性の観点から排他的に示されていないものの、現在、採用されている実装のための技術基準では、デジタル署名技術がベースとなっている。その後、トラストサービスは、国際規格ISO/IEC 27099[3)]などでも扱われている。

日本におけるトラストサービスとしては、平成12年に電子署名に係わる「電子署名及び認証業務に関する法律（平成十二年法律第百二号）」[4)]が公布され、令和3年にはタイムスタンプに係わる「時刻認証業務の認

定に関する規程（令和３年総務省告示第146号）」[5]、eシールに係わる「eシールに係る指針（令和３年６月25日）」[6] が公布されている。

電子署名は、データ・コンテンツと個人の結びつきを保証する仕組みであり、「電子署名及び認証業務に関する法律」では、公開鍵暗号を用いたデジタル署名方式の電子署名を定義している。タイムスタンプは、データ・コンテンツと時刻の結びつきを保証する仕組みであり、技術的には複数の方式があるものの、デジタル署名方式に基づくタイムスタンプが主流である。現在、一般財団法人日本データ通信協議会が運営するタイムビジネス認定センターによる認定を取得しているタイムスタンプサービスは全てデジタル署名方式である[7]。eシールは、電子署名と対比して、自然人ではなく、法人および組織とデータ・コンテンツの結びつきを保証する仕組みであり、電子署名と同様にデジタル署名方式が主流である。eシールについては現在のところ総務省指針が示されているに留まっており、引き続き制度化が期待されている。その他のトラストサービスとしては、送受信者の識別と、送受信日時の正確性、送受信データの非改ざん性などを保証するeデリバリーなどがある。

これらのトラストサービスは、すでにさまざまな用途で利用されており、今後もその利用範囲の拡大が予想される。例えば、2020年に内閣府の規制改革推進会議において、書面、押印、対面の必要性の見直しが行われ、電子署名などのトラストサービスを活用することで、必要な手続きの「デジタル完結」を目指す取り組みが進められている[8]。また、マイナンバーカードの交付率は60%を超え（2023年２月末時点）、健康保険証とマイナンバーカードを一体にした「マイナ保険証」や運転免許証とマイナンバーカードとの一体化も計画されている。デジタル庁においては、マイナンバーカードの機能をスマートフォンに搭載する検討もされており、利用者が便利に利用できる環境整備が進められている。さらに、国際的な信頼性のある自由なデータ流通の促進を目指すDFFT（Data Free Flow with Trust：信頼性のある自由なデータ流通）や、人に加えてモノもインターネットにつながるIoT（Internet of Things）でも、モノのなりすましやデータの改ざんを防ぎ、データの信頼性を保証するトラストサービスが必要不可欠である。このようにトラストサービスは、今後もその用途が拡大していくことが予想されている。その構築に際しては、技術的な仕組みに加えて、法的な保証を与える制度上の仕組みを整備することが重要となる。また、システムの観点からは、利用する人にとってユーザーエクスペリエンス（UX：User Experience）に優れた設計であることや、大量のデータを効率的に検証するためにアプリケーションが自動的にデータやコンテンツの信頼性を検証できることが必要である。

国内では、今後のトラストサービスの拡大を踏まえその具体的な推進方策を検討するために「データ戦略推進ワーキンググループ 」の下に令和３年10月に「トラストを確保したDX 推進サブワーキンググループ」が設置された（「データ戦略推進ワーキンググループの開催について」（令和３年９月デジタル社会推進会議議長決定）第４項の規定に基づく）。そこでは、トラストサービスが担保する範囲、トラスト確保のニーズおよび課題の洗い出しと検討が行われ、10項目のトラストサービスの基本方針や今後の取り組みがまとめられた[9]。

欧州では、2016年７月に施行されたeIDAS規則に続き、eIDAS規則の改正案（eIDAS2.0[1]）[10] が検討されている。米国では、FICAM（Federal Identity, Credential and Access Management）[11] が導入され、政府情報システムにアクセスする政府職員および個人に対して当該情報システムのリスク評価に応じたクレデンシャル[2]が発行され、データへのアクセス管理が導入されている。また、連邦政府職員向けの身分証であるPIV（Personal Identity Verification）カードでは、電子政府法に基づいて整備された連邦PKI（FPKI：Federal Public Key Infrastructure）から発行されるPIV証明書が利用され、本人のなりすましを防止している。FPKIはブリッジ認証局を通じて民間の認証局とも相互接続しており、民間の航空宇宙・防衛・医薬品業界などにおいて、政府基準と同等かつ相互運用性が保証された技術の実装が進められている。

このように、データ・コンテンツのデジタルトラスト（トラストサービス）は、さまざまな用途、分野で、そ

1 詳細は「2.4.6（4）注目動向［注目すべき国内外のプロジェクト］❶欧州・eIDAS規則改正案（eIDAS2.0）」を参照いただきたい。

2 システムにアクセスするための認証情報であり、例えば、IDとパスワード、証明書、ワンタイムパスワードなど。

の利用が拡大しており重要性が高まっている。

（4）注目動向

［新展開・技術トピックス］

❶ デジタルアイデンティティーウォレット

デジタルアイデンティティーウォレットは、多様なクレデンシャルをスマートフォンのアプリケーションで管理できるようにするサービスの機能である。欧州では、eIDAS規則の改正案（eIDAS2.0）において、欧州加盟各国にEUデジタルアイデンティティーウォレット（EUDIW：EU Digital Identity Wallet）の整備と国民への配布を義務付け、全欧州市民が安全・安心なオンライン認証を利用できるようにすることを目標にしている。また、AppleやGoogleはすでにウォレットアプリを実装しており、米国の一部州においては、運転免許証や州IDをスマートフォンのウォレットアプリで管理することが可能となっている。国際標準規格ISO/IEC 18013–5では、スマートフォンで運転免許証機能を実現するために必要となるインターフェース仕様および関連要件が定義されており、上記Appleのウォレットアプリはこの規格に準拠している。

❷ 自己主権型アイデンティティー（SSI）と分散型識別子（DID）、ヴェリファイアブルクレデンシャル（VC）

自己主権型アイデンティティー（SSI：Self–Sovereign Identity）は、中央集権的な管理主体が個人のデジタルアイデンティティーを管理するのではなく、個人が自らデジタルアイデンティティーを管理する新しい概念である。分散型識別子（DID：Decentralized Identity）とヴェリファイアブルクレデンシャル（VC：Verifiable Credential）は、SSIを実現する一つの方法である。 DIDは、アイデンティティーの登録・検証に分散型台帳であるブロックチェーンの仕組みを用いたアイデンティティーの管理方式であり、W3C（World Wide Web Consortium）やDIF（Decentralized Identity Foundation）において標準化が進められている。 VCは、例えば、個人の氏名、年齢、住所、運転免許証、学位証、資格証明書などの属性情報である。VCは、それぞれの情報に対応する発行者によって発行されるため、非中央集権的なクレデンシャル発行の方式として注目されている。 DIDとVCを利用することで、第三者が相手のアイデンティティーや提示された属性情報を検証することができる。

［注目すべき国内外のプロジェクト］

❶ 欧州・eIDAS規則改正案（eIDAS2.0）

eIDAS規則は、欧州の電子署名指令の枠組みを拡大し、トラストサービスの法的効力と要件、監査の枠組みを規定している。 eIDAS規則では、電子署名以外のタイムスタンプ、eシール、e デリバリーなどのトラストサービスについても法的効力が定められ、加盟国間における相互承認の枠組みも整備された。eIDAS規則では4年ごとのレビュープロセスが定められており、レビュー結果に基づいた改正案（eIDAS2.0）が現在、提案されている。eIDAS2.0では、金融、医療、旅行などの業界特有のニーズや新しい技術動向を元にトラストサービスの拡大が提案されており、新たに、電子台帳（分散台帳）、属性（資格、学位、年齢など）の証明、電子アーカイブ、リモート署名などが追加されている。また、EU市民のデジタルアイデンティティーに関する新たな枠組みとしてEUデジタルアイデンティティーウォレット（EUDIW）が提案されている。

❷ トラストを確保したDX推進サブワーキンググループ（デジタル庁）

日本ではトラストを確保したデジタルトランスフォーメーションの具体的な推進施策を検討するために、令和3年10月に「トラストを確保したDX推進サブワーキンググループ」が設置された。このワーキンググループでは、デジタル社会の実現に向けた重点計画（令和３年12月24日閣議決定）の「包括的データ戦略」に関する具体的な施策の中で示されている「令和４年度を目途にトラストを確保する枠組みの基本的な考え

方（トラストポリシー）を取りまとめる」ことを目的としている。トラスト確保の実態調査や有識者ヒアリングを通じたトラストに関するニーズと導入課題の洗い出し、実態調査に基づいたトラスト確保の検討、今後のトラスト実装ユースケースとその推進体制が検討された。令和４年７月に「トラストを確保したDX推進サブワーキンググループ報告書」がまとめられ、トラストポリシーの基本方針や今後の推進体制などが示されている。

❸ 戦略的イノベーション創造プログラム（SIP）第２期「分野間データ連携基盤」（内閣府）

内閣府の戦略的イノベーション創造プログラム（SIP）第２期の「分野間データ連携基盤開発」では、業界を超えたデータ連携の仕組みの構築を推進している。データ連携には、必要なデータの検索とデータの交換ができる仕組みが必要であり、その仕組みとして「分散型データ交換のためのコネクタ・アーキテクチャ（CADDE：Connector Architecture for Decentralized Data Exchange）」が開発されている。CADDEでは、コネクターと呼ばれるデータ交換の窓口を介してデータの交換を実現しており、データ提供者とデータ利用者のコネクター間では、必要に応じて認証認可、契約管理、検索などの機能を利用することができる。データ提供者がデータ利用者に情報を提供する際、なりすまし防止、改ざん防止を保証するために、リモート署名型の電子署名サービスを利用するデジタルトラスト基盤が開発されており、欧州のトラストサービスとの相互運用性を保証するために日欧間での相互運用性の実証実験も進められている。その中では、相互接続に必要なデジタルトラスト基盤の要件の作成や欧州と同等のリモート署名の実装、および検証などが行われている。

❹ 欧州・GAIA-Xプロジェクト

ドイツとフランスのGAIA-Xプロジェクト[12)]は、データ連携基盤の構築を通じてデータ主権とイノベーションを促進することを目的としたプロジェクトである。データの所有者がデータに対する完全な主権を保持したまま、信頼できる環境でデータ交換ができるデジタルエコシステムの確立を目指している。 GAIA-Xでは、業界ごとのデータやAI、IoT、データ分析などのデータに関する「データエコシステム」と、クラウドサービスやネットワークサービスプロバイダーからなるインフラに関する「インフラエコシステム」とがGAIA-X Federation Services（GXFS）を通じて連携している。また、データやサービスをVC（Verifiable Credential）をベースとした自己記述（Self-Description）と呼ばれる形式で定義し、eIDAS規則におけるトラステッドリスト（検証可能なトラストサービスのリスト）を用いてデータ連携時にデータの提供者やデータ、サービスの信頼性を保証する仕組みが検討されている。

（5）科学技術的課題

ここでは「（3）研究開発領域の概要、（4）注目動向」に関する科学技術的課題を紹介する。

❶ トラストサービスのポリシー

トラストサービスを社会で利用していくためには、そのサービスが社会的に信頼できることが必要である。そのためには、トラストサービスを「法的背景」、「監督と監査」、「技術基準」および「トラストリプレゼンテーション」の４つの観点から構築する必要がある。法的背景は、トラストサービスに関する法的枠組みを指しており、トラストサービスの効果や要件に関する法律上や契約上の規則となる。監督と監査は、トラストサービスが法的背景で要求されている要件を充足していることを保証するための制度を指し、技術基準は、法的背景で定められている要件の確認に用いる技術基準を指す。トラストリプレゼンテーションは、トラストサービスが法的背景で位置付けられたトラストサービスであることを検証するための仕組みである。欧州ではeIDAS規則を通じて法的背景の側面からトラストサービスを定義して、その技術基準と、監督と監査の制度を整備し、トラステッドリスト（トラストサービスのリスト）を用いて法的に有効なトラストサービス

であるか否かを技術的に検証可能とすることにより、社会的に信頼できるトラストサービスを実現している。日本ではトラストサービスの信頼性に対する画一的な基準が設けられておらず、「トラストを確保したDX推進サブワーキンググループ」でトラストポリシーの基本方針が整理されたが、今後、技術的な側面も含めて、上記の4つの観点から具体的なトラストポリシーを策定することが必要である。

❷ トラストサービスの国際的通用性の確立

国際的な信頼のある自由なデータ流通（DFFT：Data Free Flow with Trust）を実現するためには、トラストサービスの国際的通用性が求められる。国際的通用性では、法制度、技術基準、監督・監査の仕組みおよび、トラストレプレゼンテーション（信頼できるトラストサービスであることを検証できる仕組み）について、その同等性を国家間の合意、あるいは企業間で相互承認することが求められる。欧州では、eIDAS規則第14条に基づく相互承認の枠組みが設けられており、その技術的な実装についてもCEF（Connecting Europe Facilities）プロジェクトの「eSignature Building Block」において研究開発が行われている。米国では、連邦PKIのブリッジ認証局と他国の認証局を相互認証する仕組みが導入されており、他国との相互接続が可能になっている。日本でも、他国とのデータ流通のためにはトラストサービスの国際的通用性が求められるため、今後、技術基準や制度設計を行う際には、他国の基準・制度との同等性を考慮して検討することが必要である。

❸ トラストサービスの保証レベルの確立

トラストサービスを行政サービスや生活サービスで広く利用していくためには、トラストサービスがどのレベルの信頼性を持つのかを示す保証レベルの確立が必要である。デジタルアイデンティティーの保証レベルは、NIST SP 800–63や、eIDAS規則、ISO/IEC 29115などで整理され、第三者評価や相互レビューなどの評価の枠組みも存在し、デジタルアイデンティティー関連製品やサービスの導入が容易な環境が整ってきている。一方で、トラストサービスの保証レベルについては十分な整理が行われておらず、今後、トラストサービスを活用していくためには、トラストサービス自体の保証レベル、およびトラストサービスの保証レベルとデジタルアイデンティティーの保証レベルとの関係性について検討が必要である。

（6）その他の課題

❶ 電子署名用秘密鍵の保護環境の検証

日本の電子署名と欧米の電子署名の違いに、デジタル署名方式における署名用秘密鍵の保護環境に関する規定がある。欧州では、手書き署名と同等の法的効果が認められる適格電子署名において、秘密鍵の安全な保護環境としてセキュリティー評価を受けたトークン（QSCD：Qualified electronic Signature / Seal Creation Device）[3]の利用を義務付けている。米国でも、連邦PKIの証明書ポリシーによってはPIV（Personal Identity Verification）カードなど、セキュリティー評価を受けた保護環境の利用が求められており、電子署名検証時にセキュリティー評価を受けた保護環境が秘密鍵の保護に利用されていたかについても検証できる。一方、日本の電子署名法では、主務大臣から認定を受ける認証業務（認定認証業務）においても、ユーザー環境下における秘密鍵の保護にセキュリティー評価を受けたトークンの利用を求めておらず、電子署名の検証時に、セキュリティー評価を受けたトークンが利用されて秘密鍵の安全性が確保されていたかを検証できない。データ駆動型社会においてミッションクリティカルな分野でデータの信頼性を保証するためには、電子署名に使われた秘密鍵の保護環境についても検証できる仕組みを構築することが必要である。

3　署名者の秘密鍵を保護し、セキュアな署名プロセスを可能にするセキュリティー評価を受けたデバイス。

❷ 適格ウェブ認証証明書の扱い

欧州ではeIDAS規則によってサーバー証明書についても法的な枠組みを整備しており、改正案であるeIDAS2.0において、適格ウェブ認証証明書（QWAC：Qualified Website Authentication Certificate）のブラウザーにおける受け入れを強制化しようとしている。従来、ブラウザーに表示されるウェブサイトの安全性などを示す情報は、接続先のサーバー証明書とブラウザーにプリインストールされている信頼できる認証局のリストに基づいて表示されている。 eIDAS2.0では、EUのトラステッドリスト（信頼できるトラストサービスのリスト）を信頼できる認証局のリストとして追加することを要求している。一方で、ブラウザーベンダーは、信頼できる認証局を自らで管理できなくなることによりセキュリティーリスクが増大することへの懸念を示している。日本においても、現状では、政府系認証局がブラウザーにプリインストールされている信頼できる認証局に含まれておらず、今後、ブラウザーベンダーに対して、認証局のリストに追加することを要求していくかの検討が必要である。また、信頼できるウェブサイトであることをブラウザーに表示するためには、WebTrust for CAと呼ばれる海外の監査制度に基づき監査を受けた民間認証局から発行されるサーバー証明書を購入することが一般的である。他国の制度やその監査を受けた民間の認証局に依存している実態の見直しにも取り組む必要がある。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・デジタルトラストの基礎研究に従事する研究者は少なく存在感も薄い。
	応用研究・開発	○	→	・SIP 第2期「分野間データ連携基盤」などの実証実験があるものの、先進的なプロジェクトは少ない。
米国	基礎研究	◎	→	・デジタルアイデンティティーの分野で世界をリードしており、リスク分析をベースとしたデジタルアイデンティティー、トラストの研究が盛んである。
	応用研究・開発	◎	→	・特に民間企業における研究・開発および実装が盛んである（Mobile Driver's License、航空機ソフトウェアの信頼性保証など）。
欧州	基礎研究	◎	→	・データ保護、プライバシー、自己主権などの研究が盛んである。
	応用研究・開発	◎	↗	・GXFS（GAIA-X Federation Services）、EUDIW（EU Digital Identity Wallet）、EBSI（European Blockchain Service Infrastructure）など、トラストを活用した先端的な仕組み、制度設計を大規模な公的予算で積極的に推進している。
中国	基礎研究	△	→	・AI、5G通信、ビッグデータおよびクラウドコンピューティングにおける基礎研究が盛んな一方で、デジタルトラストに関する研究は少ない。
	応用研究・開発	−	−	・特に目立った活動は見られない。
韓国	基礎研究	○	→	・住民登録番号に基づいたオンラインでの本人確認方法に関する基礎研究が多い。
	応用研究・開発	◎	↗	・セクターごとに多様な認証方式、デジタル署名が開発・実装されている[13)]。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1) Denise M. Rousseau, et al., “Not So Different After All: A Cross-Discipline View Of Trust,” Academy of Management Review 23, no. 3（1998）: 393-404., https://doi.org/10.5465/amr.1998.926617.
2) The European Parliament and the Council of the European Union, “REGULATION（EU）No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,” Official Journal of the European Union L257 57（2014）: 73-114.
3) ISO/IEC JTC1 SC27, “ISO/IEC 27099：2022 Information technology — Public key infrastructure — Practices and policy framework,” International Organization for Standardization（ISO）, https://www.iso.org/standard/56590.html,（2023年2月25日アクセス）.
4) 法務省「平成十二年法律第百二号：電子署名及び認証業務に関する法律」e-GOV法令検索, https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000102,（2023年2月25日アクセス）.
5) 総務省「総務省告示第百四十六号：時刻認証業務の認定に関する規程（令和三年四月一日）」https://www.soumu.go.jp/main_content/000742664.pdf,（2023年2月25日アクセス）.
6) 総務省「eシールに関する指針（令和3年6月25日）」https://www.soumu.go.jp/main_content/000756907.pdf,（2023年2月25日アクセス）.
7) 一般財団法人日本データ通信協議会 タイムビジネス認定センター「認定事業者一覧」https://www.dekyo.or.jp/tb/contents/list/index.html,（2023年2月25日アクセス）.
8) 内閣府「書面規制、押印、対面規制の見直し・電子署名の活用促進について」https://www8.cao.go.jp/kisei-kaikaku/kisei/imprint/i_index.html,（2023年2月25日アクセス）.
9) デジタル庁「トラストを確保したDX推進サブワーキンググループ報告書（令和4年（2022年）7月29日）」https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf,（2023年2月25日アクセス）.
10) European Commission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation（EU）No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final,” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281,（2023年2月25日アクセス）.
11) Federal Chief Information Officers Council and Federal Enterprise Architecture, “Federal Identity, Credential, and Access Management（FICAM）Roadmap and Implementation

Guidance, Version 2.0," U.S. General Services Administration, https://playbooks.idmanagement.gov/docs/roadmap-ficam.pdf,（2023年2月25日アクセス）.
12) GAIA-X Federation Service, "GXFS IDM & Trust: Architecture Overview," https://www.gxfs.eu/download/3397/,（2023年2月25日アクセス）.
13) Jang GyeHyun and Lim Jong-In, "CHAPTER 1: Technologies of Trust: Online Authentication and Data Access Control in Korea," in The Korean Way With Data, Carnegie Endowment for International Peace, 11-44., https://carnegieendowment.org/files/202108-KoreanWayWithData_final5.pdf,（2023年2月25日アクセス）.