

「産業DXのためのデジタルインフラ整備事業」 成果報告会

複雑かつ機微な情報を扱うデータ連携システムに関する調査

2025年4月23日

株式会社NTTデータ経営研究所

本調査事業の背景・目的

- 次のような背景・目的のもと、本調査事業を実施した

背景

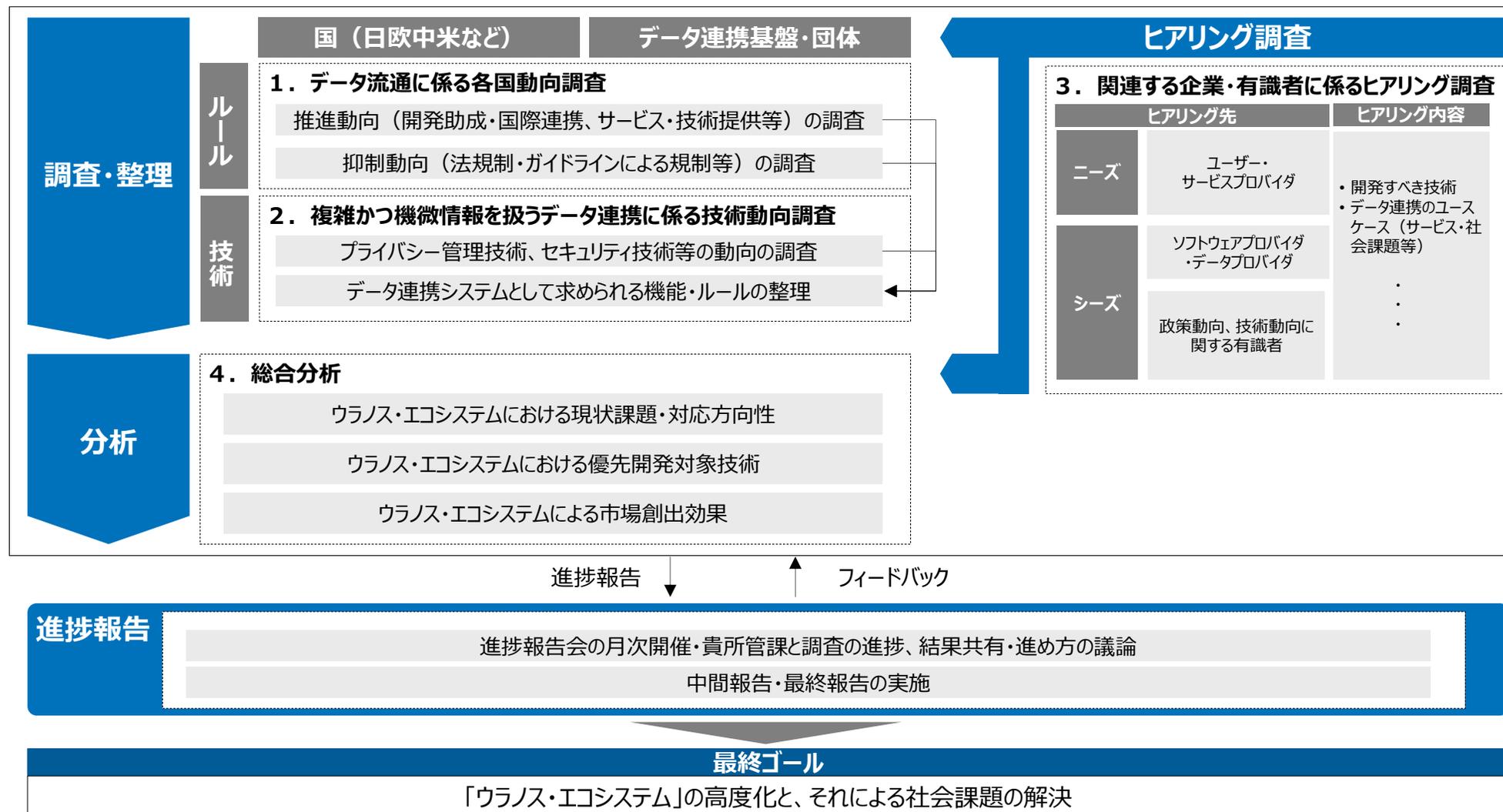
- デジタル化の急速な進展に伴い、**データの活用**は社会課題の解決や企業の付加価値創造に不可欠な要素となっており、日本は2019年に**DFFT (Data Free Flow with Trust)** というコンセプトを提唱し、WTOにおける電子商取引ルールの交渉をはじめとして関連の取組を進めてきた
- その中で経産省では、社会課題の解決に必要な、企業や業界を横断しデータを連携・活用するデータ連携に関する取組を「**ウラノス・エコシステム**」と命名し、「産業DXのためのデジタルインフラ整備事業」において、データ連携基盤の構築やそれに資するデジタルインフラの開発等を推進している
- 他方、データ連携基盤を巡る状況は複雑化しており、複数のサプライチェーンに跨るトレーサビリティ確保、自律移動ロボット等の安全な運行など、**複数のステークホルダーが相互に連携**してシステムの運用を行う必要がある分野が増えている。そして、安全性・信頼性・相互運用性の担保等、より**複雑なデータ連携を実現するための技術要素・ルール**を確保するニーズが増大している

目的

- 上記の背景を踏まえ、より複雑かつ機微情報の慎重な取扱が求められるデータ連携に必要な要素を検討し、「ウラノス・エコシステム」の高度化に向けて**今後優先的に実施すべき技術開発内容及び技術開発がもたらす効果**等の整理を行うことを目的とする

本調査事業の概要

- 各国動向・技術動向に関する机上調査・ヒアリング調査を通じて、ウラノス・エコシステムの方向性に関する示唆を得ることを大方針として実施項目ごとに作業を進めた

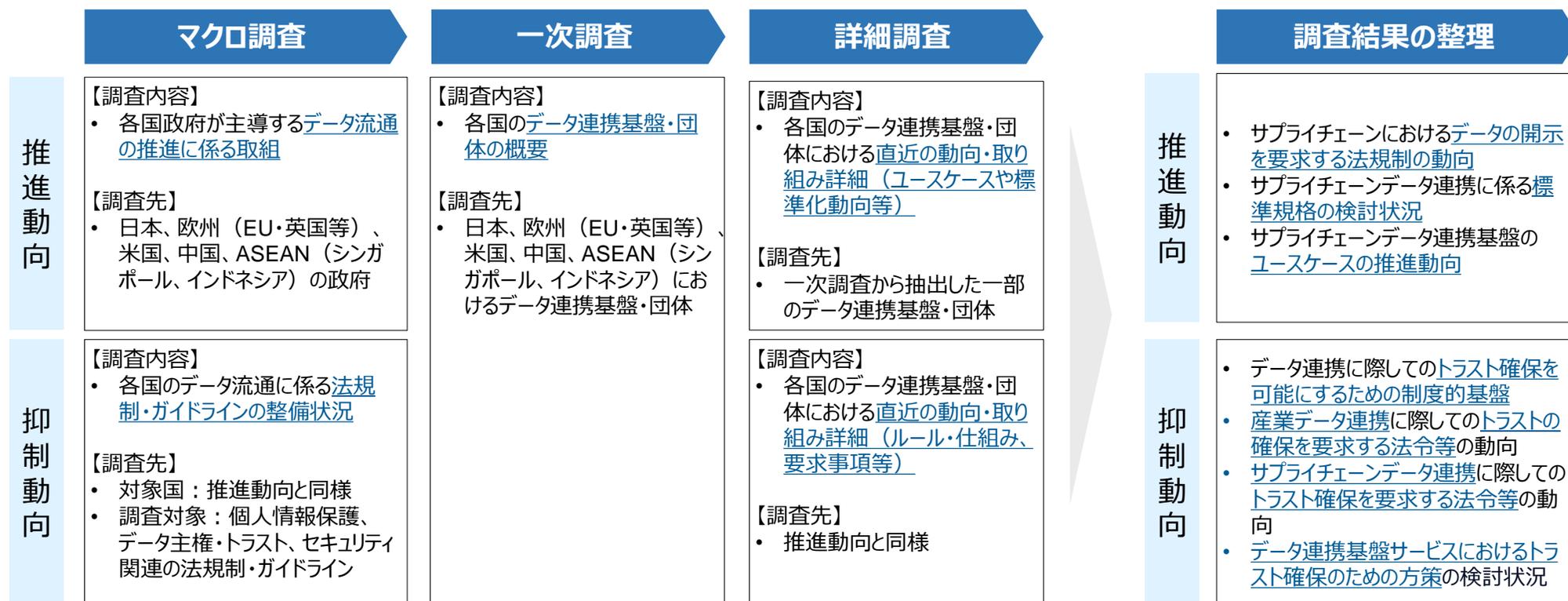


1. データ流通に係る各国動向調査

- 調査の全体像・方法
- 調査結果－推進動向
- 調査結果－抑制動向

調査の全体像・方法

- 各国政府およびデータ連携基盤・団体を対象し、推進・抑制動向の観点から調査を実施した
- 調査は、主要国・地域におけるデータ連携・流通に係る政策動向や法規制・ガイドラインの整備状況についてマクロ調査を行い、その後、マクロ調査を実施した主要国・地域におけるデータ連携基盤（団体）を抽出して、その概要について一次調査を実施した
- 一次調査でリストアップした基盤・団体から、ウラノス・エコシステムの方向性や直近の活動の活発度などを考慮して詳細調査先をリストアップし、直近の動向と取り組みの詳細を調査した
- 得られた結果は、ウラノス・エコシステムの方向性等を考慮し、主にサプライチェーンデータ連携におけるユースケースや標準化動向（推進）、トラストに係る要求事項（抑制）の観点から整理した



調査結果－推進動向

- 製造業を中心として、日本企業を含む世界各国の企業が、各国において立案・施行される法規制によって、サプライチェーンにおけるデータの開示要求への対応を迫られつつある
- また、政府機関や国際標準化機関によって、これらの対応に必要なデータ連携のための技術仕様・プロトコルの標準化が進められている
- このような状況の下、欧州を中心として、サプライチェーンデータ連携基盤のユースケースの創出が進められており、自動車分野におけるCE、CFP、DPP関連情報の領域では、一部市場展開が開始されるなど、特に進展がみられる

サプライチェーンにおける データ開示要求する法規制動向 (開示要求される情報、要求の対応時期等)

- 欧州電池規則や欧州エコデザイン規則、REACH規則等の規制法が立案・施行され、これにより、製造業の企業を中心として、政府・取引先・顧客から、脱炭素・資源循環、製品含有化学物質等に関する情報開示を要求されるようになっていく。
- 法規制の中には直近での対応を要求するものもある。例えば、欧州電池規則では、サプライチェーンのデューデリジェンスやCFP宣言について、2025年夏頃から対応を要することとしている。
- これらの法規制は、製品のライフサイクル全体にわたって、自社のみならず、広くサプライチェーン上に存在する取引先（サプライヤー／顧客）の情報をも開示することを要求しており、日本企業にも影響が及び得る

サプライチェーンデータ連携に係る 標準規格の検討状況 (標準規格等の開発・策定主体、標準規格等策定の目的・対象ユースケース等)

- CEやDPPに関して、サプライチェーンにおけるデータ連携基盤の標準化やルール形成の取組がみられた。
- CEに関しては、ISOによって、PCDS（Product circularity data sheet）の標準であるISO 59040の検討されていた。
- DPPに関しては、欧州委員会の関連機関であるCEN-CENELEC/JTC24によってバッテリー分野のDPPであるBattery Passportのシステム標準の検討が行われていた。また、国際連合によって、DPPのクロスボーダーユースケースにおける相互運用性確保のための標準プロトコルの検討が行われていた。

サプライチェーンデータ連携基盤の ユースケースの推進動向 (各ユースケースで連携される情報、対応を予定している法規制、ユースケースが進んでいる分野等)

- 欧州では、主にCatena-Xのエコシステムにおいて、サプライチェーンにおけるデータの開示を要求する法規制に対応可能な、データ連携基盤のサービス実証・市場展開が進められている。特に取組が進捗しているユースケースは、CE、CFP、DPP関連であり、産業分野の中では自動車関連の取組が特に進捗している。
- 日本でも、REACH規則等の化学物質規制への対応やDPPへの情報連携等を目的としたデータ連携基盤の実証が進められている

調査結果－抑制動向

- 欧州では、eIDAS規則によるトラストサービスの認定等が行われ、Gaia-Xのようなデータスペースを含む欧州域内のデジタルサービス利用に係るトラスト確保のための制度的基盤として機能している
- 日本においても、経団連において産業データスペースの構築に向けた提言を公表しているほか、IPAにおいて、サプライチェーンデータ連携基盤に求めるべき設計要件の定義が進められている
- またサプライチェーンデータについては、欧州エコデザイン規則（ESPR）のような法令等によって、サプライチェーン間のトラストの確保が要求されている。またCatena-Xにおいても、共通領域および個別ユースケースにおけるトラスト確保のためのガイドラインが提供されている

データ連携に際してのトラスト確保を可能にする制度的基盤

- データ連携に際してのトラスト確保を実現するため、欧州ではEU法であるeIDAS規則によって、一定の基準のもとで国家監督機関による認定を受けたトラストサービスに法的効力を付与する仕組みを整備している。
- eIDAS規則の改正法であるeIDAS 2.0においては、デジタルアイデンティティウォレットの標準規格であるEUDIWを規定し、欧州域内のデジタルサービス利用者がデータ主権を確保しながら認証を受けるための相互運用可能な手段を提供している

産業データ連携に際してのトラストの確保を要求する法令等

- 産業データの流通、連携に関しては、世界各国において、企業間でデータを交換するに際して遵守すべき事項を定めた法令（欧州データマネジメント法など）や、当事者間で取り決めるべき契約条項の標準型を示したガイドライン（AI・データの利用に関する契約ガイドラインなど）が策定されている

サプライチェーンデータ連携でトラスト確保を要求する法令等

- 欧州を中心に立案・施行が進む、サプライチェーンにおけるデータの開示を要求する法制度等においては、開示されるデータに対するトラストの確保を要求する規定が設けられている。
- 例えば欧州エコデザイン規則（ESPR）において、DPPが備えるべき設計や運用上の要求事項としてデータの認証、信頼性、完全性を確保することや、データの詐取等を防止し高レベルのセキュリティ・プライバシーを確保することが定められている

データ連携基盤サービスにおけるトラスト確保のための方策

- 欧州において個々のデータ連携基盤を束ねるエコシステムであるGaia-Xでは、エコシステムにおけるデータ流通のトラスト確保のための共通ルールとして「Gaia-X Trust Framework」を策定、Gaia-X Digital Clearing Houseが実装を担っている。
- eIDAS規則に基づく認定を受けたトラストサービスがGaia-Xエコシステムにおけるトラストアンカーとしての役割を担っている
- Catena-Xでは、自動車業界向けのオープンで協調的なデータエコシステムを提供することを目的としており、エコシステムの効果的な運用とトラストを確保するための参照文書類を定義している。
- 経団連では、「産業データスペース」の構築に向け、意義と官民が取るべき具体的なアクションを提示した提言を公表している。また、IPAでは、主に蓄電池・CFP関連情報の連携を想定したデータ連携基盤に求める基本的な設計要件を定義したガイドラインを策定している。

2. 複雑かつ機微情報を扱うデータ連携に係る技術動向調査

- 調査の全体像・方法
- 調査結果
 - 個人情報保護関連技術
 - データ主権・トラスト関連技術
 - サイバーセキュリティ関連技術

調査の全体像・方法

- より複雑かつ機微情報の慎重な取扱いが求められるデータ連携に必要な技術として、データセキュリティ技術、プライバシー強化技術等に着目し、それら主要技術について、技術概要、プレイヤー、ステータス（社会実装済、研究開発中等）等を調査した
- なお、調査対象技術はデータ連携システムに求められる機能を踏まえて選定しており、当該技術がデータ連携システムにおいてどのように活用されているのか（またはされ得るのか）を整理した

機能要件	調査対象技術	調査項目
個人情報保護	プライバシー強化技術	
データ主権・トラスト	アクセス制御・ID関連技術	
サイバーセキュリティ	ブロックチェーン関連技術	<ul style="list-style-type: none"> ● 主要なプレイヤー <ul style="list-style-type: none"> ➢ 主要な民間企業、研究機関、業界団体、国際標準化機等の企業HP（プレスリリース）、研究論文、国際標準化団体でのオープンなWGでの議論動向、勧告化された規格、業界団体の報告書等
	データセキュリティ	<ul style="list-style-type: none"> ● ステータス（コンセプト、PoC、実運用） <ul style="list-style-type: none"> ➢ 社会実装（実運用）をゴールとしたときの技術成熟度が、コンセプト、PoC、実運用のどの段階にあたるか
	エンドポイントセキュリティ	
	ネットワークセキュリティ	<ul style="list-style-type: none"> ● データ連携システムにおけるユースケース <ul style="list-style-type: none"> ➢ データ連携システムにおいてどのように活用されているのか、またはされ得るのか、どのような機能を発現し、どのようなルールの下活用されているのか
クラウドセキュリティ		



調査結果

- より複雑かつ機微情報の慎重な取扱いが求められるデータ連携に必要な技術として、データセキュリティ技術、プライバシー強化技術等に着目し、それら主要技術について、技術概要、プレイヤー、ステータス（社会実装済、研究開発中等）等を調査した
- なお、調査対象技術はデータ連携システムに求められる機能を踏まえて選定しており、当該技術がデータ連携システムにおいてどのように活用されているのか（またはされ得るのか）を整理した

技術領域	調査結果			
	技術概要	主要なプレイヤー	ステータス	ユースケース
個人情報保護 関連技術	<ul style="list-style-type: none"> • プライバシー強化技術として秘密計算技術（HE、MPC、TEE）およびデータ難読化技術（差分プライバシー、連合学習、ゼロ知識証明）を調査した • いずれの技術もデータを暗号化等により秘匿化した状態で計算等の処理を行う技術として開発・使用されている 	<ul style="list-style-type: none"> • 実用化と並行して規格開発等が行われており、ISO/IEC、IETF、W3Cおよび米国NISTなどが取り組みを進めている • 民間企業としてはMicrosoftやGoogle等の巨大グローバルITプラットフォームの他、スタートアップ企業がベンダーとして活動しているケースも見られた 	<ul style="list-style-type: none"> • 秘密計算技術については、いずれも実用化されているものの、演算式の複雑さ、演算時間等の面で得失に差が生じた • データ難読化技術についても実用化事例があるものの、ゼロ知識証明については実装難易度が高く、他の代替技術（規格）を採用する事例も見られた 	<ul style="list-style-type: none"> • データの秘匿性を確保した状態で企業間データ連携を実現する技術としての活用が注目されている • 各技術で適用し得るデータ連携のフェーズが異なり、ゼロ知識証明はサプライチェーンのコンプライアンス管理等、差分プライバシー、秘密計算、連合学習はAIモデルの最適化等への適用が見込まれる
データ主権・ トラスト 関連技術	<ul style="list-style-type: none"> • アクセス制御・ID関連技術として、DID、VC、mDLを調査した。 • プライバシー関連情報を中央集権的に管理をすることなく、個人・法人が自分自身のアイデンティティを自分自身でコントロール（SSI：Self-Sovereign Identity）できるようにするための要素技術（規格）である。 	<ul style="list-style-type: none"> • 標準化機関であるW3C、DIFが、DID規格に関するガイドラインやユースケースの開発促進に取り組んでいる。 • 民間企業ではDIFの参加企業であるDentity社やNothem Block社等のスタートアップ企業がデジタルプラットフォームを開発している動きがみられた。 	<ul style="list-style-type: none"> • カナダではDIDとVCを組み合わせた、検証者が発行者に問い合わせることなく証明書の検証を行う技術が実装されている。 • 米国では、複数の州でmDLの導入が進み、Apple社のウォレットアプリケーションを使用した空港での本人確認などのケースで実用化が進んでいる。 	<ul style="list-style-type: none"> • サプライチェーン上の各企業がデータをVC形式で署名検証できるようにした上で、署名したデータをブロックチェーンでやり取りすることにより、業界共通の製品含有化学物質のデータの非改ざん性を検証可能になることが実証された。
サイバー セキュリティ 関連技術	<ul style="list-style-type: none"> • サイバーセキュリティ関連技術として、IDS/IPS、ABEを調査した。 • IDS/IPSは、不正アクセスを検知・ブロックする技術である。 • ABEは属性を用いた閲覧制御を行う暗号技術である。 	<ul style="list-style-type: none"> • IDS/IPSについて民間企業では、MicrosoftやAWSが、クラウド上での不正アクセスに対する検知・通知・防止する機能を提供している。 • NTT関連会社において、従来型のABEよりも安全性向上の懸念を解決した登録型属性ベース暗号の実用化の動きがみられた。 	<ul style="list-style-type: none"> • IDS/IPSについては、脆弱性情報の分析や機械学習を活用した脅威の検知する機能が開発されている。 • ABEについては量子計算機に対して耐性を備えた、分散型のMA-ABEの実証が行われている。 	<ul style="list-style-type: none"> • IoTに対する新たなサイバー攻撃を効果的に検出するために、機械学習を活用したIntegrated Intrusion-Detection(IID)システムが開発されている。 • 従来型のABEの応用として、勤務時間や特定の機器ごとのデータの属性に合わせたアクセス制限を行うことが見込まれる。

調査結果－個人情報保護関連技術

- データの秘匿性を確保した状態で企業間データ連携を実現する技術としての活用が注目されている
- 各技術で適用し得るデータ連携のフェーズが異なり、ゼロ知識証明はサプライチェーンのコンプライアンス管理等、差分プライバシー、秘密計算、連合学習はAIモデルの最適化等への適用が見込まれる

技術	適用フェーズ	成熟度 (○：実装、△：PoC、×：コンセプト)	企業間データ連携における利活用の動き (○：実装、△：PoC、×：コンセプト、－：確認できず)
ゼロ知識証明	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid black; padding-bottom: 2px;"> 流通 保管 加工 分析 </div> <div style="text-align: center; margin-top: 10px;">●</div>	イーサリウム等の暗号資産の匿名取引において実装されている。その他デジタルアイデンティティ検証や機械学習の推論結果の正当性検証等での活用を見据えた実証が行われている	Gaia-Xの分散型アーキテクチャにおいて、中央管理のない自律的なデータ管理を可能にする技術の一つとして、ゼロ知識証明が重要視されている。また、Trusted Webの実証においては、ゼロ知識証明を活用したユースケースの創出等が行われている
差分プライバシー	<div style="text-align: center; margin-top: 10px;">●</div>	Apple等ではユーザーのデータを集約して分析する際に利用している。ユースケースに応じた適切なノイズの設定が進められている	差分プライバシーにより、各サプライヤーの製造データを保護しつつ、サプライチェーン全体の製造実績や生産能力の把握を行う研究が行われている
秘密計算	<div style="text-align: center; margin-top: 10px;">●</div>	一部実装され始めているが、演算の高速化やサイドチャンネル攻撃への対策が求められている	TEEを活用したユースケースとして、データ提供者が複数いる場合には対応していなかったが、近年では、データ提供者が複数の場合の利用も想定した開発が進められている
連合学習	<div style="text-align: center; margin-top: 10px;">●</div>	スマートフォンの予測変換モデルの学習に活用されている。異質なクライアントの存在を前提とした耐障害性のあるアルゴリズムの研究が行われている	Gaia-Xに準拠したCOSMIC-Xでは、工作機械の部品の故障予知保全モデルの精度向上を目指す実証が行われている。連合学習により、各社のデータを保護しつつ、ダウンタイムを最小限に抑えることが可能になる

調査結果 – データ主権・トラスト関連技術

- 個人または法人が自分自身のアイデンティティをコントロールできる規格であるDID、VC、mDLは、法人情報・製品情報の証明・検証に適用することによるサプライチェーンを横断したコンプライアンス管理等への活用が見込まれる
- 生体・行動認証技術はデータ連携基盤への利活用の動きは確認できなかった
- ブロックチェーン関連技術は、製品のライフサイクルにおける証跡データの管理への活用が見込まれる

技術	適用フェーズ 流通 保管 加工 分析	成熟度 (○ : 実装、△ : PoC、× : コンセプト)	企業間データ連携における利活用の動き (○ : 実装、△ : PoC、× : コンセプト、- : 確認できず)
DID	●	VCを発行・検証するためのソフトウェア、オープンソースのBCウォレットが実装されている。これは検証者が発行者に問い合わせることなく証明書の検証を行うので高いプライバシーレベルを確保している。	Gaia-Xの分散型アーキテクチャにおいて、中央管理のない自律的なデータ管理を可能にする技術の一つとして、SSIのコンセプトを採用し、DIDにより所有者の情報を所有者自身でコントロールすることが提唱されている。
VC	●	Microsoftではブロックチェーン(ion network)のストレージに対応した従業員・顧客等の資格情報の発行・検証サービスを提供している。	DIDと同様にGaia-Xの分散型アーキテクチャにおいてVCを使って、物理的な資格情報をサイバースペースにおいて選択的な開示が実現することを推奨している。また、EUでは、eIDAS2.0規則に基づき、EUDIWの設計・実装が進められており、その中でVCの利用が推奨されている。
mDL	●	米国では複数州でISO/IEC18013-5に基づくモバイル運転免許証(mDL)の導入及びテストを展開している。	EUにおいてEUDIWとmDLを活用して、国境を越えてもEU全域で預金口座を開設することや、EUのどこでも処方箋を発行・取得することを実現することで管理業務・認証プロセスにおけるコスト削減と加盟国間での相互運用性の向上を実現している。
生体・行動認証技術	システムへの本人認証に利用されるので該当なし	NECは、立ち止まることなく多人数を同時に認証できるシステムを販売開始した。このシステムは、小型エッジ端末とカメラ1台から導入可能で、1分間に100人のリアルタイムな認証を実現する。	有識者へのヒアリングにおいて、データ連携基盤にアクセスする社員を認証する場合、生体認証・行動認証ではなく、マイナカード連携等が良いという意見があった
ブロックチェーン関連技術	● ●	IBMは、ブロックチェーン技術を活用した食品サプライチェーン追跡ネットワーク「IBM Food Trust」の商用提供を開始している	PLA-NETJにおいては、ブロックチェーンによる分散管理によって、製品のライフサイクルにおける証跡データを管理することとしている

調査結果 – サイバーセキュリティ関連技術

- ファイアウォールを通過して不正アクセスや、DDos攻撃等の異常な通信があった場合に、その侵入を検知して管理者に通知するシステムであるIDSやIPSの機能に加えて、通信をブロックするシステムであるIPSは、Battery PassportのDPPデータ保存のセキュリティ対策として推奨されている
- 公開鍵暗号に「属性（秘密鍵を持つユーザーの属性）」と「属性を用いた閲覧制御」機能を追加した暗号技術であるABE（Attribute-Based Encryption）は、文章形式のデータだけでなく画像情報や位置情報等の様々なシーンに対応できる安全なデータ流通に活用されている

技術	適用フェーズ	成熟度 (○ : 実装、△ : PoC、× : コンセプト)	企業間データ連携における利活用の動き (○ : 実装、△ : PoC、× : コンセプト、- : 確認できず)
IDS/IPS	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid black; padding-bottom: 5px;"> 流通 保管 加工 分析 </div> <div style="border: 1px solid black; height: 100px; display: flex; align-items: center; justify-content: center;">●</div>	IDS/IPSについては、脆弱性情報の分析や機械学習を活用した脅威の検知する機能が開発されている。	Battery Passportにおいて、DPPデータ保存のセキュリティ対策としてISO/IEC 27040:2015が推奨されている。これはデータストレージセキュリティに関する技術ガイダンスであり、組織がデータストレージの計画、設計、実装において一貫したアプローチでセキュリティ対策を実施し、適切なリスク軽減レベルを定義する方法を示すものである。特に、管理インターフェースの保護にはIDS/IPSの使用がベストプラクティスとして推奨されている。
ABE	<div style="border: 1px solid black; height: 100px; display: flex; align-items: center; justify-content: center;">●</div>	文章形式のデータだけでなく画像情報や位置情報等の様々なシーンに対応できる安全なデータ流通に活用されている。また、量子計算機に対して耐性を備えた、分散型のMA-ABEの実証が行われている。	英国のUK digital identity and attributes trust frameworkでは、データ保護にあたりETSI TS 103 458が推奨されている。これは、モバイルサービスやIoT機器などにおける個人データ保護のための属性ベース暗号化(ABE)の適用に関する技術仕様書である。ABEを用いた個人データ保護の要件定義に加え、実装方法やユースケースも提供している。

総合分析

- **ウラノス・エコシステムにおける現状課題と対応**
- **ウラノス・エコシステムにおける優先開発対象技術**
- **ウラノス・エコシステムによる市場創出効果**

ウラノス・エコシステムにおける現状課題と対応

- 推進動向に係る分析結果として、ウラノスエコシステムにおいては、欧州を中心として立案・施行されているサプライチェーンデータの開示を要求する法制度や展開されているユースケースの全体的な進捗状況を踏まえ、CEやCFP、DPP等に関する情報を連携するユースケースについて、その事業性・有効性を検証すべきと考えられる
- 抑制動向に係る分析結果として、まずは日本においても欧州のように、デジタルサービス利用の信頼性確保に向けた制度的基盤を整備しつつ、これに立脚した形でウラノスエコシステムにおいて個々のデータ連携基盤と海外データ連携基盤との相互運用性確保を可能とする共通ルールを定めるべきと考えられる

推進動向に関する 分析結果

ユースケースの方向性

- 調査結果を踏まえると、法令／国際標準等の国際ルールや契約に基づき、安全かつ公正に情報連携を行うために、サプライチェーン上で**CE**や**CFP**、**DPP**等に関する情報を連携するユースケースにおいて、**データ連携基盤のニーズが高い**と史料

ユースケースの具現化 に向けたアクション

- 一方で、多くのユースケースが実証段階、あるいは実用化されて間もない段階であることを踏まえると、実証・市場投入に関して取組が進捗しているユースケースであっても、その**事業性・有効性を検証**する必要があると想定

抑制動向に関する 分析結果

トラスト確保のために 整備されるべき制度的 基盤のあり方

- 調査結果を踏まえると、日本でも欧州のように、トラストサービスに対して共通の法的根拠に基づく包括的な認定制度や、データ主権の確保のためのアイデンティティ情報管理のための共通規格などの**制度的基盤**を整備し、これを**データ連携基盤において利用可能とする必要**がある

ウラノスエコシステムに おいて実施すべきガバ ナンス

- 調査結果から、企業間の営業秘密の保持やデータ主権を確保したデータ連携の実現のための**基準（ガイドライン）**を設けることが必要と史料
- この基準策定に際しては、CEやCFP、DPP等に関する情報開示を要求する法令等による**トラスト要求に対応**できるよう、国内で提供されるデータ連携基盤が**認証・認可の方法等に関して参照すべき事項を含めるとともに、その内容については、国外データ連携基盤との間で相互認証を可能とする水準とする必要がある。**

ウラノス・エコシステムにおける優先開発対象技術

- データ連携基盤の基本技術に位置付けられ、いずれのユースケースにおいても活用が見込まれるデータ主権・トラスト関連技術（アクセス制御・ID関連制御）は早期に開発投資を行うことが有効である
- 他方、個人情報保護関連技術、サイバーセキュリティ関連技術は、ユースケースによっては有効と考えられる

技術領域	調査結果			
	社会受容性	収益性・市場性	国際協調性	国際競争性
個人情報保護 関連技術	<ul style="list-style-type: none"> 一部実装され始めているが、データ連携基盤への適用については、ニーズはあるもののユースケースは限定的で研究・実証段階が中心 	<ul style="list-style-type: none"> 秘密計算技術市場はCAGR10%以上で成長すると予測されており、医療、製造、AIモデル最適化などの多様な分野での活用が見込まれている 	<ul style="list-style-type: none"> 秘密計算技術（HE, MPC, TEE）はISO/IECやNISTなどの国際標準化機関で議論が進行中である 差分プライバシーやゼロ知識証明は、国際的なデータ連携での利用を見据えた研究が進められている 	<ul style="list-style-type: none"> 米国企業（Microsoft, IBM）はFHEやMPCで市場をリード 日本企業（NTT, ZenmuTech）は独自の秘密計算技術を開発し、ISO規格化に寄与
データ主権・ トラスト 関連技術	<ul style="list-style-type: none"> DID、VC、ブロックチェーン等は、トラストを確保するために必要な技術であり、データ連携においても基本技術に位置付けられている 	<ul style="list-style-type: none"> DID/VCはサプライチェーン管理やデジタルアイデンティティ分野での活用が期待されており、市場形成が見込まれる ブロックチェーンを活用した証跡データ管理や信頼ネットワーク構築のユースケースが実証されており、産業横断的な適用が期待される 	<ul style="list-style-type: none"> DIDやVCはW3CやDIFなどの国際標準化機関で議論され、ガイドラインやユースケース開発が進行中 Gaia-XではVC（SD-JWT）を使って、物理的な資格情報をサイバースペースにおいて選択的な開示を実現することを推奨 	<ul style="list-style-type: none"> 欧州では、mDLをEUDIWに格納し、国境を越えてもEU全域で口座開設等を可能にする実証が実施されている 米国では、複数の州でmDLの導入が進み、Apple社のウォレットを使用した空港での本人確認などのケースで実用化が進んでいる
サイバー セキュリティ 関連技術	<ul style="list-style-type: none"> 各企業がそれぞれのルールに則ってセキュリティ技術・規格を実装する形態が望ましいとされる 	<ul style="list-style-type: none"> ABEについては量子計算耐性を備えた分散型MA-ABEが開発されており、多様なシーンでの応用が期待される 	<ul style="list-style-type: none"> ISO/IEC 27040:2015において、データストレージセキュリティに関するベストプラクティスとしてIDS/IPSの使用が推奨されている ETSI TS 103 458では、ABE（属性ベース暗号）の適用がIoT機器のデータ保護に推奨されている 	<ul style="list-style-type: none"> MicrosoftやAWSがIDS/IPSを統合したクラウドセキュリティサービスを提供しており、不正アクセスに対する検知・通知機能を実装している 日本企業（NTT）は、量子計算に耐性を持つ登録型ABEの実用化を進めており、独自の技術で国際競争力を高めている

ウラノス・エコシステムによる市場創出効果

- 1. データ利活用サービスの市場、2. データ連携システムそのものの市場は、それぞれ1,100億円と試算した。また、3. セキュリティ・プライバシー強化技術に係る市場は、330億円と試算した

