IOWN時代のデータ流通を実現するデータガバナンス

現在，世界ではデータに対する取り扱いを厳格化する動きがある一方，安全にデータを処理する技術やルールを整備しデータ流通を加速する動きも出てきています．本稿では，データ流通に影響を与える世界の動向を俯瞰したのち，データの所有者が安全にデータを他者と共有できるようデータをコントロールするデータガバナンスの考え方を説明し，IOWN（Innovative Optical and Wireless Network）時代のデータガバナンスに求められる要件を説明します．

鈴木　勝彦（すずき　かつひこ）　横関　大子郎（よこぜき　だいごろう）
NTT社会情報研究所

背　景

IoT（Internet of Things）デバイスの普及やDX（デジタルトランスフォーメーション）活動の進展などにより，今まで取り扱うことのできなかった情報もデジタル化され，そのデータ量も飛躍的に増加しています．究極的には物理空間を構成するモノや人，さらには社会全体がサイバー空間上でデジタルツインとして再現され，それらを相互に連携した分析を行い，物理空間上にフィードバックすることで，両空間が融合した今までにないスマートな世界が到来するといわれています（**図1**）．その実現には，個人や業種・業界を越えたデータの流通が必要であり，さらにそれらデータは機微な情報も含むため，安心・安全なデータ流通を支える仕組みも必要です．本稿では，近年のデータ流通に影響を与える世界の動向を示した後に，主にセキュリティの観点から，IOWN（Innovative Optical and Wireless Network）時代のデータ流通を支えるために必要なデータガバナンスの考え方を説明します．

データ流通の動向

データ流通に関し，データ流通を厳格化し制限する動きと，規約などの整備によりデータ流通を促進する動きがあります（**図2**）．

■個人情報保護などデータ管理の厳格化

世界各国で個人情報保護の動きが進

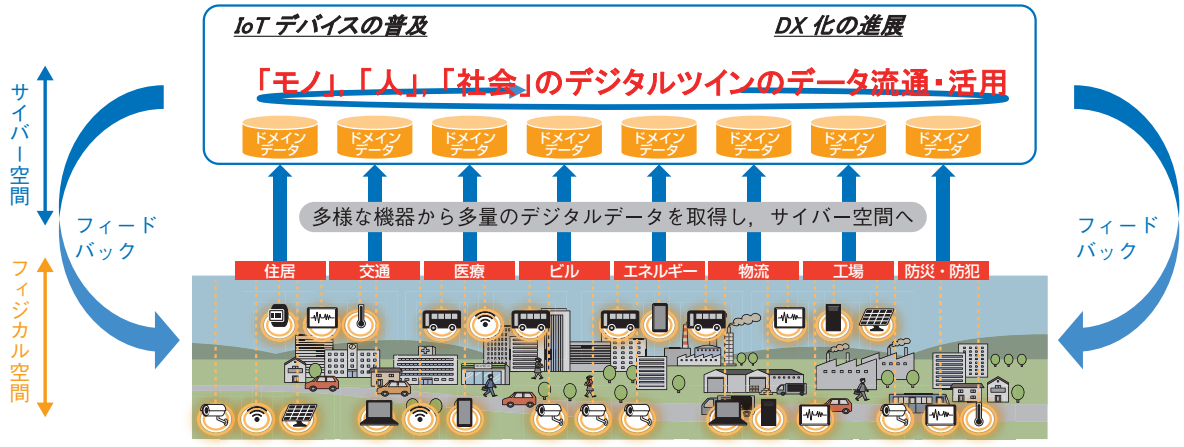

図1　IOWN時代のデータ流通

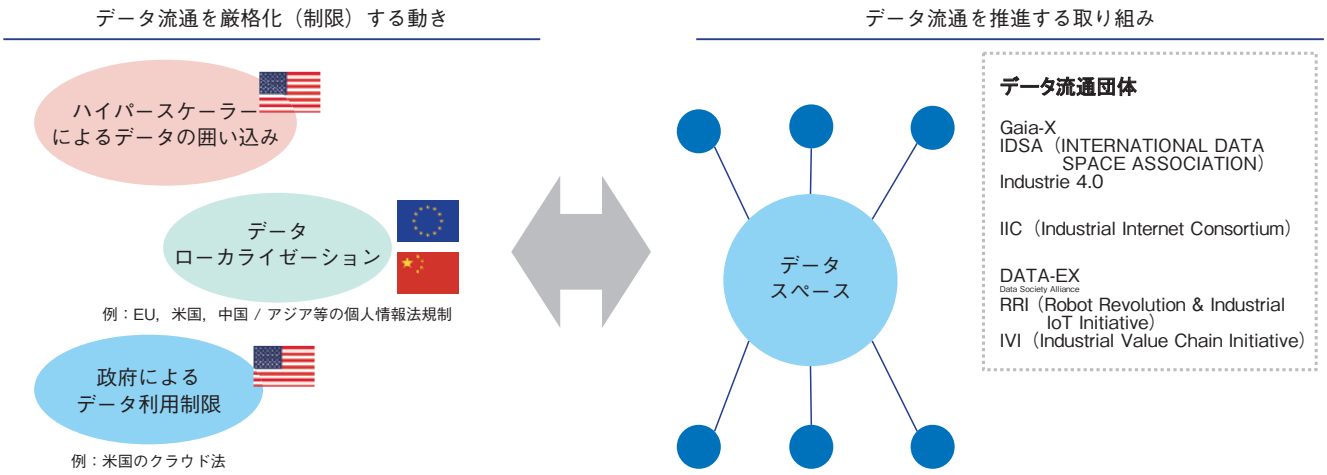

図 2　データ流通における世界の潮流

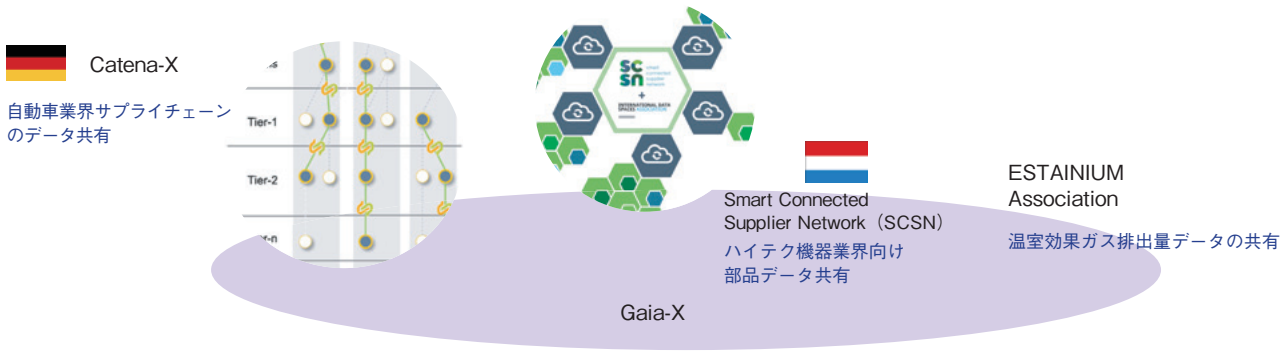

図 3　データスペースの登場

んでいます．欧州の GDPR（一般データ保護規則）は有名ですが，米国の CCPA（カリフォルニア州消費者プライバシー法）や，アジアでも中国の個人情報保護法や，韓国，タイ，インドでも個人情報保護法が施行され，個人に関する情報の流通に関してより厳格な管理が求められてきています．

また欧州では，ハイパースケーラーによるデータの囲い込みによる課題も顕在化しており，非個人データを含めさまざまなデータに対する権利保護の強化が求められています．その流れを受け，より透明性・信頼性を重視した連邦型のデータ・エコシステムを築く取り組みがIDSA（The International Data Spaces Association）[1] 等の団体により進められています．

■多様なデータスペースの登場

データ流通を活性化する動きとして，欧州を中心にデータスペース構築の動きが始まっています（**図 3**）．データスペースとは，安全性の高いデータ共有の実現を目的としたシステムや仕組みを持つコミュニティを指します．欧州では産業界を中心に 1000 社規模の業界別データスペースの構築が始まっており，データ共有の機運が高まっています．企業は原則データを出したくない，出すにしても使用履歴の追跡ができるなどの要求があるため，IDSA 等，データを安全に扱うための標準の登場を背景に，多くのデータスペースが生まれてきています．例えばドイツでは自動車産業の競争力強化を目的とし，自動車のサプライチェーン全体でデータを共有する Catena-X[2] や，オランダのハイテク機器メーカが集まり少量多品種な複雑な部品データ

の共有をめざす SCSN[3]，また 業界横断でサプライチェーン上の企業間で温室効果ガス排出量データをブロックチェーン等オープンな基盤で共有することを目的とした Estainium 協会[4]などが有名です．現在，国別や業種別などにデータスペースが登場しており，今後この動きは加速していくものと考えられます．企業を中心としたデータスペースを紹介しましたが，個人が参加する SNS やメタバースなども今後安全なデータのやり取りが求められると考えており，広義のデータスペースと考えられます．

■データスペースの統合や接続

このように登場したデータスペースですが，その統合や接続の動きもみられます．一例として，欧州のバッテリー規制に対する動きとして，バッテリーパスポートと呼ばれる材料調達からリサイクルまでの蓄電池の来歴を管理し，温室効果ガスの排出の削減をめざす取り組みがあります[5]．国別に存在する複数のデータスペースを横断して来歴を追跡する場合，その統合や接続が必要になります．この取り組みは自動車業界から開始されていますが，バッテリーに関連する他の業種にも広がると，業種を横断したデータスペースの統合や接続が求められる機会がますます増えてくることが予想されます．

■レジリエントでグローカルなサプライチェーン

近年のパンデミック，自然災害や国際情勢などにより，サプライチェーンを非常に短期間，かつ頻繁に組み替える事例も多く発生しています．各業界においては材料の調達に遅れが生じ，調達先の変更に踏み切った事例が散見されますし，半導体供給不足など広範囲な業界に影響を与えた事例も記憶に新しいと思います．

従来のグローバル化と対比した動向として，経済安全保障の観点から重要な部品に関しては国産化を進める，また特定の系列国のみでサプライチェーンを構成するなどの動きもみられます．

データ流通の観点からは，これらサプライチェーンの組み替えに対応し，新しい取引相手とダイナミック，かつスムーズにデータ流通ができることが求められます．

■情報処理技術の進展

最後に量子コンピュータ，5G（第5世代移動通信システム）や6G（第6世代移動通信システム），IOWN など情報処理技術の進展が挙げられます．大容量，低遅延，低消費電力を実現するネットワークの登場により，遠隔医療や自動運転，ドローンの管制制御等の新たな需要も生まれてきており，従来はネットワーク上を流れることがなかった機微なデータを安全に扱う仕組みが求められます．また，データ転送コストが大幅に低減されることで，分散型のデータセンタやエッジ・クラウド連携など，新たなデータ処理形態の登場が予想されます．今後は効率性と安全性を両立するデータ処理が求められるでしょう．

データガバナンスとは

データガバナンスは，統一された定義はありませんが，データ主権とも呼ばれ，データ所有者が定めたデータ取り扱い方針（ポリシー）が，データの生成されるときから消滅するまでのライフサイクルにわたって守られることを指します．ポリシーの例としては，データの複製を許可しない，データは常に暗号化していなければならないなどが挙げられます．前章のデータ流通に影響を与える世界の動向を踏まえ，IOWN 時代のデータガバナンスの実現に求められると想定される要件を説明します（**図 4**）．

■散在し分散するデータ管理の実現

先のデータスペースの例で見たようにデータは今後ますます分散して管理されるようになることが予想されます．特定の1社のみではデータを集めることも限界がありますし，国による法制度の違いなどでデータを1カ所に集められないことが増えることも予想されます．また，IOWN APN（オールフォトニクス・ネットワーク）のように大容量・低遅延のネットワークが前提となると，データの移動コストが従来よりも飛躍的に低くなります．今後求められるデータ管理としては，データは原則としてデータ所有者が希望する場所で管理でき，他者とデータ共有を行う場合は必要に応じて仮想的に集める．それら仮想的に集めたデータに対し計算処理を行い，不要になった場合は，破棄する．データを1カ所に集めるデータレイクに対し，分散したデータをあたかも1カ所にあるように見せるこのような技術をデータ仮想化と呼びます．現在データ仮想化は単一データセンタ内など比較的狭い範囲で利用されていますが，今後国やデータスペースを横断し，ダイナミックにデータを

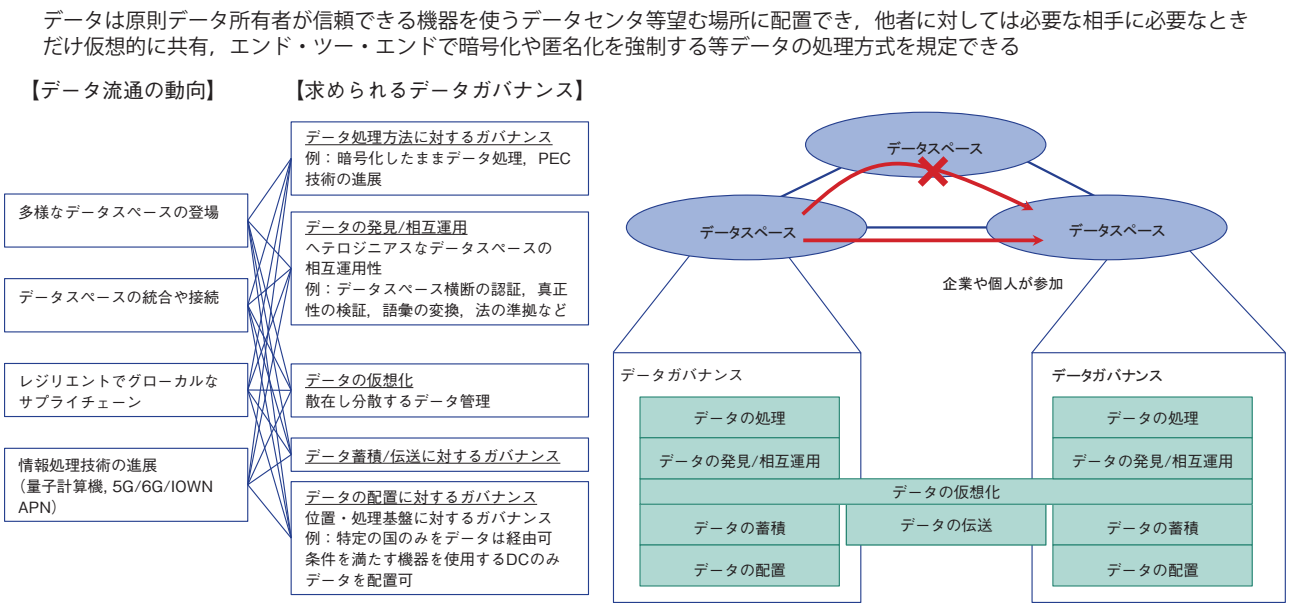

図 4　めざすデータガバナンス

仮想統合できる技術が求められると考えます[6]．

■データスペースの発見・相互運用性の実現

レジリエント，かつグローカルなサプライチェーンを構成するには，複数のデータスペースの相互運用が必要になります．一般にデータスペースは，さまざまな参加者やルールに基づいて運営されるため，新規の相手と動的にデータ流通を可能とするにはヘテロジニアスなデータスペースを相互に接続し，運用する仕組みが求められます．取引相手やデータを発見する仕組みも必要ですし，相手を発見できたとして，個人や企業などデータスペースの参加者は各々のデータスペースの独立した認証基盤で管理されているため，異なるデータスペースにおいては認証連携などの手段で，相互に，相手の真正性を確認できるようにする必要があります．同様にあるデータスペース内のデータの真正性の検証にブロックチェーンを利用しているものがありますが，それらのブロックチェーン間の相互運用性も求められるでしょう．さらにはコミュニティや地域ごとのルール，利用する語彙の変換など，よりセマンティックな相互運用性も最終的には必要になると考えられます．

■データの蓄積・伝送に対するガバナンス

データ保護の一番の基本は暗号技術による暗号化であり，データ盗聴などのリスクに備え，データの蓄積や伝送をする際には暗号技術が当たり前に用いられています．しかし，量子コンピュータの登場により RSA 等の既存の暗号が危殆化するリスクが懸念されており，耐量子計算機時代の暗号技術が求められます．現在米国の NIST では PQC と呼ばれる暗号技術の標準化が行われています．近い将来，これらを利用したデータ蓄積や伝送基盤が求められ，自既存暗号から耐量子計算機暗号へのシームレスな移行や，耐量子計算機暗号自体の危殆化への対応も必要となるでしょう[7]．

■データ処理方法に対するガバナンス

暗号技術はデータを蓄積や伝送する際に用いられますが，そのデータを用いて計算処理を行う際には一般に平文に戻し処理されます．近年では計算処理を行う際も暗号化したまま処理可能な技術も実用期に入ってきています．より一般にプライバシーを保護し，データを処理する技術の総称として PEC*が注目を集めており，Gartner

＊ PEC：Privacy Enhancing Computation 技術．暗号化したまま計算する，匿名化により本人を特定できないようにするなど，プライバシーを強化した計算技術の総称．

などからも言及されています．PECは準同型暗号や秘密分散に基づき暗号化したまま計算を秘密計算技術や，ハードウェアによるメモリ暗号化技術TEE を活用し暗号化したまま計算処理を行う Confidential Computing技術，また匿名加工技術や差分プライバシーと呼ばれる個人を特定できないよう加工する技術をはじめ広範な技術群から構成されます．クラウド事業者に対してもデータを保護したいという要求が，PEC が注目を集める背景といえるでしょう．これらの技術を活用することでエンド・ツー・エンドにデータを暗号化したまま処理することが可能となり，データ伝送の際に暗号を使うのと同様に，当たり前に利用される技術となることが予想されます(8)．

■データの位置，処理基盤に対するガバナンス

経済安全性の観点から，データ所有者がデータの蓄積場所や処理してよい場所を選択できる機能や，データを伝送してよい範囲などのデータの配布範囲を制御できる機能が求められるようになると考えています．現在のインターネットは効率性や耐故障性などを重視して設計されており，それに応じた配信経路が選択されますが，今後は，データを蓄積・処理してよい国，地域やデータスペースなどを指定できること，またデータ伝送してよい範囲を指定し，ネットワーク故障発生時などの迂回経路を用いるときも，その範囲を保証される機能など経済効率性だけに基づかず経済安全性を実現するデータ流通を支える機能が求められるでしょう(7)．

さらに，データを蓄積・処理を行うクラウドに対する条件や，クラウドが利用するデータセンタに対する条件として利用しているストレージ機器やネットワーク機器，コンピューティング機器の条件等も指定できることも求められると考えています．前者の例としては，真に機微なデータを取り扱う場合，国内の国産のクラウド基盤で処理のみを許可するなどが挙げられます．後者の例としては，特定の機器メーカの製品上でのみデータを処理することや，SBOM（ソフトウェア部品表）等が有名ですが，脆弱性などの品質上問題ないソフトウェアが使われていることが検証できた場合に限りデータの処理を許可するなどが挙げられます(9)．

今後の展開

今回紹介したデータガバナンスは，データは原則データ所有者が望む場所に配置でき，他者に対しては必要な相手に必要なときだけ共有，エンド・ツー・エンドで暗号化や匿名化等，データの処理方式を指定できるものです．データガバナンスは，今後より安全で柔軟なデータのコントロールをめざしさらなる発展が予想され，さらなるデータ流通の発展が期待されます．

■参考文献

(1) https://internationaldataspaces.org/
(2) https://catena-x.net/en/
(3) https://smart-connected.nl/
(4) https://www.estainium.eco/
(5) https://www.meti.go.jp/shingikai/mono_info_service/chikudenchi_sustainability/pdf/003_03_00.pdf
(6) 歌原・福久・緑・竹内・渡辺・池尻："IOWNプロダクトデザインセンタがめざす，IOWN技術の早期実装・普及，" NTT技術ジャーナル，Vol. 35，No.2，pp.53-56，2023.
(7) 村上・谷口・工藤・知加良・清村・向山・飯島・持田・佐成・木村："量子コンピュータ時代を見据えたセキュア光トランスポートネットワーク技術，" NTT技術ジャーナル，Vol. 35，No.2，pp.45-49，2023.
(8) 井上・森田："IOWN時代のデータガバナンスを実現するトラステッド・データスペース技術，" NTT技術ジャーナル，Vol. 35，No.2，pp.41-44，2023.
(9) 上原・鐘本・野村："セキュリティトランスペアレンシー確保技術によるソフトウェア構成の分析・可視化，" NTT技術ジャーナル，Vol. 35，No.2，pp.50-52，2023.


（左から）鈴木　勝彦／ 横関　大子郎

データ流通は近年非常に活性化しており，DX化の進展に伴いさらなる発展が期待され，情報通信企業である NTT グループにとっても注力すべきだと考えています．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠hco.ntt.co.jp