

II-3 OECDが進めるデジタル経済政策とデータトラストへの取組み

一般財団法人日本情報経済社会推進協会 電子情報利活用研究部 主席研究員 水島 九十九

1. はじめに

デジタル化が急速に加速しており、コミュニケーションや生活スタイル、仕事のやり方などを大きく変化させてきた。企業はグローバルでの競争力強化のために、DX（デジタルトランスフォーメーション）を推進し、イノベーションを促進してサービス改善を進めている。その際、デジタル化されたデータとデータを扱うためのデジタル技術が重要となってきた。

2011年のダボス会議（世界経済フォーラム）にて、「パーソナルデータはインターネットにおける石油」と報告され、それ以来、「データ＝石油」と表現されることが増えた。データが石油以上の価値を持つ資源になることが示唆された。しかし、石油と異なりデータには最初から国境がなく、元来自由に国境を移動することが可能である。そのため、目に見えないデータの利用や管理においては、プライバシーやセキュリティなどトラスト（信頼）を高めることが重要になってきている。

今回は、国際社会の先頭に立って新たな課題に取り組むOECD（経済協力開発機構、Organisation for Economic Co-operation and Development）において、議論が進められている「OECDが進めるデジタル経済政策とデータトラストへの取組み」について解説する。

2. OECDが考えるデジタル経済

OECDは、国際経済の課題を協議することを目的とした国際機関である。先進国による自由な意見交換を通じてグッドプラクティスを共有し、各種政策に関して先見性を高める論議を交わしている。「世

界最大のシンクタンク」とも呼ばれて、現在のOECD加盟国は38カ国である。OECD全体で約30の委員会がさまざまな分野で活動している。¹

その中で、CDEP（デジタル経済政策委員会、Committee on Digital Economy Policy）はデジタル経済の課題を検討する付属機関である。デジタル技術の発展により生じた課題に対して、必要な政策や規制対策を促進している。OECDにおける政策提言（勧告、recommendation）という方法により、原則やガイドラインが示されることも多く、事実上の先進国標準となるケースも多い。プライバシーガイドライン（1980年策定、2013年改定）、セキュリティガイドライン（2002年策定、2015年改定）などの勧告が公開されている。²

OECDが考えるデジタル経済は、「デジタル技術やデータ利用によって向上するすべての経済活動」と定義されている。デジタル経済の進展により、現実世界のあらゆる場所で生成された膨大なデータが、インターネットを経由してサイバー空間に蓄積される。蓄積されたデータはAIなどによって解析され、得られた結果は現実世界にフィードバックされる。データやデジタル技術を有効に活用することにより、イノベーションを創出し、新たな付加価値を提供することが期待されている。³

3. デジタル経済におけるデータトラスト

OECDは、デジタル経済において社会的な拡大を促進するために、経済政策を取りまとめ政策提言を公開している。特に、EC（電子商取引）やシェアリングエコノミーを含むオンラインビジネスを成長させるためには、利用者に関する課題解決が重要と考えら

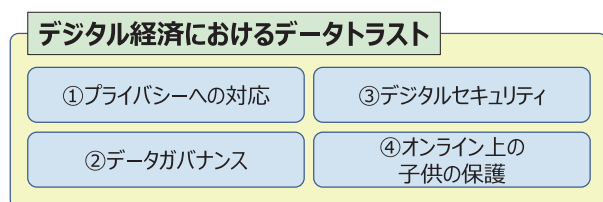
1 <https://www.oecd.org/about/>

2 <https://oecdgroups.oecd.org/Bodies/ShowBodyView.aspx?BodyID=1837&Lang=en>

3 <https://www.oecd.org/digital/ieconomy/>

れている。OECDではステークホルダーのトラストを得ることは、デジタル経済において重要な役割であり、複雑なグローバル環境における「強力なツール」になると捉えている。今日のデジタル経済において、成功した多くの企業は社会や環境の課題に迅速対応しており、ガバナンスを維持・強化し、ステークホルダーの期待に応えることで市場価値を最大化していると認識されている。OECDでは、トラストを高めることがビジネスの成功への重要な要素であると捉え、トラストの強化に取り組む企業や組織は、長期的な価値が保証されるとして政策提言を取りまとめている。

OECDでは、データトラストを高める重要な施策を4つのカテゴリーで区分している。⁴



図表II-14. OECDデータトラストの重要施策

3.1 プライバシーへの対応

OECDは、数十年にわたってプライバシーの尊重を基本的な価値として向上させ、国境を越えた個人データの自由な流れを促進する上で重要な役割を果たしてきた。基本的人権を尊重し、国内のプライバシー法制と調和させ、国際的なデータの流れを中断させないために有効なガイドラインが必要であると考えている。プライバシー対応と越境する個人データ移転について、OECDのプライバシーガイドラインの見直しが進んでいる。これは、プライバシーに関するOECDの取組みの基礎となっている。⁵

1980年、OECDプライバシーガイドラインと呼ばれる「プライバシー対応と個人データの国際流通についてのガイドラインに関する理事会勧告」は、世界共通となる個人情報保護の基本原則を規定した指針として公開された。OECD 8原則は、個人情報保護やプライバシー対応に関して、グローバルの法

規制の規範となっている。

2013年、OECDは初めてプライバシーガイドラインを改訂した。OECDの提言内容を見直し、プライバシー法制における執行協力を強化した。特に下記の2テーマが特徴となっている。⁶

- ①プライバシー対応におけるリスク管理アプローチ
- ②相互運用性向上によるグローバルなプライバシー対応

さらに現在、OECDプライバシーガイドラインの改訂や勧告附属文等の追記が検討されており、追加的なガイダンスを提供することを目指している。AIやIoTなどの新たなデジタル技術を踏まえて、個人データの収集や利用目的、安全管理措置などを規定した追加的な指針が必要であると考えられている。

具体的には、①説明責任、②データローカライゼーション、③民間部門の個人データへのガバメントアクセス、④規制のサンドボックス制度が取り上げられている。

3.2 データガバナンス

データガバナンスは一般的には、効果的かつ効率的に使用するためにデータマネジメントのすべての活動を統制することを意味する。ビジネスで利用するデータの品質とセキュリティを保証し、そのプロセスにおいて責任を確立することである。特にOECDにおいては、データへのアクセスと共有を強化することをデータガバナンスの課題として取り組んでいる。

データへのアクセスと共有は、コロナ感染症への対策やSDGs（持続可能な開発目標）の達成など社会的課題の解決に重要な役割を果たすと考えられている。しかし、データへのアクセスと共有はリスクを伴うため、デジタル経済と実社会がデータを十分に活用できなくなる可能性を示唆している。また、データアクセスを制限することは、共有することを躊躇させることにつながる。

2021年、EASD（Enhancing access to and sharing of data）の実現に向けて、「データへのアクセスと共有の強化の理事会勧告」が採択された。この勧告は、政府が一貫性のあるデータガバナンス

4 <https://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm>

5 <https://www.oecd.org/digital/ieconomy/privacy.htm>

6 <https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm>

ポリシーとフレームワークを策定し、国や組織などコミュニティにおいてデータの潜在的なメリットを引き出し、サポートすることを目指している。データ利用においてトラストを向上させ、データへのアクセスと共有を促進して、効果的かつ責任あるデータガバナンスを実現することを狙いとしている。⁷

3.3 デジタルセキュリティ

デジタルセキュリティに対するOECDの取組みは、デジタル技術の可能性を阻害することなく、トラストを高める政策提言を策定することを目指している。「サイバーセキュリティ」ではなく「デジタルセキュリティ」としているのは、サイバーセキュリティが技術的な側面や法執行も含めた国際的なセキュリティの側面に着目しているのとは対照的に、デジタルセキュリティはサイバーセキュリティの経済的および社会的側面を主に対象としていることが理由である。デジタルセキュリティへの取組みは、デジタル技術の恩恵を最大化させ、トラストを向上させることで、ステークホルダーとの間で有効な情報共有を図るものである。⁸

2015年、「デジタルセキュリティのリスク管理に関するOECD勧告」が採択された。これは2002年に採択された「情報システムとネットワークのセキュリティに関するOECDガイドライン」に代わるものである。経済的および社会的な繁栄を目指し、デジタルセキュリティリスク管理に関する提言がなされた。この勧告は経営者に対して、デジタルセキュリティリスク管理を技術的な問題として扱うのと同時に、経済的および社会的な意思決定を体系的に実行することを要求している。イノベーションを促進するために、デジタル技術の可能性を阻害することなく、デジタルセキュリティに対処する方法として8つの原則が示された。⁹

【一般原則】①意識・スキル・エンパワーメント、
②責任、③基本的人権、④協力

【運用原則】⑤リスク評価と対応サイクル、⑥セキュリティ対策、⑦イノベーション、
⑧継続性

現在、2022年末に向けて勧告の改訂作業が進んでいる。

3.4 オンライン上の子供の保護

2021年、「OECDオンライン上の子供の保護勧告」が採択された。勧告は、インターネット上の青少年保護について、保護者の役割や官民一体での取組み、国際的な目標の必要性について規定している。オンラインのリスクから子供を保護し、デジタルの世界が提供する機会と利益をバランスさせることを目指すものである。特に重要なテーマについて、2つの課題が提起されている。¹⁰

①子供のプライバシーとオンラインデータ

②子供に安全で有益なデジタル環境を確保するためのステークホルダーの役割

昨今、多くの子供はスマートフォンを所有しており、生活時間の多くをオンラインで過ごすようになった。デジタル環境は子供に多大なメリットをもたらし、コミュニケーションや教育など新しいツールを提供することにつながった。しかし同時に、ネットいじめ、プライバシー侵害など深刻なリスクも大きな課題となっている。これらのリスクは、コロナ感染症により従来以上に深刻になってきている。子供にとって安全で有益なデジタル環境の構築を促進するため、国際協力の重要性を強調している。

4. おわりに

企業活動のグローバル化において、データとデジタル技術を活用することにより、特にクラウドサービスなど国境を越えた情報の流通が容易になった。グローバル事業を成長させるために、ステークホルダーのトラストを得ることは社会的にも経済的にも重要な役割になってきている。今まで以上に、国際的な調和のとれた自由な情報流通の仕組みや、プライバシーに配慮することへの取組みが求められている。

7 <https://www.oecd.org/sti/ieconomy/enhanced-data-access.htm>

8 <https://www.oecd.org/digital/ieconomy/digital-security/>

9 <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.htm>

10 <https://www.oecd.org/sti/ieconomy/protecting-children-online.htm>