データガバナンス・ガイドライン

（案）

2025年〇月〇日

デジタル庁

はじめに

- データガバナンス・ガイドライン（以下「本ガイドライン」という。）は、主として企業の経営者を対象に、Society 5.0 の実現に向け、企業が DX（デジタル・トランスフォーメーション）に取り組むに当たり、その保有するデータを最大限に活用することで、当該企業の持続的な企業価値向上に繋げていくための、データガバナンスの必要性とその在り方、実践するに当たっての要点や留意すべきポイントをまとめたものである。

- 対象（想定読者）は、上場・非上場にかかわらず、広く企業経営者とするが、例えば、本ガイドラインに掲げた事項を基に、各々の事業の状況に応じて実践すべき事柄を明確にし、自社内に広く周知を図っていただくとともに、株主をはじめとしたステークホルダー[1]との対話にも活用していただき、企業の持続的な DX に繋げていくことを目的としている。

経営者によるデータガバナンスの重要性について

- 我が国におけるデジタル化の未来ビジョンである Society 5.0 では、世界中の無数の異なる「モノ」から収集されたデータが、汎用性の高い「システムやソフトウェア」を介して横展開されることが想定されており、現時点において既に、家電製品から自動車まで、IoT―あらゆる製品に搭載されたセンサーが収集する膨大なデータは、経済や社会が機能するために不可欠となってきている。

- このようなデジタル化に伴う経済社会の変革に対応するために、個々の製品・サービスに依存した思考から、データを分野横断的に活用することで生産性や付加価値を向上していくといった、データを起点とした戦略が求められている。そして、生成 AI を始めとする AI の急速な普及と汎用化は、この方向性を不可逆のものとしていくと考えられる。

- 海外では、既に社会全体でデータの生成・収集・利活用等の先進事例が数多くみられる。欧州では「データ・スペース」のコンセプトの下、自社内だけではなく関係するステークホルダーや産業界、さらには国境をまたいでデータを共有・連携する取組が増加しており、例えば Gaia-X や Catena-X といった取組が、多くの企業の参加の下で推

[1] 本ガイドラインにおける「ステークホルダー」とは、「企業経営をするうえで、直接的又は間接的に影響を受ける利害関係者」を指しており、当該企業の商品・サービスを直接的又は間接的に購入する顧客や消費者、さらに保有データに関係する個人等が含まれるものとしている。

進されている。国内においても、ウラノス・エコシステム[2]等の企業間さらには産業界でのデータ連携に向けた取組を進めようとする動きも出てきているが、諸外国に比して、我が国の企業・産業におけるデータの利活用はまだ限定的との指摘が多く聞かれる[3]。こうした問題意識の下、現在、政府のデジタル行財政改革会議において、我が国のデータ利活用制度の在り方について基本的な方針を策定することが示されており、医療・金融・教育・産業の分野における、社会起点のデータ共有、個人起点のデータ共有、産業分野別のデータ利活用、官民でのデータ利活用、アーキテクチャ・システム等の論点について検討が進められている。

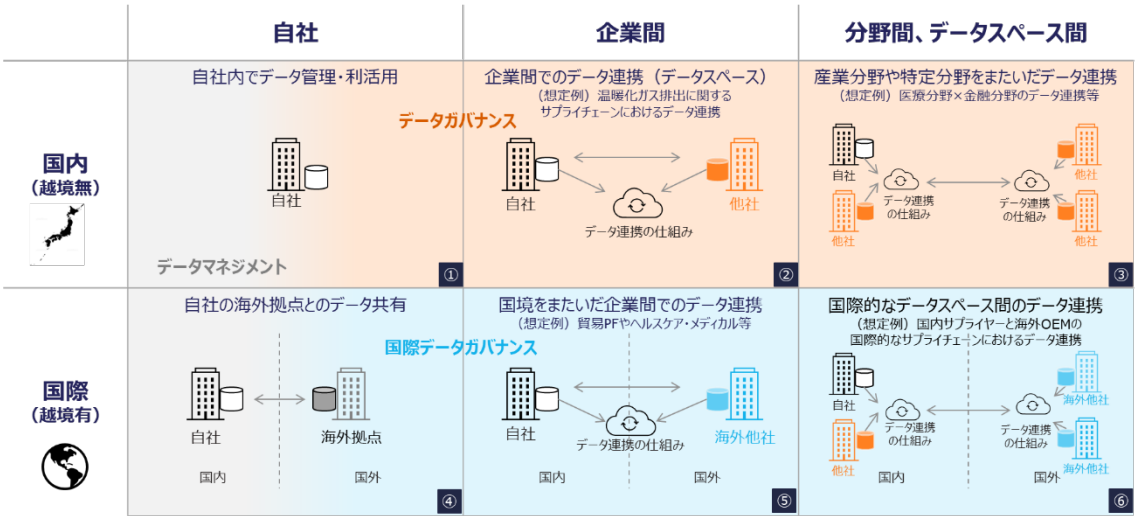
- 元来データは、特定のハードウェア等に縛られることなく、システムや組織に対して中立性を持ち、求められる規範等に則って適切に扱われることによって、自由に流通・利活用され、付加価値を創造することが可能となる。そして、データは、生成・取得から消去に至る過程（ライフサイクル）の各場面に応じて、処理や連携を経ながらデータとしての性質も変化していく。情報セキュリティでは、機密性・完全性・可用性の三要素が代表的な観点として挙げられるが、従来はそのうち機密性、つまり権限のない第三者への漏洩防止に重点が置かれ、「外に出さないこと」を最優先とする傾向が主であった。しかしながら、上記のように特定のハードウェアやシステム・組織に対して中立的なデータの利活用を促進し、企業価値を向上するには、守るべきデータを守りながら、データを共有・連携したい相手に対しては、自社やサプライチェーン内のステークホルダー間を越えて共有・連携することを前提に、相互運用性（インタオペラビリティ）を実現しておくことが重要となる。（図1参照）

---

[2] 信頼性のある自由なデータ流通（DFFT）の実現に向け、運用者や管理者等が異なる複数の情報処理システムを連携させ、企業・業界を横断したデータの利活用を促進するための官民協調の取組の総称（例：データ連携に必要となる仕様や標準等の策定、データ連携システムの開発、必要となる政策・制度の整備等）
https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos.html

[3] データを他社に提供することへのリスクやデメリットへの意識が強く、データを他社から受け取り、自社のデータと連携することで価値創造が促進されるとの意識が浸透されていないためと考えられる。

図 1.: データの共有・連携における環境の変化



- 図1. のように、自社・自組織を越えて、あるいは法域の異なる国や地域を越境してデータを共有・連携する場合、例えば、データの越境移転等が、グローバルサプライチェーンの観点からビジネスの前提となる場合、異なる法域における法令への遵守と、国際ルールへの適合性、データに付随する自社・自組織の権利・利益の保護を確保するため、各社が自社の事業領域において準拠するべき手順や技術的手段について、各々のポートフォリオを踏まえて適切に組み合わせる必要がある。

- その際、主に自社内のシステム単位で安全・安心を担保していた従来の情報セキュリティマネジメントでは、十分な安全性を確立できなくなってきている。データのライフサイクルの各段階において、それぞれの段階における法域を意識しつつ、実際にそのデータを移転するのか、あるいはデータは所定の法域内に置きながら、それを参照するためのアクセスを容認するのかといった、データ共有・連携の個別の実態も踏まえつつ、ルール・技術・プロセスを組み合わせたデータセキュリティを実施することが不可欠となる。

- 以上述べてきたように、データの利活用を最大化するためには、データを起点として、我が国を含む関係国や地域における法令の遵守を大前提におきながら、社会の状況変化や先進技術に迅速に対応し、持続的かつ組織的にデータを利活用し、企業価値の向上に繋げる企業の総合的な能力（データマチュリティ）の不断の向上が求められてい

る。データマチュリティ[4]の向上は、自社のデータマネジメントやデータガバナンスのレベルの向上に繋がることはもちろん、データを共有・連携するパートナーを選定する上で、相手方がデータを適切に扱える企業か、信頼できる企業か、といった、パートナー選定の際の重要な目安ともなり、企業のレピュテーションの向上にもつながる。即ち、データマチュリティの向上策における議論は、投資家等のステークホルダーとの対話に資する取組にもつながる。

- 一方、AI やエッジコンピューティングといった先進技術の登場によって、データは必ずしも人が扱うだけではなく、システムやソフトウェアによって自動的に生成・取得、加工・利用、移転・提供、保管されるようになってきている。AI 等の先端技術は、企業に飛躍的な価値をもたらすことが期待される一方で、これらの技術はまだ発展途上であり、今後急速に進化していくことが予測されるため、その取扱いに関しては従前の十分な検討と、運用中においても、逐次対応方法の見直しを図ることが適当であると考えられる。

- これまでは、自社・自組織内のデータ管理である「データマネジメント[5]」が求められていたが、上述のとおり、産業分野を越えた、さらにはグローバルなサプライチェーン視点でのデータ共有・連携が進みつつある中において、組織・産業・国境・法域をまたいだデータの生成・取得・利活用等を最大限に行うためには、各国の法令や国際ルールへの対応、リスクの把握、データのアクセス・分析・制御等にかかる技術導入と活用練度の向上、関連する社内・組織内プロセスの改善、データ管理・活用を担う人材の育成・確保[6]等、多岐かつ重層的な課題に対応しなければならない[7]。このような課題への対応は、我が国を含む関係国や地域における法令の遵守を大前提として、データの取り

---

[4] 組織のデータ成熟度、即ち企業の戦略的あるいは事業経営上の重要性に基づき、データを有効に使いこなせる能力であり、英国では政府機関向けデータ成熟度評価のためのフレームワーク(Data Maturity Assessment for Government: Framework)によって、5 段階の水準(Beginning・Emerging・Learning・Developing・Mastering)が設定されている。
https://www.gov.uk/government/publications/data-maturity-assessment-for-government-framework/data-maturity-assessment-for-government-framework-html

[5] 本ガイドラインにおいては「データマネジメント」は主にデータを扱う現場での施策としている。一方、データを企業の経営資源として如何に有効に活用できるかという観点から、ステークホルダーへの説明に資する活動として「データガバナンス」を位置付けている。
付録. 関連 URL:「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」参照
https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework.pdf

[6] 独立行政法人情報処理推進機構「信頼できるパートナーになるためのデータガバナンス読本」
https://www.ipa.go.jp/digital/data/f55m8k0000005msd-att/dsa004-data-governance-guidebook.pdf ページ 8 参照。

[7] 国際の場では、日本が提唱する DFFT(Data Free Flow with Trust)の実現に向けて 2023 年に OECD 内に IAP(International Arrangement for Partnership)が設立され、具体の議論を始めている。 DFFT URL:https://www.digital.go.jp/en/policies/dfft

扱いに対する顧客・取引先をはじめとする様々な主体への説明責任の観点からも、今後ますます求められていく。

- 以上のとおり、個社の DX を越えた経済社会全体の構造変革を踏まえ、伝統的な経営資源である人・モノ・金に加えて、データを新たな経営資源として捉えるとともに、法域や国境・産業・組織等をまたぐデータの共有・連携において、各国の法令等の遵守を前提に、情報システム単位での対応ではなく、データに焦点を当てた保護措置（データセキュリティ）等を実施した上で、データを最大限に利活用する「データガバナンス」をアジャイルに実施していくことが、経営者のトップダウンによって取り組むべき重要な経営課題になってきている。

以上を踏まえ、本ガイドラインでは、特に、ステークホルダーとの相互信頼の下で、データの相互運用性を確保しながら、データの共有・連携・利活用を通して企業価値を高めていくために、以下をデータガバナンスの4つの柱としている。

① 自社の事業領域において、法令やルールが変化し続ける国や地域との相互運用を可能とする、「越境データの現実に即した業務プロセス」

② データのライフサイクルを踏まえ、自社が直接には管理できない、共有・連携先に対するルール・技術・プロセスを組み合わせた、「データセキュリティ」

③ 持続的かつ柔軟で組織的に、データを最大限に利活用できる、企業の総合的な能力である、「データマチュリティ」

④ 現在も急速な進化を続ける「AI などの先端技術の利活用に関する行動指針」

さらに本ガイドでは、国際と国内環境の変化に伴う事象に対して経営者が取るべき行動、データ責任者（CDO：Chief Data Officer）や専任部門等[8]が取るべき対応について提示している。

経営者に求められる視点

- データガバナンスの目的は、先に述べた国内外の法令や社会規範の変化、技術の急速な変化に対する守りの側面だけではなく、自社の直接の影響が及ぼせない環境下におけるデータの利活用による「価値の創出」や「相互信頼の醸成」、「データ利活用の公正性の確保」等を通して、企業価値を絶え間なくアジャイルに向上していくことにある。

- このような形でデータガバナンスを実施するに当たっては、自社内の各事業のデータを横断的に取り扱うことが必要となる。そのためには、データについての責任を持つ CDO や専任部門等とデータを生成・利活用する各部門の間に加え、コーポレートガバナンスを担う責任者や部門との間において、データの利活用とリスク対応策の策定、結果の評価、施策の見直しといったサイクルを、恒常的かつアジャイルに回すことが不可欠となる。

---

[8] 本ガイドラインにおいては、企業におけるデータガバナンスを推進するためには CDO や専任の部門を置くことが重要な手段であると考えるが、それらの設置自体が目的なのではなく、それ以外の手段も含め、個別企業の実情に応じ、データを最大限に利活用できる体制を構築することが望ましい。なお、CDO や専任の部門を置くこと自体は DX 認証の必須条件ではない。CDO 又は類する組織の役割等に関しては、
付録. 関連 URL「Data Spaces Academy」（情報処理推進機構）
https://www.ipa.go.jp/digital/data/data-spaces-academy.html#the-chief-data-officer-handbook における「データを軸にした司令塔 CDO 読本」を参照。

- データガバナンスは経営者の責任として、強いリーダーシップの下で実施すべき施策であり、実行するに当たっては、以下の視点を意識しながら、後述の4つの柱等について取り組むことが重要である。

経営ビジョンと DX 戦略との連動

✓ データを最大限に活用して持続的に DX を実現し、企業価値を向上させるためには、経営ビジョンと表裏一体で推進する必要があり、DX 経営による企業価値の向上を目的とした、「デジタルガバナンス・コード [9]」と整合を図ることが適切である。

経営者による説明責任

✓ 従来の企業経営におけるデータの取り扱いにおいては、主に情報を収めたシステムを当該部門が管理し、情報を扱う現場では、定められたガイドラインに沿って運用することで遂行されていた。しかしながら、企業経営においてデータの利活用を進める中では、収集したデータに誤情報や個人情報が含まれていたり、ステークホルダーとデータを共有・連携した際や越境等した際に、共有先の国・地域の法令に触れたために、多額の賠償金を請求されたり、企業のレピュテーションが著しく侵害されるといったリスクが高まっている。

✓ したがって万が一のインシデントが発生した際には、事象の正確な把握に基づく最大のインパクトを予測し、国内外のステークホルダーや社会に対して、経営者が説明責任を果たすことが極めて重要となる。

✓ また、通常時の株主や投資家、社会に対する説明責任においては、自社が正確かつ安全なデータを他者と連携することで価値を最大化し、その能力（データマチュリティ）を向上していることを公表して行くことが、データ駆動型社会とも言われる時代に向けたサステナビリティ・トランスフォーメーション（SX）[10]の要素として、高

---

[9] 付録. 関連 URL:「デジタルガバナンス・コード 3.0 ～DX 経営による企業価値向上に向けて～」
https://www.meti.go.jp/press/2024/09/20240919001/20240919001-1.pdf
において、DX 経営における望ましい在り方の一つとして、「サプライチェーン内の取引先や多様な企業とのデータ連携を行うとともに、データガバナンスに関する法令やガイドライン等に従っている。」とされている。（ページ 9）

[10] SX（サステナビリティ・トランスフォーメーション）については、経済産業省「SX 研究会」における付録.関連 URL:「伊藤レポート（3.0）」参照
URL:https://www.meti.go.jp/press/2022/08/20220831004/20220831004.html

く評価されることが期待される。したがって、ステークホルダーへの説明責任を果たす観点からも、データガバナンスに取り組むことが重要となる。

データを最大限利活用できる体制の構築

- ✓ 企業経営を支えるデータ責任者として、CDO を設置する等、データを重要な資産と位置付け、価値創出に繋げるための体制整備を行うことが、経営者にとって重要な責務である。
- ✓ データの利活用によって各事業の利益の最大化と効率化を図り、企業価値の向上に結び付けるためには、人・モノ・金といった経営資源の配分を踏まえ、個別の事業分野を超えて、企業全体の運営や経営判断に資するためのデータ利活用のあるべき姿を、CDO 等の下で見直す必要がある。経営者のリーダーシップの下で、CDO 等が他の CxO や個別事業の責任者等と密接に連携できる体制構築に注意を払いながら、現在の情報連携システムの見直し[11]を行うことが不可欠である。
- ✓ また、情報連携システムの見直しに当たっては、経営者自身が、株主やサプライチェーン等におけるステークホルダーとのコミュニケーションを図りながら、経営ビジョンや DX 戦略との整合を図る必要がある。

企業文化への定着と人材の育成

- ✓ データを最大限に活用し、企業価値を向上し続けるためには、データが持つ価値とはらむリスクを、利活用する現場を含めて全社的に理解する必要がある。データの利活用による持続的な企業価値の向上につながる企業文化は所与のものではなく、データガバナンスを検討する段階から、目指す企業文化を見据え、経営方針として周知することが重要である。
- ✓ また、データをより有効に企業価値の向上に資するためには、データの分析や利活用に関わるスキルを向上するだけでなく、利用する AI モデルのアルゴリズム に適したデータに加工するプロンプトエンジニアリング等の、専門性の高いスキルを持つ人材の採用・育成も不可欠である。

[11]情報連携システムの見直しに当たっては、扱うデータの所在とデータに付随ずる法益への十分な注意が必要である。

- ✓ そして、変化する国内外の法令や国際ルールの調査や、破壊的イノベーションをもたらす可能性のある最新技術に対する感度を上げるための、人材育成、専門性の高い組織の編成、外部組織や有識者の活用も重要となる。

データガバナンス実装における４つの柱

1. 越境データの現実に即した業務プロセス
2. データセキュリティ
3. データマチュリティ　―価値を生み出す組織の総合力―
4. ＡＩなどの先端技術の利活用に関する行動指針

これまでの議論を踏まえ、本ガイドラインにおける上記データガバナンスの4つの柱について、以下に「基本となる考え方」「経営者が認識しておくべきこと」「望ましい方向性」を記載する。

「望ましい方向性」については、原則として、経営者がデータガバナンスについて取り組む際に参照していただくことを想定しているが、併せて CDO が自ら取り組んで頂くことが望ましい事項についても含んでいる[12]。

[12] 本ガイドライン「望ましい方向性」に記載の事項のほか、「付録. 関連 URL」に記載の資料やガイドライン等も参照のこと。

1. 越境データの現実に即した業務プロセス

1-1. 基本となる考え方

- 国外の法令や国際ルール、データを共有・連携する当該国や地域の規制等は常に更新されるとの認識の下、自社の研究開発、製品設計、製造、金融、マーケティング、販売、販売後のサービス、そして規制当局の各種承認といったバリューチェーンから、データを共有・連携する国内外のステークホルダーにわたる業務プロセスを明確にし、データのライフサイクルにわたって、利活用状況の可視化や可能な限りのトレーサビリティを確保する。

- 越境データの業務プロセス策定に当たっては、特に以下の状況におけるリスクへの理解を深め、データの越境移転等の現実に即した対策を図る。

  ① 当該国や地域における現在の法令や国際ルールに基づくリスクへの対応

  ② データの所在位置を踏まえたデータに付随する法益の確保

  ③ データの共有・連携先やサービサーの行為に起因するリスクへの対応

  ④ 業務プロセスやガバナンスの複雑さに起因するリスクへの対応

1-2. 経営者が認識しておくべきこと

- データの越境移転等におけるリスクは、当該国や地域、国際ルール等による一方的な規制導入によっても変動する。自社の海外拠点とのデータの共有・連携においても、双方のデータ共有・連携における現在及び近未来のリスクを念頭に置き、対応を進める必要がある。

- 近未来のリスク予測においては、当該国及び地域以外の動向にも、常に注意を払う必要がある。

- データを共有・連携する海外のステークホルダーにおいても、当該国や地域におけるデータローカライゼーションの導入や、異なる商慣習による目的外へのデータ利活用や漏洩等、業務プロセスを策定した段階では完全には予測できないリスクが生じる可能性がある。

1-3. 望ましい方向性

- データを共有・連携する当該国や地域の法令、国際ルールの現状に加え、今後予測される更新の方向性を第三者等を使って調査し、海外の自社拠点との双方向におけるデータの共有・連携や、ステークホルダーとの間で生じ得るリスクの評価を行い、優先して対応が必要なリスクに対して打ち手を講じている。

- 自社の海外拠点にあるデータに当該国の法域外からアクセスしたり、法域外へデータの越境移転等を行う場合には、自社の組織間であっても、当該国・地域の法令を遵守するよう細心の注意を払っている[13]。特に、当該データに第三者によって作成されたデータや、医療・金融・教育等の個人情報等が含まれる場合には、それらのデータに付随する法益を侵さないようにしている。

- 他国の関連法令や国際ルールを、外部機関等を使って恒常的に調査・モニタリングし、生じ得るリスクの評価と対応策は、現状の業務プロセスの策定経緯を把握している自社で行い、第三者や有識者による評価を受けている。業務プロセスを変更する際にも、関連する組織やステークホルダーと情報を共有したうえで、ルール等も併せてアジャイルに見直しを図っている。

- 海外とのデータの共有・連携においては、双方のシステムやデータ連携基盤等の違いによって、あるいはそれらの運営者によって、リスクや障害が生じる可能性があることから、データを共有・連携する取引先等のステークホルダー、特に、サプライチェーンにおいては国内・国外のすべてのステークホルダーとの間で、契約やルールを予め明文化しておくことによって、瑕疵責任等を明確にし、適時見直しを図っている。

- 一方でデータの共有・連携の真の目的は、DX・企業価値の向上にあることから、柔軟で拡張性の高い基盤(プラットフォーム)やツールを実装することで、データの相互運用性を確保し続けながら、そこから生じる業務プロセスやガバナンスの複雑さに起因するリスクへの対応策を採っている。

---

[13] 付録.関連 URL「産業データの越境データ管理等に関するマニュアル」を参照。
https://www.meti.go.jp/press/2024/01/20250127001/20250127001.html

2. データセキュリティ

2-1. 基本となる考え方

- 自社が取得・保有するデータに付随する権利を実効的に保護していくために、焦点を「情報システム」から「データ」に移し、データを中心にセキュリティ要件を組み替える発想の転換が必要となる。

- データセキュリティは、情報セキュリティの様に主にシステムや技術によって確立できるものでは無く、データを扱うためのルールや契約等の制度及びそれらを扱う人材等も重要な要素となる。

- 具体的には以下の要素を考慮する必要がある。

  ① データを共有・連携するステークホルダーの信用度に応じた対応

  ② データの所在位置を踏まえたデータに付随する法益の確保

  ③ データ利用の正当性

  ④ データの完全性・最新性の担保

  ⑤ データの状態と所在の可視化

  ⑥ 明文化されたルールや制度・プロセス等

  ⑦ データの状態・活用の段階に応じたリスクや適用される法令制度の分析・把握

  ⑧ 以上を、データのライフサイクルを通して許容可能なリスク内に確立すること

  ⑨ 人材育成とデータリテラシー

2-2. 経営者が認識しておくべきこと

- 従来は主に情報システム単位でのセキュリティマネジメントを実施してきたが、データの利用主体は単一ではなく、必要となるデータの品質や適切な保護手段もデータのライフサイクルによって異なる。自社内だけでなく、データを共有・連携するステークホルダーにわたるデータのライフサイクルにおいて、求められるデータの品質を CDO 等に精査させる必要がある。

- データを共有・連携する相手には、シームレスに共有するための制度・技術・プロセスを実装していく一方で、共有や連携を望まない相手にはデータへのアクセスを遮断する必要がある。このようなデータセキュリティ対策を講じることは、顧客・取引先をはじめ様々な主体からの信用を担保する上でも重要となる。

2-3. 望ましい方向性

- データの生成・転送・処理・可視化・連携・保管・消去といったライフサイクルを踏まえ、法域を越境することによって生じるリスクや、それぞれの段階においてステークホルダーに起因する潜在的なリスクを把握し、それらに対処するための方針を策定している。その際には、「基本となる考え方」に示された要素を考慮している。

- データの共有・連携は、信頼のおけるステークホルダーの間で行うべきであることから、当該国や地域の法令や国際ルール等によって、データの共有・連携が強制される場合においては、相手の信用性やデータマチュリティのレベルに応じてリスクを分析し、万が一の場合に備えた対応プロセスを予め策定してある。

- 取得したデータに関しては、その利活用をデータの作成主体によって認められた範囲にとどめ、データ利用の正当性を守らなくてはならない。特に個人情報に関わるデータを扱う場合には、細心の注意が必要となる。
  このため、例えばデータの利活用が人を介さず、ソフトウェアやシステムによって自動的に行われる場合には、AI 等を用いて、個人情報やバイアスの掛かったデータ等を分析し、削除したり匿名化するなどの、適切な処理を行う仕組みを導入している。

- また、取得するデータに対しては、その完全性に注意を払う必要があるため、データが信頼できる出所から発生し、改ざんや漏洩が無いこと、また、データを生成・発信した主体が偽装されていないことなどを担保している。データを利活用する際には、契約や明文化したルールによってデータの完全性を担保し、保証できないデータは利用しないか、少なくともその完全性を前提とした組織内での利活用に留め、第三者への共有・連携は行わないようにしている。

- データの最新性に対しても注意を払う必要があり、特に取得したデータを何らかの判断の為に分析したり、そこから2次データを生成したりする場合には、元のデータが古いと期待する成果が得られない可能性があることから、少なくともデータを生成する主体は、そのデータに必要な精度に合わせた時刻を付すようにしている。

- データの所在や取り扱いについて組織横断的な可視化を行い、適切な管理体制を置いている。データが組織内を移動する・組織外に転送される場面を問わず、データのライフサイクルに応じたルールを設定し、契約、暗号化等の技術的防護策やデジタル ID 等を通したサプライチェーン横断的なデータの管理・利用を検討している。特に、クラウドサービスを利用する際には、データが置かれる法域に対して、十分な注意を払っている[14]。

- データの利用期間がその生成主体によって定められていたり、永く保管していたりすることによって、データの生成主体や第三者にリスクが生じ得るデータに関しては、確実に廃棄している。

- 特に、例えば一部の医療データや教育データのように、個人情報として保護すべき度合いの高いデータ等は、データを共有・連携した相手が不当な活用をしたために、データを渡した主体の責任が問われることも起こり得る。一方、データを共有した先での利活用の実態を把握するには困難を伴うため、少なくともデータを直接共有する相手とは、予め責任の範囲を法的文書として残しておく。

- データセキュリティの実装に際しては、従来、機微な情報として一括りに扱われていたデータ群を、データの単位で、その重要性と共有・連携によって生じ得るリスクの大きさに応じたレベリング[15]を行い、各レベルに応じた技術的手段を施すとともに、明文化したルールや制度・プロセスを策定している。データの利活用による価値の創出が本来の目的であることを踏まえ、過度に「守りの固い」運用とならないようにしている。

---

[14] 事業に必要となるデータは当該国や地域に置かなければならないという、所謂データローカライゼーションの法制化が進んでおり、その動向には十分に注意を払う必要がある。

[15] 付録. 関連 URL:「政府機関の情報セキュリティ対策のための 統一基準(第 3 版) 解説書」 www.nisc.go.jp/pdf/policy/general/k303-072c.pdf における機密性 1, 2, 3 との整合性を確保しながら、例えば、「機密」「秘密」「営業秘密」「社外秘」「その他」といったように複数の水準を設定することが望ましい。
「営業秘密」に関しては、経済産業省ホームページ「営業秘密～営業秘密を守り活用する～」を参照。 https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

3. データマチュリティ　―価値を生み出す組織の総合力―

3-1.　基本となる考え方

- データマチュリティは、組織がデータを使いこなし、データの価値の最大化とリスクの最小化を持続的に行い、最大のパフォーマンスを出しているのかどうかを、明確化し、改善するための、企業の総合的な能力である[16]。

- 具体的には、準拠すべき法令と利用すべき技術、そして運用の方法を重層的に分析し、「越境データの現実に即した業務プロセス」や「データセキュリティ」の施策等をもって、以下を実現・向上し続けることで、DX・企業価値の向上に結び付けられる状態を目指す。

  ①　継続的なプロセスの改善

  ②　トラブルの予測と対策、経営者の説明責任

  ③　データを利活用する現場と経営者を結ぶ体制

  ④　AI などの先端技術やデータに対する費用対効果の分析

  ⑤　レガシーシステム内のデータをAIや新しいデータ基盤等で活用可能とする[17]

  ⑥　人材育成と、ステークホルダーに渡る情報の共有

3-2.　経営者が認識しておくべきこと

- データマチュリティの不断の向上が、DX や企業価値の向上に資する重要な要素である。

---

[16] 具体の内容に関しては、付録. 関連 URL「Data Spaces Academy」（情報処理推進機構）https://www.ipa.go.jp/digital/data/data-spaces-academy.html#the-chief-data-officer-handbook　における「データ経営の総合力を高めるデータマチュリティ読本」を参照

[17] 古い社内基盤（情報システム等）に格納されたデータを、AI や新しいデータ基盤等で活用できるようにデータの形式を更新することなど（データのモダナイゼーション）。

- ステークホルダーとの相互信頼を醸成し、社会への責任を果たすために、現在の自社のデータマチュリティのレベルと具体の施策を公表することが、株主や投資家にとっては、企業のサステナビリティとして評価され得る。

3-3. 望ましい方向性

- データマチュリティ向上のための方針を策定、展開し、結果を評価することで、更なる改善を施すというループを回し続ける。結果の評価は CDO 等のリーダーシップのもとで、事業の現場から独立した監査組織や外部有識者によって行われている。
- 方針の策定に当たっては、データの処理に際し、例えばデータ品質の管理や問題発生時の処理を適切なプロセスに基づき行うなど、データの価値の最大化とリスクの最小化を持続的に行っているかについて、一定の水準（スケール）を決め [18]、現在のマチュリティレベルを自己審査・評価したうえで、その結果を組織内へ周知するとともに、次に目指すべきレベルと具体の施策を展開している。
- 不測の事態に対しては、予め策定したインシデントの影響水準に則して迅速な対応を取り、経営者自らが説明責任を果たしている。
- CDO 等の下で各組織の責任者と役割を明確にし、経営の迅速な対応が可能な体制を構築している。データの標準化やデータの品質 [19]を定義する様々な条件を整備し、ツールやシステム、各種の基盤等を活用することで、現場での利活用の状況を CDO・専任部署や同様の機能を有する組織、さらには経営者に対して可視化している。
- 先端技術の採用や新しいデータの生成・取得に対する提案は、その費用対効果の分析の下で CDO 等が経営者に提言し、追加で必要となる施策と併せて展開を図っている。株主の判断を必要とする場合には、CDO 等が提案主体となるとともに必要に応じて社外の有識者の協力を得ている。
- 古い社内基盤のままで運用されている、所謂レガシーシステムのデータの活用やプロセスの可視化は、多くの企業・組織の共通課題になっている。これらのデータを AI や新しいデータ基盤等で活用できるよう、データ形式等を更新し、部門横断で

---

[18] 水準の策定に当たっては、CMMI（Capability Maturity Model Integration）における5つの評価水準等が参考になる。 ISACA CMMI URL：https://cmmiinstitute.com/cmmi/intro

[19] データ品質については、「データ品質」の要素 ISO/IEC 25012（データ品質の評価）における評価項目を参照。

の利用に適したデータ品質を実現する際には、将来的な自社・組織外とのデータ共有・連携を念頭においている。

- データマチュリティの向上には、全社的なデータリテラシーの向上だけではなく、高いデータスキルを有する人材を各組織の責任者等に置くことが不可欠である。CDO 等が主体となって、経営や人事部門と連携して人材の育成・採用計画を策定し、OJT をもって育成するとともに、そうした人材が評価・処遇される人事制度を構築している。
- データマチュリティのレベルは、自社だけでなく、データを共有・連携するステークホルダーのデータマチュリティの水準にも影響を受けるため、ステークホルダーにも自社の具体の施策を情報共有し、データマチュリティ向上への取組を共に進めることが望まれる。そして、それらステークホルダーや社会との相互信頼を醸成し続けるためにも、現在の自社の水準と具体の施策を社会に発信し続けている。

4. AI などの先端技術の利活用に関する行動指針

4-1. 基本となる考え方

- AI 等の先端技術を利活用する際には、技術の力を最大限に活かしつつ、社会や個人への悪影響を最小限に抑えるために、利活用するデータに関連する国内外の法令、サイバーセキュリティやデータセキュリティに関するガイドライン等[20]に従って方針を定め、データの収集、利活用、結果の公表や第三者への提供、更には提供先での利用に対する指針を策定し、自社内及びステークホルダーへの周知徹底を図る。

- AI は現在も進化途上にあり、AI モデルや組み込まれるアルゴリズムを含む AI システムが今後も急激に変化していくため、利用するデータに関わる上記各現場における行動指針を策定し、随時見直しを図る。

4-2. 経営者が認識しておくべきこと

- AI の利活用による企業価値向上の取組にとって、AI モデルに含まれるアルゴリズムに沿った学習データ・利用データの収集・整備は重要な要素である。

- AI 等の先端技術は、今後の急激な進化により、自社に飛躍的な価値をもたらすことが期待される一方で、収集された学習・利用データについては、データ処理のプロセスが「ブラックボックス」と言われることが多く、利用するデータに起因する個人情報に関わる問題、さらには安全保障上の重大なリスクにつながる可能性がある。

- AI や量子コンピューティングなどの分析能力の飛躍的向上は、機微なデータと機微でないデータとの線引きを困難なものにしている。自社の経営戦略にとって、機微なデータが何かを検討し（ノウハウなどの非構造化情報も含む）、本ガイドラインで示したデータガバナンスの3つの柱「データマチュリティ」、「越境データの現実に即した業務プロセス」、「データセキュリティ」の取組を踏まえた行動指針を、自社内のみならずデータを共有・連携するステークホルダーへも周知徹底することが重要である。

---

[20] 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」
https://www.meti.go.jp/policy/netsecurity/mng guide.html

- 自社のノウハウに関わるデータを過度に保護することで AI 化が遅れ、生産性が劣後することは経営上のリスクとなる。AI 開発事業者に学習データとして自社のデータを提供する際には、提供するデータや学習成果に対する機密保持契約等を結んでおくことで、競合他社等へのデータの流出や、チューニングされた AI の転用等を防止しておくことが重要である。

- AI 等の先端技術は飛躍的に進化するため、AI・IoT・量子コンピュータなどのシステム毎に、CDO 等の下で方針と行動指針を策定し、随時見直しと更新を図る。

4-3. 望ましい方向性

- AI 等の先端技術の力を最大限に活かしつつ、社会や個人への悪影響を最小限に抑えるために、企業としての方針を開示したうえで行動指針に展開し、その結果を評価して、必要に応じては公表等も行いながら、更なる改善を施すというループを回し続けている。

- 結果の評価においては、専門性の高いエンジニアに加え、法学、社会学、経営学等の専門家も含め、自社との直接の利害関係を持たない外部有識者の意見を反映している。また、行動指針の見直しを図るタイミングを判断する際にも専門的な知識が必要となるため、自社内での判断だけでなく、定期的に上記外部有識者の評価を受けている。

- チューニングされた AI が自社にとって「ブラックボックス」とならない様に、学習に用いたデータとともに、何故そのデータを使ったのかといった判断理由等の情報を、資料として自社内で管理している。

- 行動指針の策定に当たっては、「AI 事業者ガイドライン[21]」を参照するとともに、AI で利用するデータに関しては、主に以下の点を考慮している。

  ① 個人情報の保護

[21] 総務省・経済産業省「AI 事業者ガイドライン」
https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

個人情報保護法や欧州 GDPR 等の関連法令遵守のため、経営者の責任において、AI 等の先端技術の利活用における、個人情報の扱いに対するポリシーの策定・公表等を行うことにより、データに含まれ得る個人情報が保護されるよう、その重要性に応じた対応を図る。

② 機微なデータの保護

機微なデータを予め削除する場合でも、万が一の混入に備えて AI に機微な情報の削除や匿名化等の処理を行う仕組みを組み込み、AI の機械学習を実施した上で、確認テストとファインチューニングを含む対策を施し、個人情報に関わるデータ、ノウハウを含む企業の知的財産権利を尊重するための適切なセーフガードを導入する。

③ 関連するステークホルダーへの情報提供（透明性の確保）

AI でのデータの利用の仕方、AI の性質、目的等に照らして、例えば、以下について取りまとめた情報の提供及び説明を行うこと。

- AI に利用しているという事実及び活用している範囲
- データ収集及び個人情報等の削除方法等の手法
- 基盤としている AI モデル等に関する情報
- AI に掛けた結果の提供先が属する国・地域等において適用される関連法令等

④ 検証可能性の確保（説明責任）

AI や入出力データに起因する社会的問題や個人情報に関わる問題等が発生した場合の説明責任を果たすために、データ量およびデータ内容に照らした合理的な範囲で、AI システム・サービスの開発過程、機械学習、利用時の各プロセスにおける入出力データのログを記録・保存すること。

⑤ セキュリティの確保

AIとデータの双方に対して、アクセス制御の強化やデータの暗号化、データを確認したログを残すなど、サイバー攻撃に対する堅牢な防御を施し、定期的な検査やアップデート等によって、予期しない結果を引き起こしたり、悪用されたりしないよう、安全性を担保すること。

また、AI システムやクラウド型AIサービスに対する外部からの攻撃は、日々新たな手法が生まれており、これらのリスクに対応するための留意事項を確認していること。

⑥ 教育・リテラシー

AI に関わる者が、AI の正しい理解及び社会的に正しい利用ができる知識・リテラシー・倫理感を持つために、必要な教育を行うこと。

特に AI を利活用する現場では、その目的や利用するデータの範囲が予め明確にできなかったり、利用中に連続的に変化することがある。当事者が行動をセルフコント―ロール可能とするための教育も重要となる。

データガバナンス実装の先に向けて

本ガイドラインでは、Society5.0 の実現に向け、データを利活用することでDXを実現し、企業価値を高めるための「備え」を主に記述してきたが、データの利活用の最終的な目標は「企業価値の向上」にある。その実現のためには、データの相互運用性を向上することが不可欠であり、経営者のリーダーシップによって、自社内・ステークホルダー間に以下の意識付けを行うことが重要である。

- 最新技術への留意
  - コンピューティングパワーの飛躍的向上によって、社会が CPS[22]（Cyber-Physical System）を指向するようになっており、データの管理や利活用も RDB[23]（Relational Data Base） 等による定型的な大量データの解析に加えて、グラフ・データベース [24]等によるデータの関係性を基にしたリコメンデーションの創出等が重要視されつつある。また、欧州におけるデータ・スペース等の分散システム化の動きが強まるにつれ、分散型 AI[25]の研究等も活性化しつつある。
  - これらはデータの共有・連携にパラダイムシフトをもたらす、破壊的テクノロジーとなる可能性があることから、経営者は広く最新技術への感度を上げるとともに、特にこれらの技術動向に細心の注意を図る必要がある。
- 全社的なデータリテラシーの向上
  - データガバナンスは経営者の責任の下、現場を含む全社・全ステークホルダーにまたがる取り組みであり、現場のスキル向上なくしてはデータマチュリティは向上できない。
  - 日本の強みである現場の創意工夫が、データの利活用上でも実現できるように、データ関連の技術教育にとどまらず、企業価値の向上の為のデータの重要性とリスクといった、データリテラシー教育が重要である。
- データの共有促進によるサステナブルな社会の実現へ

---

[22] サイバー空間と現実世界が高度に融合されたシステム又はそのような社会

[23] 長年にわたり広く利用されてきたデータベースで、予め構造を定めた大量のデータを処理するのに適している。

[24] Graph DB：グラフ理論に基づき、データの関係性を重視した比較的新しいデータベース。

[25] Distributed AI：AI の計算処理を中央サーバーではなく、複数のデバイスやサーバーに分散して行う。

- データが企業内に滞留し利活用されないことは、企業や産業の課題にとどまらず、社会全体の非効率化や不便さに繋がる事例も現れている[26]。こうした社会課題については、企業が事業を展開する地域の他企業や組織・団体等と、より積極的にデータの共有・連携を行うことで、社会コストの低減や生活環境の改善に資するとともに、自社事業のステークホルダーの満足度の向上にもつながるといった効果が期待できる。

- 以上のように、データ連携・共有は経済社会全般にとっても有意義なものであり、そのようなデータ連携・共有を進めるためには、従来、機微な情報として一括りにして扱われていたデータ群を、データの単位で、現状を踏まえ機微な情報か否かを改めて見直し、機微性の低いデータは関係する事業者や社会と共有することで、結果的に自社の製品やサービスの価値を向上させたり、無駄な投資を防ぐことができる可能性が生じている。

- さらに、人口減少・少子高齢化が進む我が国においては、需要密度の低下により、これまで競争領域とされてきた事業においてもその収益性が低下する事態が生じている。こうした環境変化を踏まえ、これまで自社の組織内に保有してきたデータを協調領域として切り出し、他社や社会と共有・連携することで、限られた経営資源をより収益性の高いドメインに投資していくことが求められる。

- 自社が保有するデータを他社や社会と共有することを前提に、経営者がデータのライフサイクルにわたってそのリスクとベネフィットを見直し、データガバナンスに積極的に取り組むことは、自社のレピュテーションの向上やサステナビリティ、さらに社会全体のサステナビリティの向上につながる。

- このような企業の取組が、持続可能性と強靭性を備え、経済発展と社会的課題の解決を両立する、人間中心の社会としての Society 5.0 の実現につながるものと考える。

---

[26] 例えば、高層マンション群の建設によって局所的に住民が増加した結果、保育園の待機児童が急増する事態や小中学校の施設対応が困難になるといった問題、また通勤電車に人が溢れてしまうなど、地域住民に迷惑がかかるだけでなく、結果としてマンション購入者の満足度が下がったり、学校教員の期中での増員や、鉄道会社がダイヤ改正を余儀なくされるといった問題が生じている。

付録. 関連 URL

- デジタルガバナンス・コード 3.0 ～DX 経営による企業価値向上に向けて～
（経済産業省）

  https://www.meti.go.jp/press/2024/09/20240919001/20240919001-1.pdf

- 協調的なデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ
（経済産業省）

  https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework.pdf

- データの越境移転に関する研究会 報告書 （経済産業省）

  https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2.pdf

- データ利活用制度・システムの検討について （内閣府）

  https://www.cas.go.jp/jp/seisaku/digital_gyozaikaikaku/data1/data1_siryou3.pdf

- 情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るためのデジタル社会形成基本法等の一部を改正する法律案 （デジタル庁）

  https://www.digital.go.jp/laws/423e67de-d520-4d46-8260-54b4f3125544

- データの利用権限に関する契約ガイドライン （IoT 推進コンソーシアム）
（経済産業省）

  https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20170530003-1.pdf

- 産業データの越境データ管理等に関するマニュアル （経済産業省）

  https://www.meti.go.jp/press/2024/01/20250127001/20250127001.html

- 政府機関の情報セキュリティ対策のための 統一基準（第 3 版）解説書 （NISC）

  https://www.nisc.go.jp/pdf/policy/general/k303-072c.pdf

- AI 事業者ガイドライン （総務省）（経済産業省）

  https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20240419_report.html

- 価値協創のための統合的開示・対話ガイダンス 2.0（経済産業省）

  https://www.meti.go.jp/policy/economy/keiei_innovation/kigyoukaikei/Guidance2.0.pdf

- 伊藤レポート 3.0（経済産業省）

  https://www.meti.go.jp/policy/economy/keiei_innovation/kigyoukaikei/itoreport3.0_r.pdf

- Data Maturity Assessment for Government: Framework（英国）

  https://www.gov.uk/government/publications/data-maturity-assessment-for-government-framework/data-maturity-assessment-for-government-framework-html

- Data Spaces Academy（情報処理推進機構）

  https://www.ipa.go.jp/digital/data/data-spaces-academy.html#the-chief-data-officer-handbook

- ISO/IEC 38505-1: Information technology — Governance of IT — Governance of data

  https://www.iso.org/standard/56639.html

- Capability Maturity Model Integration （ISACA）

  https://cmmiinstitute.com/cmmi/intro