データのガバナンスについて
-GDPRが要請する説明責任とガバナンス-

原田要之助[1]

概要

ビジネスにコンピュータの利活用が進むにつれて、顧客情報などがデータの形式で集約されるようになった。一度、これらの集約されたデータが漏えいすると影響は極めて大きい。また、データの形で集約されているので、データがアンダーグラウンドで転売されることもある。これは、データはコピーがやりやすく、コピーされてもその事実が分からない。また、外部に漏れたときにはデータを消去することができない性質があるからである。

企業によって大規模に集められた個人情報などのビッグデータの管理については、各国で規制・法制度が実施・検討されている。これらの規制・法制度では、データの不正な利用や漏えいに対して組織体制や対策を義務づけている。組織体制についてはGDPRの説明責任に見られるように、経営者の責任が求められている。2017年5月に公表されたデータガバナンスの規格は、経営者が大規模な個人情報などのデータを管理する企業などの組織の指針である。本稿では、データガバナンスの規格を紹介し、EUのGDPRが要請する組織の説明責任との関係について述べる。

1 はじめに

多くの企業や組織では、様々なデータを収集しており、保有するデータと関連づけて、利活用している。データは集まれば集まるほどに、その有用性が増す特性を持つ。これは、「収穫加速」[2]の法則に従う[1]。この特性があるため、組織は一度、データベースを導入すると、次はその扱うデータを増やしていく。このおかげで、利用者にはメリットも大きい。例えば、昨今では、国際線に搭乗するときにチケットを持って行く必要がなく、パスポートだけで搭乗できる。このデータは、通信ネットワークで到着地に送ら

1 情報セキュリティ研究科　教授

2 カーツワイルは、IT の変革を収穫加速の法則としてとらえ、「広義の有用な情報量である秩序とカオスと時間の関係の一般法則の下位法則」として位置づけている

れ、入国管理に用いられている。もはや、紙のチケットに頼る必要がなく、無駄な作業がなくなり効率化が図られている。

しかし、このように個人に関するデータが企業などに集められると弊害も起こりうる。小売りやサービス産業では利用者の様々なデータを集め、サービス提供や販売活動に活用したり、他の企業にも有料で利用させたりして、収益につなげる[1]。これによって、個人のプライバシー領域が侵害される危険性がある。EU では、従来のデータ保護指令を強化して GDPR[2]に移行する。この規制は、組織に厳しい個人情報の取得や管理を求めている。また、組織に対してデータのガバナンスを強く要請している。

本稿では、とくに、GDPRを紹介するとともに、組織がデータを活用する際に要請される組織のデータに関するガバナンスの規格を紹介し、GDPRへの対応に向けてどのように活用するかについて述べる。なお、GDPRについては公式な日本語版がない[3]ため、本稿ではJETROが分析して公表しているものの用語を参照している[3]、[4]。

2　ITガバナンスについて

2.1 ITガバナンスの背景

企業などの組織では、ITに伴う新たな大規模な投資とITに依存するためのリスクが発生するようになった。これらを適切に管理するために、コーポレート・ガバナンスとのアナロジーでITガバナンスの概念が導入された。ITガバナンスという用語と概念[5]は、コーポレート・ガバナンスの発展として経営者に分かり易いことから企業に広く受け入れられるようになった原因でもある。ITガバナンスの国際規格は2008年にオーストラリアとニュージーランドから提案され、当時のISO/IEC JTC1 W6（その後、JTC1 W8に編成替え）で審議されて策定された[4]。また、この規格は日本の組織にも役立つと考えられたことからJIS 38500:2014[5]として日本の工業規格にもなっている。詳細については、文献[]に詳しい。

2.2 ITガバナンスの国際規格ISO/IEC38500について

IT ガバナンスの規格は 2009 年にオーストラリアから提案され、規格となった。なお、2013 年にフォーマットを ISO の規格に合わせる修正が行われた。国内においては IT ガバナンスの重要性から、JIS 38500:2014 となっている。この規格は組織が IT の利活用において経営者が実施しなければならない点についてのガイドであり、6 つの原則と IT

[3] GDPR については、国内の Web サイトでは、様々な関係者（マスメディア、コンサルタント、研究者など）が日本語で解説しているが、訳者によって用語が異なっている。

[4] ISO/IEC には、加盟国の国内規格を簡単なレビューを経て国際規格として利用するファーストトラックという制度があり、ISO/IEC38500 はこの制度を適用した。そのため、2013 年にフォーマットを ISO/IEC の規格のフォーマットに合わせるための修正が行われている（内容については変更されていない）。

ガバナンスのモデル、モデルと原則の応用の３つの部分で構成されている。モデルを図2。1に原則を表2.1に示す。

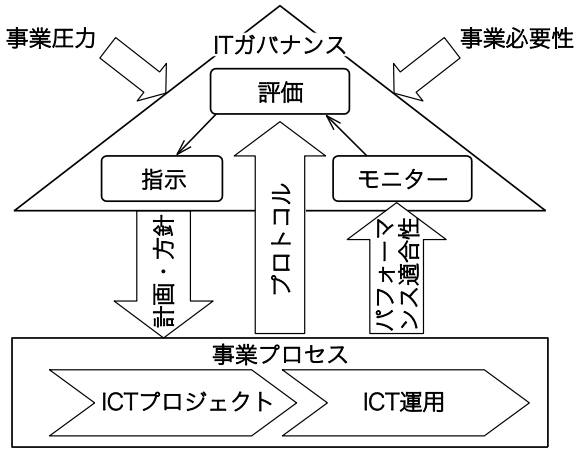

図 2.1 IT ガバナンスの EDM モデル（文献[5]より）

図 2.1 の IT ガバナンスのモデルは、組織の経営者がマネジメント層による事業プロセスに対して実施すべき 3 つの機能であるモニタ、評価、指示（3 つを併せて EDM モデルという）を示す。

表 2.1 IT ガバナンスの原則（文献[5]より）

原則 1:責任(Responsibility)
組織内の個人及び部門は、IT の供給及び需要の両面の役割について、その責任を理解して受け入れる。処置に責任を負う人もまた、その処置を遂行する権限をもつ。

原則 2:戦略(Strategy)
組織の事業戦略は、IT の現在及び将来の能力を考慮する。IT の戦略計画は、その現在及び進行中の事業戦略のニーズを満たす。

原則 3:取得(Acquisition)
IT の取得は、適切で継続的な分析を基礎として、明確で透明な意思決定による正当な理由に基づいて行う。短期的及び長期的の両面で利益、機会、コスト及びリスクを適切に均衡させる。

原則 4:パフォーマンス(Performance)
IT は組織を支援し、現在及び将来の事業のニーズに合うサービス、サービスレベル及びサービス品質を提供する点で目的に適合する。

原則 5:適合性(Conformance)
IT は、必須である全ての法律及び規制に適合する。方針及び実施は、明確に定義、実施及び強制される。

原則 6:人間行動(Human Behaviour)
IT の方針、実施及び決定は、プロセスにおける人間の全ての現在及び発展するニーズを含み、人間行動を尊重する。

表 2.1 の IT ガバナンスの原則は、組織の経営者が事業プロセスに対して実施すべき 6 つの原則を示している。経営者は、事業に対する責任や戦略のみならず、リソースの取得や事業プロセスのパフォーマンスをチェックする必要があるとしている。これは経営陣がモニタでチェックすべき項目でもある。また、組織が属する国の法制度・規制及び組織内部での決定事項、倫理への適合性（Compliance）がある。さらに、経営者が守るべき原則に人間行動（Human Behaviour）を含めているのが特徴的である。これは、組織を構成するのは人間であり、組織を経営するなかで、IT であっても、“人間”によるミスやごまかし、犯罪行為などにも留意すべきことを意味している。すなわち、経営者に向けてメッセージであり、汎用性も高い [4]。

3　GDPRについて

欧州連合は 2016 年 4 月に“一般データ保護規則”（General Data Protection Regulation: GDPR）[1]を公表した。1995 年に制定された個人データの保護を目的とした規制であるデータ保護指令（Directive 95/46/EC）を置き換えることになる。なお、GDPR は 2016 年 4 月 27 日に採択され、2 年間の移行期間の後、2018 年 5 月 25 日より適用される予定となっている。

GDPR では、個人データ[5]を収集、処理などを行う事業者に対して多くの義務を課している。 また、個人データの収集や処理、利活用する事業者の説明責任を明確に要求している。2018 年 5 月以降は、事業者は GDPR を遵守した運用が求められる。以下では、具体的に GDPR が要請する内容について、JETRO が分析した文書[2]、[3]をもとに述べる。

GDPR の一般的な特徴を以下に述べる。

- 加盟各国の個別のデータ保護法を原則廃止して、GDPR の一本にまとめ、その下で、加盟国が個別のルールを追加する構造に変更
- 規制の対象範囲をデータ保護指令よりも拡大
- 組織の説明責任（Accountability）という概念を導入
- PIA の実施及びプライバシー・バイ・デザイン、DPO の専任などを組織に要請
- 個人情報に対する権利(“忘れられる権利”や“データポータビリティの権利”など)を強化
- 違反した組織への制裁と執行

3.1　GDPR の対象と概念

[5] GDPR では、日本の個人情報にあたるものを個人データと呼んでいる。日本の個人情報保護法制の定義と区別するために、本郷では、個人データとしている

GDPR の対象となる組織は、営利活動に従事する企業のみならず、公的機関・地方自治体・非営利法人なども含まれる。とくに、組織が欧州経済領域(EEA)域内で取得した“氏名”や“メールアドレス”、“クレジットカード番号”などの個人に紐付くデータを EEA 域外に移転することを禁止している。GDPR の“個人”とは、EEA 域内の在住者の全てを指し、現地進出の日系企業に勤務する現地採用従業員のみならず日本から派遣されている駐在員も含まれる[2]ため、注意が必要である。
GDPR が規定している用語を表 3.1 に示す。

表 3.1 GDPR の基礎的な概念 文献[2]を一部修正

概念	説明	例
個人データ	識別された、または識別され得る自然人(「データ主体」)に関するすべての情報	• 自然人の氏名 • 識別番号 • 所在地データ • メールアドレス • オンライン識別子(IP アドレス、クッキー識別子) • 身体的、生理学的、遺伝子的、精神的、経済的、 文化的、社会的固有性に関する要因
処理	自動的な手段であるか否かに関わらず、個人データ、または人データの集合に対して行われる、あらゆる単一の作業、または一連の作業	• クレジットカード情報の保存 • メールアドレスの収集 • 顧客の連絡先詳細の変更 • 顧客の氏名の開示 • 上司の従業員業務評価の閲覧 • データ主体のオンライン識別子の削除 • 全従業員の氏名や社内での職務、事業所の住所、 写真を含むリストの作成
移転	定義なし[1]。[2]では、EEA 域外の第三国の第三者に対して個人データを閲覧可能にするための行為と定義している	• 個人データを含んだ電子形式の文書を電子メール で EEA 域外に送付することは「移転」に該当する

GDPR には、“データ主体”、“管理者”、“処理者”という登場人物の概念が導入されている。“データ主体”とは、「個人データが関連する当該個人のことを言う」。“管理者”とは、「単独または共同で個人データの処理の目的と手段を決定する」。また,“管理者”は、「個人データの処理の適法性と GDPR 違反に対する責任を負う」[2]。また、“処理者” は、「管理者を代理して、個人データの処理を行う自然人または法人」[2]。これらの関係を図 3.1 に示す。日本の個人情報保護法と同じように、管理者が処理者に委託する場合には、個人データを開示する必要があり、事前にデータ主体からの明示的な同意を得ることが前提となる。

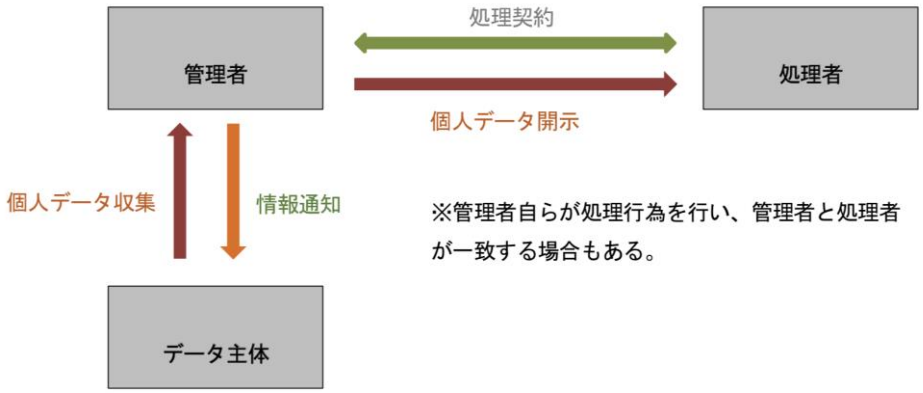

図 3.1　GDPR の登場人物の関係　文献[2]

3.2　GDPR の要求事項

GDPR では、様々な要件を組織に課している。これらの要件を満たさない場合には、制裁の対象となることに注意が必要である。これらの要求事項を表 3.2 に示す。1995 年のデータ保護指令と比べると、より、組織がエンドユーザの個人データを保護する方向となっている。

表 3.2　GDPR の要求事項　文献[2]を一部修正

説明責任 Accountability	管理者は適切な個人データ保護指針の採択、およびその実行を含め、 処理行為が適法な個人データ処理の要件をはじめとする GDPR の要件を確実に遵守し、かつそれを実証できなければならない
遵守実証の対策の実施	説明責任を果たすための遵守実証の対策の実施として必要な事項 • 内部記録:管理者および処理者は、個人データの処理行為の内部記録を保持する義務。 • データ保護責任者(Data Protection Officer :DPO)の選任 • プライバシー・バイ・デザイン（Privacy by Design）の実施 • プライバシー影響評価（Privacy Impact Analysis）の実施
個人データのセキュリティに関する義務	• 個人データのセキュリティ要件:適切なセキュリティ措置の実施 • データの侵害通知:個人データの不慮または不法な破壊、喪失、改ざん、無断開示・アクセスに繋がる保護安全性の侵害は、一定の場合に監督機関およびデータ主体に通知する義務がある
データ主体の権利の尊重	管理者は次のデータ主体の権利を尊重しその行使を円滑にする必要がある 情報権、アクセス権、訂正権、削除権(忘れられる権利)、制限権、データポータビリティの権利、異議権、および自動的な個人の意思決定に関する権利の尊重
情報権	管理者はデータ主体から個人データを収集する場合、個人データ入手時に、データ主体に一定の情報を提供する義務
アクセス権	管理者はデータ主体から処理が行われている個人データへのアクセスの請求があれば、そのコピーを提供する義務
訂正の権利	不正確な自己の個人データに関する訂正を管理者に求める権利
削除権（忘れられる権利）	データ主体は自分に関する個人データの削除を遅滞なく管理者から得る権利を有する
制限権	データ主体は管理者に対して一定の場合に個人データ処理を制限する権利を有する

データポータビリティの権利	データ主体は自分に係わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取る権利を有する
異議権	データ主体は管理者または第三者によって追求される適法な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱える権利を有する
自動化された個人の判断に関する権利	データ主体は、自分に対する法的影響を生じ得るような、プロファイリングを含む自動処理のみに基づいた判断の対象にならない権利を有する （例、人が介入しないオンライン上での借り入れ申込やインターネットでの採用活動）

表 3.2 に示した項目は、組織が全体として取り組まなければ実施が難しいものが多い。とくに、説明責任（Accountability）については、データ保護指令では無かった概念であり、この項目に含まれる範囲については、注意が必要と言えよう。大量の個人データを取り扱う組織が説明責任を実現する責任者として、DPO を要請しているのは特徴的だ。また、技術的な点でも、PIA（プライバシー・インパクト分析）のみならずプライバシー・バイ・デザインが説明責任の具体的な実施対象となっている。これらを実施するには、組織をあげての取り組みが前提となっていることがうかがえる。

さらに、データ保護指令と比べて、より個人の権利を強化した点も無視できない。とくに、情報権、アクセス権、訂正権、削除権(忘れられる権利)、制限権、データポータビリティの権利、異議権があげられている。中でも、コンピュータを用いて実施する処理にも踏み込んで、自動的な個人の意思決定に関する権利が述べられており、個人データを取り扱う管理者の注意義務は大きい。削除権やデータポータビリティなどの実施は新規項目であり、組織的な対応には時間がかかるので、関係する組織への影響は大きい。JETRO は、「社内の様々な関係者には、総務部、法務部、コンプライアンス部、IT 部、情報・システム 部、情報セキュリティ部、人事部、事業部(データを使ったビジネスを行う企業、そうした企業を顧客に持つ会社)の関係者が含まれる」[3]と解釈して、「社内の様々な関係者の数が多過ぎるため、GDPR 対応を専任で行うプロジェクトチームを組成することが望ましい」[3]としている。すなわち、組織的な取り組みをしていない限り対応が難しいと考えられる。

3.3 GDPR での個人データの第三者提供について

GDPR では「個人データの適法な処理の要件」として「データ主体が 1 つ以上の特定の目的のために自己の個人データの処理に同意を与えた場合」[2]が基本となっている。また、この要件への例外について規定している。例えば、EU 在住者の個人データを対象にするときには、「管理者が従うべき法的義務を遵守するために処理が必要な場合」の対象は EU の法的義務となっており、日本の法令を充てることはできない[3]。また、第三者提供は、EU のデータ保護指令で EU が実施した法的な解釈をベースにしている。具体的には、「管理理者または第三者によって追求される正当な利益のために処理が必要な場合は、データ主体の個人データの保護を求める基本的権利および自由と、管理者

または第三者による処理によって追及される正当な利益との比較考量を行い、後者が前者を上回る場合に個人データの利用が可能となる」[3]となっているので、きちんとした比較考察なしには活用できない。この際に要請される「適切な保護措置として行動規範、認証制度、標準契約条項(SCC)、または拘束的企業準則(BCR)」があり適用対象の解釈については[4]に詳しく述べられている。

3.4 GDPR の違反について

GDPR では組織の違反に対して、2,000 万ユーロ、または、企業の場合には前会計年度の全世界売上高の 4%のいずれか高い方としている。また、公的機関も対象としており、売り上げがない場合についても対象となる。
違反に当たる行為を表 3.3 に述べる。個人データの取得などの際の手順的な行為だけではなく、組織的な対策についても言及されている。

表 3.3 GDPR の違反行為 文献[2]を一部修正

- 16 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者よる同意または許可をとらなかった場合
- GDPR 要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合
- EU 代理人を選任する義務を怠った場合
- 処理行為の記録を保持しない場合
- 監督機関に協力しない場合
- リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合
- セキュリティ違反を監督機関に通知する義務を怠った場合およびデータ主体に通知しなかった場合
- 影響評価を行なわなかった場合
- 影響評価によってリスクが示されていたにも関わらず、処理の前に監督機関に助言を求めなかった場合
- データ保護責任者(DPO)を選任しなかった場合
- 個人データの処理に関する原則を遵守しなかった場合
- 適法に個人データを処理しなかった場合
- 同意の条件を遵守しなかった場合
- 特別分野の個人データ処理の条件を遵守しなかった場合
- データ主体の権利および行使の手順を尊重しなかった場合
- 個人データの移転の条件に従わなかった場合
- 監督機関の命令に従わなかった場合

4 データガバナンスについて

4.1 データの外部性

組織内で個人情報がデータベースに蓄積されて、利活用された場合には、より「多くの個人情報が集まるほどその効用が高まる」[1]。これについて、以下に考察する。

① ITの利便性の向上

個人情報は、収穫加速の法則にしたがって、一般的にデータが多く集まるほど利便性が高まる。そのため、競争状態にあるサービス業では、ある事業者が情報システムを利用して個人情報をデータベース化すると、その利便性が高まり、他の競争業者に対して競争優位に立つ。このことから、データベース化が競争事業者間に広がる。そのため、業界としてデータベース化が競争により広がっていく。さらに、データベースを構築した企業は、これを外部に利用させて、収益を稼ぐこともできる。これによって、データベースがより囲い込まれてしまうようになる。例えば、企業のポイントについては、多数の事業者が相互に乗り入れることでポイントの利便性と顧客の囲いこみを行っている。現在、巨大な事業者がデータベースを中心にして中小の事業者をグループに加えていく現象が見られる。これは、ITによるデータの外部性と呼べるであろう。

② ITのハードウェアの進歩

データベースの処理では、ITのハードウェアの進歩により蓄積メディアによる蓄積量が増えるとともにこれを検索するときのコンピュータの処理性能への要求も大きい。さらに、分散したデータベースを連携して一体として運用するための高速な通信が重要な要素である。一度、規模の大きいデータベースを構築して利用するようになると、前項で述べた外部性によって大規模化が加速して利便性が増す。一方、ビジネスがデータベースをもとに展開するため、データベースを導入する以前の状態には戻れなくなり、データベースがビジネス上の要となる。データベース化が加速するために、個人の情報はますますデータベースで管理されるようになる。一方、大規模なデータベースに対するセキュリティについては、データの規模による価値の増大を考慮せずに、従来の対策で済ませているところが多い。データの規模が高まることで、より、データ漏えいの影響が大きくなる。リスク分析をすれば、リスクが大きくなっていることが明白であるが、実際には考慮されていない。そのため、一度、データ漏えいが起きると企業の死活に関わる重大な問題となってしまう。

③ 顧客環境の変化

顧客側の環境においても、IT化が進んでいる。すなわち、パソコンのみならずパッド、スマートホンなどの情報端末の能力向上とコストの相対的な低下により、これらの機器を用いるケースが増大している。また、事業者はインターネットを利用した様々なサービスを拡充させている。ネットワークでの購買では、商品の発送や請求を行うために、クレジットカードなどの個人情報、住所・氏名、購入履歴などを利用することが一般的であり、結果として事業者にこれらの情報が蓄積されていく。

以上の①〜③による環境変化に伴う特性と、人間の特性としての管理ミスや事故が起きるという点を考慮すると、今後も、企業や組織において個人情報などのデータベース化が進み、人為的な情報漏えい事件はなくならないであろう。

とくに、個人情報の場合、上記に述べたように、データベースの大規模にはネットワークの外部性が見られる。これは、データベースの規模が2倍になったときに、そのデータベースの持つ効用は4倍以上となる[1]。一般にリスクは効用に比例するので、データベースが大規模になればなるほど、リスク対策をきちんとする必要がある。

ここの状況を緩和するために、個人情報保護法も改定されて個人情報を取り扱う事業者に義務を課すようになっている。ただし、企業の活動は国境に縛られては以内ため、企業に十分な規制を行うことができない。これに代わるものとしては、国際規格が役立つと考えられる。4.2節以降では、データガバナンスの規格を紹介する。

4．2 データのガバナンスの規格について

データのガバナンスについては、 ISO/IEC SC40 の WG1 で標準化が行われ、2017 年 5 月に規格が出版された。規格の経緯については[1]に詳しいので参照されたい。この規格は、組織がデータを利活用する際にどのような視点でガバナンスすべきかについて、IT ガバナンスの原則とモデル[6]、[7]を拡張したガイドラインである。対象となるデータには、組織が活動の中で利活用するあらゆるデータが含まれており、個人情報や営業関連のデータが含まれている。組織におけるデータの利活用には様々な課題があり、とくに、データの収集から始まるデータのライフサイクル、利活用の範囲、管理体制などが対象となっており、具体的な指針を示している。なお、IT ガバナンスの関連規格として、情報セキュリティガバナンスの規格[8]、[9]もあり、IT ガバナンスの原則とモデルを拡張しているので、参考になる。

データガバナンスの規格[10]、組織が個人情報やビッグデータを取り扱う際のガバナンスを主たる目的としている。すなわち、規格の主要な目的は、組織の経営陣がどのように組織内において、データのマネジメント（データの収集、収集した情報の保存と利活用、不要になったデータの廃棄に至るライフサイクルに基づく）を導入しこれに必要な仕組みの導入、運用、監督などについて述べている。

4．3 データガバナンスの規格の構成

ISO/IEC38500 の IT ガバナンスの規格[7]では、 3 章が、良好な IT ガバナンスのための枠組み（原則とモデル）、4 章が IT ガバナンスの手引き、となっていた。これをデータガバナンス[10]では、3〜9 章に展開している。これを表 4.1 に示す。この規格では、対象とするものが個人情報やビッグデータなどのデータそのものであることから、データに関するものにクローズアップしている。とくに、データに対するガバナンスが必要な全体論を 3 章にまとめ、4 章で原則とモデルの概略を述べ、5 章ではデータマネジメ

ントを述べて、ガバナンスとの違い関わりを示している。6 章と 7 章はで IT ガバナンスの原則とモデルを、データをガバナンスするための拡張し、さらに 8 章では、データに特有の側面にクローズアップしている。9 章では、規格のまとめとして，データ説明責任マップという経営陣が実施するべき内容を俯瞰した表を提示している。

データガバナンスでは、IT ガバナンスの規格にように IT 環境全般に関する一般論ではなく、2 章で述べた GDPR が要請する個人データに対する説明責任を組織としてどのように扱う場合の実用的なガイドラインとなっている。

表 4.1 データガバナンスの規格案の構成（文献[10]より）

4 データのガバナンスの向上
5 データのガバナンスのための原則、モデル、側面
6 データに関わるアカウンタビリティ（説明責任）
7 データガバナンスのガイダンス − 原則
8 データガバナンスのガイダンス − モデル
9 データガバナンスのガイダンス − データ特有の側面
10 データ・アカウンタビリティ・マップの適用

４.４　データガバナンスの規格の特徴

データガバナンスの規格案では、組織が扱うデータについて経営者がどのような考え方で望むべきかについて 4 章として「データガバナンスの向上」を設けて、経営者に対する心構え（表 4.2 参照）が述べられている。この章は、データのガバナンスをより理解できるように新たに設けられている。

表 4.2　経営者に対する心構え（文献[10]より）

経営者が組織全体でのデータの利活用が組織のパフォーマンスにプラスに貢献することを保証することで − サービス、市場、ビジネスにおけるイノベーション − データ資産の適切な導入および運用 − 保護と潜在的な価値の可能性の両方の責任と説明責任の明快さ − 有害または意図しない結果の最小化

データガバナンスを実践できている組織は表 4.3 のような利点がある。この利点は、一般的な内容ではあるが、GDPR が求めている内容が俯瞰されている。

表 4.3　データのガバナンスの利点（文献[10]より）

− データ所有者とデータユーザーがやりとりする信頼できる
− 共有するための信頼できるデータを提供できる
− 知的財産およびデータに由来する価値を保護する
− ハッカーや詐欺行為の抑止のためのポリシを策定し実践する

− データ侵害の影響を最小限に抑えるように準備されている − いつ、どのようにデータを再利用できるかを認識できている − 優れたデータ処理方法を実証できる

さらに、「データガバナンスの向上」がない場合のリスクについて述べている（表 4.4 参照）。リスクには、データに関する法制度とデータ漏えいリスクがある。なお、データガバナンスの規格における原則（Principles）については、 ISO/IEC38500 の 6 つの原則[8]をそのまま適用している。

表 4.4　ガバナンスがない場合のリスク（文献[10]より）

− 法律を遵守しない場合の罰則、特に必要なプライバシー対策に関する法律。 − 重要なビジネスデータ（製法や設計仕様）の機密性の喪失 − ビジネスパートナー、顧客および一般市民を含むステークホルダからの信頼の喪失 − 信頼できるデータまたはビジネス関連のデータがないために重要な組織機能を実行できない − 競合他社による戦略的なデータ利活用による競争の激化 − 結果として、次の点について説明責任を持つことができる。 − プライバシー、スパム、健康と安全の侵害、法律と規制の記録保持 − セキュリティ、社会的責任に関する義務付けられた基準に準拠していること − 知的財産権に関する事項

４.５　データの管理モデルについて

データガバナンスでは、データのライフサイクル（データの収集、保管、決定、報告、配布、廃棄）をベースにしたデータのマネジメントモデル（図 4.1 参照）と経営者が実施すべきガバナンスモデル（図 4.2 参照）で構成されている[10]。前者のデータのマネジメントモデルでは、データのライフサイクルをベースに経営者の果たすべき役割と組織として必要になる機能が述べられている。

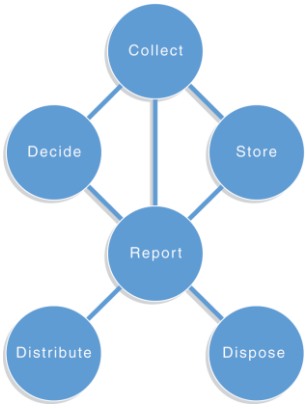

図 4.1 データマネジメントモデル（文献[10]より）

図 4.2 は、ISO/IEC38000 の EDM モデルにデータガバナンスで考慮すべき観点が追記されている。経営者が果たすべき EDM 機能として、データに関する観点が特記されている。

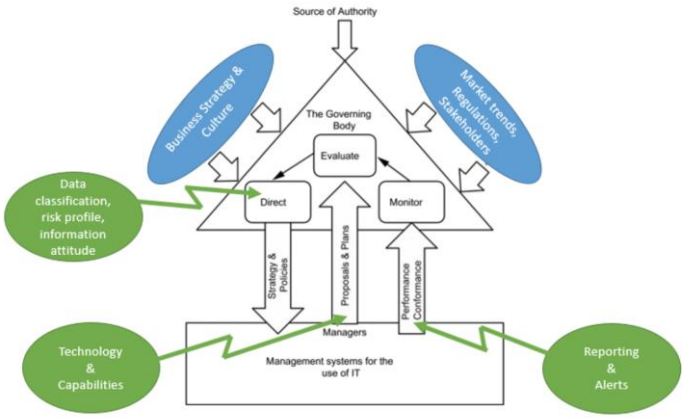

図 4.2 データガバナンスモデル（文献[10]より）

４.６　データガバナンスを担保するための監視機構（Oversight Mechanism）

ISO/IEC38500 の扱う IT ガバナンスは経営者及び外部のステークホルダなどの限られた関係者を対象としているため、モニタには内部のプロセスを経営者が内部的にチェックする仕組みだけであり、外部ステークホルダへの説明責任については十分とは言えない。すなわち、データガバナンスでは、例えば、データを取得するためには、データを収集する対象者から同意をとることや第三者提供を受けたときの制限事項など外部のステークホルダに対する説明責任が必要となる。さらに、組織として経営者が説明責任を果たしているか（注意義務として実施しているか）について経営者の監視が必要である。すなわち、データガバナンスでは、内部のガバナンスを担保するための追加的な機能について、「経営者と監視機構（Oversight Mechanism）」が必要としている。この内容を表 4.5 に示す。表 4.5 では、経営者がデータの取扱についての実行を保証するために、監視機構として、監査委員会、リスク委員会などの設置を求めるとともに、第三者評価による保証も求めている。すなわち、データガバナンスでは、経営者の監督も必要としている。

表 4.5 データの経営者と監視機構について（文献[10]より）

− 経営者は、ビジネスのデータへの依存度に応じたデータガバナンスのための監督メカニズムを確立すべきである。 − 経営者は、組織のビジネス戦略へのデータの重要性だけではなく、そのデータの活用が組織に与える潜在的な戦略リスクを明確に理解している必要がある。経営者が扱うデータに対する注意のレベルは、これらの要因に基づいている必要がある。 − 経営者は、組織のメンバーや関連するガバナンス機構（例えば、監査委員会、リスク委員会および IT 委員会など）がデータの重要性についての必要な知識を得て理解することを確実にす

る必要がある。 - 経営者は、戦略的な観点からの組織のデータ活用を経営者が監視できるよう支援する小委員会を設置することができる。小委員会の必要性は、組織のデータの重要性やその分量に依存する。 - 経営者は、データのガバナンスとマネジメントのために、適切なガバナンスのフレームワークを構築することを確実にする必要がある。 - 経営者は、ガバナンスが有効であるという保証を得るために、例えば、監査および第 3 者による評価などの仕組みを必要とすることによって、データのガバナンスと管理のためのメカニズムの有効性をモニタする必要がある

4.7　データ特有の側面

データの利活用は組織に価値をもたらすが、リスクが伴うとともに、様々の法的・契約上・倫理などの制約が伴う。これをデータガバナンスの側面として、価値（Value）、リスク（Risk）、制約（Constraint）の観点から議論している。これを表 4.6 に示す。

表 4.6 データガバナンスのデータの側面（文献[10]より）

- 価値：データは組織に有用な知識の原材料である。この価値は組織によって利活用されるまでは分からない。したがって、すべてのデータは最終的にそれに責任がある運営体制が重要となる。「価値」という用語には、データの質と量、適時性、コンテキスト（それ自体がデータ）、保存、保守、利活用、廃棄のコストが含まれる - リスク：データの種類によってリスクのレベルが異なり、経営者はデータのリスクを理解し、管理者に指示する必要がある。リスクはに、データ侵害だけでなく、データの不正利活用や、データを適切に活用しない競争上の機会損失のリスクもある - 制約：ほとんどのデータには、利活用に制約がある。法律、規制または契約上の義務が課され、プライバシー、著作権、商業的利益などの問題が含まれる。さらに、制約には、データの利活用を制限する倫理的または社会的義務、組織のポリシーが含まれる

データガバナンスでは、データのライフサイクル毎の注意点をまとめている。これを表 4.7 に示す。GDPR の要件を満たすためには、データの収集から廃棄までのプロセス毎に必要な機能や管理策を実施することが求められている。これに必要な機能がまとめられている。

表 4.7　データのライフサイクルでの注意点　文献[10] より

収集	- データ入力：組織内（ERP システム、電子メール）、組織外（ウェブサイト、モバイルアプリ）など - 他のシステムからのトランザクション：他のシステムで実行されたデータ - センサ：機械システムのセンサからの自動収集。ウェブサイトログ、ソーシャルメディア、センサデバイス（温度センサ、監視カメラ、車、信号灯、建物、IoT 等）データにアラートやアラームなどの緊急信号も含む - 新しいコンテキスト：レポートを他のデータと組合わせた追加情報。元のデータとは異なる扱いを必要とすることもある - サブスクリプション：データフィードまたは仮想データストアへのサブスクリプションを通じて得られる
保存	データに位置情報が含まれることがある。 保存される対象は組織が所有および運営するデバイスに格納されたデータ、組織の外

	部にあるデバイスや必要に応じて照合されるデータフィードなどを含む。 データが収集されると、そのデータは取り込まれ、保護され、管理され、場合によってはアーカイブされる。 組織が管理するデータ量は急速に増加している。 パブリッククラウドコンピューティング環境に保存されることもある。
報告	報告活動には、意思決定、流通または処分を支援するためのデータの手動または自動での抽出および分析が含まれまる。 重要な機能は、データの品質や通貨などの特性が関連付づいたデータフィードからデータを抽出する。 データフィードの組み合わせによって、データに新しいコンテキストが与えられることがある。 データマイニングや機械学習などによる抽出および分析手法で、自動でさらなる洞察を得たり、将来の結果を予測したりして、意思決定を行う。 匿名化や偽名化などの技術を活用して個人情報を削除しながら、センサのデータを集約して傾向を抽出することがある
決定	意思決定活動は、報告に基づいて決定が行われる。決定は、組織内の人々によって、または自動化された手段によって行われる。 データを保有する主な目的は意思決定であり、データの価値は意思決定に影響すること。 経営陣は、決定が責任レベルに対して適切に行われていることを保証する必要がある。複雑な機械学習アルゴリズムによって自動的に決定が行われる場合に特に重要である。意思決定プロセスにおける偏見、差別、またはプロファイリングに対抗するために人間の介入が必要となる。意思決定プロセスはデータを評価するので、その情報（データの「有用性」）をデータ収集および作成プロセスにフィードバックして、意思決定の価値を高め、ビジネスを改善できる。
配布	配布は、外部の関係者への配布のためのデータの抽出またはコピーが含まれる。 - 外部報告は、例えば、政府機関に要求される - B2B（Business-to-Business）データ交換、顧客への説明に利用する - データは、例えば、広告代理店または調査会社に販売される - データは、ビジネスデータなどの組織の出版ビジネスの一部でとなる（すなわち、データは製品でもある） - 配布が許可されていない場合、これはデータ侵害と分類される
廃棄	報告活動のあと、廃棄するデータを特定し、そのデータおよび重複するデータを保存から完全に削除する。データフィードの場合、二度とアクセスできなくする。 データ分析、マイニング、学習ツールの高度化により、より多くの情報からより多くの情報を抽出できるため、既存のデータの価値が高まっており、データを削除しなくなっている。しかし、廃棄はデータ漏洩のリスクを低減してくれる。データが存在しないと、不適切に利活用されることがなくなる - 無関係または間違ったデータを削除する。古いデータは傾向分析に活用できるかもしれないが役立たない -お客から、忘れられる権利などでデータの削除を求められることがある - 顧客またはサプライヤーとの契約による - 法的要件または規制要件による

４.８　IT ガバナンスの原則とモデルの適用

IT ガバナンスをデータガバナンスの拡張については、経営者が IT ガバナンス原則をもとに組織の具体的な運営を決め、EDM のモデルに基づいて実施すべき行動の観点からまとめている（ISO/IEC38505-1 規格の 7 章と 8 章）[7]。

まず，データの利活用に IT ガバナンス原則をあてはめると表 4.8 となる。とくに、この文脈では経営陣が実施すべき組織的な対応や GDPR などの法的な要件をどのように管理するかが述べられている。組織の責任や戦略、適合については分かり易いが、人間行動には組織的なデータ文化など組織文化などの抽象的な点にも触れられていることが特徴的である。組織文化がないと組織の構成員が能動的に継続してデータの管理を実践するのが難しいと考えていることが分かる。

表 4.8 IT ガバナンスの原則の適用（文献[7]を加筆修正）

原則 1：責任（Responsibility）の対象について
- IT 機能または部門を超えて、組織全体が対象
- マーケティングなどのビジネス活動に関連する重要なデータを扱う部門、製品計画に利活用されるデータを管理する部門、データの収集を担当する部門
- 組織が製品またはサービスとして直接データを提供する場合（コンテンツ、天気や株式市場レポートなど）
- データのライフサイクル全体

原則 2：戦略（Strategy）
- 技術の進歩と市場の期待を可能にする
- データ説明責任マップのすべての部分
- データ特有の側面（価値、リスク、制約）を考慮する
- 新たな機会やリスクを説明するために戦略全体を改訂する必要があるとの期待を設定する

原則 3：取得（Acquisition）

データが、組織内のその意図されたおよび/または規定された利活用ならびに外部での利活用と一貫していること。取得されたデータセットまたはデータストリームの利活用および管理おいて、価値、リスク、制約の評価がデータ戦略と一致していること

原則 4：パフォーマンス（Performance）
- データがサプライーチェーンで顧客と繋がっている場合、データ利活用が意思決定と関係しているか
- 組織内の新しいデータセットとデータストリームの採用度合
- データに対する投資収益率
- 競合他社のベンチマーク

原則 5：適合性（Conformance）
- 組織のニーズと義務を満たすポリシーに従って、すべてのデータセットとデータストリームを保護する
- PII の正しい処理
- 組織全体でのデータ保管ポリシーとその実践
- データに関するすべての法的義務の理解、および組織全体でこれらの義務が満たされていることについての保証

原則 6：人間行動（Human Behaviour）
- 組織全体で許容されるデータとデバイスの利活用の管理
- データの適切な共有、保護、解釈を促すための組織的データ文化
- ステークホルダの人間行動の影響と要件

次に、EDM のモデルの適用にあたっては、表 4.8 に示すように、経営者がデータを管理する実務者との関係性で議論されている。経営者が説明責任を果たす上では、モニタの機能でマネジメント層の活動を監視して、問題があれば対応することが重視されるためと考えられる。とくに、モニタの機能については、他の規格（ISO/IEC27001 や ISO/IEC29100 を具体的に引用して，実践面を協調している。

表 4.8 IT ガバナンスの EDM モデルの適用（文献[6]を修正）

外部圧力	- データの可用性、品質、相互作用に関する顧客の期待 - データを利活用する競合他社。 法令やステークホルダの要求事項は市場によって異なるので、経営者は、現在および将来のデータ利活用に適用される戦略および方針を市場に広く適用できるようにする必要がある - 個人情報の収集と利活用に関するプライバシーポリシーの通知と同意要件を含むデータの収集方法 - データの保存および廃棄の要件 - 偏見、差別およびプロファイリングに適切に対処する義務 - データの共有または再利用に関する知的財産の問題
評価	現在および将来のデータ利活用について検討し、判断する - データと関連する技術とプロセスの内部利活用 - 競合他社、他組織、政府および個人によるデータの利活用 - 法律、規制、社会的期待の方向性を評価する -影響を与えるその他の要因に基づいてデータの利活用をコントロールする組織のデータ管理能力の認識 - 組織がデータ侵害した場合、どの程度回復できるか - 意思決定を支援するために正しい情報を適切な形式で届けることができるか。 - クラウドコンピューティングなどの新技術を活用して自らの能力を強化できるか データ戦略とポリシーのガバナンスは、組織がポリシーを実施するために必要なリソースと能力を持っている場合にのみ可能
指示	- 組織のデータへの投資から得られる価値の最大化：組織内の資産と同様に、データには投資が必要。データの最終的な価値は、その利活用が組織の意思決定を改善できること - データリスクアペタイトに沿ったデータに関連するリスクの管理：データのデータ分類スキームの採用 - 適切なレベルのデータスチュワードシップの確保：データの説明責任活動は組織内で適切な委任。 組織のデータ文化、全体的な戦略、リスク選好、認識されたセキュリティレベル、作業の量、およびデータの利活用に関する指標と価値が指示にとって重要となる
モニタ	組織のデータ利活用のパフォーマンスをモニタすべきである。データに関連する戦略が正しく実施されていること、データの利活用と管理が内部ポリシーや規制やデータスチュワードシップ要件などの外部要件に準拠していること 監督が重要となる分野には、 - プライバシーに関する懸念、同意要件、データ利活用の透明性を含む PII の利活用（ISO / IEC 29100 参照） -効果的な情報セキュリティマネジメントシステム（ISO / IEC 27001 に記述され

	ているものなど）の利活用。必要な場合には、クラウドコンピューティングサービス（例えば、ISO / IEC 27017）における第三者データフィードおよびデータ管理を含むように拡張する - データ保存および処分の要件。 - データの再利用、共有または売却、ならびに関連する権利、ライセンスまたは著作権 - 意思決定における文化的規範、偏見、差別、またはプロファイリングを適切に考慮

４.９　説明責任マップについて

ISO/IEC38505-1[10]では、データの利活用について IT ガバナンスモデルを適用するにあたって、とくに、説明責任にフォーカスして、説明責任の必要性について明らかにしている。これは GDPR[2]では、本稿の 2 章に述べたようにデータの管理について説明責任という概念を新たに導入して、組織的な対応、とくに、経営者への厳しい説明責任を経営者に課しているからである。一方、IT ガバナンスでは、説明責任という概念を明確にしてない。そこで、データガバナンス規格では、IT ガバナンスからの拡張として、組織がデータの利活用から利益を得ている側面と組織のデータの管理面の二つの観点から検討している。

具体的には、説明責任について、データの利活用による、経営者の観点からのデータが組織にもたらす価値とリスク、組織がおかれた地域の法制度や契約などの制約という活用面の軸と収集から廃棄までのデータのライフサイクルの軸の 2 つの軸で網羅的に整理している（ISO/IEC38505-1 規格の 6 章）。次に、経営者がこのマップを参考にして、マネジメント層とで EDM を実施することを述べ（ISO/IEC38505-1 規格の 9 章）、具体的な経営者が実施すべき内容を説明責任マップに展開している（ISO/IEC38505-1 規格の 10 章）。これを表 4.9 に示す。

表 4.9 - データの説明責任マップ（文献[10]を修正）

	値	リスク	制約
収集	[V1] 経営者は、組織が戦略目標を達成するためにデータを活用または金額換算する程度を決定する必要がある	[R1]経営者は、データの収集と利活用に伴うリスクを認識し、組織にとっての全体的なリスク選好の範囲内で、許容できるレベルのデータリスクに合意する必要があります。これには、データを収集および利活用しないリスクについて検討する必要がある	[C1] 経営者は、品質、プライバシー、同意要件、利活用の透明性などの制約を考慮して、データ収集のポリシーを承認する必要がある
保存	[V2]経営者は、データの潜在的な価値を取り出せるように、データの保存とデータの購入に適切なリソースを割り当てるポリシーを承認する必要がある	[R2]経営者は、管理者に対して、ISMS をデータ及び技術サプライヤーに拡大適用して、適切なリソースとコントロールを用いてリスク選好度を超えることがないように実施すること	[C2] 経営者は、データ保存の慣行（第三者のデータ購入を含む）がデータ収集の制約を確実に実施するよう、管理者に指示する必要がある

		を、指示する必要がある	
報告	[V3]経営者は、データの完全な価値を引き出すために必要なツールと技術を活用するように管理者に指示する必要がある。	[R3]経営者は、データのコンテキストに文化的規範が含まれることやデータを集める際の潜在的な誤解の可能性について認識する必要がある	[C3] 経営者は、特にデータが異なるデータセットから集められている場合、データの関係性とその制約の重要性を認識する必要がある
決定	[V4]経営者は、組織のデータ文化が、データへのアクセス方法、データを活用した意思決定方法、意思決定プロセスからの組織学習などの行動を含むデータ戦略と一致するようにする必要がある	[R4]適切なデータとその形式は、自動または人間による意思決定のための報告書に提供される必要がある。これらの決定に責任を負う一方で、経営者は、意思決定の責任を組織にデータリスクの許容可能なレベルの範囲で委譲する必要がある	[C4]新しいデータの場合の意思決定プロセスの出力は、独自の価値、リスクおよび制約があるので、経営者は意思決定プロセスとその関連する責任についての期待値を設定する必要がある
配布	[V5]経営者は、組織が組織の戦略計画を満たすように、データ配布のポリシー（方針）を確立する必要がある	[R5]経営者は、管理者が不適切な配布を防止するための適切な管理策を実施していることを確認する必要がある	[C5]経営者は、適切な配布権限が行使され、第三者にも権限が尊重されていることを確認する必要がある
廃棄	[V6]経営者は、データがもはや価値がなくなったとき、またはもはや保存することができないときに、データを廃棄できるようにするポリシー（方針）を承認する必要がある	[R6]経営者は、データの安全かつ永続的な破壊のための管理策を含む適切なデータ廃棄プロセスを実施するよう、管理者に指示する必要がある	[C6]経営者は、データの保存と廃棄の義務をモニタし、適切なプロセスが実施されていることを確認する必要がある

まとめ

昨今、ITがビジネスで一般的に利用され、効率化のためにあらゆる情報がデータベースに記録されるようになった．このような中，データベース化されたデータがサイバーセキュリティ攻撃を受けて大規模に漏えいし、犯罪などに利用されることが増えてきた。これを防止するために、日本の個人情報保護法の改正やEUのGDPRなどの規制強化が図られている。しかし、規制の強化だけでは問題は解決しない。組織がデータを扱う上で、規制が要請するに足るマネジメントやガバナンスが必要不可欠なものとなっている。

本稿では、組織のITや情報セキュリティが組織の経営者の責任問題とするITガバナンスや情報セキュリティガバナンスを組織のデータの活用に応用する新しい規格であるISO/IEC38505-1データのガバナンス規格を紹介して、経営者に要請されている組織作りや運営について議論した。この規格は、実際のところ、EUのGDPRを想定して、組

織のあり方をガバナンスの観点で論じている。このアプローチは、日本の個人情報保護法を実施するための参考になると考えられる。今後、検討を進める予定である。

謝辞

本稿をまとめるにあたって、情報セキュリティ大学院大学の教員、研究室の学生や研究生、情報処理学会の EIP 研究会から得られた温かい助言や調査への協力に感謝する。

参考文献

［１］原田要之助、AI のガバナンスについて-IT ガバナンスの系譜からの考察-、情報セキュリティ大学院紀要　情報セキュリティ総合科学 4 号、pp. 50-70, 2016 年 11 月
［２］Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 of the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),2016年
［３］JETRO、「EU 一般データ保護規則(GDPR)」 に関わる実務ハンドブック(入門編)、2016 年
［４］JETRO、「EU 一般データ保護規則(GDPR)」 に関わる実務ハンドブック(実践編)、2017 年
［５］原田, 「AI のマネジメントとガバナンス」, IPSJ SIG Technical Report, Vol.2016-EIP-73, No.7, 2016 年
［６］ISO/IEC、ISO/IEC38500:2013、 Governance of IT、2015年
［７］日本規格協会、JIS Q38500:2014（ITガバナンス）、2014年
［８］ISO/IEC、ISO/IEC27014:2013、Governance of IT Security、2013 年
［９］日本規格協会、JIS Q27014:2014（情報セキュリティガバナンス）、2014年
［10］ISO/IEC、ISO/IEC38505-1:2017、Governance of Data、2017 年