

データガバナンスの規格と活用について - GDPR との関係の整理 -

原田 要之助^{†1}

キーワード: GDPR, ITガバナンス, データガバナンス, 改正個人情報保護法, 個人データ

昨今、多くの組織がビッグデータや個人情報を収集し活用するようになってきている。また、IoT では、様々なデバイスがネットワークに接続されて、様々な情報が集められ、例えば、個人情報と連携して利用することが可能となっている。2018 年 5 月に、データガバナンスに関する規格 (ISO/IEC38505-1) が出版された。この規格は、このような現状において、組織には収集し、保存し活用するデータについての、組織に求められるデータガバナンスについて述べている。今回は、この規格は、2018 年 5 月に EU が施行する GDPR が求めるガバナンスについて適用できることを目指している。今回は、この規格について分析し、内容の報告と、規格の活用について述べる。

Introduction and use of Data Governance standard ISO/IEC38505-1 - implementation and use of GDPR -

Yonosuke Harada

Keywords: GDPR, IT Governance, Data Governance, the revised Act on the Protection of Personal Information, personal information

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」¹の法則に従う。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、サービス提供やマーケティングに活用したり、他の企業にも有料で利用させたりして、収益につなげている。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^[1]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、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 GDPR への対応に向けた文脈で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²ため、本稿では JETRO が分析して公表している用語を用いている [2], [3]。

2. 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³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

^{†1} 情報セキュリティ大学院大学, Institute of Information Security
1 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

2 GDPR については、国内の Web サイトでは、様々な関係者 (ニュース関係者、コンサルタントなど) が訳語を示しており、訳者によって用語が異なっている。

3 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、本稿では、個人データとしている

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，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

2.1 GDPRの対象と概念

GDPRの対象となるのは，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”などの個人に紐づくデータをEEA域外に移転することを禁止している。“個人”とは，EEA域内の所在者の全てを指し，現地進出の日系企業に勤務する現地採用従業員や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。なお，GDPRが規定している用語を表2.1に示す。

表 2.1 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	<ul style="list-style-type: none"> • 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，または個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	<ul style="list-style-type: none"> • 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域外の第三国の人々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	<ul style="list-style-type: none"> • 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”。“処理者”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”のことを言う[3]。これらの関係を図2.1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必要となる。

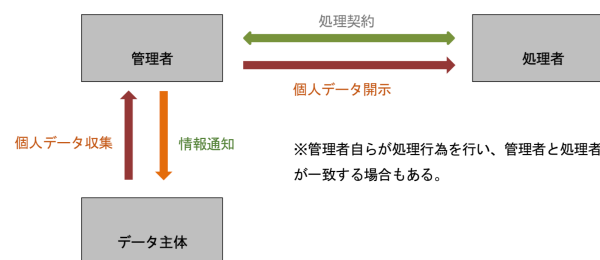


図 2.1 GDPRの登場人物の関係 文献[2]

2.2 GDPRの要求事項

GDPRでは，組織に様々な要求事項を課している。組織がこれらの要件を満たさない場合には，罰則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2.2に示す。1995年のデータ保護指令と比べると，より，組織に対して利用者の個人データを厳しく保護する方向となっている。

表 2.2 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方針の採択，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 <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

	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 2.2 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、データ保護指令に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(データ保護責任者)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項目となっている。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自動的に処理される場合の個人データの処理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の範囲は大きい。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。

2.3 GDPR での個人情報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も規定している。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、個人データの第三者提供は、EUのデータ保護指令のもとでEUが実施してきた法的な解釈をベースにしている。具体的には、「管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)」[3]があり適用対象の解釈については[3]に詳しく述べられている。

2.4 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 2.3 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 2.3 GDPR の違反行為 文献[2]を一部修正

<ul style="list-style-type: none"> 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に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かかわらず、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

3. 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[4]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[5]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。

以下では、データガバナンスの規格について述べる。

3.1 データガバナンスの規格について

データガバナンスの規格[6]は、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。

3.2 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、となっていたものを 3~9 章に展開している。これを表 3.1 に示す。ここでは、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を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 章は原則とモデルについてのガイドを示し、さらに 8 章では、データに特有のものにクローズアップしている。9 章では、データ説明責任マップという経営陣が実施すべき内容を俯瞰した表にまとめられている。

データガバナンスでは、IT ガバナンスの規格のように 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 3.1 データガバナンスの規格案の構成(文献[6]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トビリティ(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・アカウントビリティ・マップの適用

3.3 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 3.2 参照)が述べられている。この章は ISO/IEC38500 にはないもので、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 3.2 経営者に対する心構え(文献[6]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 3.3 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、2 章の GDPR が求めている内容がカバーされていることに注意されたい。

表 3.3 データのガバナンスの利点(文献[6]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ーを策定し実践する
- 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 3.4 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[5]をそのまま適用している。

表 3.4 ガバナンスがない場合のリスク(文献[6]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ーからの信頼の喪失
- 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

3.4 データガバナンスの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 3.1 参照）と経営者が実施すべきガバナンスモデル（図 3.2 参照）で構成されている。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 3.1 データマネジメントモデル（文献[6]より）

図 3.2 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。

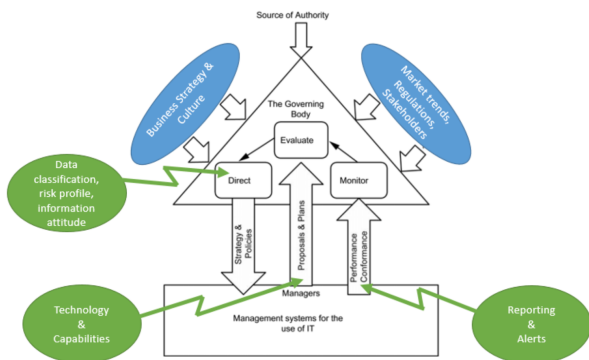


図 3.2 データガバナンスモデル（文献[6]より）

3.5 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ーなどの限られた関係者を対象としているため、モニター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であり、外部ステークホルダー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ー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 3.5 に示す。表 3.5 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 3.5 データの経営者と監視機構について（文献[6]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、監査および第三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ーする必要がある。

3.6 ガバナンスのデータ特有の側面

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、様々な法的・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 3.6 に示す。

表 3.6 データガバナンスのデータの側面（文献[6]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

<p>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</p> <ul style="list-style-type: none"> - 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、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 3.7 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 3.7 データのライフサイクルでの注意点 文献[6] より

収集	<ul style="list-style-type: none"> - 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	<p>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。</p>
報告	<p>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</p>
決定	<p>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</p>

	<p>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。</p>
配布	<p>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。</p> <ul style="list-style-type: none"> - 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	<p>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</p> <ul style="list-style-type: none"> - 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に立たない - 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

3.7 IT ガバナンスの原則とモデルの適用

データの利活用に IT ガバナンス原則をあてはめると表 3.8 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 3.8 IT ガバナンスの原則の適用 (文献[6]を加筆修正)

<p>原則 1:責任 (Responsibility) の対象について</p> <ul style="list-style-type: none"> - 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
<p>原則 2:戦略 (Strategy)</p> <ul style="list-style-type: none"> - 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
<p>原則 3:取得 (Acquisition)</p> <p>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</p>

<p>び管理において、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</p> <p>原則 4: パフォーマンス (Performance)</p> <ul style="list-style-type: none"> - データがサプライ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 <p>原則 5: 適合性 (Conformance)</p> <ul style="list-style-type: none"> - 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 <p>原則 6: 人間行動 (Human Behaviour)</p> <ul style="list-style-type: none"> - 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 - ステークホルダーの人間行動の影響と要件

<p>タ</p> <p>用と管理が内部ポリシーや規制やデータステewardシップ要件などの外部要件に準拠していること</p> <p>監督が重要となる分野には、</p> <ul style="list-style-type: none"> - 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

EDM のモデルの適用にあたっては、表 3.8 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。とくに、モニタの機能については、ISO の具体的な規格の採用について具体的に述べられている。

表 3.8 IT ガバナンスの EDM モデルの適用 (文献 [6] を修正)

外部圧力	<ul style="list-style-type: none"> - 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ー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	<p>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</p> <ul style="list-style-type: none"> - 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 <p>- 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</p> <p>組織のデータ管理能力の認識</p> <ul style="list-style-type: none"> - 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られることができるか。 - 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 <p>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</p>
指示	<ul style="list-style-type: none"> - 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テeward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。 <p>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</p>
モニタ	<p>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</p>

3.8 説明責任マップについて

ISO/IEC38505-1 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 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 2 つから検討しなおしている。

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)。

なお、IT ガバナンス (ISO/IEC385000[5]) では、原則やモデルは述べているものの、陽に説明責任の実施については触れられていない。そこで、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)。

表 3.9 - データの説明責任マップ (文献 [6] 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	[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	[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ります

		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嗜好度を越えることがないように実施することを、指示する必要がある	[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
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と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、データの安全かつ持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

3.9 データガバナンスを GDPR の準備に役立てる

ISO/IEC38505-1 のデータガバナンスの規格では、広範なデータに関するライフサイクルの観点から全てのプロセスでデータが生む価値とリスク及び契約や法令などの制約を表 3.9 の説明責任マップに網羅的に展開している。したがって、データを取り扱うために必要なものは全て揃っていると考えられる。すなわち、GDPR は、個人データに関するものであり、理論的にはデータガバナンスが GDPR の要請する説明責任を包含していると考えられる。

したがって、組織が GDPR への対応の準備として、ISO/IEC38505-1 を活用出来ると考えられる。

ただし、ISO/IEC38505-1 の規格化にあたって、直接に GDPR を対象とできないため、GDPR が要請している説明責任全てと言えるかは不明である。例えば、データポータビリティや個人データの削除権について、データのライフサイクルでは含まれていない。データポータビリティや削除については、個人の観点からのものであり、組織の観点から作成されているライフサイクルには本来含まれない。利用者からの要請で削除するものであり、データガバナンス規格が想定する削除のプロセスだけではない。全ての関連するプロセスにおいて、利用者の視点を入れる必要があるからである。

4. 結論と残された課題について

4.1 ISO/IEC38505-1 について

ISO/IEC38505-1 のデータガバナンスの規格は、3.9 節に述べたように、個人データを取り扱う組織が GDPR の準備として活用することができると考えられる。ただし、あくまでも、データを対象とした規格であり、陽に GDPR の求める個人データの管理と一致すると言えない。準備としての必要条件を満たしていると考えられるが、GDPR が要請している十分性を満たすかは分からない。

4.2 説明責任マップについて

ISO/IEC38505-1 のデータガバナンスの規格の説明責任マップについては、組織及び経営者に要請されるデータの説明責任としては、具体的に述べられており、データガバナンスが十分でないとする組織にとっては十分に役立つものと考えられる。なお、データガバナンスの規格のケーススタディ編として ISO/IEC TR38505-2 が作成中であり、2017 年末には出版される。説明責任マップをどのように適用するかが分かるので、これを活用するとよいであろう。

4.3 残された課題

ISO/IEC38505-1 のデータガバナンスの規格を日本の改正個人情報保護法や JIS Q15000 に使えるのかの検討が残されている。継続検討していく予定である。

5. 謝辞

本研究にご協力を頂きました ISO/IEC JTC1 SC40 の委員会メンバー及び日本の国内委員会メンバー、EIP 研究会の皆様様に感謝いたします。さらに温かい指導を頂いた情報セキュリティ大学院大学の教授、同僚、事務の皆様様に感謝いたします。

6. 参考文献

- [1] 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
- [2] 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
- [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(実践編), 2017 年
- [4] 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
- [5] ISO/IEC 38500:2013, Governance of IT, 2013 年, (JIS Q38500:2014, IT ガバナンス, 2014 年)
- [6] ISO/IEC38505-1:2017, Governance of Data, 2017 年