データガバナンスの背景と新規格 ISO/IEC38505-1「データガバナンス」について

情報セキュリティ大学院大学　教授
JTC1/SC40 専門委員会委員　ＷＧ1 主査
原田　要之助　氏

1.国際標準化制定の背景

ISO/IEC38505-1 制定の背景には、2018 年 5 月に適用される EU の「GDPR（General Data Protection Regulation)」が関係している。

GDPR はあらゆる業種、EU 加盟国の全組織、EU 市民を対象に事業展開している域外企業が対象となり、特に個人情報保護に関しては違反した場合の多額の罰金、アカウンタビリティの義務づけ、PIA 調査の義務づけ、漏えい時の通知義務、忘れられる権利、データポータビリティの権利など、該当企業にとってかなり厳しい制度となる。

GDPR は直接「データガバナンス」について触れてはいないが、GDPR が求める以下の要請を遵守するために経営層が行うべきことを ISO/IEC38500 で対応できないか、との議論が SC40 で出され、ISO/IEC38505-1「データガバナンス」の規格が 2017 年 5 月に制定された。

GDPR の要請事項は次のとおり。

・個人情報を扱う場合、組織による対応メカニズム、経営判断が必要
・個人情報取扱いの説明責任を追及
・組織的なインシデント対応を要請
・個人情報取扱いのための PIA の実施、プライバシー・バイ・デザインによるマネジメントシステムの構築が求められている

組織が GDPR による「アカウンタビリティ」を求められた際には、「ISO/IEC38505-1 に述べている組織体制をとっており、規格に適応しているから GDPR のいう説明責任や組織体制はできている」ということを示せると考えている。

2.ISO/IEC38505 について

ISO/IEC38505「データガバナンス」は 2 部構成からなり、2017 年 5 月にパート 1 が公表された。本規格を適用した事例集としてパート 2 があるが、2017 年 11 月現在最終投票中であり、今後各国のコメントを受け最終化することとなる。

ここでは ISO/IEC38505-1 の規格内容について紹介する。

2017 年 10 月 20 日開催 第 67 回 JIPDEC セミナー「IT ガバナンスの国際標準化（ISO/IEC3850 シリーズ）の最新動向とデータガバナンスについて」

なお、今回紹介する日本語訳は原田講師が個人的に解釈・翻訳したものである。

本規格は、①経営者が実施すべきガバナンスのタスク、②経営者が従うべき原則、③データを利活用する際の特殊性を規格化したもので、章構成は図 1 のとおりである。

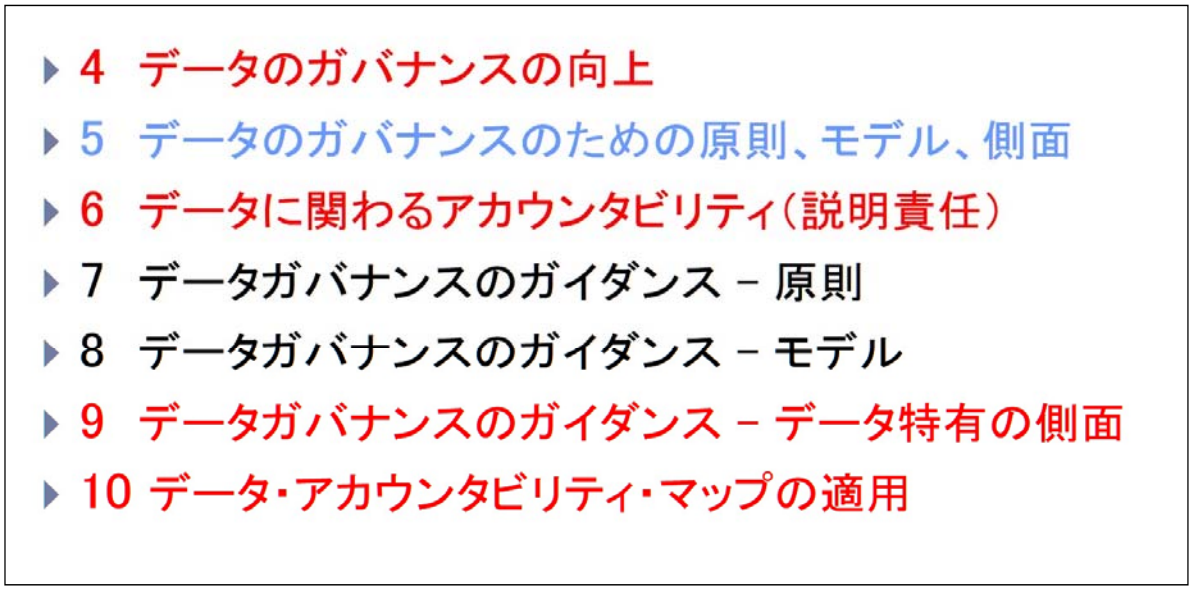


図 1.ISO/IEC38505-1「データガバナンスの章構成（ISO/IEC 38505-1:2017 より）

以下、主要な各章の内容について説明する。

（1）「4.データのガバナンスの向上」

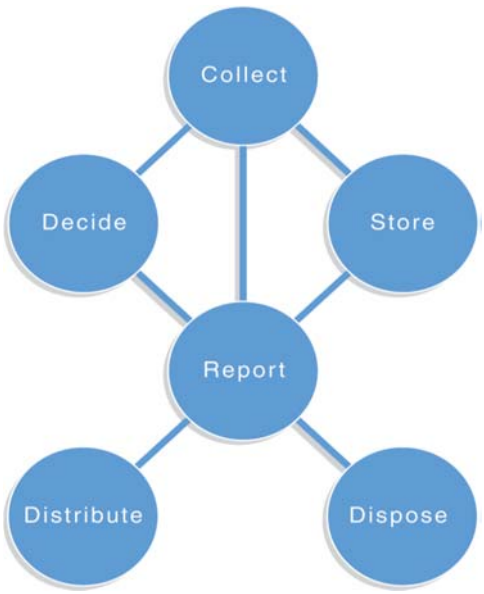
データガバナンスの利点はどこにあるのか？を一般論として説明したものである。利点は次のとおり。

・データガバナンスを実践することにより、データ資産の適切な導入と運用、保護と潜在的な価値の可能性の両方の責任と説明責任と明快さが確保できる。
・経営者（Governing Body）の責任としては、データの利活用のための権限、責任および説明責任が生じる。
・組織がリスクを管理し、制約を考慮しながらデータおよび関連する IT 投資から価値を得られる。
・効果的なマネジメントシステムを作り、経営者がガバナンスすべき

なお、データガバナンスの実践にあたっては、ガバナンスのほかに監督（Oversite）のメカニズムが必要となるとともに、データ特有の側面を考慮する必要がある。

（2）「6.データに関わるアカウンタビリティ（説明責任）」

データはライフサイクルで管理する必要があり、データモデルを図 2 のように定義した。



①収集（Collect）
②保存（Store）
③報告（Report）
④決定（Decide）
⑤配布（Distribute）
⑥廃棄（Dispose）

図 2.データモデル（ISO/IEC 38505-1:2017 より）

（3）「7.データガバナンスのガイダンス－原則」

ここでは、原則と責任、戦略、調達、パフォーマンス、適合、人間行動について説明している。

①責任	データのライフサイクル全体をカバーする必要がある
②戦略	・現在および将来の全体的な戦略目標に取り組むデータ利用計画を考慮する ・データ・アカウンタビリティ・マップを組織で規定し、すべての部分をカバーする ・ガバナンスのデータ特有の側面（価値、リスク、制約）を考慮する
③調達	データを外部から調達する場合も含め、データ配布に関し、組織内で意図して利活用する
④パフォーマンス	・データ利活用が組織内の意思決定をどの程度サポートしているかを確認する。 ・データがサプライヤや顧客と共有されている場合、データ利活用が意思決定をどれだけサポートしているかを確認する ・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率　等
⑤適合	・PII の正しい処理 ・組織のニーズと義務を満たすセキュリティポリシーに従って、すべてのデータセットとデータストリームを保護する ・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かを保証する

⑥人間行動	・組織全体で許容されるデータとデバイスの利活用を管理するポリシーの策定 ・ステークホルダーの人間行動の影響と要件 ・組織の人がきちんと理解し、文化的にデータを利活用しなければならない

(4)「データガバナンスのガイダンス－モデル」

データは EDM モデル（①評価（**E**valuate）②指示（**D**irect）③モニタ（**M**onitor）を適用して管理する必要がある。

・現在と将来の IT の利用について評価する（Evaluation）

・IT の利用が組織のビジネス目標に合致するよう、計画とポリシーを策定し、実施する（Direct）

・ポリシーへの準拠と計画に対する達成度をモニタする（Monitor）

また、外部圧力があることを理解していなければならない。たとえば、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ことを理解することが必要である。

戦略や規制に対しては以下の点を考慮する必要がある。

・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 の活用（ISO/IEC 29100 参照）。

・データの戦略的重要性を反映する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）の活用。クラウドコンピューティングサービス（たとえば、ISO/IEC 27017）における第 3 者データフィードおよびデータ管理を含むように拡張されるべきである

・データ保存および処分の要件

・データの再利用、共有または販売、ならびにその関連する権利、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する

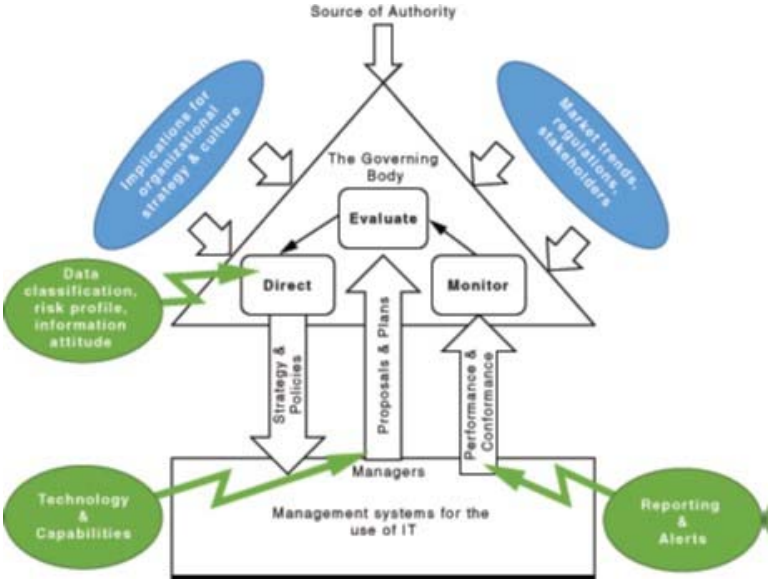


図 3. データガバナンスモデル（ISO/IEC38505-1：2017 より）

（4）「10.データ・アカウンタビリティ・マップの適用」

組織として何を行うべきかを明確にするため、「データ・アカウンタビリティ・マップ」を作成する。これはデータのライフサイクルを縦軸に、それぞれの段階での価値、リスク、制約を示したもので、ガバナンスフレームワークを開発する際に考慮しなければならない包括的なガイダンスとなる。

なお、これらの行動はすべて経営者（Governing Body）が命令し、組織での状況を評価し、必要に応じて行動を追加する必要がある。

	価値	リスク	制約
収集	[V1] 取締役会は、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ります。	[R1]取締役会は、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ります。	[C1] 取締役会は、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。
保存	[V2]取締役会は、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ります。	[R2]取締役会は、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を、指示する必要があります。	[C2] 取締役会は、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]取締役会は、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]取締役会は、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] 取締役会は、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]取締役会は、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ります。	[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、取締役会は、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、取締役会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]取締役会は、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]取締役会は、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ります。	[C5]取締役会は、適切な配権限が行使され、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ります。
廃棄	[V6]取締役会は、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]取締役会は、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ります。	[C6]取締役会は、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。

図 4.データ・アカウンタビリティ・マップ（ISO/IEC38505-1：2017 より）

2017 年 10 月 20 日開催 第 67 回 JIPDEC セミナー「IT ガバナンスの国際標準化（ISO/IEC3850 シリーズ）の最新動向とデータガバナンスについて」

3.最後に

本規格は前述のとおり、GDPR を意識し、本規格の実践が GDPR の遵守につながる、として制定された国際規格である。GDPR の適用開始は 2018 年 5 月のため、本規格と必ずしも合致しない可能性があるが、概念はカバーしていると確信している。

組織としてデータ・アカウンタビリティを保証するために何をすべきか、をとりまとめたのが本規格 ISO/IEC38505-1 である。